Wired LANs: Ethernet

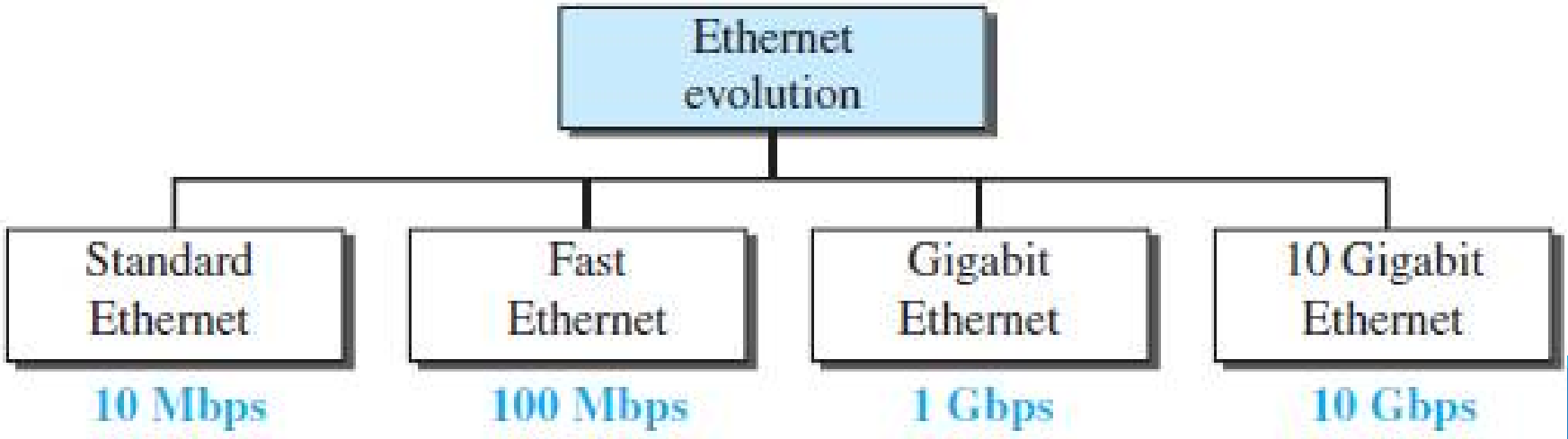
CS44 Data Communications

Dr. Shilpa Chaudhari

Department of Computer Science and Engineering
Ramaiah Institute of Technology Bangalore

Ethernet Evolution

- The Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs.
- Since then, it has gone through four generations
  - Standard Ethernet (10 Mbps)
  - Fast Ethernet (100 Mbps)
  - Gigabit Ethernet (1 Gbps)
  - 10 Gigabit Ethernet (10 Gbps)



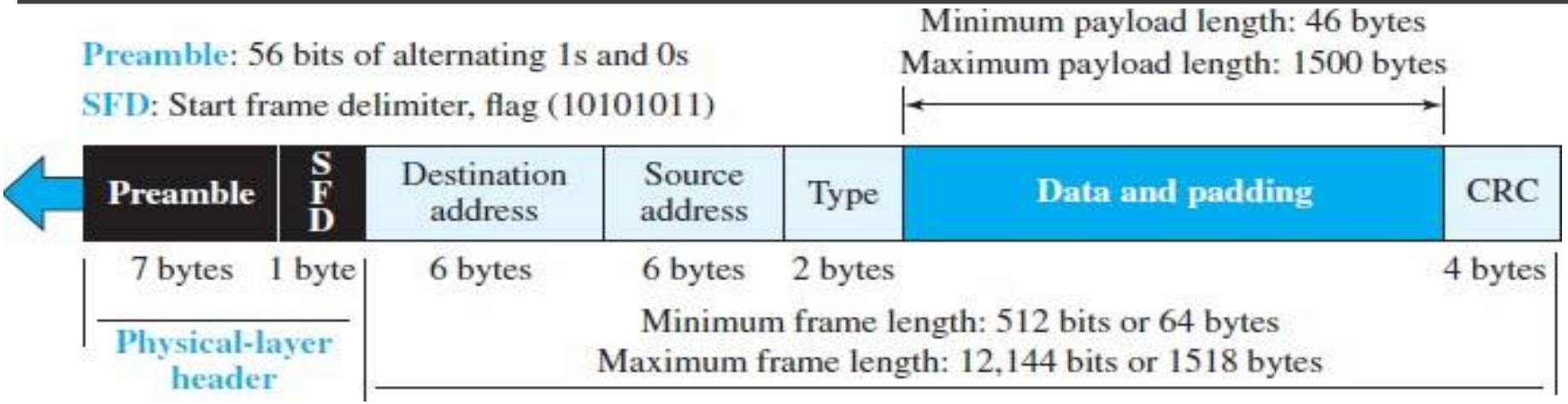
Standard Ethernet

- Original Ethernet technology with the data rate of 10 Mbps
- Although most implementations have moved to other technologies in the Ethernet evolution, there are some features of the Standard Ethernet that have not changed during the evolution
- Characteristics of the Standard Ethernet
  - Connectionless and Unreliable Service
  - Frame Format
  - Frame Length

Connectionless and Unreliable Service

- A connectionless service means each frame sent is independent of the previous or next frame
- Ethernet has no connection establishment or connection termination phases
  - The sender sends a frame whenever it has it; the receiver may or may not be ready for it.
  - The sender may overwhelm the receiver with frames, which may result in dropping frames
  - If a frame drops, the sender will not know about it
    - Since IP, which is using the service of Ethernet, is also connectionless
    - If the transport layer is also a connectionless protocol, such as UDP, the frame is lost and salvation may only come from the application layer
    - If the transport layer is TCP, the sender TCP does not receive acknowledgment for its segment and sends it again

Ethernet frame



- Ethernet is also unreliable like IP and UDP
  - If a frame is corrupted during transmission and the receiver finds out about the corruption, which has a high level of probability of happening because of the CRC-32, the receiver drops the frame silently
    - It is the duty of high-level protocols to find out about it
- Remember that an Ethernet frame is a variable-length frame
- Contains seven fields

Ethernet frame

- Preamble. This field contains 7 bytes (56 bits) of alternating 0s and 1s
  - alert the receiving system to the coming frame
  - enable it to synchronize its clock if it's out of synchronization
  - The pattern provides only an alert and a timing pulse
  - The 56-bit pattern allows the stations to miss some bits at the beginning of the frame
  - actually added at the physical layer and is not (formally) part of the frame
- Start frame delimiter (SFD)
  - 1 byte: 10101011) signals the beginning of the frame as the size of Ethernet frame is variable size
  - The SFD warns the station or stations that this is the last chance for synchronization
  - The last 2 bits are $(11)_2$ and alert the receiver that the next field is the destination address
  - The SFD field is also added at the physical layer

Ethernet frame

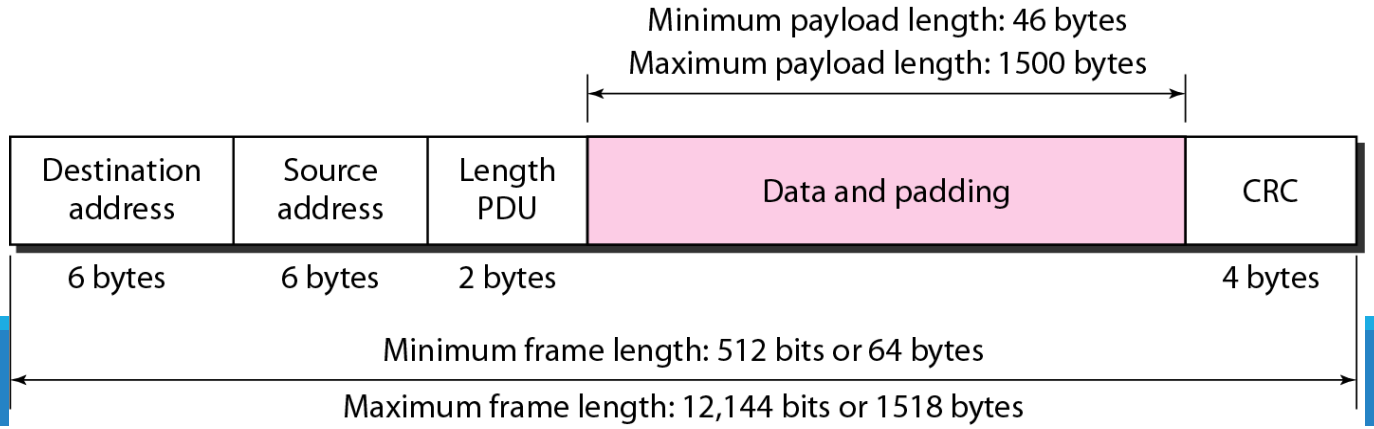
- Destination address (DA)
  - Six bytes (48 bits)
  - contains the linklayer address of the destination station or stations to receive the packet
  - When the receiver sees its own link-layer address, or a multicast address for a group that the receiver is a member of, or a broadcast address, it decapsulates the data from the frame and passes the data to the upperlayer protocol defined by the value of the type field
- Source address (SA)
  - Six bytes and contains the link-layer address of the sender of the packet
- Type
  - Defines the upper-layer protocol whose packet is encapsulated in the frame
    - This protocol can be IP, ARP, OSPF, and so on
  - It is used for multiplexing and demultiplexing.

Ethernet frame

- Data
  - encapsulated from the upper-layer protocols
  - minimum of 46 and a maximum of 1500 bytes
    - If the data coming from the upper layer is more than 1500 bytes, it should be fragmented and encapsulated in more than one frame
    - If it is less than 46 bytes, it needs to be padded with extra 0s
      - A padded data frame is delivered to the upper-layer protocol as it is (without removing the padding)
        - means that it is the responsibility of the upper layer to remove or, in the case of the sender, to add the padding
        - The upper-layer protocol needs to know the length of its data. For example, a datagram has a field that defines the length of the data
- CRC
  - contains error detection information, in this case a CRC-32
  - The CRC is calculated over the addresses, types, and data field
  - If the receiver calculates the CRC and finds that it is not zero (corruption in transmission), it discards the frame.

Frame Length

- Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame
- The minimum length restriction is required for the correct operation of CSMA/CD
  - An Ethernet frame - a minimum length of 512 bits or 64 bytes
- Part of the length is the header and the trailer
  - If 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC), then the minimum length of data from the upper layer is 64 – 18 = 46 bytes
    - If the upper-layer packet is less than 46 bytes, padding is added to make up the difference



Frame Length

- The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes
- If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes
- The maximum length restriction has two historical reasons
  - First, memory was very expensive when Ethernet was designed; a maximum length restriction helped to reduce the size of the buffer
  - Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send

frame length in bytes		data length in bytes	
Minimum	Maximum	Minimum	Maximum
64	1518	46	1500

END

Wireless LANs

IEEE 802.11 Terminology

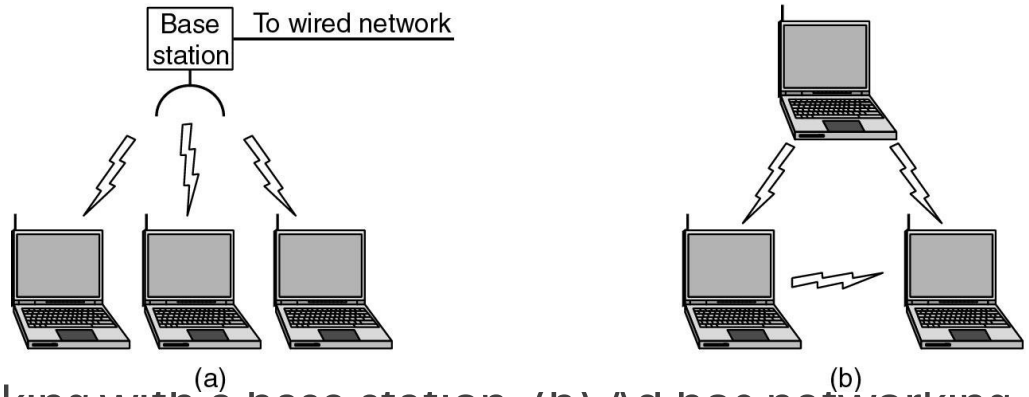
- Access point (AP): A station that provides access to the DS.
- Basic service set :

  a set is of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).

- Distribution system (DS): A system used to interconnect a set of BSSs to create an ESS.
  - DS is implementation-independent. It can be a wired 802.3 Ethernet LAN, 802.4 token bus, 802.5 token ring or another 802.11 medium.
- Extended service set (ESS):Two or more BSS interconnected by DS
  - extended service set uses two types of stations: mobile and stationary
  - The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN.

Categories of Wireless Networks

- ***Base Station*** :: all communication through an ***access point*** {note hub topology}. Other nodes can be fixed or mobile.
  - ***Infrastructure Wireless*** :: base station network is connected to the wired Internet.
- ***Ad hoc Wireless*** :: wireless nodes communicate directly with one another.
  - ***MANETs* (Mobile Ad Hoc Networks) ::** ad hoc nodes are mobile.



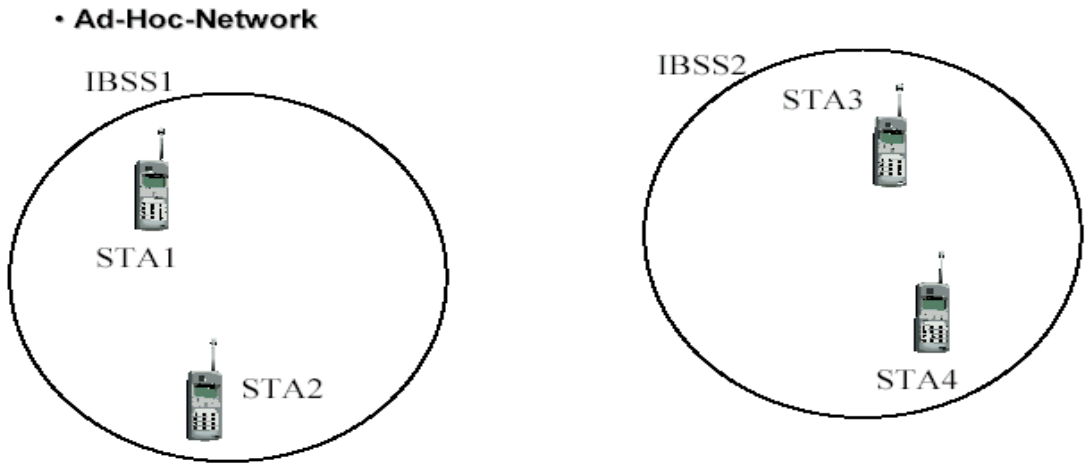
(a) Wireless networking with a base station. (b) Ad hoc networking.

Architecture

- The standard defines two kinds of services:
  - the basic service set (BSS)
    - building blocks of a wireless LAN
    - made of stationary or mobile wireless stations and an optional central base station, known as the *access point (AP)*
  - the extended service set (ESS)
    - made up of two or more BSSs with Aps
- Three types of stations based on their mobility in a wireless LAN:
  - no-transition - either stationary (not moving) or moving only inside a BSS
  - BSS-transition mobility - move from one BSS to another, but the movement is confined inside one ESS
  - ESS-transition mobility - move from one ESS to another
- IEEE 802.11 does not guarantee that communication is continuous during the move

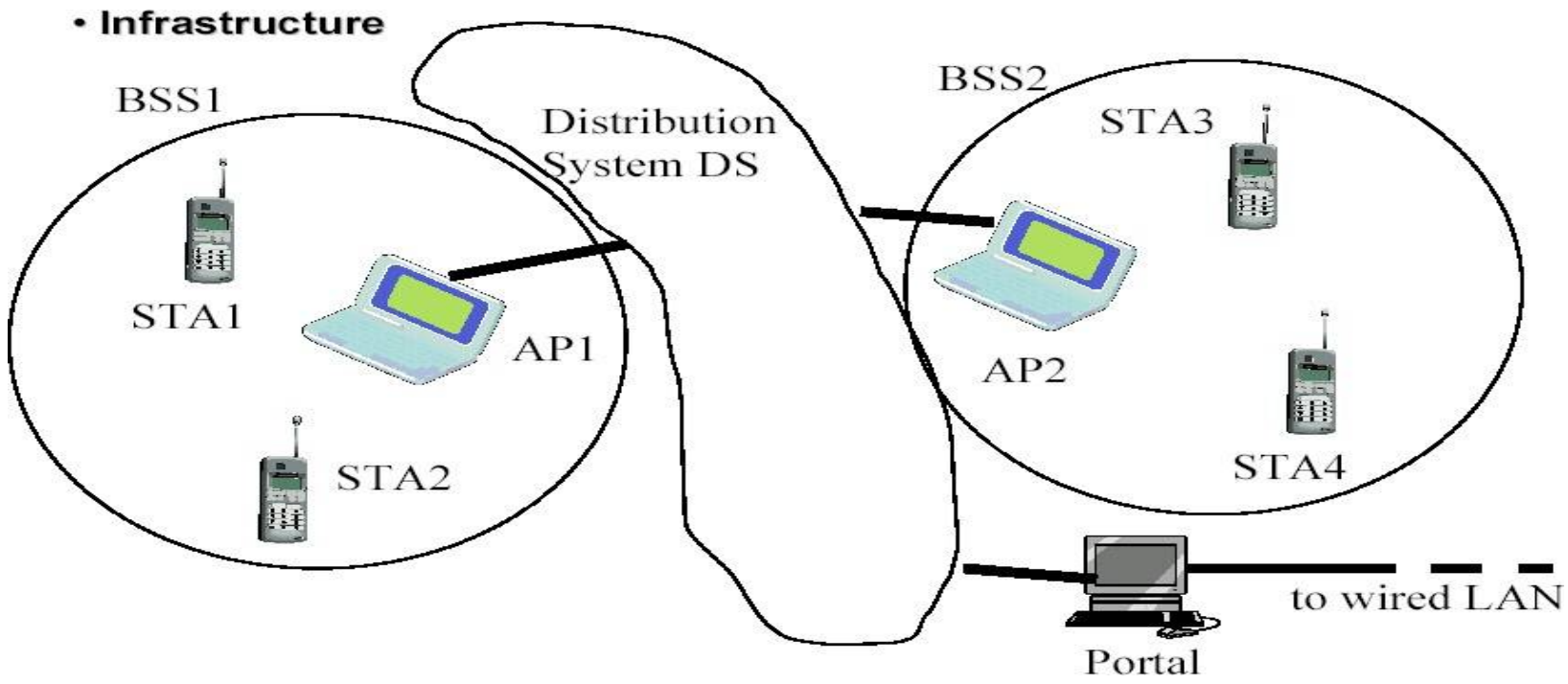
WLAN Topology - Ad-Hoc Network

- The BSS without an AP is a stand-alone network and cannot send data to other BSSs
- They can locate one another and agree to be part of a BSS



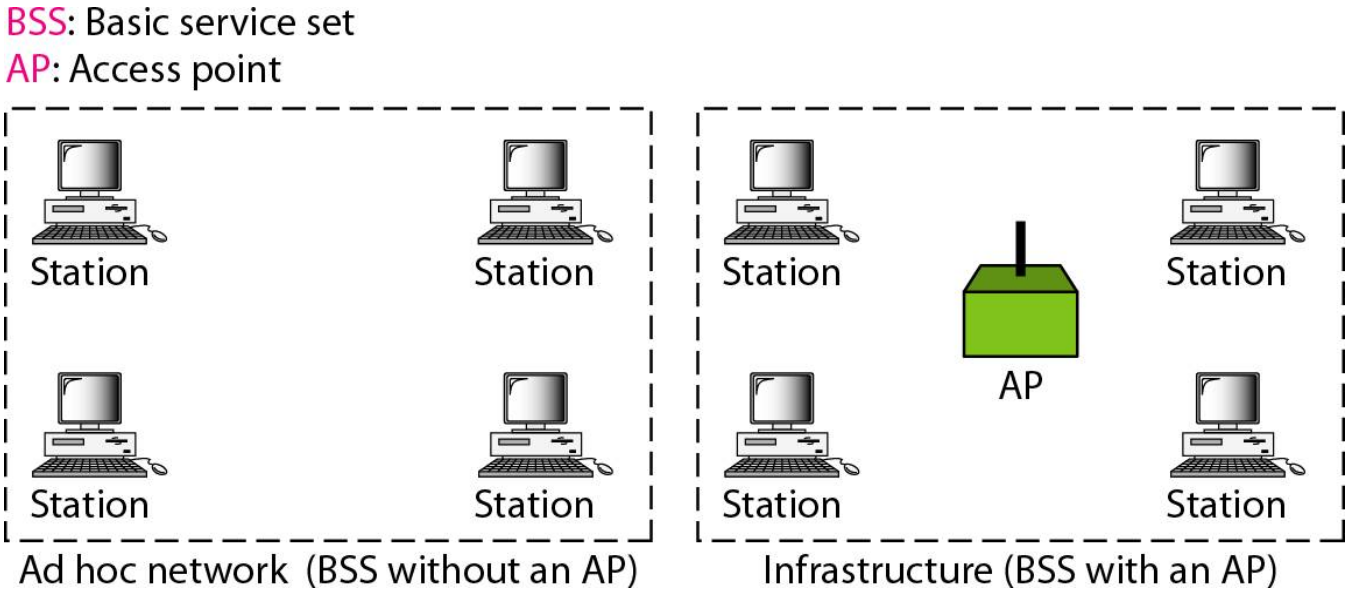
WLAN Topology Infrastructure

- EX: cellular network if we consider each BSS to be a cell and each AP to be a base station.



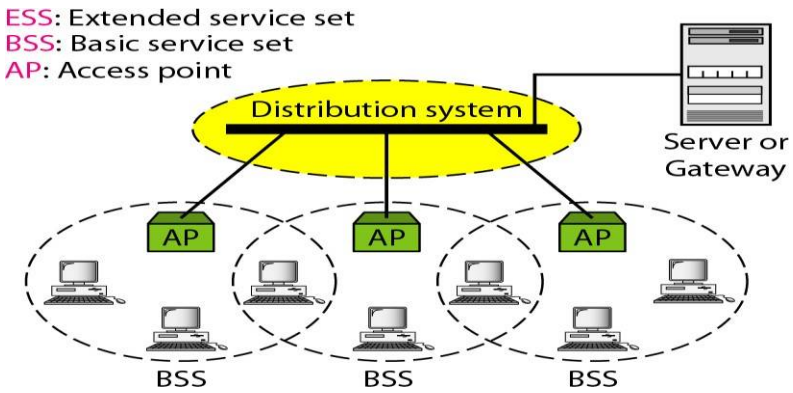
Basic service sets (BSSs)

- Building blocks of a wireless LAN
- Made of stationary or mobile wireless stations and an optional central base station, known as the *access point (AP)*
- The BSS without an AP is a stand-alone network and cannot send data to other BSSs - an *ad hoc architecture*
  - *stations* can locate one another and agree to be part of a BSS
- A BSS with an AP is sometimes referred to as an *infrastructure BSS.*



Distribution of Messages

- Distribution service (DS) - connects the APs in the BSSs
  - Used to exchange MAC frames from station in one BSS to station in another BSS



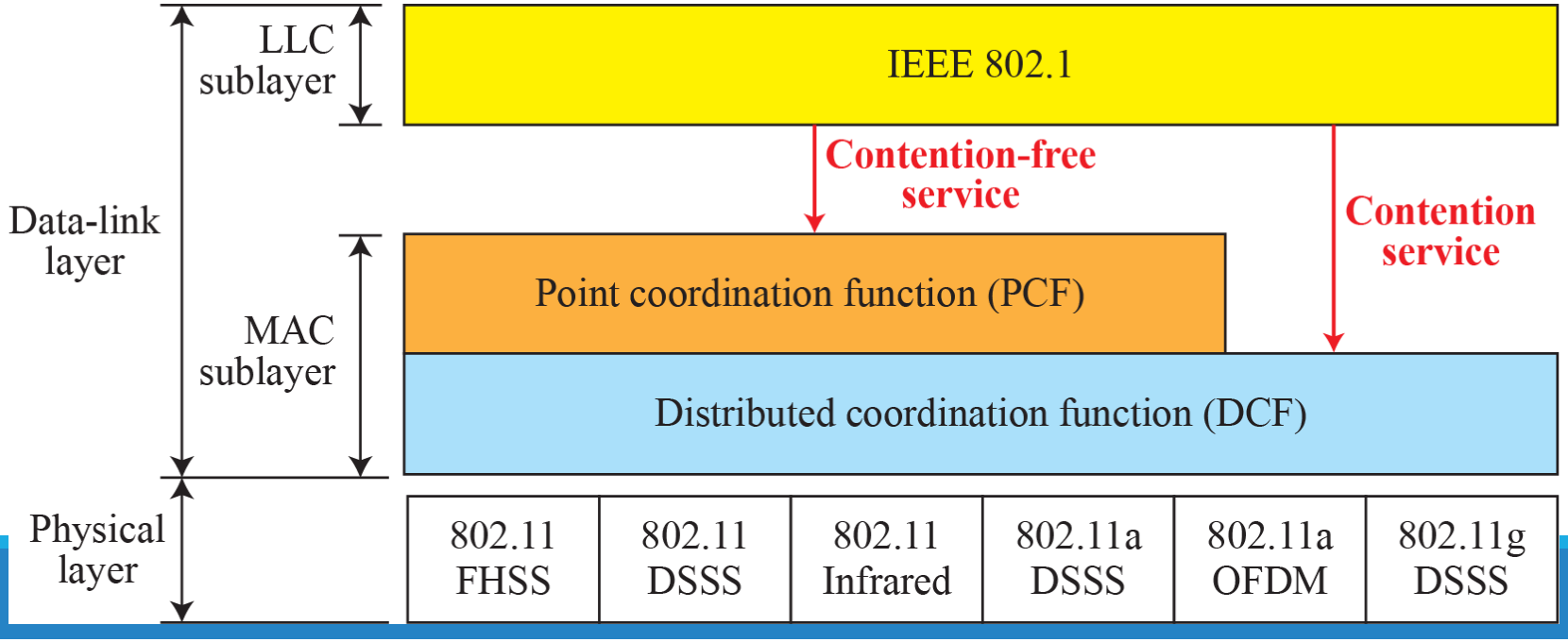
- When BSSs are connected, the stations within reach of one another can communicate without the use of an AP
  - uses two types of stations:
    - mobile - normal stations inside a BSS
    - Stationary - AP stations that are part of a wired LAN
- A mobile station can belong to more than one BSS at the same time

IEEE 802.11 Medium Access Control

- MAC layer covers three functional areas:
  - Reliable data delivery
  - Access control
  - Security

IEEE 802.11 defines two MAC sublayers:

- distributed coordination function (DCF)
- point coordination function (PCF)



MAC Sublayer

- Distributed Coordination Function (DCF)
  - Distributed access protocol
  - Contention-Based
  - Makes use of CSMA/CA rather than CSMA/CD for the following reasons:
    - Wireless LANs cannot implement *CSMA/CD for three reasons:*

1. For collision detection a station must be able to send data and receive collision signals at the same time(costly stations and increased bandwidth requirements).

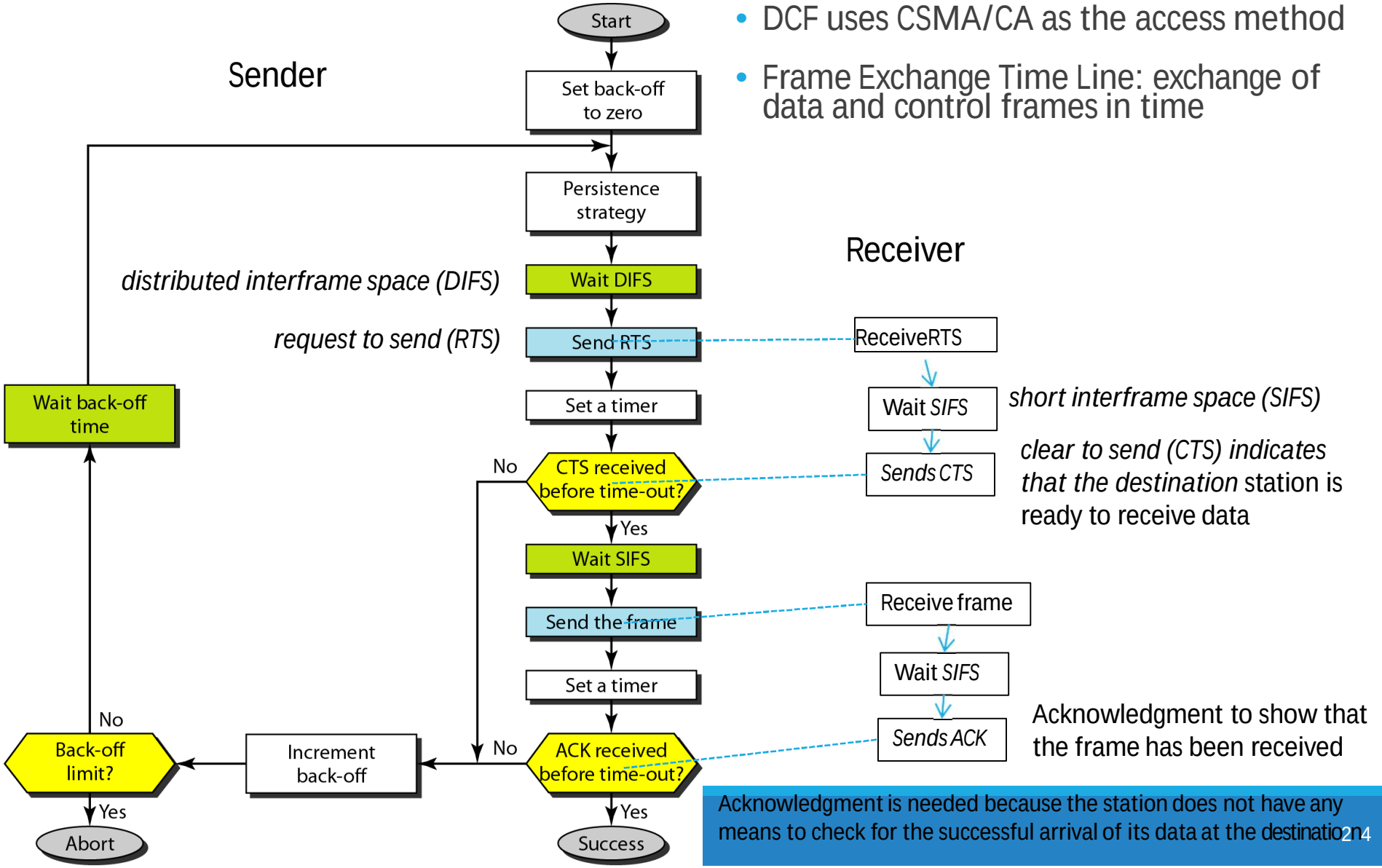
2. Collision may not be detected because of the hidden station problem.

3. The distance between stations may result in Signal fading which prevent a station at one end from hearing a collision at the other end.

Suited for ad hoc network and ordinary asynchronous traffic

Distributed Coordination Function (DCF)

- DCF uses CSMA/CA as the access method
- Frame Exchange Time Line: exchange of data and control frames in time



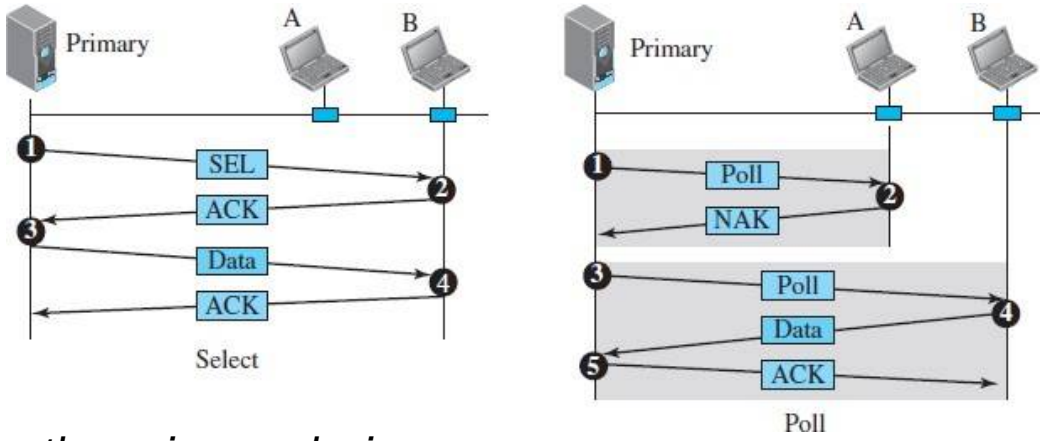
MAC Sublayer

- Point Coordination Function (PCF)
  - an optional access method on top of DCF
  - Implemented in an infrastructure network (not in an ad hoc network)
  - mostly for time-sensitive transmission services like voice or multimedia
  - a centralized, contention-free polling access method
  - The AP performs polling stations one after another, sending any data they have to the AP.

MAC Sublayer

- To give priority to PCF over DCF, another set of interframe spaces has been defined:
  - SIFS - Short Inter Frame Spacing
    - Used for immediate response actions e.g ACK, CTS
  - PIFS - Point Inter Frame Spacing
    - PIFS (PCF IFS) is shorter than the DIFS.
- if, at the same time, a station wants to use only DCF and an AP wants to use PCF, the AP has priority.
- Repetition interval has been designed to cover both contention-free (PCF) and contention-based (DCF) traffic to allow DCF accessing the media.

Polling in Repetition interval



- *used whenever the primary device has something to send.*
- *Primary* does not know whether the target device is prepared to receive
- Primary alert the secondary about the upcoming transmission and wait for an acknowledgment of the secondary's ready status using select (SEL) frame
- One field of SEL includes the address of the intended secondary

- *Used by the primary device to solicit transmissions from the secondary* devices
- When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send
- When the first secondary is approached, it responds either with a AK frame if it has nothing to send or with data if it does
- If the response is negative (a NAK frame), then the primary polls the next secondary in the same manner until it finds one with data to send
- When the response is positive (a data frame), the primary reads the frame and returns an acknowledgment (ACK frame), verifying its receipt

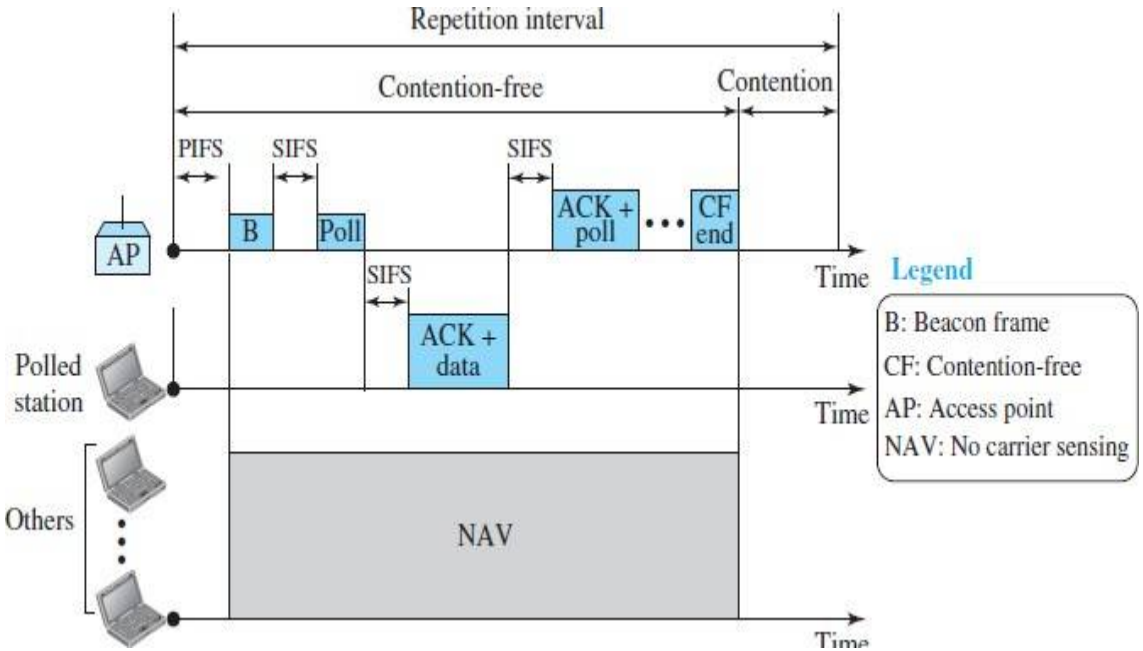
MAC Sublayer - Repetition interval

1. starts with B

3.PC (point controller) can send a poll frame, receive data, send an ACK, receive an ACK, or do any combination of these

4.PC sends a CF end (contention- free end) frame to allow the contention-based stations to use the medium

2. When the stations hear the beacon frame, they start their NAV for the duration of the contention-free period of the repetition interval



Fragmentation

- The wireless environment is very noisy.
- corrupt frame has to be retransmitted.
- Fragmentation is recommended.
  - the division of a large frame into smaller ones.
- It is more efficient to resend a small frame than a large one.

MAC Frame Format

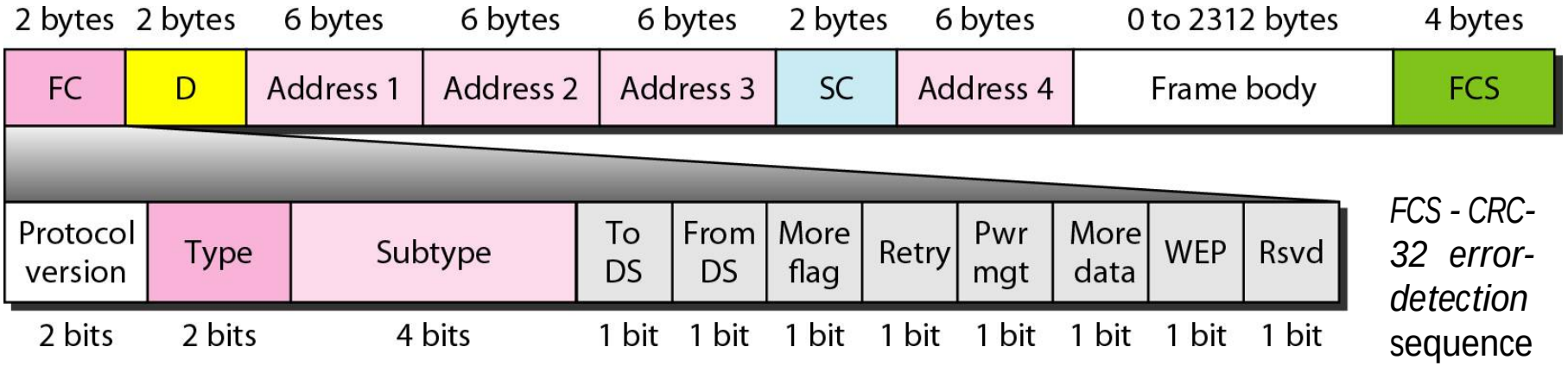
- The MAC layer frame consists of nine fields

duration of the transmission that is used to set the value of NAV. In one control frame, it defines the ID of the frame.

four address fields - meaning of each address field depends on the value of the To DS and From DS subfields

Sequence control (SC) - first four bits define the fragment number; the last 12 bits define the sequence number, which is the same in all fragments.

Frame body - information based on the type and the subtype defined in the FC field



FCS - CRC-32 error-detection sequence

Frame control (FC)- type of frame and some control information

MAC Sublayer - *Frame Format*

- Subfields in FC field

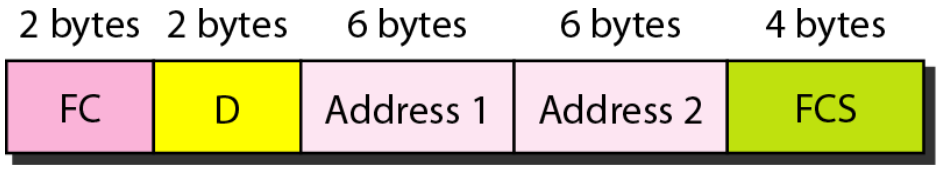
Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 14.2)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

Frame Types

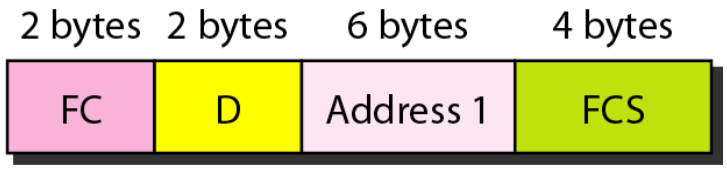
- IEEE 802.11 has three categories of frames:
  - management frames:

    used for the initial communication between stations and access points.
  - control frames.

    used for accessing the channel and acknowledging frames



RTS



CTS or ACK

value of the type field is 01; the values of the subtype fields

Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

  - data frames.

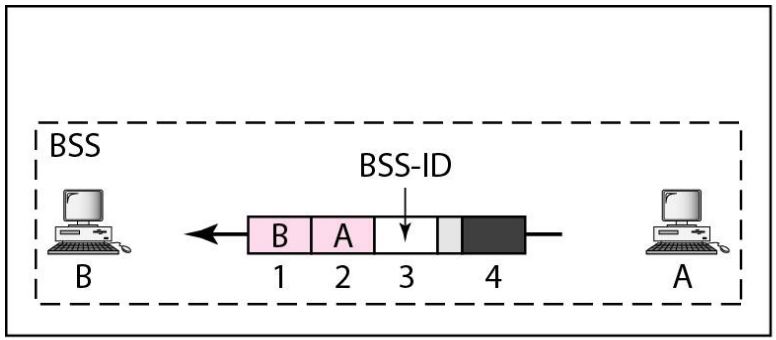
    Data frames are used for carrying data and control information.

Addressing Mechanism

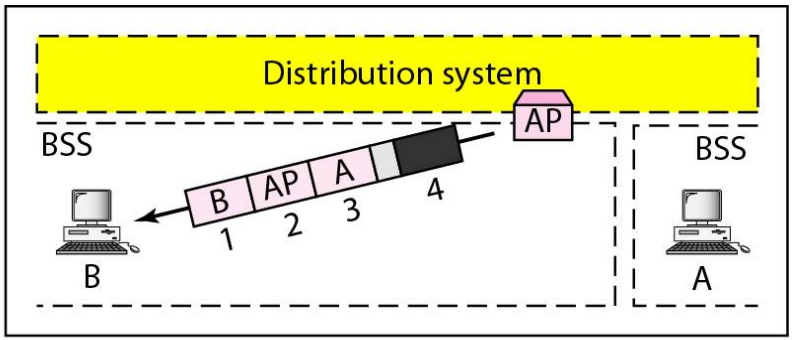
- IEEE 802.11 addressing mechanism specifies four cases defined by the value of the two flags in the FC field, *To DS and From DS*
  - Each flag can be either 0 or 1, resulting in four different situations
  - The interpretation of the four addresses (address 1 to address 4) in the MAC frame depends on the value of these flags

Addressing Mechanism

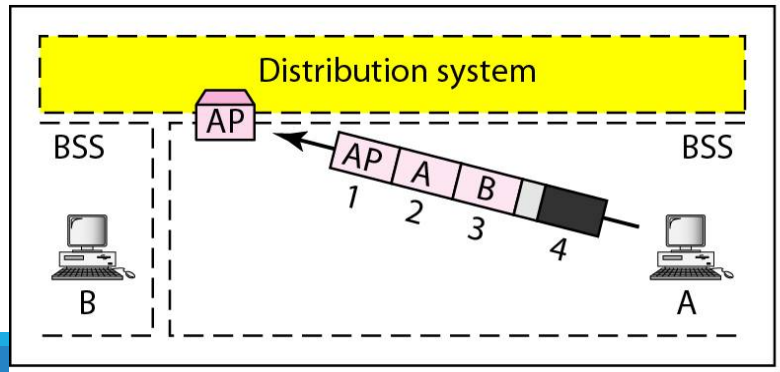
To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source



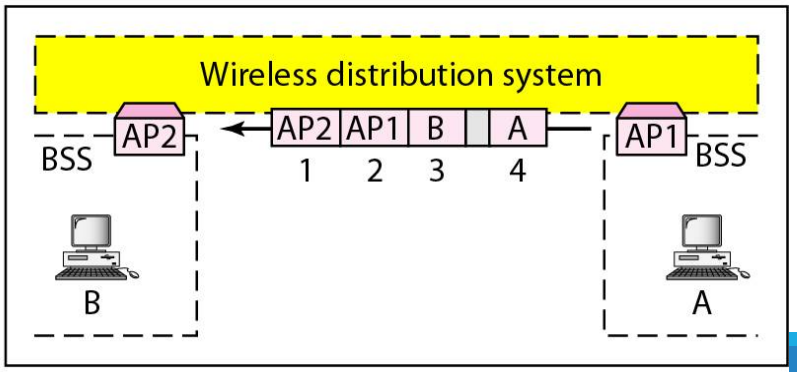
a. Case 1



b. Case 2



c. Case 3



d. Case 4

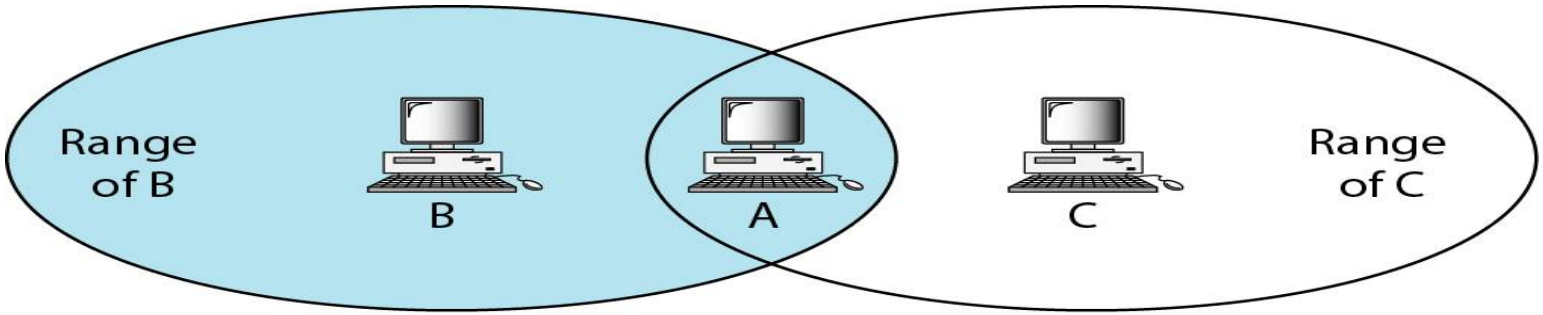
Addressing Mechanism

- Case 1: 00, To DS = 0 and From DS = 0
  - This means that the frame is not going to a distribution system and is not coming from a distribution system.
  - The ACK frame should be sent to the original sender.
- Case 2: 01, In this case, To DS = 0 and From DS = 1.
  - This means that the frame is coming from a distribution system (coming from an AP).
  - The ACK should be sent to the AP
  - The addresses are as address 3 contains the original sender of the frame (in another BSS).

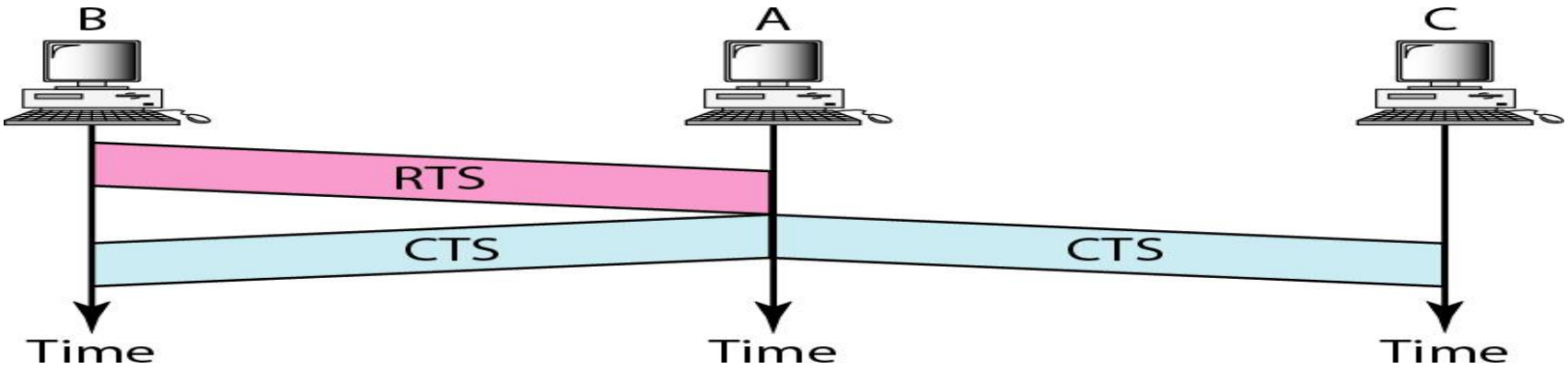
Addressing Mechanism

- Case 3: 10, To DS =1 and From DS =O.
  - This means that the frame is going to a distribution system (frame is going from a station to an AP)
  - The ACK is sent to the original station.
  - address 3 contains the final destination of the frame (in another BSS).
- Case 4:11, To DS =1 and From DS =1.
  - This is the case in which the distribution the frame is going from one AP to another AP in a wireless distribution system.
  - We do not need to define addresses if the distribution system is a wired LAN because the frame in these cases has the format of a wired LAN frame (Ethernet, for example).
  - Here, we need four addresses to define the original sender, the final destination, and two intermediate APs.

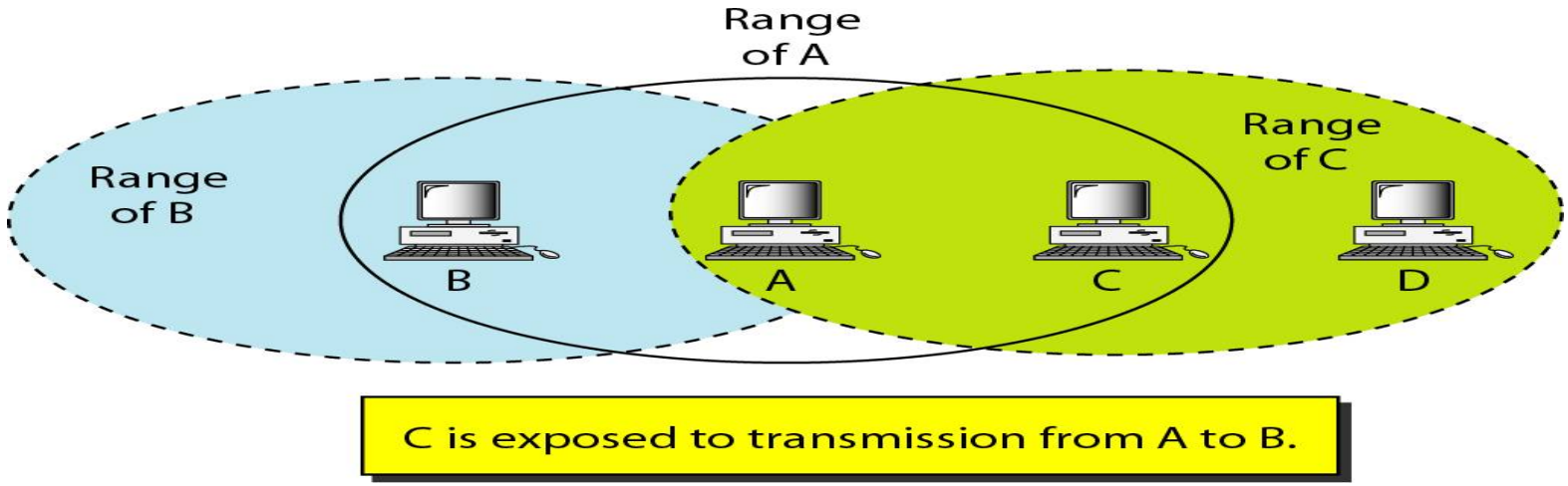
Hidden Station Problem



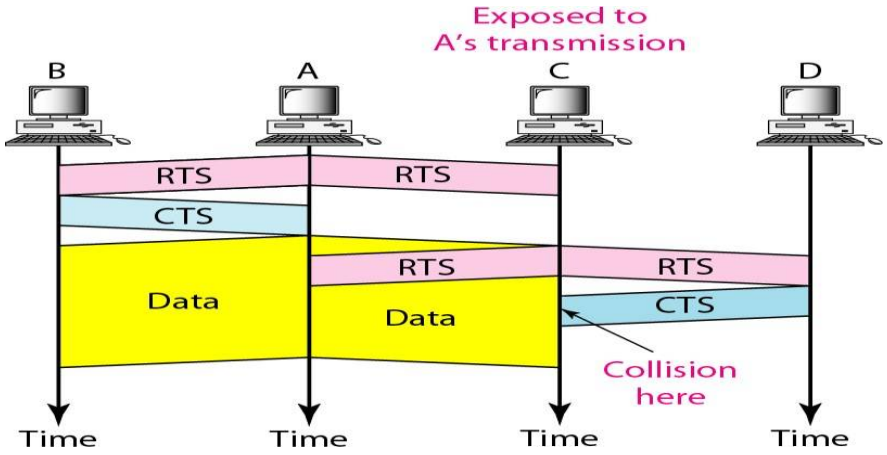
B and C are hidden from each other with respect to A.



Exposed Station Problems



- Station A is transmitting to station B.
- Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B
- However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending
- The handshaking messages RTS and CTS cannot help in this case
- Station C hears the RTS from A and refrains from sending, even though the communication between C and D cannot cause a collision in the zone between A and C; station C cannot know that station A's transmission does not affect the zone between C and D.



END

Wireless LANs

IEEE 802.11 Terminology

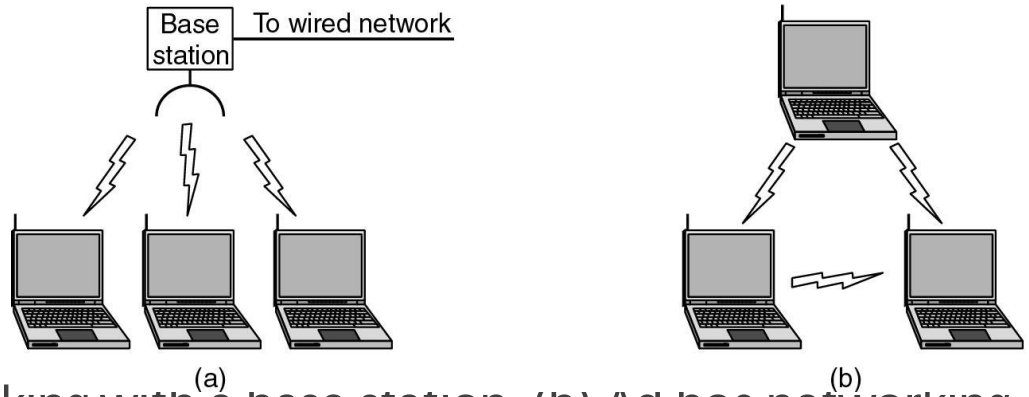
- Access point (AP): A station that provides access to the DS.
- Basic service set :

  a set is of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).

- Distribution system (DS): A system used to interconnect a set of BSSs to create an ESS.
  - DS is implementation-independent. It can be a wired 802.3 Ethernet LAN, 802.4 token bus, 802.5 token ring or another 802.11 medium.
- Extended service set (ESS):Two or more BSS interconnected by DS
  - extended service set uses two types of stations: mobile and stationary
  - The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN.

Categories of Wireless Networks

- ***Base Station*** :: all communication through an ***access point*** {note hub topology}. Other nodes can be fixed or mobile.
  - ***Infrastructure Wireless*** :: base station network is connected to the wired Internet.
- ***Ad hoc Wireless*** :: wireless nodes communicate directly with one another.
  - ***MANETs* (Mobile Ad Hoc Networks) ::** ad hoc nodes are mobile.



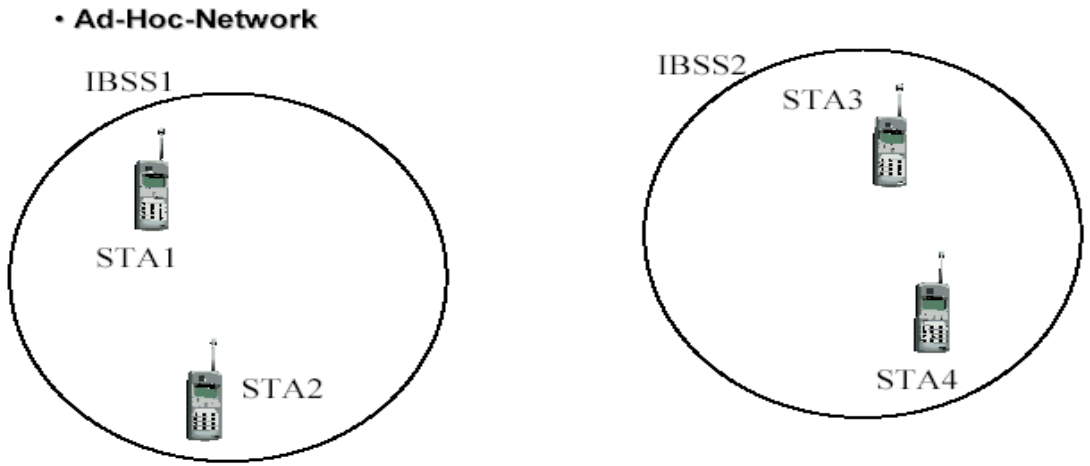
(a) Wireless networking with a base station. (b) Ad hoc networking.

Architecture

- The standard defines two kinds of services:
  - the basic service set (BSS)
    - building blocks of a wireless LAN
    - made of stationary or mobile wireless stations and an optional central base station, known as the *access point (AP)*
  - the extended service set (ESS)
    - made up of two or more BSSs with Aps
- Three types of stations based on their mobility in a wireless LAN:
  - no-transition - either stationary (not moving) or moving only inside a BSS
  - BSS-transition mobility - move from one BSS to another, but the movement is confined inside one ESS
  - ESS-transition mobility - move from one ESS to another
- IEEE 802.11 does not guarantee that communication is continuous during the move

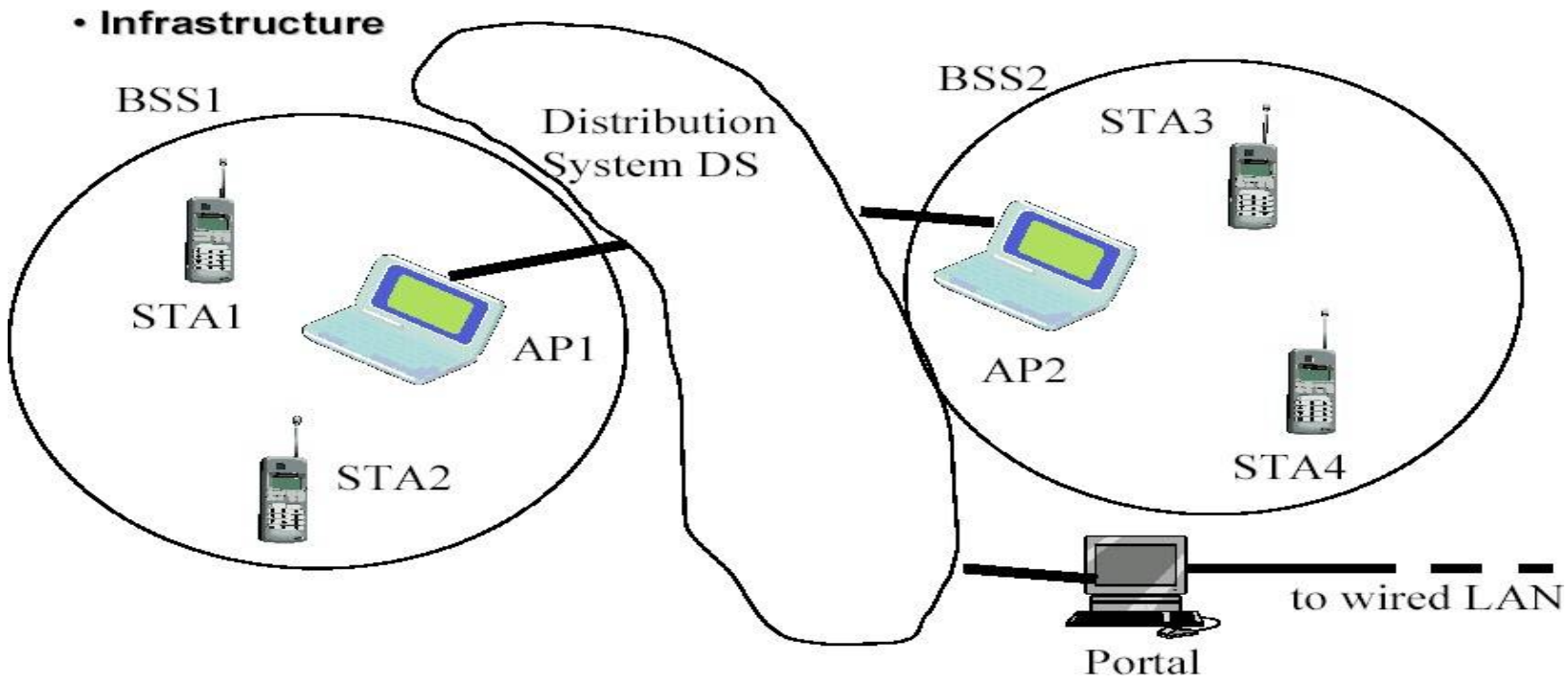
WLAN Topology - Ad-Hoc Network

- The BSS without an AP is a stand-alone network and cannot send data to other BSSs
- They can locate one another and agree to be part of a BSS



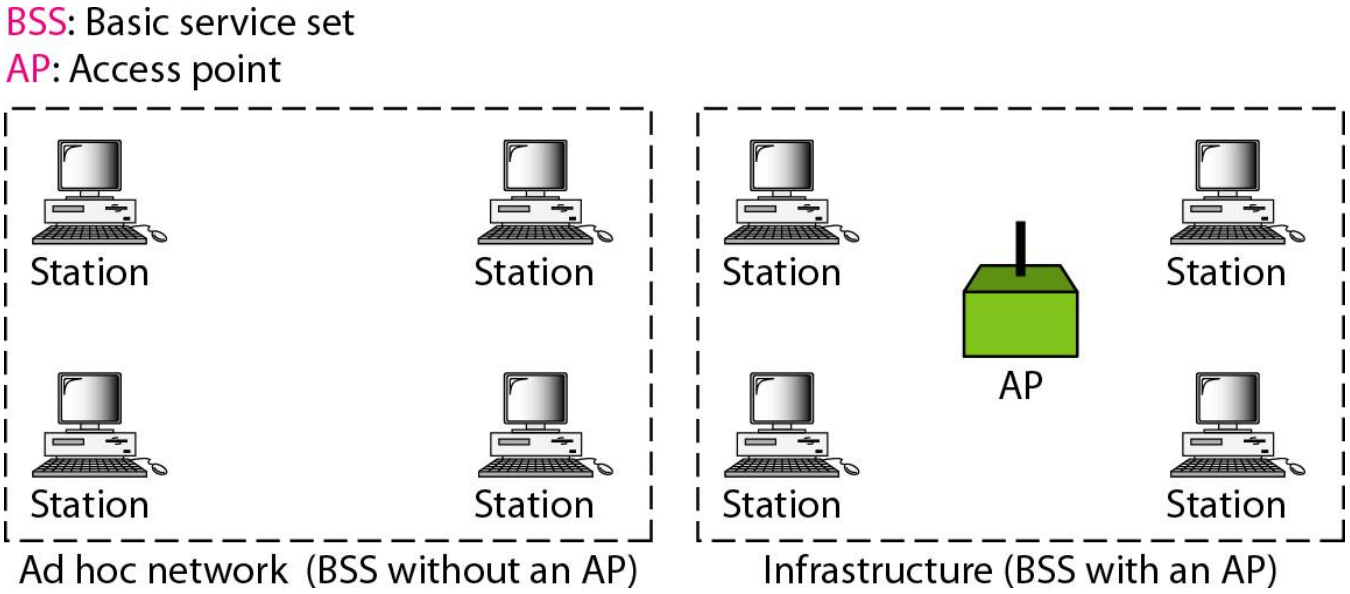
WLAN Topology Infrastructure

- EX: cellular network if we consider each BSS to be a cell and each AP to be a base station.



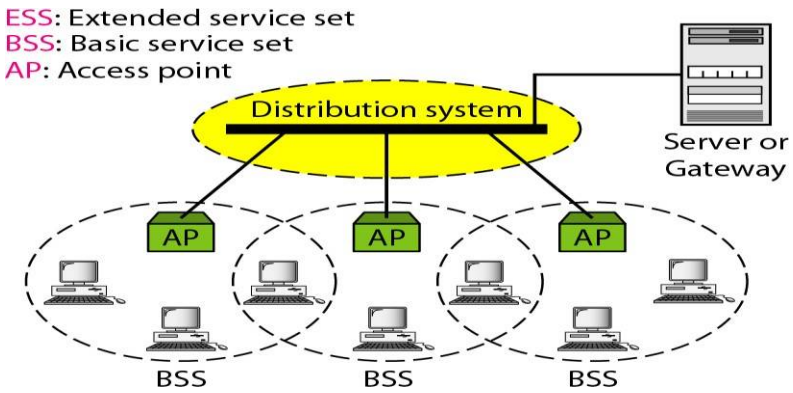
Basic service sets (BSSs)

- Building blocks of a wireless LAN
- Made of stationary or mobile wireless stations and an optional central base station, known as the *access point (AP)*
- The BSS without an AP is a stand-alone network and cannot send data to other BSSs - an *ad hoc architecture*
  - *stations* can locate one another and agree to be part of a BSS
- A BSS with an AP is sometimes referred to as an *infrastructure BSS.*



Distribution of Messages

- Distribution service (DS) - connects the APs in the BSSs
  - Used to exchange MAC frames from station in one BSS to station in another BSS



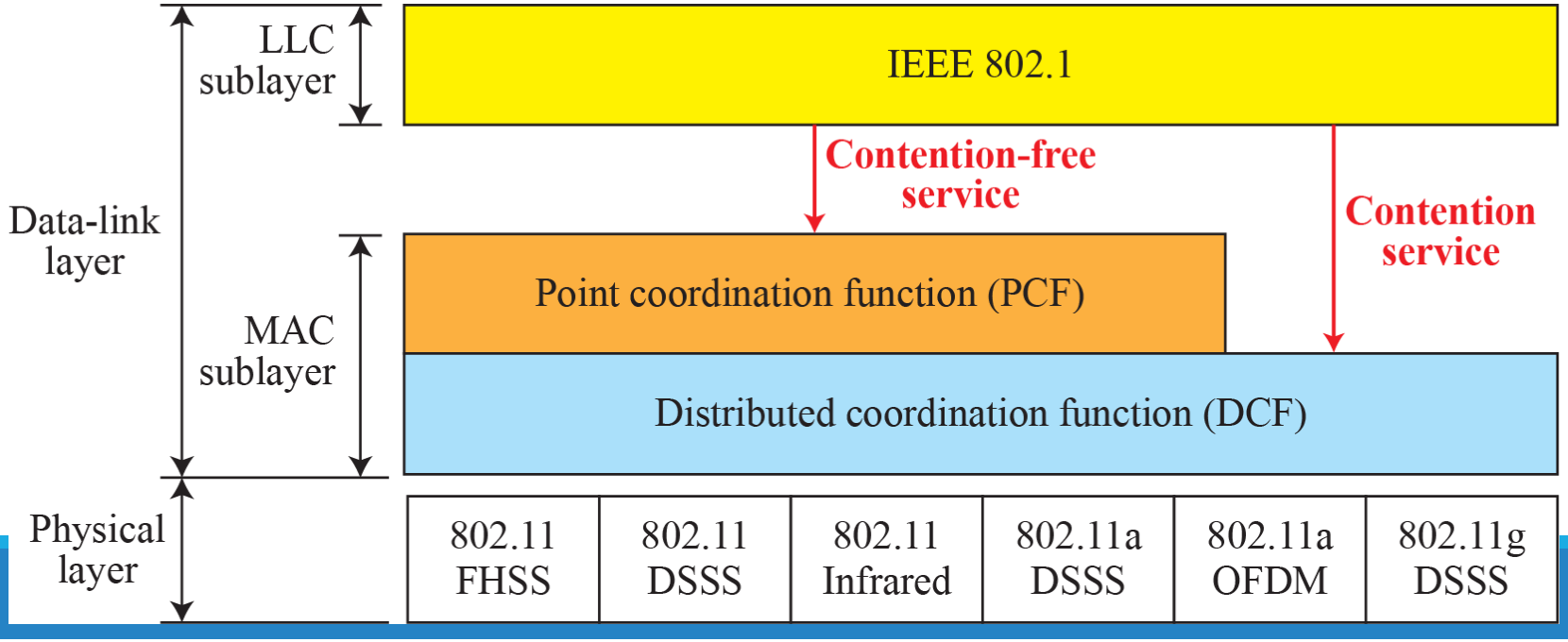
- When BSSs are connected, the stations within reach of one another can communicate without the use of an AP
  - uses two types of stations:
    - mobile - normal stations inside a BSS
    - Stationary - AP stations that are part of a wired LAN
- A mobile station can belong to more than one BSS at the same time

IEEE 802.11 Medium Access Control

- MAC layer covers three functional areas:
  - Reliable data delivery
  - Access control
  - Security

IEEE 802.11 defines two MAC sublayers:

- distributed coordination function (DCF)
- point coordination function (PCF)



MAC Sublayer

- Distributed Coordination Function (DCF)
  - Distributed access protocol
  - Contention-Based
  - Makes use of CSMA/CA rather than CSMA/CD for the following reasons:
    - Wireless LANs cannot implement *CSMA/CD for three reasons:*

1. For collision detection a station must be able to send data and receive collision signals at the same time(costly stations and increased bandwidth requirements).

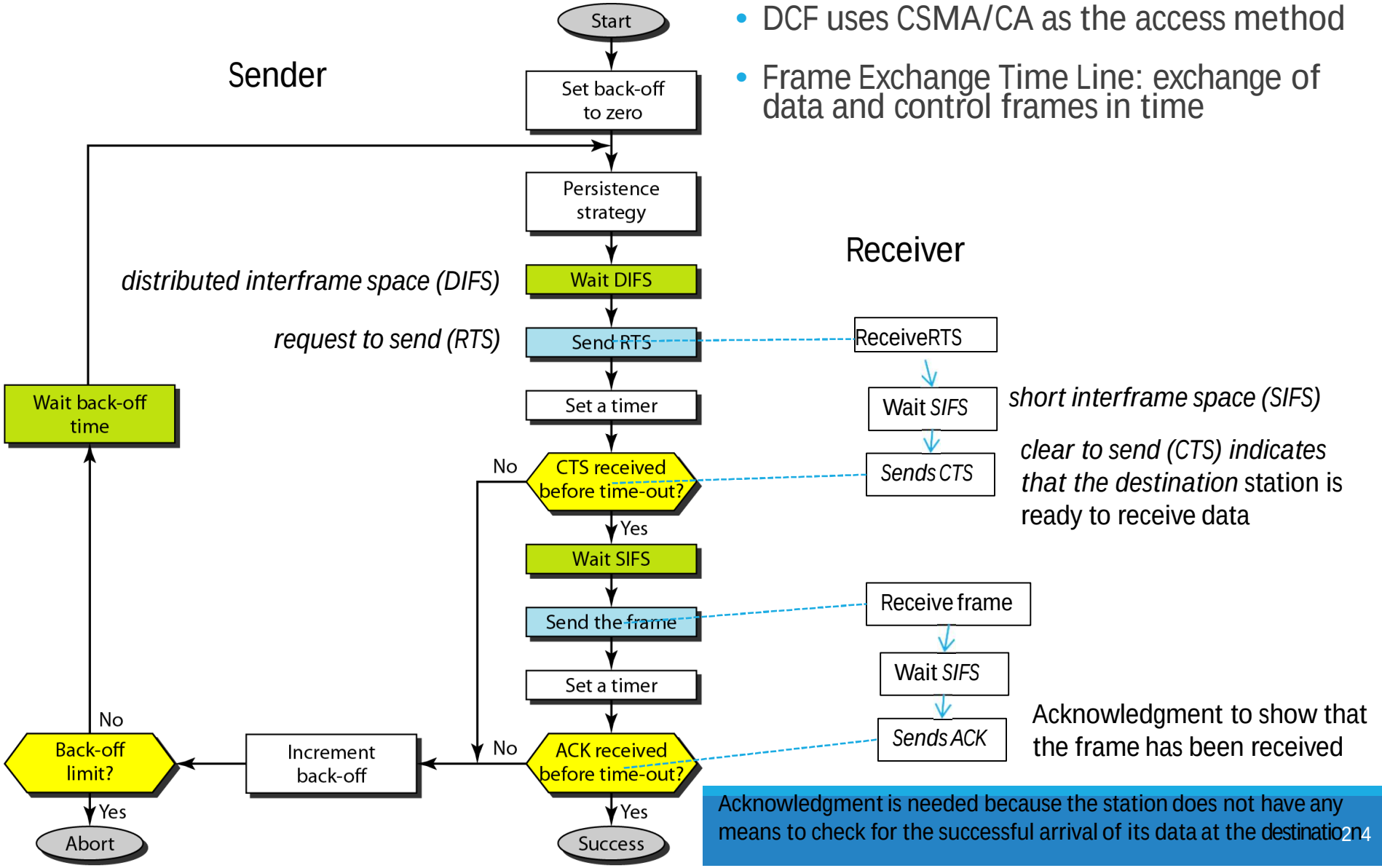
2. Collision may not be detected because of the hidden station problem.

3. The distance between stations may result in Signal fading which prevent a station at one end from hearing a collision at the other end.

Suited for ad hoc network and ordinary asynchronous traffic

Distributed Coordination Function (DCF)

- DCF uses CSMA/CA as the access method
- Frame Exchange Time Line: exchange of data and control frames in time



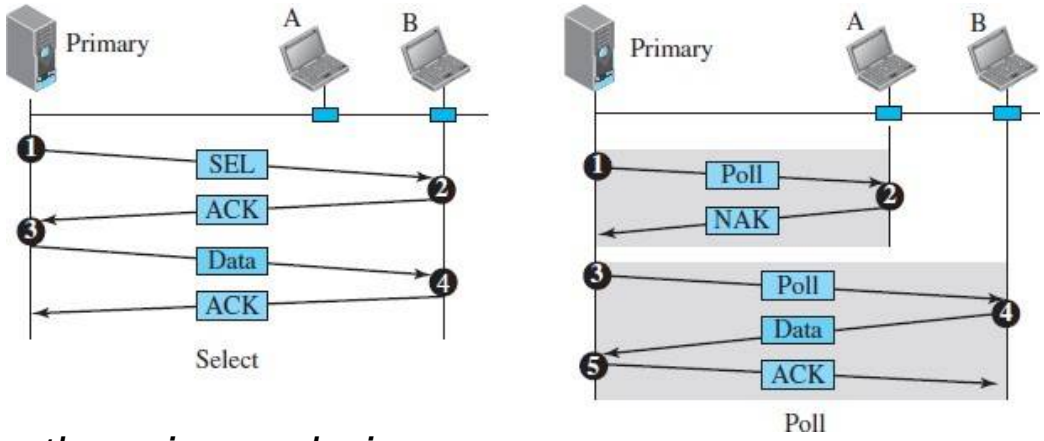
MAC Sublayer

- Point Coordination Function (PCF)
  - an optional access method on top of DCF
  - Implemented in an infrastructure network (not in an ad hoc network)
  - mostly for time-sensitive transmission services like voice or multimedia
  - a centralized, contention-free polling access method
  - The AP performs polling stations one after another, sending any data they have to the AP.

MAC Sublayer

- To give priority to PCF over DCF, another set of interframe spaces has been defined:
  - SIFS - Short Inter Frame Spacing
    - Used for immediate response actions e.g ACK, CTS
  - PIFS - Point Inter Frame Spacing
    - PIFS (PCF IFS) is shorter than the DIFS.
- if, at the same time, a station wants to use only DCF and an AP wants to use PCF, the AP has priority.
- Repetition interval has been designed to cover both contention-free (PCF) and contention-based (DCF) traffic to allow DCF accessing the media.

Polling in Repetition interval



- *used whenever the primary device has something to send.*
- *Primary* does not know whether the target device is prepared to receive
- Primary alert the secondary about the upcoming transmission and wait for an acknowledgment of the secondary's ready status using select (SEL) frame
- One field of SEL includes the address of the intended secondary

- *Used by the primary device to solicit transmissions from the secondary* devices
- When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send
- When the first secondary is approached, it responds either with a AK frame if it has nothing to send or with data if it does
- If the response is negative (a NAK frame), then the primary polls the next secondary in the same manner until it finds one with data to send
- When the response is positive (a data frame), the primary reads the frame and returns an acknowledgment (ACK frame), verifying its receipt

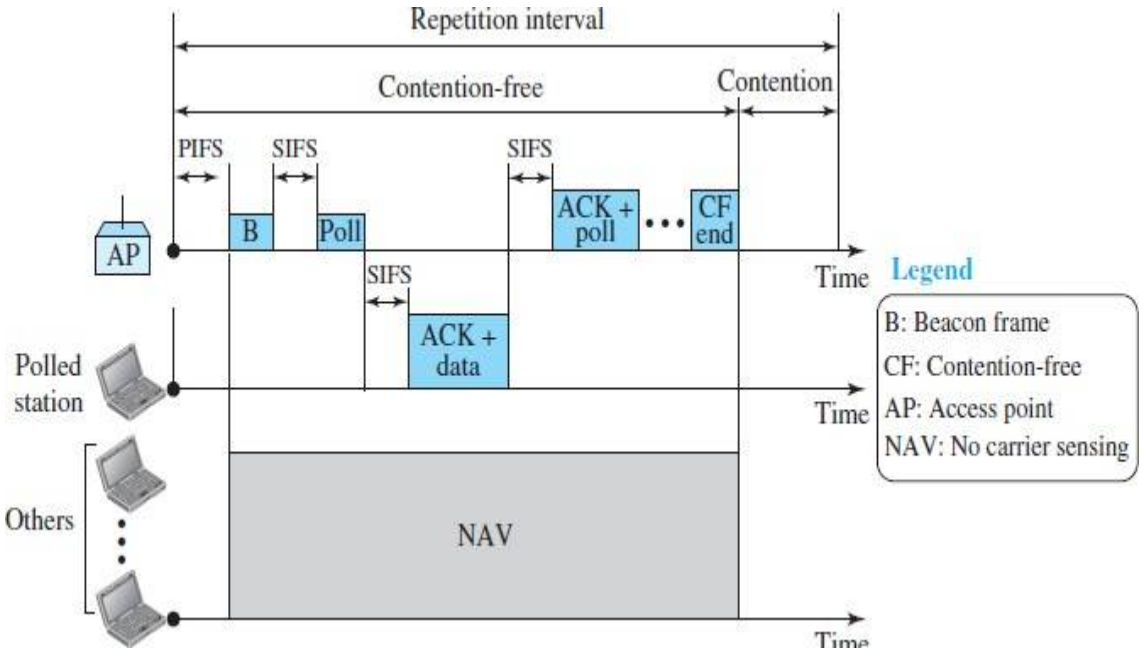
MAC Sublayer - Repetition interval

1. starts with B

3.PC (point controller) can send a poll frame, receive data, send an ACK, receive an ACK, or do any combination of these

4.PC sends a CF end (contention- free end) frame to allow the contention-based stations to use the medium

2. When the stations hear the beacon frame, they start their NAV for the duration of the contention-free period of the repetition interval



Fragmentation

- The wireless environment is very noisy.
- corrupt frame has to be retransmitted.
- Fragmentation is recommended.
  - the division of a large frame into smaller ones.
- It is more efficient to resend a small frame than a large one.

MAC Frame Format

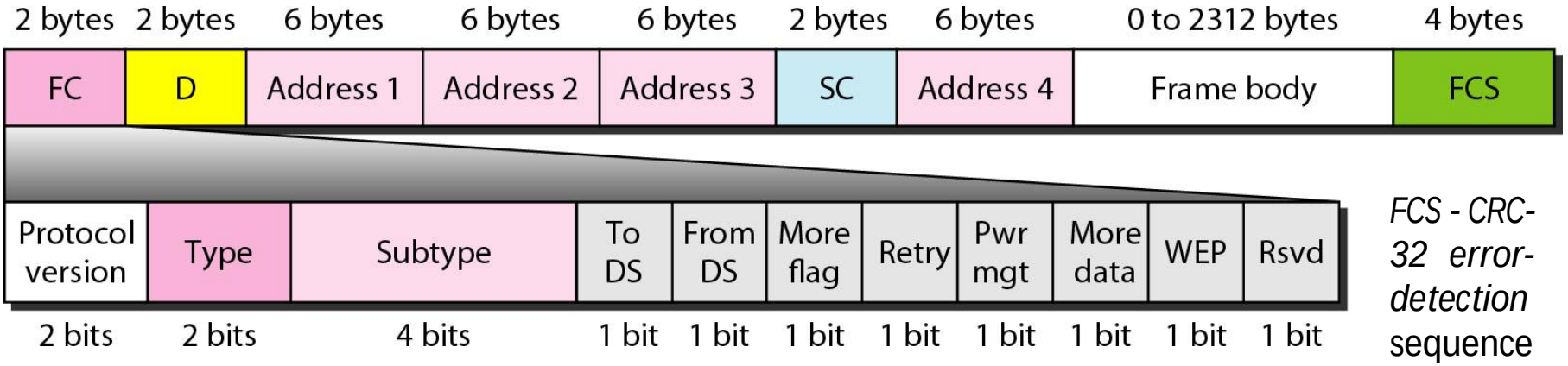
- The MAC layer frame consists of nine fields

duration of the transmission that is used to set the value of NAV. In one control frame, it defines the ID of the frame.

four address fields - meaning of each address field depends on the value of the To DS and From DS subfields

Sequence control (SC) - first four bits define the fragment number; the last 12 bits define the sequence number, which is the same in all fragments.

Frame body - information based on the type and the subtype defined in the FC field



FCS - CRC-32 error-detection sequence

Frame control (FC)- type of frame and some control information

MAC Sublayer - *Frame Format*

- Subfields in FC field

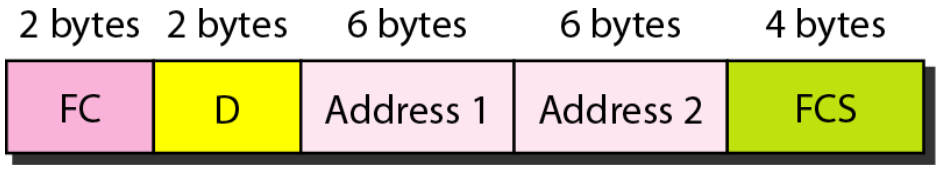
Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 14.2)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

Frame Types

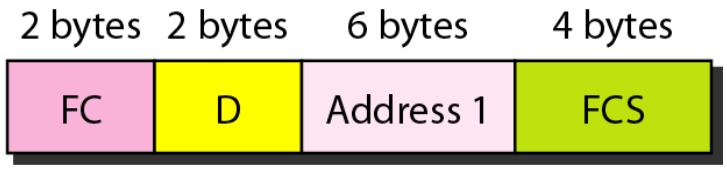
- IEEE 802.11 has three categories of frames:
  - management frames:

    used for the initial communication between stations and access points.
  - control frames.

    used for accessing the channel and acknowledging frames



RTS



CTS or ACK

value of the type field is 01; the values of the subtype fields

Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

  - data frames.

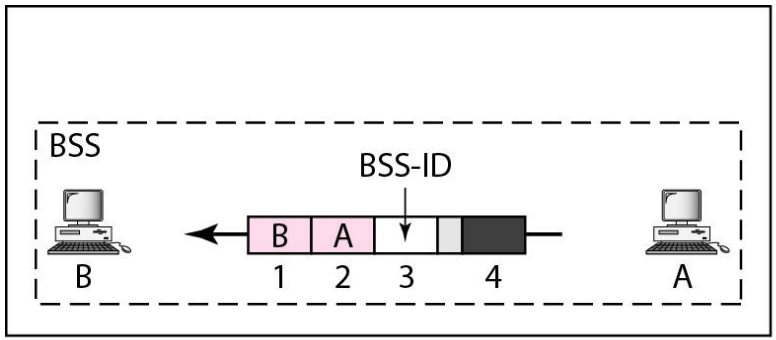
    Data frames are used for carrying data and control information.

Addressing Mechanism

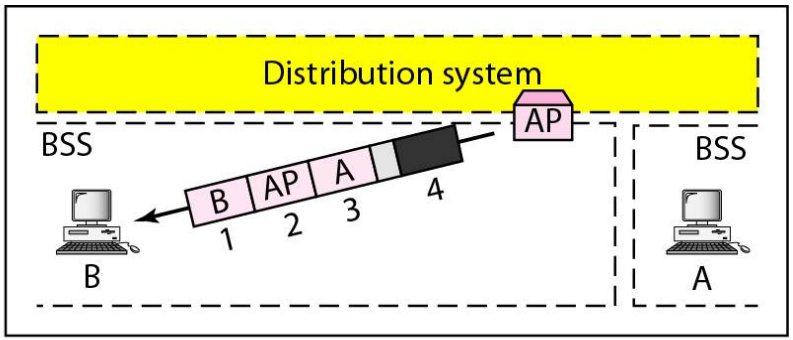
- IEEE 802.11 addressing mechanism specifies four cases defined by the value of the two flags in the FC field, *To DS and From DS*
  - Each flag can be either 0 or 1, resulting in four different situations
  - The interpretation of the four addresses (address 1 to address 4) in the MAC frame depends on the value of these flags

Addressing Mechanism

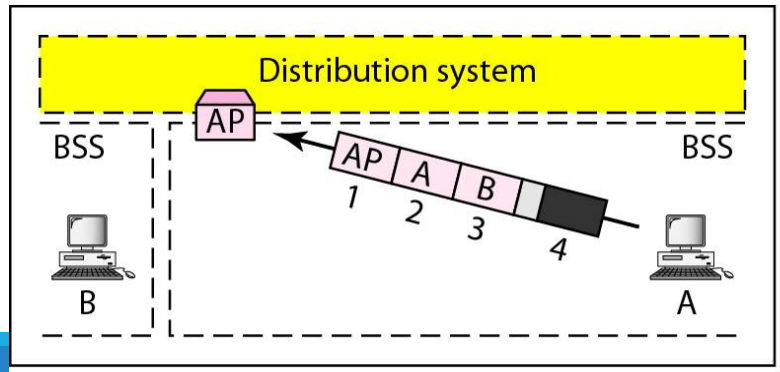
To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source



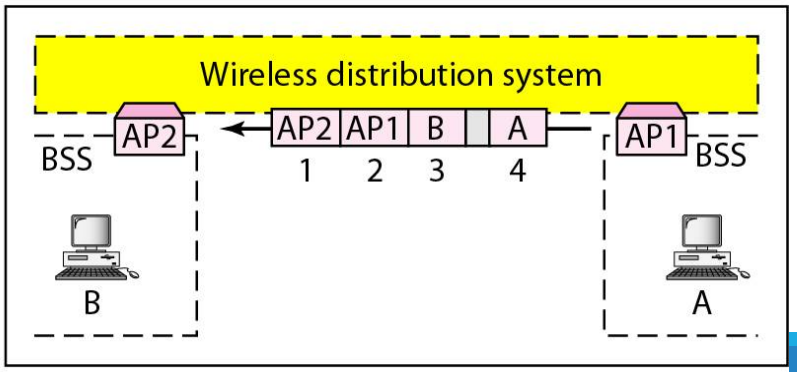
a. Case 1



b. Case 2



c. Case 3



d. Case 4

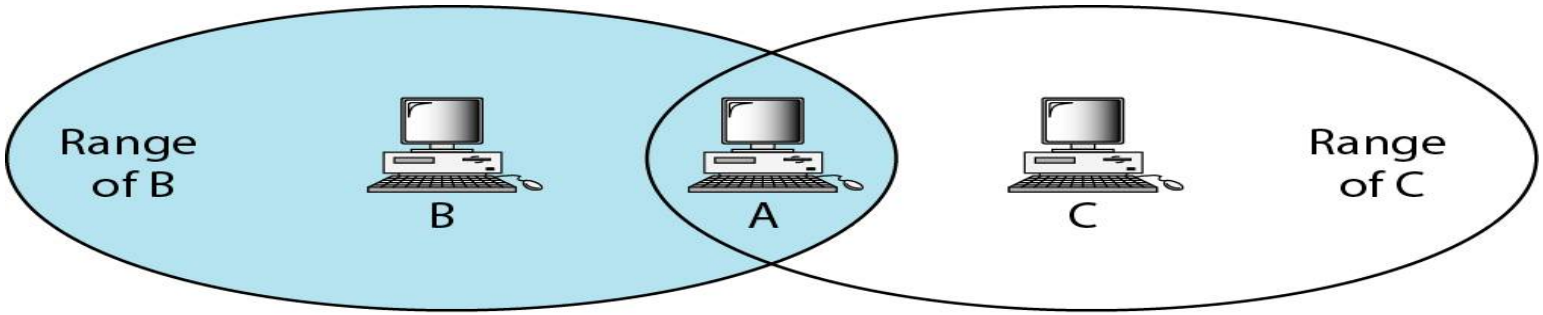
Addressing Mechanism

- Case 1: 00, To DS = 0 and From DS = 0
  - This means that the frame is not going to a distribution system and is not coming from a distribution system.
  - The ACK frame should be sent to the original sender.
- Case 2: 01, In this case, To DS = 0 and From DS = 1.
  - This means that the frame is coming from a distribution system (coming from an AP).
  - The ACK should be sent to the AP
  - The addresses are as address 3 contains the original sender of the frame (in another BSS).

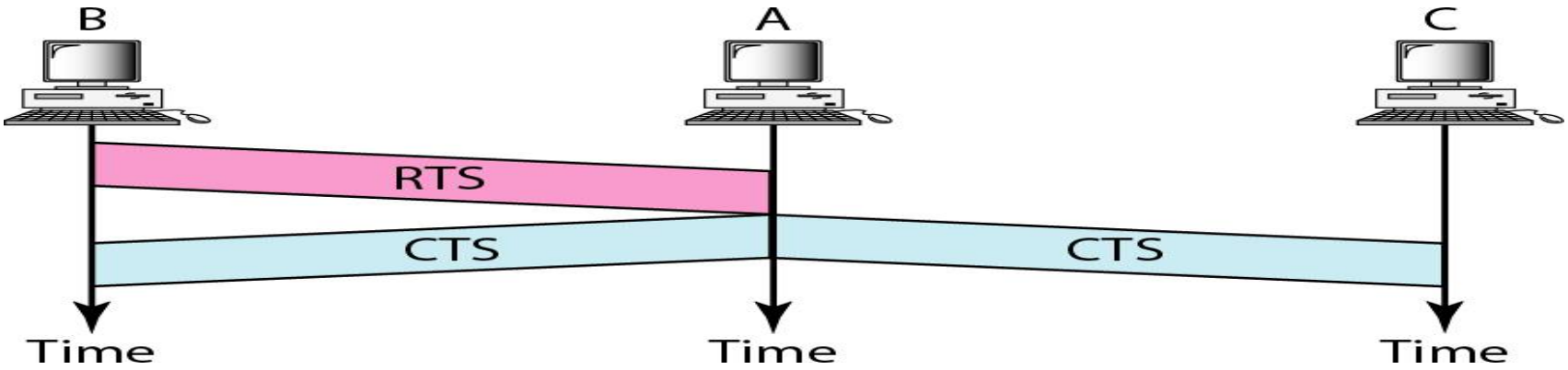
Addressing Mechanism

- Case 3: 10, To DS =1 and From DS =O.
  - This means that the frame is going to a distribution system (frame is going from a station to an AP)
  - The ACK is sent to the original station.
  - address 3 contains the final destination of the frame (in another BSS).
- Case 4:11, To DS =1 and From DS =1.
  - This is the case in which the distribution the frame is going from one AP to another AP in a wireless distribution system.
  - We do not need to define addresses if the distribution system is a wired LAN because the frame in these cases has the format of a wired LAN frame (Ethernet, for example).
  - Here, we need four addresses to define the original sender, the final destination, and two intermediate APs.

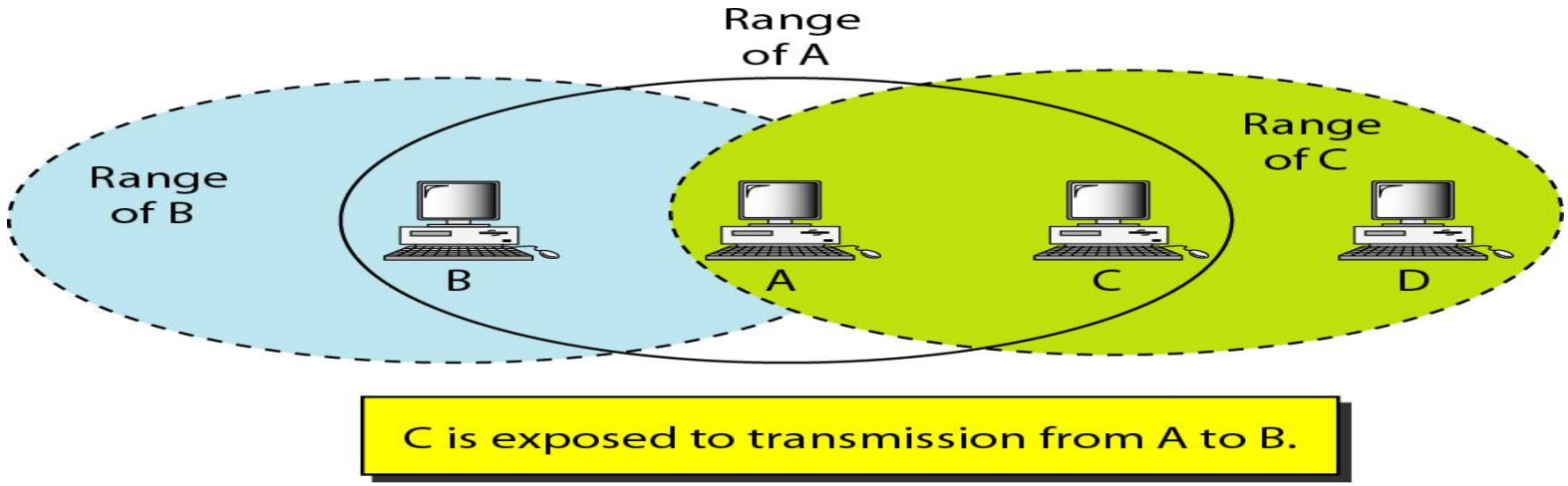
Hidden Station Problem



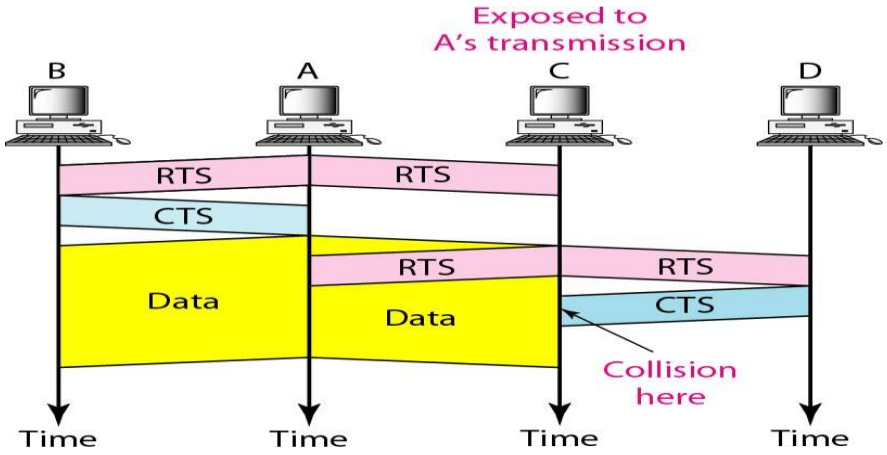
B and C are hidden from each other with respect to A.



Exposed Station Problems



- Station A is transmitting to station B.
- Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B
- However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending
- The handshaking messages RTS and CTS cannot help in this case
- Station C hears the RTS from A and refrains from sending, even though the communication between C and D cannot cause a collision in the zone between A and C; station C cannot know that station A's transmission does not affect the zone between C and D.

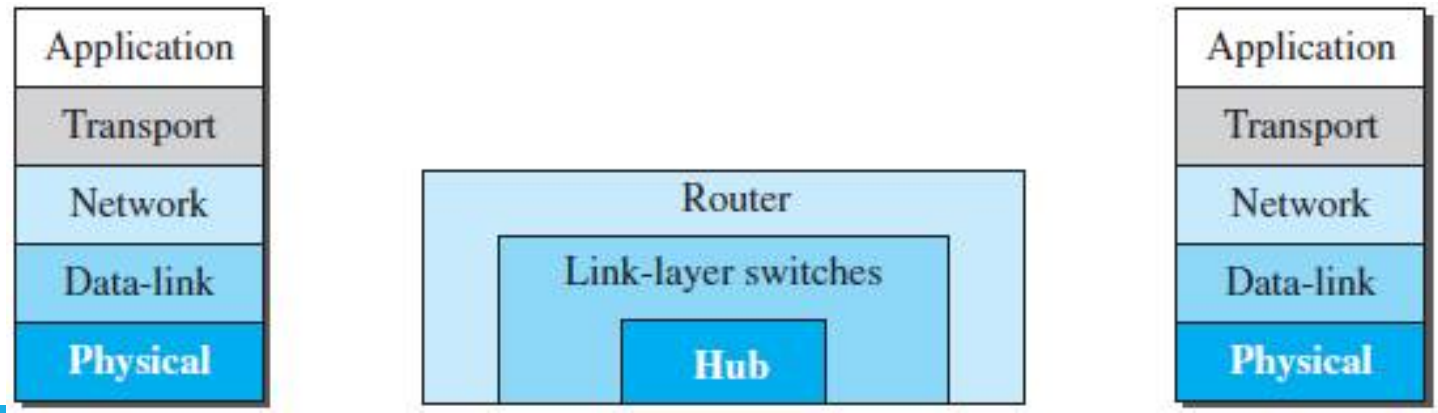


END

Connecting Devices

Connecting Devices

- We use connecting devices to connect hosts together to make a network or to connect networks together to make an internet
- Connecting devices can operate in different layers of the Internet model, there are 3 kinds of connecting devices:
  - Hubs
  - Link-layer switches
  - Routers

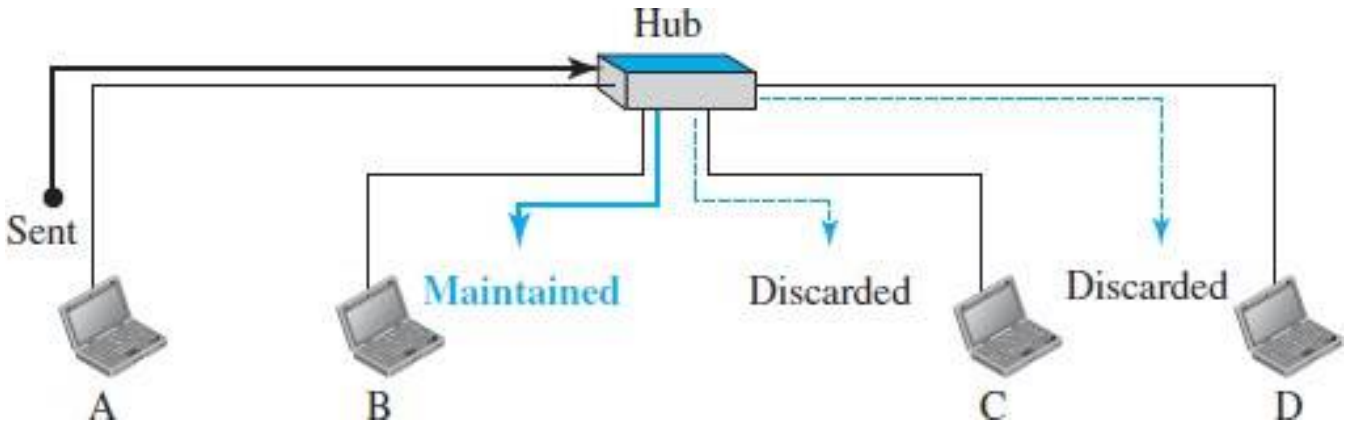


Hubs

- A hub is a device that operates only in the physical layer
- Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data
- A repeater receives a signal and, before it becomes too weak or corrupted, *regenerates and retimes the original bit pattern*
- *The repeater then sends the refreshed* signal
- In the past, when Ethernet LANs were using bus topology, a repeater was used to connect two segments of a LAN to overcome the length restriction of the coaxial cable
- Today, Ethernet LANs use star topology
  - In a star topology, a repeater is a multiport device, often called a *hub, that can be used to serve as the connecting* point and at the same time function as a repeater.

Hubs ...

- When a packet from station A to station B arrives at the hub, the signal representing the frame is regenerated to remove any possible corrupting noise, but the hub forwards the packet from all outgoing ports except the one from which the signal was received
  - Frame is broadcast - All stations in the LAN receive the frame, but only station B keeps it. The rest of the stations discard it.



Hubs ...

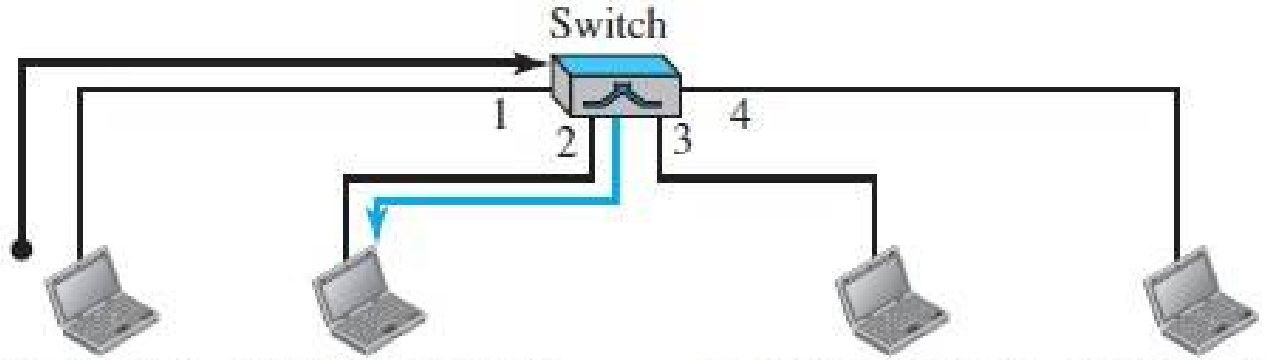
- A hub does not have a filtering capability and does not have the intelligence to find from which port the frame should be sent out
- They do not have a link-layer address and they do not check the link-layer address of the received frame
- They just regenerate the corrupted bits and send them out from every port

Link-layer switch

- *Operates in both the physical and the data-link layers*
- As a physical-layer device, it regenerates the signal it receives
- As a link-layer device, the link-layer switch can check the MAC addresses (source and destination) contained in the frame
- A link-layer switch has filtering capability - check the destination address of a frame and can decide from which outgoing port the frame should be sent
- A link-layer switch does not change the link-layer (MAC) addresses in a frame

Link-layer switch ...

- A LAN with four stations that are connected to a link-layer switch
- If a frame destined for station 71:2B:13:45:61:42 arrives at port 1, the link-layer switch consults its table to find the departing port
- According to its table, frames for 71:2B:13:45:61:42 should be sent out only through port 2; therefore, there is no need for forwarding the frame through other ports



Switching table

Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3
64:2B:13:45:61:13	4

Transparent switch

- **A switch in which the stations are completely unaware of the** switch's existence
- If a switch is added or deleted from the system, reconfiguration of the stations is unnecessary
- According to the IEEE 802.1d specification, a system equipped with transparent switches must meet three criteria:
  - ***Forwarding :*** Frames must be forwarded from one station to another correctly
  - ***Learning :*** The forwarding table is automatically made by learning frame movements in the network
  - ***Loop Problem :*** Loops in the system must be prevented

Transparent switch: *Learning*

- The earliest switches – static switching tables that were manually entered during switch setup by the system administrator
  - Simple process but was not practical
    - If a station was added or deleted, the table had to be modified manually
    - The same was true if a station's MAC address changed, which is not a rare event
      - For example, putting in a new network card means a new MAC address
- A better solution to the static table is a dynamic table that maps addresses to ports (interfaces) automatically
- A switch gradually learns from the frames' movements by inspecting both the destination and the source addresses in each frame that passes through the switch
  - The destination address is used for the forwarding decision (table lookup); the source address is used for adding entries to the table and for updating purposes

Gradual building of table

Address	Port

a. Original

Address	Port
71:2B:13:45:61:41	1

b. After A sends a frame to D

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4

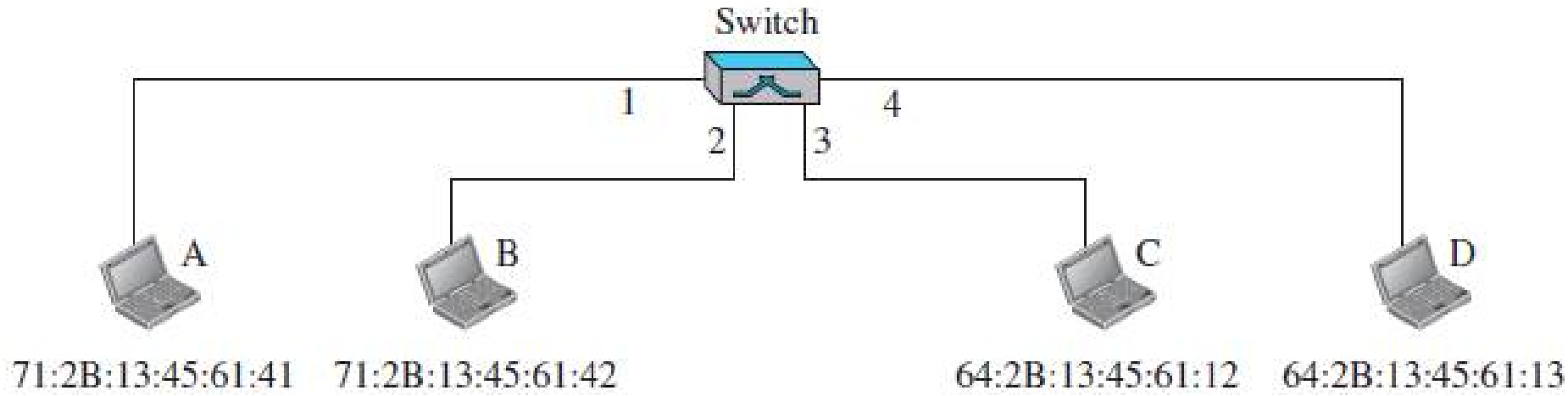
c. After D sends a frame to B

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2

d. After B sends a frame to A

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3

e. After C sends a frame to D



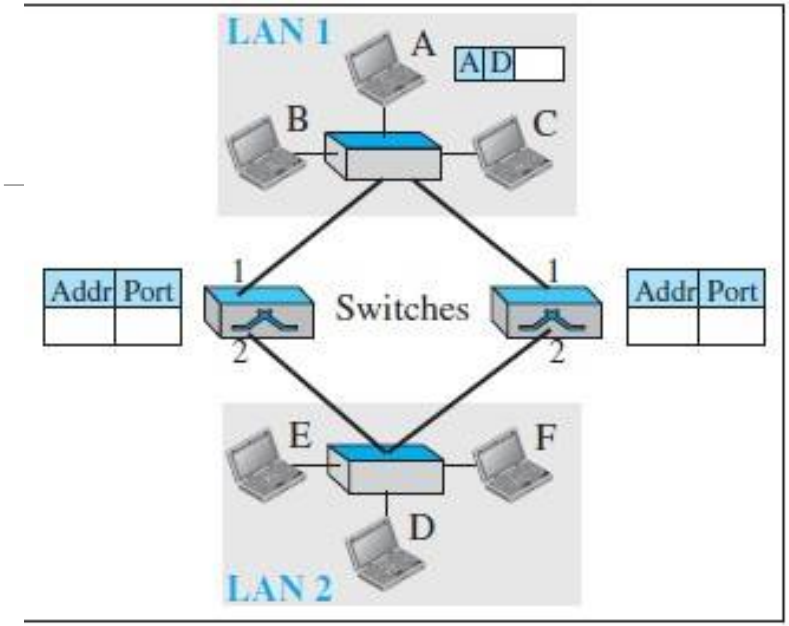
Transparent switch: Learning

1. When station A sends a frame to station D, the switch does not have an entry for either D or A
   - The frame goes out from all three ports; the frame floods the network
   - However, by looking at the source address, the switch learns that station A must be connected to port 1 - means that frames destined for A, in the future, must be sent out through port 1
   - The switch adds this entry to its table - first entry now
2. When station D sends a frame to station B, the switch has no entry for B, so it floods the network again
   - However, it adds one more entry to the table related to station D
3. The learning process continues until the table has information about every port
   - However, note that the learning process may take a long time
     - For example, if a station does not send out a frame (a rare situation), the station will never have an entry in the table

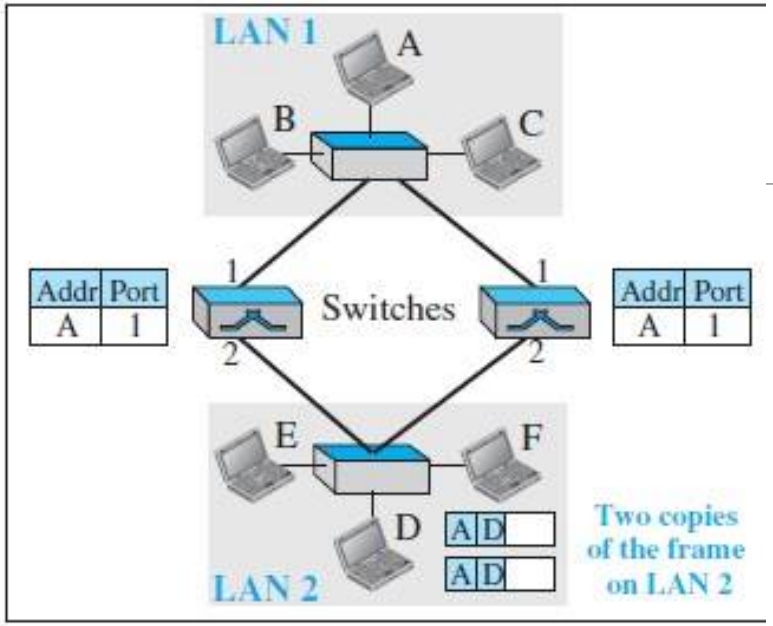
Transparent switch: *Loop Problem*

- Transparent switches work fine as long as there are no redundant switches in the system
- Redundant switches (more than one switch between a pair of LANs) to make the system more reliable
  - If a switch fails, another switch takes over until the failed one is repaired or replaced
- Redundancy can create loops in the system, which is very undesirable
  - Loops can be created only when two or more broadcasting LANs (those using hubs, for example) are connected by more than one switch

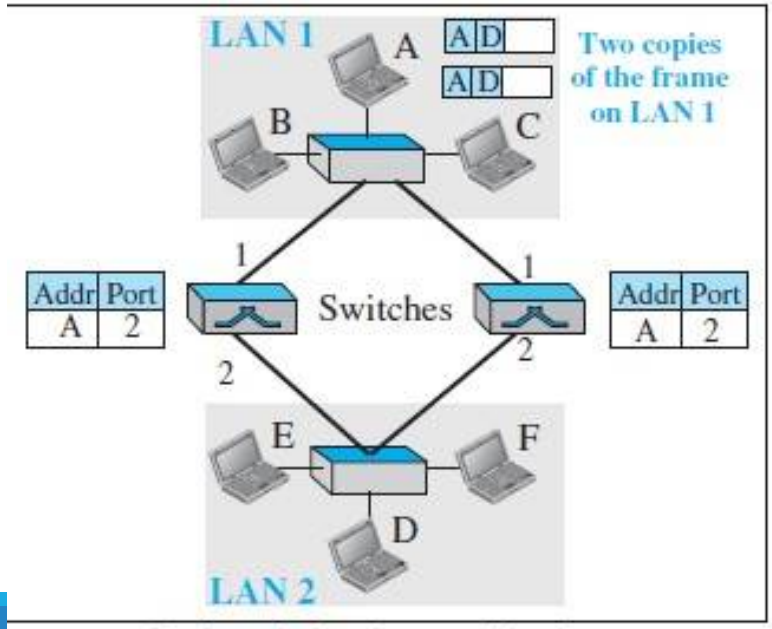
a. Station A sends a frame to station D



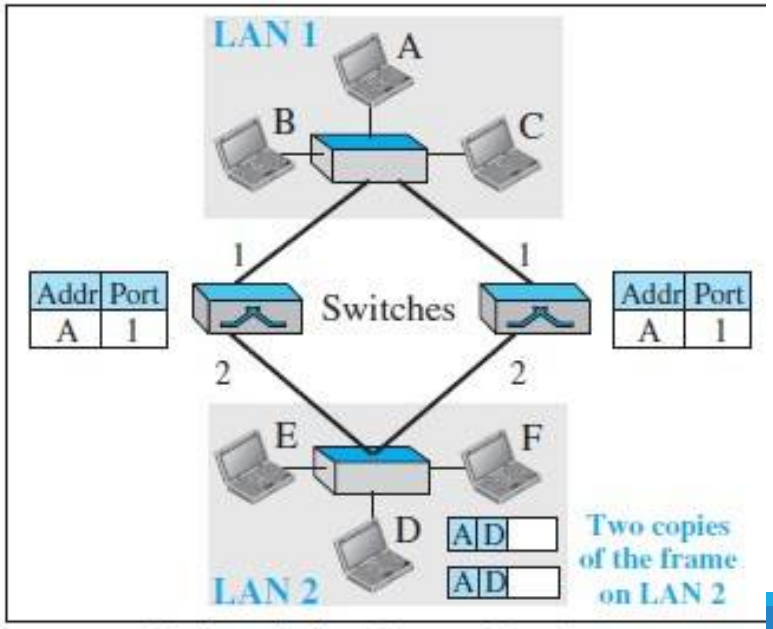
b. Both switches forward the frame



c. Both switches forward the frame



c. Both switches forward the frame



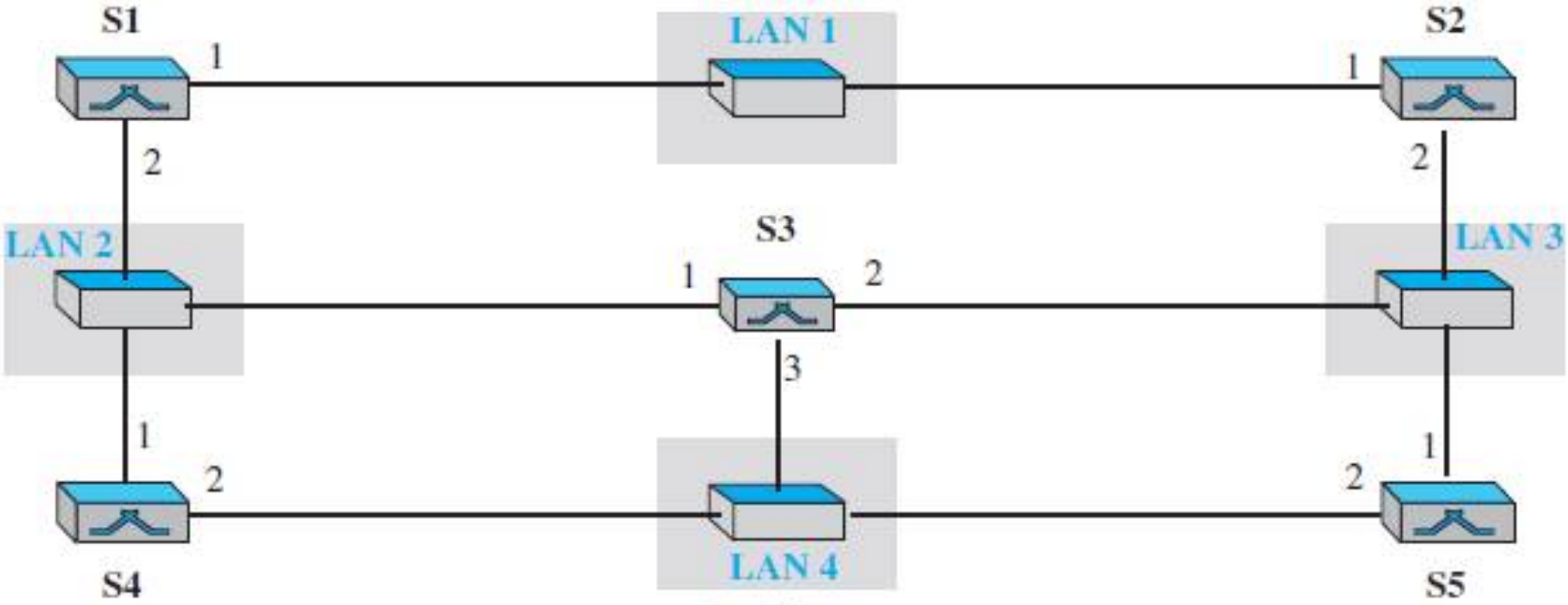
Transparent switch: *Loop Problem*

- Simple example of a loop created in a system with two LANs connected by two switches.
- **1. Station A sends a frame to station D – As the tables of both switches are empty, both** forward the frame and update their tables based on the source address A.
- **2. Now there are two copies of the frame on LAN 2**
  - **The copy sent out by the left** switch is received by the right switch, which does not have any information about the destination address D; it forwards the frame
  - The copy sent out by the right switch is received by the left switch and is sent out for lack of information about D.
    - Each frame is handled separately because switches, as two nodes on a broadcast network sharing the medium, use an access method such as CSMA/CD. The tables of both switches are updated, but still there is no information for destination D.
- **3. Now there are two copies of the frame on LAN 1 - Step 2 is repeated, and both copies** are sent to LAN2.
- **4. The process continues on and on**

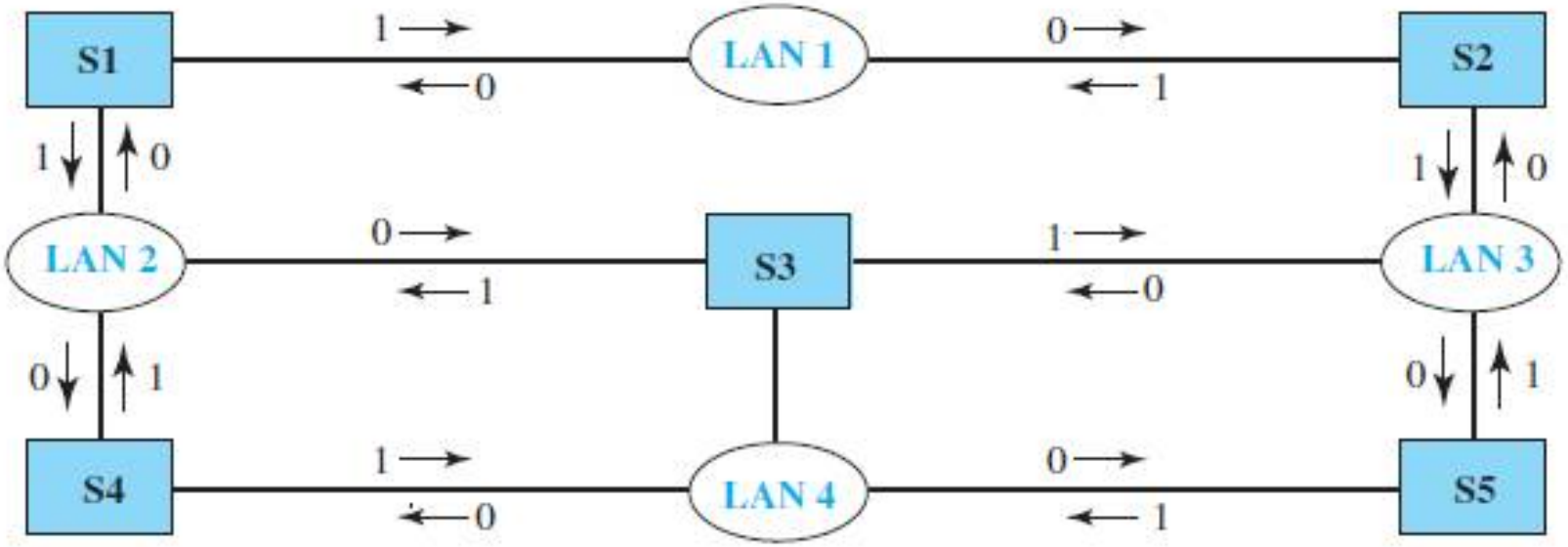
Note that switches are also repeaters and regenerate frames. So in each iteration, there are newly generated fresh copies of the frames

Spanning Tree Algorithm

- **A switched LAN – how to create a** topology in which each LAN can be reached from any other LAN through one path only (no loop) without changing the physical topology of the system
- Solution: create a logical topology that overlays the physical one
  - IEEE specification uses the spanning tree algorithm to create a loopless topology
    - In graph theory, a **spanning tree is a graph in which there is no loop**
- To find the spanning tree, we need to assign a cost (metric) to each arc
  - The interpretation of the cost is left up to the systems administrator eg. the minimum hops (hop count is normally 1 from a switch to the LAN and 0 in the reverse direction)



a. Actual system A system with four LANs and five switches



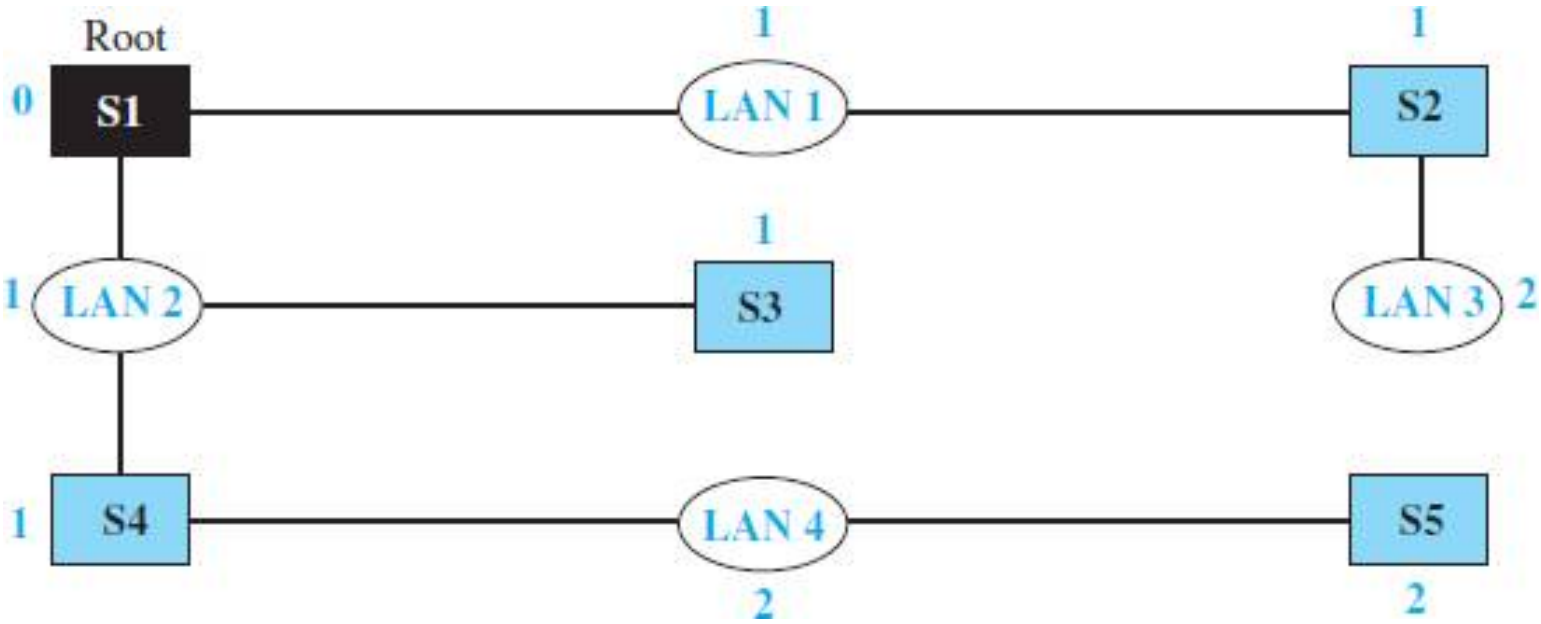
b. Graph representation with cost assigned to each arc

3-step process for finding spanning tree

- 1. Every switch has a built-in ID (normally the serial number, which is unique)
  - Each switch broadcasts this ID so that all switches know which one has the smallest ID
  - The switch with the smallest ID is selected as the *root switch (root of the tree)*
    - Assume that switch S1 has the smallest ID. It is, therefore, selected as the root switch.
- 2. The algorithm tries to find the shortest path (a path with the shortest cost) from the root switch to every other switch or LAN
  - The shortest path can be found by examining the total cost from the root switch to the destination eg. Use Dijkstra algorithm
- 3. The combination of the shortest paths creates the shortest tree
- 4. Based on the spanning tree, we mark
  - the ports that are part of it, the forwarding ports, which forward a frame that the switch receives
  - those ports that are not part of the spanning tree, the blocking ports, which block the frames received by the switch

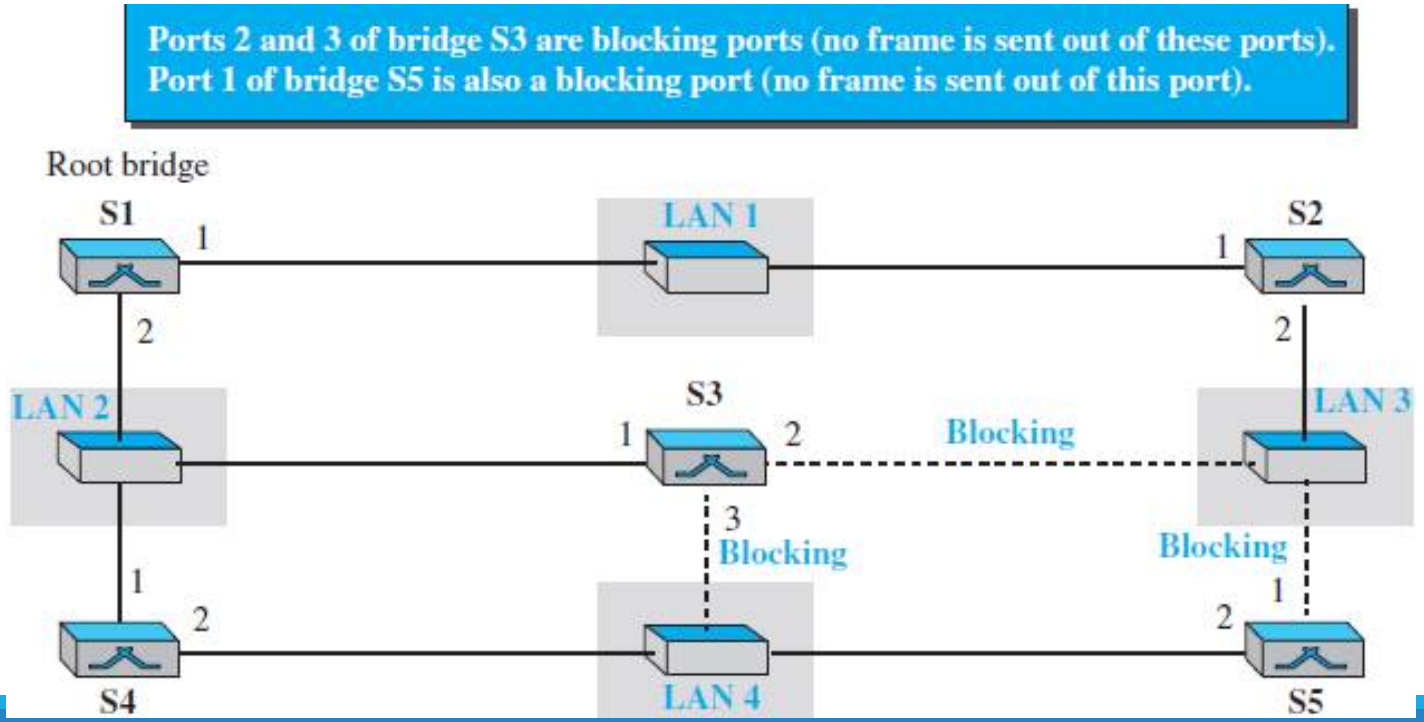
3-step process for finding spanning tree

- *Finding the shortest paths and the spanning tree in a system of switches*



3-step process for finding spanning tree

- The logical systems of LANs with forwarding ports (solid lines) and blocking ports (broken lines).
- There is only one path from any LAN to any other LAN in the spanning tree system – No loops are created
  - Real spanning tree algorithm in LAN uses dynamic process through a software package at each node



Advantages of Switches

- ***Collision Elimination:*** a link-layer switch eliminates the collision - increasing the average bandwidth available to a host in the network
  - In a switched LAN, there is no need for carrier sensing and collision detection; each host can transmit at any time
- ***Connecting Heterogenous Devices:*** can connect devices that use different protocols at the physical layer (data rates) and different transmission media
  - As long as the format of the frame at the data-link layer does not change, a switch can receive a frame from a device that uses twisted-pair cable and sends data at 10 Mbps and deliver the frame to another device that uses fiber-optic cable and can receive data at 100 Mbps

Routers

- A **router is a three-layer device - operates in the physical, data-link, and network layers**
  - As a physical-layer device, it regenerates the signal it receives
  - As a link-layer device, the router checks the physical addresses (source and destination) contained in the packet
  - As a network-layer device, a router checks the network-layer addresses
- A router is an internetworking device that connects independent networks to form an internetwork
- Router will change the MAC addresses it receives because the MAC addresses have only local jurisdictions

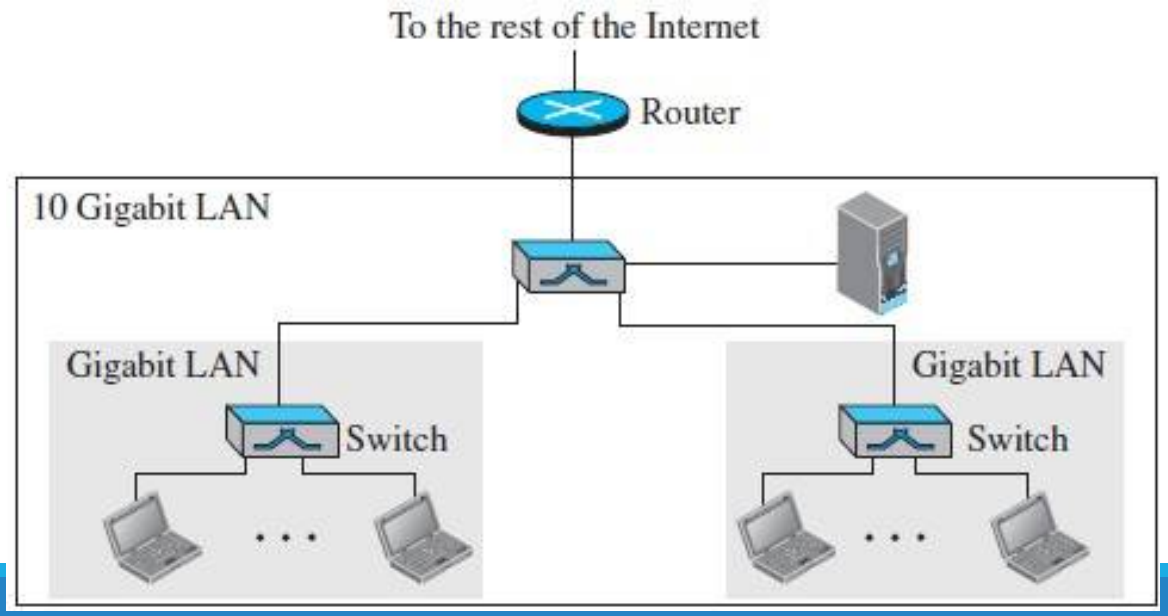
Routers ...

- There are three major differences between a router and a repeater or a switch

1. A router has a physical and logical (IP) address for each of its interfaces

2.A router acts only on those packets in which the link-layer destination address matches the address of the interface at which the packet arrives

3. A router changes the link-layer address of the packet (both source and **destination)** when it forwards the packet



Routers ...

- An organization with two separate buildings with a Gigabit Ethernet LAN installed in each building
- The organization uses switches in each LAN
- The two LANs can be connected to form a larger LAN using 10 Gigabit Ethernet technology that speeds up the connection to the Ethernet and the connection to the organization server
- A router then can connect the whole system to the Internet

END