Networks

- Allow number of independent stationary devices or computers to communicate directly
- Provides a skeletal infrastructure for a collaborative system

Networking

By
Prashant Mali [BSc,MSc(CS),CNA,LLB]

Evolutionary Trends

- 1946: First Computer ENIAC
- 1969: A network of four computers in the world
- 1984: 1,000 networked computers
- 1995: 10,000,000 computers connected
- 1998: 100,000,000 computers connected

Advantages of Networks

- Sharing Resources
- Communications
- Cooperation and Collaboration
- Distance and Remote Processing
- Productivity Improvement

Telecommunications

- Basics of communications
- Modes of transmission
- Switching techniques
- Network topologies
- Networking Standards
- Networking Devices
- Types of networks
- Communication media
- Error Detection

Basics of communications

Basic Components

1. Content or message that is to be transmitted between the parties
2. Media that carries the message from the sender to the receiver
3. Protocols that provide rules of communications

Basics of communications

Communication system must ensure the following

1. Accuracy of the message that is to be transmitted
2. Messages have to be delivered in time and in a reliable fashion to the recipient every time.
3. Provide mechanisms to ensure integrity of messages

Components

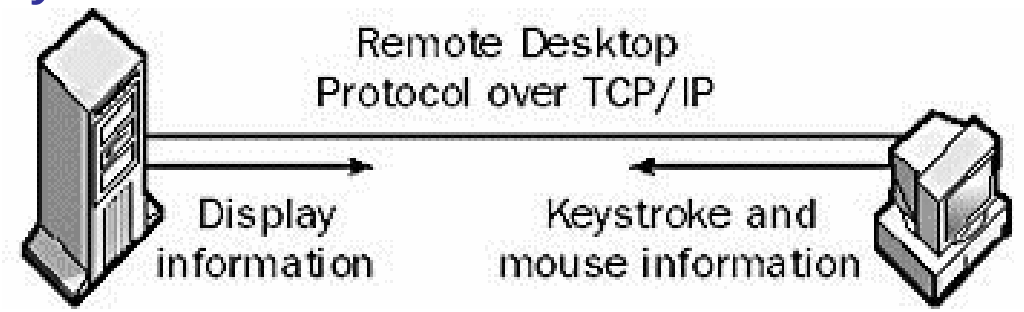
The principal components of a telecommunication system are-

1. Communication devices
2. Communication channels
3. Communication software

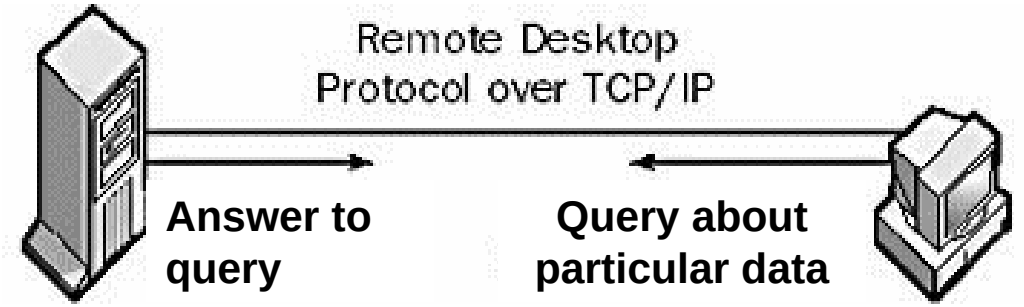
Components - Terminal

Combination of keyboard and monitor screen.

Dumb Terminals



Smart Terminals



Components - Modem

MODEM - Modulator - Demodulator

1. At the sender's end, it converts the digital signal from the computer into an analog signal to be carried over the telephone line.
2. At the receiver's end, it converts the received analog signal into digital signals for further processing by the computer.

Modem functions

Modems undertake three functions that affect the reliability of the communication subsystem:

- They increase the speed of transmission by using a form of multiplexing technique.
- Modems can reduce the number of line errors that arise through distortion if they use a process called dynamic equalization. The modem continuously measures the line characteristics and adjust for signal attenuation and distortion.
- They reduce the line errors that arise due to noise.

Components - Modem

Modem Speeds - Measured in bps - bits per second

Newer modems have speeds upto 56 Kbps

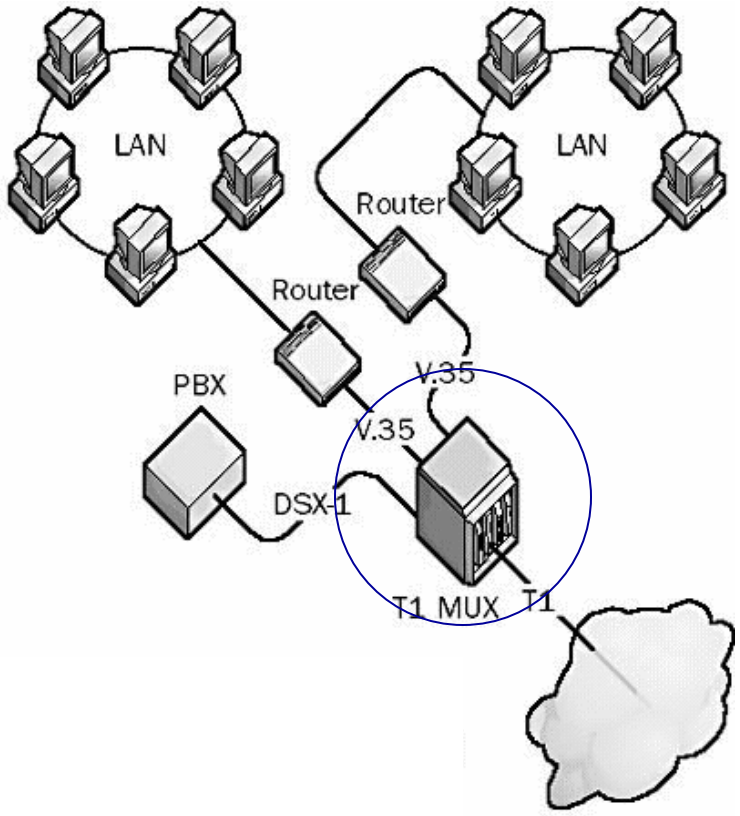
External Modems - External Units	*Rs.500-2,000*
Internal Modems - Modem cards	*Rs. 500-1,000*
PCMCIA Modems - for laptops	*Rs.500-3,000*

Components - Multiplexers

Multiplexers allow -

To use several communication channels at the same time.

To link low speed lines to high-speed lines



Multiplexers

Multiplexing techniques use static channel derivation schemes to assign transmission capacity on a fixed, predetermined basis.

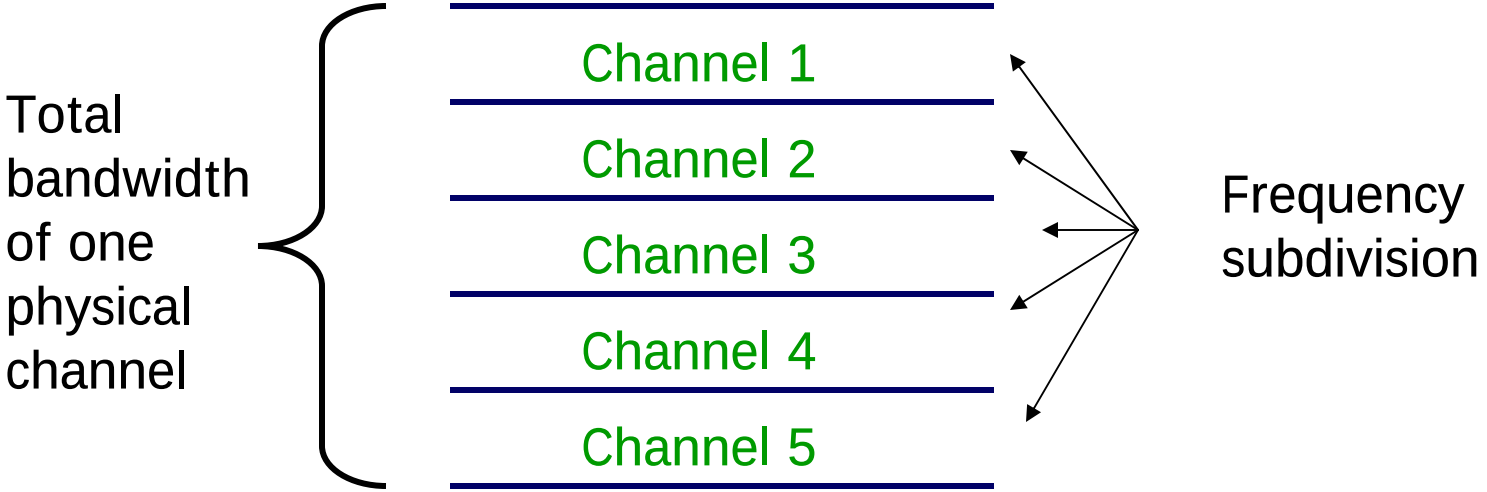
Each data source shares a common transmission medium, but has its own channel.

Two types of multiplexing are used:

- Frequency division multiplexing
- Time division multiplexing

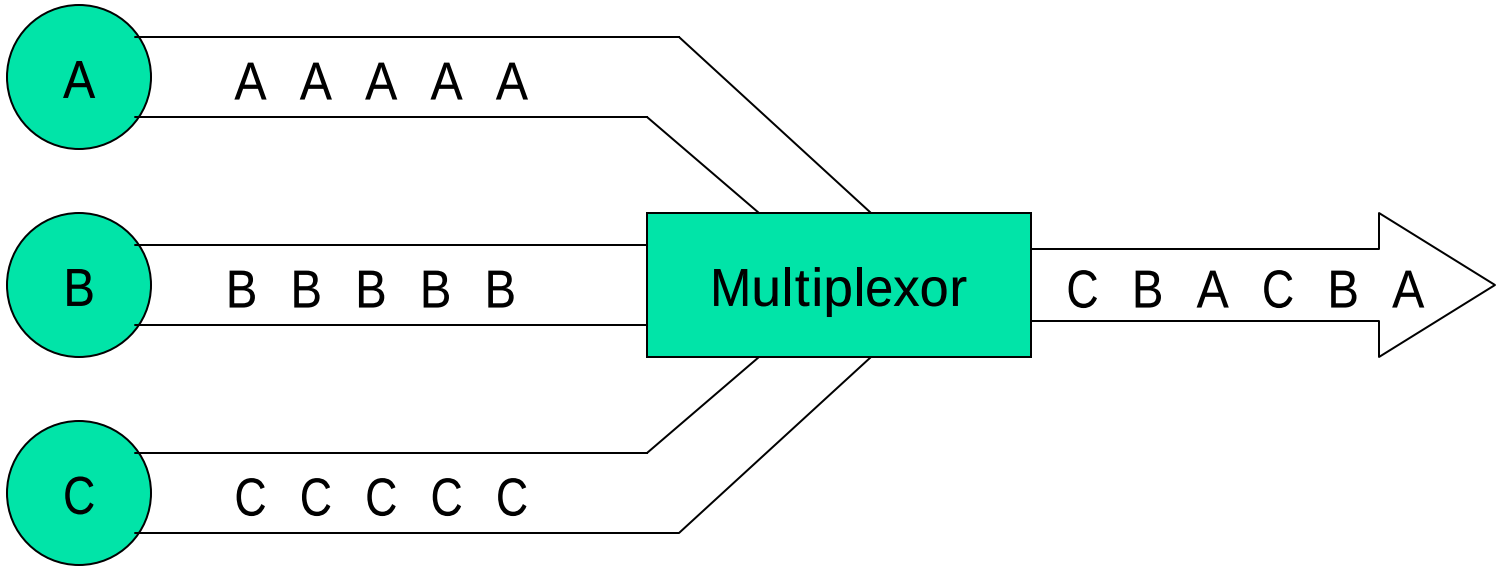
Frequency Division Multiplexing

In Frequency Division Multiplexing a single bandwidth is divided into several smaller bandwidths that are used as independent frequency channels. Thus channels are defined in terms of a frequency band.



Time Division Multiplexing

In Time Division Multiplexing small, fixed time slots are assigned to a user during which the user transmits the whole or part of the message. Thus channels are defined in terms of a time slot.



Wave Division Multiplexing

In Wave Division Multiplexing relies on the fact that a laser can be designed to emit monochromatic light. Each signal to be transmitted is attached to a laser that emits a different colour light beam. All the length beams are sent at the same time and a receiving device splits the colours into the original signals again.

Multiplexing

- Allow more efficient use to be made of the available channel capacity.
- Multiplexing techniques help protect data against subversive attacks. Wiretappers have great difficulty in disentangling the myriad of messages passing over the channel
- Multiplexers are critical components in a network and they should have a high mean-time-between-failure (MTBF).

Front-end Processors

Front-end Communication Processors

- Used mainly by big computers
- Error Control
- Formatting, Editing
- Controlling, Routing, Speed and Signal Control
- Grouping data into complete units to submit to the host CPU

Front-end Processors

Functions of Front-end Communication Processors

- Activating and deactivating the communication lines
- Translating the character codes
- Control character recognition and error checking
- Error recovery and diagnostics
- Polling and addressing of remote units

Cluster Controllers

Functions of Cluster Controllers

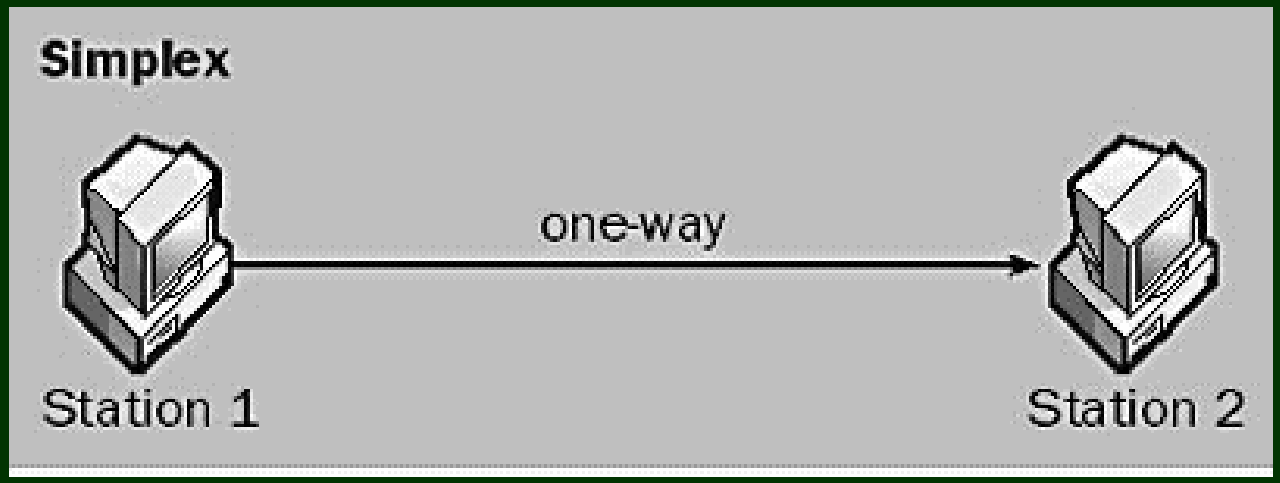
- Cluster controllers control a number of devices such as terminals, printer, and auxiliary storage devices.
- Their function is to buffer the message - they store and forward the message.
- The buffered message is then transmitted to the receivers.

Cluster Controllers

Benefits of Cluster Controllers

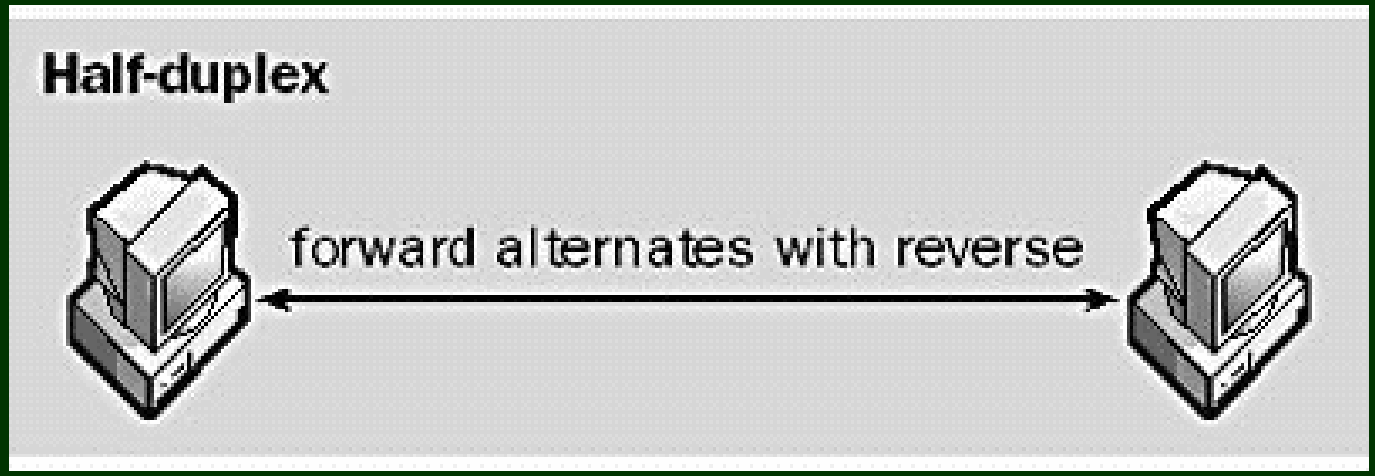
- The cost of communication logic is amortized over a number of terminals.
- There is a single point of interface to a communication circuit on both the terminal and computer ends, thus saving on I/O hardware costs.
- It is easier to manage related resources or devices that are treated as a unit.

Simplex Transmission



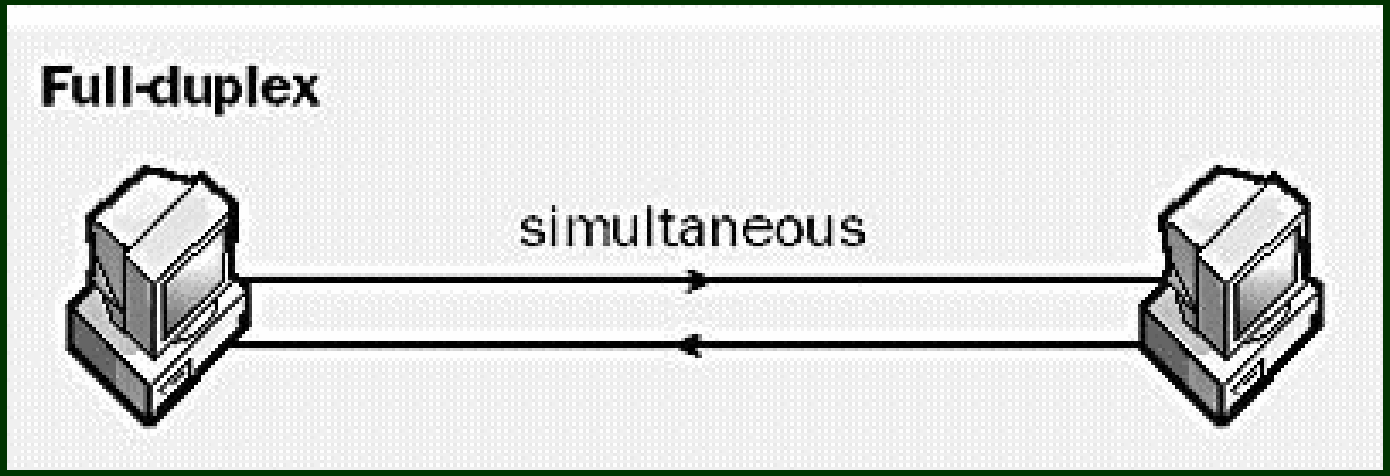
Examples

Half-Duplex Transmission



Examples

Full-Duplex Transmission



Examples

Modes of Transmission

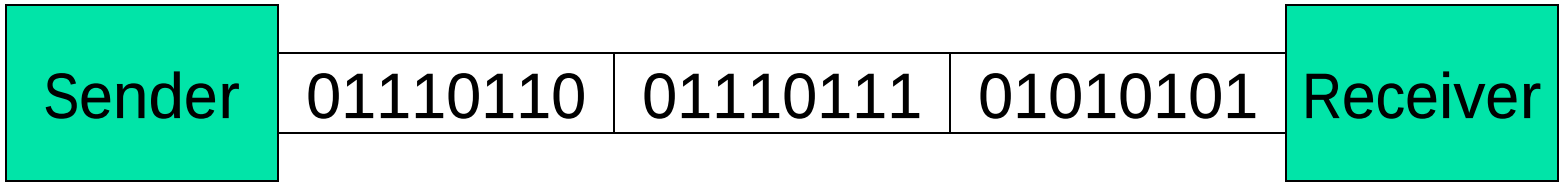
Asynchronous Transmission

- Easy to implement
- Overheads due to redundant or extra information
- Used between computer and terminal
- Comparatively inexpensive

Modes of Transmission

Synchronous Transmission

- High speed transmission
- No start and stop bits and no gaps
- Data flows in a continuous stream
- The process of grouping the bits rests with the receiver
- Expensive, since complex hardware required.



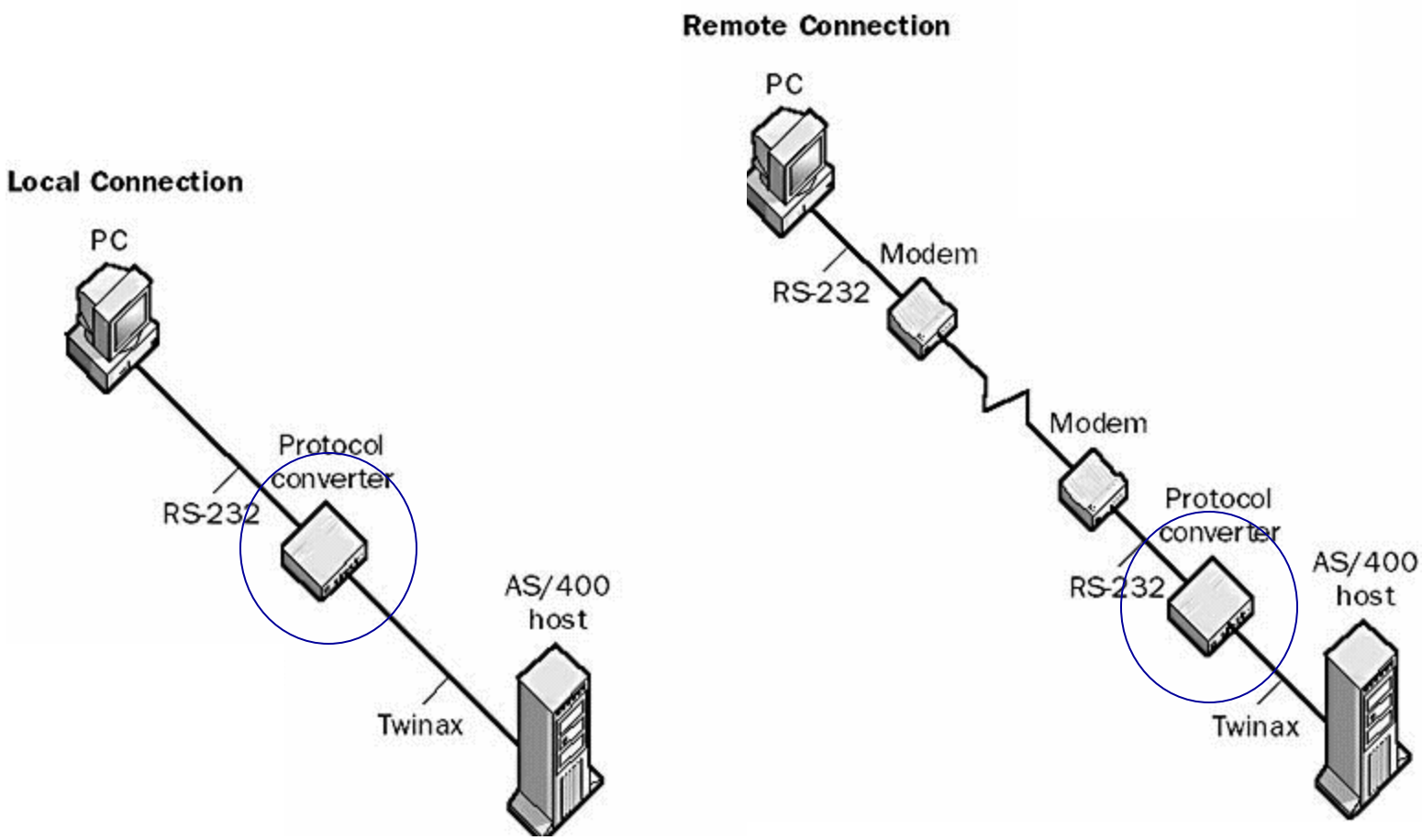
Protocol Converters

Functions of Protocol Converters

- Protocol converters are devices to convert one protocol to another such as between synchronous and asynchronous transmission.
- For example, a protocol converter might be placed between a asynchronous terminal and the host computer to facilitate synchronous transmission.

Protocol Converters

Convert from one protocol to another



Spools

Functions of Spools

- Spools are an operation that allows more efficient use of output devices. It creates spool files representing virtual output devices so that write operations to a device, such as a printer, can occur without having the physical device available.
- Think of spools as a queuing system. When the printer is busy, the printouts sent will be arranged in a queue and later printed in the order in which they were received.

Buffers

Functions of Buffers

- Buffers are a temporary storage area (used by spooling) to compensate for different rates of data flow when transmitting data from one device to another, such as from a computer to a printer.
- This process also facilitates more efficient processing since the computer can process the data stored in one buffer while an alternate buffer is being loaded.
- This reduces the time the computer processor must wait for input/output devices.

Circuit Switching

Circuit Switching -

- Establishes a physical connection between sender and receiver and keeps connection open till the end of the session.
- Public Switched Telephone Network (PSTN) and Integrated Services Digital Network (ISDN) are examples

Circuit Switching

- Guaranteed capacity of data transfer
- Used exclusively by the two subscribers of the call
- Delivery time is guaranteed

- Inflexible
- Connection set-up and tear-down required
- User pays for the circuit even when they do not use it.
- Does not provide any error or flow control on the transmitted data, so this must be performed by the users.

Packet Switching

Packet Switching -

- A sophisticated means of maximizing transmission capacity of networks.
- Message is broken into packets and each packet has sender and receiver information and control information.
- Packets are routed individually through the network depending on availability of channel for each packet.
- Passwords and all kinds of data can be included within the packet and the cost is by packet and not on message, route, or distance.

Packet Switching

Each packet has three important portions:

- Header - which holds information about the data in the packet like length of the packet, packet number, destination address, origination address.
- Body - This is the actual data that is contained in the packet which is to be delivered.
- Footer - This portion holds control information for error checking. A checksum is calculated and appended in the footer. This is checked at the receiving end.

Types of Packet Switching

Virtual Circuit - An initial set up phase is used to set up a route between the source and the destination. All packets have to follow the route that has been set up. The packets have short headers, containing only a virtual circuit identifier (VCI) and not their destination information. Each intermediate node passes the packets according to the information stored in it during the setup phase.

Most common forms are X.25 and Frame Relay, which are used for Public Data Networks (PDN)

Types of Packet Switching

Datagram Circuit - In this approach, each packet is treated as an independent identity and its header contains full information about the destination of the packet. The intermediate nodes examine the header of the packet and decide the node for the packet to be sent so that it reaches the destination.

Here packets follow different routes to the destination and hence delivery is not guaranteed. Moreover the packets arrive at the destination in different order and the destination node has to arrange them in proper order.

The main implementation of the Datagram is the Internet.

Packet Switching

- Flexible - packets travel the most optimal route and are finally assembled together
- Little set-up or tear-down overhead
- Sophisticated error and flow control procedures are applied on each link by the network.

- Delivery time is not guaranteed
- Mechanism is much more complicated and expensive.

Message Switching

Message Switching - Store-and-Forward technique. A complete message is sent to a concentration point and stored until a communication path can be established with the destination node.

- Transmission cost is dependent on the length of the message

- Delivery time is not guaranteed - each stage has to wait till the complete message is received before transmitting to the next stage.

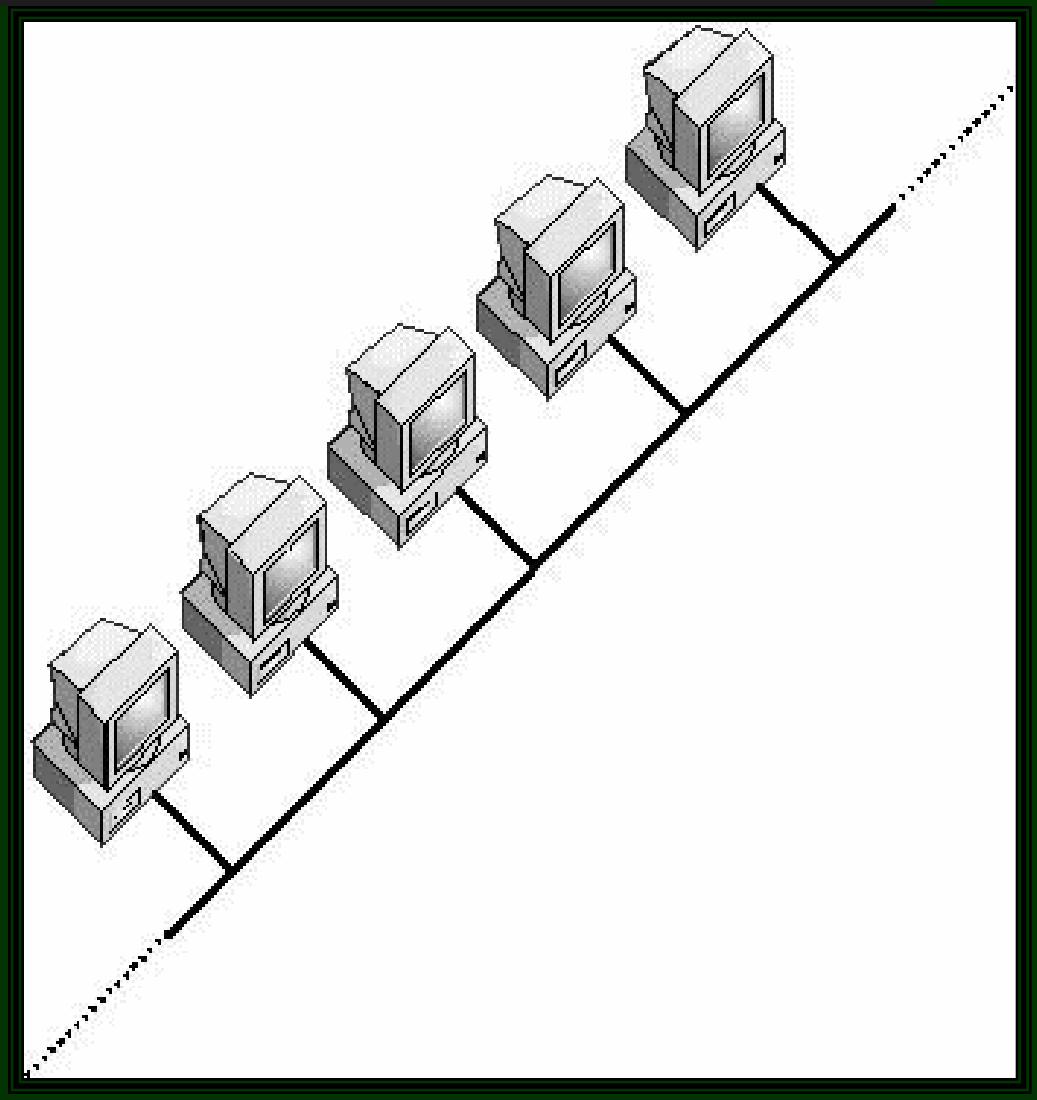
Network Topology

A network topology describes the configuration of a network - How the network components are connected together. Following are the main topologies.

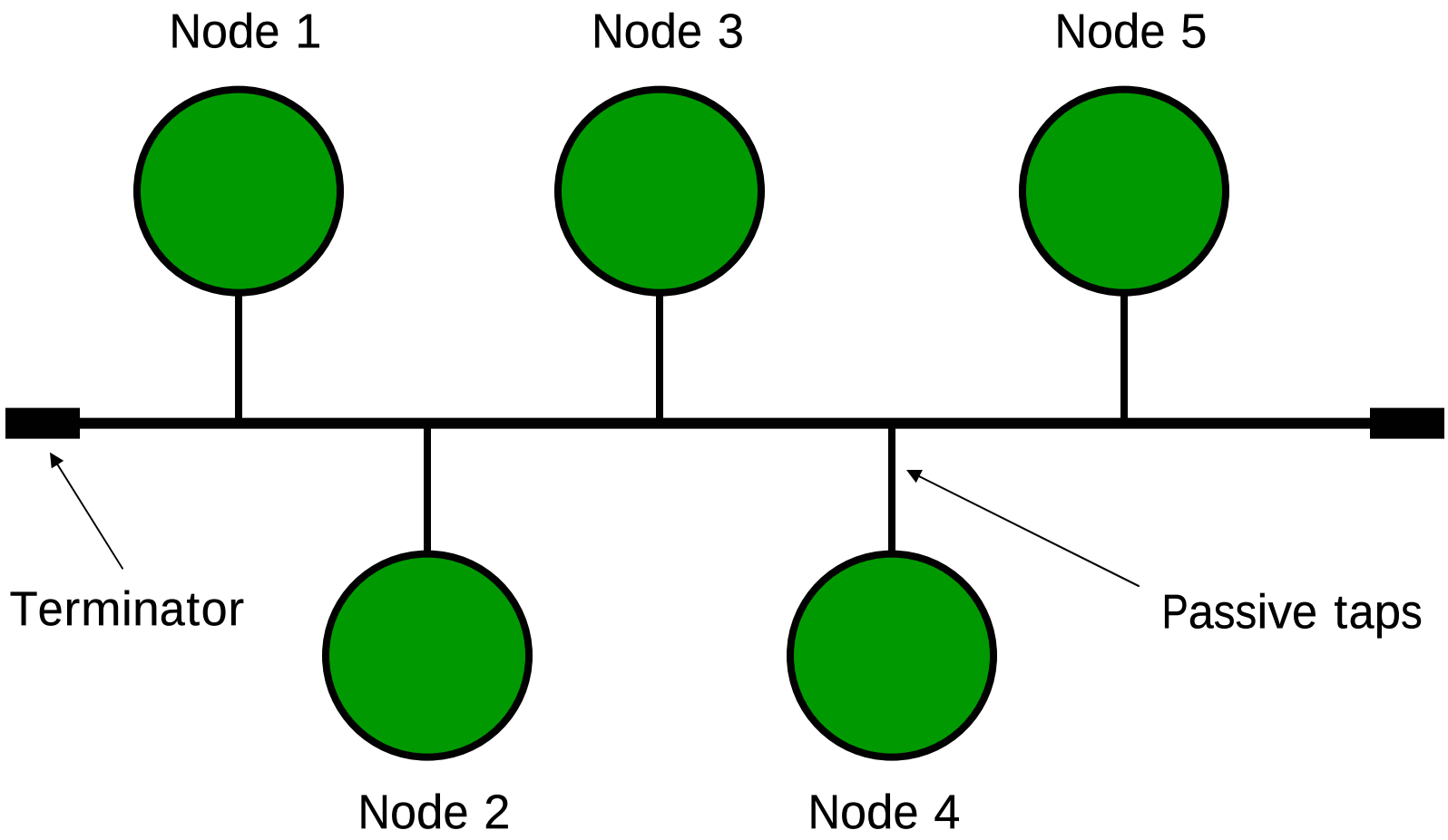
1. BUS
2. STAR
3. RING
4. MESH
5. TREE
6. HYBRID

Bus Topology

The bus topology connects workstations using a single cable. Each workstation is connected to the next workstation in a point to point fashion. All workstations connect to the same cable



Bus Topology



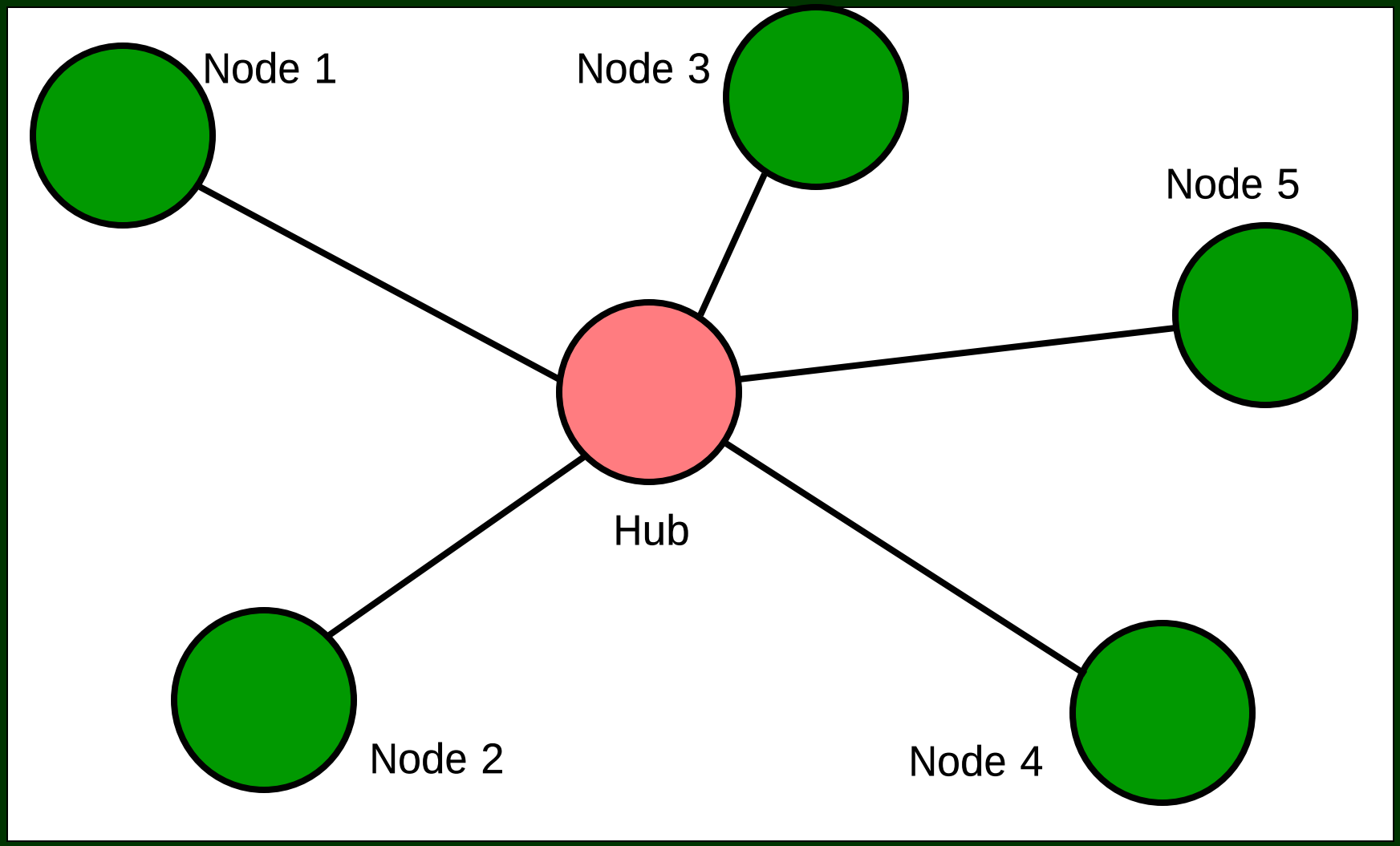
Bus Topology - Advantages

- Reliable in very small networks and easy to implement
- Inexpensive, since least amount of cable required
- Inexpensive, since no extra equipment like hubs or switches is required
- Easy to extend by adding more cable
- Repeaters can be added to extend to longer distances
- Since passive taps are used to connect nodes to the bus, failure of one node will not bring down the entire network.

Bus Topology - Disadvantages

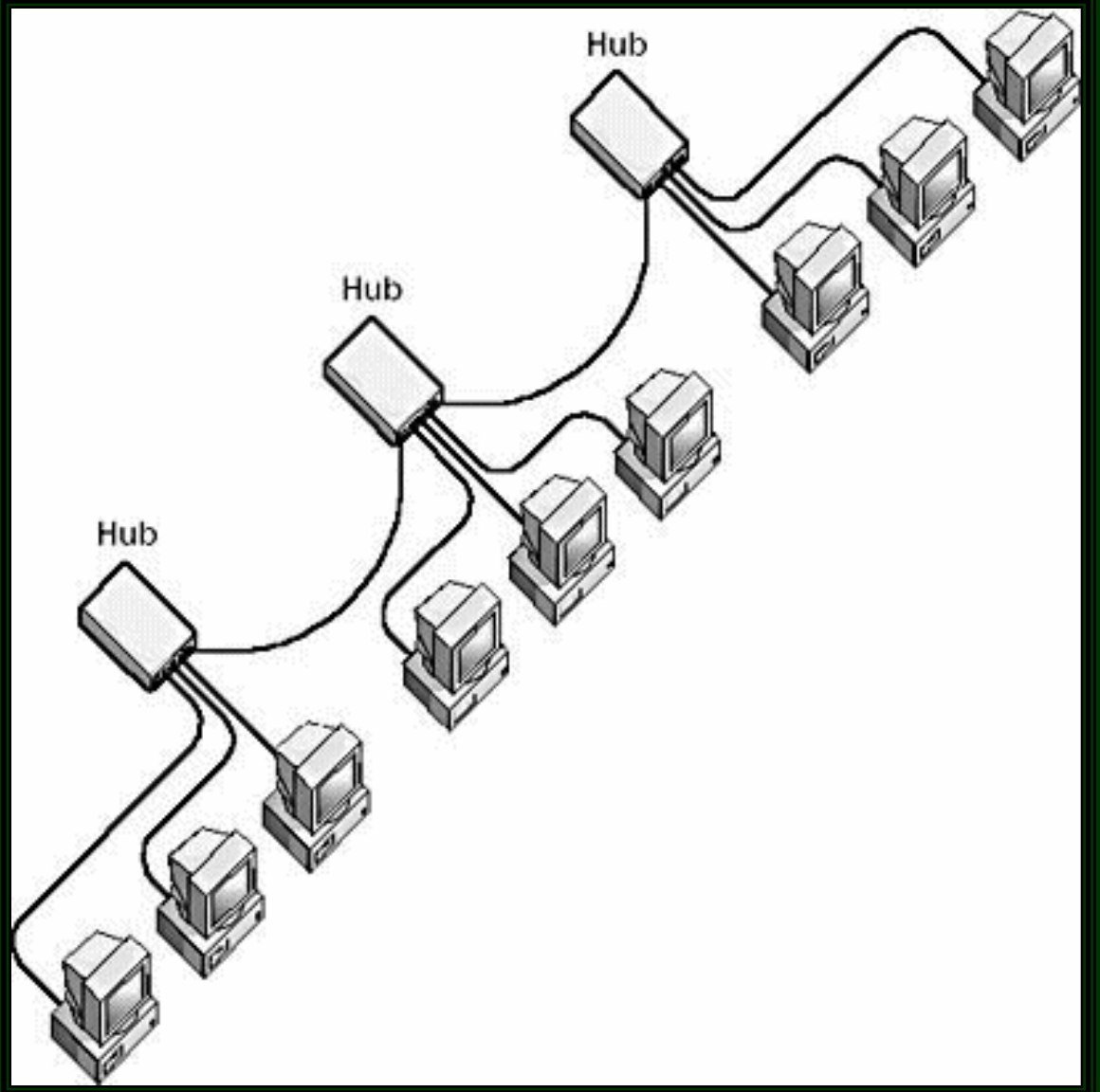
- Only one communication channel to service all the devices - traffic can get heavy and slow the network down
- Easy for sniffing since all traffic passes over a single channel
- Electric signals are weakened between connections of cables
- Not easy to troubleshoot - small malfunction will bring down entire network

Star Topology



STAR Topology

The star topology uses hubs through which all components are connected. In large networks, the hubs could be connected together, in the form of a *daisy chain.*



Star Topology - Advantages

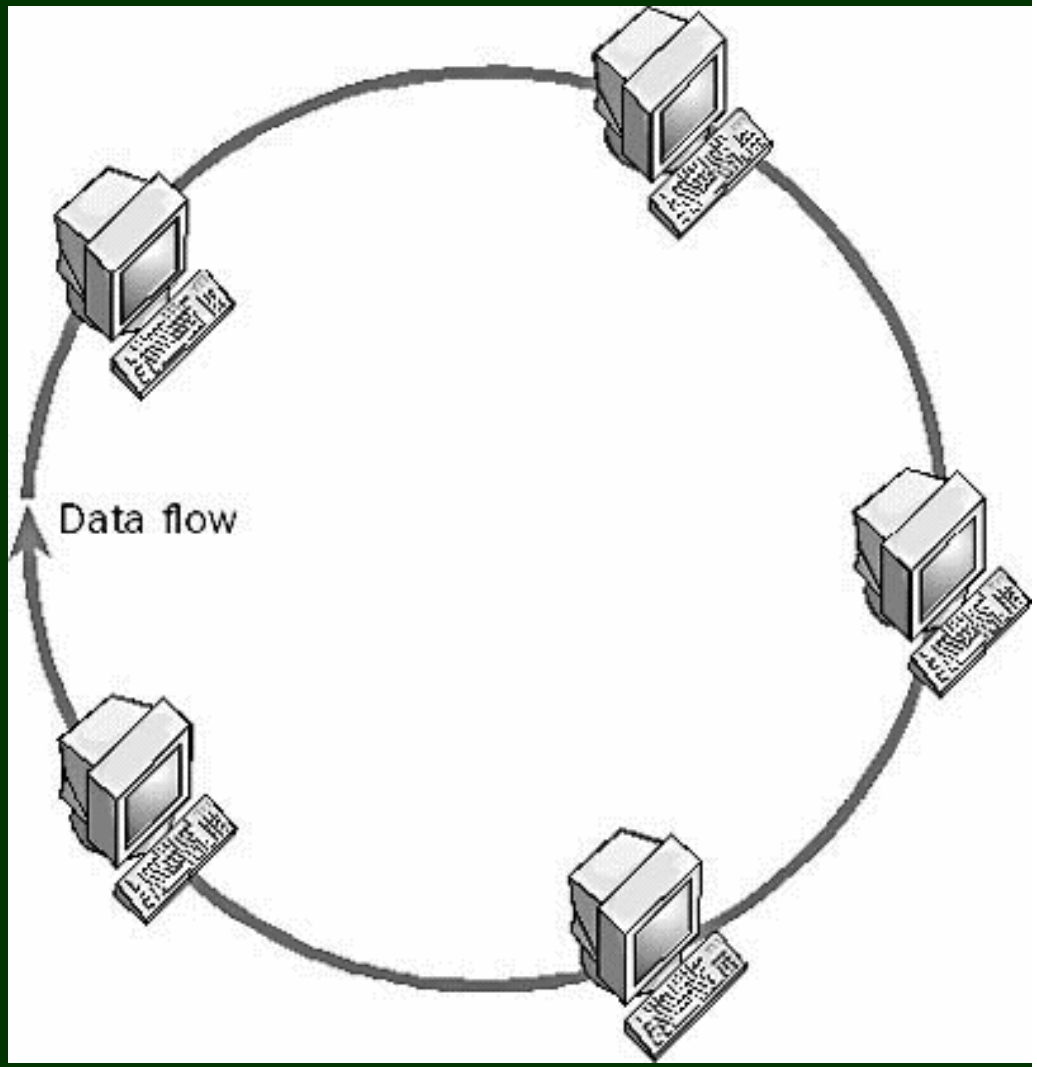
- Failure of one part or computer does not affect the entire network
- Easy to troubleshoot and to diagnose problems
- Different types of cable can be used in this configuration
- Easy to modify and add new computers
- Not easy to sniff for network traffic, since nodes are connected by separate lines to the hub.

Star Topology - Disadvantages

- Since hub is responsible for all functions, failure of the hub will cause network failure
- Extra equipment like hubs, switches required which can become expensive as the network size increases
- More cable required as compared to bus topology

Ring Topology

The ring topology connects workstations in a closed loop. Each terminal is connected to two other terminals (the next and the previous), with the last terminal being connected to the first.



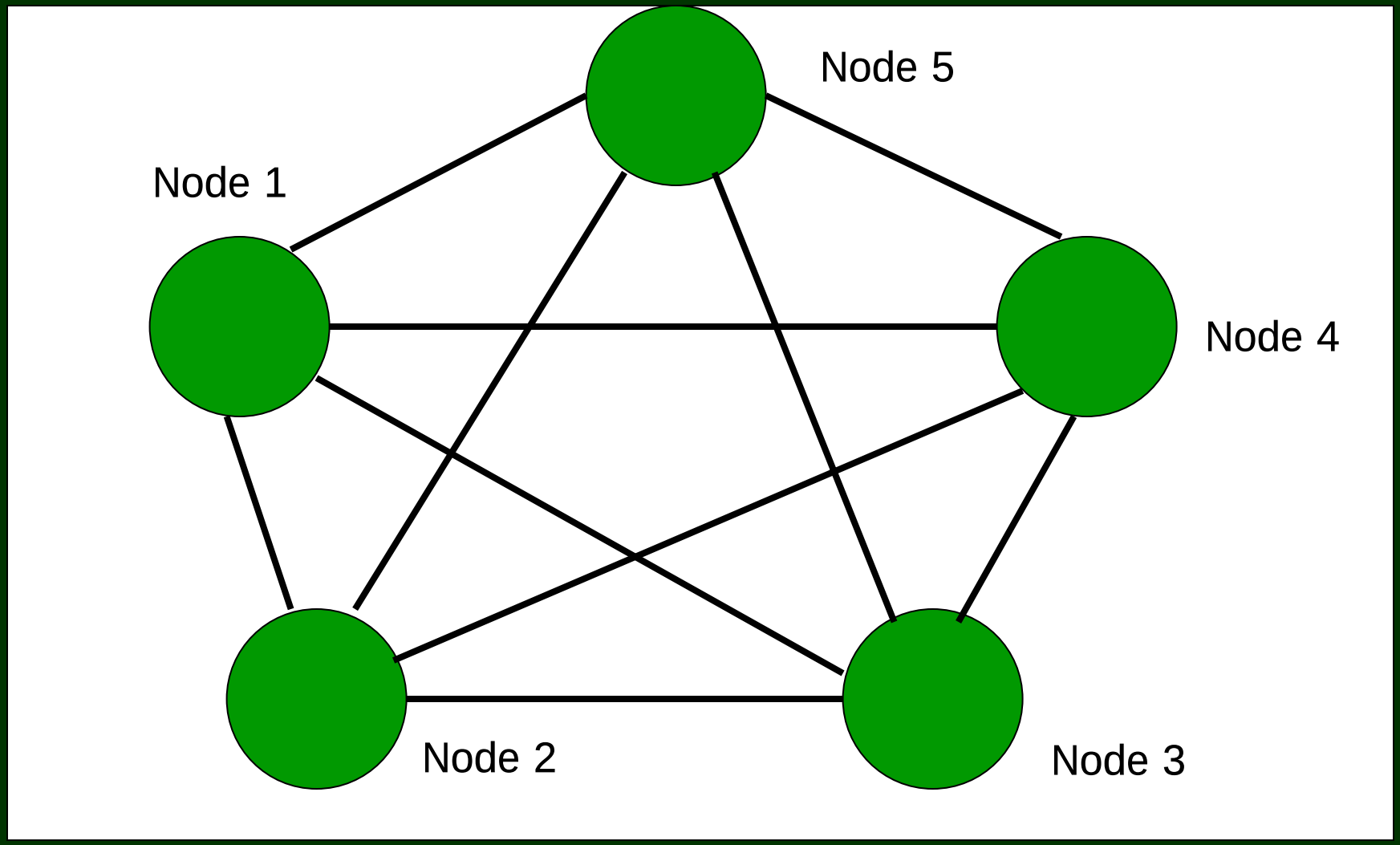
Ring Topology - Advantages

- All nodes are given equal access to network as a token is passed uni-directionally around the ring from node to node
- Each node has to wait for the token before it can transmit a message and hence no traffic jams
- Each node basically acts as a repeater and hence signal attenuation is minimum
- Network has the ability to degrade gracefully

Ring Topology - Disadvantages

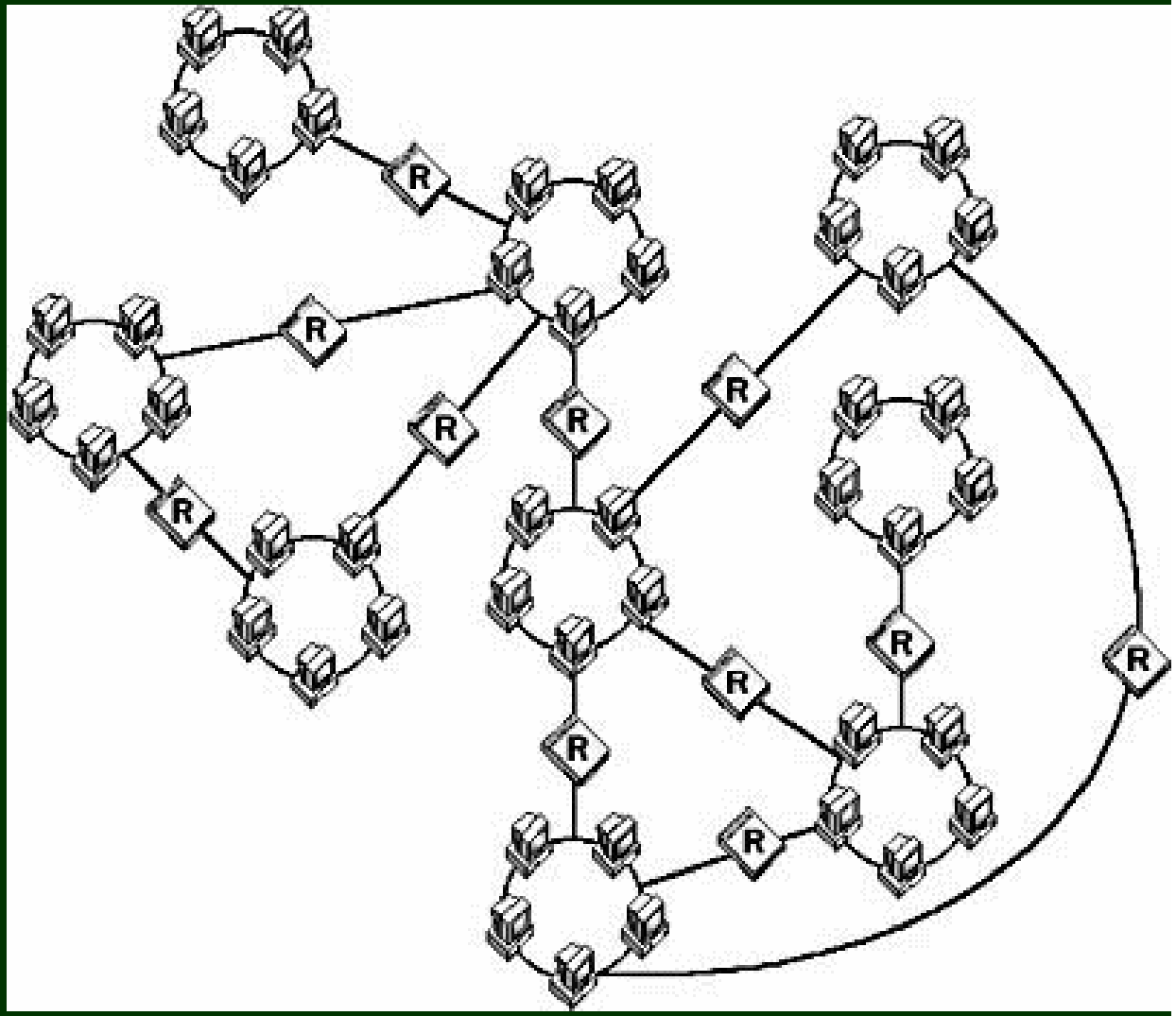
- Faults cannot be easily diagnosed
- Message delay increases as more computers are added to the network.
- Failure of any computer or node will disrupt the entire network
- Adding more computers or nodes will disrupt the network

Mesh Topology



Mesh Topology

The Mesh topology connects every node to other nodes in the network in multiple ways. Machines are directly and indirectly connected in mesh configuration.



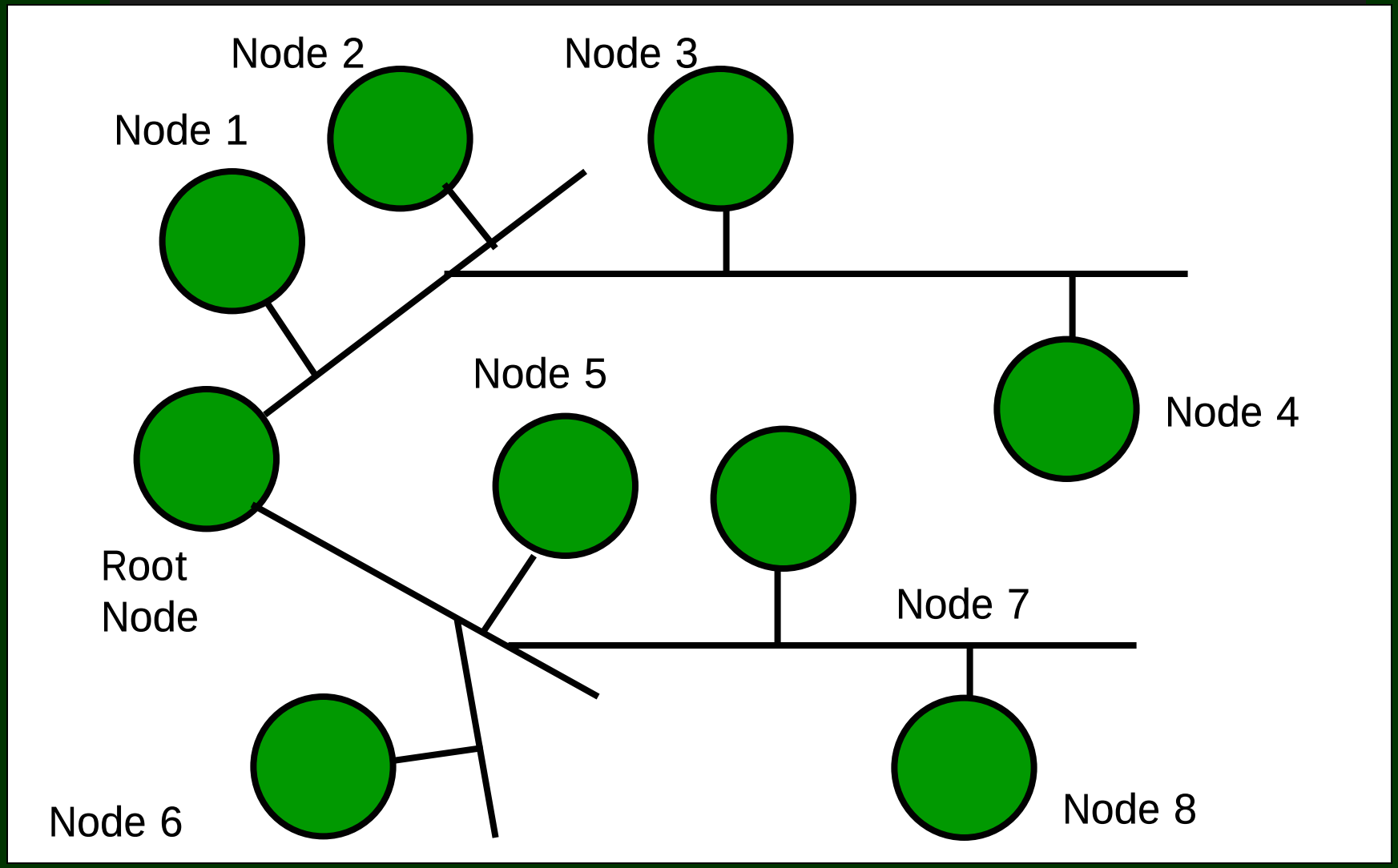
Mesh Topology - Advantages

- Lot of redundancy - minor faults will not disrupt the network.
- Reliable communication channel capacity
- Multiple paths give a high degree of fault-tolerance

Mesh Topology - Disadvantages

- Cabling costs are very high
- Expensive equipment for connecting the networks and computers is required
- Installation cost is high
- Maintenance cost is very high

Tree Topology



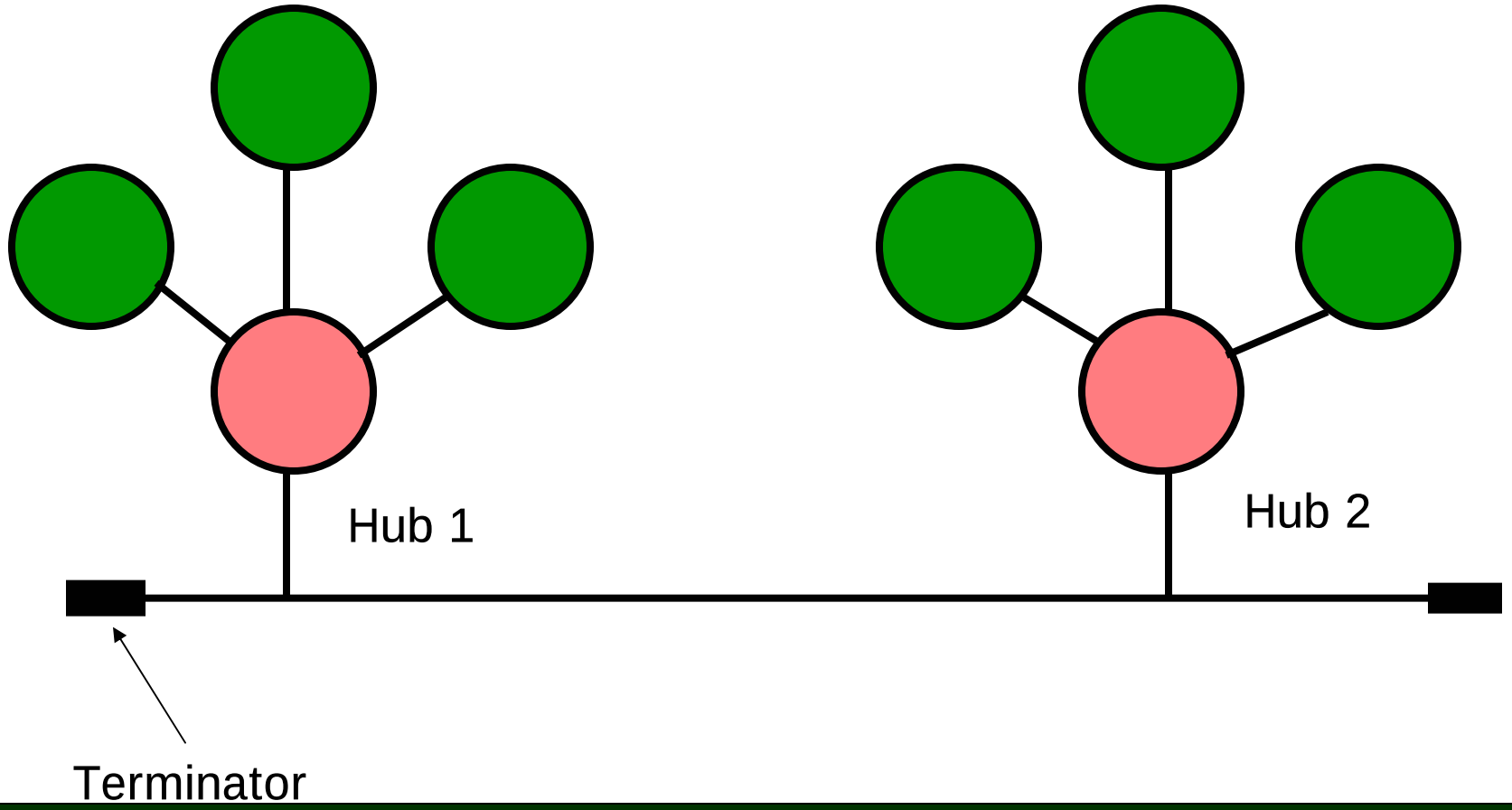
Tree Topology

- In a Tree topology, nodes in the network are connected to a branching communication line that has no closed loops.
- In this regard, a tree topology is simply a generalization of a bus topology.
- As with a bus, messages are transmitted along the transmission medium.
- It is difficult to propagate digital signals along the branching lines, hence tree topologies use analog signaling rather than digital signaling.

Hybrid Topology

- Various types of hybrid topologies exist which are a combination of the other topologies.
- For example, in a star-bus topology, hubs are connected via relatively short communication lines to a long bus.
- Star-bus networks have the control advantages-disadvantages of a bus and of star topology.

Hybrid Topology



Networking Standards

- International Standards Organization (ISO)
- Institute of Electrical and Electronic Engineers (IEEE)
- International Telecommunications Union (ITU)

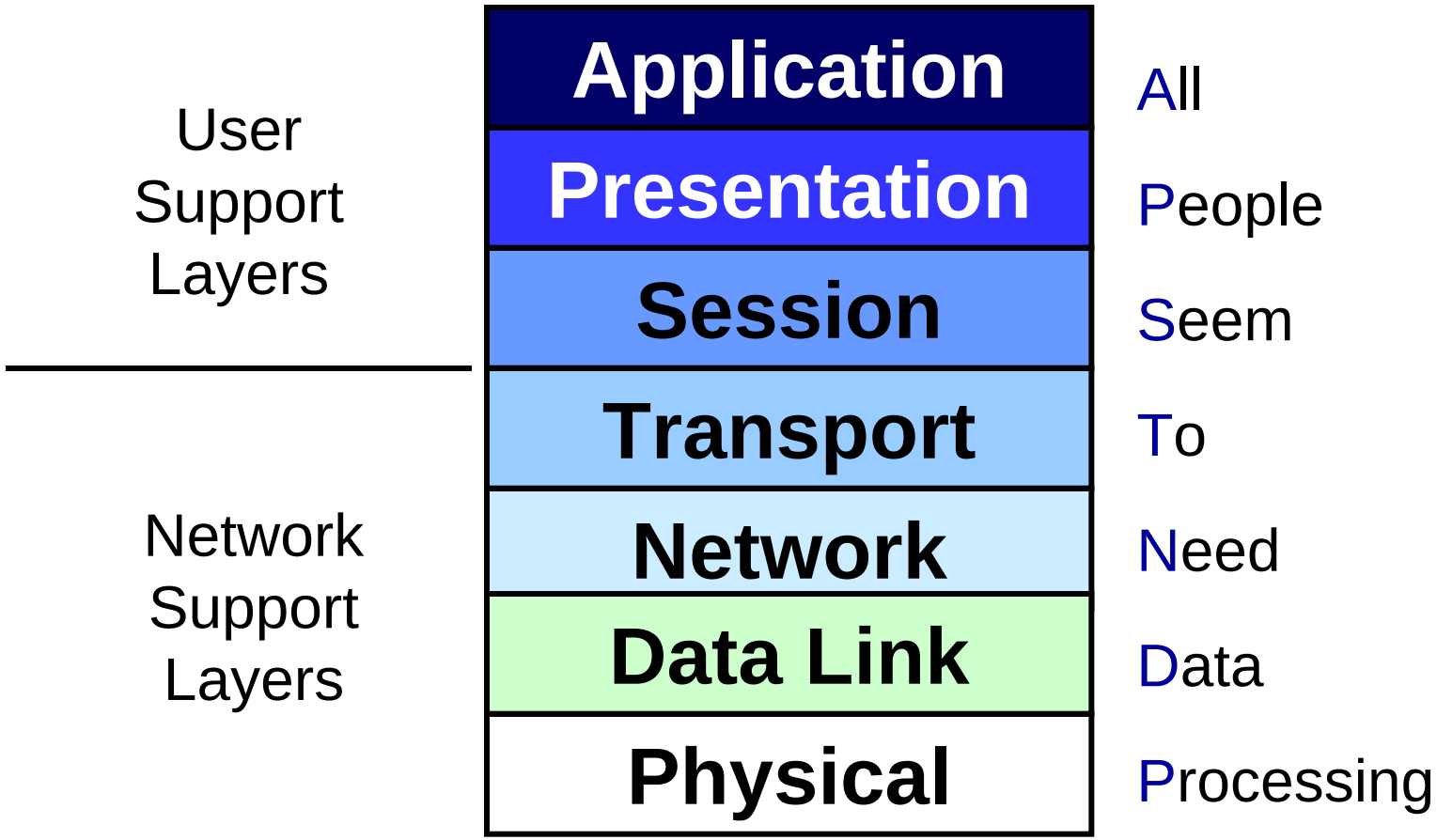
ISO developed the OSI - Open Systems Interconnect model in 1983

Open System Interconnect - OSI

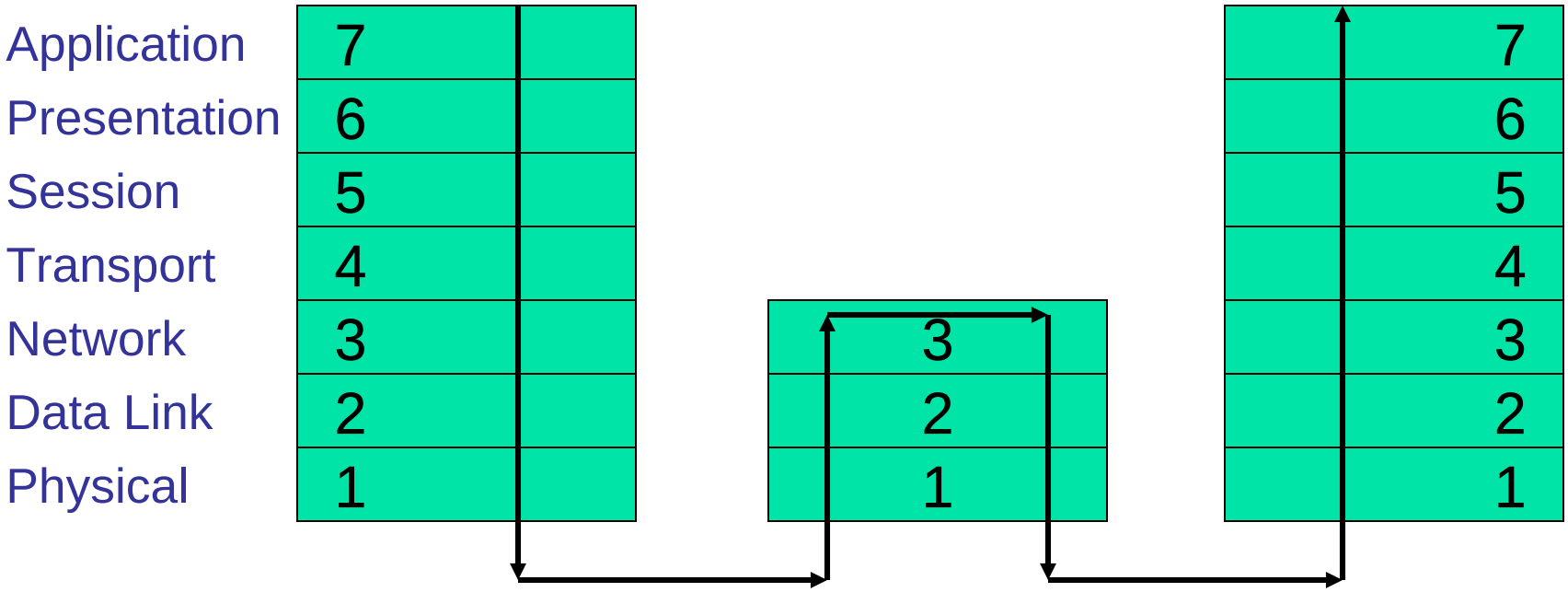
These seven layers are based on the following principles:

- Every layer should perform a specified function
- Information flow across layers should be minimized
- The functions of each layer are decided based on standards

OSI Model


User
Support
Layers
Network
Support
Layers
Application
Presentation
Session
Transport
Network
Data Link
Physical
All
People
Seem
To
Need
Data
Processing

OSI Model


Application
Presentation
Session
Transport
Network
Data Link
Physical
7
6
5
4
3
2
1
3
2
1
7
6
5
4
3
2
1

7 - Application Layer

It allows users to access the network. It facilitates user interface and support for services as

- Directory Services
- File transfer, access and management
- Mail Services
- Network virtual terminal

6 - Presentation Layer

It deals with the syntax and semantics of the information that is exchanged between systems. The functions provided are

- Changing data formats
- Data Compression
- Data Encryption

5 - Session Layer

It allows users on different machines to establish, maintain and drop sessions. It also performs the functions of:

- Manage dialog control
- Synchronize activities
- Insert checkpoints at appropriate places

4 - Transport Layer

The main function is to ensure data transfer between end points. It also performs the following functions:

- Connection control
- Error Control
- Flow control and handling of congestion
- Service point addressing
- Segmentation and reassembling

3 - Network Layer

It deals with controlling the operations of the network. It performs the functions of

- Logical addressing
- Routing

2 - Data Link Layer

Its main task is to take raw data and transform it into error free data for the network layer. It performs the functions of

- Access control
- Error control
- Flow control
- Framing
- Physical Addressing

1 - Physical Layer

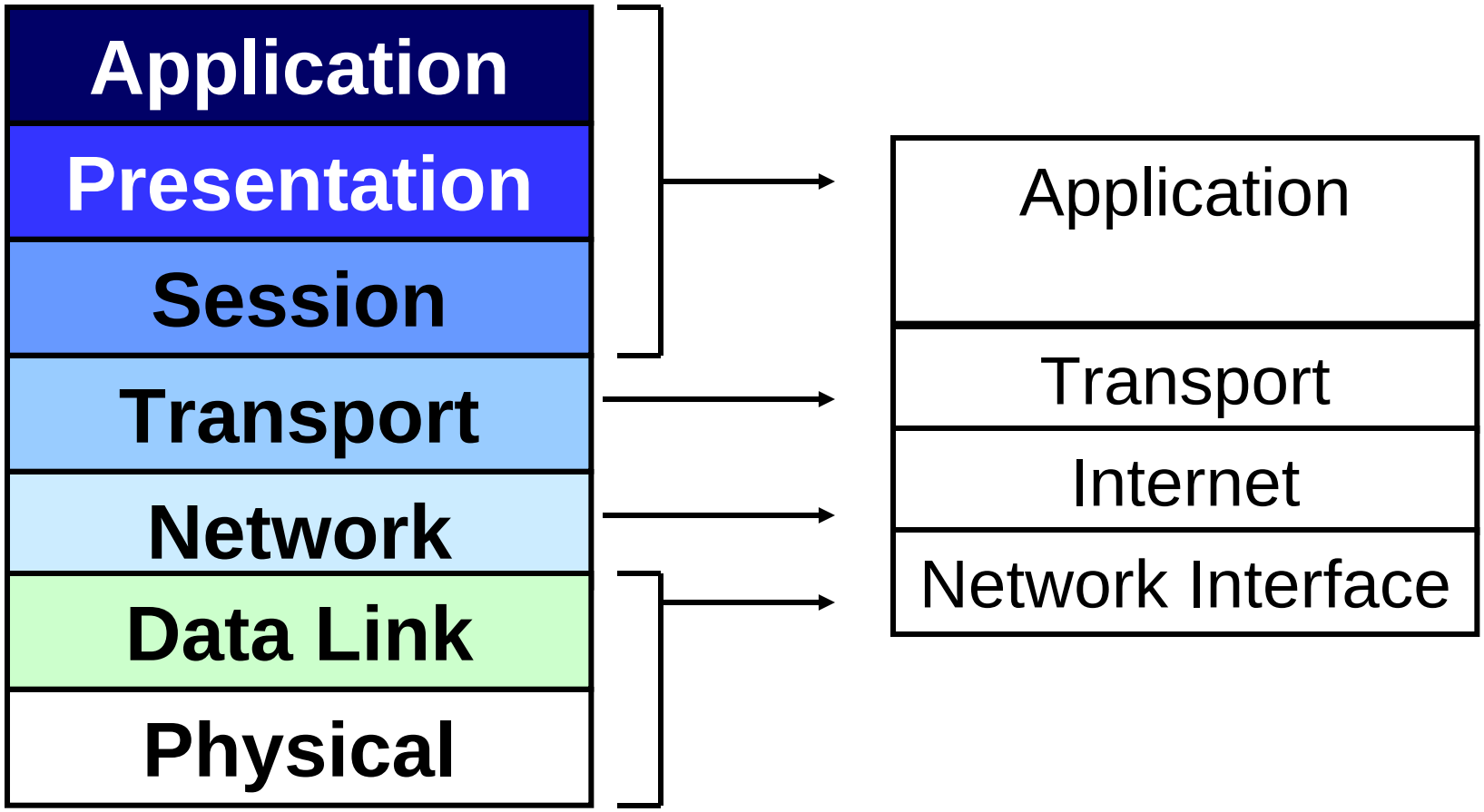
It is mainly concerned with transmitting raw data bits over a communication channel. It performs:

- Line configuration
- Physical topology
- Representation of the bits
- Synchronization of the bits
- Transfer rate
- Transmission mode

Networking Protocols

- Network protocols are standards or rules that allow computers to communicate.
- A protocol defines how computers identify one another on a network, the form that the data should take in transit, and how this information is processed once it reaches its final destination.
- Protocols also define procedures for handling lost or damaged transmissions or "packets."

TCP/IP layer mapping to OSI



Networking Devices

Following are the main types of Networking Devices

- Repeaters
- Hubs
- Bridges
- Switches
- Routers
- Gateways

Repeater

- It operates at the Physical Layer
- A network device used to regenerate or replicate a signal.
- Used to regenerate analog or digital signals distorted by transmission loss.
- Analog repeaters can only amplify the signal while digital repeaters can reconstruct a signal to near its original quality.

Rs. 500 - 1,000

Hub

- A common connection point for devices in a network.
- Used to connect segments of a LAN.
- Hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
- A Passive Hub serves as a conduit for the data, enabling it to go from one device (or segment) to another.
- An Active Hub has features that enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub. Also called manageable hubs.

Rs. 1,000 - 3,000

Bridge

- It operates at the Physical and Data Link Layers
- A device that connects two similar local-area networks (LANs), or two segments of the same LAN. (e.g. one token ring network to another token ring network.)
- Have storage capacity to store frames and act as a storage and forward device
- Bridges are protocol -independent. They simply forward packets without analyzing and re-routing messages.

Rs. 2,000 - 10,000

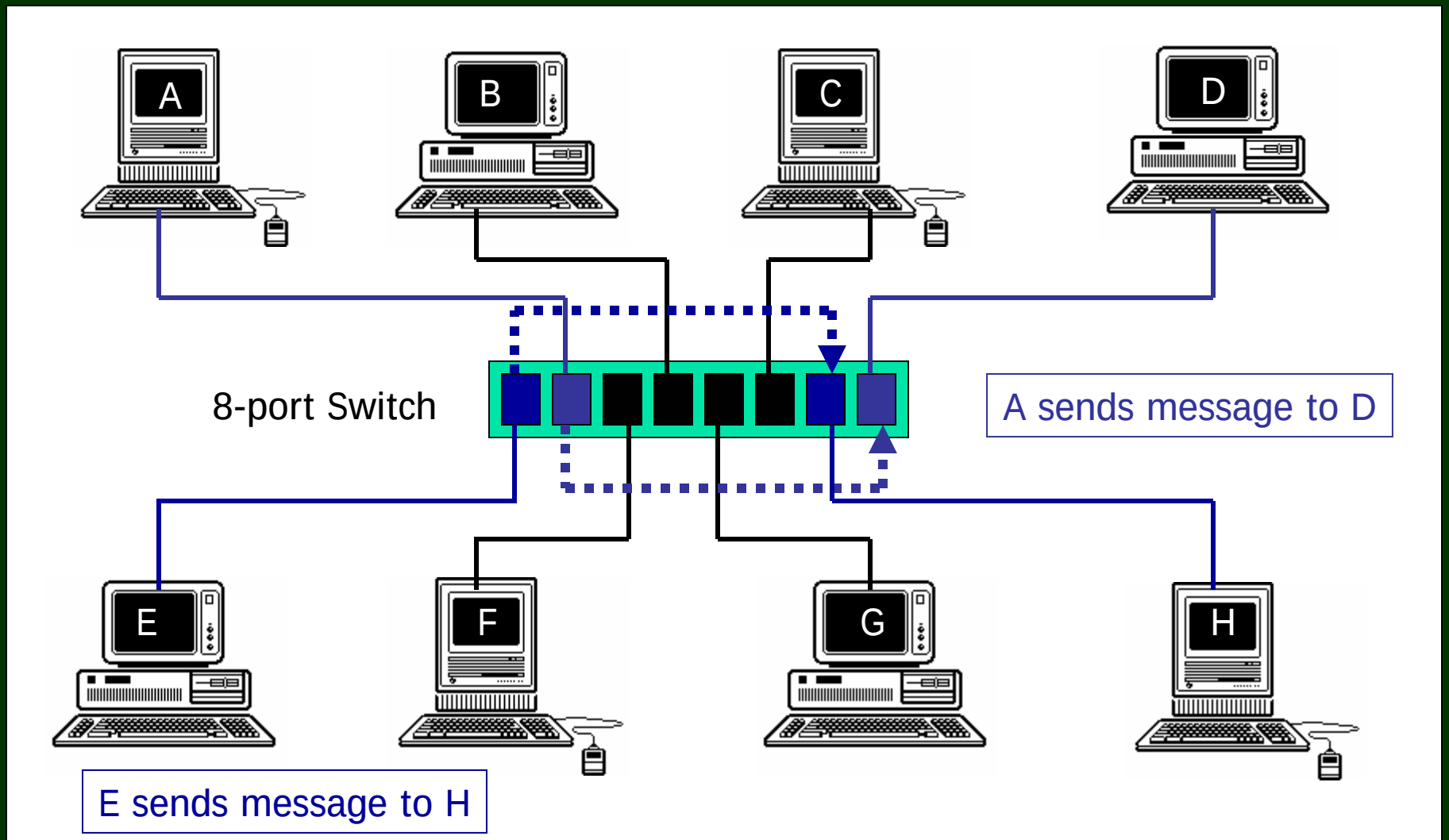
Switch

- It operates at the Physical and Data Link Layers
- Nowadays bridges have been replaced by switches, which provide a method for building bridges.
- The main difference between switches and bridges are in the number of ports (switches can have a large number of them), in the internal speed (switches work at very high speeds), and in presentation (switches may have different speed ports)

Rs. 1500 - 20,000

Switch

Switch


A
B
C
D
8-port Switch
A sends message to D
E
F
G
H
E sends message to H

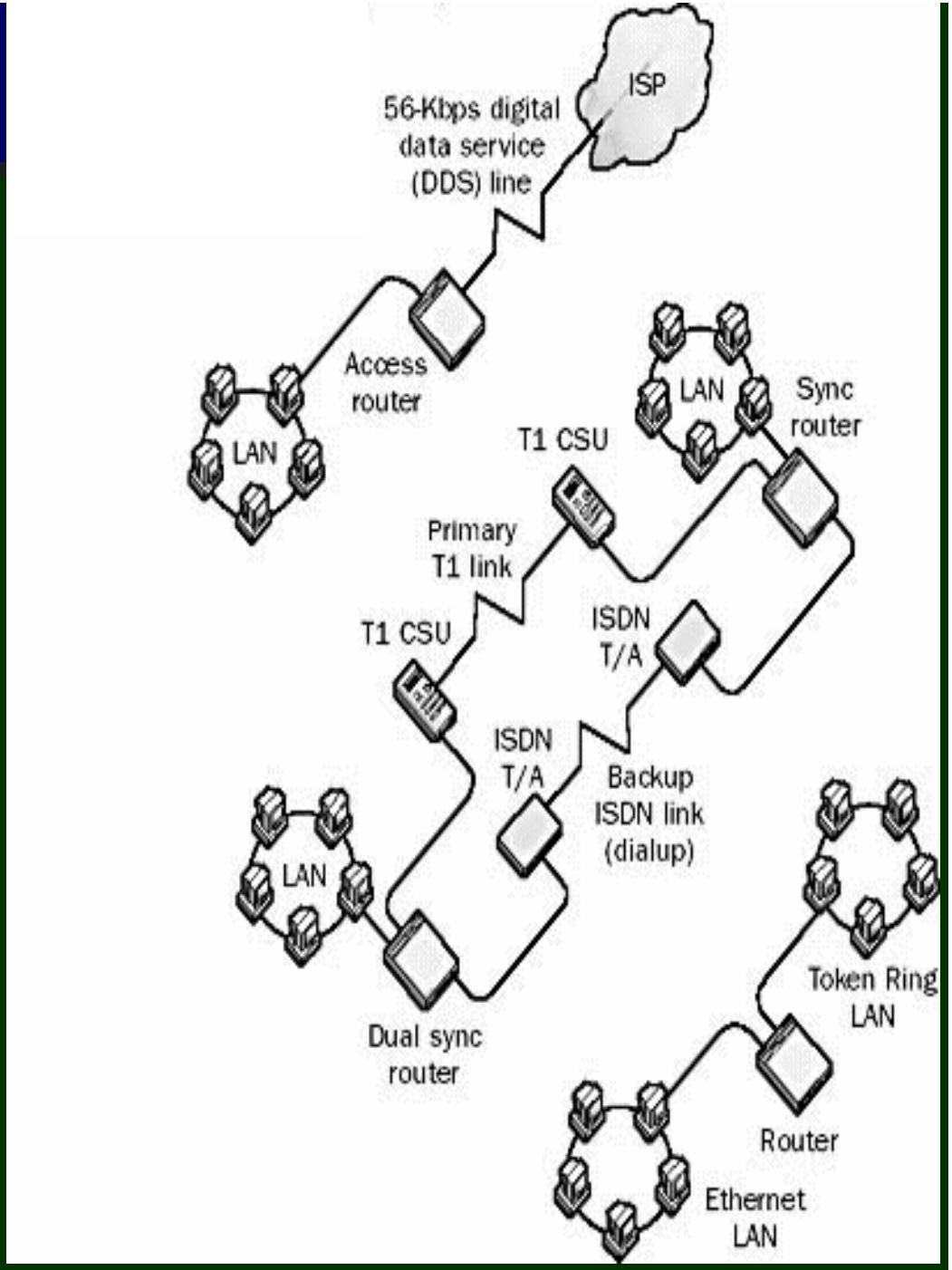
Router

- It operates at the Physical, Data Link and Network Layers
- A router performs all the functions of a bridge. In addition it can connect hetrogeneous local area networks (e.g. a bus network to a token ring network) and direct network traffic over the fastest channel between two nodes that reside on different subnetworks.
- Different networks could be LAN or WAN

Rs. 5000 – 1,50,000

Router

A Router can be utilized for many purposes.



Gateway

- Very sophisticated equipment incorporating hardware and software implementation.
- It operates at all layers of the OSI model
- Primary function of a gateway is to perform protocol conversion to allow different types of communication architectures to communicate with one another.
- Works with different protocols.

Rs. 2,00,000 - 10,00,000

Control functions

- Bridges, routers, and gateways perform several useful control functions.
- First, they allow the total network to be broken up into several smaller networks, and hence improve the overall reliability of the network.
- Failure at a node or communication line within a sub-network, for example, will not disable all the nodes of the network.
- Second, for security reasons, it might be desirable to keep different types of applications on different sub-networks.

Control functions

- Electronic Fund Transfer messages, for example, can traverse over high-security sub-network while low-exposure administrative messages can traverse over a relatively low-security sub-network. Bridges, routers, and gateways might allow the users of an internet to specify they wish their messages to traverse.
- Third, bridges, routers, and gateways may provide access control mechanisms to restrict access to sub-networks only to authorized users. Not all users in a local area network, for example, may be allowed to access the other sub-networks in the network.

Types of Networks

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- Base Band Network
- Broad Band Network
- Virtual Private Network (VPN)

Local Area Network (LAN)

- Usually within a office or a building
- Privately owned
- Uses Bus, Ring, or Star topology
- Can use copper or fiber optic cabling

Metropolitan Area Network (MAN)

- Usually over a city-wide or metropolitan area
- May be privately owned or owned and operated by a Service Provider
- Data flow can be Simplex, Half-Duplex, or Full-Duplex
- Usually uses radio links or fiber optic cabling

Wide Area Network (WAN)

- Usually over a geographically distributed area
- Owned and operated by a Service Provider
- Data flow can be Simplex, Half-Duplex, or Full-Duplex
- Uses satellites, or radio links or fiber optic cabling

Base Band Network

- The entire bandwidth of the transmission medium is used by a single digital signal
- Computers in a base band can transmit only when the channel is not busy
- Transmission is bidirectional over short distances, and repeaters must be used to increase the length of the network.
- A baseband bus is susceptible to wiretapping because only a single signal is traversing over the bus.
- Speeds of 50 Kbps to 100 Mbps

Broad Band Network

- A broadband bus uses analog signaling. Transmission is unidirectional because the amplifiers used in broadband bus networks are unidirectional devices.
- Broad Band technology supports a wide range of frequencies, typically from audio up to video frequencies
- It allows multiple high-speed signals to share a bandwidth of a single cable via frequency division multiplexing
- Can cover longer distances because analog signals are less susceptible to attenuation, distortion, etc.
- Less susceptible to wiretapping, since multiple signals are traversing the bus.
- Speeds of up to 20 Mbps are possible

Virtual Private Network (VPN)

- A VPN is used to connect the components and resources of one network to another network.
- It is a virtual network rather than a physical network
- It is typically carried out over the Internet
- VPN technology should maintain secure transmission and communication

Communication Media

- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)
- Coaxial Cables
- Optic Fiber
- Radio waves
- Microwave
- Satellite communication
- Cellular telephony

Cabling Issues

- It is the skeleton of the Network Infrastructure
- Needs to be properly planned
- Choice of cable decides future growth options
- Reliability & future-proofing are key concerns

Cabling Problems

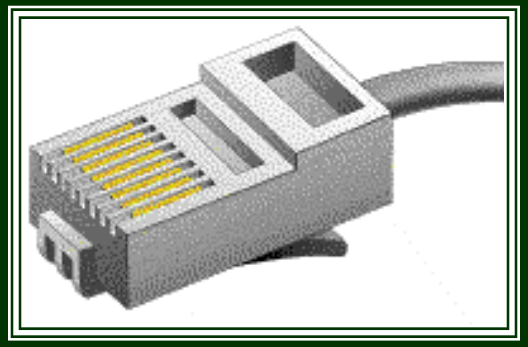
- Accounts for 70% of network failures
- Cabling should not be application specific or need based
- High cost of moves, adds and changes
- Structured cabling for modularity, flexibility and future-proofing
- Avoid noodles in the telecom closet

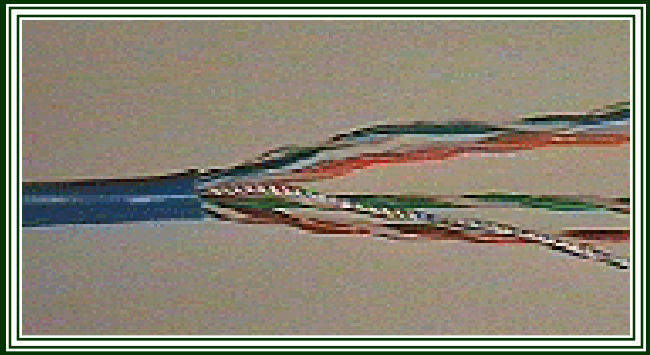
Network Cabling - Enemies

- Noise
- Cross talk
- Environment
- Rodents
- Bandwidth hungry applications / downloads
- Aging

Unshielded Twisted Pair (UTP)

- Most commonly used, suitable for data and voice
- Two conductors of copper surrounded by insulating material
- Most commonly used is the 8-pair cable with RJ45 connector
- Maximum 100 meters distance from node to hub





Shielded Twisted Pair (STP)

- Has a metal foil or shielding which eliminates cross-talk.
- Commonly used where interference is high
- Suitable for data and voice
- Two conductors of copper surrounded by insulating material
- Most commonly used is the 8-pair cable with RJ45 connector

UTP / STP

Advantages

- Cheap
- Simple to install
- Readily available
- Simple to modify

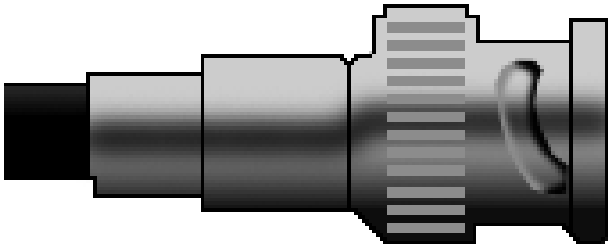
UTP / STP

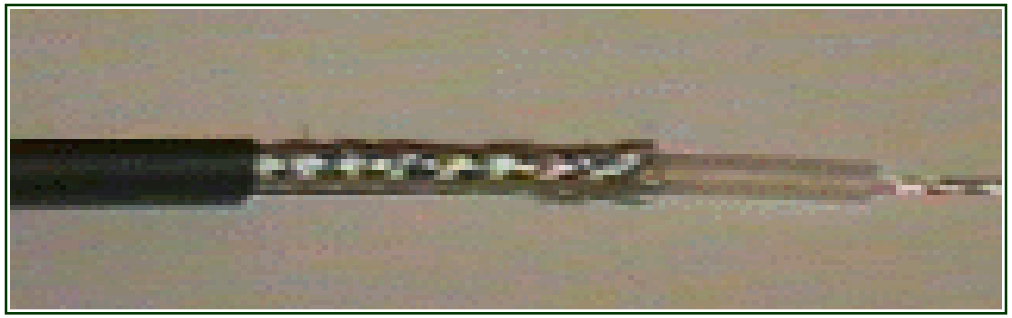
Disadvantages

- Easy to tap
- Easy to splice
- Simple to modify
- Prone to cross talk
- Electro Magnetic Interference (UTP)
- Noise

Coaxial Cables

- Cable with central core and outer shield
- High bandwidth possible
- High immunity to noise
- BNC connectors
- Longer distances possible





Coaxial Cables

Advantages

- Ease of installation
- Straightforward
- Readily available

Coaxial Cables

Disadvantages

- Thick
- Expensive
- Does not support many LANs
- Distance sensitive
- Difficult to modify

Optical Fiber

Advantages

- High speeds of transmission
- Low attenuation and degradation
- Immunity to EMI (Electromagnetic Interference)
- Security from sniffing - cannot be tapped
- Support to longer distances without repeaters
- Fiber has great potential as the raw material since silica is available in abundance

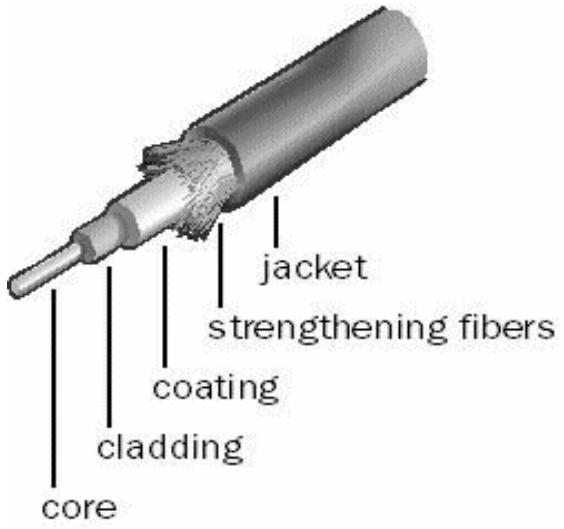
Optical Fiber

Disadvantages

- Expensive

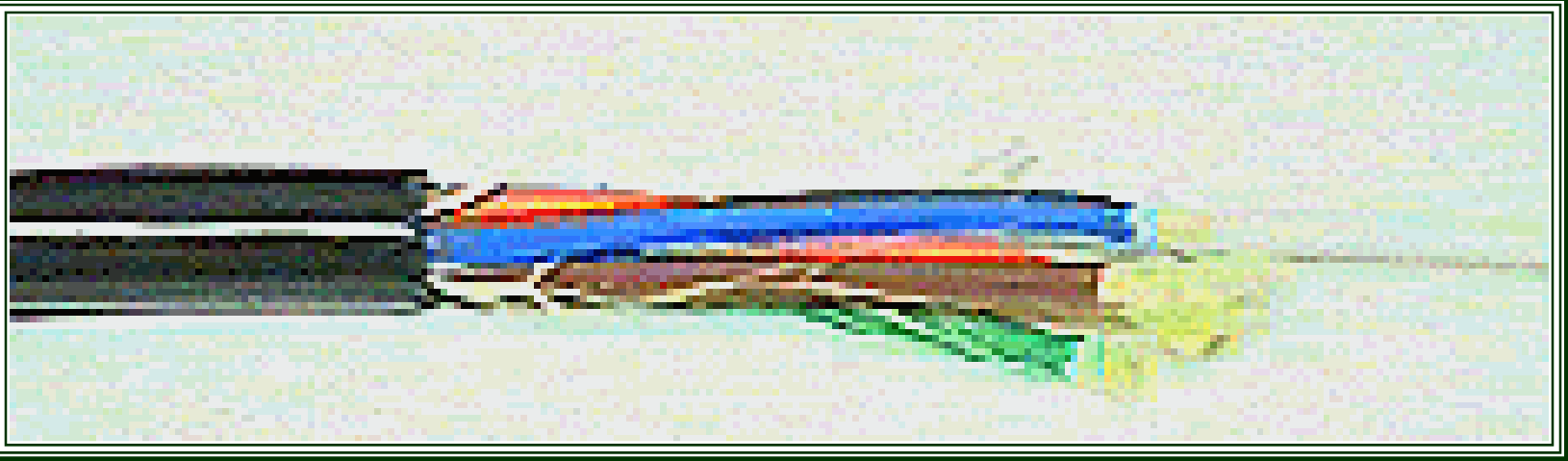
Fiber Cable - components

- Core, Cladding and Protective Sheath
- Core and Cladding are made of glass
- Core has higher index of refraction than cladding
- Core is in the center
- Cladding surrounds the core
- Sheath encapsulates the Cladding



Fiber Networks - Components

- Fiber cable
- Connectors
- Light sources (inside ACTIVE devices)



Light Sources for Fibers

- Monochromatic light source
- High intensity output
- Should be easily modulated
- Devices should be compact and easily coupled
- LED, Laser diodes, Gas ionization lamps
- LED: upto 300 MBPS
- LASERS: even 10 GBPS

Fiber Vs. Copper

Fiber	Copper
10 GBPS, 200 KM	1 GBPS, 2.5 KM
No Interference	High Interference
High Cost	Low Cost
Low Maintenance	High Maintenance

Trends

- Fiber will rule as the backbone for Telecom
- Copper will have tough competition from Wireless WAN for last Mile connectivity
- However, Copper will continue to be the preferred desk-top connectivity medium

Radio Waves

Three types of RF propagation are used:

- Ground wave - follows the curvature of the earth
- Ionospheric - The transmitter beams the signal towards the ionosphere which reflects it back to the receiver station. Factors such as change in weather, time of day, affect the transmission.
- Line of sight - The transmitter and receiver must face each other, i.e. should be visible to each other.

Radio Waves

- Used for short distances
- Cheap
- Easy to tap
- Interference
- Noise

Microwave Systems

- Line of sight carrier for voice and data signals
- Cheap
- Simple to install
- Easily available
- Easy to tap
- Affected by atmospheric conditions and objects
- Noise

Satellite Systems

- Uses several receiver/amplifier/transmitter sections called transponders to send information
- Each transponder operates at a slightly different frequency
- Affected by atmospheric conditions
- Noise

Cellular Systems

- Modern day communications use cellular telephones to a large extent. Here the cellular phones are used for communications.
- Computer systems are connected to the handset and from the handset the connection goes to the Mobile Telephone Switching Office (MTSO) and through the cellular towers placed at strategic locations connections are established.

Media Comparison

Medium	Cost	Speed	Attenuation	EMI	Security
UTP	Lowest	Moderate	High	High	Low
STP	Low	Moderate	High	Moderate	Low
Coaxial	Moderate	High	Moderate	Moderate	Low
Optical Fiber	High	High	Low	Low	High
Radio	High	Moderate	Variable	High	Low
Microwave	High	Very High	Variable	High	Moderate
Satellite	High	Very High	Variable	High	Moderate
Cellular	High	Very Low	Low	Moderate	Low

Signal Degradation

The following can degrade a signal during transmission

- Attenuation
- Delay Distortion
- Noise

Attenuation

- As a signal progresses along a transmission medium, its amplitude or strength decreases.
- This is particularly true when the medium is copper wire.
- Amplifiers, also known as repeaters, can be used to counteract this effect.

Delay Distortion

- The rate of propagation of a signal along a transmission line varies with the frequency of the signal.
- Hence, when transmitting a digital signal with varying frequency components, the various components arrive at the receiver with varying delays.
- This delay distortion increases with the rate of transmission and can result in misinterpretation of the signal.

Noise

- In the absence of a signal, a transmission line should ideally have zero electrical signal present.
- However there is generally a small amount of electrical fluctuation even in the absence of a signal. This is called noise.
- When the power of the noise is high, it can interfere with the interpretation of the signal by the receiver.

Network Interface Cards - (NICs)

- NICs are adapter cards which are installed into the computer.
- NICs can be specific for a particular type of cable or can be a combo card with multiple connection slots.
- Network cards are available for different speeds from 10 - 100 Mbps.

USB Adapter

- The Universal Serial Bus (USB) port connects to the network without having to install a separate network interface card inside a computer by using a USB adapter.

Error Detection

Commonly used error detection methods are :

- Parity Checking
- Hamming Code
- Cyclic Redundancy Check
- Loop Check

Parity Checking

Parity Checking involves adding an extra bit to a string of bits.

Each horizontal parity bit is used to check whether a character in the block has been corrupted.

0	1	0	0	1	0	0	1	0
0	1	0	1	0	0	1	1	1
0	1	0	0	0	0	0	1	1
0	1	0	1	0	1	0	1	1
0	1	0	0	0	1	0	0	1
0	1	0	0	1	0	0	1	0
0	1	0	1	0	1	0	0	0
0	1	0	0	1	0	0	1	0
0	1	0	0	1	1	1	0	1
0	1	0	0	0	1	1	1	1
1	1	1	0	1	0	0	0	1

But if a burst of noise on the line causes two bits within the same character to flip from, say, 0 to 1, a vertical parity bit check will detect the error.

Used for asynchronous transmission, that is, where data is transmitted one character at a time.

Block Sum Checking

Block Sum Checking is an extension of the parity check in that an additional set of parity bits is completed for a block of characters. The set of parity bits is known as the block sum check character.

Hamming Code

Hamming Code is used for single bit error detection and correction.

- In this method, along with the data bits, a selective set of parity bits is computed and transmitted.
- The number of parity bits used for transmission is estimated by the formula:

$$2^p = m + p + 1$$

where p = number of parity bits

m = number of data bits

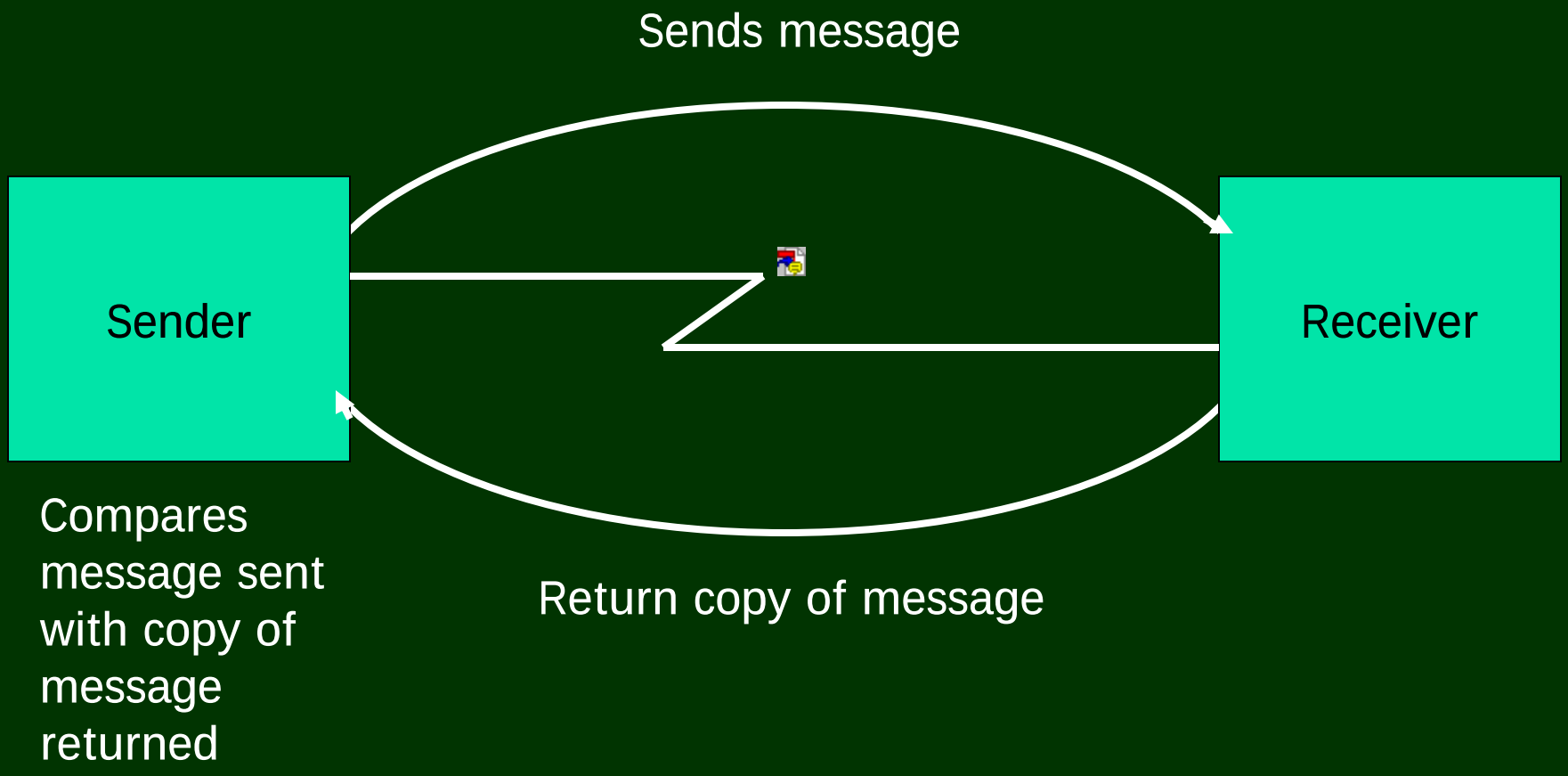
Cyclic Redundancy Checks

- With Cyclic Redundancy Checks (CRCs), the block of data to be transmitted is treated as a binary number. This number is then divided by a prime binary number.
- The remainder is attached to the block to be transmitted.
- The receiver recalculates the remainder to check whether any data in the block has been corrupted.
- CRCs tend to be used with synchronous transmission, that is, where data is transmitted as a continuous stream of bits.

Cyclic Redundancy Checks

- The sender workstation generates the CRC and transmits it with the data at the same time.
- The receiving workstation computes a CRC and compares it with the sender workstation. If both of them are equal then the block is assumed error free.
- CRCs are considered to be very effective in detecting bursts of errors during transmission.

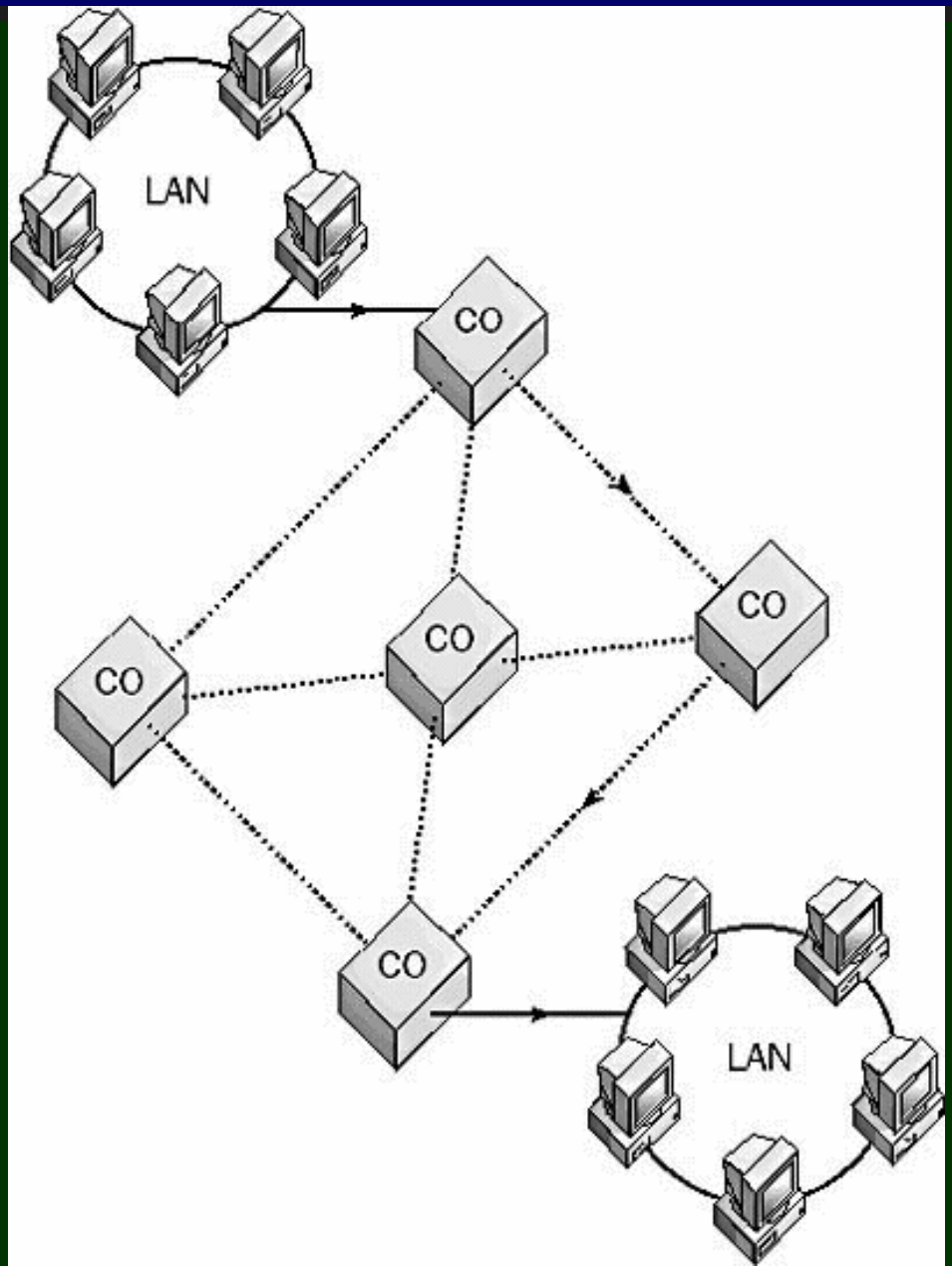
Loop Checks

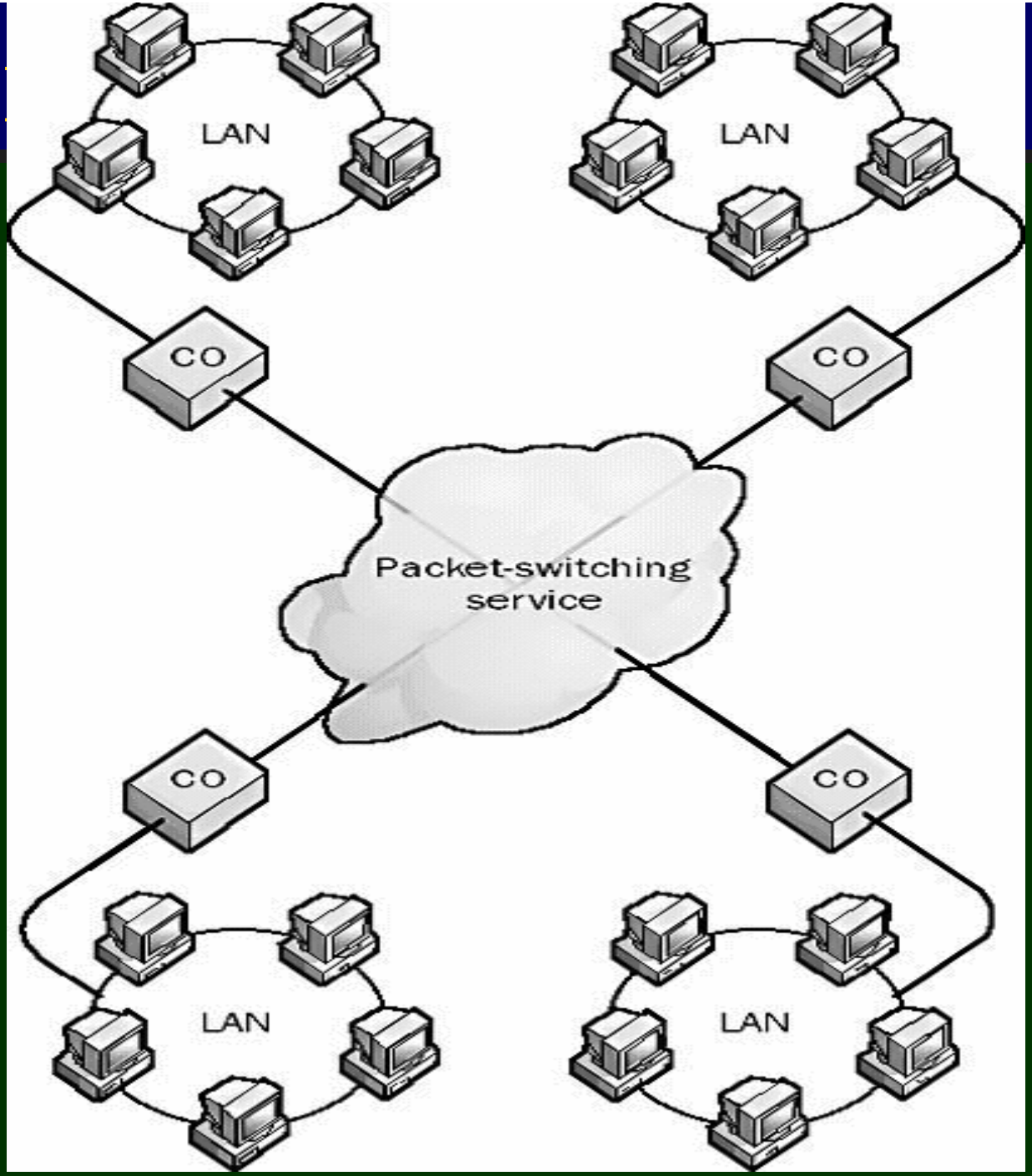

Sends message
Sender
Receiver
Compares message sent with copy of message returned
Return copy of message

Loop Checks

- A loop check involves the receiver of a message sending back the message received to the sender.
- The sender checks the correctness of the message by comparing it to a stored copy of the message sent.
- If a difference exists, the message is re-transmitted with suitable line protocol data to indicate that the previous message received was in error.
- A loop check is normally used on short length full-duplex lines, where the return path can be used for error detection purposes.

Circuit-switched services




LAN
LAN
CO
CO
Packet-switching service
CO
CO
LAN
LAN

OM

Thank You

prashant.mali@cyberlawconsulting.com