

Learning Outcome 1: Describe network concepts

Content/Topic 1: Network concepts and technologies

✓ **Definition of network**

A computer network is any set of computers or devices connected to each other with the ability to exchange data.

✓ **Advantages of network**

- A user can log on to a computer anywhere on the network and access their work files from the file server
- Computers can be managed centrally
- Time
- Sharing printers, modems etc saves money and time
- Security
- It is easy and convenient to monitor users –
- Peripherals such as printers can be shared amongst many different users.
- Software can be shared among different users.
- Communication across the network is cheap and fast.

✓ **Disadvantages of network**

1. Cabling can be expensive to install and replace.
2. A fault with the server will prevent the whole network from working.
3. Security measures are needed to restrict access to the network.
4. WANs are vulnerable to hackers and viruses.
5. If something goes wrong with the file server the whole network is unable to operate
6. The technical skills needed to manage a network are much higher than working on a stand-alone computer
7. Users may use too much bandwidth - for example when listening to music files or watching video clips - preventing others from using the network facilities properly

✓ **Application of network**

• **Communication and Collaboration**

Social Media: Platforms like Facebook, Instagram, and Twitter connect people worldwide, facilitating communication, sharing information, and building communities.

Email: One of the most fundamental network applications, email allows for efficient communication and information exchange.

Instant Messaging: Apps like WhatsApp, Messenger, and Telegram provide real-time text, voice, and video communication.

Video Conferencing: Tools like Zoom, Google Meet, and Microsoft Teams enable face-to-face meetings, regardless of location.

• **Information Access and Sharing**

Internet: The global network of networks provides access to a vast amount of information, including websites, online resources, and databases.

Cloud Computing: Networks enable the storage and access of data and applications on remote servers, providing scalability and flexibility.

File Sharing: Networks allow for the sharing of files, documents, and other digital content between devices.

• **Business and Industry**

Intranets: Private networks within organizations facilitate communication, collaboration, and information sharing among employees.

Extranets: Networks that connect an organization with its partners, suppliers, and customers.

E-commerce: Online businesses rely on networks to sell products and services, process payments, and manage inventory.

Remote Work: Networks enable employees to work from anywhere, improving flexibility and productivity.

• **Entertainment and Media**

Streaming Services: Platforms like Netflix, Hulu, and Spotify deliver movies, TV shows, and music over the internet.

Gaming: Online gaming allows players to compete and collaborate with others from around the world.

Social Media Influencers: Networks enable individuals to build large followings and monetize their content.

• **Education and Research**

Online Learning: Networks provide access to online courses, tutorials, and educational resources.

Research Collaboration: Scientists and researchers can collaborate and share data through networks.

Distance Education: Universities and colleges offer online degree programs and courses.

• **Government and Public Services**

E-Government: Governments use networks to deliver services to citizens, such as online registration, tax filing, and permits.

Public Safety: Networks are essential for emergency response, law enforcement, and public safety services.

✓ **Network classification**

Classifying network by components roles (working principle)

The network falls into two major architecture

- a) Peer to peer networks
- b) Client/server networks

1. Peer to peer

- Peer-to-peer networks are appropriate only for very small businesses or for home use.
- A peer-to-peer network can support about ten clients (workstations)
- computers are connected individuals in pair (one to one connection).
- There is no dedicated server. All the computers are equal.
- Each user has the right to decide what he would or would not like to share.

Each computer acts as both client and server. This arrangement is suitable in small office network.

Advantages	Disadvantages
inexpensive easy to set up easy maintenance No need for a network operating system Does not need an expensive server because individual workstations are used to access the files	security Scattering data

2. Client Server architecture

- ☐ This is a network Architecture in which each computer on the network is either a client or a server.
- ☐ Each client is connected to a centrally located dedicated computer called server.

Some different types of server:

- File server: managing files or disk drives
- Print server: to handle printing request
- Communication server: they are setup to handle remote users dialing into network
- Mail server: specially setup to handle client's email

Advantages	Disadvantages
<ul style="list-style-type: none"> ▪ All files are stored in a central location ▪ Network peripherals are controlled centrally ▪ Backups and network security is control centrally ▪ Users can access shared data which icentrally controlled 	<ul style="list-style-type: none"> ▪ A specialist network operating system needed ▪ The server is expensive to purchase ▪ Specialist staff such as a network manager needed ▪ If any part of the network fails a lot of disruptioncan occur

- Client: Computer that uses the services that a server provides. The client is less powerful than server.
- Server: Powerful computer that provides services to other computers on the net

Classifying network by geographical area

1. LAN (local area network)

- Local area network (LAN), which is usually a small network constrained to a smallgeographic area such as home, computer laboratory, office building...
- LAN is a fast small network

A local area network can be expanded to cover and interconnect several buildings in an area, the resulting network can be called Campus area network (CAN) or Campus environment.

2. MAN (Metropolitan Area Network).

Metropolitan area network (MAN), which is used for medium size area. Examples for a city and its surrounding or a state.

3. **Wide area network** (WAN)

Wide area network (WAN) that is usually a larger network that covers a large geographic area. It connects countries, continent even the whole world.

Other Type

- **Wireless LANs and WANs**(WLAN & WWAN) are the wireless equivalent of the LAN and WAN. Using acommunications channel that combines many types of media such as telephone lines, cables, and air waves
- **PAN** (personal area network) ex : Bluetooth

✓ Network Technologies

Networking technology allows for the exchange of data between large and small information systems used primarily bybusinesses and educational institutions.

- **IEEE802.3 Ethernet**
 - Ethernet is the most widely used standard for wired networks.

- Ethernet operates in the data link layer and the physical layer. It is a family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards.
 - Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies. For the Layer 2 protocols, as with all 802 IEEE standards, Ethernet relies on the two separate sub layers of the data link layer to operate, the Logical Link Control (LLC) and the MAC sub layers.
- **WI-FI(802.11)**
One of the most common networking standards used with wireless LANs is WI-FI(802.11) a family of wireless networking standard that use the IEEE802.11 standard
 - Access method: Carrier Sense Multiple Access/Collision Avoidance(CSMA/CA), a variation of CSMA/CD.
 - Topology: physical wireless, logical bus
 - **IEEE802.5 Token ring**
 - Token Ring is a LAN protocol defined in the IEEE 802.5 where all stations are connected in a ring and each station can directly hear transmissions only from its immediate neighbor.
 - Permission to transmit is granted by a message (token) that circulates around the ring.
 - A token is a special bit pattern (3 bytes long). There is only one token in the network.
 - **IEEE802.8 Fiber optic**
This is the technology of IEEE that introduced the use of Fiber Optic cable that enables an Internet service provider to provide higher bandwidth speeds and support more services such as Internet, phone, and TV in large distance.

Content/Topic 2. Description of Network topology

✓ **Definition of topology**

A network topology is the physical and logical arrangement of nodes and connections in a network. Administrators can use network topology diagrams to determine the best placements for each node and the optimal path for traffic flow.

With a well-defined and planned-out network topology, an organization can more easily locate faults and fix issues, improving its data transfer efficiency.

✓ **Network topology types**

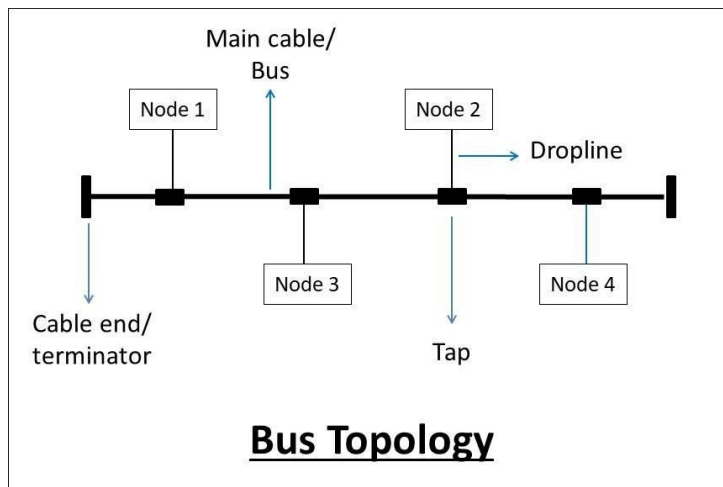
Physical – The physical network topology refers to the actual connections (wires, cables, etc.) of how the network is arranged.

Logical – The logical network topology is a higher-level idea of how the network is set up, including which nodes connect to each other and in which ways, as well as how data is transmitted through the network.

Physical Topology

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

When a sender sends a message, all other computers can hear it, but only the receiver accepts it (verifying the mac address attached with the data frame) and others reject it. Bus technology is mainly suited for small networks like LAN, etc.



In this topology, the bus acts as **the backbone** of the network, which joins every computer and peripherals in the network. Both ends of the shared channel have line terminators.

The data is sent only in one direction and as soon as it reaches the end, the terminator removes the data from the communication line (to prevent signal bounce and data flow disruption).

Taps are the connectors, while **droplines** are the cables connecting the bus with the computer. In other words, there is only a single transmission line for all nodes.

Following are the advantages of Bus topology:

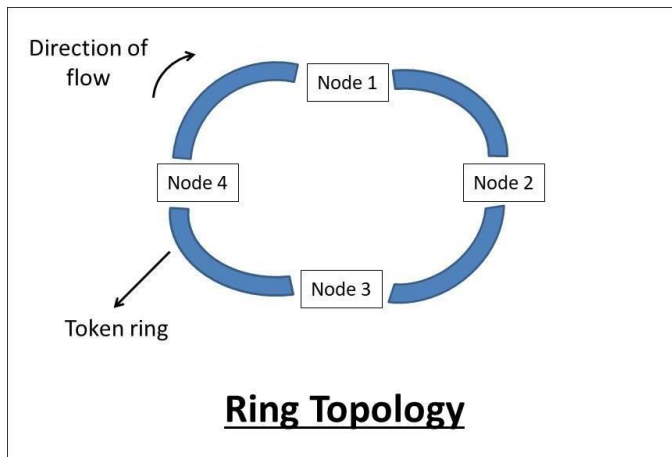
1. Simple to use and install.
2. If a node fails, it will not affect other nodes.
3. Less cabling is required.
4. Cost-efficient to implement.

Following are the disadvantages of Bus topology:

1. Efficiency is less when nodes are more (strength of signal decreases).
2. If the bus fails, the network will fail.
3. A limited number of nodes can connect to the bus due to limited bus length.
4. Security issues and risks are more as messages are broadcasted to all nodes.
5. Congestion and traffic on the bus as it is the only source of communication.

2. Ring Topology

Ring topology is a topology in which each computer is connected to exactly two other computers to form the ring. The message passing is unidirectional and circular in nature.



This network topology is deterministic in nature, i.e., each computer is given access for transmission at a fixed time interval. All the nodes are connected in a closed-loop. This topology mainly works on a token-based system and the token travels in a loop in one specific direction.

In a ring topology, if a token is free then the node can capture the token and attach the data and destination address to the token, and then leaves the token for communication. When this token reaches the destination node, the data is removed by the receiver and the token is made free to carry the next data.

For Example, Token Ring, etc.

Following are the advantages of Ring topology:

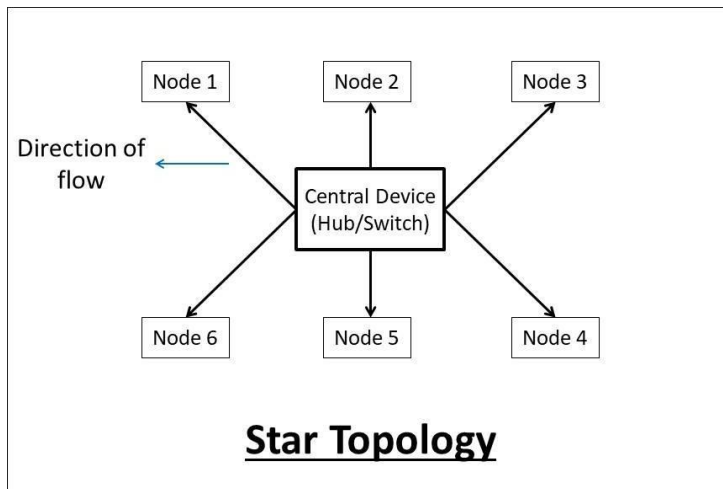
1. Easy Installation.
2. Less Cabling Required.
3. Reduces chances of data collision(unidirectional).
4. Easy to troubleshoot(the faulty node does not pass the token).
5. Each node gets the same access time.

Following are the disadvantages of Ring topology:

1. If a node fails, the whole network will fail.
2. Slow data transmission speed(each message has to go through the ring path).
3. Difficult to reconfigure(we have to break the ring).

3. Star Topology

Star topology is a computer network topology in which all the nodes are connected to a centralized hub. The hub or switch acts as a middleware between the nodes. Any node requesting for service or providing service, first contact the hub for communication.



In a star topology, hub and switch act as a server, and the other connected devices act as clients. Only one input-output port and one cable are required to connect a node to the central device. This topology is better in terms of security because the data does not pass through every node.

For Example High-Speed LAN, etc.

Following are the advantages of Star topology:

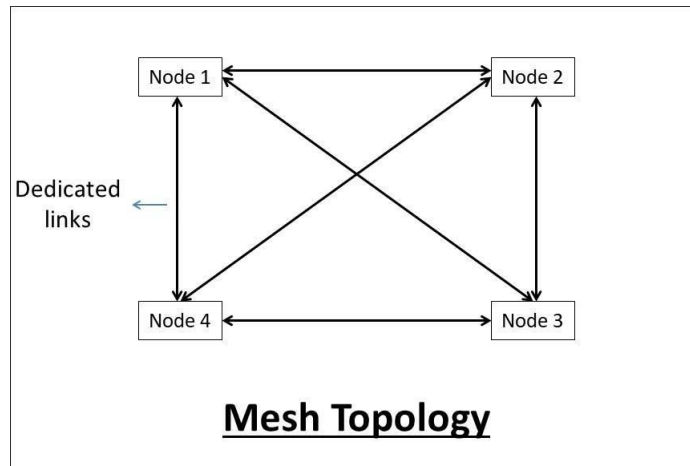
1. Centralized control.
2. Less Expensive.
3. Easy to troubleshoot(the faulty node does not give response).
4. Good fault tolerance due to centralized control on nodes.
5. Easy to scale(nodes can be added or removed to the network easily).
6. If a node fails, it will not affect other nodes.
7. Easy to reconfigure and upgrade(configured using a central device).

Following are the disadvantages of Star topology:

1. If the central device fails, the network will fail.
2. The number of devices in the network is limited(due to limited input-output port in a central device).

4. Mesh Topology

Mesh topology is a computer network topology in which nodes are interconnected with each other. In other words, direct communication takes place between the nodes in the network.



There are mainly two types of Mesh:

1. **Full Mesh:** In which each node is connected to every other node in the network.
2. **Partial Mesh:** In which, some nodes are not connected to every node in the network.

Lets say we have **n** devices in the network then each device must be connected with **(n-1)** devices of the network. Number of links in a mesh topology of n devices would be **$n(n-1)/2$** .

For Example, the Internet(WAN), etc.

Following are the advantages of Mesh topology:

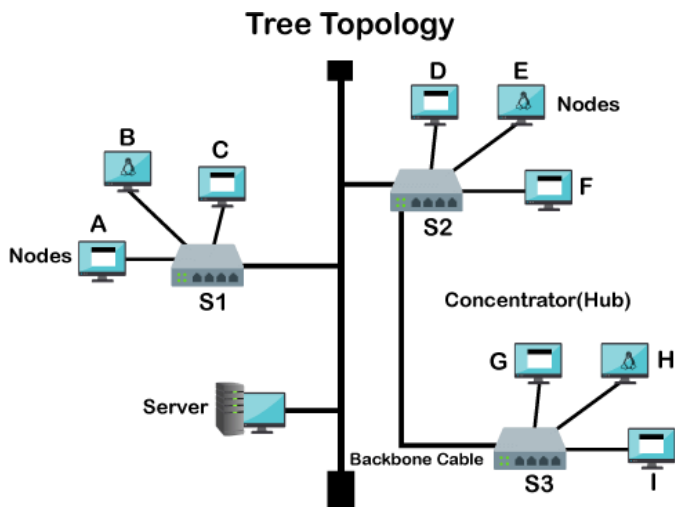
1. Dedicated links facilitate direct communication.
2. No congestion or traffic problems on the channels.
3. Good Fault tolerance due to the dedicated path for each node.
4. Very fast communication.
5. Maintains privacy and security due to a separate channel for communication.
6. If a node fails, other alternatives are present in the network.

Following are the disadvantages of Mesh topology:

1. Very high cabling required.
2. Cost inefficient to implement.
3. Complex to implement and takes large space to install the network.
4. Installation and maintenance are very difficult.

5. Tree Topology:

Tree topology is a computer network topology in which all the nodes are directly or indirectly connected to the main bus cable. Tree topology is a combination of Bus and Star topology.



In a tree topology, the whole network is divided into segments, which can be easily managed and maintained. There is a main hub and all the other sub-hubs are connected to each other in this topology.

Following are the advantages of Tree topology:

1. Large distance network coverage.
2. Fault finding is easy by checking each hierarchy.
3. Least or no data loss.
4. A Large number of nodes can be connected directly or indirectly.
5. Other hierarchical networks are not affected if one of them fails.

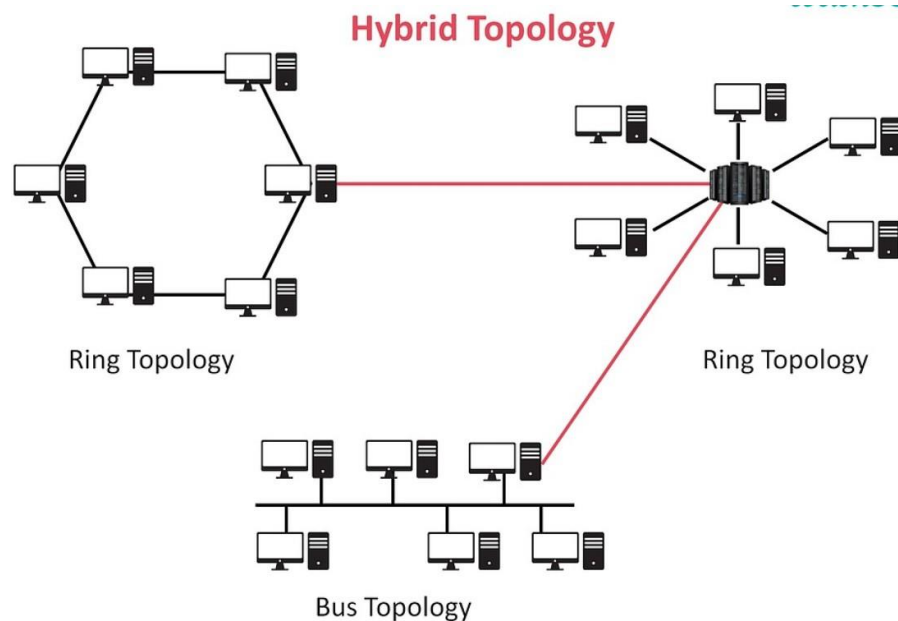
Following are the disadvantages of Tree topology:

1. Cabling and hardware cost is high.
2. Complex to implement.

3. Hub cabling is also required.
4. A large network using tree topology is hard to manage.
5. It requires very high maintenance.
6. If the main bus fails, the network will fail.

6. Hybrid Topology:

A Hybrid topology is a computer topology which is a combination of two or more topologies. In practical use, they are the most widely used.



In this topology, all topologies are interconnected according to the needs to form a hybrid. All the good features of each topology can be used to make an efficient hybrid topology.

Following are the advantages of Hybrid topology:

1. It can handle a large volume of nodes.
2. It provides flexibility to modify the network according to our needs.
3. Very Reliable (if one node fails it will not affect the whole network).

Following are the disadvantages of Hybrid topology:

1. Complex design.
2. Expensive to implement.
3. Multi-Station Access Unit (MSAU) required.

Some points need to be considered when selecting a physical topology:

- Ease of Installation.
- Fault Tolerance.
- Implementation Cost.
- Cabling Required.
- Maintenance Required.
- Reliable Nature.
- Ease of Reconfiguration and upgradation.

Content/Topic 3: Description of Network components

- ✓ **Media:** Network media is the actual path over which an electrical signal travels as it moves from one component to another.

Transmission medium is of two types:

(i) **Physical or Wired or Guided:** For example, Twisted Pair Cable, Coaxial Cable and Optical Fiber Cable.

(ii) **Logical or Wireless or Unguided:** For example, Radio waves, Microwaves and Infrared.

- ✓ **Data:** In general, a message is any grouping of information at the application layer (layer 7) of the Open Systems Interconnection (OSI) reference model that is exchanged between applications for various purposes.
- ✓ **Protocol:** A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network.
- ✓ **Devices:** The devices which are used for communication between different hardware's used in the computer network are known as network devices. These devices are also known as physical devices, networking hardware, and network equipment otherwise computer networking devices.

Here are the common network devices:

- o Router
- o Hubs
- o Switch
- o NIC
- o Repeater
- o MAU
- o Firewall
- o Access point
- o Gateway
- o Antenna...

Content/Topic 4: Classification of network devices

Network device can be classified as:

- ✓ Interconnection devices
- ✓ Access devices
- ✓ End devices

A) Interconnection devices

Interconnection device is any device that can enable computers to exchange data on a network.

1) **Repeater** : Repeaters are non-intelligent network devices that receive a signal through one port.

- ☐ They regenerate that signal and then transmit the signal again on all remaining ports.
- ☐ To extend the length of a network, repeaters can be used to connect network segments (a portion of a computer network) but they can't be used to connect different networks using different access methods.
- ☐ Repeaters reduce the loss of signal along a cable (known as attenuation) which in turn provides a more stable connection to the devices connected the repeater.

2) Bridge

- ☐ They are used to connect two or more LANs of the same type, e.g. Ethernet to Ethernet.
- ☐ Unlike repeaters, a bridge can extend the capacity as well as the length of a network because each port on a bridge has a MAC address.

3) Switch

A network switch connects devices (such as computers, printers, wireless access points) in a network to each other, and allows them to 'talk' by exchanging data packets.

4) Router:

The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets.

B) Access devices

Network access device is any device that help a user (end device) to get connected on a network.

i) Network Interface Card (NIC)

Network Interface Card (NIC) is a **hardware component** that is present on the computer. It is used to **connect different networking devices** such as computers and servers to share data over the connected network.

There are the following two types of NICs -

1. Ethernet NIC

It is made by ethernet cables. This type of NIC is most widely used in the LAN, MAN, and WAN networks.

Example: TP-LINK TG-3468 Gigabit PCI Express Network Adapter.

2. Wireless Networks NIC

It is a wireless network that allows us to connect the devices without using the cables. These types of NICs are used to design a Wi-Fi connection.

Example: Intel 3160 Dual-Band Wireless Adapter

The NIC also contains a MAC address (also known as a hardware address) which is a unique, 48-bit identifier used by many networking protocols including Ethernet and 802.11 wireless.

A MAC address looks something like this: 65:85:45: F2:C3:8E

ii) Hub

Hubs are used in Ethernet networks to connect multiple Ethernet devices together, forming a network segment (group of computers that is a portion of a network). A hub, like a repeater has no intelligence so simply broadcasts all network data across all ports.

iii) Access point

Access point An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.

C) End devices

What are End Network Devices?

The network devices that people are most familiar with are called end devices. These devices form the interface between the human network and the underlying communication network. Some examples of end devices are:

- ☐ **Computers , laptops, file servers, web servers.**
- ☐ **Network printers**
- ☐ **VoIP phones**
- ☐ **Security cameras**
- ☐ **Mobile handheld devices.**

Content/Topic 5: Description network models

The networking model **describes the architecture, components, and design used to establish communication between the source and destination systems.**

There are two basic types of networking models:

- ❑ **Protocol model** - This model closely matches the structure of a particular protocolsuite. The hierarchical set of related protocols in a suite typically represents all the functionality required to interface the human network with the data network. The TCP/IP model is a protocol model, because itdescribes the functions that occur at each layer of protocols within the TCP/IP suite.
- ❑ **Reference model**
A layered model, such as the TCP/IP model, is often used to help visualize the interaction between various protocols. A layered model depicts the operation of the protocols occurring within each layer, as well as theinteraction of protocols with the layers above and below each layer.

A reference model is not intended to be an implementation specification or to provide a sufficient level of detailto define precisely the services of the network architecture. The primary purpose of a reference model is to aid in clearer understanding of the functions and processes involved.

There are benefits to using a layered model to describe network protocols and operations. Using a layered model:

- Assists in protocol design, because protocols that operate at a specific layer have defined information that theyact upon and a defined interface to the layers above and below.
- Fosters competition because products from different vendors can work together.
- Prevents technology or capability changes in one layer from affecting other layers above and below.
- Provides a common language to describe networking functions and capabilities.

There are 2 predominant models available.

- 1) Open Systems Interconnection (OSI) Model
- 2) Transmission Control Protocol/Internet Protocol (TCP/IP) Model

OSI Model

OSI stands for Open System Interconnect. It is an open standard for establishing communication between systems.

- ❑ **Application Layer:** The entire process begins at the end user's device. This can be a phone, laptop, server, etc. The application layer provides the interface for data exchange between the program and the user. For example, Facebook's web application/mobile application is the interface through which we like, share, comment,and perform various other activities.

- **Presentation Layer:** The presentation layer ensures the translation of characters from the original format in the host system to the format of the receiving system. It also adds encryption and decryption features. Data compression is handled at this layer.
- **Session Layer:** The inclusion of this layer enables maintaining sessions during browsing. This helps with implementing authentication, authorization, synchronization, and dialog control. Let us consider examples to appreciate the significance of the session layer.
 - Authentication: Once a user logs in, he/she should remain logged in until he/she logs out. Obtaining the status of a user's authentication happens at this layer.
 - Authorization: Access rights to specific parts of a website are given to super-users and admins.
 - Dialog Control: Allows various systems running applications like WebEx to communicate. The challenge here is to send and receive data simultaneously, that is overcome by half-duplex or full-duplex protocols under the session layer.
 - Synchronization: The digital experience relies on audio and video being synchronized. The session layer ensures the timestamps of the audio and video received are in the right order.
- **Transport Layer:** The transport layer is the fourth layer in the OSI model and enables the following services:
 - Reliability: This layer ensures that a packet sent is received without corruption. If not, the packet is resent. This may add a delay. But, it is suitable for applications where data integrity is a must.
 - Flow-Control: The rate of sending information is limited by the buffer size and the receiver capacity. The delays caused due to propagation, queueing, and transmission are taken into account by the flow-control algorithms.
 - Congestion Control: In routers, the entry of packets can be decided based on the current traffic.
 - Multiplexing and Demultiplexing: Before the transport layer, the ports do not play a major role. The ports can be thought of as multiple inputs to the same network channel. The transport Layer enables multiplexing of various application inputs. On the receiving end, the transport layer sends the packets to corresponding ports. This action is similar to that of demux.

- **Network Layer:** The network layer is one of the most important layers. It enables many features such as:
 - Address Assignment: IP addresses are assigned to the host. There are two ways of assigning addresses: Static and Dynamic. Static addresses are assigned manually and do not change under any circumstances. Dynamic IP's, on the other hand, are assigned on an as-needed basis.
 - Routing: Selecting the route can be done manually or automatically. Today, most of it is automatic. There are two predominant algorithms used for routing: Distance Vector Routing and Link State Routing.
 - Fragmentation: Within the transport layer, there is a constraint on the maximum allowable size for data. Therefore, bits are segmented accordingly in the transport layer. Fragmentation is the same process applied to the segmented packets received from the transport layer. The aim is to accommodate datagrams received from the transport layer into frames.
- **Data Link Layer:** The main responsibility of the Data Link Layer (DLL) is ensuring Flow Control, Error Control, Access Control, Framing, and the reading of physical addresses. We will go over each of the processes in detail:
 - Framing: The process of taking a packet from the layer above and adding a frame to the packet is called framing. The frame includes data such as the end of the packet, message length, etc. to achieve accurate information at the receiving end.
 - Flow Control: DLL restricts the size of the traffic and waits for the receiver to acknowledge the first batch of frames before sending the next batch.
 - Error Control: Due to long-distance transmission, sometimes the bits of information might get corrupted. The corruption of bits leads to poor service. Listed below are a couple approaches to handling data corruption.
 - Discarding the data corruption bits
 - Repairing the corrupted bits

- There are other error correction algorithms like Cyclic Redundancy Check, Checksum, Parity Bits, etc.
- **Physical Layer:** This layer deals with electrical, mechanical, functional, and procedural characteristics of physical links.

Network topology comes under this layer. One prominent aspect of the physical layer is encoding.

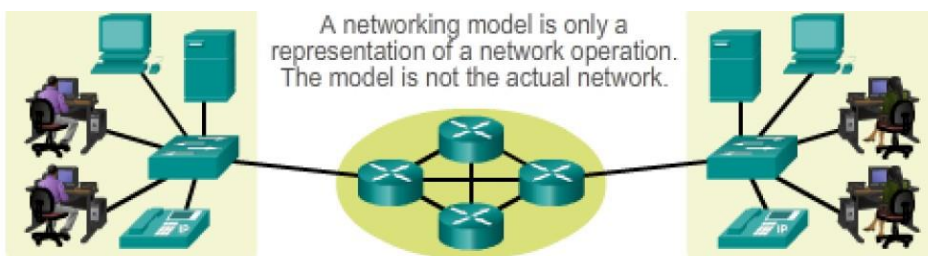
Encoding refers to the representation of data. The objective of encoding is to ensure the maximum probability that the message, being transmitted is sent without any errors.

TCP/IP Model

The network of networks that we refer to as the Internet is based on the [TCP/IP model](#). Therefore, it is also referred to as the TCP/IP Protocol Suite. It is a four-layered architecture specifically built for the internet.

The internet requires the following features:

- Reliability
- Security
- Traffic Efficiency



OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	PPP, Frame Relay, Ethernet	Network Access
Physical		

TCP/IP model uses TCP in the transport layer and IP in the network layer. The four layers of the network model are as follows.

- **Application Layer:** In the TCP/IP Model, the Application layer encompasses the first three layers in the OSI model, that is, Application layer, Presentation layer, and the Session Layer.
- **Transport Layer:** This layer is the same as the one mentioned in the OSI model. Transmission Control Protocol (TCP) is used in this model. TCP ensures reliability and helps avoid congestion in networks.
- **Network Layer:** Internet Protocol (IP) is used predominantly in this layer. Until recently, IPv4 was the most common protocol in use. It provided 32 bits for assigning addresses. It supported around 4.29 million unique devices, and therefore IPv6 was introduced. IPv6 is the protocol that allows 4.3 billion devices. It has 128 bits assigned for the network address.
- **Network Interface:** It enables the transmission of data. The layer corresponds to the data link layer and the physical layer in the OSI Model.

Learning Outcome 2: Apply network protocols and communications

Content/Topic 1: Description of Network Protocols

✓ Definition of network protocol

A network protocol defines rules and conventions for communication between network devices. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received.

✓ Common network protocols models

□ NetBEUI

NetBEUI: Pronounced net-booeey, NetBEUI is short for NetBios Extended User Interface. It is an enhanced version of the NetBIOS protocol used by network operating systems such as LAN Manager, LAN Server, Windows for Workgroups, Windows 95 and Windows NT

NetBEUI is also self-tuning and implements flow control and error detection. It defines a framing mechanism at the transport layer and implements the LLC2 protocol of the Open Systems Interconnection (OSI) reference model for networking.

□ TCP/IP


Transmission Control Protocol (TCP) is the transport protocol that manages the individual conversations between web servers and web clients. TCP divides the HTTP messages into smaller pieces, called segments. These segments are sent between the web server and client processes running at the destination host. TCP is also responsible for controlling the size and rate at which messages are exchanged between the server and the client.



Internet Protocol

IP is responsible for taking the formatted segments from TCP, encapsulating them into packets, assigning them the appropriate addresses, and delivering them across the best path to the destination host.

□ Novell NetWare

- A local-area network (LAN) operating system developed by Novell Corporation.
- It provides users and programmers with a consistent interface that is independent of the actual hardware used to transmit messages.
- NetWare is a computer network operating system developed by Novell, Inc. It initially used cooperative multitasking to run various services on a personal computer, using the IPX network protocol.

 IPX/SPX (IPX): Short for Internetwork Packet Exchange, a networking protocol used by the Novell NetWare operating systems. Like UDP/IP, IPX is a datagram protocol used for connectionless communications.

 IPX provides datagram services over packet-switched internetworks.  IPX and IP are connectionless datagram protocols.

- ✚ Its basic operation is similar to IP (Internet Protocol), but its addressing scheme, packet structure, and general scope are different
- ✚ (SPX): Short for Sequenced Packet Exchange, a transport layer protocol (layer 4 of the OSI Model) used in Novell Netware networks.
- ✚ The SPX layer sits on top of the IPX layer (layer 3) and provides connection-oriented services between two nodes on the network. SPX is used primarily by client/server applications.

☐ **AppleTalk**

- ✚ AppleTalk's purpose was to allow multiple users to share resources, such as files and printers. AppleTalk includes a number of features that allow local area networks to be connected with no prior setup or the need for a centralized router or server of any sort.

- ☐ **OSI** : The OSI model is the most widely known internetwork reference model. It is used for data network design, operation specifications, and troubleshooting.

☐ **CISCO**

Content/Topic 2: Identification of Network standards

✓ Definition network of standard

A standard is a set of rules or guidelines approved and monitored by an authorized organization

- ☐ Networking standards ensure the interoperability of networking technologies by defining the rules of communication among networked devices.
- ☐ Networking standards exist to help ensure products of different vendors are able to work together in a network without risk of incompatibility.
- ☐ The International Organization for Standardization (ISO) lays out those standards.

✓ Importance of standards

- ☐ **The primary reason for standards** is to ensure that hardware and software produced by different vendors can work together.
- ☐ to develop networks that easily share information.
- ☐ Standards also mean that customers are not locked into one vendor.
- ☐ They can buy hardware and software from any vendor whose equipment meets the standard. In this way, standards help to promote more competition and hold down prices.
- ☐ The use of standards makes it much easier to develop software and hardware that link different networks because software and hardware can be developed one layer at a time.

Some of the benefits of having approved and established standards for activities, products or services are listed below:

- ☐ Increased safety and reliability
- ☐ Protection inflammatory business interests
- ☐ Enables interoperability among various devices
- ☐ Encourages innovation and increases competition

Let's look at some of the ramifications that may occur without standards:

- ☐ Faulty product operation
- ☐ Inferior quality
- ☐ Incompatibility with other devices
- ☐ Increases risk for danger due to lack of safety standards
- ☐ Less manufacturers - limiting selection

✓ **Internet standards**

Internet standard (STD) is a specification that has been approved by the Internet Engineering Task Force (IETF). Such standard helps to promote a consistent and universal use of the internet worldwide.

✓ **Types of standards**

1. De Facto standards

De facto means by tradition or by facts. These standards are developed without any formal planning. These standards come into existence due to historical developments. These standards are still being used by many organizations in the world. Here are a few examples of de facto standards:

- The QWERTY keyboard
- Microsoft's Windows operating system, along with commonly used business applications such as Microsoft Word and Excel
- A navigation aid used when moving through a website that indicates the current page in relation to the website's remaining pages.

2. De Jure standards: De jure means according to law or regulation. These standards are developed with proper research to fulfill the requirement of data communication. The major organization to develop communication protocols and standards are as follows:

- a) American national standard institute (ANSI)
- b) Institute of electrical and electronics engineers (IEEE)
- c) International standard organization (ISO)

These standards are critically assessed before being approved. An example of a de jure standard is the

ASCII character set. Some de jure hardware standards include **USB**, **FireWire** and **HDMI**.

✓ **Standards organizations**

- Help ensure that equipment from different manufacturers can be integrated
- Key role in growth of networks and network equipment

ANSI	American National Standards Institute
IEEE	Institute of Electrical and Electronics Engineers
ITU	International Telecommunications Union
ISO	International Organization for Standardization
ISOC	Internet Society
IETF	Internet Society and the Internet Engineering Task Force
EIA/TIA	Electronic Industries Alliance and the Telecommunications Industry Association

ANSI (American National Standards Institute)

- **Established in 1918**
- **Standards for wide range of products**
- **Computer industry standards:**
 - **Screen-display attributes**
 - **Digital telecommunications**
 - **Fiber-optic cable transmissions**

IEEE (Institute of Electrical and Electronic Engineers)

- International society composed of engineering professionals
- Goals are to promote development and education in electrical engineering and computer science

ITU-Formally CCITT: The standardization efforts of ITU started in 1865 with the formation of the International Telegraph Union (ITU). ITU became a specialized agency of the United Nations in 1947.

The International Telegraph and Telephone Consultative Committee (French: Comité Consultatif International, CCITT) was created in 1956, and was renamed ITU-T in 1993. Téléphonique et Télégraphique.

ISO (International Standards Organization)

Collection of organization standards representing 146 countries • Goal is to establish international technological standards to facilitate global exchange of information and barrier-free trade

ISOC and IETF

- **ISOC (Internet Society)**
- **Professional membership society that helps to establish technical standards for the Internet**
 - **Supporter of Internet Corporation for Assigned Names and Numbers (ICANN)**
- **IETF** (Internet Engineering Task Force) : The IETF sets the standards that govern how much of the Internet will operate

(EIA): Electronic Industries Alliance (EIA): Trade organization composed of representatives from electronics manufacturing firms across US – Sets standards for its members – Helps write ANSI standards – Lobbies for legislation favorable to growth of computer and electronics industries

ITU • International Telecommunication Union • Regulates international telecommunications: – Radio and TV frequencies – Satellite and telephony specifications – Networking infrastructure – Tariffs applied to global communications • Typically, documents pertain more to global telecommunications issues than to industry technical specifications

EIA: Founded in 1924, the EIA is a U.S. organization of electronics manufacturers. The primary EIA standards for telecommunication define the serial interface between modems and computers. The most popular are the RS-232-C, RS-449, RS-422, and RS-423 serial interfaces.

Telcordia Is a standard uses a series of models for various categories of electronic, electrical and electro-mechanical components to predict steady-state failure rates which environmental conditions, quality levels, electrical stress conditions and various other parameters affect.

Content/Topic 3: Description of Network Media and Transmission

Network media refers to the communication channels used to interconnect nodes on a computer network. Typical examples of network media include copper coaxial cable, copper twisted pair cables and optical fiber cables used in wired networks, and radio waves used in wireless data communications networks.

✓ Types of Network Media

- Logical (wireless)
- Physical

Logical (Wireless)

The term logical media is used to refer to any type of electrical or electronic operation which is done without the use of “hard wired” connections. It is also referred to as Wireless or unbounded transmission media. Features:

- The signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 major types of Signals transmitted through logical media:

☐ **Radio waves**

These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range: 3 KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.

☐ **Microwaves**

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range: 1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

☐ **Infrared**

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range: 300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Physical

Physical media refers to the physical materials that are used to transmit information in data communications. These physical media are generally physical objects made of materials such as copper or glass. They can be touched and felt, and have physical properties such as weight and color. Features:

- High Speed
- Secure
- Used for comparatively shorter distances

1. Copper media

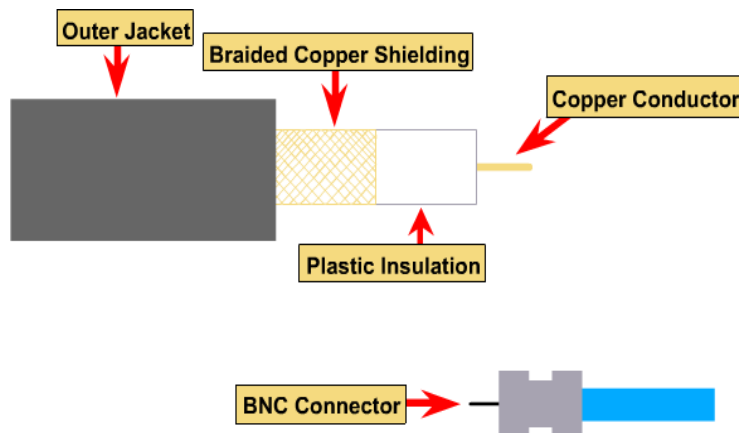
There are three main types of copper media used in networking:

- ☐ Unshielded Twisted-Pair (UTP)
- ☐ Shielded Twisted-Pair (STP)
- ☐ Coaxial

Coaxial Cable

Coaxial cable, or coax as it is commonly referred to, has been around for a long time. Coax found success in both TV signal transmission as well as in network implementations.

Construction of coaxial cabling



Coax is constructed with a copper core at the center that carries the signal, plastic insulation, braided metal shielding, and an outer plastic covering. Coaxial cable is constructed in this way to add resistance to attenuation (the loss of signal strength as it travels over distance), crosstalk (the degradation of a signal caused by signals from other cables running close to it), and EMI (electromagnetic interference).

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantage: Single cable failure can disrupt the entire network

There are two types of coaxial cabling.

- **Thinnet** is used for short-distance. The maximum length of thinnet is 185 meters
 - **Thicknet**. It supports data transfer over longer distances than thinnet. The maximum length of thinnet is 500meters
- ☐ Pairs of copper wires are encased in color-coded plastic insulation and twisted together.
 - ☐ An outer jacket, called poly-vinyl chloride (PVC), protects the bundles of twisted pairs.

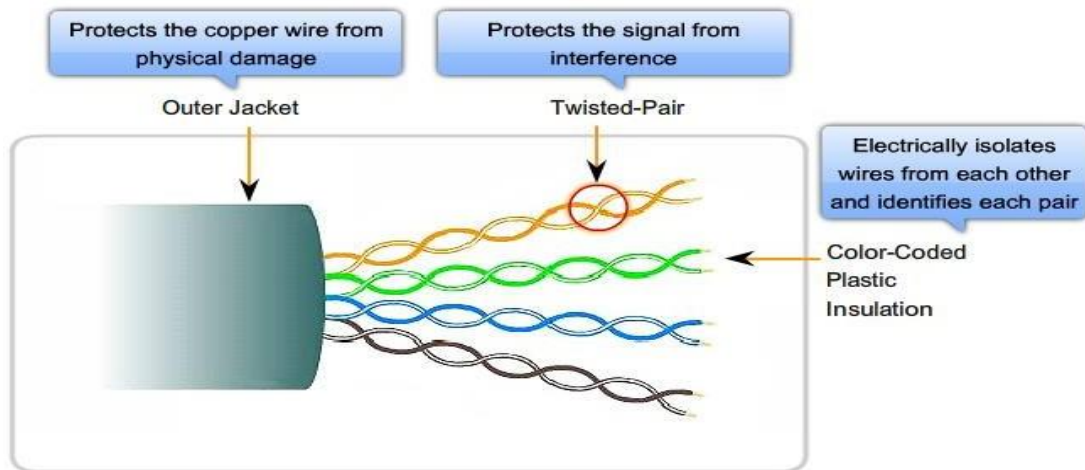
2. Twisted-Pair Cabling

- A pair of twisted wires forms a circuit that transmits data.

The twisted wires provide protection against crosstalk (electrical noise) because of the cancellation effect

Two Basic Types of Twisted-Pair Cables

- **Unshielded twisted-pair (UTP)**



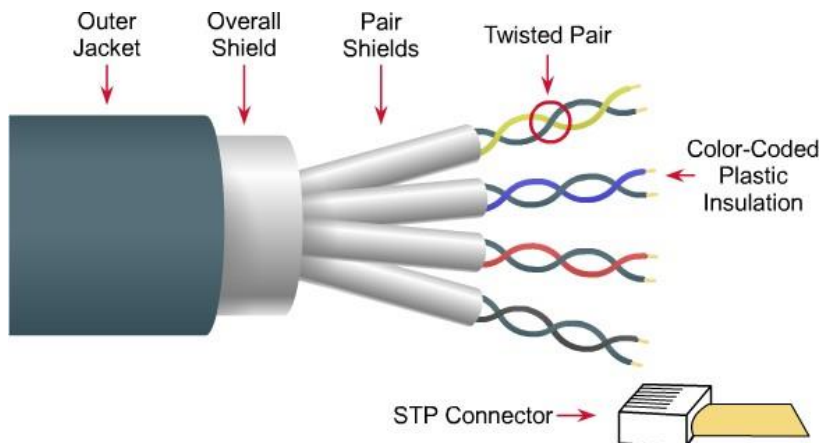
Has two or four pairs of wires

Relies on the cancellation effect for reduction of interference caused by electromagnetic interference (EMI) and radio frequency interference (RFI)

Most commonly used cabling in networks

Has a range of 328 ft (100 meters)

- **Shielded twisted-pair (STP)**



Each pair is wrapped in metallic foil to better shield the wires from electrical noise and then the four pairs of wires are then wrapped in an overall metallic braid or foil.

Reduces electrical noise from within the cable.

Reduces EMI and RFI from outside the cable

BENEFITS/DISADVANTAGES

- **Shielded Twisted Pair**

- Provides resistance to EMI and radio frequency
- Must be grounded at both end for high frequency signals
- Cancellation and twisting of wires, shielding reduces internal and external sources of interference.

- More expensive than UTP
- Cable length 100m

ScTP: Screened twisted-pair (ScTP) cabling is a hybrid of UTP and STP cable. ScTP cable typically consists of four pairs of 100 ohm, 24 AWG wire that are unshielded, but surrounded by a shield of foil and includes a single drainwire used for grounding. ScTP is less susceptible to noise because of the foil shield.

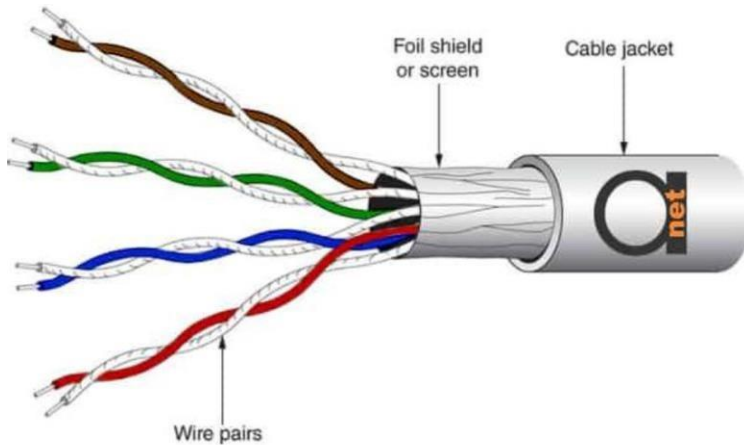


Figure: Screened twisted-pair (ScTP)

Advantages:

- Cheaper and far easier to splice
- Less susceptible to electrical interference caused by nearby equipment or wires.
- In turn are less likely to cause interference themselves.
- Because it is electrically "cleaner", STP wire can carry data at a faster speed.

Disadvantages:

- STP wire is that it is physically larger and more expensive than twisted pair wire.
- STP is more difficult to connect to a terminating block.

▪ **FSTP(Shielded and Foiled Twisted Pair)**

A combination of the two above, with foil shielding around the individual twisted wires and an overall screen which can sometimes be a flexible braid. This provides the maximum level of protection from interference and is found in the highest performance cables.

3. Fiber-Optic Cable

- A glass or plastic strand that transmits information using light and is made up of one or more optical fibers enclosed together in a sheath or jacket.
- Not affected by electromagnetic or radio frequency interference.
- Signals are clearer, can go farther, and have greater bandwidth than with copper cable.
- Usually more expensive than copper cabling and the connectors are more costly and harder to assemble.

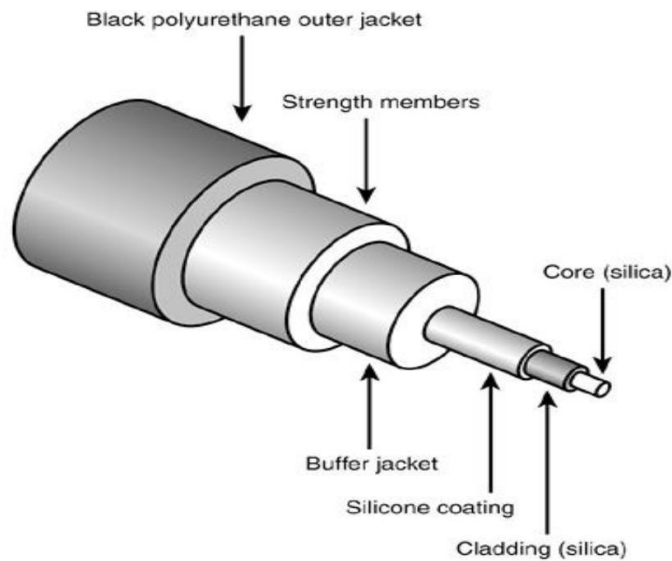


Fig.15: Composition of a fiber-optic cable

Two types of glass fiber-optic cable:

- **Single-mode**

- Single-mode fiber cable allows only one mode of light to propagate through the fiber.
- It is capable of higher bandwidth and greater distances than multimode, and it is often used for campus backbones.
- This type of fiber uses lasers as the light-generating method.
- Single-mode cable is much more expensive than multimode cable.
- Its maximum cable length is more than 10 km.

- **Multimode**

- Multimode fiber cable allows multiple modes of light to propagate through the fiber.
- It is often used for workgroup applications and intra building applications such as risers.
- It uses light-emitting diodes (LEDs) as a light-generating device.
- The maximum cable length is 2 km.

Fiber optics has several advantages over traditional metal communications lines:

- Fiber optic cables have a much greater bandwidth than metal cables.
- An optical fiber offers low power loss
- Fiber optic cables are immune to electromagnetic interference.
- Fiber optic cables are much thinner and lighter than metal wires.
- Since the fiber is a dielectric, it does not present a spark hazard.
- Fiber optic cables are less susceptible than metal cables to interference
- Data can be transmitted digitally (the natural form for computer data) rather than analogically.

The main disadvantage of fiber optics is that the cables are expensive to install. In addition, they are more fragile than wire and are difficult to split.

- ☐ transmission on optical fiber requires repeating at distance intervals.
- ☐ Cables are expensive to install but last longer than copper cables.
- ☐ Fibers can be broken or have transmission losses when wrapped around curves of only a few centimetres radius
- ☐ Optical fibers require more protection around the cable compared to copper.

✓ Baseband and broadband transmission technologies

Baseband Transmission is a transmission technique that one signal requires the entire bandwidth of the channel to send data. Broadband Transmission is a transmission technique that many signals with multiple frequencies transmit data through a single channel simultaneously.

Key differences between baseband and broadband transmissions

Baseband transmission	Broadband transmission
Transmit digital signals	Transmit analog signals
To boost signal strength, use repeaters	To boost signal strength, use amplifiers
Can transmit only a single data stream at a time	Can transmit multiple signal waves at a time
Support bidirectional communications simultaneously	Support unidirectional communication only
Support TDM based multiplexing	Support FDM based multiplexing
Use coaxial, twisted-pair, and fiber-optic cables	Use radio waves, coaxial cables, and fiber optic cables
Mainly used in Ethernet LAN networks	Mainly used in cable and telephone networks

✓ Wireless Transmission Techniques

Wireless transmission techniques are essential for connecting devices without physical cables. They provide flexibility, mobility, and ease of installation. Here are some common techniques:

1. **Electromagnetic waves:** Transmit data through the air.
 - **Frequency bands:** Used for various applications, such as:
 - **Wi-Fi (IEEE 802.11):** Provides local area network (LAN) connectivity.
 - **Cellular networks (GSM, 3G, 4G, 5G):** Enables mobile communication.
 - **Bluetooth:** Connects devices within a short range.
 - **Zigbee:** Used for low-power, low-data-rate applications.
2. **Infrared (IR) Transmission**
 - **Light waves:** Transmit data through the air.
 - **Short range:** Suitable for devices in close proximity.
 - **Applications:** Remote controls, data transfer between devices (e.g., IRDA).
3. **Microwave Transmission**
 - **High-frequency RF waves:** Transmit data over long distances.
 - **Line-of-sight:** Requires a clear path between transmitter and receiver.
 - **Applications:** Satellite communication, point-to-point links.
4. **Terahertz (THz) Transmission**
 - **Extremely high-frequency RF waves:** Promise high data rates and bandwidth.
 - **Research and development:** Still in its early stages.
 - **Potential applications:** Short-range, high-speed communication.
5. **Optical Wireless (OW)**
 - **Light waves:** Transmit data through the air.
 - **Visible light communication (VLC):** Uses existing lighting infrastructure.
 - **Infrared light communication (IR-LC):** Similar to IR transmission but with longer range.
6. **Ultrasound Transmission**
 - **Sound waves:** Transmit data through the air or underwater.
 - **Short range:** Suitable for underwater communication or medical applications.
 - **Applications:** Underwater sensors, medical imaging.

Learning Outcome 3: Apply IP addressing (IP v4&IPv6)

Content/Topic 1: Description of IP addressing concepts

IP addressing is a Network Foundation service, which makes it core to the network design. It provides the base for all other network and user services

By following recommended IP address management standards, you can avoid:

- Overlapping or duplicate subnets
- Unsummarized routes in the network
- Duplicate IP address device assignments
- Wasted IP address space
- Unnecessary complexity

An IP address is a unique number that is used to identify a network device

- An IP address is represented as a 32-bit binary number, divided into four octets (groups of eightbits):

Example: 10111110.01100100.00000101.00110110

- An IP address is also represented in a dotted decimal format.Example: 190.100.5.54

- When a host is configured with an IP address, it is entered as a dotted decimal number, such as192.168.1.5.

Unique IP addresses on a network ensure that data can be sent to and received from the correct network device

✓ IP terminologies

Client: A client is any computer hardware or software device that requests access to a service provided by a server.

server : A computer that provides data, services, or resources that can be accessed by other computers on the network.

Port: A logical connecting point for a process. Data is transmitted between processes through ports (or sockets).

Node: A node is **any physical device within a network of other tools that's able to send, receive, or forward information.**

Packet: A generic term used to define a unit of data including routing and other information that is sent through an internet.

Gateway address: Usually the address of the default route to be used to reach a network that is not specifically known.

Medium: The communications link or network that carries protocol messages.

Message: The structured data communicated by a protocol. Parameters of a message typically include the message type, sequence number, control flags, and user data.

subnetting, which is a logical division of a network.

Address - The unique number ID assigned to one host or interface in a network.

Subnet - A portion of a network that shares a particular subnet address.

Subnet mask - A 32-bit combination used to describe which portion of an address refers to the subnet and which part refers to the host.

Interface - A network connection.

✓ IP addressing classification

- **Class A** (1 – 126)
Large networks, implemented by large companies and some countries
- **Class B** (128 – 191)
Medium-sized networks, implemented by universities
- **Class C** (192 – 223)
Small networks, implemented by ISP for customer subscriptions
- **Class D** (224 – 239)
Special use for multicasting
Class D addresses do not use a subnet mask.
- **Class E**
Used for experimental testing

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

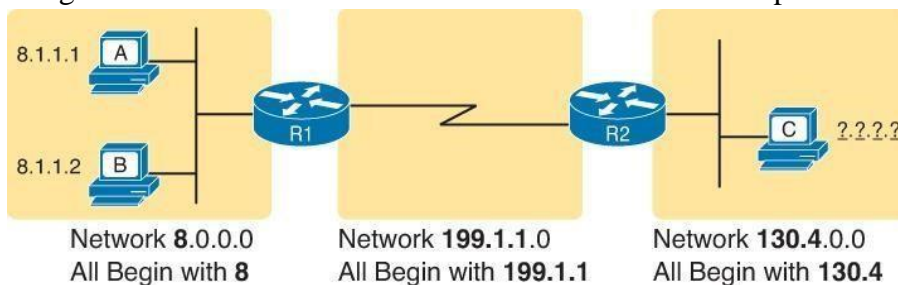
Class D	Host			
Octet	1	2	3	4

IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^{24-2})
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^{14}) 65,534 hosts per net (2^{16-2})
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^{21}) 254 hosts per net (2^{8-2})
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

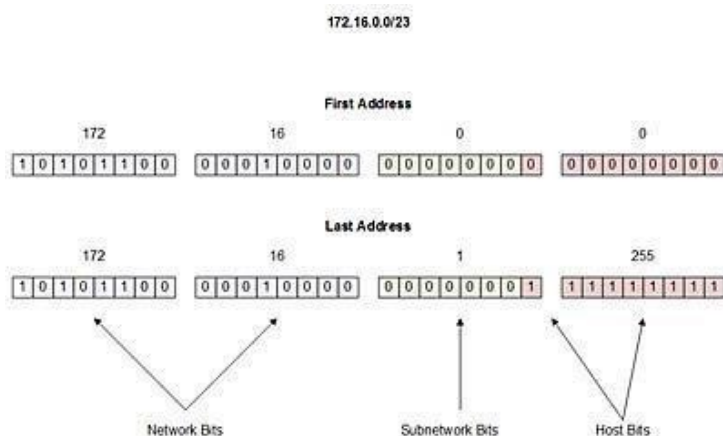
✓ IP addresses grouping

- IP addresses grouping: Rules for Grouping IP Addresses. The original specifications for TCP/IP grouped IP addresses into sets of consecutive addresses called IP networks. The addresses in a single IP network have the same numeric value in the first part of all addresses in the network.



✓ IP addressing scheme

IP Addressing Scheme. The IP header has 32 bits assigned for addressing a desired device on the network. An IP address is a unique identifier used to locate a device on the IP network. To make the system scalable, the address structure is subdivided into the network ID and the host ID.



Basic structure of an IP address

The basic structure of an IP address is like xxx.xxx.xxx.xxx, where each xxx can be any number between 0 and 255.

Each of these parts is stored in 8 bits. So, the maximum number of possible combinations for each group of numbers is 256 (i.e. each group can have any one value from the range of 0 to 255).

Each address can be technically divided into two parts. One of these parts is the network part, which represents the class of IP address that is being used in the network.

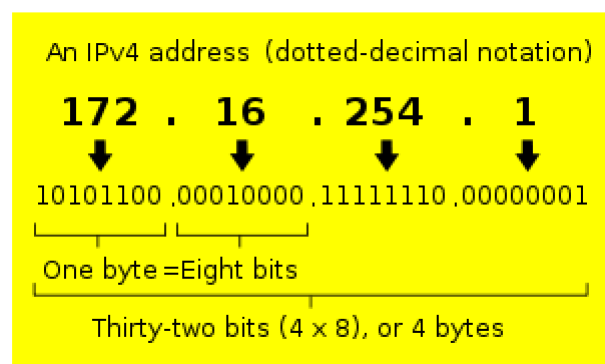
The other one is the host part, which represents the unique ID of the device in the network.

Let us consider the IP address 192.168.10.14

here **192.168.10** is the network part, and represents the network. The number 14 represents the unique ID of the device in the network.

You can find out the IP address of your PC when you are connected to a network. Here's how:

1. Click on Start button and then on Run.
2. In the box named Open, type "command" (without the quotes) and hit the Enter key.
3. In the window that appears, type "ipconfig" (minus the quotes) and hit Enter key.



An IP address (version 4) in both dot-decimal notation and binary code

An IPv4 address is typically shown as split into 4 chunks as shown above. Different ranges of IP addresses are categorised differently, with the first part of the IP specifying who or where the IP address is (the **network identifier**), and the second part defining which host/machine it is (the **host identifier**)

192.168.12.162

✓ IP addressing subnet masks

- Used to indicate the network portion of an IP address
- Is a dotted decimal number
- Usually, all hosts within a broadcast domain of a LAN (bounded by routers) use the same subnet mask.

The default subnet masks for three classes of IP addresses:

255.0.0.0 is the subnet mask
for Class A
255.255.0.0 is the subnet
mask for Class B
255.255.255.0 is the subnet
mask for Class C

The **subnet** address is used to identify **the network itself**

The **broadcast** address identifies *all* hosts on a particular network.

Broadcasts are one of three types of IP packets:

- Y **Unicasts** are packets sent from one host to one other host
- Y **Multicasts** are packets sent from one host to a *group* of hosts
- Y **Broadcasts** are packets sent from one host to all other hosts on the local network

Examining the prefix length

the prefix length is another way of expressing the subnet mask. The prefix length is the number of bits set to 1 in the subnet mask. It is written in “slash notation”, a “/” followed by the number of bits set to 1.

For example, if the subnet mask is 255.255.255.0, there are 24 bits set to 1 in the binary version of the subnet mask, so the prefix length is 24 bits or /24. The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address.

✓ Prefix length

The prefix length is another way of expressing the subnet mask. The prefix length is the number of bits set to 1 in the subnet mask. It is written in “slash notation”, a “/” followed by the number of bits set to 1.

For example, if the subnet mask is 255.255.255.0, there are 24 bits set to 1 in the binary version of the subnet mask, so the prefix length is 24 bits or /24. The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address.

Content/Topic 2: Identification of IP Addresses types

There are mainly four types of IP addresses:

- ☐ Public,
- ☐ Private,
- ☐ Static
- ☐ Dynamic.

Among them, public and private addresses are based on their location of the network private, which should be used inside a network while the public IP is used outside of a network.

Public IP Addresses

- It is an IP address available for everyone to see.
- Public IP's let the general public find out information about your computer and are available to see it, for example a web server.
- User has no control over the IP address (public) that is assigned to the computer.

- The public IP address is assigned to the computer by the Internet Service Provider

Private IP Addresses

A private IP address is a unique IP number assigned to every device that connects to your home internet network, which includes devices like computers, tablets, smartphones, which is used in your household.

It also likely includes all types of Bluetooth devices you use, like printers or printers, smart devices like TV, etc. With a rising industry of internet of things (IoT) products, the number of private IP addresses you are likely to have in your own home is growing.

A private IP address is an IP address used on a private network (e.g. a home network) that is not routable through the public internet.

So a private IP address is for security.

A public IP address can be either static or dynamic. A static public IP address does not change and is used primarily for hosting web pages or services on the Internet. On the other hand, a dynamic public IP address is chosen from a pool of available addresses and changes each time one connects to the Internet.

Most Internet users will only have a dynamic IP assigned to their computer which goes off when the computer is disconnected from the Internet. Thus when it is re-connected it gets a new IP

Private address blocks are:

Hosts that do not require access to the Internet can use private addresses

- ☐ 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
- ☐ 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
- ☐ 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

Dynamic IP address:

Dynamic IP addresses always keep changing. It is temporary and are allocated to a device every time it connects to the web. Dynamic IPs can trace their origin to a collection of IP addresses that are shared across many computers.

Static IP Addresses

A static IP address is an IP address that cannot be changed. In contrast, a dynamic IP address will be assigned by a Dynamic Host Configuration Protocol (DHCP) server, which is subject to change. Static IP address never changes, but it can be altered as part of routine network administration.

Types of Website IP Addresses

Two types of website IP Addresses are 1) Shared IP Address 2) Dedicated IP Address

Shared IP Addresses:

Shared IP address is used by small business websites that do not yet get many visitors or have many files or pages on their site. The IP address is not unique and it is shared with other websites.

Dedicated IP Addresses:

Dedicated IP address is assigned uniquely to each website. Dedicated IP addresses helps you avoid any potential backlists because of bad behavior from others on your server. The dedicated IP address also gives you the option of pulling up your website using the IP address alone, instead of your domain name. It also helps you to access your website when you are waiting on a domain transfer.

Special Use IPv4 Addresses

- ☐ **Network and Broadcast addresses** - within each network the first and last addresses cannot be assigned to hosts
- ☐ **Loopback address** - 127.0.0.1 a special address that hosts use to direct traffic to themselves (addresses 127.0.0.0 to 127.255.255.255 are reserved)
- ☐ **Link-Local address** - 169.254.0.0 to 169.254.255.255 (169.254.0.0/16) addresses can be automatically assigned to the local host
- ☐ **TEST-NET addresses** - 192.0.2.0 to 192.0.2.255 (192.0.2.0/24) set aside for teaching and learning purposes, used in documentation and network examples
- ☐ **Experimental addresses** - 240.0.0.0 to 255.255.255.254 are listed as reserved

✓ Methods of Assigning IP addresses



Automatic method-

DHCP

DHCP short for Dynamic Host Configuration Protocol is a protocol which helps to dynamically assign IP addresses, instead of having static IP addresses. When a machine connects to a network it receives a IP address.

The server that manages this dynamically assigned IP addresses is called Dynamic Host Configuration Protocol (DHCP) server.



Static addressing method

What is a static IP address?

A static IP address is an address that is permanently assigned to you by your ISP (as long as your contract is in good standing), and does not change even if your computer reboots

A static IP address is usually assigned to a server hosting websites, and providing email, database and FTP services

Static IP address Advantages

- ☐ Address does not change - good for web servers, email servers and other Internet servers.
- ☐ Use DNS to map domain name to IP address, and use domain name to address the static IP address.

Static IP address Disadvantages

- ☐ Expensive than dynamic IP address - ISPs generally charge additional fee for static IP addresses.

- Need additional security - Since same IP is assigned to a machine, hackers try brute force attack on the machine over period of time.



Dynamic method

What is a dynamic IP address?

- dynamic IP address is an IP address dynamically assigned to your computer by your ISP.
- Each time your computer (or router) is rebooted, your ISP dynamically assigns an IP address to your networking device using **DHCP protocol**.

Dynamic IP address Advantages

- Cheaper than static IP address.
- Changing IP address gives more privacy.

Dynamic IP address Disadvantages

- Requires DHCP server to obtain an IP address.
- Non-static. Each time IP address changes, you may have to find your IP address again.

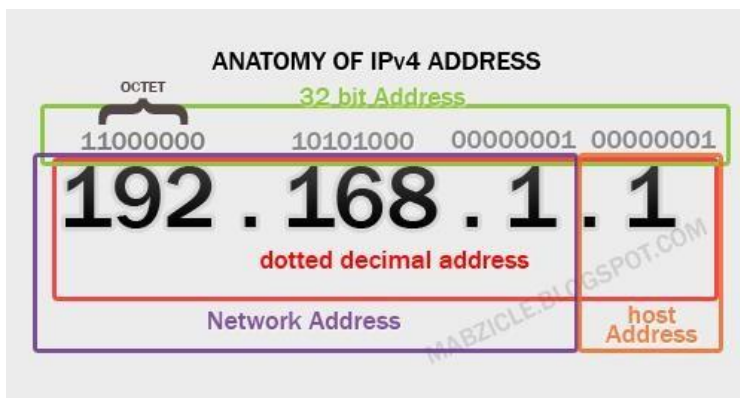
Content/Topic 3: Application of IPv4 concepts

✓ Introduction to IPv4

Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol (IP) used to facilitate communication over a network through an addressing system

- It is currently the most popular Internet protocol used to connect devices to the Internet.
 - IPv4 uses a **32-bit** address scheme allowing for a total of 2^{32} addresses (just over 4 billion addresses).
 - Each device connecting to the Internet requires an IP address.
- That means that each device including cell phones, office phones, game consoles and computers each need their own IP address in order to connect and communicate over the Internet

✓ Anatomy of IPv4 address



32 bit address

IPv4 is a 32 bit address(binary patterns). Because it consists of 4 octet(1 octet = 1byte/8 bits) so with asimple calculation: 4octets*8bits = 32 bits.

There are three types of addresses within the address range of each IPv4 network:

- ✓ Network address
- ✓ Host addresses
- ✓ Broadcast address

- **Network Address**

In each IPv4 addresses, some portion(high-order bits) represents Network address. It is a group of hosts that have identical bit patterns.

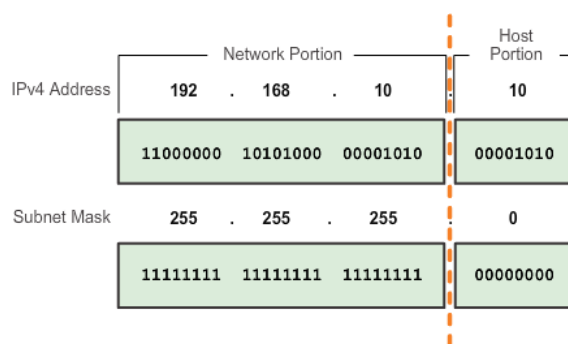
- **Host Address**

Every devices has a uniques IP address. Host address belongs in a certain **Network address**.(usually in the rightmost in the IP address)

- **Broadcast Address**

The IPv4 broadcast address is a special address for each network that allows communication to all the hosts in that network.

Network Portion and Host Portion of an IPv4 Address



- To define the network and host portions of an address, a devices use a separate 32-bit pattern called asubnet mask
- The subnet mask does not actually contain the network or host portion of an IPv4 address, it just sayswhere to look for these portions in a given IPv4 address

Valid Subnet Masks

Subnet Value	Bit Value							
	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

EXERCISES

Q: What are the maximum networks and hosts in a class A, B and C network?

For Class A, there are 126 possible networks
and 16,777,214 hosts
For Class B, there are
16,384 possible networks and 65,534 hosts
For Class C, there are 2,097,152 possible networks
and 254 hosts

✓ Calculation of IP addresses

- Binary to decimal conversion
 - Decimal to binary conversion
 - Summarization
-
- ☐ Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network.
 - ☐ Class A, B, or C network.

CIDR

Classless Interdomain Routing (CIDR) was introduced in order to improve both address space utilization and routing scalability in the Internet. It was needed because of the rapid growth of the Internet and growth of the IP routing tables held in the Internet routers.

Summarization

Route summarization - Also known as prefix aggregation, routes are summarized into a single route to help reduce the size of routing tables. For instance, one summary static route can replace several specific static route statements.

Super-netting - Occurs when the route summarization mask is a smaller value than the default traditional classful mask.

Note: A supernet is always a route summary, but a route summary is not always a supernet.

Calculating IPV4 Summary network

Step 1. List the networks in binary format.

Step 2. Count the number of far-left matching bits to determine the mask for the summary route.

Step 3. Copy the matching bits and then add zero bits to determine the summarized network address.

Fixed-length subnet mask (FLSM)

Fixed-length subnet mask (FLSM) is a subnet deployment strategy in which a block of IP addresses is split into several subnets of identical length. It is also known as classful subnetting.

Variable-length subnet mask (VLSM) refers to a strategy that allows all the subnetworks to have variable sizes. Network administrators can use VLSM subnetting to divide an IP address space into subnets of various lengths and assign them based on the needs of the network. It is also called classless subnetting.

In FLSM all subnets use same subnet mask, this leads to inefficiencies.

With classful subnetting, all subnets have the identical number of host addresses. This could present issues if you need certain subnets to have a small number of IP addresses, and you need other subnets to have a large number of IP addresses. The solutions listed below; to solving this issue does not however optimize the network configuration. This is mostly due to IP addresses being wasted:

- ☐ Variable length subnet masks (VLSMs) allow subnets to be further subnetted, and also enable routers to handle different subnet masks.
- ☐ VLSMs provide the flexibility needed to optimize the network configuration by allowing you to configure network subnets that meet the requirements of your organization. No IP addresses are wasted.
- ☐ VLSMs (nonclassful subnetting) can be defined as the process whereby which subnets are divided into smaller segments of various sizes.

The differences between FLSM and VLSM are as follows:

Attributes	FLSM	VLSM
Sub-net size	Equal	Variable
Sub-net mask	Same	Different
Number of Hosts	Equal	Variable
Configuration	Easy and simple	Complex
IP addresses wastage	More	Less
Efficiency	Less	More
Routing Protocols	Supports classful and classless	Supports classless
Applications	Suitable for private IP addresses	Suitable for public IP addresses

Classless Inter-Domain Routing (CIDR) notation

CIDR, which stands for Classless Inter-Domain Routing, is **an IP addressing scheme that improves the allocation of IP addresses**. It replaces the old system based on classes A, B, and

C. This scheme also helped greatly extend the life of IPv4 as well as slow the growth of routingtables.

Problems with class-based IP addressing

The old method of IP addressing came with inefficiencies that exhausted the availability of IPv4 addresses faster than it needed to. The classful routing system included classes A, B, and C:

- ☐ **Class A** - Over 16 million host identifiers
- ☐ **Class B** - 65,535 host identifiers
- ☐ **Class C** - 254 host identifiers

CIDR IP address would look like the following:

192.255.255.255/12

Representation: It is also a 32-bit address, which includes a special number which represents the number of bits that are present in the Block Id.

a . b . c . d / n

Where, n is number of bits that are present in Block Id / Network Id.

Example:

20.10.50.100/20

Let's see the difference between classful routing and classless routing:

S.NO	Classful Routing	Classless Routing
1.	In classful routing, VLSM (Variable Length Subnet Mask) is not supported.	While in classless routing, VLSM (Variable Length Subnet Mask) is supported.
2.	Classful routing requires more bandwidth.	While it requires less bandwidth.
3.	In classful routing, hello messages are not used.	While in classless routing, hello messages are used.
4.	Classful routing does not import subnet mask.	Whereas it imports subnet mask.
5.	In classful routing, address is divided into three parts which are: Network, Subnet and Host.	While in classless routing, address is divided into two parts which are: Subnet and Host.
6.	In classful routing, regular or periodic updates are used.	Whereas in this, triggered updates are used.
7.	In classful routing, CIDR(Classless Inter-Domain Routing) is not supported.	While in classless routing, CIDR(Classless Inter-Domain Routing) is supported.
In classful routing, fault can be detected easily.		While in classless routing, fault detection is little tough.

✓ IP addresses Diagnostic tools

Testing IP addresses

- **Diagnostic tools:** Computer diagnostics tools are pieces of software that give you the knowledge you need to be able to potentially repair your own computer. These tools are made to find problems that may be disrupting your computer's normal performance. Once a problem is found, you can

then plan your repair. The diagnostic tools listed and discussed are the followings:

ifconfig: Provides information about the basic configuration of the interface. It is useful for detecting bad IP addresses, incorrect subnet masks, and improper broadcast addresses.

arp: Provides information about Ethernet/IP address translation. It can be used to detect systems on the local network that are configured with the wrong IP address.

netstat: Provides a variety of information. It is commonly used to display detailed statistics about each network interface, the network sockets, and the network routing table.

ping: Indicates whether a remote host can be reached. ping also displays statistics about packet loss and delivery time.

nslookup: Provides information about the DNS name service.

Dig: Also provides information about name service and is similar to nslookup.

Traceroute: Prints information about each routing hop that packets take going from your system to a remote system.

✓ IP address translation

IP address translation: NAT allows internal hosts to be translated to a public address for Internet access. *Network Address Translation* (NAT) is the process where a network device, usually a Router, translates private IP into public IP.

✓ IP addressing forms

Data is transported over a network by three simple methods i.e. Unicast, Broadcast, and Multicast. So let's begin to

summarize the difference between **these three**:

- **Unicast:** from one source to one destination i.e. One-to-One
- **Broadcast:** from one source to all possible destinations i.e. One-to-All
- **Multicast:** from one source to multiple destinations stating an interest in receiving the traffic i.e. One-to-Many

Content/Topic 3: Application of IPv6 concepts

Internet protocol version 6 is the most recent version of the internet protocol, it is a communications protocol that provides an identification and location system for computers on networks.

The Need for IPv6

- ☐ IPv6 is designed to be the successor to IPv4
- ☐ Depletion of IPv4 address space has been the motivating factor for moving to IPv6
- ☐ Projections show that all five RIRs (**Regional Internet Registry**) will run out of IPv4 addresses between 2015 and 2020
- ☐ With an increasing Internet population, a limited IPv4 address space, issues with NAT and an Internet of things, the time has come to begin the transition to IPv6!
- ☐ IPv4 has theoretical maximum of 4.3 billion addresses plus private addresses in combination with NAT
- ☐ IPv6 larger 128-bit address space providing for 340 undecillion addresses
- ☐ IPv6 fixes the limitations of IPv4 and include additional enhancements such as ICMPv6

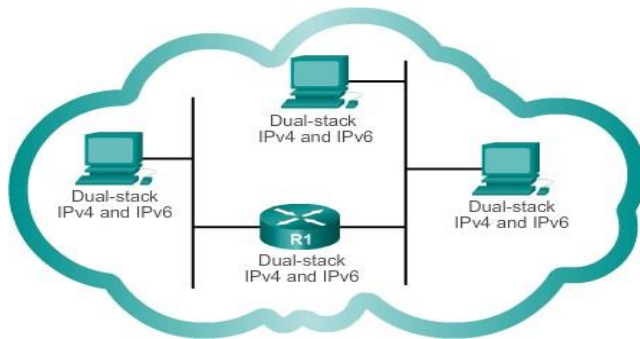
✓ Migration from IPv4 to IPv6

Comparison of IPv4 and IPv6

1. source and destination addresses are 32 bits.)	1. Source and destination addresses are 128 bits.
2. Ipv4 support small address space.	2. Supports a very large address space sufficeint for each and every people onearth.
3. Ipv4 header includes checksum.	3. ipv6 header doesn't includes the checksum.
4. addresses are represented in dotted decimal format. (Eg. 192.168.5.1)	4. Addresses are represented in 16-bitsegments Each segment is written in Hexadecimal separated by colons. (Eg. 2001:0050:020c:0235:0ab4:3456:456b:e560
5. Header includes options.	All optional data is moved to IPV6 extension header.
6. Broadcast address are used to sendtraffic to all nodes on a subnet.	6. There is no IPV6 broadcast address. Instead a link local scope all-nodesmulticast address is used.
7. No identification of packet flow for QOS handling by router is present within the ipv4 header.	7. Packet flow identification for QOShandling by routers are present within the IPv6 headerusing the flow label field.
8. uses host address (A) resource records in the Domain name system (DNS) to map host namestoipv4 addresses.	8. Uses AAAA records in the DNS to map host names to ipv6 addresses.
9. Both routers and the sending hostfragment packets.	9. Only the sending host fragments packets;routers do not.
10. ICMP Router Discovery is used to determine the IPv4 address of the best default gateway, and it is optional.	10. ICMPv6 Router Solicitation and Router Advertisement messages are used to determine the IP address of the best default gateway, and they are required

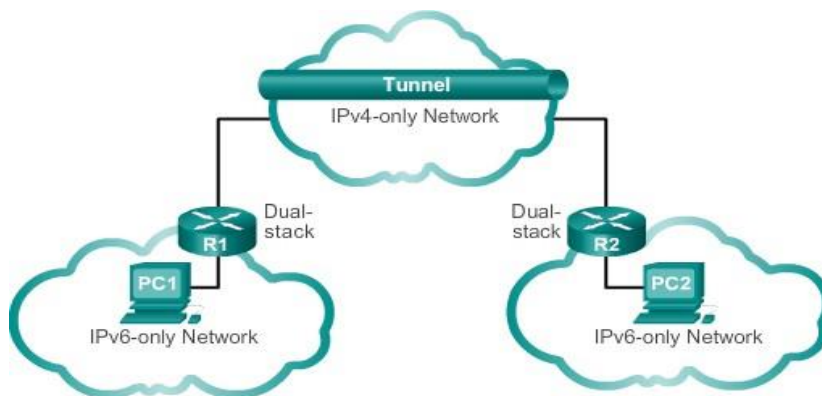
✓ IPv4 and IPv6 Coexistence

The migration techniques can be divided into three categories: #1 **Dual-stack**



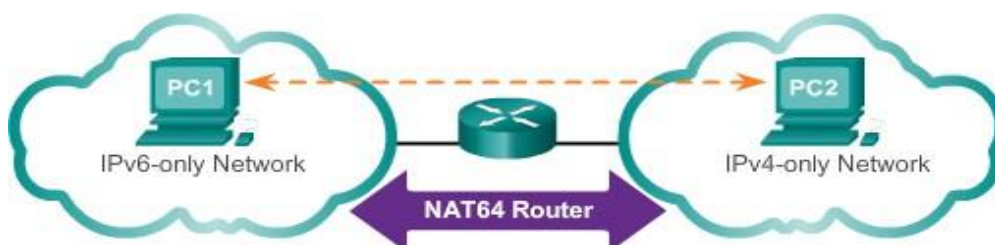
Dual-stack: Allows IPv4 and IPv6 to coexist on the same network. Devices run both IPv4 and IPv6 protocol stacks simultaneously.

#2: Tunnelling



Tunnelling: A method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet.

#3 Translation



Translation: Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. An IPv6 packet is translated to an IPv4 packet, and vice versa.

✓ Anatomy of IPv6 address

IPv6 addresses are 128 bits in length and written as a string of hexadecimal values. Every 4 bits is represented by a single hexadecimal digit; for a total of 32 hexadecimal values. IPv6 addresses are not case sensitive and can be written in either lowercase or uppercase.

Unlike IPv4 addresses that are expressed in dotted decimal notation, IPv6 addresses are represented using hexadecimal values

IPv4 address space (32 bits):

$$2^{32} =$$

4294967296

addresses IPv6

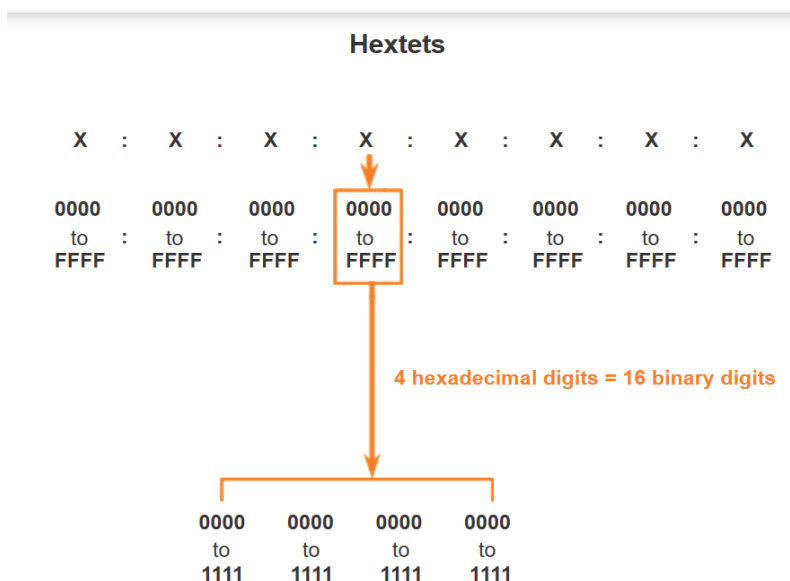
address space

(128 bits):

$$2^{128} = 340282366920938463463374607431768211456 \text{ addresses}$$

Preferred Format

The preferred format for writing an IPv6 address is x:x:x:x:x:x:x, with each “x” consisting of four hexadecimal values. When referring to 8 bits of an IPv4 address we use the term octet. In IPv6, a **hextet** is the unofficial term used to refer to a segment of 16 bits or four hexadecimal values. Each “x” is a single hextet, 16 bits or four hexadecimal digits.



IPv6 Address Representation

- Look at the binary bit patterns that match the decimal and hexadecimal values

Hexadecimal	Decimal	Binary
00		
01	0	0000 0000
02	1	0000 0001
03	2	0000 0010
04	3	0000 0011
05	4	0000 0100
06	5	0000 0101
07	6	0000 0110
08	7	0000 0111
	8	0000 1000
0A	10	0000 1010
0F	15	0000 1111
10	16	0001 0000
20	32	0010 0000
40	64	0100 0000
80	128	1000 0000
C0	192	1100 0000
CA	202	1100 1010
F0	240	1111 0000
FF	255	1111 1111

- 128 bits in length and written as a string of hexadecimal values
- In IPv6, 4 bits represents a single hexadecimal digit, 32 hexadecimal values = IPv6 address

2001:0DB8:0000:1111:0000:0000:0200FE80:0000:0000:0000:0123:4567:89AB:CDEF

- Hextet used to refer to a segment of 16 bits or four hexadecimals
- Can be written in either lowercase or uppercase

Rule 1- Omitting Leading 0s

The first rule to help reduce the notation of IPv6 addresses is any leading 0s (zeros) in any 16-bit section or hextet can be omitted

- 01AB can be represented as 1AB
- 09F0 can be represented as 9F0

- ❑ 0A00 can be represented as A00
- ❑ 00AB can be represented as AB

Preferred	2001:0DB8:000A:1000:0000:0000:0000:0100
No leading 0s	2001: DB8: A:1000: 0: 0: 0: 100
Compressed	2001:DB8:A:1000:0:0:0:100

Rule 2- Omitting All 0 Segments

- ❑ A double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hextets) consisting of all 0's
- ❑ Double colon (::) can only be used once within an address otherwise the address will be ambiguous
- ❑ Known as the *compressed format*
- ❑ Incorrect address - 2001:0DB8::ABCD::1234

Examples #1

Preferred	2001:0DB8:0000:0000:ABCD:0000:0000:0100
Omit leading 0s	2001: DB8: 0: 0:ABCD: 0: 0: 100
Compressed	2001:DB8::ABCD:0:0:100
OR	
Compressed	2001:DB8:0:0:ABCD::100

Only one :: may be used.

Examples 2

Preferred	FE80:0000:0000:0000:0123:4567:89AB:CDEF
Omit leading 0s	FE80: 0: 0: 0: 123:4567:89AB:CDEF
Compressed	FE80::123:4567:89AB:CDEF

Hexadecimal values of eight 16 bit fields

- X:X:X:X:X:X:X:X (X=16 bit number, ex: A2FE)
- 16 bit number is converted to a 4 digit hexadecimal number

• Example:

- FE38:DCE3:124C:C1A2:BA03:6735:EF1C:683D
- Abbreviated form of address

4EED:0023:0000:0000:0000:036E:1250:2B00

→4EED:23:0:0:0:36E:1250:2B00

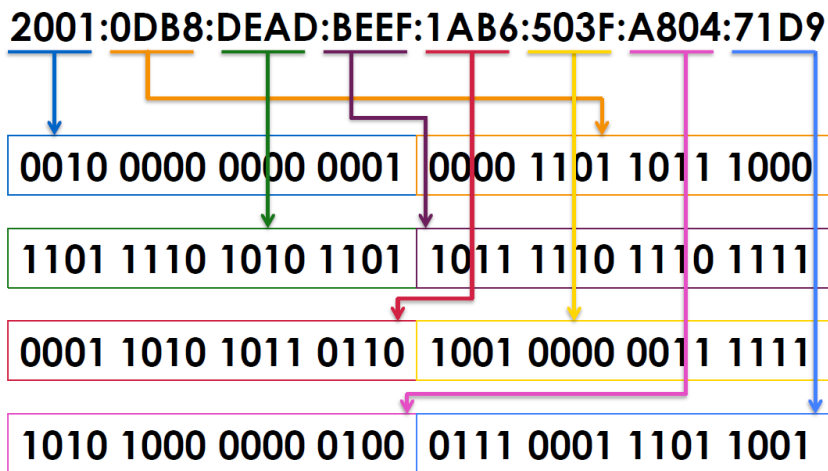
→4EED:23::36E:1250:2B00

(Null value can be used only once)

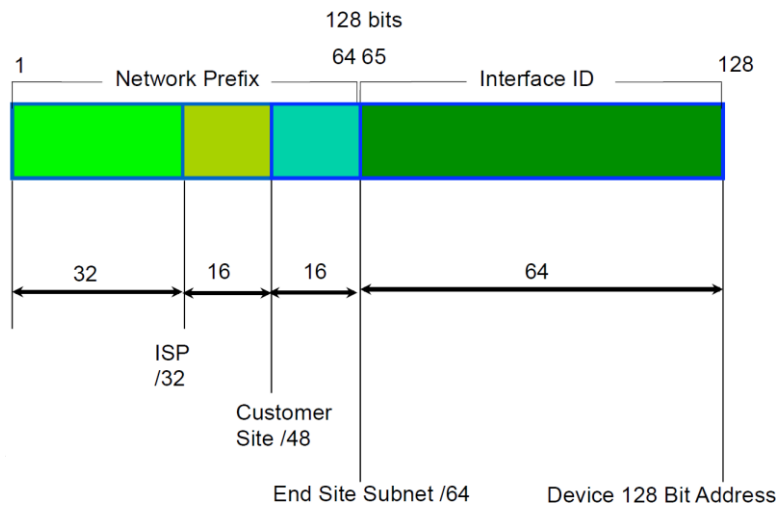
Leading zeroes

Groups of zeroes

Double colons



IPv6 addressing structure



TYPES OF IPv6

The three types of IPv6 addresses are: unicast, anycast, and multicast.

- Unicast addresses identify a single interface.
- Anycast addresses identify a set of interfaces in such a way that a packet sent to an anycast address is delivered to a member of the set.
- Multicast addresses identify a group of interfaces in such a way that a packet sent to a multicast address is delivered to all of the interfaces in the group.

IPv6 has no broadcast addresses: multicast addresses took over.

IPv6 Summary Network

Summarizing IPv6 networks into a single IPv6 prefix and prefix-length can be done in seven steps as shown in Figures 1 to 7:

Step 1. List the network addresses (prefixes) and identify the part where the addresses differ.

Step 2. Expand the IPv6 if it is abbreviated.

Step 3. Convert the differing section from hex to binary.

Step 4. Count the number of far left matching bits to determine the prefix-length for the summary route.

Step 5. Copy the matching bits and then add zero bits to determine the summarized network address(prefix).

Step 6. Convert the binary section back to hex.

Step 7. Append the prefix of the summary route (result of Step 4).