



VIT<sup>®</sup>

Vellore Institute of Technology  
(Deemed to be University under section 3 of UGC Act, 1956)

# Computer Networks

## BCSE308L

### Multiple Access

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai



# Overview

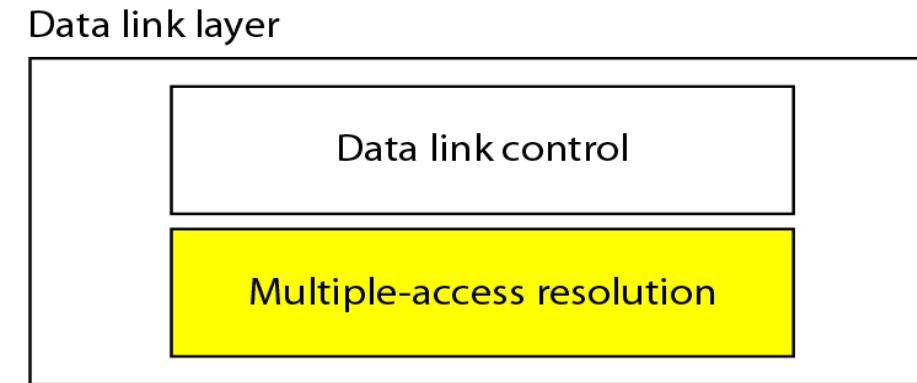
- Introduction
- Multiple Access Protocols
- Random Access Protocols
- Summary

# Introduction

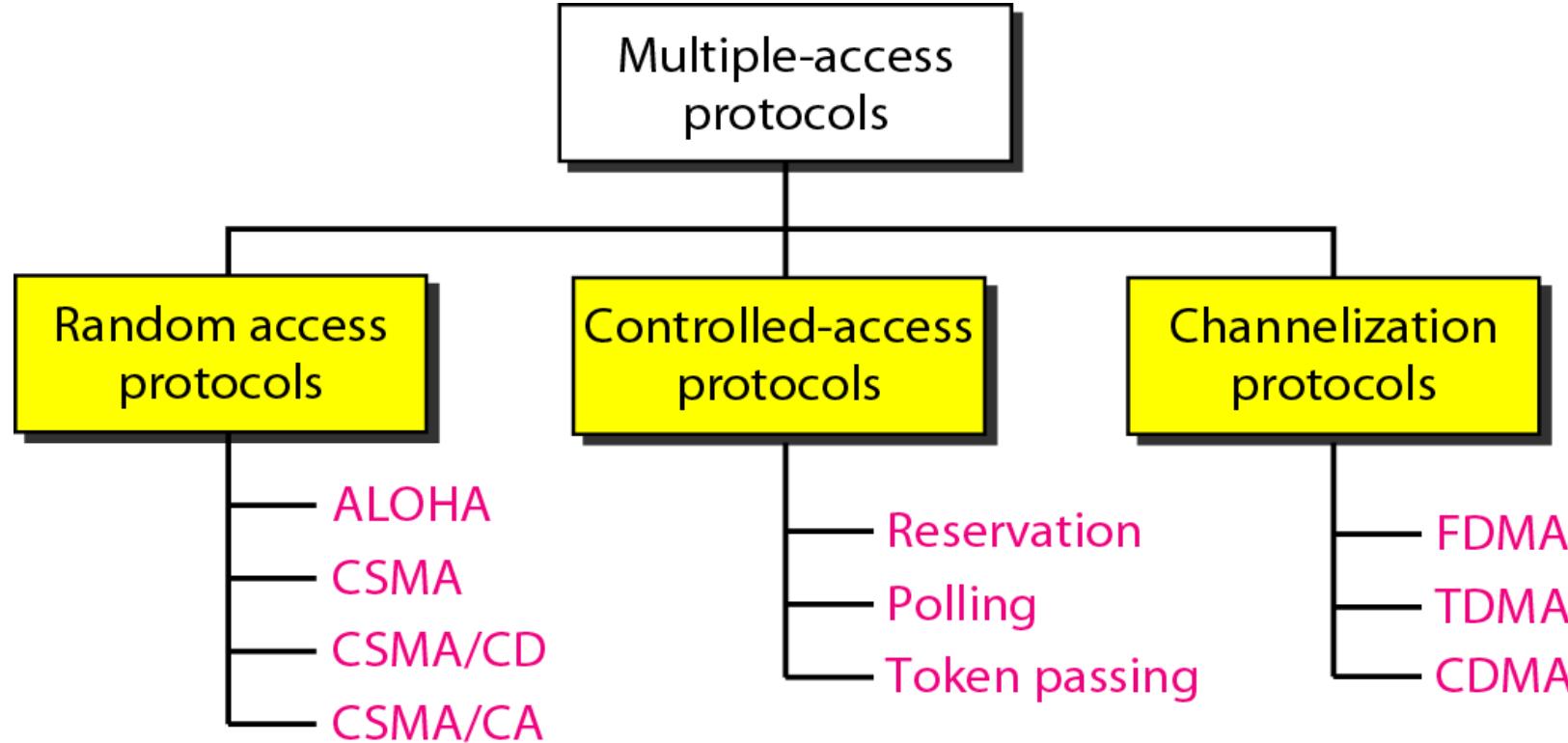
- Data link control is a mechanism which provides a link with reliable communication.
- In the data link protocols, we assumed that there is an available dedicated link (or channel) between the sender and the receiver.
- This assumption may or may not be true.
- If we have a dedicated link, as when we connect to the Internet using PPP as the data link control protocol, then the assumption is true and we do not need anything else.
- But if we use our cellular phone to connect to another cellular phone, the channel (the band allocated to the vendor company) is not dedicated.
- A person a few feet away from us may be using the same channel to talk to her friend.
- Consider the **data link layer as two sublayers**.
- The **upper sublayer** is responsible for **data link control**, and the **lower sublayer** is responsible for **resolving access to the shared media**.
- If the channel is dedicated, we do not need the lower sublayer.

# Introduction ... Contd.

- The upper sublayer that is responsible for flow and error control is called the **logical link control (LLC) layer**.
- The lower sublayer that is mostly responsible for multiple access resolution is called the **media access control (MAC) layer**.
- When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link.
- The problem of controlling the access to the medium is similar to the rules of speaking in an assembly.
- The procedures guarantee that the right to speak is upheld and ensure that two people do not speak at the same time, do not interrupt each other, do not monopolize the discussion, and so on.
- The situation is similar for multipoint networks.



# Multiple Access Protocols





# Random Access Protocols

- In **random access** or **contention** methods, no station is superior to another station and none is assigned the control over another.
- No station permits, or does not permit, another station to send.
- At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.
- This decision depends on the state of the medium (idle or busy).
- Each station can transmit when it desires on the condition that it follows the predefined procedure, including the testing of the state of the medium.

Two features give this method its name.

- 1) There is no scheduled time for a station to transmit.
  - ✓ Transmission is random among the stations.
  - ✓ That is why these methods are called **random access**.
- 2) No rules specify which station should send next.
  - ✓ Stations compete with one another to access the medium.
  - ✓ That is why these methods are also called **contention methods**.



# Random Access Protocols ... Contd.

- In a random access method, each station has the right to the medium without being controlled by any other station.
- However, if more than one station tries to send, there is an access conflict-collision-and the frames will be either destroyed or modified.
- To avoid access conflict or to resolve it when it happens, each station follows a procedure that answers the following questions:
  - ✓ When can the station access the medium?
  - ✓ What can the station do if the medium is busy?
  - ✓ How can the station determine the success or failure of the transmission?
  - ✓ What can the station do if there is an access conflict?

# Random Access Protocols ... Contd.

- The random access methods have evolved from a very interesting protocol known as **ALOHA**, which used a very simple procedure called multiple access.
- The method was improved with the addition of a procedure that forces the station to sense the medium before transmitting.
- This was called carrier sense multiple access (**CSMA**).
- This method later evolved into two parallel methods: carrier sense multiple access with collision detection (**CSMA/CD**) and carrier sense multiple access with collision avoidance (**CSMA/CA**).
- CSMA/CD tells the station what to do when a collision is detected.
- CSMA/CA tries to avoid the collision.



# Summary

## Discussed about

- Introduction
- Multiple Access Protocols
- Random Access Protocols



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**



VIT<sup>®</sup>

Vellore Institute of Technology  
(Deemed to be University under section 3 of UGC Act, 1956)

# Computer Networks

## BCSE308L

ALOHA

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai



# Overview

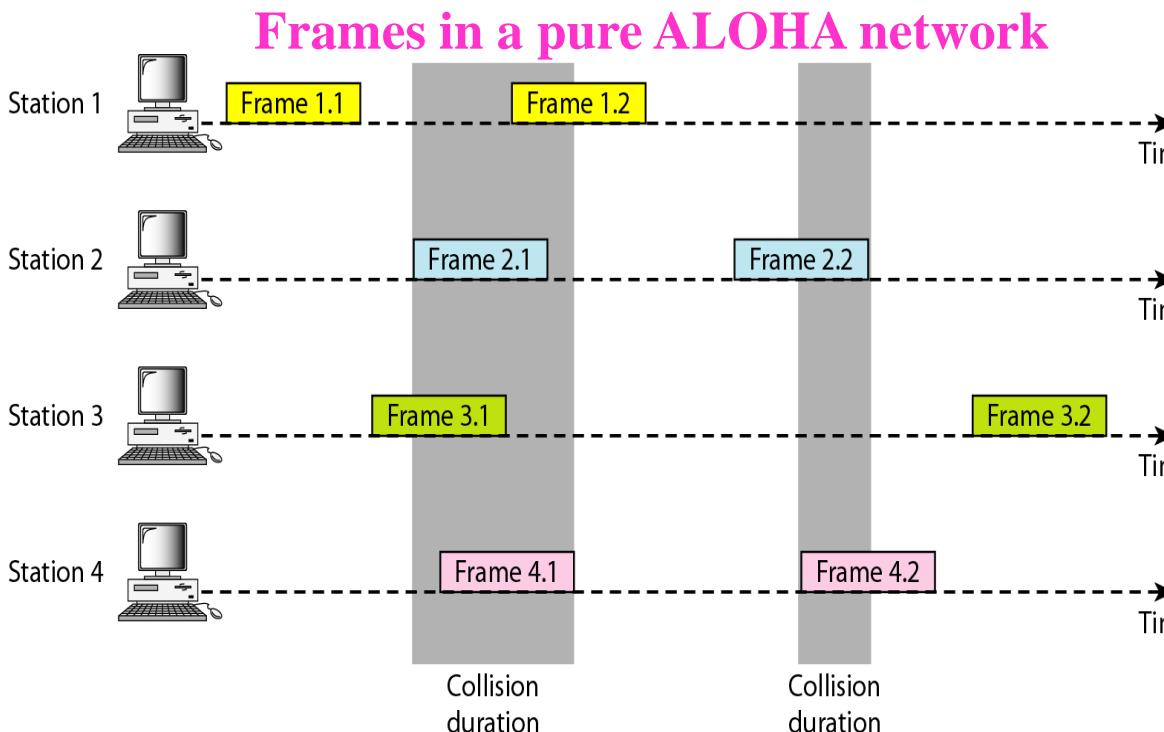
- Introduction
- Pure ALOHA
  - Vulnerable Time
  - Throughput
- Slotted ALOHA
  - Vulnerable Time
  - Throughput
- Practice Questions
- Summary

# Introduction

- ALOHA (Advocates of Linux Open-source Hawaii Association), the earliest random access method, was designed for a radio (wireless) LAN, but it can be used on any shared medium.
- There are potential collisions in this arrangement.
- The medium is shared between the stations.
- When a station sends data, another station may attempt to do so at the same time.
- The data from the two stations collide and become garbled.

# Pure ALOHA

- The original ALOHA protocol is called pure ALOHA.
- This is a simple, but elegant protocol.
- The idea is that each station sends a frame whenever it has a frame to send.
- Since there is only one channel to share, there is the possibility of collision between frames from different stations.



- There are four stations that contend with one another for access to the shared channel.
- Each station sends two frames; there are a total of eight frames on the shared medium.
- Some of these frames collide because multiple frames are in contention for the shared channel.
- Two frames survive: frame 1.1 from station 1 and frame 3.2 from station 3.
- Even if one bit of a frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed.



# Pure ALOHA ... Contd.

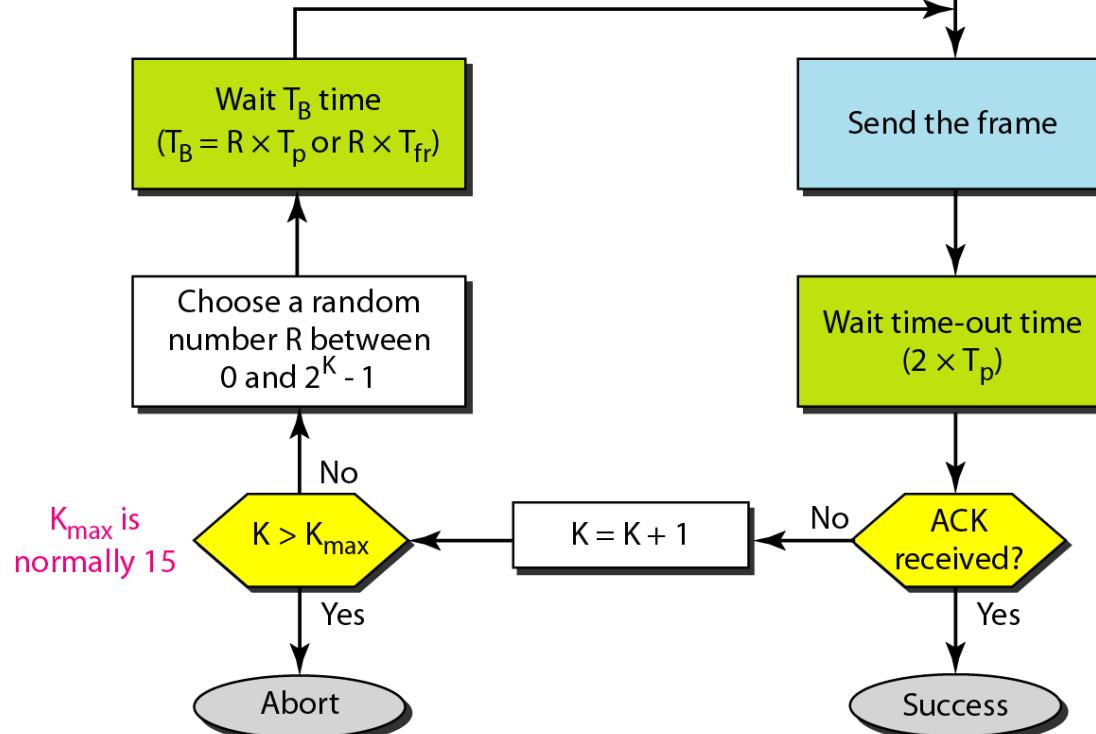
- Resend the frames that have been destroyed during transmission.
- The pure ALOHA protocol relies on acknowledgments from the receiver.
- When a station sends a frame, it expects the receiver to send an acknowledgment.
- If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.
- A collision involves two or more stations.
- If all these stations try to resend their frames after the time-out, the frames will collide again.
- Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame.
- The randomness will help avoid more collisions, call this time the back-off time  $T_B$ .
- Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames.
- After a maximum number of retransmission attempts  $K_{\max}$  a station must give up and try later.

K: Number of attempts

$T_p$ : Maximum propagation time

$T_{fr}$ : Average transmission time for a frame

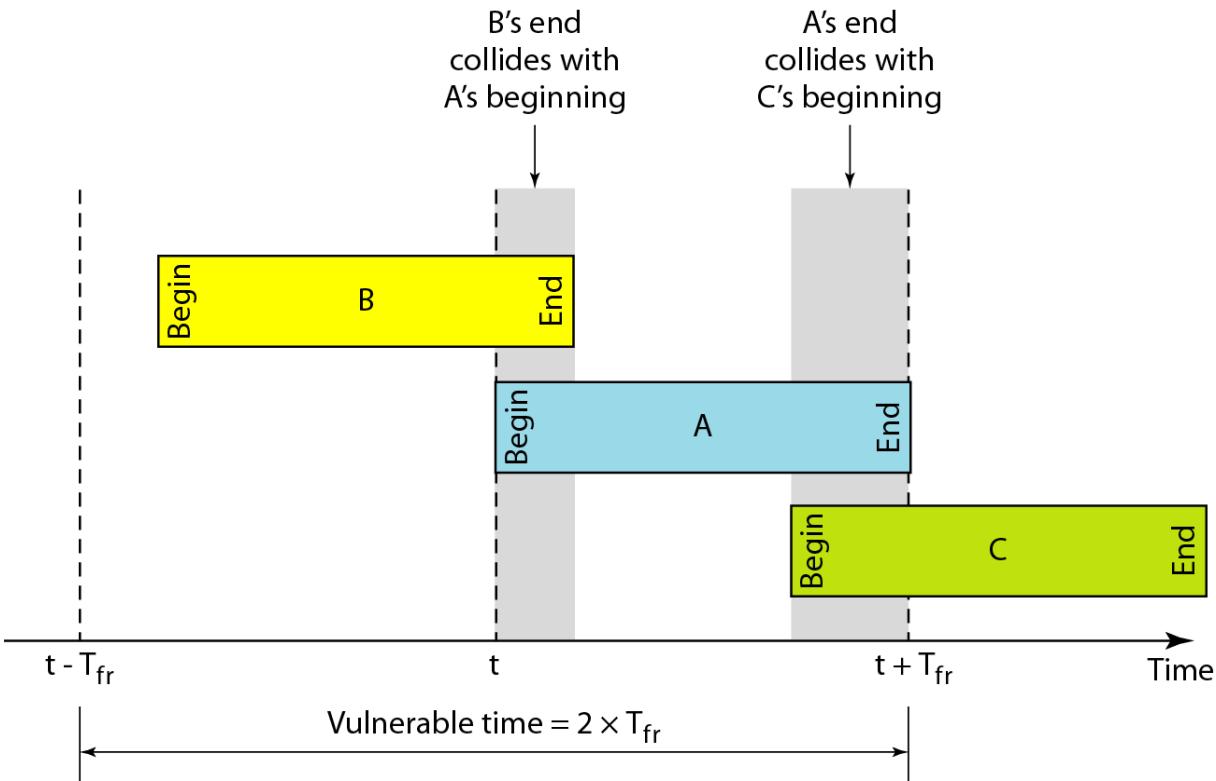
$T_B$ : Back-off time



Station has  
a frame to send

- The time-out period is equal to the maximum possible round-trip propagation delay, which is twice the amount of time required to send a frame between the two most widely separated stations ( $2 \times T_p$ ).
- The back-off time  $T_B$  is a random value that normally depends on  $K$ , the number of attempted unsuccessful transmissions.
- $T_B$  depends on the implementation, one common formula is the **binary exponential back-off**.
- For each retransmission, a multiplier in the range 0 to  $2^K - 1$  is randomly chosen and multiplied by  $T_p$  or  $T_{fr}$  to find  $T_B$ .
- The range of the random numbers increases after each collision.
- The value of  $K_{max}$  is usually chosen as 15.

# Vulnerable Time - Pure ALOHA



- Let us find the length of time, the vulnerable time, in which there is a possibility of collision.
- Assume that the stations send fixed-length frames with each frame taking  $T_{fr}$  s to send.
- Station A sends a frame at time  $t$ .
- Station B has already sent a frame between  $t - T_{fr}$  and  $t$ .
- This leads to a collision between the frames from station A and station B.
- The end of B's frame collides with the beginning of A's frame.
- Suppose that station C sends a frame between  $t$  and  $t + T_{fr}$ .
- There is a collision between frames from station A and station C.
- The beginning of C's frame collides with the end of A's frame.

- The vulnerable time, during which a collision may occur in pure ALOHA, is 2 times the frame transmission time.
- Pure ALOHA vulnerable time =  $2 \times T_{fr}$

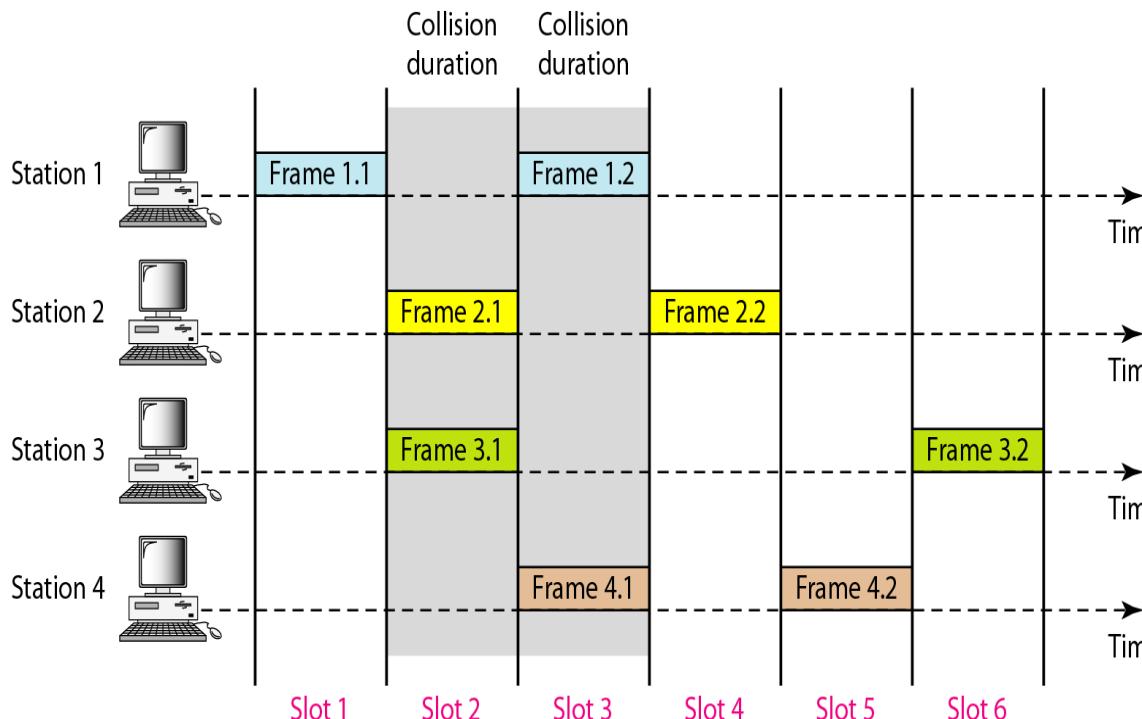
# Throughput - Pure ALOHA

- Let  $G$ , the average number of frames generated by the system during one frame transmission time.
- Then it can be proved that **the average number of successful transmissions for pure ALOHA is  $S = G \times e^{-2G}$ .**
- The maximum throughput  $S_{\max}$  is 0.184, for  $G = 1/2$ .
- If one-half a frame is generated during one frame transmission time (one frame during two frame transmission times), then 18.4 percent of these frames reach their destination successfully.
- This is an expected result because the vulnerable time is 2 times the frame transmission time.
- If a station generates only one frame in this vulnerable time and no other stations generate a frame during this time, the frame will reach its destination successfully.

# Slotted ALOHA

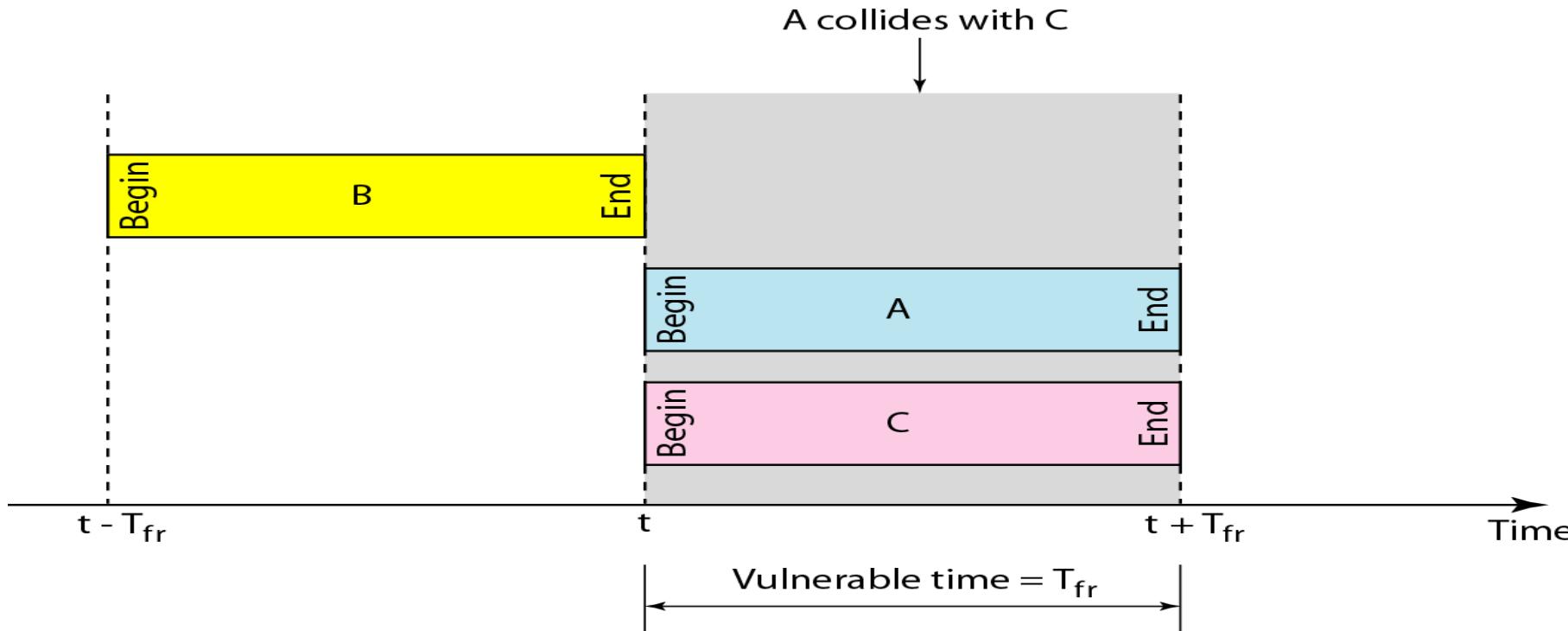
- Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
- In slotted ALOHA we divide the time into slots of  $T_{fr}$  s and force the station to send only at the beginning of the time slot.

## Frames in a slotted ALOHA network



- Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot.
- This means that the station which started at the beginning of this slot has already finished sending its frame.
- There is still the possibility of collision if two stations try to send at the beginning of the same time slot.
- The vulnerable time is now reduced to one-half, equal to  $T_{fr}$ .

# Vulnerable Time - Slotted ALOHA



- The vulnerable time for slotted ALOHA is one-half that of pure ALOHA.
- Slotted ALOHA vulnerable time =  $T_{fr}$ .

# Throughput - Slotted ALOHA

- The average number of successful transmissions for slotted ALOHA is  $S = G \times e^{-G}$ .
- The maximum throughput  $S_{max}$  is 0.368, when  $G = 1$ .
- If a frame is generated during one frame transmission time, then 36.8 percent of these frames reach their destination successfully.
- This result can be expected because the vulnerable time is equal to the frame transmission time.
- If a station generates only one frame in this vulnerable time and no other station generates a frame during this time, the frame will reach its destination successfully.



## Practice Questions

- 1) A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps.  
What is the requirement to make this frame collision-free?
- 2) A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps.  
What is the throughput if the system (all stations together) produces
  - a) 1000 frames per second
  - b) 500 frames per second
  - c) 250 frames per second
- 3) A slotted ALOHA network transmits 200-bit frames on a shared channel of 200 kbps.  
What is the throughput if the system (all stations together) produces
  - a) 1000 frames per second
  - b) 500 frames per second
  - c) 250 frames per second



# Summary

## Discussed about

- Introduction
- Pure ALOHA
  - Vulnerable Time
  - Throughput
- Slotted ALOHA
  - Vulnerable Time
  - Throughput
- Practice Questions



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**

# Computer Networks

## BCSE308L

## Carrier Sense Multiple Access (CSMA)

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai



# Overview

- Introduction
- Space/Time Model of Collision in CSMA
- Vulnerable Time in CSMA
- Persistence Methods
- Summary

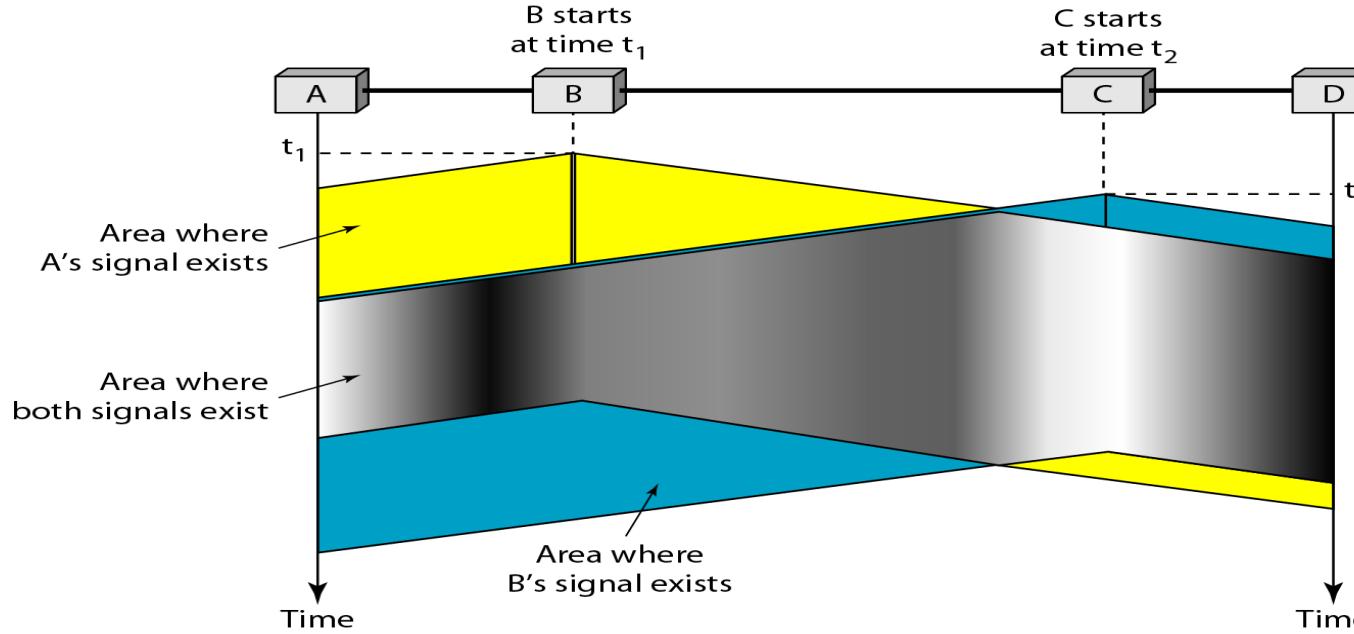


# Introduction

- To minimize the chance of collision and, therefore, increase the performance, the Carrier sense multiple access (CSMA) method was developed.
- The chance of collision can be reduced if a station senses the medium before trying to use it.
- CSMA requires that each station first listen to the medium or check the state of the medium before sending.
- CSMA is based on the principle "sense before transmit" or "listen before talk."
- CSMA can reduce the possibility of collision, but it cannot eliminate it.

# Space/Time Model of Collision in CSMA

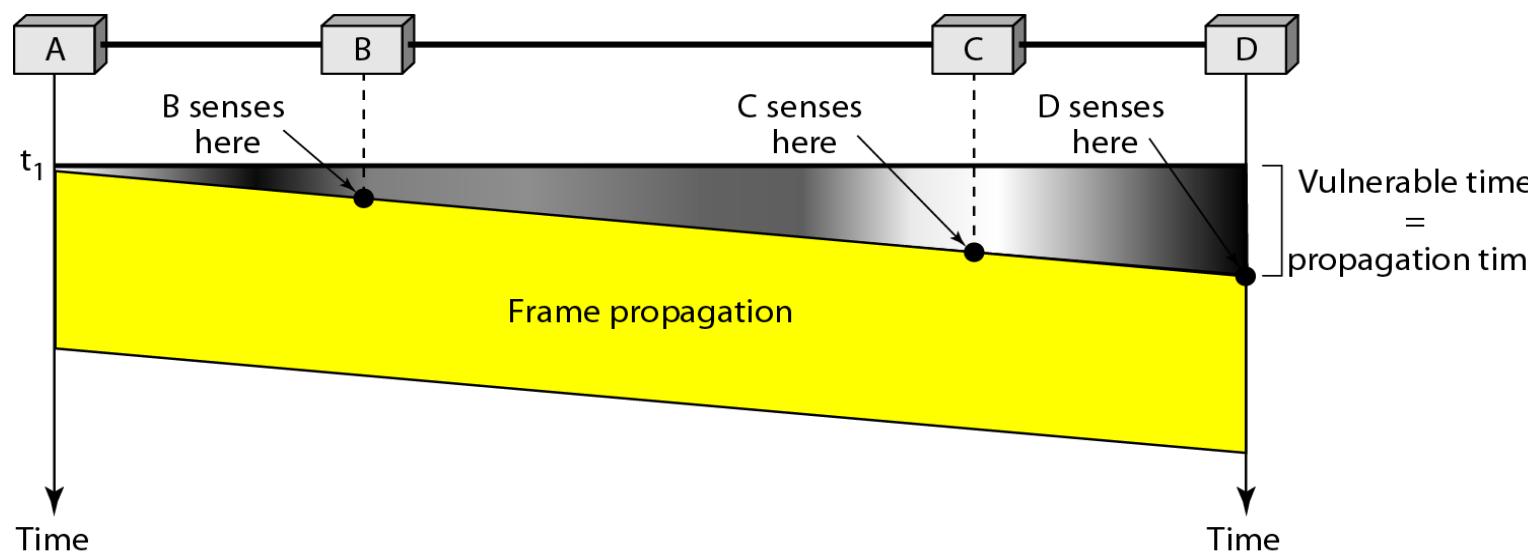
- Stations are connected to a shared channel, usually a dedicated medium.
- The possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (very short) for the first bit to reach every station and for every station to sense it.
- A station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.



- At time  $t_1$  station B senses the medium and finds it idle, so it sends a frame.
- At time  $t_2$  ( $t_2 > t_1$ ) station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C.
- Station C also sends a frame.
- The two signals collide and both frames are destroyed.

# Vulnerable Time in CSMA

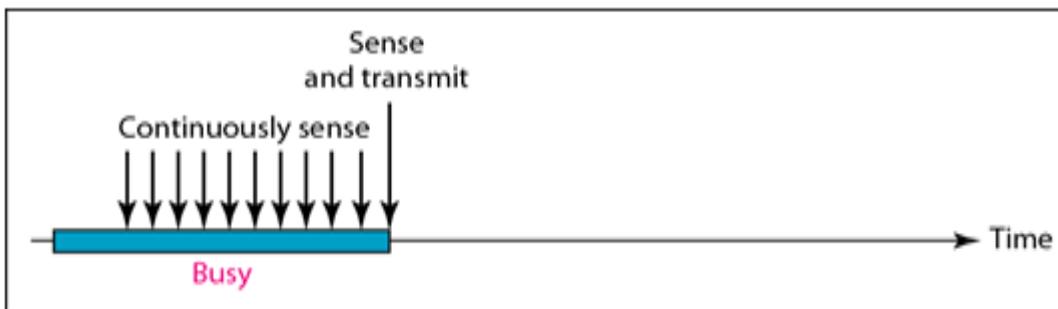
- The vulnerable time for CSMA is the propagation time  $T_p$ .
- This is the time needed for a signal to propagate from one end of the medium to the other.
- When a station sends a frame, and any other station tries to send a frame during this time, a collision will result.
- But if the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending.



- The leftmost station A sends a frame at time  $t_1$  which reaches the rightmost station D at time  $t_1 + T_p$ .
- The gray area shows the vulnerable area in time and space.

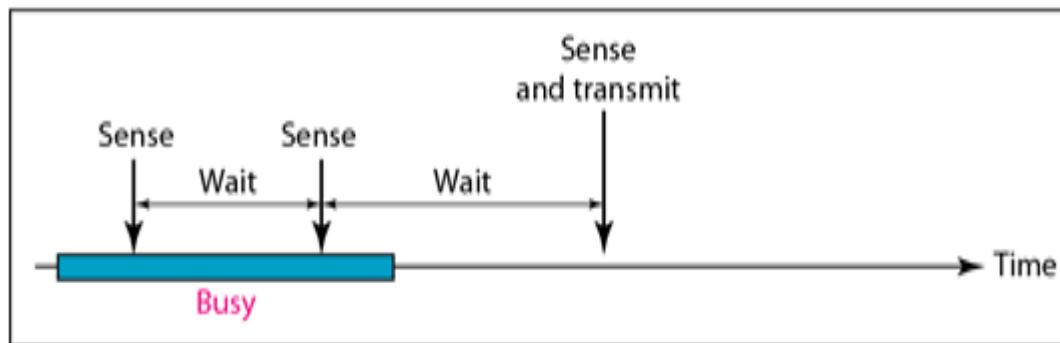
# Persistence Methods

- What should a station do if the channel is busy?
- What should a station do if the channel is idle?
- Three methods have been devised to answer these questions: **the 1-persistent method, the nonpersistent method, and the p-persistent method.**
- The **1-persistent method** is simple and straightforward.
- In this method, after the station finds the line idle, it sends its frame immediately with probability 1.
- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.



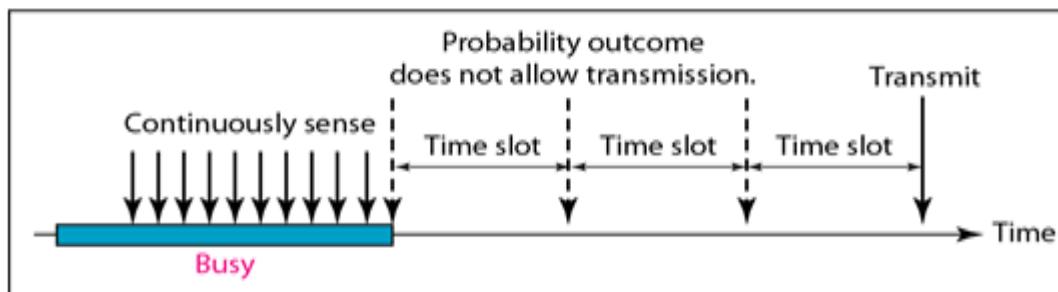
# Persistence Methods ... Contd.

- In the **nonpersistent method**, a station that has a frame to send senses the line.
- If the line is idle, it sends immediately.
- If the line is not idle, it waits a random amount of time and then senses the line again.
- The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- This method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

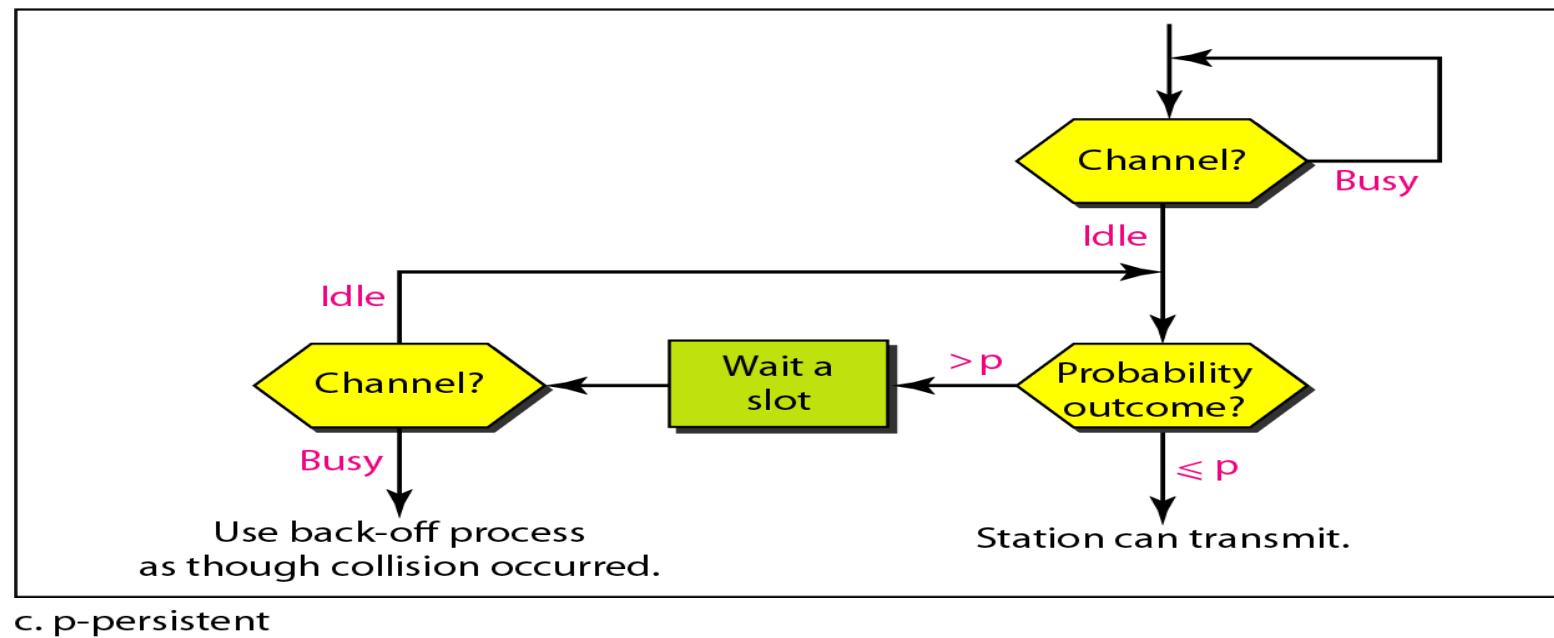
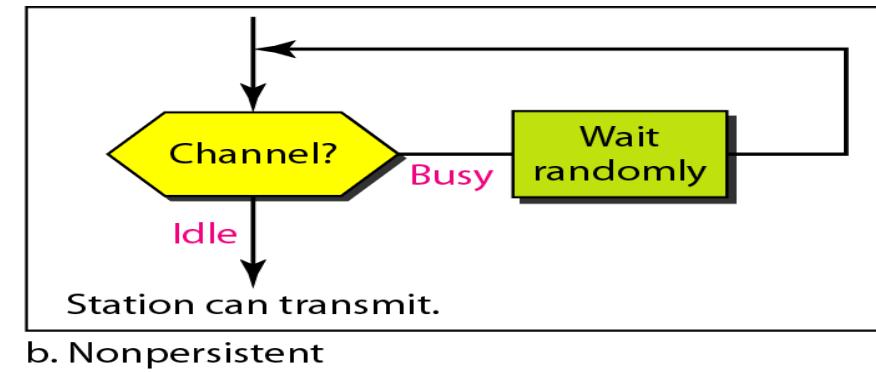
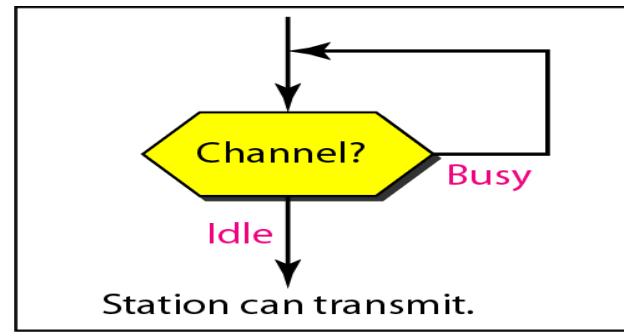


# Persistence Methods ... Contd.

- The **p-persistent method** is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
- The p-persistent approach combines the advantages of the other two strategies.
- It reduces the chance of collision and improves efficiency.
- In this method, after the station finds the line idle it follows these steps:
  1. With probability  $p$ , the station sends its frame.
  2. With probability  $q = 1-p$ , the station waits for the beginning of the next time slot and checks the line again.
    - a. If the line is idle, it goes to step 1.
    - b. If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.



# Persistence Methods ... Contd.





# Summary

## Discussed about

- Introduction
- Space/Time Model of Collision in CSMA
- Vulnerable Time in CSMA
- Persistence Methods



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**



**VIT<sup>®</sup>**

**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

# Computer Networks

## BCSE308L

## Carrier Sense Multiple Access – Collision Detection (CSMA/CD)

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai



# Overview

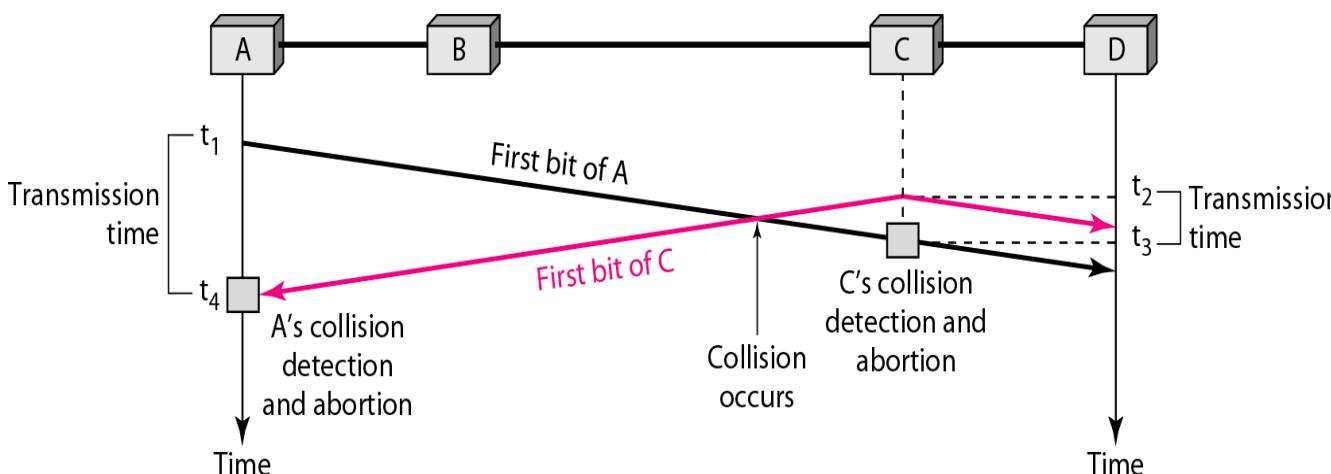
- Introduction
- Collision in CSMA/CD
- Minimum Frame Size
- Flow Diagram of CSMA/CD
- Energy Level
- Throughput
- Summary

# Introduction

- The CSMA method does not specify the procedure following a collision.
- Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful.
- If so, the station is finished.
- If, however, there is a collision, the frame is sent again.
- To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision.
- Although each station continues to send bits in the frame until it detects the collision.

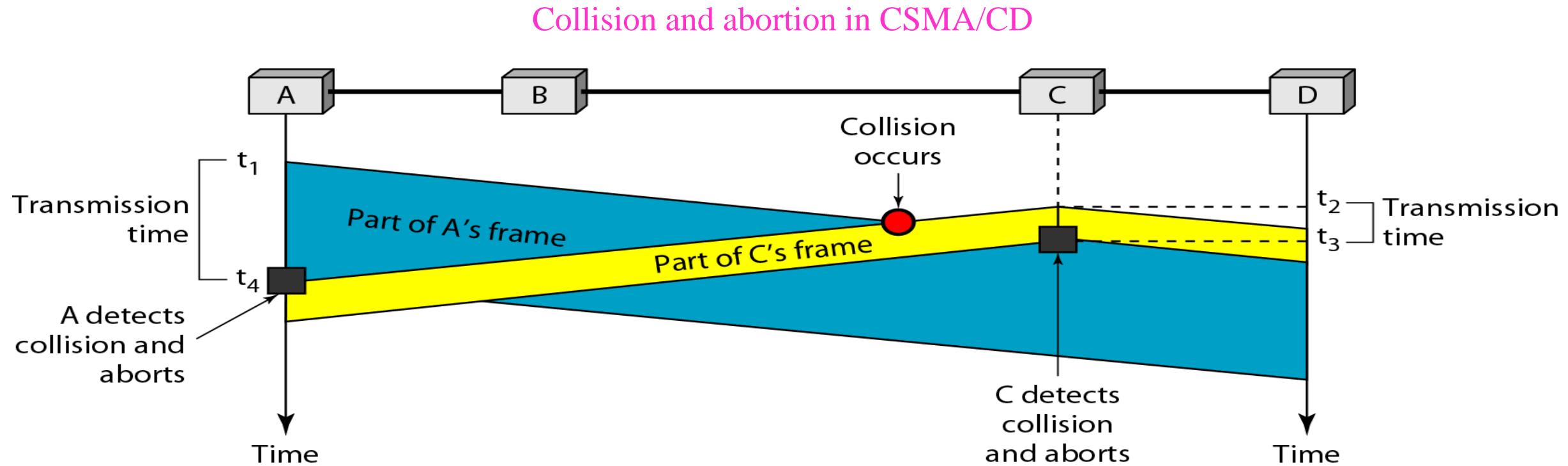
# Collision in CSMA/CD

- At time  $t_1$ , station A has executed its persistence procedure and starts sending the bits of its frame.
- At time  $t_2$ , station C has not yet sensed the first bit sent by A.
- Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right.
- The collision occurs sometime after time  $t_2$ .
- Station C detects a collision at time  $t_3$  when it receives the first bit of A's frame.
- Station C immediately or after a short time, but we assume immediately aborts transmission.
- Station A detects collision at time  $t_4$  when it receives the first bit of C's frame; it also immediately aborts transmission.



- A transmits for the duration  $t_4 - t_1$ ; C transmits for the duration  $t_3 - t_2$ .
- For the protocol to work, the length of any frame divided by the bit rate in this protocol must be more than either of these durations.
- At time  $t_4$ , the transmission of A's frame, though incomplete, is aborted; at time  $t_3$ , the transmission of B's frame, though incomplete, is aborted.

# Collision in CSMA/CD ... Contd.





# Minimum Frame Size

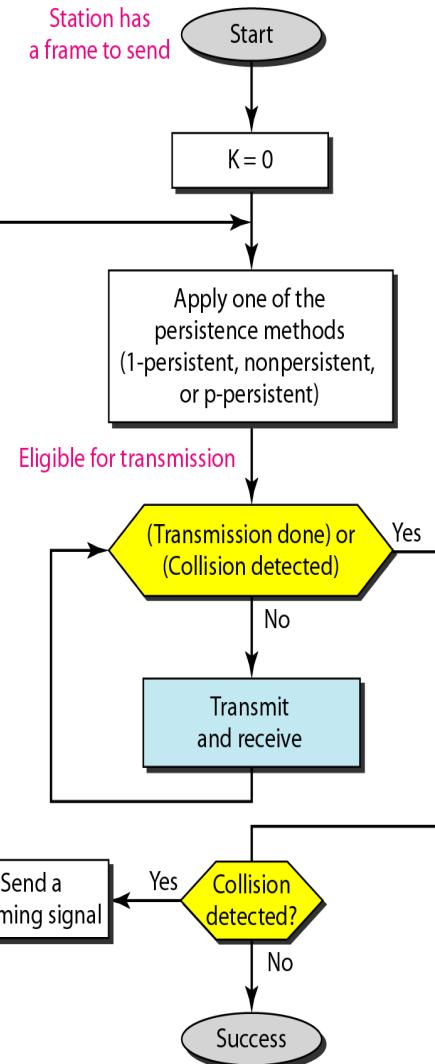
- For CSMA/CD to work, we need a restriction on the frame size.
- Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission.
- This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection.
- The frame transmission time  $T_{fr}$  must be at least two times the maximum propagation time  $T_p$ .
- If the two stations involved in a collision are the maximum distance apart, the signal from the first takes time  $T_p$  to reach the second, and the effect of the collision takes another time  $T_p$  to reach the first.
- So the requirement is that the **first station must still be transmitting after  $2T_p$** .

K: Number of attempts

$T_p$ : Maximum propagation time

$T_{fr}$ : Average transmission time for a frame

$T_B$ : Back-off time



Similar to the one for the ALOHA protocol, but there are differences:

1) Addition of the persistence process

- We need to sense the channel before we start sending the frame by using one of the persistence processes.

2) Frame transmission

- In ALOHA, transmit the entire frame and then wait for an acknowledgment.
- In CSMA/CD, transmission and collision detection is a continuous process.
- Do not send the entire frame and then look for a collision.
- The station transmits and receives continuously and simultaneously (using two different ports).

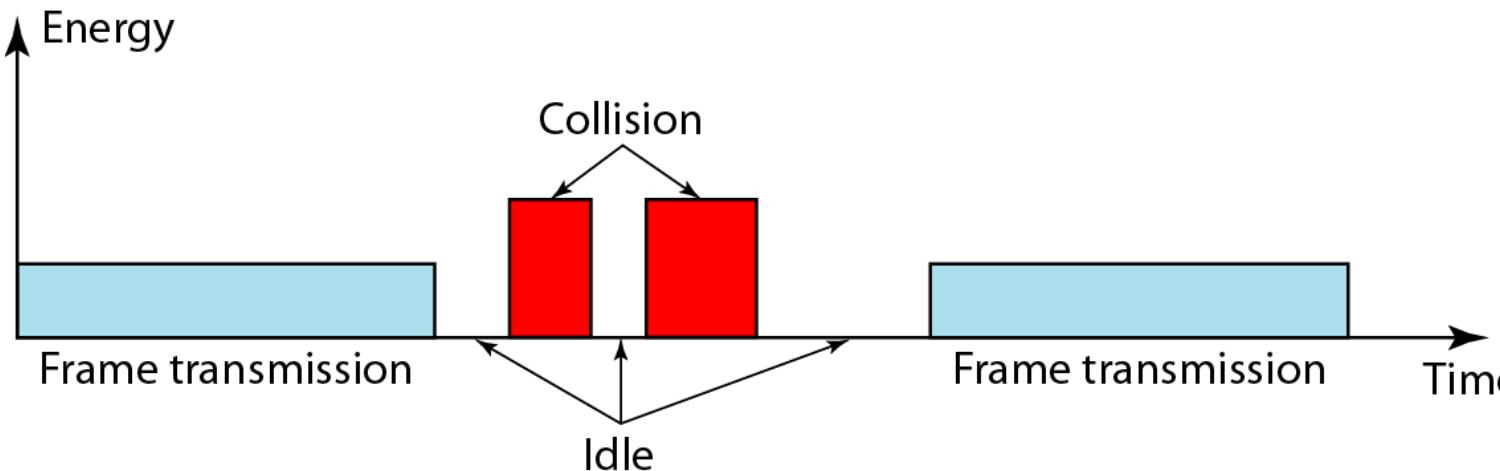
- Loop is used to show that transmission is a continuous process.
- Constantly monitor in order to detect one of two conditions: either transmission is finished or a collision is detected.
- Either event stops transmission.
- When we come out of the loop, if a collision has not been detected, it means that transmission is complete; the entire frame is transmitted.
- Otherwise, a collision has occurred.

3) Sending of a short jamming signal

- Enforces the collision in case other stations have not yet sensed the collision.

# Energy Level

- The level of energy in a channel can have three values: **zero, normal, and abnormal**.
- At the zero level, the channel is idle.
- At the normal level, a station has successfully captured the channel and is sending its frame.
- At the abnormal level, there is a collision and the level of the energy is twice the normal level.
- A station that has a frame to send or is sending a frame needs to monitor the energy level to determine if the channel is idle, busy, or in collision mode.





# Throughput

- The throughput of CSMA/CD is greater than that of pure or slotted ALOHA.
- The maximum throughput occurs at a different value of G and is based on the persistence method and the value of p in the p-persistent approach.
- For **1-persistent method** the maximum throughput is around **50 percent when G =1**.
- For **nonpersistent method**, the maximum throughput can go up to **90 percent when G is between 3 and 8**.



# Summary

## Discussed about

- Introduction
- Collision in CSMA/CD
- Minimum Frame Size
- Flow Diagram of CSMA/CD
- Energy Level
- Throughput



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**

# Computer Networks

## BCSE308L

## Carrier Sense Multiple Access – Collision Avoidance (CSMA/CA)

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai



# Overview

- Introduction
- Timing in CSMA/CA
- Interframe Space
- Contention Window
- Acknowledgment
- Flow Diagram
- Summary

# Introduction

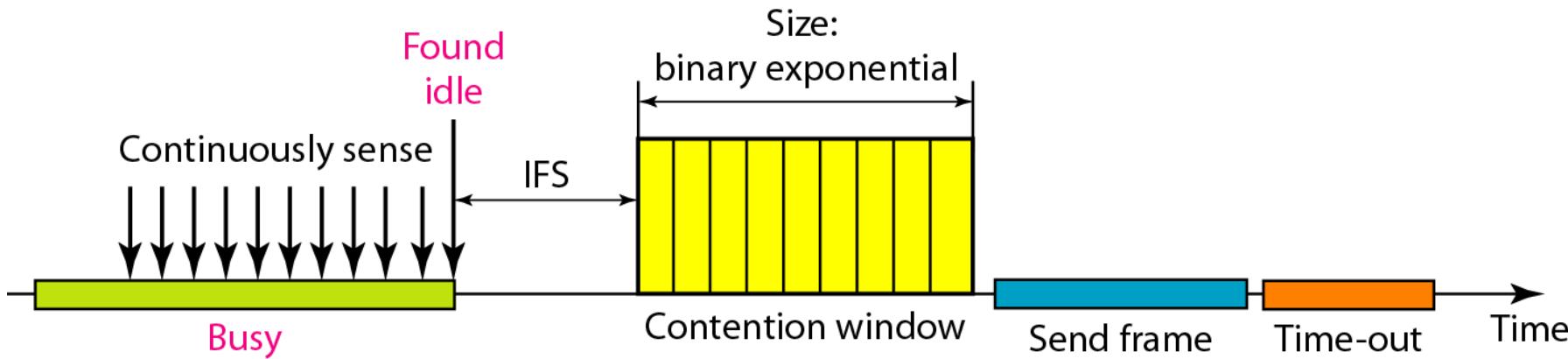
- The basic idea behind CSMA/CD is that a station needs to be able to receive while transmitting to detect a collision.
- When there is no collision, the station receives one signal: its own signal.
- When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station.
- To distinguish between these two cases, the received signals in these two cases must be significantly different.
- The signal from the second station needs to add a significant amount of energy to the one created by the first station.

# Introduction ... Contd.

- In a wired network, the received signal has almost the same energy as the sent signal because either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver.
- In a collision, the detected energy almost doubles.
- In a wireless network, much of the sent energy is lost in transmission.
- The received signal has very little energy, a collision may add only 5 to 10 percent additional energy.
- This is not useful for effective collision detection.
- Collisions need to be avoided on wireless networks because they cannot be detected.
- Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for this network.

# Timing in CSMA/CA

- Collisions are avoided through the use of CSMA/CA's three strategies: **the interframe space, the contention window, and acknowledgments**





# Interframe Space

- First, collisions are avoided by deferring transmission even if the channel is found idle.
- When an idle channel is found, the station does not send immediately.
- It waits for a period of time called the interframe space (IFS).
- The channel may appear idle when it is sensed, a distant station may have already started transmitting.
- The distant station's signal has not yet reached this station.
- The IFS time allows the front of the transmitted signal by the distant station to reach this station.
- If after the IFS time the channel is still idle, the station can send, but it still needs to wait a time equal to the contention time.
- The IFS variable can also be used to prioritize stations or frame types.
- E.g., a station that is assigned a shorter IFS has a higher priority.



# Contention Window

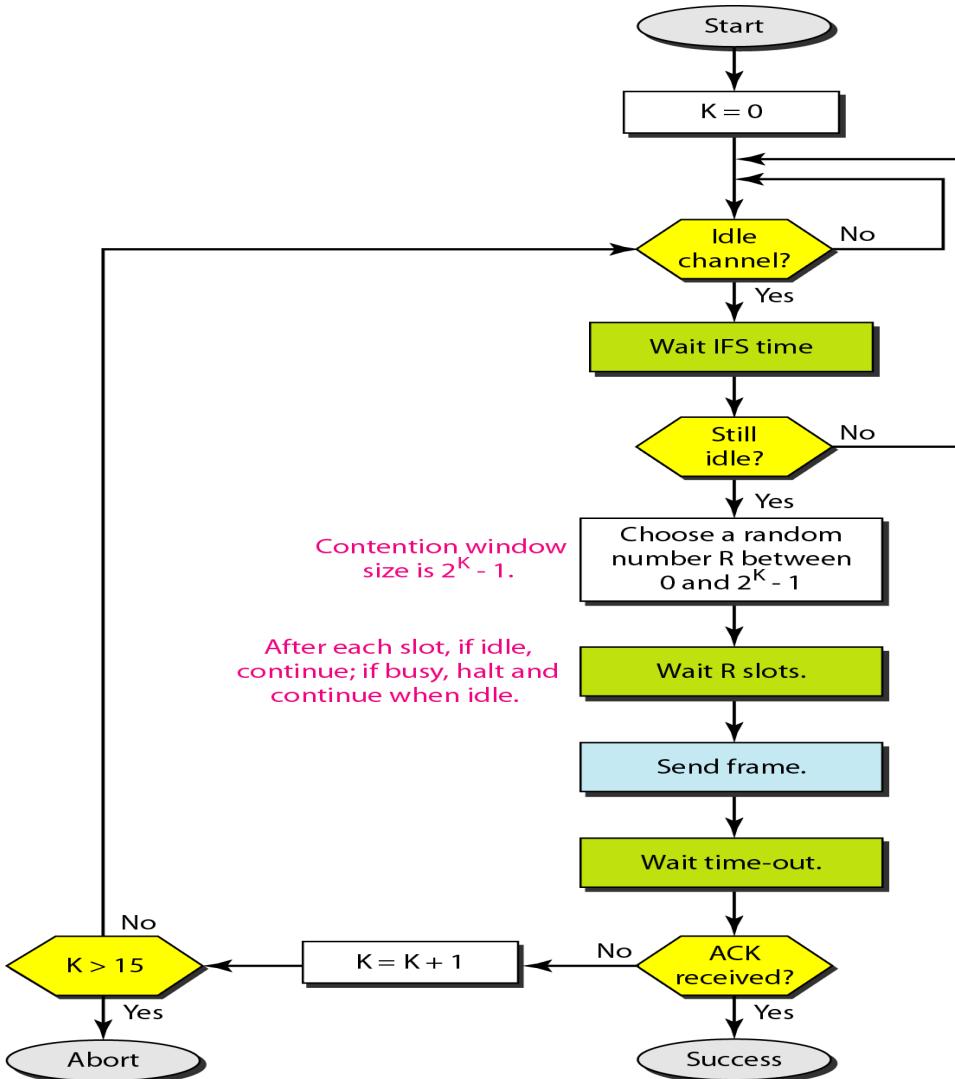
- The contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slots as its wait time.
- The number of slots in the window changes according to the **binary exponential back-off** strategy.
- This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.
- This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station.
- The contention window is that the station needs to sense the channel after each time slot.
- If the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle.
- This gives priority to the station with the longest waiting time.



# Acknowledgment

- With all these precautions, there still may be a collision resulting in destroyed data.
- In addition, the data may be corrupted during the transmission.
- The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

# Flow Diagram



- The channel needs to be sensed before and after the IFS.
- The channel also needs to be sensed during the contention time.
- For each time slot of the contention window, the channel is sensed.
- If it is found idle, the timer continues; if the channel is found busy, the timer is stopped and continues after the timer becomes idle again.



# Summary

## Discussed about

- Introduction
- Timing in CSMA/CA
- Interframe Space
- Contention Window
- Acknowledgment
- Flow Diagram



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**



VIT<sup>®</sup>

Vellore Institute of Technology  
(Deemed to be University under section 3 of UGC Act, 1956)

# Computer Networks

## BCSE308L

## Connecting Devices

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai

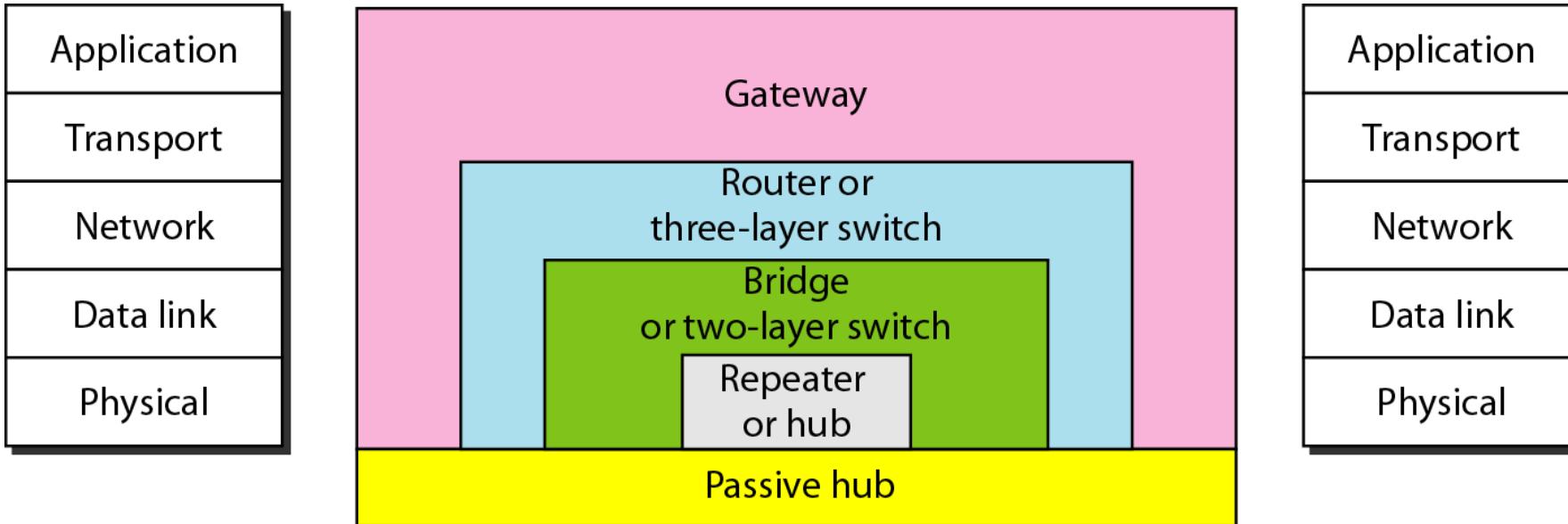


# Overview

- Introduction
- Passive Hubs
- Repeaters
- Active Hubs
- Bridges
- Two-Layer Switches
- Routers
- Three-Layer Switches
- Gateway
- Summary

# Introduction

- Connecting devices are divided into five different categories based on the layer in which they operate in a network.





# Passive Hubs

- A passive hub is just a connector.
- It connects the wires coming from different branches.
- In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point.
- This type of a hub is part of the media; its location in the Internet model is below the physical layer.

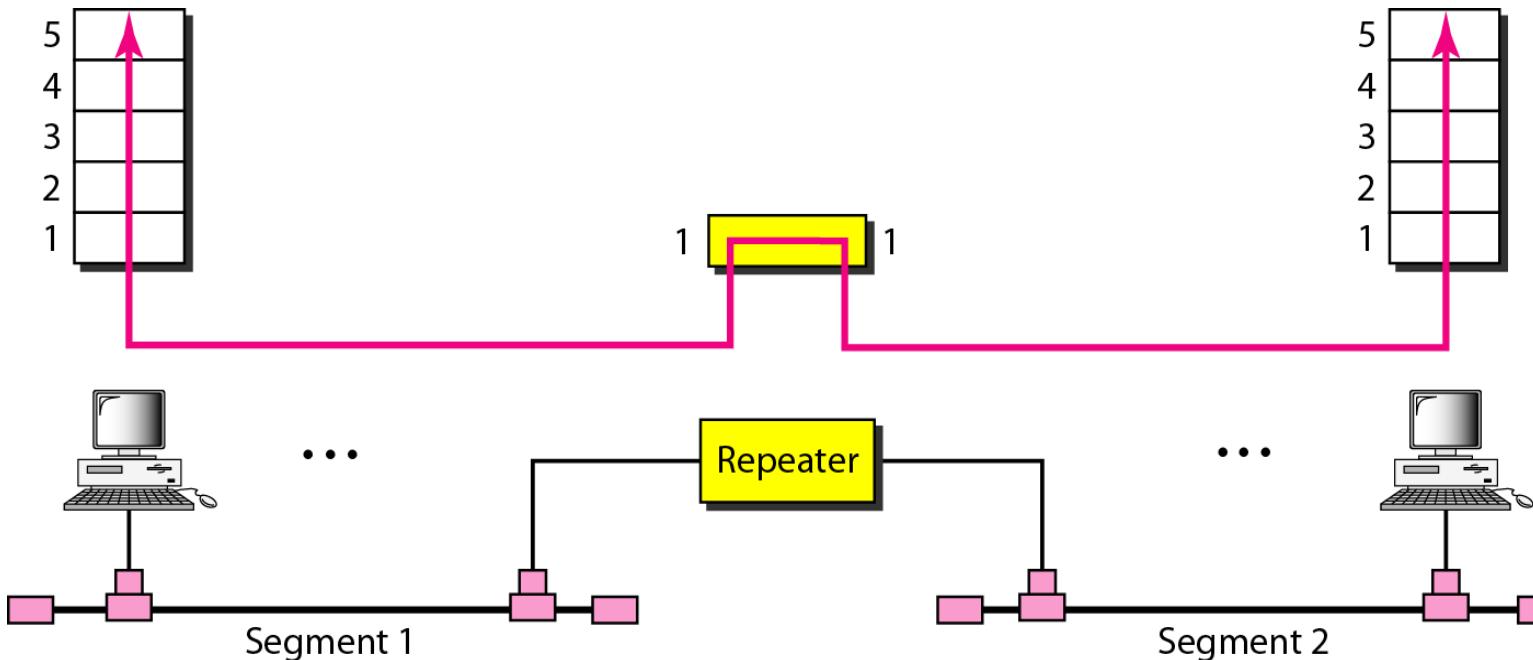


# Repeaters

- A repeater 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 the original bit pattern.
- The repeater then sends the refreshed signal.
- A repeater can extend the physical length of a LAN.

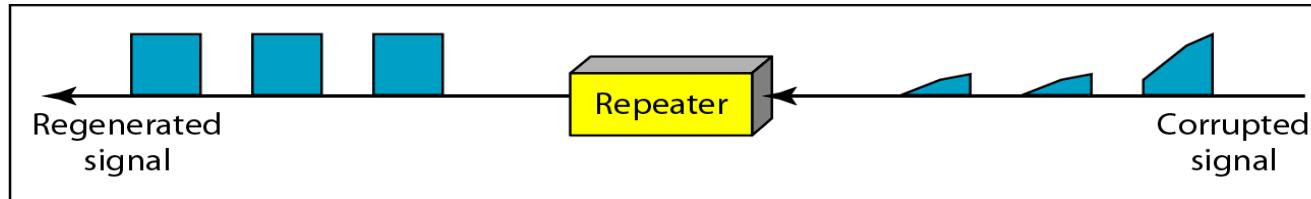
# Repeaters ... Contd.

- A repeater does not actually connect two LANs; it connects two segments of the same LAN.
- The segments connected are still part of one single LAN.
- A repeater is not a device that can connect two LANs of different protocols.

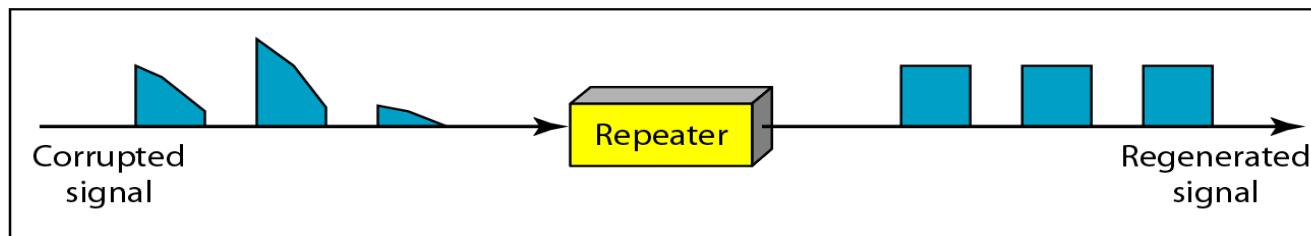


# Repeaters ... Contd.

- A repeater can overcome the 10Base5 Ethernet length restriction.
- In this standard, the length of the cable is limited to 500 m.
- To extend this length, we divide the cable into segments and install repeaters between segments.
- The whole network is still considered one LAN, but the portions of the network separated by repeaters are called segments.
- The repeater acts as a two-port node, but operates only in the physical layer.
- When it receives a frame from any of the ports, it regenerates and forwards it to the other port.



a. Right-to-left transmission.



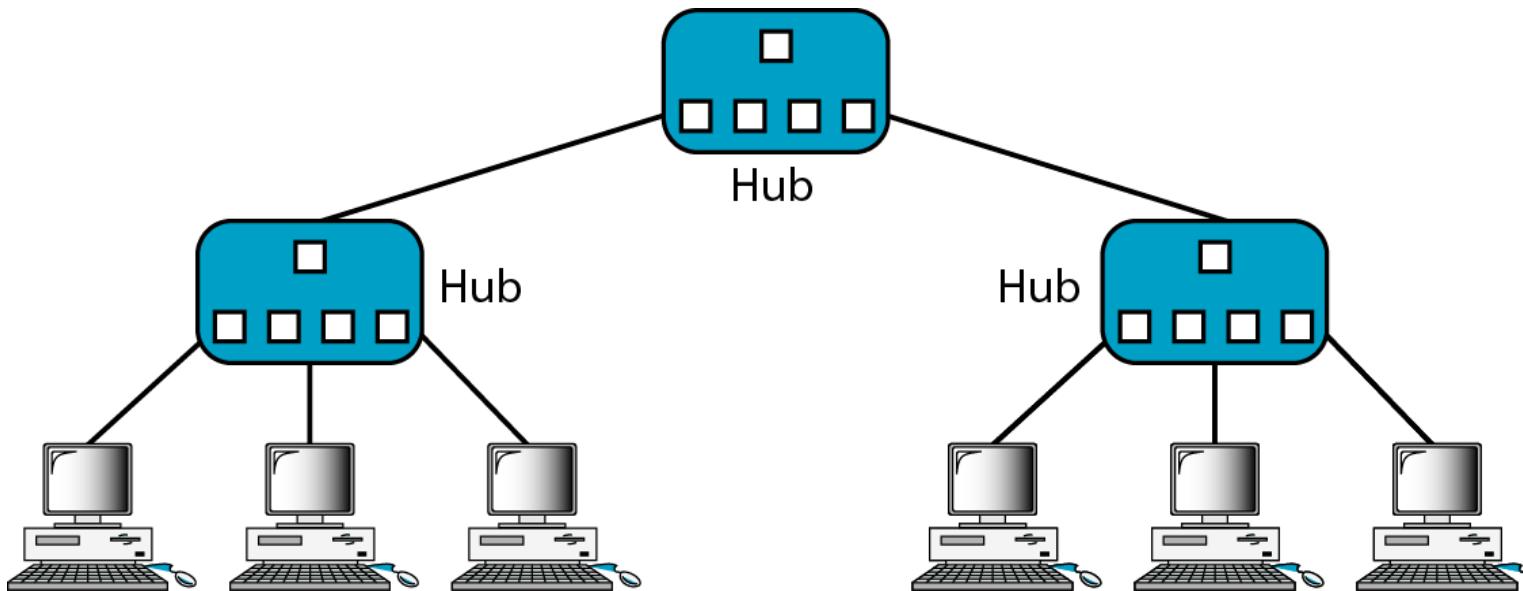
b. Left-to-right transmission.

# Repeaters ... Contd.

- A repeater forwards every frame; it has no filtering capability.
- **Repeater Vs. Amplifier**
  - An amplifier cannot discriminate between the intended signal and noise; it amplifies equally everything fed into it.
  - A repeater does not amplify the signal; it regenerates the signal.
  - When it receives a weakened or corrupted signal, it creates a copy, bit for bit, at the original strength.
  - A repeater is a regenerator, not an amplifier.
- The location of a repeater on a link is vital.
- A repeater must be placed so that a signal reaches it before any noise changes the meaning of any of its bits.
- A little noise can alter the precision of a bit's voltage without destroying its identity.
- If the corrupted bit travels much farther, however, accumulated noise can change its meaning completely.
- At that point, the original voltage is not recoverable, and the error needs to be corrected.
- A repeater placed on the line before the legibility of the signal becomes lost can still read the signal well enough to determine the intended voltages and replicate them in their original form.

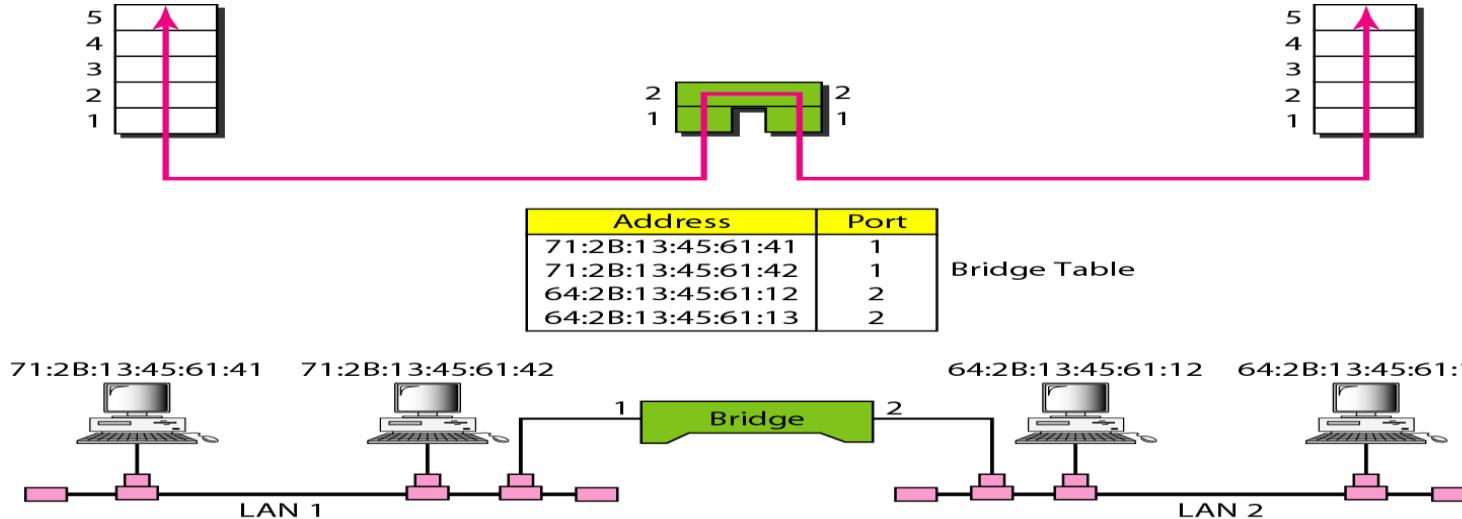
# Active Hubs

- An active hub is actually a multiport repeater.
- It is normally used to create connections between stations in a physical star topology.
- Hubs can be used to create multiple levels of hierarchy.
- The hierarchical use of hubs removes the length limitation of 10Base-T (100 m).



# Bridges

- A bridge operates in both the physical and the data link layer.
- As a physical layer device, it regenerates the signal it receives.
- As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame.



- A bridge does not change the physical (MAC) addresses in a frame.



# Bridges ... Contd.

- What is the difference in functionality between a bridge and a repeater?
  - A bridge has filtering capability.
  - It can check the destination address of a frame and decide if the frame should be forwarded or dropped.
  - If the frame is to be forwarded, the decision must specify the port.
  - A bridge has a table that maps addresses to ports.
  - A bridge has a table used in filtering decisions.

# Bridges ... Contd.

## Transparent Bridges

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



# Bridges ... Contd.

## Forwarding

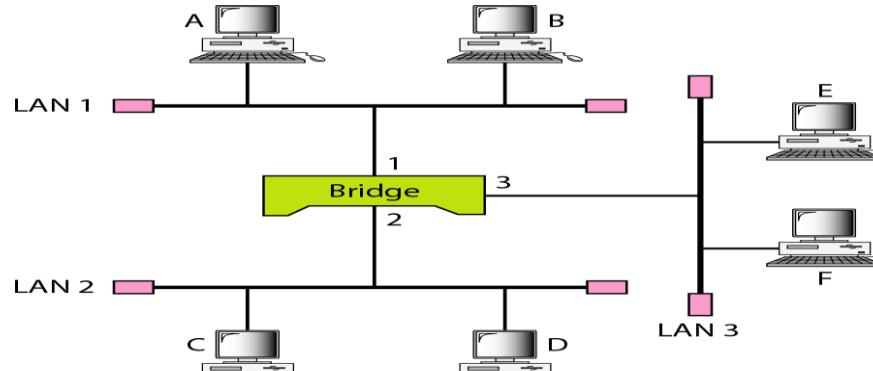
- A transparent bridge must correctly forward the frames.

## Learning

- The earliest bridges had forwarding tables that were static.
- The systems administrator would manually enter each table entry during bridge setup.
- Although the process was simple, it 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.

# Bridges ... Contd.

- A better solution to the static table is a dynamic table that maps addresses to ports automatically.
- To make a table dynamic, we need a bridge that gradually learns from the frame movements.
- To do this, the bridge inspects both the destination and the source addresses.
- 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.



Address	Port

a. Original

Address	Port
A	1

b. After A sends a frame to D

Address	Port
A	1
E	3

c. After E sends a frame to A

Address	Port
A	1
E	3
B	1

d. After B sends a frame to C

# Bridges ... Contd.

## Source Routing Bridges

- One way to prevent loops in a system with redundant bridges is to use source routing bridges.
- A transparent bridge's duties include filtering frames, forwarding, and blocking.
- In a system that has source routing bridges, these duties are performed by the source station and, to some extent, the destination station.
- In source routing, a sending station defines the bridges that the frame must visit.
- The addresses of these bridges are included in the frame.
- The frame contains not only the source and destination addresses, but also the addresses of all bridges to be visited.
- The source gets these bridge addresses through the exchange of special frames with the destination prior to sending the data frame.
- Source routing bridges were designed by IEEE to be used with Token Ring LANs.

# Two-Layer Switches

- A switch can mean two different things - a two-layer switch or a three-layer switch (the level at which the device operates).
- A three-layer switch is used at the network layer; it is a kind of router.
- The two-layer switch performs at the physical and data link layers.
- A two-layer switch is a bridge, a bridge with many ports and a design that allows better (faster) performance.
- A bridge with a few ports can connect a few LANs together.
- A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity.
- This means no competing traffic (no collision) as in Ethernet.

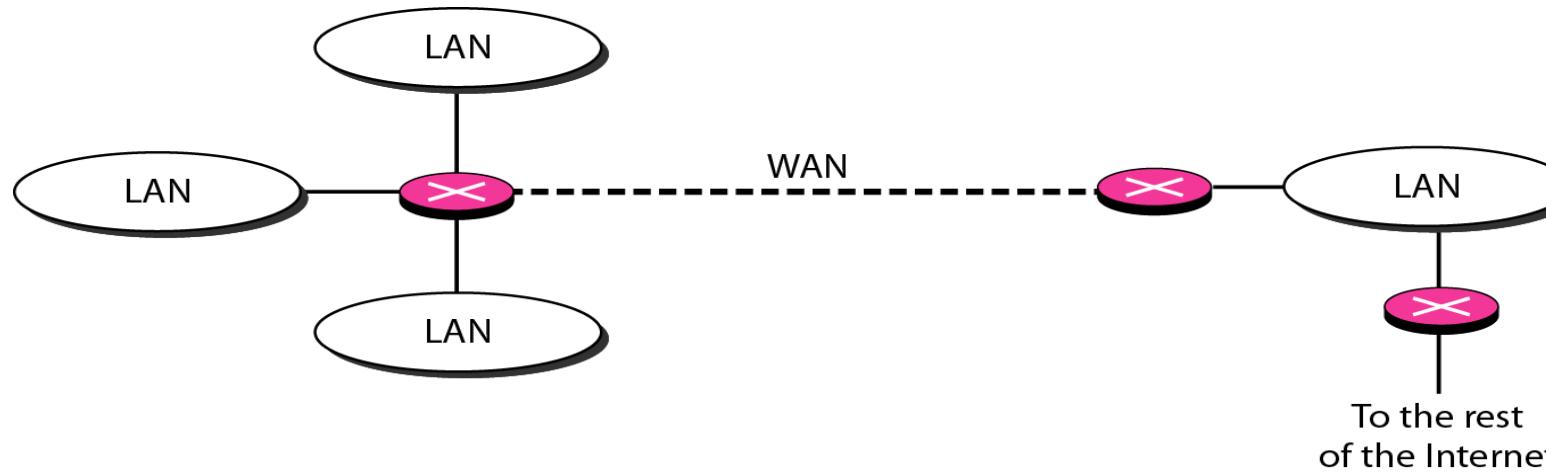


# Two-Layer Switches ... Contd.

- A two-layer switch, as a bridge does, makes a filtering decision based on the MAC address of the frame it received.
- It can be more sophisticated.
- It can have a buffer to hold the frames for processing.
- It can have a switching factor that forwards the frames faster.
- Some new two-layer switches, called cut-through switches, have been designed to forward the frame as soon as they check the MAC addresses in the header of the frame.

# Routers

- A router is a three-layer device that routes packets based on their logical addresses (host-to-host addressing).
- A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route.
- The routing tables are normally dynamic and are updated using routing protocols.





# Three-Layer Switches

- A three-layer switch is a router, but a faster and more sophisticated.
- The switching fabric in a three-layer switch allows faster table lookup and forwarding.



# Gateway

- A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model.
- A gateway takes an application message, reads it, and interprets it.
- This means that it can be used as a connecting device between two internetworks that use different models.
- For example, a network designed to use the OSI model can be connected to another network using the Internet model.
- The gateway connecting the two systems can take a frame as it arrives from the first system, move it up to the OSI application layer, and remove the message.
- Gateways can provide security.



# Summary

## Discussed about

- Introduction
- Passive Hubs
- Repeaters
- Active Hubs
- Bridges
- Two-Layer Switches
- Routers
- Three-Layer Switches
- Gateway



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**

# Computer Networks

## BCSE308L

### IEEE 802.3 (Ethernet) – Wired LANs

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai

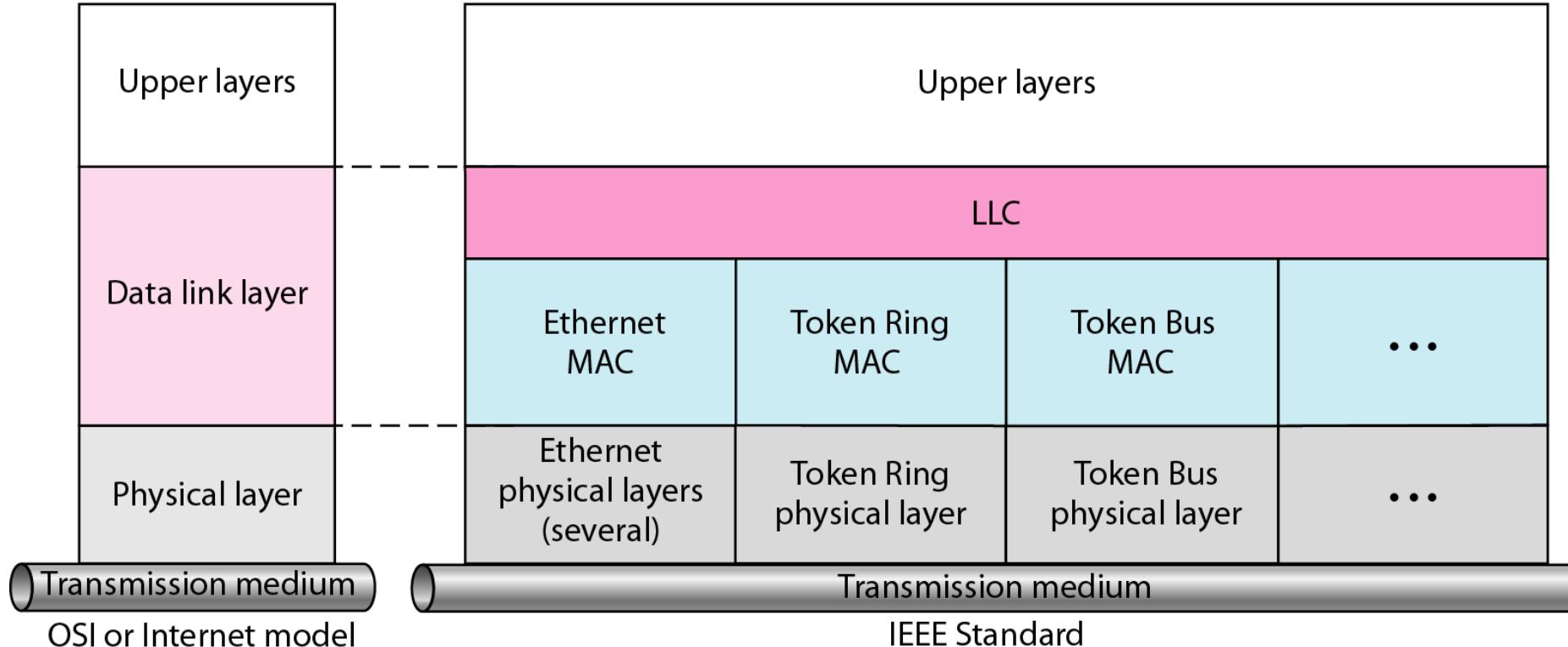


# Overview

- IEEE Standard for LANs
- Standard Ethernet
- Changes in the Standard
- Fast Ethernet
- Gigabit Ethernet
- Ten Gigabit Ethernet
- Practice Questions
- Summary

# IEEE standard for LANs

LLC: Logical link control  
MAC: Media access control

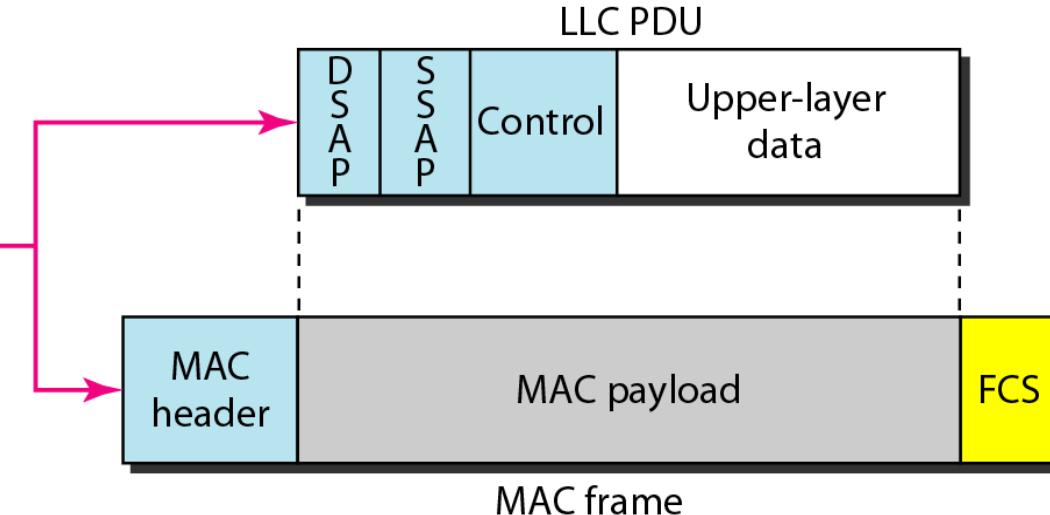
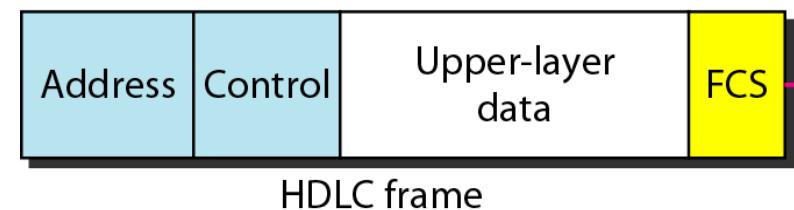


# IEEE standard for LANs ... Contd.

## *HDLC frame compared with LLC and MAC frames*

DSAP: Destination service access point

SSAP: Source service access point



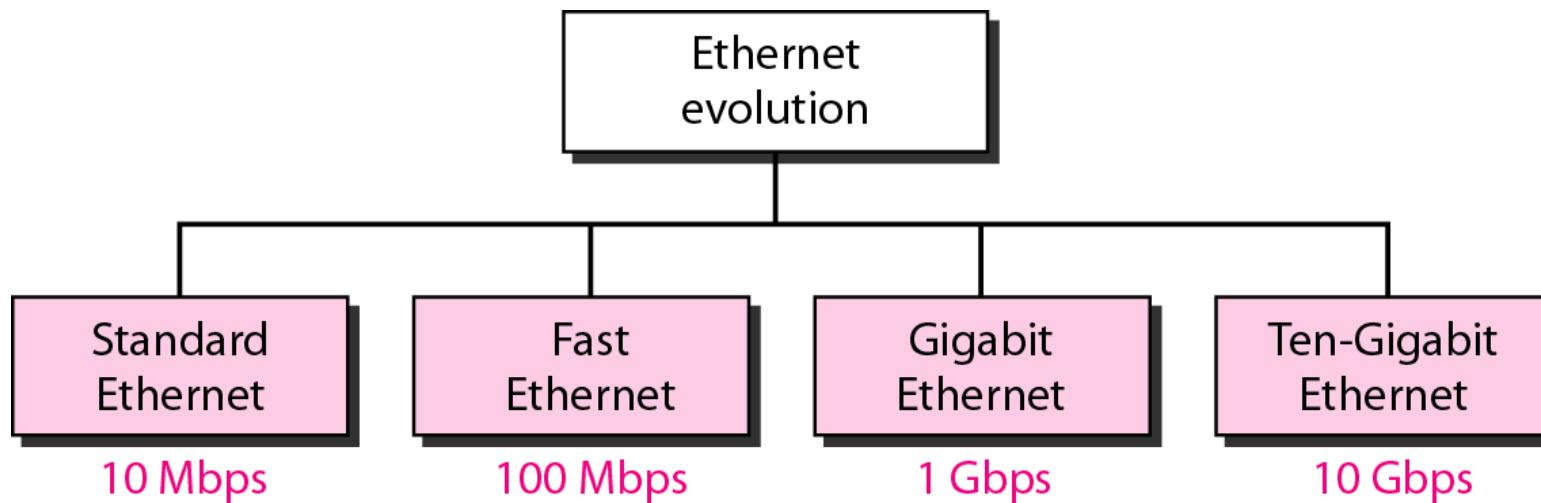


# Standard Ethernet

- The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC).
- Since then, it has gone through four generations.

# Standard Ethernet ... Contd.

***Ethernet evolution through four generations***

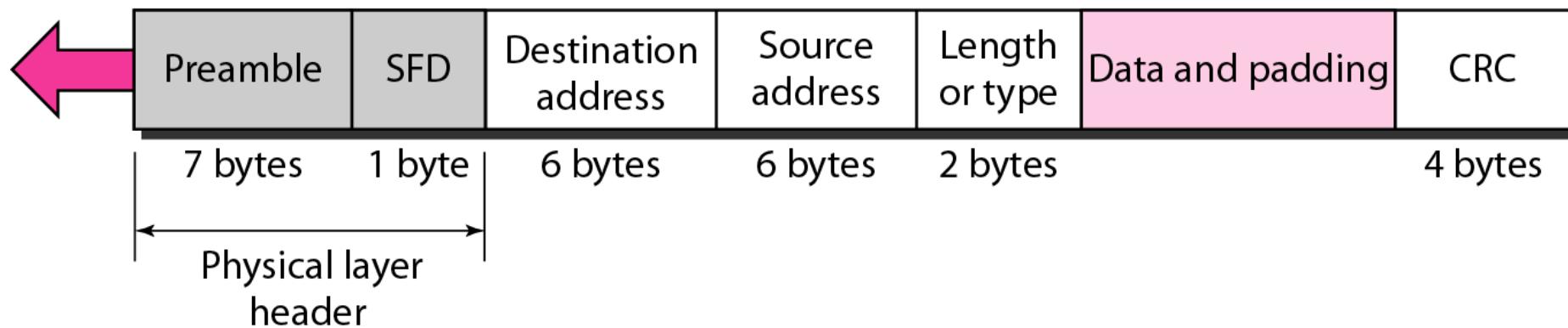


# Standard Ethernet ... Contd.

## *802.3 MAC frame*

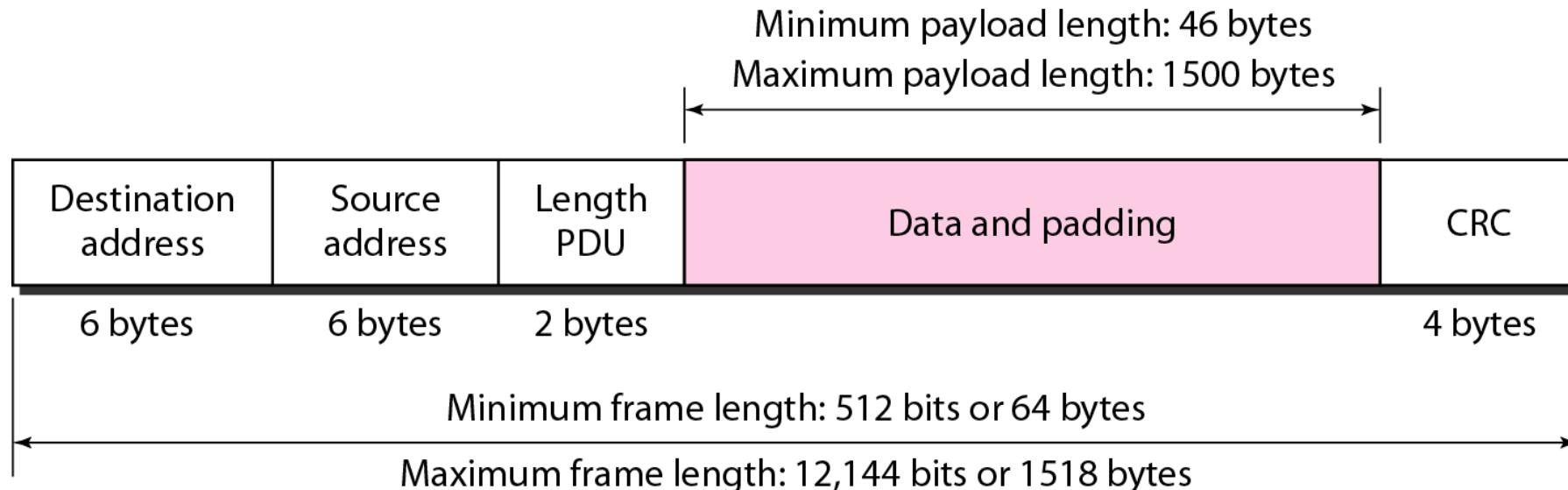
**Preamble:** 56 bits of alternating 1s and 0s.

**SFD:** Start frame delimiter, flag (10101011)



# Standard Ethernet ... Contd.

## *Minimum and maximum lengths*





# Standard Ethernet ... Contd.

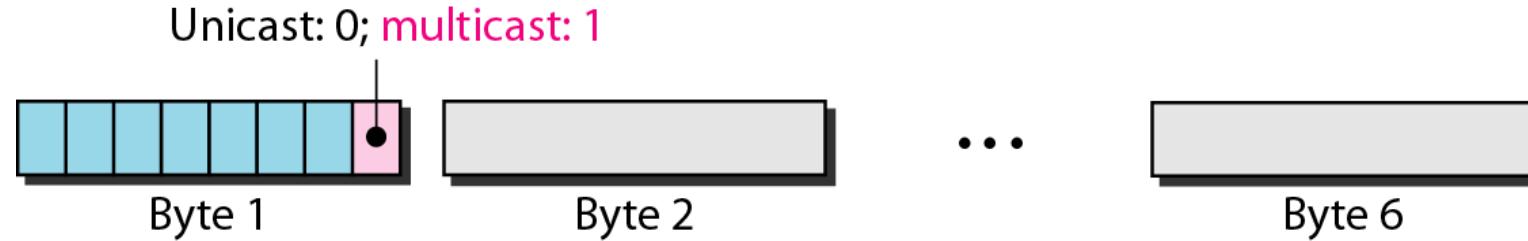
*Example of an Ethernet address in hexadecimal notation*

06 : 01 : 02 : 01 : 2C : 4B

6 bytes = 12 hex digits = 48 bits

# Standard Ethernet ... Contd.

## *Unicast and multicast addresses*



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

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

The broadcast destination address is a special case of the multicast address in which all bits are 1s.

- ④ A unicast destination address defines only one recipient; the relationship between the sender and the receiver is one-to-one.
- ④ A multicast destination address defines a group of addresses; the relationship between the sender and the receivers is one-to-many.
- ④ The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN.
  - ④ A broadcast destination address is forty-eight (48) 1s.

# Standard Ethernet ... Contd.

**Define the type of the following destination addresses:**

- a. 4A:30:10:21:10:1A
- b. 47:20:1B:2E:08:EE
- c. FF:FF:FF:FF:FF:FF

## **Solution**

*To find the type of the address, we need to look at the second hexadecimal digit from the left. If it is even, the address is unicast. If it is odd, the address is multicast. If all digits are F's, the address is broadcast.*

*Therefore, we have the following:*

- a. This is a unicast address because A in binary is 1010.
- b. This is a multicast address because 7 in binary is 0111.
- c. This is a broadcast address because all digits are F's.

# Standard Ethernet ... Contd.

Show how the address **47:20:1B:2E:08:EE** is sent out on line.

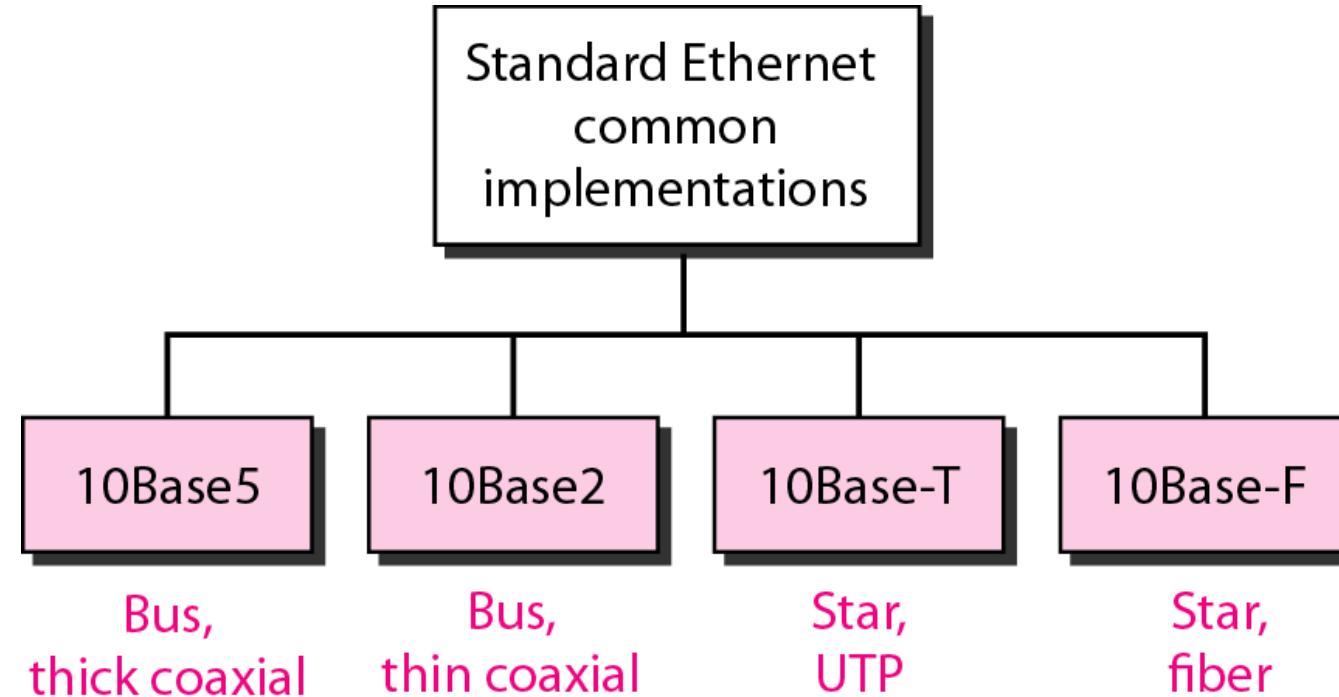
## Solution

The address is sent left-to-right, byte by byte; for each byte, it is sent right-to-left, bit by bit, as shown below:



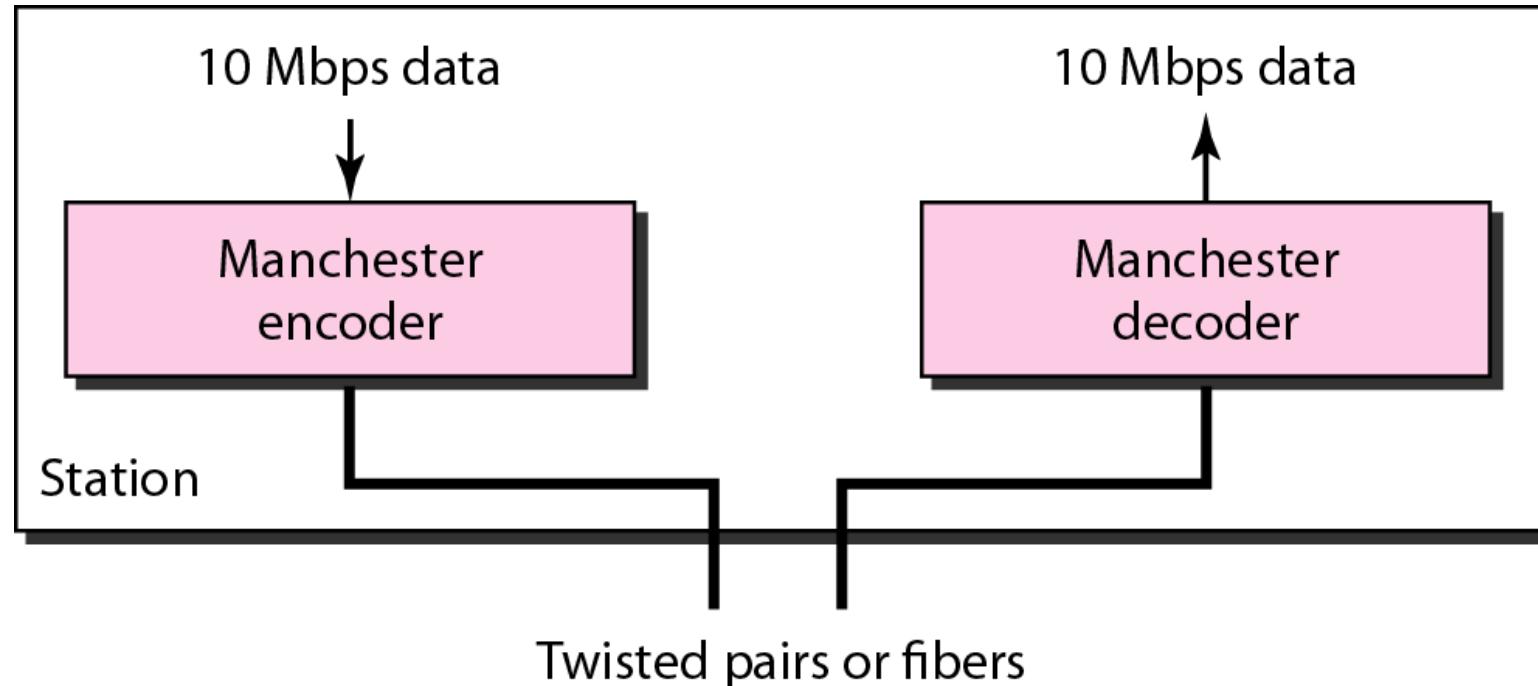
# Standard Ethernet ... Contd.

## *Categories of Standard Ethernet*



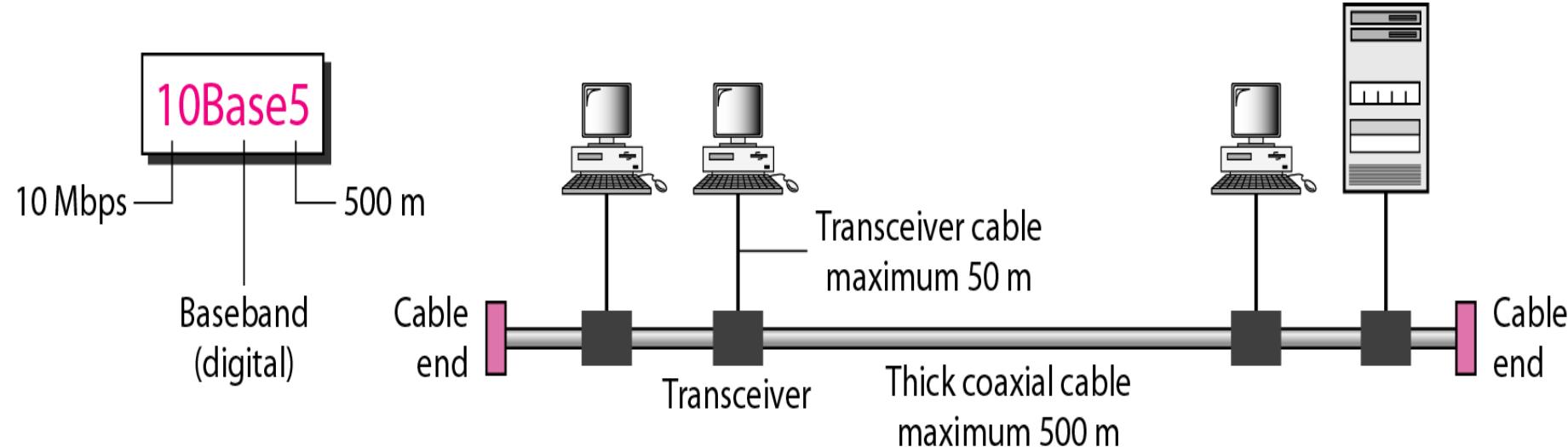
# Standard Ethernet ... Contd.

*Encoding in a Standard Ethernet implementation*



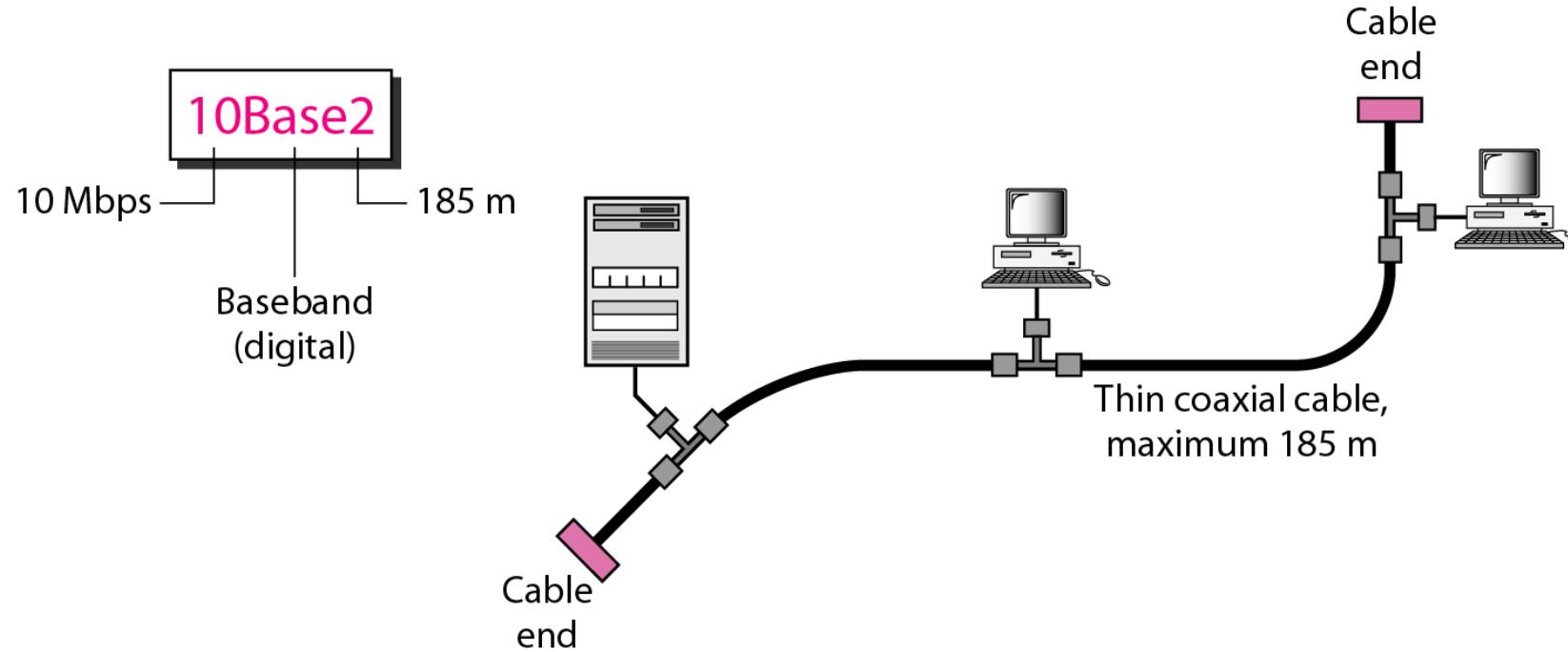
# Standard Ethernet ... Contd.

## *10Base5 implementation*



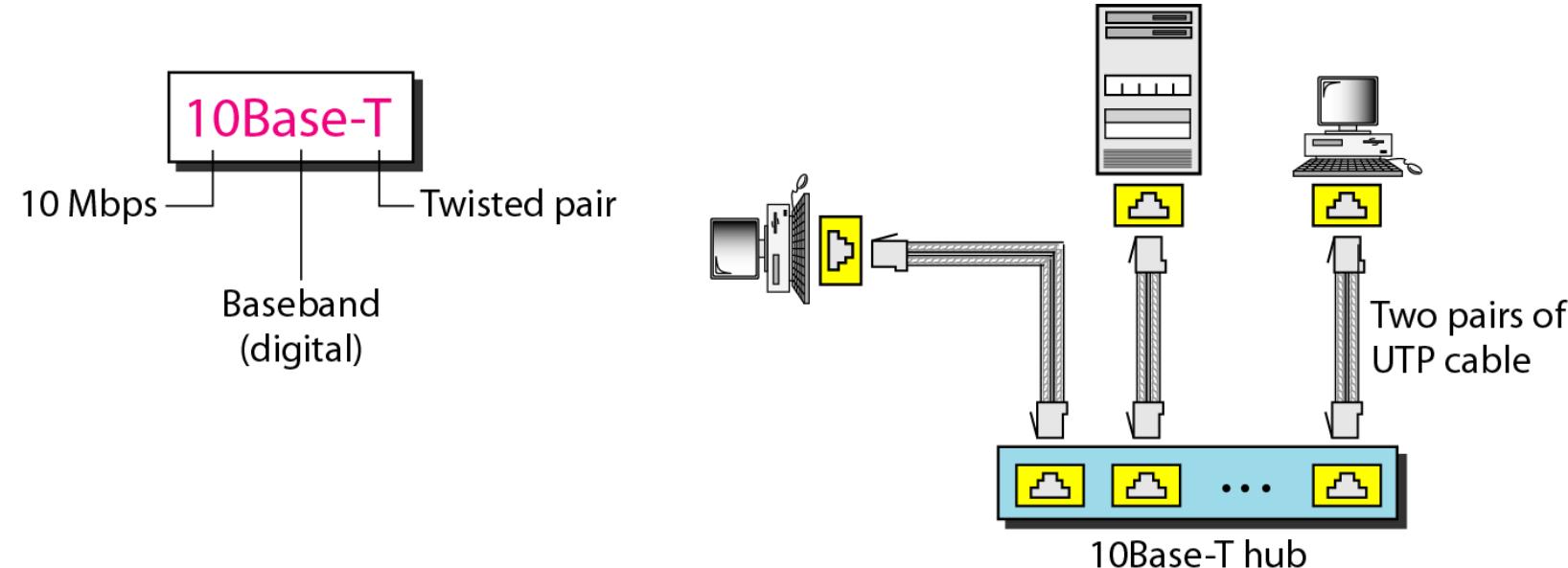
# Standard Ethernet ... Contd.

## *10Base2 implementation*



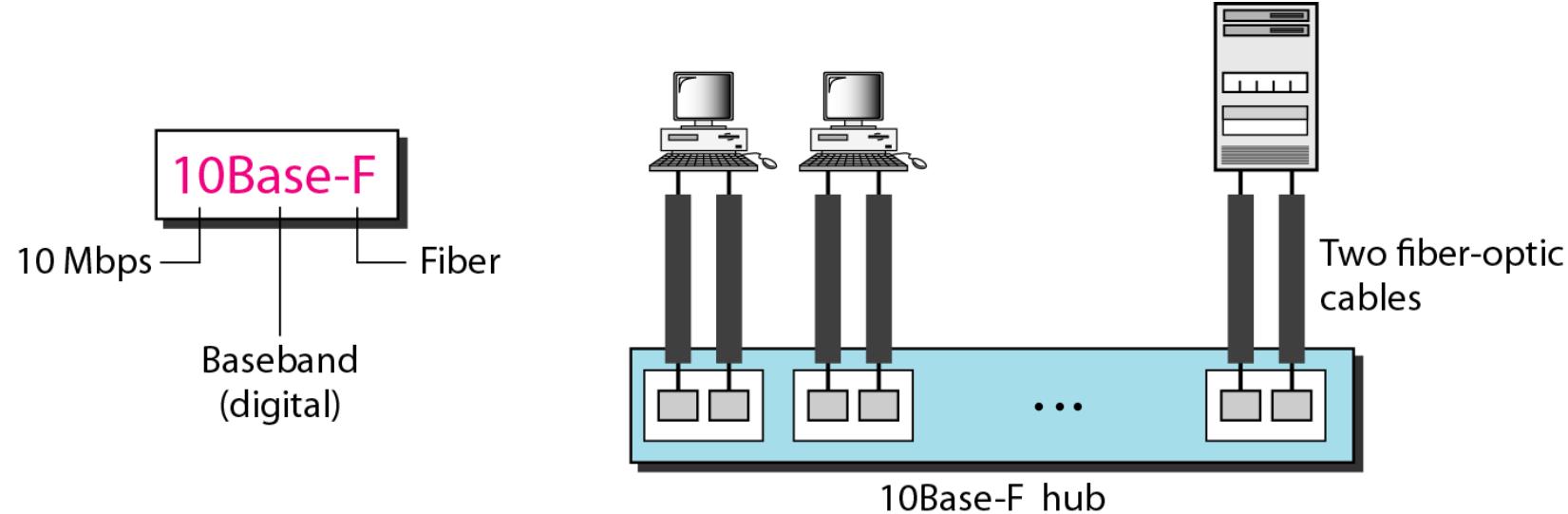
# Standard Ethernet ... Contd.

## *10Base-T implementation*



# Standard Ethernet ... Contd.

## *10Base-F implementation*





# Standard Ethernet ... Contd.

## *Summary of Standard Ethernet implementations*

Characteristics	10Base5	10Base2	10Base-T	10Base-F
Media	Thick coaxial cable	Thin coaxial cable	2 UTP	2 Fiber
Maximum length	500 m	185 m	100 m	2000 m
Line encoding	Manchester	Manchester	Manchester	Manchester

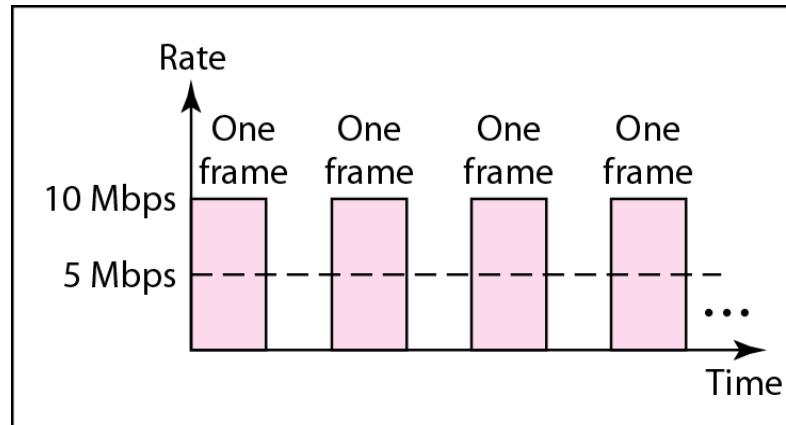


# Changes in the Standard

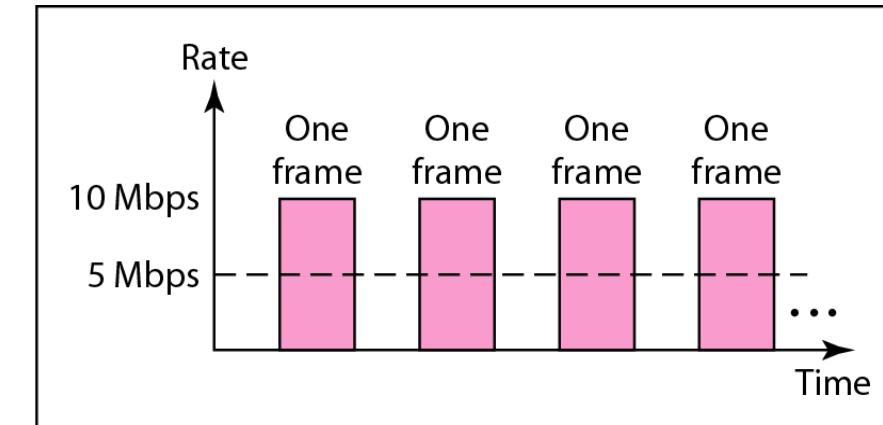
- The 10-Mbps Standard Ethernet has gone through several changes before moving to the higher data rates.
- These changes actually opened the road to the evolution of the Ethernet to become compatible with other high-data-rate LANs.
- The first step in the Ethernet evolution was the **division of a LAN by bridges**.
- Bridges have **two effects on an Ethernet LAN**.
- They raise the bandwidth and they separate collision domains.

# Changes in the Standard ... Contd.

## *Sharing bandwidth*



a. First station



b. Second station

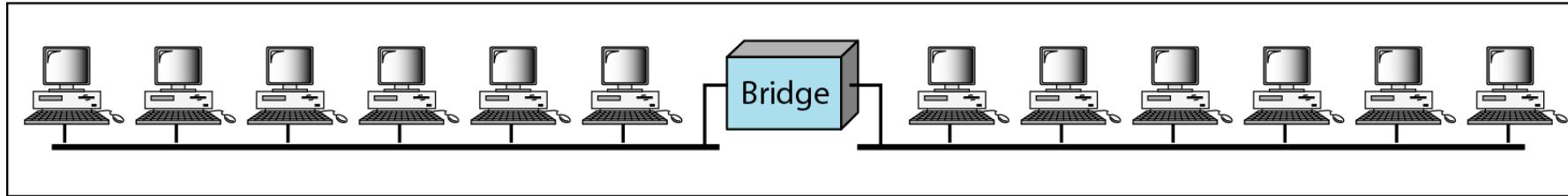
When one station is sending, the other one refrains from sending.

# Changes in the Standard ... Contd.

*A network with and without a bridge*



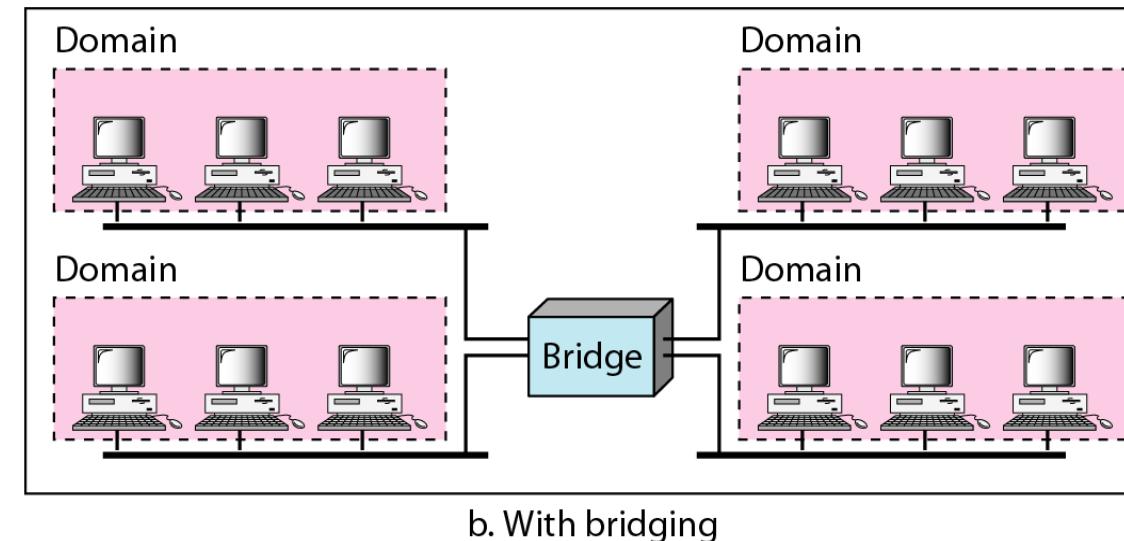
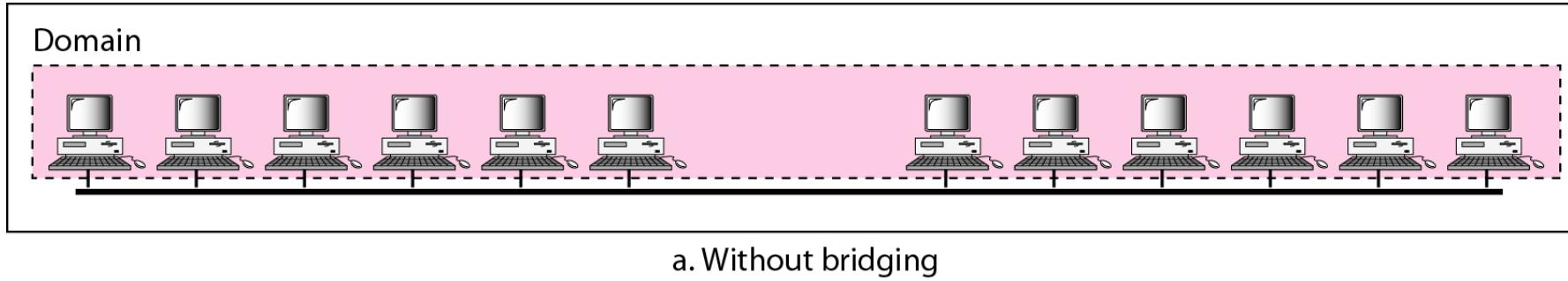
a. Without bridging



b. With bridging

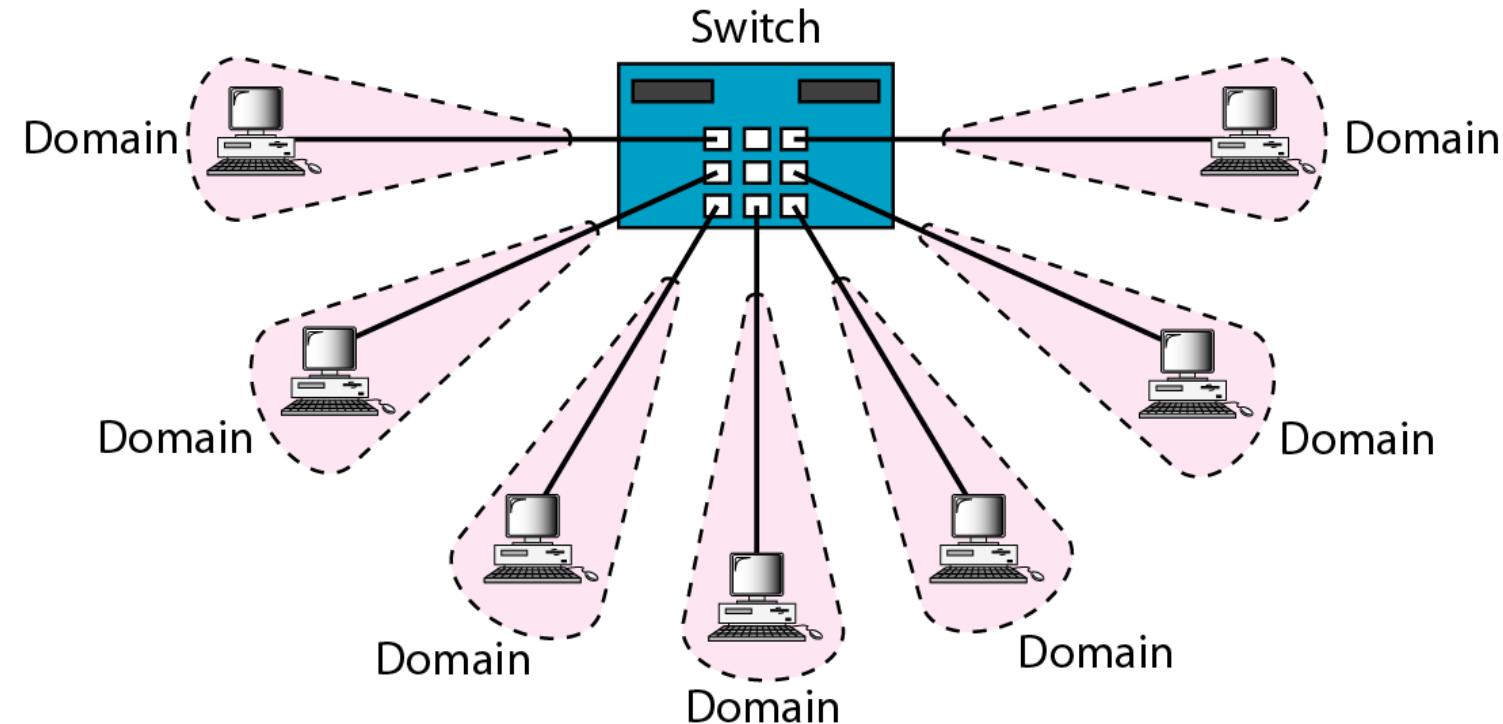
# Changes in the Standard ... Contd.

*Collision domains in an unbridged network and a bridged network*



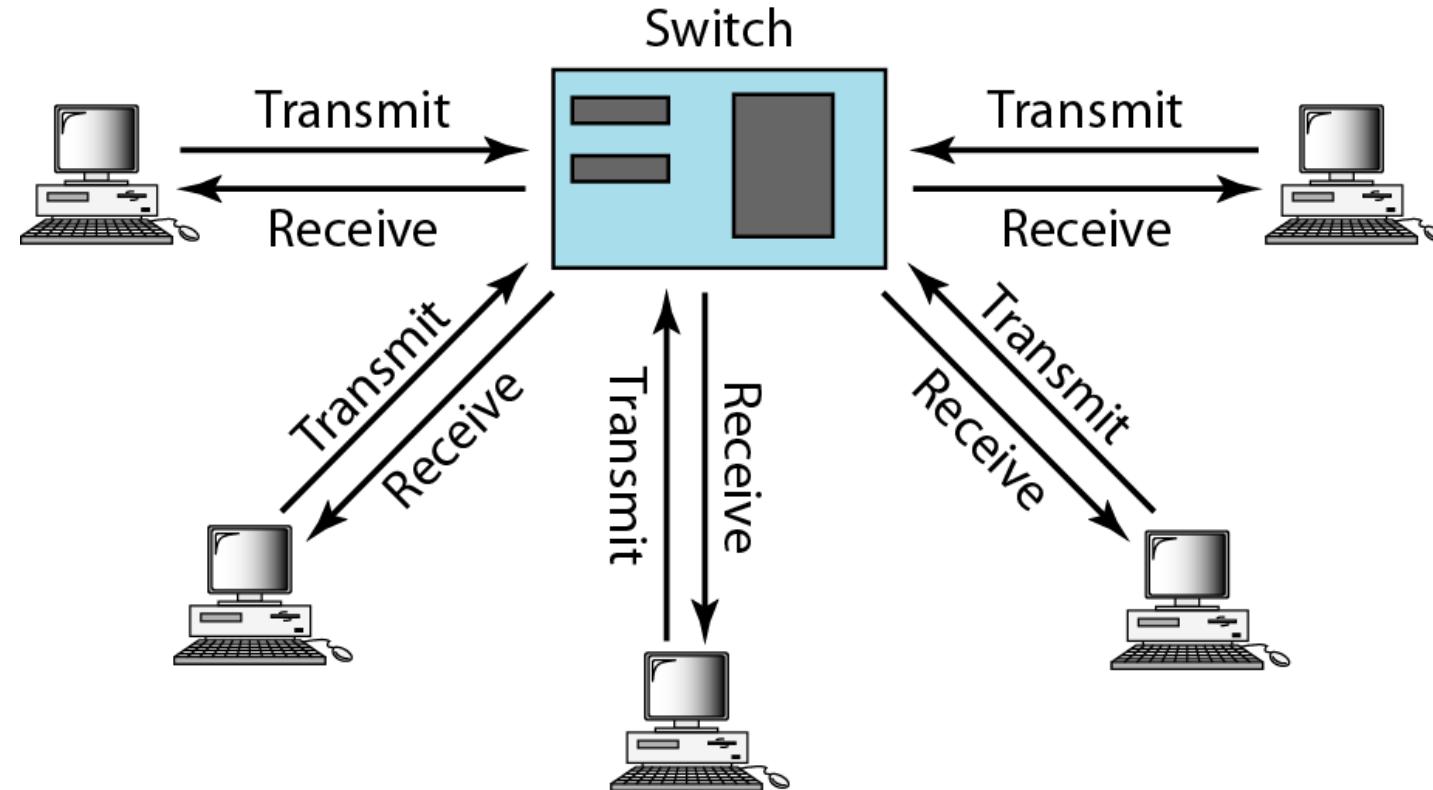
# Changes in the Standard ... Contd.

## *Switched Ethernet*



# Changes in the Standard ... Contd.

## *Full-duplex switched Ethernet*



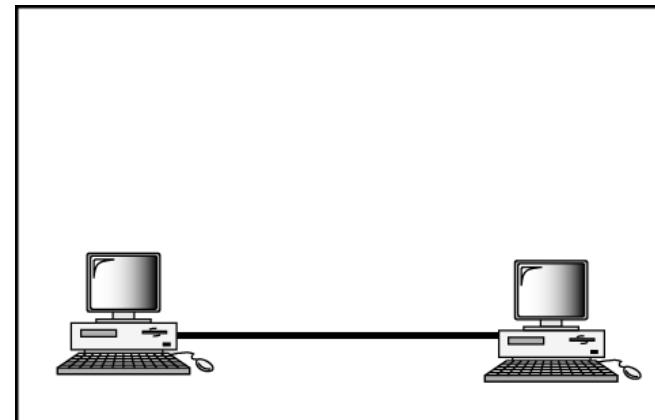


# Fast Ethernet

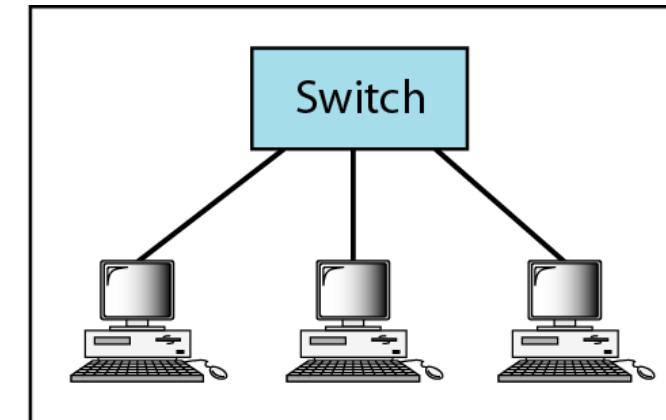
- Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel.
- IEEE created Fast Ethernet under the name 802.3u.
- Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps.
- The **goals of Fast Ethernet** can be summarized as follows:
  - ✓ Upgrade the data rate to 100 Mbps.
  - ✓ Make it compatible with Standard Ethernet.
  - ✓ Keep the same 48-bit address.
  - ✓ Keep the same frame format.
  - ✓ Keep the same minimum and maximum frame lengths.

# Fast Ethernet ... Contd.

## *Fast Ethernet topology*



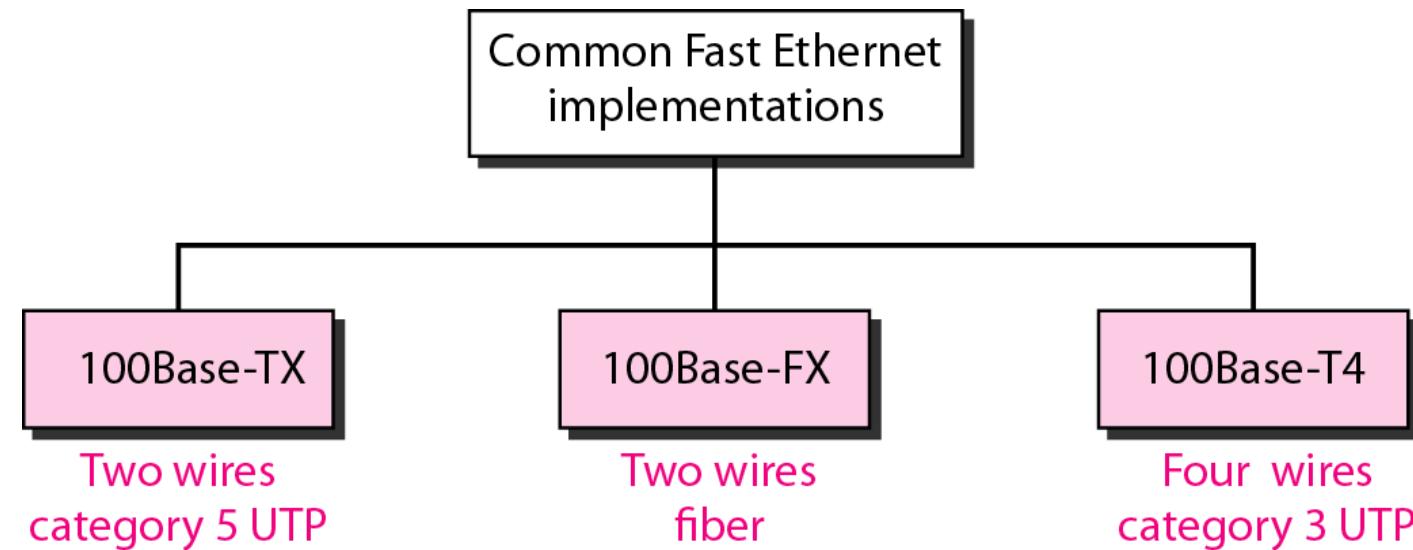
a. Point-to-point



b. Star

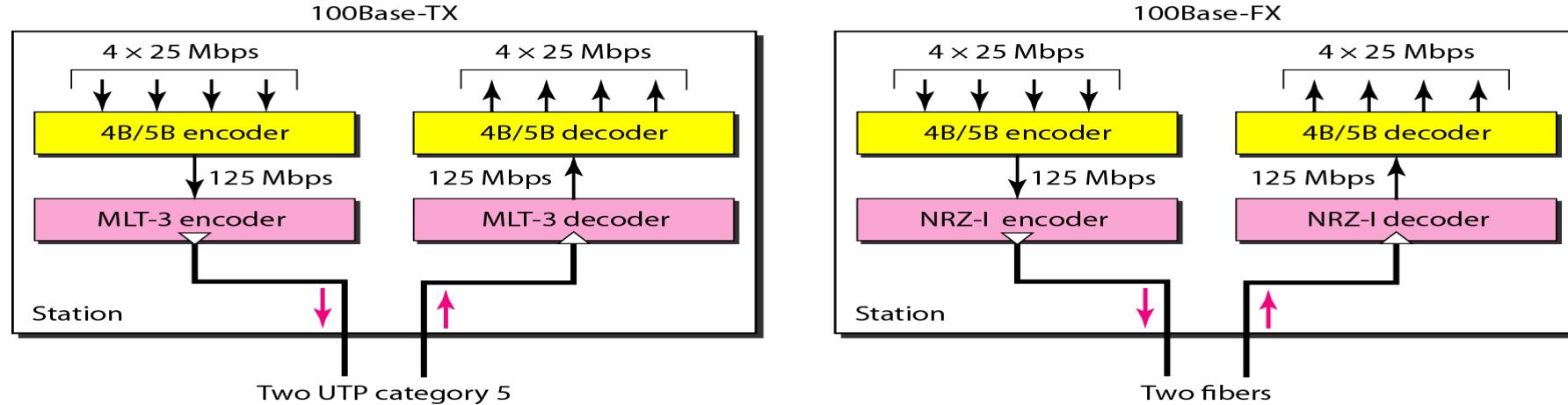
# Fast Ethernet ... Contd.

## *Fast Ethernet implementations*



# Fast Ethernet ... Contd.

## *Encoding for Fast Ethernet implementation*





# Fast Ethernet ... Contd.

## *Summary of Fast Ethernet implementations*

<i>Characteristics</i>	<i>100Base-TX</i>	<i>100Base-FX</i>	<i>100Base-T4</i>
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

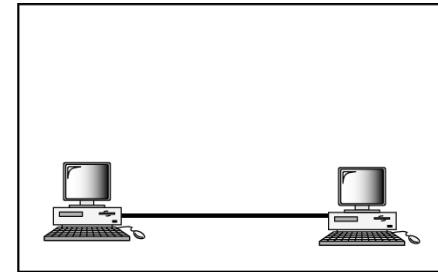


# Gigabit Ethernet

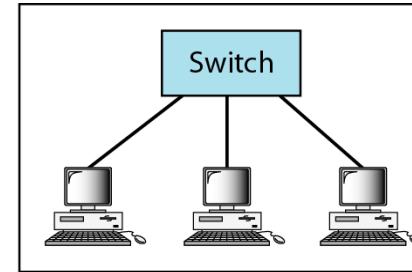
- The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps).
- The IEEE committee calls the standard 802.3z.
- In the full-duplex mode of Gigabit Ethernet, there is no collision; the maximum length of the cable is determined by the signal attenuation in the cable.
- The goals of the Gigabit Ethernet design can be summarized as follows:
  - ✓ Upgrade the data rate to 1 Gbps.
  - ✓ Make it compatible with Standard or Fast Ethernet.
  - ✓ Use the same 48-bit address.
  - ✓ Use the same frame format.
  - ✓ Keep the same minimum and maximum frame lengths.
  - ✓ To support autonegotiation.

# Gigabit Ethernet ... Contd.

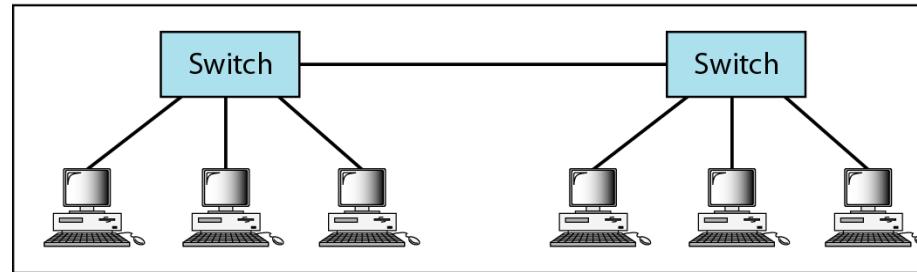
## *Topologies of Gigabit Ethernet*



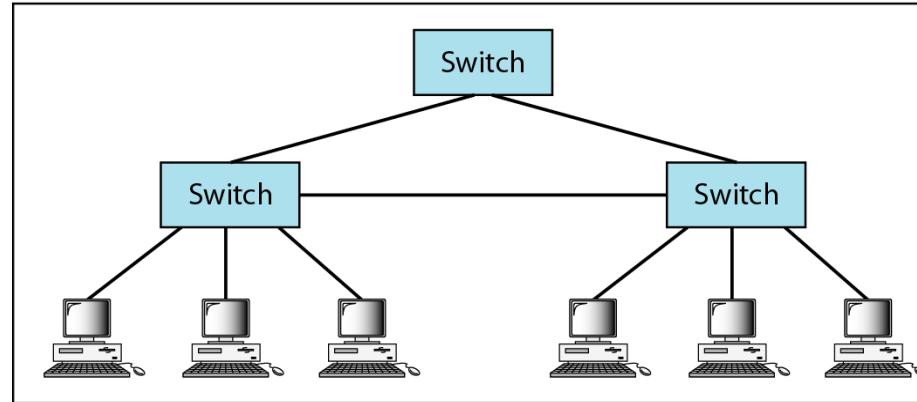
a. Point-to-point



b. Star



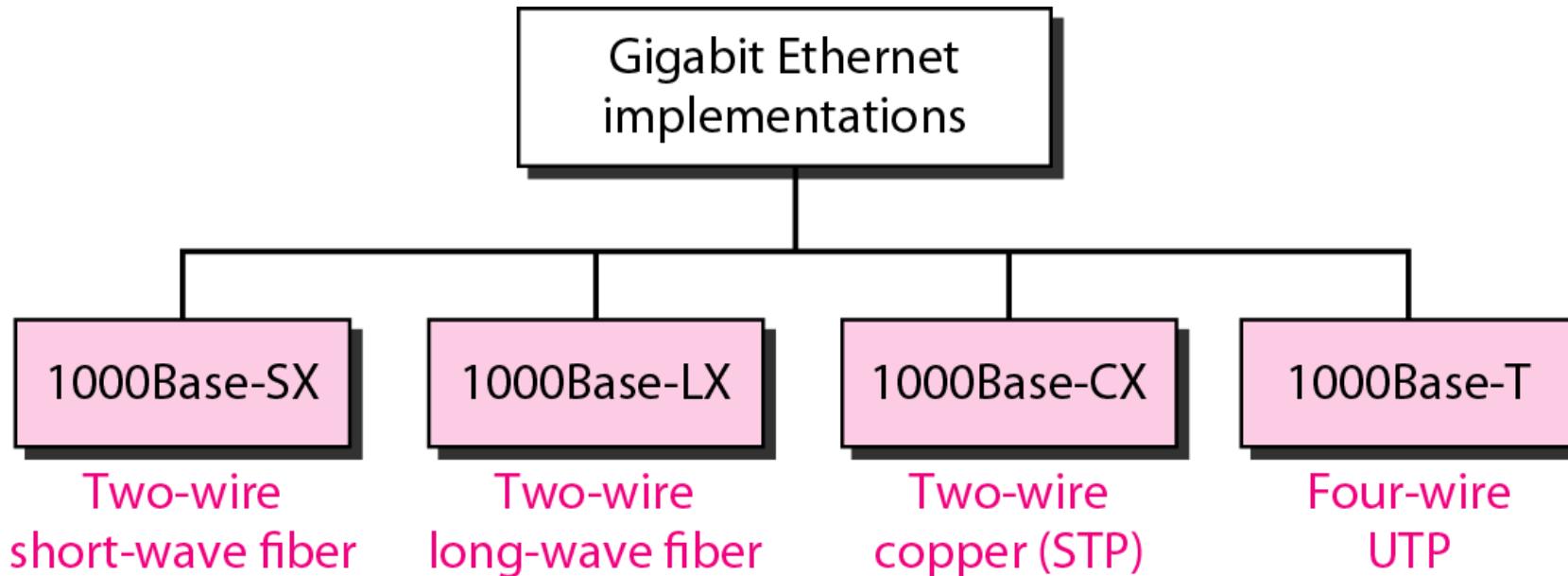
c. Two stars



d. Hierarchy of stars

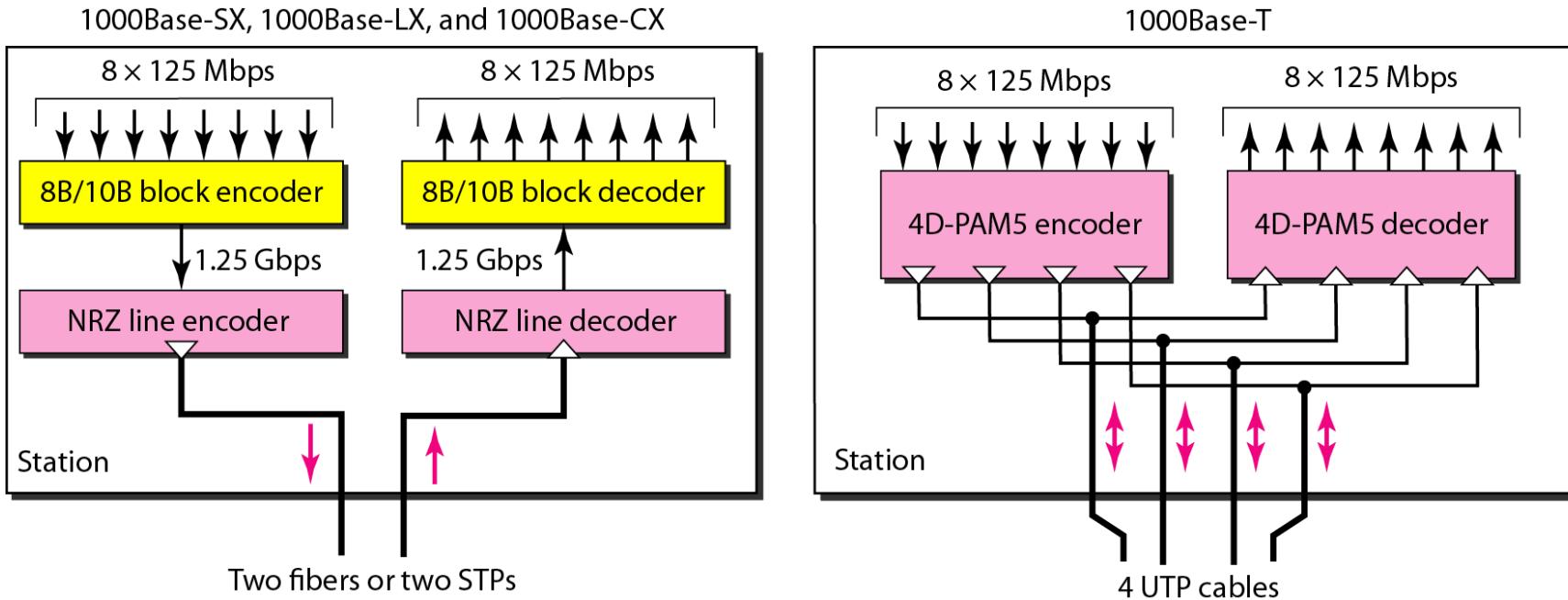
# Gigabit Ethernet ... Contd.

## *Gigabit Ethernet implementations*



# Gigabit Ethernet ... Contd.

## *Encoding in Gigabit Ethernet implementations*



# Gigabit Ethernet ... Contd.

## *Summary of Gigabit Ethernet implementations*

<i>Characteristics</i>	<i>1000Base-SX</i>	<i>1000Base-LX</i>	<i>1000Base-CX</i>	<i>1000Base-T</i>
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m
Block encoding	8B/10B	8B/10B	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

# Ten Gigabit Ethernet

- The IEEE committee created Ten-Gigabit Ethernet and called it Standard 802.3ae.
- The goals of the Ten-Gigabit Ethernet design can be summarized as follows:
  - ✓ Upgrade the data rate to 10 Gbps.
  - ✓ Make it compatible with Standard, Fast, and Gigabit Ethernet.
  - ✓ Use the same 48-bit address.
  - ✓ Use the same frame format.
  - ✓ Keep the same minimum and maximum frame lengths.
  - ✓ Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network (WAN).
  - ✓ Make Ethernet compatible with technologies such as Frame Relay and ATM.

# Ten Gigabit Ethernet ... Contd.

## *Summary of Ten-Gigabit Ethernet implementations*

Characteristics	10GBase-S	10GBase-L	10GBase-E
Media	Short-wave 850-nm multimode	Long-wave 1310-nm single mode	Extended 1550-mm single mode
Maximum length	300 m	10 km	40 km

# Practice Questions

- 1) What is the hexadecimal equivalent of the following Ethernet address?  
01011010 00010001 01010101 00011000 10101010 00001111
  
- 2) How does the Ethernet address 1A:2B:3C:AD:5E:6F appear on the line in binary?
  
- 3) If an Ethernet destination address is 07:01:02:03:04:05, what is the type of the address (unicast, multicast, or broadcast)?
  
- 4) The address 43:7B:6C:DE:10:00 has been shown as the source address in an Ethernet frame. The receiver has discarded the frame. Why?

# Practice Questions ... Contd.

5) You are tasked with designing a wired network for a large university campus that supports a variety of applications, including video conferencing, online learning, and research data transmission. The network must be able to support a large number of users, with varying levels of traffic load and quality-of-service requirements. How would you design the network using different combinations of **IEEE wired standards**? What are the strengths and weaknesses of each approach? Propose a simple topology as well.



# Summary

## Discussed about

- IEEE Standard for LANs
- Standard Ethernet
- Changes in the Standard
- Fast Ethernet
- Gigabit Ethernet
- Ten Gigabit Ethernet
- Practice Questions



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**

# Computer Networks

## BCSE308L

### IEEE 802.11 – Wireless LANs

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai



# Overview

- Architecture of IEEE 802.11
- MAC Sublayer
- Addressing Mechanism
- Physical Layer
- Practice Question
- Summary

# Architecture of IEEE 802.11

- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.
- The standard defines two kinds of services:
  - ✓ Basic Service Set (BSS)
  - ✓ Extended Service Set (ESS)

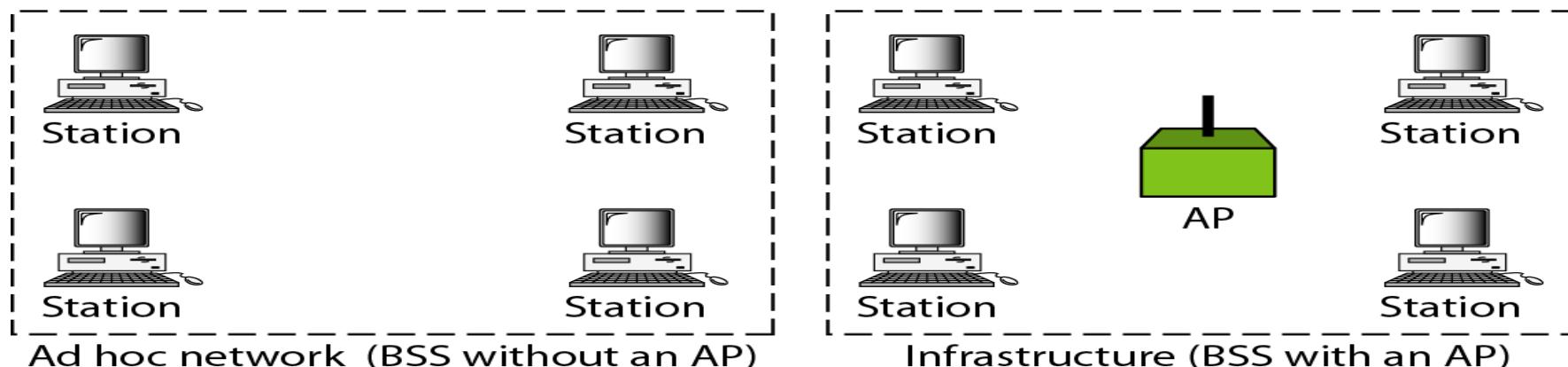
# Architecture of IEEE 802.11 ... Contd.

## Basic Service Set

- IEEE 802.11 defines the Basic Service Set (BSS) as the building block of a wireless LAN.
- A BSS is made of stationary or mobile wireless stations and an optional central base station, known as the Access Point (AP).
- A BSS without an AP is called an **ad hoc** network; a BSS with an AP is called an **infrastructure** network.

**BSS:** Basic service set

**AP:** Access point



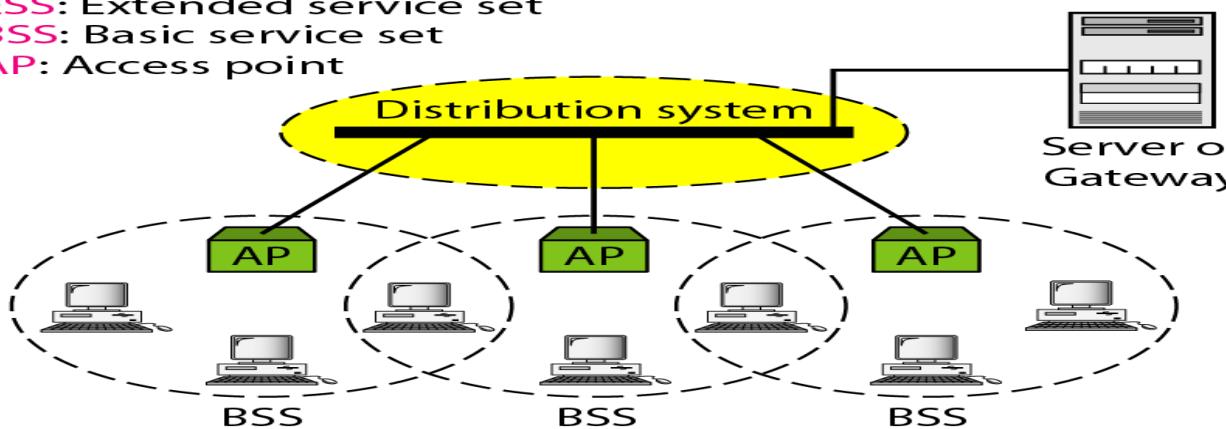
## Extended Service Set

- An Extended Service Set (ESS) is made up of two or more BSSs with APs.
- The BSSs are connected through a distribution system, which is usually a wired LAN.
- The distribution system connects the APs in the BSSs.
- IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet.
- The ESS 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.

ESS: Extended service set

BSS: Basic service set

AP: Access point



- When BSSs are connected, the stations within reach of one another can communicate without the use of an AP.
- Communication between two stations in two different BSSs usually occurs via two APs.
- The idea is similar to communication in a cellular network if we consider each BSS to be a cell and each AP to be a base station. Note that a mobile station can belong to more than one BSS at the same time.

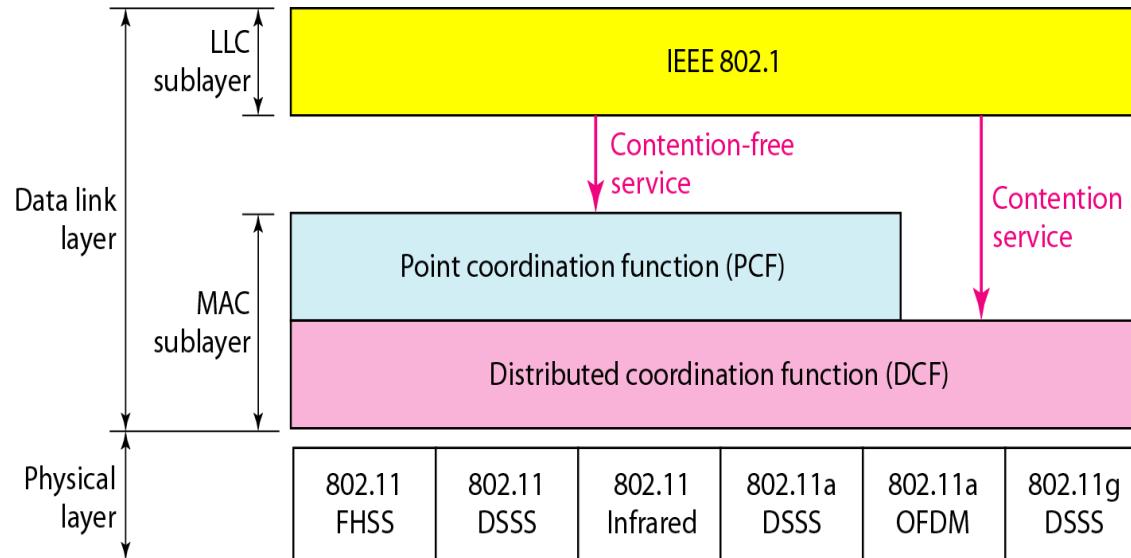


## Station Types

- IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN: **no-transition**, **BSS** transition, and **ESS-transition mobility**.
- A station with **no-transition** mobility is either stationary (not moving) or moving only **inside a BSS**.
- A station with **BSS-transition** mobility can move from one BSS to another, but the **movement is confined inside one ESS**.
- A station with **ESS-transition** mobility can move from one ESS to another.
  - IEEE 802.11 **does not** guarantee that communication is continuous during the move.

# MAC Sublayer

## MAC layers in IEEE 802.11 standard

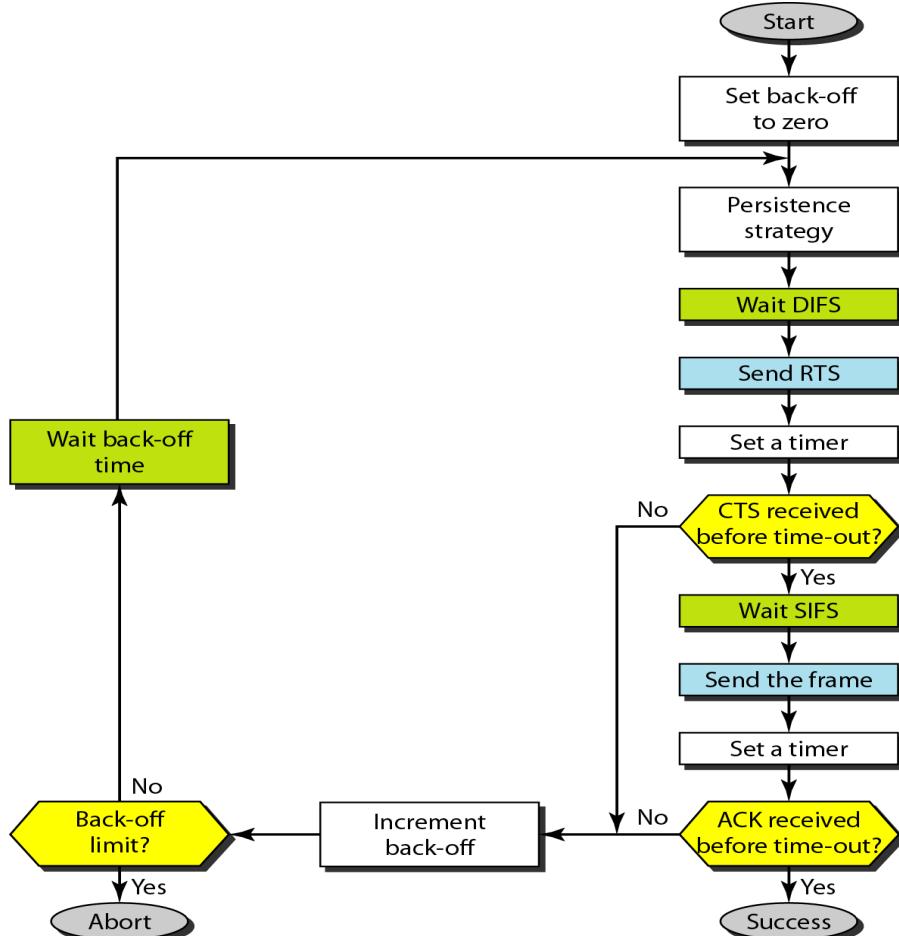


### Distributed Coordination Function

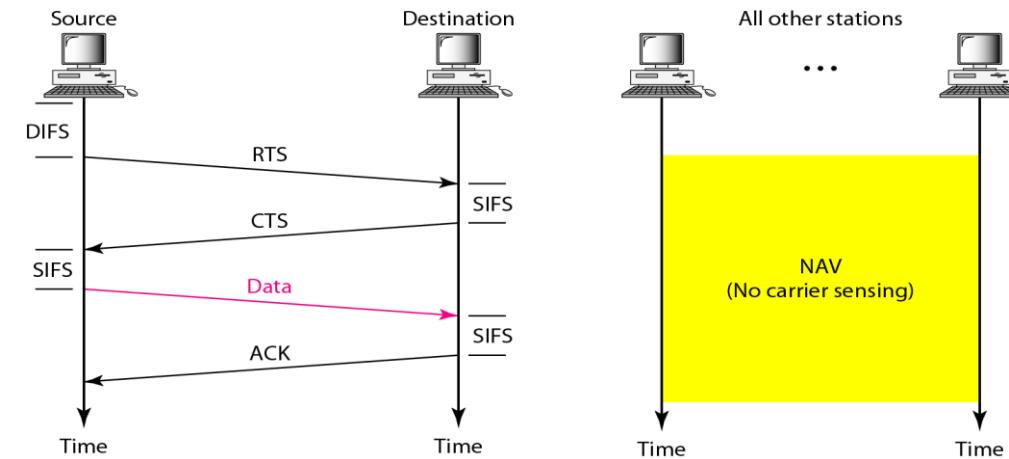
- One of the two protocols defined by IEEE at the MAC sublayer is called the distributed coordination function (DCF).
- DCF uses CSMA/CA as the access method.
- Wireless LANs cannot implement CSMA/CD for three reasons:
  - For collision detection a station must be able to send data and receive collision signals at the same time. This can mean costly stations and increased bandwidth requirements.
  - Collision may not be detected because of the hidden station problem.
  - The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.

# MAC Sublayer ... Contd.

*CSMA/CA used in Wireless LANs*



*Frame Exchange Time Line*



**DIFS:** Distributed Interframe Space

**SIFS:** Short Interframe Space

**RTS:** Request to Send

**CTS:** Clear to Send

**NAV:** Network Allocation Vector

# MAC Sublayer ... Contd.

## *CSMA/CA used in Wireless LANs ... Contd.*

- Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
  - ✓ The channel uses a persistence strategy with back-off until the channel is idle.
  - ✓ After the station is found to be idle, the station waits for a period of time called the distributed interframe space (DIFS); then the station sends a control frame called the request to send (RTS).
- After receiving the RTS and waiting a period of time called the short interframe space (SIFS), the destination station sends a control frame, called the clear to send (CTS), to the source station.
  - ✓ This control frame indicates that the destination station is ready to receive data.
- The source station sends data after waiting an amount of time equal to SIFS.
- The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received.
  - ✓ Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination.
  - ✓ On the other hand, the lack of collision in CSMA/CD is a kind of indication to the source that data have arrived.

# MAC Sublayer ... Contd.

## Network Allocation Vector (NAV)

- How do other stations defer sending their data if one station acquires access?
- How is the collision avoidance aspect of this protocol accomplished?
  - ✓ The key is a feature called NAV.
- When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel.
- The stations that are affected by this transmission create a timer called a NAV that shows how much time must pass before these stations are allowed to check the channel for idleness.
- Each time a station accesses the system and sends an RTS frame, other stations start their NAV.
- Each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired.



# MAC Sublayer ... Contd.

## Collision During Handshaking

- What happens if there is collision during the time when RTS or CTS control frames are in transition, often called the handshaking period?
- Two or more stations may try to send RTS frames at the same time.
- These control frames may collide.
- There is no mechanism for collision detection, the sender assumes there has been a collision if it has not received a CTS frame from the receiver.
- The back-off strategy is employed, and the sender tries again.

# MAC Sublayer ... Contd.

## Point Coordination Function (PCF)

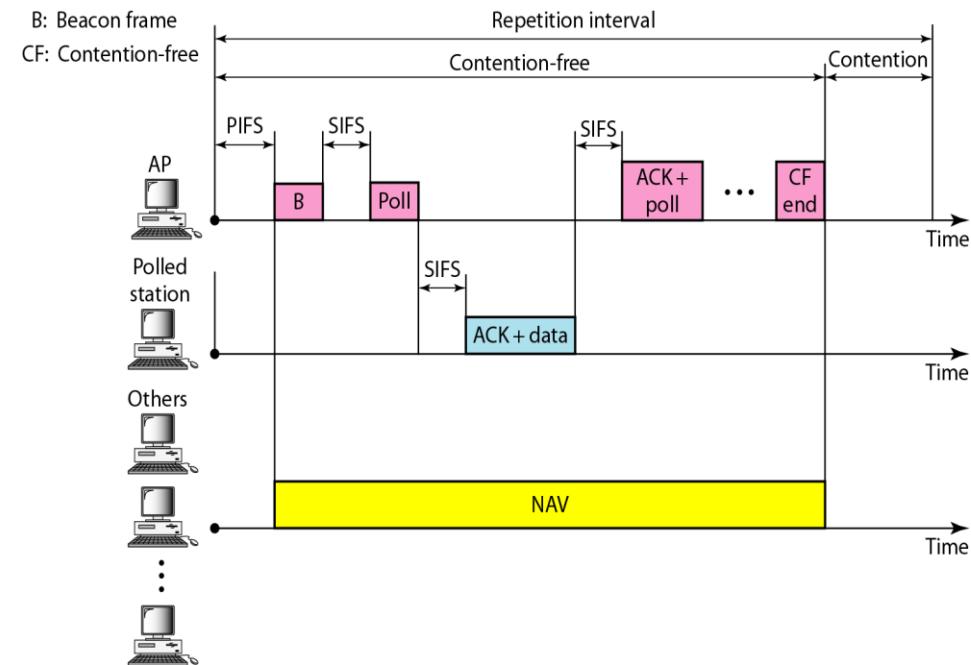
- The PCF is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network).
- It is implemented on top of the DCF and is used mostly for time-sensitive transmission.
- PCF has a centralized, contention-free polling access method.
- The AP performs polling for stations that are capable of being polled.
- The stations are polled one after another, sending any data they have to the AP.
- To give priority to PCF over DCF, another set of interframe spaces has been defined: PIFS and SIFS.
- The SIFS is the same as that in DCF, but the PIFS (PCF IFS) is shorter than the DIFS. This means that if, at the same time, a station wants to use only DCF and an AP wants to use PCF, the AP has priority.

# MAC Sublayer ... Contd.

## Point Coordination Function (PCF) ... Contd.

- Due to the priority of PCF over DCF, stations that only use DCF may not gain access to the medium.
- To prevent this, a repetition interval has been designed to cover both contention-free (PCF) and contention-based (DCF) traffic.
- The repetition interval, which is repeated continuously, starts with a special control frame, called a beacon frame.
- When the stations hear the beacon frame, they start their NAV for the duration of the contention-free period of the repetition interval.

*Example of repetition interval*





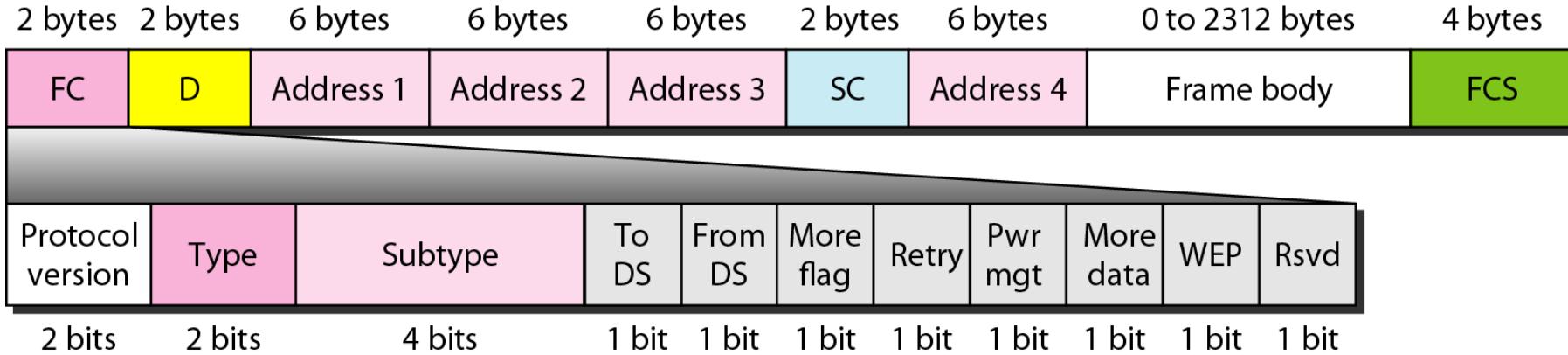
# MAC Sublayer ... Contd.

## Fragmentation

- The wireless environment is very noisy; a corrupt frame has to be retransmitted.
- The protocol, therefore, recommends fragmentation-the division of a large frame into smaller ones.
- It is more efficient to resend a small frame than a large one.

# MAC Sublayer ... Contd.

## MAC Layer Frame format



FC: Frame Control

D: Duration of transmission

SC: Sequence Control

FCS: CRC-32 error detection sequence

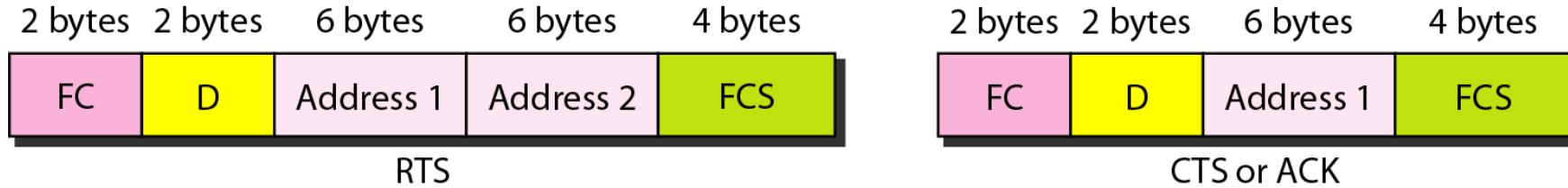
# MAC Sublayer ... Contd.

## *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

# MAC Sublayer ... Contd.

## Control frames



## Values of subfields in control frames

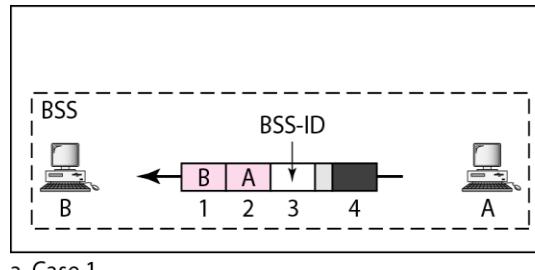
Subtype	Meaning
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

## Addresses

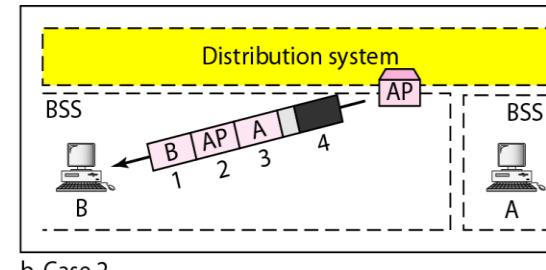
To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

# Addressing Mechanism

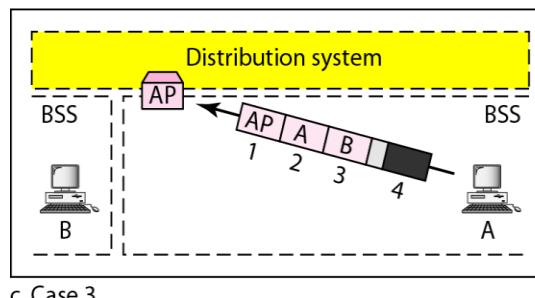
- The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, To DS and From DS.
- Each flag can be either 0 or I, resulting in four different situations.
- The interpretation of the four addresses (address 1 to address 4) in the MAC frame depends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



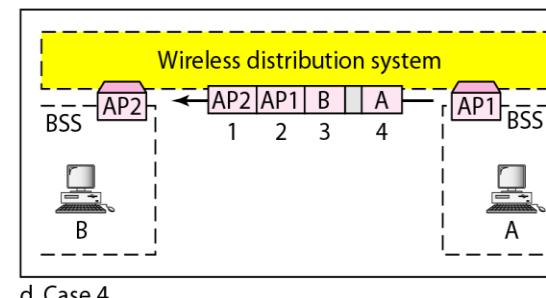
a. Case 1



b. Case 2



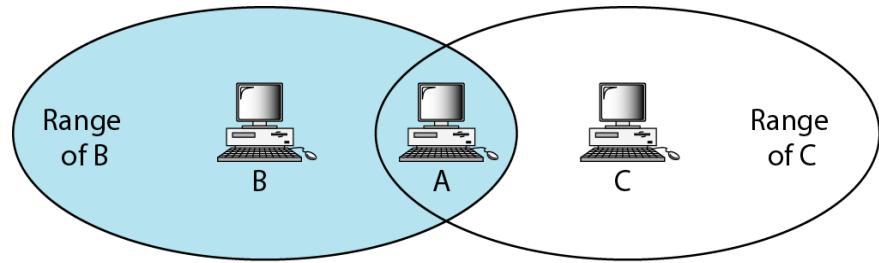
c. Case 3



d. Case 4

- Address 1 is always the address of the next device.
- Address 2 is always the address of the previous device.
- Address 3 is the address of the final destination station if it is not defined by address 1.
- Address 4 is the address of the original source station if it is not the same as address 2.

## Hidden station problem



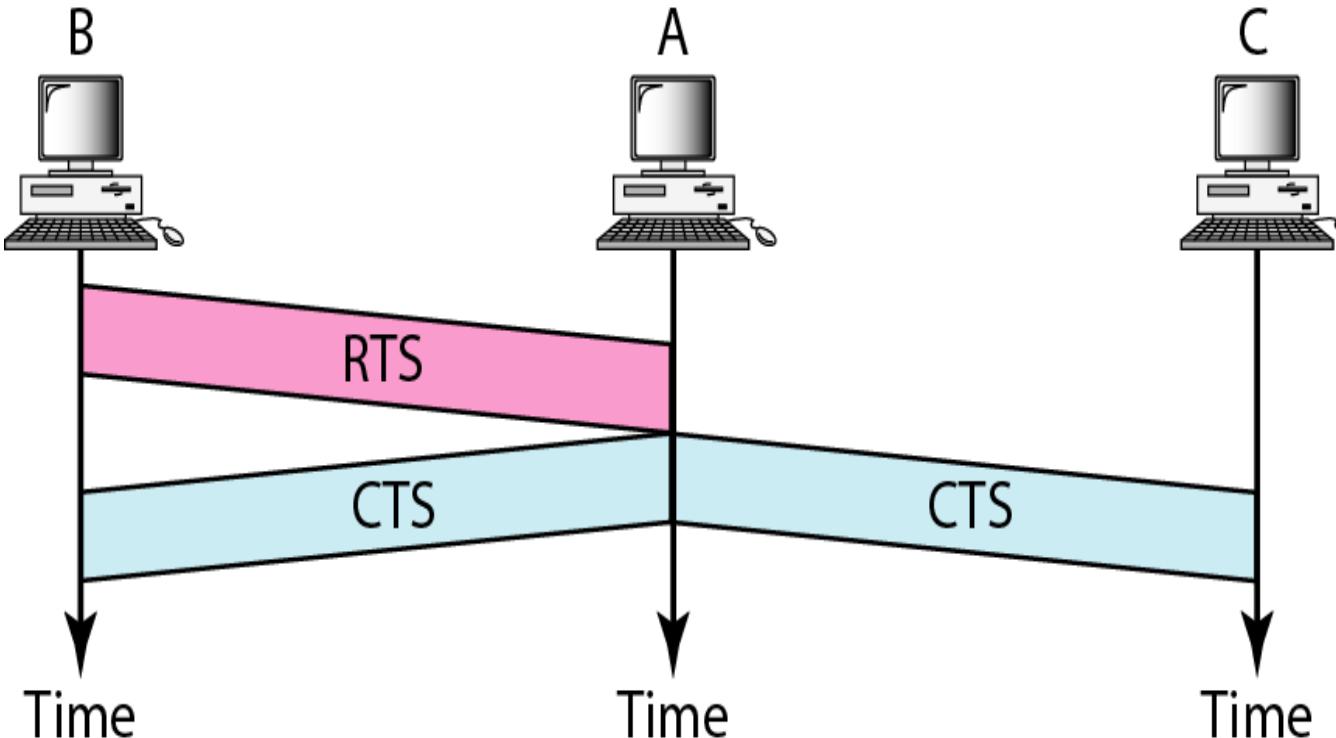
- The CTS frame in CSMA/CA handshake can prevent collision from a hidden station.

# Addressing Mechanism ... Contd.

- Station B has a transmission range shown by the left oval; every station in this range can hear any signal transmitted by station B.
- Station C has a transmission range shown by the right oval; every station located in this range can hear any signal transmitted by C.
- Station C is outside the transmission range of B; likewise, station B is outside the transmission range of C.
- Station A, however, is in the area covered by both B and C; it can hear any signal transmitted by B or C.
- Assume that station B is sending data to station A.
- In the middle of this transmission, station C also has data to send to station A.
- Station C is out of B's range and transmissions from B cannot reach C.
- C thinks the medium is free. Station C sends its data to A, which results in a collision at A because this station is receiving data from both B and C.
- In this case, stations B and C are hidden from each other with respect to A.
- Hidden stations can reduce the capacity of the network because of the possibility of collision.

# Addressing Mechanism ... Contd.

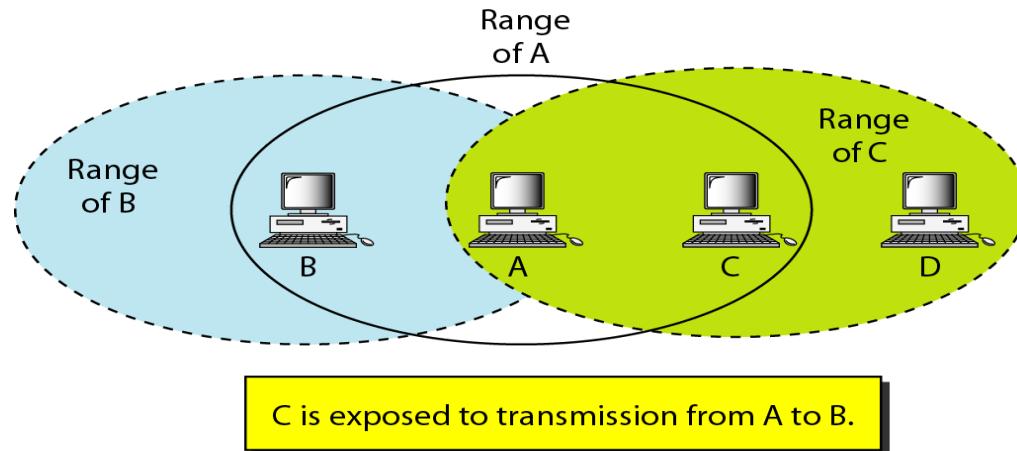
*Use of handshaking to prevent hidden station problem*



- The solution to the hidden station problem is the use of handshake frames (RTS and CTS).
- RTS message from B reaches A, but not C.
- Because both B and C are within the range of A, the CTS message, which contains the duration of data transmission from B to A reaches C.
- Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

# Addressing Mechanism ... Contd.

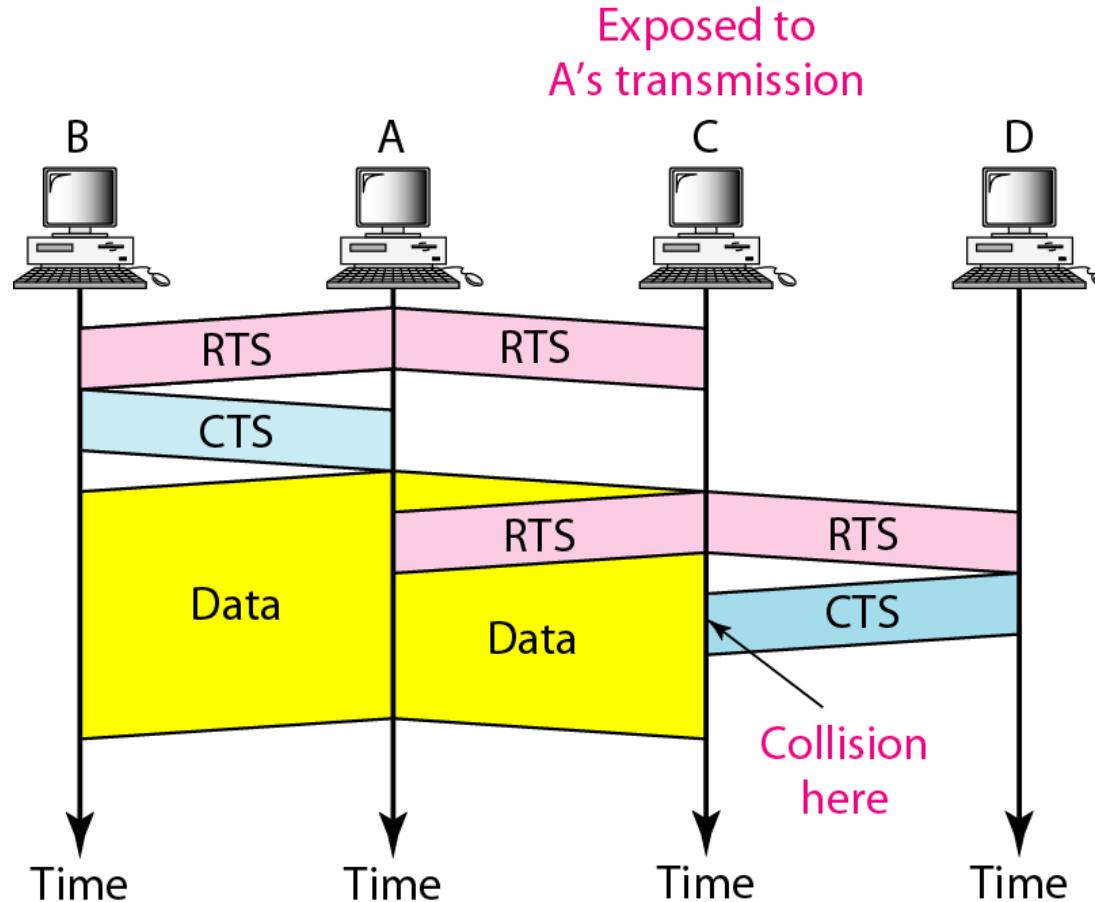
## Exposed station problem



- Consider a situation that is the inverse of the hidden station problem, the exposed station problem.
- A station refrains from using a channel when it is, in fact, available.
- 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.
- Station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending it.
- C is too conservative and wastes the capacity of the channel.

# Addressing Mechanism ... Contd.

*Use of handshaking in exposed station problem*



- The handshaking messages RTS and CTS cannot help in this case.
- Station C hears the RTS from A, but does not hear the CTS from B.
- Station C, after hearing the RTS from A, can wait for a time so that the CTS from B reaches A; it then sends an RTS to D to show that it needs to communicate with D.
- Both stations B and A may hear this RTS, but station A is in the sending state, not the receiving state.
- Station B, however, responds with a CTS.
- The problem is here. If station A has started sending its data, station C cannot hear the CTS from station D because of the collision; it cannot send its data to D.
- It remains exposed until A finishes sending its data.

# Physical Layer

## Addresses

<i>IEEE</i>	<i>Technique</i>	<i>Band</i>	<i>Modulation</i>	<i>Rate (Mbps)</i>
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

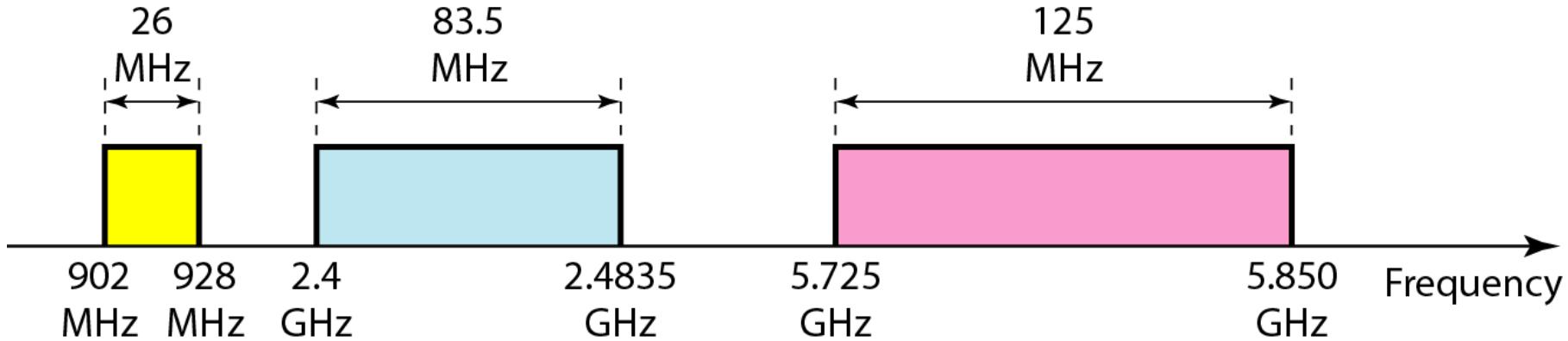
FHSS: Frequency Hopping Spread Spectrum

DSSS: Direct Sequence Spread Spectrum

OFDM: Orthogonal Frequency Division Multiplexing

# Physical Layer... Contd.

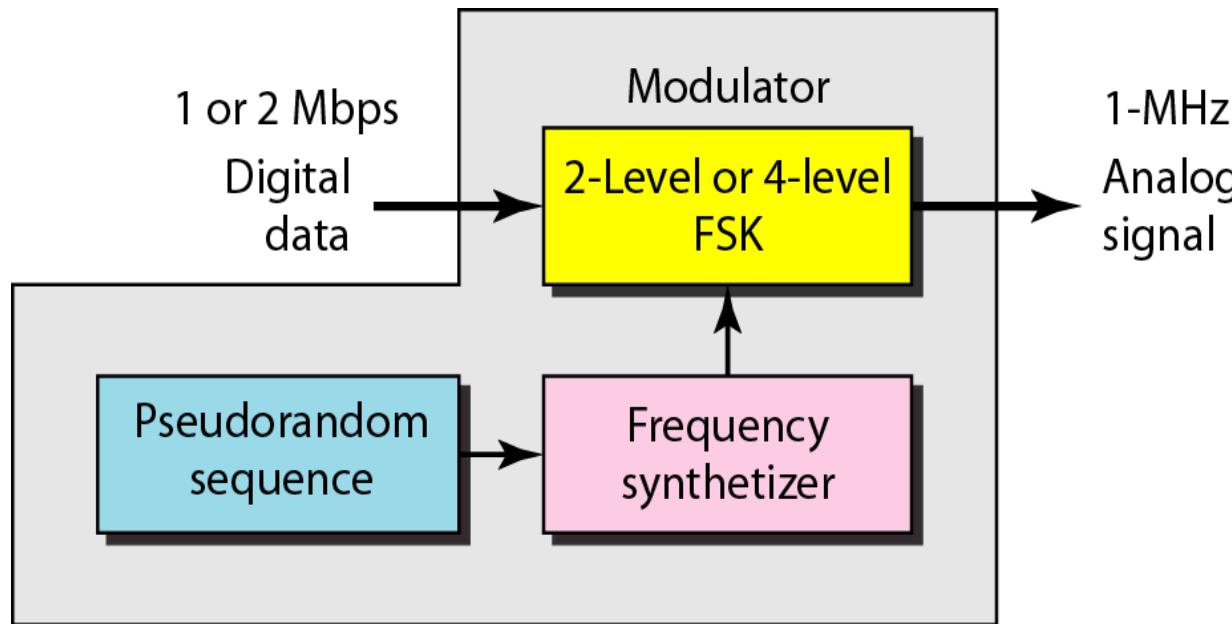
*Industrial, scientific, and medical (ISM) band*



All implementations, except the infrared, operate in the industrial, scientific, and medical (ISM) band, which defines three unlicensed bands in the three ranges 902-928 MHz, 2.400--4.835 GHz, and 5.725-5.850 GHz.

# Physical Layer... Contd.

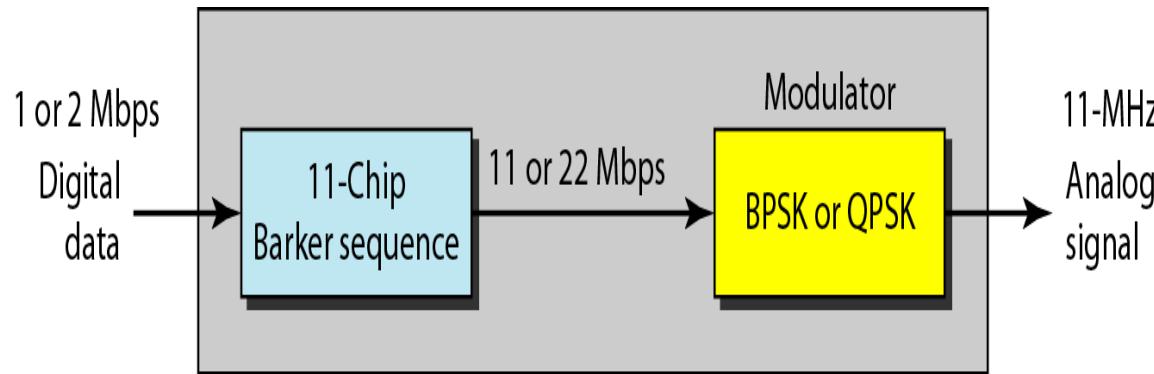
## Physical layer of IEEE 802.11 FHSS



- IEEE 802.11 FHSS uses the frequency-hopping spread spectrum (FHSS) method.
- FHSS uses the 2.4-GHz ISM band. The band is divided into 79 subbands of 1 MHz (and some guard bands).
- A pseudorandom number generator selects the hopping sequence.
- The modulation technique in this specification is either two-level FSK or four-level FSK with 1 or 2 bits/baud, which results in a data rate of 1 or 2 Mbps.

# Physical Layer... Contd.

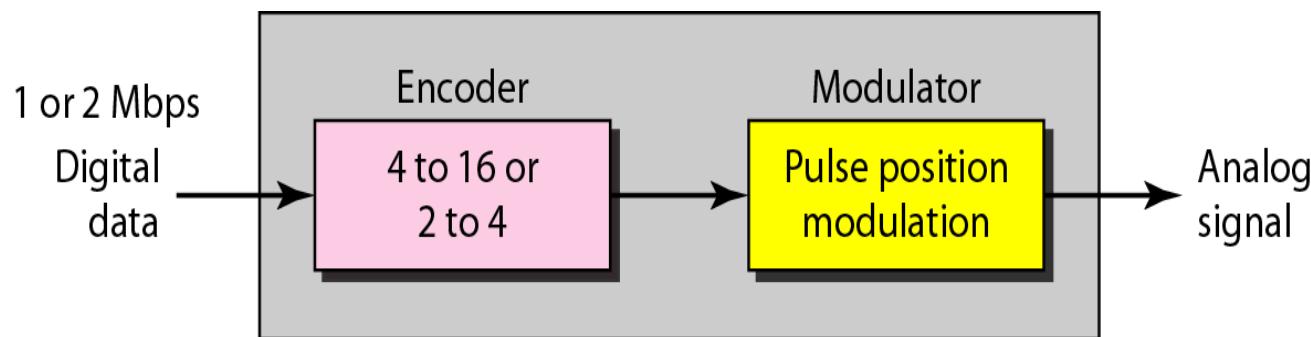
## *Physical layer of IEEE 802.11 DSSS*



- IEEE 802.11 DSSS uses the direct sequence spread spectrum (DSSS) method.
- DSSS uses the 2.4-GHz ISM band. The modulation technique in this specification is PSK at 1Mbaud/s.
- The system allows 1 or 2 bits/baud (BPSK or QPSK), which results in a data rate of 1 or 2 Mbps.

# Physical Layer... Contd.

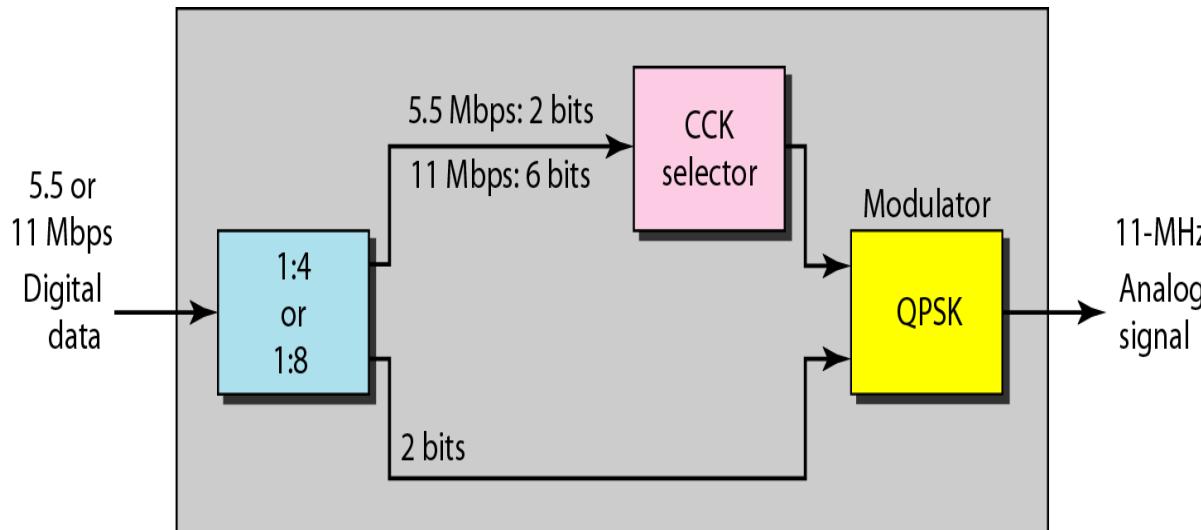
## Physical layer of IEEE 802.11 infrared



- IEEE 802.11 infrared uses infrared light in the range of 800 to 950 nm.
- The modulation technique is called pulse position modulation (PPM).
- For a 1-Mbps data rate, a 4-bit sequence is first mapped into a 16-bit sequence in which only one bit is set to 1 and the rest are set to 0.
- For a 2-Mbps data rate, a 2-bit sequence is first mapped into a 4-bit sequence in which only one bit is set to 1 and the rest are set to 0.
- The mapped sequences are then converted to optical signals; the presence of light specifies 1, the absence of light specifies 0.

# Physical Layer... Contd.

## Physical layer of IEEE 802.11b



- IEEE 802.11 b DSSS describes the high-rate direct sequence spread spectrum (HRDSSS) method for signal generation in the 2.4-GHz ISM band.
- HR-DSSS is similar to DSSS except for the encoding method, which is called complementary code keying (CCK). CCK encodes 4 or 8 bits to one CCK symbol.
- To be backward compatible with DSSS, HR-DSSS defines four data rates: 1,2, 5.5, and 11 Mbps.
- The first two use the same modulation techniques as DSSS. The 5.5-Mbps version uses BPSK and transmits at 1.375 Mbaudls with 4-bit CCK encoding.
- The II-Mbps version uses QPSK and transmits at 1.375 Mbps with 8-bit CCK encoding.



# Practice Question

You are a member of a team tasked with designing a wireless network for a smart city project. The wireless network must provide seamless connectivity for a range of devices, including smart traffic lights, environmental sensors, public safety cameras, and mobile devices. The network must also support emerging technologies such as 5G, IoT, and AI, while ensuring security, reliability, and interoperability across different networks and devices. How can the team leverage IEEE wireless protocols to design a wireless network infrastructure that enables seamless connectivity and interoperability between a wide range of devices and networks, while also addressing the challenges posed by emerging technologies such as 5G, IoT, and AI in a smart city environment?



# Summary

## Discussed about

- Architecture of IEEE 802.11
- MAC Sublayer
- Addressing Mechanism
- Physical Layer
- Practice Question



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**

# Computer Networks

## BCSE308L

## Introduction to Network Layer

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai



# Overview

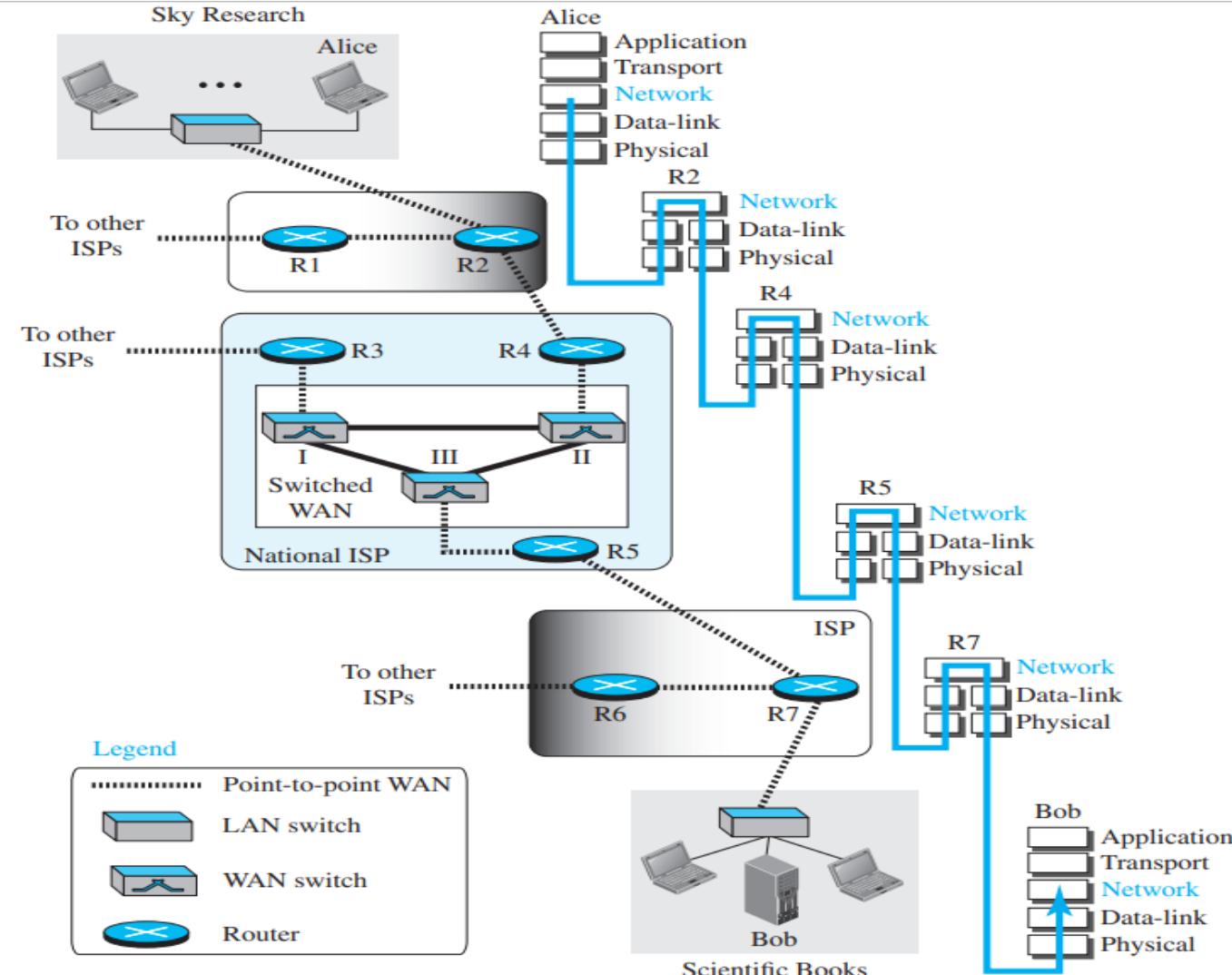
- Introduction to Logical Addressing
- Classful Addressing
- Practice Problems
- Summary



# Introduction to Logical Addressing

- Communication at the network layer is host-to-host (computer-to-computer).
- A computer somewhere in the world needs to communicate with another computer somewhere else in the world.
- Usually, computers communicate through the Internet.
- The packet transmitted by the sending computer may pass through several LANs or WANs before reaching the destination computer.
- For this level of communication, we need a global addressing scheme; we called this logical addressing.

# Introduction to Logical Addressing ... Contd.

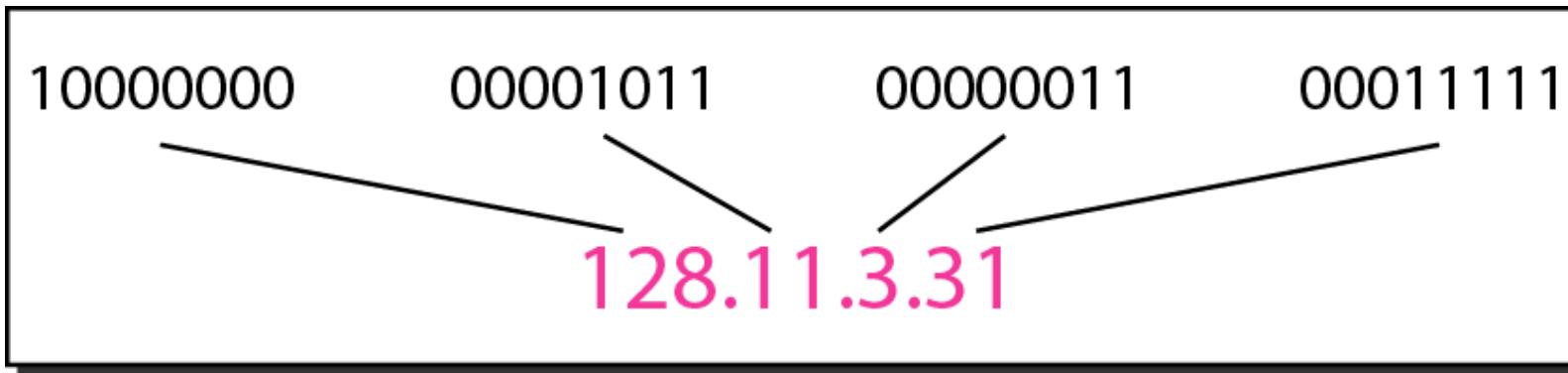




# Introduction to Logical Addressing ... Contd.

- An **IPv4 address** is a **32-bit** address that uniquely and universally defines the connection of a device (a computer or a router) to the Internet.
- IPv4 addresses are unique.
- The IP address is the address of the connection, not the host or the router, because if the device is moved to another network, the IP address may be changed.
- They are unique in the sense that each address defines one, and only one, connection to the Internet.
- Two devices on the Internet can never have the same address at the same time.
- The address space of IPv4 is  $2^{32}$  or 4,294,967,296.

## Dotted-decimal notation and binary notation for an IPv4 address



# Classful Addressing

- In classful addressing, the address space is divided into five classes: A, B, C, D, and E.
- Each class occupies some part of the address space.

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation



# Classful Addressing ... Contd.

- Each class is divided into a fixed number of blocks with each block having a fixed size.
- Number of blocks and block size in classful IPv4 addressing

<i>Class</i>	<i>Number of Blocks</i>	<i>Block Size</i>	<i>Application</i>
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

- Class A addresses were designed for large organizations with a large number of attached hosts or routers.
- Class B addresses were designed for midsize organizations with tens of thousands of attached hosts or routers.
- Class C addresses were designed for small organizations with a small number of attached hosts or routers.
- In classful addressing, a large part of the available addresses were wasted.

# Classful Addressing ... Contd.

## Netid and Hostid

- In classful addressing, an IP address in class A, B, or C is divided into netid and hostid.
- These parts are of varying lengths, depending on the class of the address.

Class	Binary	Dotted-Decimal	CIDR
A	<b>11111111</b> 00000000 00000000 00000000	<b>255</b> .0.0.0	/8
B	<b>11111111</b> <b>11111111</b> 00000000 00000000	<b>255.255</b> .0.0	/16
C	<b>11111111</b> <b>11111111</b> <b>11111111</b> 00000000	<b>255.255.255</b> .0	/24

- The netid is in color, the hostid is in black. Note that the concept does not apply to classes D and E.
- In class A, one byte defines the netid and three bytes define the hostid.
- In class B, two bytes define the netid and two bytes define the hostid.
- In class C, three bytes define the netid and one byte defines the hostid.



# Classful Addressing ... Contd.

## Mask

- The length of the netid and hostid (in bits) is predetermined in classful addressing.
- We can also use a mask (also called the default mask), a 32-bit number made of **contiguous 1s followed by contiguous 0s**.
- The concept does not apply to classes D and E.
- The mask can help us to find the netid and the hostid.
- E.g., the mask for a class A address has eight 1s, which means the first 8 bits of any address in class A define the netid; the next 24 bits define the hostid.
- The last column of the table shows the mask in the form /n where n can be 8, 16, or 24 in classful addressing.
- This notation is also called slash notation or **Classless Interdomain Routing (CIDR)** notation.

# Classful Addressing ... Contd.

## Subnetting

- During the era of classful addressing, subnetting was introduced.
- If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called subnets) or share part of the addresses with neighbors.
- Subnetting increases the number of 1s in the mask.



# Classful Addressing ... Contd.

## Supernetting

- The time came when most of the class A and class B addresses were depleted; however, there was still a huge demand for midsize blocks.
- The size of a class C block with a maximum number of 256 addresses did not satisfy the needs of most organizations.
- Even a midsize organization needed more addresses. One solution was supernetting.
- In supernetting, an organization can combine several class C blocks to create a larger range of addresses.
- Several networks are combined to create a supernet or a supernet.

# Classful Addressing ... Contd.

- An organization can apply for a set of class C blocks instead of just one.
- E.g., an organization that needs 1000 addresses can be granted four contiguous class C blocks.
- The organization can then use these addresses to create one supernet.
- Supernetting decreases the number of 1s in the mask.
- E.g., if an organization is given four class C addresses, the mask changes from /24 to /22.



# Classful Addressing ... Contd.

## Address Depletion

- The flaws in classful addressing scheme combined with the fast growth of the Internet led to the near depletion of the available addresses.
- Yet the number of devices on the Internet is much less than the  $2^{32}$  address space.
- We have run out of class A and B addresses, and a class C block is too small for most midsize organizations.
- Class A - This class can be assigned to only 128 organizations in the world, but each organization needs to have a single network (seen by the rest of the world) with 16,777,216 nodes (computers in this single network).
  - Since there may be only a few organizations that are this large, most of the addresses in this class were wasted (unused).
- Class B - Addresses were designed for midsize organizations, but many of the addresses in this class also remained unused.
- Class C - Addresses have a completely different flaw in design.
  - The number of addresses that can be used in each network (256) was so small that most companies were not comfortable using a block in this address class.
- Class E addresses were almost never used, wasting the whole class.
- One solution that has alleviated the problem is the idea of classless addressing.



# Practice Problems

- 1) Change the following IPv4 addresses from binary notation to dotted-decimal notation.
  - a. 10000001 00001011 00001011 11101111
  - b. 11000001 10000011 00011011 11111111
- 2) Change the following IPv4 addresses from dotted-decimal notation to binary notation.
  - a. 111.56.45.78
  - b. 221.34.7.82
- 3) Find the class of each address.
  - a. 00000001 00001011 00001011 11101111
  - b. 11000001 10000011 00011011 11111111
  - c. 14.23.120.8
  - d. 252.5.15.111



# Practice Problems ... Contd.

4) Find the error, if any, in the following IPv4 addresses.

- a. 111.56.045.78
- b. 221.34.7.8.20
- c. 75.45.301.14
- d. 11100010.23.14.67



# Summary

## Discussed about

- Introduction to Logical Addressing
- Classful Addressing
- Practice Problems



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**

# Computer Networks

## BCSE308L

### Classless Addressing

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai



# Overview

- Introduction
- Address Blocks
- Mask
- Network Addresses
- Hierarchy
- Address Allocation
- Practice Questions
- Summary



# Introduction

- To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented.
- In this scheme, there are no classes, but the addresses are still granted in blocks.



# Address Blocks

- In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses.
- The size of the block (the number of addresses) varies based on the nature and size of the entity.
- An Internet Service Provider (ISP), may be given thousands or hundreds of thousands based on the number of customers it may serve.
- To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:
  1. The addresses in a block must be contiguous, one after another.
  2. The number of addresses in a block must be a power of 2 (1, 2, 4, 8, ... ).
  3. The first address must be evenly divisible by the number of addresses.



# Mask

- A better way to define a block of addresses is to select any address in the block and the mask.
- A mask is a 32-bit number in which the n leftmost bits are 1s and the 32 - n rightmost bits are 0s.
- In classless addressing the mask for a block can take any value from 0 to 32.
- In IPv4 addressing, a block of addresses can be defined as  $x.y.z.t/n$  in which x.y.z.t defines one of the addresses and the /n defines the mask.
- The address and the /n notation completely define the whole block (the first address, the last address, and the number of addresses).
- The first address in the block can be found by setting the 32 - n rightmost bits in the binary notation of the address to 0s.
- The last address in the block can be found by setting the 32 - n rightmost bits in the binary notation of the address to 1s.
- The number of addresses in the block is the difference between the last and first address. It can easily be found using the formula  $2^{32-n}$ .



# Mask ... Contd.

A classless address is given as 167.199.170.82/27. Compute the number of addresses, first address, and last address.



## Mask ... Contd.

A classless address is given as 167.199.170.82/27. Compute the number of addresses, first address, and last address.

The number of addresses in the network is  $2^{32-n} = 2^5 = 32$  addresses.

The first address can be found by keeping the first 27 bits and changing the rest of the bits to 0s.

Address: 167.199.170.82/27	10100111	11000111	10101010	01010010
First address: 167.199.170.64/27	10100111	11000111	10101010	01000000

The last address can be found by keeping the first 27 bits and changing the rest of the bits to 1s.

Address: 167.199.170.82/27	10100111	11000111	10101010	01011111
Last address: 167.199.170.95/27	10100111	11000111	10101010	01011111



# Mask ... Contd.

- Another way to find the first and last addresses in the block is to use the address mask.
- The address mask is a 32-bit number in which the n leftmost bits are set to 1s and the rest of the bits ( $32 - n$ ) are set to 0s.
- A computer can easily find the address mask because it is the complement of  $(2^{32-n} - 1)$ .
- The reason for defining a mask in this way is that it can be used by a computer program to extract the information in a block, using the three bit-wise operations **NOT**, **AND**, and **OR**.
  1. The number of addresses in the block  $N = \text{NOT } (\text{mask}) + 1$ .
  2. The first address in the block = (Any address in the block) **AND** (mask).
  3. The last address in the block = (Any address in the block) **OR** [(**NOT** (mask))].



# Mask ... Contd.

- Classless Address - 167.199.170.82/27
- The mask in dotted-decimal notation is 255.255.255.224.

Number of addresses in the block:  $N = \text{NOT}(\text{mask}) + 1 = 0.0.0.31 + 1 = 32 \text{ addresses}$

First address:  $\text{First} = (\text{address}) \text{ AND } (\text{mask}) = 167.199.170.82$

Last address:  $\text{Last} = (\text{address}) \text{ OR } (\text{NOT mask}) = 167.199.170.255$



# Network Addresses

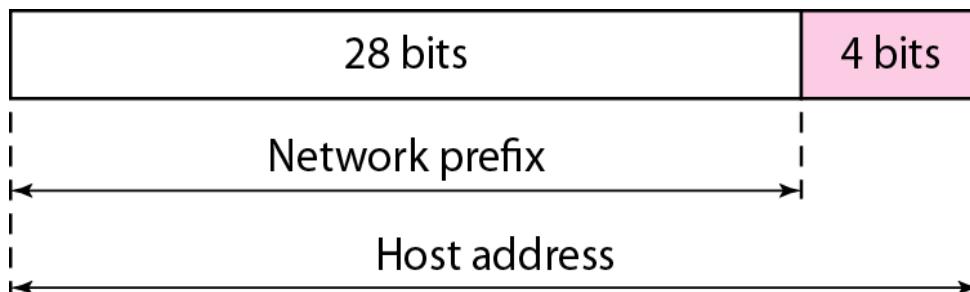
- When an organization is given a block of addresses, the organization is free to allocate the addresses to the devices that need to be connected to the Internet.
- The first address in the class, however, is normally (not always) treated as a special address.
- The first address is called the network address and defines the organization network.
- It defines the organization itself to the rest of the world.

# Hierarchy

- IP addresses, like other addresses or identifiers have levels of hierarchy.

## Two-Level Hierarchy: No Subnetting

- An IP address can define only two levels of hierarchy when not subnetted.
- The  $n$  leftmost bits of the address  $x.y.z.t/n$  define the network (organization network); the  $32 - n$  rightmost bits define the particular host (computer or router) to the network.
- The two common terms are prefix and suffix.
- The part of the address that defines the network is called the prefix; the part that defines the host is called the suffix.



The prefix is common to all addresses in the network; the suffix changes from one device to another.



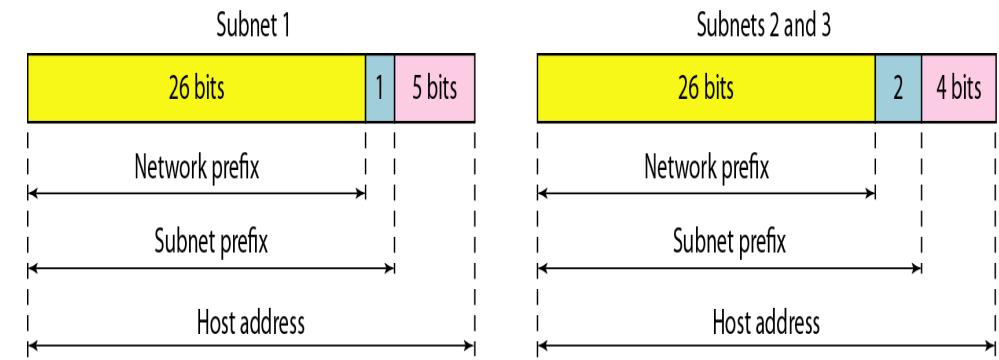
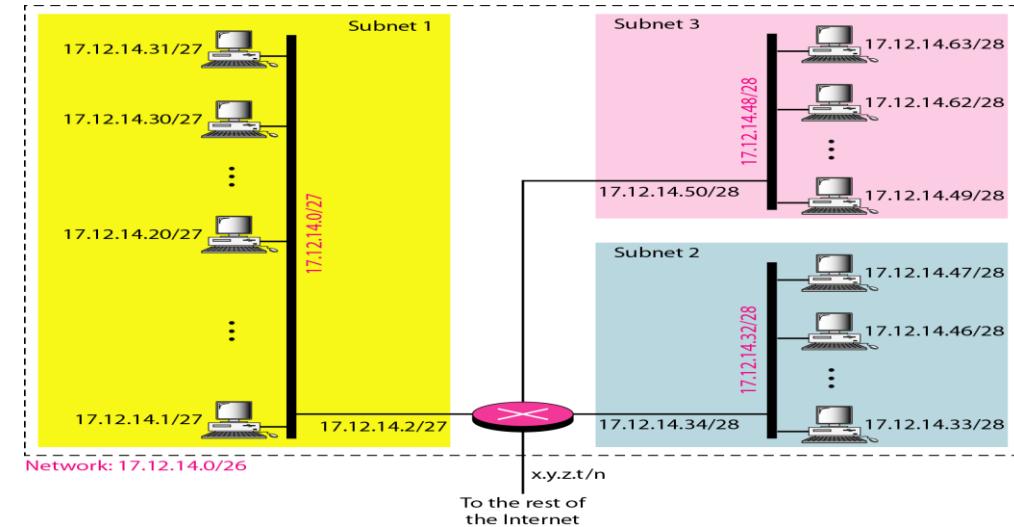
# Hierarchy ... Contd.

## Three-Levels of Hierarchy: Subnetting

- An organization that is granted a large block of addresses may want to create clusters of networks (called subnets) and divide the addresses between the different subnets.
- The rest of the world still sees the organization as one entity; however, internally there are several subnets.
- All messages are sent to the router address that connects the organization to the rest of the Internet; the router routes the message to the appropriate subnets.
- The organization, however, needs to create small subblocks of addresses, each assigned to specific subnets.
- The organization has its own mask; each subnet must also have its own.

# Hierarchy ... Contd.

- Suppose an organization is given the block 17.12.14.0/26, which contains 64 addresses.
- The organization has three offices and needs to divide the addresses into three subblocks of 32, 16, and 16 addresses.
- We can find the new masks by using the following arguments:
  - Suppose the mask for the first subnet is  $n_1$ , then  $2^{32-n_1}$  must be 32, which means that  $n_1 = 27$  [32-log<sub>2</sub>32].
  - Suppose the mask for the second subnet is  $n_2$ , then  $2^{32-n_2}$  must be 16, which means that  $n_2 = 28$  [32-log<sub>2</sub>16].
  - Suppose the mask for the third subnet is  $n_3$ , then  $2^{32-n_3}$  must be 16, which means that  $n_3 = 28$ .
- This means that we have the masks 27, 28, 28 with the organization mask being 26.





# Hierarchy ... Contd.

## More Levels of Hierarchy

- The structure of classless addressing does not restrict the number of hierarchical levels.
- An organization can divide the granted block of addresses into subblocks.
- Each subblock can in turn be divided into smaller subblocks.
- E.g., A national ISP can divide a granted large block into smaller blocks and assign each of them to a regional ISP.
  - A regional ISP can divide the block received from the national ISP into smaller blocks and assign each one to a local ISP.
  - A local ISP can divide the block received from the regional ISP into smaller blocks and assign each one to a different organization.
  - Finally, an organization can divide the received block and make several subnets out of it.



# Address Allocation

## How are the blocks allocated?

- The ultimate responsibility of address allocation is given to a global authority called the **Internet Corporation for Assigned Names and Addresses (ICANN)**.
- ICANN does not normally allocate addresses to individual organizations.
- It assigns a large block of addresses to an ISP.
- Each ISP, in turn, divides its assigned block into smaller subblocks and grants the subblocks to its customers.
- An ISP receives one large block to be distributed to its Internet users.
- This is called **address aggregation**: many blocks of addresses are aggregated in one block and granted to one ISP.



# Practice Problems

- 1) A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.39/28. What is the first address in the block? What is the last address of the block? Find the number of addresses.
- 2) An organization is granted a block of addresses with the beginning address 14.24.74.0/24. The organization needs to have 3 subblocks of addresses to use in its three subnets: one subblock of 10 addresses, one subblock of 60 addresses, and one subblock of 120 addresses. Design the subblocks.
- 3) An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows:
  - a. The first group has 64 customers; each needs 256 addresses.
  - b. The second group has 128 customers; each needs 128 addresses.
  - c. The third group has 128 customers; each needs 64 addresses.

Design the subblocks and find out how many addresses are still available after these allocations.



# Summary

## Discussed about

- Introduction
- Address Blocks
- Mask
- Network Addresses
- Hierarchy
- Address Allocation
- Practice Problems



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**

# Computer Networks

## BCSE308L

### Internet Protocol

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai

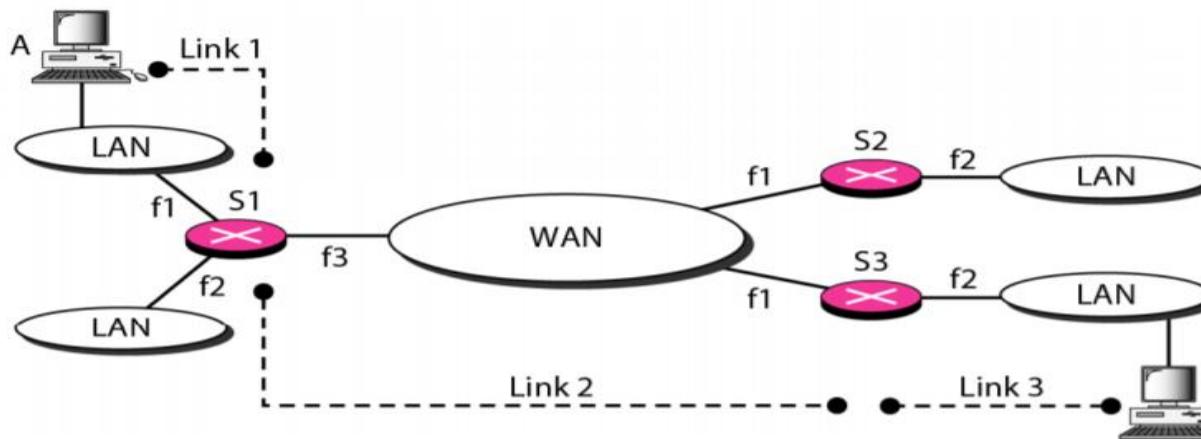


# Overview

- Introduction
- Internet as a Datagram Network
- Internet as a Connectionless Network
- IPv4
- Datagram
- Practice Questions
- Summary

# Introduction

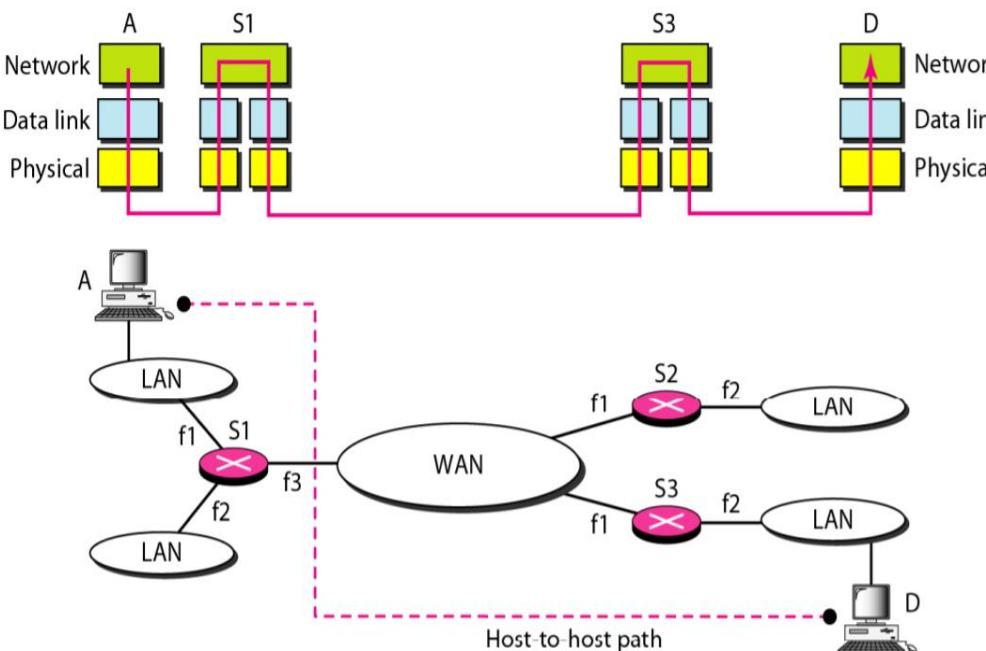
- The physical and data link layers of a network operate locally.
- These two layers are jointly responsible for data delivery on the network from one node to the next.



# Introduction ... Contd.

## Need for Network Layer

- To solve the problem of delivery through several links, the network layer was designed.
- The network layer is responsible for host-to-host delivery and for routing the packets through the routers or switches.



- The network layer at the switch or router is responsible for routing the packet.
- When a packet arrives, the router or switch consults its routing table and finds the interface from which the packet must be sent.
- The packet, after some changes in the header, with the routing information is passed to the data link layer again.
- The network layer at the destination is responsible for address verification; it makes sure that the destination address on the packet is the same as the address of the host.
- If the packet is a fragment, the network layer waits until all fragments have arrived, and then reassembles them and delivers the reassembled packet to the transport layer.



# Internet as a Datagram Network

- The Internet, at the network layer, is a packet-switched network.
- In general, switching can be divided into three broad categories: circuit switching, packet switching, and message switching.
- Packet switching uses either the virtual circuit approach or the datagram approach.
- The Internet has chosen the datagram approach to switching in the network layer.
- It uses the universal addresses defined in the network layer to route packets from the source to the destination.
- **Switching at the network layer in the Internet uses the datagram approach to packet switching.**



# Internet as a Connectionless Network

- Delivery of a packet can be accomplished by using either a connection-oriented or a connectionless network service.
- In a connection-oriented service, the source first makes a connection with the destination before sending a packet.
- When the connection is established, a sequence of packets from the same source to the same destination can be sent one after another.
- In this case, there is a relationship between packets.
- They are sent on the same path in sequential order.
- A packet is logically connected to the packet traveling before it and to the packet traveling after it.
- When all packets of a message have been delivered, the connection is terminated.

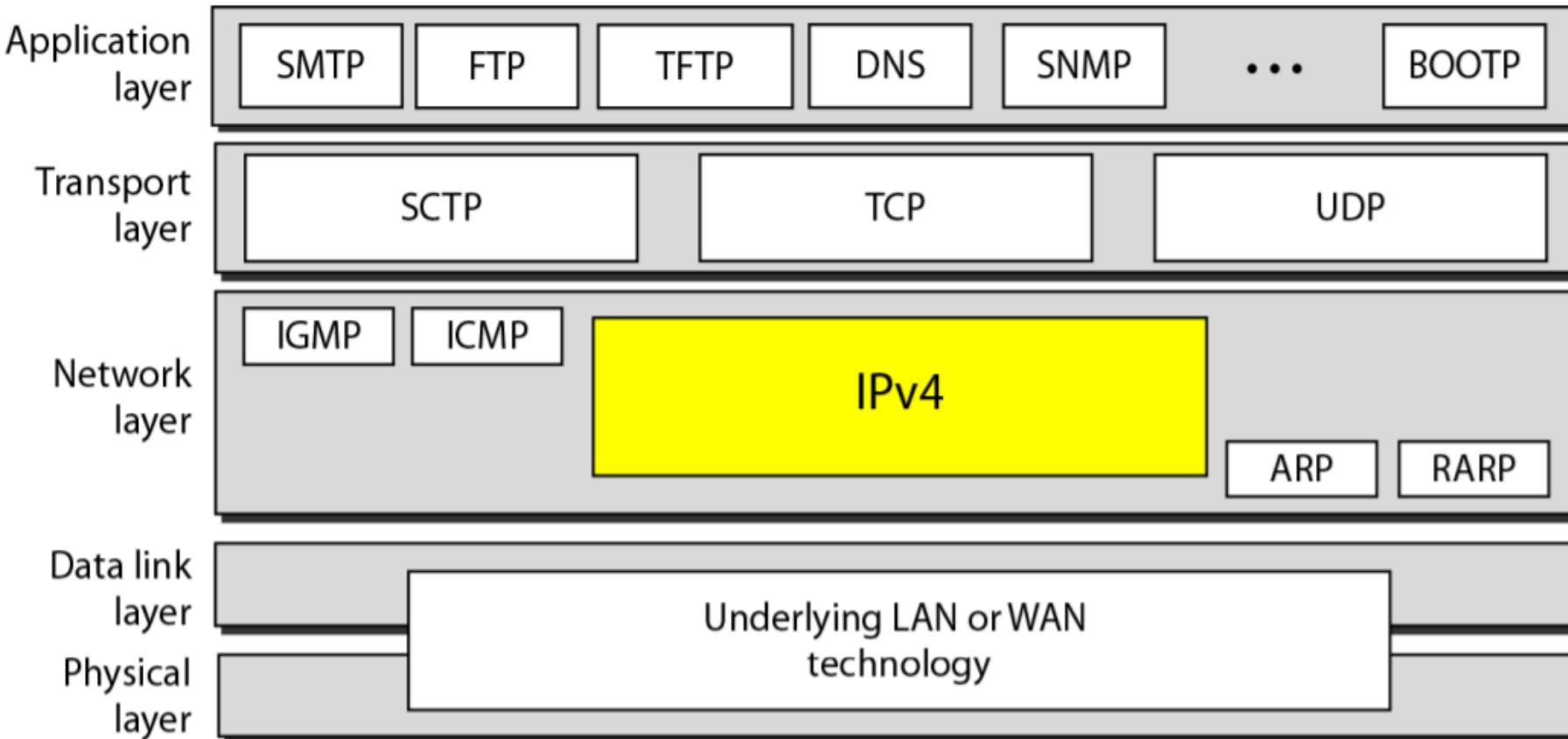


# Internet as a Connectionless Network ... Contd.

- In a **connection-oriented protocol**, the decision about the route of a sequence of packets with the same source and destination addresses can be made only once, when the connection is established.
  - Switches do not recalculate the route for each individual packet.
  - This type of service is used in a virtual-circuit approach to packet switching such as in Frame Relay and ATM.
- In **connectionless service**, the network layer protocol treats each packet independently, with each packet having no relationship to any other packet.
  - The packets in a message may or may not travel the same path to their destination.
  - This type of service is used in the datagram approach to packet switching.
  - The Internet has chosen this type of service at the network layer.
- The reason for this decision is that the Internet is made of so many heterogeneous networks that it is almost impossible to create a connection from the source to the destination without knowing the nature of the networks in advance.

# IPv4

- The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols.





# IPv4 ... Contd.

- IPv4 is an unreliable and connectionless datagram protocol-a best-effort delivery service.
- The term **best-effort** means that IPv4 provides **no error control or flow control** (except for error detection on the header).
- IPv4 assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.
- If reliability is important, IPv4 must be paired with a reliable protocol such as TCP.
- E.g., best-effort delivery service is the post office.
- The post office does its best to deliver the mail but does not always succeed.
- If an unregistered letter is lost, it is up to the sender or would-be recipient to discover the loss and rectify the problem.
- The post office itself does not keep track of every letter and cannot notify a sender of loss or damage.

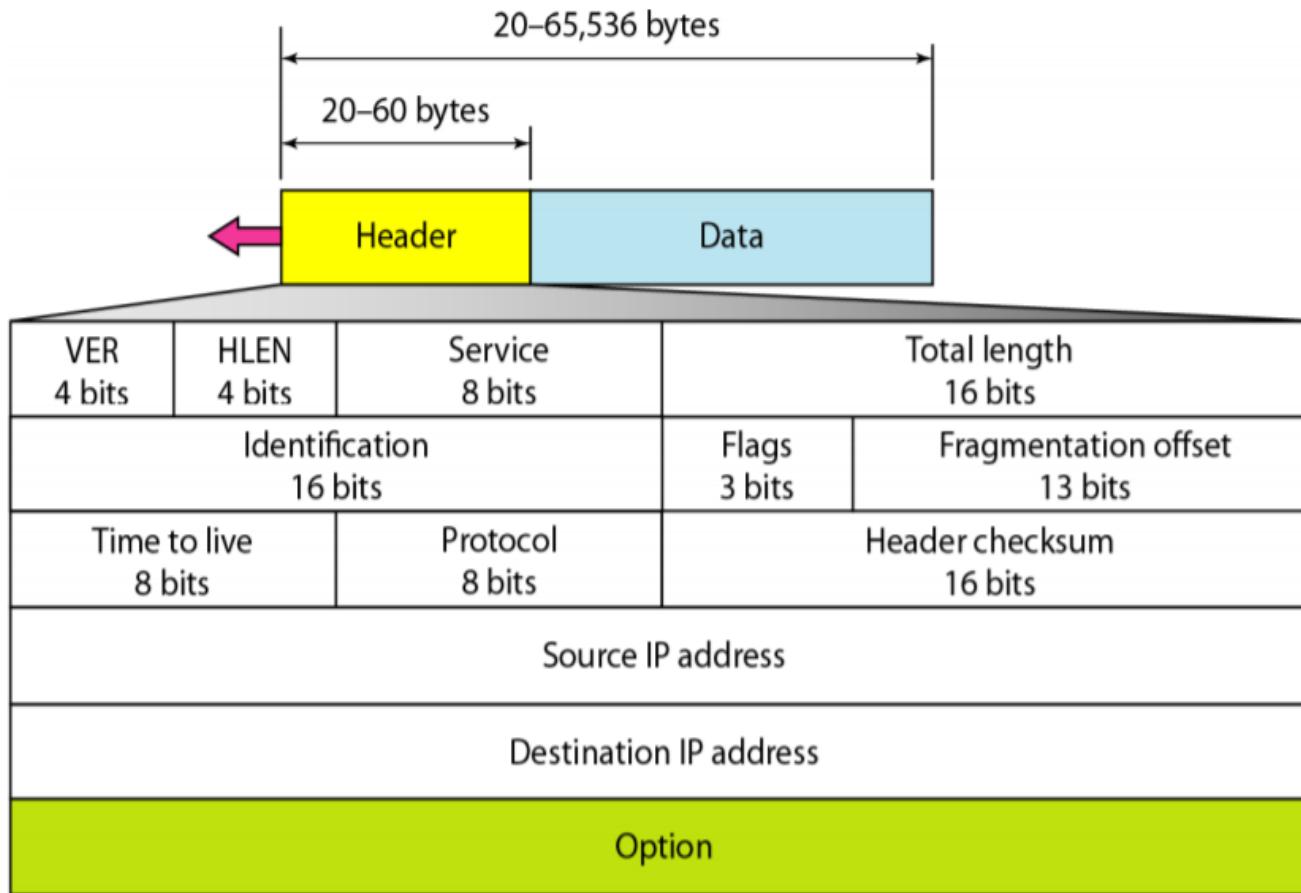


# IPv4 ... Contd.

- IPv4 is also a connectionless protocol for a packet-switching network that uses the datagram approach.
- This means that each datagram is handled independently, and each datagram can follow a different route to the destination.
- Datagrams sent by the same source to the same destination could arrive out of order.
- Some could be lost or corrupted during transmission.
- IPv4 relies on a higher-level protocol to take care of all these problems.

# Datagram

- Packets in the IPv4 layer are called datagrams.



- A datagram is a variable-length packet consisting of two parts: header and data.
- The header is 20 to 60 bytes in length and contains information essential to routing and delivery



# Version

- Version (VER)
- This 4-bit field defines the version of the IPv4 protocol.
- This field tells the IPv4 software running in the processing machine that the datagram has the format of version 4.
- All fields must be interpreted as specified in the fourth version of the protocol.
- If the machine is using some other version of IPv4, the datagram is discarded rather than interpreted incorrectly.

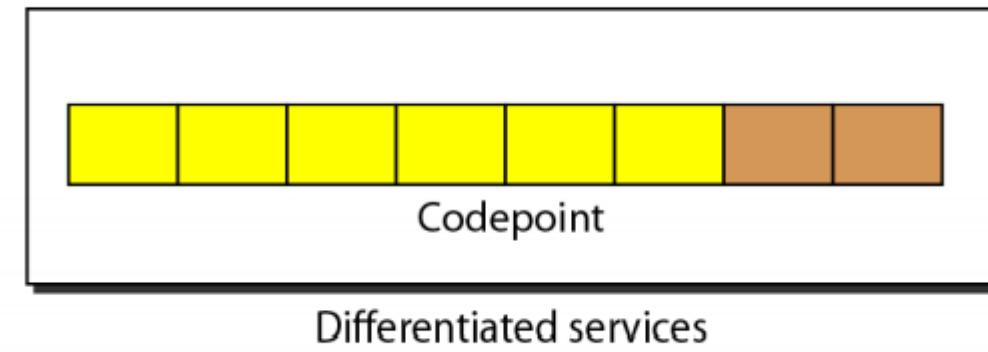
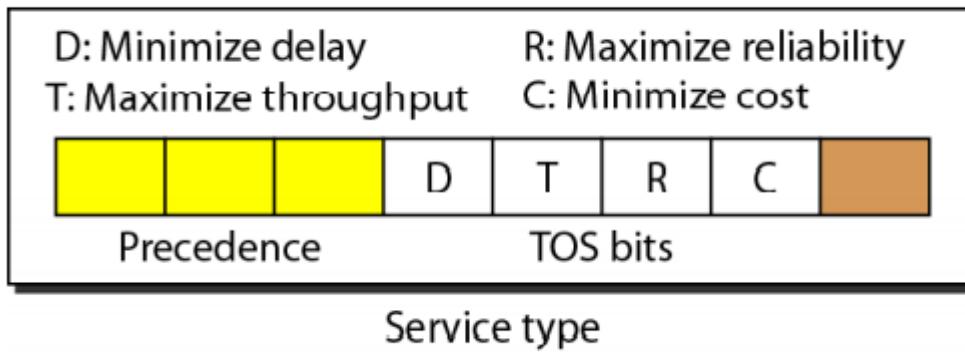


# Header Length

- Header length (**HLEN**)
- This 4-bit field defines the total length of the datagram header in 4-byte words.
- This field is needed because the length of the header is variable (between 20 and 60 bytes).
- When there are no options, the header length is 20 bytes, and the value of this field is 5.
  - $(5 \times 4 = 20)$
- When the option field is at its maximum size, the value of this field is 15.
  - $(15 \times 4 = 60)$

# Services

- IETF has changed the interpretation and name of this 8-bit field.
- This field, previously called service type, is now called differentiated services.





# Services ... Contd.

## Service Type

- In this interpretation, the first 3 bits are called precedence bits.
- The next 4 bits are called type of service (TOS) bits, and the last bit is not used.
- **Precedence** is a 3-bit subfield ranging from 0 (000 in binary) to 7 (111 in binary).
  - The precedence defines the priority of the datagram in issues such as congestion.
  - If a router is congested and needs to discard some datagrams, those datagrams with lowest precedence are discarded first.
  - Some datagrams in the Internet are more important than others.
  - E.g., a datagram used for network management is much more urgent and important than a datagram containing optional information for a group.



## Services ... Contd.

- **TOS** bits is a 4-bit subfield with each bit having a special meaning.
  - Although a bit can be either 0 or 1, one and only one of the bits can have the value of 1 in each datagram.
  - With only 1 bit set at a time, we can have five different types of services.

<i>TOS Bits</i>	<i>Description</i>
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

# Services ... Contd.

Protocol	TOS Bits	Description
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

- Application programs can request a specific type of service.
- The interactive activities, activities requiring immediate attention, and activities requiring immediate response need minimum delay.
- Those activities that send bulk data require maximum throughput.
- Management activities need maximum reliability.
- Background activities need minimum cost.



## Services ... Contd.

### Differentiated Services

- In this interpretation, the first 6 bits make up the codepoint subfield, and the last 2 bits are not used.
- The **codepoint** subfield can be used in two different ways:
  - a. When the 3 rightmost bits are 0s, the 3 leftmost bits are interpreted the same as the precedence bits in the service type interpretation.
    - In other words, it is compatible with the old interpretation.
  - b. When the 3 rightmost bits are not all 0s, the 6 bits define 64 services based on the priority assignment by the Internet or local authorities

<i>Category</i>	<i>Codepoint</i>	<i>Assigning Authority</i>
1	XXXXX0	Internet
2	XXXX11	Local
3	XXXX01	Temporary or experimental



# Total Length

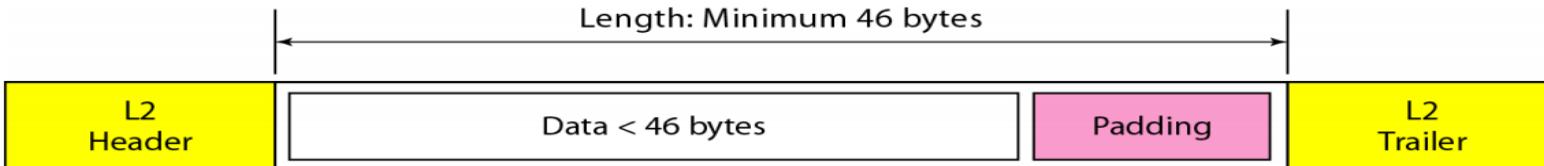
- This is a 16-bit field that defines the total length (header plus data) of the IPv4 datagram in bytes.
- To find the length of the data coming from the upper layer, subtract the header length from the total length.
- The header length can be found by multiplying the value in the HLEN field by 4.

**Length of data = total length - header length**

- Since the field length is 16 bits, the total length of the IPv4 datagram is limited to 65,535 ( $2^{16} - 1$ ) bytes, of which 20 to 60 bytes are the header and the rest is data from the upper layer.

## Need for total length field

- When a machine (router or host) receives a frame, it drops the header and the trailer, leaving the datagram.
- Why include an extra field that is not needed?
  - The answer is that in many cases we really do not need the value in this field.
  - There are occasions in which the IPv4 datagram is not the only thing encapsulated in a frame; it may be that padding has been added.
  - E.g., the Ethernet protocol has a minimum and maximum restriction on the size of data that can be encapsulated in a frame (46 to 1500 bytes).
  - If the size of an IPv4 datagram is less than 46 bytes, some padding will be added to meet this requirement.
  - In this case, when a machine decapsulates the datagram, it needs to check the total length field to determine how much is really data and how much is padding.





# Identification, Flags, and Fragmentation Offset

- These fields are used in fragmentation.



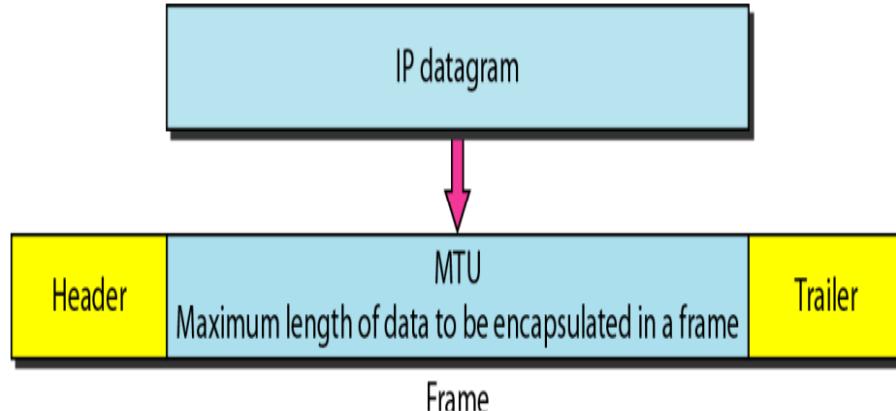
# Fragmentation

- A datagram can travel through different networks.
- Each router decapsulates the IPv4 datagram from the frame it receives, processes it, and then encapsulates it in another frame.
- The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled.
- The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel.
- E.g., if a router connects a LAN to a WAN, it receives a frame in the LAN format and sends a frame in the WAN format.

# Fragmentation ... Contd.

## Maximum Transfer Unit (MTU)

- Each data link layer protocol has its own frame format in most protocols.
- One of the fields defined in the format is the maximum size of the data field.
- When a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size, which is defined by the restrictions imposed by the hardware and software used in the network.
- The value of the MTU depends on the physical network protocol.



Protocol	MTU
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296



# Fragmentation ... Contd.

- To make the IPv4 protocol independent of the physical network, the designers decided to make the maximum length of the IPv4 datagram equal to 65,535 bytes.
- This makes transmission more efficient if we use a protocol with an MTU of this size.
- For other physical networks, we must **divide the datagram to make it possible to pass through these networks. This is called fragmentation.**
- The source usually does not fragment the IPv4 packet.
- The transport layer will instead segment the data into a size that can be accommodated by IPv4 and the data link layer in use.



# Fragmentation ... Contd.

## Identification

- This 16-bit field identifies a datagram originating from the source host.
- The combination of the identification and source IPv4 address must uniquely define a datagram as it leaves the source host.
- To guarantee uniqueness, the IPv4 protocol uses a counter to label the datagrams.
- The counter is initialized to a positive number.
- When the IPv4 protocol sends a datagram, it copies the current value of the counter to the identification field and increments the counter by 1.
- As long as the counter is kept in the main memory, uniqueness is guaranteed.
- When a datagram is fragmented, the value in the identification field is copied to all fragments.
- All fragments have the same identification number, the same as the original datagram.
- The identification number helps the destination in reassembling the datagram.
- It knows that all fragments having the same identification value must be assembled into one datagram.



# Fragmentation ... Contd.

## Flags

- This is a 3-bit field.
- The first bit is reserved.
- The second bit is called the do not fragment bit.
  - If its value is 1, the machine must not fragment the datagram.
  - If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host.
  - If its value is 0, the datagram can be fragmented if necessary.
- The third bit is called the more fragment bit.
  - If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one.
  - If its value is 0, it means this is the last or only fragment.

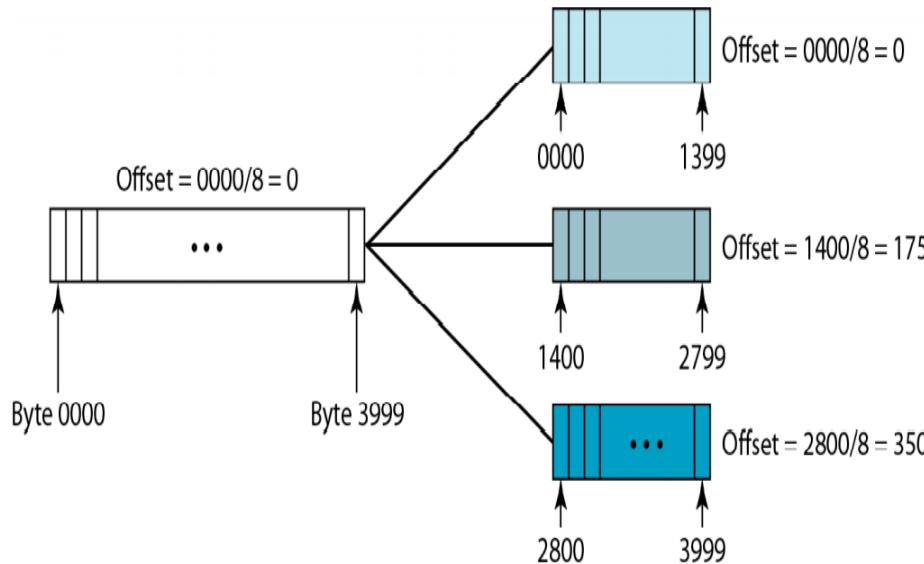


D: Do not fragment  
M: More fragments

# Fragmentation ... Contd.

## Fragmentation offset

- This 13-bit field shows the relative position of this fragment with respect to the whole datagram.
- It is the offset of the data in the original datagram measured in units of 8 bytes.



- The bytes in the original datagram are numbered 0 to 3999.
- The first fragment carries bytes 0 to 1399. The offset for this datagram is  $0/8 = 0$ .
- The second fragment carries bytes 1400 to 2799; the offset value for this fragment is  $1400/8 = 175$ .
- Finally, the third fragment carries bytes 2800 to 3999.
- The offset value for this fragment is  $2800/8 = 350$ .
- The value of the offset is measured in units of 8 bytes.
- This is done because the length of the offset field is only 13 bits and cannot represent a sequence of bytes greater than 8191.
- This forces hosts or routers that fragment datagrams to choose a fragment size so that the first byte number is divisible by 8.



# Time to Live

- A datagram has a limited lifetime in its travel through an internet.
- This field was originally designed to hold a timestamp, which was decremented by each visited router.
- The datagram was discarded when the value became zero.
- All the machines must have synchronized clocks and must know how long it takes for a datagram to go from one machine to another.
- This field is used mostly to control the maximum number of hops (routers) visited by the datagram.
- When a source host sends the datagram, it stores a number in this field.
- This value is approximately 2 times the maximum number of routes between any two hosts.
- Each router that processes the datagram decrements this number by 1.
- If this value, after being decremented, is zero, the router discards the datagram.

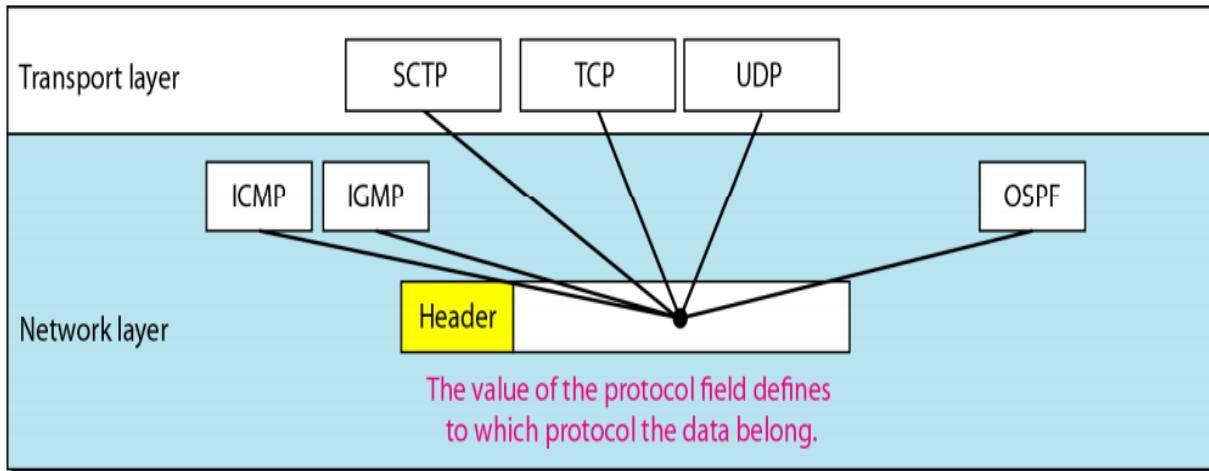


# Time to Live ... Contd.

- This field is needed because routing tables in the Internet can become corrupted.
  - A datagram may travel between two or more routers for a long time without ever getting delivered to the destination host.
  - This field limits the lifetime of a datagram.
- Another use of this field is to intentionally limit the journey of the packet.
  - E.g., if the source wants to confine the packet to the local network, it can store 1 in this field.
  - When the packet arrives at the first router, this value is decremented to 0, and the datagram is discarded.

# Protocol

- This 8-bit field defines the higher-level protocol that uses the services of the IPv4 layer.
- An IPv4 datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP, and IGMP.
- This field specifies the final destination protocol to which the IPv4 datagram is delivered.
- Since the IPv4 protocol carries data from different other protocols, the value of this field helps the receiving network layer know to which protocol the data belong.



Value	Protocol
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF



# Checksum

- The value of the checksum field is set to 0.
- Then the entire header is divided into 16-bit sections and added together.
- The result (sum) is complemented and inserted into the checksum field.
- The checksum in the IPv4 packet covers only the header, not the data.
- There are two good reasons for this:
  - First, all higher-level protocols that encapsulate data in the IPv4 datagram have a checksum field that covers the whole packet.
  - Therefore, the checksum for the IPv4 datagram does not have to check the encapsulated data.
  - Second, the header of the IPv4 packet changes with each visited router, but the data do not.
- So the checksum includes only the part that has changed.
- If the data were included, each router must recalculate the checksum for the whole packet, which means an increase in processing time.



# Checksum ... Contd.

4	5	0	28								
		1	0 0								
4		17	0								
10.12.14.5											
12.6.7.9											
4, 5, and 0	→	4	5	0	0						
28	→	0	0	1	C						
1	→	0	0	0	1						
0 and 0	→	0	0	0	0						
4 and 17	→	0	4	1	1						
0	→	0	0	0	0						
10.12	→	0	A	0	C						
14.5	→	0	E	0	5						
12.6	→	0	C	0	6						
7.9	→	0	7	0	9						
Sum	→	7	4	4	E						
Checksum	→	8	B	B	1						



# Source Address and Destination Address

## Source address

- This 32-bit field defines the IPv4 address of the source.
- This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

## Destination address

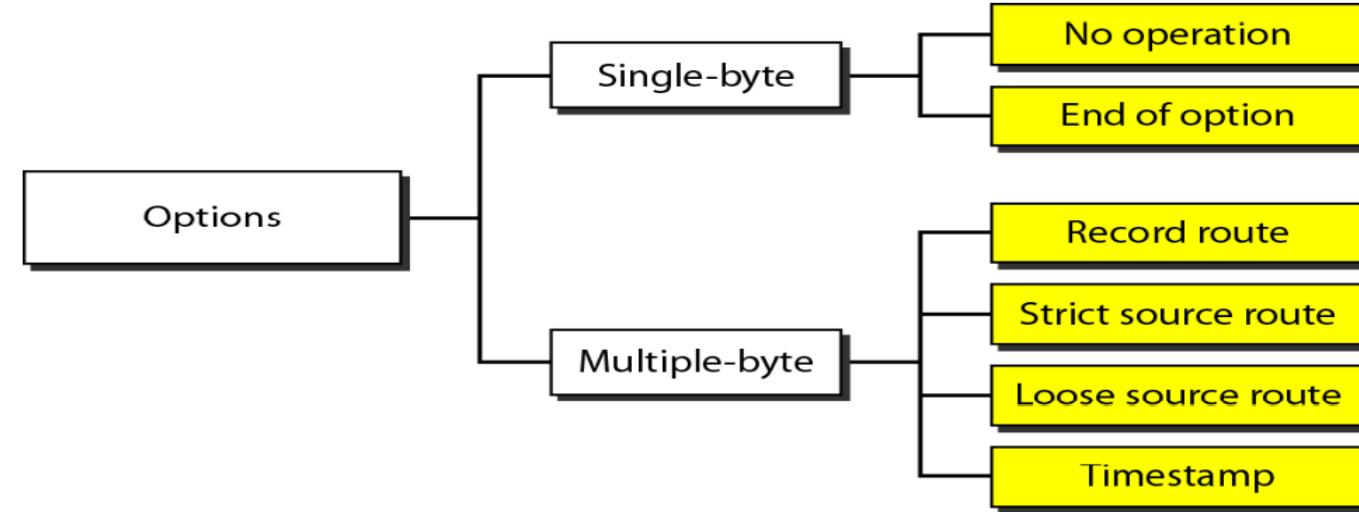
- This 32-bit field defines the IPv4 address of the destination.
- This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.



# Options

- The header of the IPv4 datagram is made of two parts: a fixed part and a variable part.
- The fixed part is 20 bytes long.
- The variable part comprises the options that can be a maximum of 40 bytes.
- Options, as the name implies, are not required for a datagram.
- They can be used for network testing and debugging.
- Options are not a required part of the IPv4 header, option processing is required of the IPv4 software.
- This means that all implementations must be able to handle options if they are present in the header.

# Options ... Contd.



- A **no-operation** option is a 1-byte option used as a filler between options.
- An **end-of-option** option is a 1-byte option used for padding at the end of the option field.
  - It, however, can only be used as the last option.
- A **record route** option is used to record the Internet routers that handle the datagram.
  - It can list up to nine router addresses.
  - It can be used for debugging and management purposes.



# Options ... Contd.

- A **strict source route** option is used by the source to predetermine a route for the datagram as it travels through for several purposes.
  - The sender can choose a route with a specific type of service, such as minimum delay or maximum throughput.
  - It may choose a route that is safer or more reliable for the sender's purpose.
  - E.g., a sender can choose a route so that its datagram does not travel through a competitor's network.
  - If a datagram specifies a strict source route, all the routers defined in the option must be visited by the datagram.
  - A router must not be visited if its IPv4 address is not listed in the datagram.
  - If the datagram visits a router that is not on the list, the datagram is discarded and an error message is issued.
  - If the datagram arrives at the destination and some of the entries were not visited, it will also be discarded and an error message issued.



# Options ... Contd.

- A **loose source route** option is similar to the strict source route, but it is less rigid.
  - Each router in the list must be visited, but the datagram can visit other routers as well.
- A **timestamp** option is used to record the time of datagram processing by a router.
  - The time is expressed in milliseconds from midnight, Universal time or Greenwich mean time.
  - Knowing the time a datagram is processed can help users and managers track the behavior of the routers in the Internet.
  - We can estimate the time it takes for a datagram to go from one router to another.
    - Estimate because, although all routers may use Universal time, their local clocks may not be synchronized.



# Practice Questions

- 1) An IPv4 packet has arrived with the first 8 bits as  $(01000010)_2$ . The receiver discards the packet. Why?
- 2) In an IPv4 packet, the value of HLEN is  $(1000)_2$ . How many bytes of options are being carried by this packet?
- 3) In an IPv4 packet, the value of HLEN is 5, and the value of the total length field is  $(0028)_{16}$ . How many bytes of data are being carried by this packet?
- 4) A packet has arrived with an M bit value of 0. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?
- 5) A packet has arrived with an M bit value of 1. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?
- 6) A packet has arrived with an M bit value of 1 and a fragmentation offset value of 0. Is this the first fragment, the last fragment, or a middle fragment?
- 7) A packet has arrived in which the offset value is 100. What is the number of the first byte? Do we know the number of the last byte?
- 8) A packet has arrived in which the offset value is 100, the value of HLEN is 5, and the value of the total length field is 100. What are the numbers of the first byte and the last byte?



# Practice Questions ... Contd.

- 9) Consider the following (hexadecimal) values in an IP header.

Version: 4

HLEN: 5

ToS: 0

Total length: 28

Identification bit: 1

Flag: 0

Fragmentation offset: 0

TTL: 4

Protocol: 6

Source IP: 10101211

Destination IP: 14020301

Calculate the checksum (hexadecimal Value) and explain the verification at the receiver side.

- 10) Assume that an IP datagram of size 2000 bytes (payload+header) arrives at router R1. R1 has to forward this IP datagram to a host X in a network with Maximum Transfer Unit (MTU) as 500 bytes. Illustrate the process of fragmentation with number of fragments created during packet transmission, HLEN, Total length, Do not Fragment, More Fragment, Fragmentation offset fields for both original datagram and fragment.



# Summary

## Discussed about

- Introduction
- Internet as a Datagram Network
- Internet as a Connectionless Network
- IPV4
- Datagram
- Practice Questions



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**

# Computer Networks

## BCSE308L

### Introduction to IPv6

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai

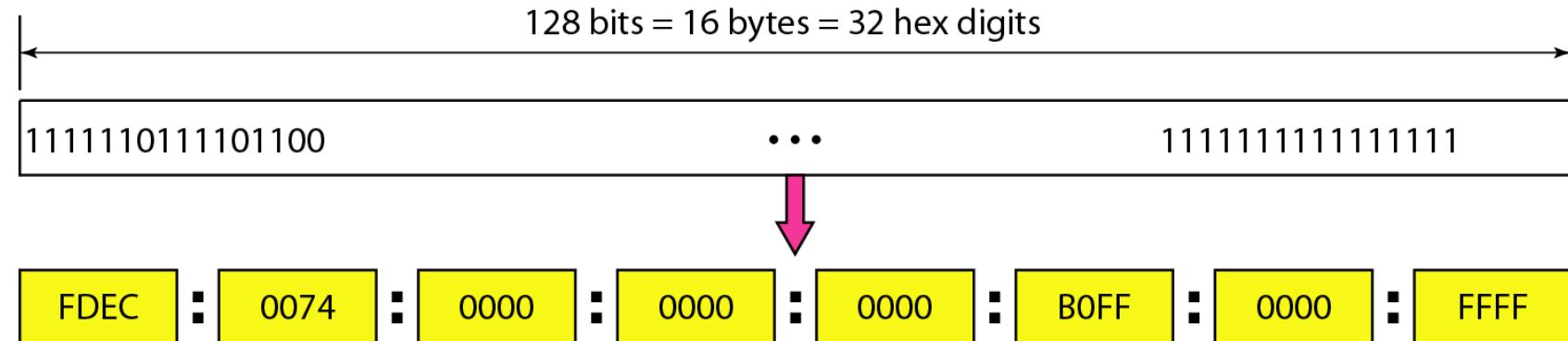


# Overview

- Introduction
- Representation
- Address Space
- Address Space Allocation
- Practice Questions
- Summary

# Introduction

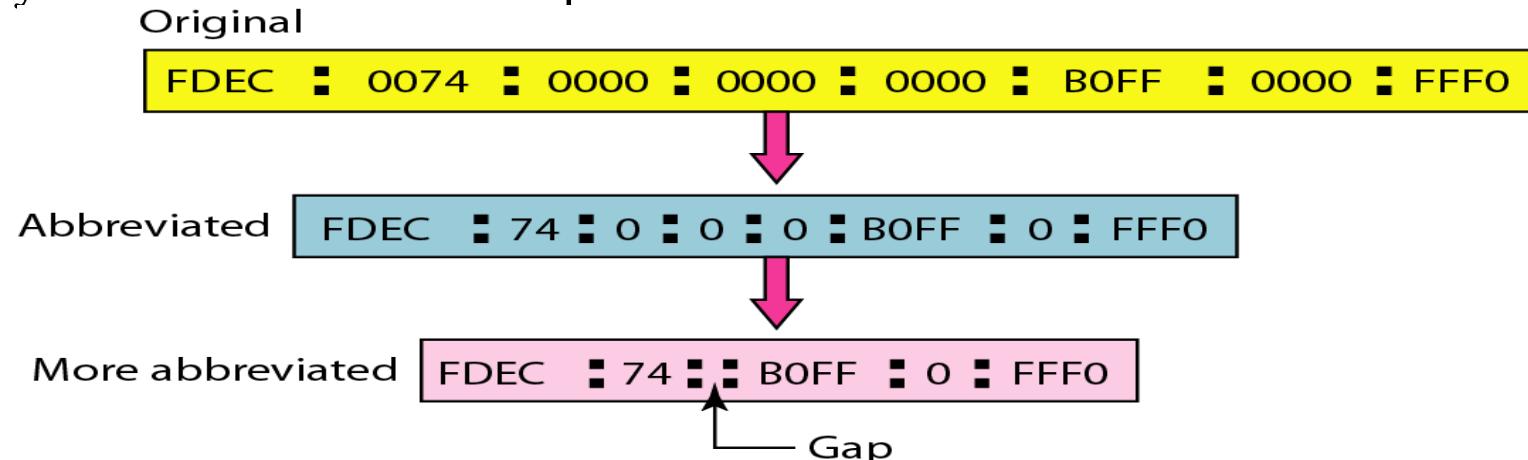
- The main reason for migration from IPv4 to IPv6 is the **small size of the address space in IPv4**.
- An IPv6 address is **128 bits or 16 bytes (octets) long**, four times the address length in IPv4.





# Representation

- An IPv6 address, even in hexadecimal format, is very long, many of the digits are zeros. In this case, we can abbreviate the address.
- The leading zeros of a section can be omitted.
  - Using this form of abbreviation, 0074 can be written as 74, 000F as F, and 0000 as 0. Note that 3210 cannot be abbreviated.
- Further abbreviation, often called zero compression, can be applied to colon hex notation if there are consecutive sections consisting of zeros only.
  - We can remove all the zeros and replace them with a double semicolon.
  - This type of abbreviation is allowed only once per address. If there is more than one run of zero sections, only one of them can be compressed.





# Representation ... Contd.

Expand the address 0:15::1:12:1213 to its original.



# Representation ... Contd.

Expand the address 0:15::1:12:1213 to its original.

Align the left side of the double colon to the left of the original pattern and the right side of the double colon to the right of the original pattern to find how many 0s we need to replace the double colon.

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
0: 15: : 1: 12:1213

This means that the original address is.

0000:0015:0000:0000:0000:0001:0012:1213
---



# Representation ... Contd.

## Mixed Notation

- Sometimes we see a mixed representation of an IPv6 address: colon hex and dotted decimal notation.
- This is appropriate during the transition period in which an IPv4 address is embedded in an IPv6 address (as the rightmost 32 bits).
- We can use the colon hex notation for the leftmost six sections and four-byte dotted-decimal notation instead of the rightmost two sections.
- However, this happens when all or most of the leftmost sections of the IPv6 address are 0s.
- For example, the address (::130.24.24.18) is a legitimate address in IPv6, in which the zero compression shows that all 96 leftmost bits of the address are zeros.



# Address Space

- The address space of IPv6 contains  $2^{128}$  addresses.
- This address space is  $2^{96}$  times the IPv4 address—definitely no address depletion.
- To give some idea about the number of addresses, we assume that only 1/64 (almost 2 percent) of the addresses in space can be assigned to the people on planet Earth and the rest are reserved for special purposes.
- We also assume that the number of people on the earth is soon to be  $2^{34}$  (more than 16 billion).
- Each person can have  $2^{88}$  addresses to use. Address depletion in this version is impossible.



# Address Space ... Contd.

## Three Address Types

- In IPv6, a destination address can belong to one of three categories:
  - Unicast
  - Anycast
  - Multicast



# Address Space ... Contd.

## Unicast Address

- A unicast address defines a single interface (computer or router).
- The packet sent to a unicast address will be routed to the intended recipient.



# Address Space ... Contd.

## Anycast Address

- An anycast address defines a group of computers that all share a single address.
- A packet with an anycast address is delivered to only one member of the group, the most reachable one.
- An anycast communication is used, for example, when there are several servers that can respond to an inquiry.
- The request is sent to the one that is most reachable.
- The hardware and software generate only one copy of the request; the copy reaches only one of the servers.
- IPv6 does not designate a block for anycasting; the addresses are assigned from the unicast block.



# Address Space ... Contd.

## Multicast Address

- A multicast address also defines a group of computers.
- However, there is a difference between anycasting and multicasting.
- In anycasting, only one copy of the packet is sent to one of the members of the group; in multicasting each member of the group receives a copy.
- IPv6 has designated a block for multicasting from which the same address is assigned to the members of the group.
- IPv6 does not define broadcasting, even in a limited version.
- IPv6 considers broadcasting as a special case of multicasting.



# Address Space Allocation

- Like the address space of IPv4, the address space of IPv6 is divided into several blocks of varying size and each block is allocated for a special purpose.
- Most of the blocks are still unassigned and have been set aside for future use.

*Prefixes for assigned IPv6 addresses*

<i>Block prefix</i>	<i>CIDR</i>	<i>Block assignment</i>	<i>Fraction</i>
0000 0000	0000::/8	Special addresses	1/256
<b>001</b>	<b>2000::/3</b>	<b>Global unicast</b>	<b>1/8</b>
1111 110	FC00::/7	Unique local unicast	1/128
1111 1110 10	FE80::/10	Link local addresses	1/1024
1111 1111	FF00::/8	Multicast addresses	1/256

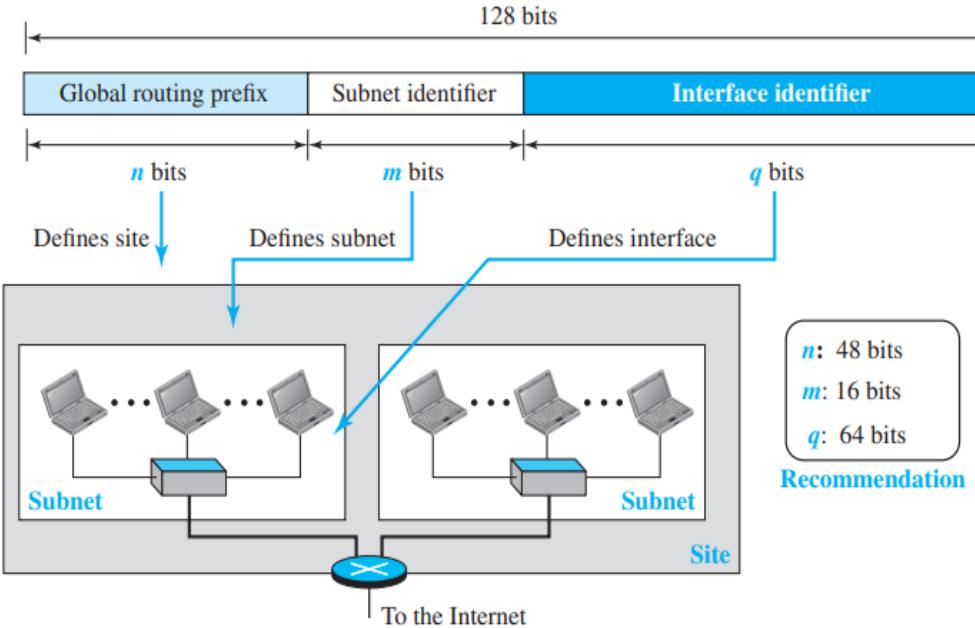


## Global Unicast Addresses

- The block in the address space that is used for unicast (one-to-one) communication between two hosts in the Internet is called the global unicast address block.
- CIDR for the block is 2000::/3, which means that the three leftmost bits are the same for all addresses in this block (001).
- The size of this block is  $2^{125}$  bits, which is more than enough for Internet expansion for many years to come.
- An address in this block is divided into **three parts: global routing prefix (n bits), subnet identifier (m bits), and interface identifier (q bits)**.

# Address Space Allocation ... Contd.

## Global Unicast Addresses ... Contd.



- The global routing prefix is used to route the packet through the Internet to the organization site, such as the ISP that owns the block.
- Since the first three bits in this part are fixed (001), the rest of the 45 bits can be defined for up to  $2^{45}$  sites (a private organization or an ISP).
- The global routers in the Internet route a packet to its destination site based on the value of n.
- The next m bits (16 bits based on recommendation) define a subnet in an organization.
- This means that an organization can have up to  $2^{16} = 65,536$  subnets, which is more than enough.
- The last q bits (64 bits based on recommendation) define the interface identifier.
- The interface identifier is similar to hostid in IPv4 addressing, although the term interface identifier is a better choice because, the host identifier actually defines the interface, not the host.
- If the host is moved from one interface to another, its IP address needs to be changed.



# Address Space Allocation... Contd.

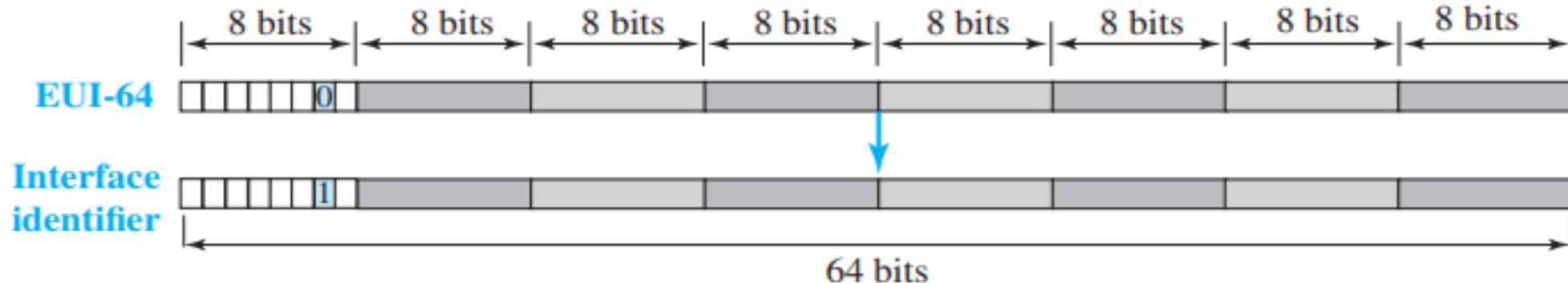
## Global Unicast Addresses ... Contd.

- In IPv4 addressing, there is not a specific relation between the hostid (at the IP level) and link-layer address (at the data-link layer) because the link-layer address is normally much longer than the hostid.
- The IPv6 addressing allows this relationship.
- A link-layer address whose length is less than 64 bits can be embedded as the whole or part of the interface identifier, eliminating the mapping process.
- Two common link layer addressing schemes can be considered for this purpose:
  - ✓ 64-bit extended unique identifier (EUI-64) defined by IEEE
  - ✓ 48-bit link-layer address defined by Ethernet

# Address Space Allocation... Contd.

## Mapping EUI-64

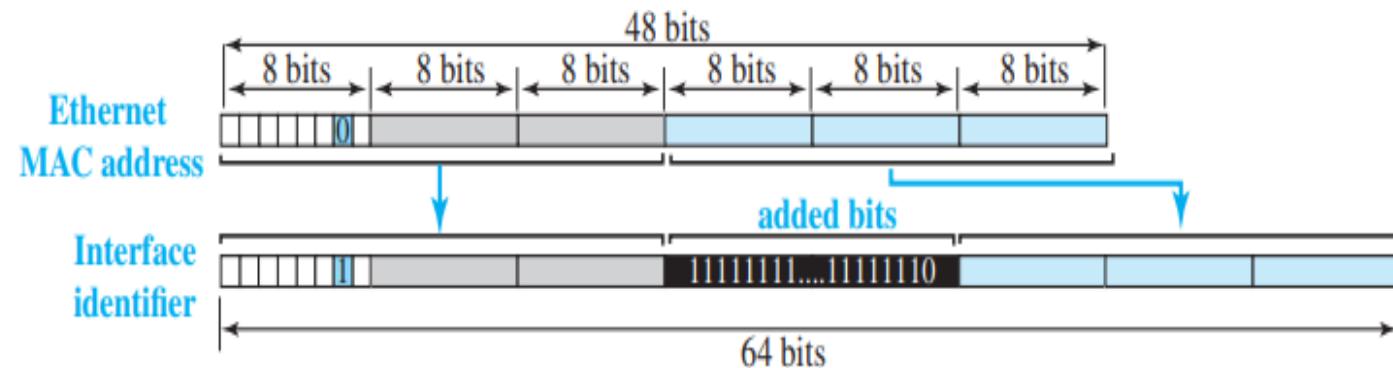
- To map a 64-bit physical address, the global/local bit of this format needs to be changed from 0 to 1 (local to global) to define an interface address.



# Address Space Allocation... Contd.

## Mapping Ethernet MAC Address

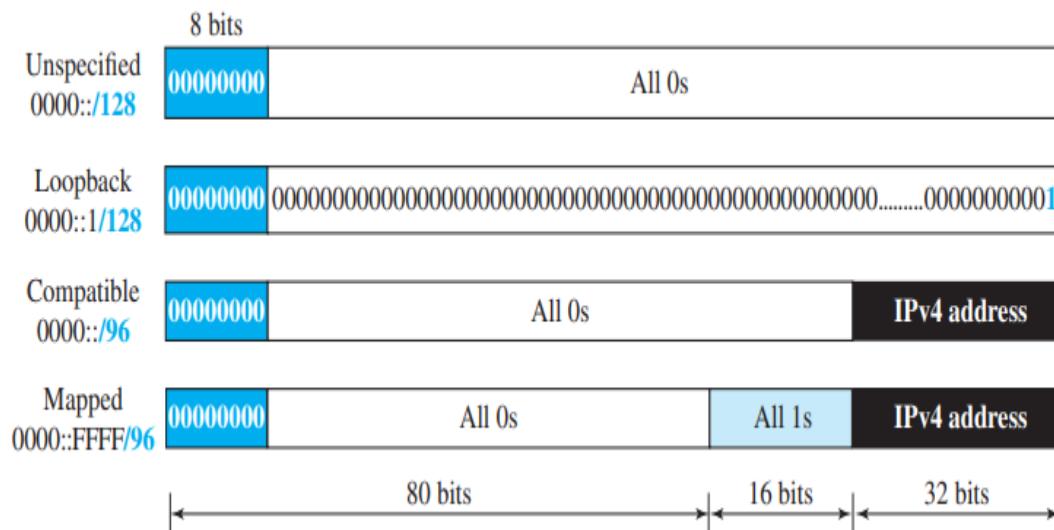
- Mapping a 48-bit Ethernet address into a 64-bit interface identifier is more involved.
- We need to change the local/global bit to 1 and insert an additional 16 bits.
- The additional 16 bits are defined as 15 ones followed by one zero, or  $\text{FFFE}_{16}$ .



# Address Space Allocation... Contd.

## Special Addresses

- Addresses that use the prefix (0000::/8) are reserved, but part of this block is used to define some special addresses.



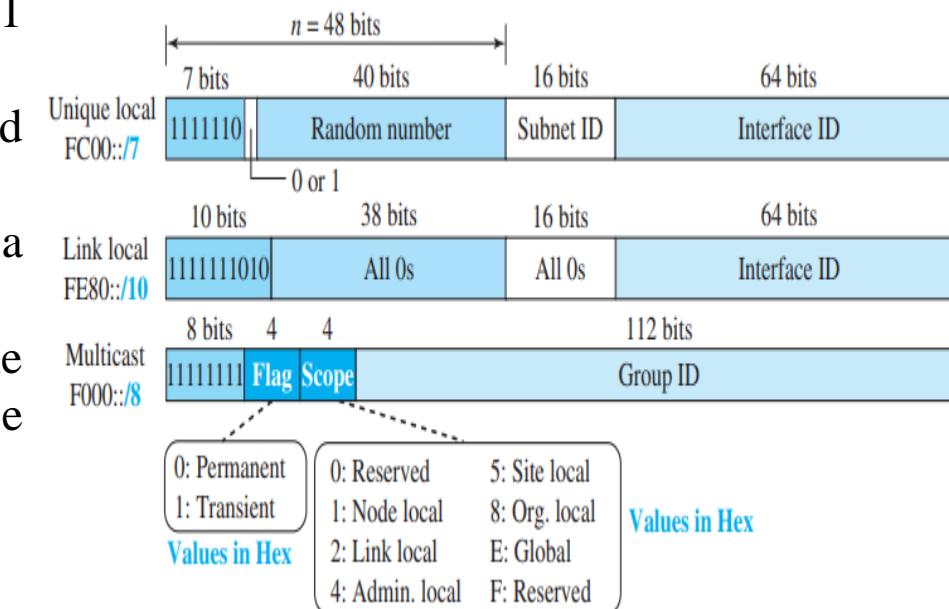
- The unspecified address is a subblock containing only one address, which is used during bootstrap when a host does not know its own address and wants to send an inquiry to find it.
- The loopback address also consists of one address.
- In IPv4 the block is made of a range of addresses; in IPv6, the block has only a single address in it.
- During the transition from IPv4 to IPv6, hosts can use their IPv4 addresses embedded in IPv6 addresses.
- Two formats have been designed for this purpose: compatible and mapped.
- A compatible address is an address of 96 bits of zero followed by 32 bits of IPv4 address.
  - ✓ It is used when a computer using IPv6 wants to send a message to another computer using IPv6.
- A mapped address is used when a computer already migrated to version 6 wants to send an address to a computer still using version 4.



# Address Space Allocation... Contd.

## Other Assigned Blocks

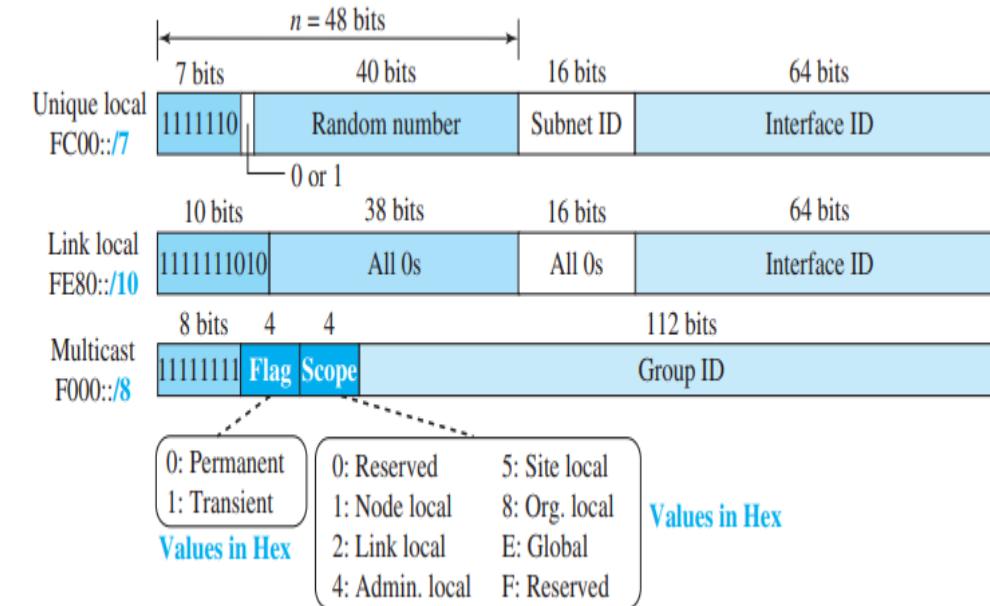
- IPv6 uses two large blocks for private addressing and one large block for multicasting.
- A subblock in a unique local unicast block can be privately created and used by a site.
- The packet carrying this type of address as the destination address is not expected to be routed.
- This type of address has the identifier 1111 110, the next bit can be 0 or 1 to define how the address is selected (locally or by an authority).
- The next 40 bits are selected by the site using a randomly generated number of length 40 bits.
- This means that the total of 48 bits defines a subblock that looks like a global unicast address.
- The 40-bit random number makes the probability of duplication of the address extremely small. Note the similarity between the format of these addresses and the global unicast.
- The second block, designed for private addresses, is the link local block.
- A subblock in this block can be used as a private address in a network.
- This type of address has the block identifier 111111010.
- The next 54 bits are set to zero.
- The last 64 bits can be changed to define the interface for each computer.



# Address Space Allocation... Contd.

## Other Assigned Blocks ... Contd.

- Multicast addresses are used to define a group of hosts instead of just one.
- In IPv6 a large block of addresses are assigned for multicasting.
- All these addresses use the prefix 11111111.
- The second field is a flag that defines the group address as either permanent or transient.
- A permanent group address is defined by the Internet authorities and can be accessed at all times.
- A transient group address, on the other hand, is used only temporarily.
- Systems engaged in a teleconference, for example, can use a transient group address.
- The third field defines the scope of the group address

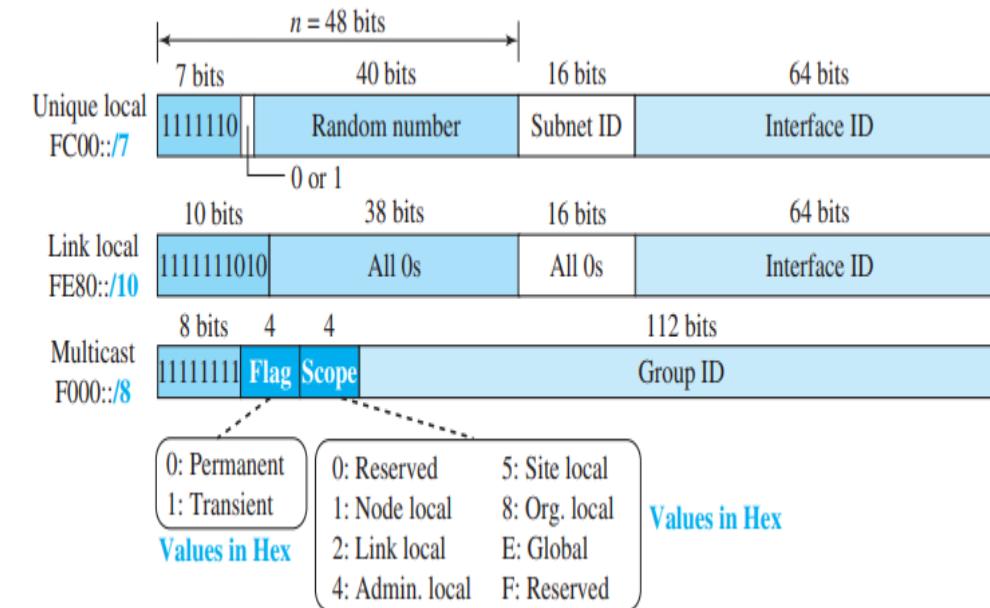




# Address Space Allocation... Contd.

## Other Assigned Blocks ... Contd.

- Multicast addresses are used to define a group of hosts instead of just one.
- In IPv6 a large block of addresses are assigned for multicasting.
- All these addresses use the prefix 11111111.
- The second field is a flag that defines the group address as either permanent or transient.
- A permanent group address is defined by the Internet authorities and can be accessed at all times.
- A transient group address, on the other hand, is used only temporarily.
- Systems engaged in a teleconference, for example, can use a transient group address.
- The third field defines the scope of the group address





# Practice Questions

1) Show abbreviations for the following addresses:

- a. 0000:FFFF:FFFF:0000:0000:0000:0000:0000
- b. 1234:2346:3456:0000:0000:0000:0000:FFFF
- c. 0000:0001:0000:0000:0000:FFFF:1200:1000
- d. 0000:0000:0000:0000:FFFF:FFFF:24.123.12.6

2) Decompress the following addresses and show the complete unabbreviated IPv6 address:

- a. ::2222
- b. 1111::
- c. B:A:CC::1234:A

3) An organization is assigned the block 2000:1456:2474/48. What is the CIDR notation for the blocks in the first and second subnets in this organization?

4) Using the format we defined for Ethernet addresses, find the interface identifier if the physical address in the EUI is (F5-A9-23-EF-07-14-7A-D2)<sub>16</sub>.

5) An organization is assigned the block 2000:1456:2474/48. What is the IPv6 address of an interface in the third subnet if the IEEE physical address of the computer is (F5-A9-23-EF-07-14-7A-D2)<sub>16</sub>.



# Summary

## Discussed about

- Introduction
- Representation
- Address Space
- Address Space Allocation
- Practice Questions



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**



**VIT<sup>®</sup>**

**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

# Computer Networks

## BCSE308L

### The IPv6 Protocol

**Dr. Bhuvaneswari Amma N.G.**  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai



# Overview

- Introduction
- Packet Format
- Extension Header
- Summary



# Introduction

## Changes implemented in the protocol in addition to changing address size and format

- Better header format
  - IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the data.
  - This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
- New options
  - IPv6 has new options to allow for additional functionalities.
- Allowance for extension
  - IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

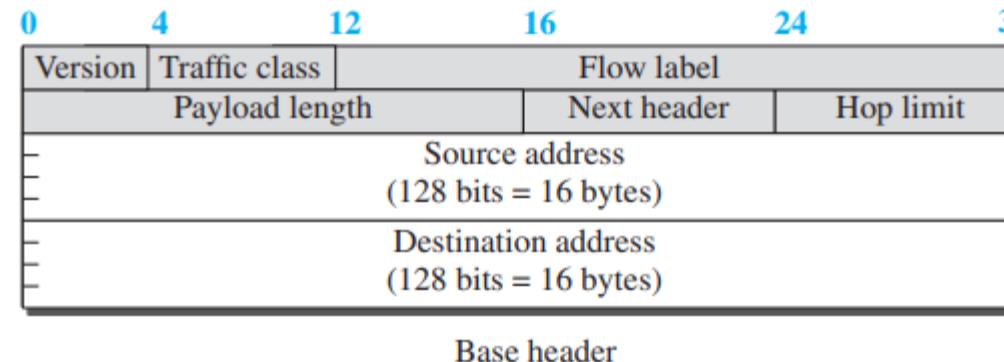
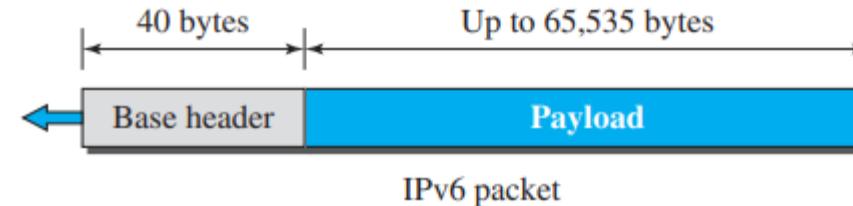


# Introduction ... Contd.

- **Support for resource allocation**
  - In IPv6, the type-of-service field has been removed, but two new fields, **traffic class** and **flow label**, have been added to enable the source to request special handling of the packet.
  - This mechanism can be used to support traffic such as real-time audio and video.
- **Support for more security**
  - The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

# Packet Format

- Each packet is composed of a base header followed by the payload.
- The base header occupies 40 bytes, whereas payload can be up to 65,535 bytes of information.





# Packet Format ... Contd.

## Version

- The 4-bit version field defines the version number of the IP.
- For IPv6, the value is 6.

## Traffic class

- The 8-bit traffic class field is used to distinguish different payloads with different delivery requirements.
- It replaces the type-of-service field in IPv4.

## Flow label

- The flow label is a 20-bit field that is designed to provide special handling for a particular flow of data.



# Packet Format ... Contd.

## Payload length

- The 2-byte payload length field defines the length of the IP datagram excluding the header.
- **Note:** IPv4 defines two fields related to the length: header length and total length.
- In IPv6, the length of the base header is fixed (40 bytes); only the length of the payload needs to be defined.

## Next header

- The next header is an 8-bit field defining the type of the first extension header (if present) or the type of the data that follows the base header in the datagram.
- This field is similar to the protocol field in IPv4.



# Packet Format ... Contd.

## Hop limit

- The 8-bit hop limit field serves the same purpose as the TTL field in IPv4.

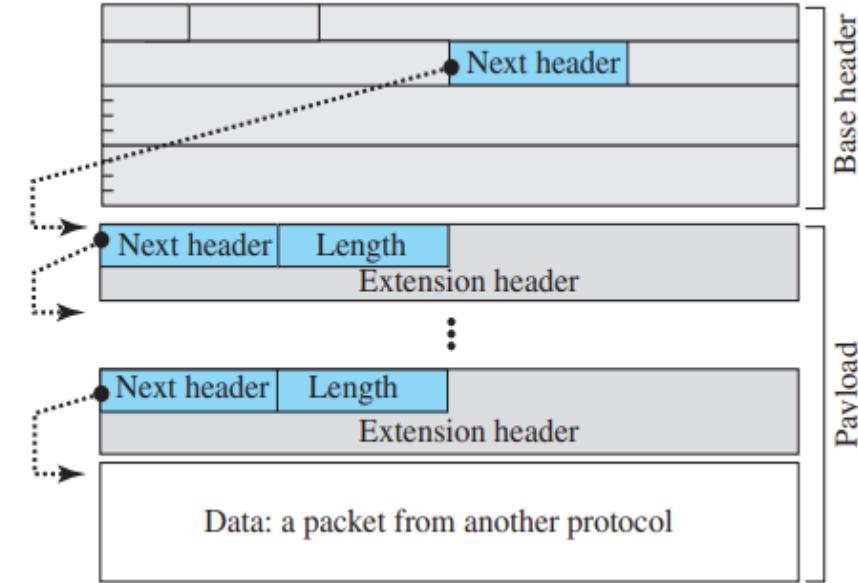
## Source and destination addresses

- The source address field is a 16-byte (128-bit) Internet address that identifies the original source of the datagram.
- The destination address field is a 16-byte (128-bit) Internet address that identifies the destination of the datagram

# Packet Format ... Contd.

## Payload

- Compared to IPv4, the payload field in IPv6 has a different format and meaning.
- The payload in IPv6 means a combination of zero or more extension headers (options) followed by the data from other protocols (UDP, TCP, and so on).
- In IPv6, options, which are part of the header in IPv4, are designed as extension headers.
- The payload can have as many extension headers as required by the situation.
- Each extension header has two mandatory fields, **next header** and the **length**, followed by information related to the particular option.
- Each next header field value (code) defines the type of the next header (hop-by-hop option, source routing option, . . .); the last next header field defines the protocol (UDP, TCP, . . .) that is carried by the datagram.



### Some next-header codes

00:	Hop-by-hop option
02:	ICMPv6
06:	TCP
17:	UDP
43:	Source-routing option
44:	Fragmentation option
50:	Encrypted security payload
51:	Authentication header
59:	Null (no next header)
60:	Destination option



# Packet Format ... Contd.

## Concept of Flow and Priority in IPv6

- The IP protocol was originally designed as a connectionless protocol.
- The tendency is to use the IP protocol as a connection-oriented protocol.
- In version 6, the flow label has been directly added to the format of the IPv6 datagram to allow us to use IPv6 as a connection-oriented protocol.
  - To a router, a flow is a sequence of packets that share the same characteristics, such as traveling the same path, using the same resources, having the same kind of security, and so on.
  - A router that supports the handling of flow labels has a flow label table.
  - The table has an entry for each active flow label; each entry defines the services required by the corresponding flow label.
  - When the router receives a packet, it consults its flow label table to find the corresponding entry for the flow label value defined in the packet.
  - It then provides the packet with the services mentioned in the entry.
  - The flow label itself does not provide the information for the entries of the flow label table; the information is provided by other means, such as the hop-by-hop options or other protocols.



# Packet Format ... Contd.

## Concept of Flow and Priority in IPv6 ... Contd.

- The flow label can be used to speed up the processing of a packet by a router.
- When a router receives a packet, instead of consulting the forwarding table and going through a routing algorithm to define the address of the next hop, it can easily look in a flow label table for the next hop.
- The flow label can be used to support the transmission of real-time audio and video.
- Real-time audio or video, particularly in digital form, requires resources such as high bandwidth, large buffers, long processing time, and so on.
- A process can make a reservation for these resources beforehand to guarantee that real-time data will not be delayed due to a lack of resources.



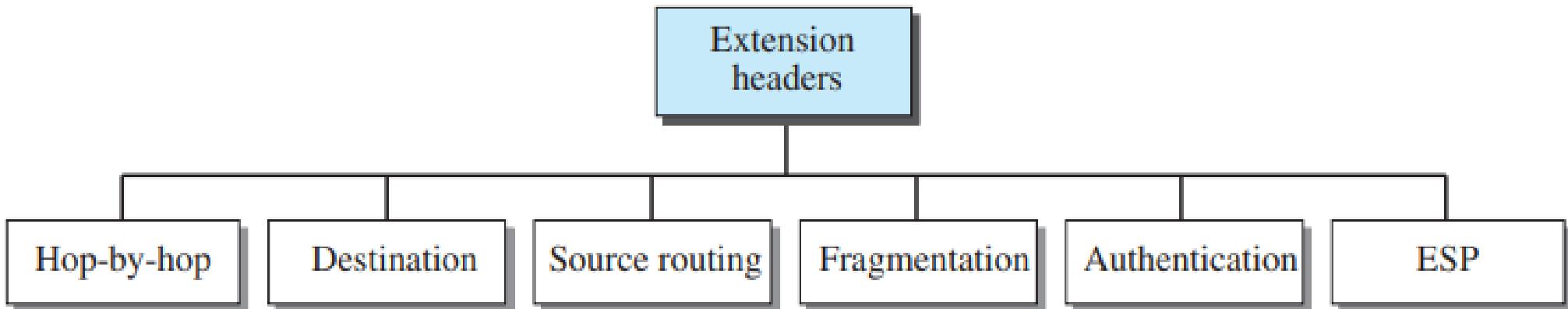
# Packet Format ... Contd.

## Fragmentation and Reassembly

- There are still fragmentation and reassembly of datagrams in the IPv6 protocol, but there is a major difference.
- IPv6 datagrams can be fragmented only by the source, not by the routers; the reassembly takes place at the destination.
- The fragmentation of packets at routers is not allowed to speed up the processing of packets in the router.
- The fragmentation of a packet in a router needs a lot of processing.
- The packet needs to be fragmented, all fields related to the fragmentation need to be recalculated.
- In IPv6, the source can check the size of the packet and make the decision to fragment the packet or not.
- When a router receives the packet, it can check the size of the packet and drop it if the size is larger than allowed by the MTU of the network ahead.
- The router then sends a packet-too-big ICMPv6 error message to inform the source.

# Extension Header

- An IPv6 packet is made of a base header and some extension headers.
- The length of the base header is fixed at 40 bytes.
- To give more functionality to the IP datagram, the base header can be followed by up to six extension headers.
- Many of these headers are options in IPv4.





# Extension Header ... Contd.

## Hop-by-Hop Option

- The hop-by-hop option is used when the source needs to pass information to all routers visited by the datagram.
- For example, routers must be informed about certain management, debugging, or control functions. Or, if the length of the datagram is more than the usual 65,535 bytes, routers must have this information.
- So far, only three hop-by-hop options have been defined: Pad1, PadN, and jumbo payload.

### Pad1

- This option is 1 byte long and is designed for alignment purposes. Some options need to start at a specific bit of the 32-bit word.
- If an option falls short of this requirement by exactly one byte, Pad1 is added.

### PadN

- PadN is similar in concept to Pad1.
- The difference is that PadN is used when 2 or more bytes are needed for alignment.

### Jumbo payload

- The length of the payload in the IP datagram can be a maximum of 65,535 bytes.
- If for any reason a longer payload is required, we can use the jumbo payload option to define this longer length.



# Extension Header ... Contd.

## Destination Option

- The destination option is used when the source needs to pass information to the destination only. Intermediate routers are not permitted access to this information.
- The format of the destination option is the same as the hop-by-hop option.
- So far, only the Pad1 and PadN options have been defined.

## Source Routing

- The source routing extension header combines the concepts of the strict source route and the loose source route options of IPv4.



# Extension Header ... Contd.

## Fragmentation

- The concept of fragmentation in IPv6 is the same as that in IPv4. However, the place where fragmentation occurs differs.
- In IPv4, the source or a router is required to fragment if the size of the datagram is larger than the MTU of the network over which the datagram travels.
- In IPv6, only the original source can fragment.
- A source must use a Path MTU Discovery technique to find the smallest MTU supported by any network on the path.
- The source then fragments using this knowledge.
- If the source does not use a Path MTU Discovery technique, it fragments the datagram to a size of 1280 bytes or smaller.
- This is the minimum size of MTU required for each network connected to the Internet.



# Extension Header ... Contd.

## Authentication

- The authentication extension header has a dual purpose: **it validates the message sender and ensures the integrity of data.**
- The former is needed so the receiver can be sure that a message is from the genuine sender and not from an imposter.
- The latter is needed to check that the data is not altered in transition by some hacker.

## Encrypted Security Payload

- The encrypted security payload is an extension that provides confidentiality and guards against eavesdropping.



# Extension Header ... Contd.

## Comparison of Options between IPv4 and IPv6

- The no-operation and end-of-option options in IPv4 are replaced by Pad1 and PadN options in IPv6.
- The record route option is not implemented in IPv6 because it was not used.
- The timestamp option is not implemented because it was not used.
- The source route option is called the source route extension header in IPv6.
- The fragmentation fields in the base header section of IPv4 have moved to the fragmentation extension header in IPv6.
- The authentication extension header is new in IPv6.
- The encrypted security payload extension header is new in IPv6.



# Summary

## Discussed about

- Introduction
- Packet Format
- Extension Header



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**



**VIT<sup>®</sup>**

**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

# Computer Networks

## BCSE308L

### Special Addresses

**Dr. Bhuvaneswari Amma N.G.**  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai



# Overview

- Introduction
- This-host address
- Limited-broadcast address
- Loopback address
- Private addresses
- Multicast addresses
- Address Aggregation
- Longest Matching Mask
- Practice Questions
- Summary



# Introduction

- Five special addresses that are used for special purposes.
  - This-host address
  - Limited-broadcast address
  - Loopback address
  - Private addresses
  - Multicast addresses



# This-host Address

- The only address in the block **0.0.0.0/32** is called the this-host address.
- It is used whenever a host needs to send an IP datagram but it does not know its own address to use as the source address.



# Limited-broadcast Address

- The only address in the block **255.255.255.255/32** is called the limited-broadcast address.
- It is used whenever a router or a host needs to send a datagram to all devices in a network.
- The routers in the network, however, block the packet having this address as the destination; the packet cannot travel outside the network.



# Loopback Address

- The block **127.0.0.0/8** is called the loopback address.
- A packet with one of the addresses in this block as the destination address never leaves the host; it will remain in the host.
- Any address in the block is used to test a piece of software in the machine.
- E.g., We can write a client and a server program in which one of the addresses in the block is used as the server address.
- We can test the programs using the same host to see if they work before running them on different computers.



# Private Addresses

- Four blocks are assigned as private addresses:
- 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, and 169.254.0.0/16.



# Multicast Addresses

- The block **224.0.0.0/4** is reserved for multicast addresses.

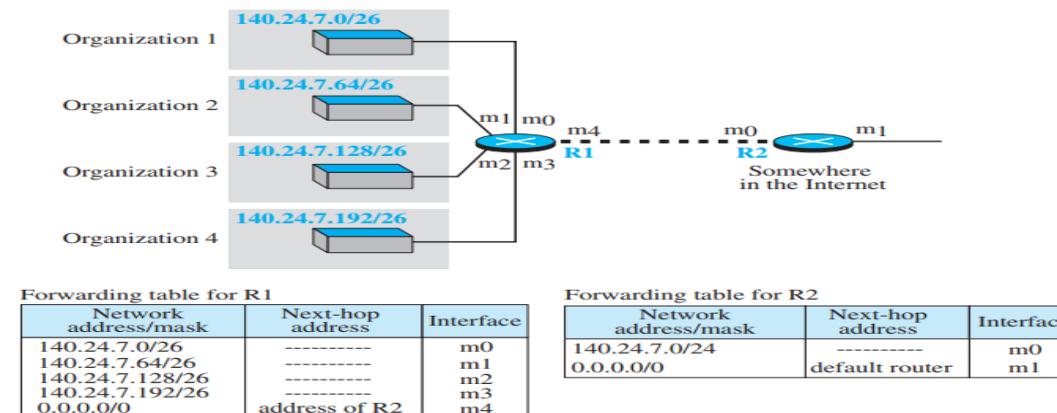


# Address Aggregation

- When we use classful addressing, there is only one entry in the forwarding table for each site outside the organization.
- The entry defines the site even if that site is subnetted.
- When a packet arrives at the router, the router checks the corresponding entry and forwards the packet accordingly.
- When we use classless addressing, it is likely that the number of forwarding table entries will increase.
- This is because the intent of classless addressing is to divide up the whole address space into manageable blocks.
- The increased size of the table results in an increase in the amount of time needed to search the table.
- To alleviate the problem, the idea of address aggregation was designed.

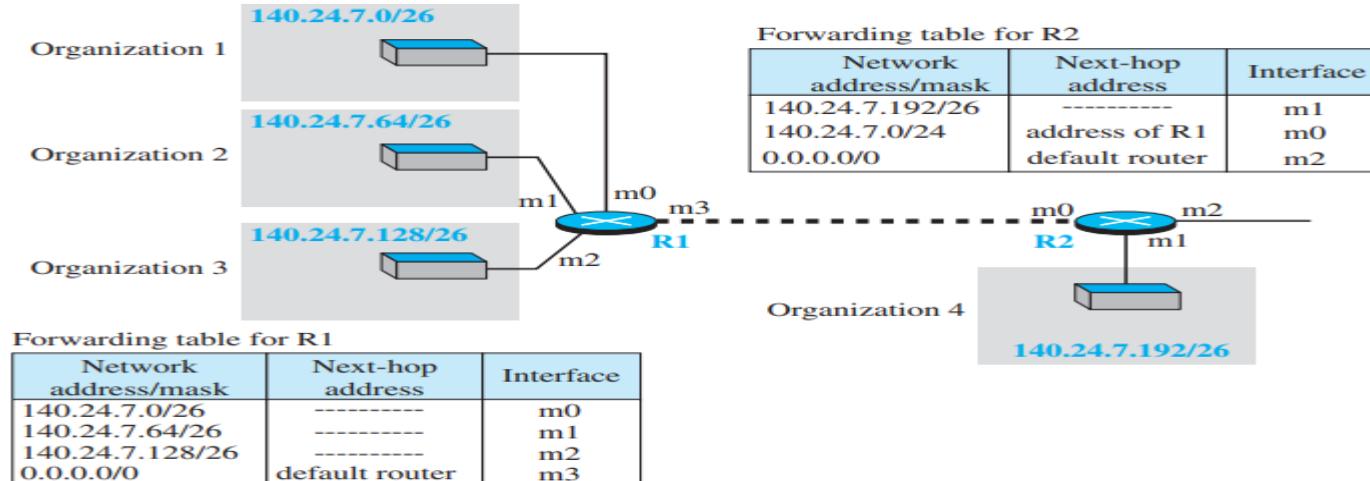
# Address Aggregation

- R1 is connected to networks of four organizations that each use 64 addresses. R2 is somewhere far from R1.
- R1 has a longer forwarding table because each packet must be correctly routed to the appropriate organization. R2, on the other hand, can have a very small forwarding table.
- For R2, any packet with destination 140.24.7.0 to 140.24.7.255 is sent out from interface m0 regardless of the organization number.
- This is called address aggregation because the blocks of addresses for four organizations are aggregated into one larger block.
- R2 would have a longer forwarding table if each organization had addresses that could not be aggregated into one block.



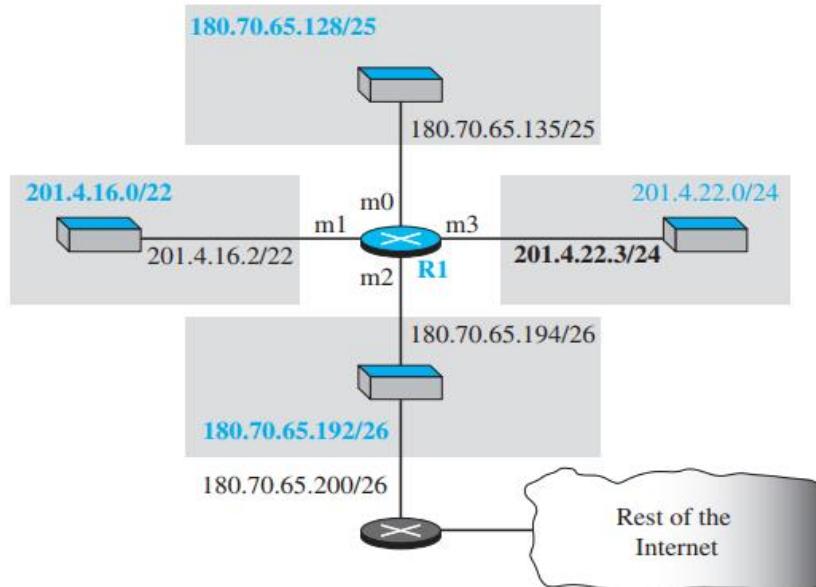
# Longest Matching Mask

- What happens if one of the organizations is not geographically close to the other three?
- For example, if organization 4 cannot be connected to router R1 for some reason, can we still use the idea of address aggregation and still assign block 140.24.7.192/26 to organization 4?
- The answer is yes, because routing in classless addressing uses another principle, longest mask matching.
- This principle states that the forwarding table is sorted from the longest mask to the shortest mask.
- If there are three masks, /27, /26, and /24, the mask /27 must be the first entry and /24 must be the last.
- If this principle solves the situation in which organization 4 is separated from the other three organizations.



# Practice Questions ... Contd.

Make a forwarding table for router R1 using the configuration in the given network.

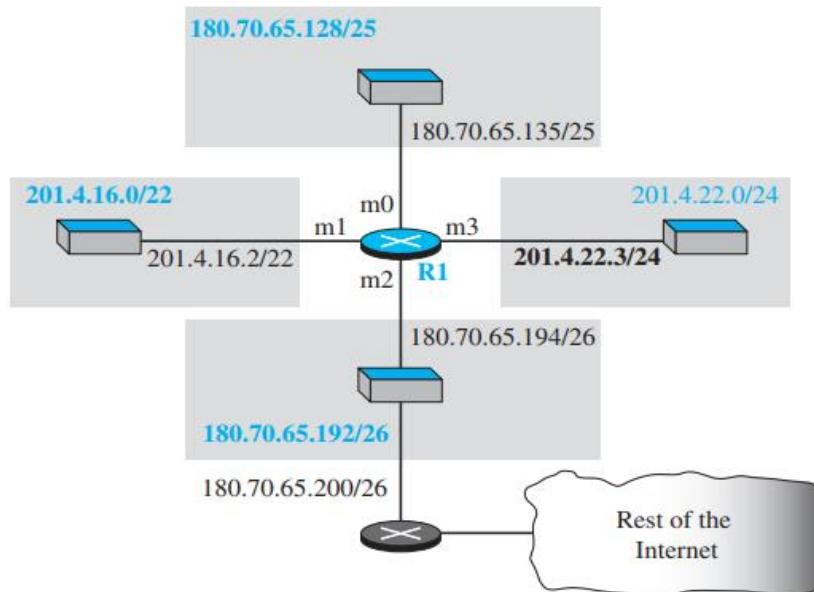


Network address/mask	Next hop	Interface
180.70.65.192/26	—	m2
180.70.65.128/25	—	m0
201.4.22.0/24	—	m3
201.4.16.0/22	—	m1
Default	180.70.65.200	m2

Leftmost bits in the destination address	Next hop	Interface
10110100 01000110 01000001 11	—	m2
10110100 01000110 01000001 1	—	m0
11001001 00000100 00011100	—	m3
11001001 00000100 000100	—	m1
Default	180.70.65.200	m2

# Practice Questions

Show the forwarding process if a packet arrives at R1 with the destination address 180.70.65.140.



The router performs the following steps:

1. The first mask (/26) is applied to the destination address. The result is 180.70.65.128, which does not match the corresponding network address.
2. The second mask (/25) is applied to the destination address. The result is 180.70.65.128, which matches the corresponding network address. The next-hop address and the interface number m0 are extracted for forwarding the packet.



# Summary

## Discussed about

- Introduction
- This-host address
- Limited-broadcast address
- Loopback address
- Private addresses
- Multicast addresses
- Address Aggregation
- Longest Matching Mask
- Practice Questions



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**

# Computer Networks

## BCSE308L

## Delivery, Forwarding, and Routing

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai



# Overview

- Introduction
- Delivery
- Forwarding
- Forwarding Techniques
- Forwarding Process
- Routing Table
- Summary



# Introduction

**Delivery, forwarding, and routing of IP packets to their final destinations**

- **Delivery** refers to the way a packet is handled by the underlying networks under the control of the network layer.
- **Forwarding** refers to the way a packet is delivered to the next station.
- **Routing** refers to the way routing tables are created to help in forwarding.
  - Routing protocols are used to continuously update the routing tables that are consulted for forwarding and routing.



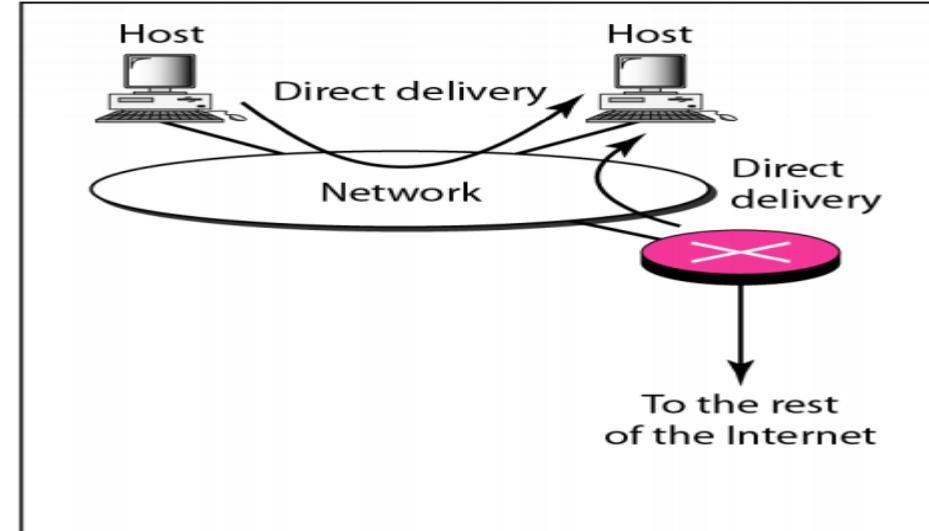
# Delivery

- The network layer supervises the handling of the packets by the underlying physical networks.
- This handling is defined as the delivery of a packet.
- The delivery of a packet to its final destination is accomplished by using two different methods of delivery, **direct and indirect**.

# Delivery ... Contd.

## Direct Delivery

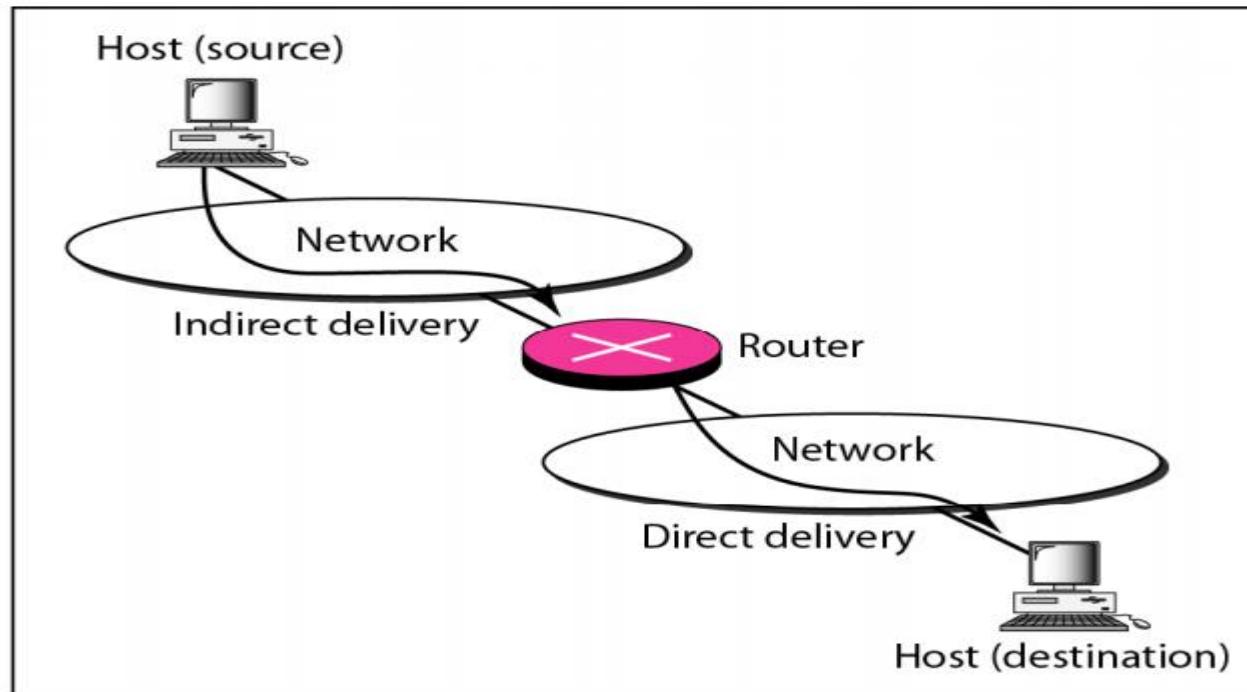
- In a direct delivery, the final destination of the packet is a host connected to the same physical network as the deliverer.
- Direct delivery occurs when the source and destination of the packet are located on the same physical network or when the delivery is between the last router and the destination host.
- The sender can easily determine if the delivery is direct. It can extract the network address of the destination (using the mask) and compare this address with the addresses of the networks to which it is connected.
- If a match is found, the delivery is direct.



# Delivery ... Contd.

## Indirect Delivery

- If the destination host is not on the same network as the deliverer, the packet is delivered indirectly.
- In an indirect delivery, the packet goes from router to router until it reaches the one connected to the same physical network as its final destination.



- A delivery always involves one direct delivery but zero or more indirect deliveries.
- The last delivery is always a direct delivery.



# Forwarding

- Forwarding means to place the packet in its route to its destination.
- Forwarding requires a host or a router to have a routing table.
- When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination.
- This simple solution is impossible today in an internetwork such as the Internet
  - because the number of entries needed in the routing table would make table lookups inefficient.

# Forwarding Techniques

- Several techniques can make the size of the routing table manageable and also handle issues such as security.

## Next-Hop Method Versus Route Method

- One technique to reduce the contents of a routing table is called the next-hop method.
- In this technique, the routing table holds only the address of the next hop instead of information about the complete route (route method).
- The entries of a routing table must be consistent with one another.

a. Routing tables based on route

Destination	Route
Host B	R1, R2, host B

Destination	Route
Host B	R2, host B

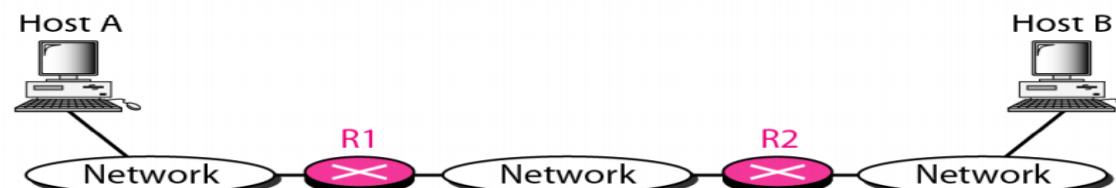
Destination	Route
Host B	Host B

b. Routing tables based on next hop

Destination	Next hop
Host B	R1

Destination	Next hop
Host B	R2

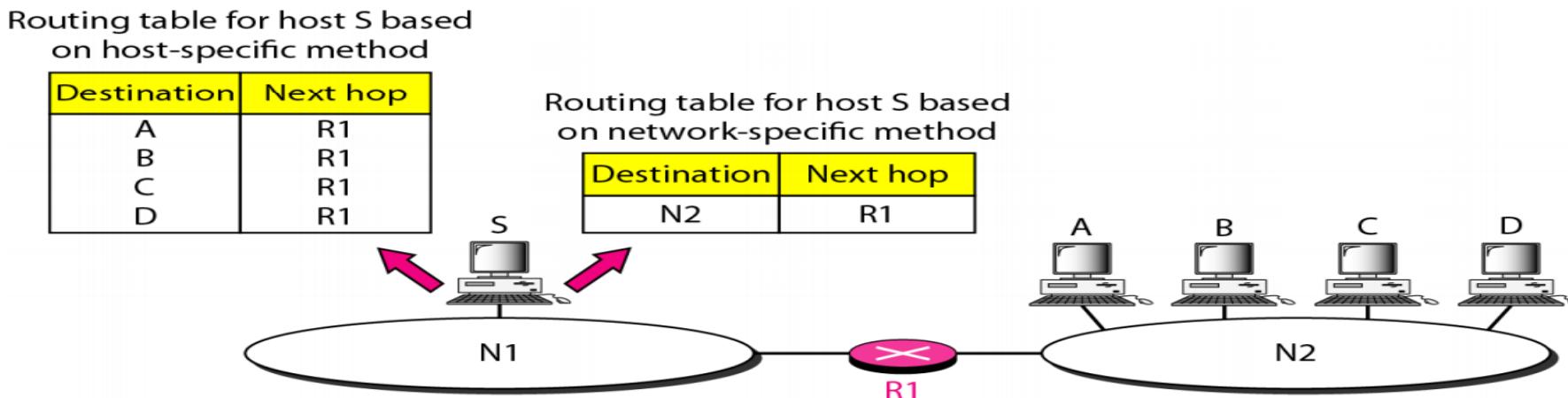
Destination	Next hop
Host B	---



# Forwarding Techniques ... Contd.

## Network-Specific Method Versus Host-Specific Method

- A second technique to reduce the routing table and simplify the searching process is called the **network-specific method**.
- Instead of having an entry for every destination host connected to the same physical network (host-specific method), only one entry that defines the address of the destination network itself.
- Treat all hosts connected to the same network as one single entity.
- E.g., if 1000 hosts are attached to the same network, only one entry exists in the routing table instead of 1000.

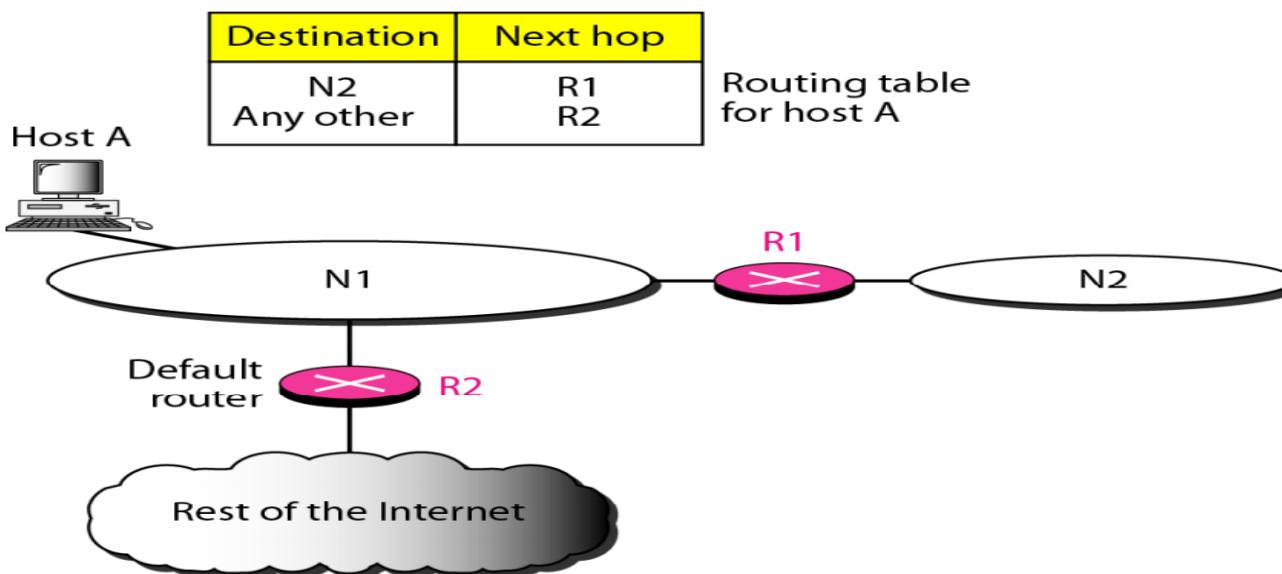


Host-specific routing is used for purposes such as checking the route or providing security measures.

# Forwarding Techniques ... Contd.

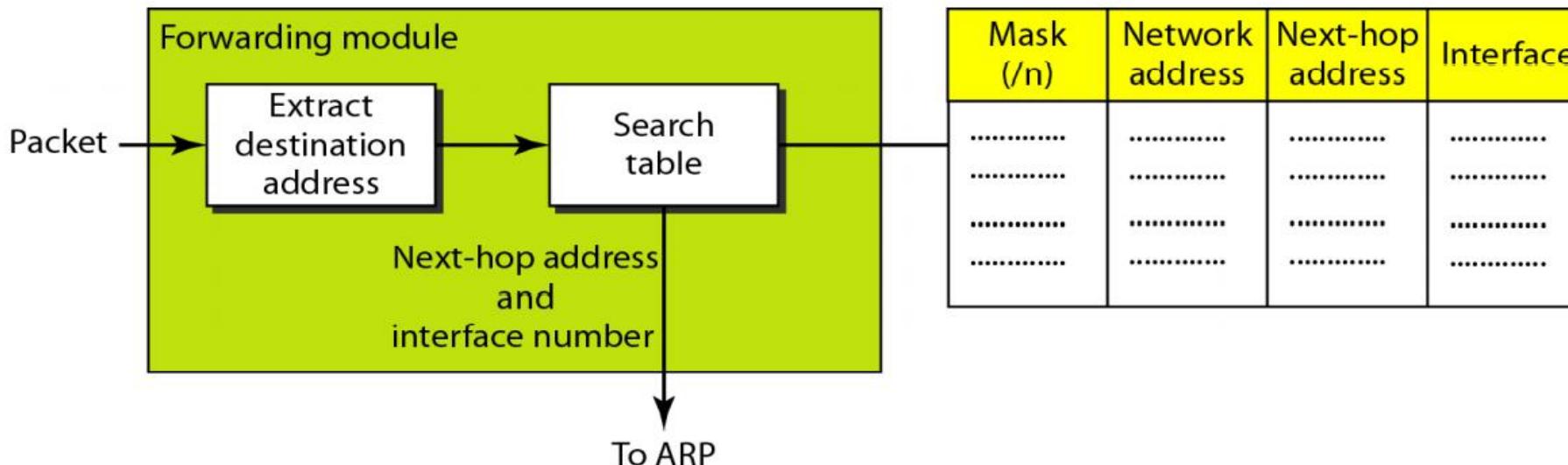
## Default Method

- Host A is connected to a network with two routers.
- Router R1 routes the packets to hosts connected to network N2.
- For the rest of the Internet, router R2 is used.
- So instead of listing all networks in the entire Internet, host A can just have one entry called the **default** (normally defined as network address **0.0.0.0**).



# Forwarding Process

- Assume that hosts and routers use classless addressing because classful addressing can be treated as a special case of classless addressing.
- In classless addressing, the routing table needs to have one row of information for each block involved.
- The table needs to be searched based on the network address (first address in the block).
- Unfortunately, the destination address in the packet gives no clue about the network address.
- To solve the problem, we need to include the mask (/n) in the table; we need to have an extra column that includes the mask for the corresponding block.



Need at least four columns in our routing table; usually there are more.



# Routing Table

- A host or a router has a routing table with an entry for each destination, or a combination of destinations, to route IP packets.
- The routing table can be either static or dynamic.

## Static Routing Table

- A static routing table contains information entered manually.
- The administrator enters the route for each destination into the table.
- When a table is created, it cannot update automatically when there is a change in the Internet.
- The table must be manually altered by the administrator.
- A static routing table can be used in a small internet that does not change very often, or in an experimental internet for troubleshooting.
- It is poor strategy to use a static routing table in a big internet such as the Internet.



# Routing Table ... Contd.

## Dynamic Routing Table

- A dynamic routing table is updated periodically by using one of the dynamic routing protocols such as RIP, OSPF, or BGP.
- Whenever there is a change in the Internet, such as a shutdown of a router or breaking of a link, the dynamic routing protocols update all the tables in the routers (and eventually in the host) automatically.
- The routers in a big internet such as the Internet need to be updated dynamically for efficient delivery of the IP packets.



# Routing Table ... Contd.

## Format

- A routing table for classless addressing has a minimum of four columns.
- However, some of today's routers have even more columns.
- The number of columns is vendor-dependent, and not all columns can be found in all routers.

Mask	Network address	Next-hop address	Interface	Flags	Reference count	Use
.....	.....	.....	.....	.....	.....	.....

- **Mask** - This field defines the mask applied for the entry.
- **Network address** - This field defines the network address to which the packet is finally delivered. In the case of host-specific routing, this field defines the address of the destination host.
- **Next-hop address** - This field defines the address of the next-hop router to which the packet is delivered.
- **Interface** - This field shows the name of the interface.



# Routing Table ... Contd.

**Flags** - This field defines up to five flags.

- Flags are on/off switches that signify either presence or absence.
- The five flags are U (up), G (gateway), H (host-specific), D (added by redirection), and M (modified by redirection).

## a. U (up)

- The U flag indicates the router is up and running.
- If this flag is not present, it means that the router is down.
- The packet cannot be forwarded and is discarded.

## b. G (gateway)

- The G flag means that the destination is in another network.
- The packet is delivered to the next-hop router for delivery (indirect delivery).
- When this flag is missing, it means the destination is in this network (direct delivery).

## c. H (host-specific)

- The H flag indicates that the entry in the network address field is a host-specific address.
- When it is missing, it means that the address is only the network address of the destination.



# Routing Table ... Contd.

## d. D (added by redirection)

- The D flag indicates that routing information for this destination has been added to the host routing table by a redirection message from ICMP.

## e. M (modified by redirection)

- The M flag indicates that the routing information for this destination has been modified by a redirection message from ICMP.
- **Reference count** - This field gives the number of users of this route at the moment.
- E.g., if five people at the same time are connecting to the same host from this router, the value of this column is 5.
- **Use** - This field shows the number of packets transmitted through this router for the corresponding destination.



# Summary

## Discussed about

- Introduction
- Delivery
- Forwarding
- Forwarding Techniques
- Forwarding Process
- Routing Table



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**

# Computer Networks

## BCSE308L

## Unicast Routing Protocols

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai



# Overview

- Introduction
- Optimization
- Intra and Inter-Domain Routing
- Popular Routing Protocols
- Summary



# Introduction

- A routing table can be either **static or dynamic**.
- A static table is one with manual entries.
- A dynamic table, on the other hand, is one that is updated automatically when there is a change somewhere in the internet.
- Today, an internet needs dynamic routing tables.
- The tables need to be updated as soon as there is a change in the internet.
- For instance, they need to be updated when a router is down, and they need to be updated whenever a better route has been found.

# Introduction ... Contd.

- Routing protocols have been created in response to the demand for dynamic routing tables.
- A routing protocol is a combination of rules and procedures that lets routers in the internet inform each other of changes.
- It allows routers to share whatever they know about the internet or their neighborhood.
- The routing protocols also include procedures for combining information received from other routers.



# Optimization

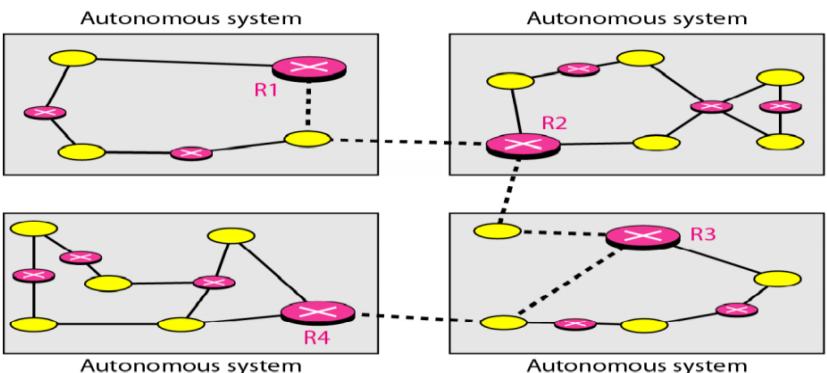
- A router receives a packet from a network and passes it to another network.
- A router is usually attached to several networks.
- When it receives a packet, to which network should it pass the packet?
  - The decision is based on optimization.
- Which of the available pathways is the optimum pathway?
- What is the definition of the term optimum?
  - One approach is to assign a **cost** for passing through a network, metric.
  - However, the metric assigned to each network depends on the type of protocol.
  - Some simple protocols, such as the **Routing Information Protocol (RIP)**, treat all networks as equals.
  - The cost of passing through a network is the same; it is one hop count.
  - So if a packet passes through 10 networks to reach the destination, the total cost is 10 hop counts.

# Optimization ... Contd.

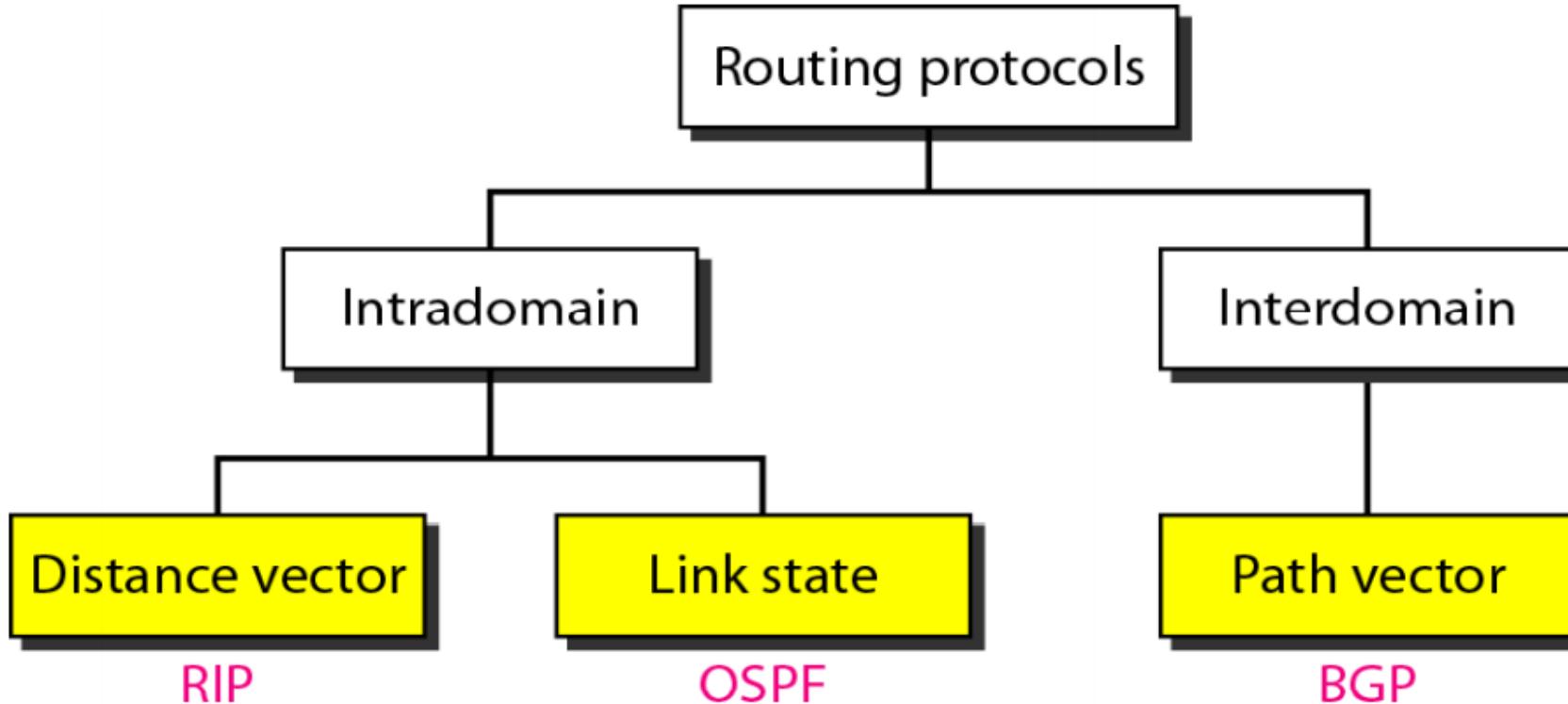
- Other protocols, such as **Open Shortest Path First (OSPF)**, allow the administrator to assign a cost for passing through a network based on the **type of service** required.
- A route through a network can have different costs (metrics).
- E.g., if maximum throughput is the desired type of service, a satellite link has a lower metric than a fiber-optic line.
  - If minimum delay is the desired type of service, a fiber-optic line has a lower metric than a satellite link.
- Routers use routing tables to help decide the best route.
- OSPF protocol allows each router to have several routing tables based on the required type of service.
- Other protocols define the metric in a totally different way.
- In the **Border Gateway Protocol (BGP)**, the criterion is the **policy**, which can be set by the administrator.
- The policy defines what paths should be chosen.

# Intra and Inter-Domain Routing

- Today, an internet can be so large that one routing protocol cannot handle the task of updating the routing tables of all routers.
- For this reason, an internet is divided into autonomous systems.
- An **autonomous system (AS)** is a group of networks and routers under the authority of a single administration.
- Routing inside an autonomous system is referred to as **intradomain routing**.
- Routing between autonomous systems is referred to as **interdomain routing**.
- Each autonomous system can choose one or more intradomain routing protocols to handle routing inside the autonomous system.
- However, only one interdomain routing protocol handles routing between autonomous systems.



# Popular Routing Protocols



- Routing Information Protocol (RIP) is an implementation of the distance vector protocol.
- Open Shortest Path First (OSPF) is an implementation of the link state protocol.
- Border Gateway Protocol (BGP) is an implementation of the path vector protocol.



# Summary

## Discussed about

- Introduction
- Optimization
- Intra and Inter-Domain Routing
- Popular Routing Protocols



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**

# Computer Networks

## BCSE308L

## Distance Vector Routing

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai

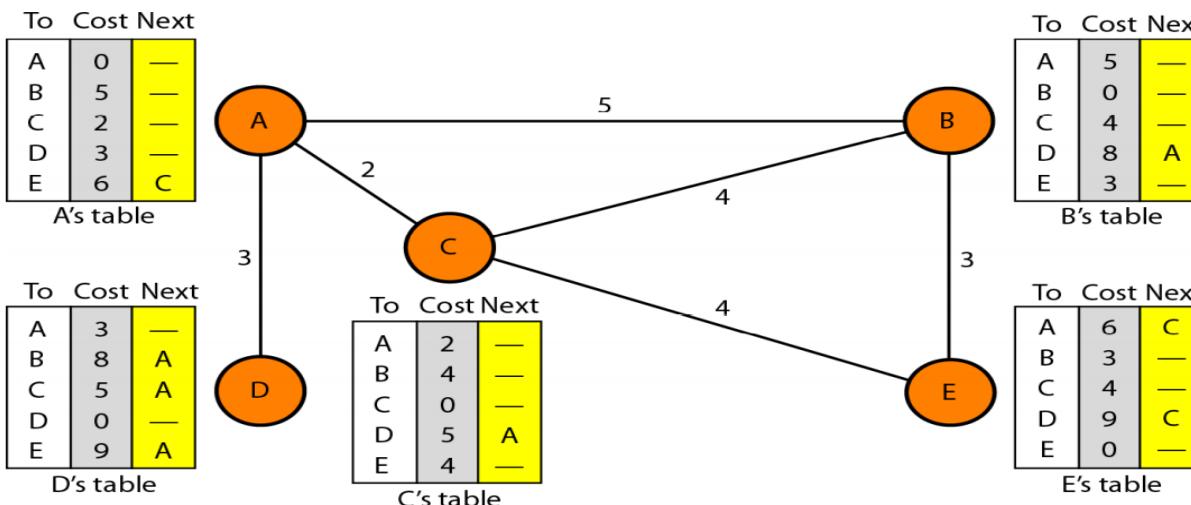


# Overview

- Introduction
- Sharing
- Updating
- When to Share?
- Two-Node Instability
- Three-Node Instability
- Routing Information Protocol
- Practice Questions
- Summary

# Introduction

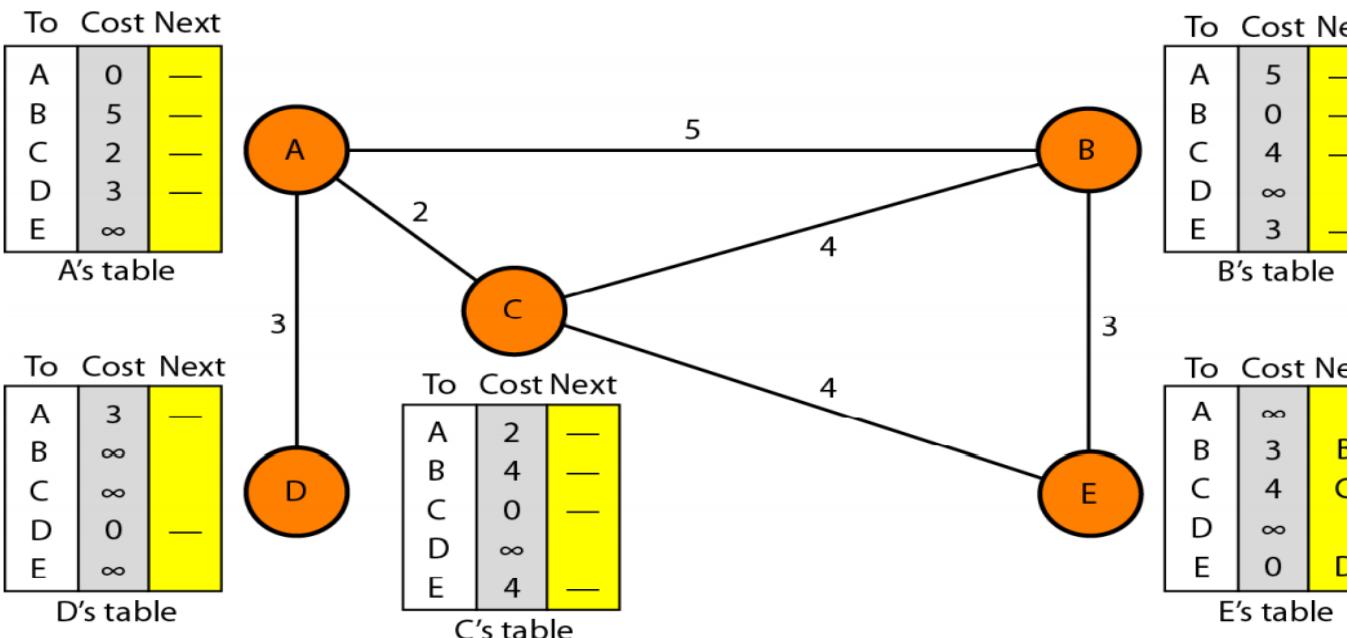
- In distance vector routing, the least-cost route between any two nodes is the route with minimum distance.
- In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node.
- The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).
- We can think of nodes as the cities in an area and the lines as the roads connecting them.
- A table can show a tourist the minimum distance between cities.



- The table for node A shows how we can reach any node from this node.
- For example, our least cost to reach node E is 6.
- The route passes through C.

# Initialization

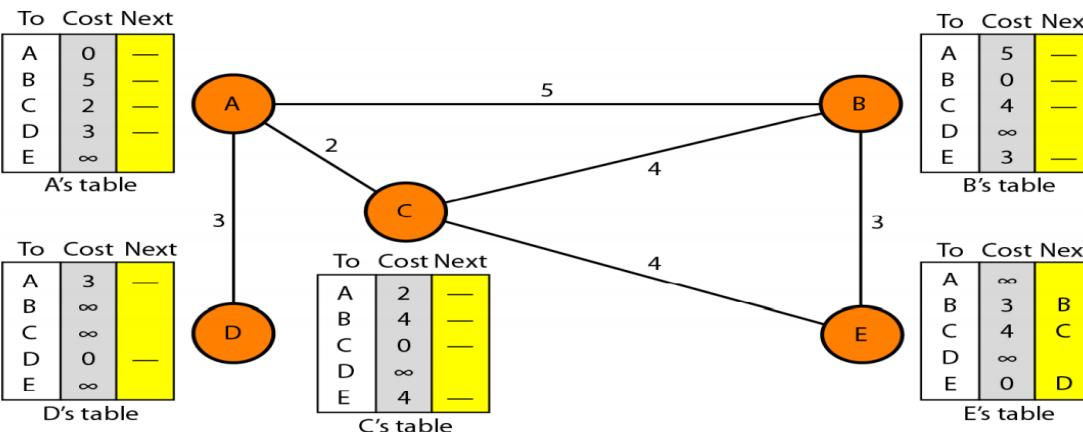
- Each node knows how to reach any other node and the cost.
- At the beginning, however, this is not the case.
- Each node can know only the distance between itself and its immediate neighbors, those directly connected to it.
- So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors.



The distance for any entry that is not a neighbor is marked as infinite (unreachable).

# Sharing

- The whole idea of distance vector routing is the sharing of information between neighbors.
- Although node A does not know about node E, node C does.
- So if node C shares its routing table with A, node A can also know how to reach node E.
- Node C does not know how to reach node D, but node A does.
- If node A shares its routing table with node C, node C also knows how to reach node D.
- Nodes A and C, as immediate neighbors, can improve their routing tables if they help each other.



# Sharing ... Contd.

How much of the table must be shared with each neighbor?

- A node is not aware of a neighbor's table.
- The best solution for each node is to send its entire table to the neighbor and let the neighbor decide what part to use and what part to discard.
- However, the third column of a table (next stop) is not useful for the neighbor.
- When the neighbor receives a table, this column needs to be replaced with the sender's name.
- If any of the rows can be used, the next node is the sender of the table.
- A node therefore can send only the first two columns of its table to any neighbor.
- Sharing here means sharing only the first two columns.

# Updating

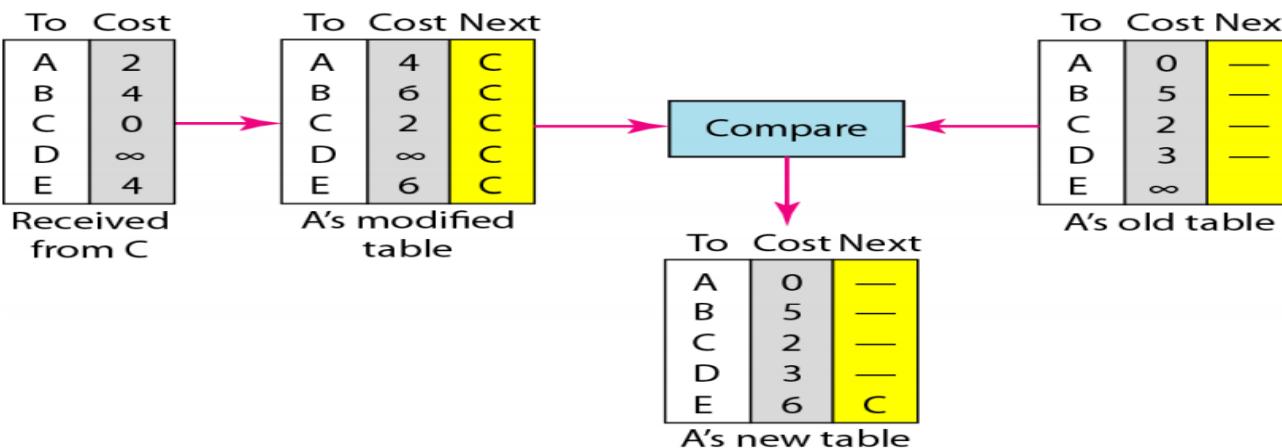
When a node receives a two-column table from a neighbor, it needs to update its routing table.

Updating takes three steps:

1. The receiving node needs to add the cost between itself and the sending node to each value in the second column.
  - If node C claims that its distance to a destination is  $x$  mi, and the distance between A and C is  $y$  mi, then the distance between A and that destination, via C, is  $x + y$  mi.
2. The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row.
  - The sending node is the next node in the route.

# Updating ... Contd.

3. The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.
- If the next-node entry is different, the receiving node chooses the row with the smaller cost.
    - If there is a tie, the old one is kept.
  - If the next-node entry is the same, the receiving node chooses the new row.
    - For example, suppose node C has previously advertised a route to node X with distance 3.
    - Suppose that now there is no path between C and X; node C now advertises this route with a distance of infinity.
    - Node A must not ignore this value even though its old entry is smaller.
    - The old route does not exist any more.
    - The new route has a distance of infinity.



# Updating ... Contd.

## Points to emphasize:

- First, when any number is added to infinity, the result is still infinity.
- Second, the modified table shows how to reach A from A via C.
  - If A needs to reach itself via C, it needs to go to C and come back, a distance of 4.
- Third, the only benefit from this updating of node A is the last entry, how to reach E.
  - Node A did not know how to reach E (distance of infinity); now it knows that the cost is 6 via C.
- Each node can update its table by using the tables received from other nodes.
- If there is no change in the network itself, such as a failure in a link, each node reaches a stable condition in which the contents of its table remains the same.

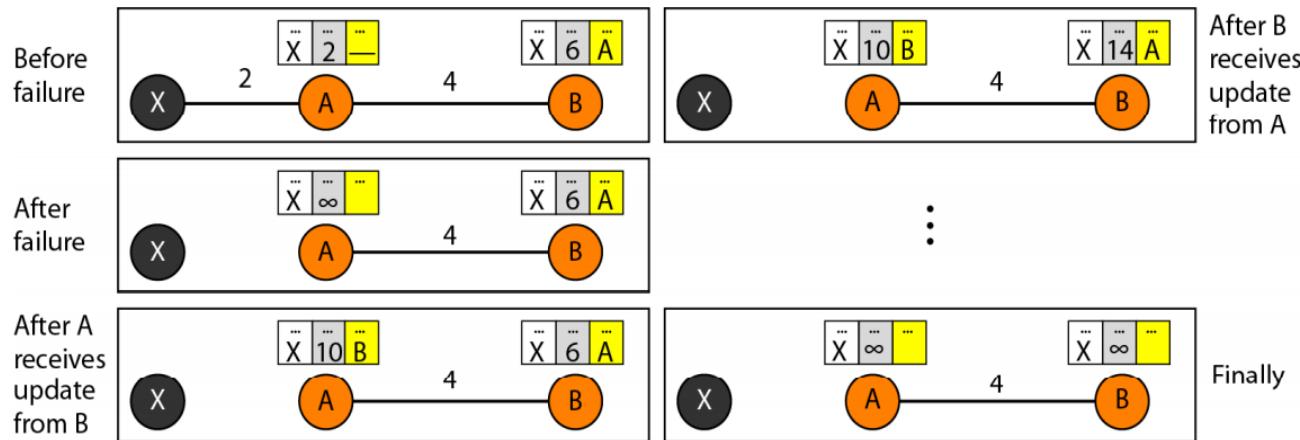
# When to Share?

When does a node send its partial routing table (only two columns) to all its immediate neighbors?

- The table is sent both periodically and when there is a change in the table.
- **Periodic Update**
- A node sends its routing table, normally every 30 s, in a periodic update.
- The period depends on the protocol that is using distance vector routing.
- **Triggered Update**
- A node sends its two-column routing table to its neighbors anytime there is a change in its routing table.
- The change can result from the following:
  1. A node receives a table from a neighbor, resulting in changes in its own table after updating.
  2. A node detects some failure in the neighboring links which results in a distance change to infinity.

# Two-Node Loop Instability

A problem with distance vector routing is instability, which means that a network using this protocol can become unstable.



- At the beginning, both nodes A and B know how to reach node X.
- But suddenly, the link between A and X fails.
- Node A changes its table.
- If A can send its table to B immediately, everything is fine.
- The system becomes unstable if B sends its routing table to A before receiving A's routing table.
- Node A receives the update and, assuming that B has found a way to reach X, immediately updates its routing table.

- Based on the triggered update strategy, A sends its new update to B.
- Now B thinks that something has been changed around A and updates its routing table.
- The cost of reaching X increases gradually until it reaches infinity.
- At this moment, both A and B know that X cannot be reached.
- During this time the system is not stable.
- Node A thinks that the route to X is via B; node B thinks that the route to X is via A.
- If A receives a packet destined for X, it goes to B and then comes back to A.
- Similarly, if B receives a packet destined for X, it goes to A and comes back to B.
- Packets bounce between A and B, creating a two-node loop problem.

# Two-Node Loop Instability ... Contd.

## Solutions for Instability

- **Defining Infinity**
  - The first obvious solution is to redefine infinity to a smaller number, such as 100.
  - For our previous scenario, the system will be stable in less than 20 updates.
  - Most implementations of the distance vector protocol define the distance between each node to be 1 and define 16 as infinity.
  - However, this means that the distance vector routing cannot be used in large systems.
  - The size of the network, in each direction, can not exceed 15 hops.
- **Split Horizon**
  - In this strategy, instead of flooding the table through each interface, each node sends only part of its table through each interface.
  - If, according to its table, node B thinks that the optimum route to reach X is via A, it does not need to advertise this piece of information to A; the information has come from A (A already knows).
  - Taking information from node A, modifying it, and sending it back to node A creates the confusion.
  - In our scenario, node B eliminates the last line of its routing table before it sends it to A.
  - In this case, node A keeps the value of infinity as the distance to X.
  - Later when node A sends its routing table to B, node B also corrects its routing table.
  - The system becomes stable after the first update: both node A and B know that X is not reachable.

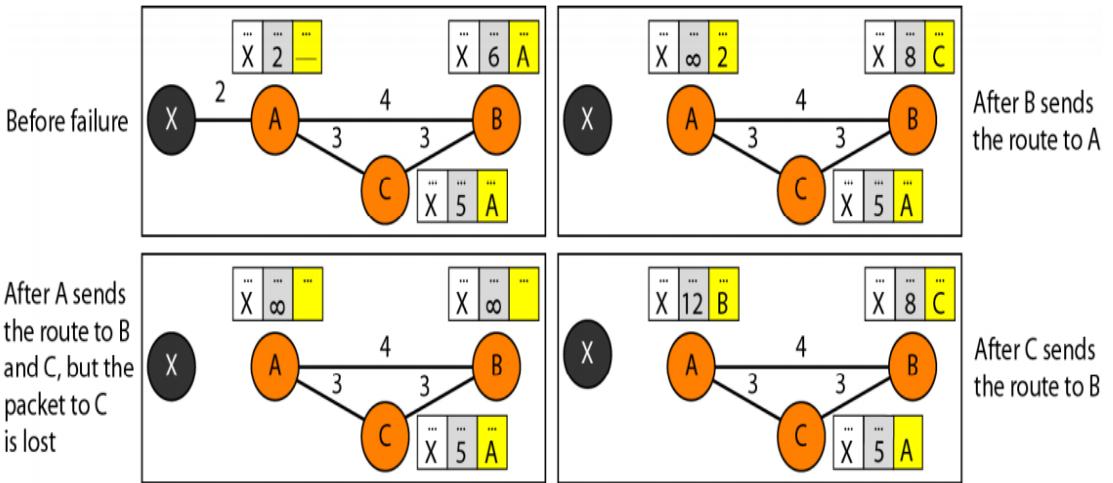
# Two-Node Loop Instability ... Contd.

- **Split Horizon and Poison Reverse**

- Using the split horizon strategy has one drawback.
- Normally, the distance vector protocol uses a timer, and if there is no news about a route, the node deletes the route from its table.
- When node B in the previous scenario eliminates the route to X from its advertisement to A, node A cannot guess that this is due to the split horizon strategy (the source of information was A) or because B has not received any news about X recently.
- The split horizon strategy can be combined with the poison reverse strategy.
- Node B can still advertise the value for X, but if the source of information is A, it can replace the distance with infinity as a warning: "Do not use this value; what I know about this route comes from you."

# Three-Node Loop Instability

- The two-node instability can be avoided by using the split horizon strategy combined with poison reverse.
- However, if the instability is between three nodes, stability cannot be guaranteed.



- Suppose, after finding that X is not reachable, node A sends a packet to B and C to inform them of the situation.
- Node B immediately updates its table, but the packet to C is lost in the network and never reaches C.
- Node C remains in the dark and still thinks that there is a route to X via A with a distance of 5.
- After a while, node C sends to B its routing table, which includes the route to X.
- Node B is totally fooled here.

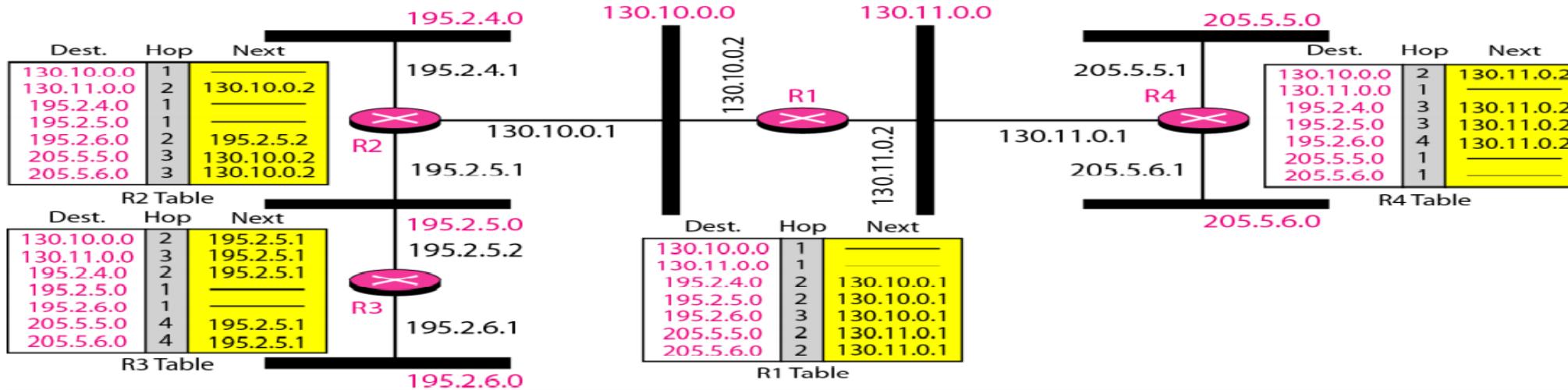
- It receives information on the route to X from C, and according to the algorithm, it updates its table, showing the route to X via C with a cost of 8.
- This information has come from C, not from A, so after awhile node B may advertise this route to A.
- Now A is fooled and updates its table to show that A can reach X via B with a cost of 12.
- The loop continues; now A advertises the route to X to C, with increased cost, but not to B.
- Node C then advertises the route to B with an increased cost.
- Node B does the same to A. And so on.
- The loop stops when the cost in each node reaches infinity.



# Routing Information Protocol

- The Routing Information Protocol (RIP) is an intradomain routing protocol used inside an autonomous system.
- It is a very simple protocol based on distance vector routing.
- RIP implements distance vector routing directly with some considerations:
  1. In an autonomous system, we are dealing with routers and networks (links). The routers have routing tables; networks do not.
  2. The destination in a routing table is a network, which means the first column defines a network address.
  3. The metric used by RIP is very simple; the distance is defined as the number of links (networks) to reach the destination. For this reason, the metric in RIP is called a hop count.
  4. Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.
  5. The next-node column defines the address of the router to which the packet is to be sent to reach its destination.

# Routing Information Protocol ... Contd.

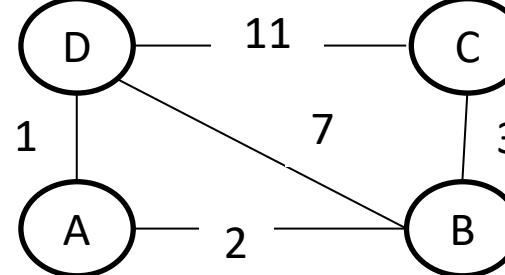


## Routing table for R1

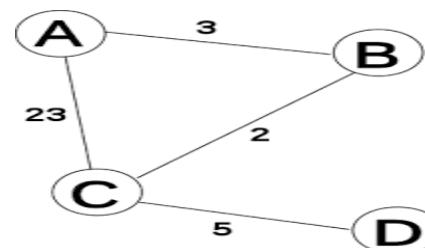
- The table has seven entries to show how to reach each network in the autonomous system.
- Router R1 is directly connected to networks 130.10.0.0 and 130.11.0.0, which means that there are no next-hop entries for these two networks.
- To send a packet to one of the three networks at the far left, router R1 needs to deliver the packet to R2.
- The next-node entry for these three networks is the interface of router R2 with IP address 130.10.0.1.
- To send a packet to the two networks at the far right, router R1 needs to send the packet to the interface of router R4 with IP address 130.11.0.1.

# Practice Questions

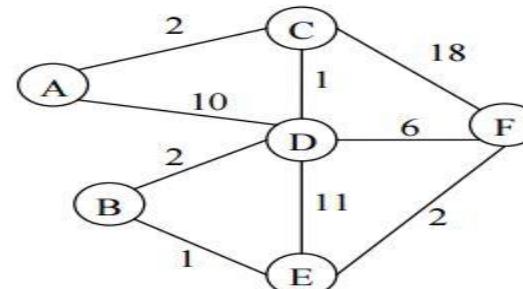
- 1) Compute the routing table of the nodes A, B, C, and D in the following network using Distance Vector Routing.



- 2) Compute the routing table of the nodes A, B, C, and D in the following network using Distance Vector Routing.



- 3) Compute the routing table of the nodes A, B, C, D, E, and F in the following network using Distance Vector Routing.





# Summary

## Discussed about

- Introduction
- Sharing
- Updating
- When to Share?
- Two-Node Instability
- Three-Node Instability
- Routing Information Protocol
- Practice Questions



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**

# Computer Networks

## BCSE308L

### Link State Routing

Dr. Bhuvaneswari Amma N.G.  
Assistant Professor (Sr.)  
SCOPE, VIT Chennai

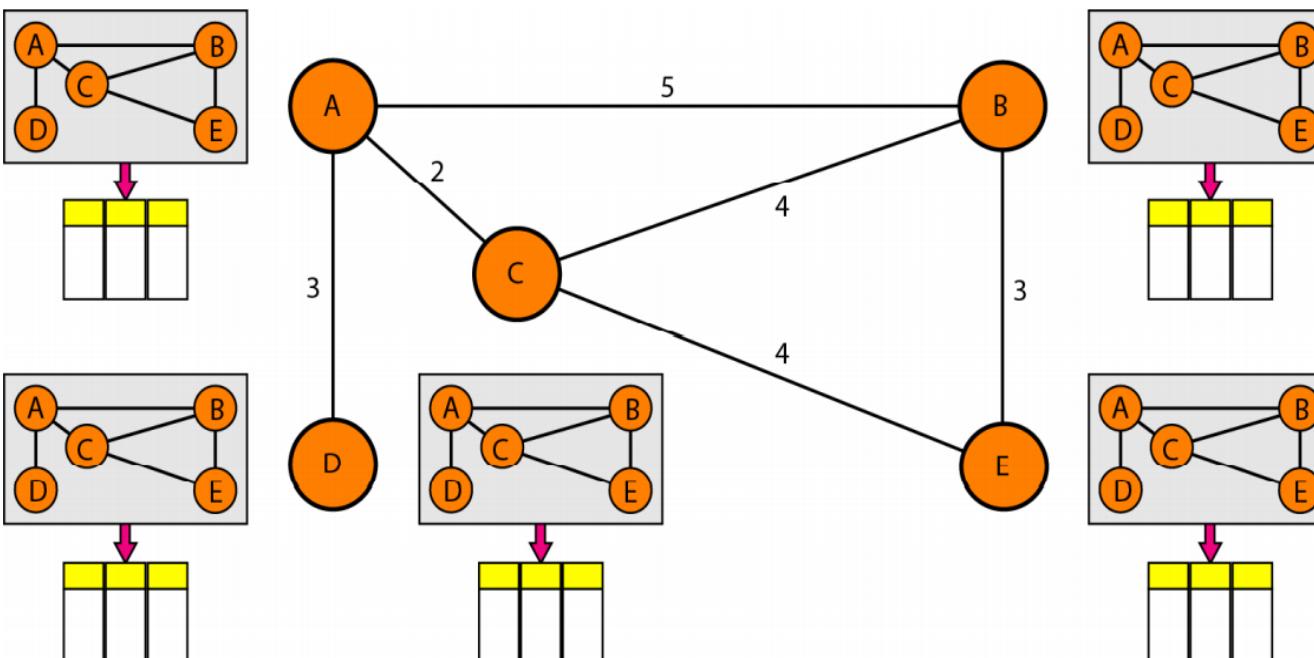


# Overview

- Introduction
- Building Routing Tables
- Open Shortest Path First Protocol
- Practice Questions
- Summary

# Introduction

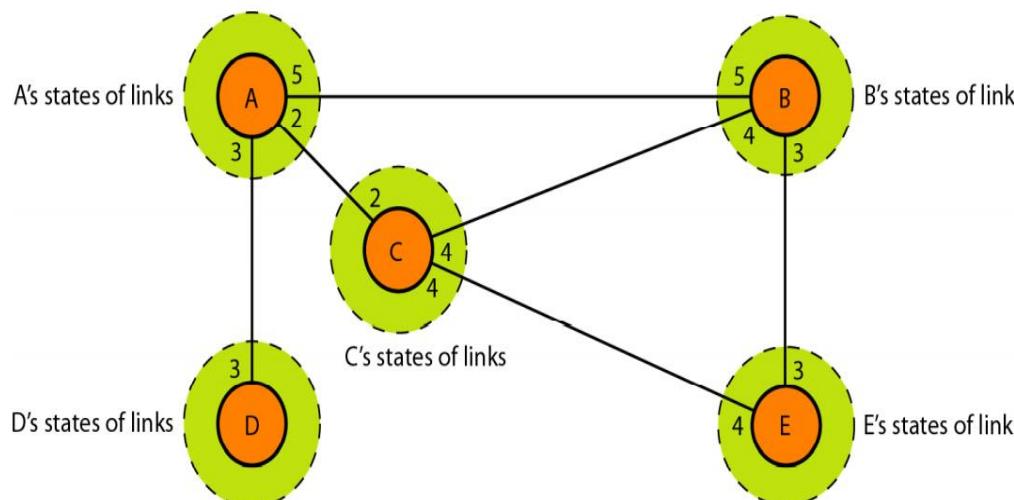
- Link state routing has a different philosophy from that of distance vector routing.
- In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including
  - the type, cost (metric), and condition of the links (up or down)-the node can use **Dijkstra's algorithm** to build a routing table.



- The figure shows a simple domain with five nodes.
- Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology.
- This is analogous to a **city map**.
- While each person may have the same map, each needs to take a different route to reach her specific destination.

# Introduction ... Contd.

- The topology must be dynamic, representing the latest state of each node and each link.
- If there are changes in any point in the network (a link is down, for example), the topology must be updated for each node.
- How can a common topology be dynamic and stored in each node?
  - No node can know the topology at the beginning or after a change somewhere in the network.
  - Link state routing is based on the assumption that, although the global knowledge about the topology is not clear, each node has partial knowledge: it knows the state (type, condition, and cost) of its links.
  - The whole topology can be compiled from the partial knowledge of each node.



- Node A knows that it is connected to node B with metric 5, to node C with metric 2, and to node D with metric 3.
- Node C knows that it is connected to node A with metric 2, to node B with metric 4, and to node E with metric 4.
- Node D knows that it is connected only to node A with metric 3, and so on.
- Although there is an overlap in the knowledge, the overlap guarantees the creation of a common topology-a picture of the whole domain for each node.

# Building Routing Tables

- In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node.
  1. Creation of the states of the links by each node, called the link state packet (LSP).
  2. Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.
  3. Formation of a shortest path tree for each node.
  4. Calculation of a routing table based on the shortest path tree.

# Building Routing Tables ... Contd.

## Creation of Link State Packet (LSP)

- A link state packet can carry a large amount of information.
- For the moment, however, we assume that it carries a minimum amount of data: **the node identity, the list of links, a sequence number, and age.**
- The first two, node identity and the list of links, are needed to make the topology.
- The third, sequence number, facilitates flooding and distinguishes new LSPs from old ones.
- The fourth, age, prevents old LSPs from remaining in the domain for a long time.
- LSPs are generated on two occasions:
  1. When there is a change in the topology of the domain.
    - Triggering of LSP dissemination is the main way of quickly informing any node in the domain to update its topology.
  2. On a periodic basis.
    - The period in this case is much longer compared to distance vector routing.
    - There is no actual need for this type of LSP dissemination.
    - It is done to ensure that old information is removed from the domain.
    - The timer set for periodic dissemination is normally in the range of 60 min or 2 h based on the implementation.
    - A longer period ensures that flooding does not create too much traffic on the network.

# Building Routing Tables ... Contd.

## Flooding of LSPs

- After a node has prepared an LSP, it must be disseminated to all other nodes, not only to its neighbors.
- The process is called flooding and based on the following:
  1. The creating node sends a copy of the LSP out of each interface.
  2. A node that receives an LSP compares it with the copy it may already have.
- If the newly arrived LSP is older than the one it has (found by checking the sequence number), it discards the LSP.
- If it is newer, the node does the following:
  - a. It discards the old LSP and keeps the new one.
  - b. It sends a copy of it out of each interface except the one from which the packet arrived.
    - This guarantees that flooding stops somewhere in the domain (where a node has only one interface).



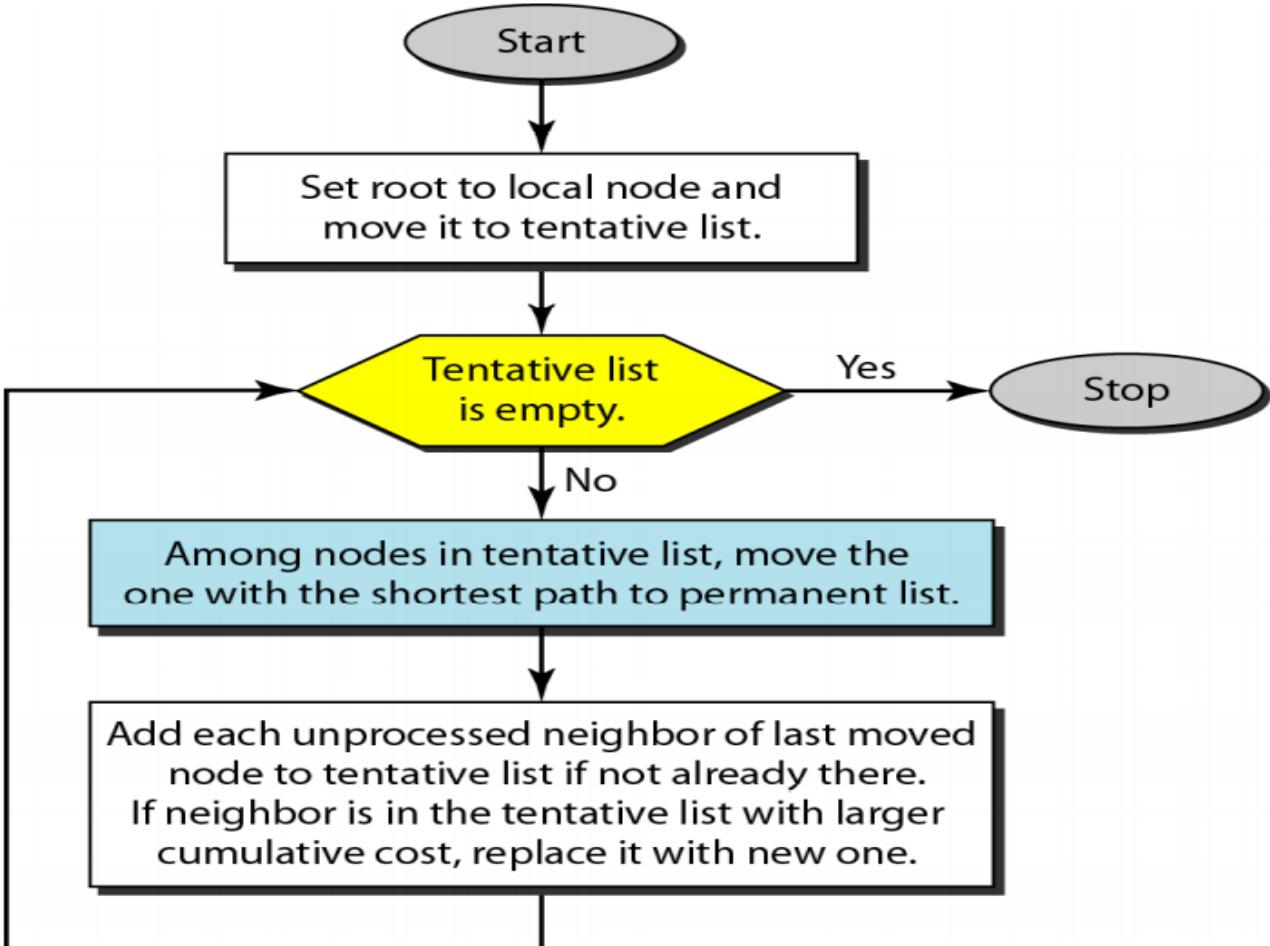
# Building Routing Tables ... Contd.

## Formation of Shortest Path Tree: Dijkstra Algorithm

- After receiving all LSPs, each node will have a copy of the whole topology.
- However, **the topology is not sufficient to find the shortest path to every other node; a shortest path tree is needed.**
- A tree is a graph of nodes and links; one node is called the root.
- All other nodes can be reached from the root through only one single route.
- A shortest path tree is a tree in which the path between the root and every other node is the shortest.
- What we need for each node is a shortest path tree with that node as the root.
- The Dijkstra's algorithm creates a shortest path tree from a graph.
- The algorithm divides the nodes into two sets: **tentative and permanent**.
- It finds the neighbors of a current node, makes them tentative, examines them, and if they pass the criteria, makes them permanent.

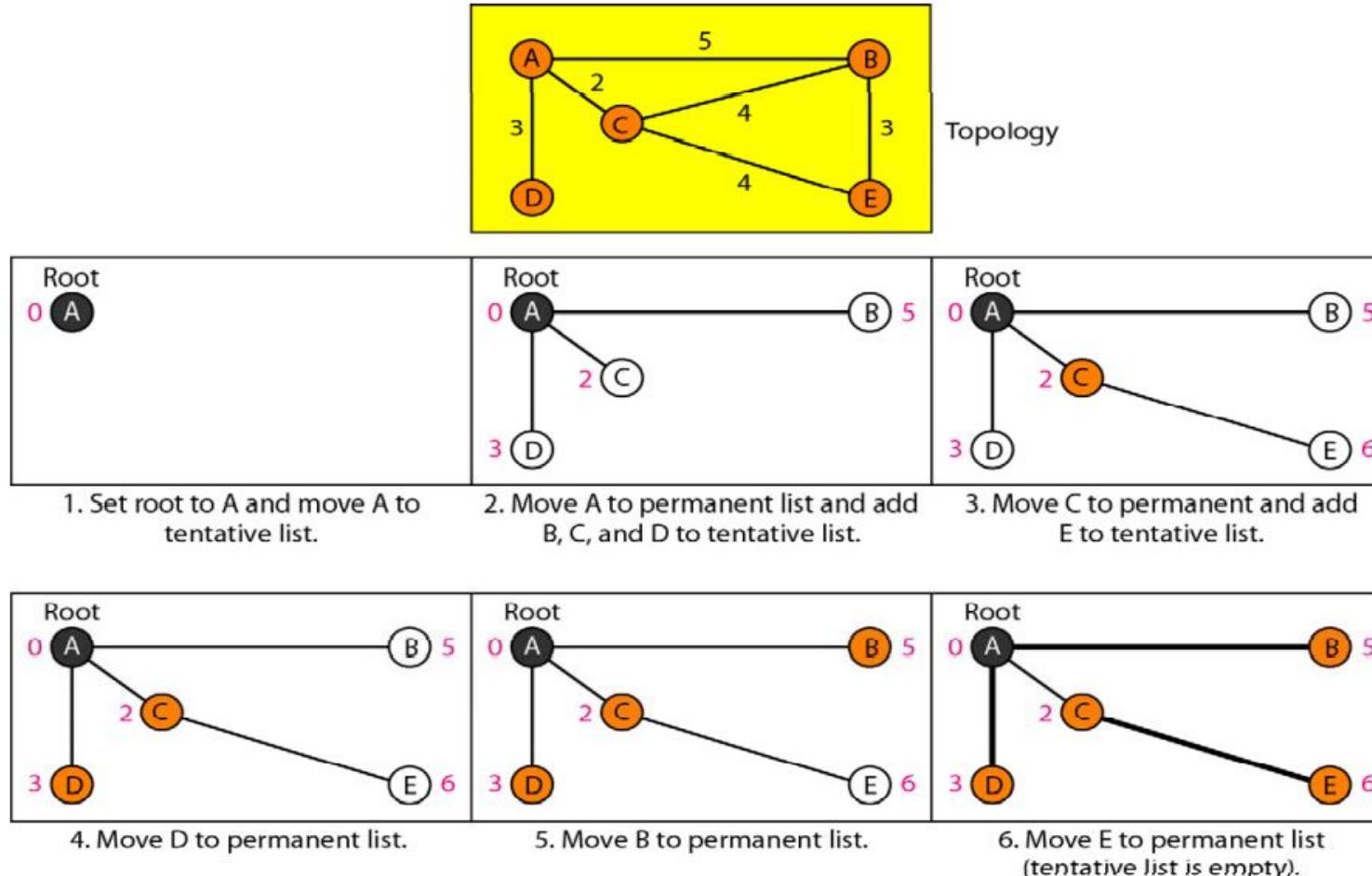
# Building Routing Tables ... Contd.

## Dijkstra's Algorithm



# Building Routing Tables ... Contd.

## Example of Formation of Shortest Path Tree



- To find the shortest path in each step, we need the cumulative cost from the root to each node, which is shown next to the node.
- At the end of each step, we show the permanent (filled circles) and the tentative (open circles) nodes and lists with the cumulative costs.

# Building Routing Tables ... Contd.

1. We make node A the root of the tree and move it to the tentative list. Our two lists are

Permanent list: empty Tentative list: A(0)

2. Node A has the shortest cumulative cost from all nodes in the tentative list.

We move A to the permanent list and add all neighbors of A to the tentative list. Our new lists are

Permanent list: A(0) Tentative list: B(5), C(2), D(3)

3. Node C has the shortest cumulative cost from all nodes in the tentative list.

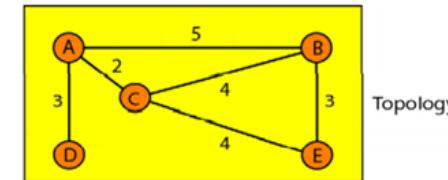
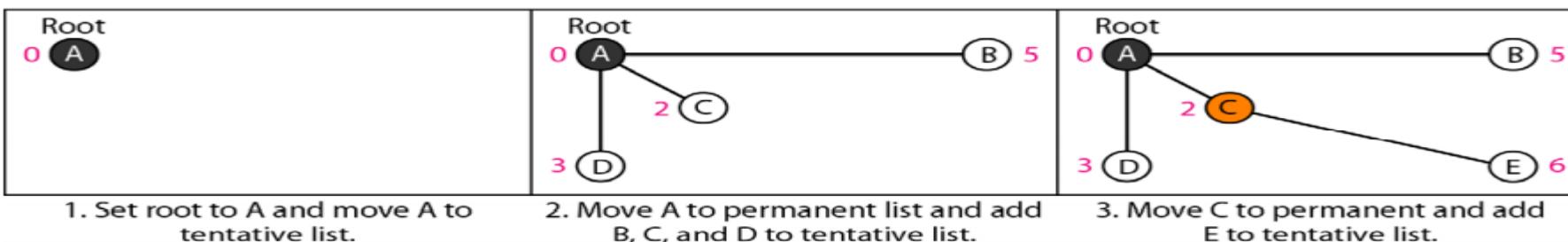
We move C to the permanent list. Node C has three neighbors, but node A is already processed, which makes the unprocessed neighbors just B and E.

However, B is already in the tentative list with a cumulative cost of 5.

Node A could also reach node B through C with a cumulative cost of 6.

Since 5 is less than 6, we keep node B with a cumulative cost of 5 in the tentative list and do not replace it. Our new lists are

Permanent list: A(0), C(2) Tentative list: B(5), D(3), E(6)



# Building Routing Tables ... Contd.

4. Node D has the shortest cumulative cost of all the nodes in the tentative list.

We move D to the permanent list. Node D has no unprocessed neighbor to be added to the tentative list.

Our new lists are Permanent list: A(0), C(2), D(3) Tentative list: B(5), E(6)

5. Node B has the shortest cumulative cost of all the nodes in the tentative list.

We move B to the permanent list.

We need to add all unprocessed neighbors of B to the tentative list (this is just node E).

However, E(6) is already in the list with a smaller cumulative cost.

The cumulative cost to node E, as the neighbor of B, is 8.

We keep node E(6) in the tentative list. Our new lists are Permanent list: A(0), B(5), C(2), D(3) Tentative list: E(6)

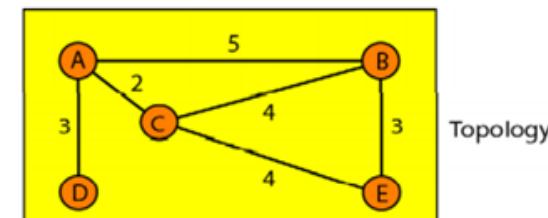
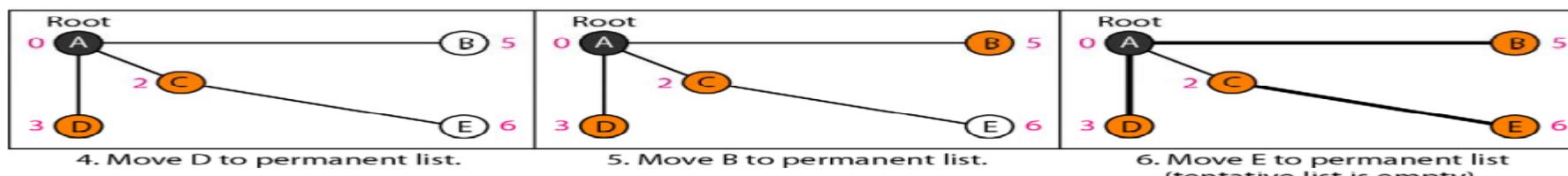
6. Node E has the shortest cumulative cost from all nodes in the tentative list.

We move E to the permanent list.

Node E has no neighbor. Now the tentative list is empty.

We stop; our shortest path tree is ready.

The final lists are Permanent list: A(0), B(5), C(2), D(3), E(6) Tentative list: empty



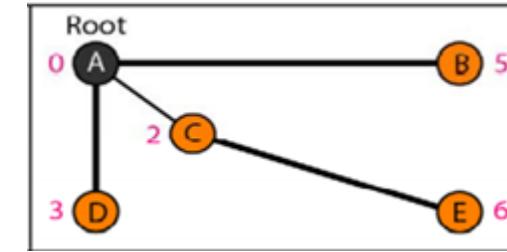
# Building Routing Tables ... Contd.

## Calculation of Routing Table from Shortest Path Tree

- Each node uses the shortest path tree protocol to construct its routing table.
- The routing table shows the cost of reaching each node from the root.

***Routing table for node A***

<i>Node</i>	<i>Cost</i>	<i>Next Router</i>
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C



# Open Shortest Path First Protocol

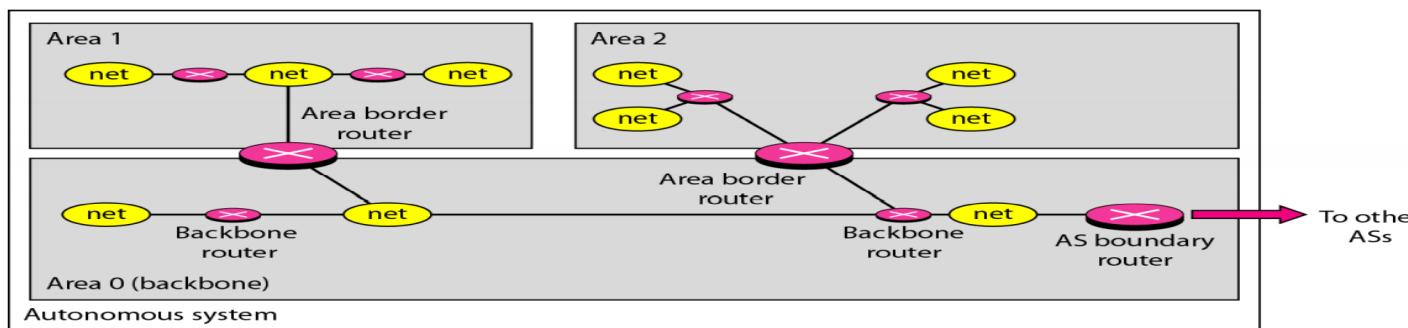
- The Open Shortest Path First or OSPF protocol is an intradomain routing protocol based on link state routing.
- Its domain is also an autonomous system.

## Areas

- To handle routing efficiently and in a timely manner, OSPF divides an autonomous system into areas.
- An area is a collection of networks, hosts, and routers all contained within an autonomous system.
- An autonomous system can be divided into many different areas.
- All networks inside an area must be connected.

# Open Shortest Path First Protocol ... Contd.

- Routers inside an area flood the area with routing information.
- At the border of an area, special routers called area border routers summarize the information about the area and send it to other areas.
- Among the areas inside an autonomous system is a special area called the backbone; all the areas inside an autonomous system must be connected to the backbone.
- The backbone serves as a primary area and the other areas as secondary areas.
- This does not mean that the routers within areas cannot be connected to each other, however.
- The routers inside the backbone are called the backbone routers.
- If, because of some problem, the connectivity between a backbone and an area is broken, a virtual link between routers must be created by an administrator to allow continuity of the functions of the backbone as the primary area.
- Each area has an area identification.
- The area identification of the backbone is zero.



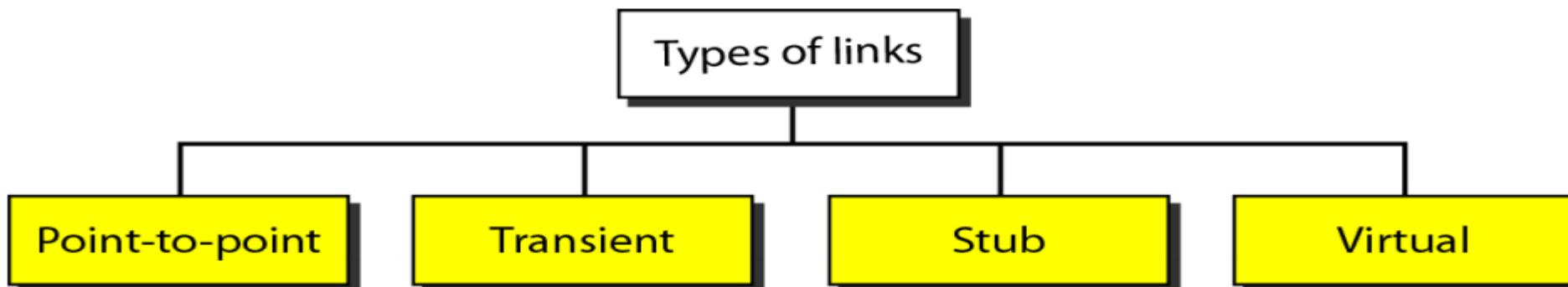
# Open Shortest Path First Protocol ... Contd.

## Metric

- The OSPF protocol allows the administrator to assign a cost, called the metric, to each route.
- The metric can be based on a type of service (minimum delay, maximum throughput, and so on).
- A router can have multiple routing tables, each based on a different type of service.

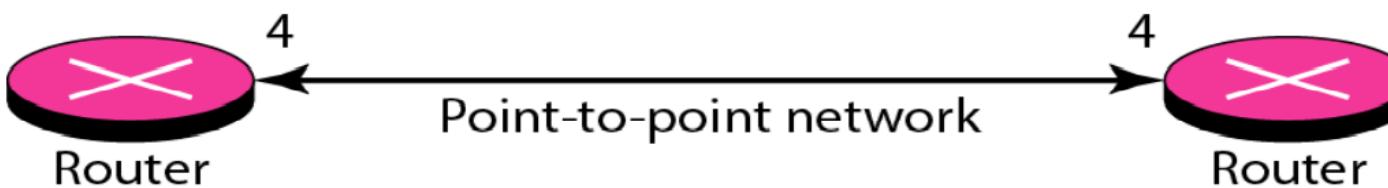
## Types of Links

- In OSPF terminology, a connection is called a link.
- Four types of links have been defined: **point-to-point**, **transient**, **stub**, and **virtual**.



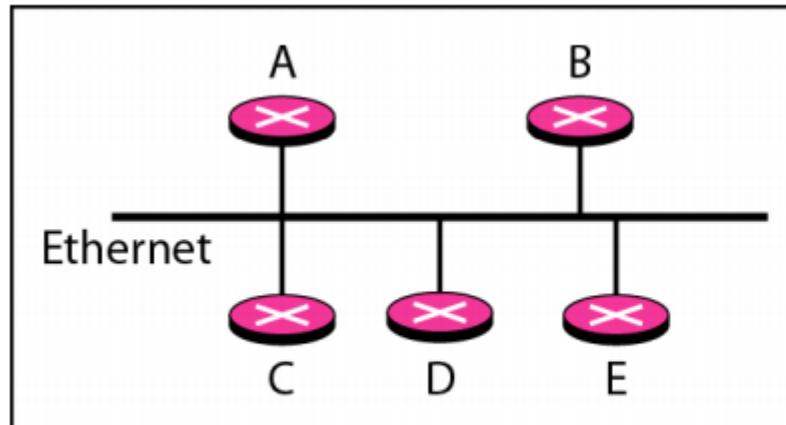
# Open Shortest Path First Protocol ... Contd.

- A **point-to-point link** connects two routers without any other host or router in between.
- The purpose of the link (network) is just to connect the two routers.
- An example of this type of link is two routers connected by a telephone line or a T line.
- There is no need to assign a network address to this type of link.
- Graphically, the routers are represented by nodes, and the link is represented by a bidirectional edge connecting the nodes.
- The metrics, which are usually the same, are shown at the two ends, one for each direction.
- Each router has only one neighbor at the other side of the link.

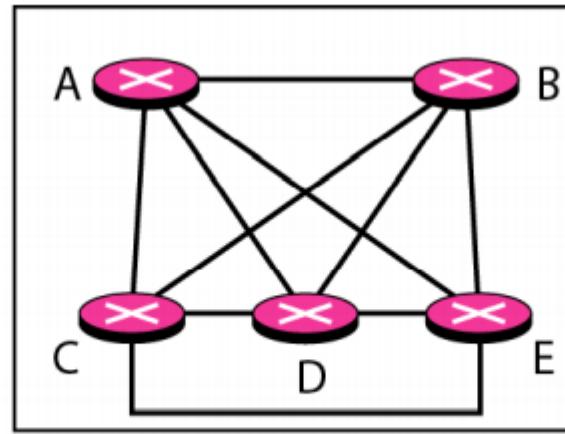


# Open Shortest Path First Protocol ... Contd.

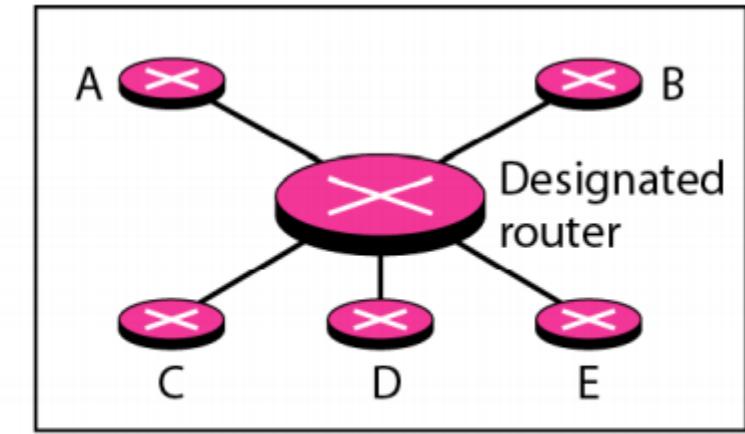
- A **transient link** is a network with several routers attached to it.
- The data can enter through any of the routers and leave through any router.
- All LANs and some WANs with two or more routers are of this type.
- In this case, each router has many neighbors.



a. Transient network



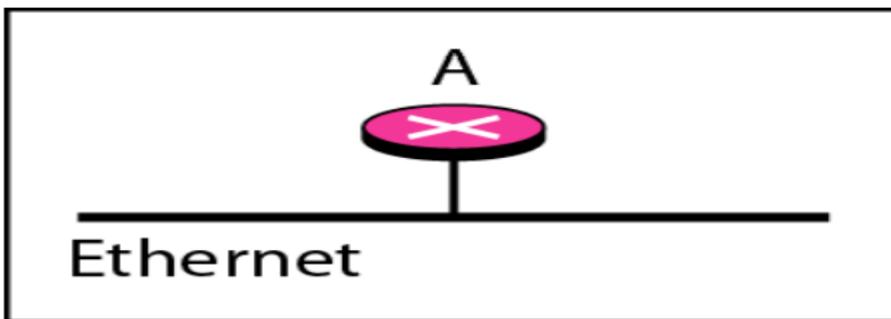
b. Unrealistic representation



c. Realistic representation

# Open Shortest Path First Protocol ... Contd.

- A **stub link** is a network that is connected to only one router.
- The data packets enter the network through this single router and leave the network through this same router.
- This is a special case of the transient network.
- This situation can be shown using the router as a node and using the designated router for the network.
- However, the link is only one-directional, from the router to the network.



a. Stub network



b. Representation



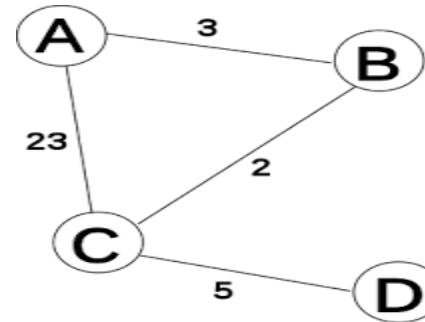
# Open Shortest Path First Protocol ... Contd.

- When the link between two routers is broken, the administration may create a **virtual link** between them, using a longer path that probably goes through several routers.

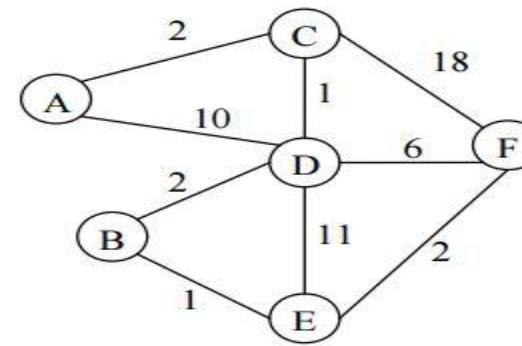


# Practice Questions

1) Compute the routing table of the nodes A, B, C, and D in the following network using Dijkstra's Algorithm.



2) Compute the routing table of the nodes A, B, C, D, E, and F in the following network using Link State Routing.





# Summary

## Discussed about

- Introduction
- Building Routing Tables
- Open Shortest Path First Protocol
- Practice Questions



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**Thank You!**