

# Advanced computer Networks

# UNIT 2

- **Network interface card(NIC):**
- A network interface card (NIC) is a circuit board or card that is installed in a computer so that it can be connected to a network.
- A network interface controller (NIC, also known as a network interface card, network adapter, LAN adapter or physical network interface, is a computer hardware component that connects a computer to a network



- A network interface card provides the computer with a dedicated, full-time connection to a network. Personal computers and workstations on a local area network (LAN) typically contain a network interface card specifically designed for the LAN transmission technology
- Fig 2.2 shows an example of a simple communication between a routing device and laptop host

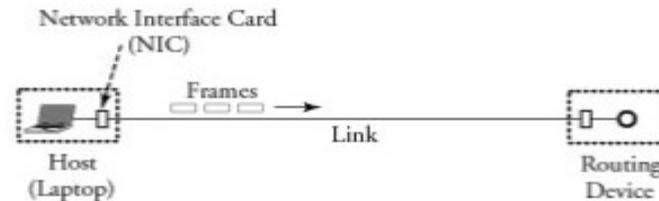


Figure 2.2 The role of a network interface card (NIC) in interfacing between devices and a link

- A NIC allows computers to communicate over a computer network using cable.
- NIC mainly implemented in layer 2 (DLL)protocols.
- It deals with link addressing schemes and provides physical access to a network medium
- NIC has bidirectional ports
- Fig 2.3 shows incoming message arrives at frame processing unit through this frames and link addressing is processed.

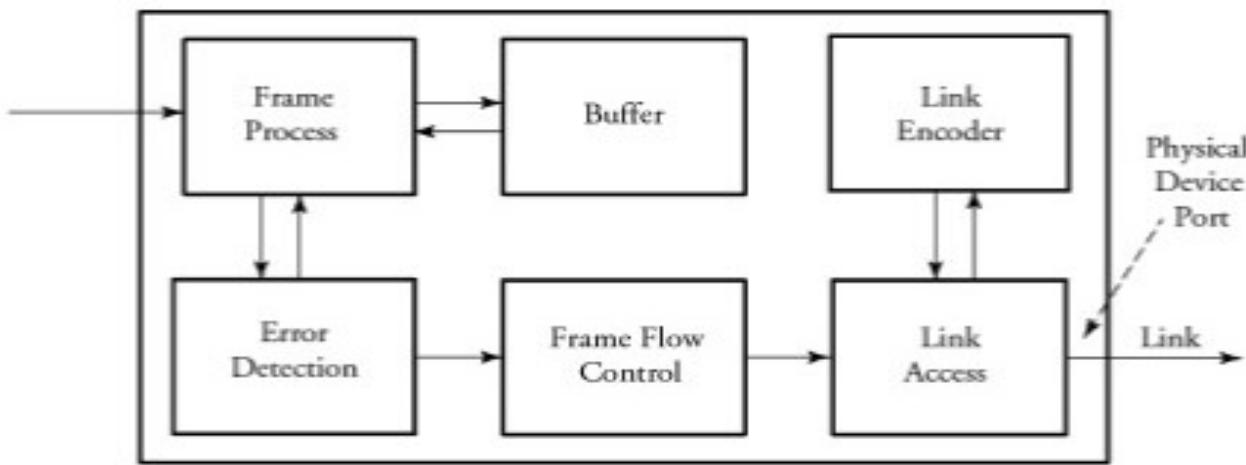


Figure 2.3 A block diagram of a network interface card (NIC)

- Frames are temporarily stored in a buffer to provide time for the completion of the other outstanding frames in NIC.
- Arriving frames are inspected at the error detection unit to learn any possible errors
- This process is followed by the frames flow control which is responsible for control of the frame transmission rate over the link
- The link access unit tries to access a free channel for frames to transmit over the link.

## ■ **Switching and Routing devices**

- Switching and routing devices are designed to receive frames or packet and transmit them to different parts of the network based on certain policy and protocol.
- They are categorized by their capabilities and functionality
- They are mainly classified into three categories
- Layer 1 devices
- Layer 2 devices
- Layer 3 devices

- Fig 2.4 depicts the interconnection and switching function at layer 1 , layer 2, layer 3 of five layer protocol stack.

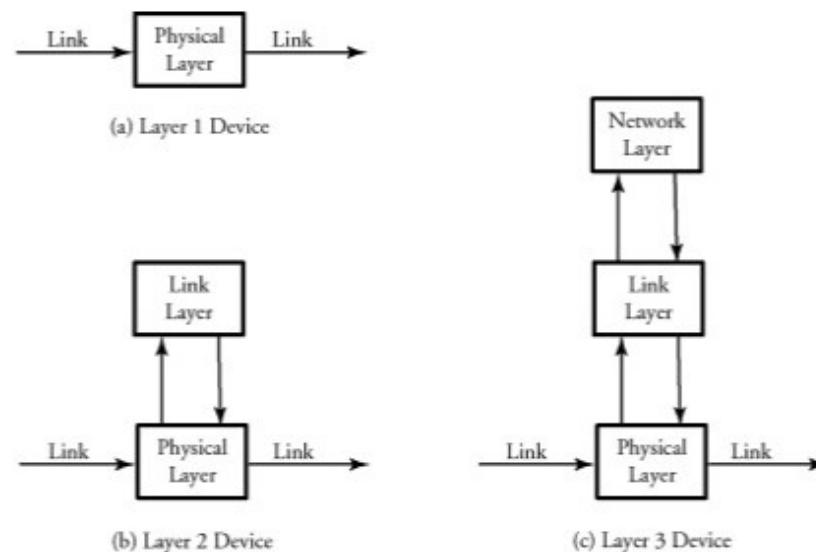
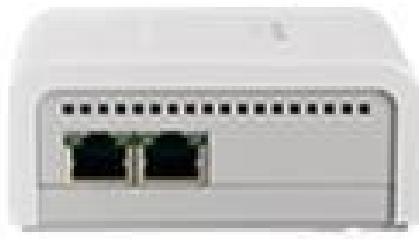


Figure 2.4 Connections in different layers of the protocol stack

- **Layer 1 devices**
- Layer 1 of protocol stack defines electrical ,procedural and functional specifications for activating and maintaining physical link between end systems.
- Two well known devices in this category are
  1. Repeater
  2. Hubs
  3. Fig 2.4(a) shows the point to point connection between layer 1 devices



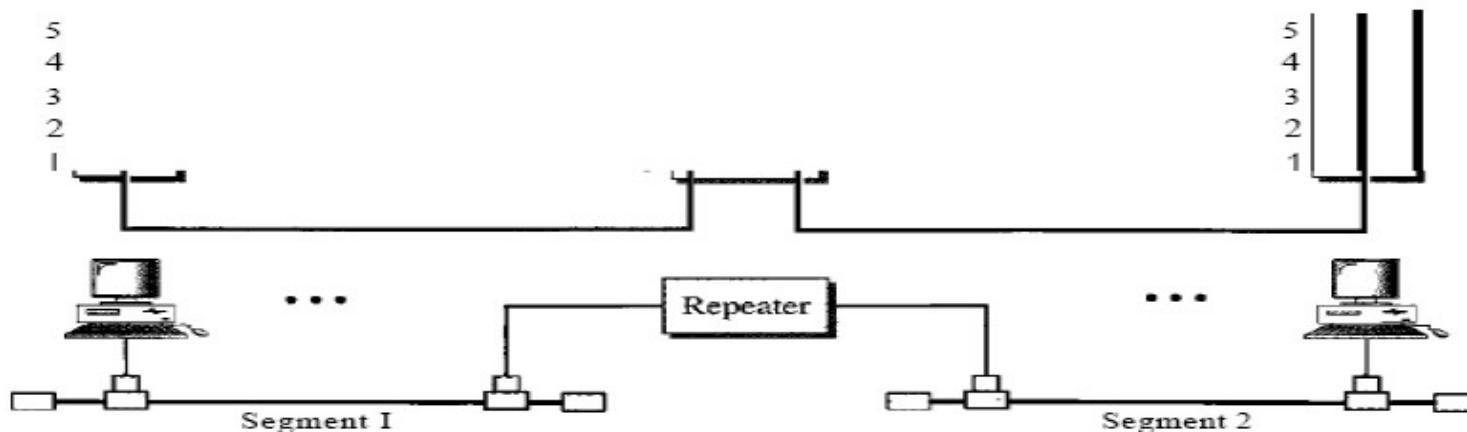
**Repeater**



**Hub**

## ■ **Repeaters:**

- Repeaters are considered to be a simplest switching devices designed primarily to interconnect two host without involvement of complex routing process
- The main function of repeater are signal strengthening , signal regeneration
- Signal regeneration is needed when transmission lengthen is extended.



---

A repeater connects segments of a LAN.

---

---

A repeater forwards every frame; it has no filtering capability.

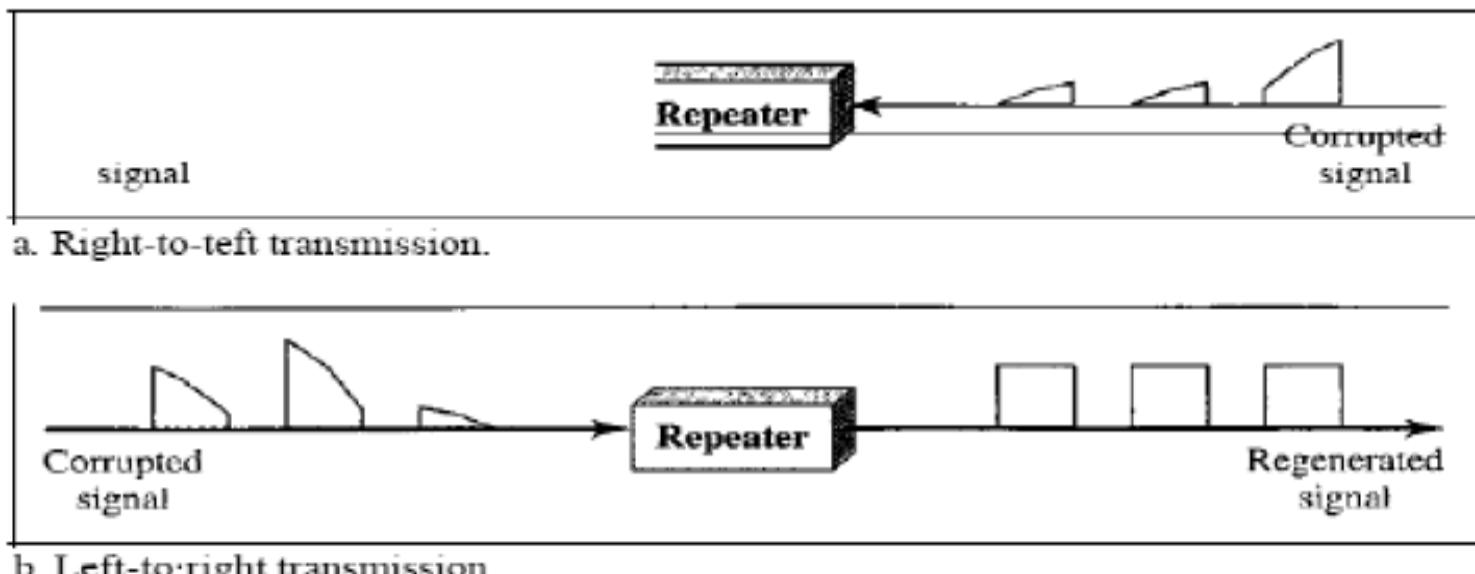
---

---

A repeater is a regenerator, not an amplifier.

---

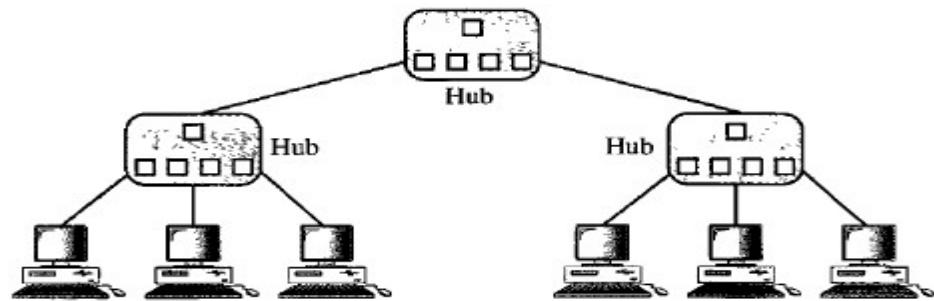
Figure 15.3 Function of a repeater



## ■ **Hubs:**

- Hub is another simple connecting device used to provide interconnection among multiple users in layer 1
- It is similar to repeater but connects several users in LAN.
- It is multipoint repeater.
- It performs multipoint connection using hub to copy and forward packet or frame among multiple users.

## ■ Figure 1 A hierarchy of hubs



## ■ Layer 2 devices

- Layer 1 device can transmit a data to all the users in the LAN
- Layer 2 device can make a decision where to forward a frame .
- They perform data link layer functions like forwarding ,formatting and error detection
- However Hubs just duplicate data and send it in all the ports
- Layer 2 device holds forwarding table that shows layer 2 address and forwarded through which port

- Layer 2 devices are
- 1. bridges
- 2 switches
- A **bridge** connects **two** or more LANs segments .  
When a frame arrives, software in the bridge extracts the destination address from the frame header **and** looks it up in a table to see where send the frame

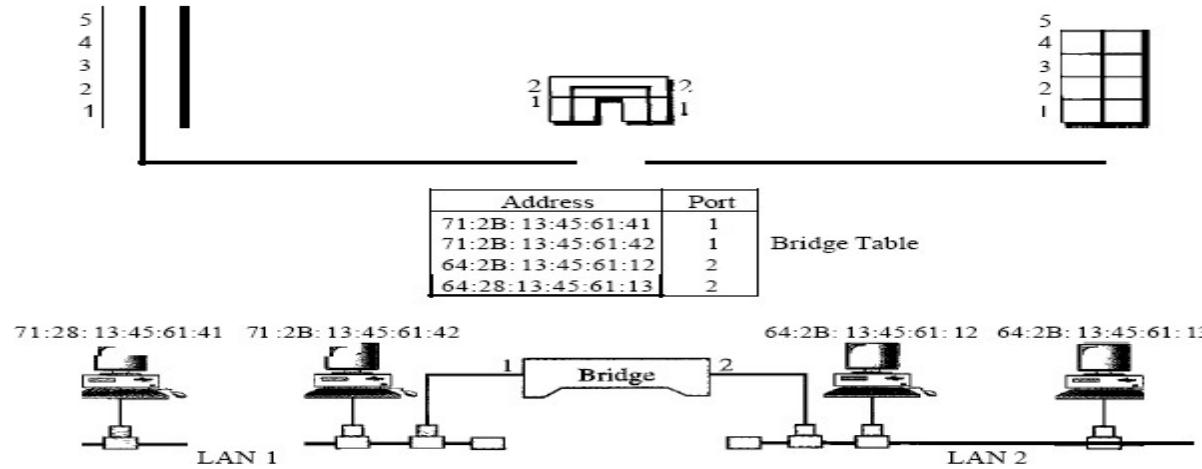


- A bridge operates in both the physical and the data link layer.
- As a physical layer device, it regenerates the signal it receives.
- As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame.
- One may ask, What is the difference 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
- Let us give an example. In Figure 2, two LANs are connected by a bridge.

- If a frame destined for station 712B13456142 arrives at port 1, the bridge consults its table to find the departing port. According to its table, frames for 712B13456142 leave through port 1; therefore, there is no need for forwarding, and the frame is dropped. On the other hand, if a frame for 712B13456141 arrives at port 2, the departing port is port 1 and the frame is forwarded.

## ■ Figure 2 A bridge connecting two LANs



## ■ **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.

## ■ Two-Layer Switches

- When we use the term switch, we must be careful because a switch can mean two different things. We must clarify the term by adding the level at which the device operates. We can have a two-layer switch or a three-layer switch.
- 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

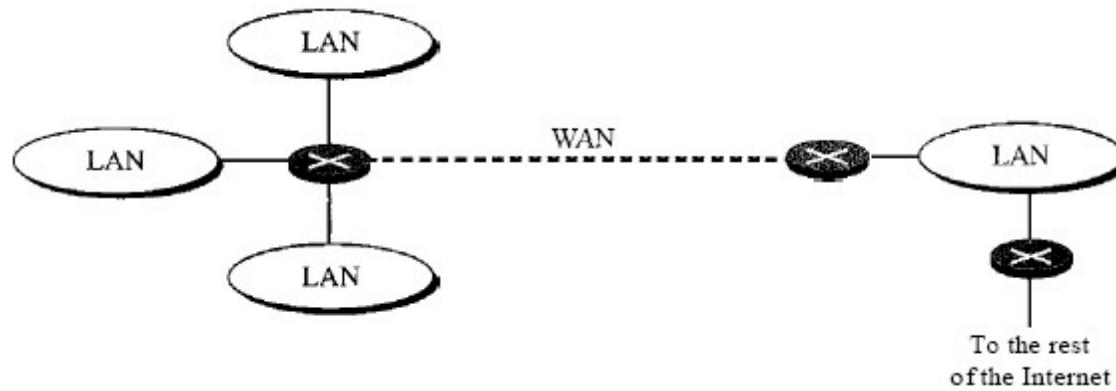
- A two-layer switch, as a bridge does, makes a filtering decision based on the MAC address of the frame it received.
- However, a two-layer switch can be more sophisticated. It can have a buffer to hold the frames for processing. It can have a switching factor that forwards the frames faster. Some new 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.

- **Layer 3 devices**

- **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. Figure 3 shows a part of the Internet that uses routers to connect LANs and WANs.

- Figure 3 Routers connecting independent LANs and WANs



## ■ Router Structure

- Routers are building blocks of WAN
- Packets arrive at  $n$  input ports and routed out from  $n$  output ports.
- The system consists of four main parts
- Input port processor
- output port processor
- Switch fabric and switch controller

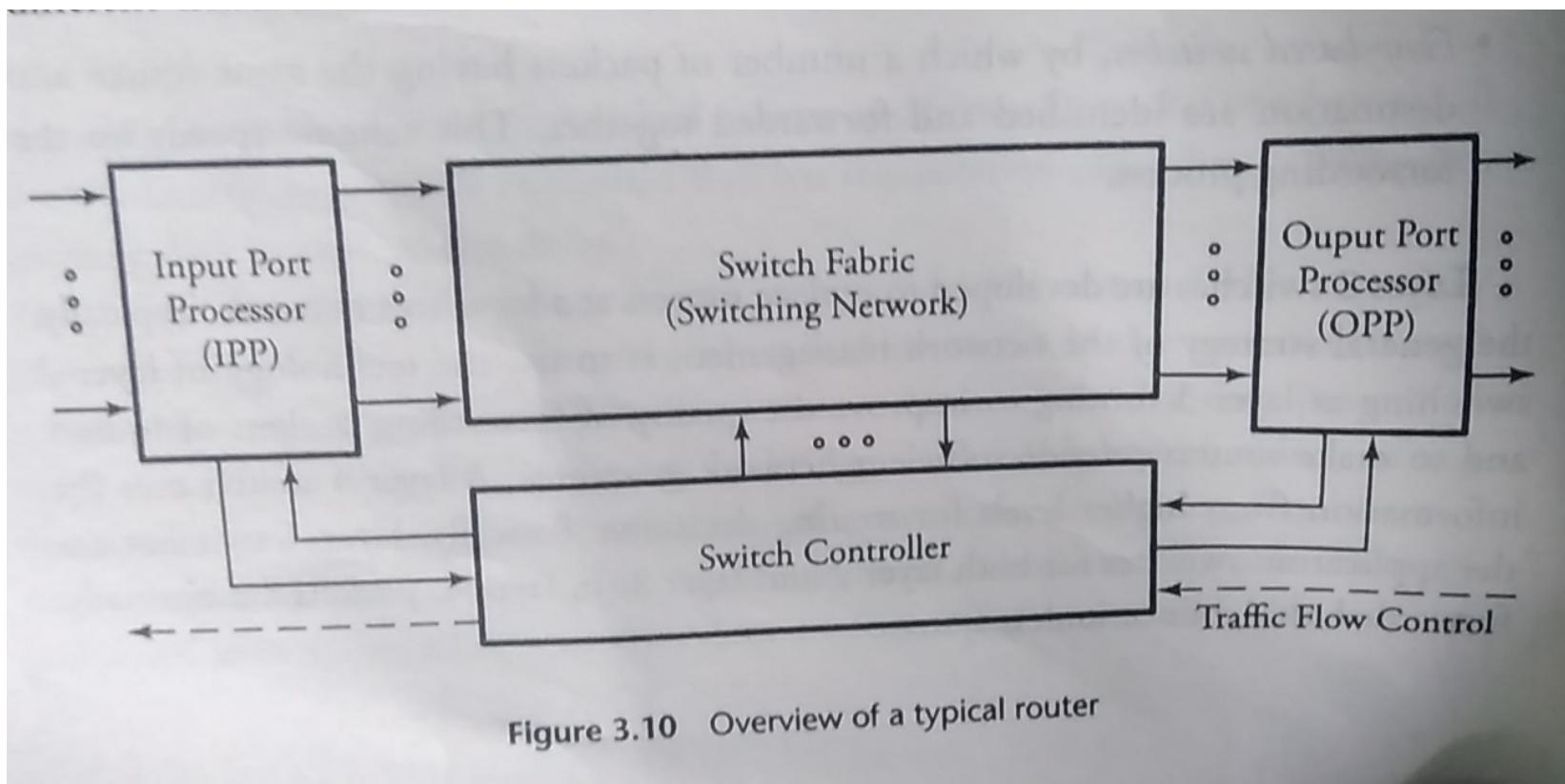


Figure 3.10 Overview of a typical router

- An IPP consists of several main module
- Packet fragmentation
- Main buffer
- Routing table
- Packet encapsulation
- QoS

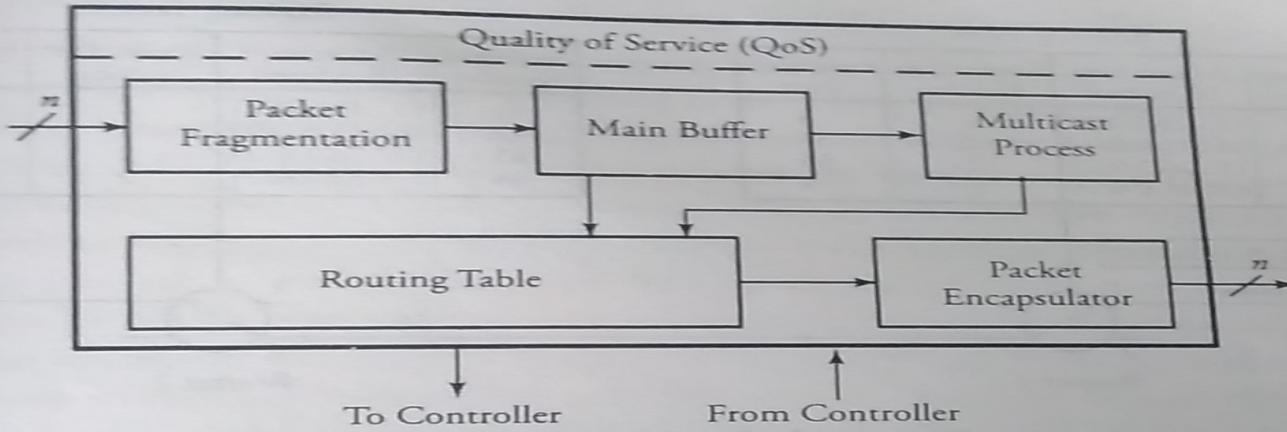


Figure 3.11 Overview of a typical IPP in routers

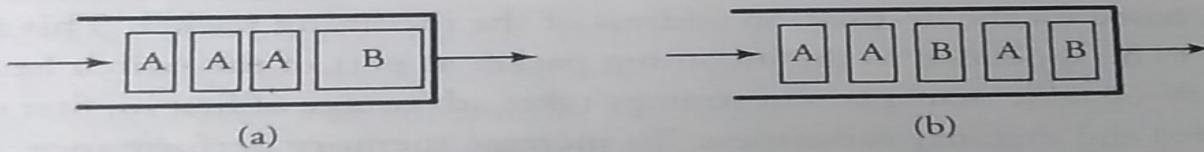


Figure 3.12 Packet fragmentation: (a) without fragmentation; (b) with fragmentation

## ■ **Packet fragmentation**

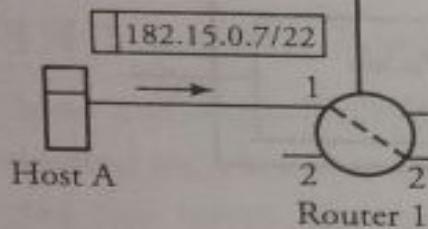
- The packet fragmentation unit converts packets to smaller size.
- Large packets cause different issues at the network and link layer.
- Another example occurs when large packets must be buffered at the input port interface of a router , as buffer slots are usually 512 bytes long
- One solution to this problem is to partition packets into smaller fragments and then reassemble them at output port processor unit after processing them in the switch system.

## ■ **Routing table**

- Routing table is a look up table contains all the destination address and corresponding switch output port.
- Routing algorithms fills this routing table.
- The purpose of the routing table is to look up an entry corresponding to the destination address of the incoming packets and to provide the output port
- As soon as routing decision is made all the information should be saved on the routing table.

Routing Table

Sequence Number	Destination IP Address	Router Port Number	Estimated Cost
4	143.28.3.0/21	1	4
5	182.15.0.0/22	2	56
6	155.76.2.0/22	2	56
7	131.46.0.0/24	1	4



Routing Table

Sequence Number	Destination IP Address	Router Port Number	Estimated Cost
41	135.18.5.0/21	2	3
42	182.15.0.0/22	1	0
43	197.76.2.0/23	2	3
44	171.55.0.0/21	2	3

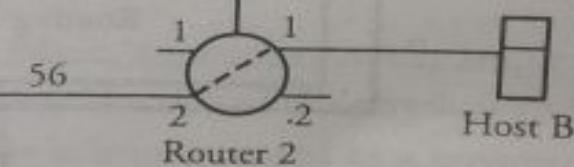


Figure 3.13 Routing tables at routers

- **Packet encapsulation:**
- Packet encapsulation unit formats the incoming packet with a header before forwarding the packet to switch.
- **Congestion controller:**
- Congestion can be controlled in several , sending reverse –warning packet to the upstream node to avoid exceeding traffic in out going line

## ■ Multicast Process

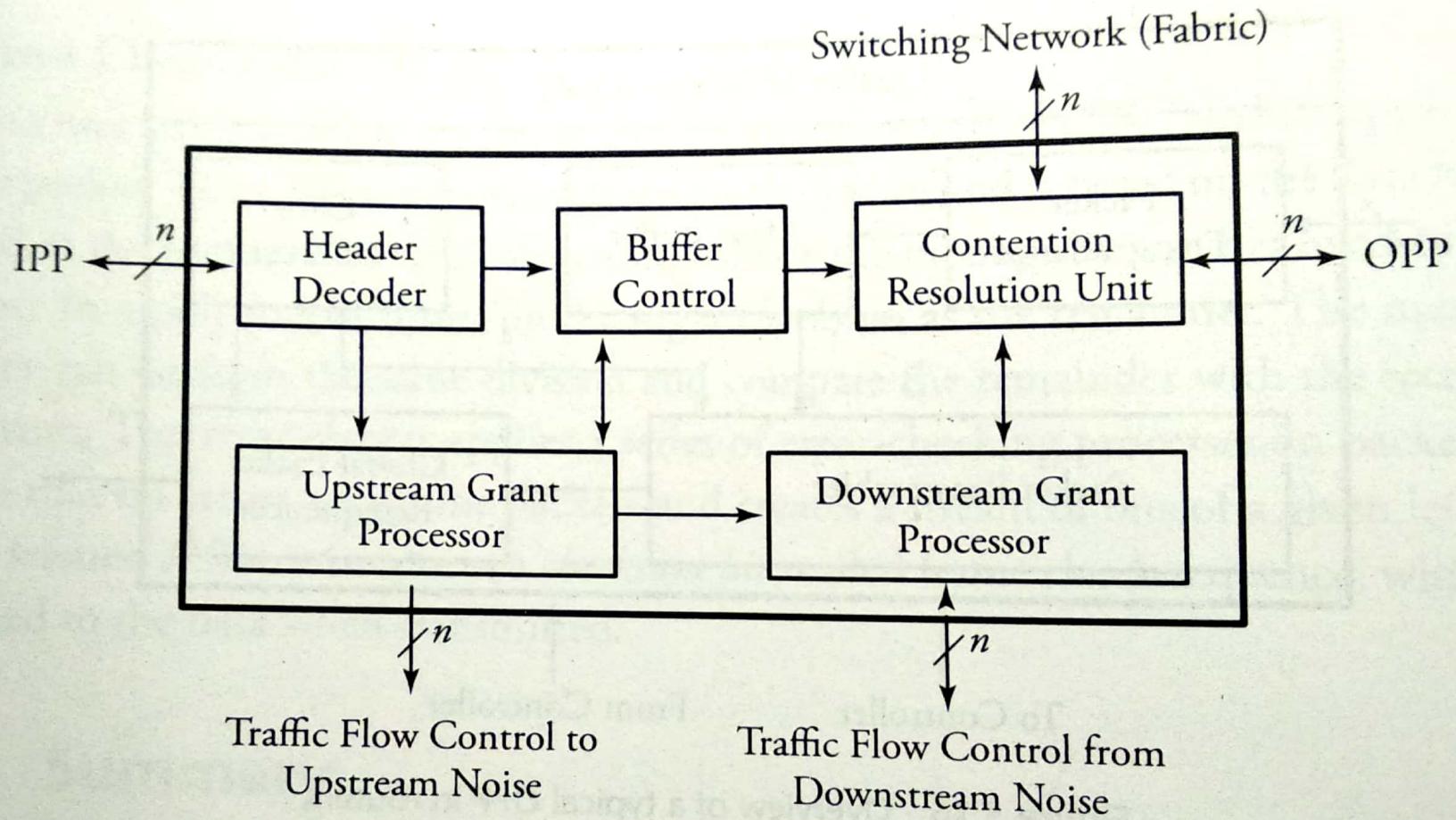
- Multicast process is necessary for copying packets when multiple copies are expected to be made on a switching node.
- Multicasting is the data transmission from one source to the group of destinations.
- Data networks must be able to support such multimedia applications by multicasting data, voice and video.

## ■ Switch Fabric

- In the switch fabric, the packets are routed from input ports to the desired output ports.
- A packet can also be multicast to more than one output.
- Finally in the output processors, packets are buffered and resequenced in order to avoid packet misordering

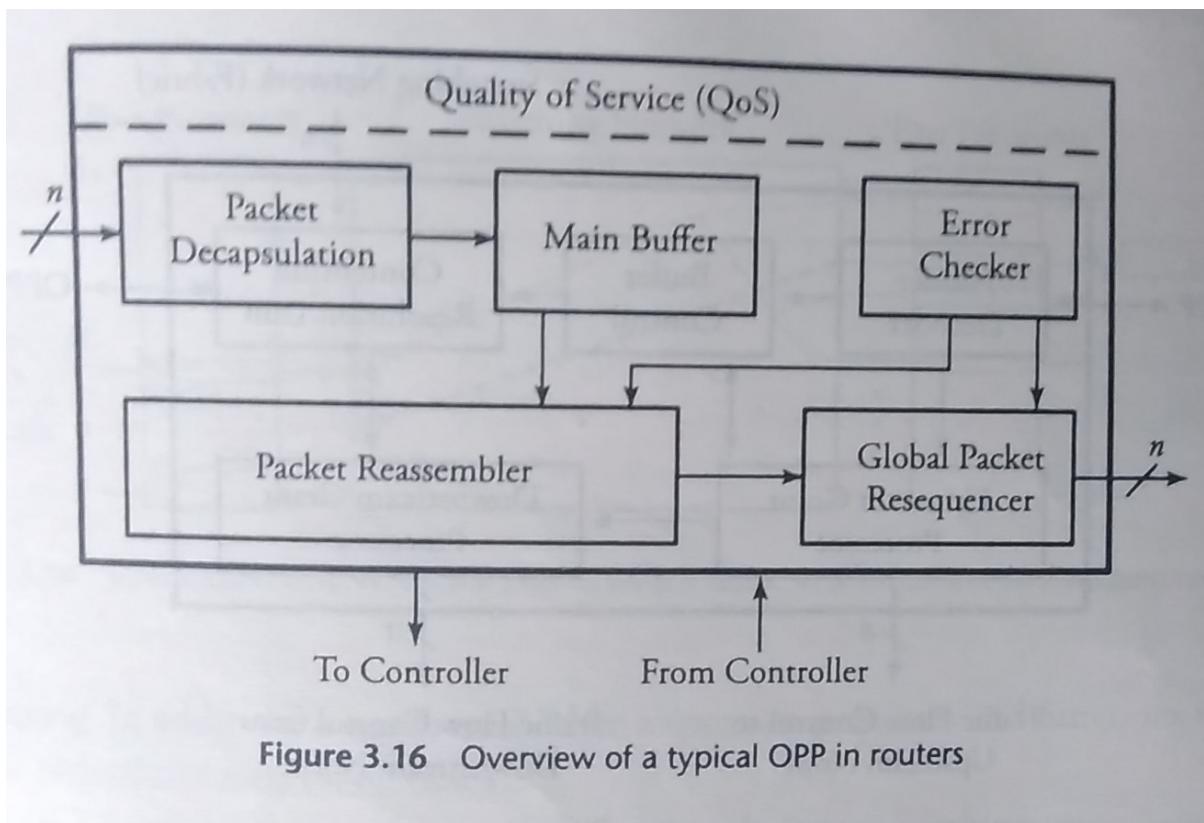
## ■ Switch Controller

- The controller part takes the decision leading to the transmission of packets to the requested output.
- The controller receives packets from an IPP, but only the headers of packets are processed in the controller.



## ■ **Output port Processors**

- Implementing OPP in switches includes parallel to serial multiplexing,
- main buffer,
- local packet re sequencer,
- global packet re sequencer,
- error checker and
- packet reassemble.



**Figure 3.16** Overview of a typical OPP in routers

- **Main buffer**
- The purpose of the main buffer is to control the rate of outgoing packets , which impacts the quality of service.
- After receiving a data from switch it will forward to packet reassembler.

## ■ **Reassemble**

- the OPP receives a stream of fragmented packets. The OPP reassemble into a single packet based on the information available from the fragment field of header.
- The packet reassemble buffer is used to combine fragments of IP packets.

## ■ 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. In this book, we use the terms router and three-layer switch interchangeably.

## ■ **Gateway**

- Although some textbooks use the terms gateway and router interchangeably, most of the literature distinguishes between the two. 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.

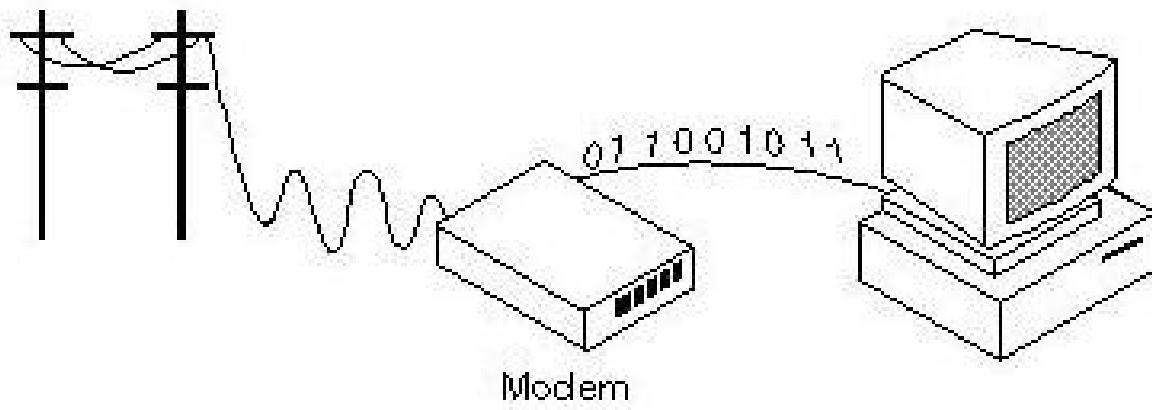
- This means that it can be used as a connecting device between two internetworks that use different models. For example, a network designed to use the OSI model can be connected to another network using the Internet model. The gateway connecting the two systems can take a frame as it arrives from the first system, move it up to the OSI application layer, and remove the message. Gateways can provide security

## ■ Modems

Modem is a short form for Modulator/Demodulator

The term modem is a composite word that refers to the two functional entities that make up the device; a signal modulator and a signal demodulator. A modulator creates a band-pass analog signal from binary data. A demodulator recovers the binary data from the modulated signal

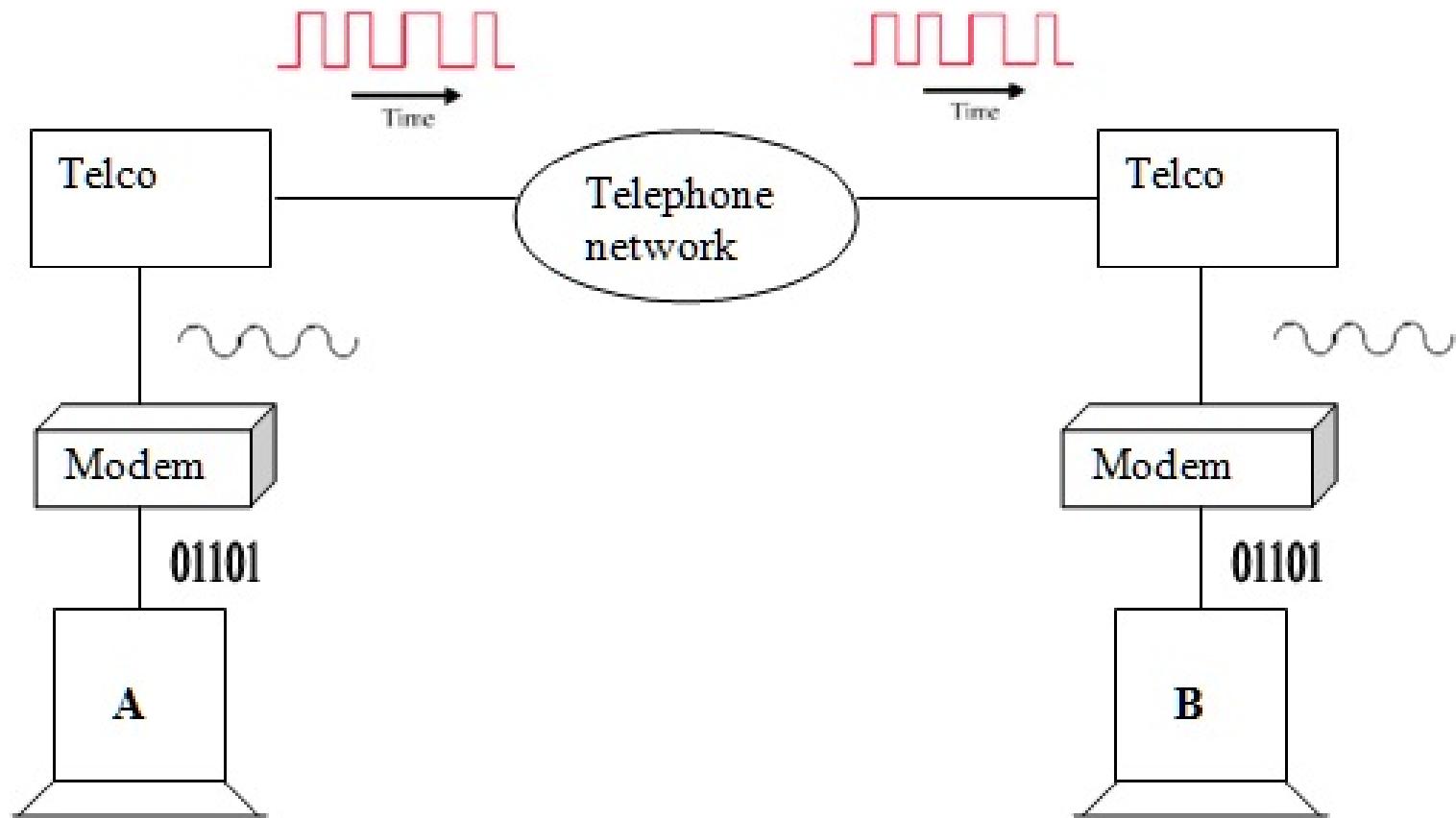
Enables a computer to transfer data over the telephone or cable lines



## ■ TELEPHONE MODEMS

Traditional telephone lines can carry frequencies between 300 and 3300 Hz, giving them BW of 3000 Hz; All this range is used for transmitting voice, where a great deal of interference and distortion can be accepted without loss of intelligibility.

The effective BW of a telephone line being used for data Transmission is 2400 Hz, covering the range from 600 to 3000 Hz.



- Figure shows the relationship of modems to a communication link. The computer on the left sends binary data to the modulator portion of the modem; the data is sent as an analog signal on the telephone lines. The modem on the right receives the analog signal, demodulates it through its demodulator, and delivers data to the computer on the right.
- The communication can be bidirectional, which means the computer on the right can also send data to the computer on the left using the same modulation and demodulation processes.

# Features of Modem

Transmission speed

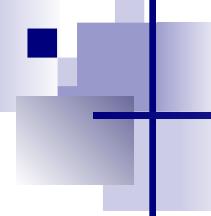
Voice or Data communication

Data compression

Auto answering

Fax capability

- Basic Types of Modems
- Internal - A modem card that you can plug into an expansion slot on the motherboard
- External – Connected to the PC through a cable, which is plugged into serial port on the back of the system unit



## Note

---

Bandwidth utilization is the wise use of available bandwidth to achieve specific goals.

Efficiency can be achieved by multiplexing; i.e., sharing of the bandwidth between multiple users.

*Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared. Multiplexing is the set of techniques that allows the (simultaneous) transmission of multiple signals across a single data link. As data and telecommunications use increases, so does traffic.*

Topics discussed in this section:

- Frequency-Division Multiplexing
- Wavelength-Division Multiplexing
- Synchronous Time-Division Multiplexing
- Statistical Time-Division Multiplexing

Figure 6.1 *Dividing a link into channels*

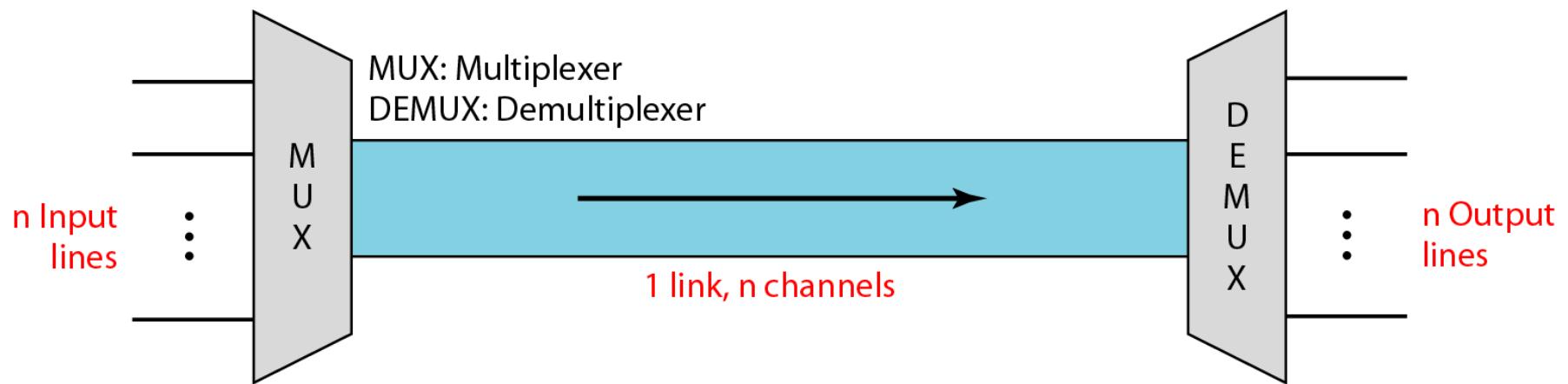


Figure 6.2 *Categories of multiplexing*

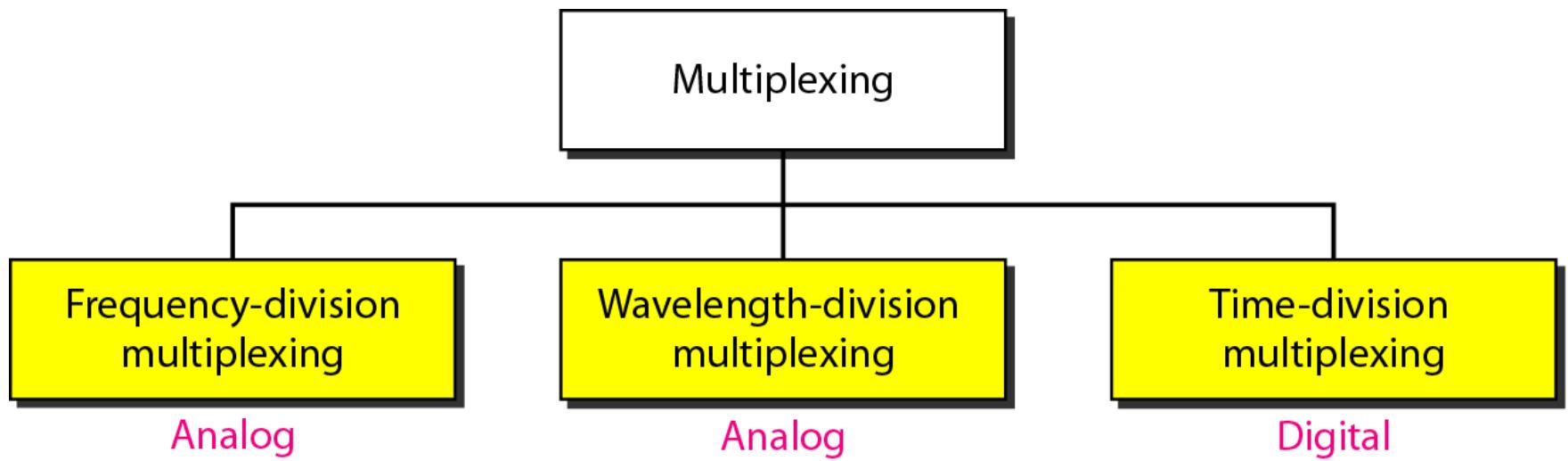


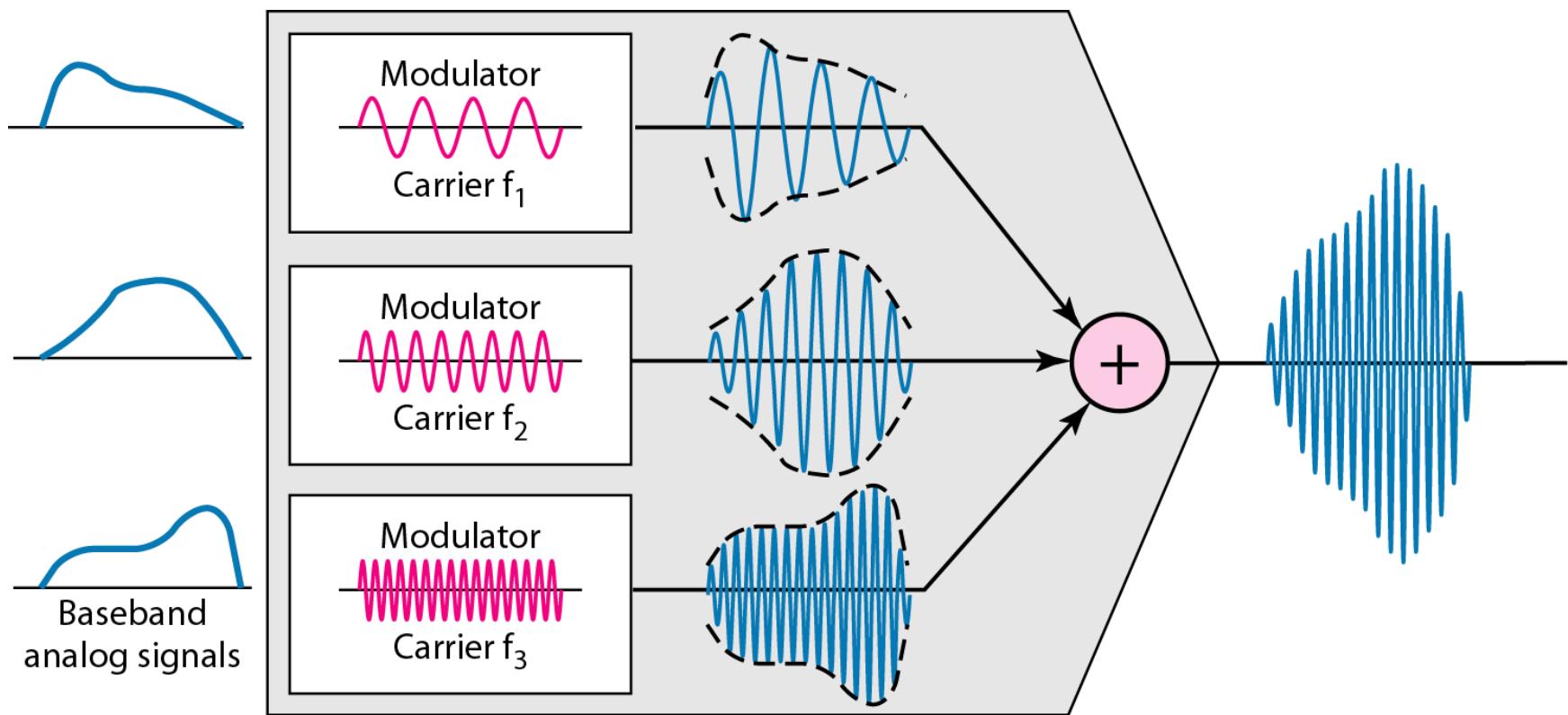
Figure 6.3 *Frequency-division multiplexing (FDM)*



## *Note*

Frequency-division multiplexing (FDM) is a technique by which the total bandwidth available in a communication medium is divided into a series of non-overlapping frequency bands, each of which is used to carry a separate signal. This allows a single transmission medium such as a cable or optical fiber to be shared by multiple independent signals. Another use is to carry separate serial bits or segments of a higher rate signal in parallel.

Figure 6.4 *FDM process*



# FM

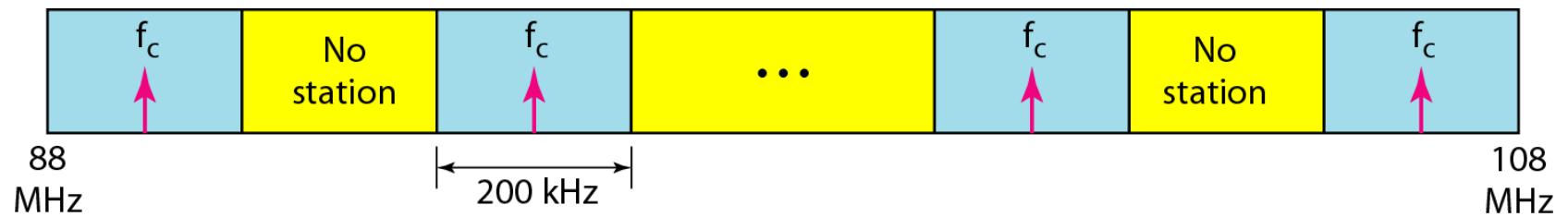
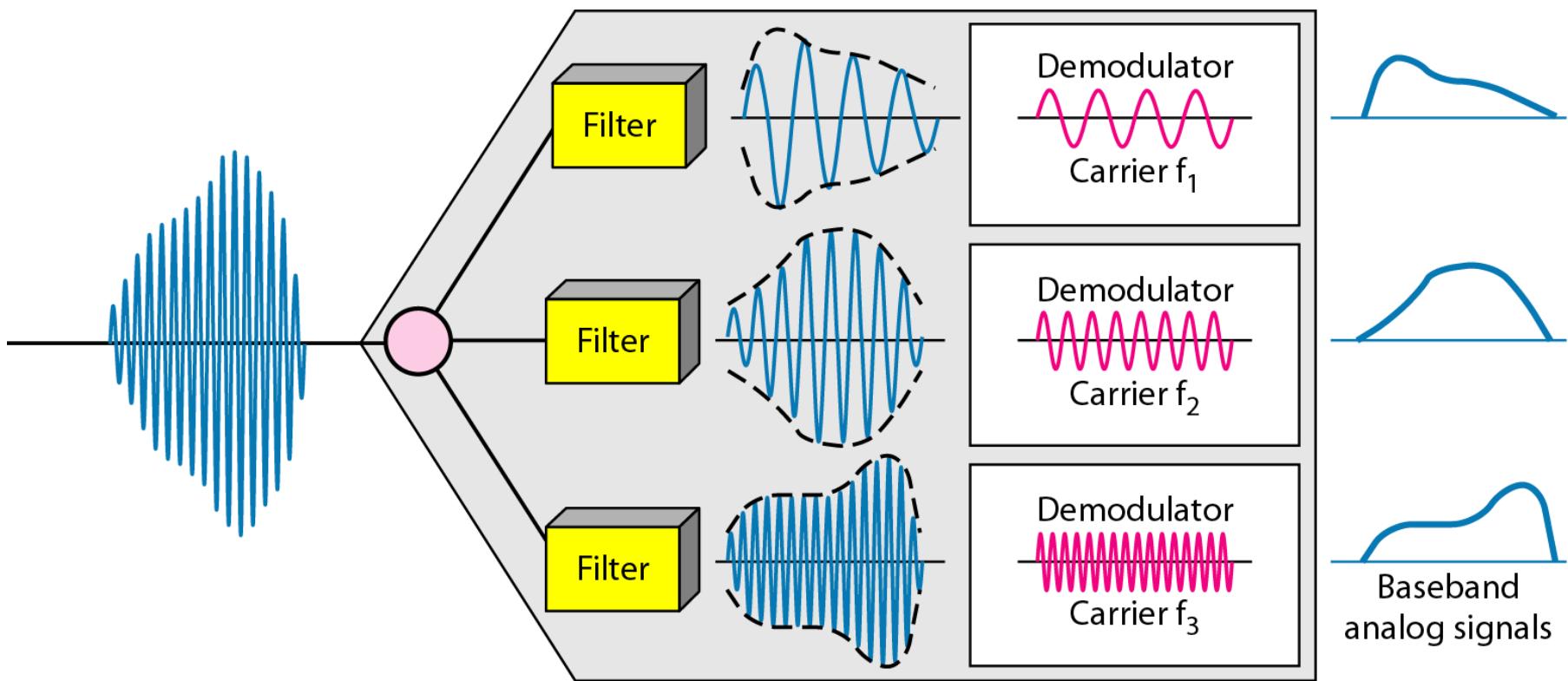


Figure 6.5 *FDM demultiplexing example*

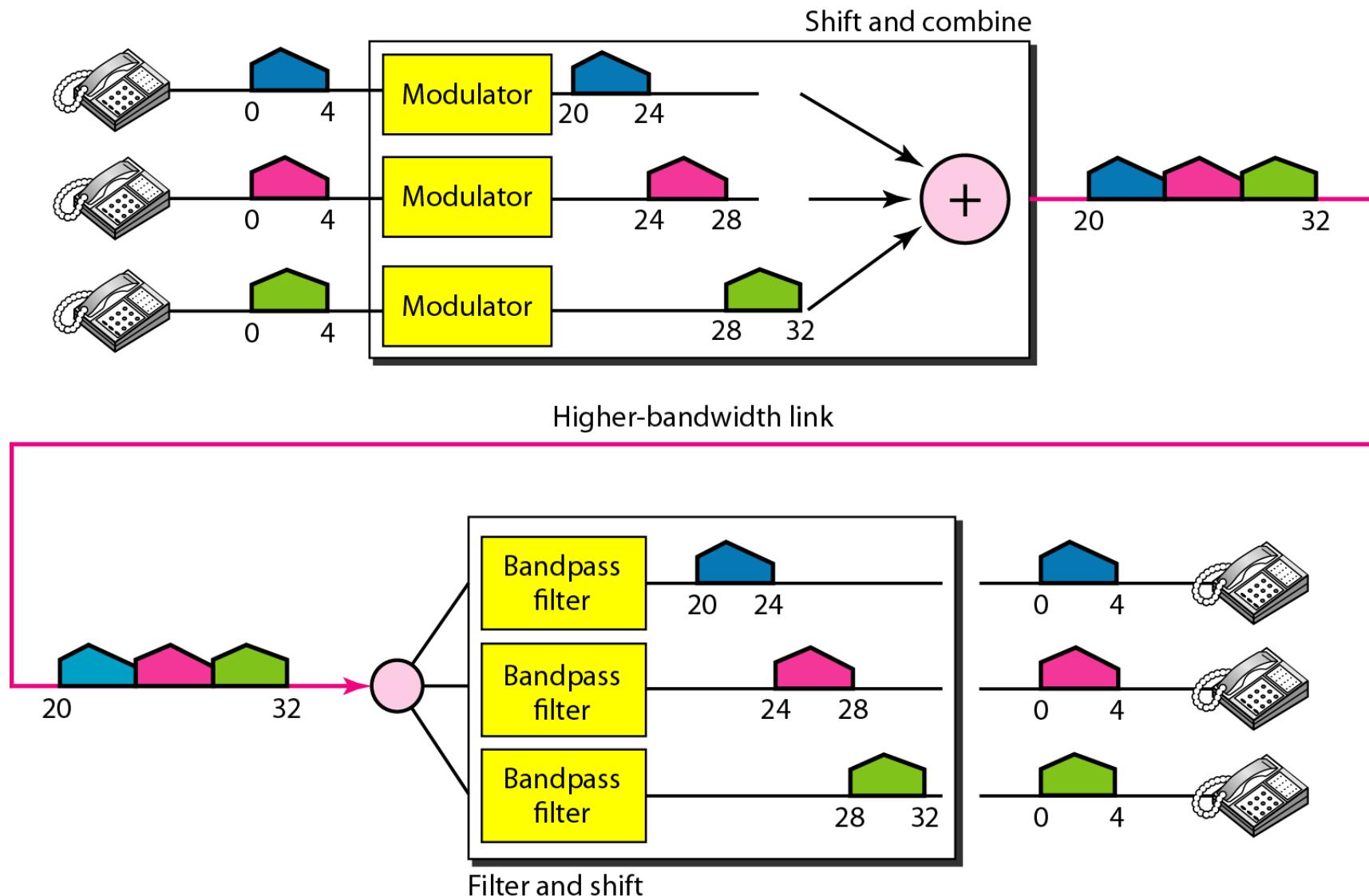


Assume that a voice channel occupies a bandwidth of 4 kHz. We need to combine three voice channels into a link with a bandwidth of 12 kHz, from 20 to 32 kHz. Show the configuration, using the frequency domain. Assume there are no guard bands.

### Solution

We shift (modulate) each of the three voice channels to a different bandwidth, as shown in Figure 6.6. We use the 20- to 24-kHz bandwidth for the first channel, the 24- to 28-kHz bandwidth for the second channel, and the 28- to 32-kHz bandwidth for the third one. Then we combine them as

Figure 6.6 Example 6.1



*Five channels, each with a 100-kHz bandwidth, are to be multiplexed together. What is the minimum bandwidth of the link if there is a need for a guard band of 10 kHz between the channels to prevent interference?*

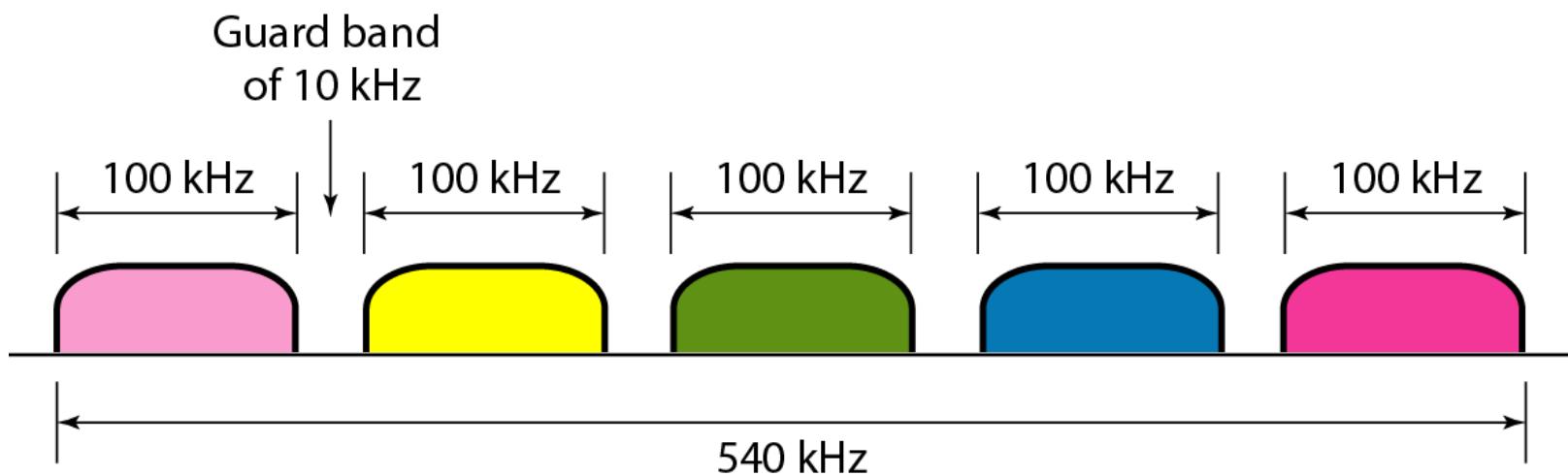
*Solution*

*For five channels, we need at least four guard bands. This means that the required bandwidth is at least*

$$5 \times 100 + 4 \times 10 = 540 \text{ kHz},$$

*as shown in Figure 6.7.*

Figure 6.7 *Example 6.2*



## *Note*

WDM is an analog multiplexing technique to combine optical signals. Wavelength division Multiplexing (WDM) is a technology which multiplexes a number of optical carrier signals onto a single optical fiber by using different wavelengths (i.e., colors) of laser light. This technique enables bidirectional communications over one strand of fiber, as well as multiplication of capacity.

Figure 6.10 *Wavelength-division multiplexing (WDM)*

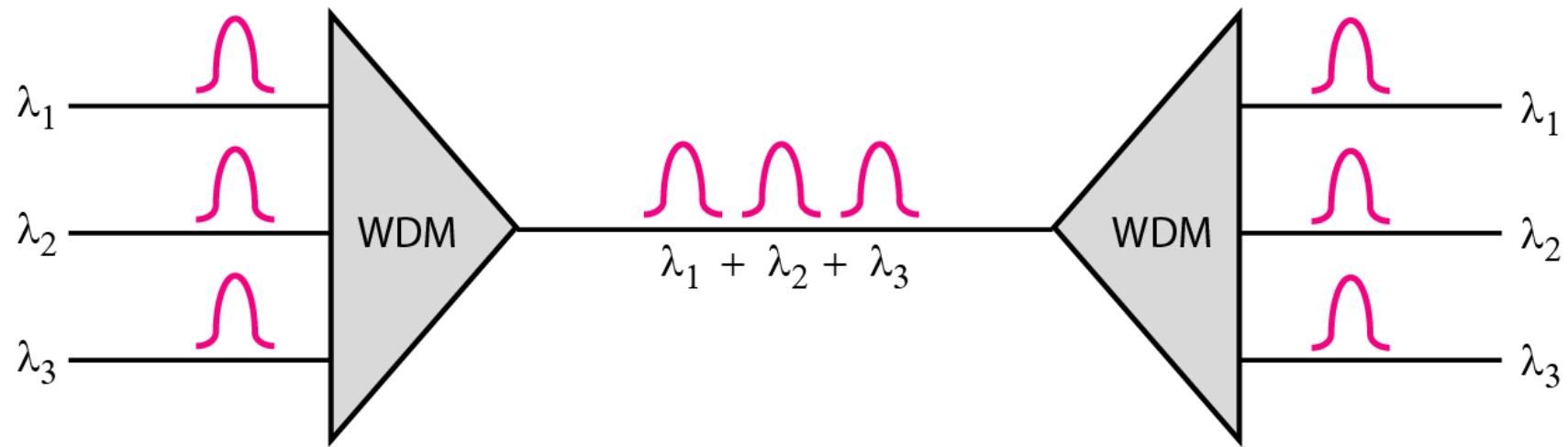


Figure 6.11 *Prisms in wavelength-division multiplexing and demultiplexing*

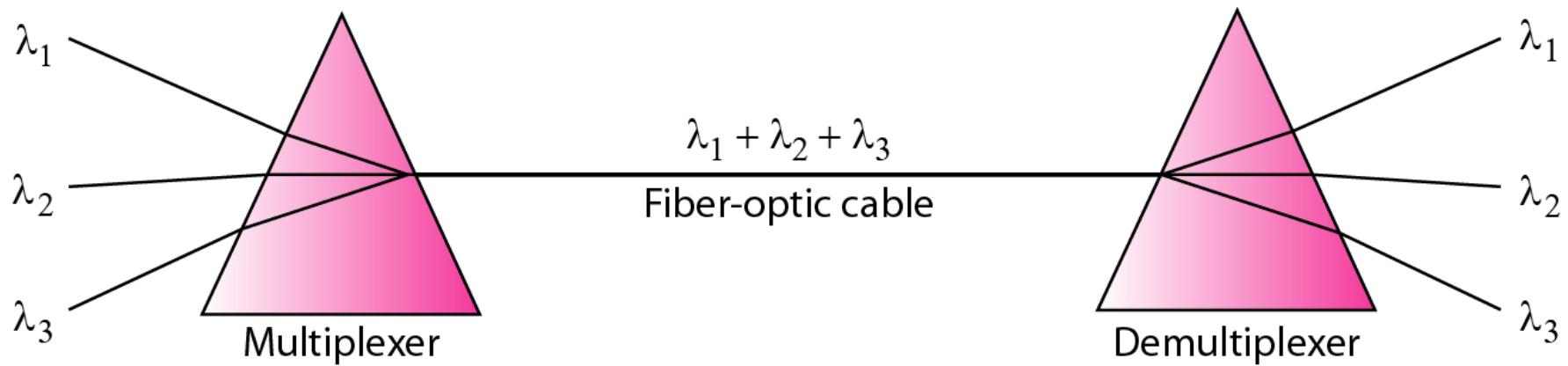
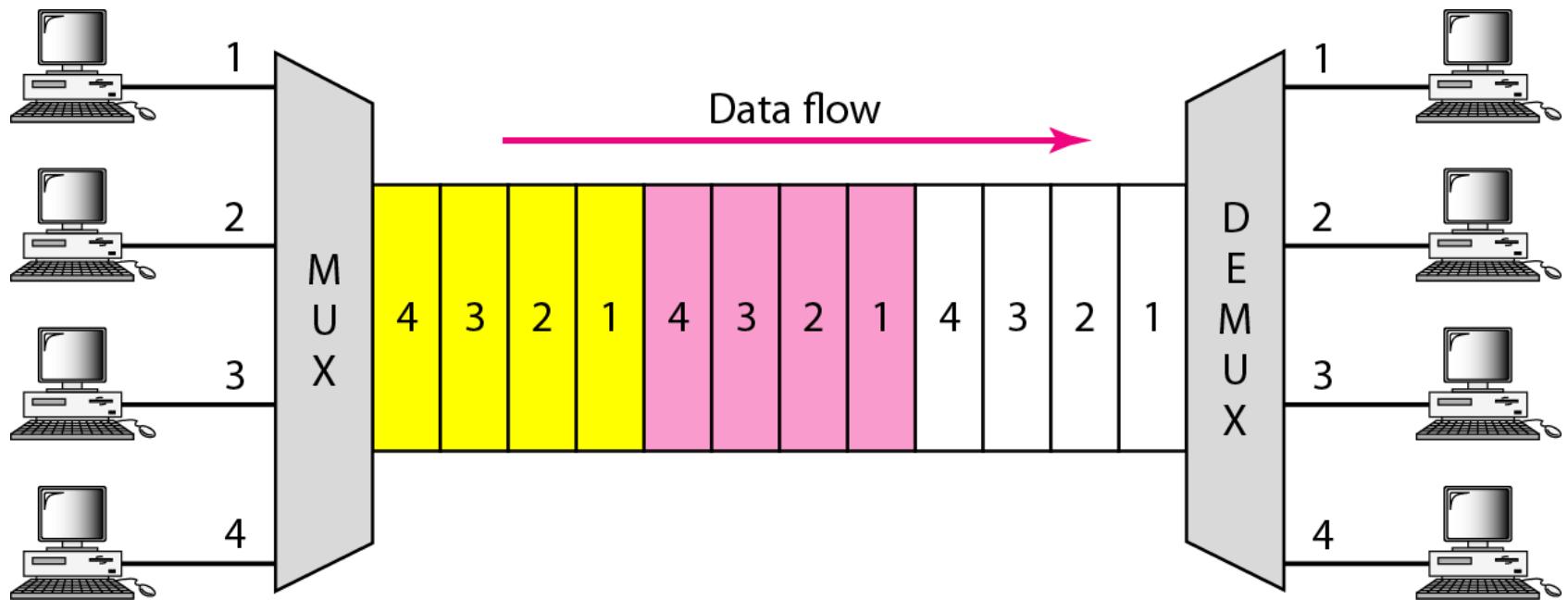


Figure 6.12 Time Division Multiplexing (TDM)





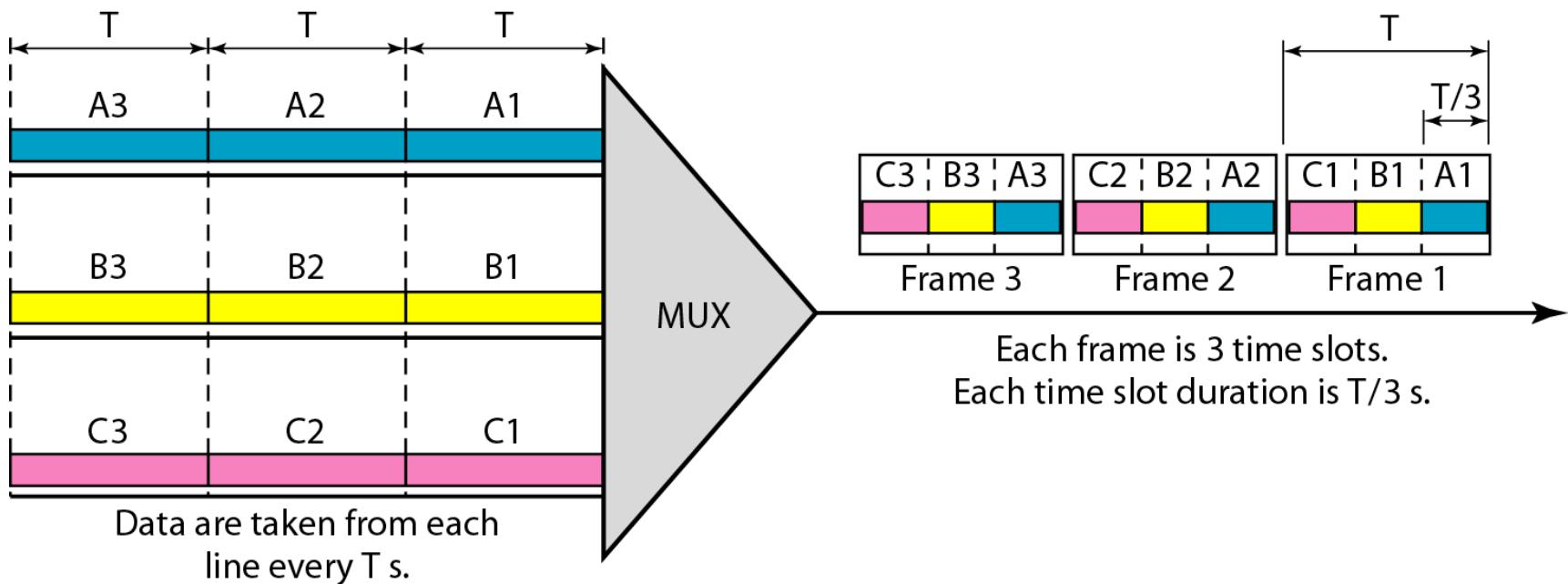
## *Note*

---

TDM is a digital multiplexing technique for combining several low-rate digital channels into one high-rate one.

---

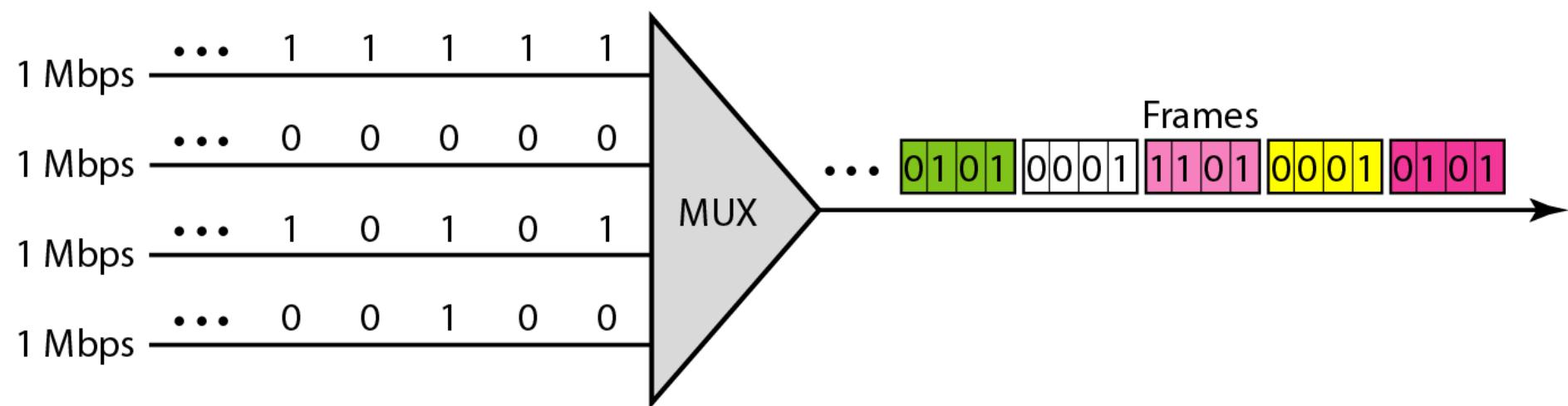
Figure 6.13 *Synchronous time-division multiplexing*



## *Note*

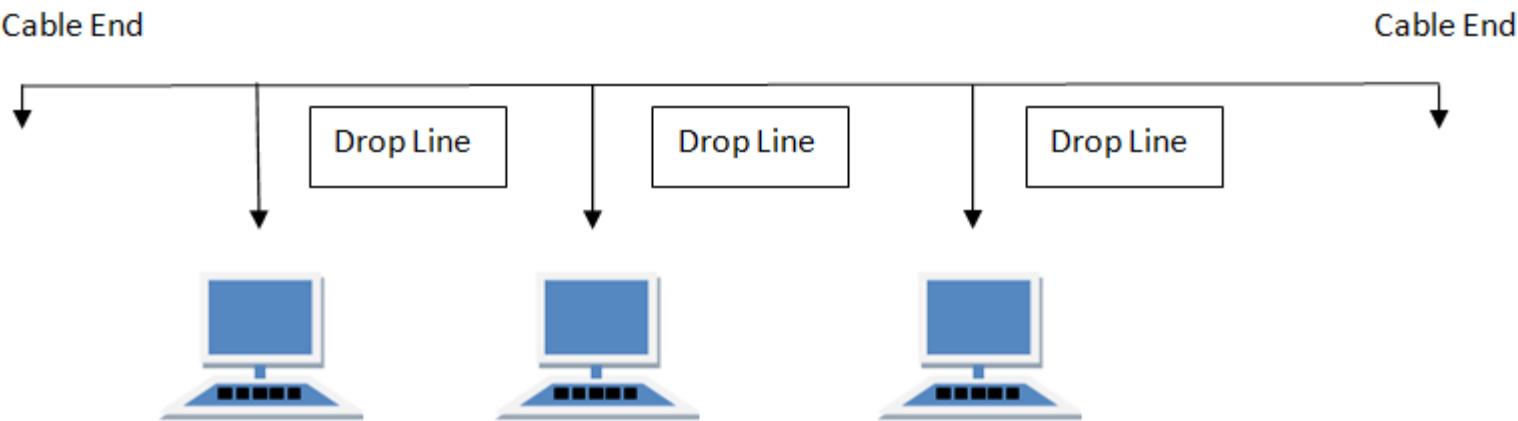
In synchronous TDM, the data rate of the link is  $n$  times faster, and the unit duration is  $n$  times shorter.

Figure 6.14 *Example 6.6*



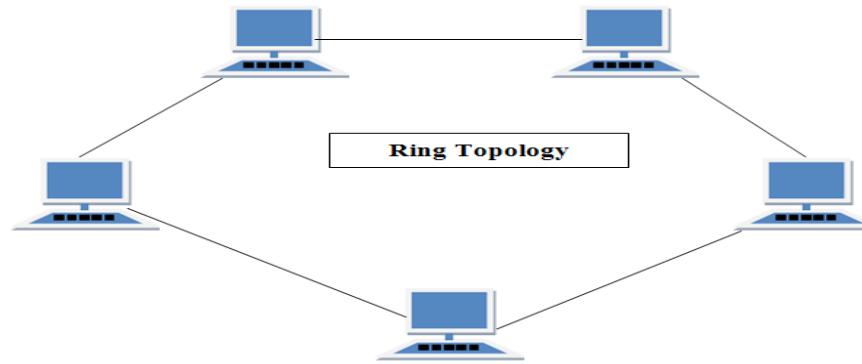
# LAN and Basic Topologies

- **BUS Topology**
- Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



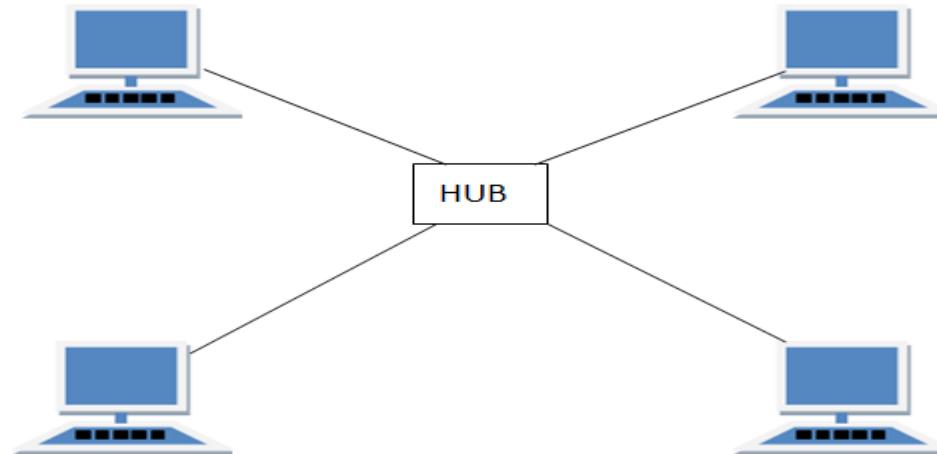
## ■ **RING Topology**

- It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

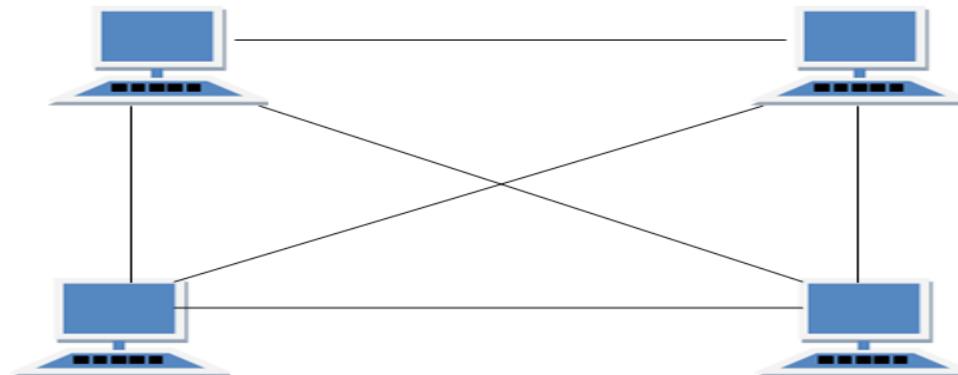


## ■ **STAR Topology**

- In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

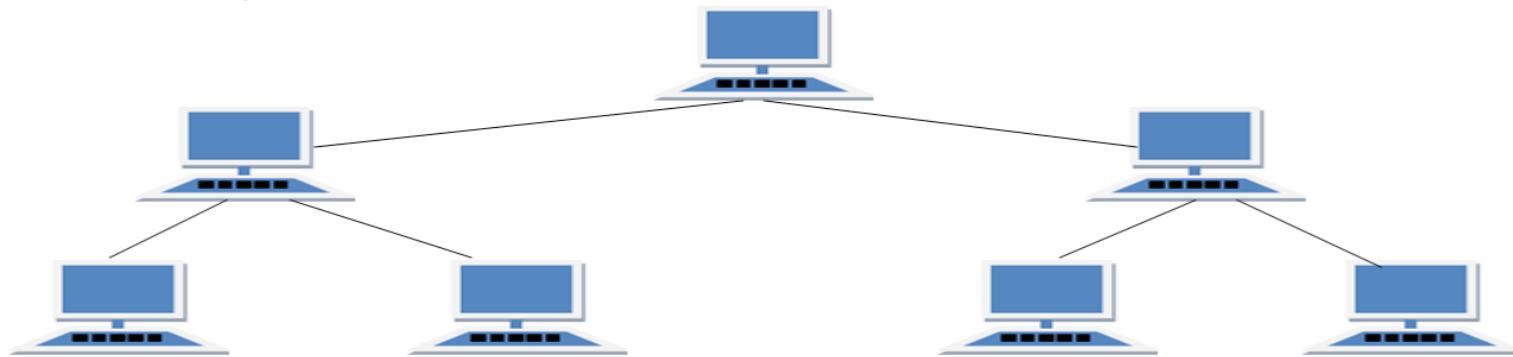


- Mesh Topology
- It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has  $n(n-1)/2$  physical channels to link  $n$  devices.



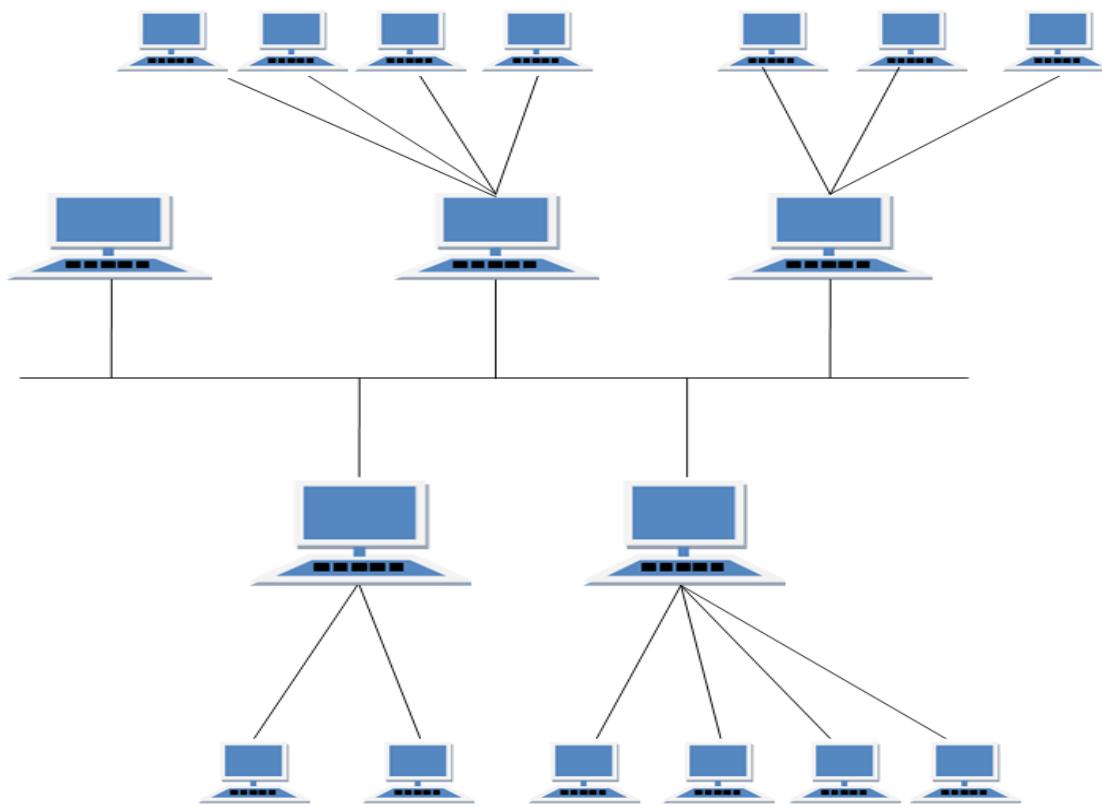
## ■ TREE Topology

- It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



## ■ **HYBRID Topology**

- It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology)



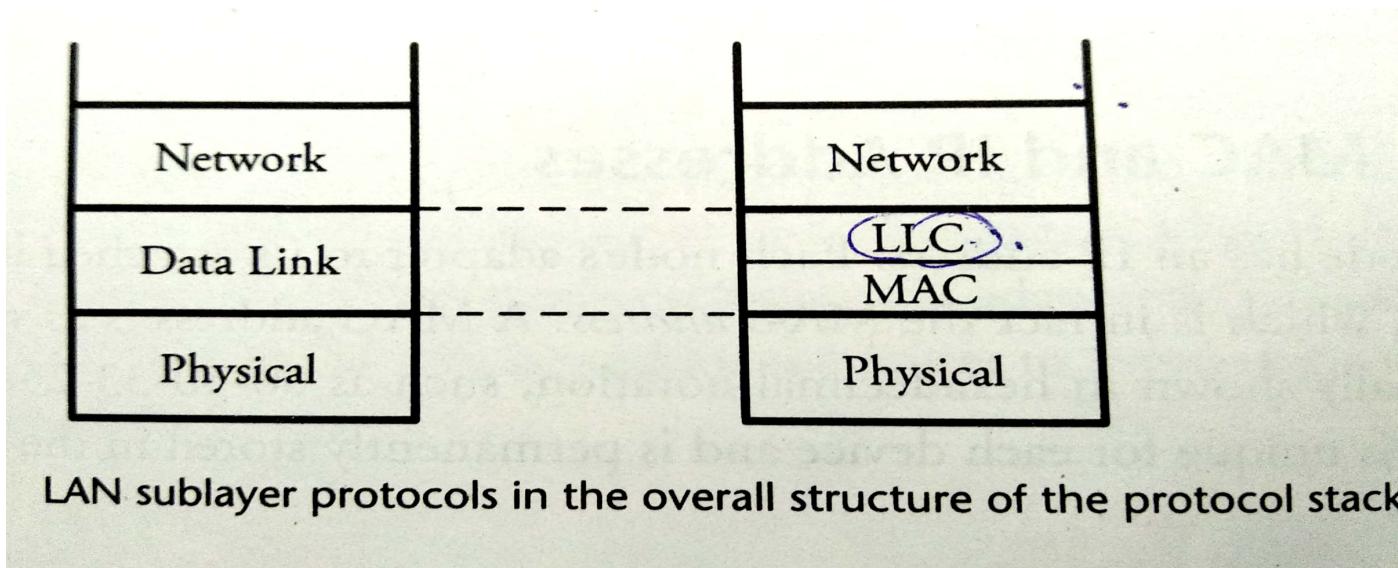
# LAN Protocols

- Protocols designed for Layer 3 is independent of the Underlying network topology.
- Hence, the protocols designed for LAN are normally considered with data link layer and physical layer.
- The physical layer is concerned with signal transmission, reception, encoding and decoding process.
- The IEEE 802 standard divides the data link layer in to two sub-layers called as Logical Link control (LLC) and Medium Access Control (MAC) Layers.

- The LLC layer implements flow control and error control apart from providing interface to the network.
- The MAC layer primarily controls the access to transmission medium and is responsible for framing.

## ■ Logical Link Layer (LLC)

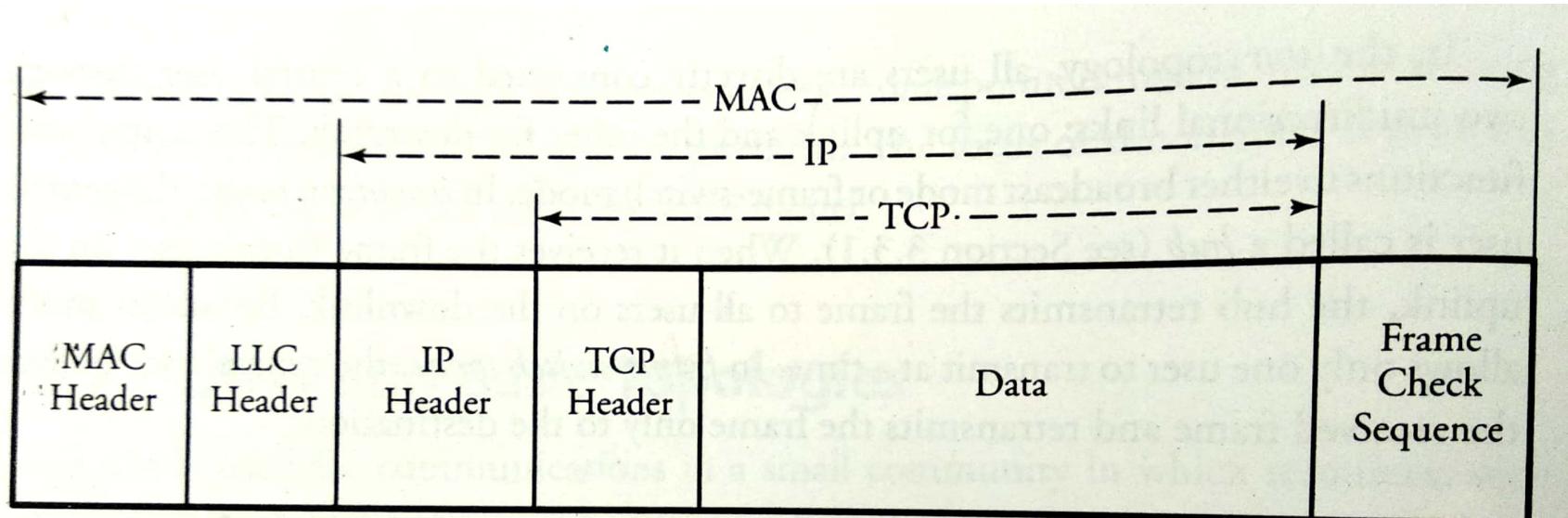
Data to be transmitted to the higher layers is passed down to the logical link layer, which determines the mechanism for addressing users across the medium.



- The LLC also controls the exchange of data between two users.
- LLC appends the header to form the LLC protocol data unit, which is then sent to the MAC layer.
- MAC layer which appends the header and the frame check sequence to create the MAC frame.

# Medium Access Control (MAC)

- A LAN is required to provide shared access to the transmission medium.
- To ensure efficient access to a medium, users has to satisfy some rules.
- The MAC format is given in the following figure



**Figure 5.3** Generic MAC frame format

- MAC header gives the MAC control information, such as MAC address of the destination and the priority level.
- LLC contains the data from the Logical Link layer.
- IP header specifies the IP header of the original packet.
- TCP header specifies the TCP header of the original packet.
- Frame checker sequence is used for error checking

# MAC and IP Addresses

- Each node has the IP Address.
- Each node's adapter to its attached link has a link layer address, which is known as the MAC address.
- A MAC address is as wide as 6 bytes

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

6 bytes = 12 hex digits = 48 bits

- MAC Address is unique for each device and is permanently stored in the adapter's read only memory.
- Consequently, networking manufacturers need to purchase MAC addresses for their products.
- Unlike an IP address, a MAC address is not hierarchical.
- The advantage of MAC addressing is that a device may not need to have an IP address in order to communicate with the surrounding devices in its own LAN.

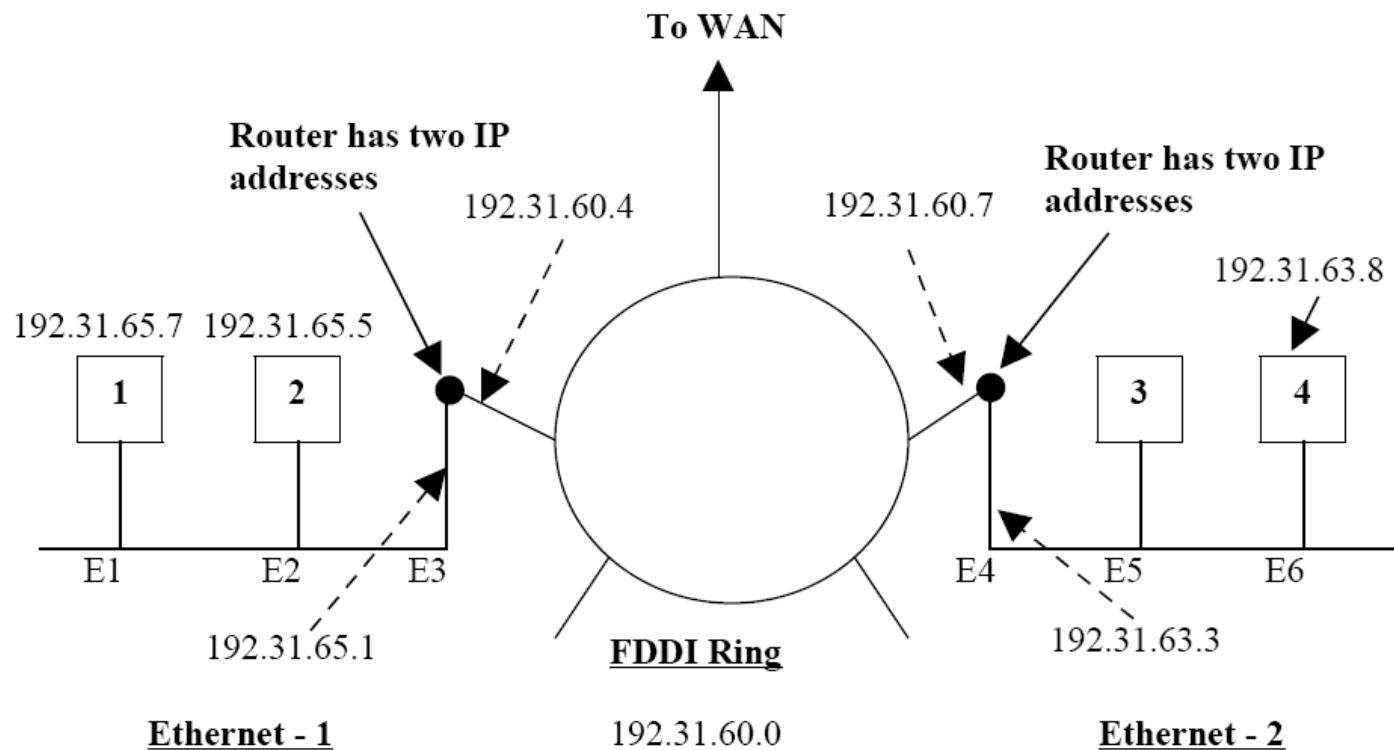
# Address Resolution Protocol (ARP)

- ARP is used to convert IP address to MAC addresses or vice versa.
- Suppose the user wants to transmit the packet to the destination.
- If it does not know the Link Layer Address of the destination.
- The sender broadcast the ARP packet requesting the link layer Address the

## ■ MAC and IP Address

- Address Resolution Protocol [ARP]
- Every host on the internet has one or more IP addresses
- For sending a packet these addresses are not used because the data link layer hardware, does not understand IP
- Nowadays, most hosts at companies and universities are attached to a LAN by an interface board that only understands LAN addresses.
- Manufacturers of Ethernet boards, request a block of addresses from a central authority to ensure no two boards have same address
- Ethernet boards send and receive frames based on **48 – bit Ethernet addresses** [They know nothing about 32 – bit IP addresses]

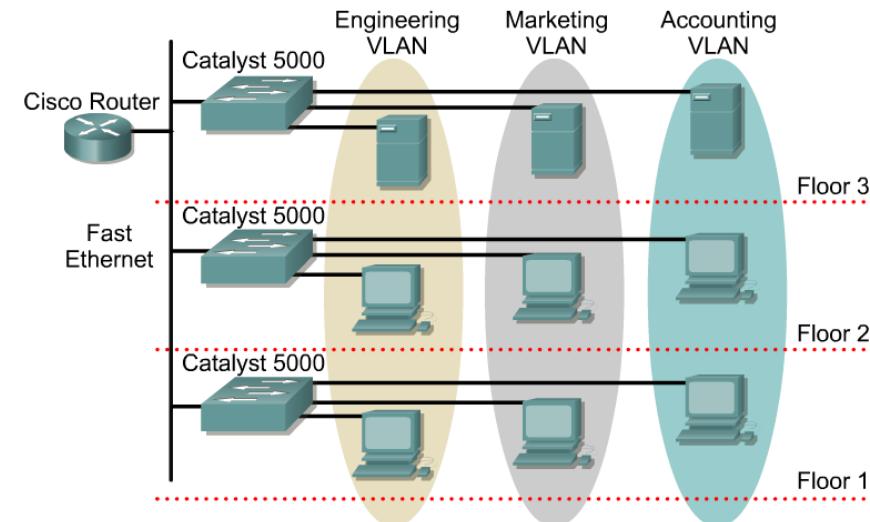
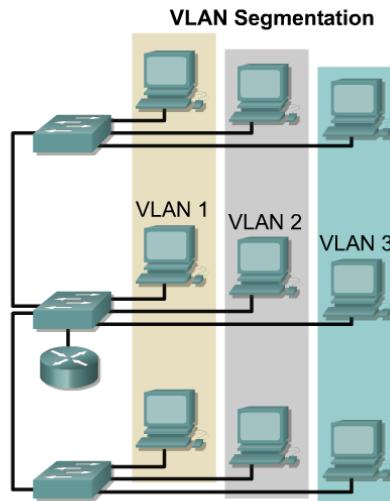
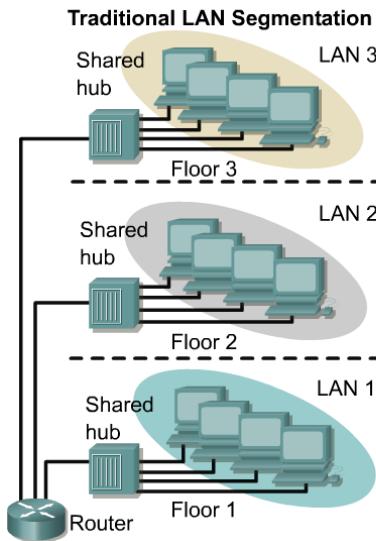
- How do IP addresses get mapped onto data link layer addresses [i.e. Ethernet] ?
- Example:
- In the below fig we have two Ethernet one with IP address 192.31.65.0 and one with 192.31.63.0
- These two are connected via FDDI [Fiber Distributed data Interface] ring with IP address 192.31.60.0, each machine on FDDI ring has an FDDI address, labeled through F1 to F3
- Each machine on Ethernet has Unique Ethernet address, [E1 through E6 ]



- **How user on host-1 sends a packet to a user on host-2?**
- Let us start out by seeing how a user on host 1 sends a packet to a user on host 2.
- Let us assume the sender knows the name of the intended receiver, possibly something like [mary@eagle.cs.uni.edu](mailto:mary@eagle.cs.uni.edu).
- The first step is to find the IP address for host 2, known as eagle.cs.uni.edu. This lookup is performed by the Domain Name System.
- For the moment, we will just assume that DNS returns the IP address for host 2 (192.31.65.5).
- The upper layer software on host-1 **builds a packet** with destination IP address and gives it to **IP software** to transmit
- The IP software checks whether the destination is on its own network
- But IP software, **needs a way** to find the destination Ethernet address
- **1st Solution:**
  - Using **Configuration File**, in the system maps IP addresses onto Ethernet addresses, In case of thousands of machines, updating these files is an error prone, time consuming job
- **2nd Solution:**
  - Host-1 output a **broadcast packet** on to Ethernet asking: **Who owns IP address 192.31.65.5?**
  - Every machine checks its IP addresses, host-2 alone respond with Ethernet address [E2]
  - Thus host-1 learns that IP address 192.31.65.5 is on host with Ethernet address [E2]
  - The protocol for asking this question and getting reply is called **Address Resolution Protocol [ARP]**

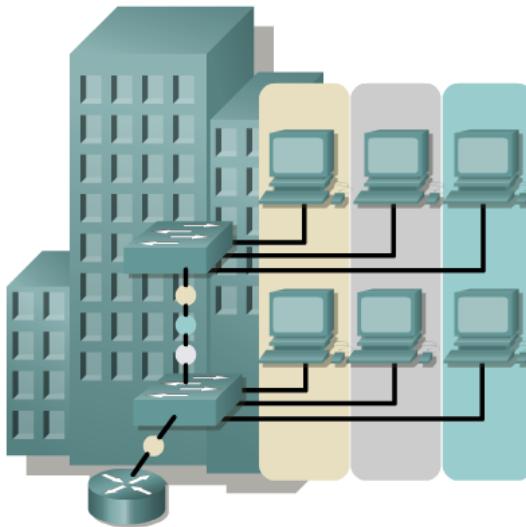
- **Reverse Address Resolution Protocol [RARP]**
  - ✖ Given an Ethernet address, what is the corresponding IP address? This problem occurs when booting a Diskless work station
  - ✖ The solution is to use the **RARP**
  - ✖ The RARP allow a newly booted workstation to broadcast its Ethernet address and say **“My 48 – bit Ethernet address is 14.04.05.18.01.25, Does any one out there know my IP address?”**
  - ✖ The **RARP Server**, sees this request, looks up the Ethernet address in its Configuration files and sends back the corresponding IP address
- ✖ **Drawbacks:**
  - ✖ RARP uses destination address of all 1's [i.e. limited broadcasting] to reach RARP server. However such a broadcast are not forwarded by routers, so RARP server is needed on each network
  - ✖ To overcome this drawback, use alternative Bootstrap protocol called **BOOTP**
  - ✖ BOOTP uses UDP messages, which forwarded over routers
  - ✖ It provides **additional information**, to diskless work station such as
    - > Include IP address of File server holding memory image
    - > IP address of default routers
    - > Subnet mask to use

# VLAN introduction



- **VLANs provide segmentation based on broadcast domains.**
- VLANs logically segment switched networks based on the functions, project teams, or applications of the organization regardless of the physical location or connections to the network.
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.

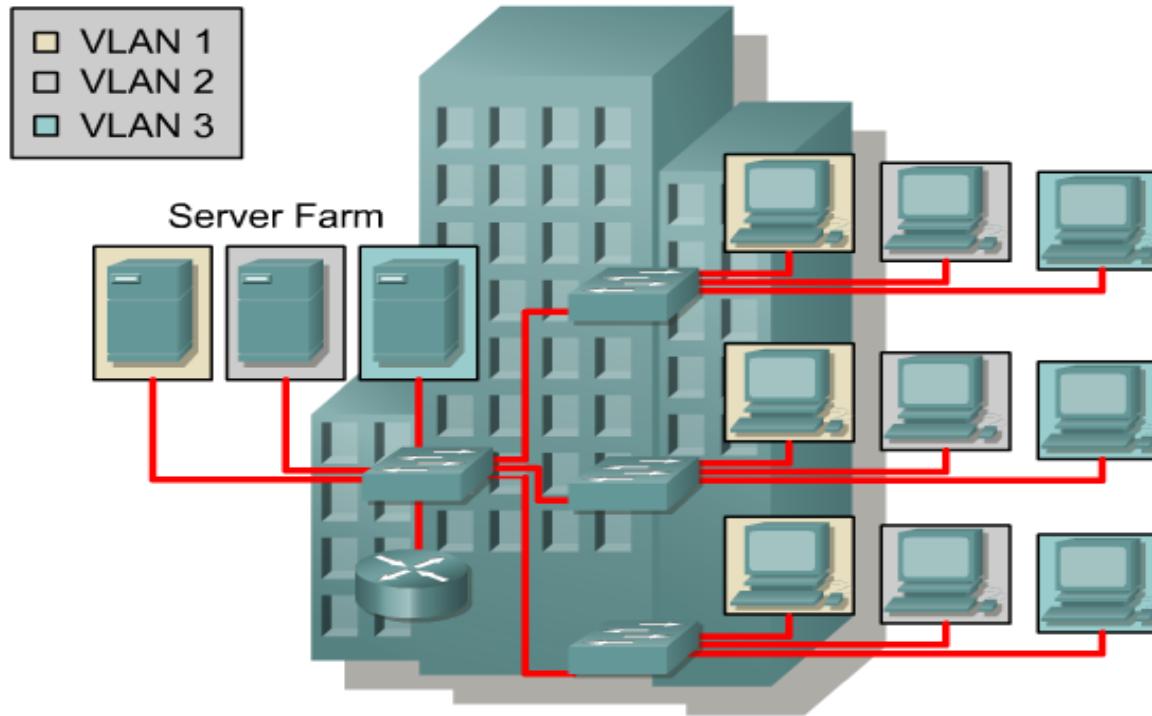
# VLAN introduction



- A group of ports or users in same broadcast domain
- Can be based on port ID, MAC address, protocol, or application
- LAN switches and network management software provide a mechanism to create VLANs
- Frame tagged with VLAN ID

- **VLANs are created to provide segmentation services traditionally provided by physical routers in LAN configurations.**
- VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain.
- Traffic should only be routed between VLANs.

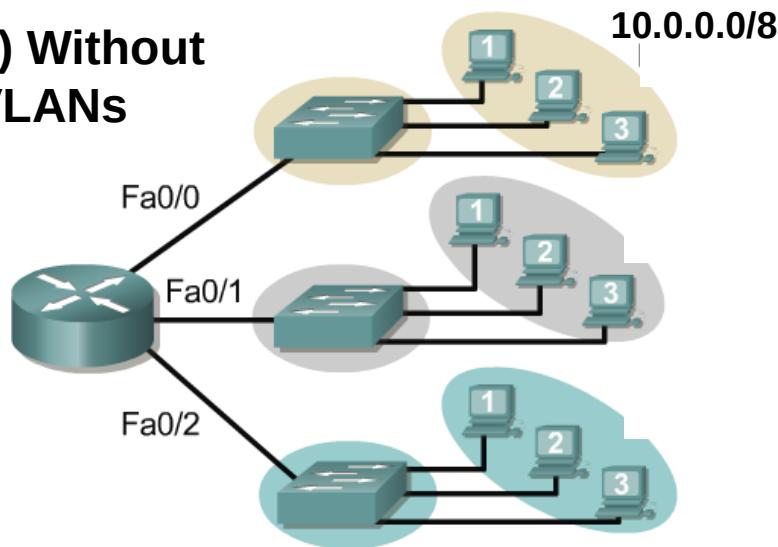
# Broadcast domains with VLANs and routers



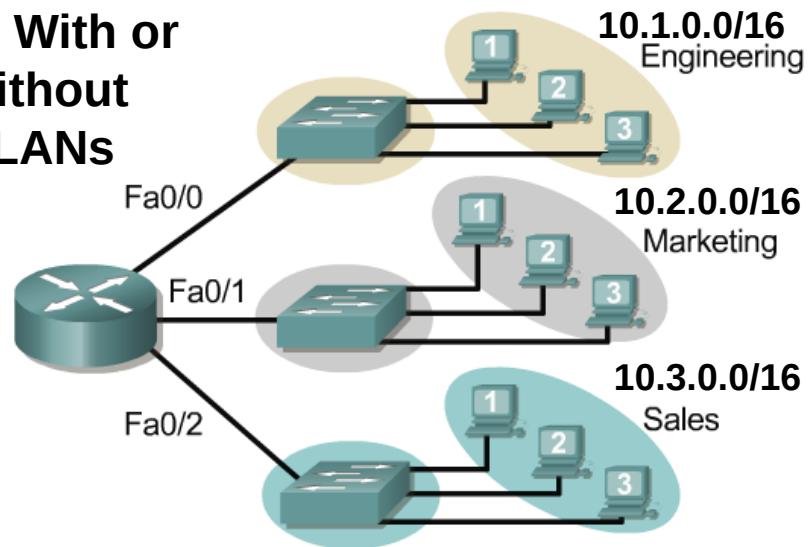
- A VLAN is a broadcast domain created by one or more switches.
- The network design above creates three separate broadcast domains.

# Broadcast domains with VLANs and routers

## 1) Without VLANs



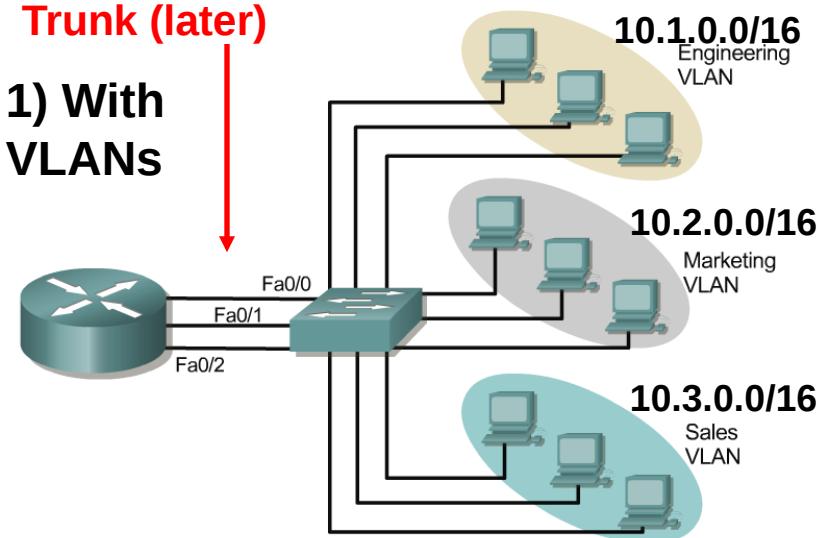
## 2) With or without VLANs



- 1) No VLANs, or in other words, One VLAN. Single IP network.
- 2) With or without VLANs. However this can be and example of no VLANs. In both examples, each group (switch) is on a different IP network.
- 3) Using VLANs. Switch is configured with the ports on the appropriate VLAN.

**One link per VLAN or a single VLAN Trunk (later)**

## 1) With VLANs



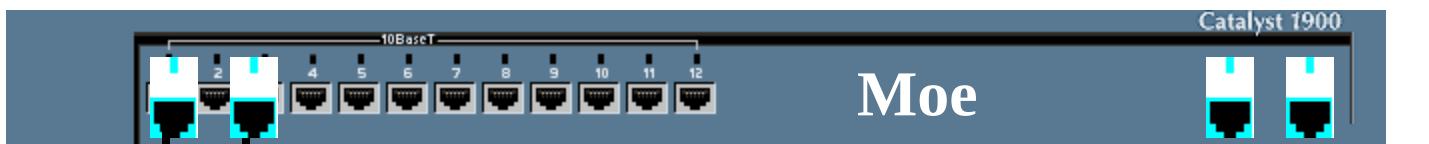
# Non-tagging Switches

- Lets first see how multiple VLANs are interconnected using switches that do not have the tagging capability.

# Non-tagging Switches

For each VLAN, there must be a link between the two switches. One link per VLAN. Be sure the switch ports on the switches are configured for the proper VLAN.

**Port 1 = VLAN 1 & Port 2 = VLAN 2**

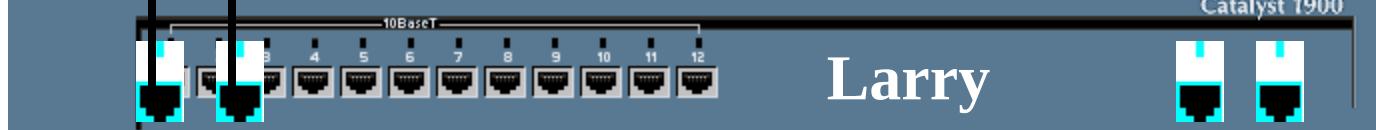


1  
2

VLAN 1: Port 1 on switch Moe is connected to Port 1 on Switch Larry.

VLAN 2: Port 2 on switch Moe is connected to Port 2 on Switch Larry.

1  
2



**Port 1 = VLAN 1 & Port 2 = VLAN 2**

**100BaseT Ports**

# Advantages

- Each VLAN gets its own dedicated link with its own bandwidth.

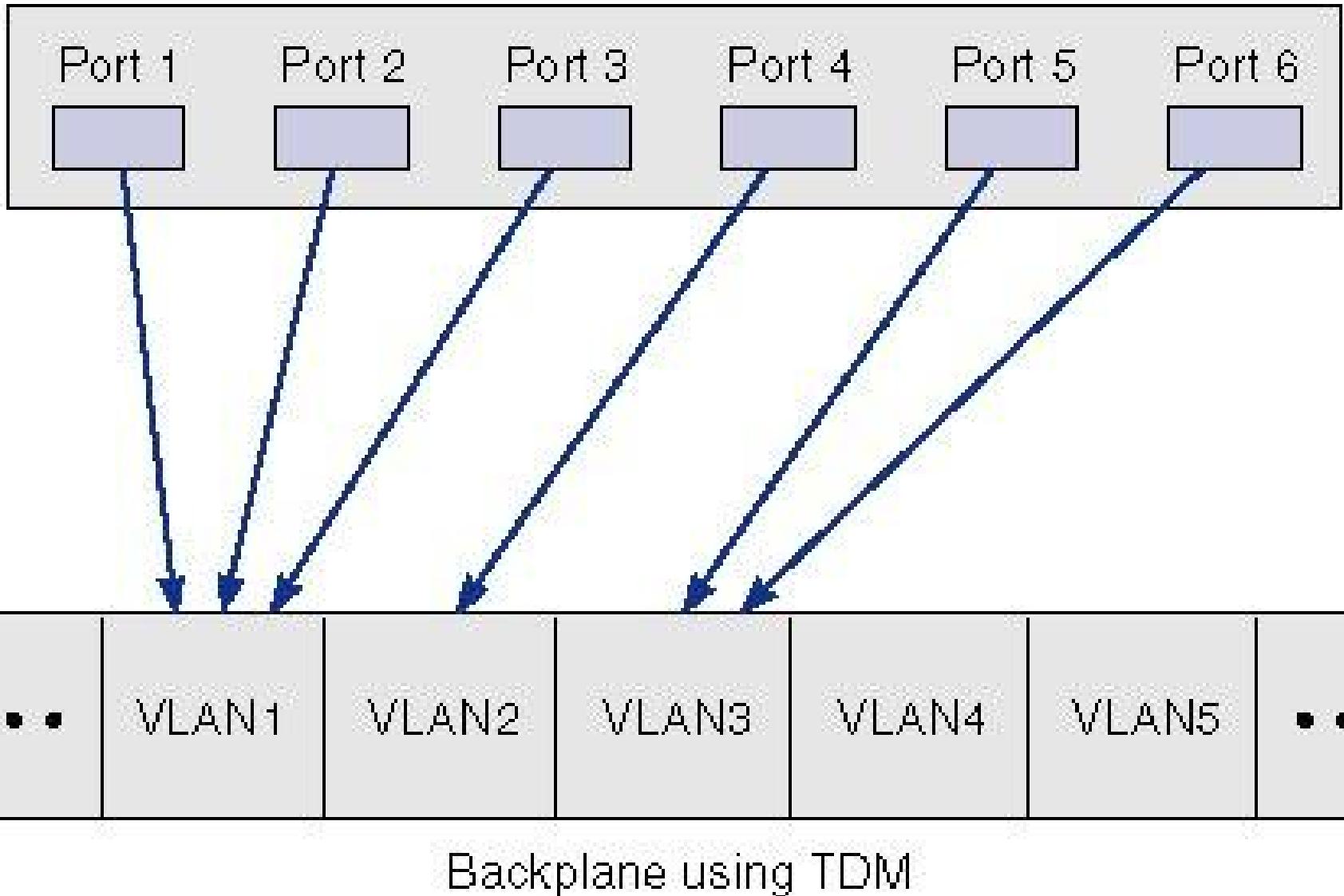
# Disadvantages

- This requires a separate link for each VLAN. There may not be enough ports on the switch to accommodate a lot of different VLANs.

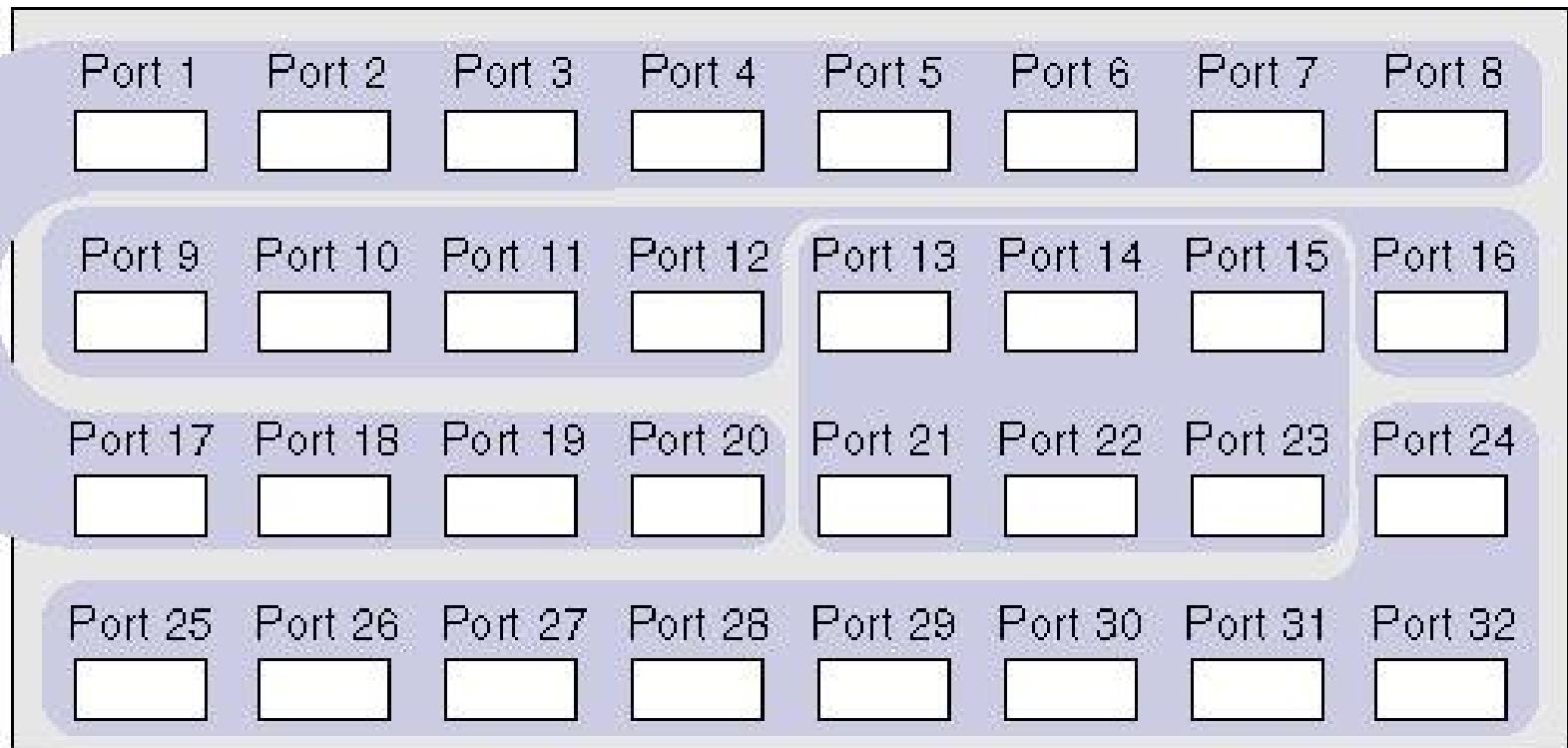
# Port-Based VLANs (Layer-1 VLANs)

- Port-based VLANs use the physical port address to form the groups for the VLAN.
- It is logical to connect computers that are physically close together on the LAN into ports that are physically close together on the switch, and to assign ports that are physically close together into the same VLAN.
- This is the approach used in traditional LAN design: physical location determines the LAN, but is not always the most effective approach.

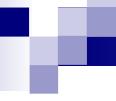
# Port-Based VLANs



# VLAN Example



VLANs used to balance capacity against network traffic



# MAC-Based VLANs

## Layer-2 VLANs

- MAC-based VLANs use the same data link layer addresses to form the VLAN groups.
- The advantage is that they are simpler to manage when computers are moved.

## Layer-3 VLANs

- IP-based VLANs use the network layer address (i.e. TCP/IP address) to form the VLAN groups. Layer-3 VLANs reduce the time spent reconfiguring the network when a computer is moved as well.
- Some layer-3 VLANs can also use the network layer protocol to create VLAN groups. This flexibility enables manager even greater precision in the allocation of network capacity.

## Layer-4 VLANs

- Application-based VLANs use the application layer protocol in combination with the data link layer and network layer addresses to form the VLAN groups.
- The advantage is a very precise allocation of network capacity.