Computer Network
Chapter 1

Prepared By:

Patanjali

Lecturer in ECE

Govt. Polytechnic Jhajjar

Networking

- **Computer network** A collection of computing devices that are connected in various ways in order to communicate and share resources

  Usually, the connections between computers in a network are made using physical wires or cables

  - However, some connections are **wireless**, using radio waves or infrared signals

Networking

- The generic term **node** or **host** refers to any device on a network
- **Data transfer rate** The speed with which data is moved from one place on a network to another
- Data transfer rate is a key issue in computer networks

Networking

- Computer networks have opened up an entire frontier in the world of computing called the **client/server model**

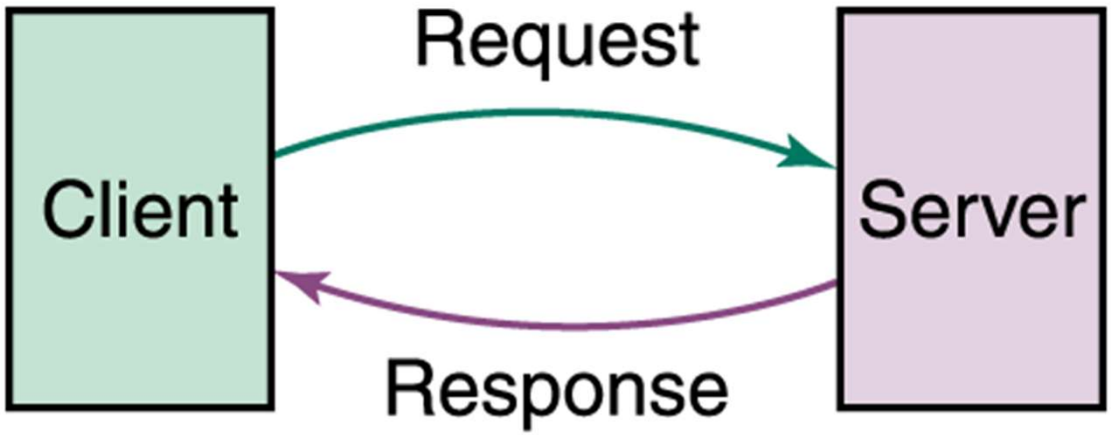


Figure 15.1 **Client/Server interaction**

Networking

- **File server** A computer that stores and manages files for multiple users on a network
- **Web server** A computer dedicated to responding to requests (from the browser client) for web pages

Peer-to-Peer Architecture

Peer-to-peer architecture (P2P architecture) is a commonly used computer networking architecture in which each workstation, or node, has the same capabilities and responsibilities. It is often compared and contrasted to the classic client/server architecture, in which some computers are dedicated to serving others.

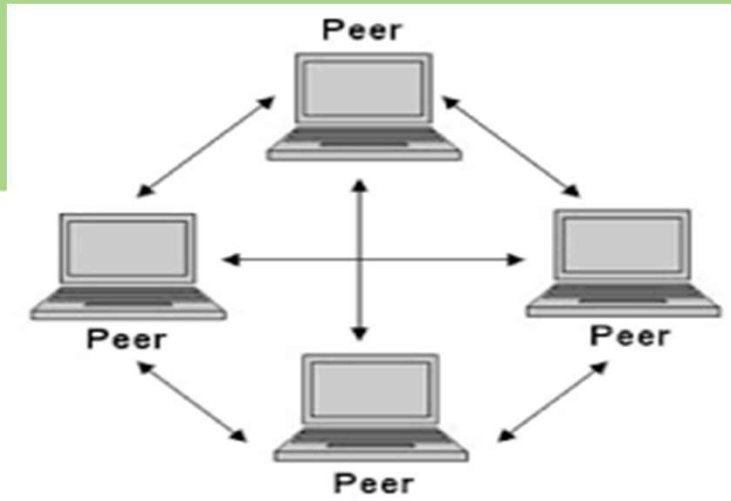
P2P may also be used to refer to a single software program designed so that each instance of the program may act as both client and server, with the same responsibilities and status.

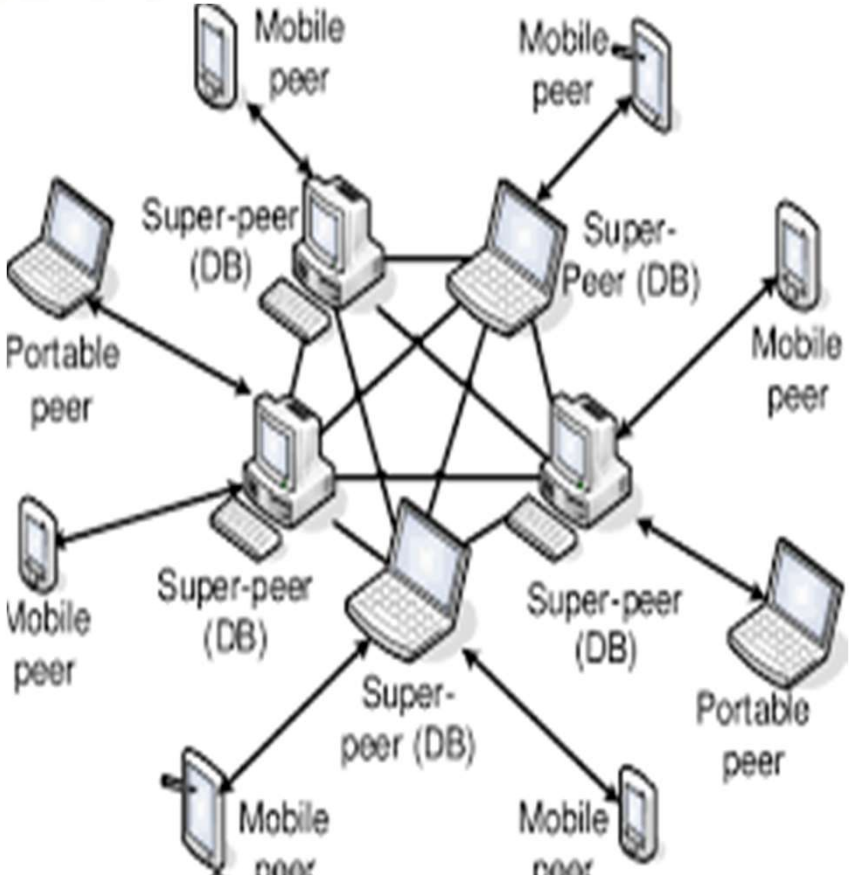
P2P networks have many applications, but the most common is for content distribution. This includes software publication and distribution, content delivery networks, streaming media and peer casting for multicasting streams, which facilitates on-demand content delivery. Other applications involve science, networking, search and communication networks. Even the U.S. Department of Defense has started researching applications for P2P networks for modern network warfare strategies.

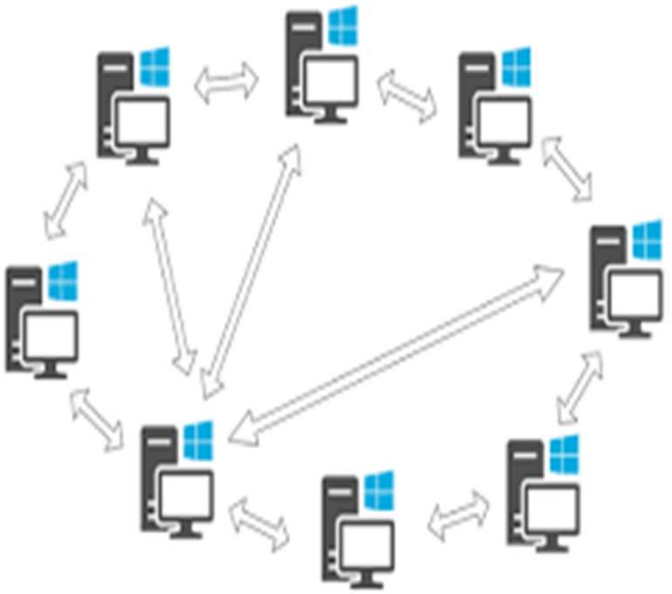
There are three models of unstructured P2P computer network architecture:
Pure P2P

Hybrid P2P

Centralized P2P

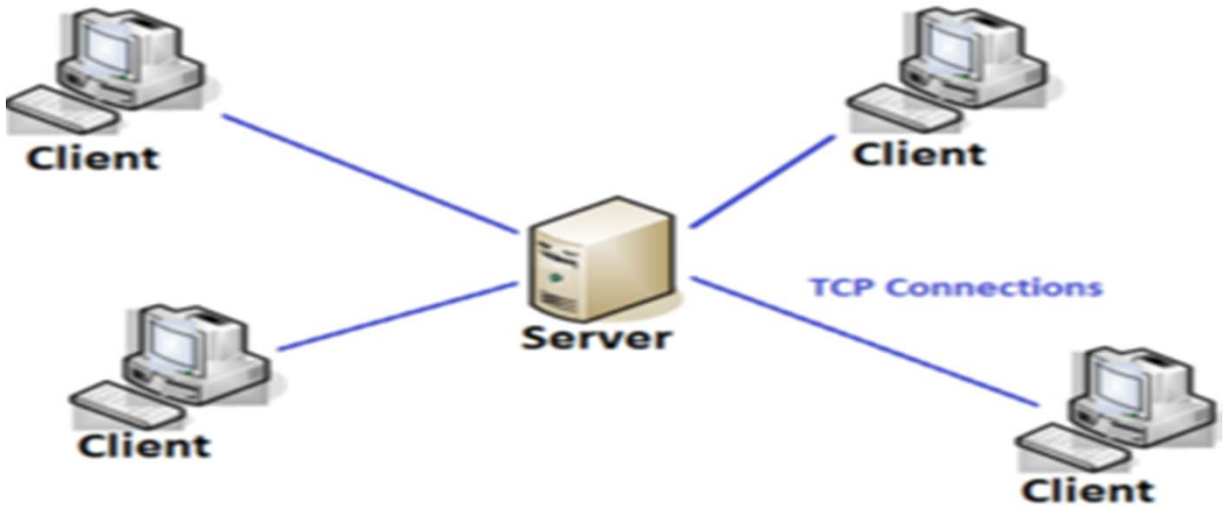

Peer
Peer
Peer
Peer


Mobile peer
Mobile peer
Super-peer (DB)
Super-Peer (DB)
Portable peer
Mobile peer
Mobile peer
Super-peer (DB)
Super-peer (DB)
Super-peer (DB)
Portable peer
Mobile peer
Mobile peer



Client Server Architecture

Client Server Architecture is a computing model in which the server hosts, delivers and manages most of the resources and services to be consumed by the client. This type of architecture has one or more client computers connected to a central server over a network or internet connection. This system shares computing resources. **Client/server architecture** is also known as a networking computing model or client/server network because all the requests and services are delivered over a network.[1]



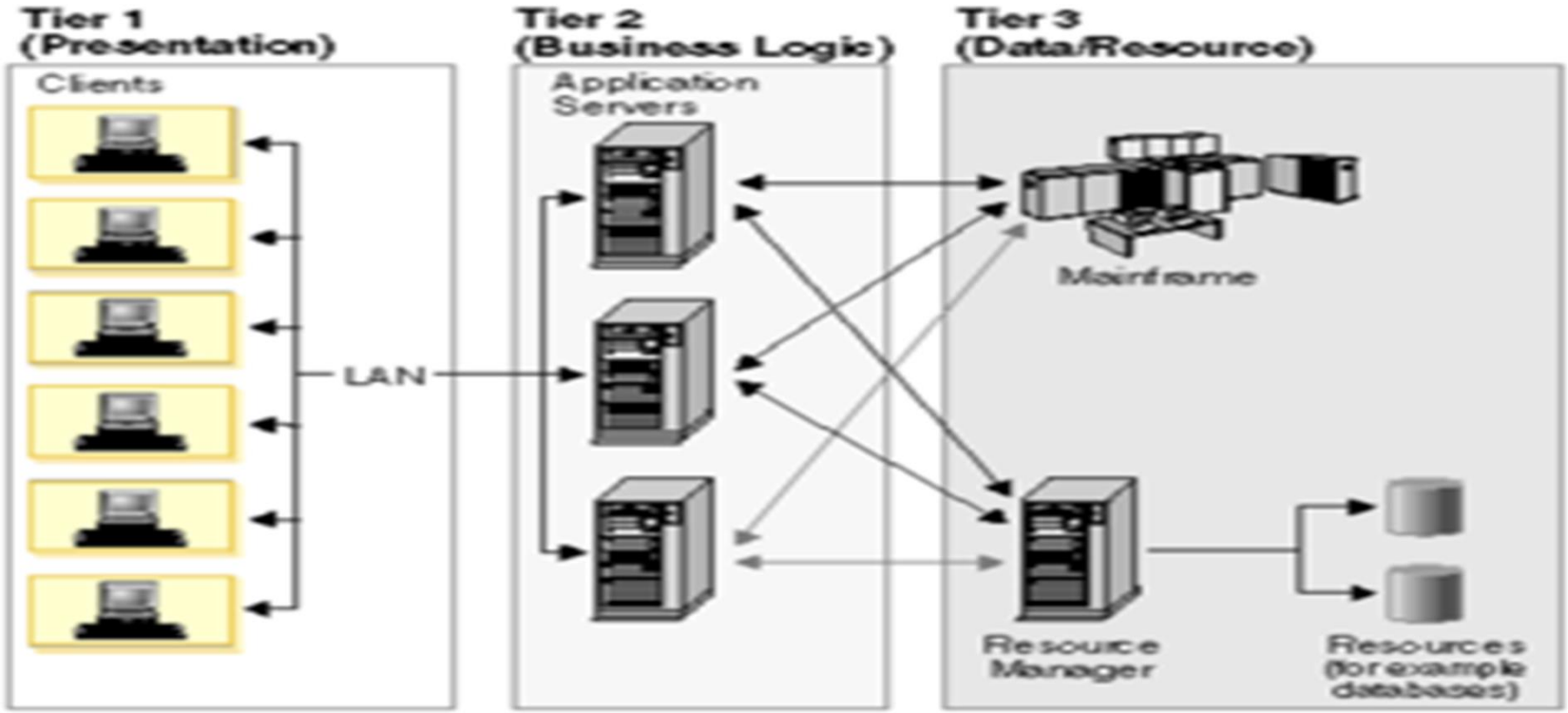
The Purpose of Client/Server Architecture

We are in an era where information technology plays a critical role in business applications, considered as an area an organization would highly invest in order to widen the opportunities available to compete the global market. “A competitive global economy will ensure obsolescence and obscurity to those who cannot or are unwilling to compete”(Client/Server Architecture,2011), according to this statement it’s necessary for organizations sustain its market position by reengineering prevailing organizational structures and business practices to achieve their business goals. In short it’s a basic need to evolve with the change of technological aspects. Therefore organizations should undergo a mechanism to retrieve and process its corporate data to make business procedures more efficient to excel or to survive in the global market. The client/server model brings out a logical perspective of distributed corporative processing where a server handles and processes all client requests. This can be also viewed as a revolutionary milestone to the data processing industry. “Client/server computing is the most effective source for the tools that empower employees with authority and responsibility.”(Client/Server Architecture,2011)

Characteristics of a Client-Server Architecture

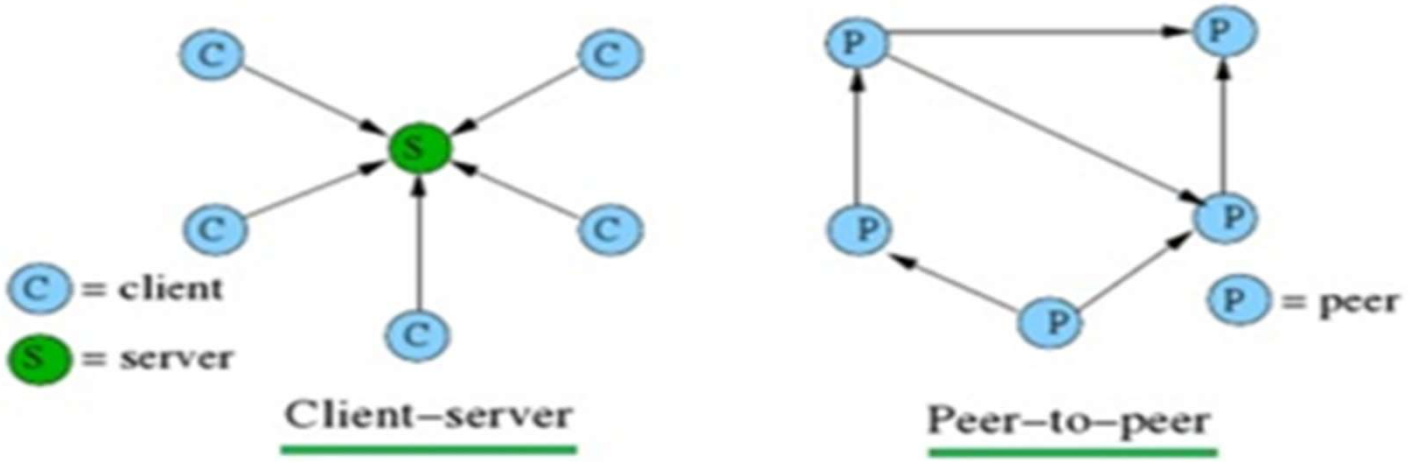
Client and server machines need different amount of hardware and software resources.
Client and server machines may belong to different vendors.
Horizontal scalability (increase of the client machines) and vertical scalability (migration to a more powerful server or to a multiserver solution)
A client or server application interacts directly with a transport layer protocol to establish communication and to send or receive information.
The transport protocol then uses lower layer protocols to send or receive individual messages. Thus, a computer needs a complete stack of protocols to run either a client or a server.
A single server-class computer can offer multiple services at the same time; a separate server program is needed for each service.

Three-tier Client Server Architecture



Client Server Vs. Peer to Peer

In distributed architecture, one or more dedicated machines are used only as server while all the other machines are used as clients. In this scenario, clients can communicate via server.
In this mode, client initiates communications.
Client issues request to a server.
Server replies or performs some service.
In peer to peer architecture, Each of the host or instance of application program can function as both client and server simultaneously. Both of them has equivalent responsibilities and status.
In this mode, any participant can initiate communication.
Any device can generate a request.
Any device may provide a response.



Types of Networks

- **Local-area network (LAN)** A network that connects a relatively small number of machines in a relatively close geographical area

Types of Networks

- Various configurations, called topologies, have been used to administer LANs
  - **Ring topology** A configuration that connects all nodes in a closed loop on which messages travel in one direction
  - **Star topology** A configuration that centers around one node to which all others are connected and through which all messages are sent
  - **Bus topology** All nodes are connected to a single communication line that carries messages in both directions

Types of Networks

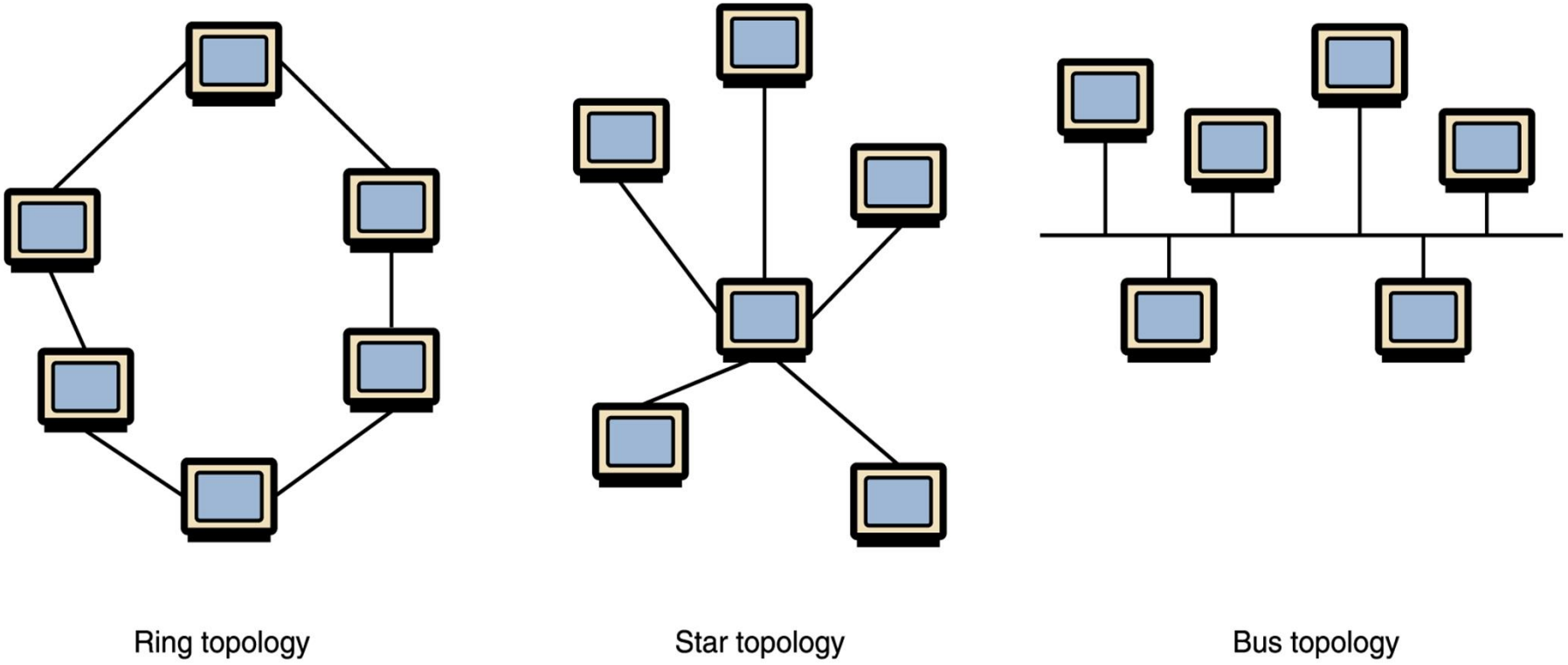


Figure 15.2 **Various network topologies**

- A bus technology called **Ethernet** has become the industry standard for local-area networks

Types of Networks

- **Wide-area network (WAN)** A network that connects two or more local-area networks over a potentially large geographic distance
  - Often one particular node on a LAN is set up to serve as a **gateway** to handle all communication going between that LAN and other networks
  - Communication between networks is called internetworking
  - The **Internet**, as we know it today, is essentially the ultimate wide-area network, spanning the entire globe

Types of Networks

- **Metropolitan-area network (MAN)** The communication infrastructures that have been developed in and around large cities

So, who owns the Internet?

Well, nobody does. No single person or company owns the Internet or even controls it entirely. As a wide-area network, it is made up of many smaller networks. These smaller networks are often owned and managed by a person or organization. The Internet, then, is really defined by how connections can be made between these networks.

Types of Networks

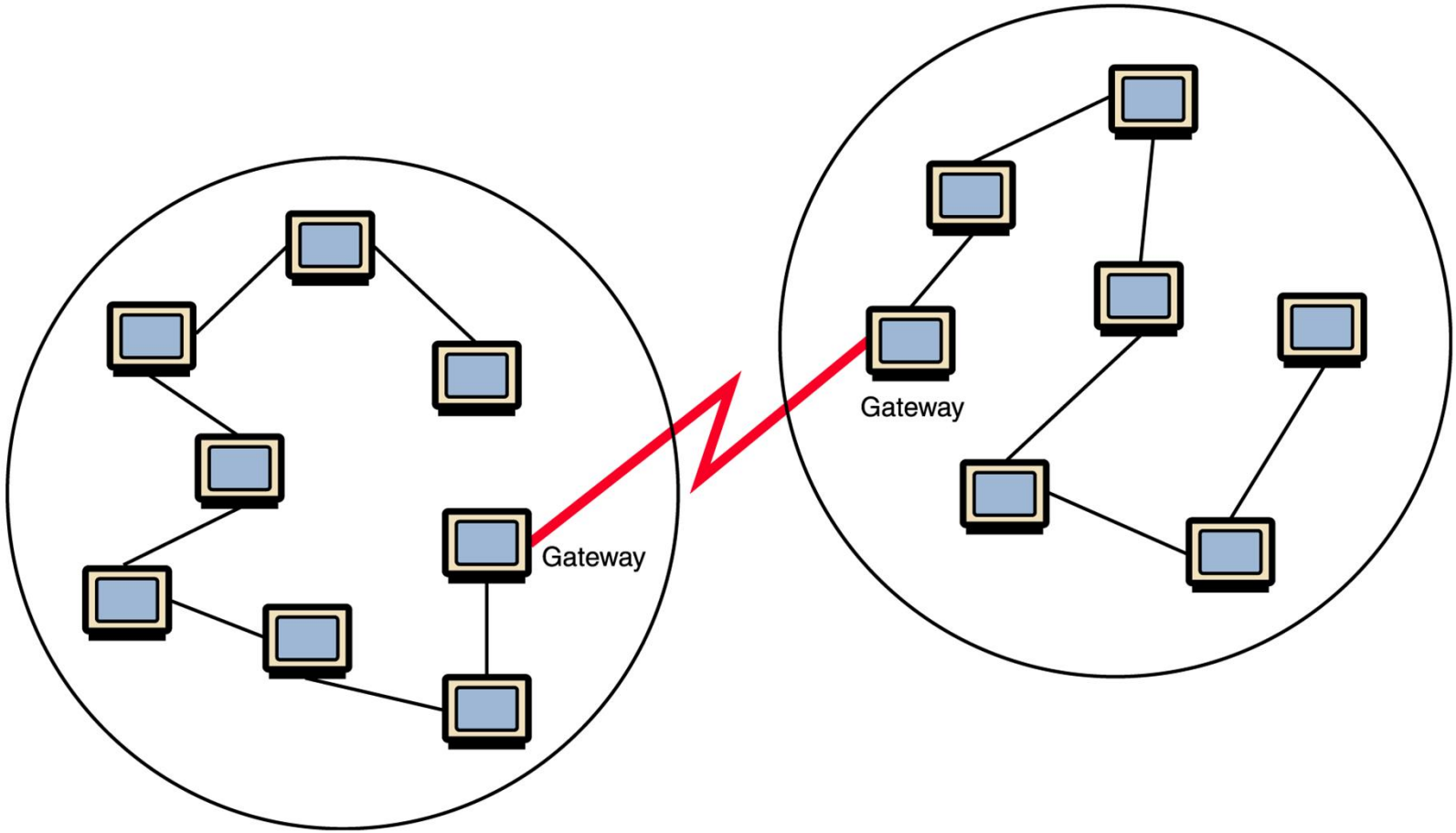


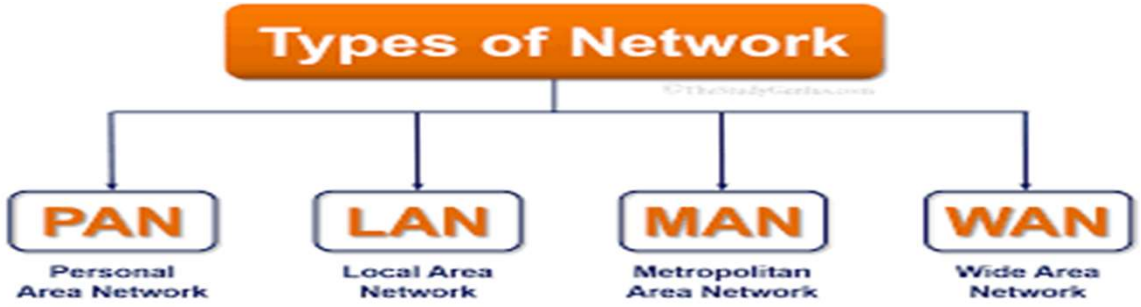
Figure 15.1 **Local-area networks connected across a distance to create a wide-area network**

Network types

The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN, and WAN are the three major types of networks designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area; **MAN** covers an area larger than LAN and **WAN** comprises the largest of all.

Network types

- LAN
- MAN
- WAN



Local Area Network (LAN)

LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

Data transmits at a very fast rate as the number of computers linked is limited. By definition, the connections must be high speed and relatively inexpensive hardware (Such as hubs, network adapters, and Ethernet cables). LANs cover a smaller geographical area (Size is limited to a few kilometers) and are privately owned. One can use it for an office building, home, hospital, schools, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted-pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

Metropolitan Area Network (MAN)

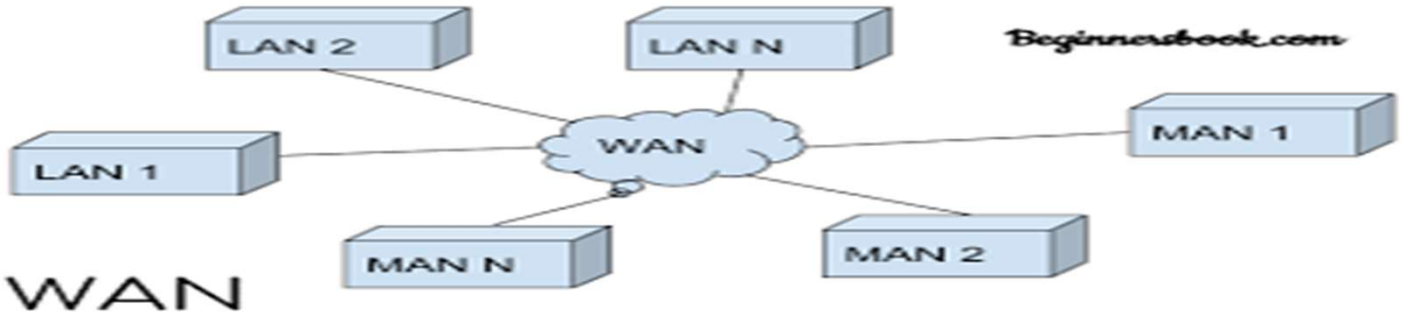
MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but reside in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need high-speed connectivity. Speeds of MAN range in terms of Mbps. It's hard to design and maintain a Metropolitan Area Network.

Metropolitan Area Network (MAN)

The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN are moderate. Devices used for transmission of data through MAN are Modem and Wire/Cable. Examples of a MAN are the part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

Wide Area Network (WAN)

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LANs via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive.
There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network.WAN's data rate is slow about a 10th LAN's speed since it involves increased distance and increased number of servers and terminals etc. Speeds of WAN ranges from a few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for the transmission of data through WAN are Optic wires, Microwaves, and Satellites. An example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is a dial-up line that connects a home computer to the Internet.



Internet Connections

- **Internet backbone** A set of high-speed networks that carry Internet traffic

  These networks are provided by companies such as AT&T, GTE, and IBM

- **Internet service provider (ISP)** A company that provides other companies or individuals with access to the Internet

Switching in Network

Switching is process to forward packets coming in from one port to a port leading towards the destination. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

- **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

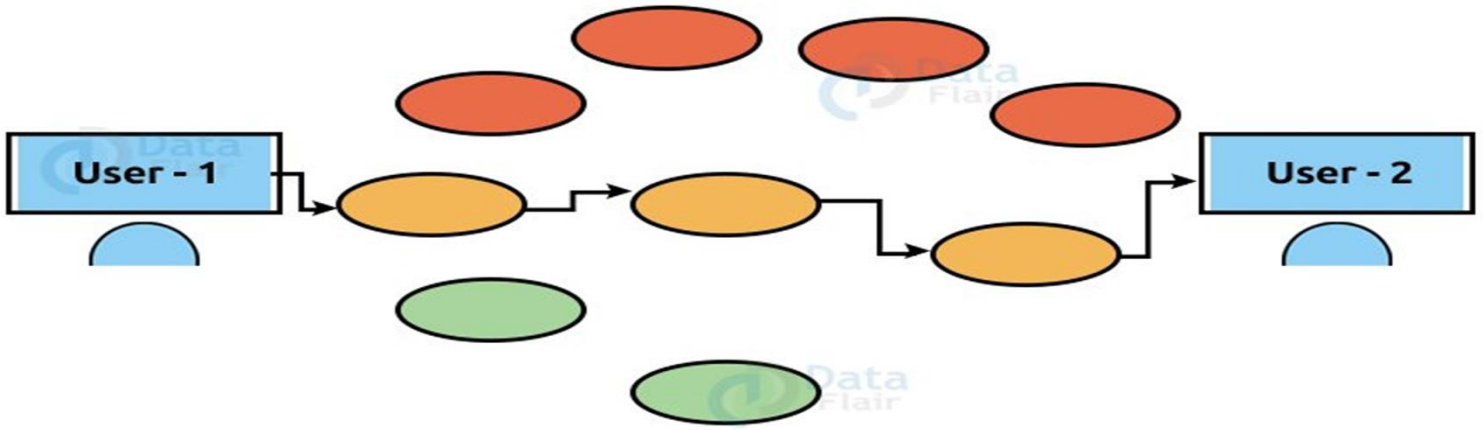
Types of Switching:

- ❑ Circuit Switching
- ❑ Messaging Switching
- ❑ Packet Switching

Circuit Switching

Circuit switching is a switching method that creates a dedicated channel between the transmitter and the receiver.

- Once the link is created via the Circuit Switching Technique, the dedicated path will exist until the connection is cancelled. Circuit switching in a network works in the same manner that the telephone does.
- Before communication takes place, a complete end-to-end route must exist.
- When a user wishes to transfer data, audio, or video using the circuit switching approach, a request signal is sent to the receiver, and the receiver responds with an acknowledgment to guarantee the availability of the dedicated path for message transmission. After obtaining acknowledgment, the data is sent through a designated route.
- In a public telephone network, circuit switching is used. It is used to transmit voice. In the circuit switching technology, fixed data may be transmitted at the same time.



Circuit Switching

Advantages of Circuit Switching:

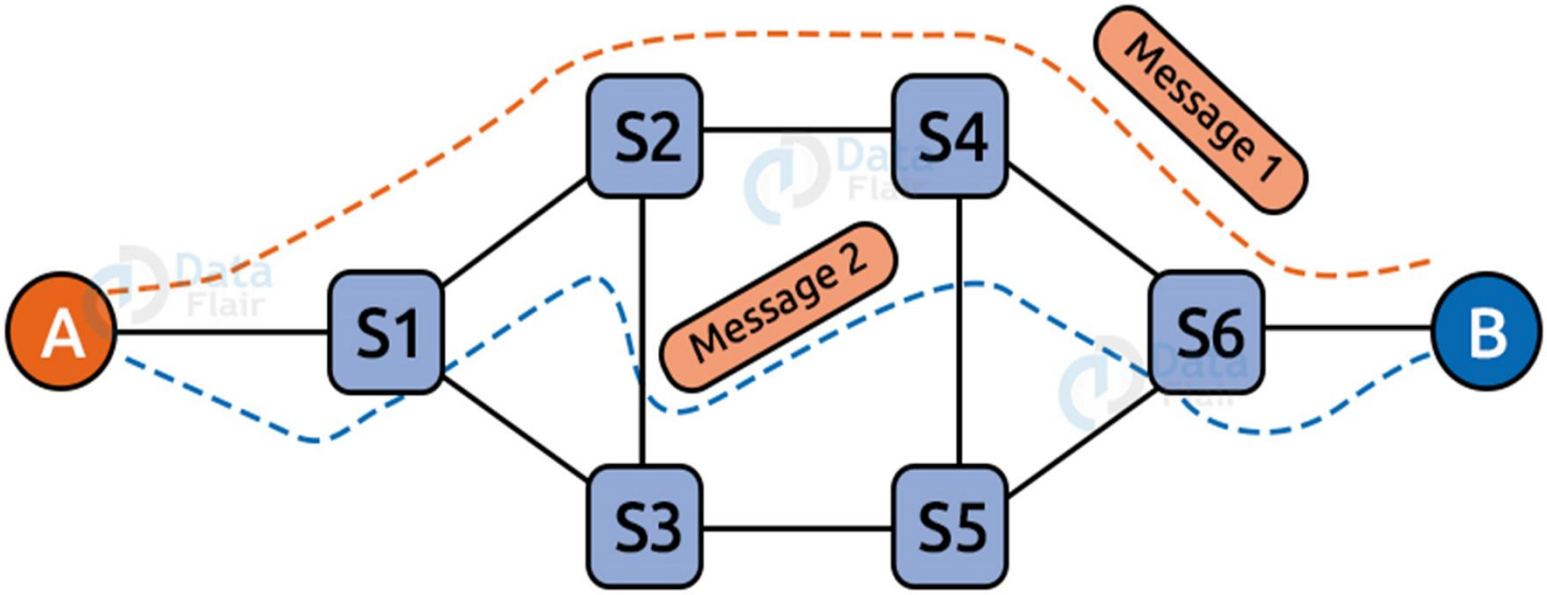
- The communication channel is dedicated and exclusive in the case of the Circuit Switching method.
- It has a fixed bandwidth.

Disadvantages of Circuit Switching:

- The only delay in data transfer happens once the dedicated channel is created.
- It takes around 10 seconds to establish a connection, during which no data may be sent.
- This is more costly than other switching approaches since each connection requires a dedicated route.
- It is inefficient to utilize since the capacity of the path is squandered after the path is built and no data is transmitted.
- In this situation, the connection is devoted, thus even if the channel is free, no additional data may be sent.

Message Switching

Message switching is a switching mechanism that transfers a message as a full and complete unit and routes it through intermediate nodes which store and forward the message. There is no specific path between the sender and recipient in the Message Switching method.



Message Switching

- Message switching is a switching mechanism that transfers a message as a full and complete unit and routes it through intermediate nodes which store and forward the message. There is no specific path between the sender and recipient in the Message Switching method.The message's destination address is added. Message Switching enables and facilitates dynamic routing by routing the message through intermediary nodes based on the information and data included in the message. Message switches are configured in such a way that they give the most efficient routes. Every node saves the full message before forwarding it to the next node. This is referred to as a store and forward network.

***Advantages of Message Switching**:*

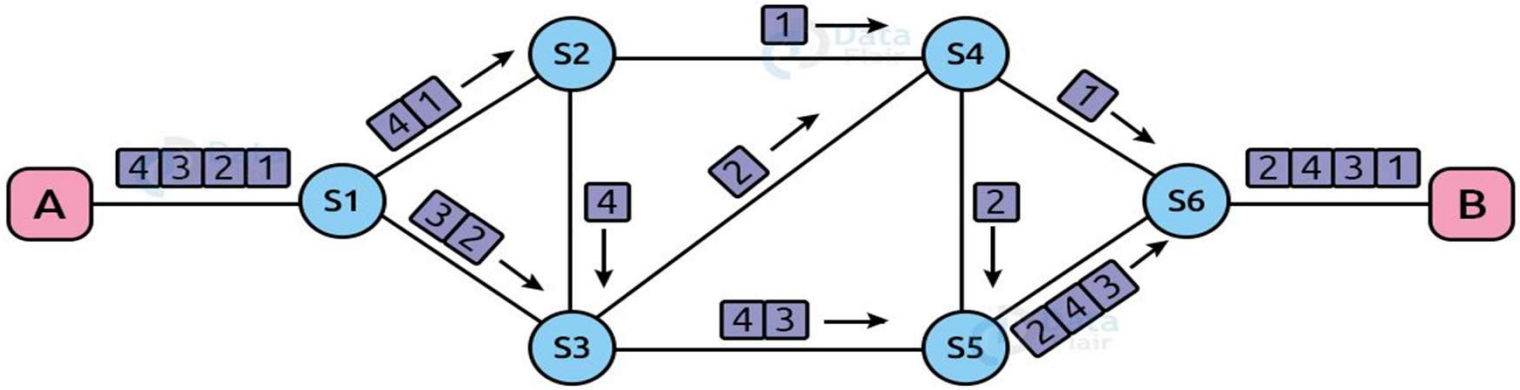
- Data channels are shared across connecting devices, which improves the efficiency with which available bandwidth is used.
- Because the message is briefly held in the nodes, traffic congestion can be minimised.
- The network may be managed using message priority.
- The size of the message transmitted across the network can be altered. As a result, it can handle data of any scale.

Disadvantages of Message Switching:

- The message switches must have enough storage to hold the messages until they are forwarded.
- Long delays can arise as a result of the message switching technique's storing and forwarding capabilities.

Packet Switching

Packet switching is a switching technique in which the message is split into smaller bits and delivered separately rather than all at once. The message is broken down into smaller bits known as packets, and each packet is assigned a unique number to indicate its sequence at the receiving end. The headers of each packet contain information such as the source address, destination address, and sequence number. Packets will go across the network in the quickest possible way. At the receiving end, all packets are reassembled in the right order. If any packet is missing or corrupted, the message will be resent. If the packets are received in the right order, the acknowledgment message is delivered.



Methods to achieve Packet Switching

Datagram Packet Switching:

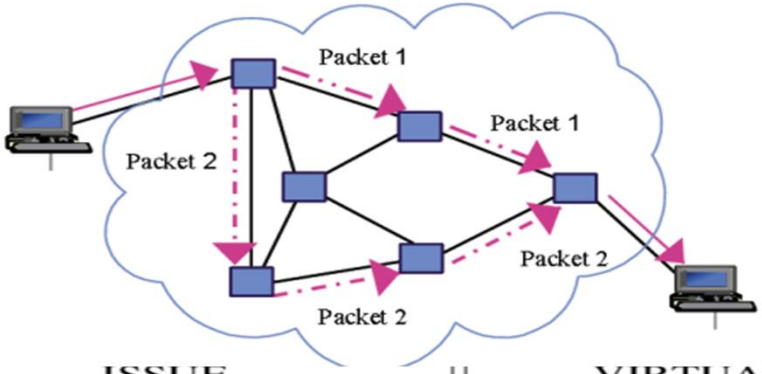
It is a packet switching approach that treats each packet, known as a datagram, as a distinct entity. Each packet contains information about the destination, which the switch utilizes to route the packet to the right location. At the receiving end, the packets are reassembled in the right order. The route is not set in the Datagram Packet Switching method. To forward packets, intermediate nodes have to make important routing decisions. It is also known as connection-less switching.

Virtual Circuit Packet Switching

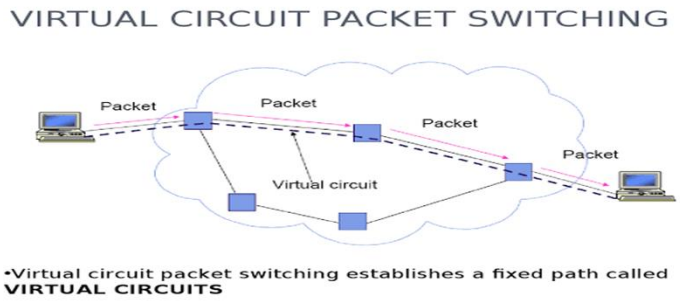
Another name for virtual circuit switching is connection-oriented switching. Before messages are transmitted, a preplanned path is established in the case of virtual circuit switching. The call request and call accept packets are used to connect the sender and recipient. The route is fixed in this situation for the duration of a logical link.

Difference between Datagram and Virtual Circuit Packet Switching

Datagram



Virtual Circuit



ISSUE	VIRTUAL CIRCUIT	DATAGRAM
Addressing	Each packet contains a short VC number	Each packet contains the source and the destination address
State Information	State information about each VC is maintained	Does not hold packet level state information
Routing	Route is chosen when VC is setup. All packets follow this route	Each packet is routed independently
Congestion control	Easy if enough buffers can be allocated in advance	Difficult
Resource failure	All VCs passing through the failed resource are terminated	Packets are lost only during resource failure
Suitability	Connection-oriented service	Connection-oriented and connectionless service

Advantages of Packet Switching:

•Because packet switching devices do not require huge secondary storage to hold packets, costs are reduced to some extent. As a result, we can claim that the packet switching approach is cost-effective.

•If any of the nodes are busy, packets can be redirected. This guarantees that the Packet Switching method delivers consistent communication.

•Packet switching is a time-saving method. It does not require any established path prior to transmission, and several users can utilise the same communication channel at the same time, making effective use of available bandwidth.

Disadvantages of Packet Switching:

Packet Switching cannot be used in applications that need low latency and high-quality services.

The protocols used in packet-switching are quite complicated and have a significant implementation cost.

If the network is overcrowded or damaged, lost packets must be retransmitted. It can also result in the loss of crucial data if mistakes are not recovered

Circuit Switching	Packet Switching(Datagram type)	Packet Switching(Virtual Circuit type)
Dedicated path	No Dedicated path	No Dedicated path
Path is established for entire conversation	Route is established for each packet	Route is established for entire conversation
Call setup delay	packet transmission delay	call setup delay as well as packet transmission delay
Overload may block call setup	Overload increases packet delay	Overload may block call setup and increases packet delay
Fixed bandwidth	Dynamic bandwidth	Dynamic bandwidth
No overhead bits after call setup	overhead bits in each packet	overhead bits in each packet

Internet Connections

- There are various technologies available that you can use to connect a home computer to the Internet
  - A **phone modem** converts computer data into an analog audio signal for transfer over a telephone line, and then a modem at the destination converts it back again into data
  - A **digital subscriber line** **(DSL)** uses regular copper phone lines to transfer digital data to and from the phone company's central office
  - A **cable modem** uses the same line that your cable TV signals come in on to transfer the data back and forth

Internet Connections

- **Broadband** A connection in which transfer speeds are faster than 128 bits per second
  - DSL connections and cable modems are broadband connections
  - The speed for **downloads** (getting data from the Internet to your home computer) may not be the same as **uploads** (sending data from your home computer to the Internet)

Open Systems

- **Proprietary system** A system that uses technologies kept private by a particular commercial vendor

  One system couldn't communicate with another, leading to the need for

- **Interoperability** The ability of software and hardware on multiple machines and from multiple commercial vendors to communicate

  Leading to

- **Open systems** Systems based on a common model of network architecture and a suite of protocols used in its implementation

Open Systems

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

Figure 15.5 **The layers of the OSI Reference Model**

- The International Organization for Standardization (ISO) established the **Open Systems Interconnection (OSI) Reference Model**
- Each layer deals with a particular aspect of network communication

Network Protocols

- Network protocols are layered such that each one relies on the protocols that underlie it
- Sometimes referred to as a **protocol stack**

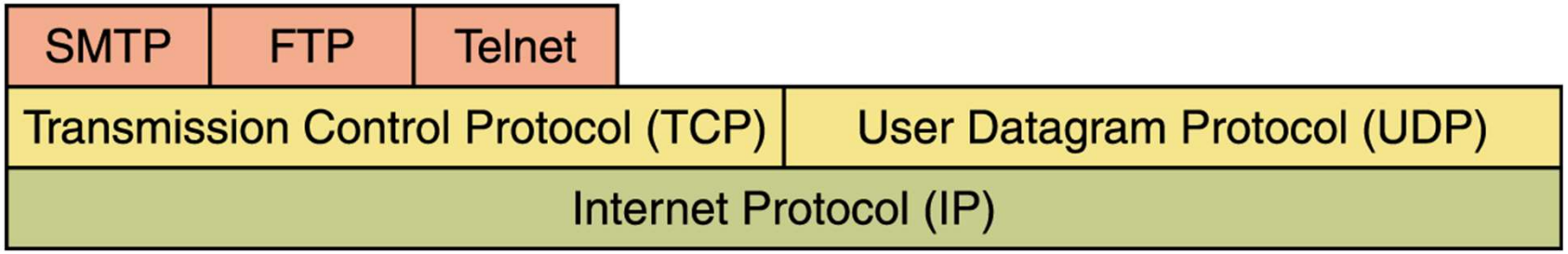


Figure 15.6 **Layering of key network protocols**

TCP/IP

- TCP stands for **Transmission Control Protocol**

  TCP software breaks messages into packets, hands them off to the IP software for delivery, and then orders and reassembles the packets at their destination

- IP stands for **Internet Protocol**

  IP software deals with the routing of packets through the maze of interconnected networks to their final destination

TCP/IP (cont.)

- UDP stands for **User Datagram Protocol**
  - It is an alternative to TCP
  - The main difference is that TCP is highly reliable, at the cost of decreased performance, while UDP is less reliable, but generally faster

High-Level Protocols

- Other protocols build on the foundation established by the TCP/IP protocol suite
  - Simple Mail Transfer Protocol (SMTP)
  - File Transfer Protocol (FTP)
  - Telnet
  - Hyper Text Transfer Protocol (http)

MIME Types

- Related to the idea of network protocols and standardization is the concept of a file's MIME type
  - MIME stands for **Multipurpose Internet Mail Extension**
  - Based on a document's MIME type, an application program can decide how to deal with the data it is given

MIME Types

Protocol	Port
Echo	7
File Transfer Protocol (FTP)	21
Telnet	23
Simple Mail Transfer Protocol (SMTP)	25
Domain Name Service (DNS)	53
Gopher	70
Finger	79
Hyper Text Transfer Protocol (HTTP)	80
Post Office Protocol (POP3)	110
Network News Transfer Protocol (NNTP)	119
Internet Relay Chat (IRC)	6667

Figure 15.7
Some protocols and the ports they use

Firewalls

- **Firewall** A machine and its software that serve as a special gateway to a network, protecting it from inappropriate access
  - Filters the network traffic that comes in, checking the validity of the messages as much as possible and perhaps denying some messages altogether
  - Enforces an organization's **access control policy**

Firewalls

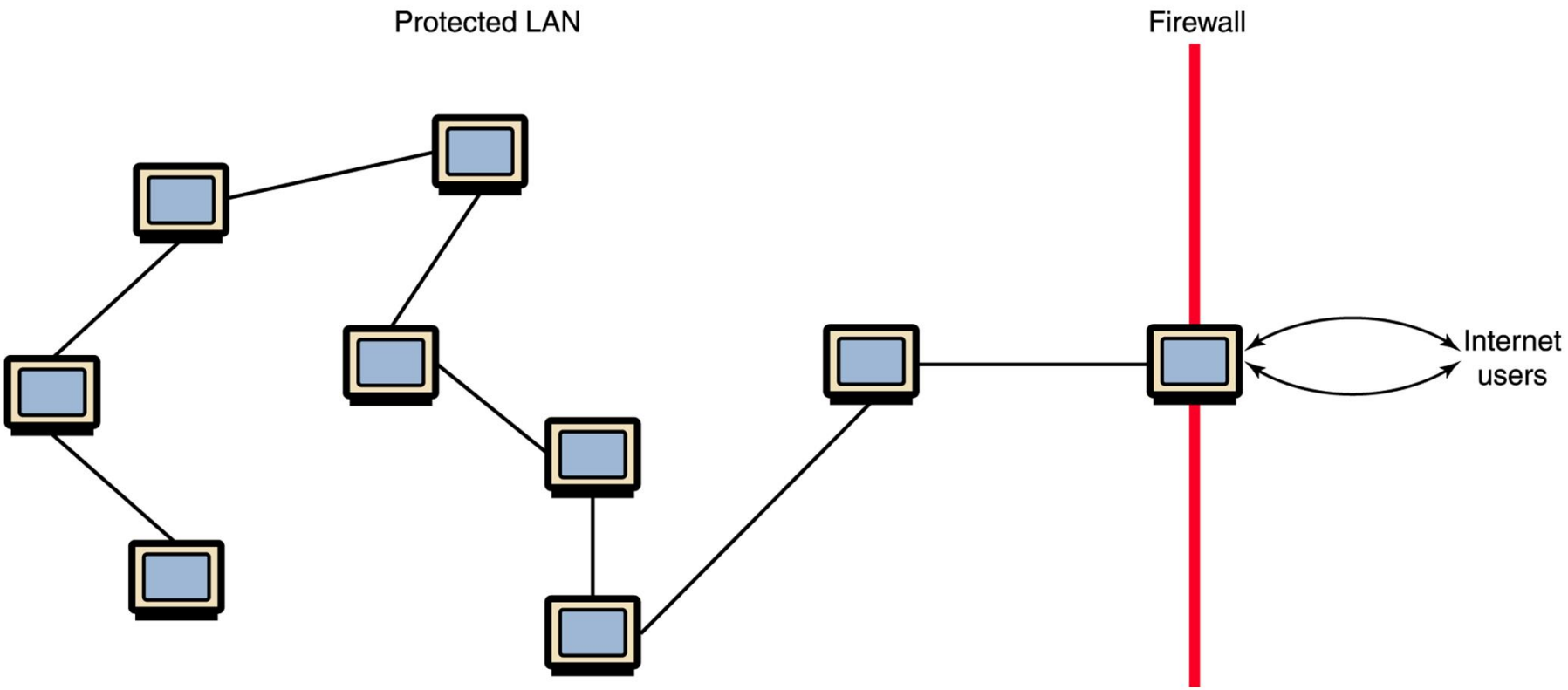


Figure 15.8 **A firewall protecting a LAN**

Network Addresses

- **Hostname** A unique identification that specifies a particular computer on the Internet

  For example

  matisse.csc.villanova.edu

  condor.develocorp.com

Network Addresses

- Network software translates a hostname into its corresponding IP address

  For example

  205.39.145.18

Network Addresses

- An **IP address** can be split into
  - **network address**, which specifies a specific network
  - **host number**, which specifies a particular machine in that network

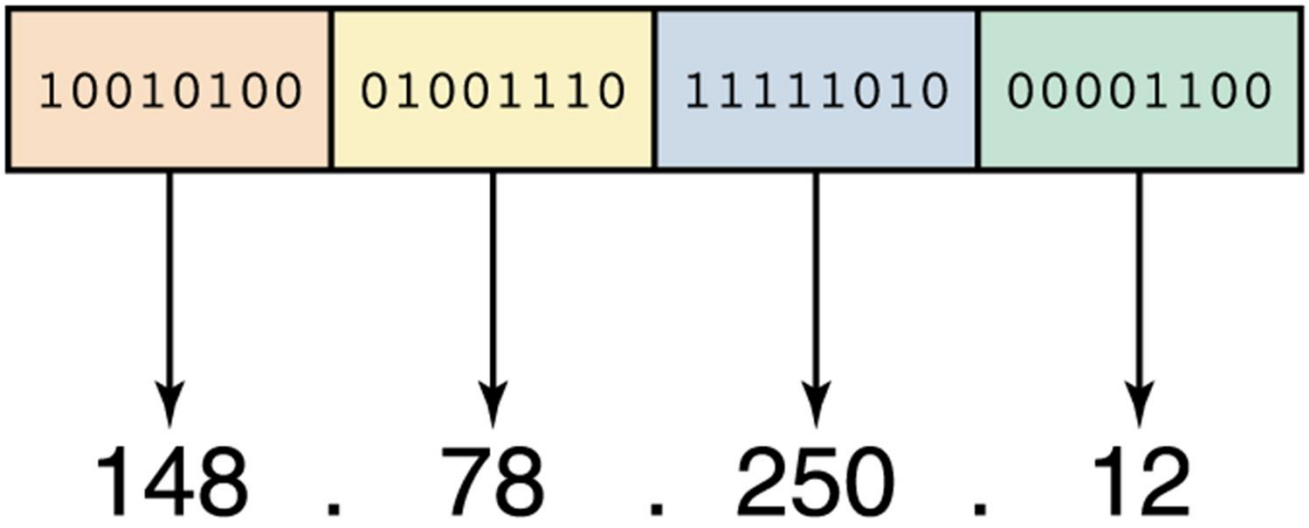


Figure 15.9
An IP address is stored in four bytes

Domain Name System

- A hostname consists of the computer name followed by **the domain name**
- csc.villanova.edu is the domain name
  - A domain name is separated into two or more sections that specify the organization, and possibly a subset of an organization, of which the computer is a part
  - Two organizations can have a computer named the same thing because the domain name makes it clear which one is being referred to

Domain Name System

- The very last section of the domain is called its **top-level domain (TLD)** name

Top-Level Domain	General Purpose	New TLDs	General Purpose
.com	U.S. Commercial	.biz	Business
.net	Network	.info	Information
.org	Nonprofit organization	.pro	Professional
.edu	U.S. Educational	.museum	Museums
.int	International	.aero	Aerospace industry
.mil	U.S. Military	.coop	Cooperative
.gov	U.S. Government		

Figure 15.10 **Top-level domains, including some relatively new ones**

Domain Name System

- Organizations based in countries other than the United States use a top-level domain that corresponds to their two-letter country codes

Country Code TLD	Country
.au	Australia
.br	Brazil
.ca	Canada
.gr	Greece
.in	India
.ru	Russian Federation
.uk	United Kingdom

Figure 15.11
Some of the top-level domain names based on country codes

Domain Name System

- The **domain name system** (DNS) is chiefly used to translate hostnames into numeric IP addresses
  - DNS is an example of a distributed database
  - If that server can resolve the hostname, it does so
  - If not, that server asks another domain name server

Computer Network
Chapter 2 & 3

Prepared By :

Patanjali

Lecturer in ECE Deptt.

Govt. Polytechnic Jhajjar

Layering in Networked computing

- OSI Model
- TCP/IP Model
- Protocols at each layer

Learning outcomes

- Understand the need of layering in Networked computing
- Understand the OSI model and the tcp/ip model
  - Understand the function protocols and their role at each layer.
    - TCP protocol
    - UDP protocol
- Understand the role of header in communication between layers
- Understand how data sent from one host arrive to the target host.

What is layering in Networked computing?

- Breaks down communication into smaller, simpler parts.

Why a layered model?

- Easier to teach communication process.
- Speeds development, changes in one layer does not affect how the other levels works.
- Standardization across manufactures.
- Allows different hardware and software to work together.
- Reduces complexity

The OSI Reference Model

The OSI Model

- OSI “ Open Systems Interconnection".
- OSI model was first introduced in 1984 by the International Organization for Standardization (ISO).
  - Outlines **WHAT** needs to be done to send data from one computer to another.
  - Not **HOW** it should be done.
  - Protocols stacks handle how data is prepared for transmittal (to be transmitted)
- In the OSI model, The specification needed
  - are contained in 7 different layers that interact with each other.

What is “THE MODEL?”

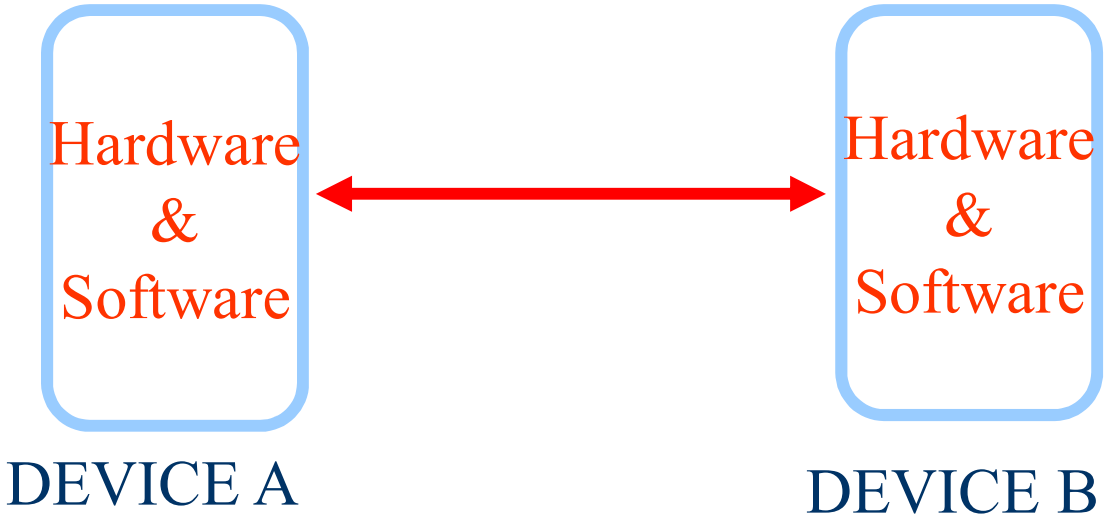
- Commonly referred to as the OSI reference model.
- The OSI model
  - is a theoretical blueprint that helps us understand how data gets from one user’s computer to another.
  - It is also a model that helps develop standards so that all of our hardware and software talks nicely to each other.
  - It aids standardization of networking technologies by providing an organized structure for hardware and software developers to follow, to insure there products are compatible with current and future technologies.

7 Layer OSI Model

- Why use a reference model?
  - Serves as an outline of rules for how protocols can be used to allow communication between computers.
  - Each layer has its own function and provides support to other layers.
- Other reference models are in use.
  - Most well known is the TCP/IP reference model.
  - We will compare OSI and TCP/IP models
- As computing requirements increased, the network modeling had to evolve to meet ever increasing demands of larger networks and multiple venders.
- Problems and technology advances also added to the demands for changes in network modeling.

Evolution of the 7-Layers

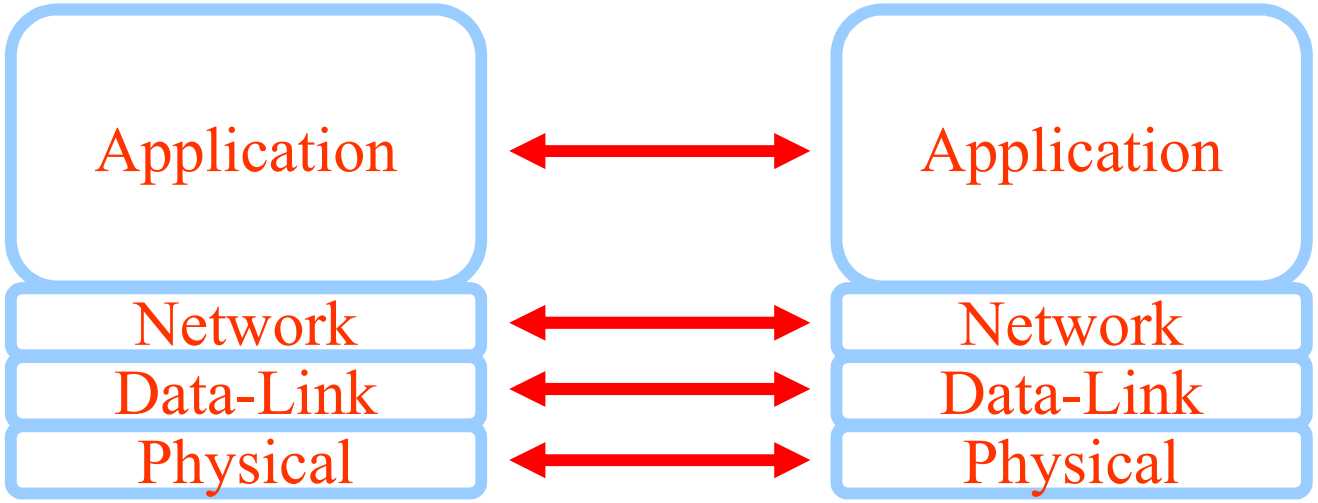
- Single Layer Model - First Communication Between Computer Devices
  - Dedicated copper wire or radio link
  - Hardware & software inextricably intertwined
  - Single specification for all aspects of communication



Evolution of the 7-Layers (1)

- Two Layer Model
  - **Problem:** Applications were being developed to run over ever-increasing number of media/signaling systems.
  - **Solution:** Separate application aspects from technical (signaling and routing) aspects
  - **Application Layer:** Concerned with user interface, file access and file transfer

Evolution of the 7-Layers (3)



- Four Layer Model - Network connectivity inherently requires travel over intermediate devices (nodes)
- Technical Standards Level divided into Network, Data-link and Physical Layers

http://www.howtheosimodelworks.com/

Evolution of the 7-Layers (3) cont.

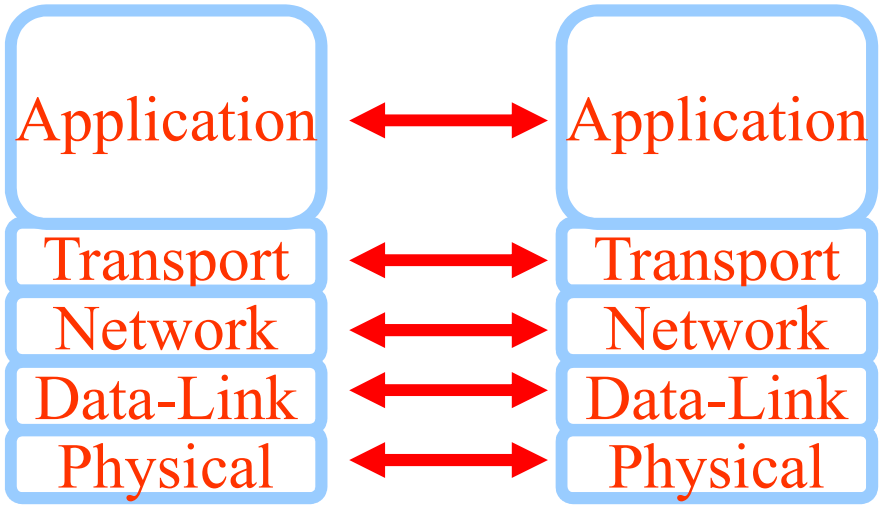
Physical Layer

–Describes physical aspects of network: cards, wires, etc

–Specifies interconnect topologies and devices

- Network Layer
  - –Defines a standard method for operating between nodes
  - –Address scheme is defined (IP)
  - –Accounts for varying topologies
- Data-Link
  - –Works with Network Layer to translate logical addresses (IP) into hardware addresses (MAC) for transmission
  - –Defines a single link protocol for transfer between two nodes

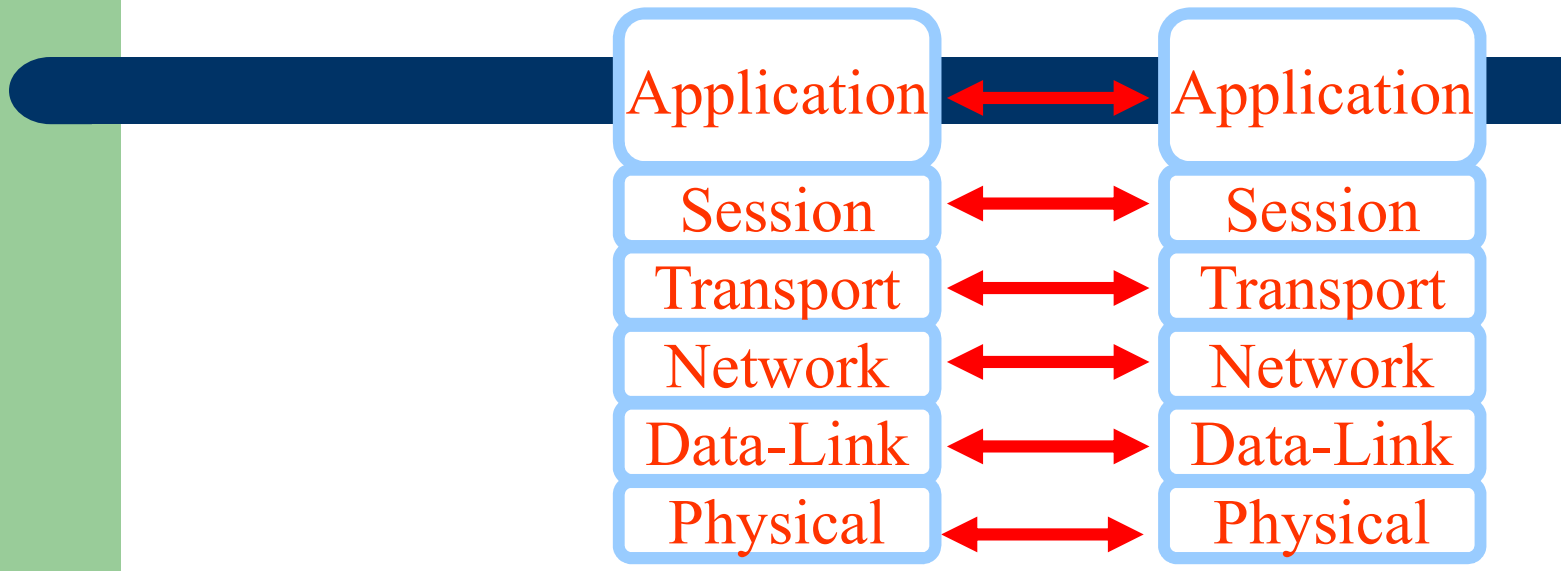
Evolution of the 7-Layers (4)



- Five Layer Model – Increase Quality of Service (QOS)
  - •Variable levels of data integrity in network
  - •Additional data exchanges to ensure connectivity over worst conditions
  - •Became the Transport Layer

http://www.howtheosimodelworks.com

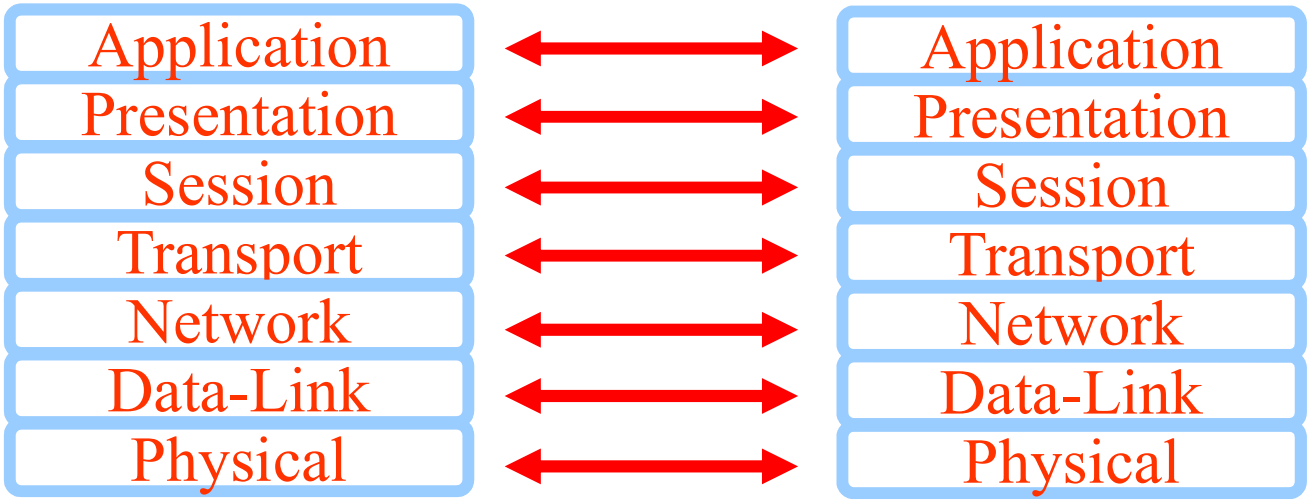
Evolution of the 7-Layers (5)



- Six Layer Model - Dialogue Control and Dialogue Separation
  - Means of synchronizing transfer of data packets
  - Allows for checkpointing to see if data arrives (at nodes and end stations)
  - Became Session Layer

http://www.howtheosimodelworks.com/

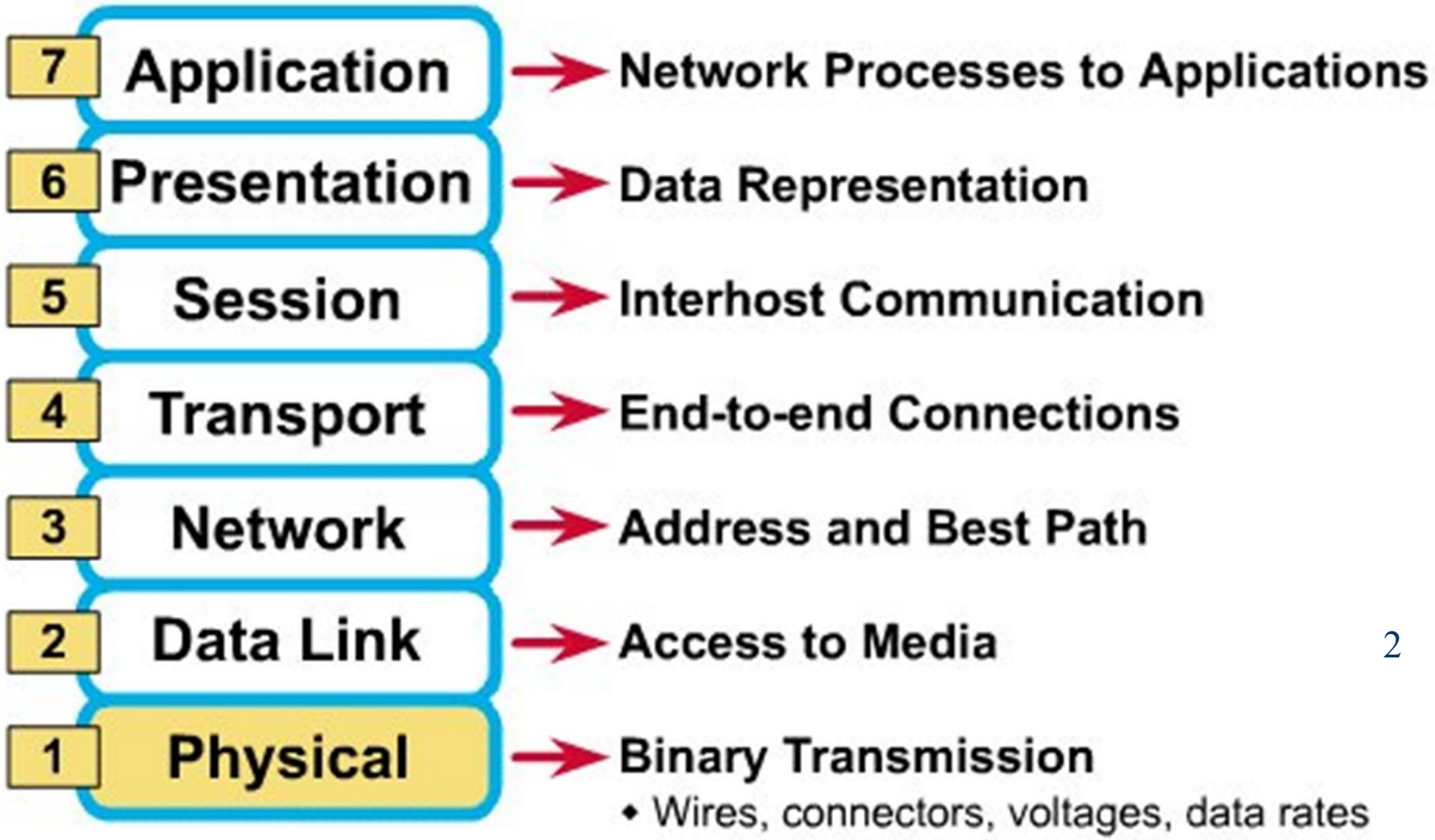
Evolution of the 7-Layers (6)



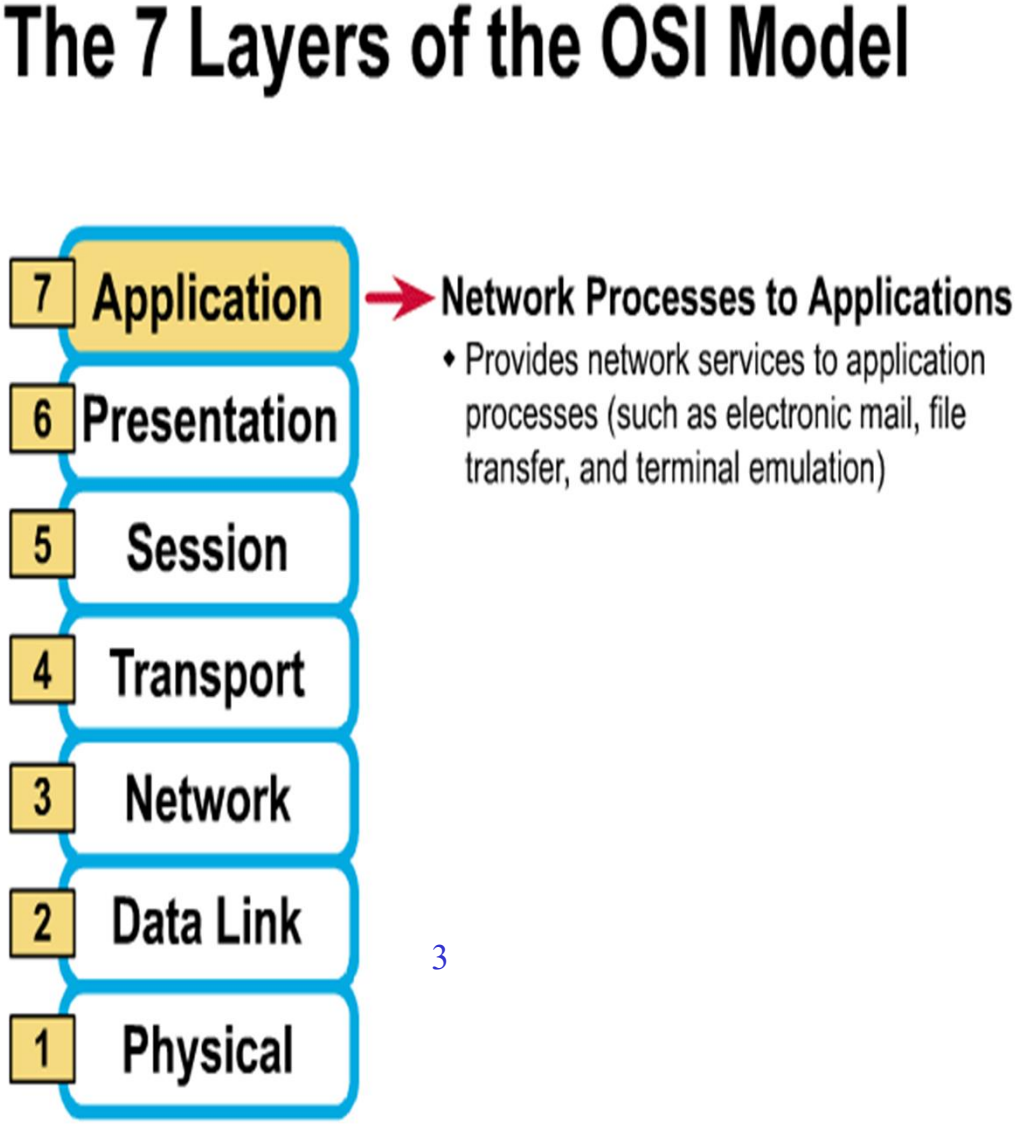
- The Seven Layer OSI Model - Addition of Management and Security
  - Standardizing notation or syntax for application messages (abstract syntax)[1]
  - Set of encoding rules (transfer syntax)
  - Became the Presentation Layer

http://www.howtheosimodelworks.com/

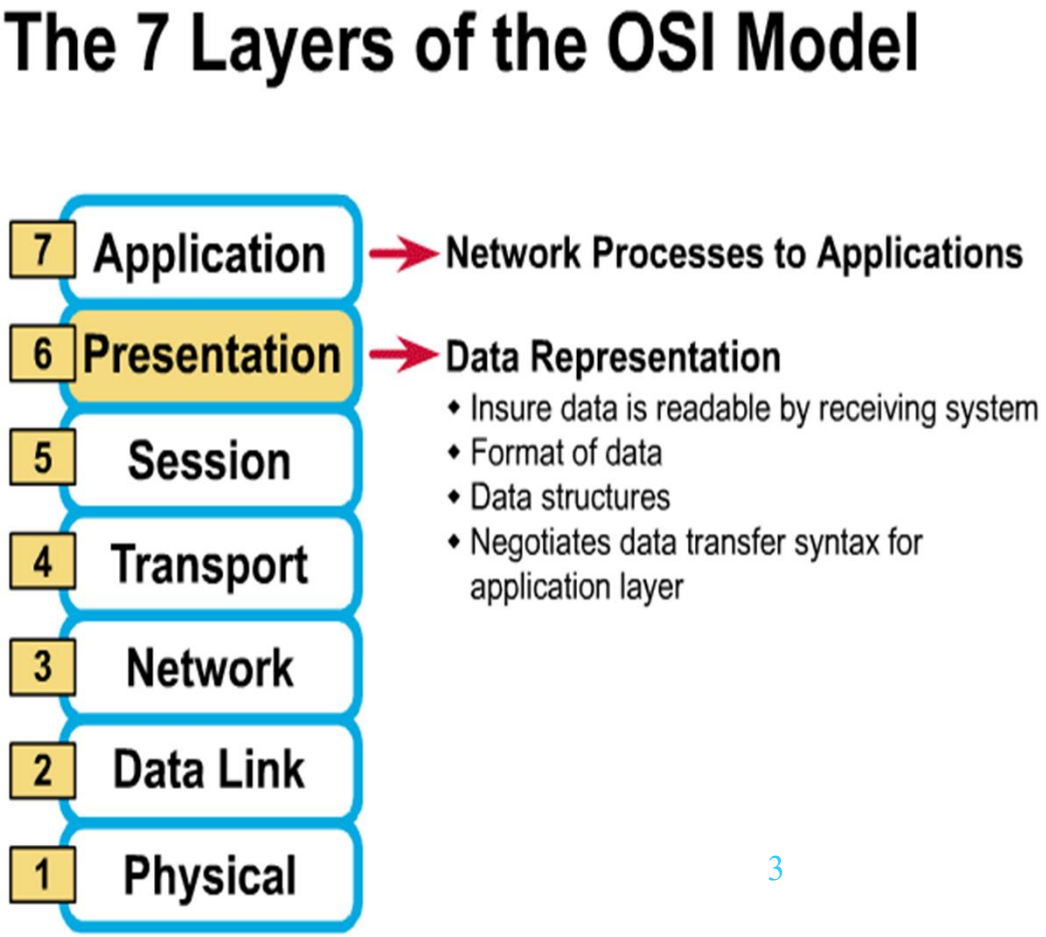
What Each Layer Does



- Gives end-user applications access to network resources
- Where is it on my computer?
  - Workstation or Server Service in MS Windows

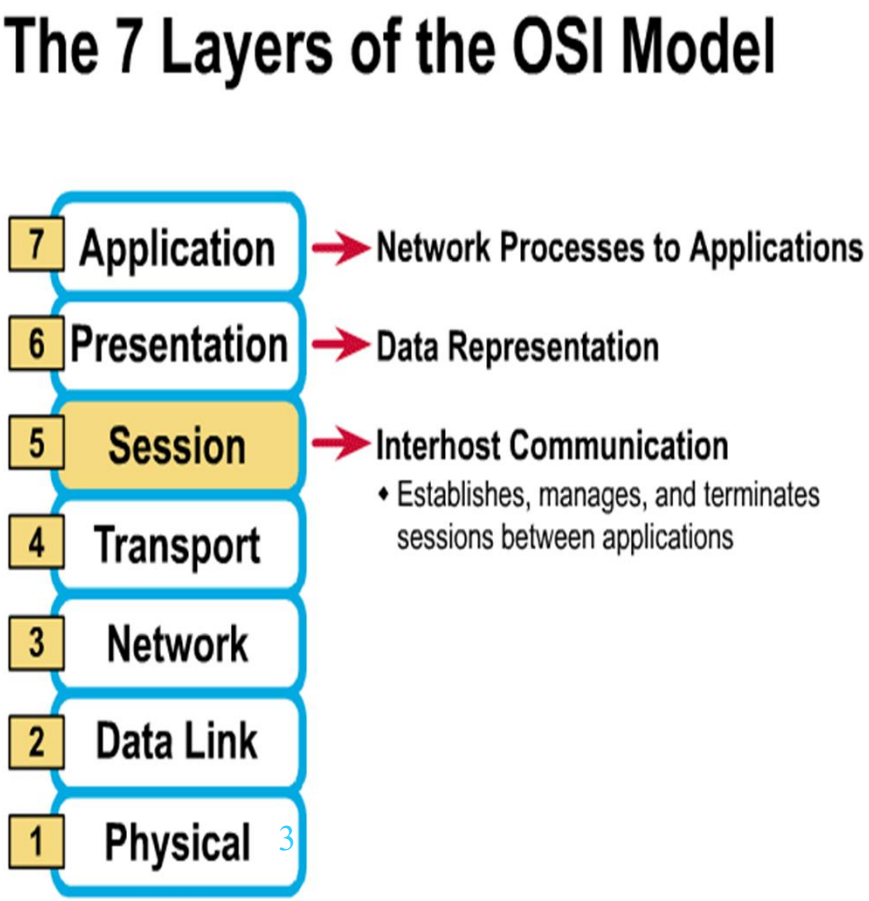


Presentation Layer



Session Layer

- Allows applications to maintain an ongoing session
- Where is it on my computer?
  - Workstation and Server Service (MS)
  - Windows Client for NetWare (NetWare)



Transport Layer

- Provides reliable data delivery
- It's the TCP in TCP/IP
- Receives info from upper layers and segments it into packets
- Can provide error detection and correction

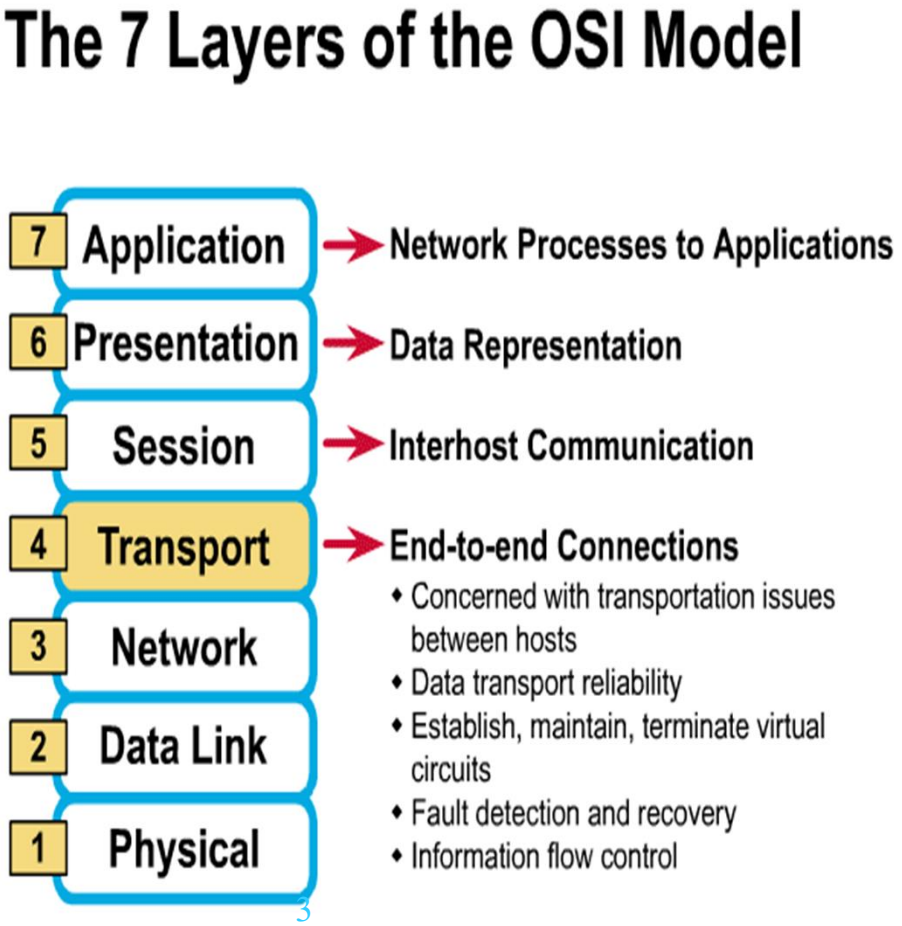
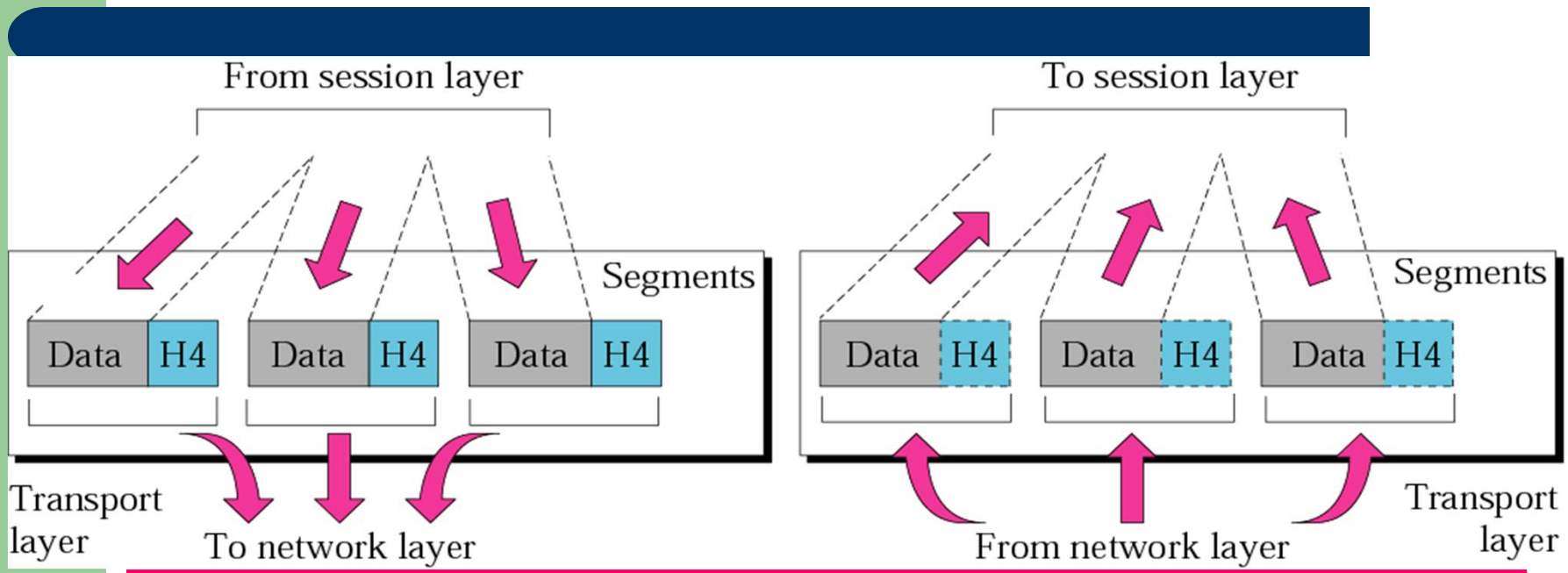


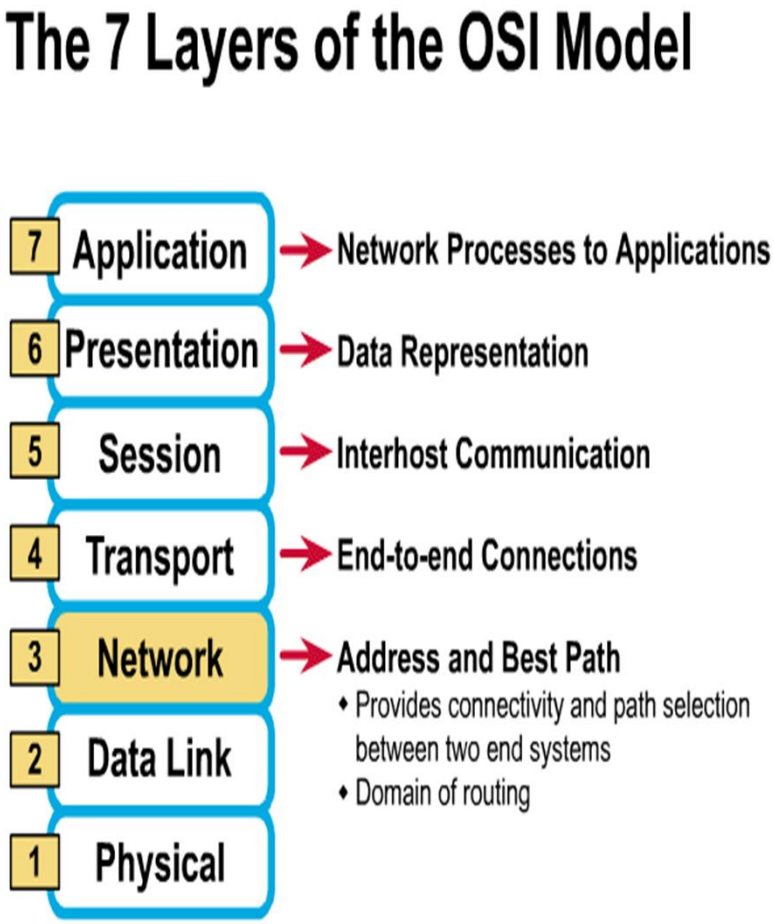
Figure 2.9 *Transport layer*



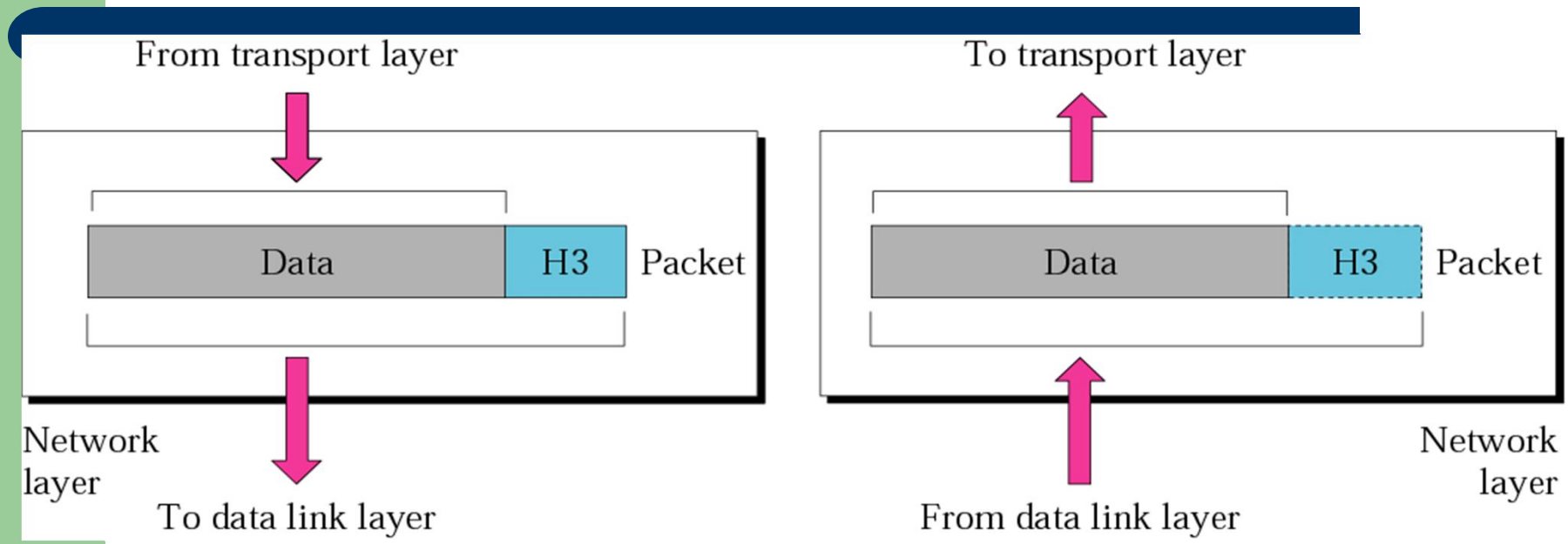
The transport layer is responsible for the delivery of a message from one process to another.

Network Layer

- Provides network-wide addressing and a mechanism to move packets between networks (routing)
- Responsibilities:
  - Network addressing
  - Routing
- Example:
  - IP from TCP/IP



Network layer



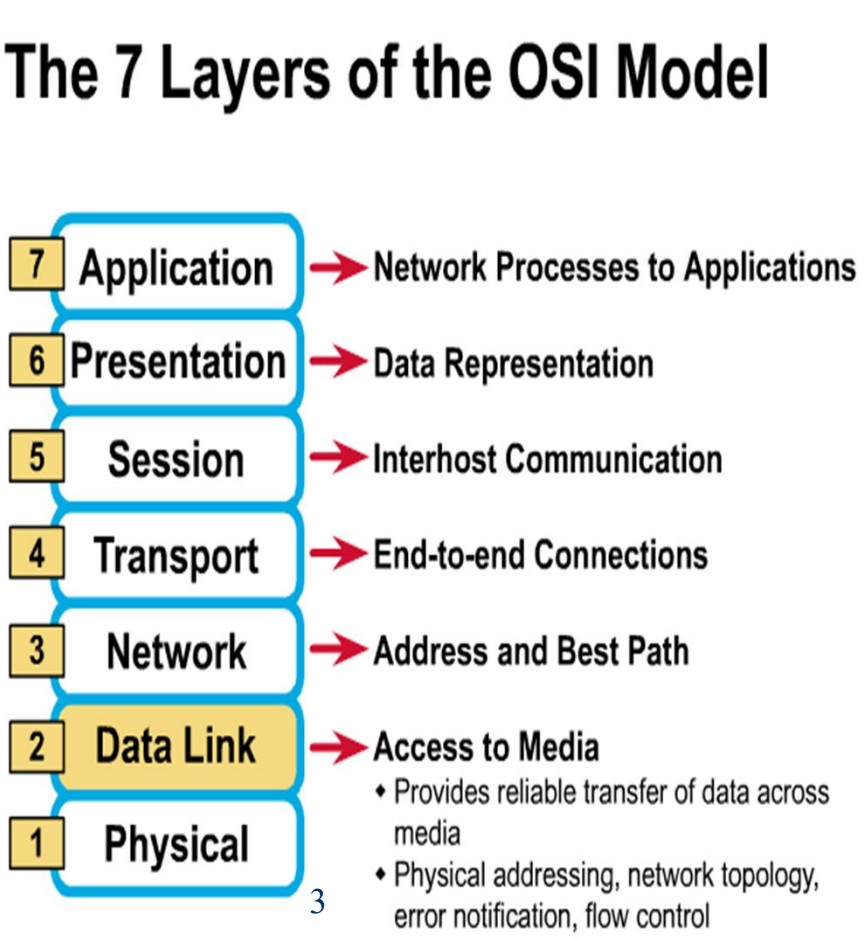
The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Network Addresses

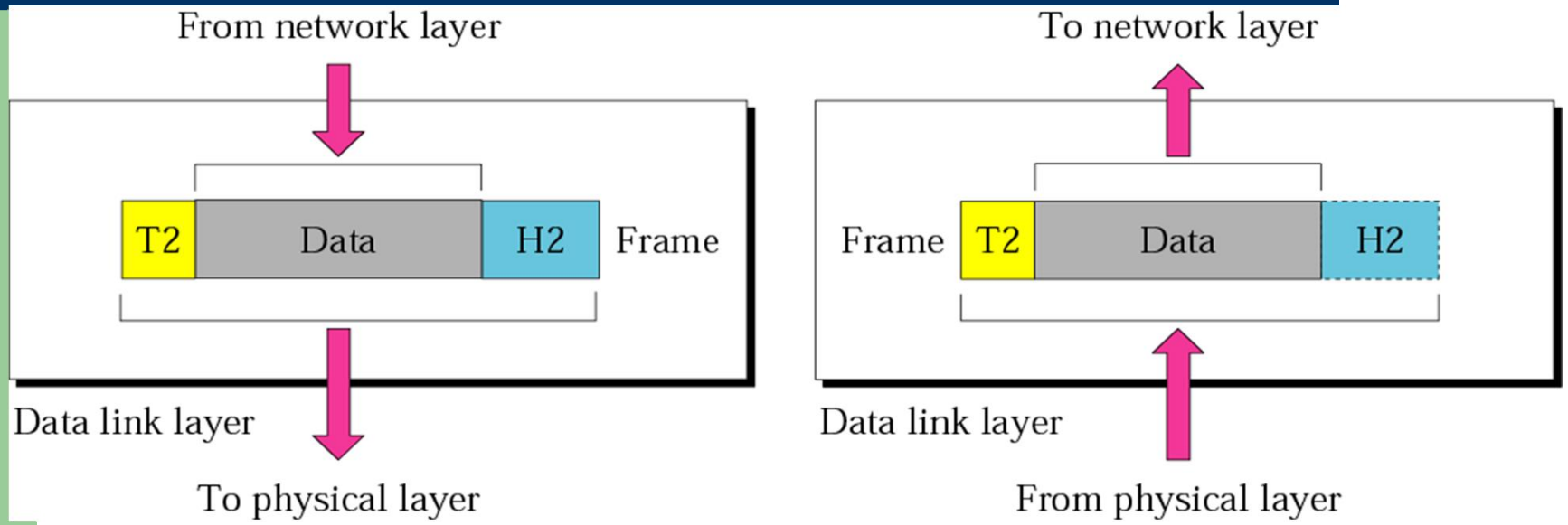
- Network-wide addresses
- Used to transfer data across subnets
- Used by routers for packet forwarding
- Example:
  - IP Address
- Where is it on my computer?
  - TCP/IP Software

Data Link Layer

- Places data and retrieves it from the physical layer and provides error detection capabilities



Data link layer



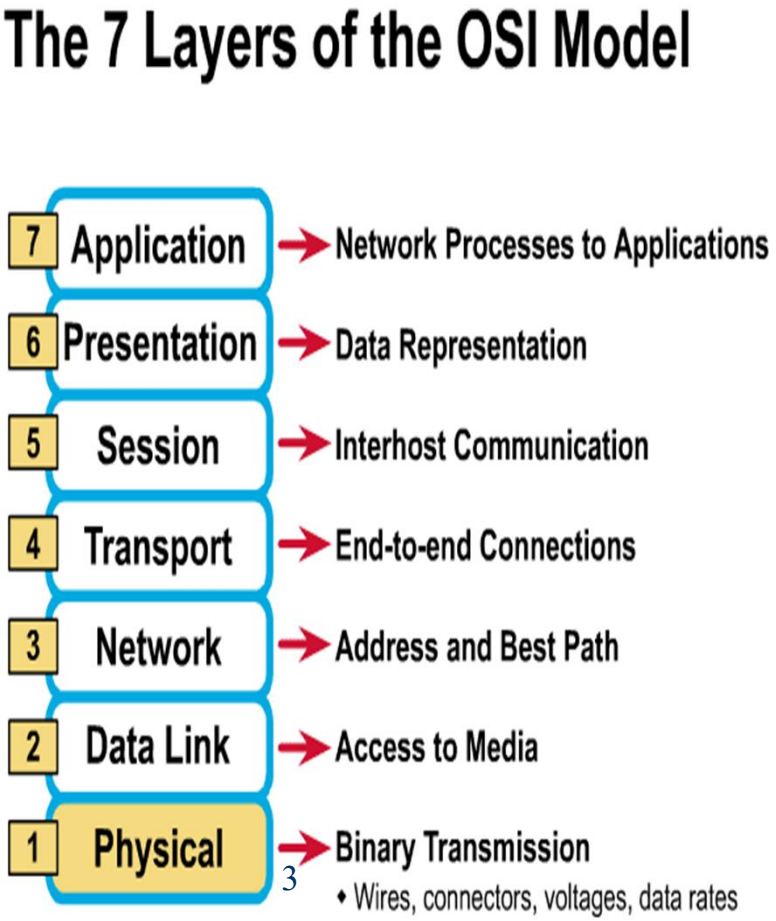
The data link layer is responsible for moving frames from one hop (node) to the next.

Sub-layers of the Data Link Layer

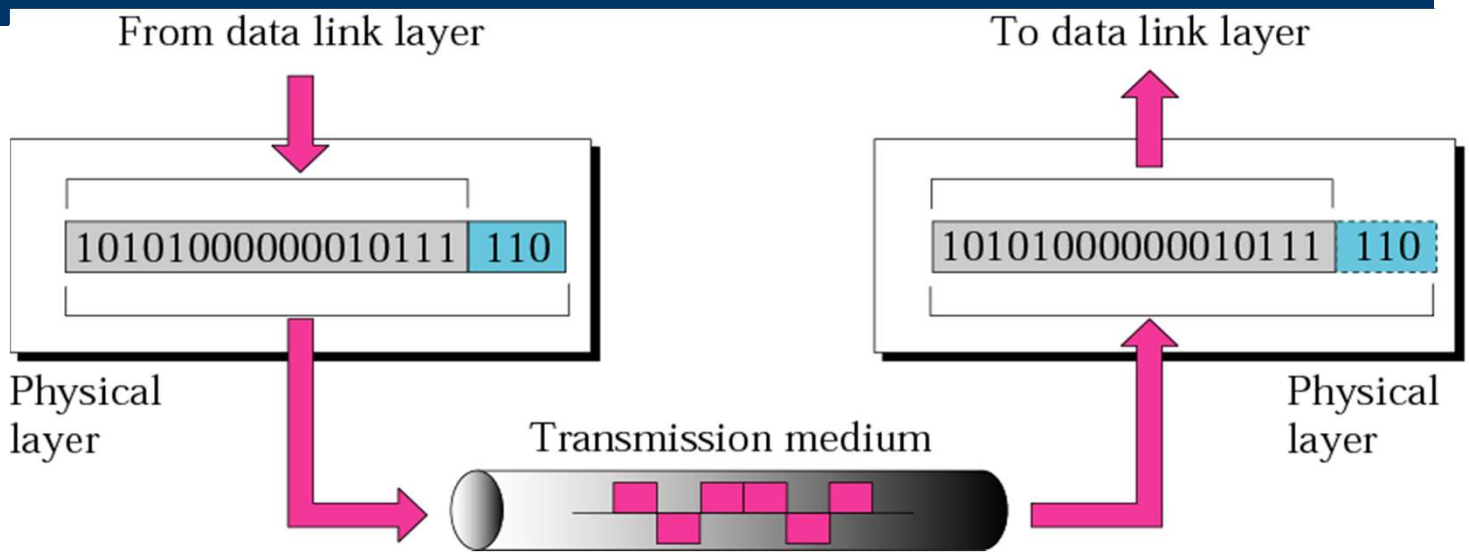
- MAC (Media Access Control)
  - Gives data to the NIC
  - Controls access to the media through:
    - CSMA/CD Carrier Sense Multiple Access/Collision Detection
    - Token passing
- LLC (Logical Link Layer)
  - Manages the data link interface (or Service Access Points (SAPs))
  - Can detect some transmission errors using a Cyclic Redundancy Check (CRC). If the packet is bad the LLC will request the sender to resend that particular packet.

Physical Layer

- Determines the specs for all physical components
  - Cabling
  - Interconnect methods (topology / devices)
  - Data encoding (bits to waves)
  - Electrical properties
- Examples:
  - Ethernet (IEEE 802.3)
  - Token Ring (IEEE 802.5)
  - Wireless (IEEE 802.11b)



Physical layer



The physical layer is responsible for the movement of individual bits from one hop (node) to the next.

Physical Layer (cont'd)

- What are the Physical Layer components on my computer?
- NIC
  - Network Interface Card
  - Has a unique 12 character Hexadecimal number permanently burned into it at the manufacturer.
  - The number is the MAC Address/Physical address of a computer
- Cabling
  - Twister Pair
  - Fiber Optic
  - Coax Cable

How Does It All Work Together

- Each layer contains a Protocol Data Unit (PDU)
  - PDU's are used for peer-to-peer contact between corresponding layers.
  - Data is handled by the top three layers, then Segmented by the Transport layer.
  - The Network layer places it into packets and the Data Link frames the packets for transmission.
  - Physical layer converts it to bits and sends it out over the media.
  - The receiving computer reverses the process using the information contained in the PDU.

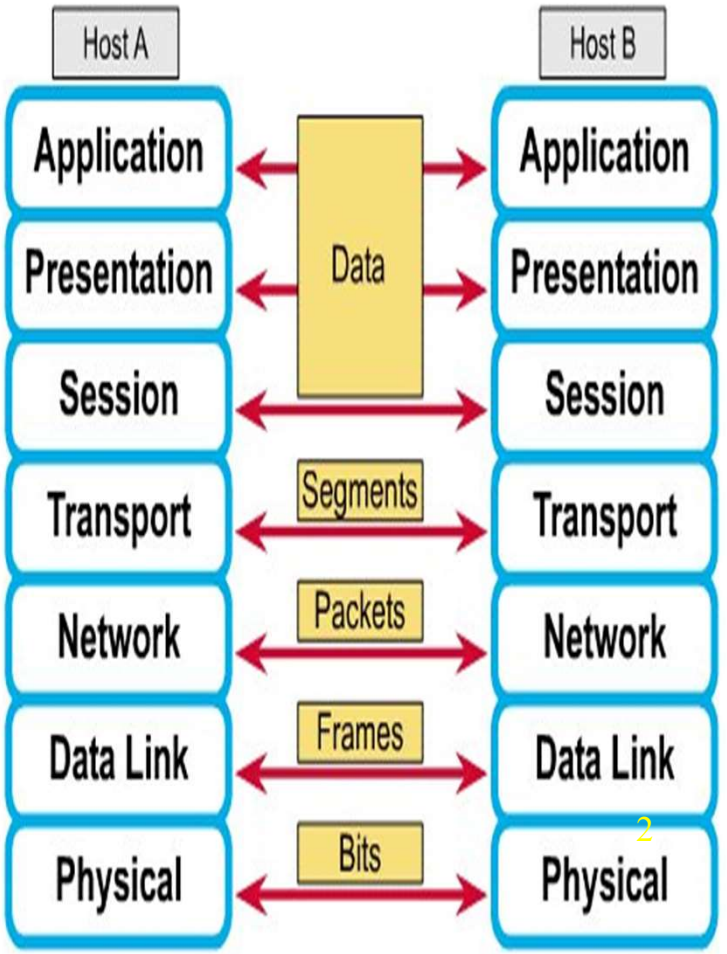
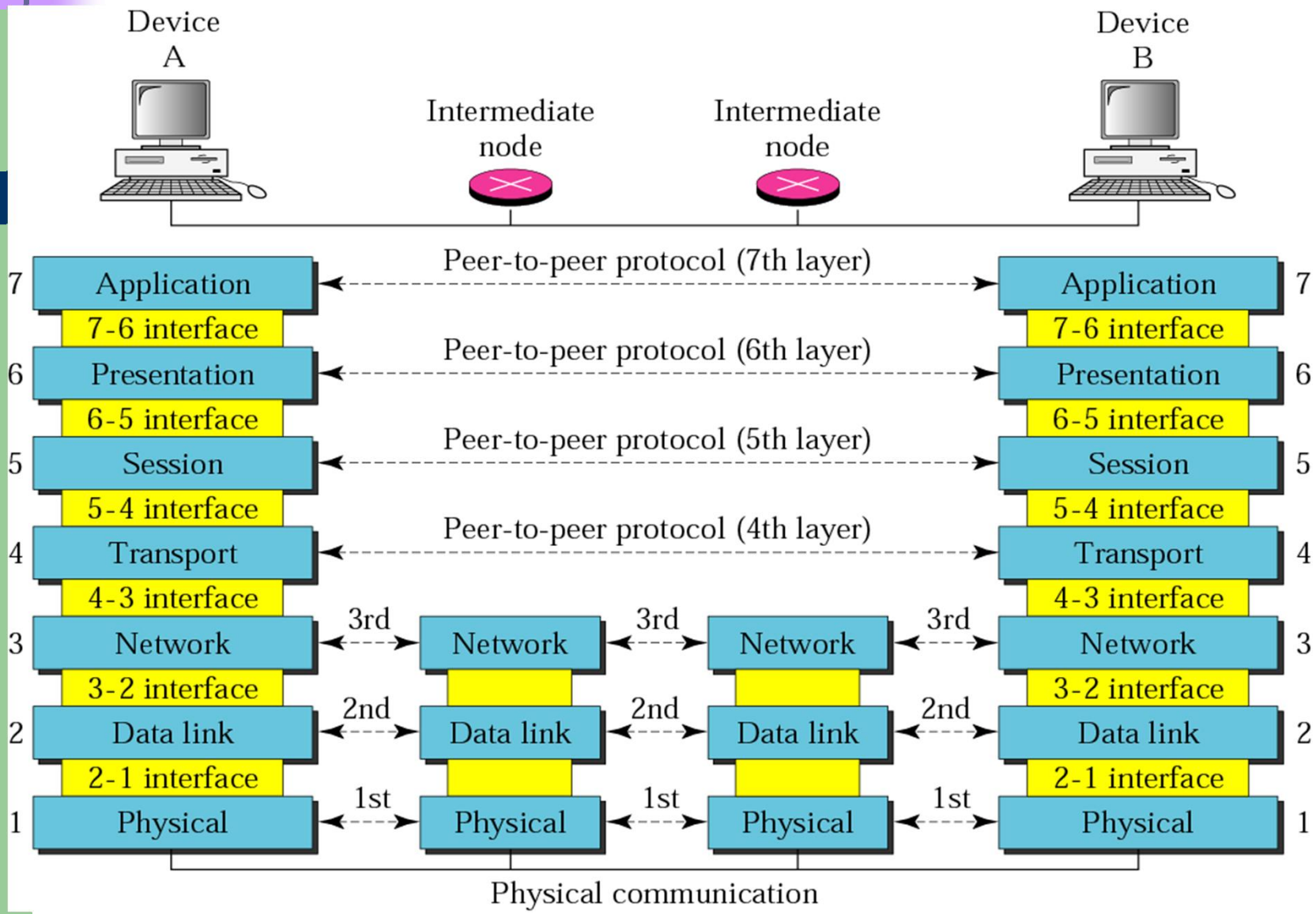


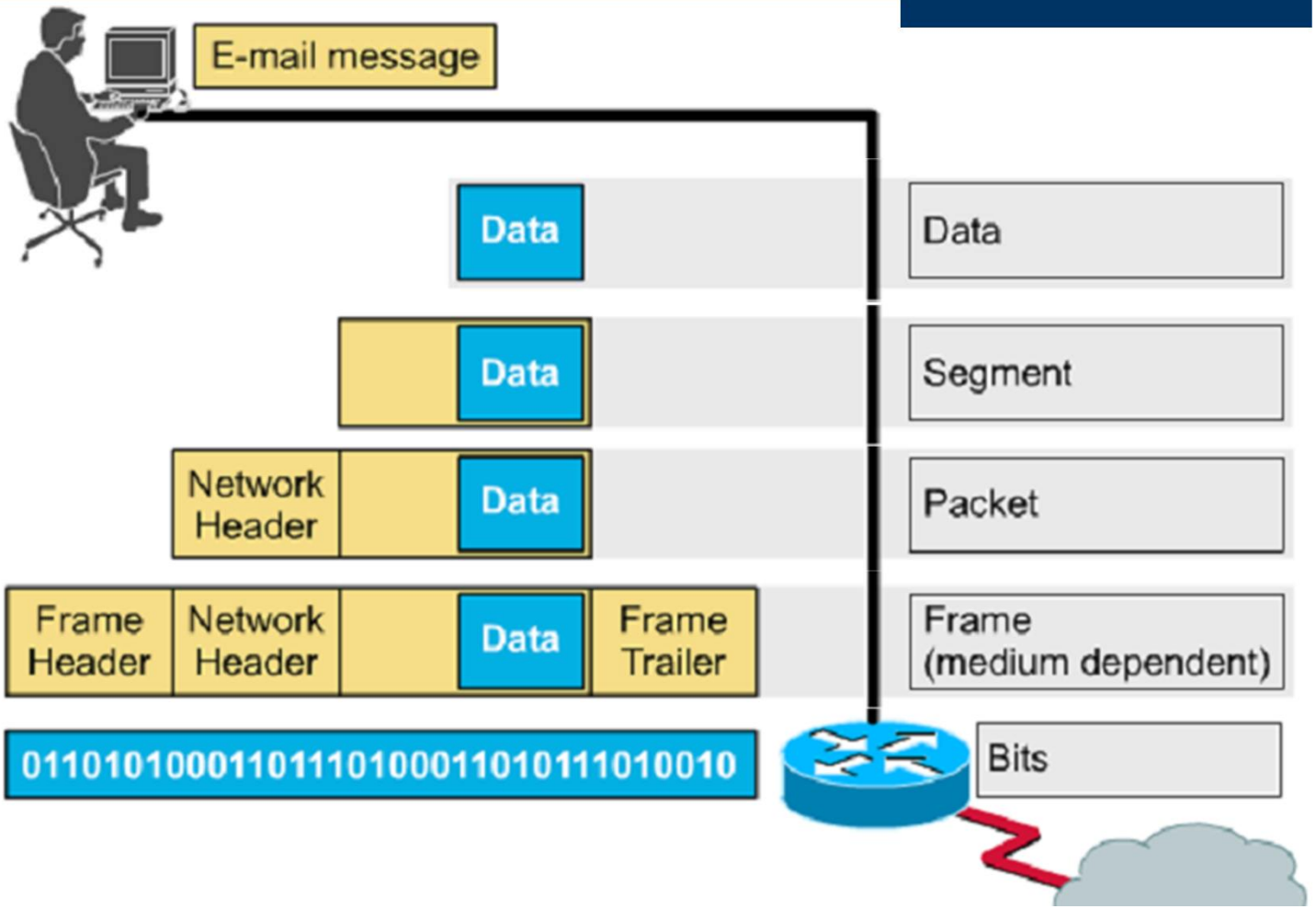
Figure 2.2 *OSI layers*



Data Encapsulation In TCP/IP

- At each layer in the TCP/IP protocol stack
    - Outgoing data is packaged and identified for delivery to the layer underneath
- PDU – Packet Data Unit – the “envelop” information attached to a packet at a particular TCP/IP protocol
    - e.g. header and trailer
- Header
    - PDU’s own particular opening component
    - Identifies the protocol in use, the sender and intended recipient
- Trailer (or packet trailer)
    - Provides data integrity checks for the payload

Encapsulation example: E-mail



Encapsulation

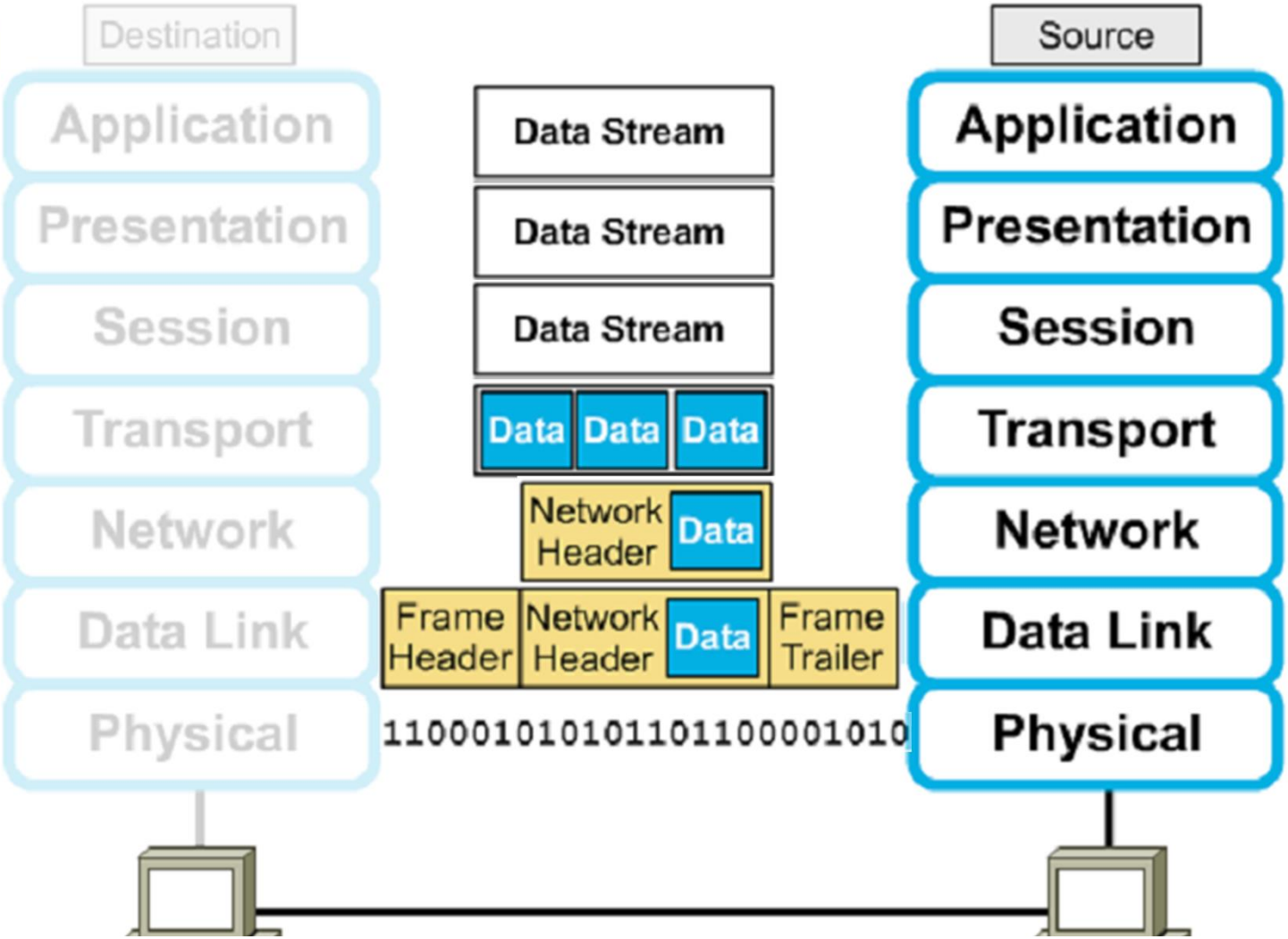


Figure 2.3 *An exchange using the OSI model*

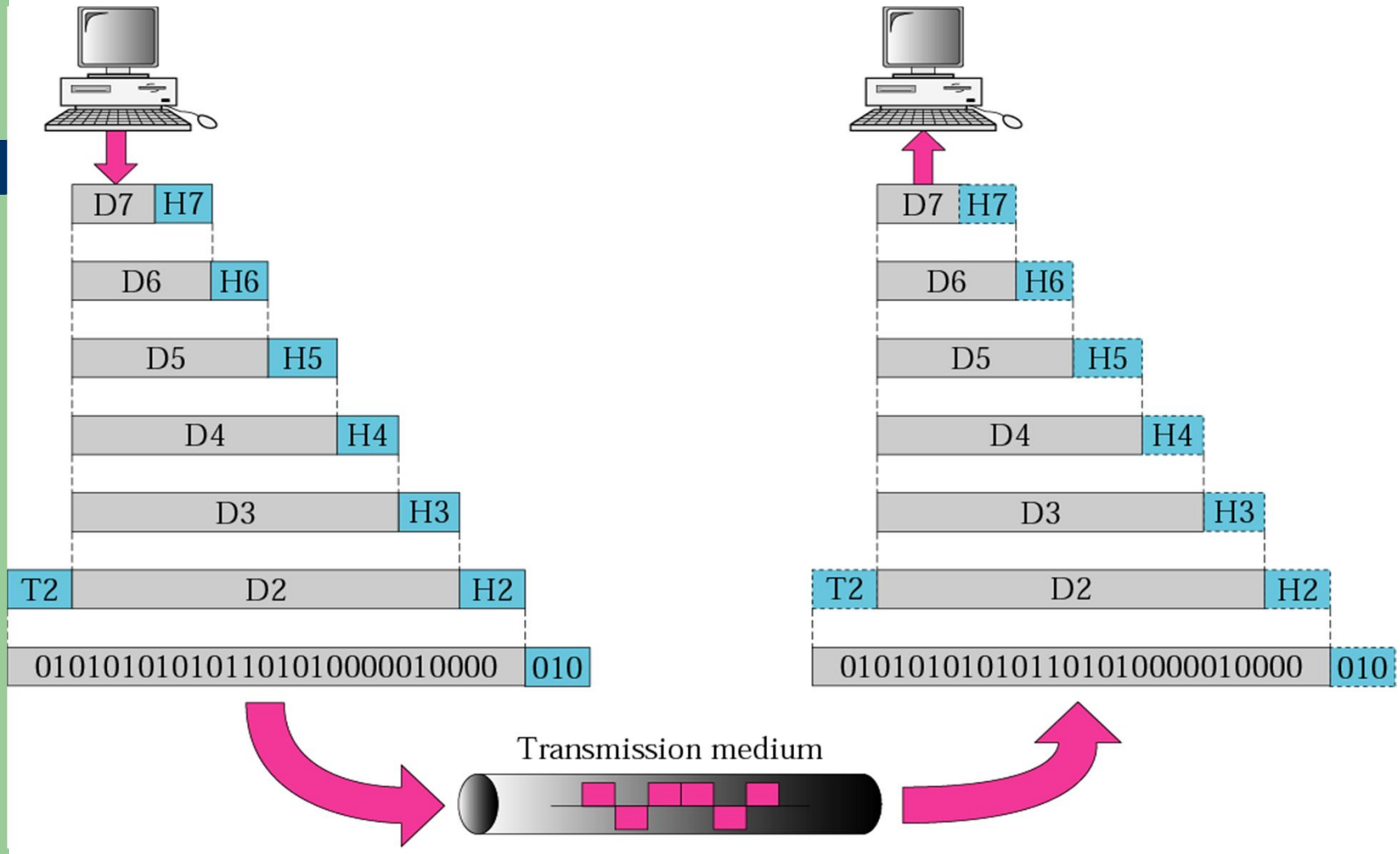
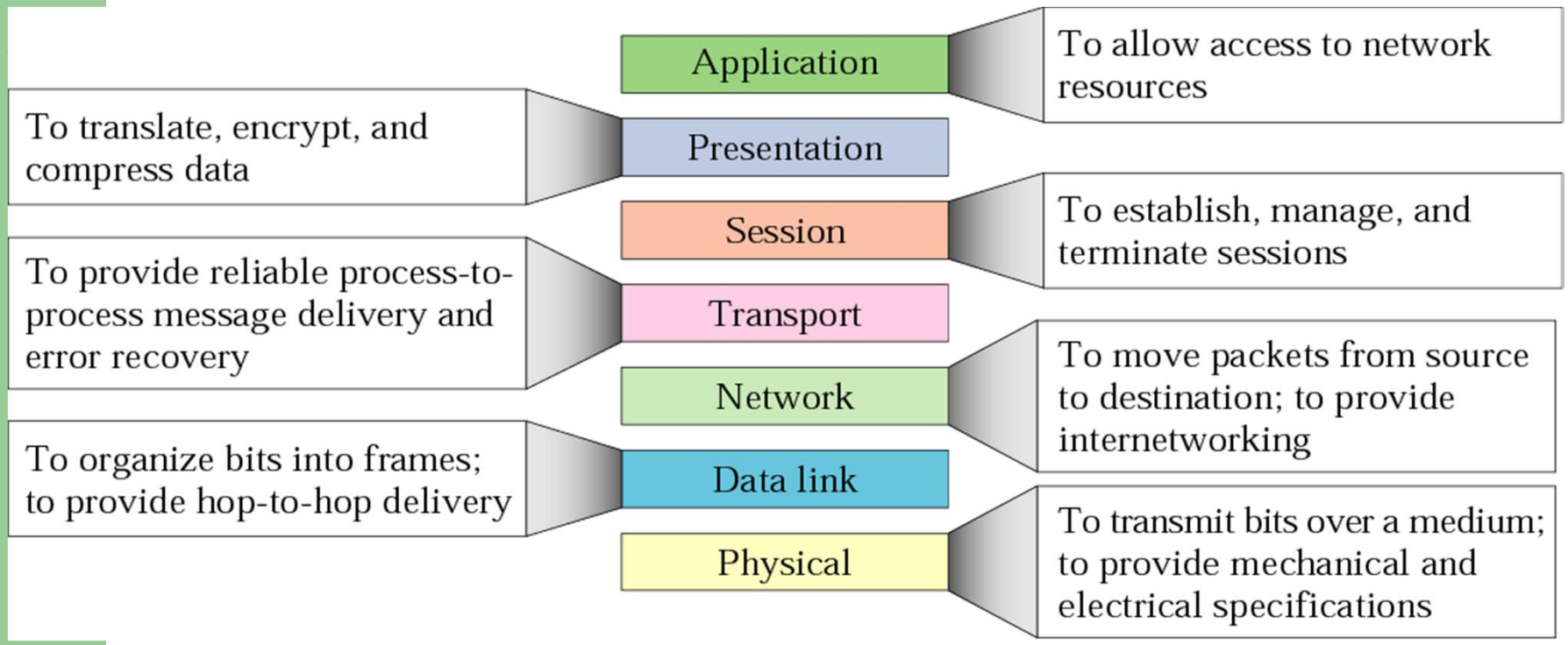


Figure 2.14 *Summary of layers*



The Postal Analogy

How would the OSI compare to the regular Post Office

- Application
- Presentation
- Session
- Transport
- Network
- Data-Link
- Physical

- **A-** Write a 20 page letter to a foreign country.
- **P-** Translate the letter so the receiver can read it.
- **S-** Insure the intended recipient can receive letter.
- **T-** Separate and number pages. Like registered mail, tracks delivery and requests another package if one is “lost” or “damaged” in the mail.
- **N-** Postal Center sorting letters by zip code to route them closer to destination.
- **D-** Local Post Office determining which vehicles to deliver letters.
- **P-** Physical Trucks, Planes, Rail, autos, etc which carry letter between stations.

Remembering the 7 Layers

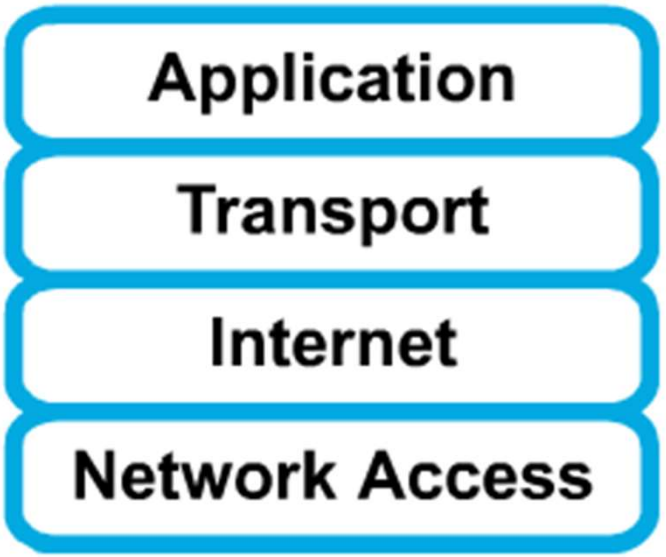
7 - **A**pplication	**A**ll
6 - **P**resentation	**P**eople
5 - **S**ession	**S**eem
4 - **T**ransport	**T**o
3 - **N**etwork	**N**eed
2 - **D**ata Link	**D**ata
1 - **P**hysical	**P**rocessing

TCP/IP model development

- The late-60s The Defense Advance Research Projects Agency (DARPA) originally developed Transmission Control Protocol/Internet Protocol (TCP/IP) to interconnect various defense department computer networks.
- The Internet, an International Wide Area Network, uses TCP/IP to connect networks across the world.

4 layers of the TCP/IP model

- Layer 4: Application
- Layer 3: Transport
- Layer 2: Internet
- Layer 1: Network access



It is important to note that some of the layers in the TCP/IP model have the same name as layers in the OSI model.
Do not confuse the layers of the two models.

The network access layer

- Concerned with all of the issues that an IP packet requires to actually make the physical link. All the details in the OSI physical and data link layers.
  - Electrical, mechanical, procedural and functional specifications.
  - Data rate, Distances, Physical connector.
  - Frames, physical addressing.
  - Synchronization, flow control, error control.

The internet layer

- Send source packets from any network on the internetwork and have them arrive at the destination independent of the path and networks they took to get there.
  - Packets, Logical addressing.
  - Internet Protocol (IP).
  - Route , routing table, routing protocol.

The transport layer

- The transport layer deals with the quality-of-service issues of reliability, flow control, and error correction.
  - Segments, data stream, datagram.
  - Connection oriented and connectionless.
  - Transmission control protocol (TCP).
  - User datagram protocol (UDP).
  - End-to-end flow control.
  - Error detection and recovery.

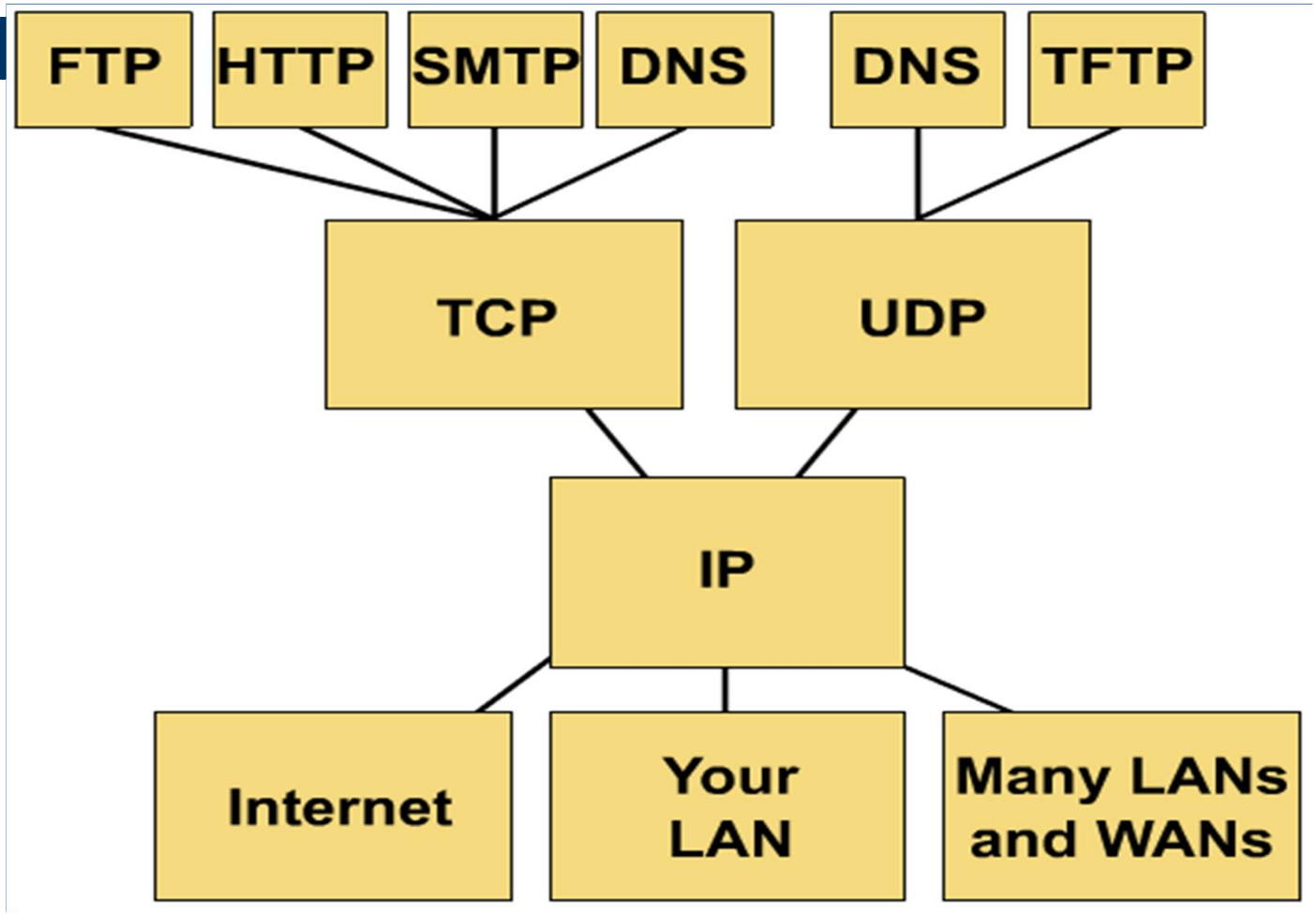
TCP/IP Reference Model (cont)

- 3. Transport layer (layer 3)
  - Allows end-to-end communication
  - Connection establishment, error control, flow control
  - Two main protocols at this level
    - Transmission control protocol (TCP),
      - Connection oriented
        - Connection established before sending data
        - Reliable
    - user datagram protocol (UDP)
      - Connectionless
        - Sending data without establishing connection
        - Fast but unreliable
-

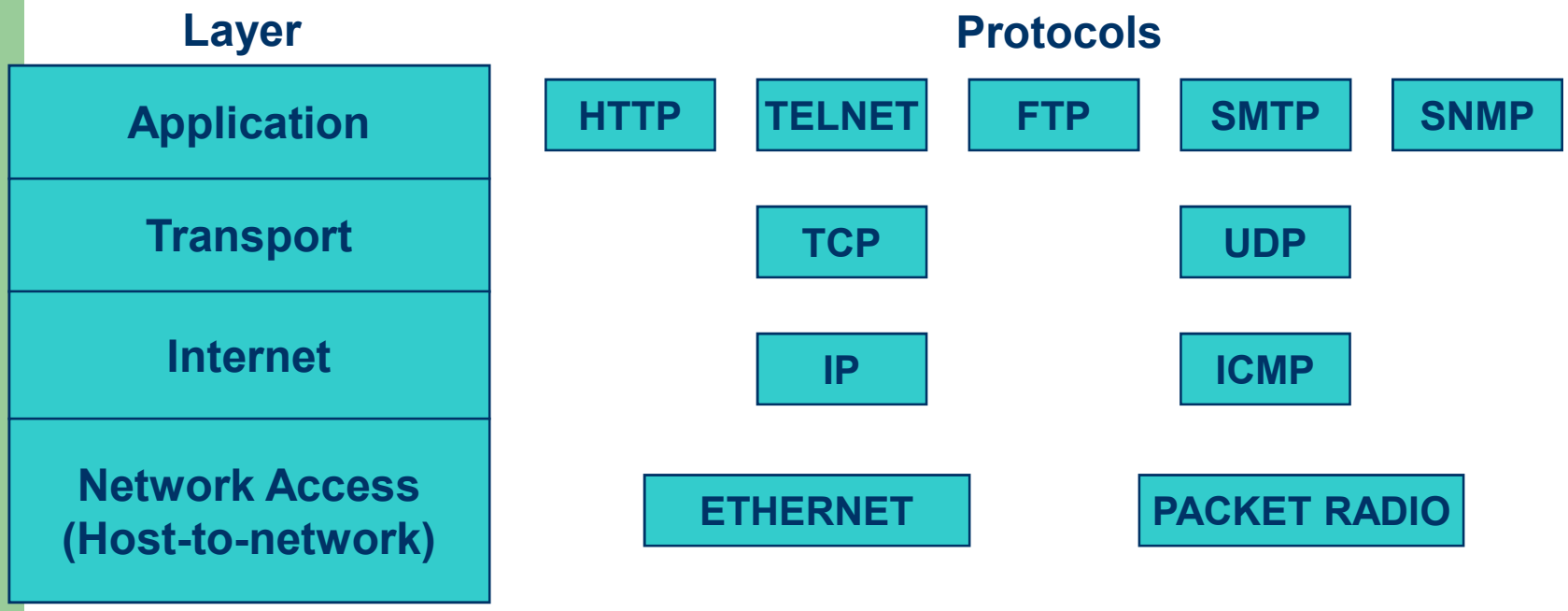
The application layer

- Handles high-level protocols, issues of representation, encoding, and dialog control.
- The TCP/IP combines all application-related issues into one layer, and assures this data is properly packaged for the next layer.
  - FTP, HTTP, SMNP, DNS ...
  - Format of data, data structure, encode …
  - Dialog control, session management …

TCP/IP protocol stack



TCP/IP Reference Model



Protocols at the application layer

- HTTP:
  - browser and web server communicatin
- FTP :
  - file transfer protocol
- TELNET:
  - remote login protocol
- POP3: Retrieve email
  - POP3 is designed to delete mail on the server as soon as the user has downloaded it
- IMAP (Internet Message Access Protocol)
  - Retrieve emails,
  - retaining e-mail on the server and for organizing it in folders on the serve

Protocols at the transport layer

- Transmission control protocol (TCP),
  - Connection oriented
    - Connection established before sending data
    - Reliable
- user datagram protocol (UDP)
  - Connectionless
    - Sending data without establishing connection
    - Fast but unreliable

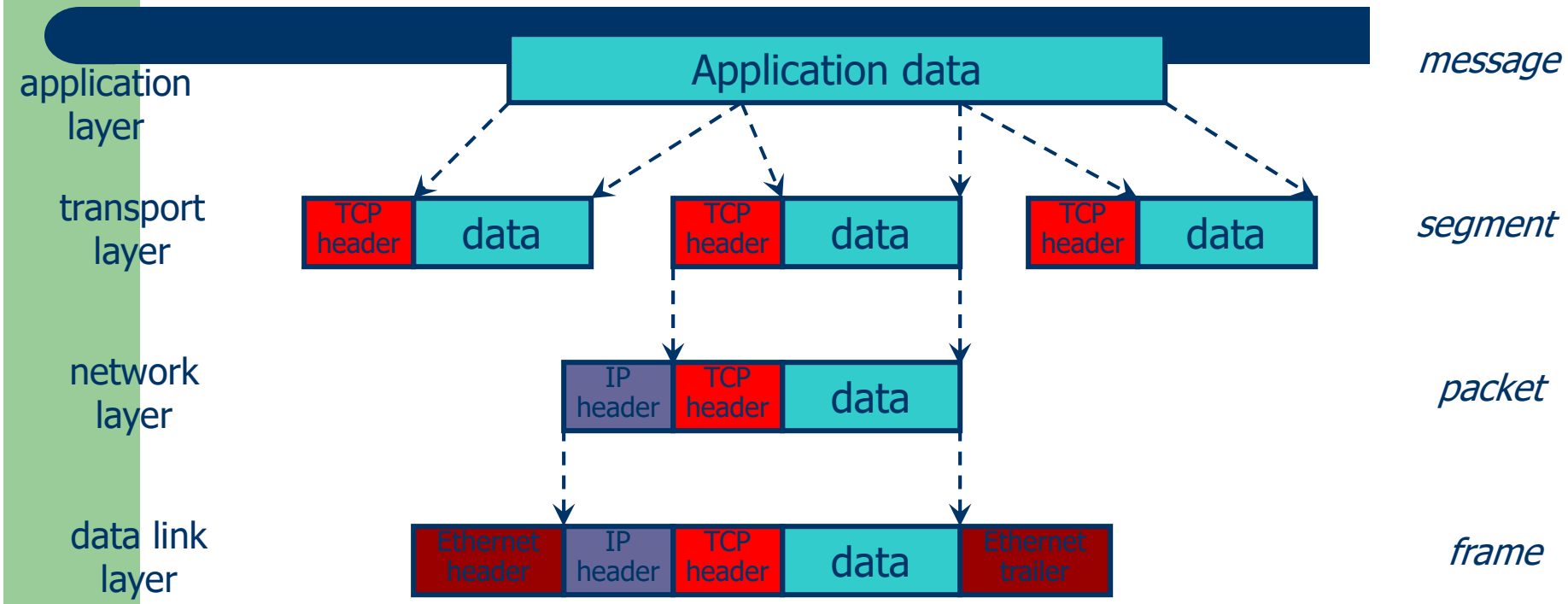
Protocol at the network layer

- IP
  - Path selection ,
  - routing and addressing
- ICMP (Internet Control Message Protocol)
  - sends error messages relying on IP
    - a requested service is not available
    - a host or router could not be reached

Protocols at the link layer

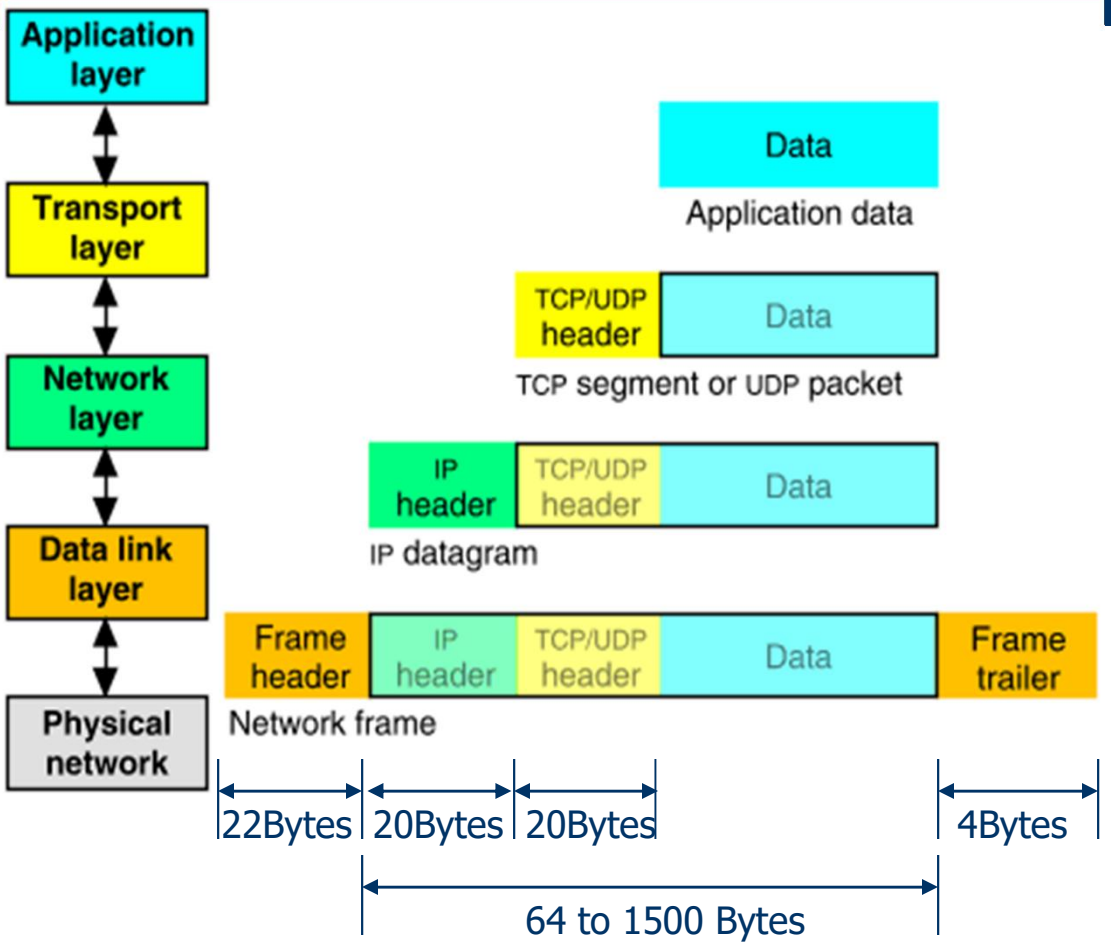
- Ethernet
  - Uses CSMA/CD
- Token Ring

Data Formats

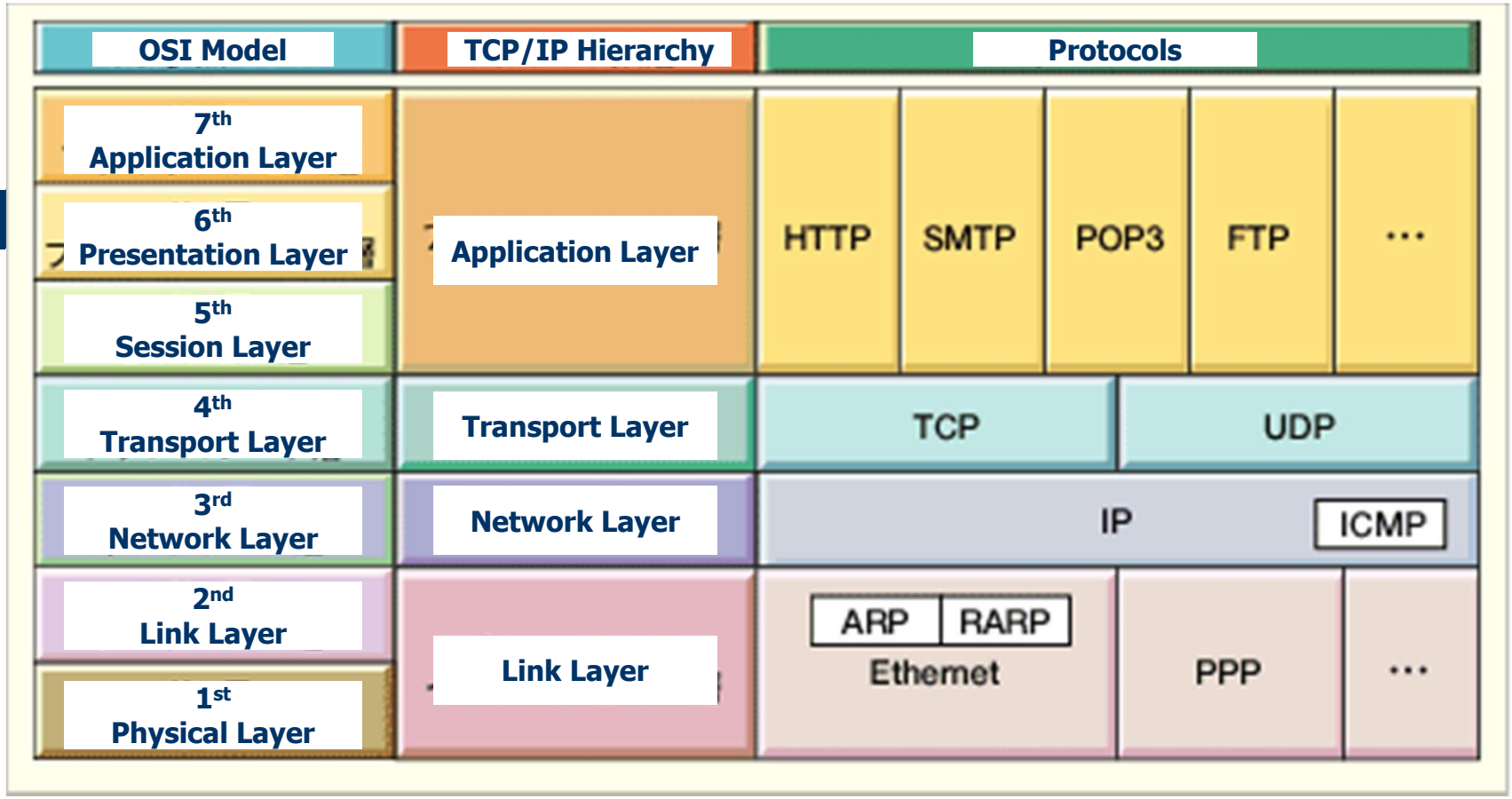


Packet Encapsulation (TCP/IP)

- The data is sent down the protocol stack
- Each layer adds to the data by prepending headers



Comparing TCP/IP with OSI



Link Layer : includes device driver and network interface card
Network Layer : handles the movement of packets, i.e. Routing
Transport Layer : provides a reliable flow of data between two hosts
Application Layer : handles the details of the particular application

How the OSI and TCP/IP Models Relate in a Networking Environment

OSI Model Layer	OSI Model Name	Pneumonic	Equipment	Equipment Purpose	Data	Protocols	Words to Remember	TCP/IP Model
Layer 7	**A**pplication	**A**ll	Computer	Regular Computer or A Special Gateway. Used to combine networks using different communication protocols	**D**ata	Redirector, FTP, Telnet, SMTP, SNMP, Netware Core	Browsers	Application
Layer 6	**P**resentation	**P**eople					Common Data Format	Application
Layer 5	**S**ession	**S**eem				NFS, SQL, RPC, X-Win	Dialogues and Conversations	Application
Layer 4	**T**ransport	**T**o	Computer		**S**egment	TCP and UDP	Quality of Service, and Reliability	Transport
Layer 3	**N**etwork	**N**eed	Router	Segment Network into Smaller ***Broadcast*** Domains	**P**acket	Routable Protocols. (IP, IPX, AppleTalk)	Path Selection, Routing, and Addressing	Internet
Layer 2	**D**ata Link -MAC -LLC	**D**ata	Bridge (2 Ports) or Switch and NIC	Segment Network into Smaller ***Collision*** Domains	**F**rame	NDIS, ODI, MAC Address, Ether Talk	Frames and Media Access Control (MAC)	Network Access
Layer 1	**P**hysical	**P**rocessing	Repeater, Hub (Multi-port), Cabling	One Collision AND One Broadcast Domain	**B**it	Physical	Signals and Media	Network Access

Internet applications

- TCP/IP takes care of the hard problems
  - Location of the destination host
  - Making sure the data is received in the correct order and error free
- Coding Internet applications
  - Turns out to be straightforward.
- The key concept of Internet programming is
  - The client-server model

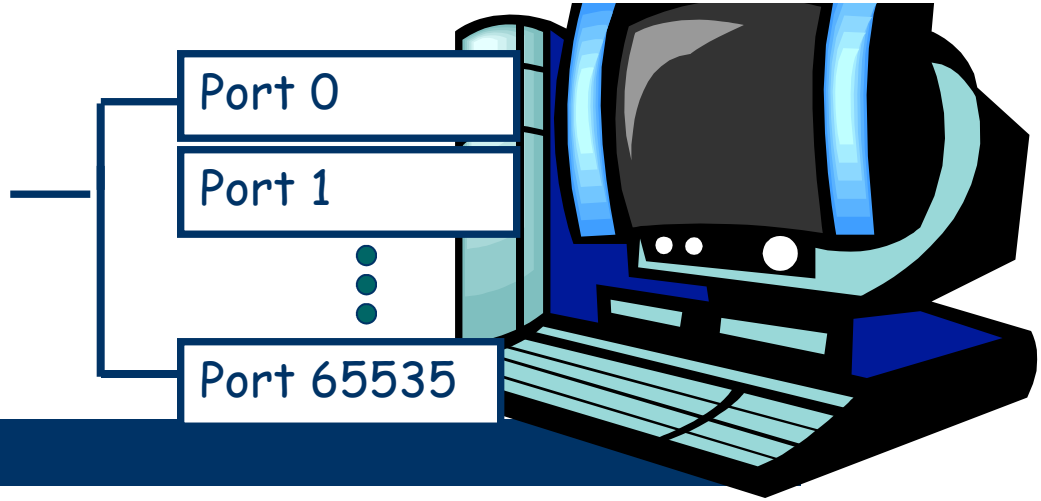
Client-Server model

- Client and server processes operate on machines which are able to communicate through a network:
  - The Server waits for requests from client
  - When a request is received
  - The server lookup for the requested data
  - And send a response the client
- Sockets and ports
  - A socket is and end-point of way communication link between two programs
  - A port number bound to a socket specifies the protocol need the be used at the receiving end
- Example of servers
  - File servers
  - Web servers
- Example of client applications
  - Browsers
  - Email clients

What is a socket?

- An interface between application and network.
  - Create a socket
    - Socket(Protocolfamily, type-of-communicatio, specific- protocol);
  - The application creates a socket
  - The socket *type* dictates the style of communication
    - reliable vs. best effort
    - connection-oriented vs. connectionless

Ports



- Each host has 65,536 ports
  - 20,21: FTP
  - 23: Telnet
  - 80: HTTP
- A socket provides an interface to send data to/from the network through a port

Protocols

- For a great graphic of protocol stacks in relationship to the OSI model, visit http://www.lex-con.com/osimodel.htm
- For more information on the OSI model, including an animated graphic and various protocol information, visit http://www.certyourself.com/OSIguide.shtml

Subnetting

- Subnetting is the process of stealing bits from the HOST part of an IP address in order to divide the larger network into smaller sub-networks called subnets. After subnetting, we end up with NETWORK SUBNET HOST fields. We always reserve an IP address to identify the subnet and another one to identify the broadcast subnet address. Here are three reasons why you may want to use subnetting:
-
- Conservation of IP addresses: Imagine having a network of 20 hosts. Using a Class C network will waste a lot of IP addresses (254-20=234). Breaking up large networks into smaller parts would be more efficient and would conserve a great amount of addresses.
- Reduced network traffic: The smaller networks that created the smaller broadcast domains are formed, hence less broadcast traffic on network boundaries.
- Simplification: Breaking large networks into smaller ones could simplify fault troubleshooting by isolating network problems down to their specific existence.

Supernetting

Supernetting is the procedure of combine the small networks into larger space. In subnetting, Network addresses's bits are increased. on the other hand, in subnetting, Host addresses's bits are increased. Subnetting is implemented via Variable-length subnet masking, While supernetting is implemented via Classless interdomain routing.

Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.

Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

More specifically,

When multiple networks are combined to form a bigger network, it is termed as super-netting

Super netting is used in route aggregation to reduce the size of routing tables and routing table updates

- There are some points which should be kept in mind while supernetting:
- All the Networks should be contiguous.
- The block size of every networks should be equal and must be in form of 2^n.
- First Network id should be exactly divisible by whole size of supernet.

Difference between Subnetting and Supernetting

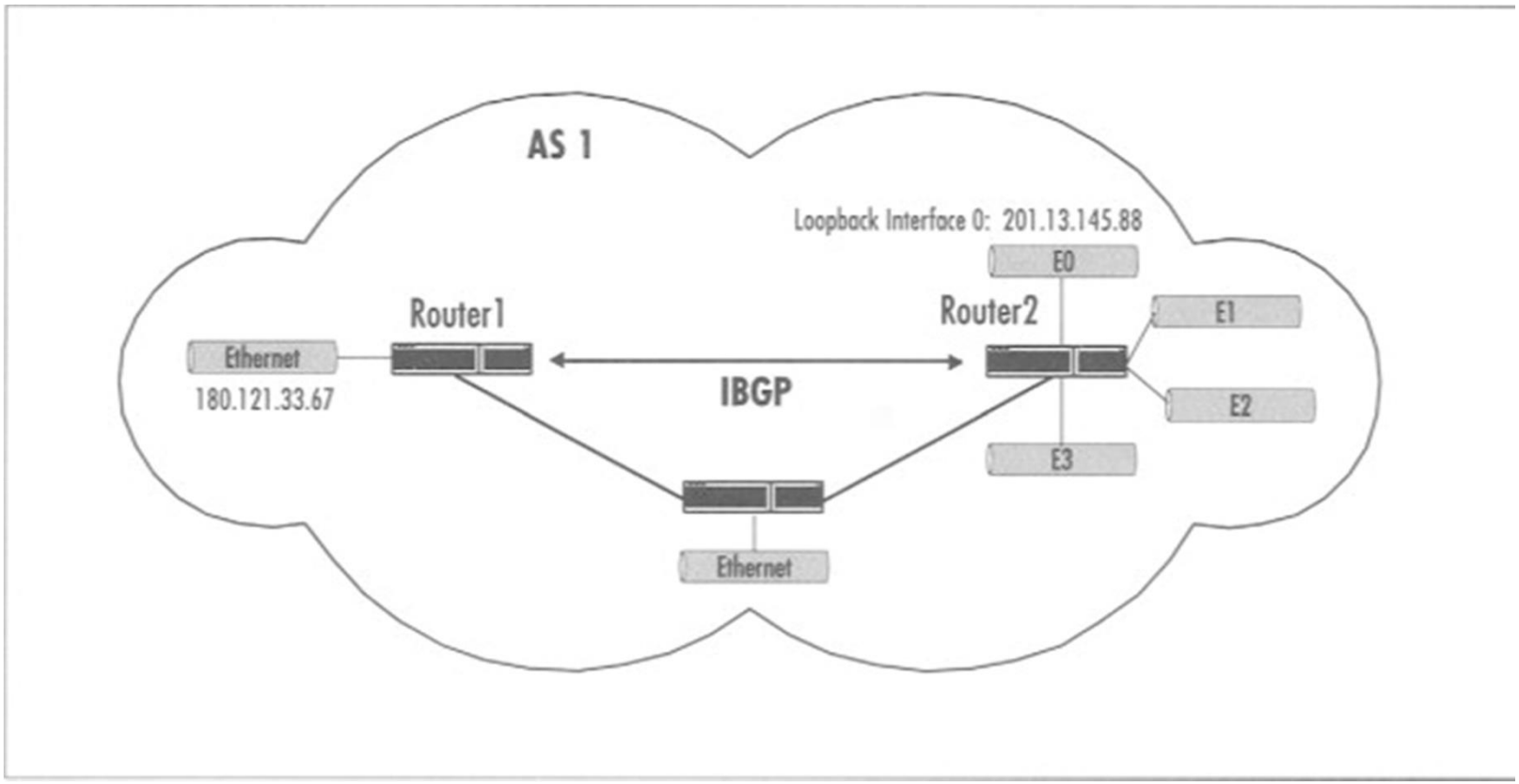
S.NO	SUBNETTING	SUPERNETTING
1.	Subnetting is the procedure to divide the network into sub-networks.	While supernetting is the procedure of combine the small networks.
2.	In subnetting, Network addresses's bits are increased.	While in subnetting, Host addresses's bits are increased.
3.	In subnetting, The mask bits are moved towards right.	While In supernetting, The mask bits are moved towards left.
4.	Subnetting is implemented via Variable-length subnet masking.	While supernetting is implemented via Classless interdomain routing.
5.	In subnetting, Address depletion is reduced or removed.	While It is used for simplify routing process.

Loop back concept

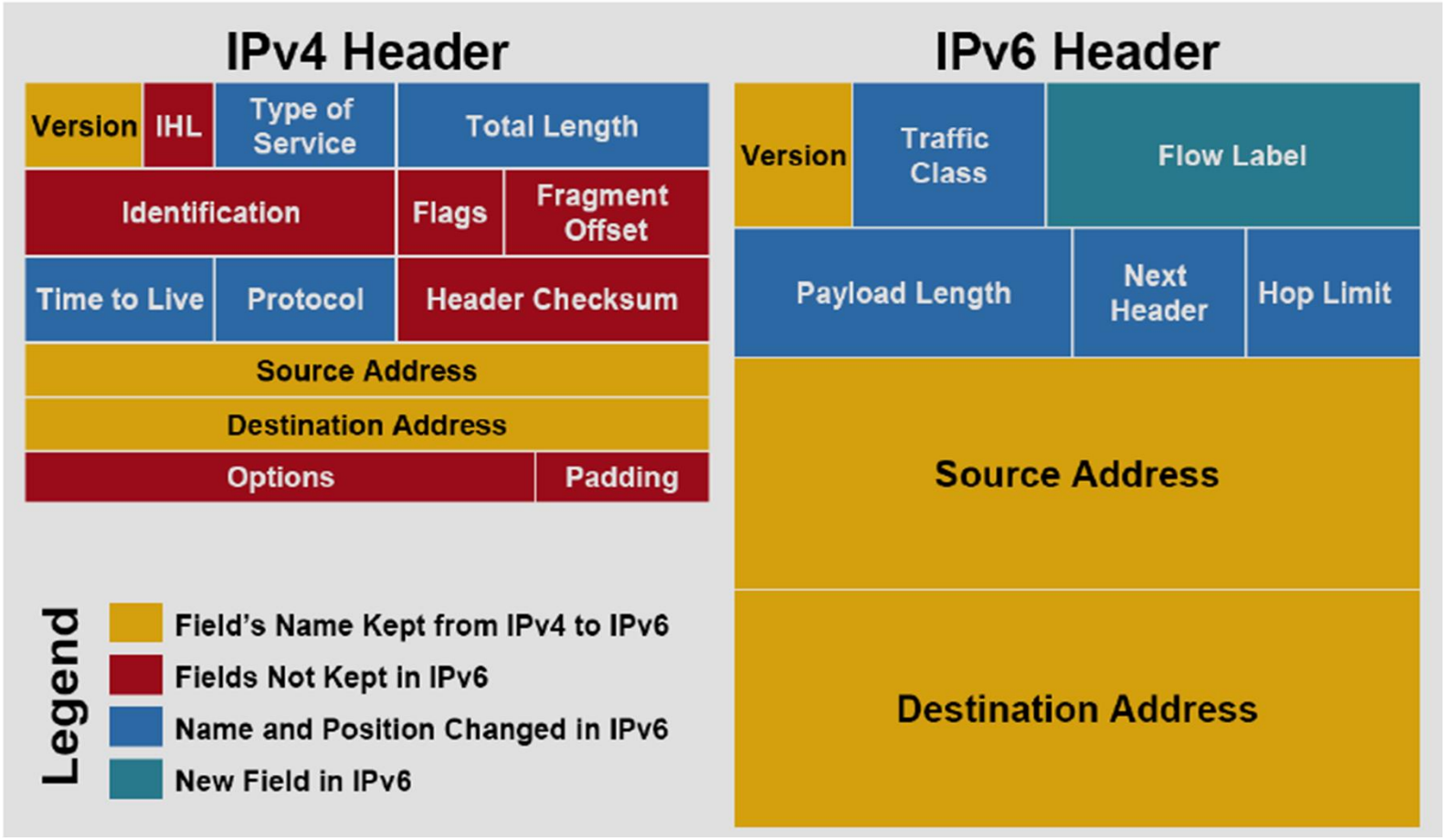
is the routing of electronic signals, digital data streams, or flows of items back to their source without intentional processing or modification. It is primarily a means of testing the communications infrastructure.

There are many example applications. It may be a communication channel with only one communication endpoint. Any message transmitted by such a channel is immediately and only received by that same channel. In telecommunications, loopback devices perform transmission tests of access lines from the serving switching center, which usually does not require the assistance of personnel at the served terminal. Loop around is a method of testing between stations that are not necessarily adjacent, wherein two lines are used, with the test being done at one station and the two lines are interconnected at the distant station. A patch cable may also function as loopback, when applied manually or automatically, remotely or locally, facilitating a loop-back test.

Loop back concept



IPV4 and IPV6 packet Format



Configuring IPv4 or IPv6 Routing

Click Network and Sharing Center on your computer. Click Local Area Connections and then click Properties to **configure** network addresses and other information. Click the Networking tab and then, click either Internet Protocol Version 4 (TCP/**IPv4**) or Internet Protocol Version 6 (TCP/**IPv6**) and then click Properties.

Thank You

Computer Network
Chapter 4
Cables and Connectors

Prepared By :

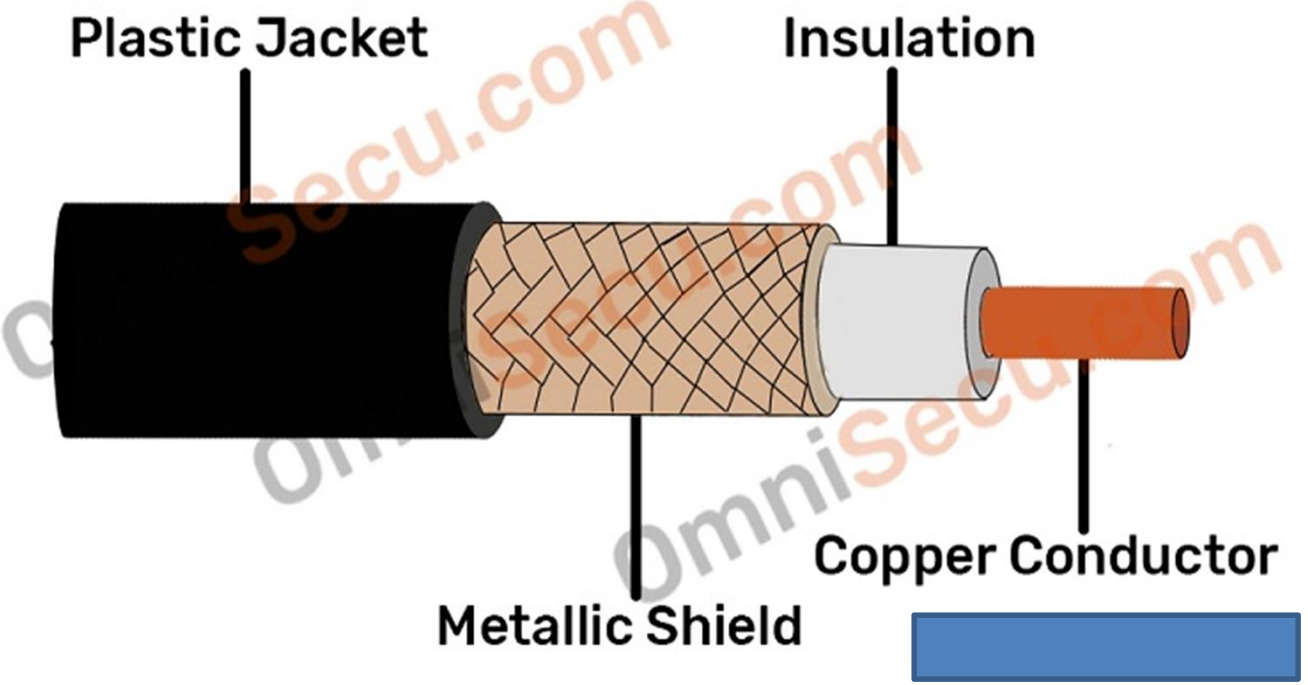
Patanjali
Lecturer in ECE
Govt. Polytechnic Jhajjar

Cables Used in Networking

Coaxial Cables

Coaxial cable looks similar to the cable used to carry TV signal. A solid-core copper wire conductor runs down the middle of the cable. Around that solid-core copper wire is a layer of insulation, and covering that insulation is braided wire and metal foil shield, which shields against electromagnetic interference. A final layer of plastic insulation jacket covers the braided wire.

Following image shows the general structure of coaxial cable.



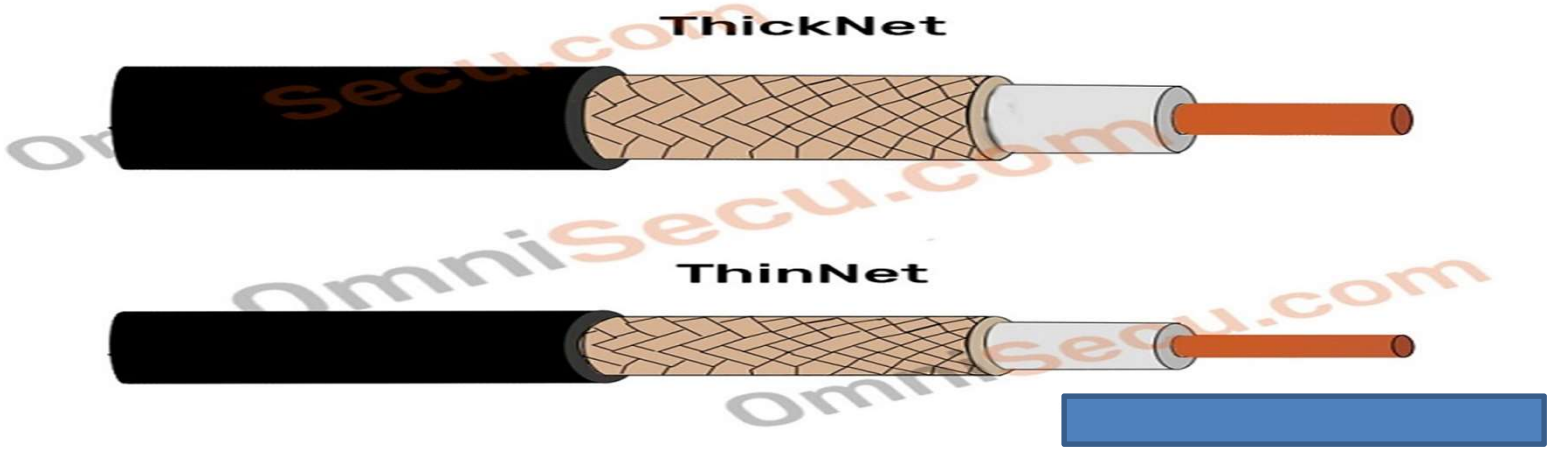
There are two types of coaxial cabling: Thin Net and Thick Net. Thin Net is a flexible coaxial cable about ¼ inch thick. Thin Net is used for short-distance. Thin Net connects directly to a workstation's network adapter card using a British Naval Connector (BNC). The maximum length of thin net is 185 to 200 meters. Thick Net coaxial cable is thicker cable than Thin Net. Thick Net cable is about ½ inch thick and can support data transfer over longer distances than Thin Net. Thick Net has a maximum supported cable length of 500 meters and usually is used as a backbone to connect several smaller Thin Net-based networks. here are two Ethernet media standards defined for coaxial cable-based Ethernet. Those standards are 10Base2 and 10Base5.

10Base2 has a bandwidth speed of 10 Mbps, to a maximum distance of 200 meters. 10 denotes bandwidth speed and 2 denotes 200 meters. Base denotes **baseband type of signal.** Coaxial cable used for 10Base2 Ethernet media standard is Thin Net.

10Base5 has a bandwidth speed of 10 Mbps, to a maximum distance of 500 meters. 10 denotes bandwidth speed and 5 denotes 500 meters. Base denotes **baseband type of signal**. Coaxial cable used for 10Base5 Ethernet media standard is ThickNet.

The bandwidth available for both 10Base2 (Thin net Ethernet) and 10Base5 (Thick net Ethernet) were 10 Mbps (Megabits per second).

Type of Cable used to wire **Local Area Networks (LAN)** these days is Twisted Pair cable. It is extremely difficult to find a live business network using coaxial cable.



Twisted Pair Cables

Twisted-pair cable is the most common type of cabling you can see in today's **Local Area Networks (LAN)** networks. A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk. Crosstalk is the undesired signal noise generated by the electromagnetic fields of the adjacent wires.

When a wire is carrying a current, the current creates a magnetic field around the wire. This field can interfere with signals on nearby wires. To eliminate this, pairs of wires carry signals in opposite directions, so that the two magnetic fields also occur in opposite directions and cancel each other out. This process is known as cancellation.

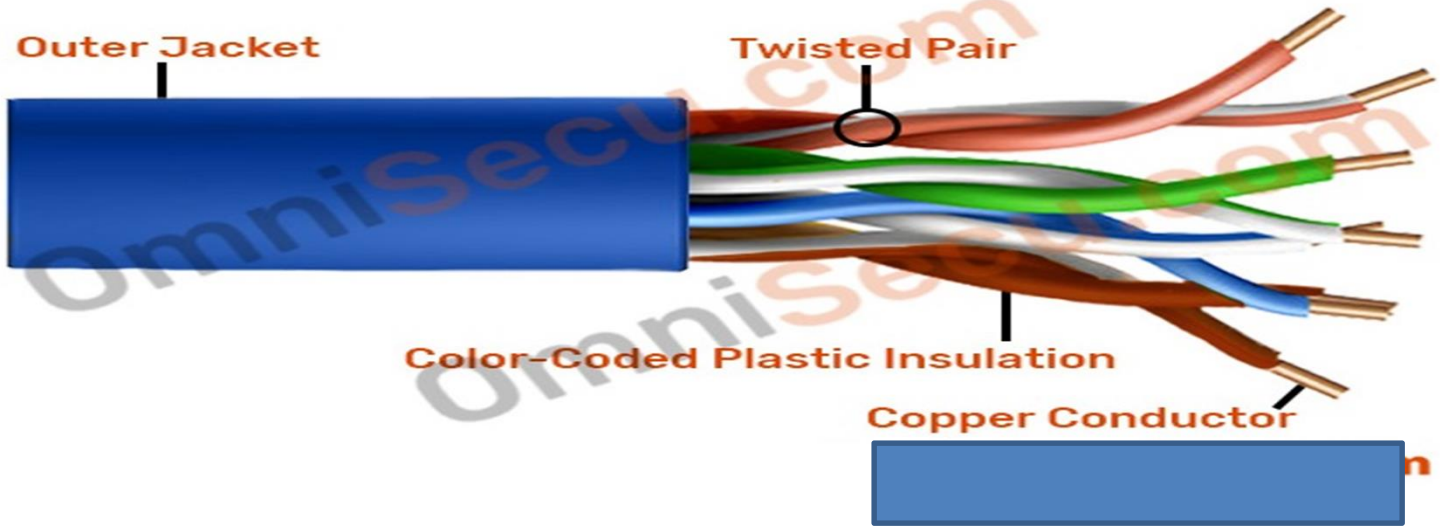
Color codes used for Twisted Pair wire’s plastic insulation are Orange, Orange-White, Blue, Blue-White, Green, Green-White, Brown and Brown-White.

Two types of twisted pair cables are Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP).

Unshielded Twisted Pair (UTP) cables

Unshielded Twisted Pair (UTP) cable is the most common networking media. Unshielded Twisted Pair (UTP) consists of four pairs of thin, copper wires covered in color-coded plastic insulation that are twisted together. The wire pairs are then covered with a plastic outer jacket. UTP cables are of small diameter and it doesn’t need grounding. Since there is no shielding for UTP cabling, it relies only on "cancellation" to avoid noise.

Following image shows Unshielded Twisted Pair (UTP) cable.



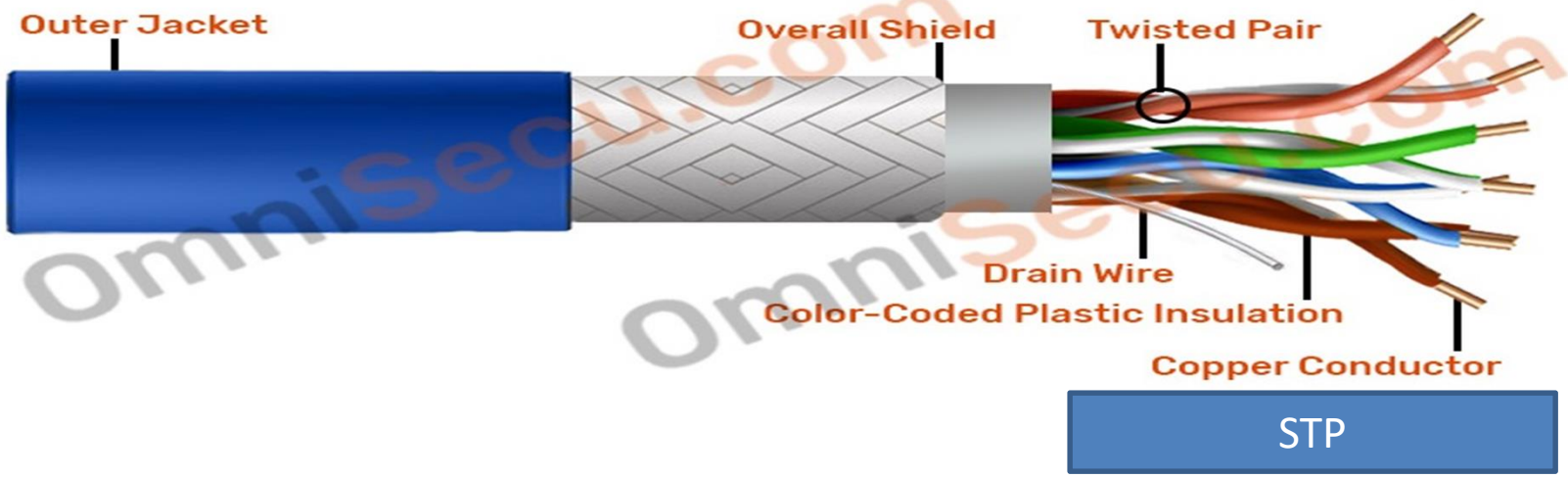
Shielded Twisted Pair (STP) cables

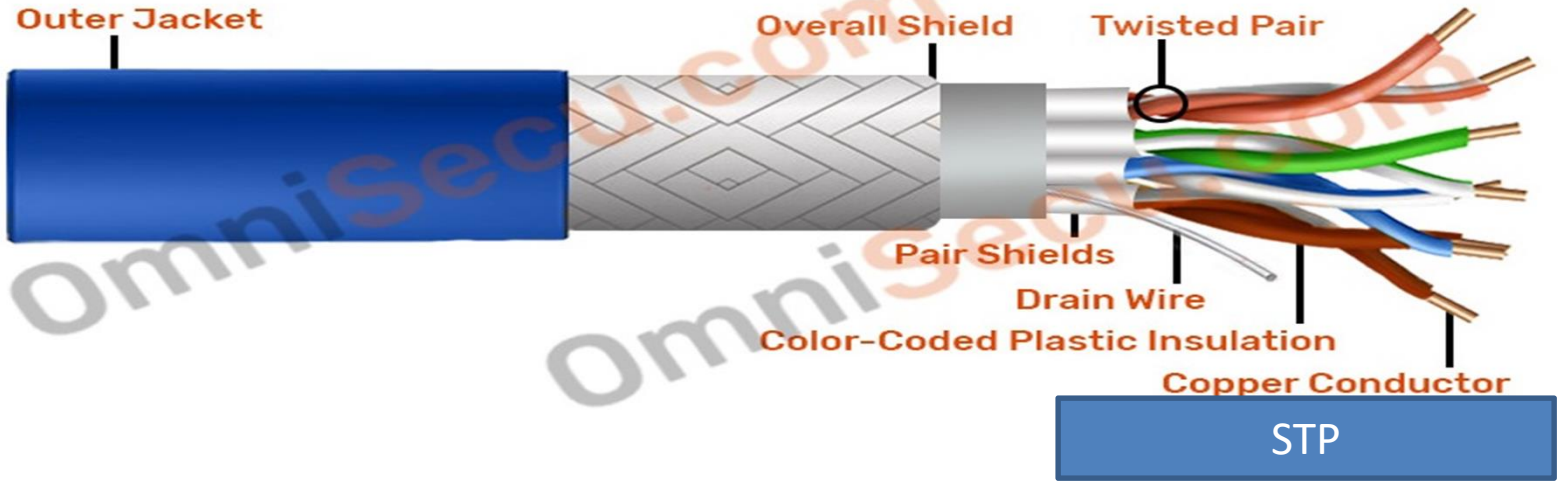
Shielded Twisted Pair (STP) cables additionally have an overall conducting metallic shields covering four twisted pair wires. There may be another conducting metallic shields covering individual twisted pairs also. These metallic shields blocks out electromagnetic interference to prevent unwanted noise from the communication circuit.

Drain wires are also used in Shielded Twisted Pair (STP) cables together with metallic shields for grounding purpose. The drain wire provides a low-resistance connection to shield for better grounding. The main purpose of drain wire is to carry away unwanted interference noise to ground.

Click following link to learn about **different types of STP cables - F/UTP, S/UTP, SF/UTP, S/FTP, F/FTP, U/FTP cables**.

Following images show two different types of Shielded Twisted Pair cables (STP).

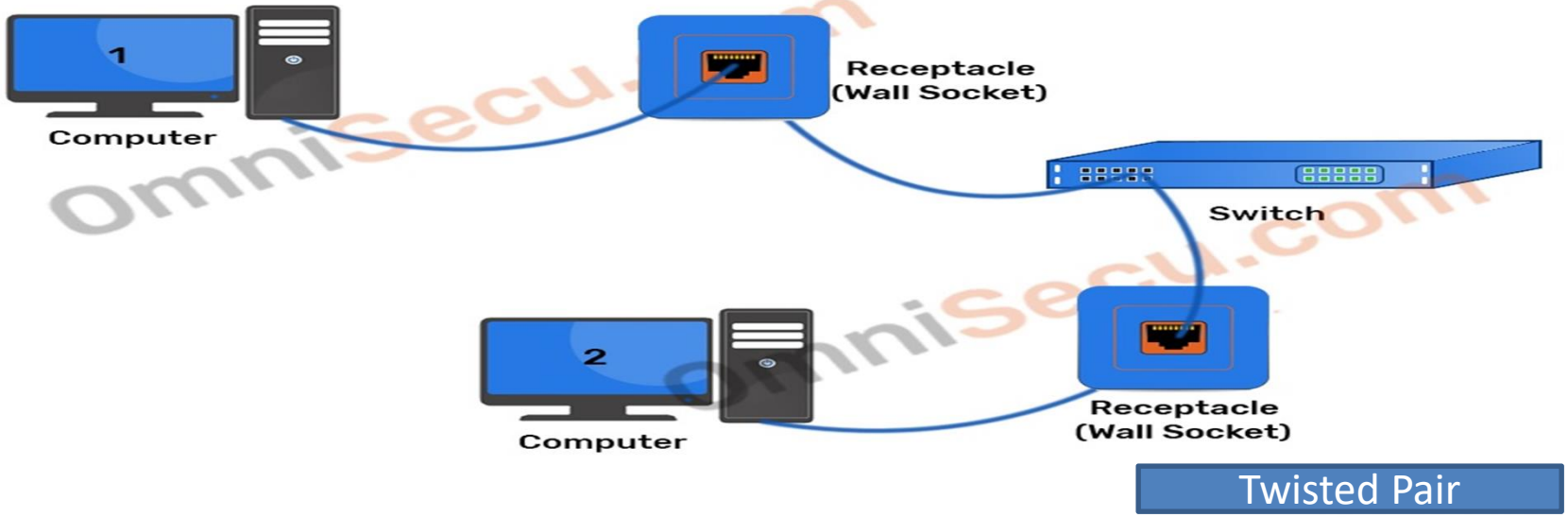




The connector used on a UTP cable is called as RJ-45 (Registered Jack 45) connector. Below picture shows an RJ45 jack, attached to UTP cable. Eight color-coded wires inside Twisted-Pair cable is attached to eight pins in a RJ45 jack as shown below. Each wire in the Twisted Pair cable is crimped into 8 pins in the RJ45 jack.

One end of the Twisted Pair cable with RJ45 jacks attached is plugged in to computer's **Ethernet NIC card** port and other end is plugged to the wall mount plate with female RJ45 port (receptacle), as shown below.

From the wall mount RJ45 female receptacle, Twisted Pair cable is wired to the **Local Area Network (LAN) switches**. Please refer below image.



Twisted pair cables Categories

Twisted pair cables have different categories. Each category of twisted pair cabling was designed for a specific type of communication or transfer rate. The most popular categories in use today is Cat 6, Cat 6a and Cat 7. Cat 6, Cat 6a and Cat 7 twisted pair cables can reach transfer rates of over 1000 Mbps (1 Gbps).

Generally twisted pair cables support a maximum distance of 100 Meters (from **NIC Card** to Switch Port), without signal distortion.

The following table shows different twisted pair categories and corresponding transfer rate.

UTP Category	Purpose	Frequency	Transfer Rate
Category 1	Voice Only		
Category 2	Data	4 MHz	4 Mbps
Category 3	Data	16 MHz	10 Mbps
Category 4	Data	20 Mbps	16 Mbps
Category 5	Data	100 MHz	100 Mbps
Category 5e	Data	100 MHz	1 Gbps
Category 6	Data	250 MHz	Upto 10 Gbps
Category 6a	Data	500 MHz	Upto 10 Gbps
Category 7	Data	600 MHz	Upto 10 Gbps
Category 7a	Data	1 GHz (1000 MHz)	40 to 100 Gbps

Optical Fiber Cabling

Optical Fiber cables use optical fibers that carry digital data signals in the form of modulated pulses of light. An optical fiber consists of an extremely thin cylinder of glass, called the core, surrounded by a concentric layer of glass, known as the cladding. There are two fibers per cable—one to transmit and one to receive. The core also can be an optical-quality clear plastic, and the cladding can be made up of gel that reflects signals back into the fiber to reduce signal loss.

There are two types of fiber optic cable: **Single Mode Fiber (SMF)** and **Multi Mode Fiber (MMF)**.

1. Single-mode Fiber (SMF) uses a single ray of light to carry transmission over long distances. Please click next link to learn more about **single mode fiber (SMF)**.
2. Multi-mode Fiber (MMF) uses multiple rays of light simultaneously with each ray of light running at a different reflection angle to carry the transmission over short distances. Multi-mode fiber cables can transmit data at 100 Mbps (megabits per second) for distances up to 2 kilometers (100Base-FX), 1 Gbps up to 1000 meters (1 kilometer), and 10 Gbps up to 550 meters. Please click next link to learn more about **multimode fiber (MMF)**.

Differences between STP and UTP twisted pair cables

Shielded Twisted Pair	Unshielded Twisted Pair
STP - Shielded Twisted Pair cable.	UTP - Unshielded Twisted Pair cable.
STP is costlier in price than UTP.	UTP is cheap in price compared with STP.
STP require grounding of cable.	UTP requires no grounding of cable.
STP reduces electromagnetic interference more than UTP	Electromagnetic interference is more in UTP
Low crosstalk in STP	Crosstalk in UTP is more than STP
STP is fast compared with UTP	UTP is slow compared to STP

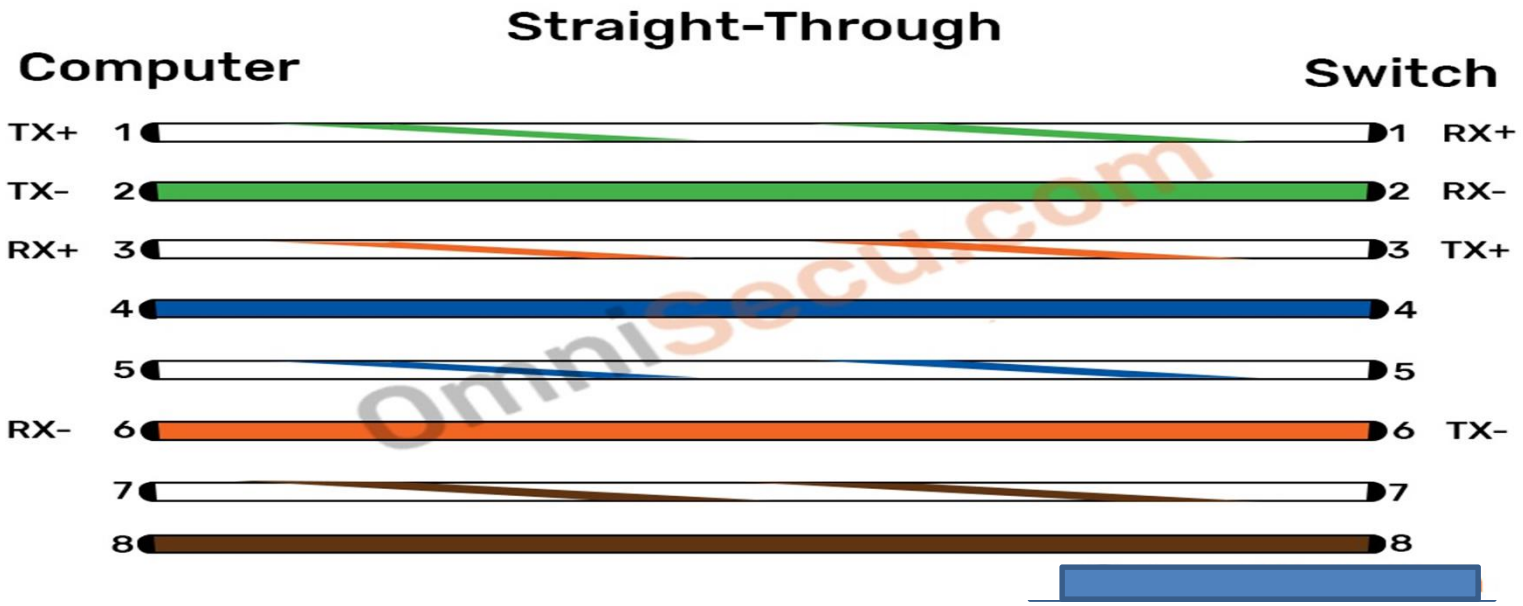
Straight-Through and Cross-Over cables

Straight-Through Cables

In Ethernet (10 Mbps) and FastEthernet (100 Mbps) standards **UTP cabling** use only four wires when sending and receiving information on the network. The four wires used for sending and receiving information in Ethernet (10 Mbps) and FastEthernet (100 Mbps) standards are wires 1, 2, 3, and 6. When you configure the wire for the same pin at either end of the cable, this is known as a straight-through cable.

Note that Gigabit Ethernet standards use all the eight wires in **twisted pair cables** for sending and receiving information on the network. Please visit next link to learn about **Gigabit Ethernet Pinout**.

From the figure we can see that the wires 1 and 2 are used to transmit the data from the computer and 3 and 6 are used to receive data on the computer. The transmit wire on the computer matches with the receive wire on the **switch**. For the transmission of data to take place, the transmit pins on the computer should match with the receive pins on the **switch** and the transmit pins on the **switch** should match to receive pins on the computer. Here we can see that the pins 1, 2, 3 and 6 on the computer matches with pins 1, 2, 3 and 6 on the **switch**. Hence, we use the term Straight-through.



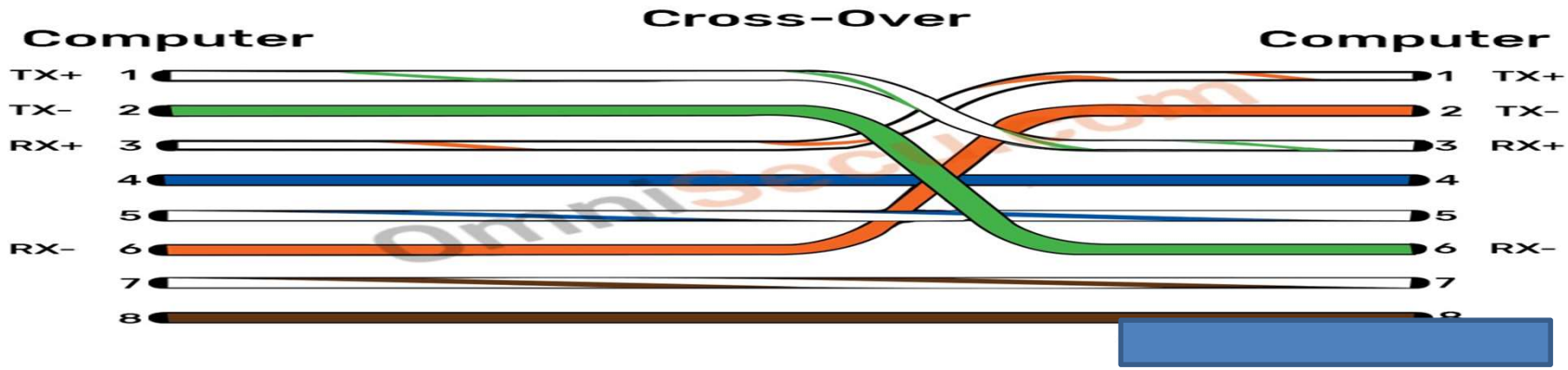
Cross-Over Cables

If we want to connect two computers together with a straight-through cable, we can see that, the transmit pins will be connected to transmit pins and receive pins will be connected to receive pins. We will not be able to directly connect two computers or two **switches** together using straight through cables.

To connect two computers together without using a **switch** (or two switches directly), we need a crossover cable by switching wires 1 and 2 with wires 3 and 6 at one end of the cable. If we shift the pins, we can make sure that the transmit pins on Computer A will match with the receive pins on Computer B and the transmit pins on Computer B will match with the receive pins on Computer A.

Following image shows the wire/pin positions Cross-over **Unshielded Twisted Pair cable**, using **TIA/EIA 568A/568B standards**.

Note that the white striped wires are used to connect positive pins and solid color wires are used to connect negative pins.



Ethernet Media Standards

Media Standard	Cable Type	Bandwidth Capacity	Maximum Length
10Base2	Coaxial	10 Mbps	185m
10Base5	Coaxial	10 Mbps	500m
10BaseT	UTP (CAT 3 or higher)	10 Mbps	100m
100BaseTX	UTP (CAT 5 or higher)	100 Mbps	100m
10BaseFL	Fibre Optic	10 Mbps	2Km
100BaseFX	Fibre Optic	100 Mbps	HD 400m/FD 2km
1000BaseT	UTP (CAT 6 or higher)	1 Gbps (1000 Mbps)	100m
10GBase-T	UTP (Cat 6a or higher)	10 Gbps (10000 Mbps)	100m
1000BaseSX	Fibre Optic	1 Gbps (1000 Mbps)	MMF 550m
1000BaseLX	Fibre Optic	1 Gbps (1000 Mbps)	MMF 500m/SMF 10km
1000BaseCX	Fibre Optic	1 Gbps (1000 Mbps)	100m
10GbaseSR	Fibre Optic	10 Gbps	300m
10GbaseLR	Fibre Optic	10 Gbps	SMF 10km

Network Cable Connectors Types and Specifications

RJ-11 (Registered Jack)
Standard telephone cable connectors, **RJ-11** has 4 wires (and RJ-12 has 6 wires). **RJ-11** is the acronym for Registered Jack-11, a four- or six-wire connector primarily used to connect telephone equipment.

RJ-11 Pin	Signal Name
1	VCC (5 volts regulated)
2	Power Ground
3	One Wire Data
4	One Wire Ground

RJ-45 (Registered Jack)
The acronym for **Registered Jack-45** is RJ-45. The **RJ-45** connector is an eight-wire connector that is commonly used to connect computers to a local area network (LAN), particularly Ethernet LANs. Although they are slightly larger than the more commonly used **RJ-11** connectors, RJ-45s can be used to connect some types of telephone equipment.

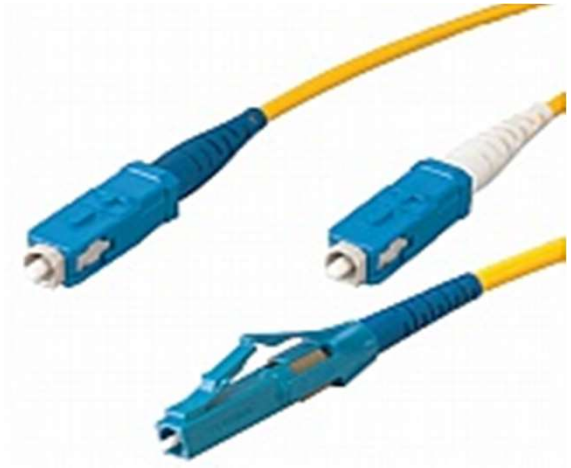
RJ 45

F-Type

The **F connector** is a type of RF connector commonly used for cable and universally for satellite television. They are also used for the cable TV connection in DOCSIS cable modems, usually with RG-6 tri-shield cable. The F connector is inexpensive, yet has good performance up to 1 GHz. One reason for its low cost is that it uses the center wire of the coaxial cable as the pin of the male connector. The male connector body is typically crimped onto the exposed outer braid. Female connectors have a 3/8-32 thread. Most male connectors have a matching threaded connecting ring, though push-on versions are also available.

ST (Straight Tip) and SC (Subscriber Connector or Standard Connector)

Fiber network segments always require two fiber cables: one for transmitting data, and one for receiving. Each end of a fiber cable is fitted with a plug that can be inserted into a network adapter, hub, or switch. In the North America, most cables use a square SC connector (Subscriber Connector or Standard Connector) that slides and locks into place when inserted into a node or connected to another fiber cable, Europeans use a round ST connector (Straight Tip) instead.



SC Connector

ST Connector

Network Connecting Devices

Network devices can relate PCs or other electronic tools to share documents or resources like printers or fax machines. Devices can install a Local Area Network (LAN) are the general type of network devices used by the public. A LAN needed a hub, router, cabling or radio innovation, connection cards, and a high-speed modem if an online connection is necessary.

Most networks are small—think of a small office or home—and even large networks are often divided into smaller segments. That smaller segment is set apart from the larger network by a device that can filter data and help the network be more efficient.

These devices that filter traffic are called connectivity devices, and there are several different types:

•Bridge

•Hub

•Switch

•Router

Here's what these connectivity devices, working together, are primarily responsible for:

•Controlling traffic. Large networks need a way to filter and isolate data traffic.

•Connectivity. These devices can connect different types of networks using different types of network protocols.

•Hierarchical addressing. Segmenting the network with connectivity devices provides an actual (physical) example of delivering actual data to the right destination through the IP address's network ID and host ID.

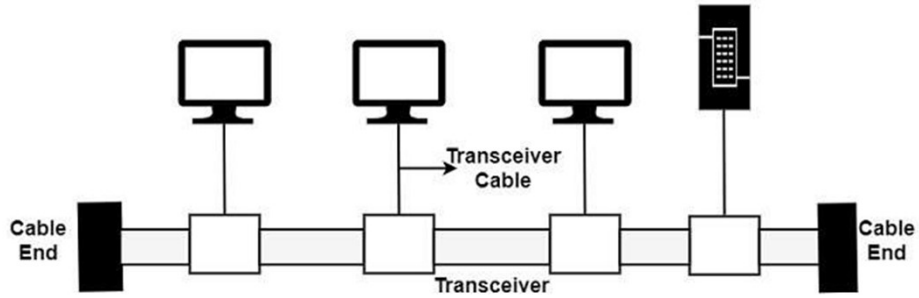
Network Interface Card (NIC)

Network Interface Card is a device that linked your computer to a network. A NIC is a display in the figure. The cards are set up in a development slot in each mainframe and server on the connection.

Transceivers

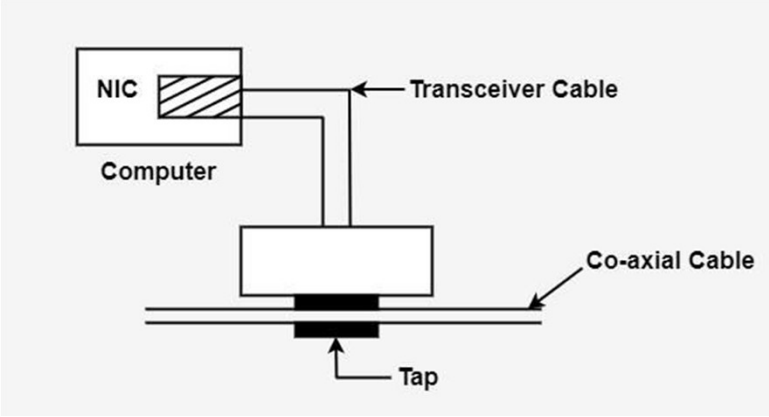
The Transceiver (Transmitter/Receiver) is a device that attaches a computer to a network cable. Transceivers are developed into NIC (Network Interface Card).

The Transceiver is essential for transmitting, receiving, and finding collisions. The transceiver is linked to the station through a transceiver cable that supports disconnect paths for sending and receiving, as display in the figure.



A transceiver can be external or internal. An external transceiver is set up adjacent to the media. An internal transceiver is set up within the station on the network interface card (NIC).

The external transceiver is displayed in the figure −



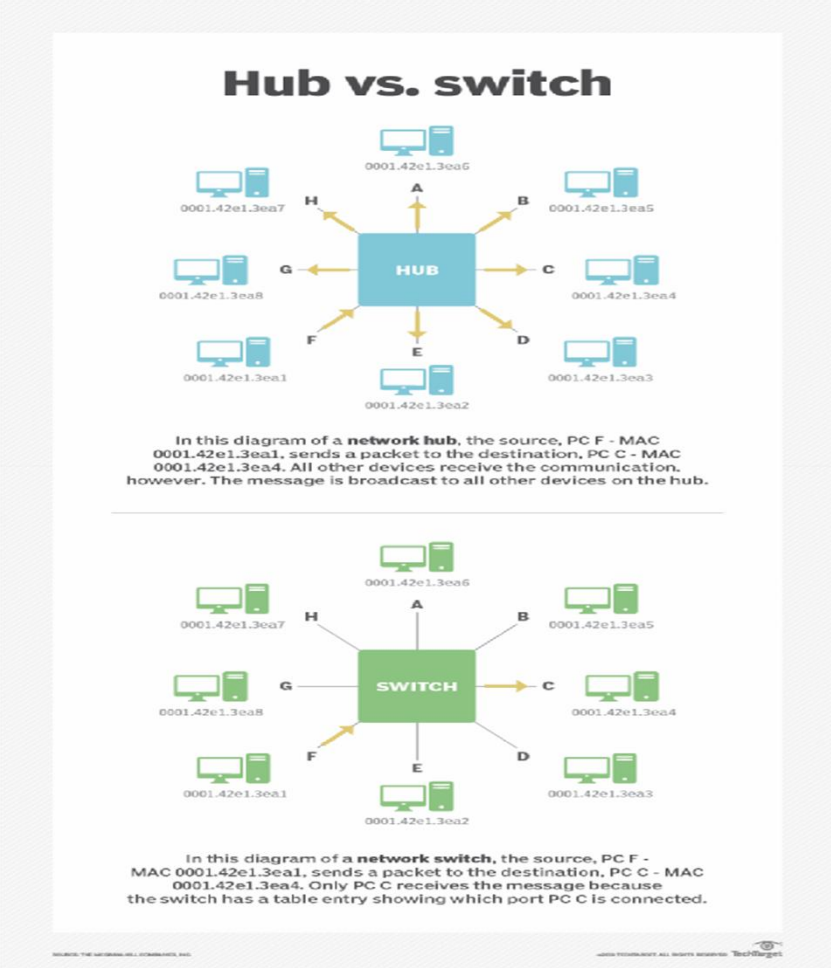
What is a network hub?

A network hub is a node that broadcasts data to every computer or Ethernet-based device connected to it. A hub is less sophisticated than a switch, the latter of which can isolate data transmissions to specific devices.

Network hubs are best suited for small, simple local area network (LAN) environments. Hubs cannot provide routing capabilities or other advanced network services. Because they operate by

forwarding packets across all ports indiscriminately, network hubs are sometimes referred to as "dumb switches."

With limited capabilities and poor scalability, network hubs had primarily one competitive advantage over switches: lower prices. As switch prices fell in the early to mid-2000s, hubs began getting phased out of use. Today, hubs are far less commonly deployed. But network hubs have some niche uses and continue to offer a simple means of networking.

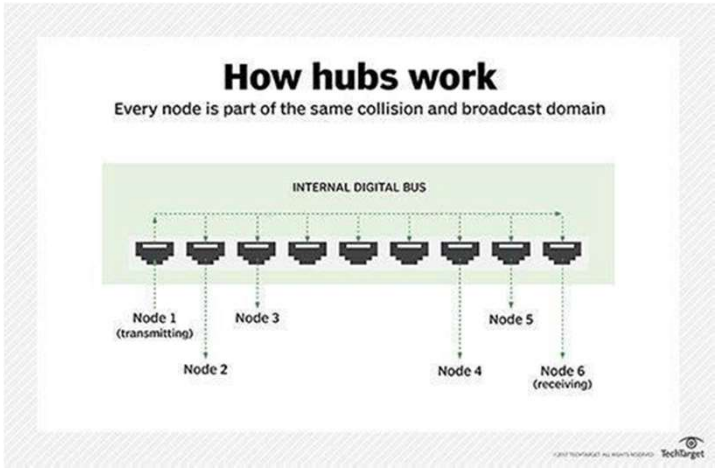


Compare the difference between a hub and a switch.

How network hubs work

Network hubs are categorized as Layer 1 devices in the Open Systems Interconnection (OSI) reference model. They connect multiple computers together, transmitting data received at one port to all of its other ports without restriction. Hubs operate in half-duplex.

This model raises security and privacy concerns, because traffic could not be safeguarded or quarantined. It also presents a practical issue in terms of traffic management. Devices on a hub function as a network segment and share a collision domain. Thus, when two devices connected to a network hub transmit data simultaneously, the packets will collide, causing network performance problems. This is mitigated in switches or routers, as each port represents a separate collision domain.



See how a network hub works.

All devices connected to a network hub share all available bandwidth equally. This differs from a switch environment, where each port is allotted a dedicated amount of bandwidth.

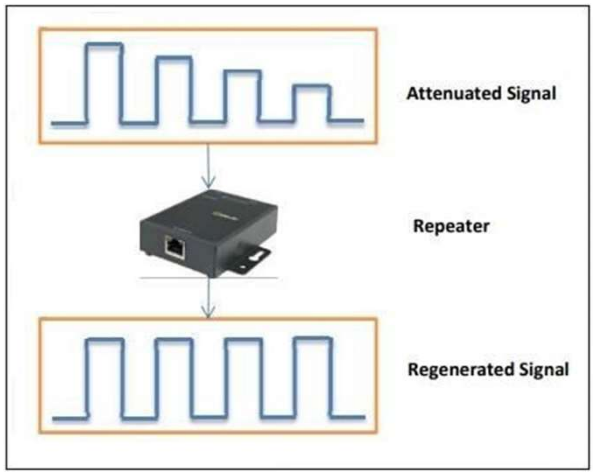
Types of network hubs

There are two types of network hubs: active and passive. A third designation, intelligent hubs, is synonymous with a switch.

- **Active hubs** repeat and strengthen incoming transmissions. They are also sometimes referred to as repeaters.
- **Passive hubs** simply serve as a point of connectivity, without any additional capabilities.

Repeaters

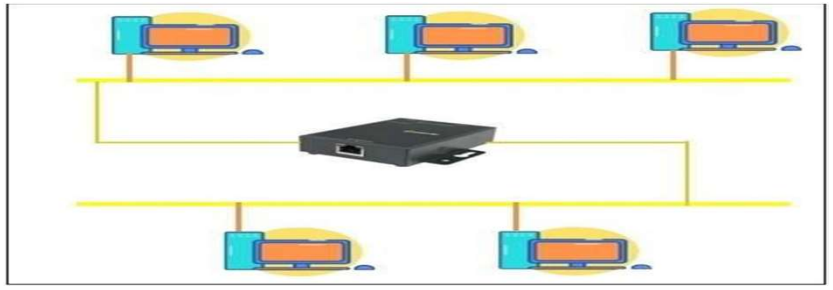
Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.



Why are Repeaters needed?

When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals.

Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss.So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN. This is shown in the following diagram –



Types of Repeaters

According to the types of signals that they regenerate, repeaters can be classified into two categories −

- **Analog Repeaters** − They can only amplify the analog signal.
- **Digital Repeaters** − They can reconstruct a distorted signal.

According to the types of networks that they connect, repeaters can be categorized into two types −

- **Wired Repeaters** − They are used in wired LANs.
- **Wireless Repeaters** − They are used in wireless LANs and cellular networks.

According to the domain of LANs they connect, repeaters can be divided into two categories −

- **Local Repeaters** − They connect LAN segments separated by small distance.
- **Remote Repeaters** − They connect LANs that are far from each other.

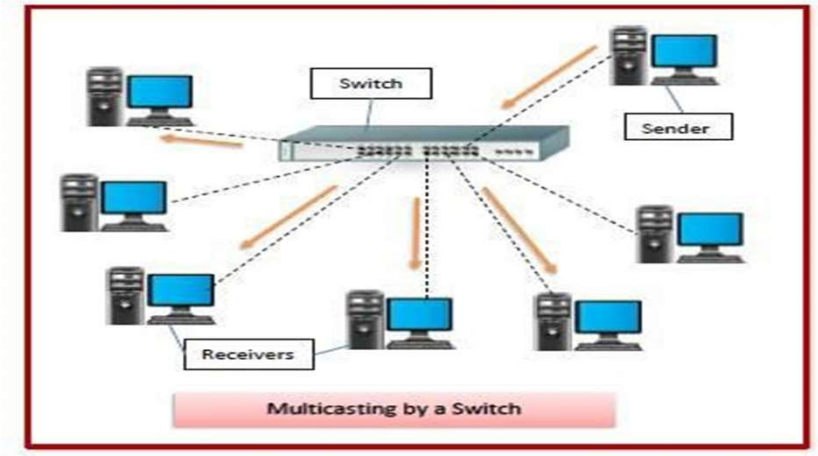
Advantages of Repeaters

- Repeaters are simple to install and can easily extend the length or the coverage area of networks.
- They are cost effective.
- Repeaters don’t require any processing overhead. The only time they need to be investigated is in case of degradation of performance.
- They can connect signals using different types of cables. Disadvantages of Repeaters
- Repeaters cannot connect dissimilar networks.
- They cannot differentiate between actual signal and noise.
- They cannot reduce network traffic or congestion.
- Most networks have limitations upon the number of repeaters that can be deployed.

Switches

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).It supports unicast, multicast as well as broadcast communications.



Features of Switches

•A switch operates in the layer 2, i.e. data link layer of the OSI model.

•It is an intelligent network device that can be conceived as a multiport network bridge.

•It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.

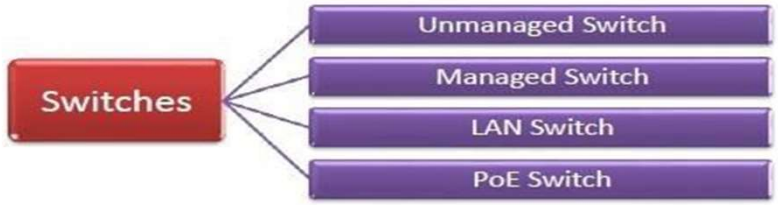
•It uses packet switching technique to receive and forward data packets from the source to the destination device.

•It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.

•Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.

- Switches are active devices, equipped with network software and network management capabilities.
- Switches can perform some error checking before forwarding data to the destined port.
- The number of ports is higher – 24/48. Types of Switches

There are variety of switches that can be broadly categorised into 4 types −



- **Unmanaged Switch** − These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices needs to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.
- **Managed Switch** − These are costly switches that are used in organisations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.
- **LAN Switch** − Local Area Network (LAN) switches connects devices in the internal LAN of an organization. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.
- **PoE Switch** − Power over Ethernet (PoE) switches are used in PoE Gogabit Ethernets. PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections

What is Routing Protocols?

Routing Protocols are the set of defined rules used by the routers to communicate between source & destination. They do not move the information to the source to a destination, but only update the routing table that contains the information.

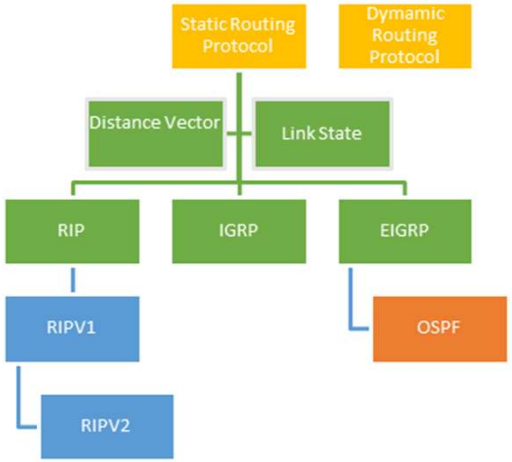
Network Router protocols helps you to specify way routers communicate with each other. It allows the network to select routes between any two nodes on a computer network.

Types of Routing Protocols

There are mainly two types of Network Routing Protocols

•Static

•Dynamic



Routing Protocols

Static Routing Protocols

Static routing protocols are used when an administrator manually assigns the path from source to the destination network. It offers more security to the network.

Advantages

•No overhead on router CPU.

- No unused bandwidth between links.
- Only the administrator is able to add routes

Disadvantages

- The administrator must know how each router is connected.
- Not an ideal option for large networks as it is time intensive.
- Whenever link fails all the network goes down which is not feasible in small networks.

Dynamic Routing Protocols

Dynamic routing protocols are another important type of routing protocol. It helps routers to add information to their routing tables from connected routers automatically. These types of protocols also send out topology updates whenever the network changes' topological structure.

Advantage:

- Easier to configure even on larger networks.
- It will be dynamically able to choose a different route in case if a link goes down.
- It helps you to do load balancing between multiple links.

Disadvantage:

- Updates are shared between routers, so it consumes bandwidth.
- Routing protocols put an additional load on router CPU or RAM.

Distance Vector Routing Protocol (DVR)

Distance Vector Protocols advertise their routing table to every directly connected neighbor at specific time intervals using lots of bandwidths and slow converge.

In the Distance Vector routing protocol, when a route becomes unavailable, all routing tables need to be updated with new information.

Advantages:

- Updates of the network are exchanged periodically, and it is always broadcast.
- This protocol always trusts route on routing information received from neighbor routers.

Disadvantages:

- As the routing information are exchanged periodically, unnecessary traffic is generated, which consumes available bandwidth.

Internet Routing Protocols:

The following are types of protocols which help data packets find their way across the Internet:

Routing Information Protocol (RIP)

RIP is used in both LAN and WAN Networks**.** It also runs on the Application layer of the OSI model. The full form of RIP is the Routing Information Protocol. Two versions of RIP are

- RIPv1
- RIPv2

The original version or RIPv1 helps you determine network paths based on the IP destination and the hop count journey. RIPv1 also interacts with the network by broadcasting its IP table to all routers connected with the network.

RIPv2 is a little more sophisticated as it sends its routing table on to a multicast address.

Interior Gateway Protocol (IGP)

IGRP is a subtype of the distance-vector interior gateway protocol developed by CISCO. It is introduced to overcome RIP limitations. The metrics used are load, bandwidth, delay, MTU, and reliability. It is widely used by routers to exchange routing data within an autonomous system.

This type of routing protocol is the best for larger network size as it broadcasts after every 90 seconds, and it has a maximum hop count of 255**.** It helps you to sustain larger networks compared to RIP. IGRP is also widely used as it is resistant to routing loop because it updates itself automatically when route changes occur within the specific network. It is also given an option to load balance traffic across equal or unequal metric cost paths.

Link State Routing Protocol

Link State Protocols take a unique approach to search the best routing path. In this protocol, the route is calculated based on the speed of the path to the destination and the cost of resources.

Routing protocol tables:

Link state routing protocol maintains below given three tables:

- **Neighbor table:** This table contains information about the neighbors of the router only. For example, adjacency has been formed.
- **Topology table:** This table stores information about the whole topology. For example, it contains both the best and backup routes to a particular advertised network.

- **Routing table:** This type of table contains all the best routes to the advertised network.

Advantages:

- This protocol maintains separate tables for both the best route and the backup routes, so it has more knowledge of the inter-network than any other distance vector routing protocol.
- Concept of triggered updates are used, so it does not consume any unnecessary bandwidth.
- Partial updates will be triggered when there is a topology change, so it does not need to update where the whole routing table is exchanged.

Exterior Gateway Protocol (EGP)

EGP is a protocol used to exchange data between gateway hosts that are neighbors with each other within autonomous systems. This routing protocol offers a forum for routers to share information across different domains. The full form for EGP is the Exterior Gateway Protocol. EGP protocol includes known routers, network addresses, route costs, or neighboring devices.

Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a hybrid routing protocol that provides routing protocols, distance vector, and link-state routing protocols. The full form routing protocol EIGRP is Enhanced Interior Gateway Routing Protocol. It will route the same protocols that IGRP routes using the same composite metrics as IGRP, which helps the network select the best path destination.

Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) protocol is a link-state IGP tailor-made for IP networks using the Shortest Path First (SPF) method.

OSPF routing allows you to maintain databases detailing information about the surrounding topology of the network. It also uses the Dijkstra algorithm (Shortest path algorithm) to recalculate network paths when its topology changes. This protocol is also very secure, as it can authenticate protocol changes to keep data secure.

Here are some main difference between these Distance Vector and Link State routing protocols:

Distance Vector	**Link State**
Distance Vector protocol sends the entire routing table.	Link State protocol sends only link-state informa It is
susceptible to routing loops.	It is less susceptible to routing loops.
Updates are sometimes sent using broadcast.	Uses only multicast method for routing updates.

Distance Vector	Link State
It is simple to configure.	It is hard to configure this routing protocol.
Does not know network topology.	Know the entire topology.
Example RIP, IGRP.	Examples: OSPF IS-IS.

Intermediate System-to-Intermediate System (IS-IS)

ISIS CISCO routing protocol is used on the Internet to send IP routing information. It consists of a range of components, including end systems, intermediate systems, areas, and domains.

The full form of ISIS is Intermediate System-to-Intermediate System. Under the IS-IS protocol, routers are organized into groups called areas. Multiple areas are grouped to make form a domain.

Border Gateway Protocol (BGP)

BGP is the last routing protocol of the Internet, which is classified as a DPVP (distance path vector protocol). The full form of BGP is the Border Gateway Protocol.

This type of routing protocol sends updated router table data when changes are made. Therefore, there is no auto-discovery of topology changes, which means that the user needs to configure BGP manually.

What is the purpose of Routing Protocols?

Routing protocols are required for the following reasons:

•Allows optimal path selection

•Offers loop-free routing

•Fast convergence

•Minimize update traffic

•Easy to configure

•Adapts to changes

•Scales to a large size

•Compatible with existing hosts and routers

•Supports variable length

Classful Vs. Classless Routing Protocols

Here are some main difference between these routing protocols:

Classful Routing Protocols	Classless Routing Protocols
Classful routing protocols never send subnet mask detail during routing updates.	Classless routing protocols can send IP subnet mask information while doing routing updates.
RIPv1 and IGRP are classful protocols. These two are classful protocols as they do not include subnet mask information.	RIPv2, OSPF, EIGRP, and IS-IS are all types of class routing protocols which has subnet mask information within updates.

HOW TO CONFIGURE YOUR ROUTER

The configuration process of a broadband Wi-Fi router doesn't have to be an ordeal. Although ISPs try their best to make it easier to install their products, one can still burrow deeper into the router's configuration pages to establish security, access controls, and granular management.

At any rate, setting up a tightly managed, secure home network is possible by following these five steps.

•Connect your router

The broadband Wi-Fi router is the bridge between the Internet and your home network. It is how all the devices on your network communicate with one another. The device that has to be connected to the Wi-Fi router, has to have an appropriate network adapter. The first step to configure is to physically connect your router to a modem provided by your ISP with an Ethernet cable, by following these steps:

- Firstly, unplug or turn off the cable or DSL modem.
- Plugin your wireless router and connect the network cable into the port on the router that is labelled "Internet" or "WAN."
- Connect the other end to the cable or DSL modem and start up the modem.
- Do not try to connect any devices such as laptops or tablets until you have a high strength signal indicating a WAN connection on both the router and modem.

•Access the router's interface and build it

The next step involves accessing the router's interface in the following steps:

- Connect an Ethernet cable to one of the LAN ports on the router and the other end to the Ethernet port of the laptop.
- Click to open "Network and Internet" and then "Network and Sharing Centre."
- From the left-hand window, click "Change adapter settings."
- Right-click on "Local Area Connection" and then click on "Properties." to select the IP version.

5. Hold the cursor on “Internet Protocol Version 4 (TCP/IP v4)” and once again, click "Properties."

6. Push the click on "Use the following IP address:" and enter the information as shown in the image above.

7. Once the changes are done, open up a browser and go to the web address using the account name "admin" and password "admin." This is now all set to configure security and other settings.

8. Most router manufacturers use the same default IP address, admin account, and passwords on all their routers. The router's documentation provided by the manufacturer will tell you the specific IP address and account login information.

9. Configure security and IP addressing

10. After accessing the router, the next order of business is getting the security, SSID, and IP addressing settings right. These settings are found under the "Basic" settings of the interface. They may also be under "Security" or "Wireless Settings". Further steps are:

5. Change the default administrator password which is usually under the "System" tab or page of the interface. Just enter a new password in the new password field.

6. Change the router's default SSID. The SSID is the broadcasted name of the unique wireless network you own. Use a unique name to avoid confusion.

7. Assign security. Go into the router's wireless security page. Opt for WPA security, as it requires clients connecting to it to use a password, for connecting.

8. Set up IP addressing. For most networks, the router comes at its default DHCP setting.

9. Disconnect the laptop and reboot it. When the laptop comes back from reboot the user can see the SSID name of your wireless network and be able to connect to it with the password you created.

11. Set up sharing and control

12. Now that you have a network set up, you can now set up a way for all the devices to access data on the network. This can be done by setting up a "Home Network" by using your current location.

13. Set up user accounts

Further, try to set up user accounts with your Wi-Fi router plans

- Select the User Accounts icon. The User accounts settings will allow you to configure your account.

2. To add and configure other devices to access the network, from User Accounts, click on "Manage User Accounts," and then click on the "Advanced" tab.

3. Under "Advanced User Management" click "Advanced" and select the user and add them to your network. The advanced setting also comes with the Wi-Fi router recharge plans.

4. Using these 5 simple approaches, you can set up and configure your router seamlessly. Skip the complex process of bypassing router settings and have a streamlined self-configured browsing experience.

Voice over Internet Protocol (VoIP)

- **Voice over Internet Protocol (VoIP)**, is a technology that allowing you to make voice calls over a broadband Internet connection instead of an analog (regular) phone line. Some VoIP services allow you to call people using the same service, but others may allow you to call anyone. They can have a telephone number – including local, long-distance, mobile, and international numbers or not. Some VoIP services only work over your computer or a special VoIP phone while other services allow you to use a traditional phone connected to a VoIP adapter.

How VoIP / Internet Voice Works –

- Voice is converted into a digital signal by VoIP services that travel over the Internet. If the regular phone number is called, the signal is converted to a regular telephone signal i.e. an analog signal before it reaches the destination. VoIP can allow you to make a call directly from a computer having a special VoIP phone, or a traditional phone connected to a special adapter. Wireless hot spots in locations such as airports, hospitals, cafes, etc allow you to connect to the Internet and can enable you to use VoIP service wirelessly.

Equipments Required –

- A high-speed Internet connection is required which can be through a cable modem or high-speed services such as a local area network. A computer, adaptor, or specialized phone is required. Some VoIP services only work over your computer or a special VoIP phone. Other services allow you to use a traditional phone connected to a VoIP adapter. If you use your computer some software and an inexpensive microphone are needed. VoIP phones plug directly into your broadband connection and operate largely like a traditional telephone. If you use a telephone with a VoIP adapter, you can dial just as you always have, and the service provider may also provide a dial tone.

Advantages of VoIP –

- Some VoIP services offer features and services that are not available with a traditional phone, or are available but only for an additional fee.

- Paying for both a broadband connection and a traditional telephone line can be avoided.

3. Smoother connection than an analog signal can be provided.

Disadvantages of VoIP –

- Some VoIP services don't work during power outages and the service provider may not offer backup power.
- Not all VoIP services connect directly to emergency services through emergency service numbers.
- VoIP providers may or may not offer directory assistance.

Network Security refers to the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data, has a degree of solutions against many **cyber threats**.

The most basic example of Network Security is password protection which the user of the network oneself chooses. In recent times, Network Security has become the central topic of cyber security with many organizations inviting applications from people who have skills in this area. The network security solutions protect various **vulnerabilities of the computer systems** such as:

- Users
- Locations
- Data
- Devices
- Applications

Network Security: Working

The basic principle of network security is protecting huge stored data and networks in layers that ensure the bedding of rules and regulations that have to be acknowledged before performing any activity on the data.

These levels are:

- Physical
- Technical
- Administrative

These are explained as following below.

1.Physical Network Security:
This is the most basic level that includes protecting the data and network through unauthorized personnel from acquiring control over the confidentiality of the network. These include external peripherals and routers that might be used for cable connections. The same can be achieved by using devices like biometric systems.

•Technical Network Security:
It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One is protected from unauthorized users, and the other is protection from malicious activities.

•Administrative Network Security:
This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.

Types of Network Security:
The few types of network securities are discussed below :

•Access Control:
Not every person should have a complete allowance for the accessibility to the network or its data. One way to examine this is by going through each personnel's details. This is done through Network Access Control which ensures that only a handful of authorized personnel must be able to work with the allowed amount of resources.

•Antivirus and Anti-malware Software:
This type of network security ensures that any malicious software does not enter the network and jeopardize the security of the data. The malicious software like Viruses, Trojans, and Worms is handled by the same. This ensures that not only the entry of the malware is protected but also that the system is well equipped to fight once it has entered.

•Cloud Security:
•Now a day, a lot many organizations are joining hands with cloud technology where a large amount of important data is stored over the internet. This is very vulnerable to the malpractices that few unauthorized dealers might pertain. This data must be protected and it should be ensured that this protection is not jeopardized by anything. Many businesses embrace SaaS

applications for providing some of their employees the allowance of accessing the data stored over the cloud. This type of security ensures creating gaps in the visibility of the data.

Client Server Technology

Client-server is a computer model that separates client and server, and usually interlinked using a computer network. Each instance of a client can send data requests to one of the servers online and expect a response.

In turn, some of the available servers can accept these requests, process them and return the result to the client. Although the concept be applied to various uses and applications, the architecture is almost the same.

Often clients and servers communicate through a computer network with separate hardware, but the client and server can reside on the same system. The machine is a host server that is running one or more server programs that share their resources with clients.

A client does not share its resources, but requests content from a server or service function. Clients, therefore, initiate communication sessions with the servers that wait for incoming requests.

Client-server – Description

The character of client-server describes the relationship of programs in an application. The server component provides a function or service to one or many clents, who start their service requests.

Functions such as exchanging email, Internet access and database access, are built based on client-server model. For example, a web browser is a client program running on a user's computer that can access information stored on a web server on the Internet. Users accessing banking services from your computer using a Web browser client to send a request to a web server in a bank.

That program may in turn forward the request to its own program database client that sends a request to a server database on another computer to retrieve bank account information. The balance is returned to the client database of the bank, which in turn serves it back to the client browser and displays the results to the user.

The client-server model has become one of the central ideas of network computing. Many business applications being written today use the client-server model. In marketing, the term has been used to distinguish distributed computing by smaller dispersed computers from the "computing" monolithic centralized mainframe computers.

Each instance of client software can send data requests to one or more servers connected. In turn, the servers can accept these requests, process them and return the requested information to the client. Although this concept can be applied to a variety of reasons for different types of applications, the architecture remains fundamentally the same.

Features of the Client

1. Always start applications servers;
2. Waits for responses;
3. Get answers;
4. Usually connects to a small number of servers at once;
5. Normally, interacts directly with end users through any user interface, such as graphical user interface.

Server Features

- Always wait for a request from a client;
- Serves clients′ requests, then responds with the requested data to clients;
- A server can communicate with other servers in order to meet a client′s request.

Client-server Architecture – Benefits

- In most cases, the client-server architecture enables the roles and responsibilities of a computing system to be distributed among several independent computers that are known to itself through a network. This creates an additional advantage to this architecture: greater ease of maintenance. For example, you can replace, repair, upgrade or even relocate a server clients, while continuing to be the conscience and not affected by this change;
- All data is stored on servers, which typically have far greater security controls than most clients. Servers can better control access and resources to ensure that only clients with appropriate permissions can access and change data;
- Since data storage is centralized, updates the data are much easier to administer, compared to the P2P paradigm, where a P2P architecture, data updates may need to be distributed and applied to each point in the network, which is the is time-consuming error-prone, as there may be thousands or even millions of peers;
- Many advanced technologies for client-server are now available that are designed to ensure safety, ease of user interface and ease of use;
- Works with many different clients of different capabilities.

Client-server Architecture – Disadvantages

- Network traffic blocking is one of the problems related to client-server model. As the number of simultaneous requests the client to a particular server, the server may become overloaded;
- The client-server paradigm lacks the robustness of a P2P network. Under client-server, if a critical server fails, the clients′ requests can not be met. In P2P networks, resources are usually

distributed among multiple nodes. Even if one or more nodes depart and abandon a downloading file, for example, the remaining nodes should still have the data necessary to complete the download.

What is Server Management?

Server management includes all of the monitoring and maintenance required for servers to operate reliably and at optimal performance levels. Server management also involves the management of hardware, software, security, and backups all in service of keeping the IT environment operational and efficient. The key objectives of server management are:

•Minimize server slowdowns and downtime while maximizing reliability

•Secure and protect server environments

•Scale servers and related operations to meet the needs of the organization over time

Server Management Basics

The overall impact of server management on IT is quite comprehensive, making its scope an umbrella that covers nearly everything the department handles. Let's take a closer look at some of the specifics within this broad-reaching concept:

Hardware Management

Starting with the foundation of effective server management, we have the hardware. Everything depends on functioning hardware. Within this wider subject, there are a few key hardware elements that should be monitored and managed closely as part of any server management strategy:

Central Processing Unit (CPU): Essentially the brain of a server, the CPU performs all the calculations to make programs run. Because they're not only essential but heavily used, CPUs need to be constantly monitored to avoid overtaxing them -- a problem that can result in everything from slowed operations to complete system crashes. There are several ways to address an overtaxed CPU. Upgrading is the most obvious option, but you can also add more CPU resources from another asset, halt resourcing-hogging processes, or fine-tune system-wide performance to take the load off of the CPU.

CPU Temperature: Doing all of that work makes CPUs run hot. Servers, in general, produce ample amounts of heat, which is why server farms are at times built-in cold locations (even underground or underwater). If CPUs run too hot, they can fail with disastrous results.

Servers are built with cooling systems and thermometers that allow for easier server management, even by remote. If a server's temperature gets too high, an IT technician can shut down the hardware and assess the situation before the heat goes critical. Overheating issues are often caused by excess strain on the system or failed cooling devices.

Random Access Memory (RAM): RAM is a server's working memory, the temporary storage used for fast operations and caching. RAM has a direct correlation to a system's performance, especially in the cases of certain high-demand software. Running out of RAM during normal use can impede performance and may prevent certain applications from running at all.

Hard Drive: The hard drive or hard disks provide persistent storage for the server. Important data is stored here, and because hard disks are also used for caching in many cases, they can create performance issues when they're near capacity.

Hard drive usage needs to be monitored so that the required amount of storage capacity is always available when needed. Additionally, hard drive health should be watched closely to prevent costly failures resulting in lost data.

Operating Environment: The server should be kept in a location with optimal environmental conditions. Humidity should be kept in check, and the server room should allow for optimal cooling. For security reasons, servers should only be accessible to authorized individuals.

Software Management

Your IT infrastructure also depends on software to function. As such, software should be subject to constant monitoring and scheduled maintenance, just like hardware. Understanding the software within your IT environment makes it easier to identify performance issues and perform troubleshooting.

Security

Security is a key concern in all aspects of IT, and server management should involve keeping a secure network from the inside out. While security policies differ depending on the organization, there are several standard considerations for most use cases:

•Staying on top of all software and firmware updates (using a patch management tool when possible)

•Installing and updating antivirus software

•Install and configure firewalls to keep out unauthorized network traffic

•Set a password policy and set access controls

•Encrypting sensitive data storage and data in transit

•Implementing SIEM tools, log, and SOC monitoring

•Incorporate tools and procedures demanded by security best practices and any relevant compliance standards

Data Backups

A critical concern for security and business continuity is regular backups and backup testing. Data loss from disaster or a ransomware attack can cripple most organizations -- a robust backup solution can be a lifesaver in these situations. Options for backup include local, cloud, and server backup software to support both physical and virtual servers.

Management of backups is an important consideration here. Not only do backups need to be properly configured for the use case, but they should also be regularly tested to ensure functionality before they're needed. An IT professional that needs to manage backups for many different clients and workstations across multiple networks -- such as a managed service provider -- will need a multi-tenant solution with a single portal for easy management.

Power Backups

The server's power supply should also have a fallback to ensure data isn't lost during a power outage. Many options are available for this function, including uninterruptible power supplies (USPs) with built- in surge protection, power conditioning, and emergency power that can keep the server running for a short time during an outage.

What About Virtual Servers?

Virtualization is commonplace in modern IT and brings its own considerations. A physical server usually runs one instance on a single piece of hardware, but a virtual server can allow multiple servers to be hosted on one machine.

Virtual servers, or virtual machines (VM), allows you to do more with less hardware. While convenience is embraced by the IT community, virtual environments can be slightly more complex to manage than physical servers. That said, the same management principles that apply to traditional server management also apply to virtual servers.

Internal Versus External Server Management

Organizations have a few choices to make when it comes to server management. Not every organization needs (or can budget for) an in-house team to manage their servers and IT environment.

If personnel or costs aren't an issue, internal management provides the advantage of having total control of your server environments. If your own IT team will be handling server management, it's important that they have the right tools for the task. Many tools are available for system administrators, giving them features like automation, notifications, and reporting that make the job easier to manage.

Remote monitoring and management tools can offer many of these essential functions while also giving your team the ability to interface with the server and make adjustments or repairs remotely. For large enterprises, this capability is nearly essential.

Organizations that don't want to take on the task of server management internally have the option to go with external server management. By working with a managed service provider or other outside IT

company, they can put the responsibility of server monitoring and maintenance on outsourced professionals.

RAID (Redundant Arrays of Independent Disks)

RAID, or “Redundant Arrays of Independent Disks” is a technique which makes use of a combination of multiple disks instead of using a single disk for increased performance, data redundancy or both. The term was coined by David Patterson, Garth A. Gibson, and Randy Katz at the University of California, Berkeley in 1987.

Why data redundancy?

Data redundancy, although taking up extra space, adds to disk reliability. This means, in case of disk failure, if the same data is also backed up onto another disk, we can retrieve the data and go on with the operation. On the other hand, if the data is spread across just multiple disks without the RAID technique, the loss of a single disk can affect the entire data.

Key evaluation points for a RAID System

•**Reliability:** How many disk faults can the system tolerate?

•**Availability:** What fraction of the total session time is a system in uptime mode, i.e. how available is the system for actual use?

•**Performance:** How good is the response time? How high is the throughput (rate of processing work)? Note that performance contains a lot of parameters and not just the two.

•**Capacity:** Given a set of N disks each with B blocks, how much useful capacity is available to the user?

RAID is very transparent to the underlying system. This means, to the host system, it appears as a single big disk presenting itself as a linear array of blocks. This allows older technologies to be replaced by RAID without making too many changes in the existing code.

Different RAID levels RAID-0 (Stripping)

•Blocks are “stripped” across disks.

Disk 0	Disk 1	Disk 2	Disk 3
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

- In the figure, blocks “0,1,2,3” form a stripe.
- Instead of placing just one block into a disk at a time, we can work with two (or more) blocks placed into a disk before moving on to the next one.

Disk 0	Disk 1	Disk 2	Disk 3
0	3	4	6
1	3	5	7
8	10	12	14
9	11	13	15

Evaluation:

•Reliability: 0
There is no duplication of data. Hence, a block once lost cannot be recovered.

•Capacity: N*B
The entire space is being used to store data. Since there is no duplication, N disks each having B blocks are fully utilized.

RAID-1 (Mirroring)

•More than one copy of each block is stored in a separate disk. Thus, every block has two (or more) copies, lying on different disks.

Disk 0	Disk 1	Disk 2	Disk 3
0	0	1	1
2	2	3	3
4	4	5	5
6	6	7	7

- The above figure shows a RAID-1 system with mirroring level 2.
- RAID 0 was unable to tolerate any disk failure. But RAID 1 is capable of reliability.

Evaluation:

Assume a RAID system with mirroring level 2.

- Reliability: 1 to N/2

1 disk failure can be handled for certain, because blocks of that disk would have duplicates on some other disk. If we are lucky enough and disks 0 and 2 fail, then again this can be handled as the blocks of these disks have duplicates on disks 1 and 3. So, in the best case, N/2 disk failures can be handled.

- Capacity: N*B/2

Only half the space is being used to store data. The other half is just a mirror to the already stored data.

RAID-4 (Block-Level Stripping with Dedicated Parity)

- Instead of duplicating data, this adopts a parity-based approach.

Disk 0	Disk 1	Disk 2	Disk 3	Disk 4
0	1	2	3	P0
4	5	6	7	P1
8	9	10	11	P2
12	13	14	15	P3

- In the figure, we can observe one column (disk) dedicated to parity.
- Parity is calculated using a simple XOR function. If the data bits are 0,0,0,1 the parity bit is XOR(0,0,0,1) = 1. If the data bits are 0,1,1,0 the parity bit is XOR(0,1,1,0) = 0. A simple approach is that even number of ones results in parity 0, and an odd number of ones results in parity 1.

C1	C2	C3	C4	Parity
0	0	0	1	1
0	1	1	0	0

- Assume that in the above figure, C3 is lost due to some disk failure. Then, we can recompute the data bit stored in C3 by looking at the values of all the other columns and the parity bit. This allows us to recover lost data.

Evaluation:

- Reliability: 1

RAID-4 allows recovery of at most 1 disk failure (because of the way parity works). If more than one disk fails, there is no way to recover the data.

- Capacity: (N-1)*B

One disk in the system is reserved for storing the parity. Hence, (N-1) disks are made available for data storage, each disk having B blocks.

RAID-5 (Block-Level Stripping with Distributed Parity)

- This is a slight modification of the RAID-4 system where the only difference is that the parity rotates among the drives.

Disk 0	Disk 1	Disk 2	Disk 3	Disk 4
0	1	2	3	P0
5	6	7	P1	4
10	11	P2	8	9
15	P3	12	13	14
P4	16	17	18	19

- In the figure, we can notice how the parity bit “rotates”.

- This was introduced to make the random write performance better.

Evaluation:

- Reliability: 1

RAID-5 allows recovery of at most 1 disk failure (because of the way parity works). If more than one disk fails, there is no way to recover the data. This is identical to RAID-4.

- Capacity: (N-1)*B

Overall, space equivalent to one disk is utilized in storing the parity. Hence, (N-1) disks are made available for data storage, each disk having B blocks.

What about the other RAID levels?

RAID-2 consists of bit-level stripping using a Hamming Code parity. RAID-3 consists of byte-level striping with dedicated parity. These two are less commonly used.

RAID-6 is a recent advancement that contains a distributed double parity, which involves block-level stripping with 2 parity bits instead of just 1 distributed across all the disks. There are also hybrid RAIDs, which make use of more than one RAID levels nested one after the other, to fulfill specific requirements.

Cryptography and its Types

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography:

In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features Of Cryptography are as follows:

1. **Confidentiality:**

Information can only be accessed by the person for whom it is intended and no other person except him can access it.

2. **Integrity:**

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

- **Non-repudiation:**

The creator/sender of information cannot deny his intention to send information at later stage.

- **Authentication:**

The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography:

In general there are three types Of cryptography:

- **Symmetric Key Cryptography:**
- It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

- **Hash Functions:**

There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

- **Asymmetric Key Cryptography:**

Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

Ethical hacking

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

Hacking experts follow four key protocol concepts:

- **Stay legal**. Obtain proper approval before accessing and performing a security assessment.
- **Define the scope**. Determine the scope of the assessment so that the ethical hacker's work remains legal and within the organization's approved boundaries.

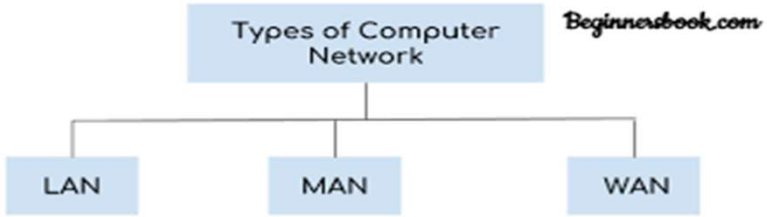
3. **Report vulnerabilities**. Notify the organization of all vulnerabilities discovered during the assessment. Provide remediation advice for resolving these vulnerabilities.
4. **Respect data sensitivity**. Depending on the data sensitivity, ethical hackers may have to agree to a non-disclosure agreement, in addition to other terms and conditions required by the assessed organization.
5. An ethical hacker should have a wide range of computer skills. They often specialize, becoming subject matter experts (SME) on a particular area within the ethical hacking domain.

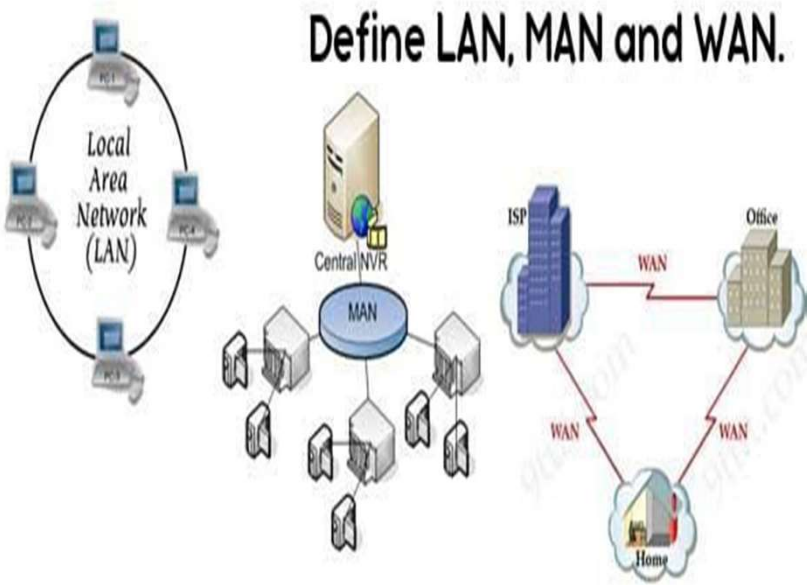
All ethical hackers should have:

- Expertise in scripting languages.
- Proficiency in operating systems.
- A thorough knowledge of networking.
- A solid foundation in the principles of information security.

Network Types on the bases of Geographical Area

Types of area networks – LAN, MAN and WAN



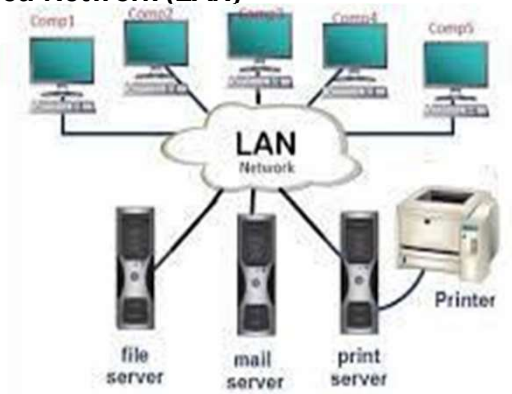


The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN,
MAN and WAN are the three major types of the network designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is

the geographical area they cover, i.e. **LAN** covers the smallest area; **MAN** covers an area larger than LAN and **WAN** comprises the largest of all.
There are other types of Computer Networks also, like :

- PAN (Personal Area Network)
- SAN (Storage Area Network)
- EPN (Enterprise Private Network)
- VPN (Virtual Private Network)

Local Area Network (LAN) –



LAN or Local Area Network connects network devices in such a way that personal computer and workstations can share data, tools and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol.
Private addresses are unique in relation to other computers on

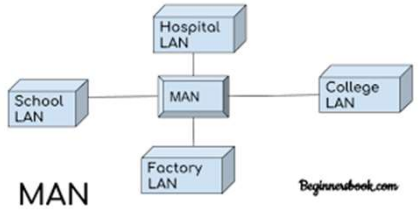
the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.
Data transmits at a very fast rate as the number of computers linked are limited. By definition, the connections must be high speed and relatively inexpensive hardware (Such as hubs,
network adapters and Ethernet cables). LANs cover smaller geographical area (Size is limited to a few kilometers) and are privately owned. One can use it for an office building, home,
hospital, schools, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

Early LAN's had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN. The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. The fault tolerance of a LAN is more and there is less congestion in this network. For example : A bunch of students playing Counter Strike in the same room (without internet).

Metropolitan Area Network (MAN) –
MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need a high-speed connectivity. Speeds of MAN ranges in terms of Mbps. It's hard to design and maintain a Metropolitan Area Network.

The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be

owned by a single organization. The data transfer rate and the propagation delay of MAN is moderate. Devices used for transmission of data through MAN are: Modem and Wire/Cable. Examples of a MAN are the part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.



Wide Area Network (WAN) –

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LAN's via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive.
There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long distance transmission, the noise and error tend to be more in WAN.

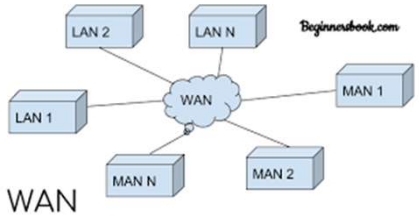
WAN's data rate is slow about a 10th LAN's speed, since it involves increased distance and increased number of servers and terminals etc. Speeds of WAN ranges from few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for transmission of data through WAN are: Optic wires, Microwaves and Satellites. Example of a Switched WAN is the asynchronous

transfer mode (ATM) network and Point-to-Point WAN is dial-up line that connects a home computer to the Internet.

Conclusion –

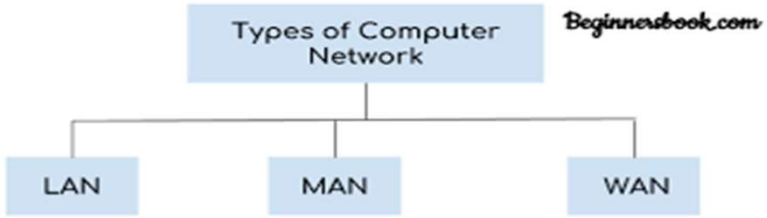
There are many advantages of LAN over MAN and WAN, such as LAN's provide excellent reliability, high data transmission rate, they can easily be managed, and shares peripheral devices too.

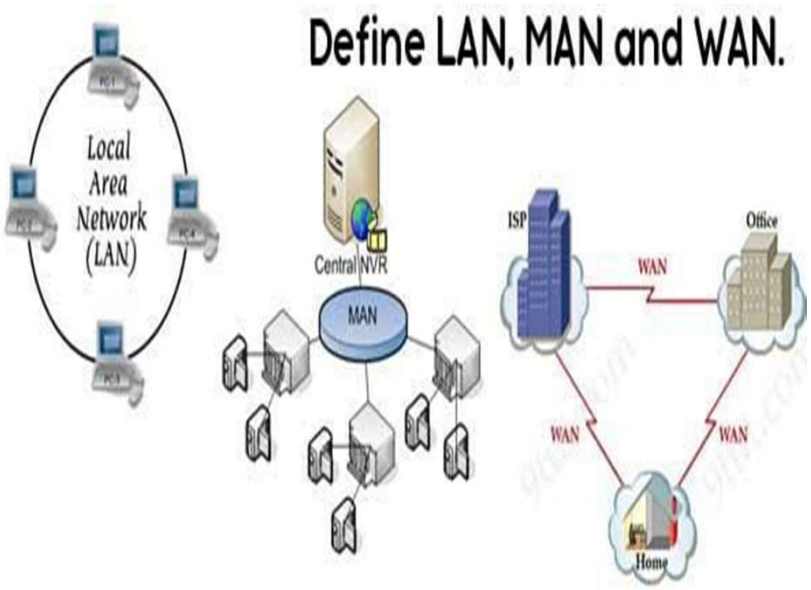
Local Area Network cannot cover cities or towns and for that Metropolitan Area Network is needed, which can connect city or a group of cities together. Further, for connecting Country or a group of Countries one requires Wide Area Network.



Network Types on the bases of Geographical Area

Types of area networks – LAN, MAN and WAN

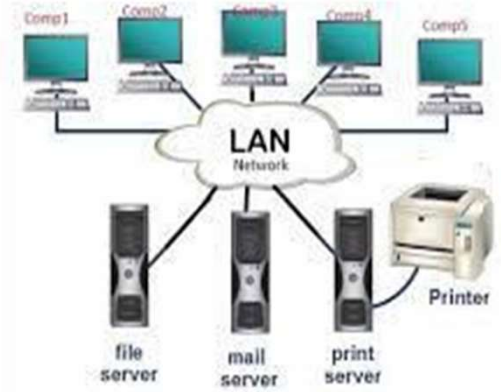




The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN,
MAN and WAN are the three major types of the network designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area; **MAN** covers an area larger than LAN and **WAN** comprises the largest of all.
There are other types of Computer Networks also, like :

- PAN (Personal Area Network)
- SAN (Storage Area Network)
- EPN (Enterprise Private Network)
- VPN (Virtual Private Network)

Local Area Network (LAN) –



LAN or Local Area Network connects network devices in such a way that personal computer and workstations can share data, tools and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol.

Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

Data transmits at a very fast rate as the number of computers linked are limited. By definition, the connections must be high speed and relatively inexpensive hardware (Such as hubs, network adapters and Ethernet cables). LANs cover smaller geographical area (Size is limited to a few kilometers) and are privately owned. One can use it for an office building, home, hospital, schools, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

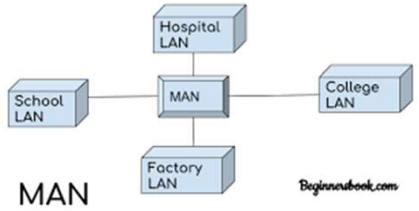
Early LAN’s had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN. The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN typically relies mostly on wired connections for increased

speed and security, but wireless connections can also be part of a LAN. The fault tolerance of a LAN is more and there is less congestion in this network. For example : A bunch of students playing Counter Strike in the same room (without internet).

Metropolitan Area Network (MAN) –

MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need a high-speed connectivity. Speeds of MAN ranges in terms of Mbps. It's hard to design and maintain a Metropolitan Area Network.

The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN is moderate. Devices used for transmission of data through MAN are: Modem and Wire/Cable. Examples of a MAN are the part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.



Wide Area Network (WAN) –

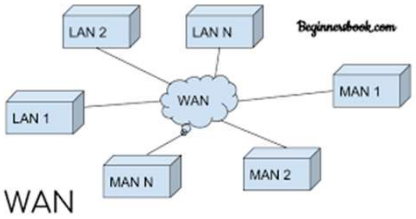
WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a

connection of LAN connecting to other LAN's via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive.
There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long distance transmission, the noise and error tend to be more in WAN.

WAN's data rate is slow about a 10th LAN's speed, since it involves increased distance and increased number of servers and terminals etc. Speeds of WAN ranges from few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for transmission of data through WAN are: Optic wires, Microwaves and Satellites. Example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is dial-up line that connects a home computer to the Internet.

Conclusion –

There are many advantages of LAN over MAN and WAN, such as LAN's provide excellent reliability, high data transmission rate, they can easily be managed, and shares peripheral devices too.
Local Area Network cannot cover cities or towns and for that Metropolitan Area Network is needed, which can connect city or a group of cities together. Further, for connecting Country or a group of Countries one requires Wide Area Network.



WAN