SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited with 'A' grade by NAAC
Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai - 600 119.

# SCSA1502-COMPUTER NETWORKS AND DESIGN

## UNIT - II

# SCSA1502-COMPUTER NETWORKS AND DESIGN

## Unit II-Underlying LAN Concepts

# UNIT 2

# UNDERLYING LAN CONCEPTS

LAN connectivity for small businesses – Integration – Token-Ring – Ethernet – ATM LAN emulation – Inter LAN Switching – LAN to Mainframe – Building networks.

# COURSE OBJECTIVE'S

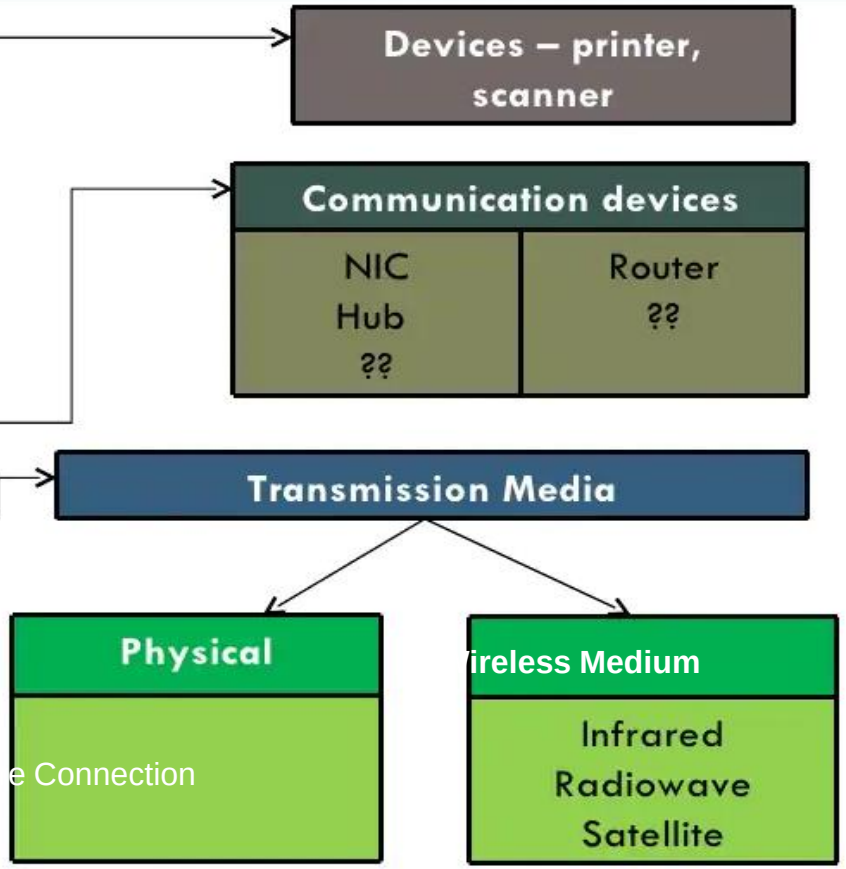
- To recognize the principles of the big picture of computer networks.
- To understand the networking environment.
- To know the importance of VPNs.
- To convey the availability of tools and techniques for networking.
- To discuss about evolving technologies in networks.

# COURSE OUTCOME

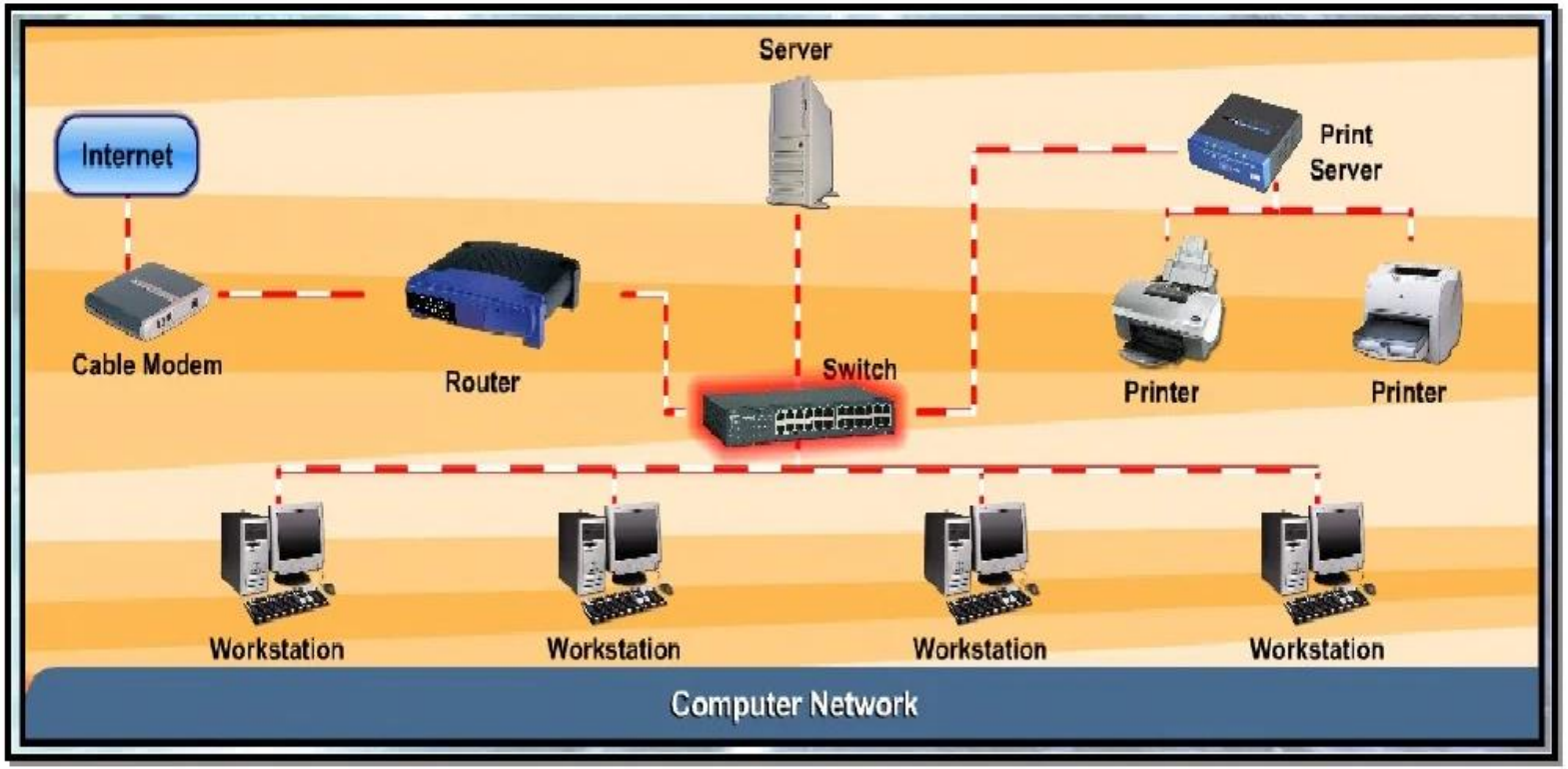
- CO1 - Understand the principles of networks.
- CO2 - Interpret LAN concepts and design.
- CO3 - Gain knowledge in evolving technologies.
- CO4 - Clearly outline the logic behind VPNs.
- CO5 - Know the importance of tools and techniques in building a network.
- CO6 - Understand the underlying working concepts of a real-time network.

# Definition of computer networks

**A computer network** is a collection of **computers** and **devices** connected together via **communication devices** and **transmission media**. For examples it may connect computers, printers and scanners.



# Typical network architecture




General structure of a Computer Network

# Need for Networking

- Resource sharing -Through a network , data , s/w and h/w resources can be shared irrespective of the physical location of the resources and the user.
- Reliability – A file can have its copies on two or more computers of the network
- Cost – Sharing resources reduces the cost
- Communication – Information can be exchanged at a very fast speed

# Network Components

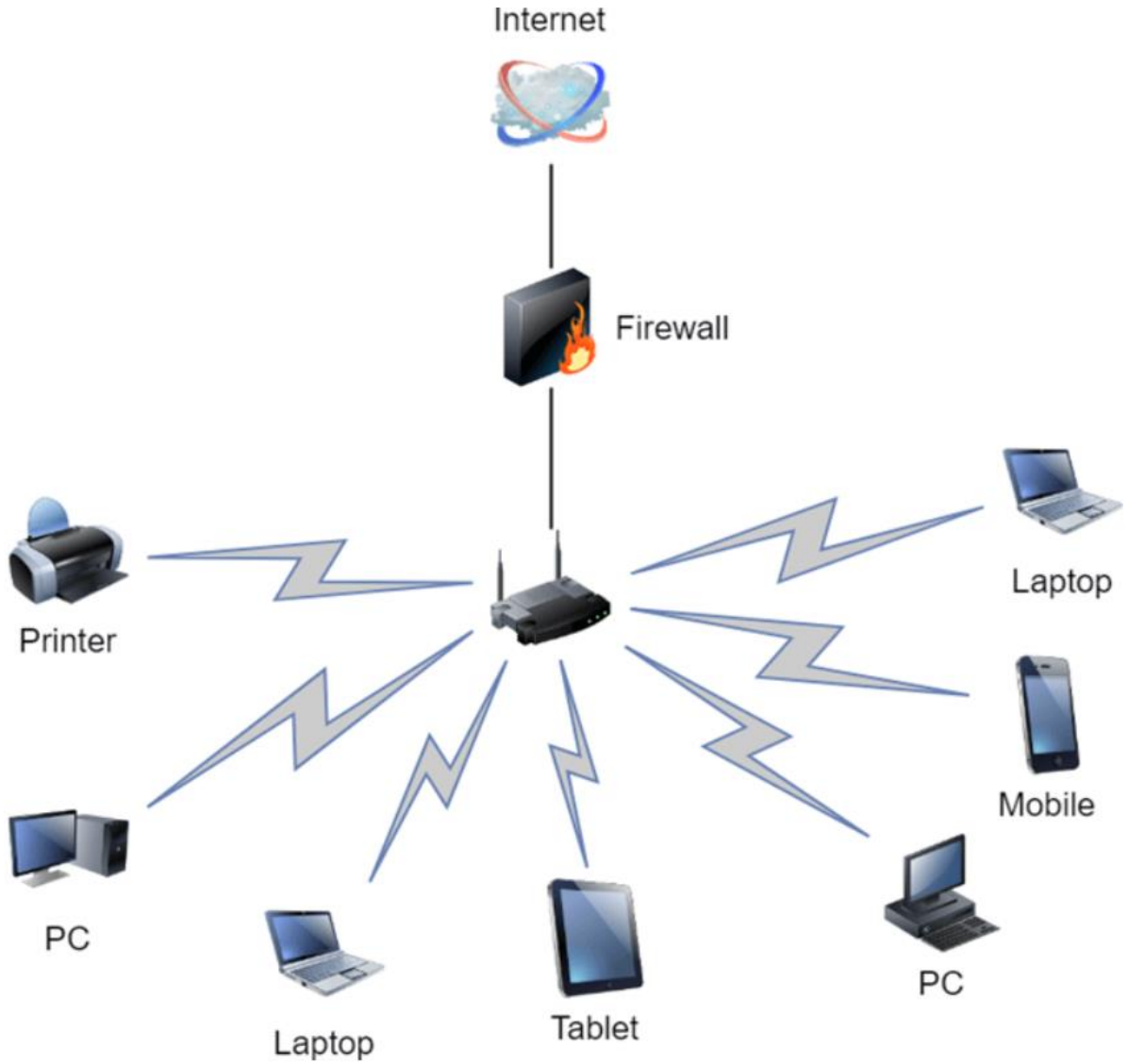


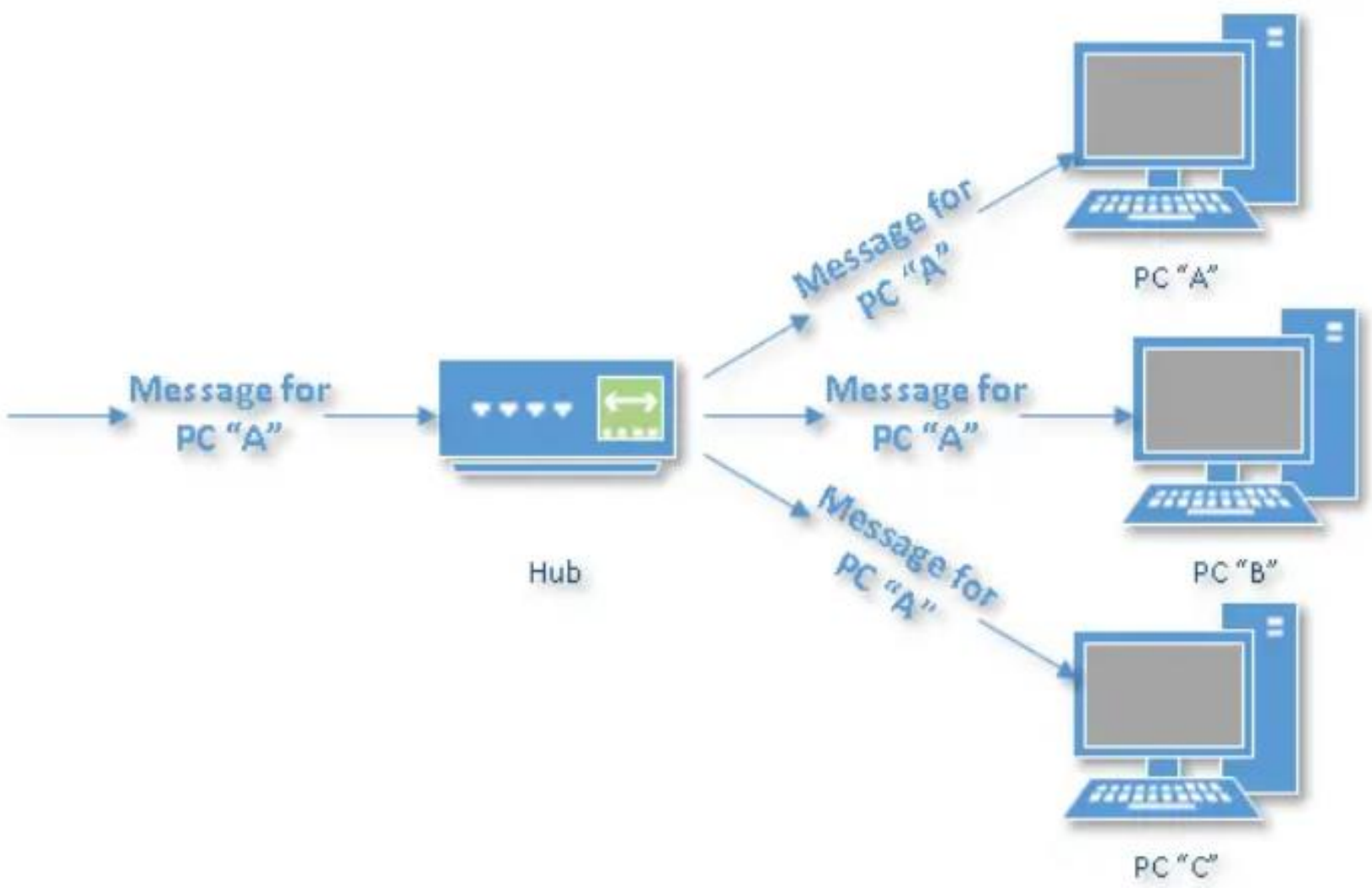

Image Courtesy:Basics of Computer Networking: What is, Advantages, Components, Uses (guru99.com)

# SWITCHES / HUB

- A switch (**switch**ing hub) in the context of networking refers to a device which filters and forwards data packets across a network.
- Unlike a standard hub which simply replicates what it receives on one port onto all the other ports, a switching hub keeps a record of the MAC addresses of the devices attached to it.
- When the switch receives a data packet, it forwards the packet directly to the recipient device by looking up the MAC address.
- A network switch can utilize the full throughput potential of a networks connection for each device making it a natural choice over a standard hub.
- In other words, say for instance you had a network of 5 PCs and a server all connected with 10Mbps UTP cable, with a hub the throughput (10Mbps) would be shared between each device, with a switch each device could utilize the full 10Mbps connection.

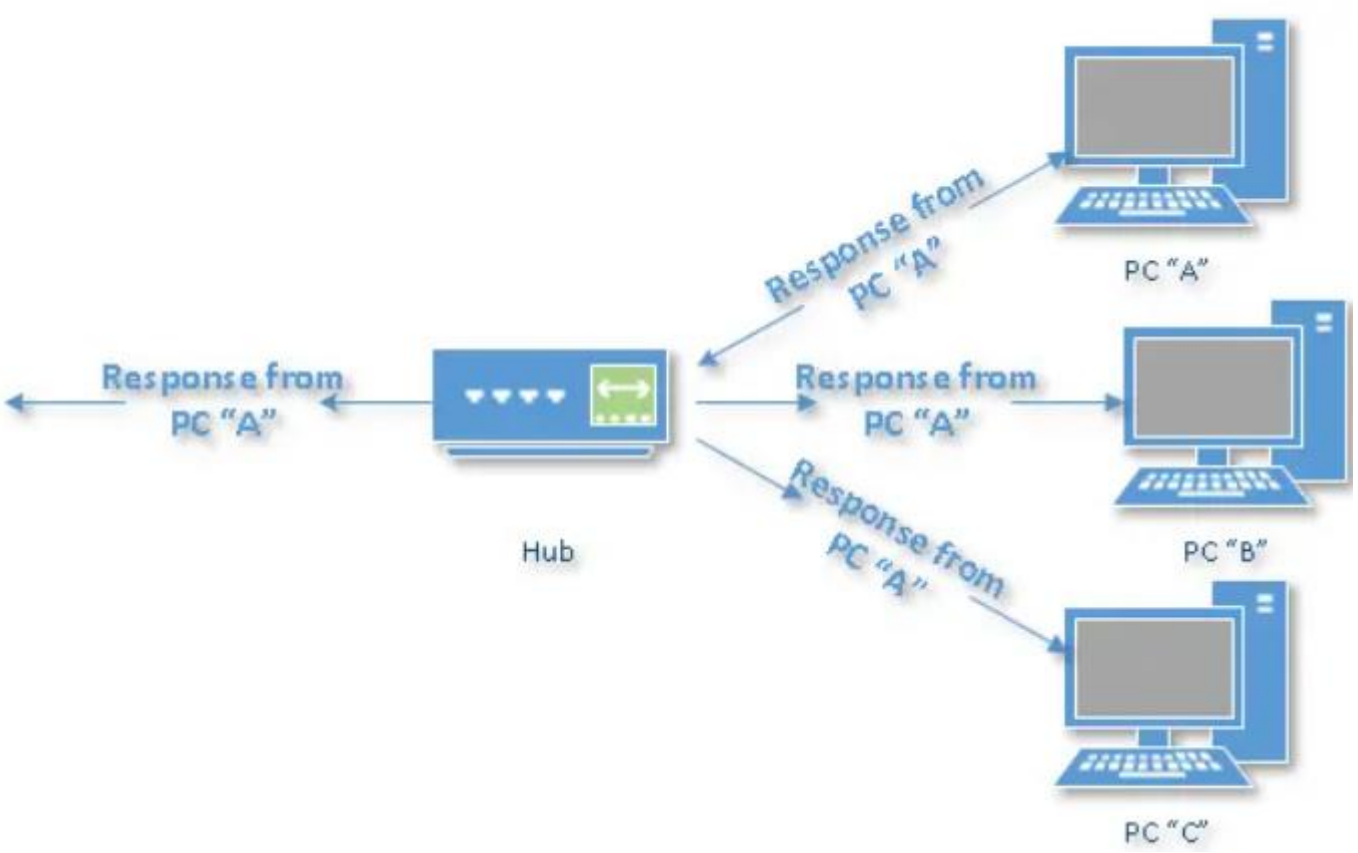
# HUBS

- **Incoming data passing through a hub**



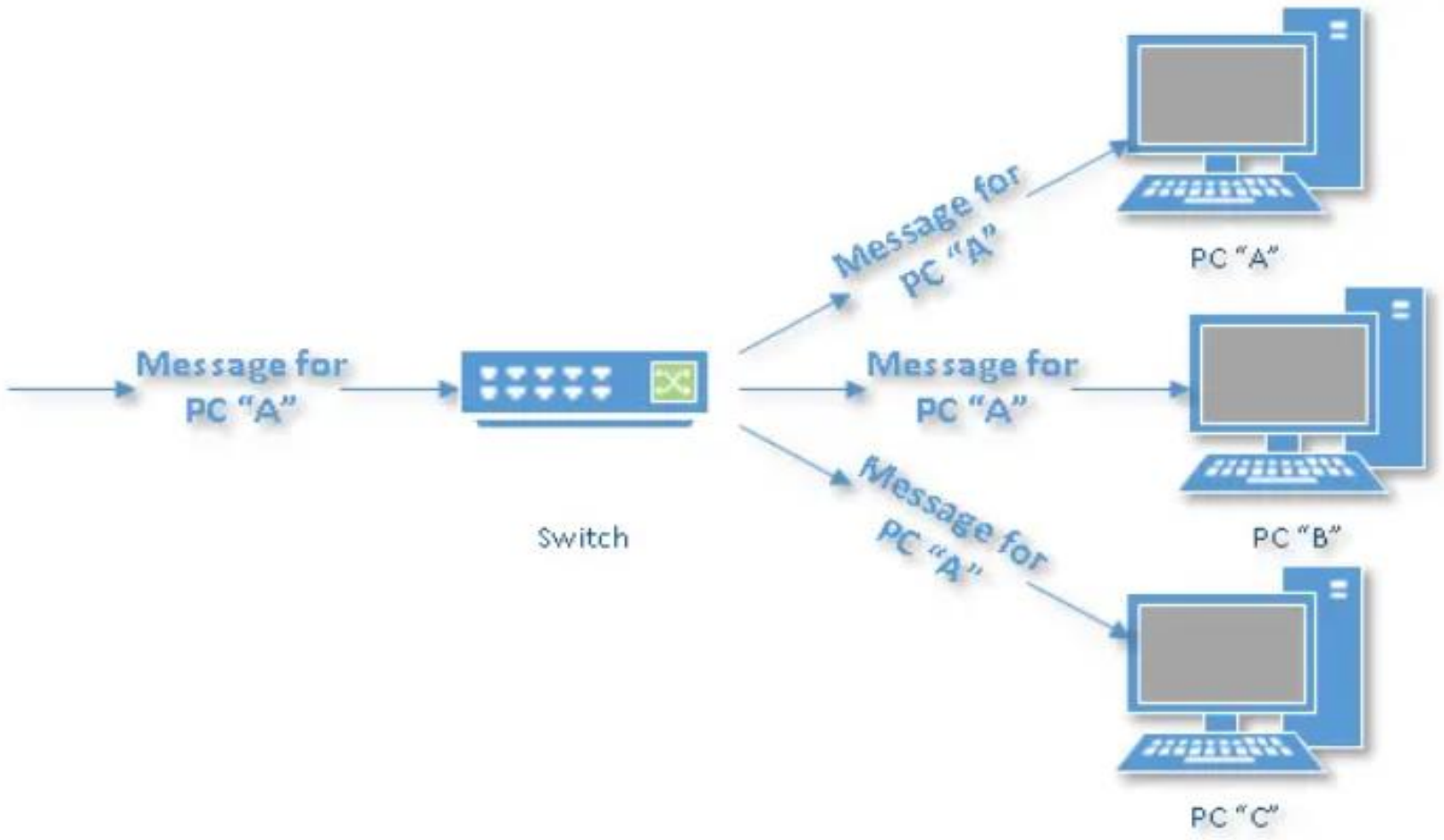
# HUBS

**Returned response passing through a hub.**



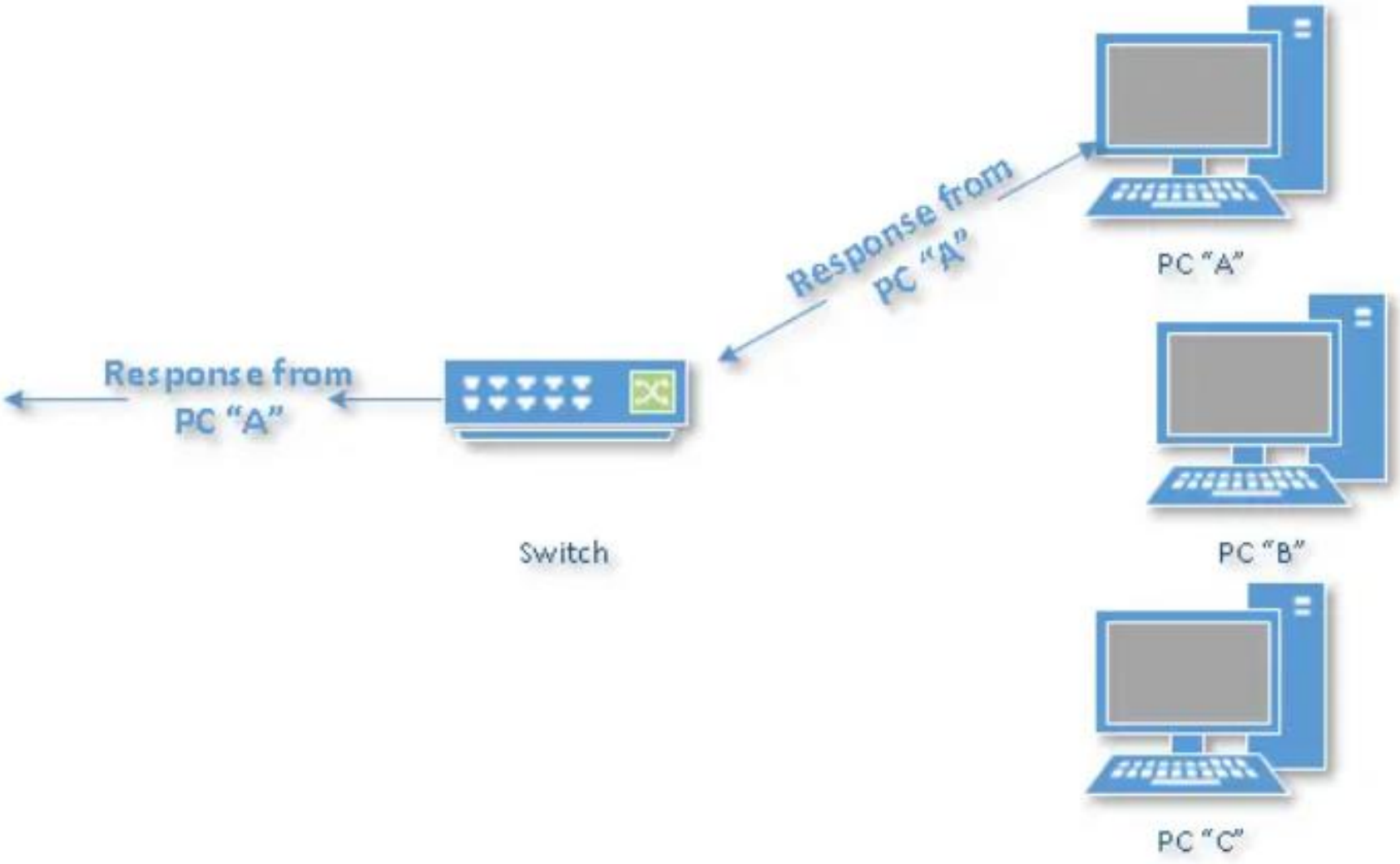
# SWITCH

- **Incoming data passing through a switch**



# SWITCH

- Returned response passing through a switch

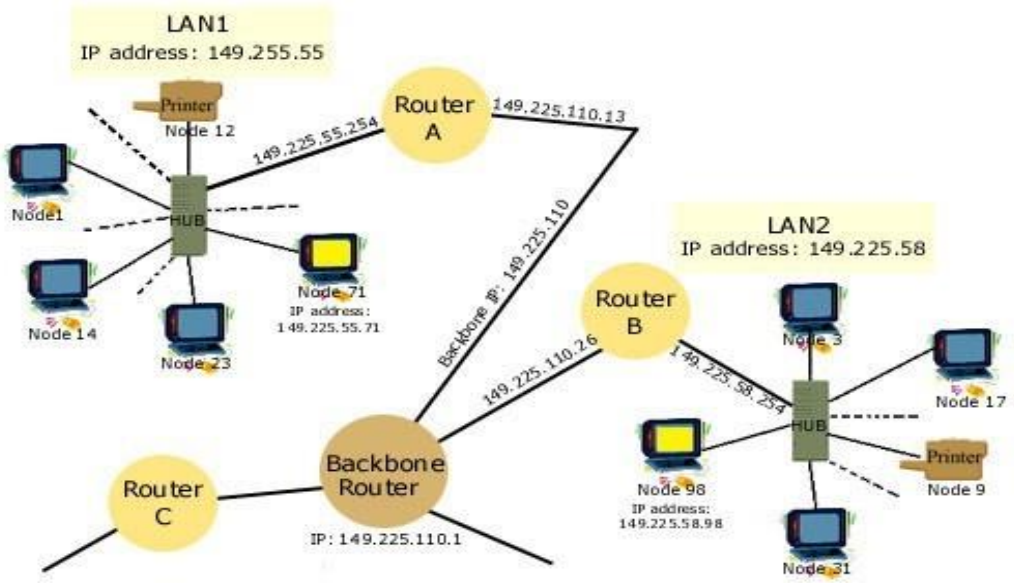


# DIFFERENCE BETWEEN HUB AND SWITCH

| HUB | SWITCH |
|---|---|
| Hub is operated on **Physical layer of OSI model**. | While switch is operated on **Data link layer of OSI Model**. |
| Hub is a broadcast type transmission. | While switch is a Unicast, multicast and broadcast type transmission. |
| Hub have 4/12 ports. | While switch can have 24 to 48 ports. |
| In hub, there is only one collision domain. | While in switch, different ports have own collision domain. |
| Hub is a half duplex transmission mode. | While switch is a full duplex transmission mode. |
| In hub, Packet filtering is not provided. | While in switch, Packet filtering is provided. |
| Hub cannot be used as a repeater. | While switch can be used as a repeater. |
| Hub is not an intelligent device that sends message to all ports hence it is comparatively inexpensive. | While switch is an intelligent device that sends message to selected destination so it is expensive. |
| Hub is simply old type of device and is not generally used. | While switch is very sophisticated device and widely used. |
| Hacking of systems attached to hub is complex. | Hacking of systems attached to switch is little easy. |

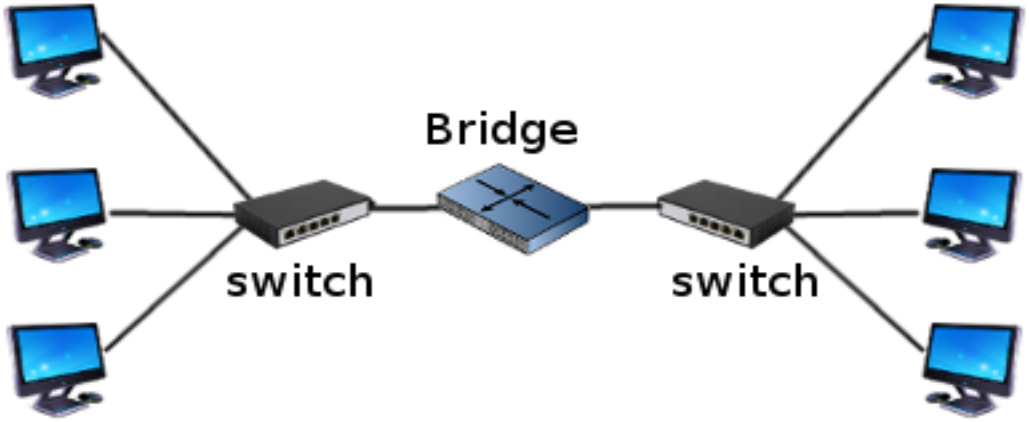
# ROUTERS

- ✓ A router is a device or a software in a computer that determines the next network point to which a packet should be forwarded toward its destination
- ✓ Allow different networks to communicate with each other
- ✓ A router creates and maintain a table of the available routes and their conditions and uses this information along with distance and cost algorithms to determine the best route for a given packet
- ✓ A packet will travel through a number of network points with routers before arriving at its destination



# BRIDGES

- A bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring)
- A bridge examines each message on a LAN, "passing" those known to be within the same LAN, and forwarding those known to be on the other interconnected LAN (or LANs)

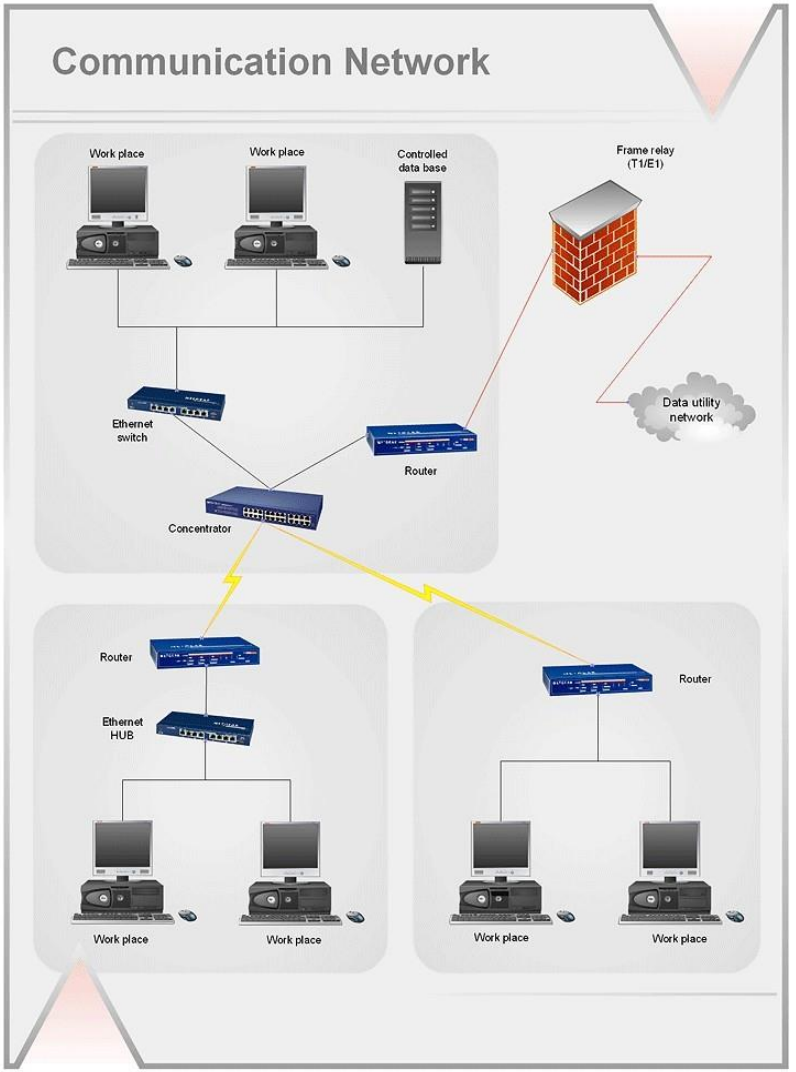


# ROUTER's Vs BRIDGE's

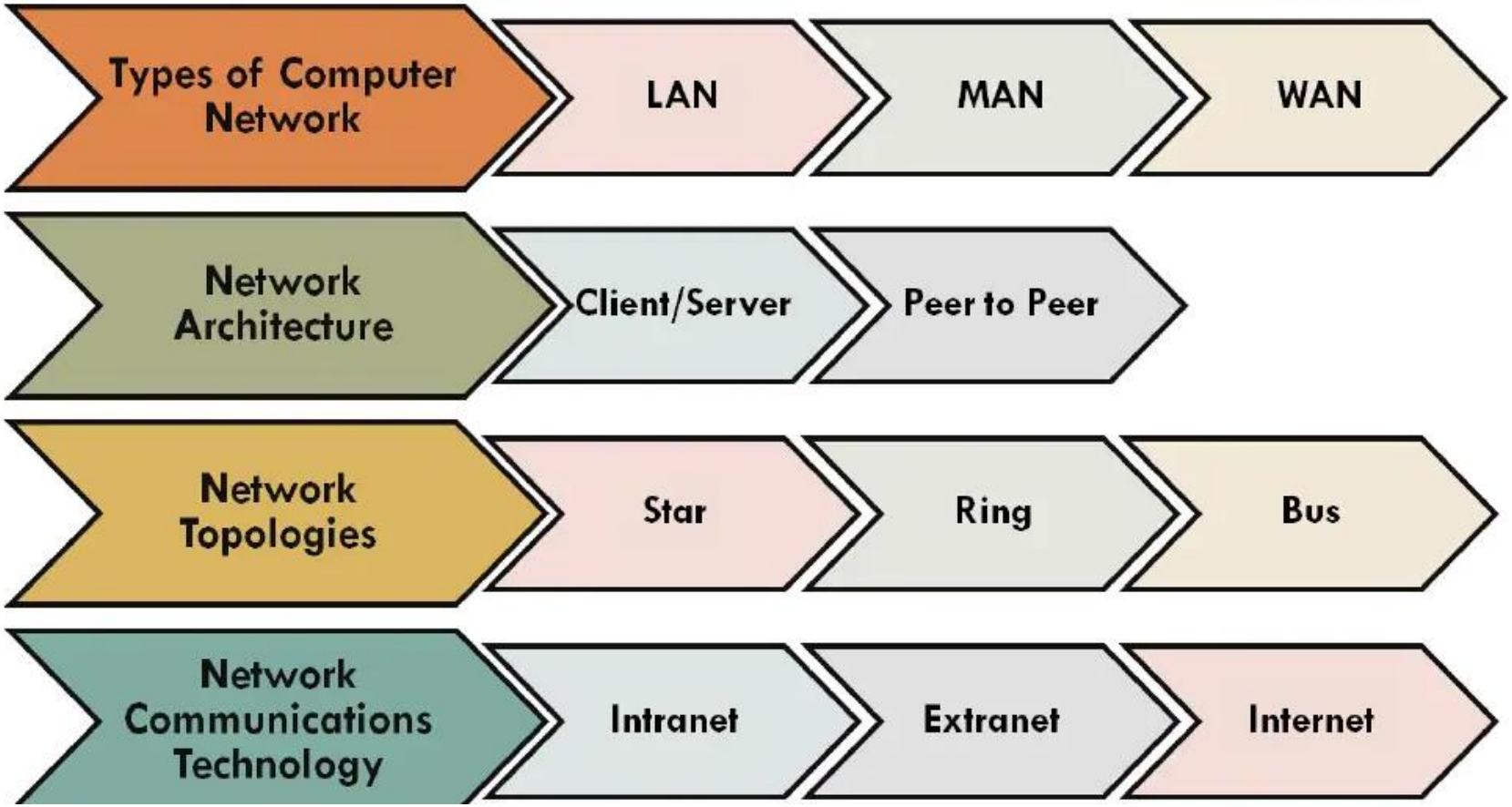
| S.NO | Bridge | Router |
|---|---|---|
| 1. | Bridge works in **data link layer.** | Router works in **network layer**. |
| 2. | Through bridge, data or **information is not stored and sent in the form of packet**. | Through router, data or information is **stored and sent in the form of packet**. |
| 3. | There are **only two ports** in bridge. | While there are **more than two ports** in router. |
| 4. | **Bridge connects two different LANs.** | Router is used by LAN as well as MAN for **Connection of nodes**. |
| 5. | In bridge, routing table is not used. | While in routers, **routing table is used**. |
| 6. | Bridge works on single broadcast domain. | While router works on more than single broadcast domain. |
| 7. | Bridges are easy to configure. | While Routers are difficult to setup and configure. |
| 8. | **Bridge focuses on MAC address** . | **Router focuses on protocol address.** |
| 9. | Bridge is comparatively inexpensive. | While Router is relatively expensive device. |
| 10. | Bridges are good for segment network and extends the existing network. | While Routers are good for joining remote networks. |

# GATEWAY

- Gateway is considered as a networked device that acts as an entry point from one network to other networks
- Gateway is a device that connects dissimilar networks.
- Establishes intelligent connection between a local network and external networks with completely different structures
- A gateway acts as a safeguard to all local networks and connects the local networks to public networks.
- It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway

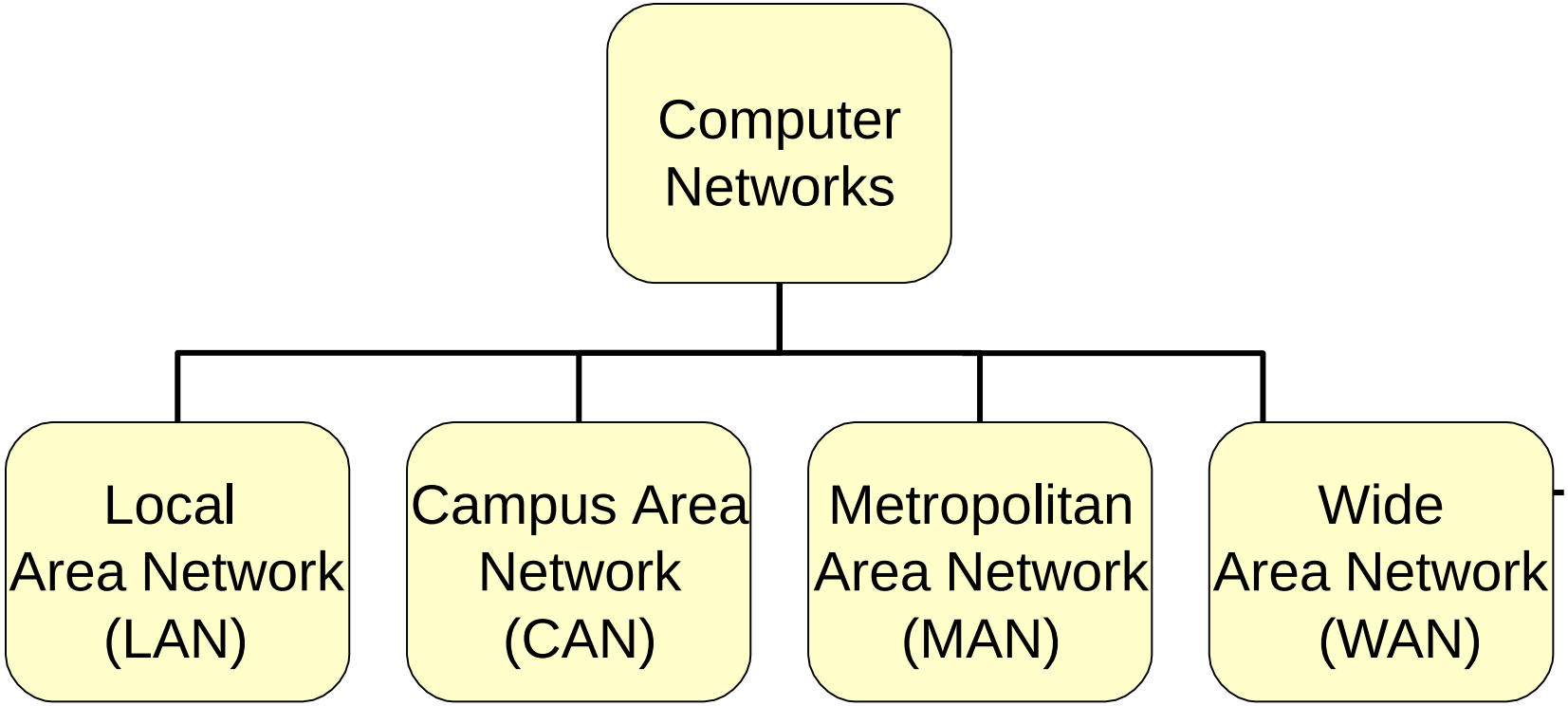


# CLASSIFICATIONS



# Types of Computer Networks

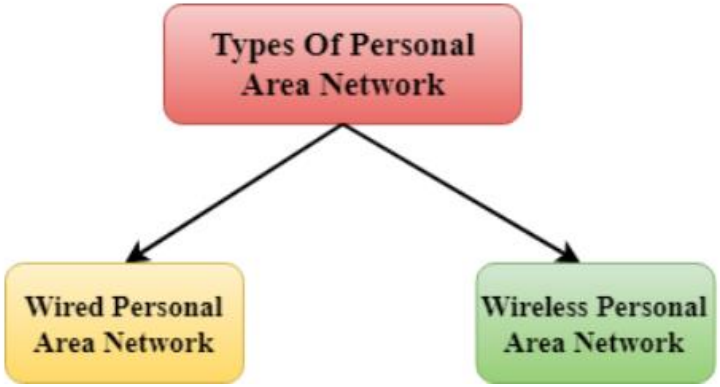
- Networks are classified depending on the geographical area covered by the network



# Personal Area Network

- PAN networks are usually wireless, established in an on- demand or ad-hoc fashion when needed to communicate between two or more devices.
- PAN networks can be used between devices owned by two different parties, or between two devices owned by one person, such as a PDA and a laptop or mobile phone.
- These networks are usually characterized as short-range, often limited to 10 meters or less in range.

Example: Bluetooth



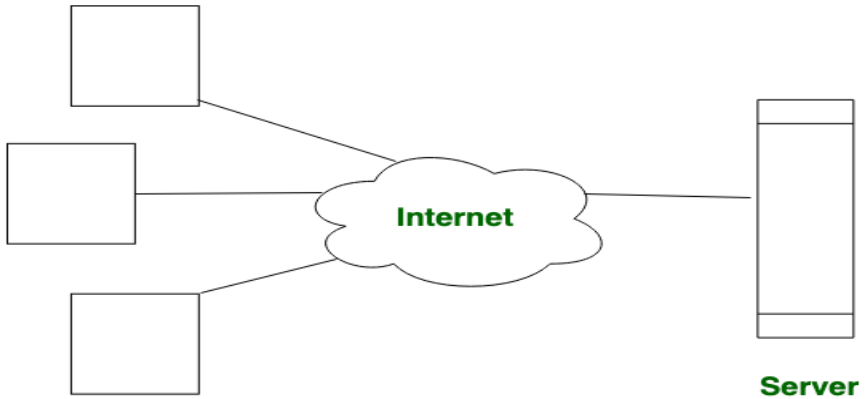

# Network Architecture

Major (Two) classifications based on Architecture are

- Peer-to-Peer network
- Server based network

# Client Server Application

- This model are broadly used network model.
- In Client-Server Network, Clients and server are differentiated, Specific server and clients are present.
- In Client-Server Network, Centralized server is used to store the data because its management is centralized. In Client-Server Network, Server respond the services which is request by Client.




Client-Server Network Model

# Advantages and disadvantages

Advantages of client/server networks

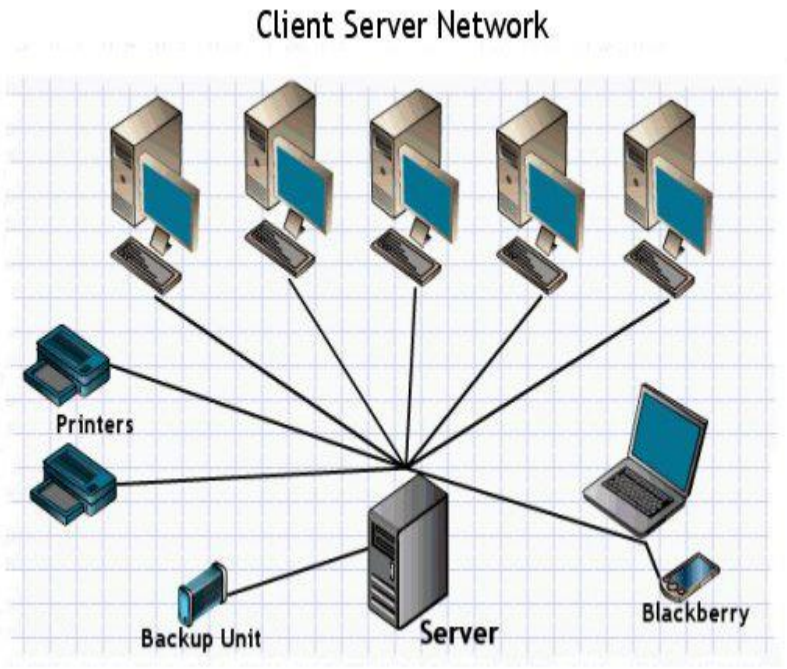
- Facilitate resource sharing – centrally administrate and control
- Facilitate system backup and improve fault tolerance
- Enhance security – only administrator can have access to Server
- Support more users – difficult to achieve with peer-to-peer networks

Disadvantages of client/server networks

- High cost for Servers
- Need expert to configure the network
- Introduce a single point of failure to the system

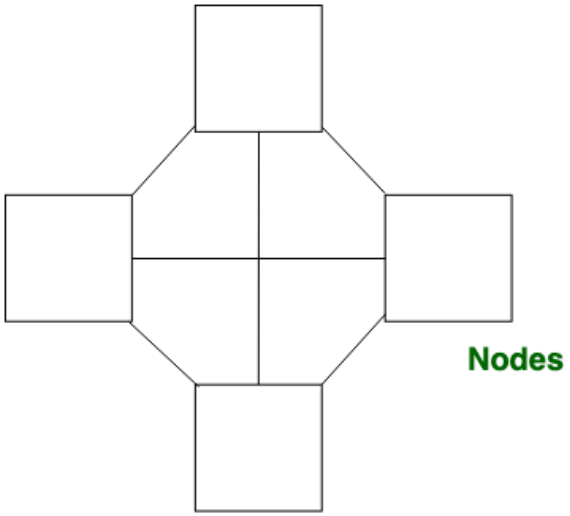
# Application

- Mail server
- Application server
- Message server
- Proxy server
- Database server
- Web server



# Peer to Peer network

- This model does not differentiate the clients and the servers
- In this each and every node is itself client and server.
- In Peer-to-Peer Network, Each and every node can do both request and respond for the services.




Peer-to-Peer Network Model

# Peer to Peer network

- In the P2P (Peer-to-Peer) network, “peers” generally represent computer system.
- These peers are connected to each other with help of Internet.
- Files might be shared directly without requirement of central server among these systems on the network.
- In this architecture, system is generally decomposed into various computational nodes that contain the same and equivalent capabilities, abilities, and responsibilities.

# Advantages and disadvantages

Advantages of peer-to-peer networks:

- Low cost
- Simple to configure
- User has full accessibility of the computer

Disadvantages of peer-to-peer networks:

- May have duplication in resources
- Difficult to uphold security policy
- Difficult to handle uneven loading

Where peer-to-peer network is appropriate:

- 10 or less users
- No specialized services required
- Security is not an issue
- Only limited growth in the foreseeable future

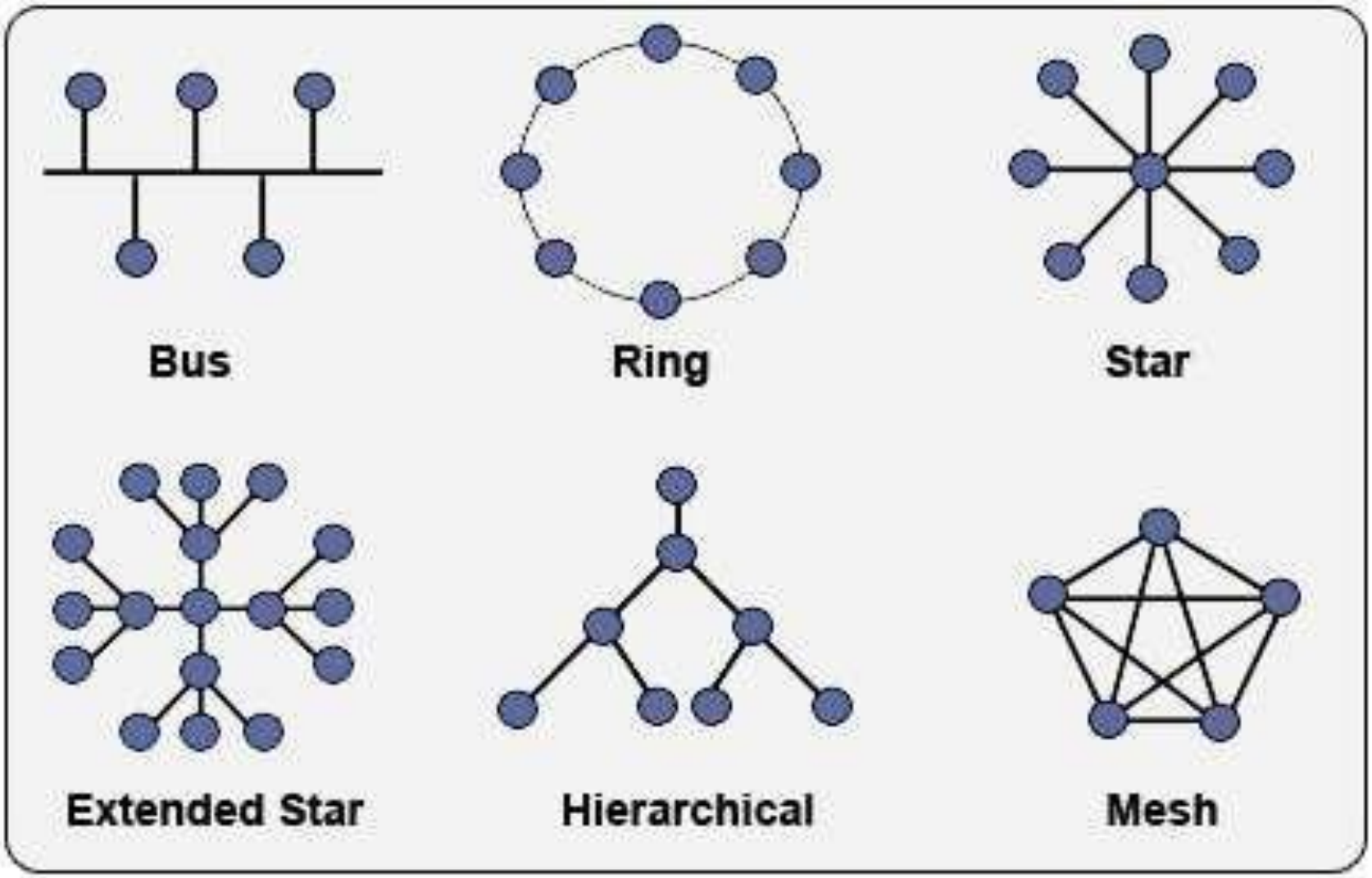
# LAN Architecture

- Topologies
- Transmission medium
- Layout
- Medium access control

# Topology

- Topology refers to the layout of connected devices on a network.
- Here, some logical layout of topology.
  - Mesh
  - Star
  - Bus
  - Ring
  - Tree and Hybrid

# Network Topology



# Considerations for choosing topology

- Money-Bus n/w may be the least expensive way to install a n/w.
- Length-of cable needed- the linear bus n/w uses shorter lengths of cable.
- Future growth-with star topology, expending a n/w is easily done by adding another devices.
- Cable type-most common used cable in commercial organization is twisted pair. Which often used with star topologies.

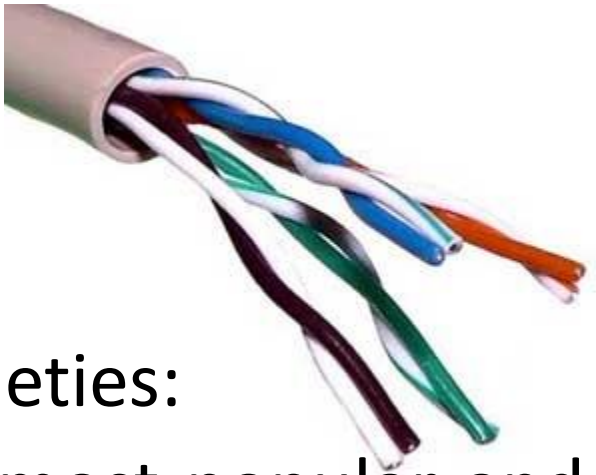
# LAN transmission medium

- **What is Network Cabling?**
- Cable is the medium through which information usually moves from one network device to another.
- There are several types of cable which are commonly used with LANs.
- In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types.
- The type of cable chosen for a network is related to the network's topology, protocol, and size.

# Types of cables used in networks

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable

# Twisted pair cable



- Twisted pair cabling comes in two varieties:
- Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks.
- The quality of UTP may vary from telephone-grade wire to extremely high-speed cable.
- The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices.
- The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot.

# Categories of Unshielded Twisted Pair

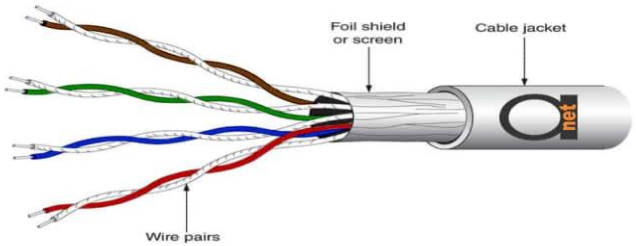
| Category | Speed | Use |
|---|---|---|
| 1 | 1 Mbps | Voice Only (Telephone Wire) |
| 2 | 4 Mbps | LocalTalk & Telephone (Rarely used) |
| 3 | 16 Mbps | 10BaseT Ethernet |
| 4 | 20 Mbps | Token Ring (Rarely used) |
| 5 | 100 Mbps (2 pair) | 100BaseT Ethernet |
| | 1000 Mbps (4 pair) | Gigabit Ethernet |
| 5e | 1,000 Mbps | Gigabit Ethernet |
| 6 | 10,000 Mbps | Gigabit Ethernet |

# Unshielded Twisted Pair Connector

- The standard connector for unshielded twisted pair cabling is an RJ-45 connector.
- This is a plastic connector that looks like a large telephone-style connector. A slot allows the RJ-45 to be inserted only one way.
- RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry.
- This standard designates which wire goes with each pin inside the connector.

# Shielded Twisted Pair (STP) Cable

- Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.).
- If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.
- Shielded twisted pair cable is available in three different configurations:
- Each pair of wires is individually shielded with foil.
- There is a foil or braid shield inside the jacket covering all wires (as a group).
- There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

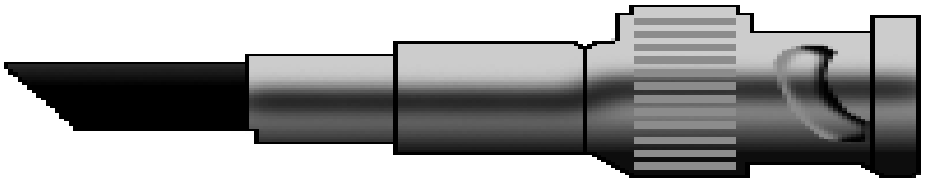


# Coaxial Cable

- Coaxial cabling has a single copper conductor at its center.
- A plastic layer provides insulation between the center conductor and a braided metal shield.
- The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.
- Although coaxial cabling is difficult to install, it is highly resistant to signal interference.
- In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

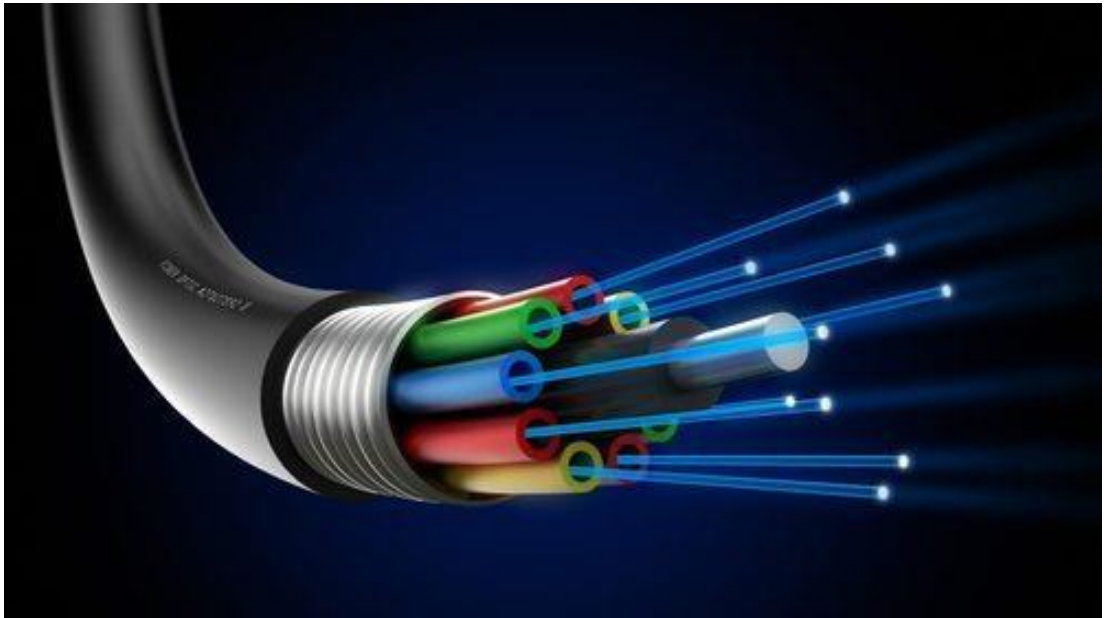
# Coaxial Cable Connectors

- The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector
- Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.



# Fiber Optic Cable

- Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials
- It transmits light rather than electronic signals eliminating the problem of electrical interference.
- immunity to the effects of moisture and lighting.
- transmit signals over much longer distances than coaxial and twisted pair.



# Specification of Cables

| Specification | Cable Type |
|---|---|
| 10BaseT | Unshielded Twisted Pair |
| 10Base2 | Thin Coaxial |
| 10Base5 | Thick Coaxial |
| 100BaseT | Unshielded Twisted Pair |
| 100BaseFX | Fiber Optic |
| 100BaseBX | Single mode Fiber |
| 100BaseSX | Multimode Fiber |
| 1000BaseT | Unshielded Twisted Pair |
| 1000BaseFX | Fiber Optic |
| 1000BaseBX | Single mode Fiber |
| 1000BaseSX | Multimode Fiber |

# Installing Cable - Some Guidelines

- Always use more cable than you need. Leave plenty of slack.
- Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.

# Wireless LANs

- Use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations, servers, or hubs.
- Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data.
- For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.
- Wireless networks are great for allowing laptop computers, portable devices, or remote computers to connect to the LAN.
- Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

# Wireless LANs

- The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast.
- Line-of-sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network.
- Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

# Wireless standards and speeds

| Standard | Max Speed | Typical Range |
|---|---|---|
| 802.11a | 54 Mbps | 150 feet |
| 802.11b | 11 Mbps | 300 feet |
| 802.11g | 54 Mbps | 300 feet |
| 802.11n | 100 Mbps | 300+ feet |

# OSI model
# and
# its layer architecture

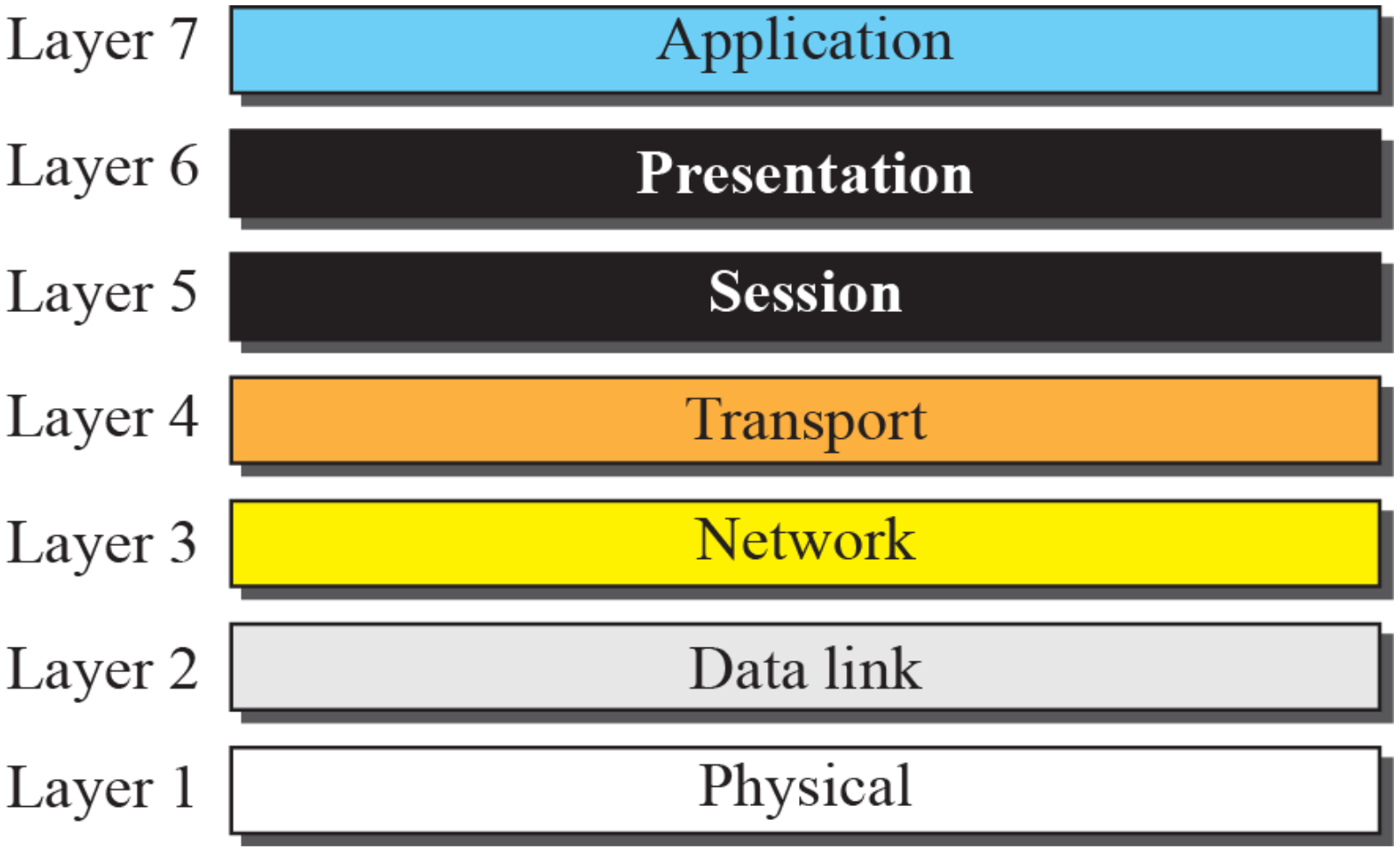
# The OSI Model

- International standard organization (ISO) established a committee in 1977 to develop an architecture for systems communication.
- Open System Interconnection (OSI) reference model is the result of this effort.
- This model allows any two different systems to communicate regardless of their underlying architecture.

# Cntd..

- The OSI model describes how data flows from one computer, through a network to another computer.
- The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible and robust.
- The OSI model consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

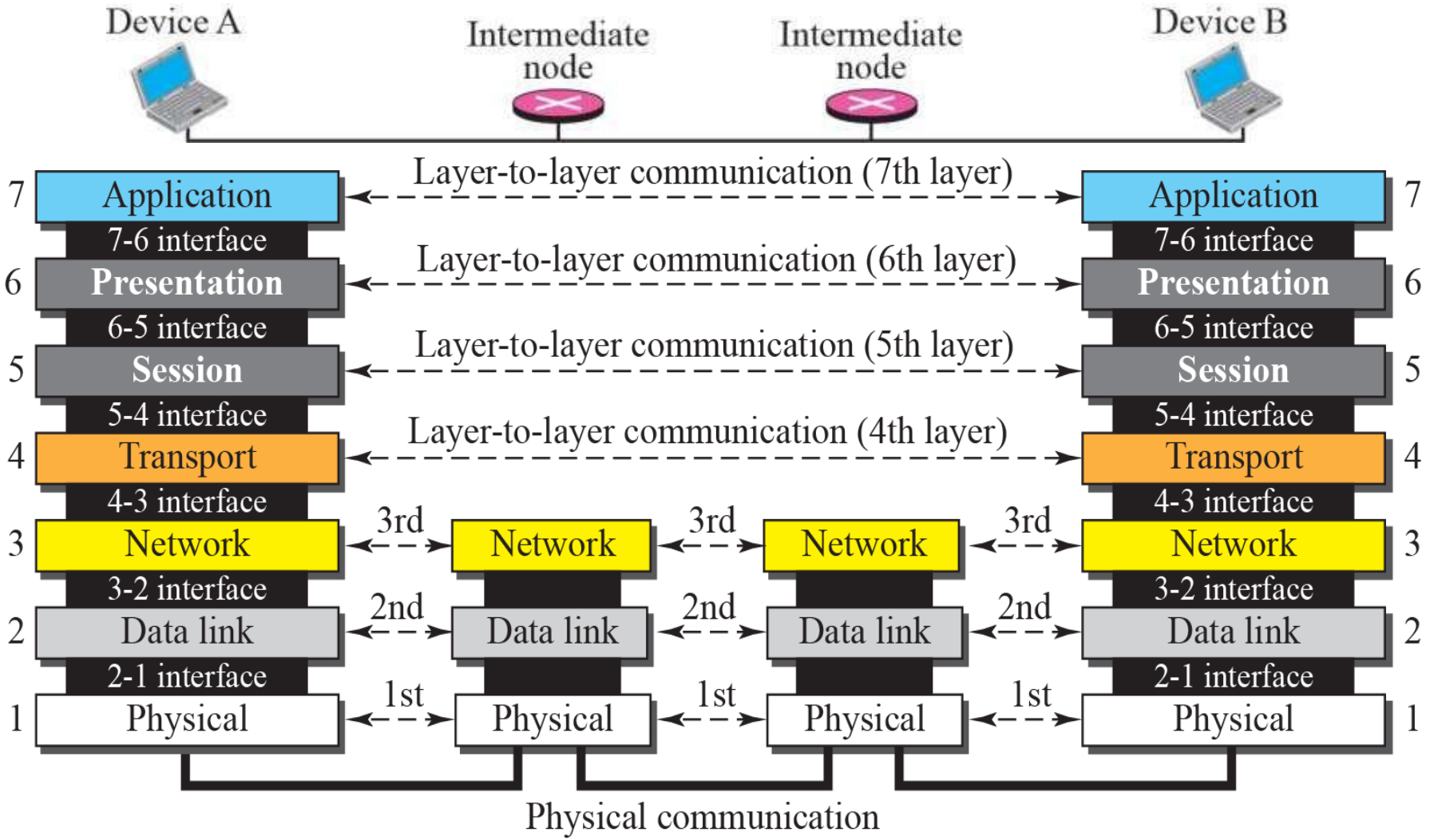
# Seven layers of the OSI model



# Why so many layers?

- To reduce the complexity, networks are organized as a stack of layers, one below the other.
- Each layer performs a specific task,. It provides services to an adjacent layer.

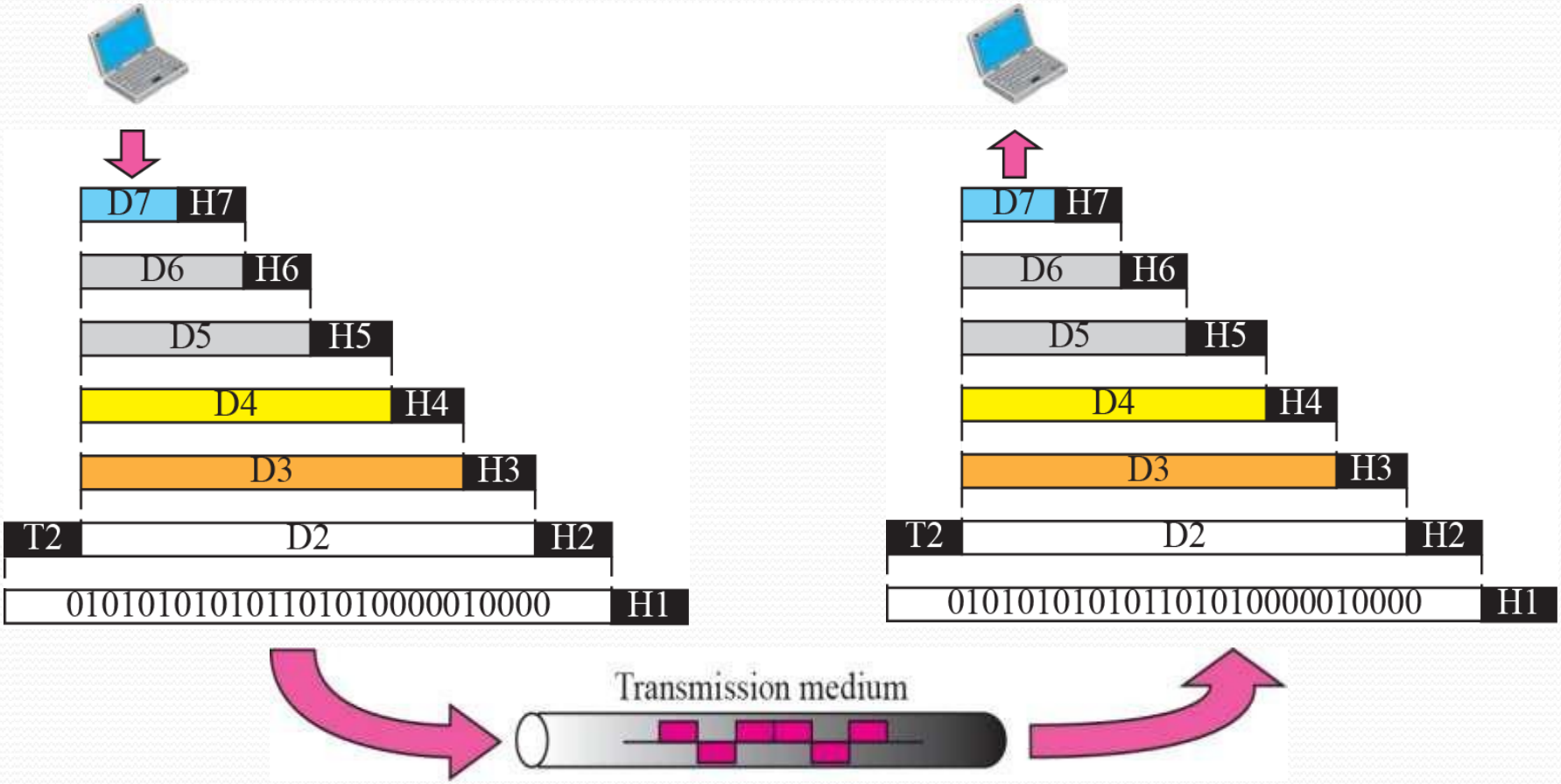
# OSI Layers


Device A
Intermediate node
Intermediate node
Device B
Layer-to-layer communication (7th layer)
Layer-to-layer communication (6th layer)
Layer-to-layer communication (5th layer)
Layer-to-layer communication (4th layer)
7
Application
7-6 interface
6
Presentation
6-5 interface
5
Session
5-4 interface
4
Transport
4-3 interface
3
Network
3-2 interface
2
Data link
2-1 interface
1
Physical
3rd
2nd
1st
Physical communication

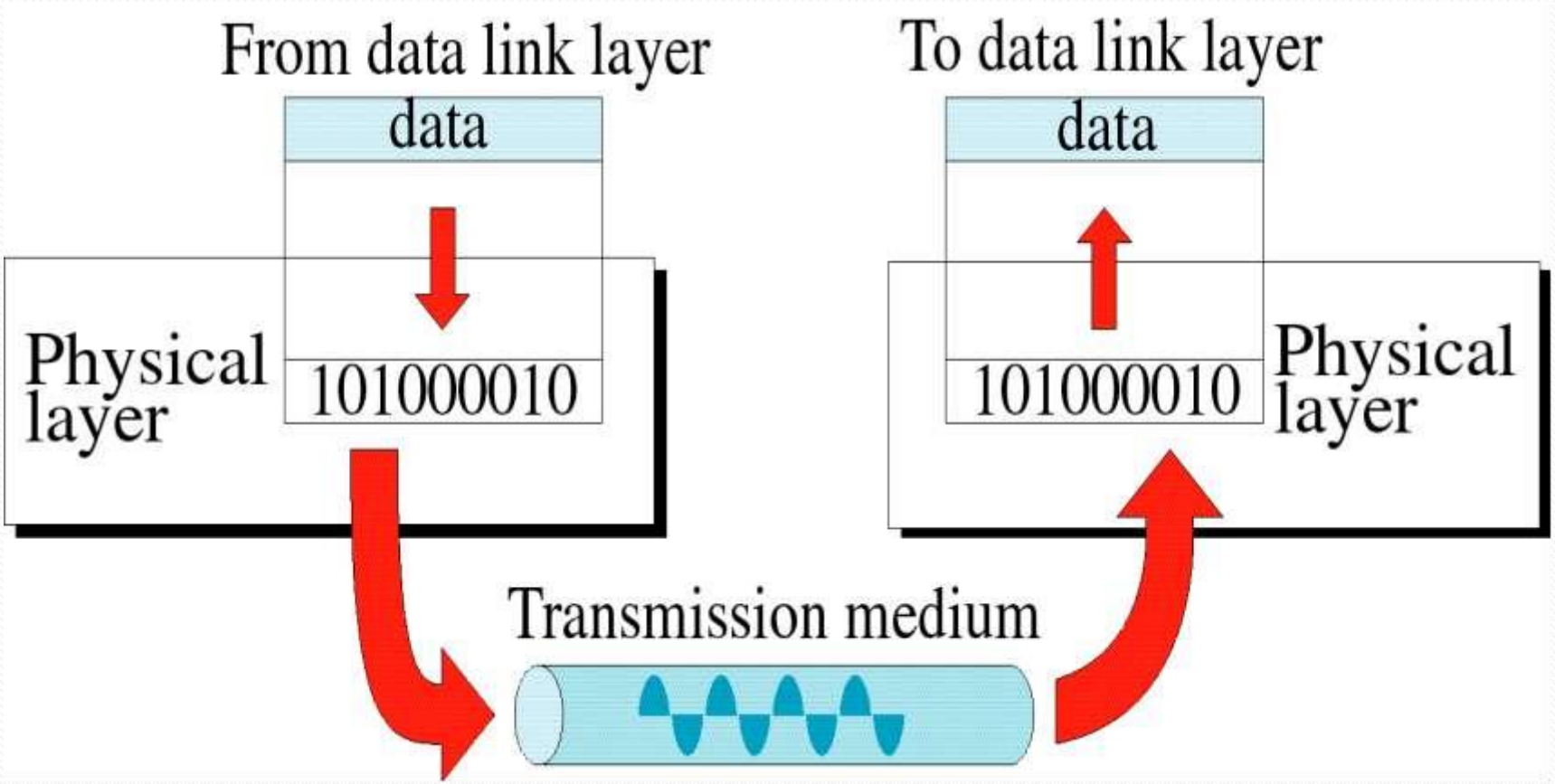
# Cntd..

- Layers 1,2, 3- physical, data link and network are network support layers.
- Layer 4, the transport layer, links the two subgroups.
- Layers 5,6,7- session, presentation, and application are user support layers.

# An exchange using the OSI model



# Physical layer



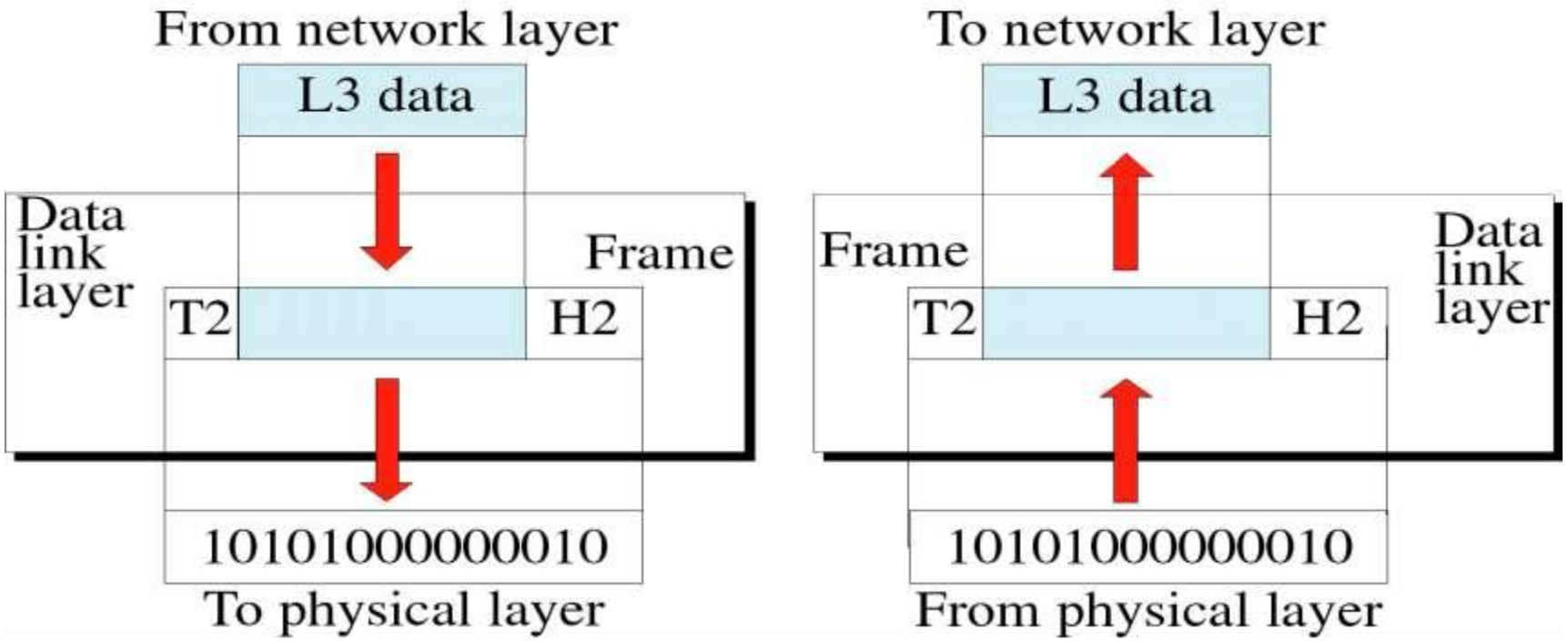
# Physical Layer

- Physical layer is the bottom(layer 1) of OSI model.
- It is responsible for the actual physical connection between the devices.
- The physical layer is responsible for movements of individual bits from one node to next.

# Functions of Physical Layer

- Convert bits to signals
- Bit synchronization
- Manage physical connection
- Bit rate control
- Physical topology
- Transmission mode
- Multiplexing
- Switching

# Data Link Layer

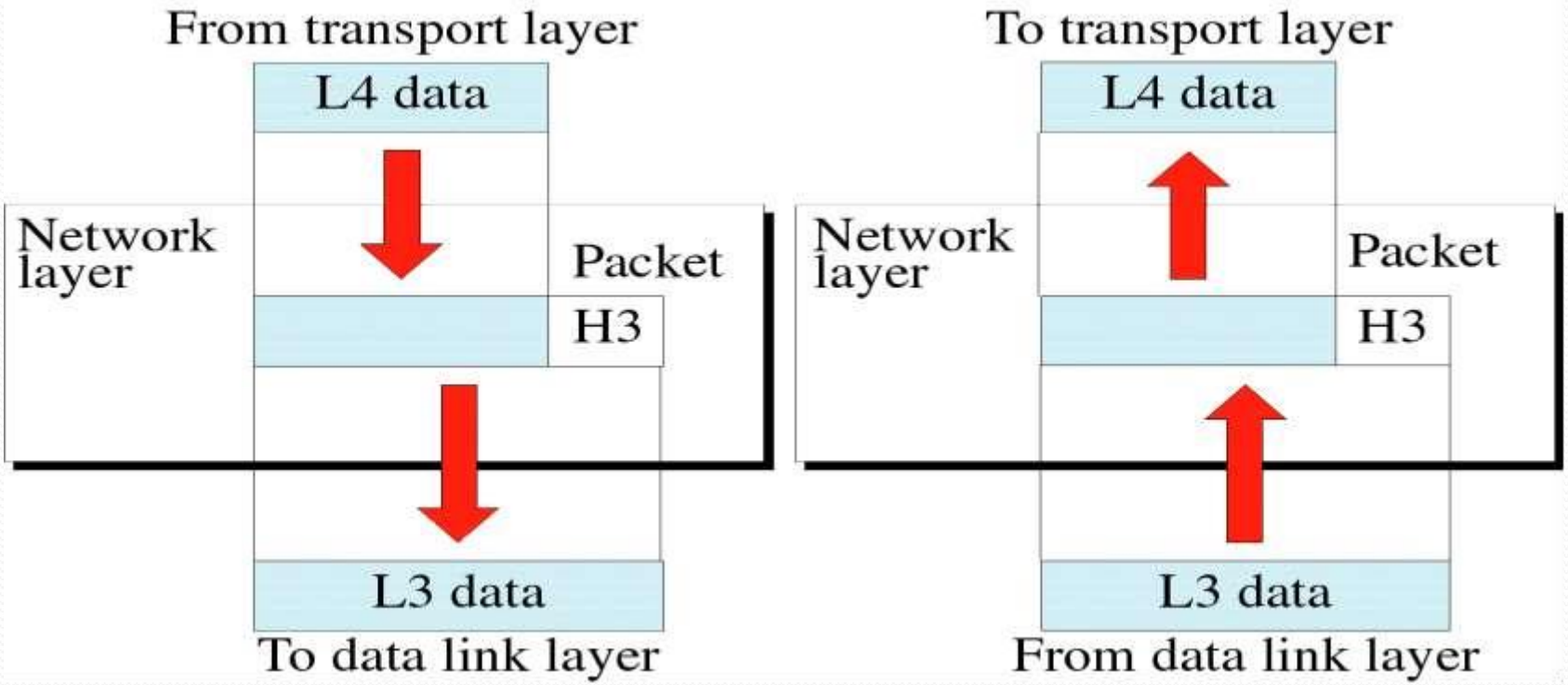



- The data link layer is responsible for moving frames from one node to the next.

# Functions of Data Link Layer

- Framing:- divides the data from N/W layer into frames.
- Physical Addressing:- Add a header to the frame to define the physical address of the source and the destination machines.
- Flow Control:- It is the traffic regulatory mechanism implemented by Data Link layer that prevents the fast sender from drowning the slow receiver.
- Error Control:- It provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- Feedback:- after transmitting the frames, the system waits for the feedback.

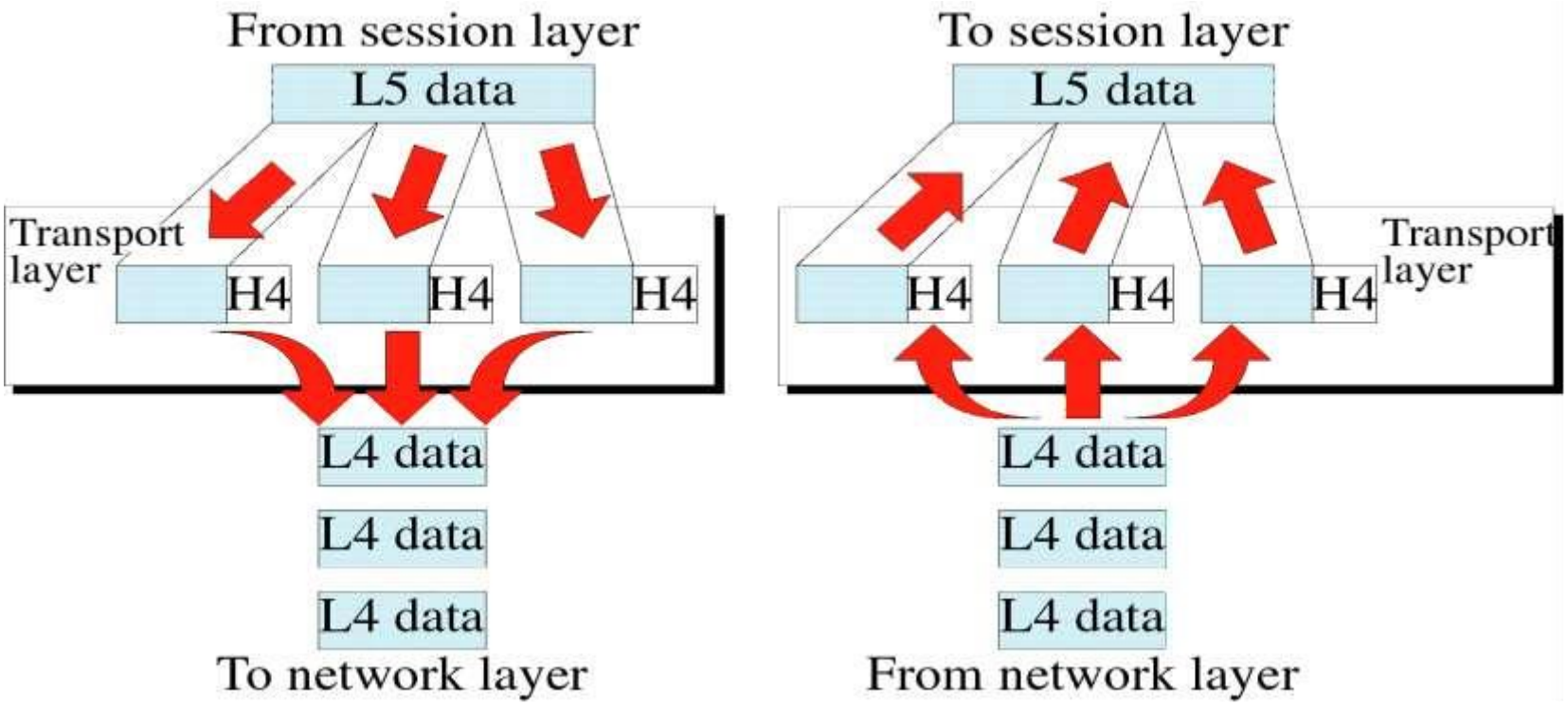
# Network Layer



# Functions of Network layer

- It is responsible for the source to destination delivery of a packets across multiple networks.
- Routing:- Provide mechanism to transmit data over independent networks that are linked together.
- Logical addressing:- Adds Logical addresses of sender and Receiver.

# Transport Layer




- It is responsible for source process to destination process delivery of entire message.

# Cntd…

- Transport layer provides two types of services:

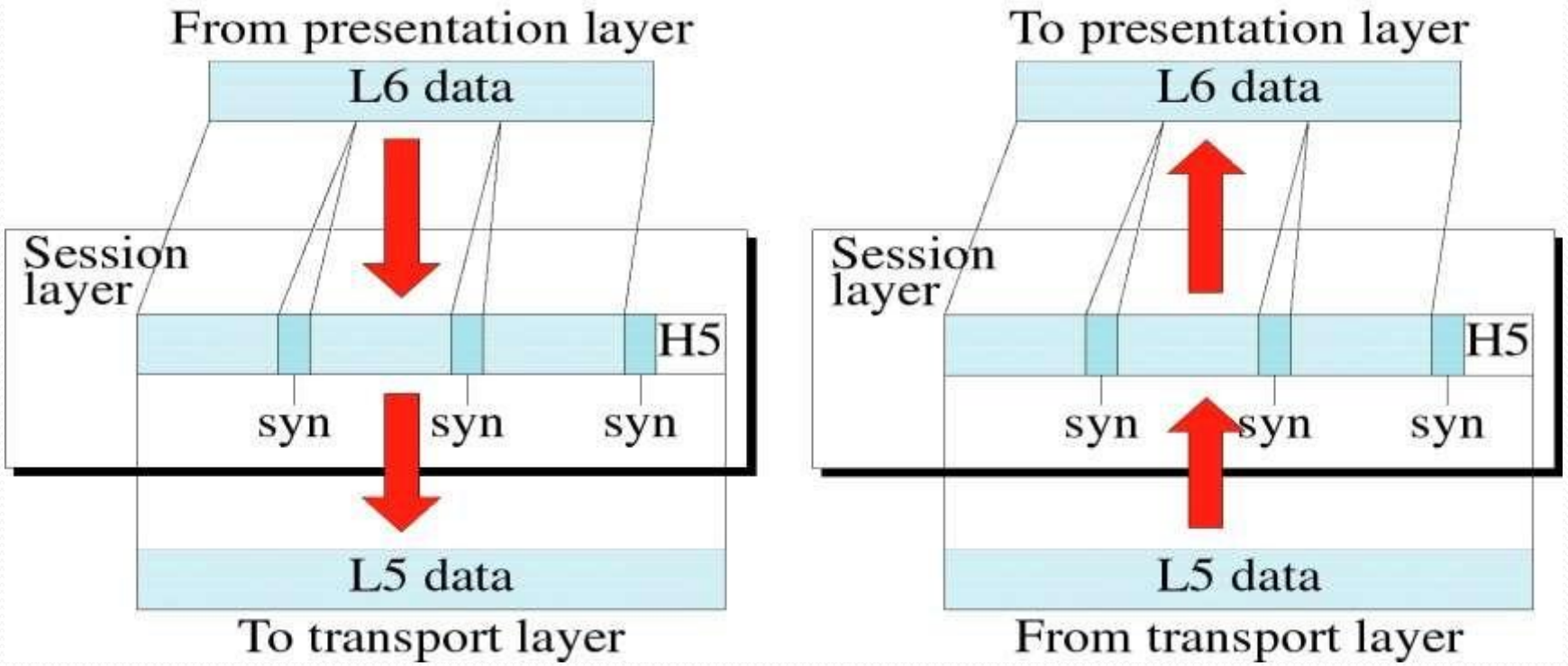
- 1) Connection Oriented Transmission: In this type of transmission the receiving device sends an acknowledgment back to the source after a packet or group of packet is received.

- 2) Connectionless Transmission: In this type of transmission the receiver does not acknowledge receipt of a packet.

# Functions of Transport Layer

- Segmentation and Reassembly: Divide the message received from Session layer into Segments and number them to make a sequence for reassembly at the receiving side.
- Service point addressing: Transport layer makes sure that the message is delivered to the correct process on destination machine.
- Error Control: Make sure that the entire message arrives without errors else retransmit.
- Flow Control: Transport layer makes sure that the sender is synchronized with receiver

# Session Layer




- It is responsible for beginning, maintaining & ending the communication between two devices, which is called session.

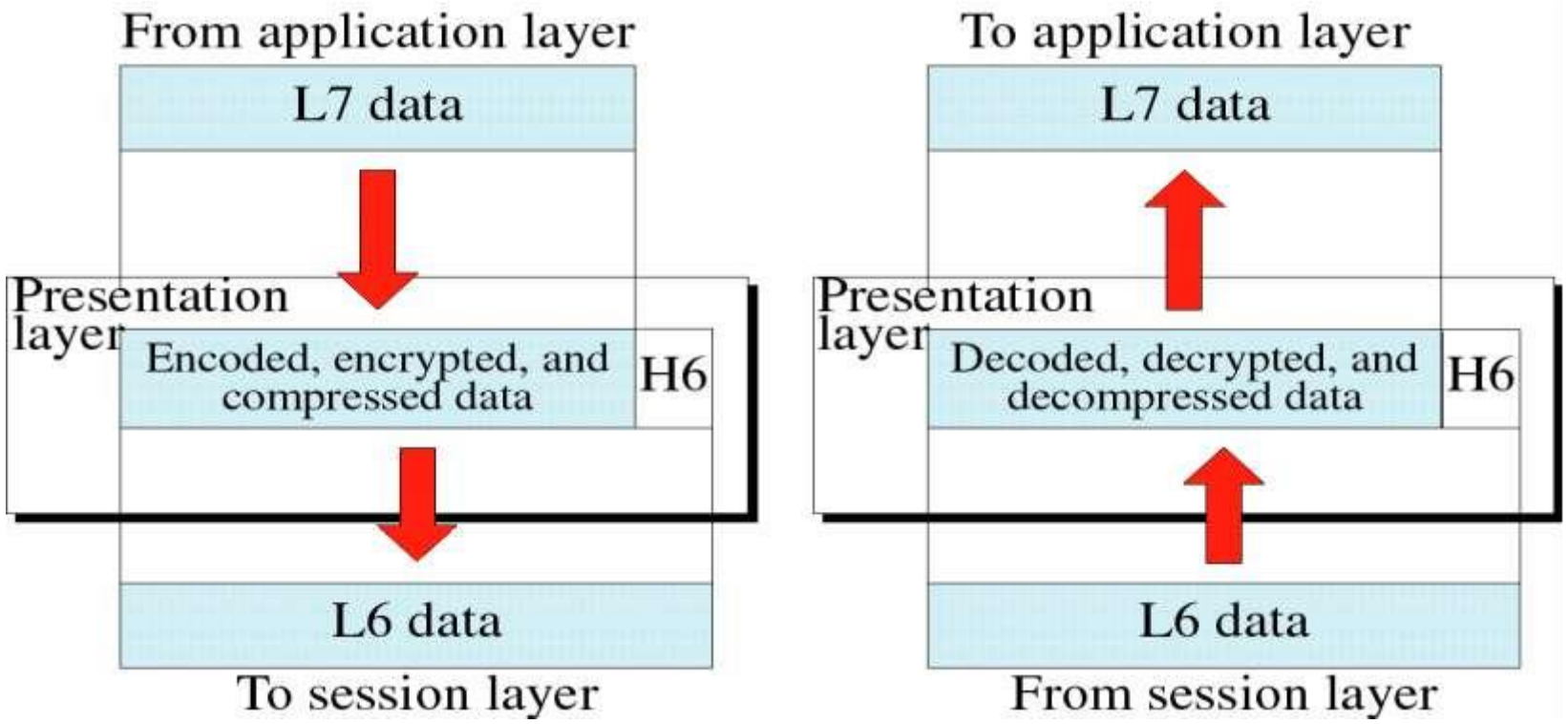
# Functions of Session Layer

- Establishment, maintaining and ending a session:
- Sends SYN packet – establish request
- Receives ACK & SYN- established
- To end – Sender sends ACK

- Dialog Control: The session layer allows two systems to enter into a dialog.

- Synchronization: Allows a process to add checkpoints to a stream of data.

# Presentation Layer

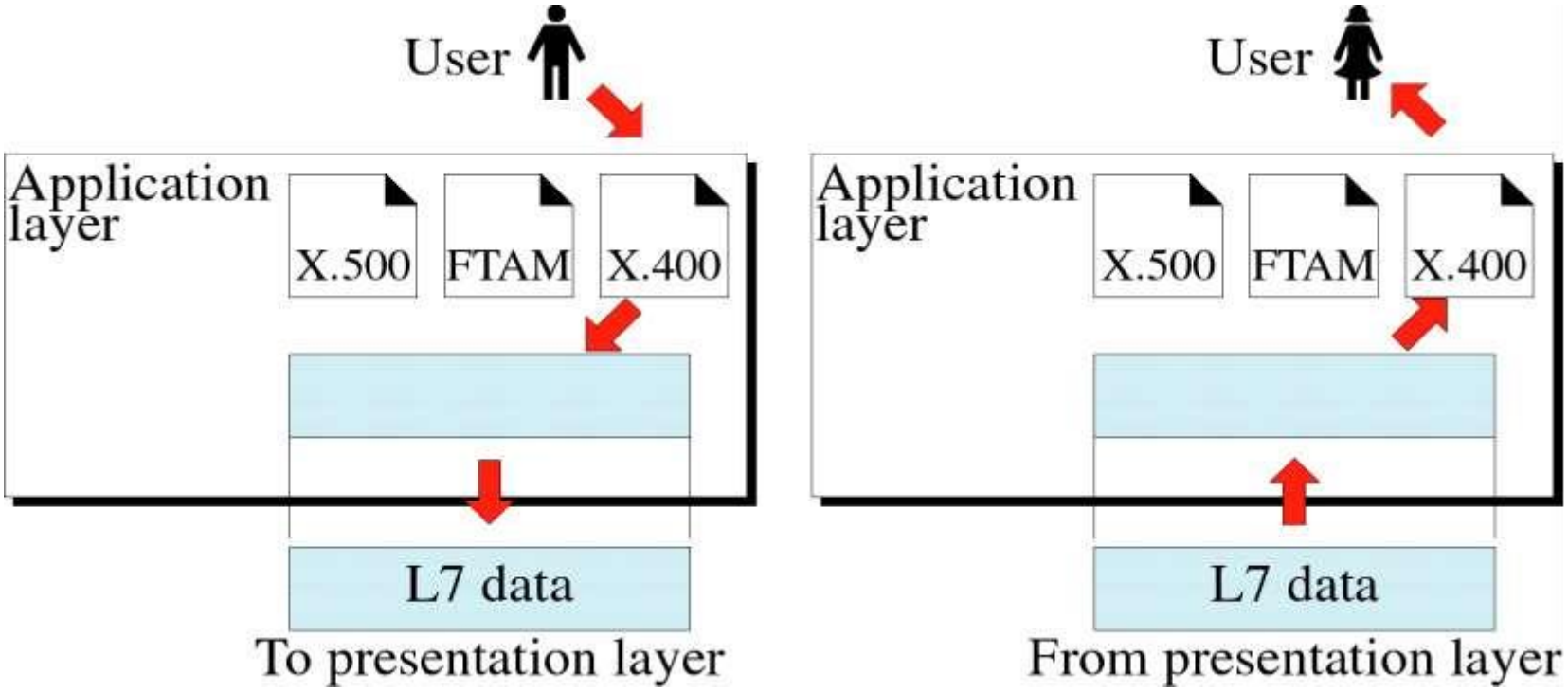



- This layer is concerned with the syntax and semantics of the information exchanged between two systems.

# Functions of Presentation Layer

- Data Translation: Encoding and Decoding  Sender to Common format on Sending side  Common to Receiving format on Receiver side
- Data Encryption: For security and privacy purpose.
- Data Compression: Data compression reducesthe number of bits contained in the information.

# Application Layer




- Provides User interfaces and support for Services, like e- mail, file transfer.

# Functions of Application Layer

- **Network Virtual terminal:** It allows a user to log on to a remote host.
- **File Transfer Access, and Management:** This application allows a user to access files in a remote host.
- **Mail Services:** This applicationprovides various e-mail services.
- **Distributed Services:** This application provides the global information about database sources and access for various objects and services.

# LAN design for Small business

Requirements:

- A CPA firm with 5 departments
- Total of 560 employees
- One building
  - No current LAN operating
  - Need for easy future expansion
  - Need for fast access for each department
- Reliability of the network

# LAN design for Small business
# Design goals

- Functionality - the network must work with reasonable speed and reliability.
- Scalability - the network must be able to grow without any major changes to the overall design.
- Adaptability - the network must be designed with an eye toward future technologies, and should include no element that would limit implementation of new technologies as they become available.
- Manageability - the network would be designed to facilitate network monitoring and management.

# Network design outline

- Gathering the users requirements and expectations
- Determining data traffic patterns now and in the future based on growth and Server placements
- Defining all of the layer 1, 2 &3 devices and along with LAN and WAN topology
- Document the physical and logical network implementation

# Methodology

- Analyze customer’s requirements
- Choose and Develop LAN structure (topology)
- Set up addressing and routing

# Step 1: Analyse requirements

- Business issues
- Technology issues
- Administrative issues

# Some datas to be gathered

- Corporate Structure – small CPA firm with 560 employees.
- Business information flow - ?
- Applications in use - ?
- Current topology - NONE
- Performance characteristics of current network - N/A
- Determine if documented policies are in place - ?
- Mission-critical data - ?
- Mission-critical operations - ?
- Approved protocols and platforms - ?
- Control versus distributed authority - ?
- Availability requirements –
- Throughput
- Response time
- Access to resources

# Network load analysis

- Client/Server applications
- Host/terminal applications
- Routing protocols
- Regularly scheduled services, such as file backup
- Estimate worst-case traffic load during the busiest times for users and during regularly scheduled network services

# Step 2: choosing and developing topology

- Keeping in mind the first step requirements choose a suitable topology.

- Another issue that comes into play is how Tall is the building and how are the departments physically located in it.

# Step 3: Addressing and Routing

- In this step the LAN engineer must carefully to consider where to place bridges and routers in order to minimize collision domains and to provide back up routes in case of bridge failures.
- Creating subnets and networks.
- Mapping physical and logical addressing.
- Develop and document the IP addressing scheme.

# Selecting the Physical medium

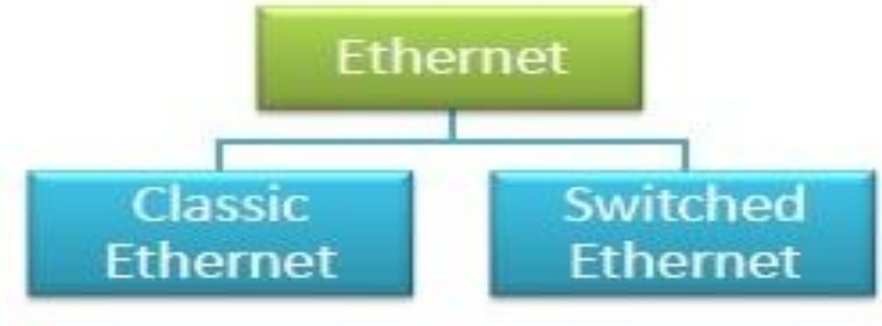
- Considering the requirement for fast access and the possibility for a future expansion the best fitting LAN would be fast Ethernet
- With the same consideration in mind the specific choice would be 100Base-TX using CAT5(UTP or STP).

# More specification

- Choosing main distribution facility (MDF) and intermediate distribution facilities (IDF). MDF is usually placed in the base of the building, Whereas each floor can have its own IDF.
- Choice of backbone (vertical) cabling .
- Choice of horizontal cabling.

# ETHERNET

- Ethernet is most widely used LAN Technology, which is defined under IEEE standards 802.3. The reason behind its wide usability is Ethernet is easy to understand, implement, maintain and allows low-cost network implementation. Also, Ethernet offers flexibility in terms of topologies which are allowed. Ethernet generally uses Bus Topology. Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer. For Ethernet, the protocol data unit is Frame since we mainly deal with DLL. In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD. It supports data transfer rates of 10/100/1000 Mbps.



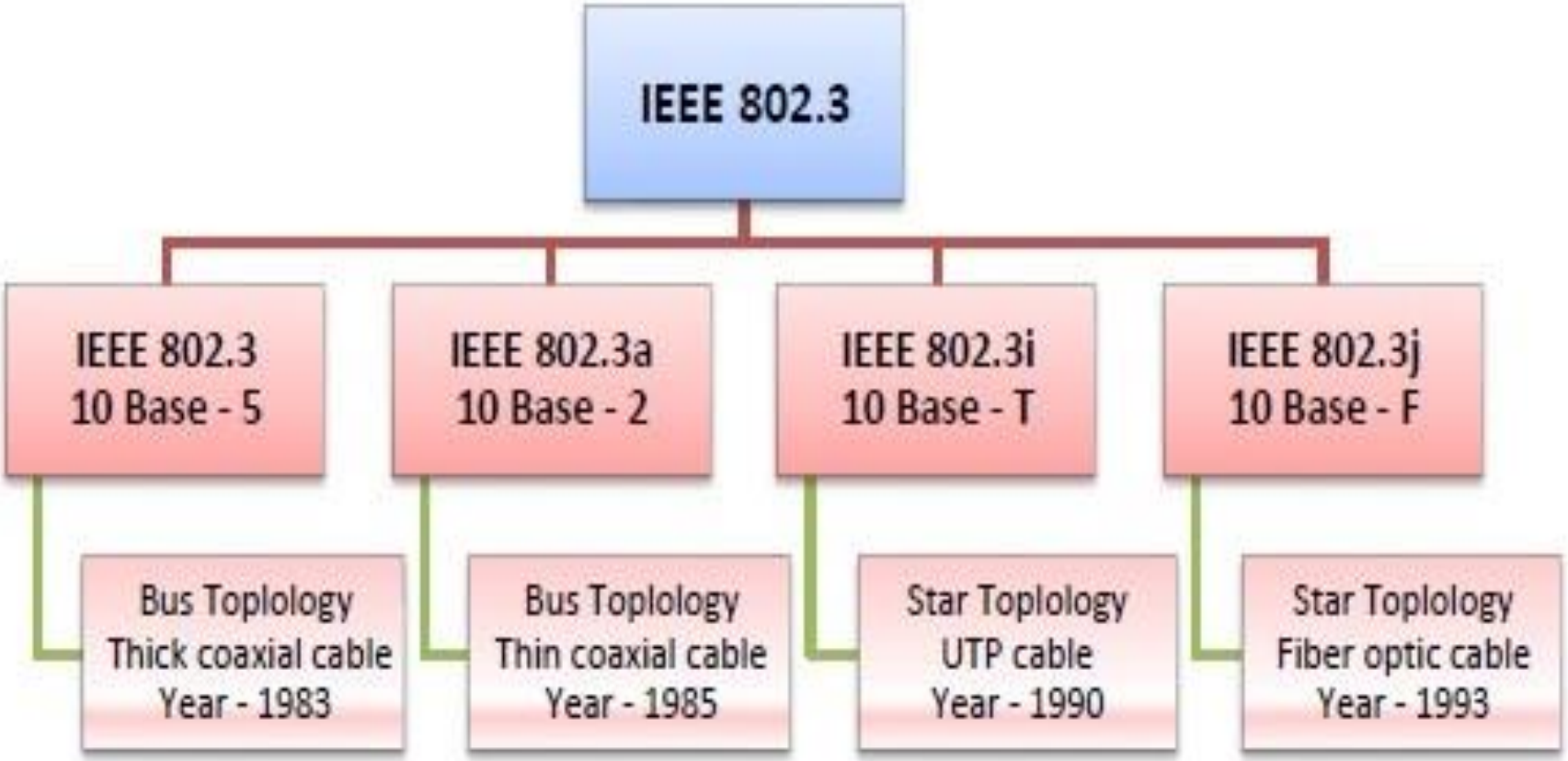
# What are classic Ethernet and switched Ethernet

- Classic Ethernet is the original form of Ethernet that provides data rates between 3 to 10 Mbps. The stations are connected by hubs that allow each station to communicate with every other station in the LAN. There are number of varieties of classic Ethernet, commonly referred as 10BASE-X. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denotes use of baseband transmission, and X is the type of medium used.
- In switched Ethernet, the hub connecting the stations of the classic Ethernet is replaced by a switch. The switch connects the high-speed backplane bus to all the stations in the LAN. The switch-box contains a number of ports, typically within the range of 4 – 48. A station can be connected in the network by simply plugging a connector to any of the ports. Connections from a backbone Ethernet switch can go to computers, peripherals or other Ethernet switches and Ethernet hubs.

# IEEE 802.3 Popular Versions of classic Ethernet

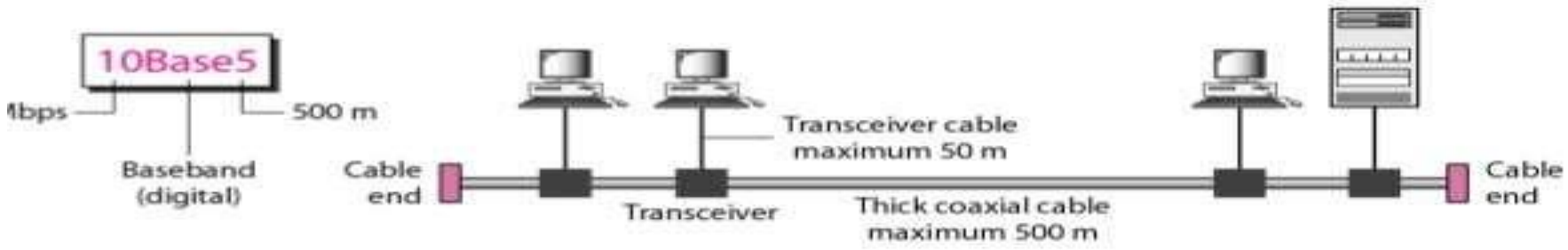
- **IEEE 802.3**: This was the original standard given for 10BASE-5. It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500m.
- **IEEE 802.3a**: This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise).
- **IEEE 802.3i**: This gave the standard for twisted pair (10BASE-T) that uses unshielded twisted pair (UTP) copper wires as physical layer medium. The further variations were given by IEEE 802.3u for 100BASE-TX, 100BASE-T4 and 100BASE-FX.
- **IEEE 802.3j**: This gave the standard for Ethernet over Fiber (10BASE-F) that uses fiber optic cables as medium of transmission.

# Types of Ethernet



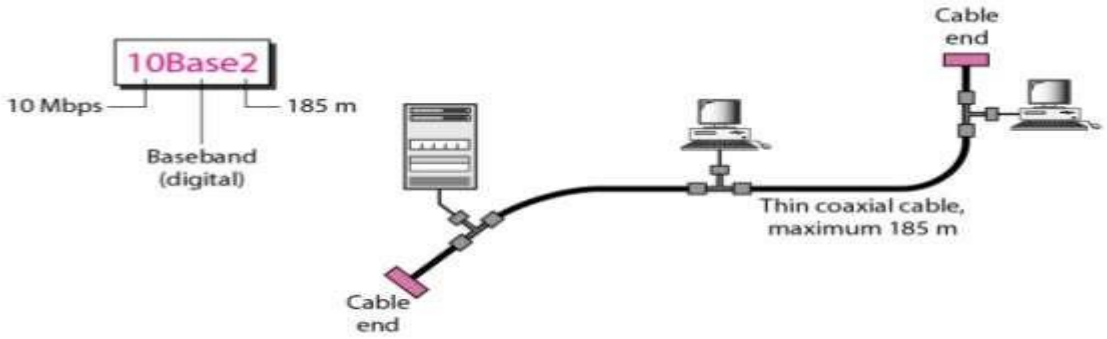
# 10Base5


- Thick Ethernet.
- Up to 100 stations can be connected to the cable using vampire taps (bus)
- The system is difficult to install and maintain.
- The 10 refers to its transmission speed of 10 Mbit/s. The BASE is short for baseband signaling as opposed to broadband,
- The 5 stands for the maximum segment length of 500 meters (1,600 ft.).
- It was the first Ethernet specification to use a bus topology with a external transceiver connected via a tap to a thick coaxial cable.



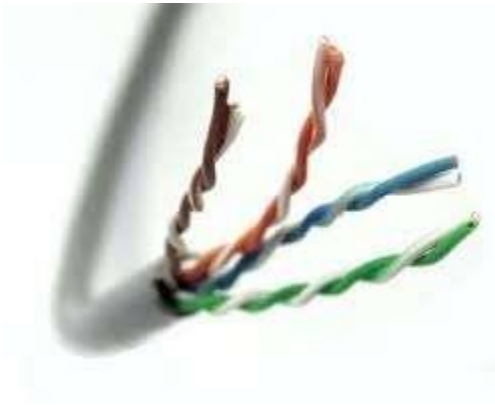
# 10BASE2

- **10BASE2** (also known as **cheapernet**, **thin Ethernet**, **thinnet**, and **thinwire**) is a variant of Ethernet that uses thin coaxial cable, terminated with BNC connectors
- 10BASE2 coax cables have a maximum length of 185 meters (607 ft).
- The maximum practical number of nodes that can be connected to a 10BASE2 segment is limited to 30 with a minimum distance of 50 cm.



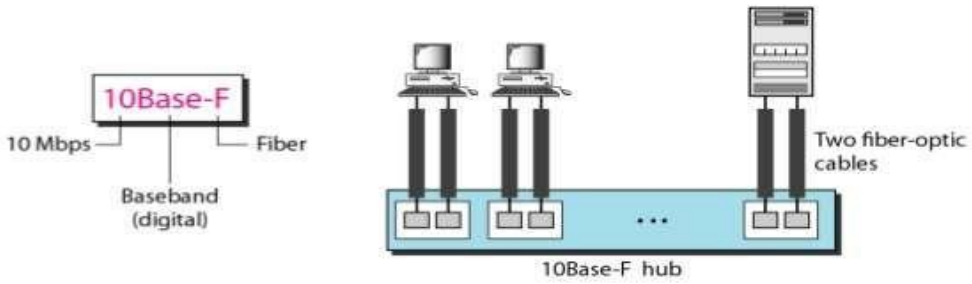

# 10Base-T

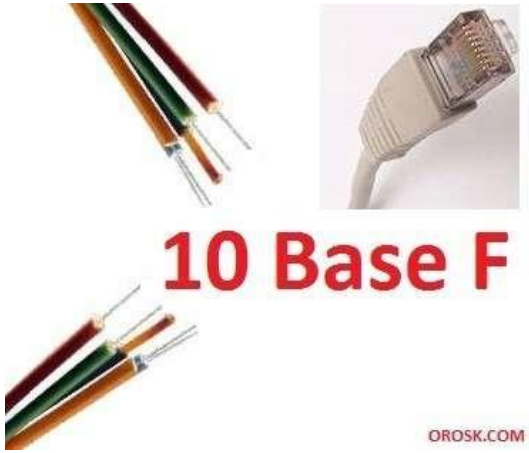
- Cables look like thick phone cables, but with 8 copper wires instead of 2 or 4, and they go from each computer' to a Hub or a Switch.
- Supported speed is 10 MBit/second.
- It uses star topology and the station are connected via two pairs of twisted cable(one for sending another for receiving)between the station and the hub.
- The maximum length of the twisted cable here is defined as 100m,to minimize the effect of attenuation in the twisted cable

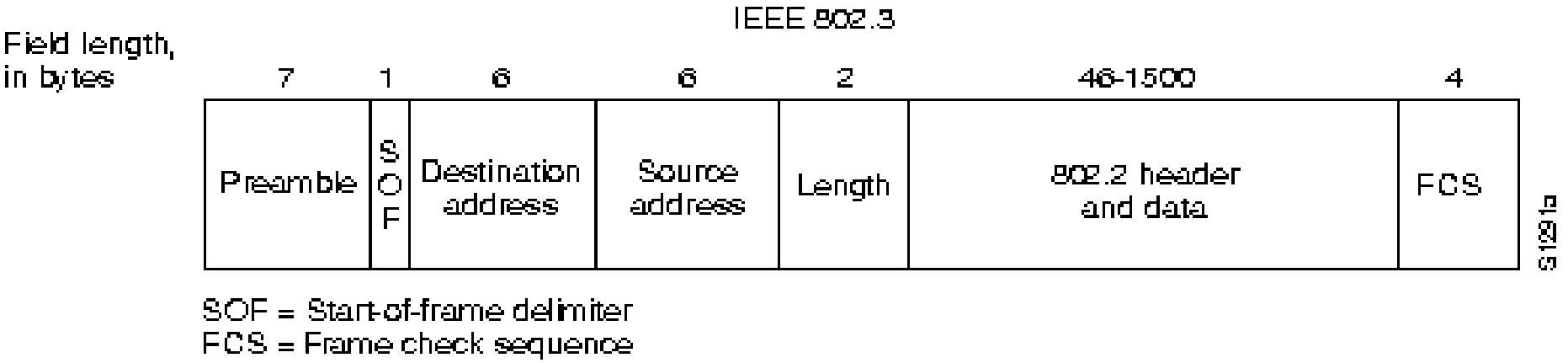
# 10Base-F

- Same as 10Base-T, but cables transmit light pulses, instead of electrical signals
- Using star topology.
- Expensive due to the cost of the connectors and terminators.



# IEEE 802.3 Frame Format



# Preamble


- Length of the field is 7 bytes.
- Each byte contain the bit pattern of 10101010.
- Manchester encoding produces a square wave for this bit pattern with Frequency of 10 MHz.
- Time period of 5.6 μsec.

# IEEE 802.3 Frame Format

| Preamble | SFD | D Address | S Address | |
|---|---|---|---|---|

- Start of Frame delimiter
  - Contains 10101011 to indicate the start of Frame
- Source Address
  - Contains either 2 bytes or 6 bytes
- Destination Address
  - Contains either 2 bytes or 6 bytes
  - For ordinary addressing the higher order bit is 0
  - For group addressing the higher order bit is 1
    i.e Multicasting
  - For Broadcasting of the frame in the network all the bits are made as 1's

# IEEE 802.3 Frame Format

| Preamble | SFD | D Address | S Address | Length | |
|---|---|---|---|---|---|

Length

–Tells how many bytes are present in the data field 0 to a maximum of 1500

–A data field of 0 bytes is legal, it causes a problem

–When a computer detects a collision, it truncates the current frame which means that corrupted frames appear on the cable all the time

–To make it easier to distinguish valid frames from corrupted frames (due to collisions), 802.3 states that valid frames to be at least 64 bytes long from destination address to checksum

# IEEE 802.3 Frame Format

| Preamble | SFD | D Address | S Address | Length | Data | Pad | Checksum |
|---|---|---|---|---|---|---|---|

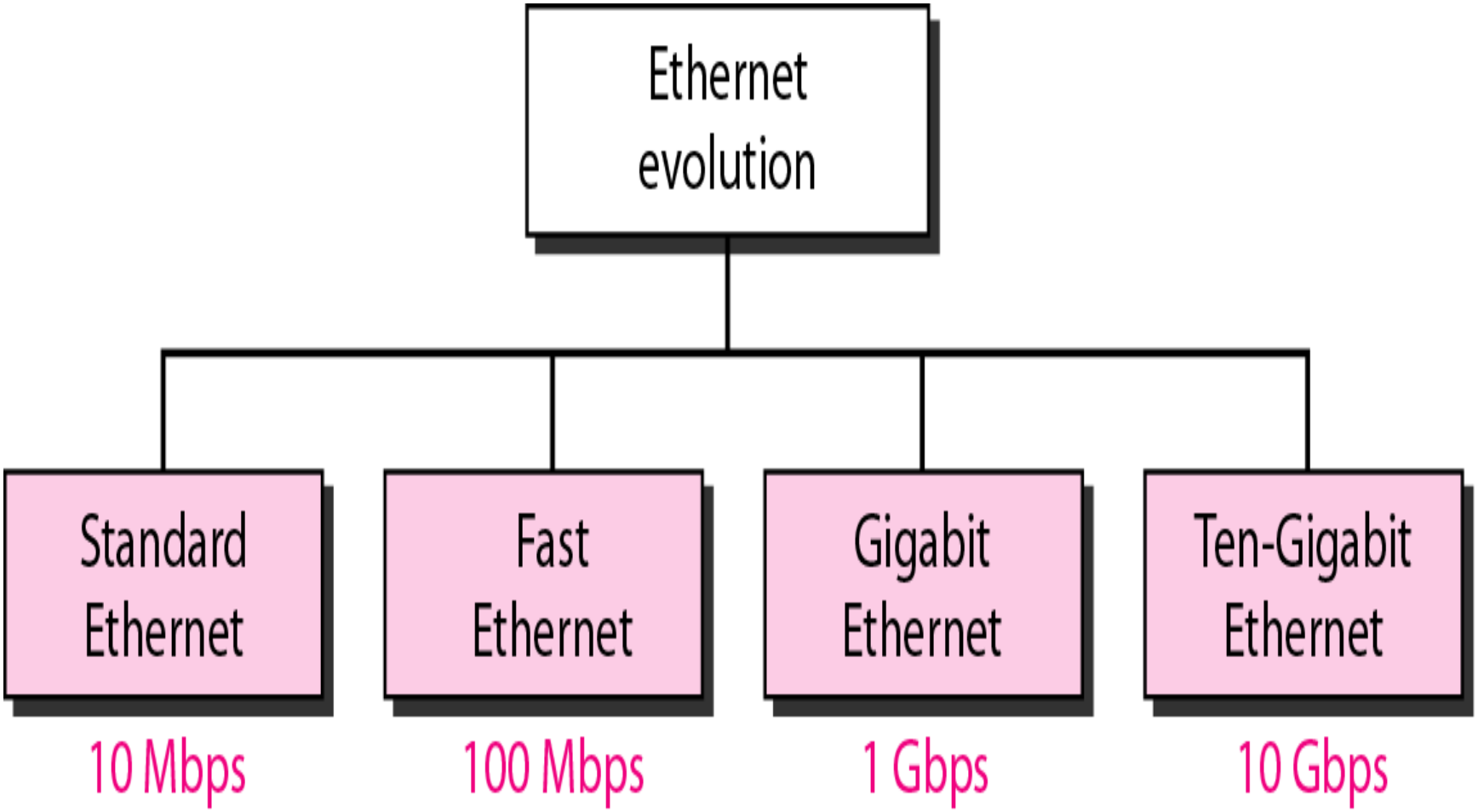
- Pad field

If the data portion is less than 46 bytes, the pad field is used to fill out the frame to the minimum size of 64 bytes

- Checksum

The Checksum is used to detect if any data bits have been corrupted during transmission

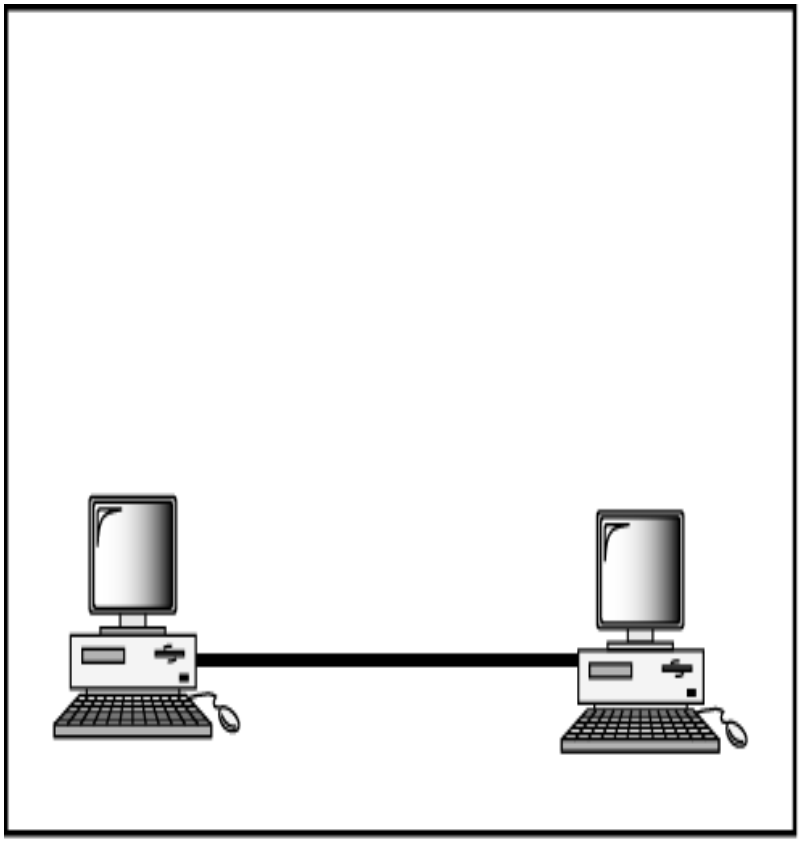
# Types of Ethernet



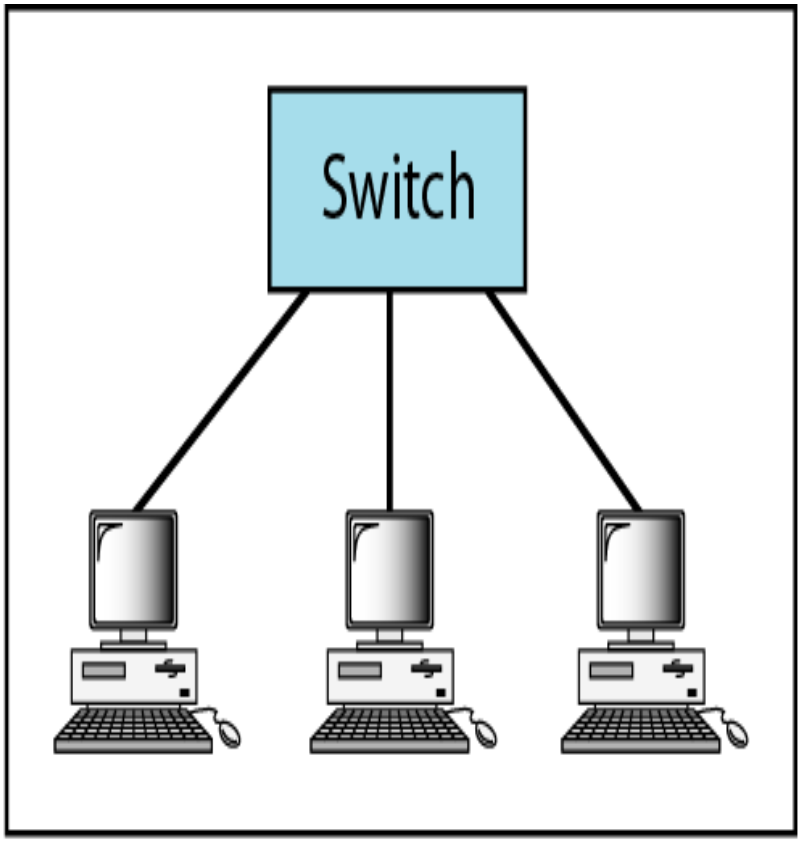
# Fast Ethernet

- Fast Ethernet is an Ethernet standard for 100-Mbps data transmission defined by the IEEE 802.3u specification.
- It can transmit data 10 times faster at a rate of 100 Mbps.
- Fast Ethernet is used for departmental backbones, connections to high-speed servers, and connections to workstations running bandwidth-intensive software such as CAD or multimedia applications.
- uses the same Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
- They are generally wired in a star topology using special Fast Ethernet hubs and switches.

# Topology used in Fast Ethernet

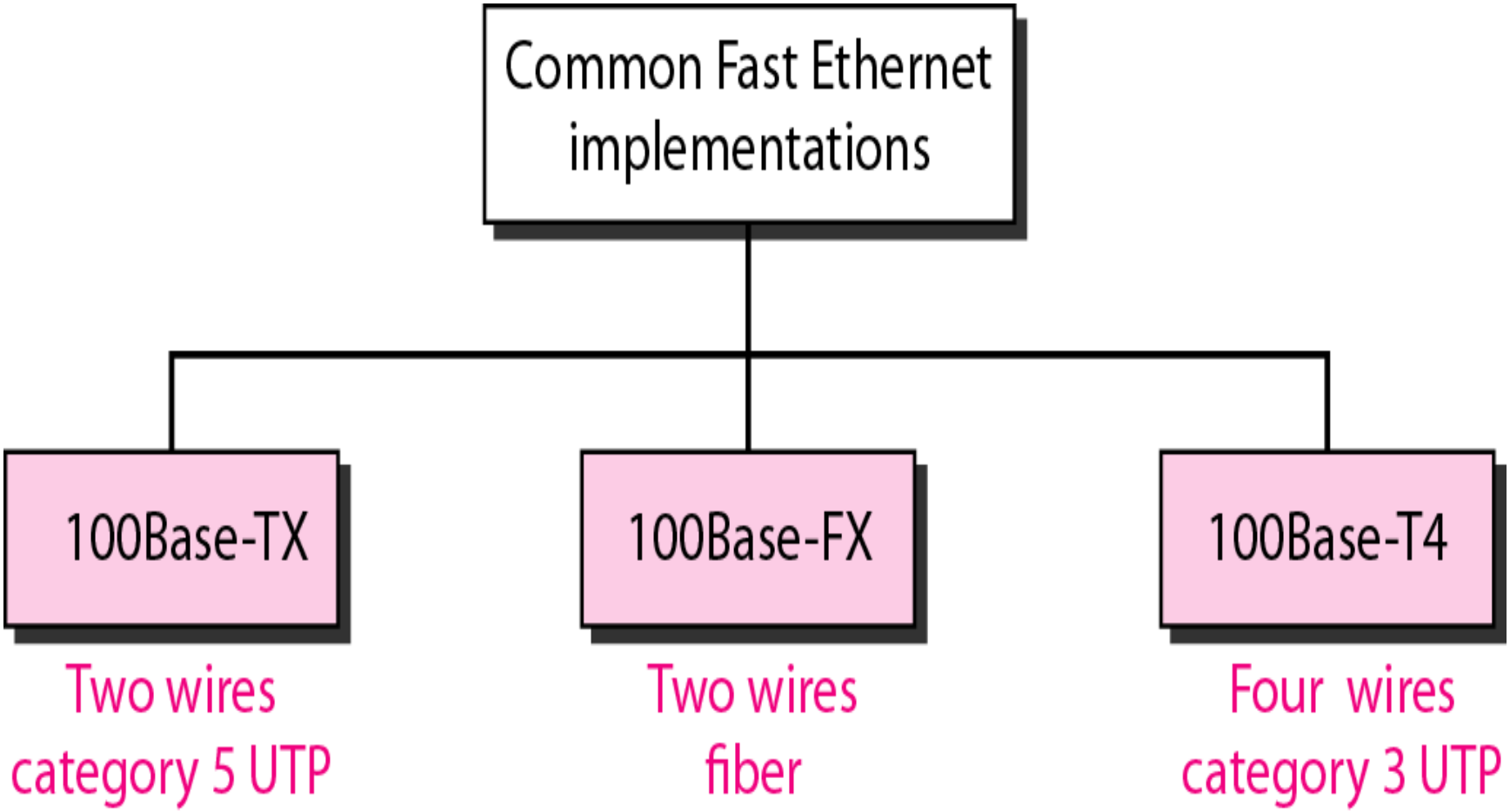


a. Point-to-point




b. Star

# Varities of Fast Ethernet Cables



# Gigabit Ethernet

- The need for higher data rate resulted in the design of the Gigabit Ethernet (1000 Mbps).
- The IEEE committee calls the standard 802.3z.
- All configurations of gigabit Ethernet are point to point.
- Point-to-point, between two computers or one computer – to –switch.
- It supports two different modes of operation: full duplex mode and half duplex mode.
- Full duplex is used when computers are connected by a switch.No collision is there and so CSMA/CD is not used.

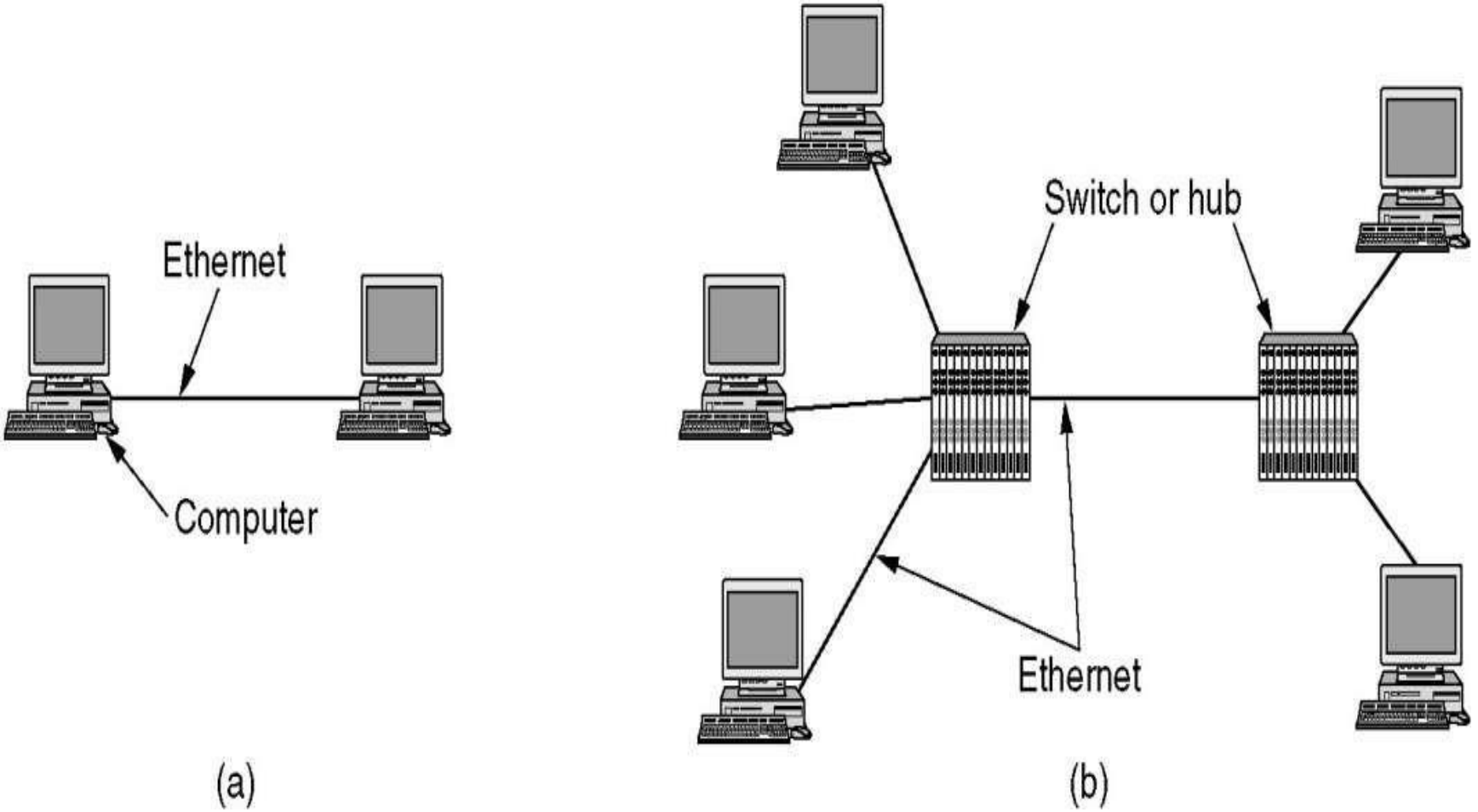
## Goals of Gigabit Ethernet

- Upgrade the data rate to 1Gbps.
- Make it compatible with standard or fast Ethernet.
- Use the same address ,frame format.
- Keep the same minimum and maximum frame length.
- To support auto negotiation as defined in Fast Ethernet

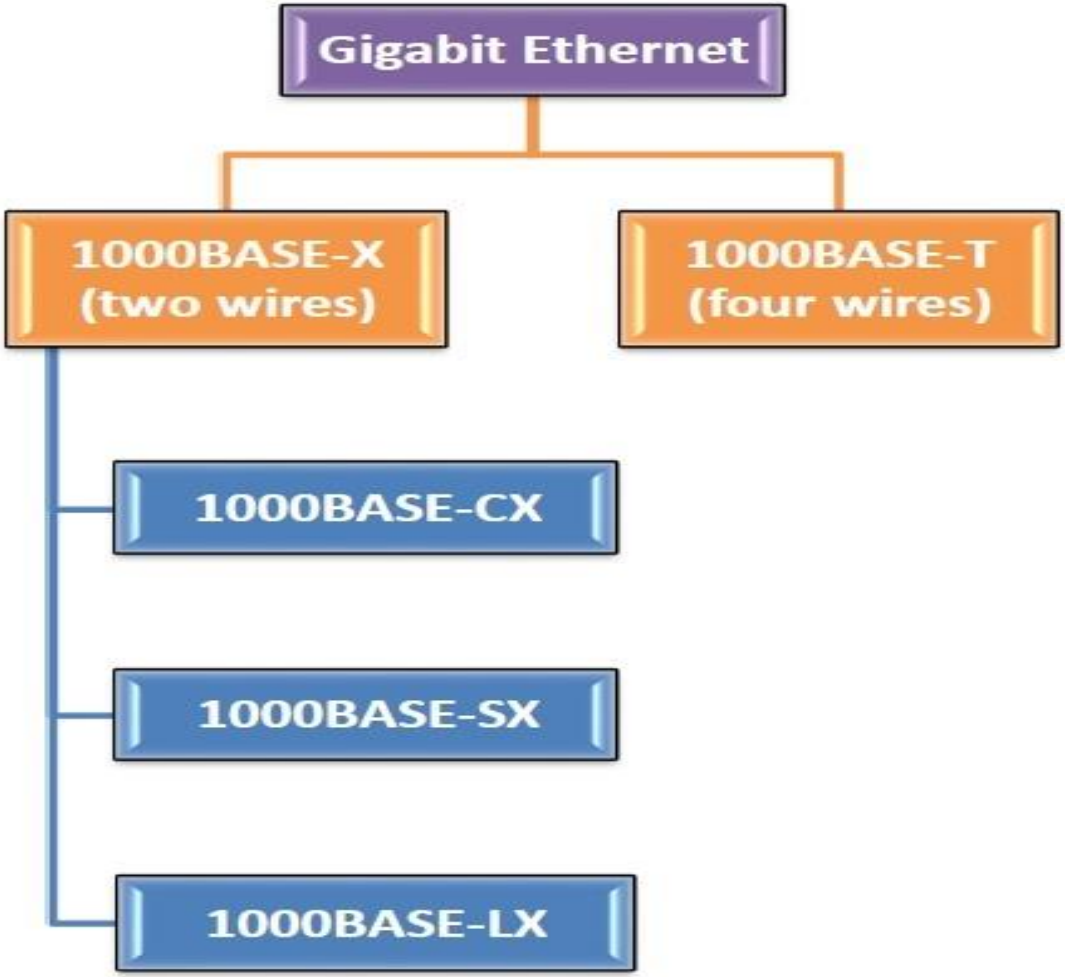
# Gigabit Ethernet

- Half duplex is used when computers are connected by a hub.
- Collision in hub is possible and so CSMA/CD is required.
- The 802.3z committee considered a radius of 25 meters to be unacceptable and added two new features to increase the radius-Carrier Extension and Frame Bursting.
- Carrier Extension tells the hardware to add its own padding bits after the normal frame to extend the frame to 512 bytes.
- Frame Bursting allows a sender to transmit a concatenated sequence of multiple frames in a single transmission. If the total burst is less than 512 bytes, the hardware pads it again.

# Topology used in GigaBit Ethernet

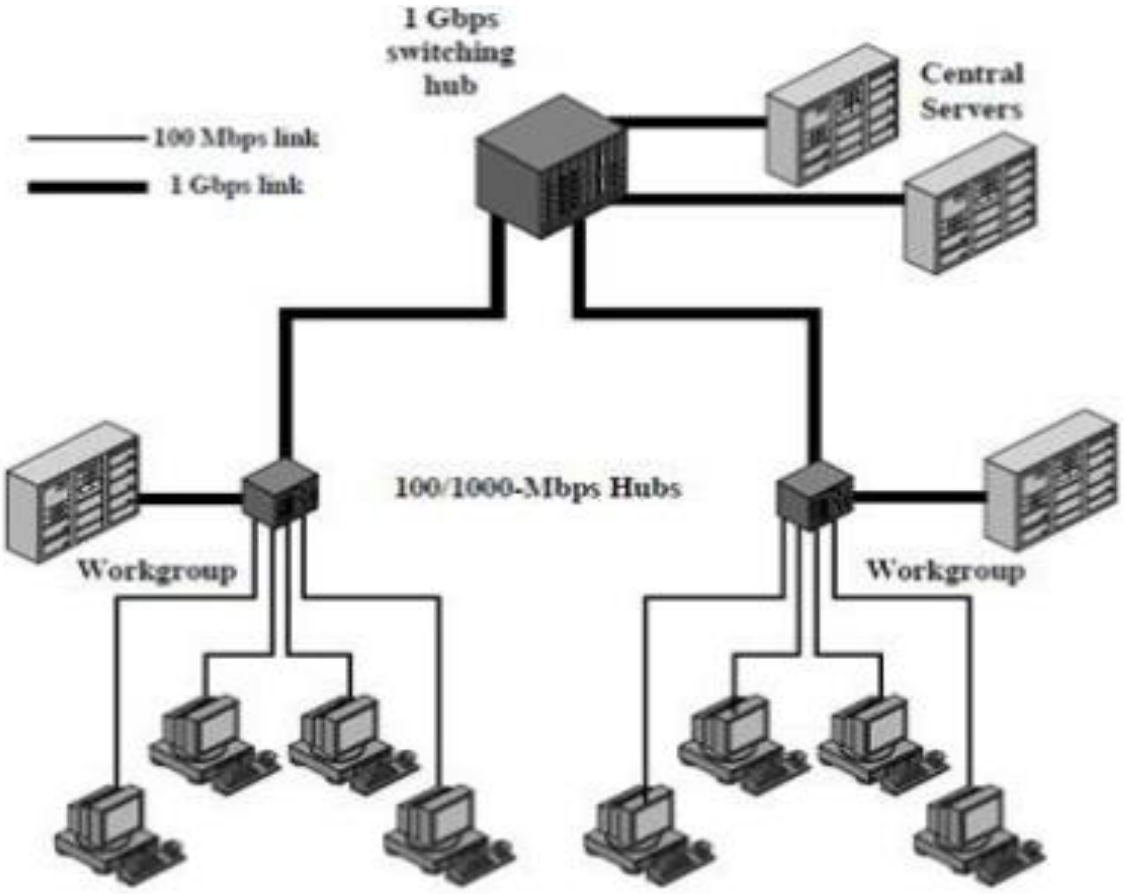


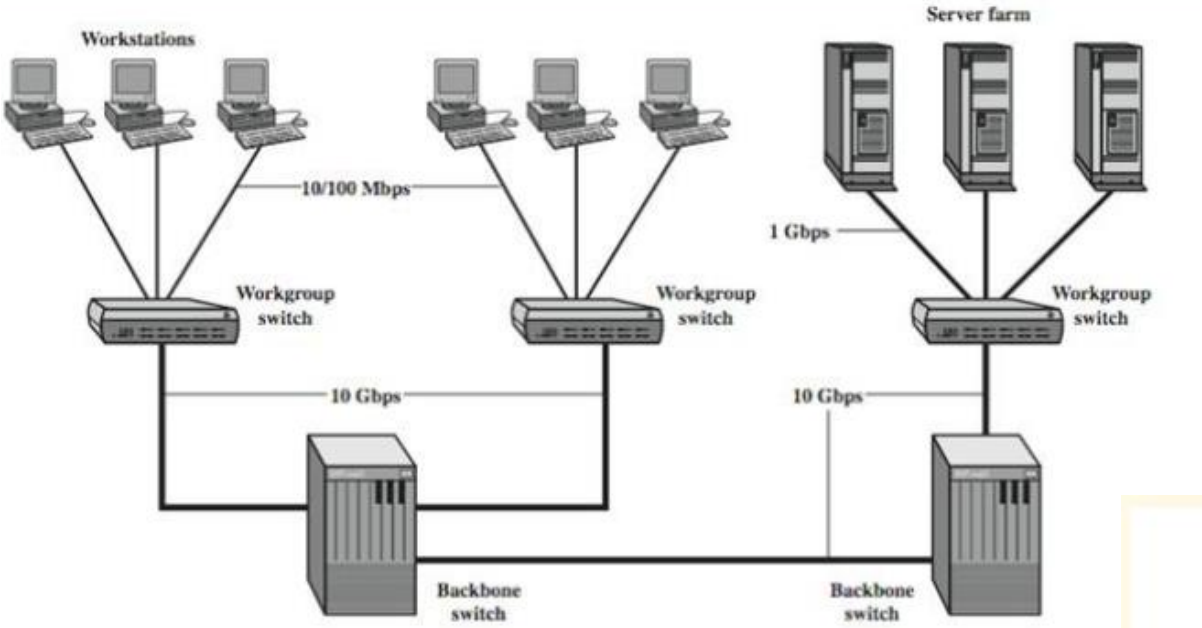
# Varieties of Gigabit Ethernet



| Name | Cable | Max. segment | Advantages |
|---|---|---|---|
| 1000Base-SX | Fiber optics | 550 m | Multimode fiber (50, 62.5 microns) |
| 1000Base-LX | Fiber optics | 5000 m | Single (10 μ) or multimode (50, 62.5 μ) |
| 1000Base-CX | 2 Pairs of STP | 25 m | Shielded twisted pair |
| 1000Base-T | 4 Pairs of UTP | 100 m | Standard category 5 UTP |

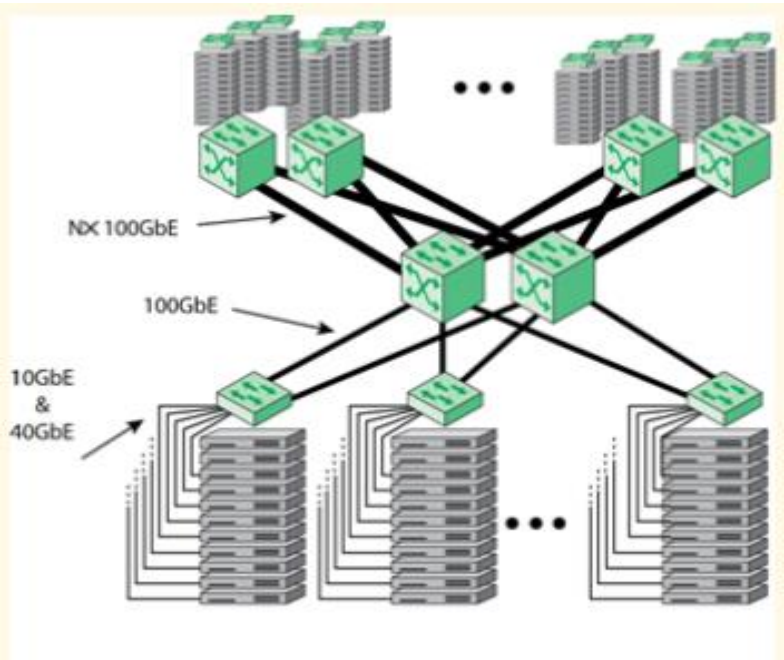
# GigaBit Ethernet Example





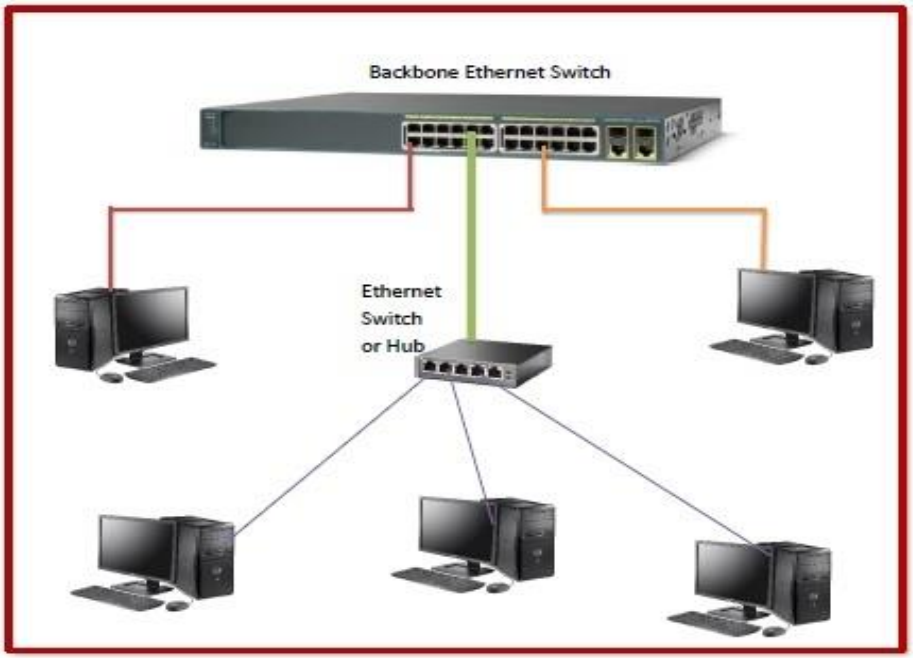

10Gpbs Ethernet configuration

100Gpbs Ethernet configuration



# Switched Ethernet

- In switched Ethernet, the hub connecting the stations of the classic Ethernet is replaced by a switch.
- The switch connects the high-speed backplane bus to all the stations in the LAN. The switch-box contains a number of ports, typically within the range of 4 – 48.
- A station can be connected in the network by simply plugging a connector to any of the ports. Connections from a backbone Ethernet switch can go to computers, peripherals or other Ethernet switches and Ethernet hubs.

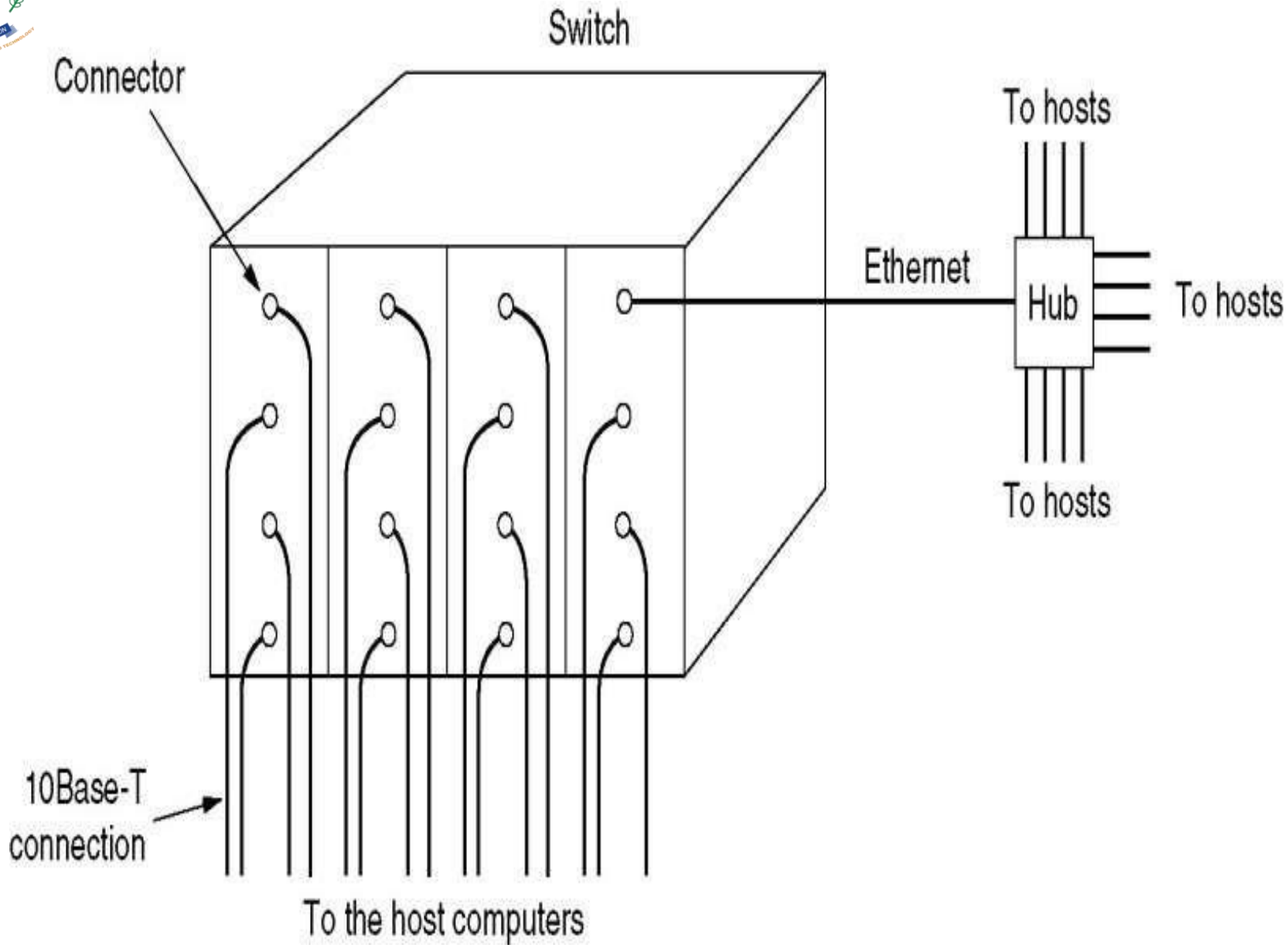


# Switched Ethernet

- When a station wants to transmit a frame, it outputs a frame to switch.
- The plug-in card checks to see if the frame is for the other station on the same card. If so, it is copied there otherwise it is sent over high speed back-plane to destination station's card.

# Switched Ethernet

- All ports on the same card are wired together to form a local on-card LAN.
- Collisions on this on-card LAN are detected and handled using CSMA/CD protocol.
- One transmission per card is possible at any instant. All the cards can transmit in parallel.
- With this design each card forms its own collision domain.
- In other design, each input port is buffered, so incoming frames are stored in the card's on board RAM.
- It allows all input ports to receive (and transmit) frame at same time


Switch
Connector
To hosts
Ethernet
Hub
To hosts
To hosts
10Base-T
connection
To the host computers

# Frame Transmission

- The preamble and start-of-frame delimiter are inserted in the PRE and SOF fields.
- The destination and source addresses are inserted into the address fields.
- The LLC data bytes are counted, and the number of bytes is inserted into the Length/Type field.
- The LLC data bytes are inserted into the Data field. If the number of LLC data bytes is less than 46, a pad is added to bring the Data field length up to 64.
- An FCS value is generated over the DA, SA, Length/Type, and Data fields and is appended to the end of the Data field.

- After the frame is assembled, actual frame transmission will depend on MAC.
- There are two Media Access Control(MAC) protocols defined for Ethernet: Half-Duplex Full-Duplex
- Half-Duplex is the traditional form of Ethernet that uses the CSMA/CD protocol.Full-Duplex bypasses the CSMA/CD protocol
- Full-duplex mode allows two stations to simultaneously exchange data over a point to point link that provides independent transmit and receive paths

# Half Duplex

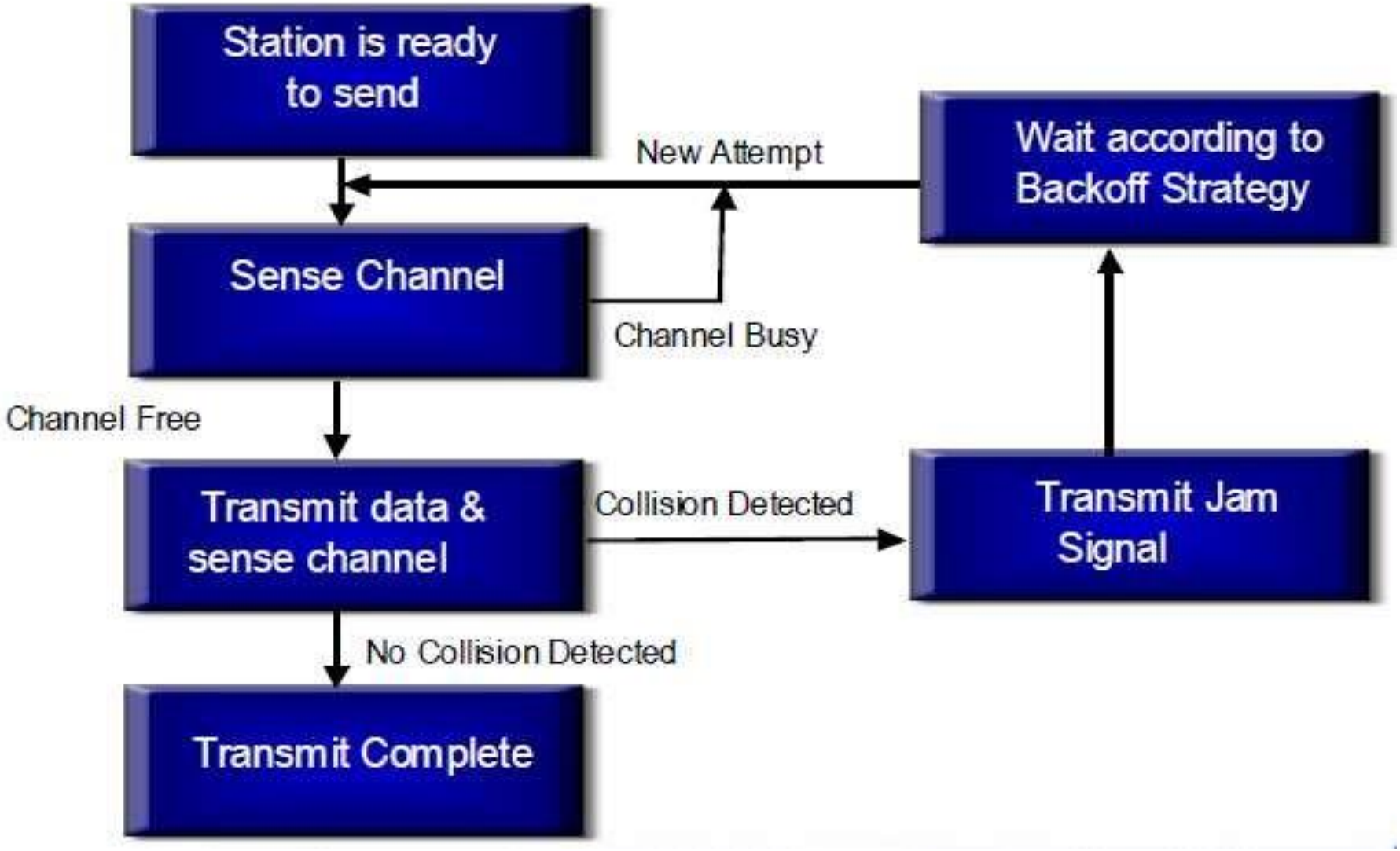
- Refers to the transmission of data in just one direction at a time.
- Half-Duplex Ethernet is the traditional form of Ethernet that uses the CSMA/CD.
- The CSMA/CD access rules are summarized by the protocol's acronym: carrier sense multiple access collision detect
- Half duplex Ethernet assumes that all the "normal" rules of Ethernet are in effect on the local network.

# Collision Detection

- The network is monitored for presence of a transmitting station (carrier sense).
- After sending the jam sequence the transmitting station waits a random period of time (called "backoff").
- If an active carrier is not detected then the station immediately begins transmission of the frame.
- While the transmitting station is sending the frame, it monitors the medium for a collision.

- If a collision is detected, the transmitting station stops sending the frame data and sends a 32-bit "jam sequence.
- If repeated collisions occur, then transmission is repeated , the random delay is increased with each attempt
- Once a station successfully transmits a frame, it clears the collision counter it uses to increase the backoff time after each repeated collision.

# CSMA/CD Flow


Station is ready to send
New Attempt
Wait according to Backoff Strategy
Sense Channel
Channel Busy
Channel Free
Transmit data & sense channel
Collision Detected
Transmit Jam Signal
No Collision Detected
Transmit Complete

# Full Duplex

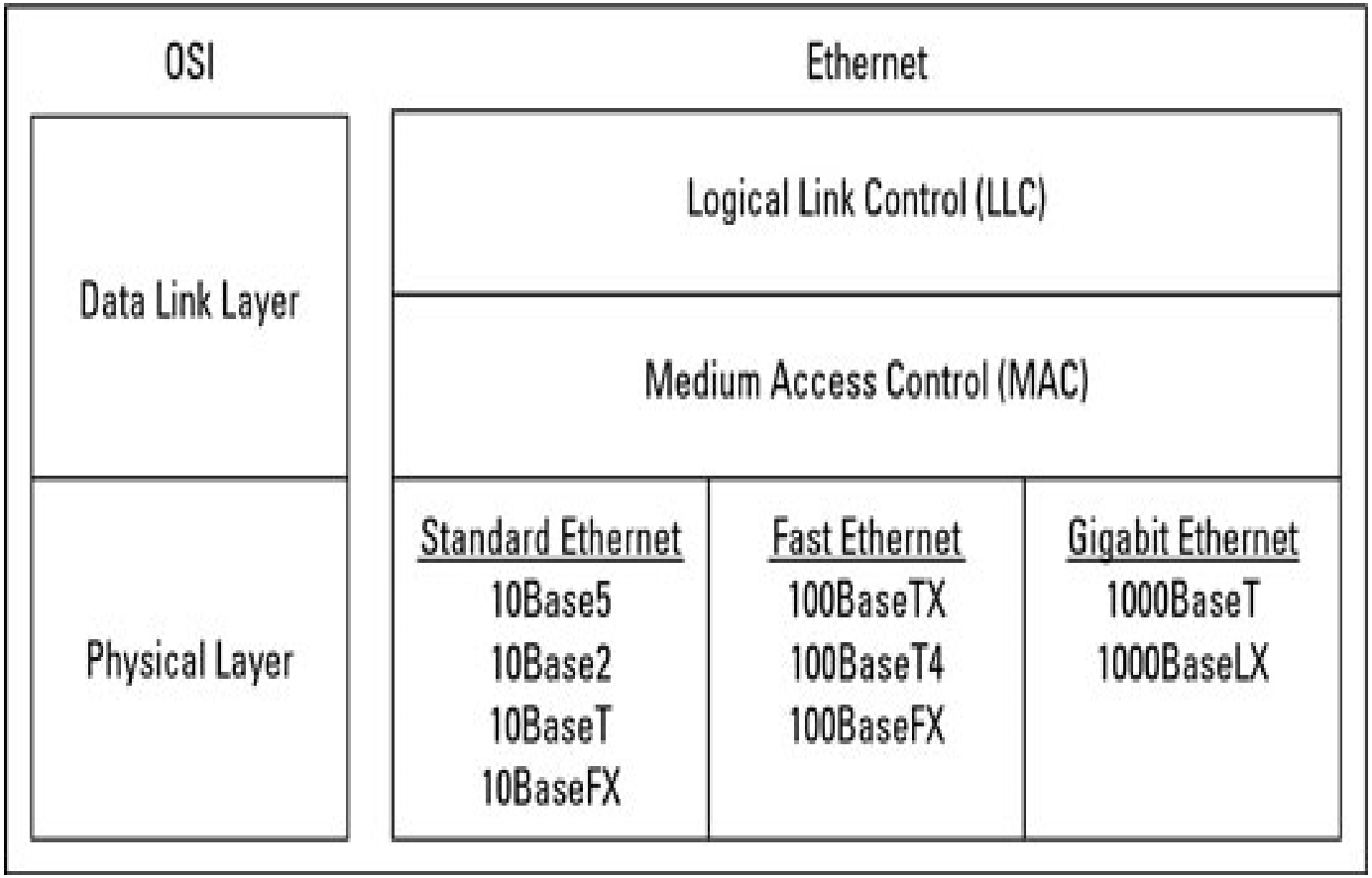
- Based on the IEEE 802.3x standard, “Full-Duplex” MAC type bypasses the CSMA/CD protocol
- Full-duplex mode allows two stations to simultaneously exchange data over a point to point link
- The aggregate throughput of the link is effectively doubled
- A full-Duplex 100 Mb/s station provides 200 Mb/s of bandwidth

- Full-Duplex operation is supported by: 10-Base-T, 10Base-FL, 100Base-TX, 100Base- FX, 100Base- T2, 1000Base-CX, 1000Base-SX, 1000Base-LS, and 1000Base-T.
- Full-Duplex operation is NOT supported by:10Base5, 10Base2, 10Base-FP, 10Base-FB, and 100Base- T4.
- Full-Duplex operation is restricted to point to point links connecting exactly two stations

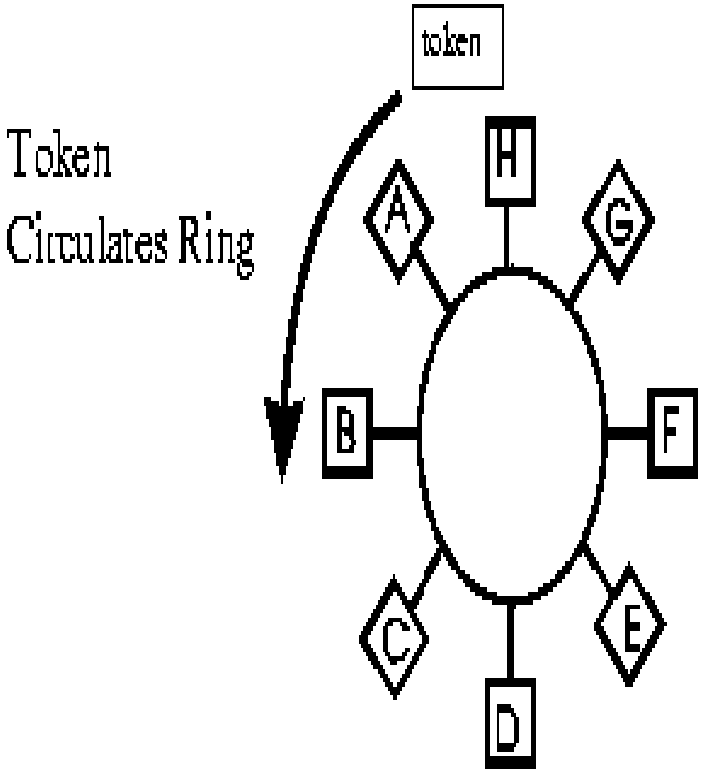
# Frame Reception

- Full-duplex MACs must have separate frame buffers and data paths to allow for simultaneous frame transmission and reception.
- The destination address of the received frame is checked to determine whether the frame is destined for that station
- If an address match is found
  - the frame length is checked and the received FCS is compared to the FCS that was generated during frame reception.
  - If the frame length is okay and there is an FCS match, the frame type is determined by the contents of the Length/Type field.
  - The frame is then parsed and forwarded to the appropriate upper layer.

# Ethernet protocol



# IEEE 802.5 TOKEN RING




- There is a point to point link between stations that form a ring.
- Physical Layer Topology: *Ring*
  - Stations connected in a loop
  - Signals go in only one direction, station-to-station
- In a token ring a special bit format called a token circulated around all the stations.

# Token Ring

- IEEE 802.5 – Token ring

***Token Ring***

- set of nodes connected in a ring.
- Data always flow in a particular direction around the ring.
- Each node in the ring receiving the frame from its **upstream neighbor** and then forwarding them to its **downstream neighbor.**

**Token** – used to access the ring

- Token is a special sequence of bits, circulates around the ring.
- Each node receives and forwards the token.

- When a **node sees the token**,
  - If it has a frame to transmit, it takes the token off the ring and inserts the frame into the ring.
  - Each node along the way simply forwards the frame. Destination node saving the copy of the frame into the adaptor and forwards the message to the next node.
  - When the frame reaches the sender, it strips the frame off the ring and reinserts the token.

# Token Ring Contd…

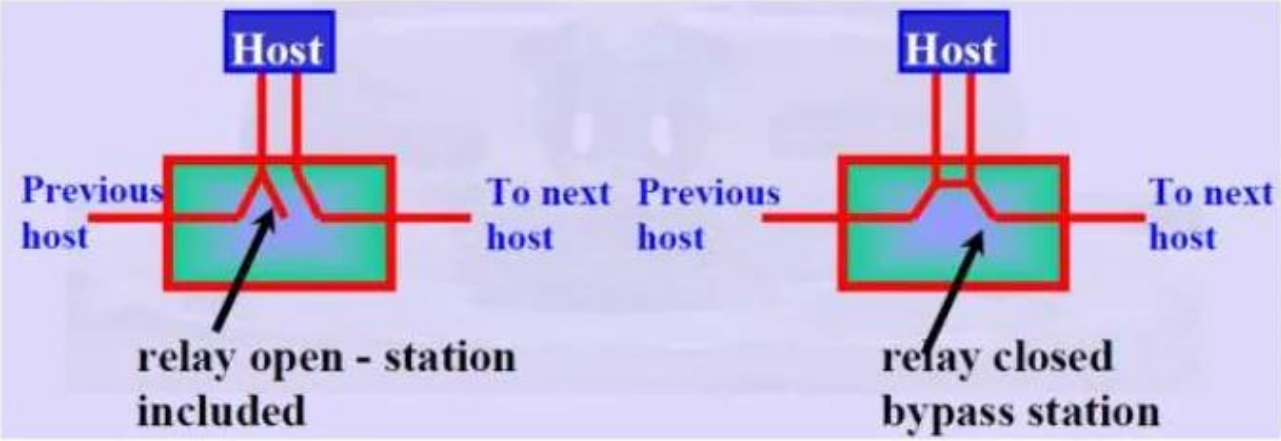
- Each node in the ring gets a chance to transmit.
- Nodes are serviced in a round robin manner.

## ***Physical Properties***

- Uses ring topology.
- **Problem** – any node or link failure leads to entire network failure.

***Solution:***

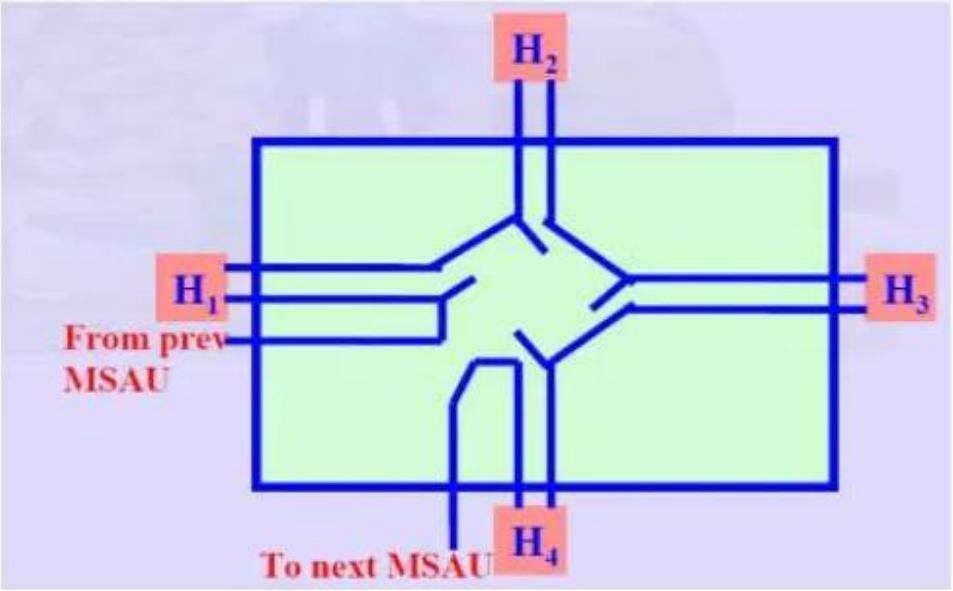
- Connecting each station into the ring using **electromechanical relay.**
  - If station is healthy, relay is opened. i.e., station is included in the ring.
  - If station fails, it stops providing power. So relay is closed and the ring automatically bypasses the station.



# Token Ring Contd…

***Multi station Access Unit (MSAU)***

- Several relays packed into a single box.
- Easy to add / remove stations from the network.




***Characteristics:***

- Supports 4Mbps or 16Mbps data rate.
- Differential Manchester encoding scheme is used.
- Number of stations in the ring is limited to 250 for IEEE802.5 (260 for IBM Token ring).

# Token Ring Contd…

- Station that has token can send data.
- Each transmitted packet contains the destination address of the intended receiver.
  - It may be unicast address, multicast address or broadcast address.
- Each node in the ring look inside the packet to see if it is the intended receiver.
  - If so, copies the data frame and pass it to the ring and the packet find the way back to the sender.
- Then sending station remove the frame from the ring and reinserts the token to the ring.

***Issues:***

- How much data a given node is allowed to transmit?

**Token Holding Time (THT)** – time period given to nodes to hold the token.

- But unfair to stations to other than the station holding the token
- This will be avoided using TRT (Token Rotation Time)

**TRT ≤ Active nodes * THT + Ring Latency**

# Token Ring Contd…

**Ring Latency** – how long it takes the token to circulate around the ring when no one has data to send.

**Active nodes** – number of nodes that have data to send.

***Reliable Transmission***

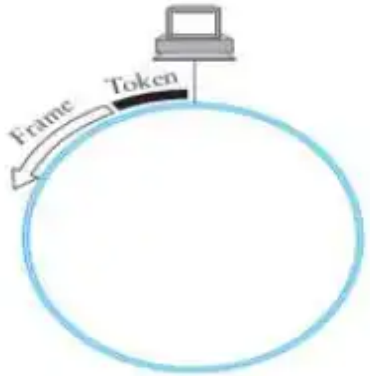
- IEEE 802.5 provides reliable data delivery using 2 bits (A&C) in the packet trailer.
- Initially these bits are set to 0.
- When a station sees a frame for which it is the intended recipient,
  - It sets A bit into '1'
- When it copies the frame into local adaptor buffer,
  - It sets the C bit into '1'
- When the sender sees the frame come back over the ring
  - If A = 0 – receiver is not functioning well.
  - If A = 1, but C = 0 then destination does not accepted the frame due to some reason (eg., Lack of buffer)

**Priority Bits:**

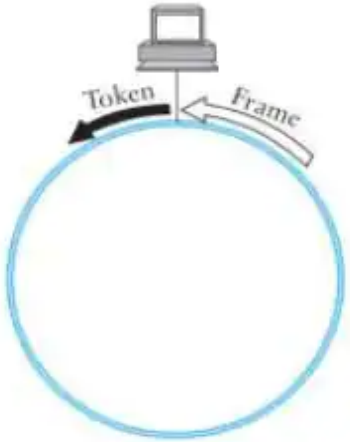
- The token contains 3 bit priority field.
- Each device that want to transmit the packet assigns a priority to that packet & the device can hold the token, if the priority is at least as great as tokens priority.
- Lower priority packets circulate for long in ring

## *Token Release*

- Early Release
  - After transmitting packet




- Delayed Release
  - After removing the packet when it returns to the sender



# Token Ring Contd…

***Token Ring Maintenance:***

- Token rings have a designated monitor.
- The monitor's job is ensure the health of the token.
- Any station in the ring can become the monitor.
  - Monitor is first elected when the ring is first connected or failure of the current monitor.
- Healthy monitor periodically announces its presence with a special control message.
  - If a station fails to see the control message for some period of time, it will assume that the monitor has failed and will try to become the monitor.
- When a station decides that a new monitor is needed, it transmits a "Claim Token" frame, announcing its intent to become the new monitor.
  - If the token circulates back to the sender, it can assume that it is OK for it to become a monitor.
  - If some other is trying to become the monitor at the same instant, the sender might see the "claim token" message from that other station first,
    - Highest Address wins

# Token Ring Contd…

***Roles of Monitor:***

- May need to insert additional delay into the ring
- Detecting the missing token
- Watches for a passing token and maintains a timer equal to the maximum possible token rotation time.

  (NumStations * THT) + Ring Latency

  Ring Latency – total propagation delay on the ring.
- Checks for corrupted or orphaned frame.
  - Corrupted frame – checksum error or invalid formats.
  - Orphaned frame – transmitted correctly on the ring, but whose parent died.

    i.e., sending station went down before it could remove the frame from the ring.
    - Its detected by using a "Monitor" bit.
    - Monitor bit is "0" on transmission
    - Set to '1' when it passes the monitor first time.
    - If the monitor sees a frame with this bit is set, it knows the frame is going by for the second time and it drains the frame off the ring.
- Detection of dead stations.
  - If any station suspects failure on the ring, it can send "beacon" frame to suspect destination.
    - Status of the ring can be established and malfunctioning station can be bypassed in the MSAU

# FRAME

- Starting delimiter and ending delimiter mark the beginning & ending of the frame.
- Access control consist of token bit, monitor bit, priority bit.
- Destination address & source address fields gives the address.
- Checksum field is used to detect transmission errors.

# Frame status field

- ✓ When a frame arrives at the interface A bit is turned on.
- ✓ If the interface copies the frame to the station the C bit is turned on.
- ✓ 3 combinations:

  A=0 C=0 : Destination not present or not powered.

  A=1 C=0 : destination present but frame not accepted.

  A=1 C=1 : Destination present and frame copied.

This increases reliability and acts as automatic acknowledgement.

# Integrating Voice and LAN Infrastructures and Applications

- INTEGRATION OF VOICE AND LAN NETWORKS will be an essential IT strategy for many businesses in the next three to five years.
- Consolidating the long separate voice and data networks has implications not only for the network infrastructure, but also for the PC, the telephone set, the PBX, and the IT organization itself.
- road map to guide organizations in making the right voice LAN-related investment decisions.

# PROBLEMS ADDRESSED

- Voice LAN is the transmission of voice traffic over a LAN infrastructure.
- Voice LAN enables server-based telephony architecture for voice switches, terminals/phone sets, and Applications.
- Today, voice traffic is transmitted across a separate circuit-switched infrastructure with a PBX or key system (for smaller offices) serving as a centralized switch.
- Under a voiceLAN scheme, both data and voice traffic are interleaved and switched as frames or cells over the same data network.

# Reasons for running their voice traffic over the LAN infrastructure

- Single infrastructure
- Single organization
- Breaking PBX lock-in

# MIGRATING THE LAN INFRASTRUCTURE

- A first step in deploying voiceLAN is to upgrade the present LAN infrastructure to support the demands of voice traffic without affecting the flow of existing data traffic.
- Infrastructure refers to the cabling plant and the local networking equipment used to carry traffic from end station to end station (i.e., hub, bridge, router, switches, and network adapters).
- The PBX is not considered part of the infrastructure in a voiceLAN environment; rather, the PBX will evolve into a call server that can be considered another type of end station on the LAN.

# Solutions for Delay-Sensitive Applications

- Voice needs only 64 Kbps, and compression or packetization reduces bandwidth requirements further.
- More important, voice is a delay-sensitive application that demands minimal latency.
- **Desktop Switching**
- **Minimize Routing**
- **Controlling LAN Backbone Traffic**
    - **Frame Switching/IP-based Solution**
    - **ATM-centric approaches**

# Frame Switching/IP-based Solution

- Ethernet (especially Fast Ethernet) trunks for interconnecting desktop switches to each other or to LAN backbone segment switches.
- Ethernet frames are switched across the network, delay problems may still occur for voice.
- Ethernet has no mechanism for prioritizing one frame over another. Therefore, as network traffic increases, small frames carrying a voice payload may often have to wait in switch buffer queues behind large frames carrying data.
- Because voice has a delay tolerance of only 75 milliseconds, the lack of prioritization across a switched Ethernet network may degrade the quality of voice communications. Furthermore, this fundamental problem will not disappear with expanded bandwidth under Fast (or Gigabit) Ethernet.

# RSVP

- Most promising solutions to Ethernet's lack of prioritization or guaranteed latency is to handle the problem at Layer 3 via the RSVP.
- RSVP, which was developed by the IETF and leading network product vendors, operates by reserving bandwidth and router/switch buffer space for certain high-priority IP packets such as those carrying voice traffic.
- RSVP's best-effort capability is sufficient for several delay-sensitive applications, such as non-realtime streaming video or audio. However, it is questionable whether RSVP can support real-time voice communications over the LAN to a level of quality and reliability that is acceptable in a business environment.

# ATM-Based Backbone Solutions

- ATM was designed specifically to support both voice and data traffic over a common infrastructure and provides multiple QoS levels.
- ATM's CBR service guarantees a virtual circuit of fixed bandwidth for high-priority traffic such as voice. In addition, ATM uses a relatively small, fixed-length cell (53 bytes) rather than a variable-length frame to transport traffic, thereby limiting the maximum time any one cell must wait in a switch buffer queue.
- The use of ATM links/trunks between LAN switches neatly solves the problem of supporting both voice and data traffic for that portion of the network.

- ATM to the desktop is more problematic, however. The most common standard for ATM LANs operates at 155 Mbps over Category 5 UTC cable or optical fiber.
- However, deploying 155 Mbps ATM to every desktop is currently too expensive for the vast majority of organizations (although it is beginning to be deployed as a LAN backbone technology).
- In order to deploy a reliable voiceLAN solution cost-effectively using ATM, a lower-cost access technology must be deployed to the desktop.
- However, this access technology must also be able to extend the benefits of ATM's QoS from the ATM backbone all the way to the desktop.
- An organization can choose from among several potential access solutions, including ATM25, Ethernet using IP/RSVP, or Ethernet/CIF.

# ATM25 Access

- ATM25, as its name implies, is a 25 Mbps version of ATM designed specifically for desktop connectivity to a 155 Mbps ATM backbone.
- ATM25 provides all of the QoS benefits of higher-speed ATM and can be used to build end-to-end ATM networks.
- ATM25 can also operate over Category 3 UTC cable, whereas 155 Mbps ATM and Fast Ethernet require organizations to upgrade their UTP cabling to Category 5 UTP cable.
- The downside of ATM25 is that it requires replacing all legacy network adapters where voiceLAN will be deployed. In addition, ATM25 adapters and switches are still considerably more expensive than 10Base-T Ethernet adapters and switches.

# Ethernet RSVP/IP Access

- The desktop end station sends voice in IP packets (further encapsulated inside Ethernet frames) to the switch, using RSVP to request bandwidth to be reserved for the voice conversation.
- The desktop switch then terminates the IP connection and converts the voice payload to ATM cells for transmission across the backbone (or the desktop switch may forward these IP datagrams across the ATM backbone without terminating the IP connection).
- The desktop switch is also responsible for mapping the RSVP bandwidth reservation request (at the IP level of the architecture) to an appropriate ATM QoS for the ATM connection.

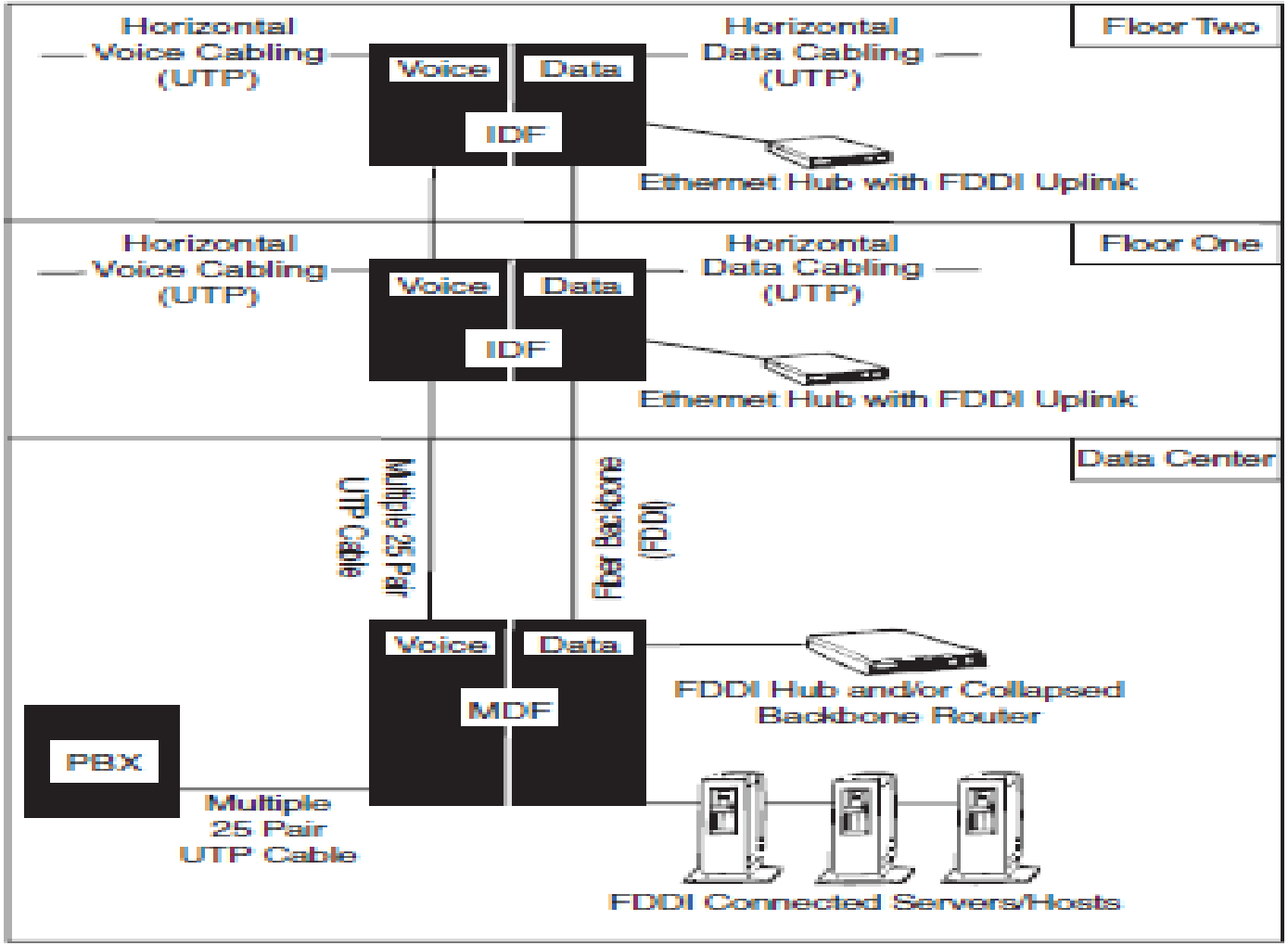
# Ethernet CIF Access

- CIF allows a desktop application to place voice traffic in ATM cells that are subsequently inserted into Ethernet frames by the network adapter driver for transport over the link from the adapter to switch. At the Ethernet switch, cells are extracted from the frames and sent across the ATM backbone.
- CIF's ability to guarantee quality of service comes at a price. CIF requires installation of special software or NIC drivers in workstations to accomplish the framing of ATM cells. In addition, transporting traffic inside of ATM cells, which are in turn encapsulated by frames, entails significant overhead, reducing the usable bandwidth on an Ethernet segment to 6 Mbps to 7 Mbps.

# CONSOLIDATION OF THE CABLING PLANT

- No matter what technology is used for voice transport (i.e., ATM or IP), voiceLAN deployment requires optical fiber in the risers of buildings for backbone connectivity.
- Most large organizations have already installed fiber for their LAN backbone and therefore no upgrade to the cabling plant is necessary.

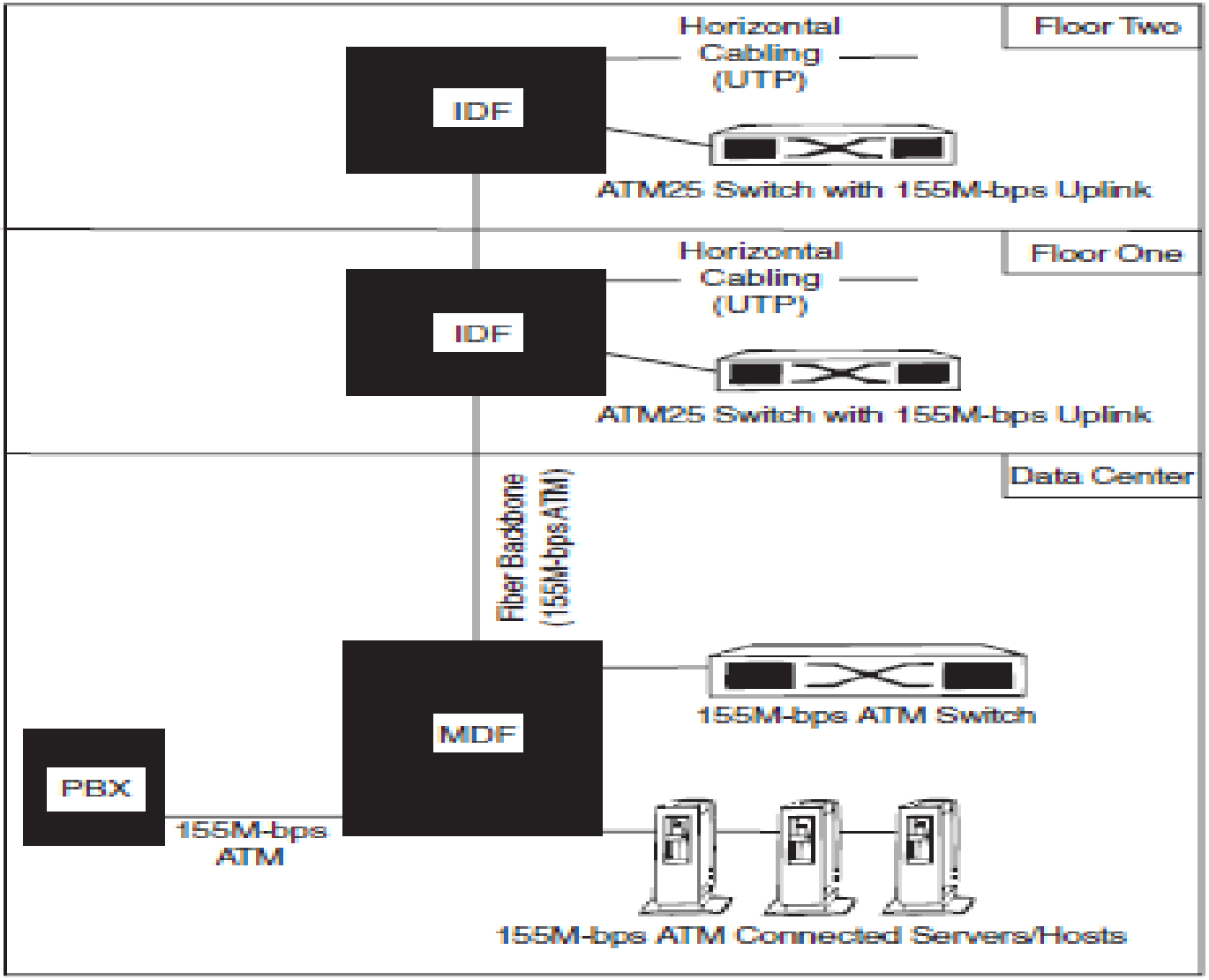
# Legacy voice and data cabling infrastructures




**Key:**

| | |
|---|---|
| FDDI | fiber distributed data interface |
| IDF | intermediate distribution frame |
| MDF | main distribution frame |
| PBX | private branch exchange |
| UTP | unshielded twisted pair |

# Consolidated cabling infrastructure




**Key:**

| | |
|---|---|
| FDDI | fiber distributed data interface |
| IDF | intermediate distribution frame |
| MDF | main distribution frame |
| PBX | private branch exchange |
| UTP | unshielded twisted pair |

# MIGRATING THE DESKTOP

- The deployment of voiceLAN also entails a migration of the desktop PC to become telephony-enabled.This migration has two components: hardware and software.

# Hardware Upgrades

- In a pure voiceLAN architecture, all voice calls are received via a PC and its LAN adapter card rather than via a desktop telephone wired to a PBX or voice switch.
- There are two alternative human interfaces for people to interact with the PC to receive voice communications: the PC itself and the traditional desktop telephone.

# PC as the interface

- Voice traffic is processed by a PC sound card and the user employs a PC-attached microphone and headset.
- Appropriate for users who are already using a microphone and headset
- Voice packets are processed by the PC's CPU.
- Hampering performance of other applications that might be running simultaneously.
- In addition, if the PC locks up, the user's conversation may be interrupted.
- Phone set must be able to connect directly to the PC so that voice traffic can be Received directly from the network adapter card without having to pass through the CPU.
- Today this can be accomplished through a third-party plug-in card.

# Universal Serial Bus

- A more elegant solution for accomplishing a direct connection is the USB interface, originally developed by Intel.
- The USB supports 12 Mbps of throughput and allows USB-compatible telephone sets to connect directly to the PC without the need for an additional plug-in card. This alternative greatly reduces the cost of deploying voiceLAN. Several vendors have released or will soon release telephones conforming to the USB standard.

# Firewire bus

- The Firewire bus runs at speeds of up to 400 Mbps, which makes it appropriate for video traffic as well as voice.
- This high level of performance also may make Firewire too expensive for ubiquitous deployment, particularly if voiceLAN, not video, is the driving application.
- Deploying USB-compatible phones is currently the most prudent choice for voiceLAN migration at the desktop.

# Software Upgrades

- To take maximum advantage of voiceLAN technology, PC-resident applications need to communicate with the PBX and PC-attached desktop phone sets. For this, a standardized software interface is required.
- Microsoft Corp. has introduced a newer API, combining its Windows data transmission API (Winsock) with its voice communications API (TAPI).
- This consolidated API, known as Winsock 2, makes it even easier for developers to write integrated voice and data communications applications.

# MIGRATING THE PBX

- Legacy Telephony
- Linking Distributed PBX Components
- Server-Based Telephony

# Legacy Telephony

- Today's PBX and telephony systems are analogous to the host and dumb terminal model of the mainframe era. PBXs are relatively inflexible, proprietary, and expensive to maintain and upgrade in the same way mainframes are. Phone sets are still the most ubiquitous desktop instrument for telephony communications, but the PC offers the most intuitive interface to advanced features. Moving from the traditional PBX model to a server based telephony model represents the final stage in the migration to a fully integrated voice and data network.

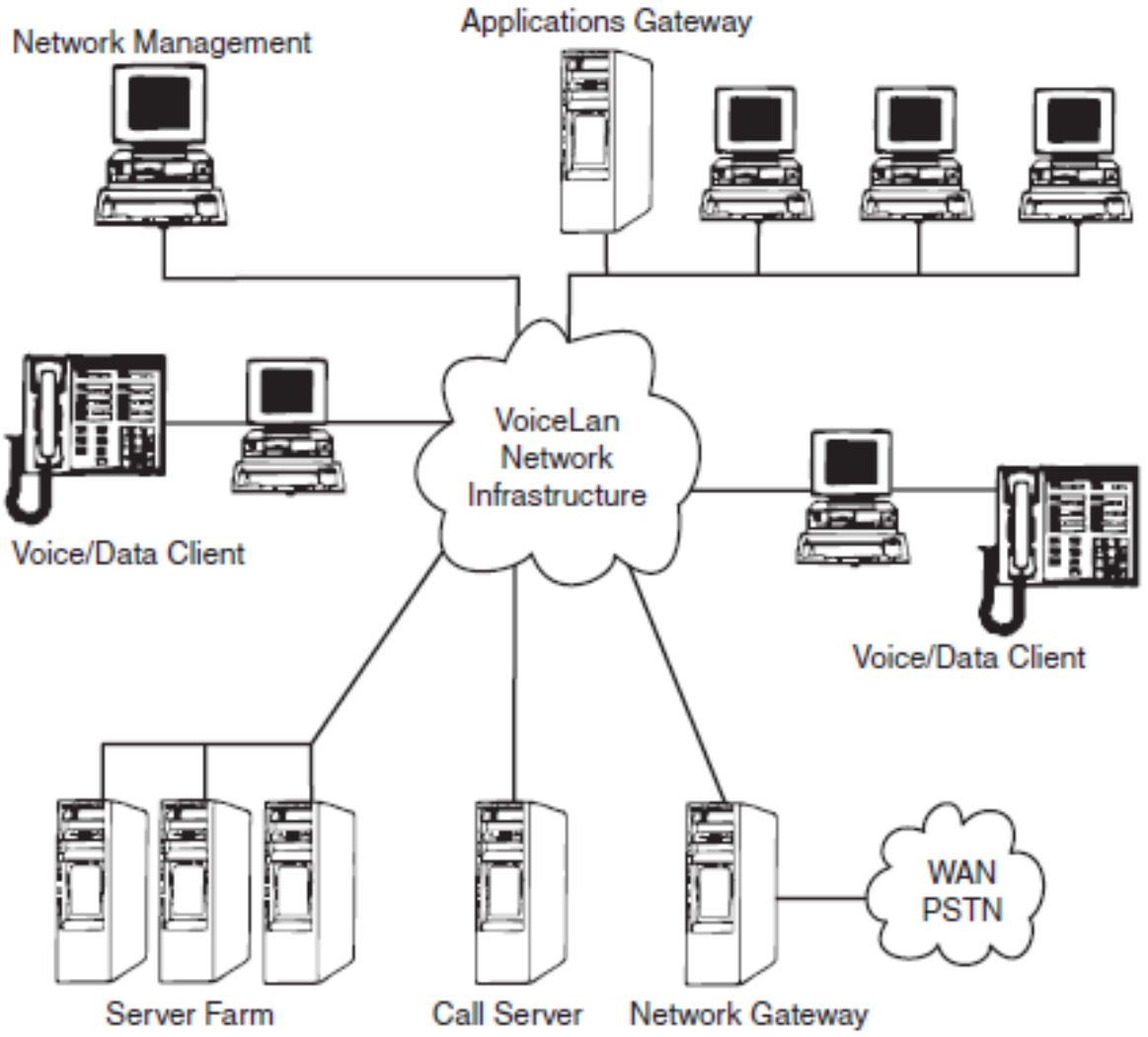
# Linking Distributed PBX Components

- This type of architecture has traditionally required a dedicated fiber backbone to connect multiple units
- This infrastructure is already in place in most larger campus network environments. In this case, the horizontal connection between the PBXs and the telephone sets at the desktop can continue to use the traditional voice network infrastructure.
- There are two advantages to this architecture:
  1. Distributed PBXs scale more cost-effectively than a single, large PBX.
  2. The necessity for installing and maintaining dual backbones, one for voice and one for data, is eliminated.

# Server-Based Telephony

- A server-based telephony architecture allows for the traditional functions of the PBX to be broken down into its components and distributed on the voiceLAN network.
- The switching function of the PBX can be handled by the frame or cell switches of the data network, whereas the call control function can be moved to a server. Specific telephony applications can also be moved to distributed application servers and integrated with other networked data applications.

# VoiceLAN architecture




**Key:**
PSTN public switched telephone network
WAN wide area network

# Initial Implementation Tips

- Server-based telephony should be implemented initially in specific workgroup environments.
- Where a voiceLAN model is implemented, the user's port on the legacy PBX should be left unchanged until the voiceLAN deployment has stabilized and has been thoroughly tested.

# Desktop Telephony Applications

- GUI phone
- Integration with PIM software
- GUI voice mail
- Integrated messaging

# MIGRATING USERS

- **Collaborative applications-** A server-based telephony architecture facilitates the integration of voice communications to collaborative software that allows multiple people to work on the same document while communicating.
- **Voice/database applications-** At present, computer telephony integration permits a certain level of integration between PBXs and databases; however, deploying such applications is expensive and generally reserved for telemarketing or customer service applications. A server-based telephony architecture allows high-end CTI functionality to be deployed on a much wider scale and to be made accessible to the general user population.

# Decision points/recommendations for VoiceLAN migration

| Decision Points / Migration Steps | Typical Situation | Recommendation | Impact |
|---|---|---|---|
| **Strategy** | • Voice not a part of IT strategy<br>• Separate budgets<br>• Separate planning<br>• Separate organizations | • Ensure voice and voiceLAN are embedded in IT strategy<br>• Voice must be considered integral component of overall plan | • As compelling events occur and decisions are made, organization continually moves closer to voiceLAN goal |
| **Enterprise** | • More bandwidth required for workgroup or user applications<br>• Corporate pressure to reduce costs and provide productivity improvements<br>• Cost savings or simplicity (elimination of duplicate infrastructures) sought | • Evaluate opportunity to converge voice/data on single backbone<br>• Upgrade or replace existing backbone LAN<br>• Converge voice/data functional organizations | • Bandwidth issue resolved<br>• Simplified infrastructure<br>• Organization positioned for voiceLAN |

# Decision points/recommendations for VoiceLAN migration

| | | | |
|---|---|---|---|
| **Workgroup** | • Application-specific bandwidth requirements<br>• Productivity improvements and competitive advantage sought<br>• Remote offices demanding "head-office" type functionality and access | • Voice-enable applications<br>• Evaluate server-based telephony solutions<br>• Exploit opportunity to trial voiceLAN technology on workgroup basis<br>• Extend voiceLan-capable technology to workgroup via ATM or switched Ethernet access network | • Maximize productivity<br>• Move another step closer to voiceLAN<br>• Force a break from traditional voice model |
| **Desktop** | • Disparate voice and computing instruments and applications<br>• Dual wiring infrastructure<br>• Lost productivity | • Ensure strategy supports evolution to single wiring to the desktop<br>• Opportunity to evaluate computer-attached telephones<br>• Roll out in logical manner (starting with R&D organization, then general business groups, finally call centers) | • Final leg of voiceLAN convergence to the desktop<br>• Achieve simplicity, cost savings through streamlined moves/changes<br>• New applications deployment and enhanced productivity |

# ATM LAN Emulation

- LAN emulation allows users of an ATM network to run any higher-layer protocol in its existing state without requiring any changes.
- LANE is a method of performing basic bridging functionality between a host on an ATM-attached bridge and an ATM-attached host, or between two ATM attached hosts.
- Because LANE masks much of the complexity from users while allowing them to benefit from ATM, it has become the standard of choice for transporting data traffic across heterogeneous networks

# GOALS OF LANE

- To provide seamless and transparent bridging between an arbitrary number of hosts, where the hosts may be ATM native or connected to the ATM cloud via an interworking device.
- To support the goal of transparent operation, the connection-oriented nature of ATM is concealed. To allow seamless operation, features found in the shared-medium domain such as broadcast are emulated.
- Ease of use is addressed at the outset by designing in support for services, including automatic configuration and address registration, that allow true plug-and-play operation. A secondary goal is simplicity of design.