Wireless Network

There are two types of wireless networks:

Ad Hoc and Infrastructure

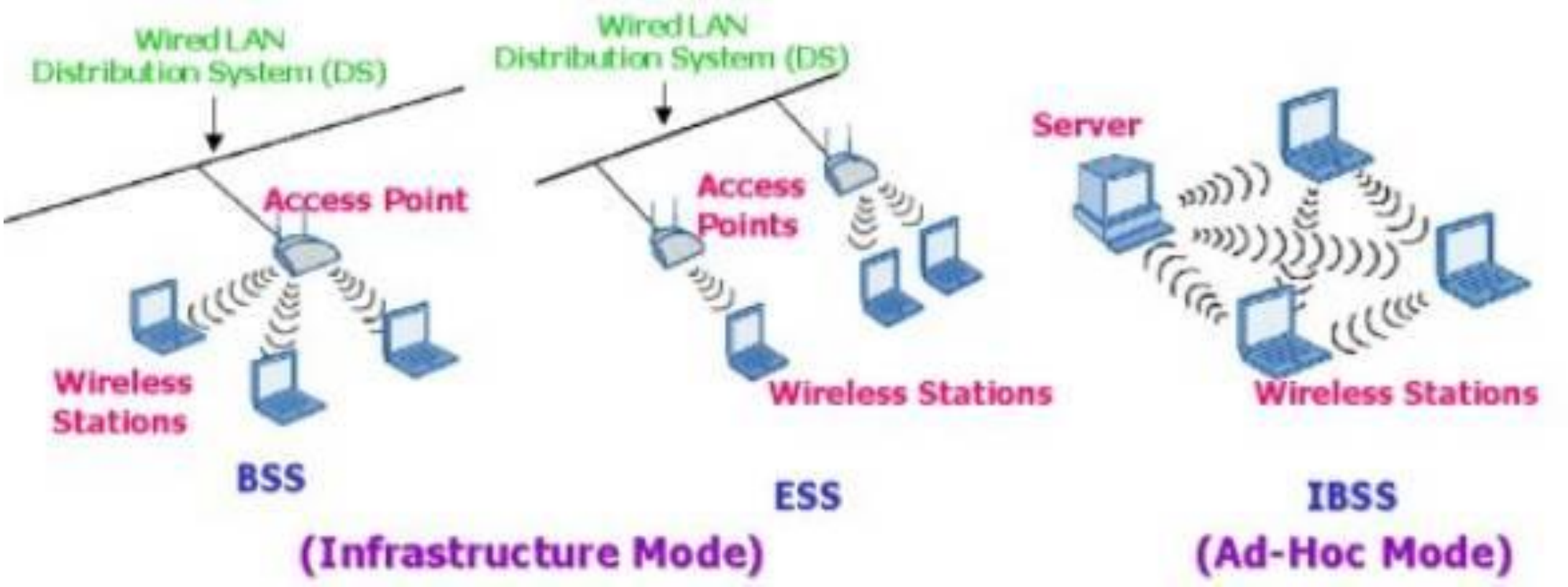
Ad Hoc: Mobile clients connect directly **without an intermediate access point**.

Operating systems such as Windows have made this peer-to-peer network easy to set up.

Infrastructure networks contain special nodes called **access points (APs)**.

APs are connected via existing networks.

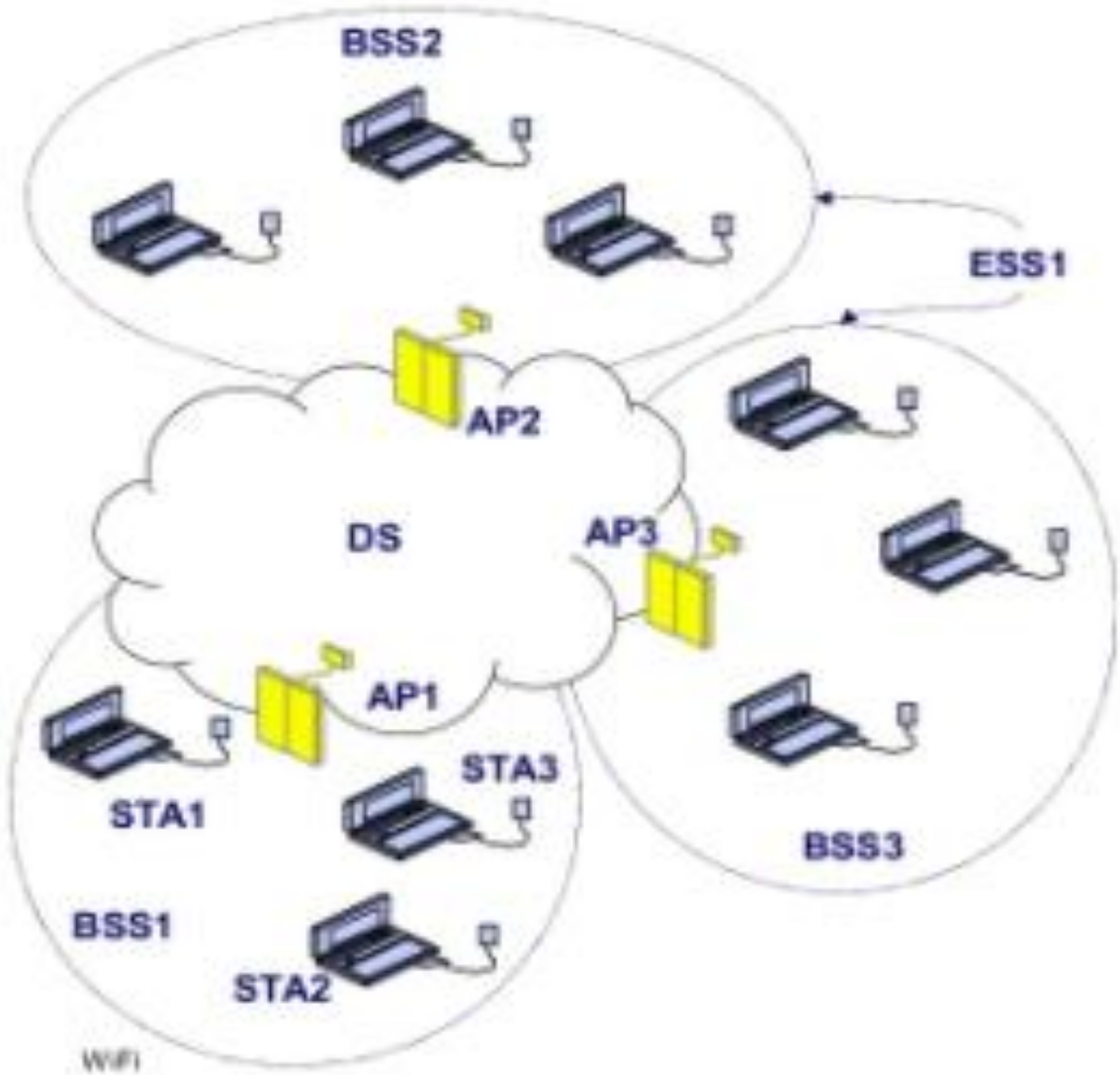
APs can interact with wireless nodes and existing wired network.


Wired LAN
Distribution System (DS)
Access Point
Wireless
Stations
BSS
Wired LAN
Distribution System (DS)
Access
Points
Wireless Stations
ESS
(Infrastructure Mode)
Server
Wireless Stations
IBSS
(Ad-Hoc Mode)

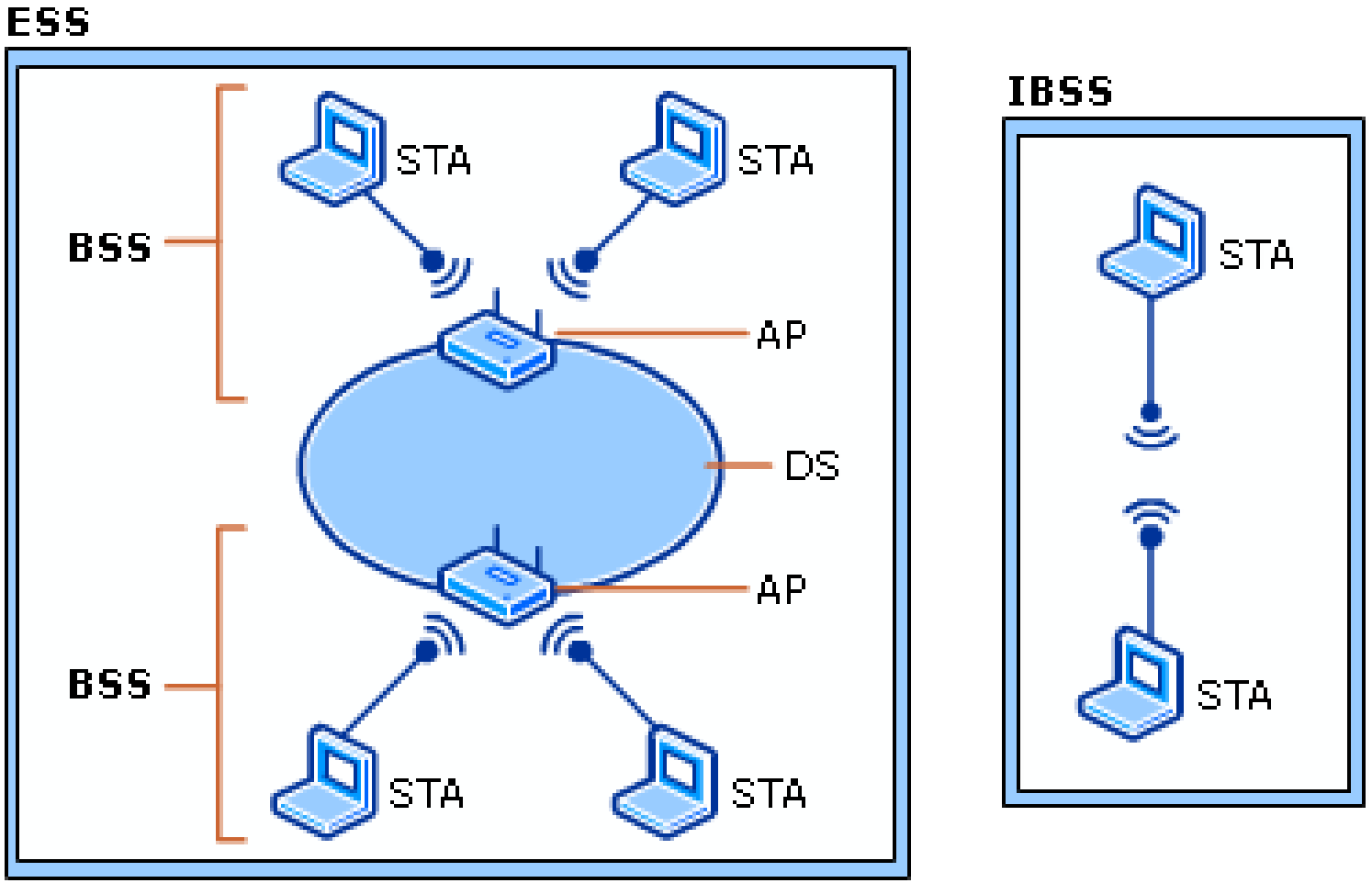
BASIC COMPONENT OF WIRELESS NETWORK

How to connect a wi-fi device…?

- Stations (STA)
  - any wireless device
- Access Point (AP)
  - connects BSS to DS
  - controls access by STA's
- Basic Service Set (BSS)
  - a region controlled by an AP
  - mobility is supported within a single BSS
- Extended Service Set (ESS)
  - a set of BSS's forming a virtual BSS
  - mobility is supported between BSS's in an ESS
- Distribution Service (DS)
  - connection between BSS's



BASIC COMPONENT OF WIRELESS NETWORK

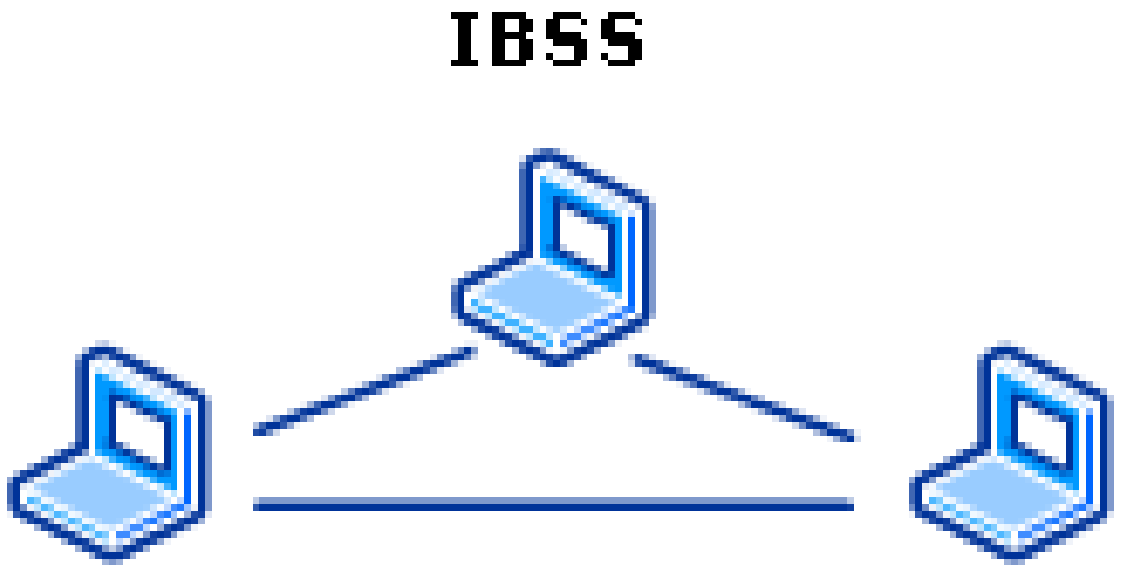


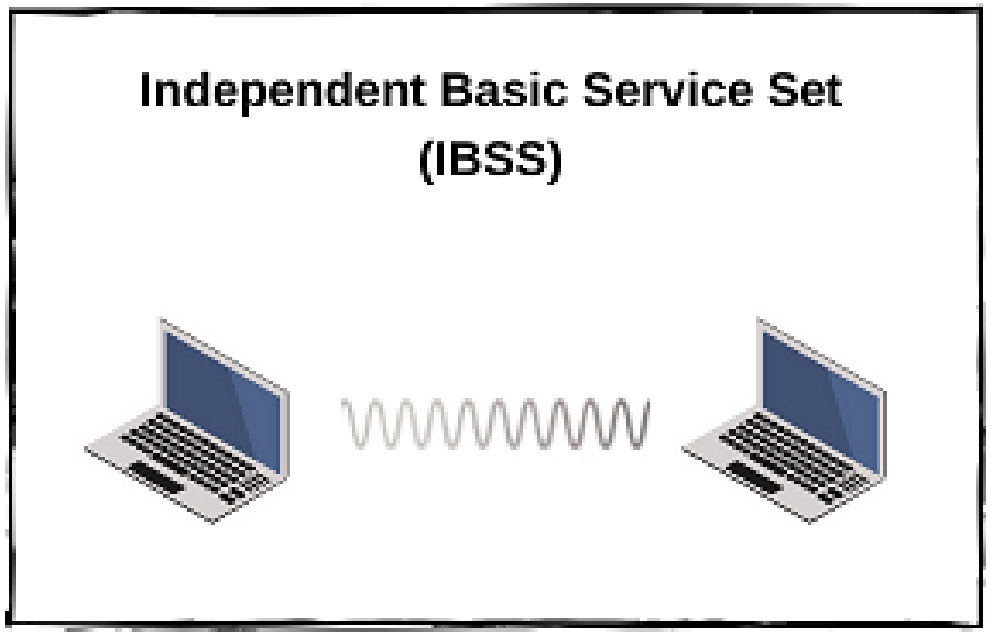
Independent Basic Service Set (IBSS) :

Two or more wireless devices connect directly **without an access point (AP)** also called as an **ad hoc network.**

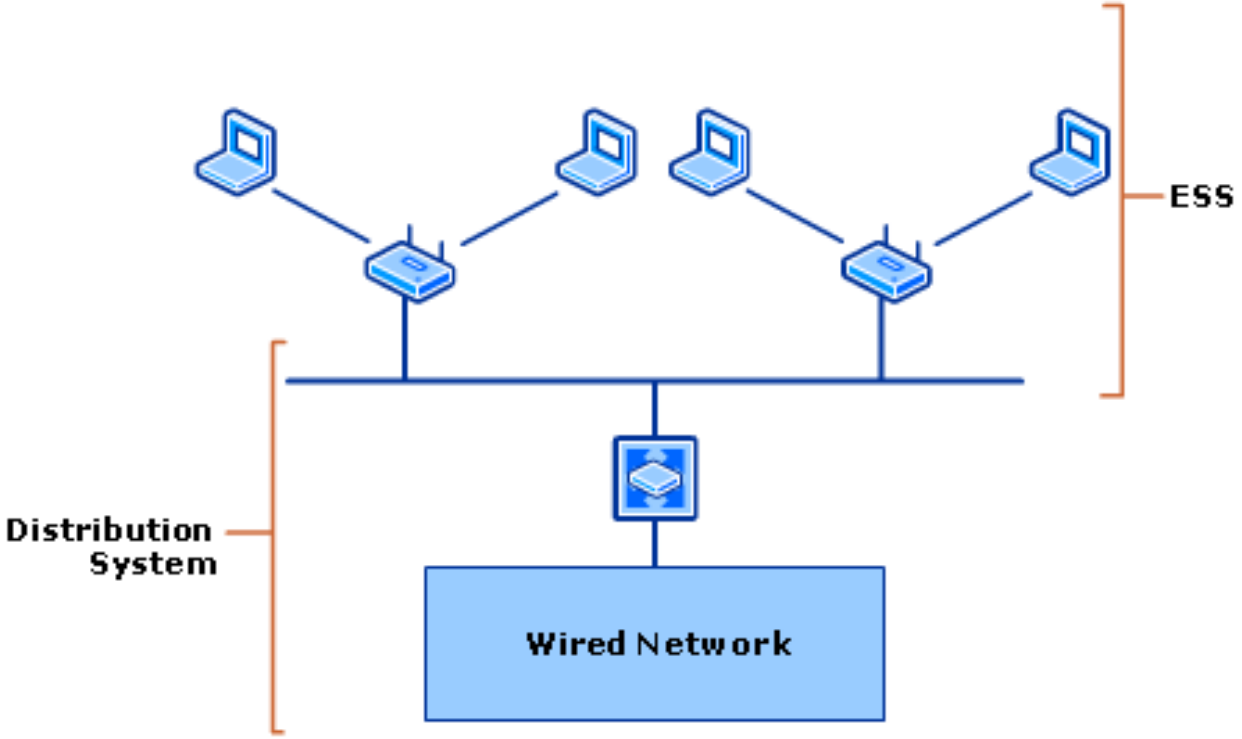
One of the devices has to start and advertise an SSID, similar to what an AP would do.

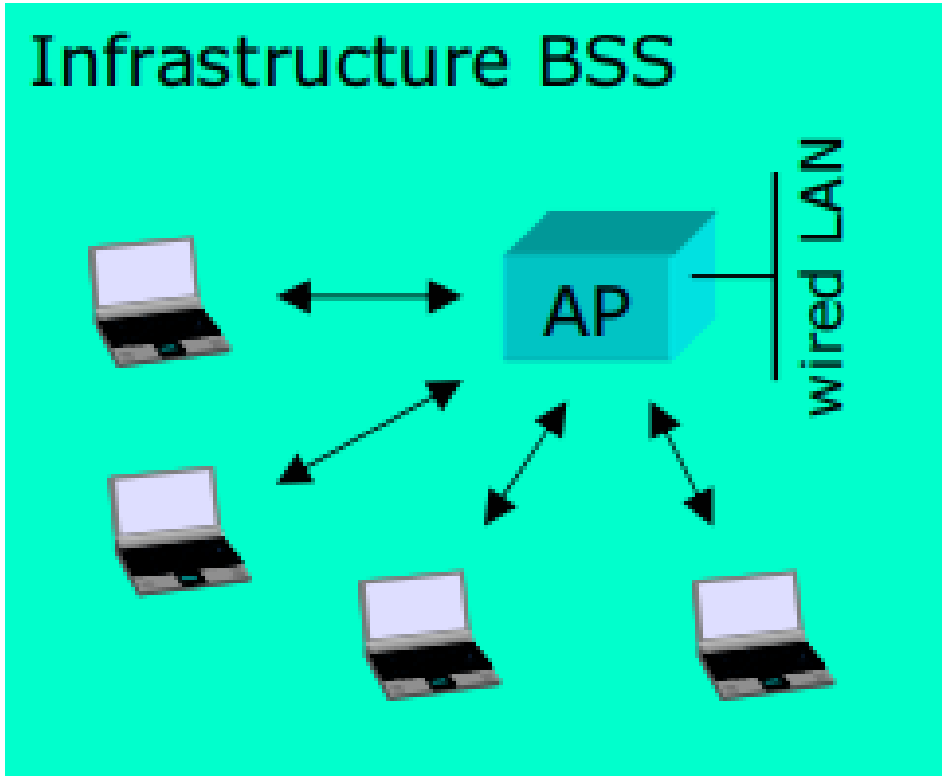
Other devices can then join the network.





Infrastructure Mode





Infrastructure Mode

In infrastructure mode, we connect all wireless devices to a central device called as AP.

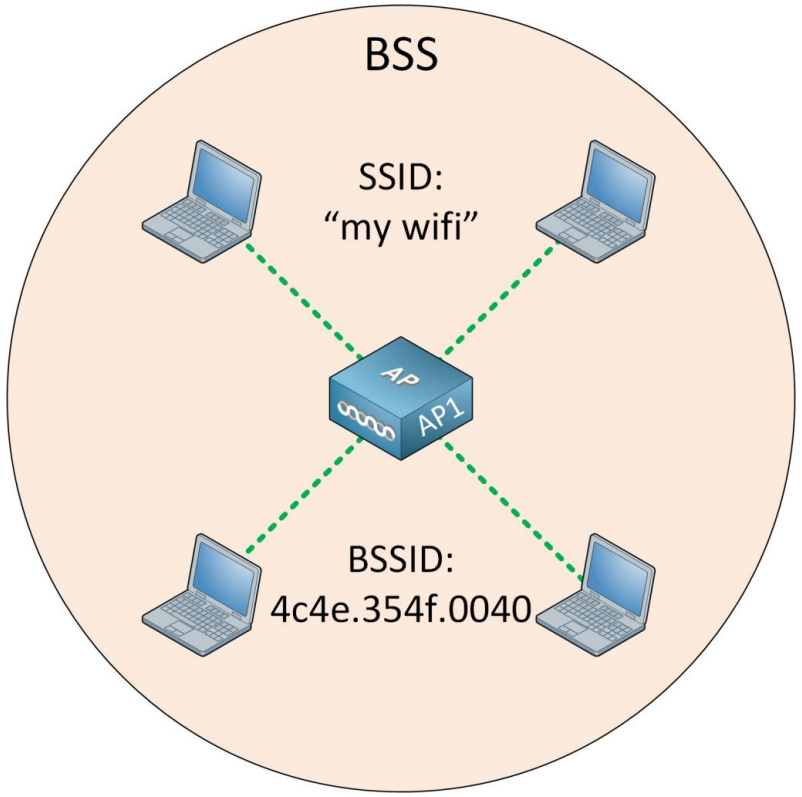
All data goes through the AP.

Basic Service Set (BSS)

With a Basic Service Set (BSS), wireless clients connect to a wireless network through an AP.

Each wireless client advertises its capabilities to the AP, and the AP grants or denies permission to join the network.

The AP and its wireless clients use the same channel to transmit and receive.



The **SSID** is the name of the wireless network

The AP also advertises the Basic Service Set Identifier **(BSSID)**.

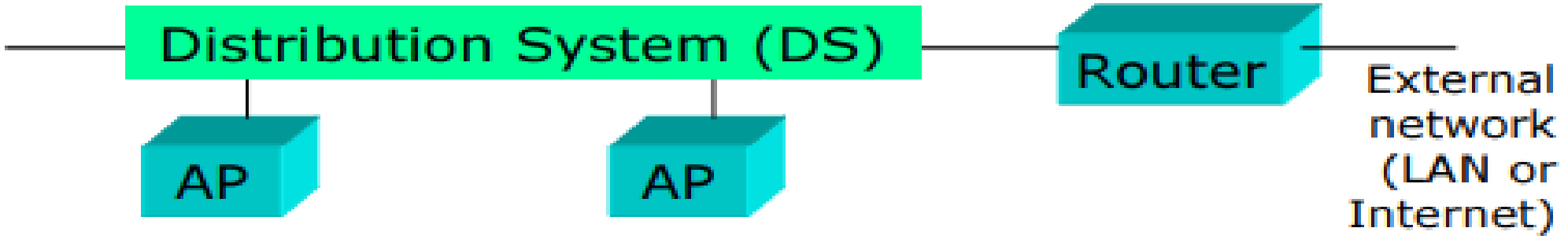
BSSID is the **MAC address of the AP’s radio**, a unique address that identifies the AP.

All wireless clients have to connect to the AP.

This means the AP’s signal range defines the size of the BSS called as the Basic Service Area (BSA).

Distribution system

This is the mechanism by which APs and other nodes in the wired IP subnetwork communicate with each other.



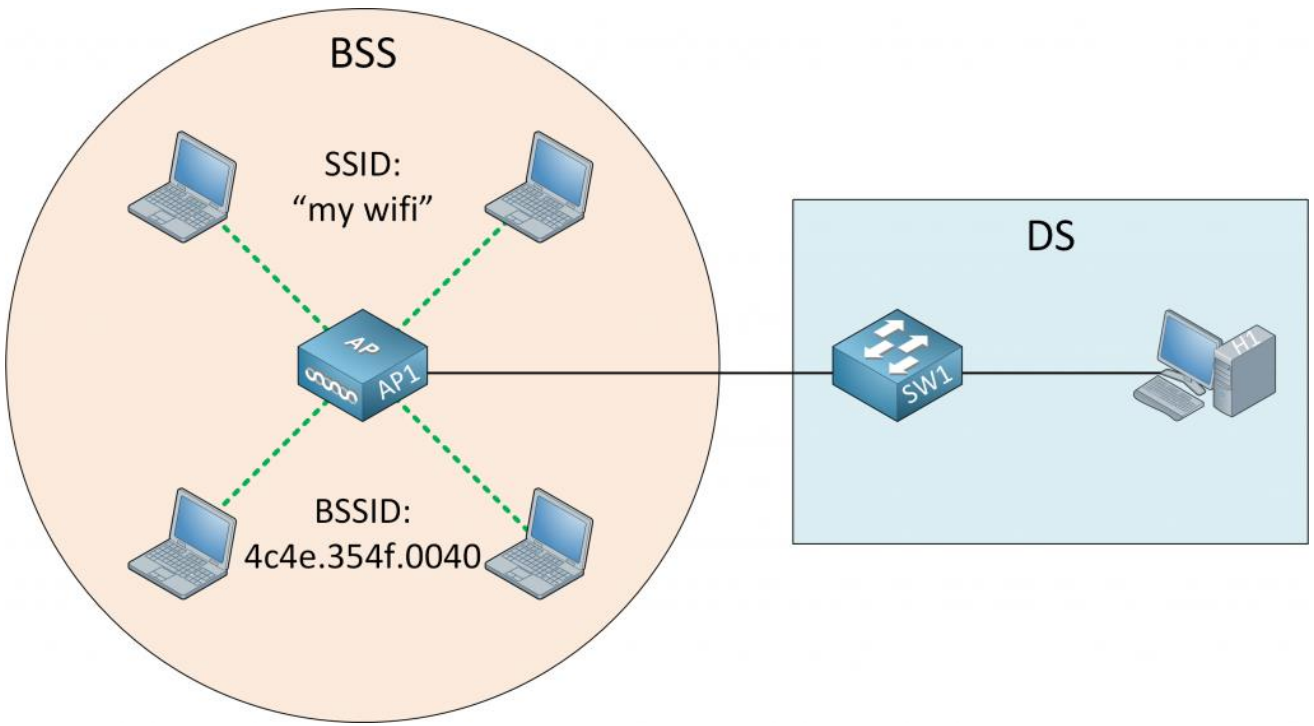
Distribution System (DS)

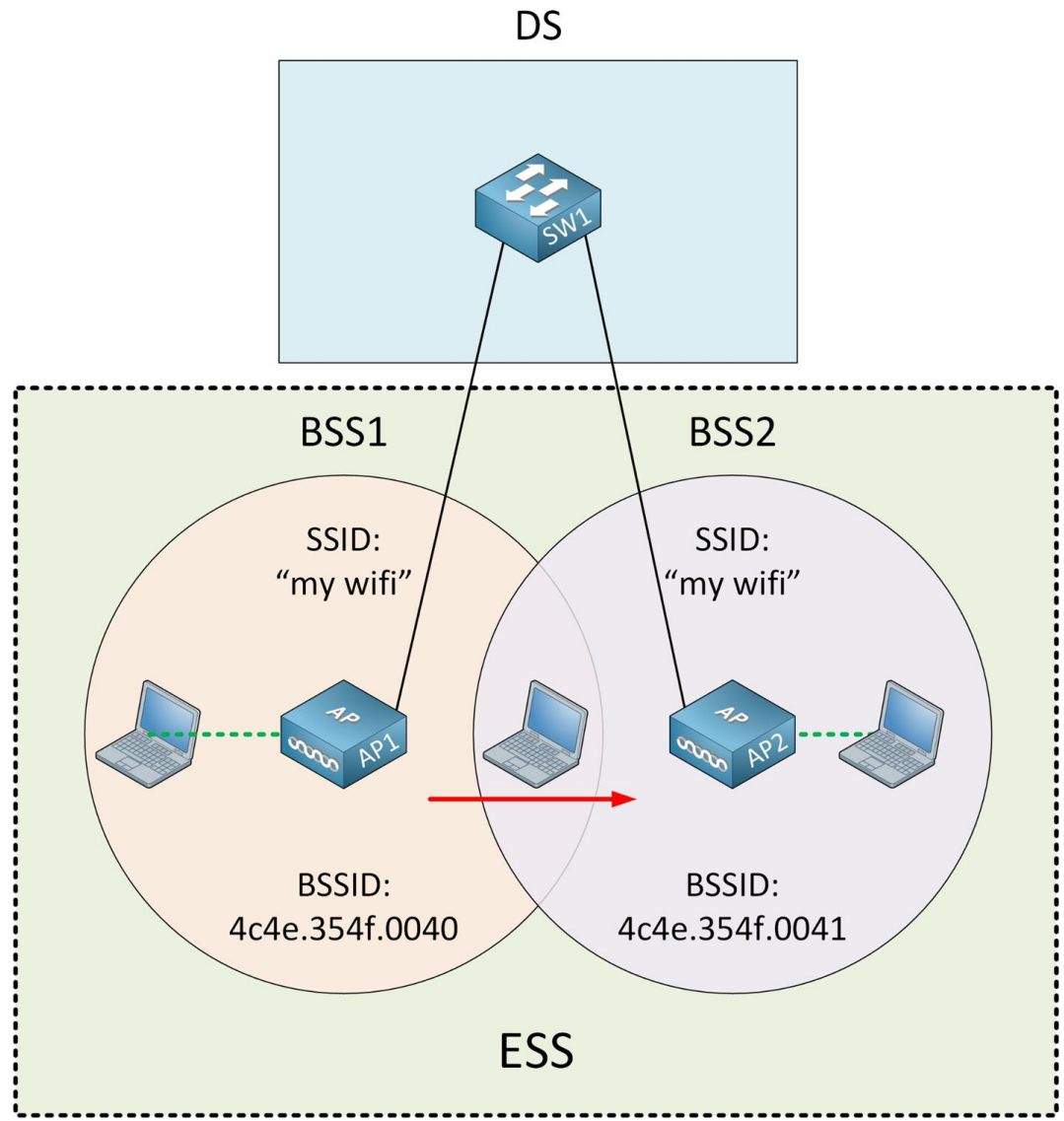
A BSS is a standalone network with a single AP.

Most wireless networks, however, are an extension of the wired network.

An AP supports both wired and wireless connections.

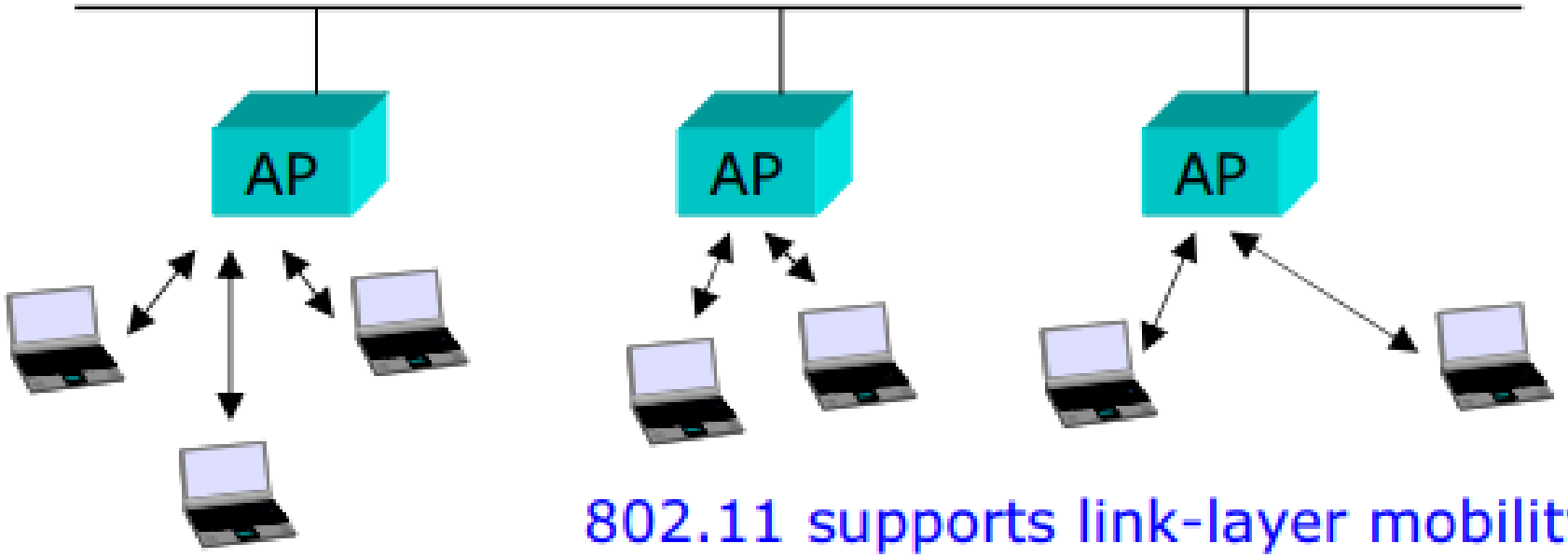
The AP bridges the wireless and wired L2 Ethernet frames, allowing traffic to flow from the wired to the wireless network and vice versa.


BSS
SSID:
“my wifi”
AP
AP1
BSSID:
4c4e.354f.0040
DS
SW1
H1

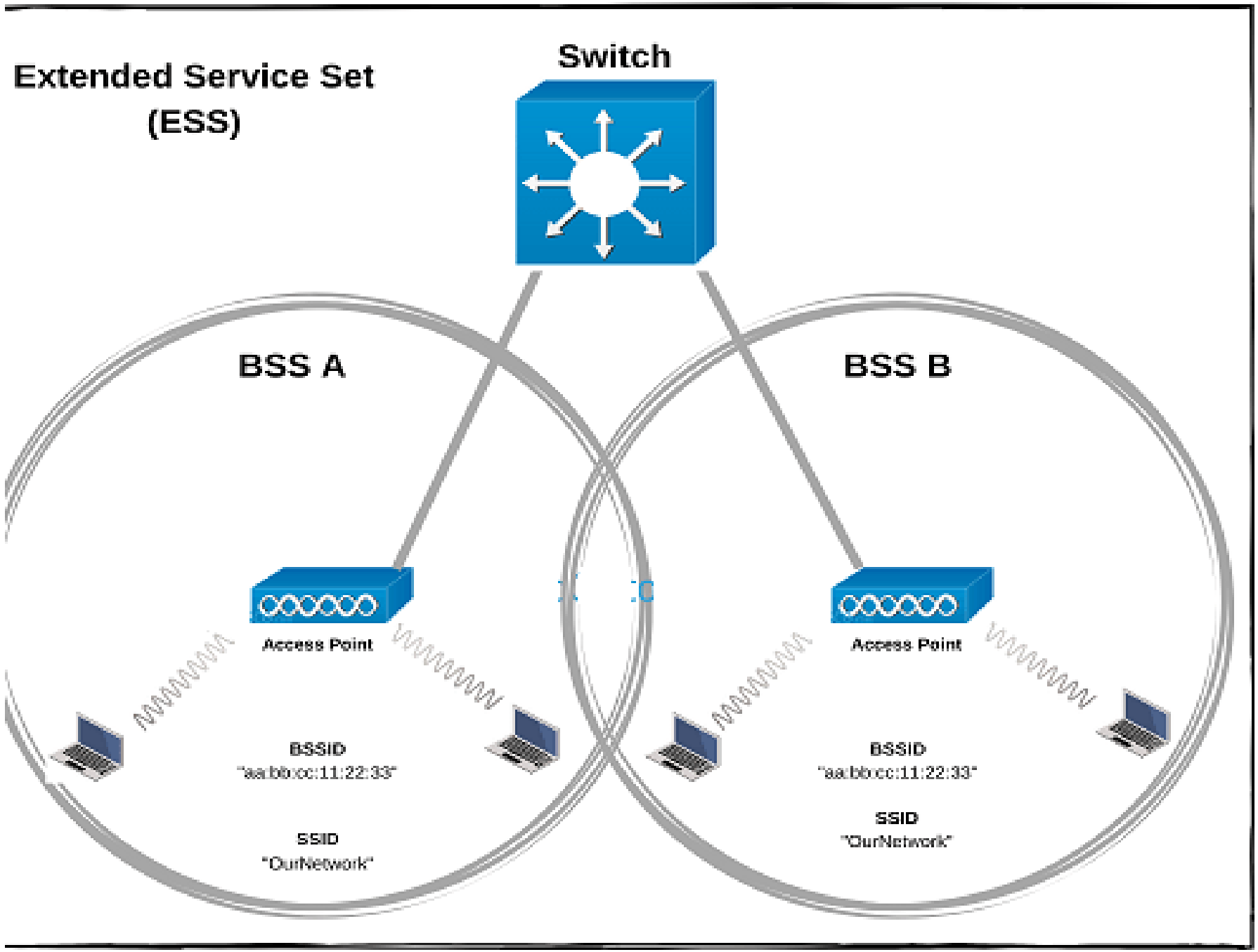

DS
SW1
BSS1
BSS2
SSID:
“my wifi”
SSID:
“my wifi”
AP
AP1
AP
AP2
BSSID:
4c4e.354f.0040
BSSID:
4c4e.354f.0041
ESS

Extended Service Set (ESS)

This is a larger WLAN network consisting of a number of BSS networks interconnected via a common backbone



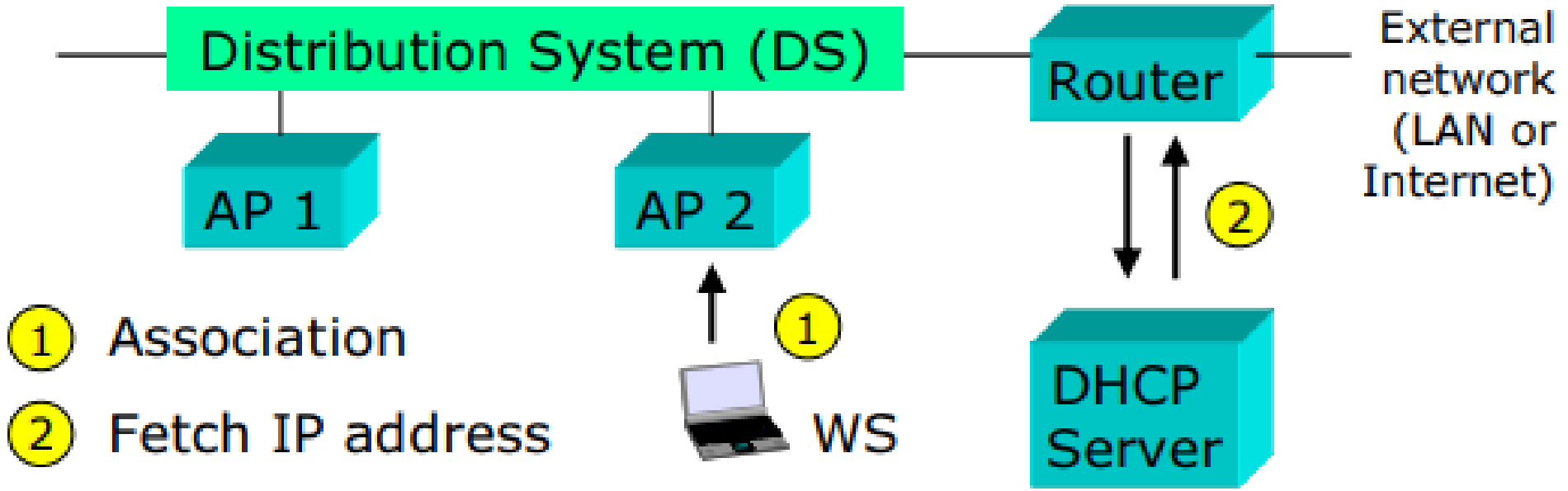
802.11 supports link-layer mobility within an ESS (but not outside the ESS)


Extended Service Set
(ESS)
Switch
BSS A
BSS B
Access Point
Access Point
BSSID
"aa:bb:cc:11:22:33"
SSID
"OurNetwork"
BSSID
"aa:bb:cc:11:22:33"
SSID
"OurNetwork"

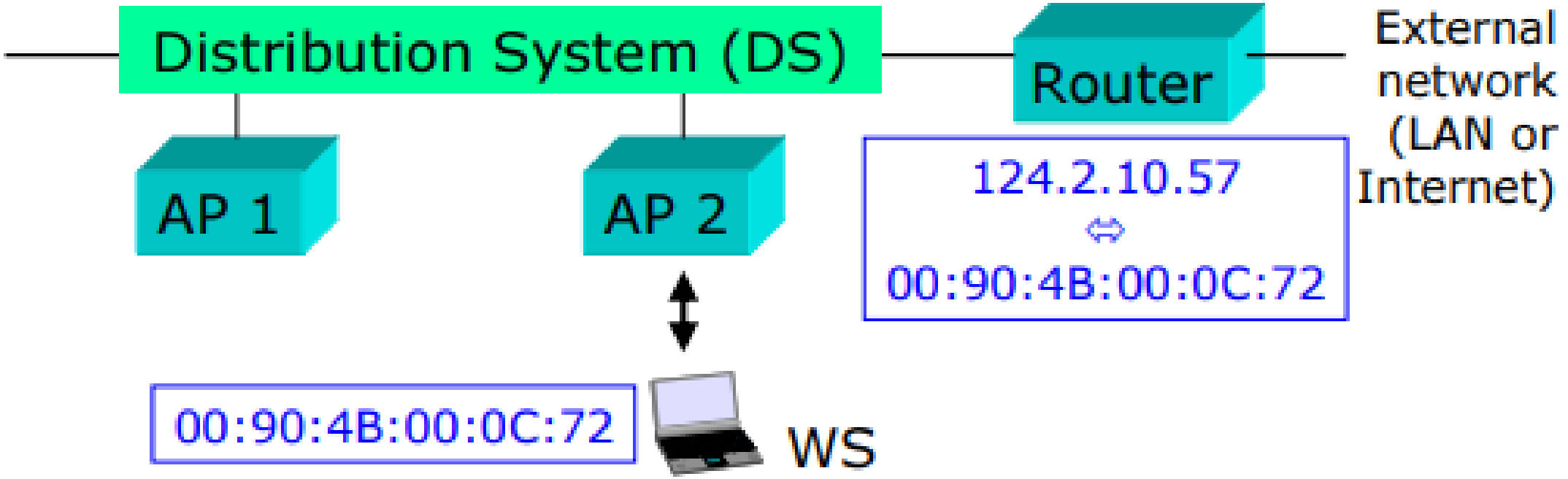
Mode	Service Set Name	Description
Ad hoc	Independent Basic Service Set (IBSS)	Allows two devices to communicate directly. No AP is needed.
Infrastructure (one AP)	Basic Service Set (BSS)	A single wireless LAN created with an AP and all devices that associate with that AP.
Infrastructure (more than one AP)	Extended Service Set (ESS)	Multiple APs create one wireless LAN, allowing roaming and a larger coverage area.

Basic routing example

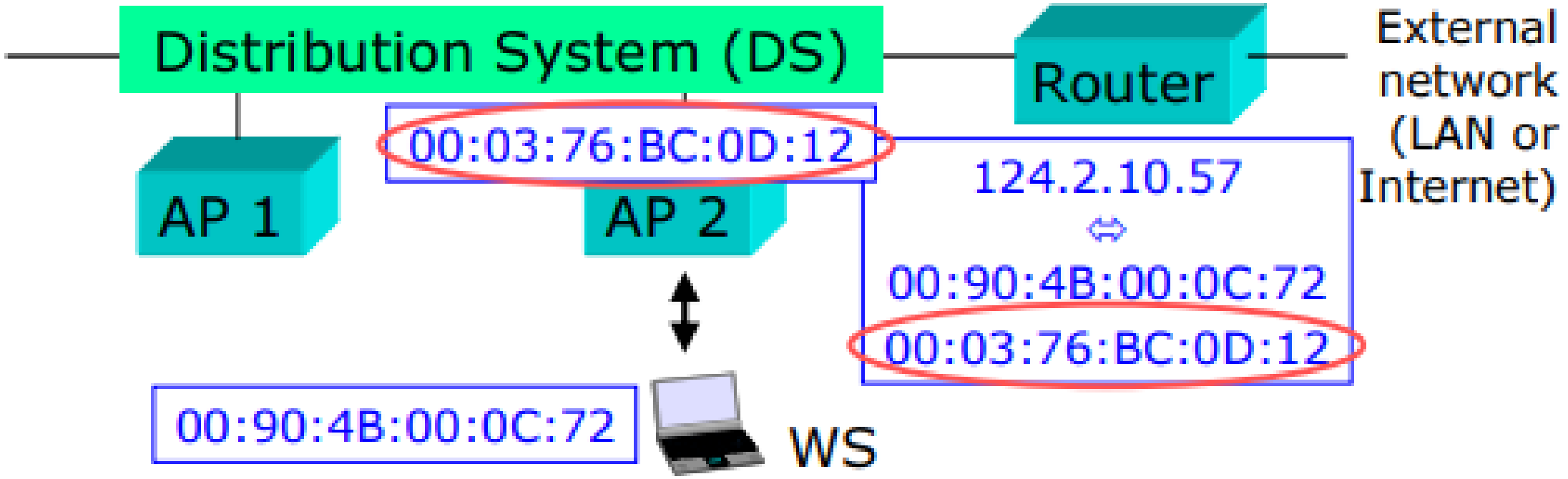
When WS associates with AP 2, the router in charge of the IP subnet addressing obtains an IP address from the DHCP (Dynamic Host Configuration Protocol) server.



The router must maintain binding between this IP address and the MAC address of the wireless station.



The router must also know (and use) the MAC address of the access point via which the packets must be routed. For this purpose, a special protocol (IAPP) is needed!



- Association
  - Establishes initial association between station and AP
- 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

- **Association:**

The identity of an **STA** and its address should be known to the **AP** before the STA can transmit or receive frames on the WLAN.
This is done during association, and the information is used by the AP to facilitate routing of frames.

- **Reassociation**:

The established association is transferred from one AP to another using reassociation.

This allows STAs to move from one BSS to another.

- **Disassociation**:

When an existing association is terminated, a notification is issued by the STA or the AP.

This is called disassociation and is done when nodes leave the BSS or when nodes shut down.

- **Distribution**:

  Distribution takes care of routing frames.

  If the destination is in the same BSS, the frame is transmitted directly to the destination, otherwise the frame is sent via the DS.

- **Integration**:

  Non-IEEE 802.11 networks, which may have different addressing schemes or frame formats

  To send frames through such non-IEEE 802.11 networks, the integration service is invoked.

- **Authentication**:

  Authentication is done in order to establish the identity of stations to each other.

  The authentication schemes range from relatively insecure handshaking to public-key encryption schemes.

- **Deauthentication**:

  Deauthentication is invoked to terminate existing authentication.

- **Privacy**:

  The contents of messages may be encrypted to prevent eavesdroppers from reading the messages.

• **Data delivery**:

IEEE 802.11 provides **a way to transmit and receive data**.

But the transmission is not guaranteed to be completely reliable.

Nodes in an ad hoc wireless network **share a common broadcast radio channel**.

The radio spectrum is limited, So the bandwidth available for communication in such networks is also limited.

Access to this shared medium should be controlled.

All nodes must receive a fair share of the available bandwidth

The bandwidth must be utilized efficiently.

The characteristics of the wireless medium are different from the wired medium

So ad hoc wireless networks need to address unique issues.

This includes node **mobility, limited bandwidth availability, error-prone broadcast channel, hidden and exposed terminal problems, and power constraints**

These issues are not applicable to wired networks

So, a different set of protocols is required for controlling access in ad hoc networks.

Problems in Ad Hoc Channel Access- Issues and need

- **Distributed operation**
  - Fully distributed involving minimum control overhead
- **Synchronization**
  - Mandatory for TDMA-based systems
- **Hidden terminals**
  - Can significantly reduce the throughput of a MAC protocol
- **Exposed terminals**
  - To improve the efficiency of the MAC protocol, the exposed nodes should be allowed to transmit in a controlled fashion without causing collision to the on-going data transfer
- **Access delay**

Wireless Link Characteristics

Decreased signal strength:

Radio signal attenuates as it propagates through matter (e.g.. **a radio signal passing through a wall**).
Even in free space, the signal will disperse, resulting in decreased signal strength (sometimes referred to as path loss) as the distance between sender and receiver increases.

Interference from other sources :

Standardized wireless **frequencies** (eg. 2 2.4 GHz) **shared by other devices** (eg. phone); devices (motors, a microwave) interfere re as as well

Multipath propagation :

Radio signal reflects off objects/ground, reaching destination at slightly different times as it takes paths of different lengths between a sender and receiver.

This results in the blurring of the received signal at the receiver.

Moving objects between the sender and receiver can cause multipath propagation to change over time.

Bit errors will be more common in wireless links than in wired links which make communication across (even a point to point) wireless link much more "difficult"

SNR: signal-to-noise ratio

This host receives an electromagnetic signal that is a combination of a degraded form of the original signal transmitted by the sender **(degraded due to the attenuation and multipath propagation effects) and background noise in the environment.**

The signal-to- noise ratio (SNR) is a relative measure of the strength of the received signal (i.e., the information being transmitted) and this noise.

The SNR is typically measured in units of decibels (dB).

larger SNR-easier to extract signal from noise

For a given modulation scheme, **the higher the SNR, the lower the BER.**

Since a sender can increase the SNR by increasing its transmission power, a sender can decrease the probability that a frame is received in error by increasing its transmission power.

There are also disadvantages associated with increasing the transmission power:
More energy must be used by the sender (an important concern for battery- powered mobile users), and the sender's transmissions are more likely to interfere with the transmissions of another sender.

Bit Error Rate (BER) and Bit Error Ratio (BER)

Bit Error Rate (BER)

- is the number of bit errors per unit time

Bit Error Ratio (BER) (also often BER)

- is the number of errors divided by the number of transmitted bits

Bit Error Rate is the Bit Error Ratio (BER) multiplied by bit rate.

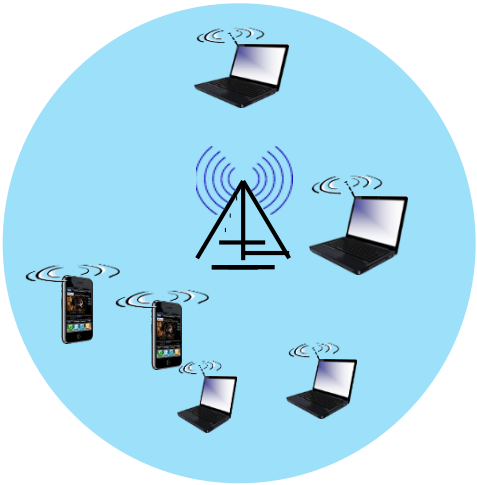
For example

- Transmit 10 bits i.e. (1011000111)
- Receive 10 bis i.e. (1011000011)
- 1 bit is wrong
- BER= 1/10 = 0.1 or 0.10%

Wireless link characteristics (1)

important differences from wired link ….

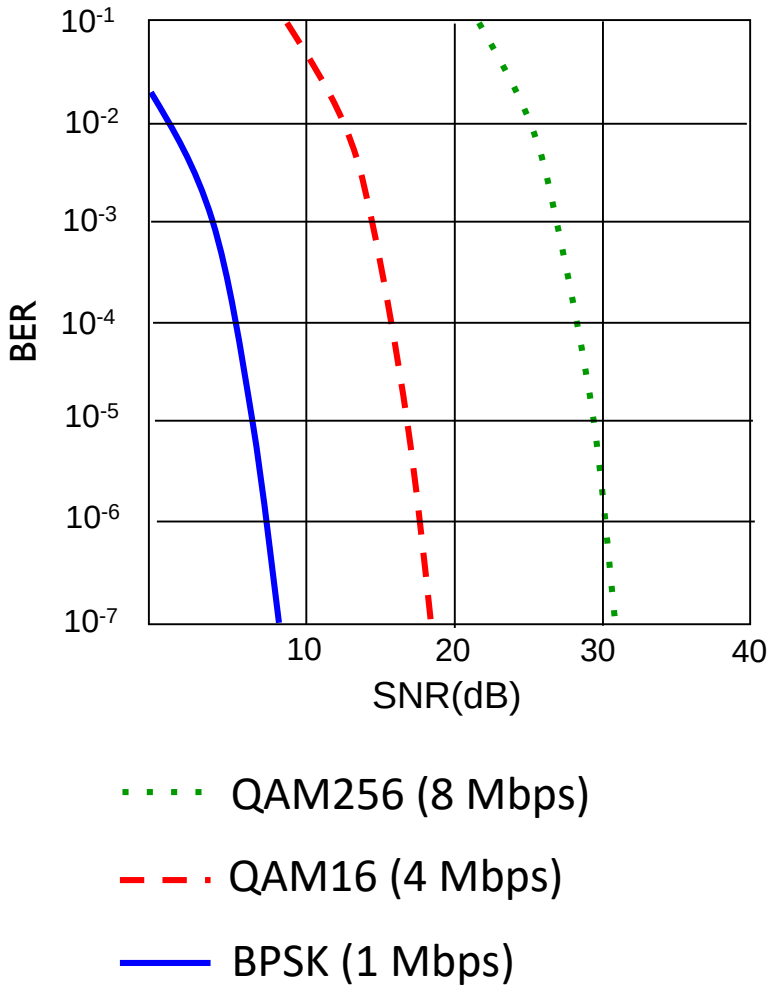
- decreased signal strength*:* radio signal attenuates as it propagates through matter (path loss)
- interference from other sources: wireless network frequencies (e.g., 2.4 GHz) shared by many devices (e.g., WiFi, cellular, motors): interference
- multipath propagation: radio signal reflects off objects ground, arriving at destination at slightly different times



…. make communication across (even a point to point) wireless link much more “difficult”

Wireless link characteristics (2)

- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a "good thing")
- SNR versus BER tradeoffs
  - *given physical layer:* increase power -> increase SNR->decrease BER
  - *given SNR:* choose physical layer that meets BER requirement, giving highest throughput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)

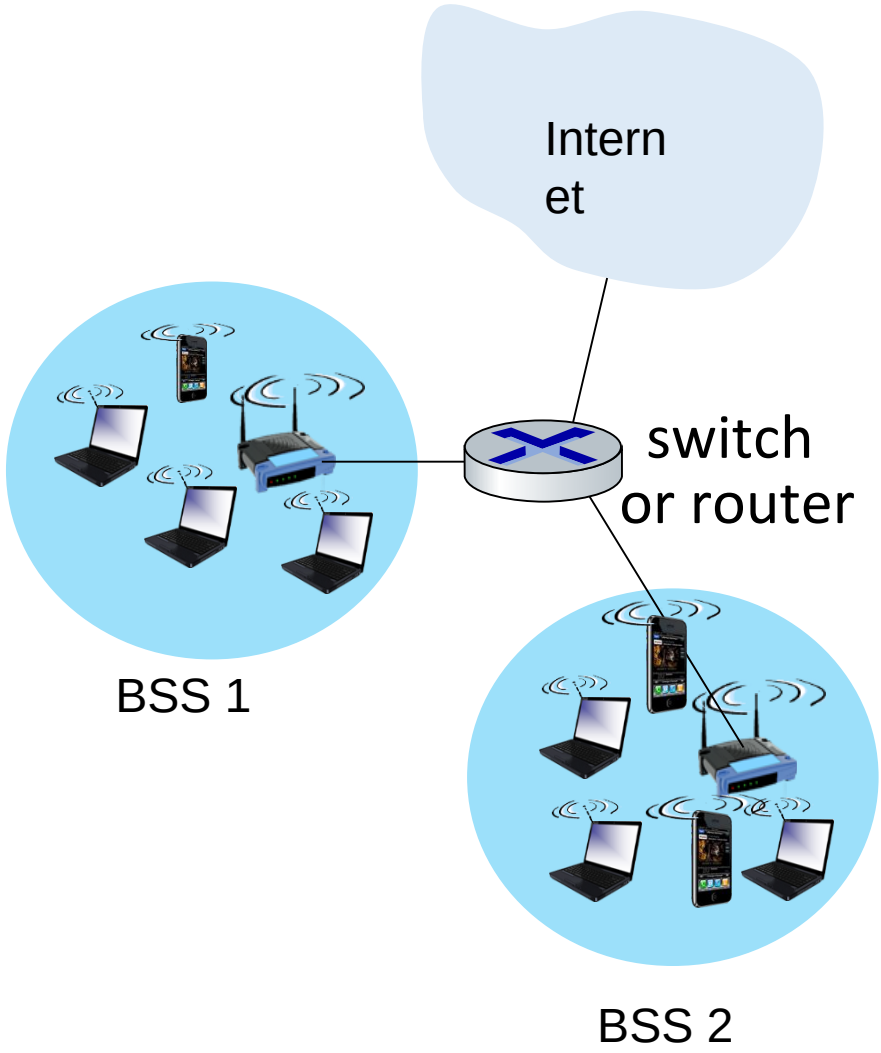


IEEE 802.11 Wireless LAN

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47Gpbs	70m	5 Ghz
802.11ax (WiFi 6)	2020 (exp.)	14 Gbps	70m	2.4, 5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz

- all use CSMA/CA for multiple access, and have base-station and ad-hoc network versions

802.11 LAN architecture

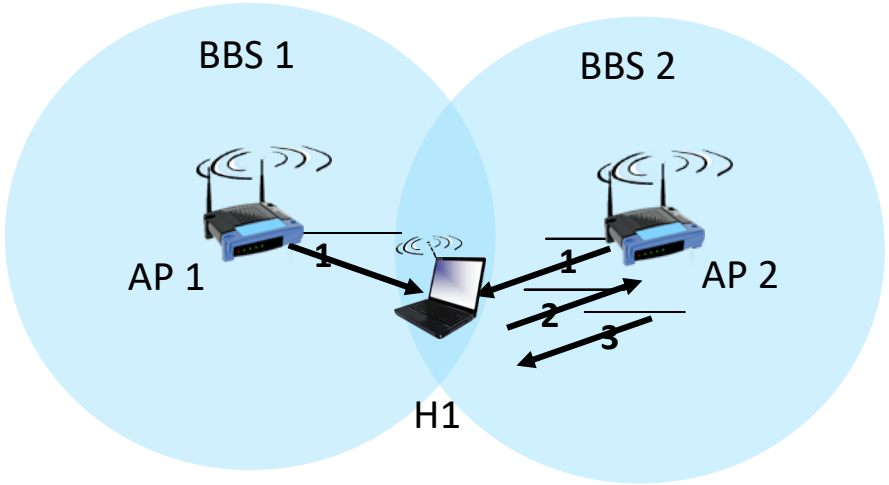


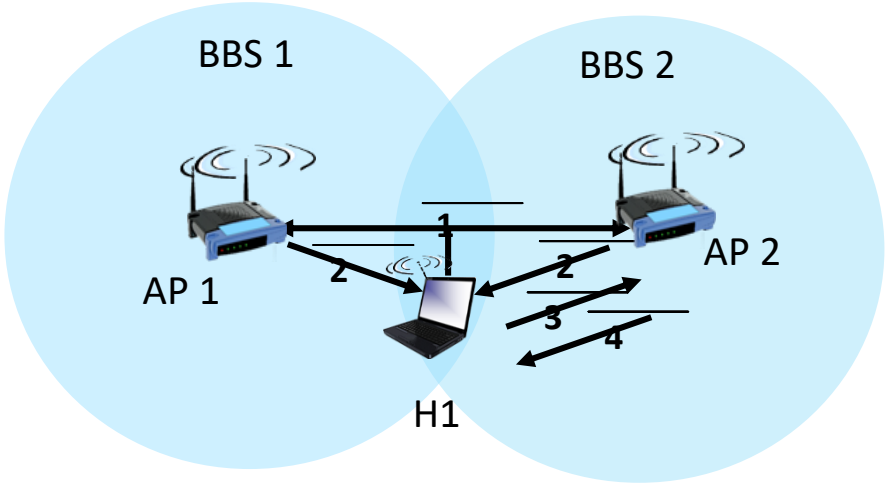
- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka “cell”) in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

802.11: Channels, association

- spectrum divided into channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- arriving host: must associate with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - then may perform authentication [Chapter 8]
  - then typically run DHCP to get IP address in AP's subnet

802.11: passive/active scanning





passive scanning:

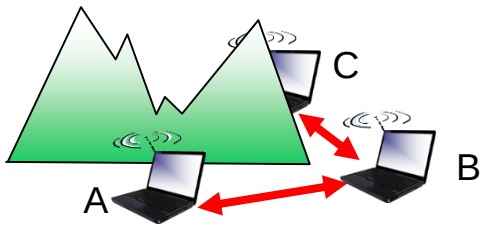
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

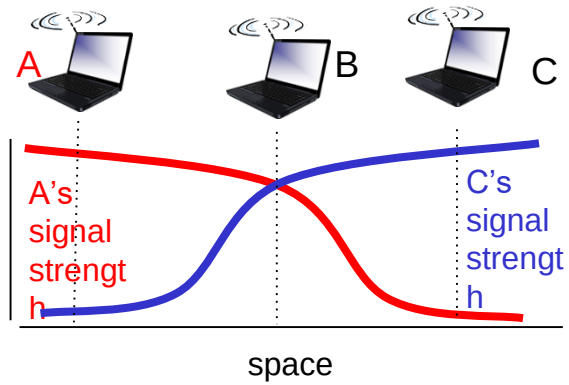
active scanning:

(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

IEEE 802.11: multiple access

- avoid collisions: 2^+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with detected ongoing transmission by another node
- 802.11: *no* collision detection!
  - difficult to sense collisions: high transmitting signal, weak received signal due to fading
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/CollisionAvoidance





IEEE 802.11 MAC Protocol: CSMA/CA

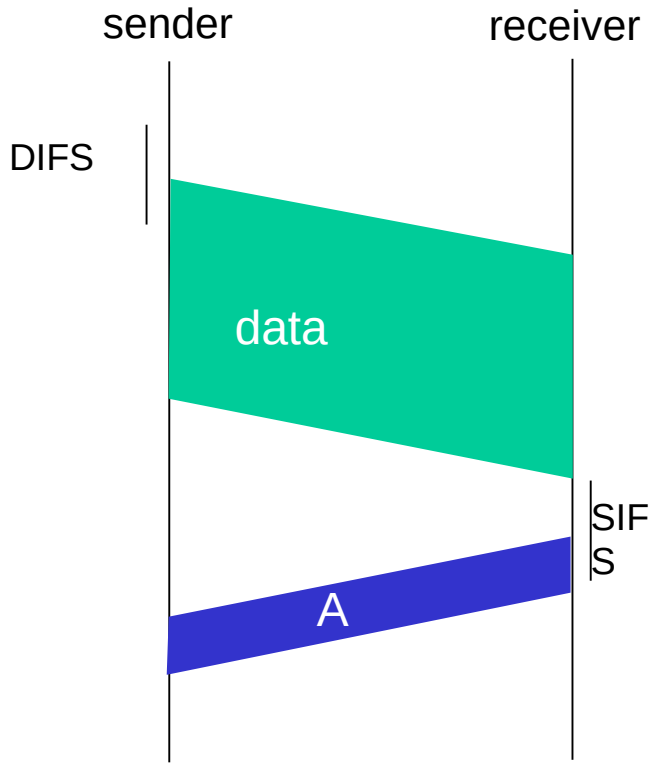
802.11 sender

1 if sense channel idle for **DIFS** then
transmit entire frame (no CD)

2 if sense channel busy then
start random backoff time
timer counts down while channel idle
transmit when timer expires
if no ACK, increase random backoff interval, repeat 2

802.11 receiver

if frame received OK
return ACK after **SIFS** (ACK needed due to hidden terminal problem)



DIFS - It's the minimum time interval that a device must wait before transmitting a frame (data packet) after detecting the end of a previous transmission.

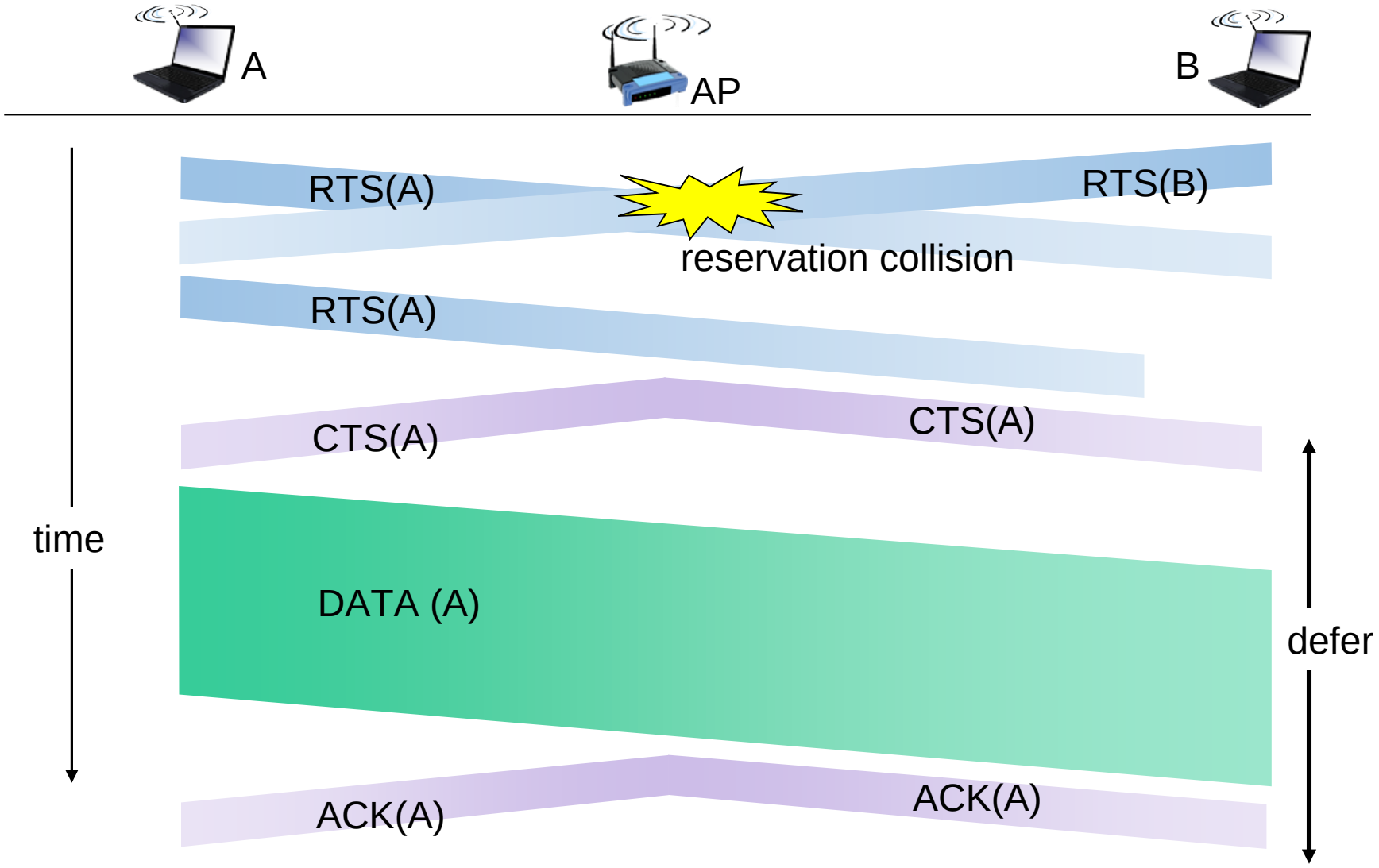
SIFS is the minimum time gap between two successive frames, ensuring that stations in the same network can accurately transmit and receive data without interference.

Avoiding collisions (more)

idea: sender "reserves" channel use for data frames using small reservation packets

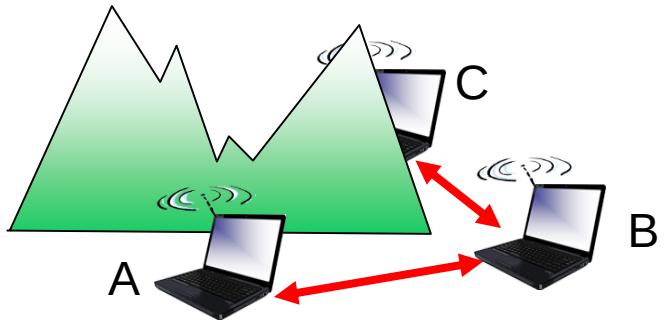
- sender first transmits *small* request-to-send (RTS) packet to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

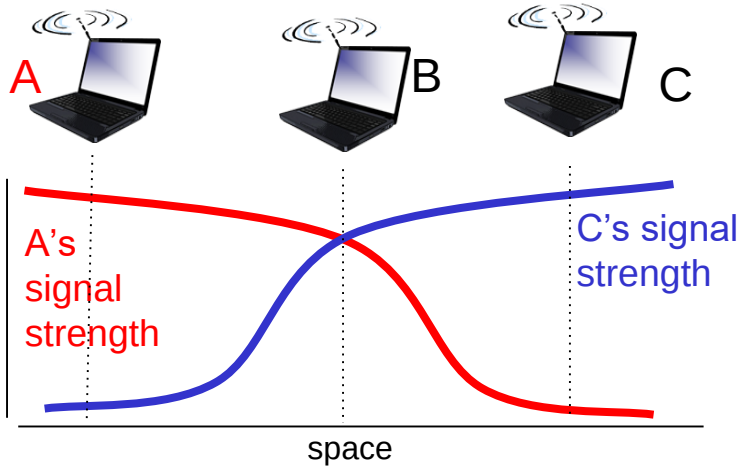
Collision Avoidance: RTS-CTS exchange



Wireless link characteristics (3)

Multiple wireless senders, receivers create additional problems (beyond multiple access):





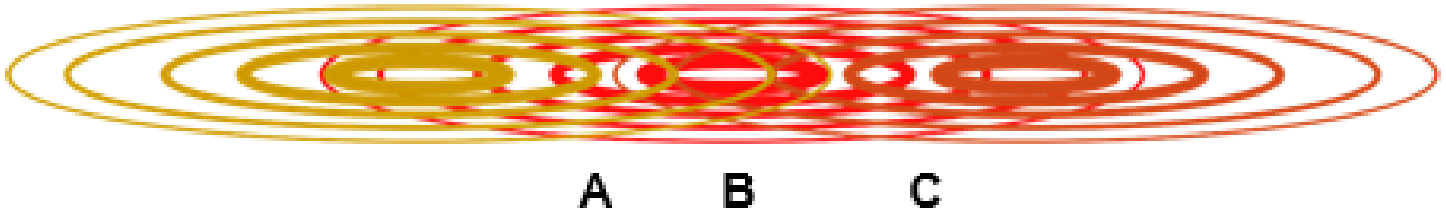
Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other means A, C unaware of their interference at B

Signal attenuation:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

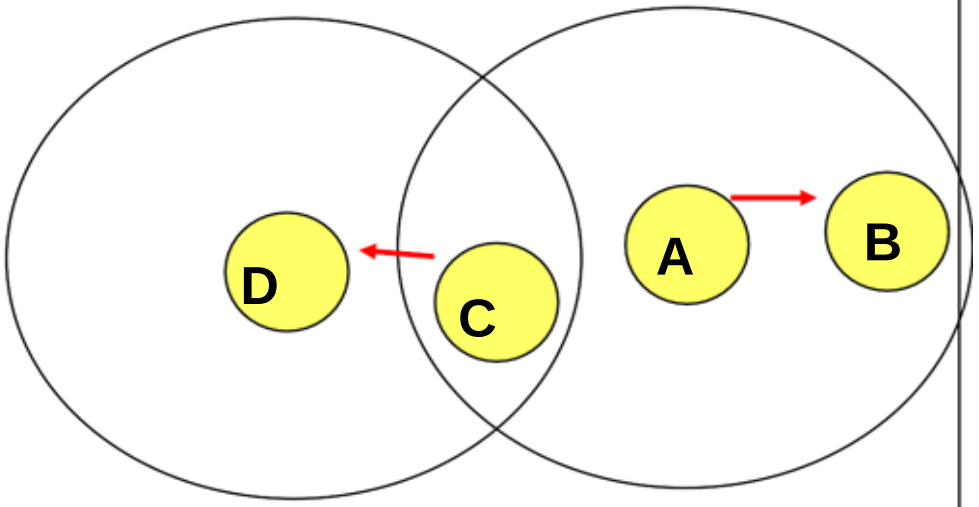
Hidden Terminal Problem

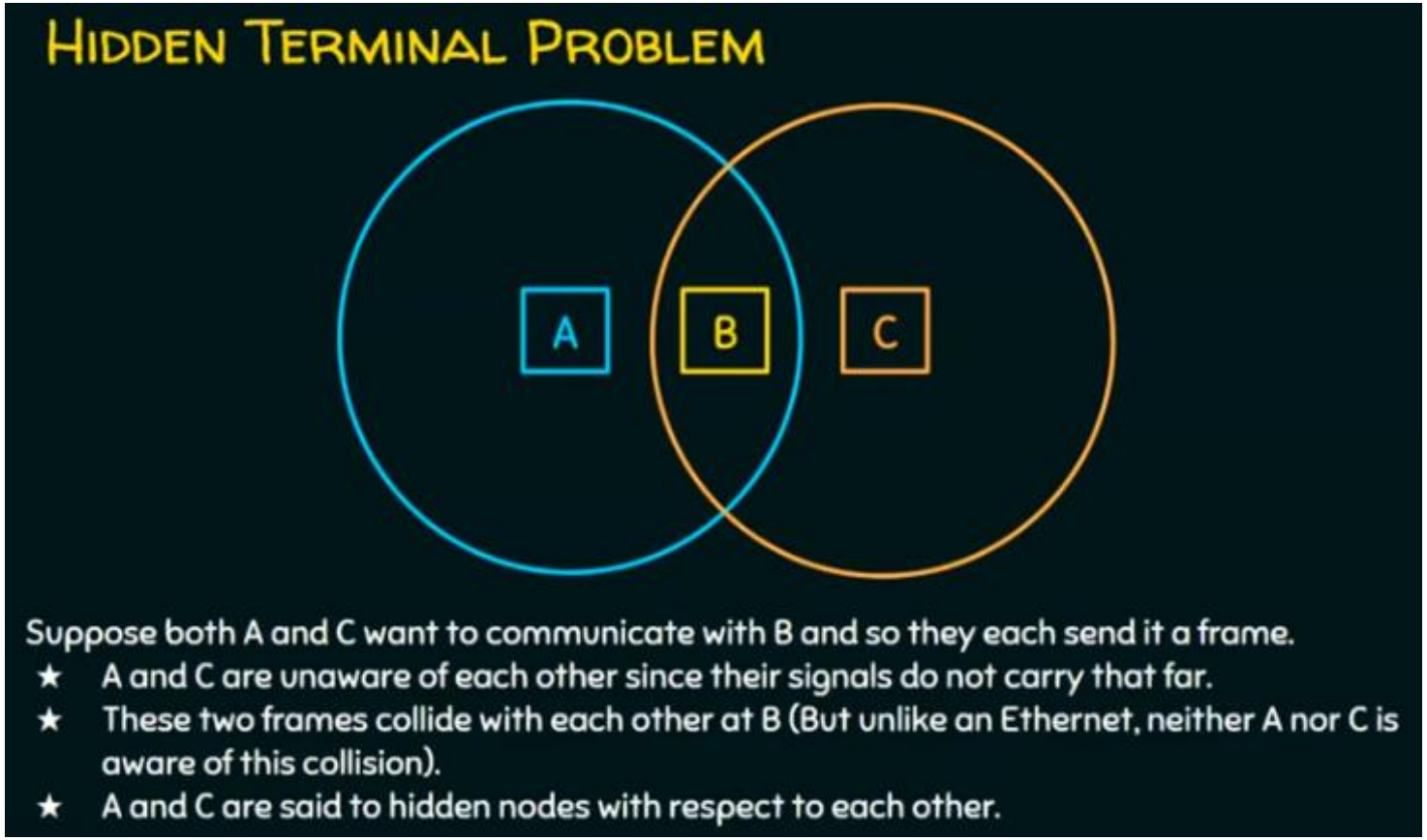


- A and C cannot hear each other.
- A sends to B, C cannot receive A.
- C wants to send to B, C senses a “free” medium.
- Collision occurs at B.
- A cannot receive the collision.
- A is “hidden” for C.

Exposed Terminal Problem

- A starts sending to B.
- C senses carrier, finds medium in use and has to wait for A->B to end.
- D is outside the range of A, therefore waiting is not necessary.
- A and C are “exposed” terminals

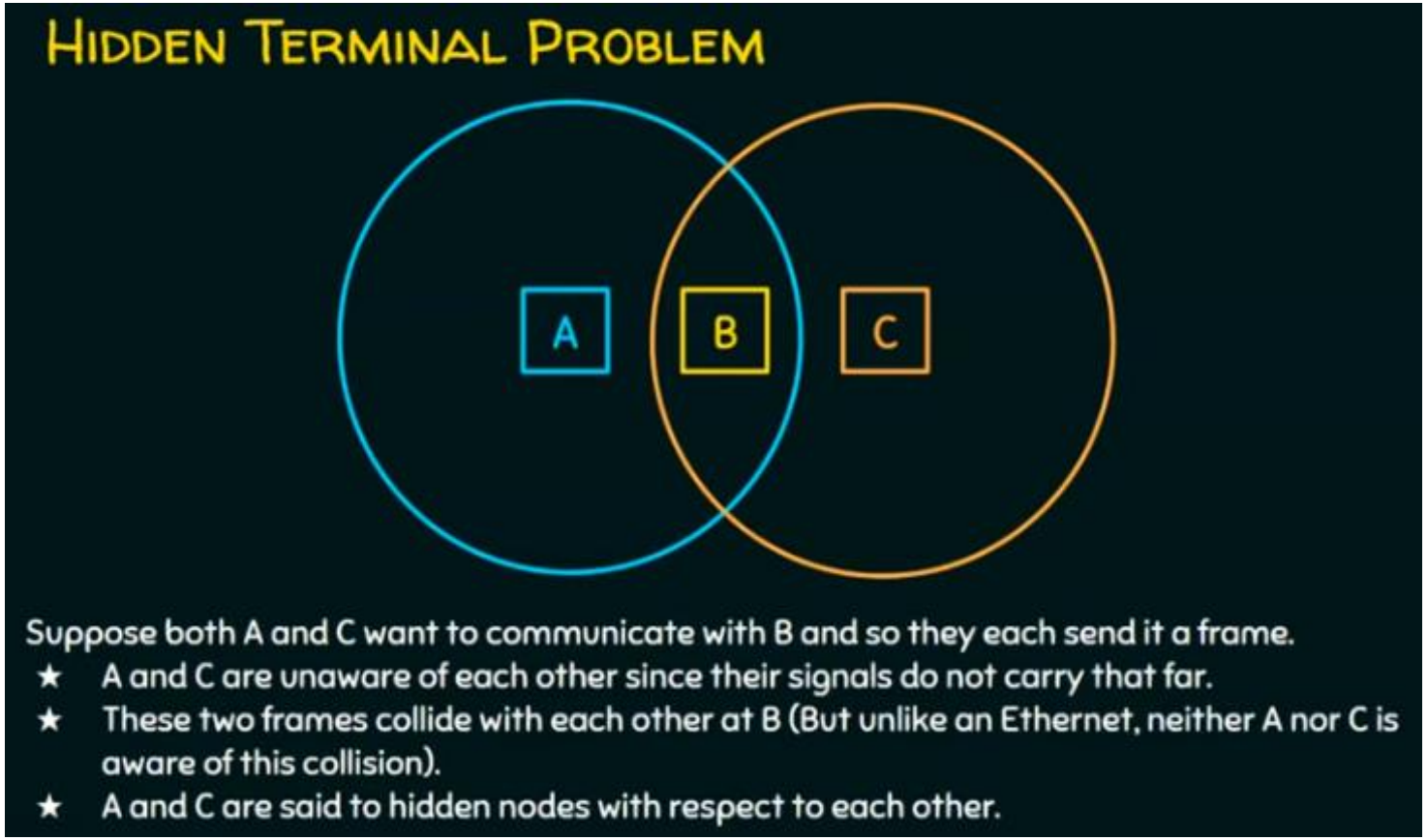




Suppose we have node A and this is a wireless node obviously, it will have a coverage range.

1. Coverage range for the node A
2. Another node C also has a coverage range
3. A and C are the two nodes that are here in this example
4. The coverage area of A is not disturbing to C
5. At the same time, the coverage area of C is not at all disturbing A.
6. if A is sending some data to any node except C, C will be definitely unaware of this transmission Because A's coverage area and C's coverage area

7. The problem comes when we have another node B.
8. B is in the coverage area of A as well as the coverage area of C
9. So B can transmit to A as well as B can transmit to C
10. A can transmit to B but not to C and C can transmit to B but not to A



according to A, C is hidden and

according to C, A is hidden

because of these two hidden terminals, there is a collision at B this is what exactly the hidden terminal problem

B is in both coverage areas suppose both A and C want to communicate with B

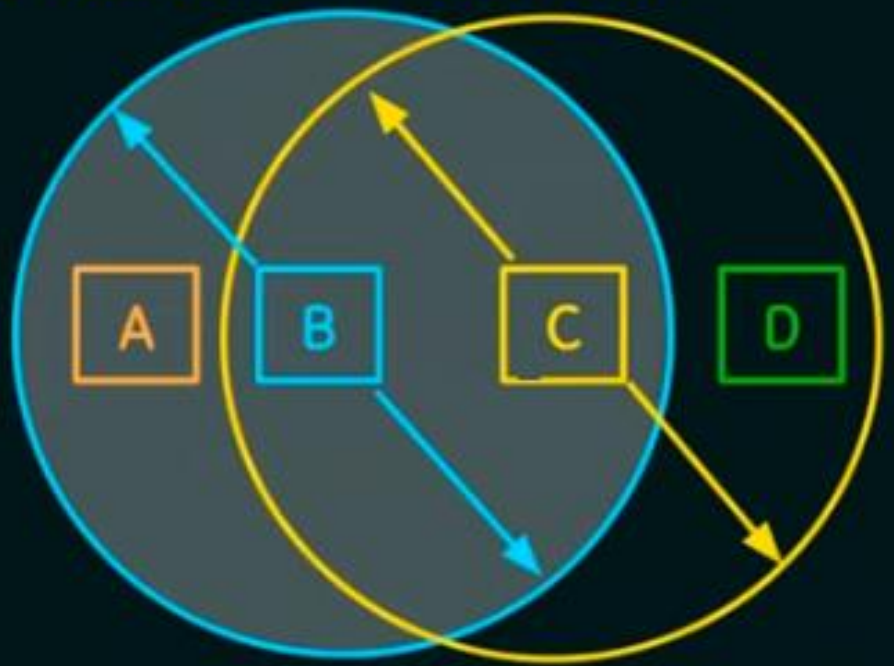
so they each send it a frame if A and C have a frame send it to B and both are sending it at the same time

But **A and C are unaware** of each other since their signal do not carry that far

So these two frames collide with each other at B so when a and C transmit at the same time the collision happens at B

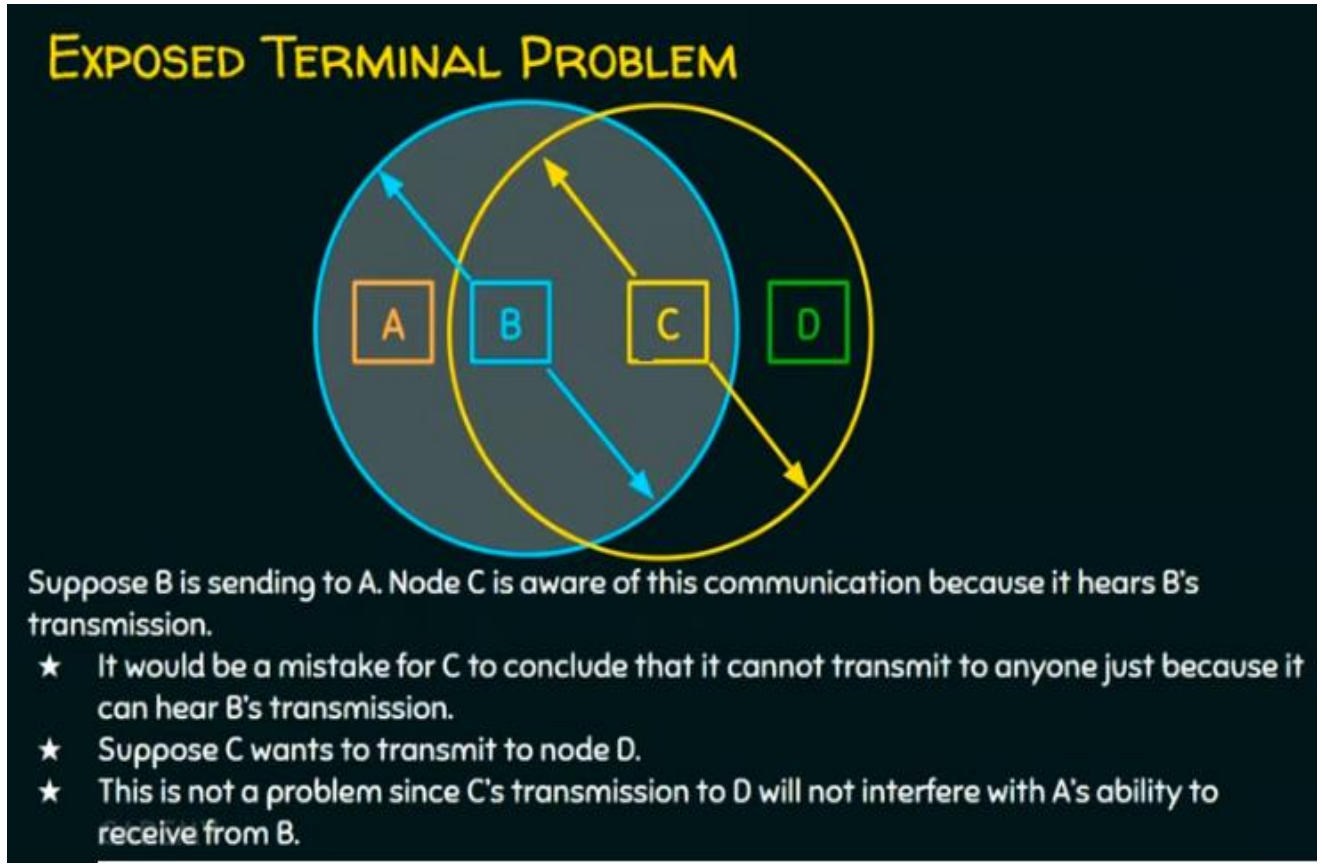
So neither A nor C is aware of this collision this is actually the problem A and C are said to be hidden with respect to each other

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.
- ★ This is not a problem since C's transmission to D will not interfere with A's ability to receive from B.



1. Node B will be having its own coverage range
2. Node C is also having a coverage range
3. Node B and C are in the coverage range of each other

The exposure terminal problem

We have a node B which has its coverage area

For NODE B, A and C are in the same coverage area of B

For NODE C, B and D are in the coverage area of C

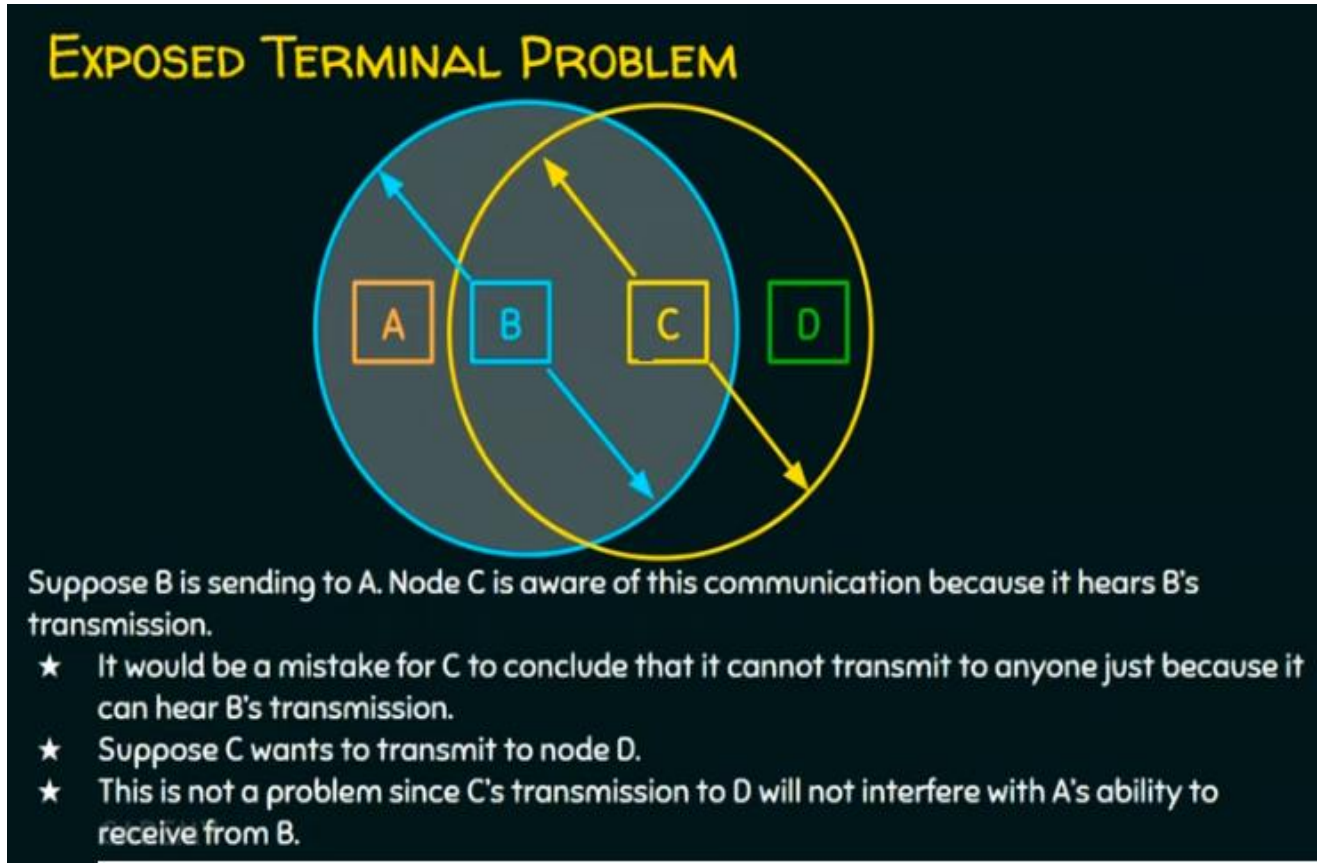
Now the exposed terminal problem is:

Suppose node B is sending to NODE A.

C will obviously hear this conversation because C is in the coverage range of B

Node C is aware of this communication because it here is B’s transmission

NODE C conclude that it cannot transmit to anyone just because it can hear B's transmission



Suppose NODE C wants to send it to NODE D

C'S transmission to D will not at all interfere the A's ability to hear or receive from B.

Because whatever C is going to transmit to D.

So whatever C is going to transmit to B is not at all going to affect A.

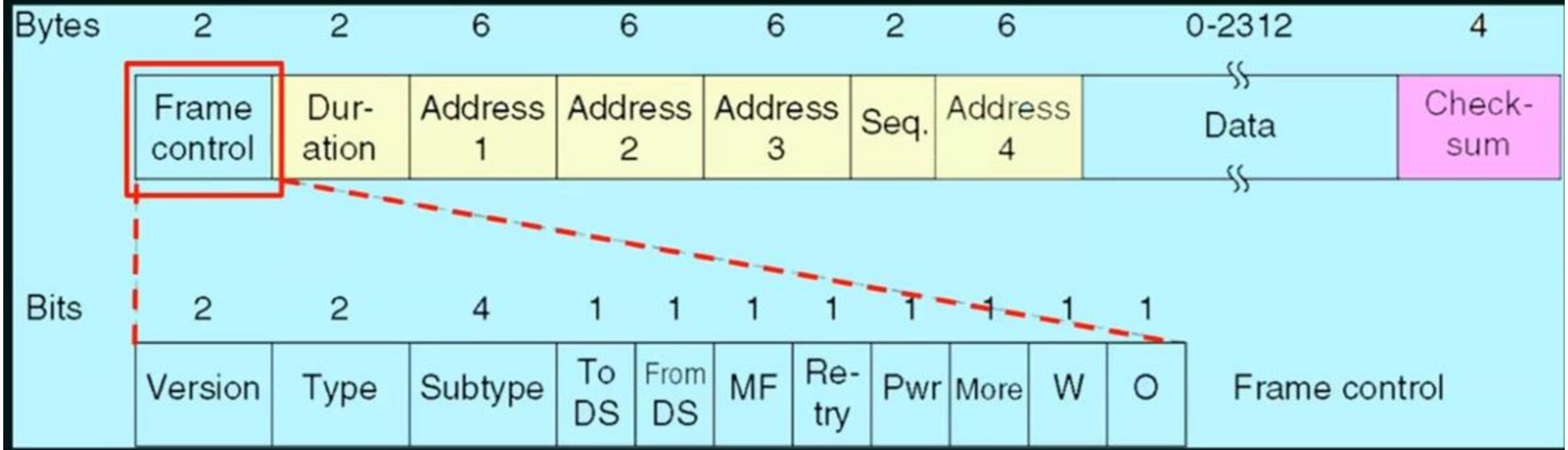
Because A not at all in the coverage area of C

But C can conclude that because of the conversation it hears from B which is actually intended to A .

It cannot send it to anybody

This is the exposed terminal problem

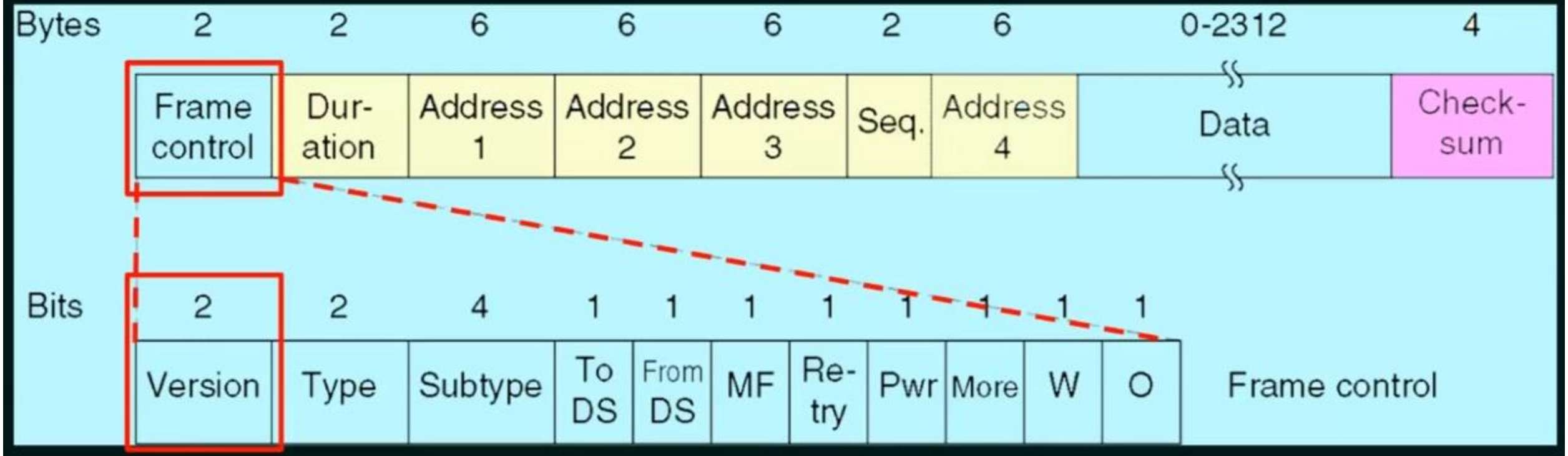
IEEE 802.11 Wi-Fi Frame Format



Frame Control:

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

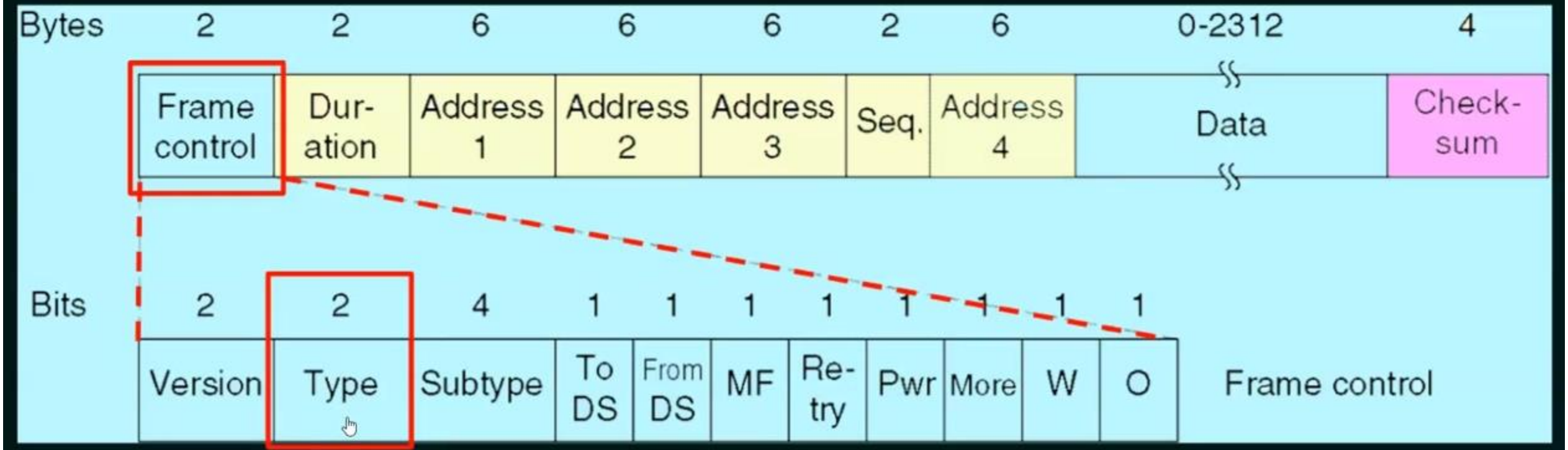
IEEE 802.11 Wi-Fi Frame Format



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.

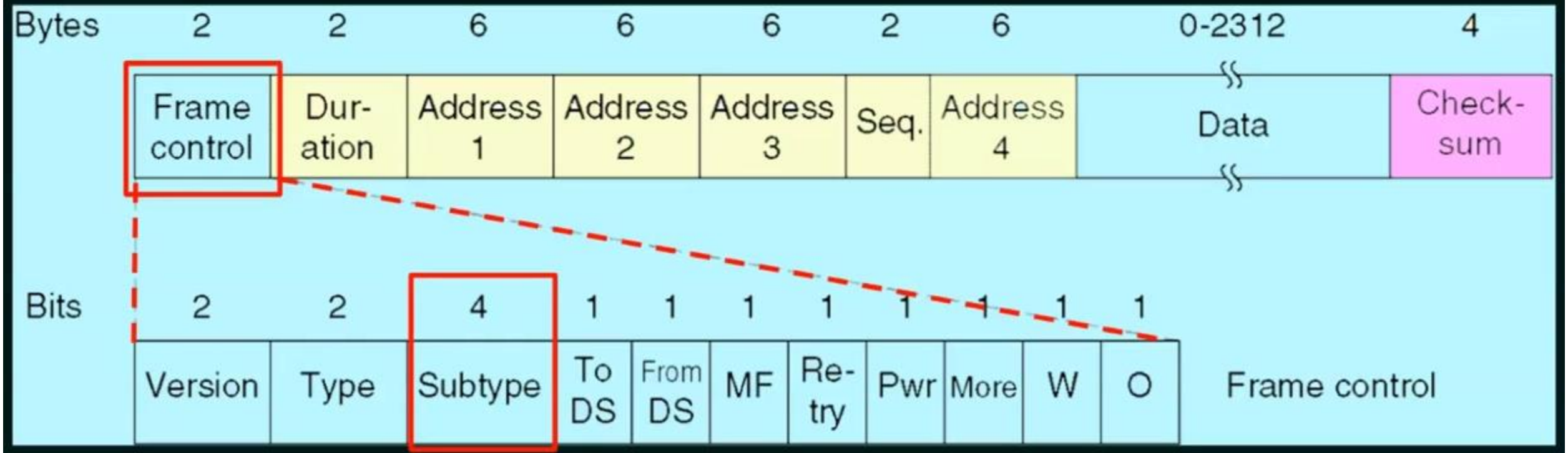
IEEE 802.11 Wi-Fi Frame Format



Type:

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

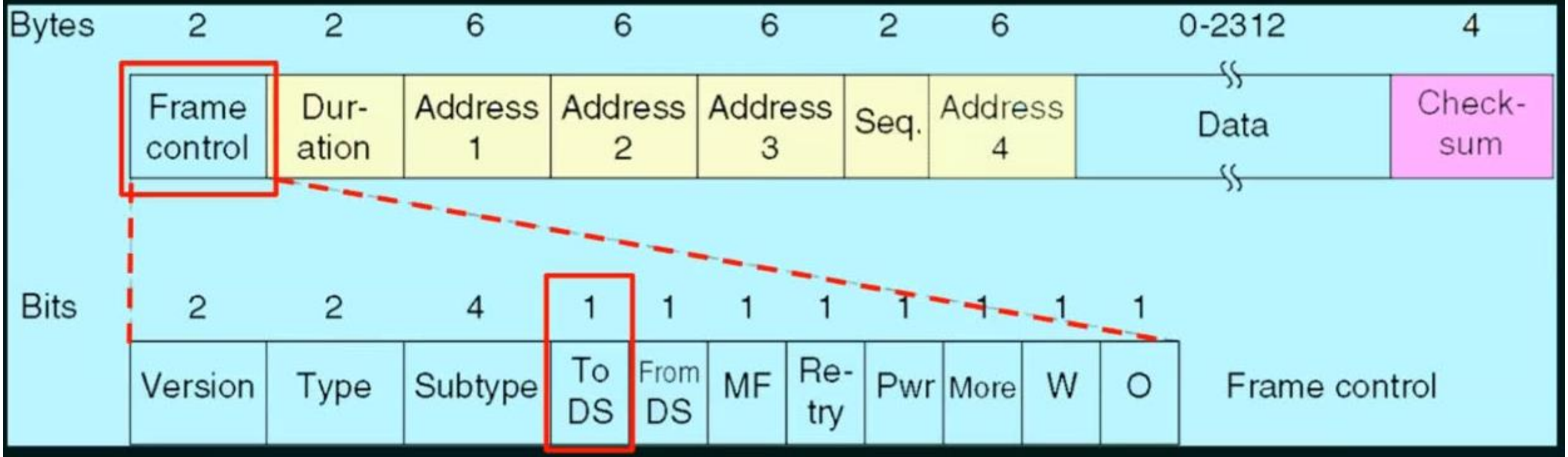
IEEE 802.11 Wi-Fi Frame Format



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.

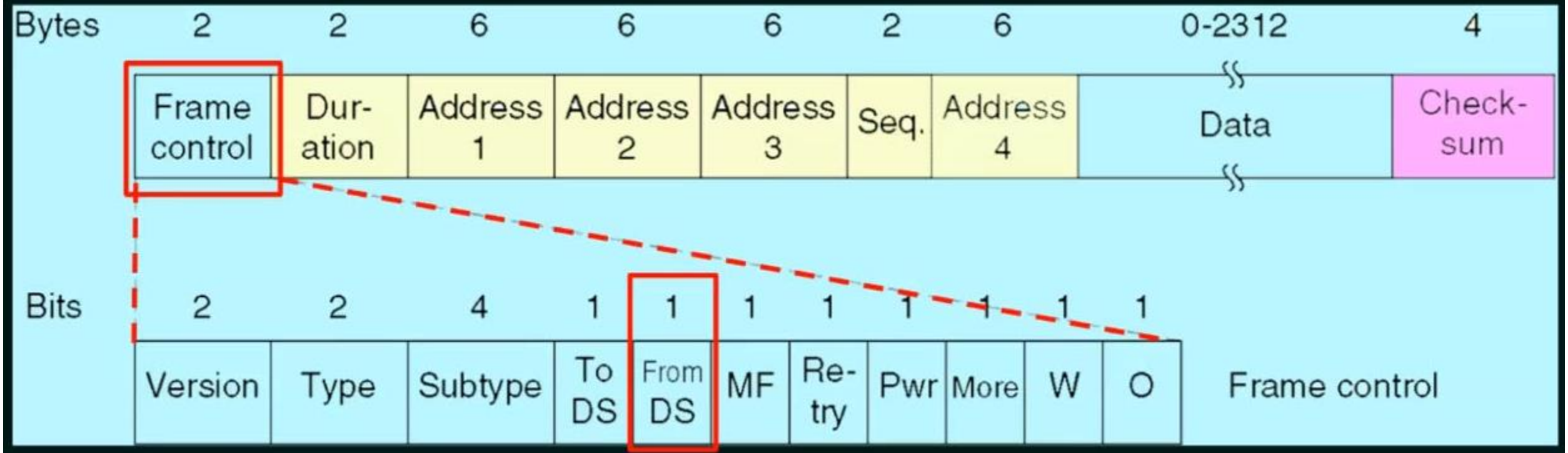
IEEE 802.11 Wi-Fi Frame Format



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.

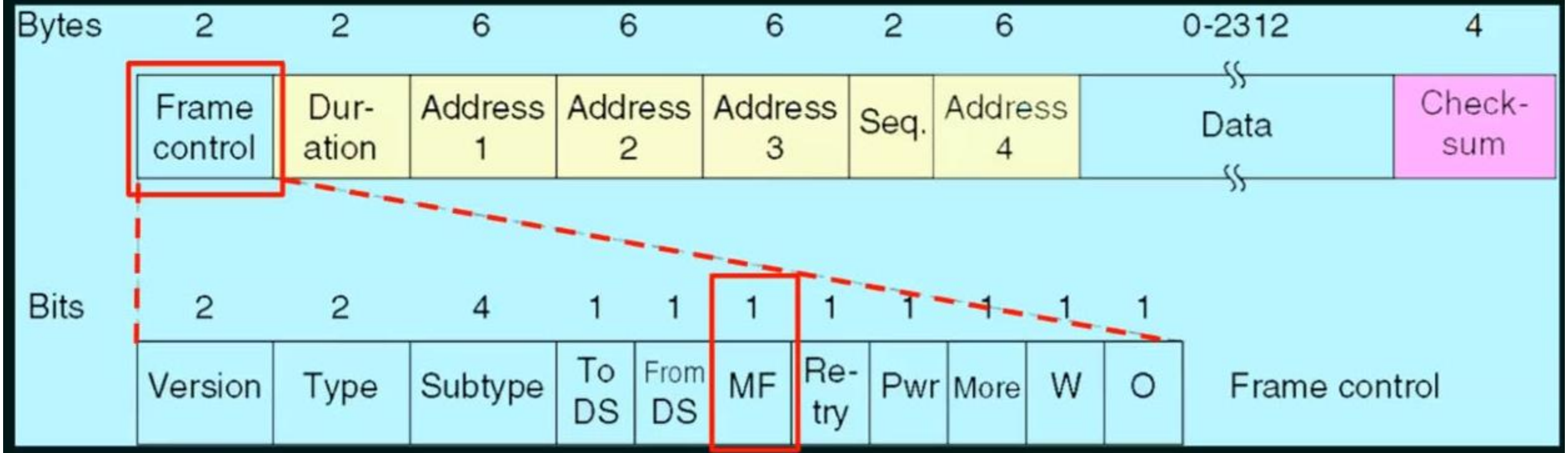
IEEE 802.11 Wi-Fi Frame Format



From DS:

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

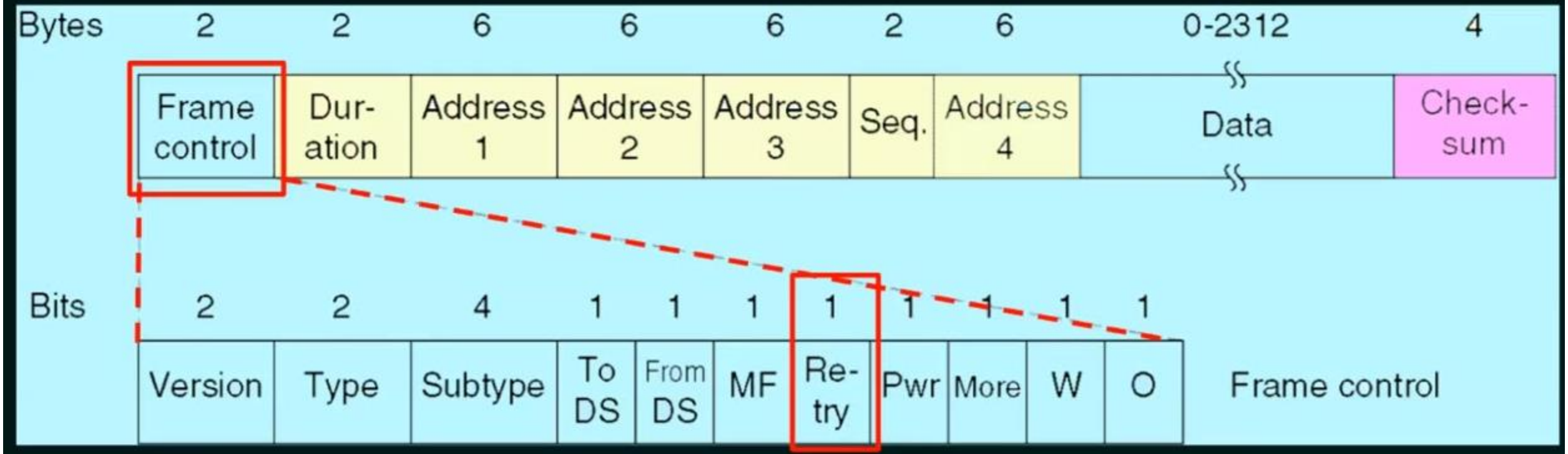
IEEE 802.11 Wi-Fi Frame Format



More Fragments:

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

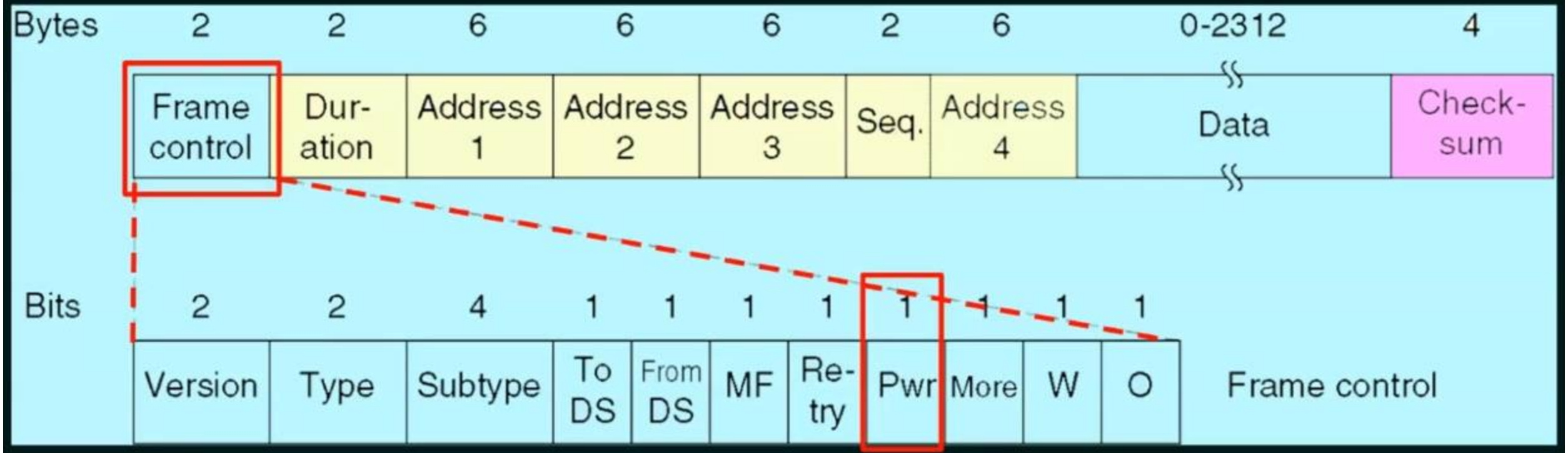
IEEE 802.11 Wi-Fi Frame Format



Retry:

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

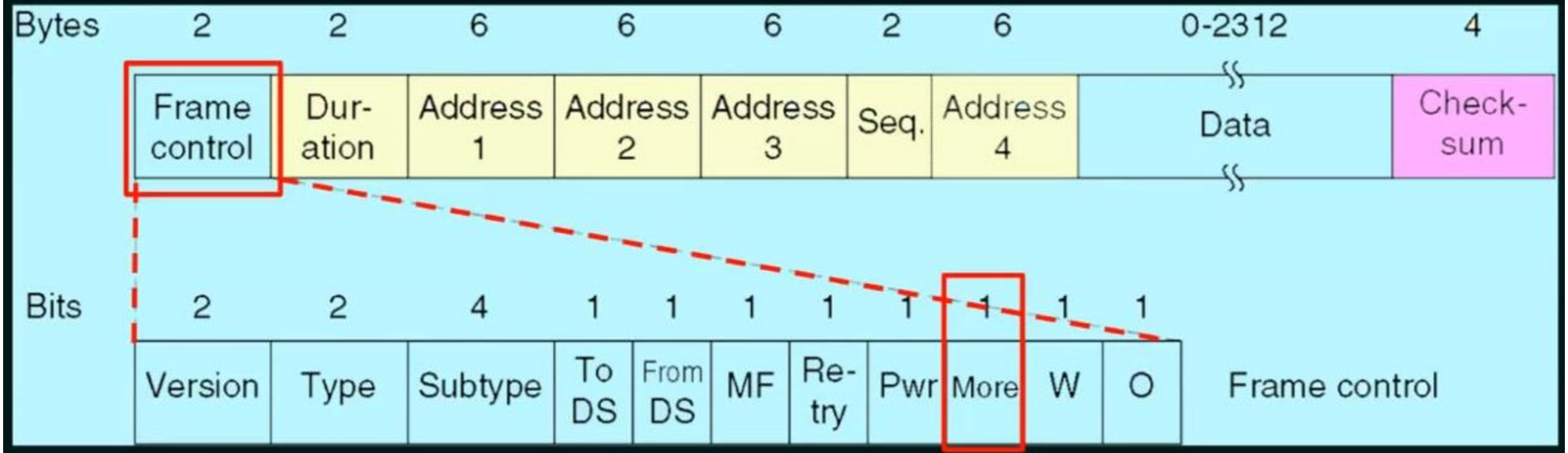
IEEE 802.11 Wi-Fi Frame Format



Power Management:

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

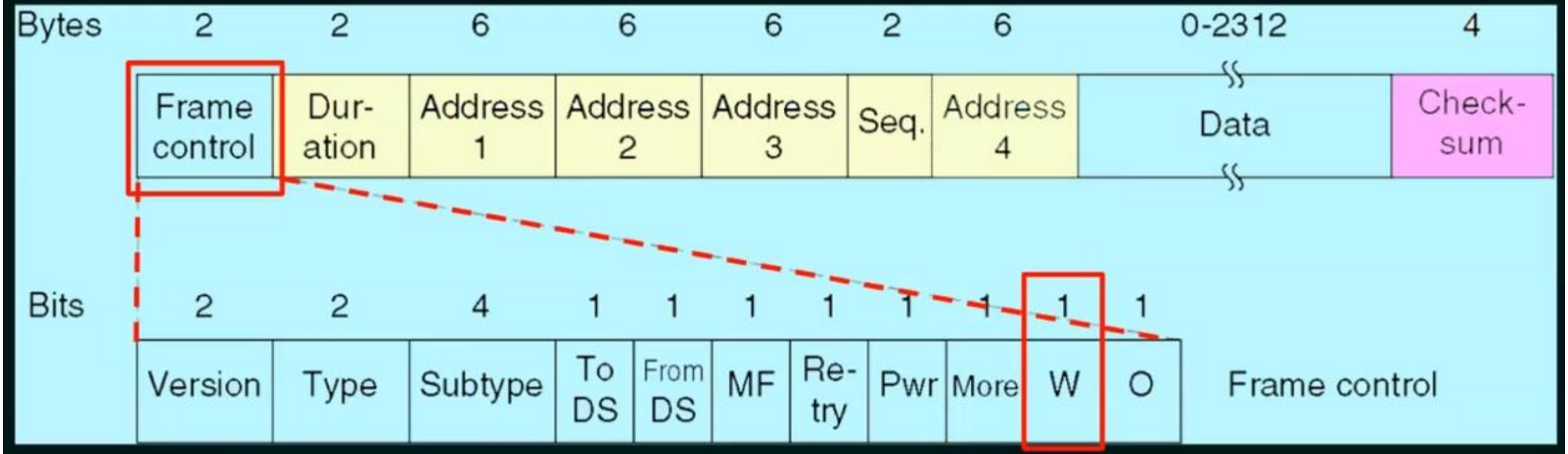
IEEE 802.11 Wi-Fi Frame Format



More Data:

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

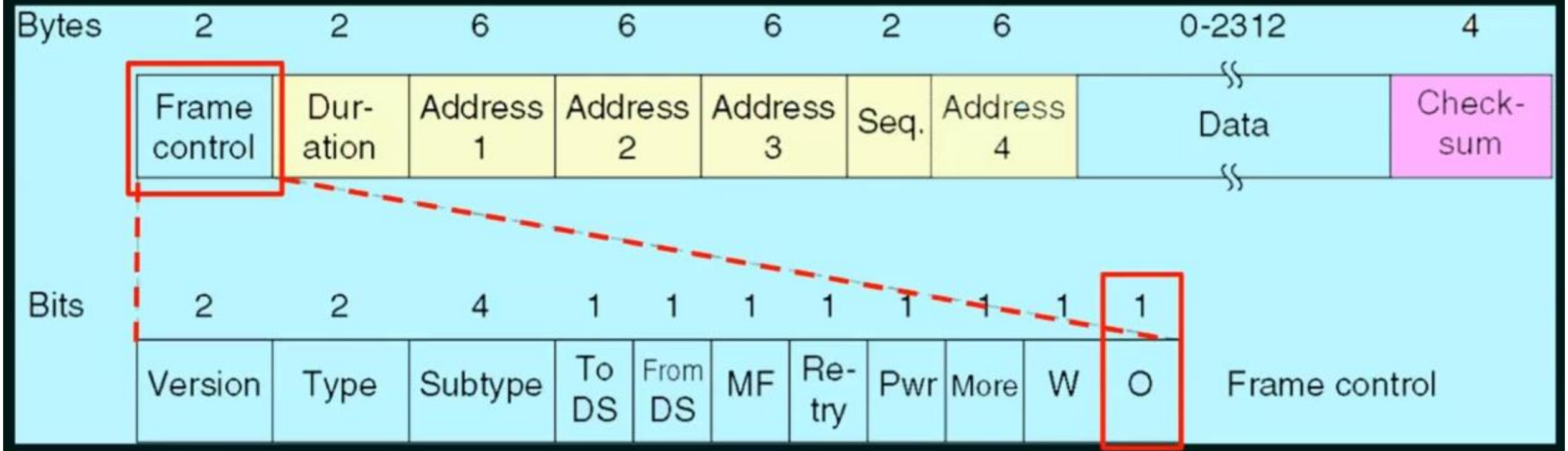
IEEE 802.11 Wi-Fi Frame Format



WEP:

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

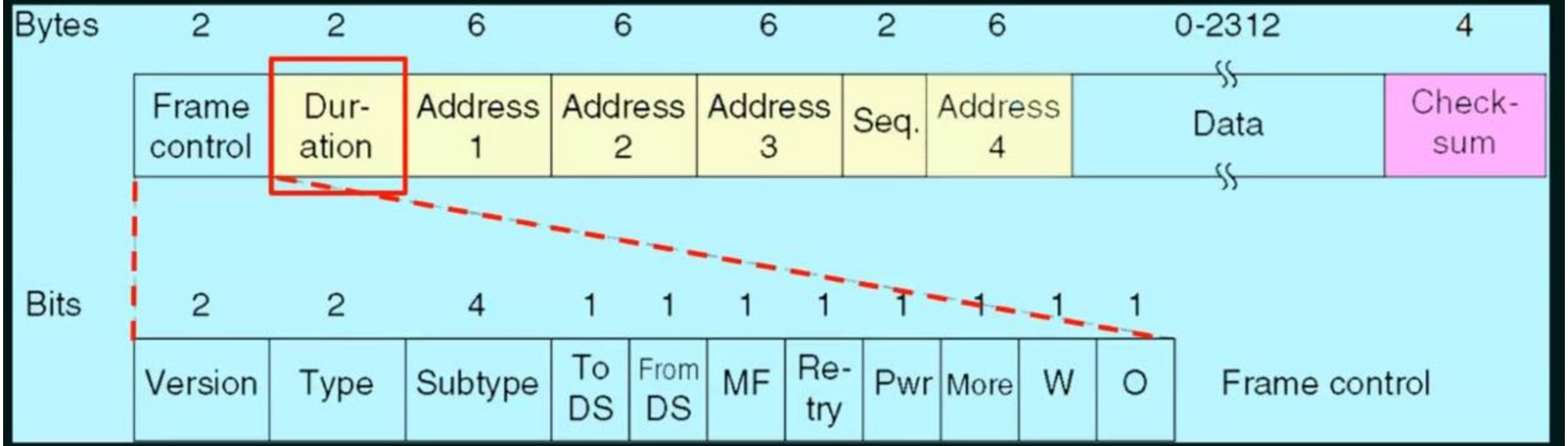
IEEE 802.11 Wi-Fi Frame Format



Order:

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

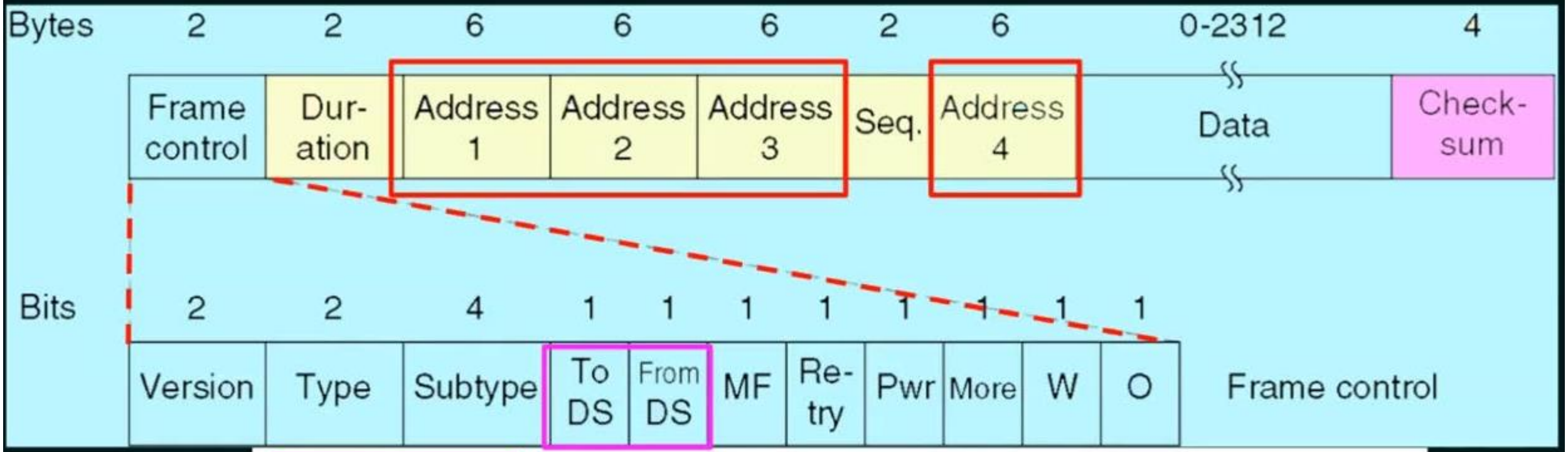
IEEE 802.11 Wi-Fi Frame Format



Duration:

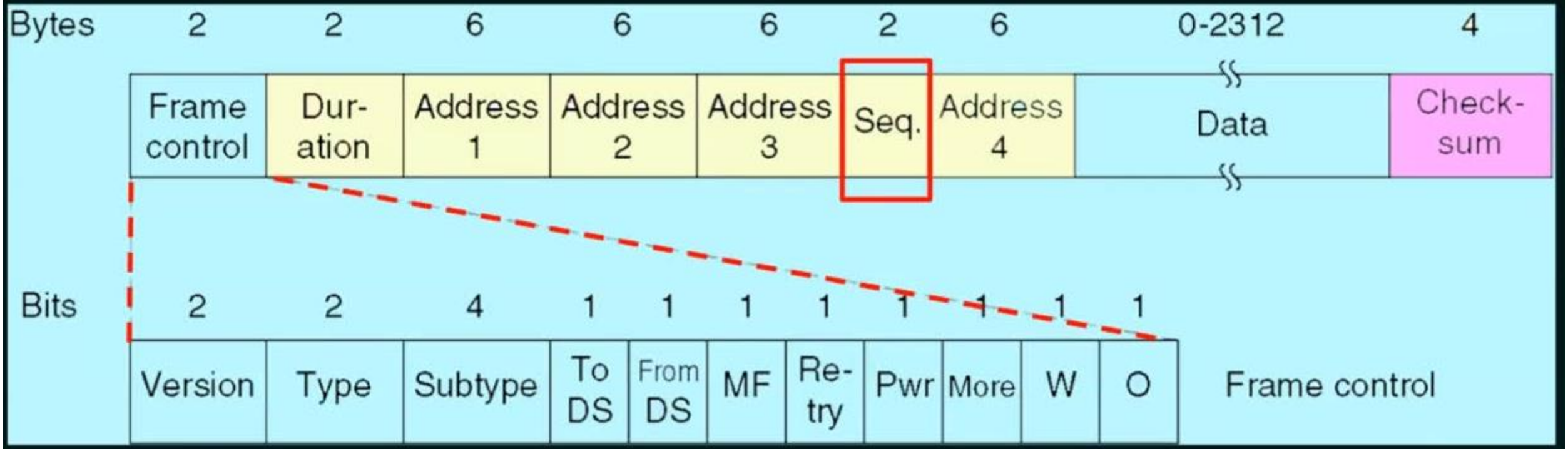
★ It is a 2-byte field that specifies the time period for which the frame and its acknowledgement occupy the channel.

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

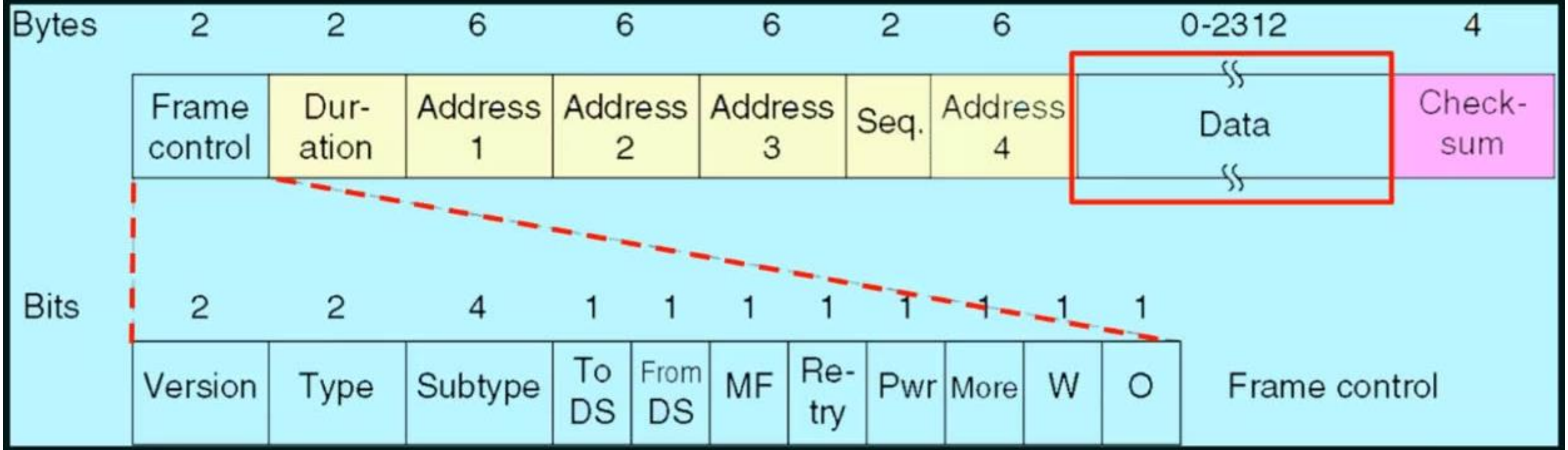
IEEE 802.11 Wi-Fi Frame Format



Sequence:

★ It a 2 bytes field that stores the frame numbers. It detects duplicate frames and determines the order of frames for higher layers. Among the 16 bits, the first 4 bits provides identification to the fragment and the rest 12 bits contain the sequence number that increments with each transmission.

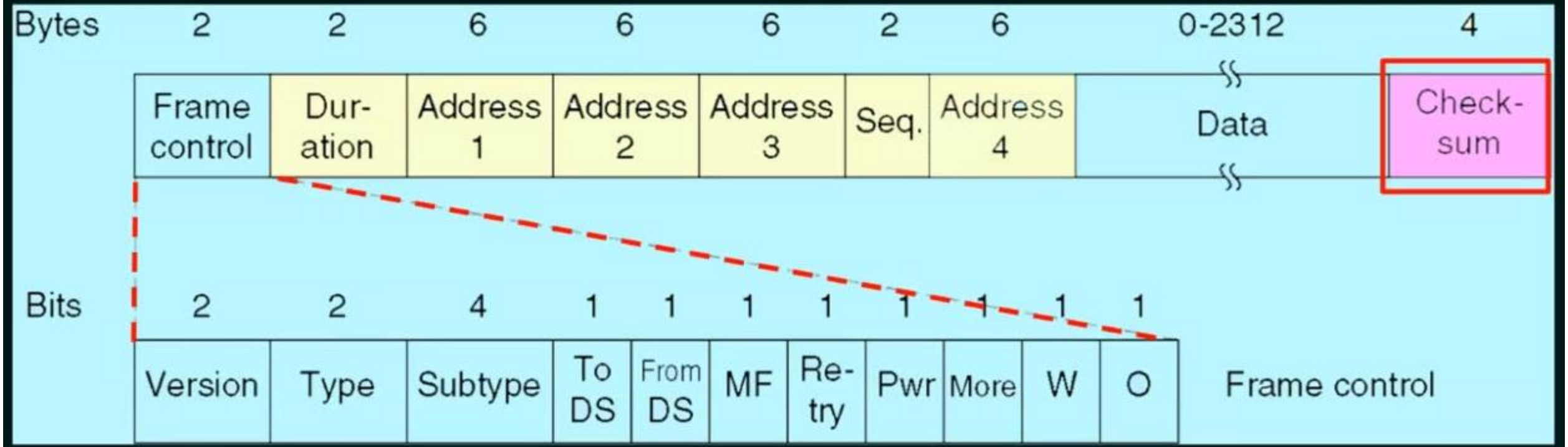
IEEE 802.11 Wi-Fi Frame Format



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.

MAC protocol categories

- **Based on operation :**
  - ***Synchronous protocols:*** All nodes need to be synchronized. Global time synchronization is difficult to achieve.
  - ***Asynchronous protocols*:** These protocols use relative time information for effecting reservations.

- **Based on who initiates a communication request.**
  - ***Receiver-initiated protocols***
  - ***Sender-initiated protocols***

Types of protocol

1. Synchronous MAC Protocols

- In synchronous MAC protocols, **all nodes in the network are synchronized to the same time.**
- Achieved by a **timer** master broadcasting a regular beacon.
  - All nodes listen for this beacon and synchronize their clocks to the master's time.
- Central coordination is, needed to synchronize time events.

1. Asynchronous MAC Protocols

- Nodes **do not** necessarily follow the same time.
- A more distributed control mechanism is used to coordinate channel access
- Access to the channel tends to be **contention-based.**

Contention-Based Protocols

- A nodes does not make any resource reservation a *priori*.
- Whenever it receive a packet to be transmitted, it contends with its neighbor nodes for access to the shared channel.
- Nods are not guaranteed periodic access to the channel
- Thus can't provide QoS guarantees to sessions .
- E.g. :
  - pure ALOHA, slotted ALOHA, CSMA, IEEE 802.11, etc
- The "listen before talk" operating procedure in IEEE 802.11 is the most well known contention-based protocol.

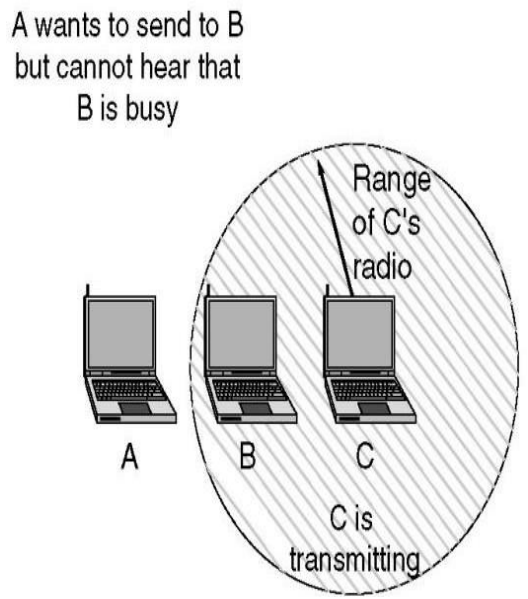
Problems in Ad Hoc Channel Access

- **Hidden Terminal Problem**
- **Shortcomings of the RTS-CTS Solution**
- **Exposed Node Problem**

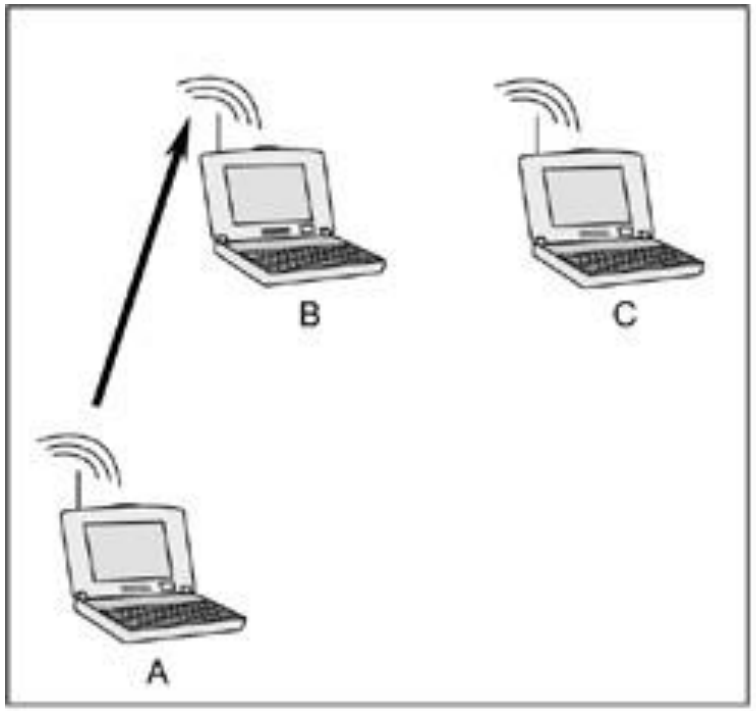
Hidden Terminal Problem

- Found in **contention-based protocols**.
  - **A contention-based protocol** (CBP) is a communications protocol for operating wireless telecommunication equipment that **allows many users to use the same radio channel without pre-coordination**.

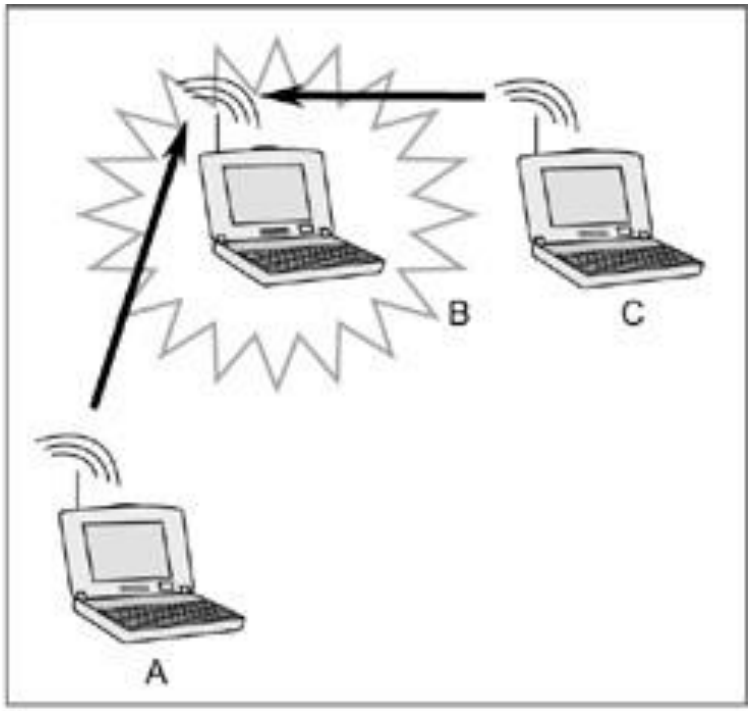
- Two nodes are said to be hidden from one another (out of signal range) when both attempt to send information to the same receiving node, resulting in a collision of data at the receiver node



Hidden Terminal Problem



1. A transmits to B. (C does not hear this.)



2. C transmits to B ... Collision!

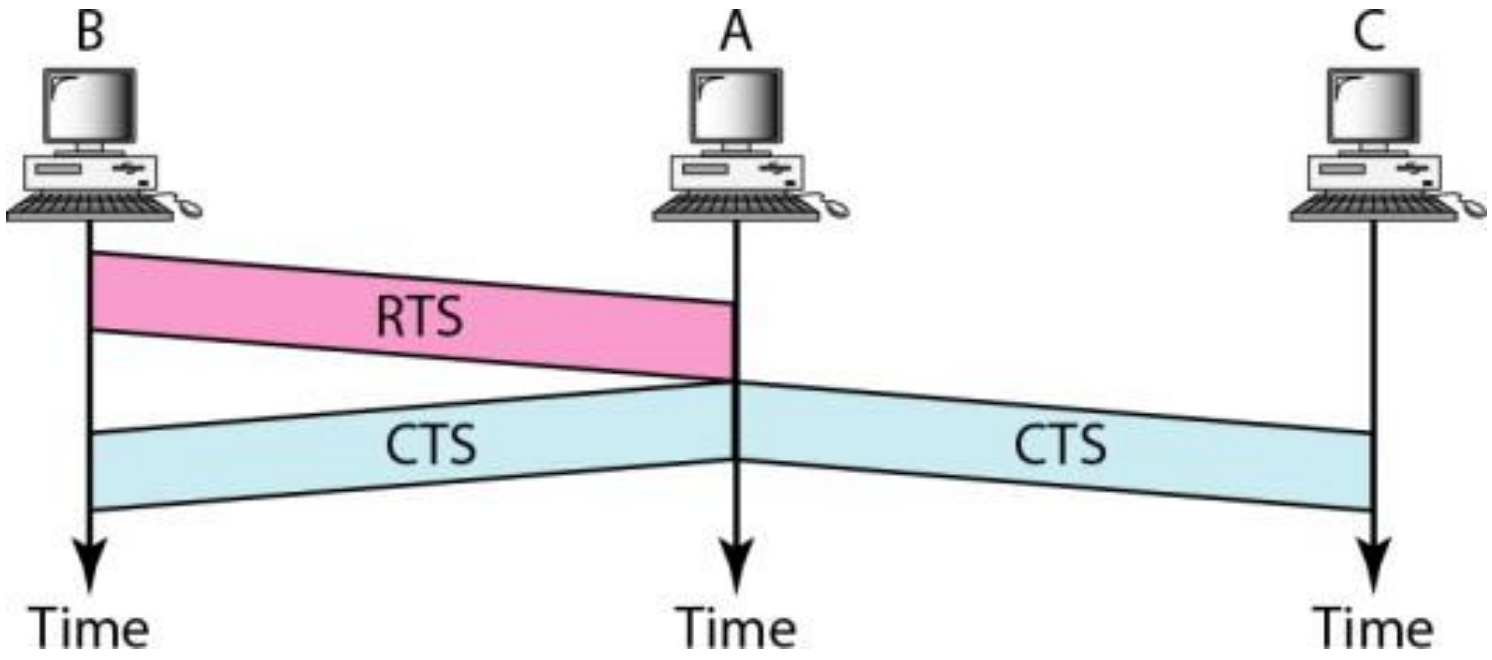
Possible Solution

RTS-CTS handshake Protocol

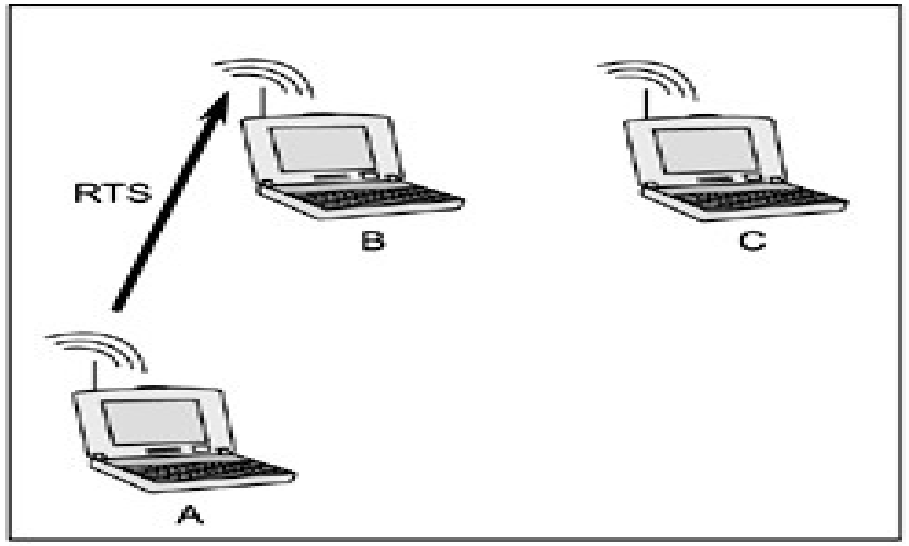
- To avoid collision, all of the receiver's neighbouring nodes need to be informed about the **status of the channel**.
  - This can be **achieved** by using a **handshake protocol**
  - reserving the channel using control messages
- **Resolves hidden node problems**
- An RTS (**Request To Send**) message can be used **by a node** to indicate its wish **to transmit data**.
- The receiving node can allow this transmission by sending a grant using the **CTS** (**Clear To Send**) message.
- Because of the **broadcast nature of these messages,** all neighbors of the sender and receiver will be **informed that the medium will be busy,** thus preventing them from transmitting and avoiding collision.

CSMA/CA: RTS-CTS Solution

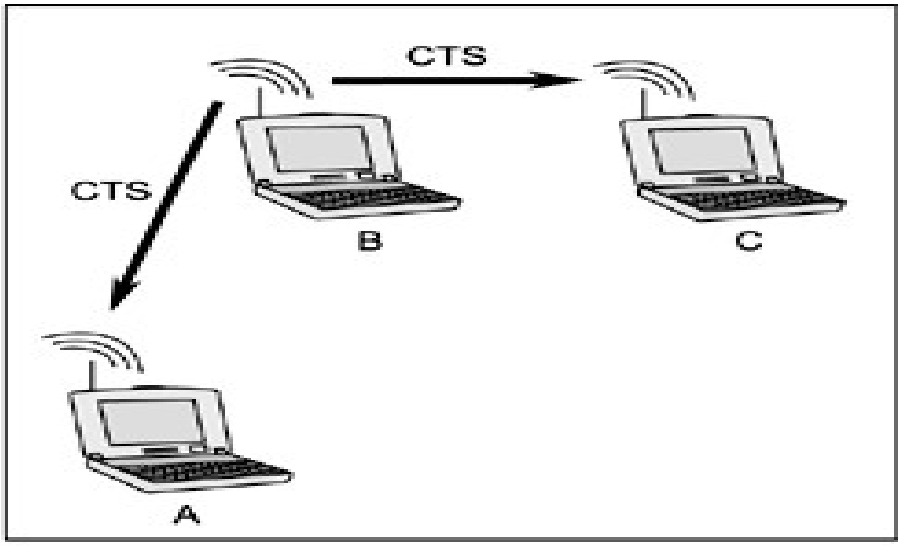
- With collision avoidance, stations exchange small control
- packets to determine which sender can transmit to a receiver.



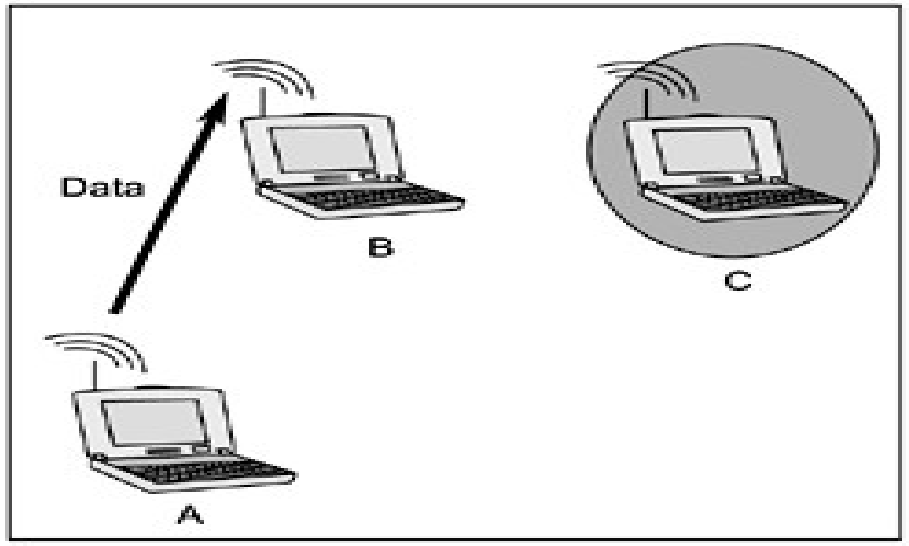
RTS-CTS handshake



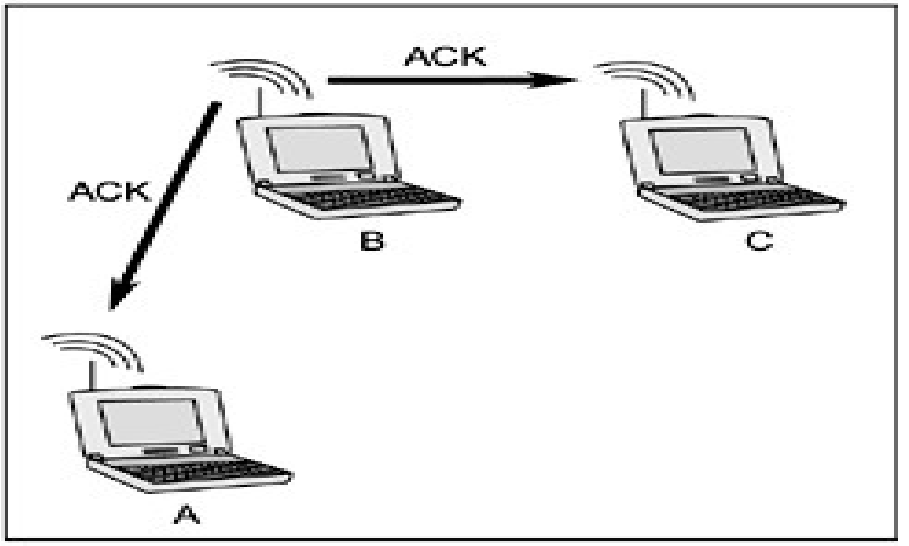
1. A transmits request (RTS) to B.



2. B replies that the channel is clear (CTS).
Both A & C overhear the broadcast.



3. A sends its data to B.
C is blocked from transmitting.



4. B acknowledges the data transfer.

Shortcomings of RTS-CTS Solution

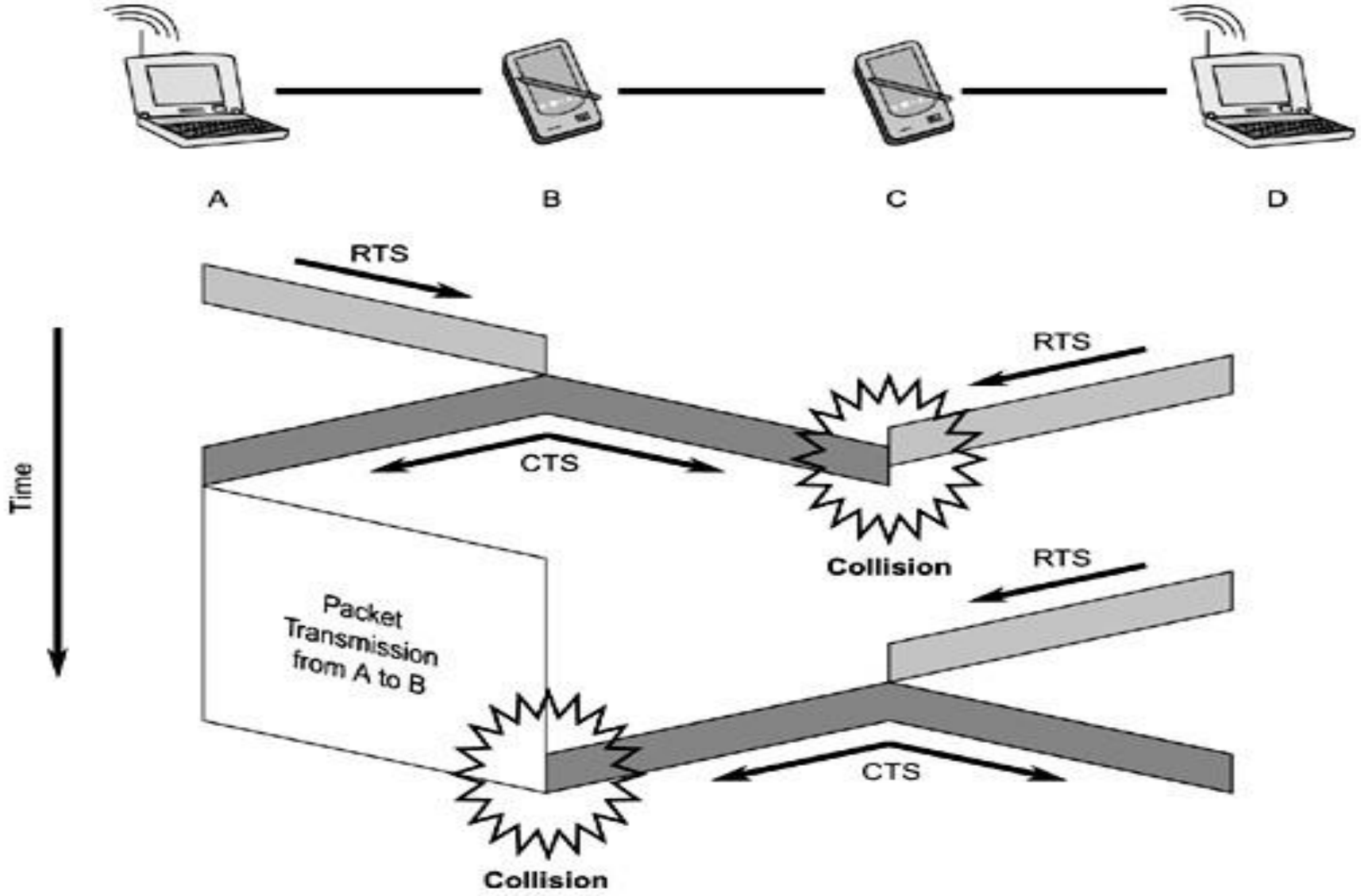
The RTS-CTS method is not a perfect solution to the hidden terminal problem.

Problematic scenario occurs when

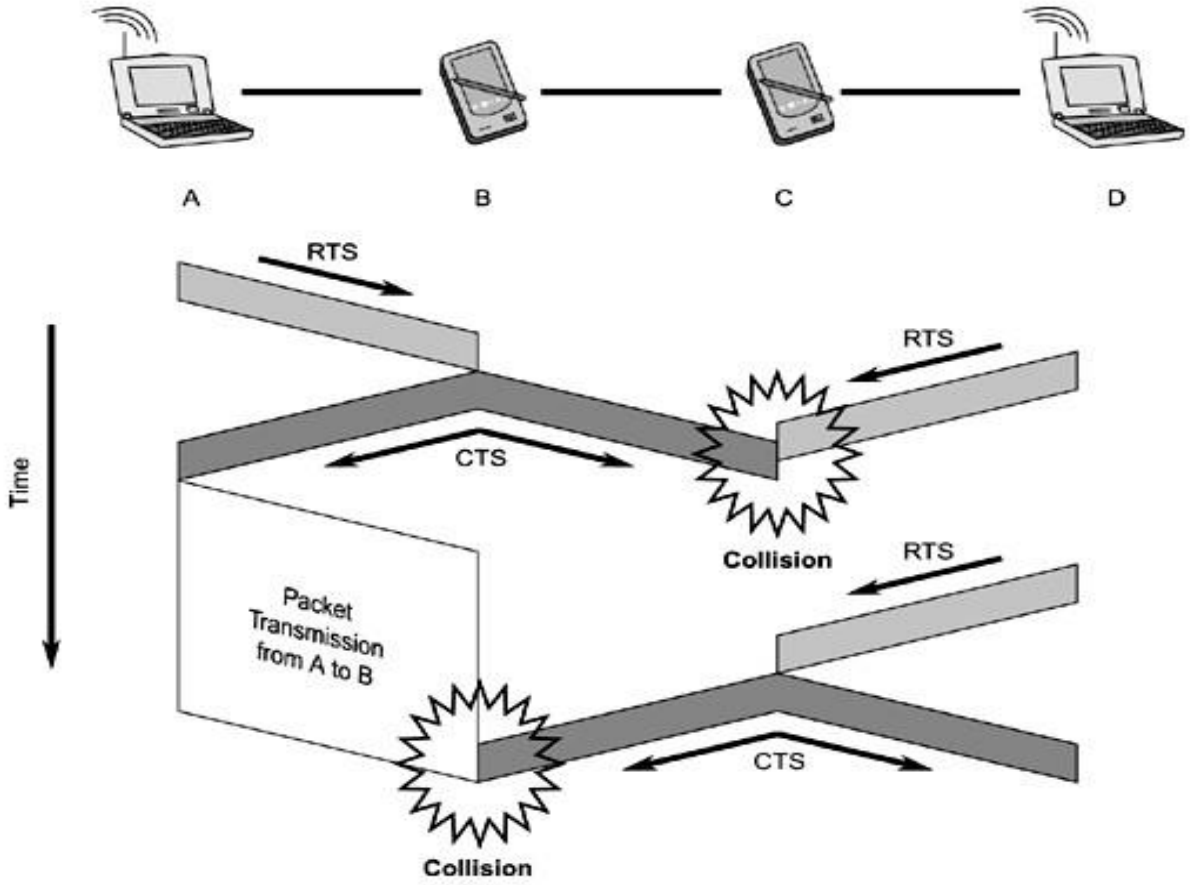
1. **RTS and CTS control messages are sent by different nodes.**

1. **Multiple CTS messages are granted to different neighboring nodes, causing collisions.**

a) Shortcomings of RTS-CTS Solution



a) Shortcomings of RTS-CTS Solution



- **Cases when collisions occur and the RTS and CTS control messages are sent by different nodes.**

1. Node B is granting a CTS to the RTS sent by node A.
2. This collides with the RTS sent by node D at node C. Node D is the hidden terminal from node B.
3. **As node D does not receive the expected CTS from node C, it retransmits the RTS.**
4. When node A receives the CTS, it is not aware of any collision at node C and hence it proceeds with a data transmission to node B.
5. Unfortunately, It collides with the CTS sent by node C in response to node D's RTS.

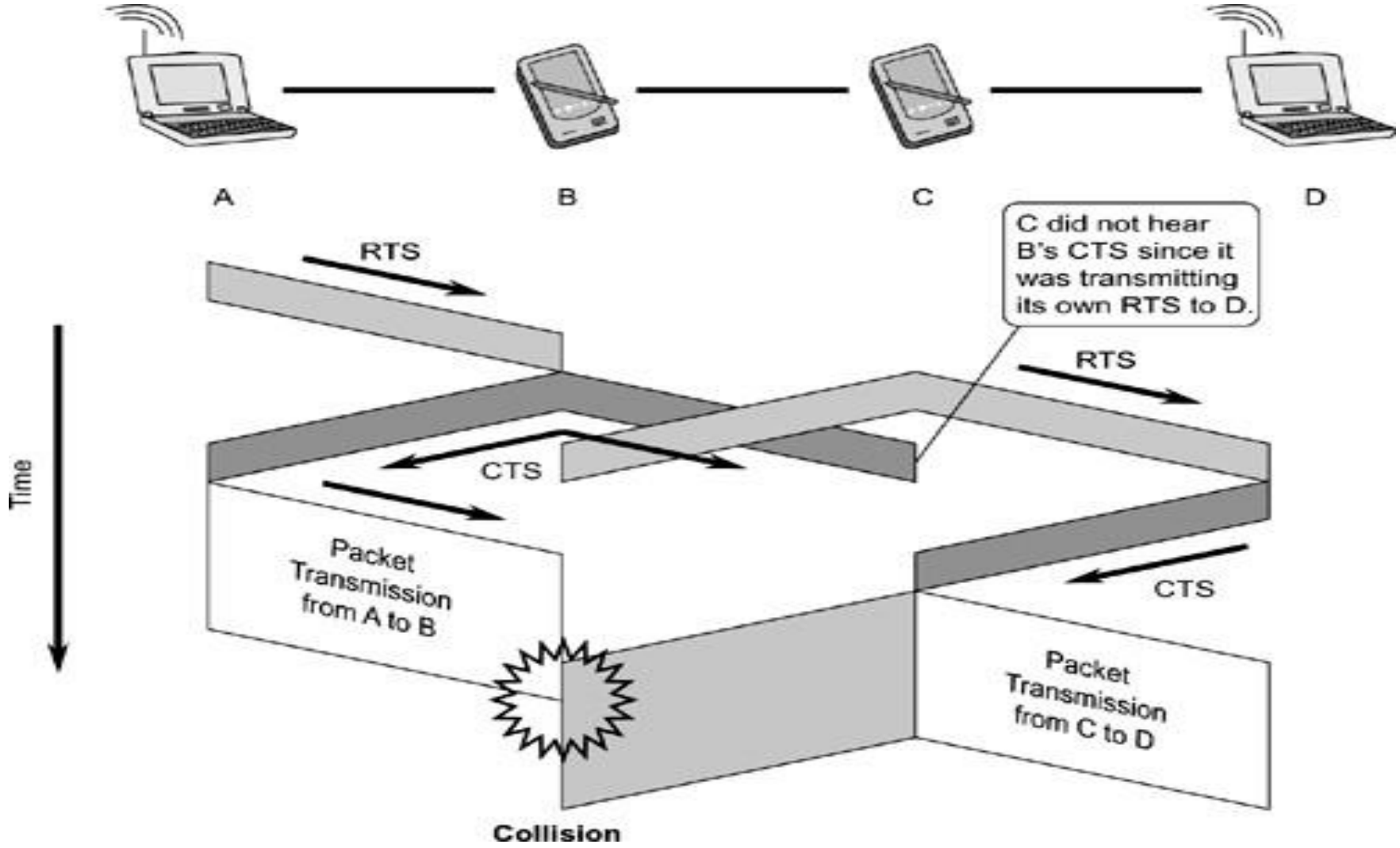
a) Shortcomings of RTS-CTS Solution

- **Cases when collisions occur and the RTS and CTS control messages are sent by different nodes.**

1. Node B is granting a CTS to the RTS sent by node A.
2. This collides with the RTS sent by node D at node C. Node D is the hidden terminal from node B.
3. As node D does not receive the expected CTS from node C, it retransmits the RTS.
4. When node A receives the CTS, it is not aware of any collision at node C and hence it proceeds with a data transmission to node B.
5. Unfortunately, It collides with the CTS sent by node C in response to node D's RTS.

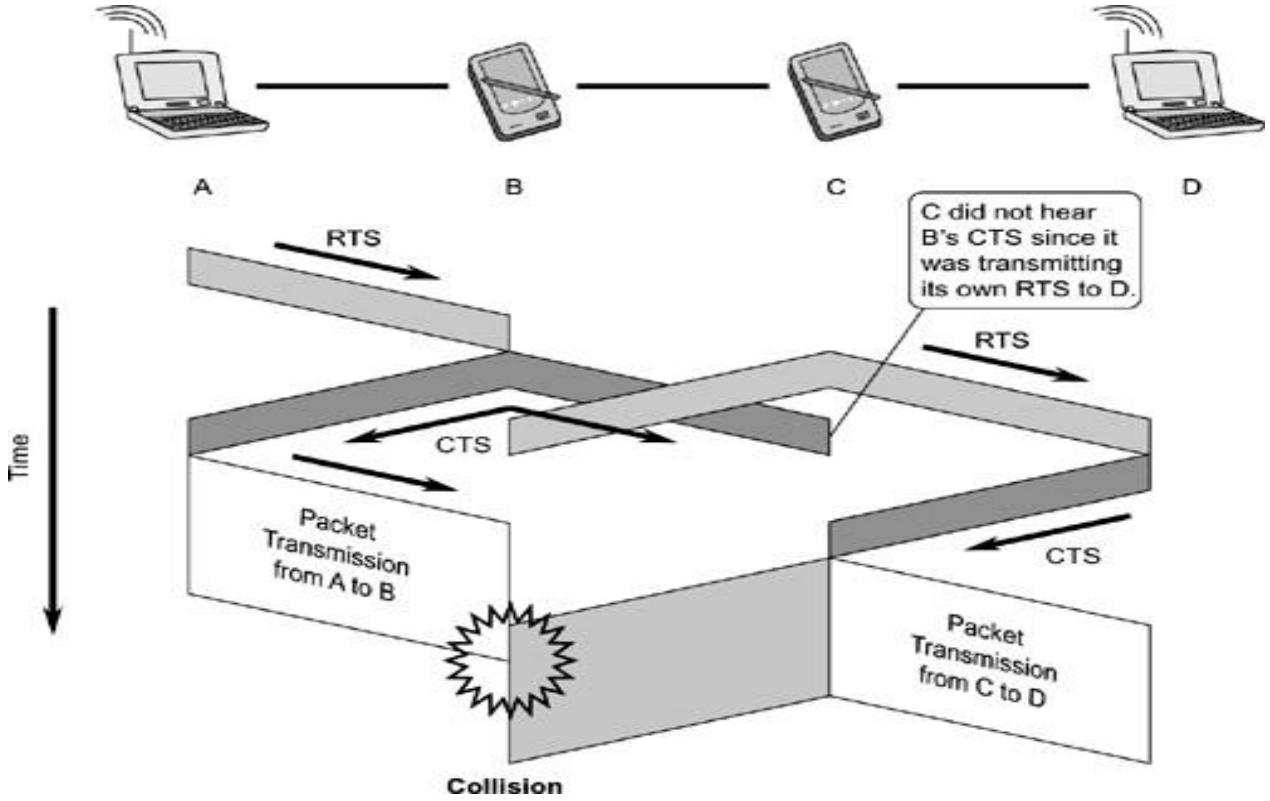
b) Shortcomings of RTS-CTS Solution

Multiple CTS messages are granted to different neighboring nodes, causing collisions.



b) Shortcomings of RTS-CTS Solution

Multiple CTS messages are granted to different neighboring nodes, causing collisions.



1. Two nodes are sending RTS messages to different nodes at different points in time.
2. Node A sends an RTS to node B. When node B is returning a CTS message back to node A, node C sends an RTS message to node B.
3. Because node C cannot hear the CTS sent by node B while it is transmitting an RTS to node D, node C is unaware of the communication between nodes A and B.
4. Node D proceeds to grant the CTS message to node C.
5. Since both nodes A and C are granted transmission, a collision will occur when both start sending data.

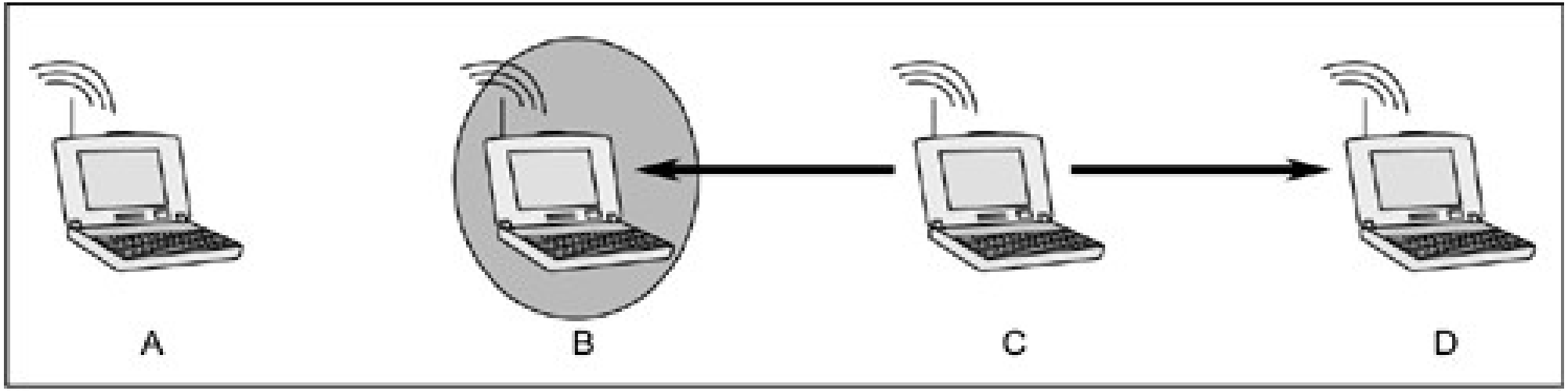
b) Shortcomings of RTS-CTS Solution

Multiple CTS messages are granted to different neighboring nodes, causing collisions.

1. Two nodes are sending RTS messages to different nodes at different points in time.
2. Node A sends an RTS to node B.When node B is returning a CTS message back to node A, node C sends an RTS message to node B.
3. Because node C cannot hear the CTS sent by node B while it is transmitting an RTS to node D, node C is unaware of the communication between nodes A and B.
4. Node D proceeds to grant the CTS message to node C.
5. Since both nodes A and C are granted transmission, a collision will occur when both start sending data.

Exposed Node Problem

- Overhearing a data transmission from neighboring nodes can inhibit one node from transmitting to other nodes. This is known as the **exposed node problem.**
- **An exposed node is a node in range of the transmitter, but out of range of the receiver.**



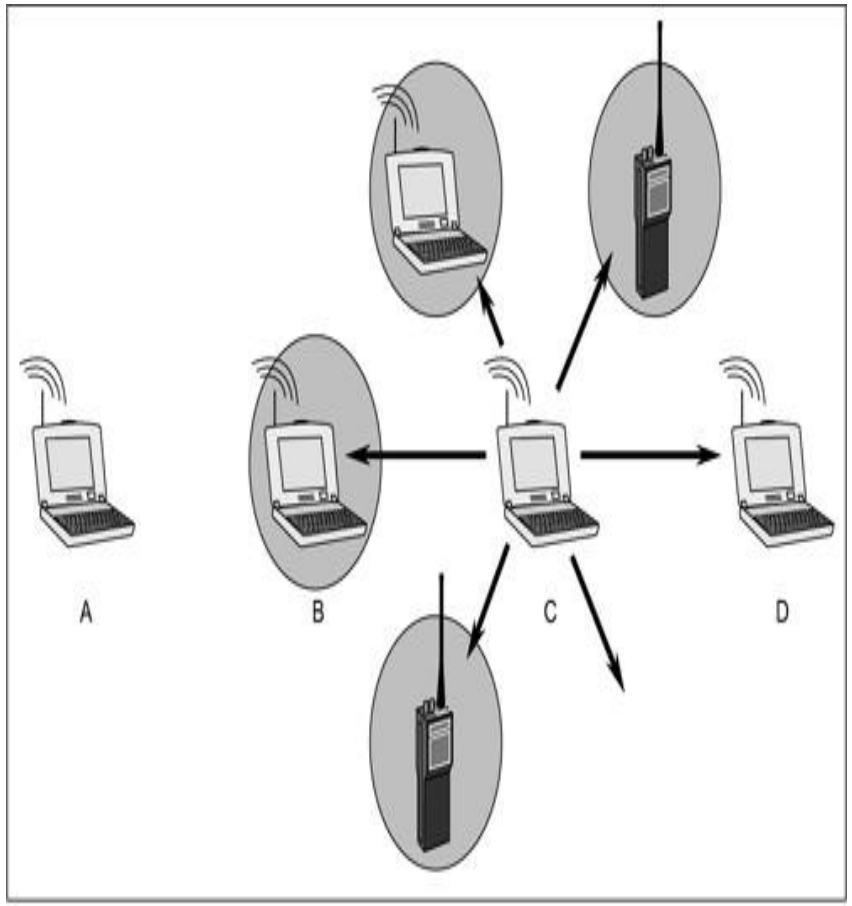
- C is transmitting to D.
- B overhears this, and is blocked.
- B wants to transmit to A, but is being blocked by C.
- Wasted bandwidth!

Solution to the exposed node problem

- **Use of separate control and data channels**
  - Power-Aware Multi-Access Protocol with Signaling (PAMAS)
  - Dual Busy Tone Multiple Access (DBTMA) .
- **Use of Antennas**
  - **Directional antennas**

Use of antennas.

- Mobile node using an **Omni-directional antenna** can result in several surrounding nodes being "**exposed**“
- Thus prohibiting them from communicating with other nodes.
- Lowers network availability and system throughput.

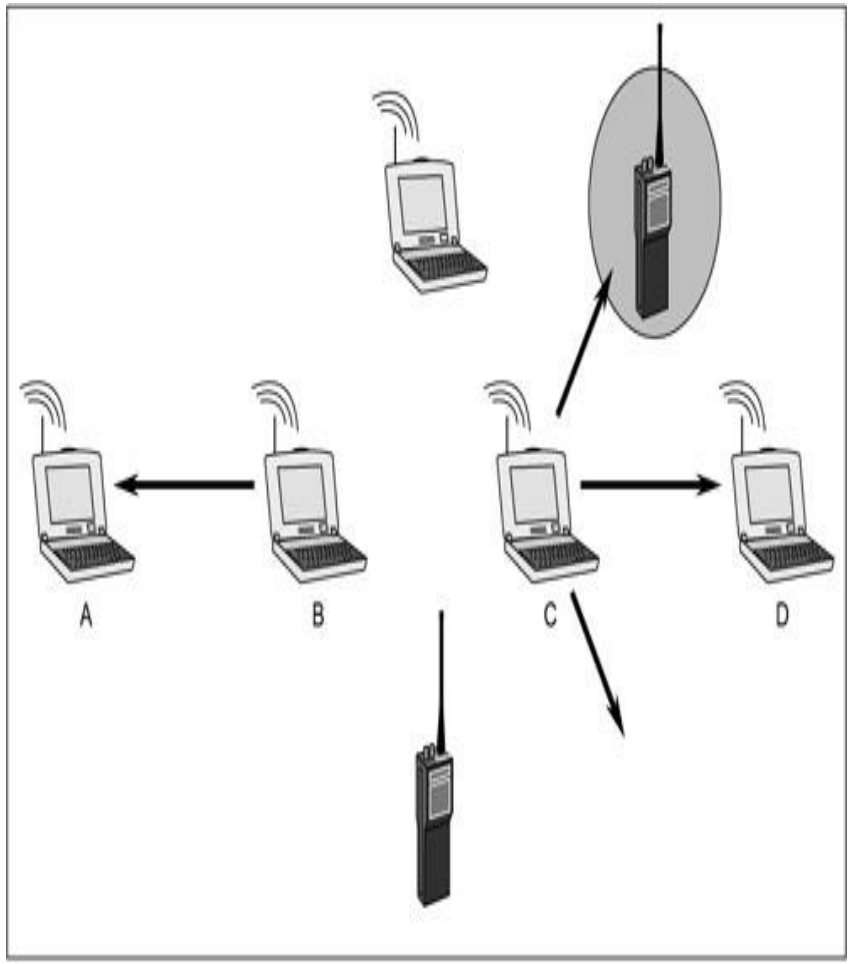


Omni-directional antenna used. All neighbors are exposed.

Omni-directional antenna *radiates radio wave power uniformly in all directions in one plane, with the radiated power decreasing with elevation angle above or below the plane, dropping to*

Use of antennas (cont…)

- If **directional antennas** are employed, the problem of network availability and system throughput can be mitigated.
- **Node C** can continue communicating with the receiving palm pilot device without impacting the communication between nodes A and B.
- The directivity provides spatial and connectivity isolation not found in omni-directional antenna systems.



Directional antenna reduces this problem! B is not blocked from sending to A.