



CompTIA Network+

The Complete Course

TELCOMA

Introduction to Network

Content:

1. What is Network?
2. Types of Networks:
 - Local Area Network
 - Metropolitan Area Network
 - Wide Area Network
 - Personal Area Network
 - Storage Area Network
 - Enterprise Private Network
 - Virtual Private Network

What is Network?

A group of devices are connected to each other to form a network.

Network is the collection of two or more computers, servers and other network elements.

The connection between the devices may be wired or wireless.

Example of Network is Internet.

Types of Networks:

Based on Network Size:

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)

Based on Purpose:

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

Personal Area Network

It is a computer network which is organized within the environment of individual users.

It is the interconnection of information technology devices such as computers, telephones, tablets and personal digital assistants.



Personal Area Network

Local Area Network:

It is a computer network whose range is restricted to a particular geographic area such as office building, college campus etc.

Its range lies within the radius of less than 1 km.

The installation and maintenance of this network is easy.

Transmission technology used in LAN network are Ethernet and Wi-Fi.



Metropolitan Area Network:

A Metropolitan Area network (MAN) is similar to local area network (LAN) but it connects the entire city or campus.

MAN is formed by connecting various LANs.

Its range lies between 2 - 50 km.

The design and maintenance of network is difficult.



Wide Area Network:

A Wide Area Network (WAN) is the computer network which extends to a larger geographical area.

It connects different smaller networks including LANs and MANs.

The speed of network is slow.

Example is Internet.



Storage Area Network:

A Storage area network (SAN) is a dedicated high speed network.

It interconnects and presents a shared pool of storage devices to multiple servers.

SAN is assembled using cabling, Host Bus Adapter (HBAs) and switches.

SAN network is more expensive, complex and difficult to manage.

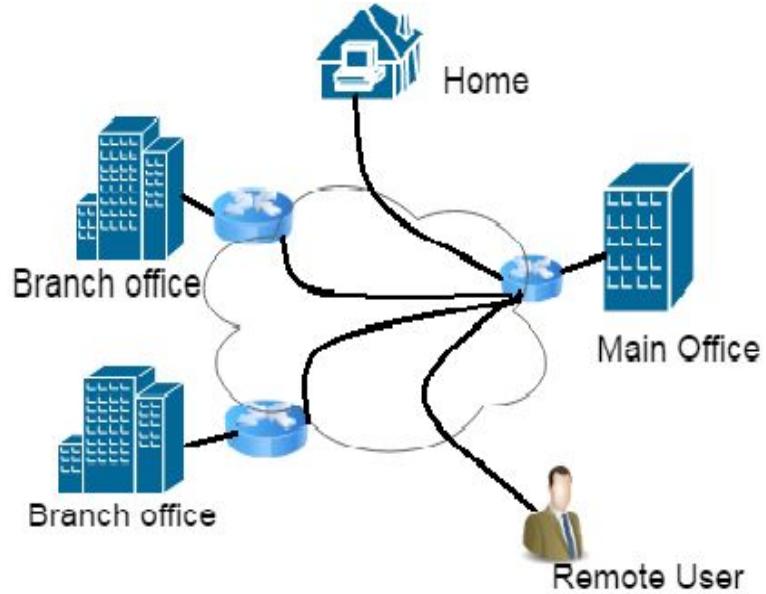


Enterprise Private Network:

A Enterprise Private network (EPN) is the network built by an enterprise to connect various company sites e.g. production site, shops, marketing office and head office.

It is built to share same computer resources in the network.

It integrates all the system within an organization.



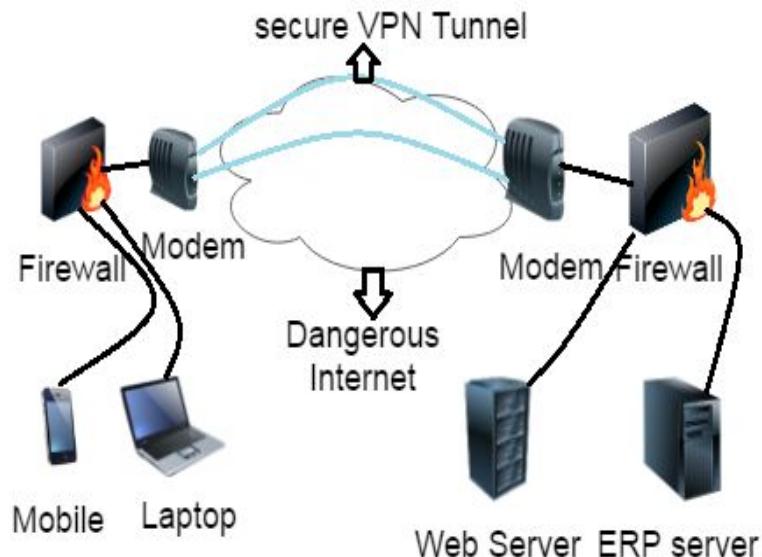
Enterprise Private Network

Virtual Private Network:

A Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network i.e internet

A VPN is created by establishing a virtual point-to-point connection by using dedicated connections, virtual tunneling protocols and traffic encryption

To gain access to the VPN, a user is authenticated using a unique identification and a password.



Virtual Private Network

Network Elements

Content:

1. Network Elements

- Router
- Switch
- Hub
- Bridge
- NIC card
- Gateway
- Modem
- Repeater
- Firewall
- DHCP server
- DNS server

Network Elements/Devices:

These are kind of telecommunication equipment that provide support and service to the user.

Example: Router, Switch, Hub, Bridges, NIC card and Gateway etc.

Router:

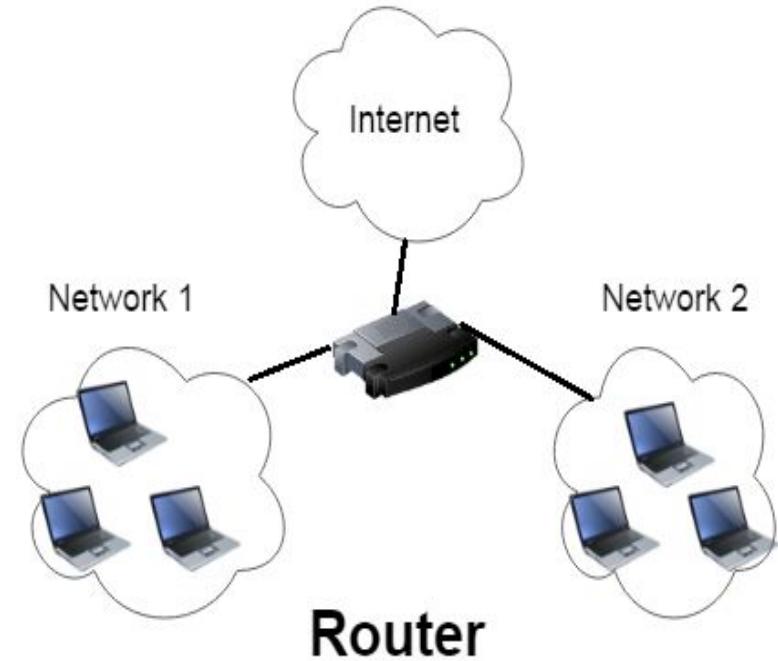
Router is a networking device that forward packets between networks.

It works at Network Layer (Layer 3).

It is used to connect two or more networks.

It use IP addresses to transfer data packets between sender and receiver.

It manages the traffic load in the network.



Switch:

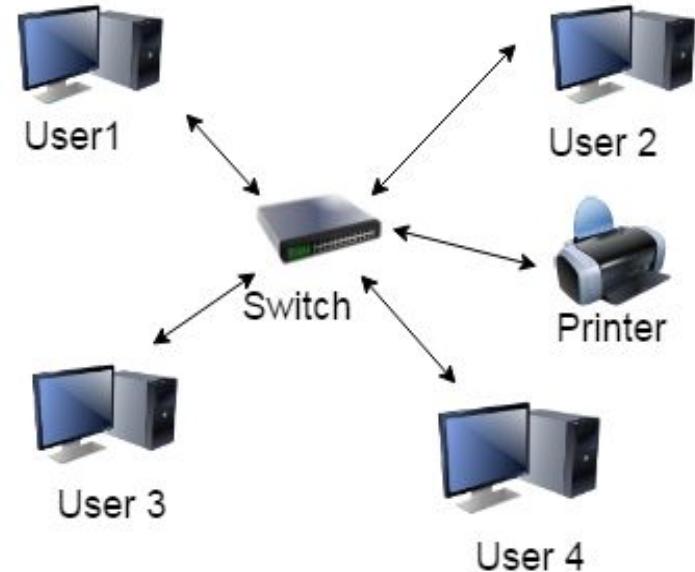
Switch is a networking device used to connect many devices together in the network.

It works on data link layer(Layer 2)

It is used in LAN network to connect two or more nodes in the same or different network.

Switch use MAC address to route the packet in the network

Switch contain 24/48 ports



Switch

Hub:

Hub is also a networking device which connects various nodes or devices in the network.

It is same as that of switch but the difference is it broadcast the packets to all nodes which are connected to it.

It works on Physical Layer (Layer 1).

It contain 4/12 ports.

It cannot store or learn MAC addresses.



Bridge:

Bridge is a networking device which connects two or more LAN networks that uses the same protocols (i.e Ethernet or Token Rings).

It works on Physical or Data link layer.

It recognizes the MAC address.

Bridges has one incoming and outgoing port.



Network Interface Controller/Card:

It is also known as Network or LAN adapter, physical network interface.

NIC cards are the computer's hardware components (circuit board) which is installed to connects the computer to the computer's network.

It provide the computer a dedicated, full time connection to the network.

Ethernet cable is used to connect the computer to the network



NIC Card

Gateway:

Gateways is a network point that act as the entrance point to the another network.

It controls the traffic between the network.

It repackage and convert the data going from one network to the another network.

Example: if we are using internet connection at home, then gateway is the internet service provider that provide access to the entire internet.



Modem:

Modem is an internetworking device which is used to transmit data in a network.

Its main function is to modulates and demodulates the data signals.

It consists of 2 ports. One connected to ISP and the next port is connected to router. It works on Data link layer(Layer 2).

A modem can work without a router (as to connect single pc with internet).



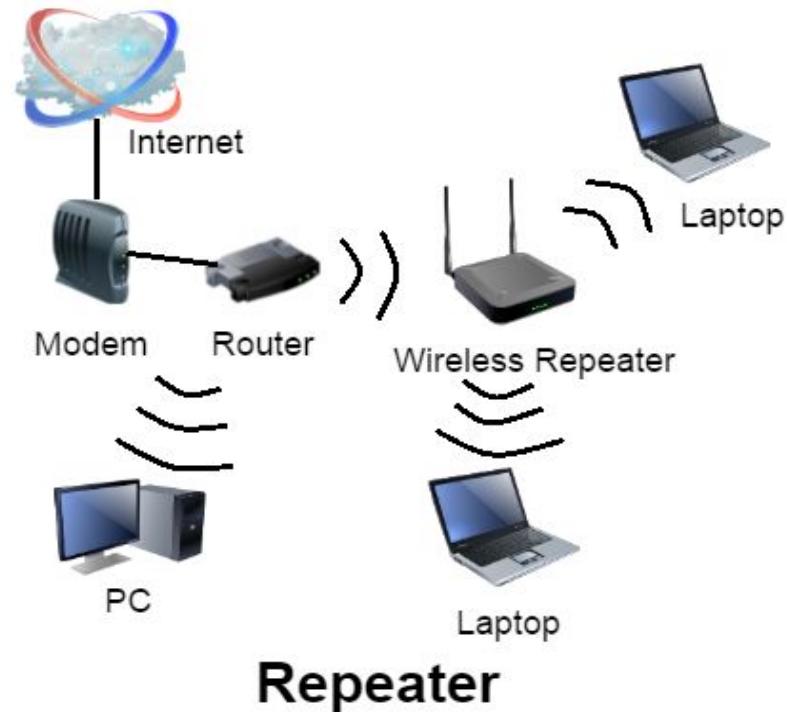
Repeater:

Repeater is a networking device that receive a signal and retransmit it

Repeaters are installed in the network to transmit the signals to longer distance.

Types of repeaters are telephone repeaters, optical communication repeaters and radio repeaters.

It works on Physical layer(Layer 1)



Firewall:

Firewall is a network security system which defines the rules to control incoming and outgoing network traffic.

It may be a hardware or software based.

It act as a barrier between trusted zone (e.g private or corporate network) and untrusted zone (e.g. the internet)

Software based firewalls are cyberoam UTM, FireEye, Cisco ASA, Fortinet FortiGate.

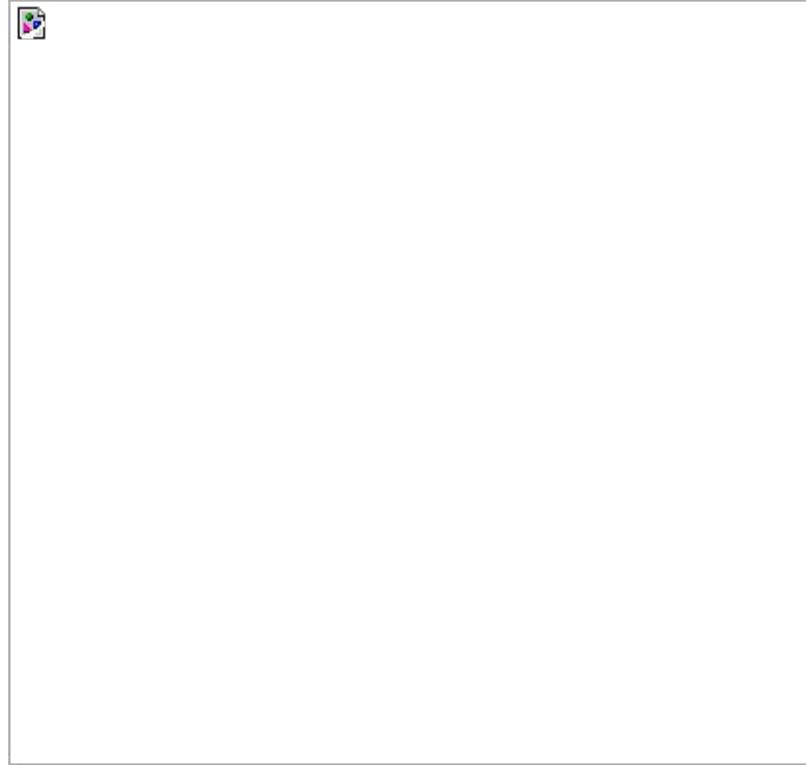


DHCP server:

Dynamic host configuration protocol (DHCP) is a client/server protocols

It enables server to automatically assign an IP address to a computer and other related information such as subnet mask and default gateways from a defined range of numbers configured for a given network.

DHCP server maintain a pool of an IP address and leases an address to any DHCP enabled client when it start up on the network.

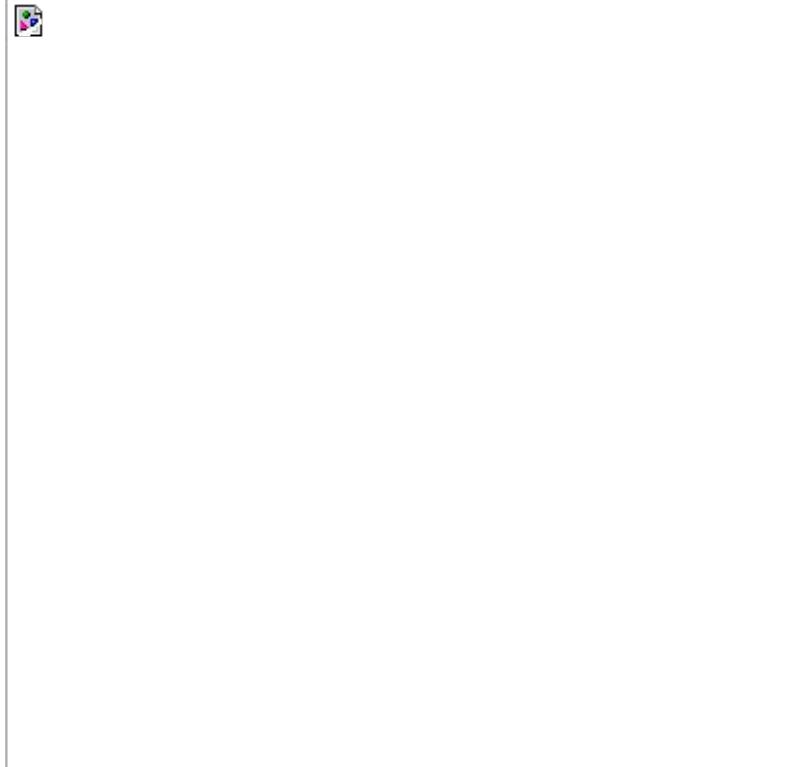


DNS Server:

DNS server is a name resolution protocol for TCP/IP network.

It is a standard for managing the names of public websites and other internet domains.

It allow us to type the name of website in the web browser like google.com and our computer automatically find the address on the internet(216.58.196.14)



Network Topology

Content

1. About Network Topology
2. Different Network Arrangement
3. Types of Network Topologies:
 - Physical Topology
 - Logical Topology

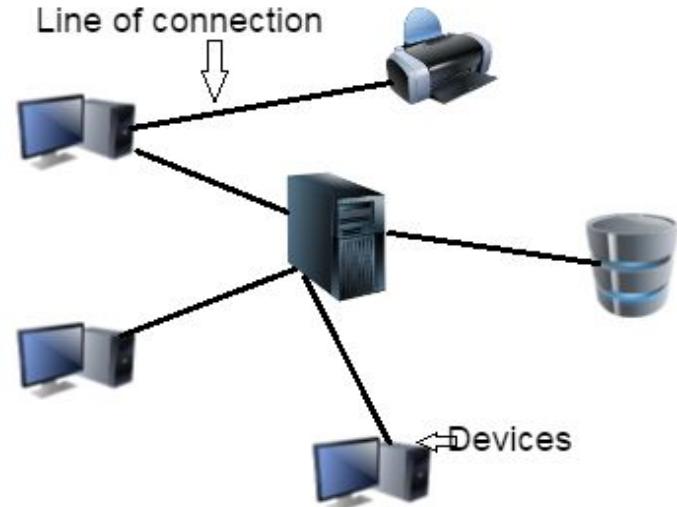
Network Topology:

Network Topology is the arrangement of network, connecting various nodes (i.e. printer, router, computers and other devices) through line of connection.

It describes the way in which different elements are arranged.

It represents a schematic description of a network.

Network Topology



Network Topology

Different Network Arrangements:

Client/Server network:

It is designed for the end users called clients, to access resources such as files, songs, video collections or some other services from a central computer called server.

In this network, server is a centralized and a powerful computer.

Server's sole purpose is to serve its clients.

Peer to peer network:

Peer to peer network is created by connecting two or more computers and they share their resources with each other in the network.

Each computer will act as server and client.

This network is less expensive as compared to client/server network.

Different Network Arrangements:



Types of Network Topology:

Physical Topology:

It refers to the layout of cabling, the location of the nodes and the interconnection between the nodes and the cabling.

Physical topology is of various kinds.

Logical Topology:

It refers to the flow of data within the network, regardless of its physical design.

It defines how the data should be transferred between nodes or devices.

Physical Topology

Content:

1. Various Types of Physical Topologies:

- Point to Point
- Bus Topology
- Star Topology
- Ring Topology
- Mesh Topology
- Hybrid Topology
- Tree Topology

1. Point to Point topology

Point to Point topology has a dedicated path between two nodes or devices.

It is a simplest topology.

Example: A Child's Tin Can Telephone.

Point to Point Topology



Point to Point topology:

Advantages:

Ease of installation and maintenance.

Easy to understand.

Connections are reliable, secure and fast.

Disadvantages:

As we require lots of cables to design this network so this is an expensive network.

If connection at one end breaks, then there is no communication between two devices.

2. Bus Topology:

In this topology, each nodes are connected to a single cable through interface connectors.

The central cable is the backbone of the network and is known as bus.

The signals are travel in both direction alternately.

The data is send to all the nodes which are connected to central cable but intended node accept the data by matching its machine code.

This topology is used in small network.

Bus Topology



Types of Bus topology:

Linear bus Topology:

In this type of topology, the nodes are connected to a common transmission medium which has exactly two endpoints.

Distributed bus topology:

In this type of topology, the nodes are connected to a common transmission medium which has two or more endpoints.

These endpoints are created by adding branches to the main section of the transmission medium.

Type of Bus Topology:



Bus Topology:

Advantages:

Installation is less costly because less cables are required as compared to other network topologies.

Easy to understand.

Easy to expand by joining two cables together.

Disadvantages:

If central cable break down, then the whole system will fails.

As the no. of nodes increases in network, it led to heavy traffic and performance issues.

3. Star Topology:

In star topology, each node is connected to a single central node called hub, router or switch.

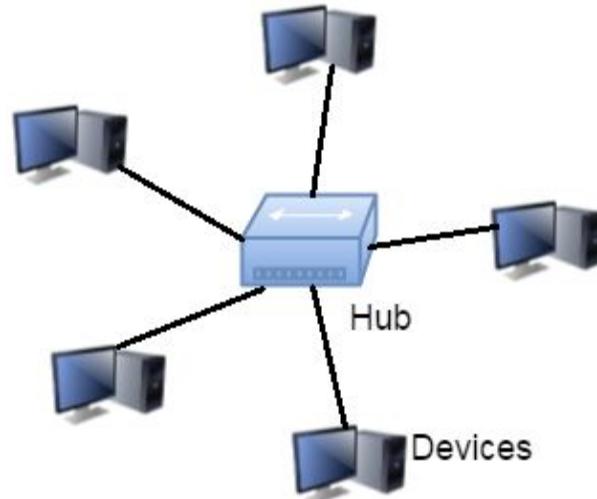
Each node is connected through a point to point connection.

Central node act as a signal repeater.

Every node is indirectly connected to each other node with the help of central node.

Example: Client connected to the server.

Star Topology



Star Topology

Types of Star Topology:

Extended Star Topology:

Extended star topology is a network arrangement in which there are two or more repeaters between the central node.

Distributed Star Topology:

Distributed star topology is a type which represents linear arrangement of network devices i.e. Daisy Chained.

Types of Star Topology



Star Topology:

Advantages:

Easy to troubleshoot.

Easy to install and maintain.

Hub can easily be upgrade.

Fast connection with few nodes and less traffic.

Disadvantages:

Cost of installation is high.

If the central node stop working then the whole system will fails.

Performance is based on the Hub that is it depend upon its capacity.

4. Ring Topology:

Ring topology is a bus topology in a closed loop.

Each node is directly connected to other node within the same network.

When one node sends the data, then it passes through each intermediate nodes in the ring until it reaches its destination.

Each intermediate nodes repeat/retransmit the data to keep signal strong.

Ring Topology



Types of Ring topology:

Unidirectional Ring Topology:

It handles the data traffic in one direction either clockwise or anticlockwise.

This topology is also known as half duplex network.

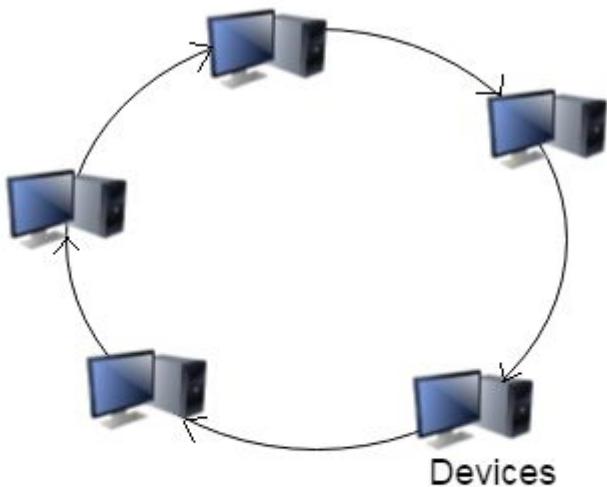
The unidirectional ring topology is easy to maintain as compared to bidirectional ring topology.

Bidirectional ring topology:

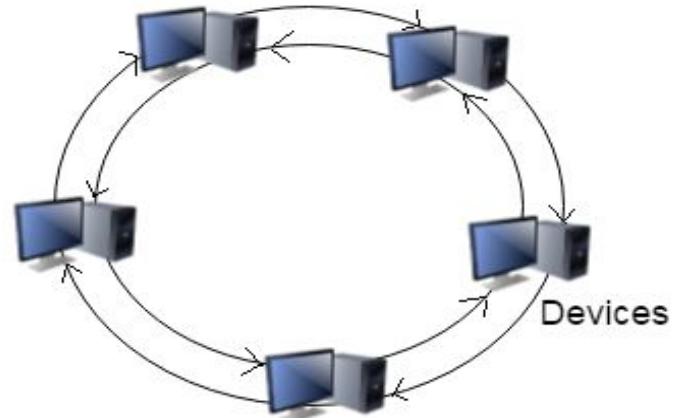
It handles the data traffic in both the directions.

This topology is also known as full duplex network.

Types of Ring Topology



**Unidirectional Ring
Topology**



**Bidirectional Ring
Topology**

Ring Topology:

Advantages:

Network is cheap to install.

High performance network.

Disadvantages:

Difficult to troubleshoot this network.

Adding or deleting of nodes disturb the whole network.

Failure of one node disturb the other nodes.

5. Mesh Topology:

Mesh network represent the point to point connection of each node.

Mesh network has $n(n-1)/2$ physical channel to link n devices.

Mesh Topology



Types of Mesh Network:

Fully Connected Mesh Network:

In this network, every node in the network has a connection to each of the other node in that network.

Partially Connected Mesh Network:

In this network, at least two of the node in the network connected to multiple other nodes in that network.

Types of Mesh Topology



Mesh Network:

Advantages:

This network is a secure network as each node has its own dedicated path.

It is robust.

Easy to troubleshoot.

Disadvantages:

It is difficult to install and configure.

High installation cost.

Difficult to understand.

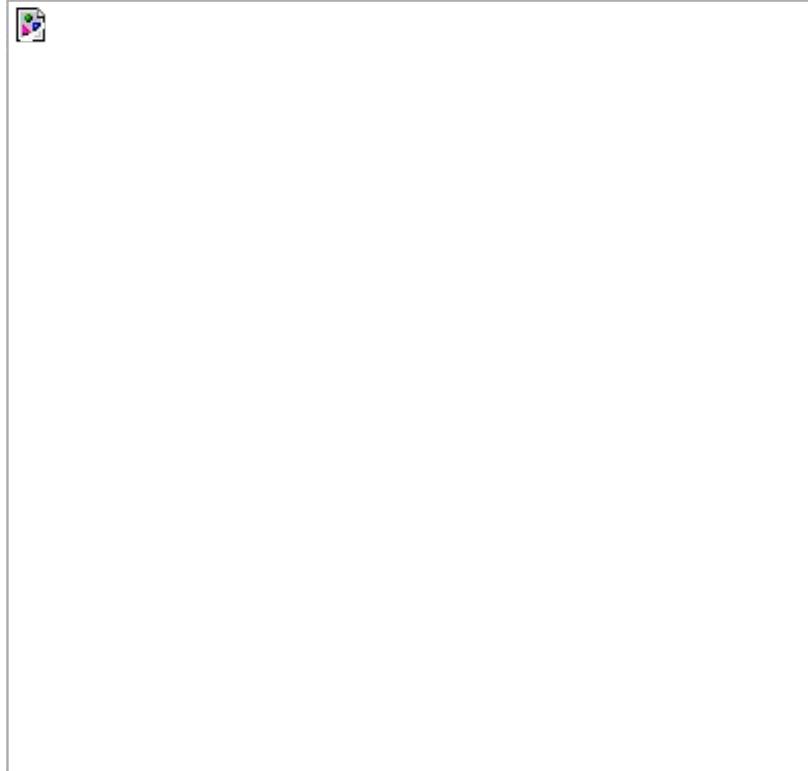
6. Hybrid Topology:

Hybrid topology is the mixture of one or more topologies including bus, mesh, star and tree topologies etc.

Example: If there is a ring topology in one department and the bus topology in another and we connect the both department

Connecting these two topology forms the Hybrid topology.

Hybrid Topology



Hybrid Topology:

Advantages:

Easy to troubleshoot.

Network can easily be expand.

Flexible.

Disadvantages:

Design is complex.

Network installation is difficult.

Expensive network.

7. Tree Topology:

There is a root node in the network and all the other nodes are connected to the root node.

This form a Hierarchy.

Used in Wide Area Network.

Tree Topology



Tree Topology:

Advantages:

Expansion of network is easy.

Ease of installation and maintenance.

Error detection is easy.

Disadvantages:

Expensive network as more cables are required

If the root node stop functioning then the whole network will fail.

OSI Reference Model

Content

1. OSI Reference Model
2. Need of OSI Reference model
3. Architecture
 - Application Layer
 - Presentation Layer
 - Session Layer
 - Transport Layer
 - Network Layer
 - Data Link Layer
 - Physical Layer

Internetworking Model:

Internetworking models are used to make communication between two devices flexible.

Before the invent of these models, the computer communicate with other computer if they are from same manufacturer.

OSI reference Model

It stands for Open system interconnection

Created in late 1970's and it is used in networking.

It is a set of rules and regulations created by ISO (International Organisation for standardization) to make flexible communication between two devices.

It is a primary layered architectural model of network.

OSI model helps the vendors to create interoperable network devices and softwares in the form of protocols. So that different vendor's devices could work with each other.

Need of Reference Model:

Why we need this OSI reference model?

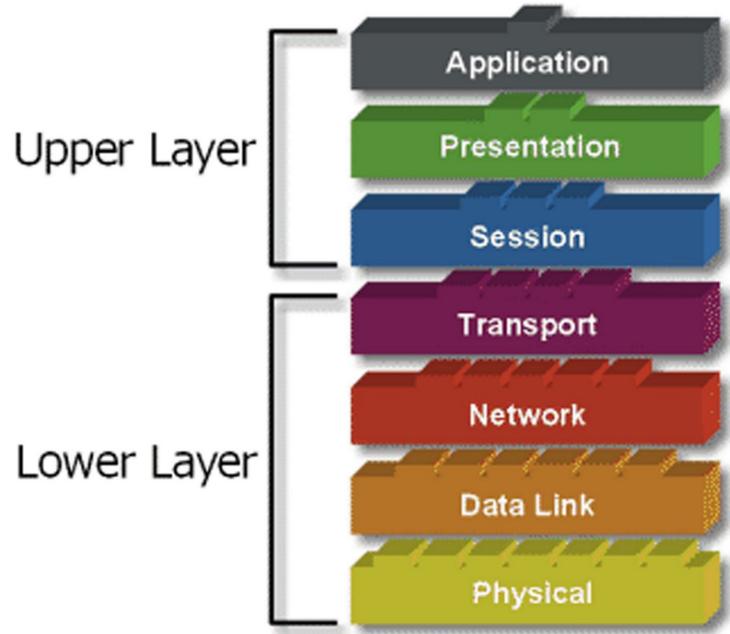
- To make communication possible between two devices which are manufactured by different vendors.
- To implement rules and regulations which are used by every device in the network while communicating.
- Basically,OSI model make communication flexible.

OSI Model Architecture:

It consists of 7 layers

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

OSI Model Architecture



OSI Model Architecture:

1. Application Layer(Layer 7):

It provide an interface between network application and network protocols.

Network applications such as web browser, gmail, Dropbox etc and network protocols which carry request to the destination such as http, ftp, smtp, pop3 etc

It is a user interface where user actually communicate with the devices. It is a software present in computers or devices

Example: Composing a mail in Gmail Software.

OSI Model Architecture:

2. Presentation Layer (Layer 6):

As it name suggest, it present data to the upper layer i.e. Application Layer

It is responsible for data formatting.

It indicate the destination system about the type of file being sent to it by sender.

Example: .mp3 file, jpg file, .txt file, .docx file etc

OSI Model Architecture:

3. Session Layer (Layer 5):

It establish, maintain and terminate the connection between two devices.

Connection may be a simplex, half duplex or full duplex.

It also check wheather the destination system is available or not.

Session Layer perform synchronization.

OSI Model Architecture:

4. Transport Layer (Layer 4):

Transport layer function is to support end to end delivery of packets in network.

It perform these functions:

- Segmentation: It is a process of dividing a large user data into smaller units (packets) for transmission over a data communication network.
- Sequence number: In this process, Sequence number is added to the smaller unit packets.so that it can be arrange at the receiver side.

OSI Model Architecture:

4. Transport Layer (Layer 4):

- Assigning Transmission Protocol: it decide how to transmit the data over network using TCP or UDP protocol
- Assigning logical port number: It define the port of device where the packets have to routed such as http=80,ftp=21,smtp=25 etc

OSI Model Architecture:

TCP Protocol:

It Stands for Transmission control Protocol.

It is connection oriented Protocol

Reliable connection

Speed is slow

Example: http, https, ftp, telnet, smtp use TCP protocol

UDP Protocol:

It Stands for User datagram Protocol.

It is a Simpler,connectionless Protocol.

Not reliable connection.

Speed is fast.

Example: VoIP, DNS,RIP use UDP

OSI Model Architecture:

5. Network Layer (Layer 3):

The main function of network layer is:

This layer done wrapping of segments to form packets.

It add source and destination IP address or Logical address with packets.

At this layer, Router is used to route the packets in the network.

OSI Model Architecture:

6. Data Link Layer (Layer 2):

The main function of data link layer are:

Here the wrapping of packets is done to form frame.

Wrapping is done by adding MAC address or Physical address to the packets.

At this Layer, Switch is used to forward packet in the network.

OSI Model Architecture:

6. Data link Layer (Layer 2):

Further Data link layer has two sublayers:

- LLC(Logical Link Control)- The functions perform by this layer are error checksum/correction, frame synchronization and also check network layer protocol i.e IPv4 or IPv6 .
- MAC(Media Access Control)- This layer is used to add source and destination MAC address or machine address to the frame and it also convert the data in the form of bits.

OSI Model Architecture:

7. Physical Layer (Layer 1):

This layer provide the physical connectivity between the devices via transmission medium such as coaxial wire, optical fiber and wireless.

It is used to send the digital bits through transmission medium.

It handle the bit flow transmission.

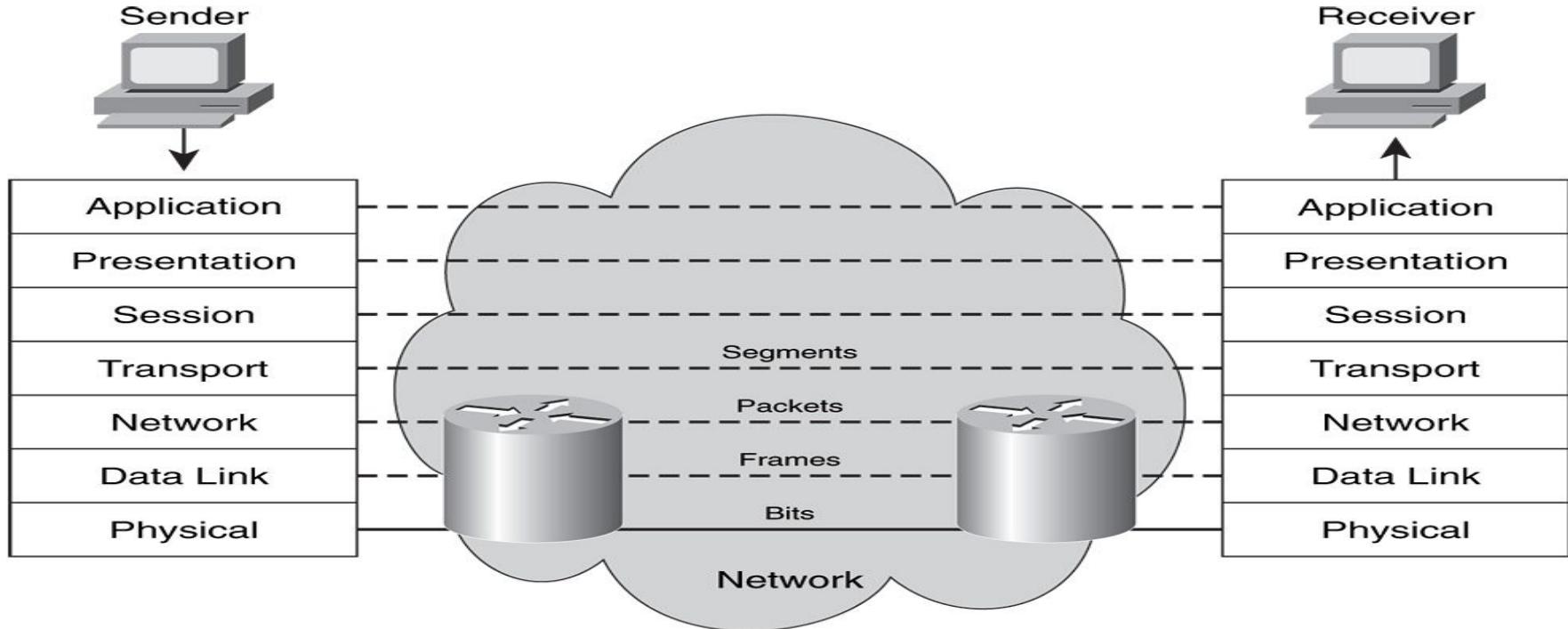
NIC (network interface card) or Hub are used at this Layer.

Working of OSI Model

Content:

1. How OSI model works
2. Advantage of OSI model
3. Disadvantage of OSI model

How OSI model Works?



How OSI model works?

Working of OSI model is explain by using web browser

- The web browser serves as the user interface for accessing a website. The web browser invokes the HTTP to interface with the remote web server.
- The Internet can provide data in a wide variety of formats, so Presentation layer present the type of data format. Common formats on the Internet include HTML, XML, PHP, GIF, and JPEG.
- The Session layer is responsible for establishing, maintaining, and terminating the session between devices and determining whether the communication is half-duplex or full-duplex.

How OSI model works?

Working of OSI model is explain by using web browser

- HTTP utilizes the Transport layer to ensure the reliable delivery of data. It packages the higher-layer data into segments. A sequence number is assigned to each segment so that data can be reassembled upon arrival. It also assign port no and transmission protocol.
- The best path to route the data between the client and the web server is determined by a Network layer. IP address of client and server is added and it also encapsulates segments into packets.

How OSI model works?

Working of OSI model is explain by using web browser

- Data cannot be sent directly to a logical address. As packets travel from network to network, IP addresses are translated to hardware addresses, which are a function of the Data-Link layer. The packets are encapsulated into frames to be placed onto the physical medium.
- The data is finally transferred onto the network medium at the Physical layer, in the form of bits. Signaling and encoding mechanisms are defined at this layer, as is the hardware that forms the physical connection between the client and the web server.

Advantages of OSI Reference Model:

- It make the communication easier by dividing the process into smaller and simpler units.
- This model define the function occurring at each layer.
- It allow communication between various Hardware and software devices from different vendors.
- It simplify teaching and learning process.
- OSI is an idealised networking model.

Disadvantages of OSI Reference Model:

- OSI model has a complex architecture.
- It is not widely used by all devices in the network.
- For fast setup OSI model require agreement between third parties - user and service provider.

TCP/IP Protocol Suite

Content

1. TCP/IP Protocol Suite
2. Architecture
 - o Application Layer
 - o Transport Layer
 - o Network/Internet Layer
 - o Physical Layer/Network interface layer
3. Advantages and disadvantages

TCP/IP Protocol Suite:

TCP/IP stands for Transmission Control Protocol and Internet Protocol

The TCP/IP protocol suite is a collection of protocols that define the Internet.

It was developed by Department of Defence's Project Research Agency (ARPA, later DARPA)

The main aim to design this model is to provide end to end data communication specifying how data should packetized, addressed, transmitted, routed and received in the network.

It is a project of network interconnection to connect remote machines.

TCP/IP Protocol Suite:

TCP/IP is a two-layer program.

The higher layer represent Transmission Control Protocol which manages the assembling of a message into smaller packets that are transmitted over the Internet.

The lower layer represent Internet Protocol which add the IP or MAC address to packets so that it gets to the right destination.

TCP/IP uses the client/server model of communication in which a client user requests and server provide a service in the network.

TCP/IP Architecture:

Old Model of TCP/IP Consist of 4 Layers but its updated model consist of 5 layers:

1. Application Layer
2. Transport Layer
3. Network/Internet Layer
4. Data Link Layer
5. Physical Layer/Network interface layer

Each layer in TCP/IP model corresponds to one or more layers of the 7-layer Open Systems Interconnection (OSI) model.

TCP/IP Model Architecture:

Layer #	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc...	Messages	n/a
4	Transport	TCP/UDP	Segments/Datagrams	Port #s
3	Network or Internet	IP	Packets	IP Address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	10 Base T, 802.11	Bits	n/a

TCP/IP Architecture:

1. Application Layer:

The Application layer provides interface between the application and protocols.

It represents ability to access the services of the other layers and defines the protocols that applications use to exchange data.

The most widely-known Application layer protocols are :

- The Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the Web pages.
- The File Transfer Protocol (FTP) is used for file transfer.

TCP/IP Architecture:

1. Application Layer:

- The Simple Mail Transfer Protocol (SMTP) is used for the transfer of mail messages and attachments.
- Telnet, a terminal emulation protocol, is used for logging on remotely to network hosts.

The Application layer protocols which facilitate the use and management of TCP/IP networks are DNS, RIP etc

Examples of Application layer are Windows Sockets and NetBIOS.

TCP/IP Architecture:

2. Transport layer:

It is also known as Host to Host Transport Layer.

The Transport layer is responsible for end to end delivery of data packets.

The protocols of the Transport layer are TCP and UDP.

It performs functions such as multiplexing, segmenting or splitting of data

Transport layer adds header information to the data.

Transport layer arranges the packets to be sent, in sequence.

TCP/IP Architecture:

3. Network Layer:

It is also known as Internet Layer.

The Network layer performs basic functions such as addressing, packaging, and routing of data packets.

This layer holds the whole architecture together and helps the packet to travel independently to the destination.

The Internet layer is analogous to the Network layer of the OSI model.

TCP/IP Architecture:

3. Network Layer:

The protocols used at Network layer are:

- The Internet Protocol (IP) is responsible for IP addressing, routing, and the fragmentation and reassembly of packets.
- The Address Resolution Protocol (ARP) is responsible for the resolution of the IP address to the Network Interface layer address such as a MAC address.
- The Internet Control Message Protocol (ICMP) is responsible reporting errors due to the unsuccessful delivery of IP packets.

TCP/IP Architecture:

4. Data Link Layer:

Functions performed are:

- Data Framing: it encapsulates the data messages into frames that are sent over the network at the physical layer.
- Addressing: Data link layer add this MAC address with data message.
- Error Detection and Correction: The data link layer handles errors that occur at the lower levels of the network stack. For example: cyclic redundancy check (CRC) field.

TCP/IP Architecture:

4. Data Link Layer:

The following are the functions performed by sublayer of data link layer:

- **Logical Link Control (LLC):**

Logical link control is responsible for the establishment and control of logical links between local devices on a network.

LAN technology use the IEEE 802.2 LLC protocol.

TCP/IP Architecture:

4. Data Link Layer:

- **Media Access Control (MAC):**

This Layer is used by devices to control access to the network medium.

As many networks use a shared medium so management of the shared medium is necessary to reduce conflicts.

For example - Ethernet uses the CSMA/CD method of media access control.

TCP/IP Architecture:

5. Physical Layer:

It is also known as network interface layer and Network access Layer.

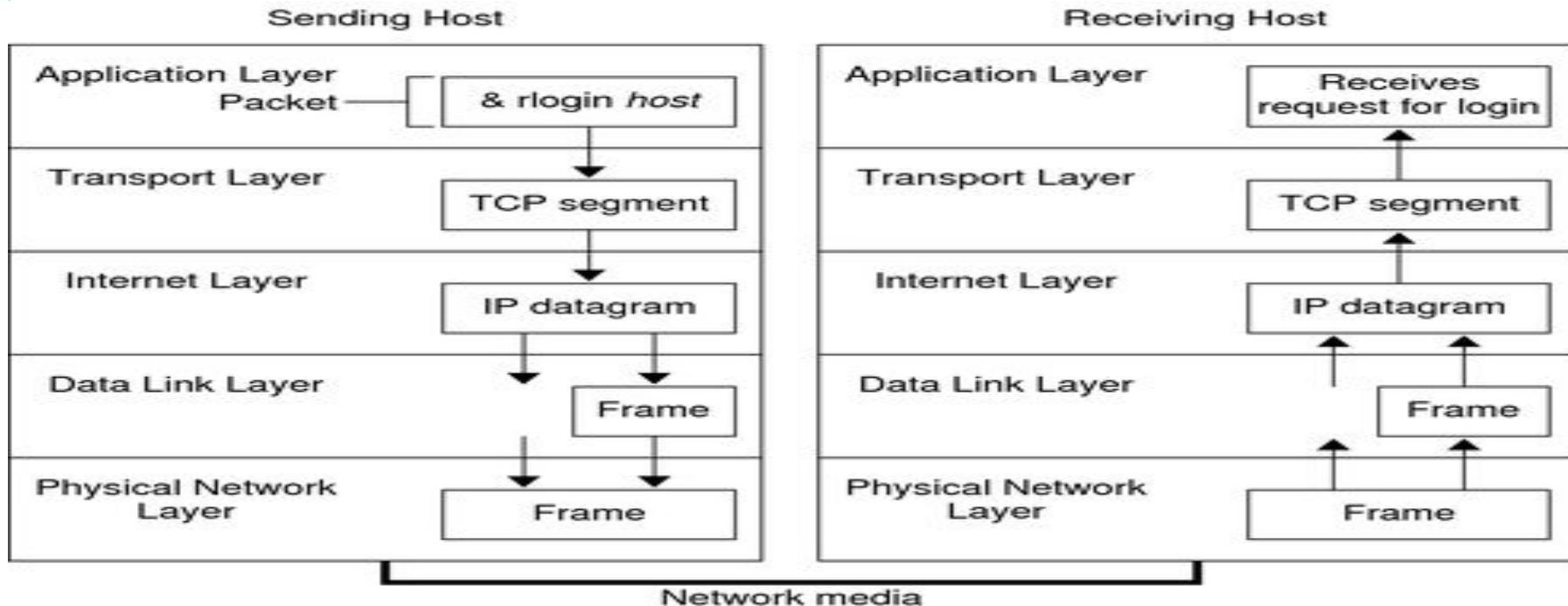
Protocols are used to connect host to host and network to network.

The Network Interface layer is responsible for sending and receiving TCP/IP packets on the network medium.

These include LAN technologies and WAN technologies.

The Network Interface layer is same as Physical layers of the OSI model.

TCP/IP model:



Advantages of TCP/IP Model:

- TCP/IP model is model which is operated independently.
- It is scalable model.
- It follows client/server architecture.
- It is used with number of routing protocols.
- It can be easily used to establish a connection between two computers.

Disadvantages of TCP/IP Model:

- The transport layer is not responsible for delivery of packets.
- The model cannot be used in any other application.
- Replacing any protocol is not easy.
- It has no clear description about services, protocols and interfaces at each layer.

TCP/IP Protocols

Content:

1. Protocols
 - o TCP
 - o UDP
 - o ICMP
 - o IGMP

Protocols:

- **Transmission Control Protocol (TCP):**

The main protocol of the Internet protocol suite is Transmission Control Protocol (TCP), so that's why the entire suite is referred as TCP/IP.

It provides reliable, ordered, and error-checked delivery of a stream of bits between applications running on user device

Internet applications such as the World Wide Web, email and file transfer rely on TCP.

Protocols:



Transmission Control Protocol (TCP) Header

Protocols:

- **Transmission Control Protocol (TCP) Header:**
 - Source port - 16 Bit number it represents the Source Port number.
 - Destination port - 16 Bit number it represents the Destination Port number.
 - Sequence number - 32 Bit number is used for numbering TCP data segments.
 - Acknowledgment Number - It is of 32 Bit number field that indicates that the sending device is expecting a next sequence number from the other device.

Protocols:

- **Transmission Control Protocol (TCP) Header:**
 - Data Offset - It is also known as Header Length field. The number of 32 bit words in the TCP Header. The minimum size header is 5 words . This field hold the user.
 - Reserved - It is of 6 bit always set to 0 and reserved for future use.
 - Control Bits - It is of 6 bits. Control Bits manage the entire process of connection establishment,maintenance and termination.

URG: Urgent Pointer field

ACK: Acknowledgment field

PSH: Push Function

RST: Reset the connection

SYN: Synchronize sequence no

FIN: No more data from sender

Protocols:

- **Transmission Control Protocol (TCP) Header:**
 - Window - It indicates the size of the receive window that the receiver is currently willing to receive. It specifies the number of bytes to be received in the acknowledgment field
 - Checksum - The checksum field is used for error-checking of the header field and data. It is of 16 bits long.
 - Urgent Pointer - When the URG bit is set, the urgent data is given priority over other data streams. It is of 16 bits and shows the end of the urgent data

Protocols:

- **User datagram Protocol (UDP):**

UDP is a simple connectionless transmission model. It uses minimum number of protocol for data transmission.

UDP provides checksums for data integrity and port numbers for addressing the packet in the network.

There is no guarantee of delivery, ordering, or duplicate of data packets in the network.

Protocols:



User Datagram Protocol (UDP) Header

Protocols:

- **User datagram Protocol (UDP) Header:**

UDP header consists of four fields each of 2 bytes in length:

- Source Port - (16 bits) It indicate the port number of source device from where data originates.
- Destination Port - (16 bits) It indicate the port number of destination device where the data have to send.

Protocols:

- **User datagram Protocol (UDP) Header:**
 - UDP length - It indicates the length (in bytes) of the UDP header and the encapsulated data. The minimum value for this field is 8 bytes.
 - UDP Checksum - (16 bits) The checksum field is used for error-checking of the header field and data. This field is optional in IPv4 addressing, and mandatory in IPv6 addressing. If this field remains unused then it contains all zeros

Protocols:

- **Internet Control Message Protocol (ICMP):**

The Internet Control Message Protocol is a protocol which we use in Internet protocol suite.

ICMP is used by network devices, like routers, to send error messages and operational information.

Difference between ICMP and other transport protocols such as TCP and UDP is that it is not used for exchanging data between systems in network.

Protocols:



Internet Control Message Protocol (ICMP)

Protocols:

- **Internet Control Message Protocol (ICMP) Header:**

The ICMP header starts after the IPv4 header. ICMP packets have an 8-byte header and variable-sized data section.

- Type - The type field indicate the type of ICMP packet. This is always different from ICMP type to type. This field is of 8 bits.
- Code - All ICMP types have different codes. Some types only have a single code, while others have several codes. This field is 8 bits in length.

Protocols:

- **Internet Control Message Protocol (ICMP) Header:**
 - Checksum - The Checksum is a 16 bit field used for error-checking of the header field and data.
 - ICMP content - This field have variable size and contain the user data if any.

Protocols:

- **Internet Group Management Protocol (IGMP)**:

The Internet Group Management Protocol (IGMP) is a communications protocol

It is used by hosts and routers on IPv4 networks to establish multicast group memberships.

IGMP is also used for networking applications such as online streaming video and gaming.

IGMP is used on IPv4 networks.

Protocols:



Internet Group Management Protocol (IGMP)

Protocols:

- **Internet Group Management Protocol (IGMP) Header:**
 - Version - (4 bits) It indicate the type of version of IGMP packet i.e. v1,v2 or v3
 - Type - (4 bits) It indicates the type of IGMP Packet Example Type 1 for create group msg, type 2 for create group reply and so on.
 - Code - (8 bits) It indicate the IGMP packet code related to the type of IGMP packet. Different IGMP types have different codes.

Protocols:

- **Internet Group Management Protocol (IGMP) Header:**
 - Checksum - The checksum is the 16-bit used for error-checking of the header field and data.
 - Group Address - It is of 32 bit. In a Create Group Request message, the group address field contains zero and In all other Request messages, the group address field contains a host group address.

TCP/IP Applications

Content:

1. TCP/IP Applications
 - o WWW
 - o Telnet
 - o SSH
 - o Email
 - o FTP

TCP/IP Applications:

1. World Wide Web:

Web is a collection of servers that stores specially formatted documents using language such as HTML.

Web browsers are designed to request HTML pages from web servers and then open them.

The Internet must be used to access the web pages from web server.

http:// plus IP address is used to access web page from web servers.

Example http://192.168.4.1

TCP/IP Applications:

1. World Wide Web:

As internet addresses are difficult to remember, so text addresses of websites are entered which are easy to memorize.

DNS protocol is used by web server to convert text addresses into IP addresses.

HTTP protocol is used by web to identify how messages are formatted, transmitted, requested and responds to the transfer of HTML formatted file.

Microsoft server name is Internet Information Services

TCP/IP Applications:

2. Telnet:

Telnet is a user command which is used to access the remote computer.

Telnet user can access remote computer by having its username and password.

It use TCP/IP port number 23

For example: it is used by program developers and anyone who has a need to use specific applications or data located at a particular host computer.

TCP/IP Applications:

3. Secure Socket Shell (SSH):

Secure Socket shell is a network protocol which provides a capability to the user to access a remote computer with a secure way

Secure Socket Shell program is similar to that of Telnet but it include data encryption and authentication

It use a TCP/IP port 23

The encryption used by SSH provide confidentiality and integrity of data over an unsecured network.

TCP/IP Applications:

4. E-Mail:

E-Mail or Electronic Mail play a major part in internet revolution.

It is a method of exchanging messages and attachments over the internet.
This is a free service which is offered by ISP.

It provide a quick way for people to communicate with one another.

Email servers accept, forward, deliver and store messages.

Web based services providing access to email are Google's Gmail,
Microsoft Windows live Outlook, Yahoo! Mail

TCP/IP Applications:

4. E-Mail:

Protocols used by E-mail program are: SMTP,POP3 and IMAP4

- Simple Message Transfer Protocol (SMTP): SMTP protocol is used by a client send mail .It use TCP/IP port 25.
- Post Office Protocol Version 3 (POP3): POP3 protocol is used to receive email from SMTP server. It use TCP/IP port 110. This protocol is not used now.
- Internet Message Access protocol version 4 (IMAP4): IMAP4 is an alternative to POP3. it is used to retrieve an email from email server. It use TCP/IP port 143. It also support some extra features.

TCP/IP Applications:

5. File Transfer Protocol (FTP):

File Transfer Protocol is a standard network protocol used for transferring computer files between network devices in a network.

FTP is similar to that of HTTP protocol but FTP transfer is more reliable and fast.

FTP provides a secure transmission that protect the username and password and encrypt the content of a file.

FTP use SSL/TLS (Secure socket layer/Transport layer security) to provide security. Sometime FTP is also known as SFTP.

TCP/IP Ports

Content:

1. TCP/IP Port numbers
2. Difference between OSI and TCP/IP model

TCP/IP Port Number:

A Port number is a 16 bit value and it range lies between 0 to 65535.

Port number from 0 to 1023 are the well known port numbers and these port numbers are reserved for specific TCP/IP application.

Port number from 1024 to 49151 are registered ports and these are used by less common TCP/IP applications.

Port number from 49152 to 65535 are dynamic or private ports.

For example: web server port number is 80,

TCP/IP Port Numbers:

Some of the well-known TCP/IP Port :

FTP	(File Transfer Protocol)	20/21
SSH	(Secure Socket Shell)	22
Telnet	-	23
SMTP	(Simple Mail Transfer Protocol)	25
DNS	(Domain Name System)	53
DHCP	(Dynamic Host Configuration Protocol)	67/68
TFTP	(Trivial File transfer Protocol)	69
HTTP	(Hypertext Transfer Protocol)	80
POP3	(Post Office Protocol version 3)	110
IMAP	(Internet Message Access Protocol)	143

TCP/IP Port Number:

Netstat commands to check TCP/IP port connection:

To know with whom our computer is communicating type netstat commands in command line such as

netstat -n = show many different connections to which our computer is connected through TCP/IP

netstat -an = show all active TCP/IP connection.

netstat -ano = show the process ID of different connection

Difference b/w OSI and TCP/IP Model:

OSI Reference Model:

- OSI stand for Open System Interconnection.
- OSI is a protocol independent standard, which act as a communication gateway between the network
- OSI Model consist of 7 Layers.
- In OSI model ,the transport layer take guarantee for the delivery of packets.

TCP/IP Model

- TCP/IP stands for Transmission Control Protocol/ Internet Protocol.
- TCP/IP model is a communication protocol, which allows connection of hosts over a network.
- TCP/IP Model consist of 5 layers.
- In TCP/IP model the transport layer does not guarantees for the delivery of packets.

Difference b/w OSI and TCP/IP Model:

OSI Reference Model:

- OSI model has a separate Presentation layer and Session layer.
- Here, network layer provides both connection oriented and connectionless service.
- OSI model is a theoretical model used for learning.

TCP/IP Model:

- TCP/IP does not have a Presentation layer or Session layer.
- In this, network layer provides connectionless service.
- TCP/IP is a practical model is used in networking.

TCP/IP Security

Content:

1. TCP/IP security
 - Encryption
 - Integrity
 - Non Repudiation
 - Authentication
 - Authorization

TCP/IP Security:

Security in TCP/IP model plays a main role. To make the TCP/IP data and network secure, TCP/IP add these five security features.

1. Encryption
2. Integrity
3. Non Repudiation
4. Authentication
5. Authorization

TCP/IP Security:

1. Encryption:

In network, data is transmitted in the form of 1 and 0 and it is very easy for hackers to steal the data and read or modify it.

Encryption is a process of converting user data into a code in such a way that only authorized parties can access it.

Encryption is the most effective way to achieve data security.

Encryption can be one in two ways:

- Symmetric Key Algorithm Standard (SKAS)
- Asymmetric Key Algorithm Standard (AKAS)

TCP/IP Security:

2. Integrity:

It is a process to guarantees that the data received is the same as original data sent by sender.

It indicate that their is no difference between send data and received data in the network.

Integrity covers the situation of data stealing in the network and modification of interrupted data by the hackers.

In TCP/IP hash tool is used to provide data Integrity.

TCP/IP Security:

2. Integrity:

Cryptographic Hash function is a mathematical function that run over a string of binary digits of data (of any length) and results in a value of fixed length called a checksum.

Hash function is one way function that is it is irreversible function. We cannot create data bits using its checksum bits.

Secure Hash Algorithm is used now which include a family of cryptographic hash functions such as SHA1, SHA2 and SHA 3.

TCP/IP Security:

3. Non Repudiation:

Non Repudiation is a process of making sure that the party with which we are signing any contract or a communication cannot deny the authenticity of their signature on a document.

It is a service that provides proof of the integrity and origin of data that the data is coming from a person or entity it was to came from.

Non Repudiation provide assertion of authentication with high assurance that the person or entity with which we are dealing are genuine.

Non Repudiation is done by Digital Signatures or PKI

TCP/IP Security:

4. Authentication:

Authentication is the process of positively identifying an individual trying to access data, usually based on a username and password.

It is any process by which a system verifies the identity of a user who wants to access it.

TCP/IP security standards are Point to Point Protocol (PPP), Authentication Authorization Accounting (AAA) , Extensible Authentication Protocol (EAP) and 802.1X etc.

TCP/IP Security:

5. Authorization:

Authorization is the function of specifying the right to access resources such as personal information and data over computer network.

In general "to authorize" means is to define an access policy.

Access Control List (ACL) is a list of access control entries (ACE).

ACE are identified by the different trustees and they specifies the access rights allowed, denied, or audited for that trustee.

TCP/IP Security:

5. Authorization:

Three type of access control lists modals are:

MAC (Mandatory Access Control) - access is strictly controlled by system administrator

DAC (Discretionary Access Control) - allow each user to control access to their own data

RBAC (Role Based Access Control) - assign permission to a particular role in an organisation

Encryption & Non-Repudiation

Content:

1. Encryption technique
 - o Symmetric Key Algorithm Standard (SKAS)
 - o Asymmetric Key Algorithm Standard (AKAS)
2. Non-Repudiation technique
 - o Digital Signature
 - o Public Key Infrastructure (PKI)

TCP/IP Security:

1. Encryption:

- Symmetric Key Algorithm Standard (SKAS): are algorithms for cryptography that use the same cryptographic keys for both encryption and decryption of data.

SKAS use DES (Data Encryption Standard) which is a first standard used for encryption. DES use 64 bit block and a 56 bit key.

After DES, many other encryption techniques are invented such as 3DES, International Data Encryption Algorithm (IDEA) and Blowfish.

TCP/IP Security:

1. Encryption:

- Symmetric Key Algorithm Standard (SKAS):

Rivest Cipher 4 (RC4) was a very popular SKAS algorithm technique used to encrypt data from 2001 to 2013.

Now most of the TCP/IP applications use Algorithm Encryption Standard (AES) technique.

AES use 128 bit block size and 128-,192- or 256- bit key size.

TCP/IP Security:

1. Encryption:

- Symmetric Key Algorithm Standard (SKAS):

SKAS has one serious drawback that if anyone get a hold of the key can encrypt and decrypt data easily.

So there is a need to create a new method which allow the encrypter to send a key to the decrypter without the fear of intervention

So that method is AKAS (Asymmetric key algorithm standard)

TCP/IP Security:

1. Encryption:

- Asymmetric Key Algorithm Standard (AKAS): is method of cryptography that use the two different cryptographic keys for both encryption and decryption of data.

In AKAS, Public Key Cryptography is used to exchange the key securely between two communicating devices.

The two key generated are : Private key is used by sender to encrypt the data and Public key is used by receiver to decrypt the data.

These two keys are called key pairs and are generated at same time and designed to work together.

TCP/IP Security:

2. Non Repudiation:

Digital Signature: are digital code which is attached to an electronically transmitted document or message to verify its contents and the sender's identity.

Digital Signature are hash of messages encrypted by a private key.

Digital signature solve the problem of tampering and impersonation in digital communications.

It is widely used by e-mail user.

TCP/IP Security:

2. Non Repudiation:

Public Key Infrastructure (PKI): is a set of rules and regulations need to create, manage, use and store digital certificates and manage public-key encryption.

PKI is used to facilitate the secure electronic transfer of data for a different network activities such as e-commerce, internet banking and confidential email.

It is required for such network activities where simple passwords are not sufficient for authentication.

TCP/IP Security:

2. Non Repudiation:

Public Key Infrastructure (PKI): The Digital certificates are used to verify the exchange of public keys in network.

When someone wants to create a secure website then he or she have to buy a certificate signed by a certificate authority (CA) such as Verisign, Thawte or GoDaddy.

Public key cryptography is a cryptographic technique which enables internet users to securely communicate over an insecure public network.

TCP/IP Security:

2. Non Repudiation:

Public Key Infrastructure (PKI): consists of

- Certificate Authority (CA) stores, issues and signs the digital certificates.
- Registration Authority verifies the identity of different entities requesting their digital certificates to be stored at the CA.
- Central Directory indicate secure location to store certificates.
- Certificate Management System used to manage the access to stored certificates and the delivery of the certificates to be issued.
- Certificate Policy define rules to issue certificates.

Authentication

Content:

1. TCP/IP Authentication security standards
 - PPP (Point to Point Protocol)
 - AAA (Authentication, Authorization and Accounting)
 - EAP (Extensible Authentication Protocol)

TCP/IP Security:

1. Authentication:

Point to Point Protocol (PPP):

PPP is a data link layer protocol i.e. layer 2.

It is used to establish a direct connection between two devices.

PPP can provide connection authentication, transmission encryption and compression.

PPP uses Challenge Handshake Authentication Protocol (CHAP) to provide a more secure authentication process.

TCP/IP Security:

1. Authentication:

Point to Point Protocol (PPP):

In CHAP authentication technique, actual password cannot be send over the link.

Microsoft develop more detailed version of CHAP known as MS-CHAP (MS-CHAPv2 is its current version).

MS-CHAPv2 is widely used in dial-up connections is more secure than any other authentication technique

TCP/IP Security:

4. Authentication:

Authentication, Authorization and Accounting (AAA):

PPP protocol work very well for devices connected end to end for communication.

The two devices are authenticated on the basis of username and password.

But what happen if devices wants to communicate and they don't have point to point link.A number of intermediate devices are present in between two devices in a network

TCP/IP Security:

1. Authentication:

Authentication, Authorization and Accounting (AAA):

This means each intermediate device goes through separate authentication process.

For this a new method of authentication is developed name AAA.

AAA is designed on the basis of port identification.

Based on this AAA method two standards are developed such as RADIUS and TACACS+

TCP/IP Security:

1. Authentication:

Authentication, Authorization and Accounting (AAA): AAA include three parts:

- **Authentication**: It gives the computer the right to access the network.
- **Authorization**: After a device get authenticated now it determine a device that what it can or cannot do on network.
- **Accounting**: Now server can do accounting related to device which is authenticated that how many time a user logon or logoff from network or various online activities perform by device .

TCP/IP Security:

1. Authentication:

Extensible Authentication Protocol (EAP): EAP is not a protocol but it is a general purpose PPP wrapper use in wireless technology.

EAP forms a huge success in authentication process. Due to this a need was felt to develop a EAP solution for Ethernet.

EAP solution for Ethernet is known as 802.1X

802.1X is a port based authentication process which is used to access and control the network. It use full AAA process for authentication

TCP/IP Security:

1. Authentication:

Extensible Authentication Protocol (EAP): Most commonly used EAP standards are:

- EAP PSK (Personal Shared Keys)
- EAP TLS (Transport Layer Security)
- EAP TTLS (Tunneled TLS)
- EAP MSCHAPv2 also known as PEAP (Protected Extensible Authentication Protocol)
- EAP MD5 (Message digest algorithm version 5)
- LEAP (Lightweight Extensible Authentication Protocol)

TCP/IP Secure Application

Content:

1. Secure TCP/IP application
 - o HTTPS
 - o SCP
 - o SFTP
 - o SNMP
2. TCP/IP Standard
 - o SSL/TLS
 - o IPsec

Secure TCP/IP Applications:

By using these protocols TCP/IP form a new application based on securities

These Secure TCP/IP applications are:

- HTTP Secure (HTTPS): HTTPS use SSL/TLS to provide authentication and encryption to web pages. It provide a connection to a trusted and verified web sites.
- Secure Control Protocol (SCP): SCP is used by SSH to transfer data securely between two devices. SCP replaces the FTP.

Secure TCP/IP Applications:

- Secure FTP (SFTP): also known as SSH FTP and used to transfer files over the network.
- Simple Network Management Protocol (SNMP): SNMP is a tool used for network management.

It is used for collecting information and configuring network devices such as servers, printers, hubs, switches etc.

It collects the information like CPU usage, network utilization and details about firewall. SNMPv1, SNMPv2 and (current version) SNMPv3 are versions of SNMP.

TCP/IP Standards:

Most popular TCP/IP standards over internet used for encryption as well as authentication are SSL/TLS and IPsec.

1. Secure Socket Layer/Transport Layer Security (SSL/TLS):

SSL was developed by Netscape. SSL require server which contain the certificates.

When a client request the SSL server to access its resources then SSL server send a copy of that certificate to the client.

Then client checks the certificate and authenticate the server (is genuine or not).

TCP/IP Standards:

1. Secure Socket Layer/Transport Layer Security (SSL/TLS):

Then a secure and encrypted link is created between the SSL client and SSL servers.

TLS is a upgrade version of SSL. TLS is similar to SSL but TLS is more robust and flexible and can work with any TCP/IP application

SSL works with HTML,FTP, SMTP and various other older TCP application

Whereas TLS work with old and new TCP applications like VoIP and VPN.

TCP/IP Standards:

2. IPsec:

IPsec is a protocol which provide encryption and authentication at Internet/Network Layer of TCP/IP model.

IPsec is used in IPv6.

IT work in two different modes: Transport and tunnel mode.

IPsec use different protocols to provide authentication and encryption such as Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Security association and Key Management Protocol (ISAKMP) and Internet Key exchange (IKE) etc.

Ethernet Specification

Content

1. About Ethernet
2. Broadband signal and Baseband signal
3. How data is transmitted over Ethernet
 - o CSMA/CD

Ethernet:

Bob Metcalfe, first invented the Ethernet network on May 22, 1973 to interconnect advanced computer workstations.

Ethernet is a network protocol referred as IEEE 802.3 protocol.

It was introduced in 1980 and then standardized in 1983 as IEEE 802.3

It is a family of computer networking technologies that controls how data is transmitted over a LAN and MAN network

Ethernet:

The protocol has evolved and improved over time and now it can deliver speed up to gigabits per second.

It is used to connect computers and devices. It connects any type of computer to its network if that device has an Ethernet adapter or network card.

Ethernet uses hybrid star-bus topology to connect devices in the network

Ethernet Works on Layer 1 and Layer 2 of OSI model.

Ethernet:

Broadband signal and Baseband signal:

In broadband, analog signal are used to transmit data using FDMA technique. Transmission of data is unidirectional and signals can travel at long distance.

In baseband, digital signal are used to transmit data. It doesn't support FDMA technique. Baseband support bidirectional transmission and it can travel shorter distance.

Ethernet:

How data is transmitted over Ethernet cable?

Ethernet is a shared medium for sending packets of data. There are rules to avoid conflicts and to protect data integrity over Ethernet.

Device check when the network is available for sending packets.

It is possible that two or more devices at different locations will attempt to send data at the same time. When this happens, a packet collision occurs.

Ethernet:

CSMA/CD

- In order to eliminate collisions, ethernet uses a protocol called Carrier Sense Multiple Access/Collision Detection (CSMA/CD).
- CSMA/CD is a protocol which defines which device should use a ethernet cable at given time.
- Carrier Sense means each device in the network first sense the ethernet cable before sending packets
- They check the cable weather it is free or any data traffic is present over it and accordingly send their data.

Ethernet:

- Multiple access means every device in ethernet network have equal access to the ethernet. When ethernet cable is free.
- If two devices sense the cable at same time and found that cable is free.they start transmitting their data at same time over shared ethernet.
- This led to collision of data in network.
- NIC cards of both devices notice the collision and then these both devices wait for a random time to again send the packet.
- The device which generate the lowest random number begin to retransmit first.

Ethernet:

- The other device wait for ethernet wire to get free.
- Collision Domain is a group of devices that has a capability to send the packet at same time in the ethernet network.
- This led to a collision in a network.

Ethernet at Physical Layer

Content:

1. Ethernet Evolution
 - o Standard Ethernet
 - o Fast Ethernet
 - o Gigabit Ethernet
 - o Ten Gigabit Ethernet

Ethernet at Physical Layer:

The Ethernet at physical layer defines the electrical or optical properties of the physical connection between a device and the network.

It tells about the medium of transmission used between the network devices

Its speed ranges from 1 Mbit/s to 10 Gbit/s.

The physical medium can be a coaxial cable , twisted pair cable or optical fiber.

Ethernet at Physical Layer:

Ethernet Evolution:

1. Standard Ethernet (10mbps)
 - o 10Base5 (Thick coaxial wire)
 - o 10base2 (Thin coaxial wire)
 - o 10BaseT (UTP cable)
 - o 10BaseF (Optical Fiber Cable)
2. Fast Ethernet (100mbps)
 - o 100BaseTX (2 UTP wire)
 - o 100BaseFX (2 Fiber wire)
 - o 100Base T 4 (4 UTP wire)

Ethernet at Physical Layer:

Ethernet Evolution:

3. Gigabit Ethernet (1gbps)
 - o 1000Base SX (Short wave, Optical Fiber)
 - o 1000Base LX (Long wave, Optical Fiber)
 - o 1000Base CX (STP wire, 2 Copper wire)
 - o 1000Base T (STP wire, 4 Copper wire)
4. Ten Gigabit Ethernet (10gbps)

Ethernet at Physical Layer:

1. Standard Ethernet (10Mbps /Baseband signal)

Ethernet	Distance	Node per hub	Topology	Cable Type
10Base5	500 m	-	Bus	Thick coaxial
10base2	185 m	-	Bus	Thin coaxial
10BaseT	100 m	1024	Star-bus	CAT 3/UTP
10BaseF	2000 m	1024	Star-bus	Multimode OF

Ethernet at Physical Layer:

2. Fast Ethernet (100mbps /Baseband signal)

Ethernet	Distance	Node per hub	Topology	Cable Type
100Base T4	100 m	1024	Star-Bus	CAT3
100baseTX	100 m	1024	Star-Bus	CAT5/STP/UTP
100BaseFX	2000 m	1024	Star-Bus	Multimode OF

Ethernet at Physical Layer:

3. Gigabit Ethernet (1gbps /Baseband signal)

Ethernet	Distance	Node per hub	Topology	Cable Type
1000Base SX	550 m	-	Bus	Shortwave fiber
1000base LX	5 km	-	Bus	Longwave fiber
1000Base CX	25 m	1024	Star-bus	Copper STP 2
1000Base T	100 m	1024	Star-bus	Copper UTP 4

Ethernet at Physical Layer:

To understand standard Ethernet code, we have to understand the meaning of each code:

- 10 - at the beginning indicate the speed of network i.e. 10Mbps.
- BASE - indicates the type of signaling used i.e. baseband.
- 2 or 5 - at the end indicates the maximum length of cable in meters.
- T - at the end stands for twisted-pair cable.
- X - at the end stands for full duplex-capable cable.
- FL - at the end stands for fiber optic cable.

Ethernet at Data Link Layer

Content:

1. Ethernet at data link layer
2. Ethernet address
3. Ethernet frame

Ethernet at Data link Layer:

Ethernet at data link layer is responsible for ethernet addressing ,Hardware addressing or MAC addressing.

At data link layer, Ethernet encapsulates packets that are coming from Network Layer and form frames and then transmit over physical media.

Ethernet MAC addresses are in hexadecimal format. It consists of 6 byte (48 bits).Here first three bytes tells the identity of the vendor and the last three bytes tells node identity.

At Data Link layer, no modification is required to the MAC address when going between different physical layer interfaces, such as from Ethernet to Fast Ethernet

Ethernet at Data link Layer:

Ethernet Addressing:

A MAC address (Media Access Control address) is a unique code which is stored on network interface cards or ethernet cards. There are two types of MAC addresses:

- Universal Administered MAC addresses assigned to devices by their manufacturers (burned-in).
- Organizationally Unique Identifiers (OUI) are administered by the IEEE Standards Association

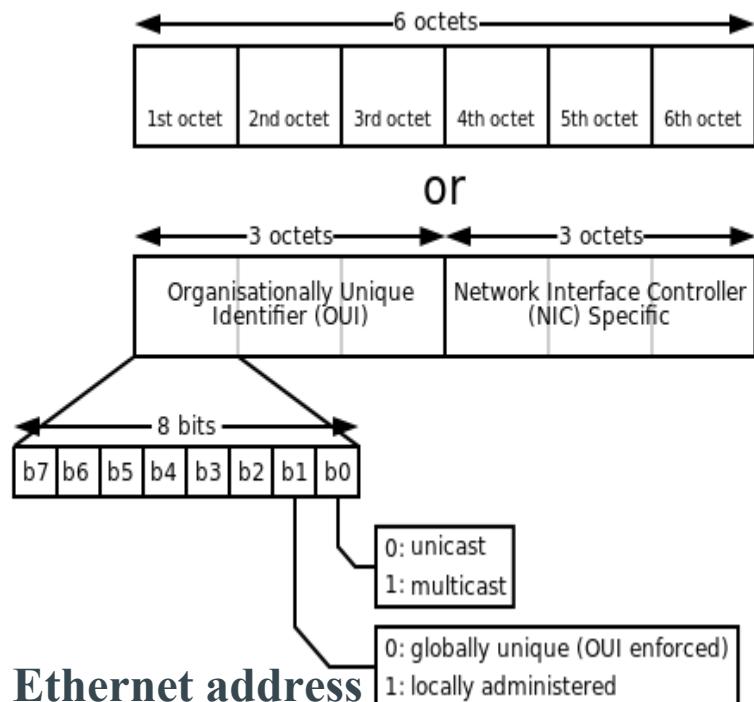
Ethernet at Data link Layer:

Ethernet Addressing: MAC address format

- The first three bytes tell about the manufacturer also known as the Organizationally Unique Identifier (OUI).
- The 1st bit of the first byte is referred to as unicast or multicast bit.
If the bit is set to 0 (zero), the frame is meant to reach only one receiving NIC. This type of transmission is called unicast.
If the bit is set to 1, the frame will be sent only once to particular nodes in network; This is called multicast addressing.
- The 2nd bit of the first byte is referred to as the U/L bit (Universal/Local) which identifies how the address is administered i.e. Globally unique or locally administered.

Ethernet Address

Each NIC card/ethernet adapter contain a unique code which is provided by the manufacturer, that unique code is known as Media Access Control address or Ethernet Address.



Ethernet at Data link Layer:

Example 1:

MAC address = **04**-00-00-00-00-00

The first byte in binary form is 000001**00**, where the first bit is 0.

This define that the address is unicast address.

Here the second bit is also 0

This define that the address is a universally administered address.

Ethernet at Data link Layer:

Ethernet Frames:

The main function of data link layer is to convert bits into bytes and then bytes into frames.

It encapsulates the packet that are coming from network layer to frame and then transmit it to the physical layer for transmission.

Ethernet Frame

The MAC frame format for Ethernet, IEEE 802.3 used within the 10 and 100 Mbps systems is shown as

7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes
Preamble	SFD	Destination Address	Source Address	Length	Data and Padding	FCS

IEEE 802.3 Ethernet Frame

Ethernet at Data link Layer:

The frame consists of seven parts divided into three main areas:-

1. Header

- Preamble (PRE) - This is seven bytes long. It consists of a pattern of alternating ones and zeros, and this informs the receiving stations about the start of frame and enable synchronisation. (10 Mbps Ethernet)
- Start of Frame Delimiter (SFD) - This consists of one byte. It contains an alternating pattern of ones and zeros but ending in two ones.

Ethernet at Data link Layer:

- Destination Address (DA) - This field contains the address of receiving station. The leftmost bit indicates whether the destination is an individual address(0 bit) or a group address(1 bit).
- Source Address (SA) - The source address consists of six bytes, and it is used to identify the sending station.
- Length / Type - This field is two bytes in length. It gives MAC information and indicates the number of client data types that are contained in the data field of the frame.

Ethernet at Data link Layer:

Payload

- Data - This contains the payload data and its size ranges up to 1500 bytes. If the length of the field is less than 46 bytes, then the padding data is added to fill the data block

3. Trailer

- Frame Check Sequence (FCS) - This is four bytes long. It contains a 32 bit Cyclic Redundancy Check (CRC) that is generated over the Destination Address, Source Address, Length / Type and Data fields.

Ethernet Standard & Features

Content:

1. IEEE Standards
2. Features of Ethernet
 - o Port mirroring
 - o Power over Ethernet

IEEE Standard:

IEEE 802.3 is a working group which define the physical layer and data link layer (MAC) of wired Ethernet.

Ethernet is defined under a number of IEEE standards and each standard define a different type of Ethernet.

Each of the Ethernet IEEE 802.3 standards can be uniquely identified.

These IEEE standards are being updated as a new Ethernet cable is evolved.

Some of them are also defined below.

IEEE Standard:

Standards	Year	Description
802.3a	1985	10Base-2 (thin Ethernet)
802.3c	1986	10Mb/s repeater specifications (clause 9)
802.3d	1987	FOIRL (fiber link)
802.3i	1990	10Base-T (twisted pair)
802.3j	1993	10Base-F (fiber optic)
802.3u	1995	100Base-T (Fast Ethernet and auto-negotiation)
802.3z	1998	1000Base-X (Gigabit Ethernet)
802.3ab	1999	1000Base-T (Gigabit Ethernet over twisted pair)
802.3ac	1998	VLAN tag (frame size extension to 1522 bytes)
802.3ae	2002	10-Gigabit Ethernet
802.3at	2005	Power over Ethernet Plus

Features of Ethernet:

Power over Ethernet (PoE):

Power over Ethernet (PoE) is a networking feature which is defined by the IEEE 802.3af and 802.3at standards.

It is a solution in which electric power is pass along with data on twisted pair Ethernet cabling.

This allows a single cable to provide both data connection and electric power to device such as wireless access points, IP cameras and VoIP phones.

Thus there is no need of an extra AC power cord to be attached to device.

Features of Ethernet:

Power over Ethernet (PoE):

This minimizes the amount of cable required and reduce the difficulties and cost of installing extra outlets

The IEEE standards for PoE require category 5 cable for high power levels and allow using category 3 cable for low power level.

For example, a digital security camera which requires two connections to be made when it is installed. One for network connection, in order to be able to communicate with video recording and display equipment and other for power supply. So here PoE is used.

Features of Ethernet:

Port Mirroring:

Port mirroring is used on a network switch to send a copy of network packets seen on one switch port to another switch port in network.

This is used for monitoring network traffic.

Port mirroring on a Cisco Systems switch is known as Switched Port Analyzer (SPAN) or Remote Switched Port Analyzer (RSPAN).

Features of Ethernet:

Port Mirroring:

Other vendors have different names for it, such as Roving Analysis Port (RAP) on 3Com switches.

Network engineers or administrators use port mirroring to analyze and debug data or diagnose errors on a network.

Wired Transmission Media

Part 1

Content:

1. Coaxial cables
2. BNC connector
3. Twisted Pair Cables
 - o Shielded Twisted Pair Cable
 - o Unshielded Twisted Pair Cable
4. RJ-45 connector

Wired Media And Connectors:

1. Co axial Cables:

Coaxial cable or coax is a type of cable in which inner conductor is surrounded by plastic jacket with a braided shield over it.

It include one physical channel that carries the signal and it is surrounded by another concentric physical channel, both running along the same axis. That's why it known as "coaxial".

Copper shield is covered by using PVC (Polyvinylchloride) or FEP (Fluoroethylene Propylene) plastic.

Wired Media And Connectors:

1. Co axial Cables:

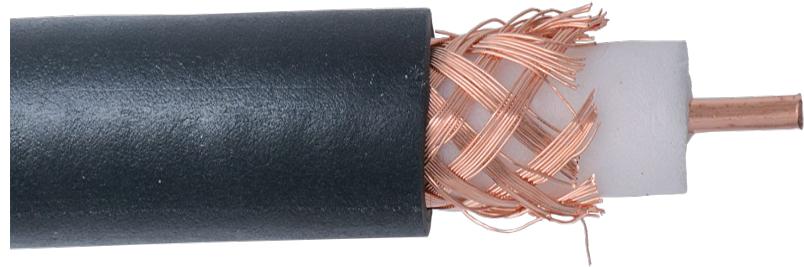
For a High Frequency electrical signals it provide an interference-free transmission path.

RG6 and RG59 are the coaxial cable grades used for home video devices such as TV.

RG59 used for short distance communication and RG6 is expensive cable used for long distance transmission.

Example: Thinnet,Thicknet,Television Cable

Coaxial Cables



Wired Media And Connectors:

BNC connector:

BNC stands for Bayonet Neil-Concelman or British Naval Connector.

It is a miniature quick connect/disconnect radio frequency connector with a positive locking mechanism.

Mating is achieved with a quarter turns of the coupling nut.

BNC are lightweight and reliable connectors.

Wired Media And Connectors:

BNC connector:

They are mostly made in 50 or 75 ohm version.

BNC connector are used with coaxial cable in radio, television and other radio-frequency electronic equipment, test instruments, and video signals.

BNC connector



Wired Media and Connectors:

2. Twisted Pair cable:

Twisted pair cables consist of two conductors, each with its own plastic insulation and they are twisted together.

One wire is used to send signals to the destination and second wire is used as ground reference.

They are twisted together to reduce crosstalk and EMI (electromagnetic interference) from external source.

At the receiver side there will be no signal difference because unwanted signals are cancelled out.

Wired Media and Connectors:

2. Twisted Pair cable:

It is used to transmit analog and digital signals and frequency signals ranges from 100Hz to 5MHz.

Types of Twisted Pair cables are UTP and STP.

Wired Media And Connectors:

Unshielded twisted pair:

The unshielded twisted pair cables don't have an outer protection.

These cables have covering jacket made of PVC or FEP plastics.

This cable is used in computer network as ethernet cables.

Shielded Twisted pair:

The shielded twisted pair cables has a metal foil which cover the each pair of insulating conductor and have a outer layer cover made of PVC or FEP plastics.

This cable are used in factories with large electronics equipments.

Wired Media And Connectors:

Unshielded twisted pair:

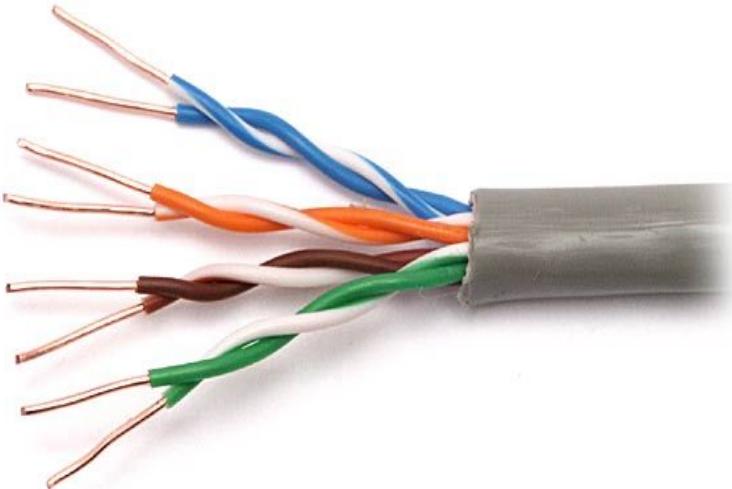
These Cables are less immune to external noise or interference.

UTP cables are also known as CAT cable (Category Rating)

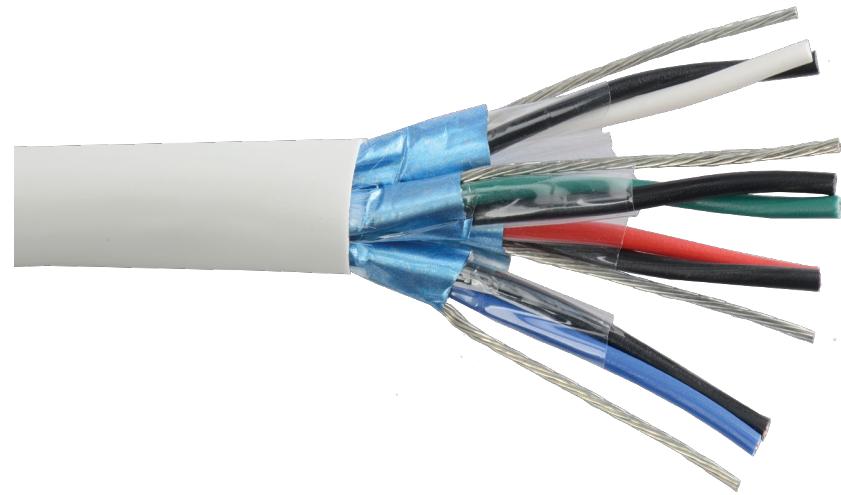
Shielded Twisted pair:

These cables are more immune to external noise and interference due to presence of metallic shield.

Wired Media And Connectors:



Unshielded Twisted Pair Cable



Shielded Twisted Pair Cable

Wired Media And Connectors:

Variety of CAT cables are:

CAT rating	Frequency	Bandwidth	Used for
CAT 1	<1 MHz	-	Voice only
CAT 2	4 MHz	4 mbps	Data
CAT 3	16 MHz	16 mbps	Data
CAT 4	20 MHz	20 mbps	Data
CAT 5	100 MHz	100 mbps	Data
CAT 5e	100 MHz	1 gbps	Data
CAT 6	250 MHz	10 gbps	Data
CAT 6a	500 MHz	10 gbps	Data

Wired Media And Connectors:

RJ 45 Connector:

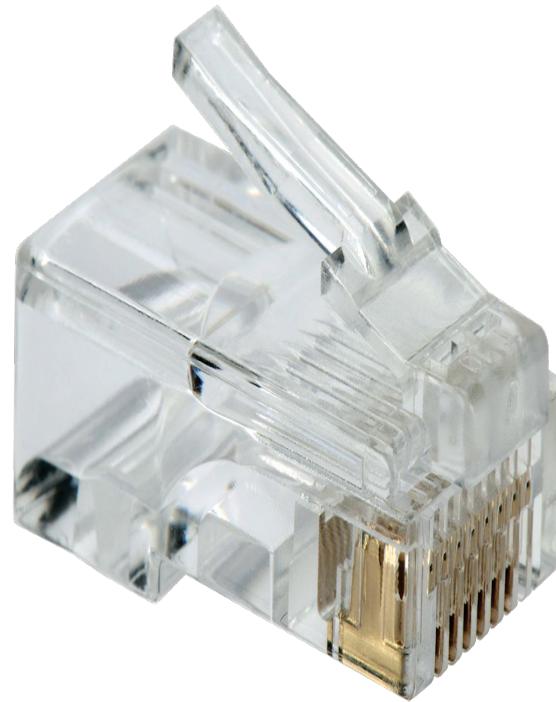
A Registered jack (RJ-45) is a standard type of physical network interface with 8 pin/8 position plug. '45' refers to the number of interface standard.

It is used to connect computer onto Ethernet based LAN network

Two wiring schemes are used T568A and T568B to terminate the twisted-pair cable onto the connector interface.

It is used with CAT5 and CAT6 cables.

RJ-45 Connector



Wired Transmission Media

Part 2

Content:

1. Optical Fiber Cables
 - o Single optical fiber
 - o Multimode optical fiber
 - o Graded Index optical fiber
 - o Step Index optical fiber
2. Optical connector
3. Serial Cables
 - o RS -232
 - o USB cable

Wired Media And Connectors:

Optical Fiber cables :

Optical fiber is a cylindrical non-conducting waveguide that transmit the light along its axis.

It consist of core and cladding layer and refractive index of core is greater than cladding.

It transfer the light signal to a longer distance.

It follow the principle of total internal reflection (TIR) to transmit the light through glass medium.

There are 2 types of optical fiber cable.

Wired Media And Connectors:

Single mode Optical fiber:

This fiber has a small diameter of core and only one mode of light will travel through it.

It is used in long distance communication with high bandwidth links.

The diameter of core is 9 microns and cladding is of 125 microns.

Launching of light in this fiber is difficult.

Multimode optical fiber:

This fiber can support multiple light rays to travel through it.

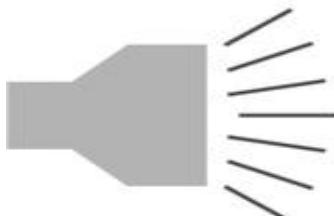
The diameter of core/ cladding is 50/125 and 62.5/125 microns.

This fiber contain large side of core as compared to single mode optical fiber.

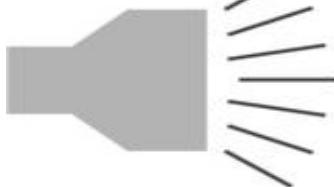
Launching of light in this fiber is easy. It is further of two types.

Wired Media And Connectors:

Light source



Light source



Multimode fiber



Single Mode Optical Fiber and Multimode Optical Fiber

Wired Media And Connectors:

Step Index Fiber:

In this fiber, the refractive index of the core is uniform and at the interface of core and cladding the refractive index change abruptly.

The size of core is large so it can support multiple modes. It is used in short distance communication.

The diameter of core/cladding is 200/380 microns

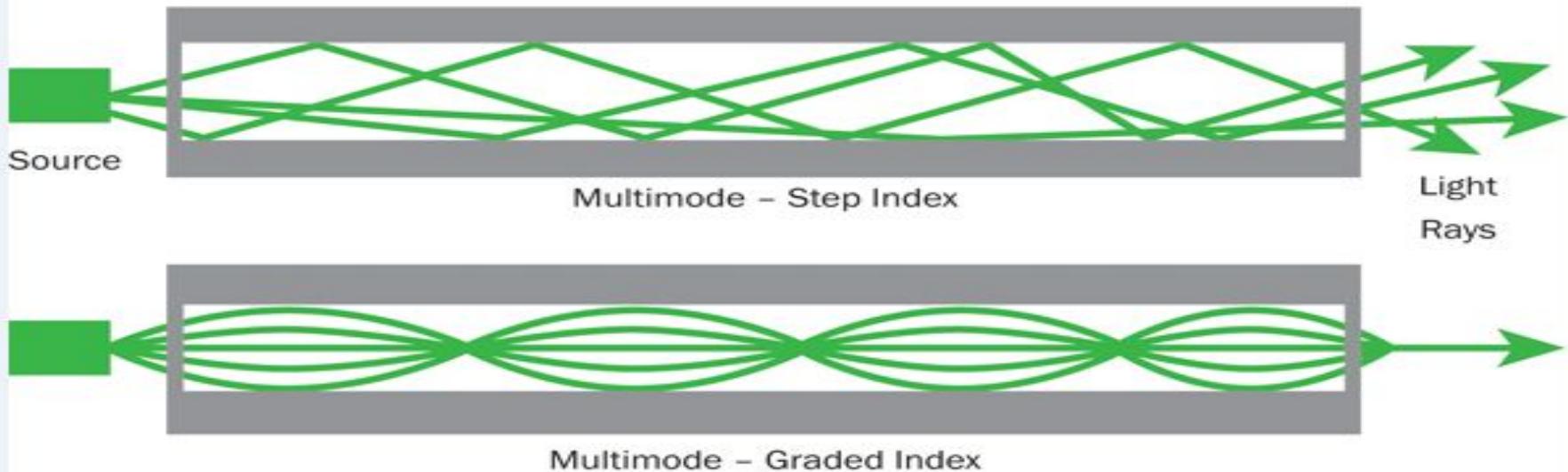
Graded Index optical fiber:

In this fiber, the refractive index of core is non-uniform i.e. the refractive index decreases gradually from the axis of the fibre to its surface.

Light rays propagate in the form of skew rays or helical rays. This fiber reduce the modal dispersion .

It is also used for long distance transmission of signals.

Wired Media And Connectors:



Step Index Multimode Fiber and Graded Index Multimode fiber

Wired Media And Connectors:

SC connector:

SC stands for subscriber Connector or standard connector.

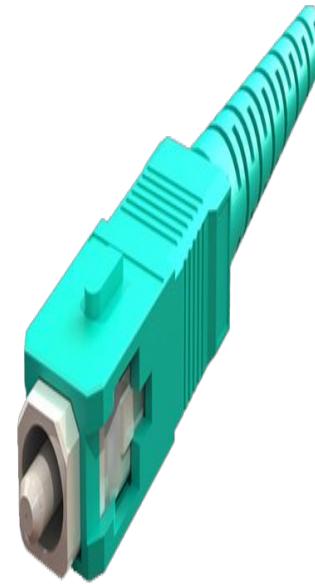
It has a 2.5mm Zirconia Ceramic ferrule and a push-pull latching mechanism which is similar to common audio and video cables. It is used for a fast and reliable connection in telecommunications networks.

Two fiber cables and two SC connectors (Dual SC) are used for bidirectional transmission.

The SC connector are available in standard colours as blue (singlemode), green (singlemode) and beige (multimode).

Example: CATV - Cable television, Fibre-To-The-Home , LAN, MAN and WAN network

SC Connector



Wired Media And Connectors:

ST connector:

ST stands for Straight tip connector. This connector has a bayonet mount and a long cylindrical 2.5 mm ceramic or polymer ferrule that hold the fiber.

Most ferrules are ceramic, but some are metal or plastic.

It is most popular connector for multimode networks

Usage of this connector decline from recent years because it cannot be used in single mode fiber and FTTH applications as fiber is terminated with an angled polish in this connector.

ST Connector



Wired Media And Connectors:

LC connector:

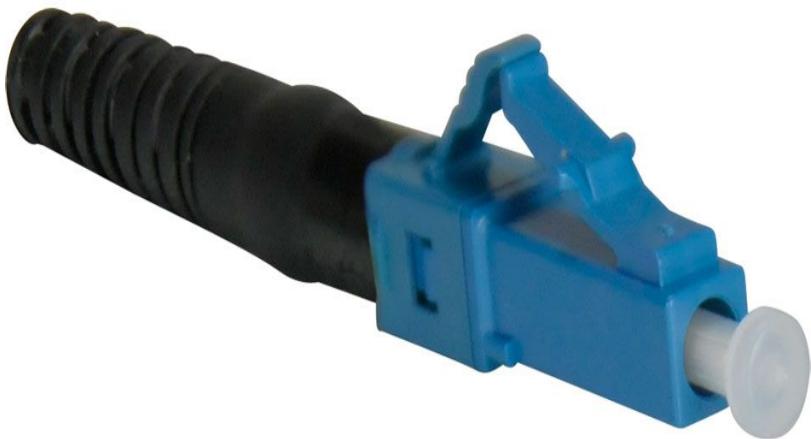
LC stands for Lucent Connector and it is a miniaturized version of the fiber-optic SC connector.

It look is similar as SC, but there is size difference LC connector has a size 1.25mm ferrule whereas SC connector is of 2.5mm.

It give the replacement to the SC connector in market but LC is more costly than SC.

It is used in networking and FTTH applications

LC Connector



Wired Media And Connectors:

MT-RJ Connector:

MT-RJ stands for Mechanical Transfer Registered Jack.

MT-RJ is a fiber-optic Cable Connector in which two fibers are plug and combine together with locating pins on the plug.

The MT-RJ looks similar to a RJ45 connector.

It is used for networking applications such as Ethernet network.

It's size is small as compared to SC connector.

The MT-RJ Connector is low cost and small size.

MT-RJ Connector



Wired Media And Connectors:

Serial Cables:

'Serial' means the bits are send one by one through cables or fiber and it is interpreted by the network card at the other end.

It use serial communication protocol to transfer the data between two device.

Type of serial cables are RS 232 and USB cables.

Wired Media And Connectors:

RS 232:

RS 232 is a standard for serial communication of data in the network.

This cable connects the DTE (Data Terminal Equipment) such as computer and DCE (Data communication equipment) such as modem.

RS 232 standard defines the electrical characteristics , timing of signals, the meaning of signals, and the physical size and pinout of connectors

It has low transmission speed, large voltage swing and large standard connectors.

RS-232 Cable



Wired Media And Connectors:

USB Cables:

Universal Serial Bus is an industry standard that defines the communication protocols

It is used for connection, communication, and power supply between computers and electronic devices.

RS 232 cables are replaced by USB in many devices

USB cables are available in many version according to their use.

These cables has fast transmission speed and use low power supply.

USB Cable



Transmission Media

Content:

1. Properties of Cables:
 - o Noise Immunity
 - o Speed of transmission
 - o Frequency
 - o Distance of transmission
2. Wiring Standard
3. Cabling Connection:
 - o Straight through cable
 - o Crossover Cable
 - o Rollover Cable
 - o Hardware loopback

Properties of Cables:

1. Noise Immunity:

Noise is a random fluctuation in an electrical signal.

Noise generated in cables affect the information or data signals.

Coaxial cables are adversely affected by the noise created by external sources.

Fiber cables are more immune to noise effects.

So, cable with more immunity to noise should be design to reduce the signal degradations.

Properties of Cables:

2. Speed of Transmission:

Each cables have there own speed of transmitting signals like coaxial cables transmit data at lower rate whereas fiber cable transmit signals at faster rates.

So according to the demand of network, desired cables must be installed.

Properties of Cables:

3. Frequency:

Each cable has a specified maximum frequency that define how much transmission bandwidth it can handle.

CAT 5 cables are tested at 100 MHz maximum frequency and transmit signal at 1gbps in short distances.

CAT6 is tested at 250 MHz frequency and it handle data at 1gbps in long distance communication.

So according to the demand of bandwidth in network desired cables should installed.

Properties of Cables:

3. Distance of transmission:

Each cable has different speed of transmission it means these cables can transmit signals in some define range or distance.

Some cables are installed for long distance communication and some are used for short distance communication because as the signal travel it start degrading due to loses.

Wiring Standard:

1. TIA/EIA 568A and TIA/EIA 568B:

The Telecommunication Industry Association/Electronics Industries Alliance (TIA/EIA) is a set of telecommunication standards which defines the industry standard for correct crimping of 4-pair UTP cable.

It include two wiring standards:

- TIA/EIA 568A
- TIA/EIA 568B

Wiring Standard:

TIA/EIA 568A

1		White and Green
2		Green
3		White and Orange
4		Blue
5		White and Blue
6		Orange
7		White and Brown
8		Brown

TIA/EIA 568B

1		White and Orange
2		Orange
3		White and Green
4		Blue
5		White and Blue
6		Green
7		White and Brown
8		Brown

TIA/EIA 568A and TIA/EIA 568B

Cable Connections:

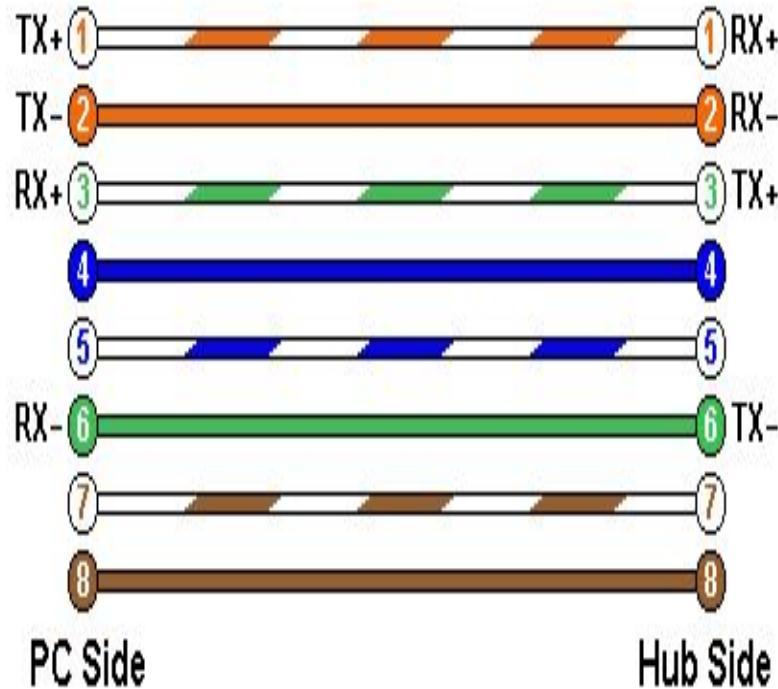
1. Straight through cables:

It is used to do the straight connection between the devices such as connection between host and clients

These cables have the pin assignments on each end of the cable.

Like Pin 1 connector A connect to Pin 1 on connector B, Pin 2 to Pin 2 and so on.

Straight Through Cable



Cable Connections:

2. Crossover cables:

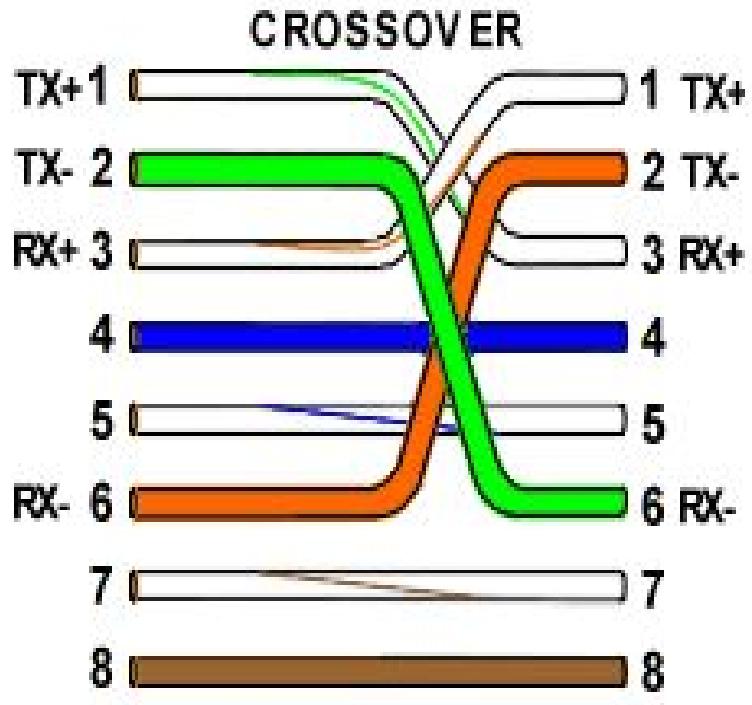
Crossover cables are same as Straight-Through cables but with little difference that TX and RX wires are crossed it means they are at opposite positions on both end of the cable.

In this type of connection , 586B standard is used

Example Pin 1 on connector A goes to Pin 2 on connector B. Pin 2 on connector A goes to Pin 1 on connector B etc.

This is used to connect two hosts directly such as connecting a computer directly to another computer, connecting a switch directly to another switch, or connecting a router to a router.

Crossover cable



Cable Connections:

3. Rollover Cables:

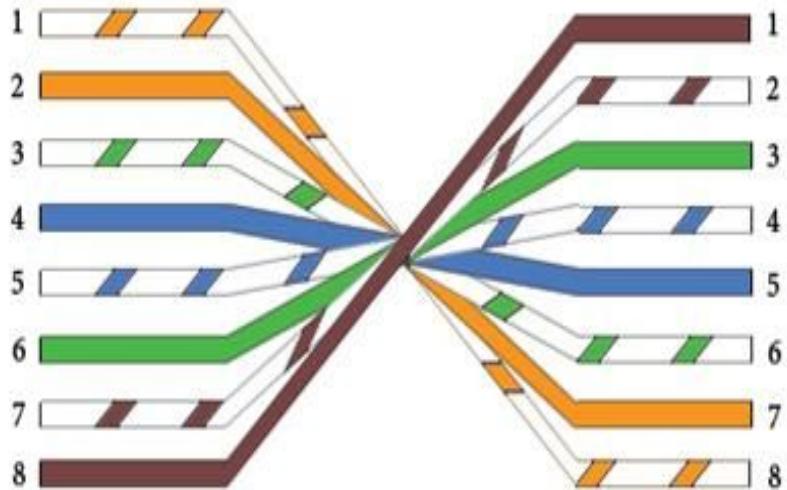
Rollover cables have opposite pin assignments on each end of the cable .

Like Pin 1 of connector A will connected to Pin 8 of connector B.Pin 2 of connector A will be connected to Pin 7 of connector B and so on.

They are not used to carry data but used to create an connection between the device.

Rollover Cable

Rollover Wiring Guide
568-B



Cable Connections:

4. Hardware Loopback:

Hardware loopback connection are used to check the capability of a device that it can transmit and receive the signal efficiently in the network

This is a process of routing a signals or data back to their source without any modification.

This is used to test the transmission or transportation infrastructure of a network devices.

Wireless Transmission Media

Content:

1. Wireless Media
 - 1.1. Radiowaves
 - 1.2. Microwaves
 - 1.3. Infrared waves

Wireless Media:

Radiowaves:

Radio waves are a part of electromagnetic radiation

It wavelengths in the electromagnetic spectrum is longer than infrared light.

It frequency ranges from 300 GHz to 3 kHz,

It is used for mobile radio communication, broadcasting, navigation systems, satellites communication, computer networks and various other applications.

These waves are generated by radio transmitters and always received by radio receivers.

Wireless Media

Omnidirectional antennas:

Omnidirectional antenna are type of antenna which radiate radio waves in all directions.

It is used in RF wireless devices such as cellular mobile phone and wireless routers.

This antenna radiate equally in all directions.

Omnidirectional Antenna



Wireless Media

Microwaves:

Microwaves are the type of electromagnetic radiation

It wavelengths ranges from 1m to one mm.

It frequency ranges between 300 MHz and 300 GHz.

It is used by mobile phone communication, satellite communication, fixed traffic speed cameras and for radar, which is used by aircraft, ships and weather forecasters.

Wireless Media

Unidirectional Antenna:

Unidirectional propagation antenna is an antenna that's propagation pattern is in one direction.

This antennas are good for communicating with someone when you know their location.

Example: Radar antennas, Yagi-Uda antennas, Satellite dish



Unidirectional Antenna



Wireless Media:

Infrared waves:

Infrared (IR) is an invisible radiant energy signal present in electromagnetic radiation its frequency ranges from 430 THz to 300 GHz

It is used in industrial, scientific, and medical applications.

It is widely used in military applications like target acquisition, surveillance, night vision, and tracking.

Cable Installation

Content:

1. Structured cabling
2. Essential Components of Structured Cabling
 - Telecommunication Room
 - Horizontal Cabling
 - Work Area
3. Steps to install the Structured Cabling

Structured Cabling:

A set of standards to form a functioning, dependable and real world network are known as Structured Cabling

These standards are defined by TIA/EIA.

Standards Cabling is used in computer network, Telephone network and Video conferencing setup.

The main motive of structured cabling is to create a safe, reliable cabling infrastructure for all the device in the network.

The first topology used to connect devices together is Star topology.

Structured Cabling Components:

The three essential components used to form structured cabling network are:

1. Telecommunication Room
2. Horizontal Cabling
3. Work Area

Structured Cabling Component:

1. Telecommunication Room: It is a central location from where cables runs to every PC in work area.
2. Horizontal Cabling: All cables run horizontally from the telecommunication room to the PC,s. This type of cabling is called horizontal cabling.
3. Work Area: It represent a office or cubicle that contain a group of PC or a telephones.

These three components are arranged by following standards defined by TIA/EIA.

Structured Cabling Component:



Structured Cabling Component:

1. Horizontal cabling:

A horizontal cabling is the type of cabling in which the wires run horizontally from a work area to a telecommunication room.

The cable used for structured cabling are CAT 5e or UTP cables.

A single piece of cable that runs from a work area to a telecommunication room is called a run.

The two type of UTP cable used in horizontal cabling are:

Structured Cabling Component:

Solid Core Cable

It use a single solid wire.

Better conductor.

It is stiff and break if handle roughly.

TIA/EIA specified to use this cable for structured cabling.

Stranded Core Cable

Each wire use a bundle of tiny strands.

It is not a good conductor.

It cannot break if handle roughly.

This cable is used as patch cable in structured cabling

Structured Cabling Component:



Solid Core and Stranded Core cables

Structured Cabling Component:

2. Telecommunication Room:

Telecommunication room is a central location where wiring from all devices get connected to switch.

It is the heart of the basic star topology.

Actual name for this device is IDF (Intermediate Distribution Frame)

IDF is a place where all the horizontal cables from all work area come together.

Structured Cabling Component:

2. Telecommunication Room:

Equipment racks are the central component of every telecommunication room.

It provide a safe and a stable platform for all the hardware devices in the network.

All Equipment racks are 19 inch wide but may varies in height.

Height measurement unit of equipment rack is “UNIT” (U).

A 1U is equal to 1.75 inch.

Structured Cabling Component:



Equipment Racks

Structured Cabling Component:

2. Telecommunication Room:

Patch Panels and Cables:

Patch panel is a box with a row of female port in the front and permanent connection in the back, to which we connect the horizontal cable.

Most commonly used connector with patch panel is 110 block or 110 punchdown block.

UTP cable is connected to it by using punchdown tool.

110 block introduce less crosstalk.

Structured Cabling Component:

2. Telecommunication Room:

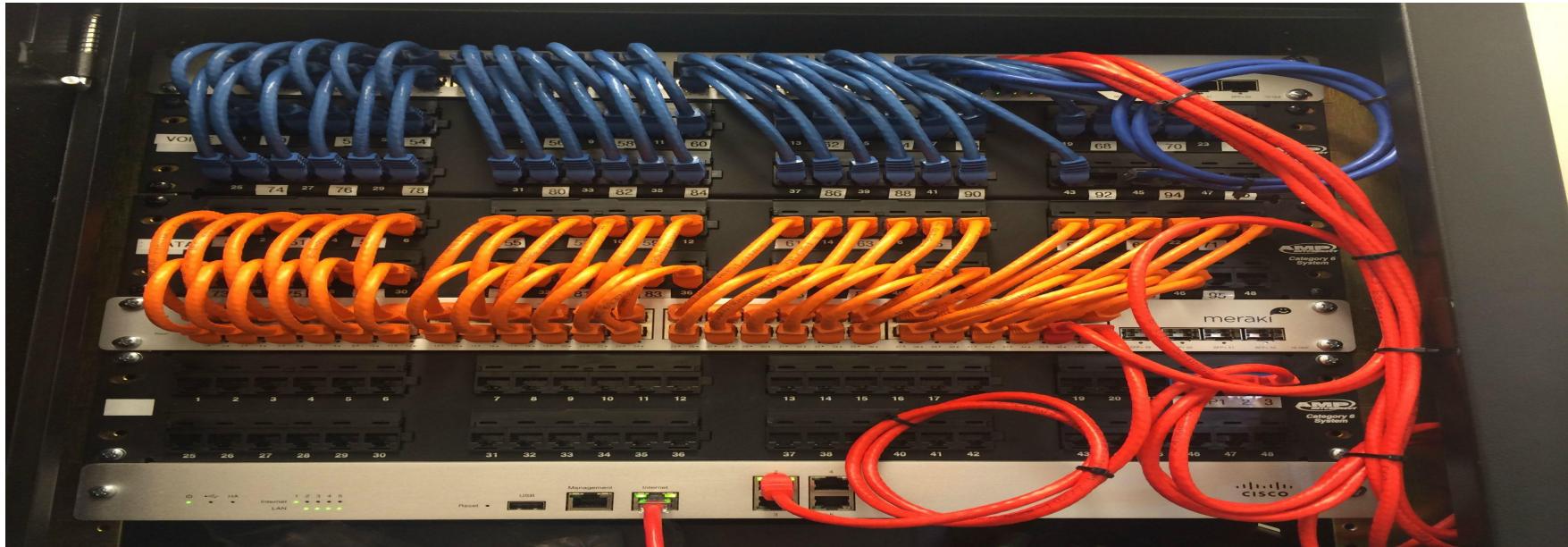
Patch Panels and Cables:

The ANSI/TIA 606 B standard define proper labeling and documentation of cabling, patch panels and wall outlets.

Patch panels are available in wide variety of configuration for STP, UTP and Fiber optics.

Stranded core cables are used in patch panels for cabling.

Structured Cabling Component:



Patch Panel

Structured Cabling Component:

3. Work Area:

Work-area connect the end-user equipment like computers, telephones and other network element to outlets of the horizontal cabling system.

It represent a office or cubicle that contain a group of PC or a telephones

Work area components are extend from the telecommunication room via horizontal cabling to the Work area.

Structured Cabling:

Steps to install the Structured Cabling are:

To install the structured cabling professional installer begin it by accessing the whole site and make plans for installation.

1. First step to install structured cabling is to get the floor plan. Floor plan act as a key to proper planning. A good floor plan shows us a closet location that serves as telecommunication room and location of work area.
2. After floor plan, the next step is to map the horizontal cables and workplace i.e. mapping the runs.

Structured Cabling:

Steps to install the Structured Cabling are:

3. Next step is to find the appropriate location for telecommunication room.
4. Then determine the cables which is used for horizontal cabling and for patch panels.
5. Lay down the cabling and make the connection between the work area and telecommunication room.
6. After completing the cable lay down process, then test the cable run and cable connection.

Network Address

Content:

1. Network Address
2. Types of network address
 - Physical address
 - Logical address
3. Different Classes of Logical address
4. IP address Representation

Network Address:

A network address is the unique code or number which is given to each node or device in the network.

Each device has its own unique address and it make easy for the users to communicate within a network

Examples of network addresses are:

- A telephone no in the public switched telephone (PSTN) network
- An IP address in the Internet
- MAC address in an Ethernet network etc

Types of Network Address:

Physical address:

- The MAC (Media Access Control) address is a physical address.
- MAC address is 48 bits in length.
- This unique code is given by manufacturer which is encoded in NIC card.
- It is associated with Data Link Layer of OSI model.

Logical Address:

- The IP (Internet Protocol) address is a Logical Address.
- IP address is 32 bits in length.
- IP address are assigned by ISP (Internet service provider) to the device.
- It is associated with network layer of OSI model.

Types of Network Address:

Physical address:

- It is also known as Hardware address.
- The format of address is Hexadecimal.
- Example of MAC address 00-23-4E-47-21-01
- MAC address are used by many different Layer 2 devices some are Ethernet, Token Ring and Fibre Channel.

Logical Address:

- It is also known as virtual address.
- Format of address is Decimal ranges from 0 to 255.
- Example of IP address 209.161.122.70.
- The IP address is used to identify the different computers and websites on the internet or intranet.

Different Classes of Logical address:

Class	Address	No. of Network	No. of Host
Class A	0-126	126	16777214
Class B	128-191	16384	65534
Class C	192-223	2097152	254
Class D	224-239	Multicasting addresses	
Class E	240-255	Reserved for future use	

Different Classes of Logical address:

Class	1st octet higher order no.	Network/Host Id
Class A	0	N.H.H.H
Class B	10	N.N.H.H
Class C	110	N.N.N.H
Class D	1110	-
Class E	1111	-

Different Classes of Logical address:

Ranges 127.x.x.x are reserved for the loopback testing , for example, 127.0.0.1 is the loopback address.

All IP addresses uniquely identifies a device in the network.

Some IP Addresses cannot used in the network because they are used for some special purposes.

All zero's in Host ID represent the Network Address.

All One's in Host ID represent the Broadcast address.

IP address Representation:

Every IP address is broken down into four sets of octets and translated into binary to represent the actual IP address.

For an example, IP address :192.168.5.2

Binary Representation	128	64	32	16	8	4	2	1
192	1	1	0	0	0	0	0	0
168	1	0	1	0	1	0	0	0
5	0	0	0	0	0	1	0	1
2	0	0	0	0	0	0	1	0

IP address Representation:

Representation of IP address:

Conversion of decimal to binary

For an example, IP address 150.70.10.21

IP Address	150	70	10	21
Binary Value	10011000	01000110	00001010	00010101
Numerical value	$128+16+8=150$	$64+4+2=70$	$8+2=10$	$16+4+1=21$

Automatically Assigned IP address:

There are IP addresses that are automatically assigned (dynamic allocation) when you set up a home network.

192.168.1.0 0 is automatically assigned network address.

192.168.1.255 255 is commonly used as Broadcast address.

192.168.1.1 1 is commonly used as Gateway Address.

Types of Logical address

Content:

1. Type of Logical Address
 - o Public IP address
 - o Private IP address
2. Subnet Mask

Type Of Logical Address:

Logical Network Is divided into two parts:

1. Private IP address
2. Public IP address

Type Of Logical Address:

Public IP Address:

The public IP address is assigned to the computer by the Internet Service Provider when it is connected to the Internet Service.

A public IP address can be assigned as static or dynamic.

A static public IP address remain unchanged and is used for hosting web pages or services on the Internet.

A dynamic public IP address is chosen from a pool of available addresses and it changes each time as a device connects to the Internet.

Type Of Logical Address:

Private IP Address:

An Private IP address is a IP number which falls within one of the IP address ranges reserved for private networks such as a Local Area Network (LAN).

The Internet Assigned Numbers Authority (IANA) has reserved the following 3 blocks of the IP address as private networks :

Class A	10.0.0.0	-	10.255.255.255
Class B	172.16.0.0	-	172.31.255.255
Class C	192.168.0.0	-	192.168.255.255

Type Of Logical Address:

Private IP Address:

For example, if a network A consists of 20 computers, each of them can be given an IP starting from 192.168.1.1 to 192.168.1.20.

Thus the assigned IP address must range as mentioned above for efficient communication between computers of Private Network.

Devices with private IP addresses cannot connect directly to the Internet.

Computers outside the local network cannot connect directly to a device having private IP address or device within Private network..

Type Of Logical Address:

Private IP Address:

If the private network is connected to the Internet then each computer will have a private IP address as well as a public IP address.

Public IP Address is assigned by ISP (Internet Service Provider) to connect a device to the internet.

Private IP is used for communication within the network and the public IP is used for communication over the Internet

Subnet Mask:

A Subnet mask is a 32-bit number that divides the IP address into network address and host address.

It is used to determine to what subnet an IP address belongs to.

Subnet Mask is made by setting network bits to all "1"s and host bits to all "0"s.

Subnet Mask Of different classes are:

Class A 255.0.0.0/8

Class B 255.255.0.0/16

Class C 255.255.255.0/24

Network Layer Protocol

Content:

1. Network Layer Protocol
 - o ARP Mapping Logical to Physical address
 - o RARP Mapping Physical to logical address

Network Layer Protocol:

There are two type of network Protocol:

1. ARP Address Resolution Protocol
2. RARP Reverse Address Resolution Protocol

These Protocols are used for mapping physical address into logical address or vice-versa.

Network Layer Protocol:

1. Address Resolution Protocol (ARP):

The address resolution protocol (ARP) is a protocol used in network to map (Logical Address) IP network addresses to the (Physical Address) hardware addresses used by a data link protocol.

In IPv4 ,an IP address is 32 bits long whereas in an Ethernet LAN, however, addresses of an attached device is 48 bits long known as MAC address.

A table called the ARP cache, is used to maintain a relation between each MAC address and its corresponding IP address.

Network Layer Protocol:

1. Address Resolution Protocol (ARP):

ARP provides the protocol rules for making this relation and providing address conversion in both directions.

For example: There are 2 computers in network wants to communicate. Computer A wants to send packet to computer B but Computer A only knows the IP address of Computer B but don't know its MAC address.

So, to get MAC address. First of all Computer A checks the ARP cache table to find corresponding MAC address to IP address of Computer B.

Network Layer Protocol:

1. Address Resolution Protocol (ARP):

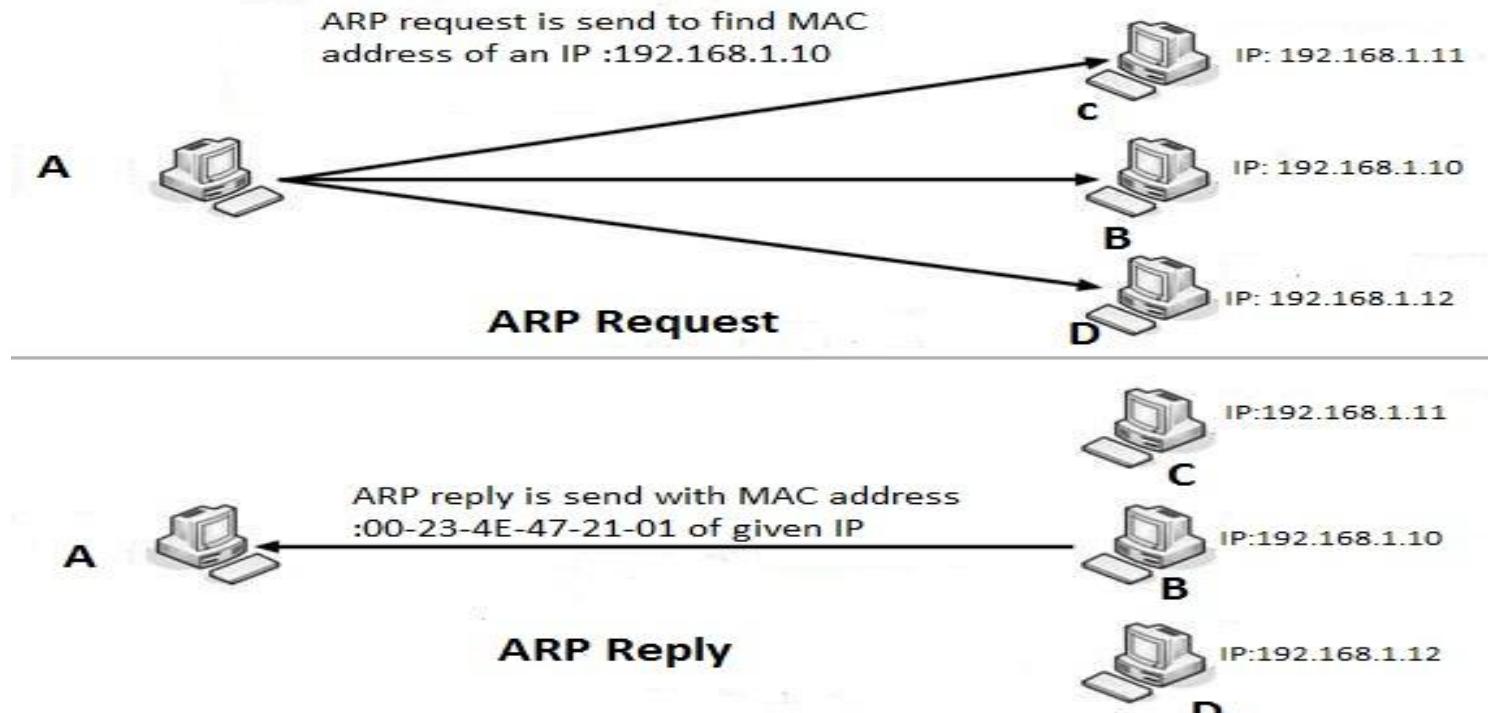
if not found then, Computer A broadcast a ARP request Message in the network. Each Computer in Network check the ARP request and match the given IP address.

After matching IP address Computer B sends a unicast message to Computer A with its IP address and MAC address.

This MAC address get stored in ARP cache for future use.

Now Computer A can send packets to Computer B.

Network Layer Protocol:



Address Resolution Protocol (ARP)

Network Layer Protocol:

2. Reverse Address Resolution Protocol (RARP):

The Reverse Address Resolution Protocol (RARP) is a computer networking protocol used by a client computer to request its Internet Protocol(IPv4) address from a computer network, using MAC address or hardware address.

It is a protocol by which a device in a LAN can request to have its IP address from a gateway server's ARP cache.

A network administrator creates a table in a LAN gateway router that maps the physical machine MAC addresses to corresponding IP addresses.

Network Layer Protocol:

2. Reverse Address Resolution Protocol (RARP):

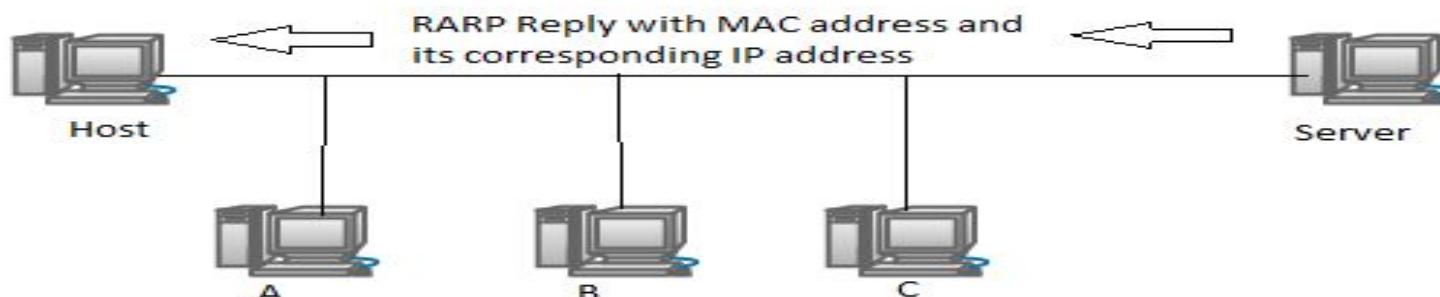
For example: When a new machine is set up in the network, it sends RARP requests on the router in the network to be sent its IP address which corresponds to its MAC address.

Assuming that an entry has been set up in the router table, the RARP server returns the IP address to the machine and stores it for future use.

Network Layer Protocol:



RARP Request



RARP Reply

Reverse Address Resolution Protocol (RARP)

Calculation of Network Addresses

Content:

1. Calculation of
 - Subnet mask
 - Broadcast ID
 - Network ID
 - Other IP's

Calculation:

How to calculate the subnet mask, broadcast IP address, network IP address and other related IP address of given IP address.

1. **192.168.1.5**

Here 192 in first octet represent the class of an IP address. Thus this IP address belongs to Class C.

Then calculate the subnet mask, as this IP belongs to class C so the subnet mask of class C be : 255.255.255.0 or /24

Thus,

192.168.1

5

Network bits

Host bits

Calculation:

We know Network IP address contain all zeros in host bits. So, to find n/w IP make all host bits equal to 0.

$11000000.10101000.00000001.00000000 = 192.168.1.0$

Thus Network IP address is 192.168.1.0

We know Broadcast IP address contain all one's in host bits. So, to find Broadcast IP make all host bits equal to 1.

$11000000.10101000.00000001.11111111 = 192.168.1.255$

Thus Broadcast IP address is 192.168.1.255

Calculation:

So IP address ranges from 192.168.1.0 to 192.168.1.255

192.168.1.0 - N/w address

192.168.1.1

.....

.....

192.168.1.254

192.168.1.255 - Broadcast address

Total IP address = 256

1 Network IP and 1 Broadcast IP both are invalid IP addresses.

So, there are total 254 IP addresses which are valid and can be used in network.

Calculation:

We can also calculate as

No. of Host bits =8

$2^8 = 256$ -total IP addresses

$2^{8-2} = 254$ - valid IP address

Calculation:

Calculate the subnet mask, broadcast IP address, network IP address and other related IP address of given IP address:

2. **170.168.60.1**

Here 170 in first octet represent the class of an IP address. Thus this IP address belongs to Class B.

Then calculate the subnet mask, as this IP belongs to class B so the subnet mask of class B : 255.255.0.0 or /16

Thus,

170.168. 60.1

Network bits

Host bits

Calculation:

We know Network IP address contain all zeros in host bits. So, to find n/w IP make all host bits equal to 0.

$10101010.10101000.00000000.00000000 = 170.168.0.0$

Thus Network IP address is 170.168.0.0

We know Broadcast IP address contain all one's in host bits. So, to find Broadcast IP make all host bits equal to 1.

$10101010.10101000.11111111.11111111 = 170.168.255.255$

Thus Broadcast IP address is 170.168.255.255

Calculation:

So IP address ranges from 170.168.0.0 to 170.168.255.255

170.168.0.0 - N/w address

.....

170.168.0.255

170.168.1.0

.....

170.168.1.255

170.168.2.0

.....

170.168.2.255

.....

170.168.255.254

170.168.255.255 - Broadcast address

Calculation:

Total IP address = 65536 (256×256)

1 Network IP and 1 Broadcast IP both are invalid IP addresses.

So, there are total 65534 IP addresses which are valid and can be used in network.

Or We can also calculate as

No. of Host bits = 16

$2^{16} = 65536$ - total IP addresses

$2^{16} - 2 = 65534$ - valid IP address

Subnetting

Content:

1. Subnetting
2. CIDR (Classless Inter Domain Routing)
3. Variable length Subnet Mask (VLSM)
4. Who manages IP addresses?
5. Why we need subnetting?
6. How to assign IP address to device?

Subnetting:

Subnetting is a process of dividing large network into the smaller network based on layer 3 (Network Layer) IP address.

A subnet is a logical subdivision of an IP network.

Subnetting provides a method of allocating a part of the host address space to network addresses, which generate more networks.

Subnetting allows to add sub-networks without the need to acquire a new IP addresses from ISP.

Subnetting:

Benefits of Subnetting:

It reduces the network traffic by reducing the size of broadcasts domain.

It enables users to access a work network from their homes.

Subnetting helps in reducing the network complexity.

It increase the security options in the network

By using subnetting, network addresses can be decentralized it means the administrator of the network can monitor the subnet.

Classless Inter Domain Routing (CIDR):

Classless Inter-Domain Routing is a method for allocating IP addresses and routing in the Network.

CIDR is introduced in 1993 by Internet Engineering Task Force .

It replace the previous classful addressing method to design a network in the Internet.

Its goal was to reduce the rapid exhaustion of IPv4 addresses.

Classless Inter Domain Routing (CIDR):

IP address consist of two groups of bits:

The most significant bits are the network address or network prefix , which identifies a whole network or subnet.

The least significant bits are the host address, which specifies a particular interface of a host on that network.

This division is used in CIDR to perform subnetting.

CIDR is based on the variable-length subnet masking (VLSM) technique.

Variable Length Subnet Mask (VLSM):

Variable length subnet mask(VLSM) technique is used in CIDR

VLSM is a process of dividing an IP address space into the subnet of different sizes without wasting IP addresses. Example 192.168.1.160/30

VLSM is closely related to CIDR.

VLSM allows various network/ subnet to have different subnet masks.

CIDR allows routers to group the various routes together to reduce the amount of routing information at the core routers whereas VLSM helps how to optimise the available address space.

Who manages IP addresses?

The Internet Assigned Numbers Authority (IANA) manages the IP address.

It defines space allocations globally and forms five regional Internet registries (RIRs) to allocate IP address blocks to ISP such as BSNL, Airtel, Vodafone etc.

Five Regional Internet Registries (RIRs) are:

RIPENCC (Reseaux IP Europeens Network coordination center) - Europe

APNIC (Asia pacific network information centre) - Asia

AFRINIC (African Network Information Centre) - Africa

ARIN (American registry for internet numbers) - North America

LACNIC (Latin america network information centre) - Latin America

Who manages IP addresses?

If a device wants to connect to internet then that device request the ISP for the IP address.

As ISP get the range of IP addresses from Regional Internet Registries (according to the location of device).

Where RIR's get defined IP range from Internet Assigned Numbers Authority (IANA).

A device request to ISP which pass the request to particular RIR and RIR forward request to the IANA.

In this way, device get an IP address from the range of IP Addresses.

Why we need Subnetting?

Let take an example, Any Internet Service Provider (ISP) require 120 IP addresses to install a new network. Then ISP request to APNIC for IP addresses.

APNIC provide a IP address 193.172.16.0/24 to the ISP

As this is Class C address ,and we know class C have 254 valid IP address in total.

network required only 120 IP address but APNIC provide 254 IP address. which led to the wastage of 134 IP address.

Why we need Subnetting?

As IP address are very costly and to stop the wastage of IP addresses a method is introduced known as Subnetting.

Like Class C have 256 IP address in total.

We can divide these IP addresses as



This is known as Subnetting

Assigning IP address:

IP address can be assign in two ways to the device:

1. Static IP address
2. Dynamic IP address

Assigning IP address:

Static IP address:

A static IP address is an IP address that are manually configured for a device.

A static IP address is called static because it doesn't change.

Static IP addresses are also known as fixed IP addresses or dedicated IP addresses.

Dynamic IP address:

A dynamic IP address is an IP address that is automatically assigned to each device in a network.

This automatic assignment of IP addresses is done by a DHCP server.

Dynamic IP address is called *dynamic* because it will change on future connections to the network.

Subnetting of Class C

Content:

1. Subnetting of Class C

Subnetting of Class C:

1. 194.168.5.0/24

Here 194 in 1st octet indicate that this is Class C IP address
/24 represents the subnet Mask i.e. 255.255.255.0

<u>194.168.5</u>	.0
Network bits	Host Bits

No .of Host bits=8

$2^8=256$ Total IP address

$2^8-2= 254$ Total valid IP address

Subnetting of Class C:

Now do subnetting of this IP address:

1. 194.168.5.00000000

If we **borrow 1 bit form Host bits to Network bits.**

<u>194.168.5.0</u>	<u>0000000</u>
25 Network Bits	7 Host bits

- How many Subnetworks are created?

2^n where n is the no. of bits borrowed from host by network.

So, $2^1 = 2$

Thus, 2 subnetworks are created by borrowing one bit from host to network. Each subnetwork will contain 128 IP addresses in total.

Subnetting of Class C:

- How many valid IP address will be there in one subnetwork?
 2^{n-2} where n indicate the no. of host bit left after borrowing a bit.
So, $2^7-2 = 128-2 = 126$
There are 126 valid IP address in total.
- Subnet Mask of this IP address become: 192.168.5.0/25

Subnetting of Class C:

2. 194.168.5.00000000

If we **borrow 2 bit form Host bits to Network bits.**

<u>194.168.5.00</u>	<u>000000</u>
26 Network Bits	6 Host bits

How many Subnetworks are created?

2^n where n is the no. of bits borrowed from host by network.

So, $2^2 = 4$

Thus, 4 subnetworks are created by borrowing 2 bits from host to network.

Each subnetwork will contain 64 total IP addresses.

Subnetting of Class C:

- How many valid IP address will be there in one subnetwork?
 2^{n-2} where n indicate the no. of host bit left after borrowing a bit.
So, $2^6-2 = 64-2 = 62$
There are 62 valid IP address in total.
- Subnet Mask of this IP address become: 192.168.5.0/26

Same way we can borrow 3,4 or so on to create subnetwork.

Bits can be borrow according to the no. of subnetwork we want to create.

Subnetting of Class C:

Example: Find network IP, Broadcast IP, Subnet Mask and Host range of IP address 200.200.100.0/24

Solution: It is a Class C address with subnet Mask: 255.255.255.0

If we borrow 1 bit from host bits to network bit

200.200.100.0 0000000

25 Network Bits 7 Host bits

Subnetwork created: $2^n = 2^1 = 2$

Valid IP Address: $2^{n-2} = 2^{7-2} = 126$

Subnetting of Class C:

2 subnetwork created are:

200.200.100.0/25 - subnet 1

200.200.100.128/25 - subnet 2

Subnet Mask: 255.255.255.128

(Last address of subnetwork is subnet mask of all other networks)

Now calculate host range:

Subnetting of Class C:

200.200.100.0 - Network IP

200.200.100.1

.....
Valid IP's

200.200.100.126

200.200.100.127 - Broadcast IP

200.200.100.128 - Network IP

200.200.100.129

.....
Valid IP's

200.200.100.254

200.200.100.255 - Broadcast IP

Subnet 1

Subnet 2

Subnetting of Class A & B

Content:

1. Subnetting of Class B
2. Subnetting of Class A

Subnetting of Class B:

Subnetting of Class B is done when we require more IP than 255 IP's in Class C.

Class B contain 65536 IP addresses in total.

As Class B contain large no of IP's so we count from least significant bits to make the calculation easy.

Subnetting of Class B:

1. 172.16.250.12/16

Here 172 in 1st octet indicate that this is Class B IP address
/16 represents the subnet Mask i.e. 255.255.0.0

<u>172.16</u>	<u>.250.12</u>
Network bits	Host Bits

No. of Host bits=16

$2^{16}=65536$ Total IP address

$2^{16}-2= 65534$ Total valid IP address

Subnetting of Class B:

Now do subnetting of this IP address:

1. 172.16.250.12

If we **borrow 5 bit form Host bits to Network bits.**

<u>172.16.00000</u>	<u>000.00000000</u>
21 Network Bits	11 Host bits

Subnetwork created: $2^n = 2^5 = 32$

Valid IP Address: $2^{n-2} = 2^{11-2} = 2048-2 = 2046$

Subnetting of Class B:

32 subnetwork created are:

172.16.0.0/21 - subnet 1

172.16.8.0/21 - subnet 2

172.16.16.0/21 - subnet 3

.....

.....

172.16.248.0/21 - subnet 32

Subnet Mask: 255.255.248.0 or /21

(Last address of subnetwork is subnet mask of all other networks)

Now calculate host range:

Subnetting of Class B:

Network IP address	Valid IP address	Broadcast IP address
Subnet 1 172.16.0.0	172.16.1.0 - 172.16.6.0	172.16.7.255
Subnet 2 172.16.8.0	176.16.9.0 - 172.16.14.0	172.16.15.255
Subnet 3 172.16.16.0	176.16.17.0 - 172.16.22.0	172.16.23.255
Subnet 4 172.16.24.0	176.16.25.0 - 172.16.30.0	172.16.31.255
.....
.....
Subnet 32 172.16.248.0	176.16.249.0 - 172.16.254.0	172.16.247.255 172.16.255.255

Subnetting of Class A:

1. 10.0.0.0/8

Here 10 in 1st octet indicate that this is Class A IP address
/8 represents the subnet Mask i.e. 255.0.0.0

<u>10</u>	<u>.0.0.0</u>
Network bits	Host Bits

No. of Host bits=24

$2^{24}=16777216$ Total IP address

Subnetting of Class A:

Now do subnetting of this IP address:

1. 10.0.0.0

If we **borrow 11 bit form Host bits to Network bits.**

10.00000000.000

19 Network Bits

00000.00000000

13 Host bits

Subnetwork created: $2^n = 2^{11} = 2048$

Valid IP Address: $2^{n-2} = 2^{13-2} = 4192-2 = 4190$

Subnetting of Class A:

2048 subnetwork created are:

10.0.0.0/19 - subnet 1

10.0.32.0/19 - subnet 2

10.0.64.0/19 - subnet 3

.....

.....

10.0.224.0/19 - subnet n

10.1.0.0/19

10.1.32.0/19

.....

10.2.224.0/19

10.255.224.0/19 - Subnet 2048

Subnetting of Class A:

Subnet Mask: 255.0.224.0 or /19

(Last address of subnetwork is subnet mask of all other networks)

Similarly we can find the host range as find in Class B and Class C.

IPv4

Content:

1. IPv4
 - o Address type
 - o Notations
 - o IPv4 Packet Format
2. Network Address Translation (NAT)

IPv4:

Internet Protocol Version 4 (IPv4) is the fourth version of the IP address.

It is a connectionless protocol used in packet-switched networks, such as Internet.

It provides the logical connection between network devices by providing identification to each device.

IPv4 is designed and specified in IETF publication RFC 791.

IPv4:

Address Type:

Address Space is the total number of addresses used by the protocol.

IPv4 is a 32 bit address which means it consists of 2^{32} (i.e. 4,294,967,296) address space

Example: 117.149.29.2 is an IPv4 address

Theoretically, more than 4 billion devices can be connected to internet.

But due to imposed restrictions on IP addresses, actual number is much less.

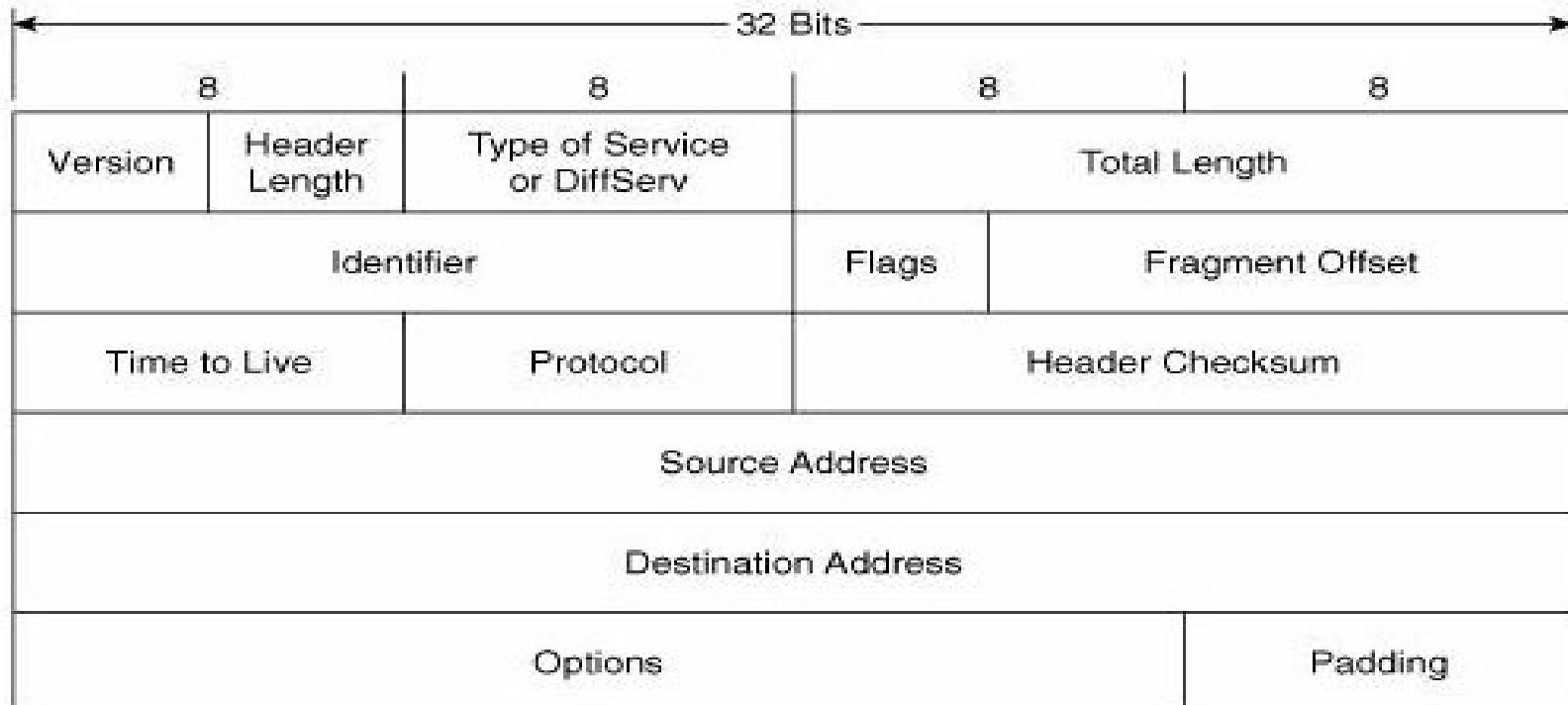
IPv4:

Notation: IPv4 address can be represented in two way:

- Binary Notation: IPv4 is a 32 bit address in which there are 4 octet each having the bytes.
- Dotted Decimal Notation: IPv4 address are written in decimal notation to make it more compact and easier to read. Each number in dotted decimal notation value ranges from 0 to 255.



IPv4:



IPv4 Packet Format

IPv4:

IPv4 Packet Format:

The IPv4 packet header consists of 14 fields,out of which 13 are used. It consists of 20 bytes of data.

- **Version**:- The first header field in an IP packet is a 4 bit long which indicates the version of the internet header.This four-bit field is set to binary 0100 for IPv4 or binary 0110 for IPv6.
- **Header length**:- It is also known as Internet Header Length (IHL). The second field (4 bits) tells the number of 32-bit words in the header. The minimum value for this field is 5.

IPv4:

- **Type of Service(ToS):-** It also known as Differentiated Services Code Point (DSCP). This field is used to carry information to provide quality of service features. With the development of new technologies that require real-time data streaming. Example Voice over IP (VoIP).
- **Total Length:-** This field is of 16 bit which defines the size entire datagram, including header and data (in bytes). The minimum-length datagram is 20 bytes and the maximum is 65,535 bytes.
- **Identifiers:-** The identification field is used for uniquely identifying fragments of an original IP datagram.

IPv4:

- **Flags:-**A 3 bits field is used to control and identify fragments. They are
 - bit 0: Reserved; must be zero.
 - bit 1: Don't Fragment (DF)
 - bit 2: More Fragments (MF)
- **Fragment Offset:-**The fragment offset field is 13 bits long and specifies the offset of a particular fragment.
- **Protocol:-**This field indicate the protocol used in the data portion of the IP datagram.
- **Header Checksum:-** It is of 16-bit which is used for error-checking of the header.

IPv4:

- **Time To Live (TTL)**:-It is of 8 bit field which indicates the maximum time for which a datagram is allowed to remain in the internet system. The intention is to cause undeliverable datagrams to be discarded. The maximum datagram lifetime (hops) in the range of 0-255.
- **Source address** :- This field indicate the IP address of source of packet.
- **Destination address** :- This field indicates the IP address of receiver of the packet.
- **Options**:- This is an optional field reserved for future use.

IPv4:

Network Address Translation:

NAT stands for Network Address Translation or Network Address Translator.

It is the virtualization of Internet Protocol (IP) addresses.

Network Address Translation is the process where a network device (like firewall) assigns a public address to a computer inside a private network.

This helps in improving security and decrease the need of large number of IP addresses in an organization.

IPv4:

Network Address Translation:

In NAT, the private address range is used i.e. 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.

NAT technique works well for computers that only have to access resources inside the network, for example host want to access file servers and printers.

Thus using private address routers inside the private network can route traffic between private addresses with no trouble.

IPv4:

Network Address Translation:

If a host want to access resources outside the network from Internet, then the host must contain public IP address.

In this way (NAT) Network Address Translation works.

IPv4:



Network Address Translation (NAT)

IPv6

Part 1

Content:

1. IPv6

- Features of IPv6
- Why we need IPv6 IP address?
- Notation

IPv6:

IPv6 (Internet Protocol Version 6) is also known as IPng (Internet Protocol next generation) and it is the most recent version of the Internet Protocol (IP).

It is a network layer protocol that provides an identification and location of computers on networks and routes the traffic across the Internet.

IPv6 is introduced by the Internet Engineering Task Force (IETF) in 1998.

It was introduced to replace the widely used IPv4 addresses that is considered as the backbone of the modern Internet.

In 2004, Japan and Korea were first in public deployments of IPv6.

IPv6:

Features of IPv6:

- It can support 128 bit long source and destination addresses.
- The header of IPv6 is simplified by moving all unnecessary information.
- It provide end to end connectivity by providing IP address to each device in network and can communicate through the Internet without using NAT.
- It make faster forwarding/routing by simply removing the unnecessary detail from header.
- IPv6 have IPSec security, which make it more secure than IPv4.

IPv6:

Features of IPv6:

- IPv6 does not have any broadcast support. It uses multicast to communicate with multiple hosts.
- IPv6 introduced a Anycast mode of packet routing in which packet is route to the nearest destination.
- It enables hosts to roam in different geographical area and remain connected with the same IP address.
- IPv4 used 6 bits DSCP (Differential Service Code Point) and 2 bits ECN (Explicit Congestion Notification) to provide better Quality of Service
- It support smooth transition as the header is less loaded, so routers can take forwarding decisions quickly as they arrive.

IPv6:

Why we need IPv6 IP address?

To make communication possible every device which is connected to internet gets a unique number known as an IP address.

Internet addressing system IPv4, has capacity for about 4.2 billion addresses.

The problem arise with the increase in number of new devices like computers, smart phones, TVs, smart watches, cars etc these addresses are not enough to meet the demand of new devices.

IPv6:

Why we need IPv6 IP address?

Thus, there a shortage of IPv4 addresses occur.

So many methods were adopted to prevent the depletion of IPv4, like Subnetting, VLSM and NAT etc these methods were no longer able to provide IP address to networks for future demands.

IPv6:

Why we need IPv6 IP address?

IPv4 is of 32 bits address, it can provide 2^{32} IP addresses.

$$2^{32} = 4294967296$$

= 4.2 billion

To overcome this limitation IPv6 Addresses are introduced:

IPv6 is of 128 bits which is 4 times of the IPv4 in bits size.

$$2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456 \quad \text{total IP}$$

addresses

= 340 trillion

Thus, this is the reason with the deployment of IPv6 address.

IPv6:

Structure:

An IPv6 address is of 128 bits long

It is divided into eight 16-bits blocks.

Each block is then converted into 4-digit.

it is represented by Hexadecimal numbers separated by colon symbols.

IPv6:

Structure:

For example:

IPv6 address represented in binary format and divided into eight 16-bits blocks:

```
001000000000001 0000000000000000 0011001000111000  
110111111100001 0000000001100011 0000000000000000  
0000000000000000 111111011111011
```

Each block is then converted into Hexadecimal and separated by ':' symbol:

2001:0000:3238:DFE1:0063:0000:0000:FEFB

IPv6:

Structure:

Some rules to shorten the IPv6 address:

Rule.1: Discard leading Zero(es):

Leading zeros of a section can be omitted ,only leading 0s can be dropped not trailing 0s, such as in block 5

2001:0000:3238:DFE1:**0063**:0000:0000:FEFB

2001:0000:3238:DFE1:**63**:0000:0000:FEFB

IPv6:

Structure:

Rule 2: Replace consecutive zero's

If two or more blocks contain consecutive zeroes, omit them all and replace it with double colon sign “::” such as in 6th and 7th block

2001:0000:3238:DFE1:63:0000:0000:FEFB

2001:0000:3238:DFE1:63::FEFB

IPv6:

Structure:

Rule 2:

Consecutive blocks of zeroes can be replaced only once, if there are still blocks of zeroes in the address, they can be replaced by single zero, such as in 2nd block

2001:0000:3238:DFE1:63::FEFB
2001:0:3238:DFE1:63::FEFB

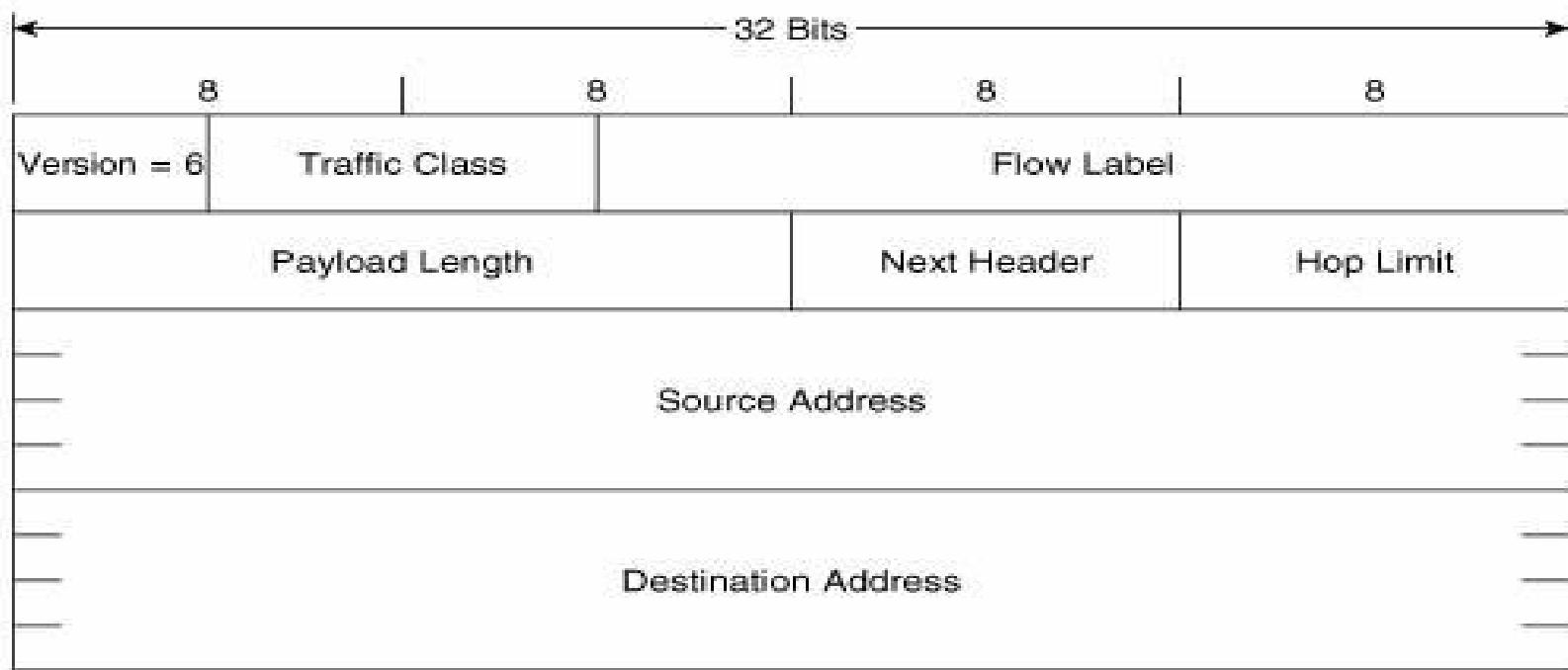
IPv6

Part 2

Content:

1. IPv6 Header format
2. Extension headers
3. Advantage of IPv6
4. Type of IPv6 address

IPv6:



IPv6 Packet Format

IPv6:

IPv6 Packet format:

- **Version:** It is of 4 bits and remain constant i.e 6 or bit sequence 0110.
- **Traffic Class:** It is of 8 bits. This field hold two values. The 6 most-significant bits are used for differentiated services and remaining two bits are used for ECN where the source provides data traffic information.
- **Flow Label:** It is of 20 bits and used for giving real-time applications special service and also help to detect spoofed packets.
- **Payload Length:** It is of 16 bits. When a Hop-by-Hop extension header holds a Jumbo Payload option then the length is set to zero

IPv6:

IPv6 Packet format:

- **Next Header:** It is 8 bits long which specifies the type of the next header i.e. it specifies the transport layer protocol used by a packet's payload.
- **Hop Limit:** It is 8 bits long and the value of this field decreases by one at each intermediate node visited by the packet. When the counter reaches 0 the packet is discarded. This field replace the time to live field of IPv4.
- **Source Address:** It is 128 bits long and indicate the IP address of source node.
- **Destination Address:** It is 128 bits long and it indicate the IP address of destination node.

IPv6:

Extension Header: Extension Header are added to give greater functionality to the IP datagram in IPv6 address.

It is added with a base header.

These are the extension header:

- Hop-by-Hop option
- Source Routing
- Fragmentation
- Authentication
- Encrypted security payload
- Destination option

IPv6:

Extension Header:

- **Hop-by-Hop option:**

It is used when the source needs to pass information to all routers visited by the datagram.

The jumbo payload option is used to define a payload longer than 65,535 bytes.

- **Source Routing:**

The source routing Extension header is a method to specify the route for an IPv6 datagram

IPv6:

Extension Header:

- **Fragmentation:**

Fragmentation header is used when a packet to be send is larger than the Maximum Transmission Unit (MTU) a path can hold.

Then the sending node splits the packet into fragments.

The Fragment extension header carries the information necessary to reassemble the original packet at destination node.

- **Authentication:**

Authentication extension header contains information used to verify the authenticity of the packet.

IPv6:

Extension Header:

- **Encrypted Security Payload:**

It is used to contain information used to verify the Confidentiality of most parts of the packet.

- **Destination Option:**

Destination Option is used to examine the optional information of data packet by the destination node.

IPv6:

Advantages:

1. Larger address space
2. Better header format
3. New additional options
4. Allowance for extension
5. More security

Type of IPv6 address:

The type of network communication in IPv6 are:

1. Unicast Address
2. Multicast Address
3. Anycast Address

Type of IPv6 address:

1. Unicast Address:

Unicast is a type of communication where data is sent from one computer to another computer in a network.

Unicast is a one-to-one type of network communication.

In Unicast type of communication, there is only one sender, and only one receiver.

Example for IPv6 Unicast type of network communication: Browsing a website, Downloading a file from a FTP Server etc

Type of IPv6 address:

2. Multicast Address:

Multicast is a type of communication where data is send to a group of devices in the network.

IPv6 multicast data is sent to a group and only members of that group receive the Multicast data.

In Multicast, the sender transmit only one copy of data and it is delivered to group of devices.

For example: Online TV

Type of IPv6 address:

3. Anycast Address:

Anycast is a type of network communication in which IPv6 datagrams from a source are routed to the nearest device from a group servers which provide the same service.

Every nodes which provide the same service are configured with same Anycast destination address.

Transition from IPv4 to IPv6

Content:

1. Transition from IPv4 to IPv6
 - o Dual Stack
 - o Tunneling
 - o Header translation

Transition from IPv4 to IPv6:

Due to huge number of devices on internet, transition from IPv4 to IPv6 cannot happen suddenly.

So, to make communication possible between every device in network we need transition from IPv4 to IPv6.

Types of transition are:

1. Dual stack
2. Tunneling
3. Header Translation

Transition from IPv4 to IPv6:

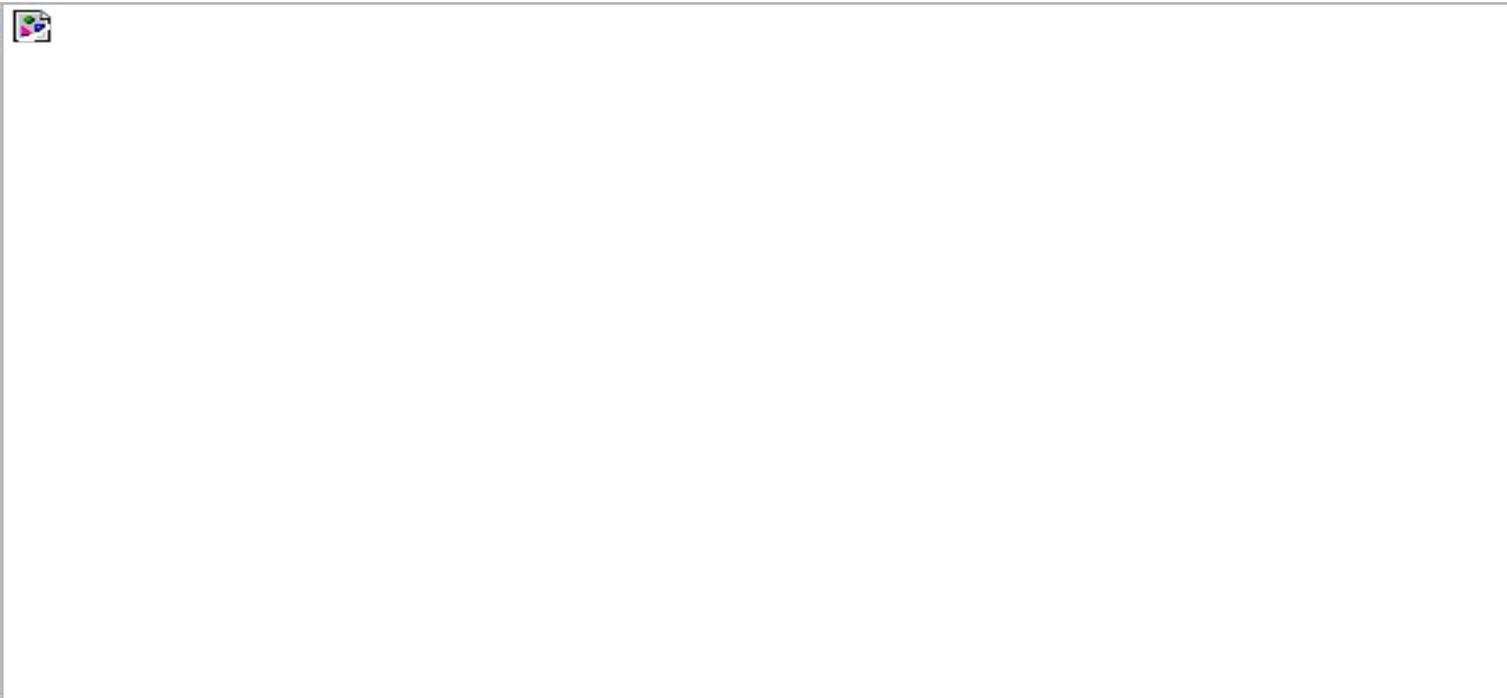
1. Dual Stack:

In Dual Stack, a router or a host is equipped with both IPv4 and IPv6 addresses.

In the diagram shown,a hosts from IPv4 as well as IPv6 can access the server with the help of a Dual Stack Router

The Dual Stack Router, can communicate with both the networks. Using Dual Stack router we can also send and receive data belonging to both protocols simultaneously.

Transition from IPv4 to IPv6:



Dual Stack Transition

Transition from IPv4 to IPv6:

2. Tunneling:

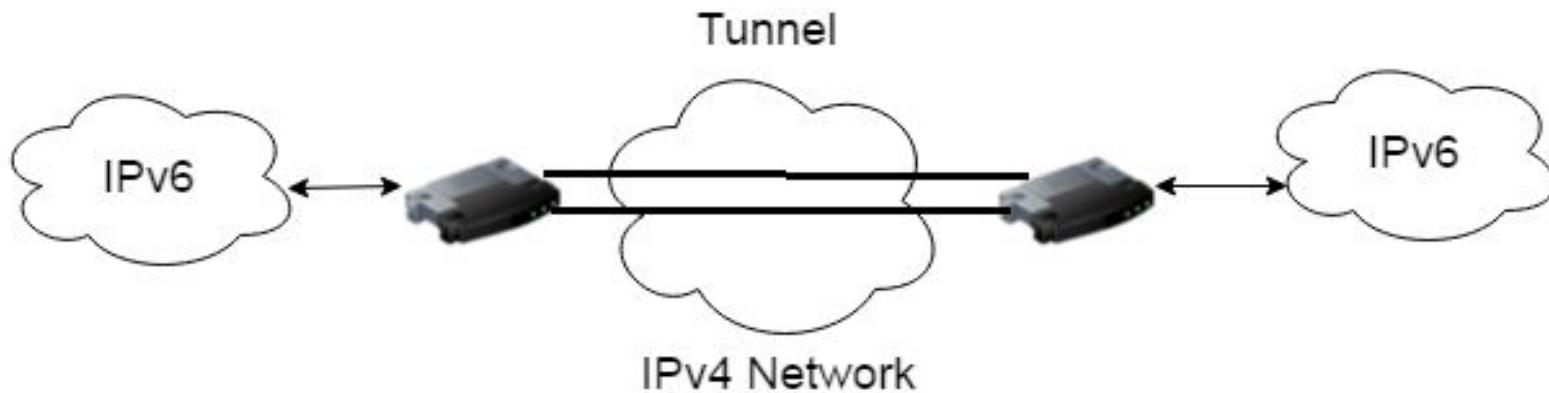
Tunneling is a technique in which two computers using IPv6 addressing want to communicate with each other and the packets have to pass through a region of IPv4 addressing.

So, to pass the packet through this region, it must contain IPv4 address.

In this when a packet enters the IPv4 region, IPv6 packet encapsulates in a IPv4 packet and when it leaves that region IPv6 packet exits from the IPv4 packet.

In such way, the IPv4 region creates a tunnel to pass the IPv6 packets.

Transition from IPv4 to IPv6:



Tunneling

Transition from IPv4 to IPv6:

3. Header Translation:

In a network, when a transmitter device transmit a packet in IPv6 format and the receiver still work at IPv4 format.

Then the tunneling technique will not work.

So, header translation technique is used in which header of IPv6 packet is converted to an IPv4 packet.

Header Translation use the mapped address to translate IPv6 to IPv4 address.

Transition from IPv4 to IPv6:



Header Translation

Routing

Content:

1. Router
2. Functions of Routers
3. Interface ports of Router
4. Routing tables

Router:

Router is an internetworking component that connects different networks together.

It may be a hardware or software based.

In packet-switched networks such as the internet, a router is a device that determines the best way for a packet to be forwarded to its destination.

It uses headers and routing tables to determine the best path for forwarding the packets in the network.

It works at Network layer of an OSI model and Internet layer of TCP/IP model.

For example: Cisco 2600 series router

Router:



Functions of Router:

Main function of Routers are:

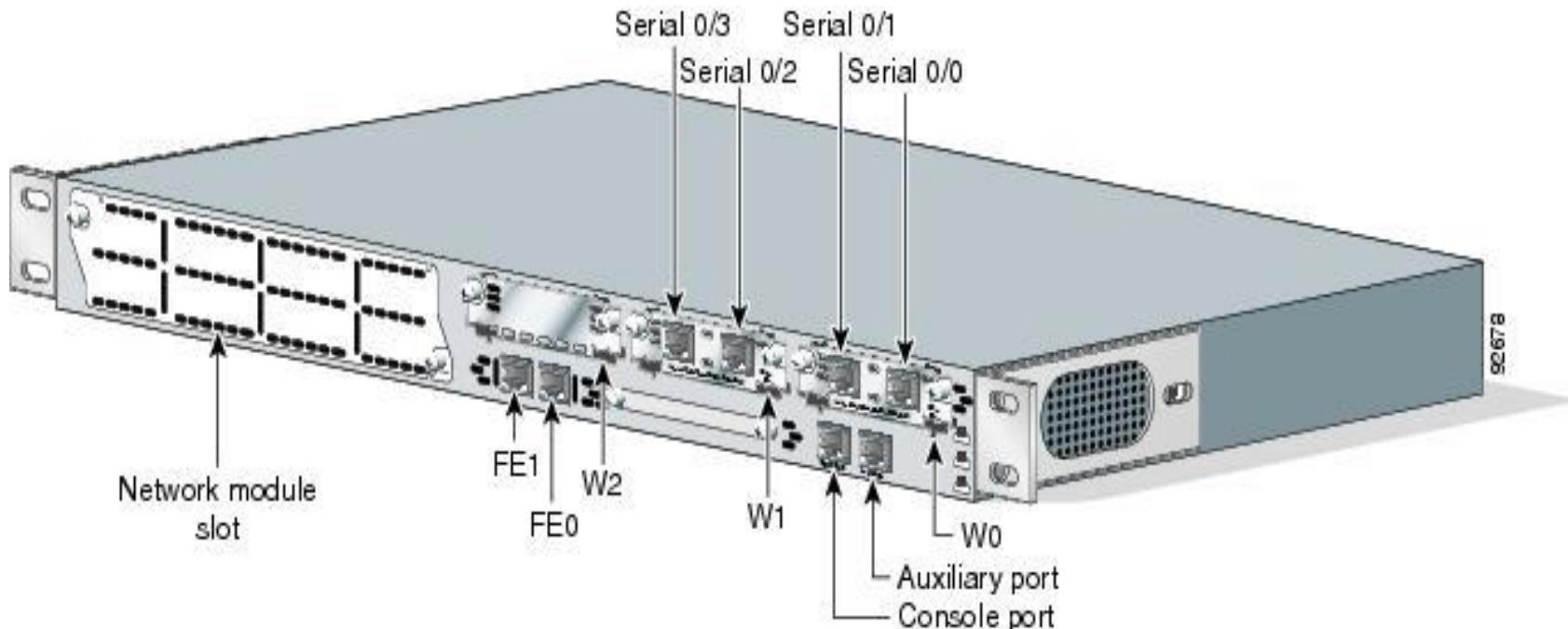
1. Router connect the two or more different network such as two LANs or WANs or a LAN and its ISP's network.
2. It routes the packet in the network by learning IP address of the devices.
3. It provide the best routing path to the packet in the network.
4. It verify and maintain the routing information.
5. It keep the information about the source and destination of a packet

Interface Ports of Router:

Interface Ports of router are:

1. Power
2. On/Off Switch
3. Auxiliary RJ-45
4. Console port
5. Synchronous serial port
6. Ethernet AUI port
7. System OK LED
8. Synchronous serial LED
9. Ethernet AUI LED

Interface Ports of Router:



Interface ports

Interface Ports of Router:

Interface Ports of router are:

- The interfaces on a router provide network connectivity to the router.
- The LAN interfaces on routers include Ethernet, Fast Ethernet, Fiber Distributed Data Interface (FDDI) or Token Ring.
- The AUI (Attachment Unit Interface) port on router is used to provide LAN connectivity.
- Some routers have separate interfaces for ATM (Asynchronous Transfer Mode).

Interface Ports of Router:

Interface Ports of router are:

- The WAN interface on router include Sync and Async serial interfaces.
- ISDN (Integrated Services Digital Network) interfaces are used to provide the ISDN connectivity using which we can transmit both voice and data.
- The console and auxiliary ports of router are used for managing or configuring the router.
- “show ip interface brief” command is the most useful command to see the interfaces of router.

Routing Table:

Routing table is a set of rules which determine where to route the packet in the Internet protocol (IP) network.

Every Router in a Network maintain the routing table.

Every packets which are traveling in network, contain IP address of source and destination device.

When receive these packet it match the address with the information that routing table contain and find the best route to transfer packet.

Routing tables can be maintain dynamically or manually.

Routing Table:

Information include by Routing table is:

- Destination IP: IP address of final destination.
- Subnet Mask: define network ID of IP address.
- Next Hop: IP address of another hop to which the packet is forwarded.
- Interface: defines the ports of router used for forwarding a packet
- Metric: it is used to find a cost-effective route as it assign costs to each route in the network.

Routing table:

RRAS-ROUTER1 - IP Routing Table						
Destination	Network mask	Gateway	Interface	Metric	Protocol	
10.57.76.0	255.255.255.0	10.57.76.1	Local Area C...	1	Local	
10.57.76.1	255.255.255.255	127.0.0.1	Loopback	1	Local	
10.255.255.255	255.255.255.255	10.57.76.1	Local Area C...	1	Local	
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local	
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local	
192.168.45.0	255.255.255.0	192.168.45.1	Local Area C...	1	Local	
192.168.45.1	255.255.255.255	127.0.0.1	Loopback	1	Local	
224.0.0.0	224.0.0.0	192.168.45.1	Local Area C...	1	Local	
224.0.0.0	224.0.0.0	10.57.76.1	Local Area C...	1	Local	
255.255.255.255	255.255.255.255	192.168.45.1	Local Area C...	1	Local	
255.255.255.255	255.255.255.255	10.57.76.1	Local Area C...	1	Local	

Routing Table:

How Router create Routing tables?

In a network, when a sender device sends the packet to the destination device then sender add IP address of both the devices.

Then the packet goes to router.

Router examine the packet and find its IP addresses in its Routing table.

When router gets the perfect match, then it determine the perfect route (cost effective route) to forward the packet in the network.

Routing Table:

How Router create Routing tables?

If any new device add in the network than router update the routing table according to its IP address.

Thus router update their information which is contain in routing table for effective routing.

Routing Protocol

Content:

1. Type of Routes
 - o Static Routes
 - o Dynamic Routes
 - o Default Routes
2. Static Routing Protocol
3. Dynamic Routing Protocol

Type of Routes:

Routing is a process of selecting best path in a network.

There are two type of route:

- Static route
- Dynamic route

Type of Routes:

Static Route:

Static route are configured manually by network administrator.

When any change in the network occur then administrator manually update the static route according to the changes.

It is used for simple and small network.

More secure route.

Type of Routes:

Dynamic Route:

Dynamic routes are the routes which router gets from other routers via routing protocol.

Whenever there is any change in network then the router update the information automatically.

It is used in large network.

Less secure route.

Types of Routes:

Default Route:

Default route is one kind of special route.

Default route can be configured manually and also generated by routing protocol such as OSPF.

Default route is used when a router receive a packet whose destination is not listed in the routing table.

Thus router transfer the packet to next hop defined by default route.

Default route can be configured by setting destination address and mask to be 0's.

Static Routing Protocol:

A static route is a special route which is configured by network administrator manually.

Static routing is a type of network routing technique used for manual configuration and selection of a network route.

It is used where the network parameters and environment are expected to remain constant.

Static routing is not a routing protocol; instead, it is the routing technique.

For configuring static route on cisco router type- ip route static<destination network><subnet mask><exit interface or next hop ip>

Static Routing Protocol:

Advantage:

No overhead information is required.

No bandwidth usage between links.

Form Highly secure network.

Disadvantage:

Complete knowledge of network is required.

Not easy to implement on large network.

All routers have to update manually, If network topology change.

Dynamic Routing Protocol:

Dynamic routing protocol is used to find best route to forward the packet to the destination.

The common protocol used by dynamic routing protocols are RIP, OSPF, ISIS and BGP etc.

In dynamic routing protocol, the router automatically updates its routing table according to the changes in the network.

For configuring dynamic route set destination address and subnet mask address to zero.

Dynamic Routing Protocol:

Advantage:

Less manual configuration is required while adding and deleting networks.

Routers are updated automatically, if any change occur in network.

More scalable protocol.

Disadvantage:

More load is present on routers in the network.

Network knowledge is required.

Less secure network.

Dynamic Routing Protocol

Content:

1. Dynamic Routing Protocols
 - IGP and EGP
2. IGP types:
 - Distance Vector Routing Protocol
 - Link State Routing Protocol
 - Hybrid Routing Protocol

Dynamic Routing Protocol:

Dynamic Routing Protocol is a set of protocols used for finding best route to forward packet in a network.

Dynamic route configured automatically without any administrator intervention.

Dynamic route are more adapt to any change in network.

Dynamic Routing protocol can be divided into :

- IGP (Interior Gateway Protocol)
- EGP (Exterior Gateway Protocol)

Dynamic Routing Protocol:

Autonomous System:

Autonomous system is a collection of networks managed by single entity or organization and they follow different routing policies.

Autonomous systems are allocated with unique number ranges from 1 to 65534 which is assigned by IANA.

- Public AS numbers = 1 to 64511 (used on internet)
- Private AS numbers = 64512 to 65534 (used internally within an organization)

Dynamic Routing Protocol:

1. Interior Gateway Protocol:

Interior Gateway Protocol is a set of routing protocol which are used within one autonomous system.

For example: RIP, IS-IS etc

It mainly search and calculate routes within an autonomous system.

Dynamic Routing Protocol:

2. Exterior Gateway Protocol:

Exterior Gateway Protocol is used to connect different autonomous system such as BGP .

It control communication between different autonomous system with routing policies and route filtering mechanism.

Dynamic Routing protocol

Different type of routing protocols are:

1. Distance vector Routing
 - o RIPv1
 - o RIPv2
 - o BGP
 - o IGRP
2. Link state Routing
 - o OSPF
 - o IS-IS
3. Hybrid Routing
 - o EIGRP

Dynamic Routing Protocol:

1. Distance-Vector Routing Protocol:

Distance vector routing protocols was the first routing protocols used in TCP/IP network.

It use two things to choose the best path i.e. distance calculation and a network interface port.

It specifies the distance from the destination and indicate the direction or interface to which packet should be forwarded.

In this router will periodically informs its neighbours about any network change.

Dynamic Routing Protocol:

1. Distance-Vector Routing Protocol:

In distance vector routing, routers share the entire routing table with each other after every 30 seconds (approx.).

Distance vector routing algorithm works in small network containing less router.

Example of Distance vector routing protocols are RIPv1, RIPv2 and BGP.

Dynamic Routing Protocol:

2. Link-state Routing Protocol:

Link-State routing protocol is a faster protocol which use less bandwidth over WAN network.

Link-state packets (LSP) are used to determine the names of neighbouring router and the cost or distance to any neighboring routers and associated network.

As in distance vector routing protocol, the routers shares their routing table at a regular interval, this increase the traffic load in the network.

Dynamic Routing Protocol:

2. Link-state Routing Protocol:

But in link-state routing protocol, the routers simply shares the changes if occur in their routing table.

In Link state routing protocol, the routers also share the information about its neighbouring routers.

Example of Link-state Routing Protocol are OSPF and IS-IS .

Dynamic Routing Protocol:

3. Hybrid Routing Protocol:

Hybrid routing protocol is a combination of distance vector routing protocol and link-state routing protocol.

Hybrid routing protocol use distance vector for more accurate metrics to determine the best path to destination network.

It use link state protocol for sending routing information if their is any change in the network topology.

Dynamic Routing protocol:

3. Hybrid Routing Protocol:

Hybrid routing allow rapid convergence in the network.

It require less processing power and memory.

Example of Hybrid routing protocol are EIGRP.

Distance Vector Routing Protocol Part 1

Content:

1. Routing Information Protocol (RIP)
 - o How RIP works?
 - o RIPv1 and RIPv2

Distance Vector Routing Protocol:

1. Routing Information Protocol:

RIP Stands for Routing Information Protocol.

First routing protocol designed.

RIP use UDP port 520 to exchange information of routing.

RIP use hop count as the metric. RIP has the maximum hop count of 15.

RIPv1 routers send routing table after every 30 seconds.

This cause a serious problem of network overload in large networks.

Distance Vector Routing Protocol:

1. Routing Information Protocol:

Hold down timing is 180 second i.e. router wait for updation in routing table for 180 second.

Drawback in RIP:

RIP does not see bandwidth of a link or congestion in the network. It only consider minimum hop count.

Load balancing is also a drawback.

Distance Vector Routing Protocol:

1. Routing Information protocol:

How RIP works?

When a router starts, it makes routing table according to directly connected network segments.

Then the router broadcasts the routing table information to all the routers in the network.

Now in network, routers start receiving and processing the updates.

Distance Vector Routing Protocol:

1. Routing Information protocol:

The routers obtain routes to all network segments as they receiving the updates periodically.

Finally, the network converges.

Distance-vector Routing Protocol:



Distance-vector Routing Protocol:

RIPv1

RIPv1 does not support VLSM and CIDR.

RIPv1 does not support authentication.

In RIPv1 packets are transmitted in broadcast mode.

RIPv2

RIPv2 support VLSM and CIDR.

RIPv2 support plain text authentication and MD5 authentication.

In RIPv2 packets are transmitted using broadcast and multicast mode.

Distance Vector Routing Protocol Part 2

Content:

1. Border Gateway Protocol (BGP)
2. Interior Gateway Routing Protocol (IGRP)

Distance-vector Routing Protocol:

2. Border Gateway Protocol:

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol. It is designed to exchange routing information among autonomous systems (AS) on the Internet.

It makes routing decisions based on paths, network policies and rules configured by a network administrator and is involved in making core routing decisions.

BGP is a protocol which make internet work.

Distance-vector Routing Protocol:

2. Border Gateway Protocol:

BGP is of two type:

- Interior Border Gateway Protocol, Internal BGP, or iBGP used to communicate within an AS.
- Exterior Border Gateway Protocol, External BGP, or eBGP used by different AS to communicate with each other.

BGP is standard for Internet routing used by Internet service providers (ISPs) to establish routing between one another.

Distance-vector Routing Protocol:

2. Border Gateway Protocol:

BGP is a powerful dynamic routing protocol.

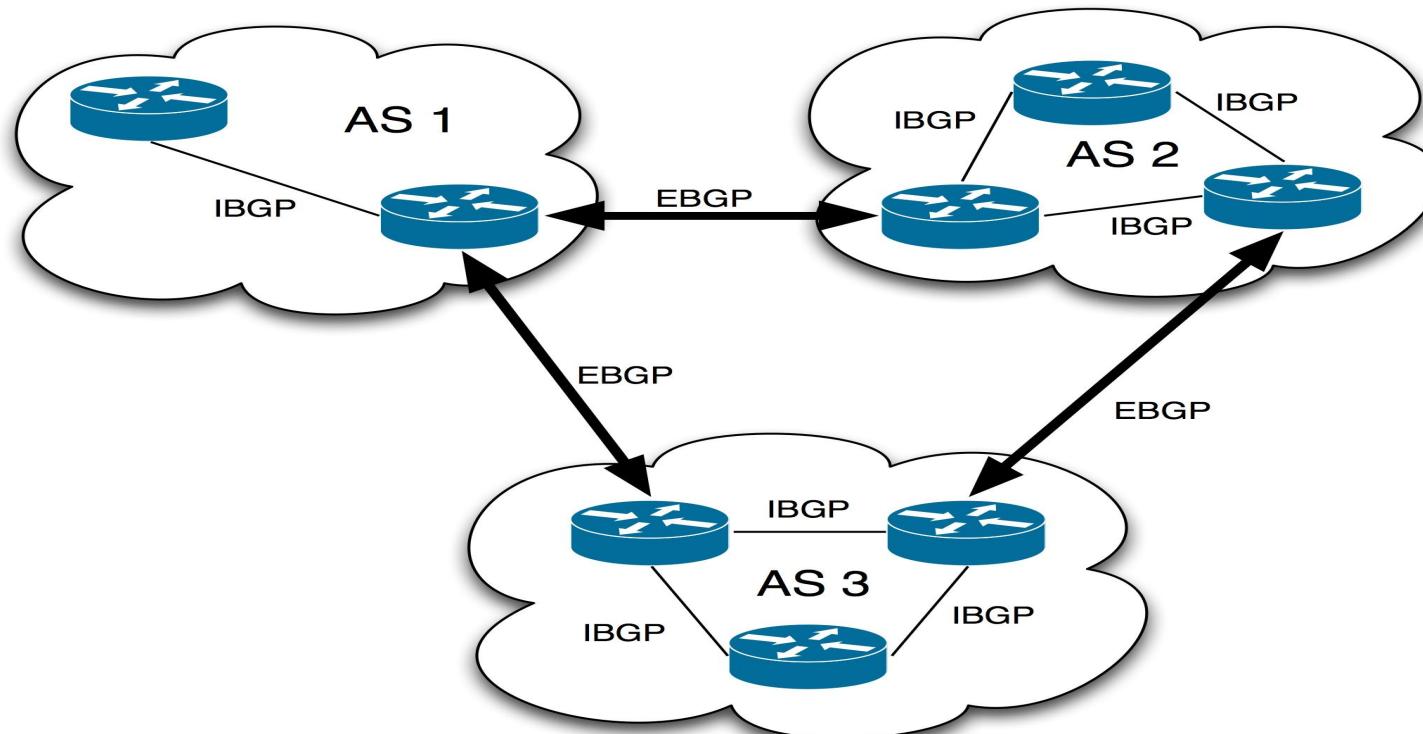
Current version of BGP is “BGP version 4”.

BGP implements and supports route aggregation, used to simplify routing table into manageable levels.

BGP mainly focus on security and scalability of a network.

It is one of the slowest converging routing protocols.

Distance-vector Routing Protocol:



Distance-vector Routing Protocol:

3. Interior Gateway routing protocol:

IGRP is a distance vector routing protocol developed by Cisco.

It is used by routers to exchange routing data within an autonomous system.

IGRP was created to overcome the limitations of RIP of maximum hop count of only 15 and a single routing metric when used within large networks.

It can support multiple metrics for each route, including bandwidth, delay and reliability.

Distance-vector Routing Protocol:

3. Interior Gateway routing protocol:

The maximum configurable hop count of IGRP is 255 (default 100).

It routing updates are broadcast every 90 seconds (by default).

It can support classful routing protocol.

Link State Routing Protocol

Part 1

Content:

1. Open shortest path first (OSPF)
 - o Types of Router
 - o Types of Packet
 - o How OSPF works

Link-state Routing protocol:

1. Open Shortest Path First:

Open Shortest Path First (OSPF) is a routing protocol operating within a single autonomous system (AS).

OSPF was designed by IETF (internet engineering task force) and is one of interior gateway protocol.

It choose best path in a network on the basis of "Link state".

OSPF routers keep information about the state of all network connections or links between the network.

Link-state Routing protocol:

1. Open Shortest Path First:

In case of link failure, it also converges on a new loop-free routing structure within seconds.

It computes the shortest-path tree for each route using link state routing algorithm (LSA) or shortest path first algorithm (SPF).

It calculate shortest path using a method based on Dijkstra's algorithm.

It is defined as OSPF Version 2 in IPv4 and OSPF version 3 in IPv6.

Link-state Routing protocol:

1. Open Shortest Path First:

OSPF converges quickly and it support multiple, equal-cost routes to the destination.

OSPF support CIDR and authentication of packets.

A router that detect the change in a network topology, it immediately multicasts the information to all other OSPF device in the network so they will all have the same routing table information.

All router store the routing information in database known as link-state database.

Link-state Routing protocol:

1. Open Shortest Path First:

OSPF routers divide the single autonomous systems into areas where each area consists of a group of connected routers. These areas are known as OSPF routing area.

The idea of dividing the OSPF network into areas is to simplify administration and routing process.

OSPF does not choose TCP/IP transport protocol it uses protocol number 89 to encapsulate IP packets.

Link State Routing Protocol:



Link-state Routing protocol:

1. **Open Shortest Path First**: The type of routers used in OSPF are:

- Internal Router
- Area Border Router
- Backbone Router
- AS boundary Router

Link State Routing Protocol:



Link-state Routing protocol:

1. Open Shortest Path First:

Designated Routers (DR) and Backup Designated Routers (BDR):

OSPF can elect one router to be a Designated Router (DR) and one router to be a Backup Designated Router (BDR) based upon the network.

For example, in large networks, OSPF elect a DR and BDR to serve as the central point for exchanging OSPF routing information.

Each non-DR or non-BDR router will exchange routing information only with the DR and BDR. Thus this reduces OSPF traffic.

Link-state Routing protocol:

1. Open Shortest Path First:

DR will then distribute topology information to every other router inside the same area.

This reduce the exchange of link state information and routing information in the network.

BDR router work if DR router stop working.

Link-state Routing protocol:

1. Open Shortest Path First: OSPF packet types:

- Hello packet: discover neighbour and maintain the neighbour relation.
- DD packet: it contain LSA and LSA headers.
- LSR packet: request specific link state from router to router.
- LSU packet: send specifically requested link state record.
- LSAck packet: used to acknowledge the received LSU packet.

Link-state Routing protocol:

1. Open Shortest Path First:

How OSPF work?

An OSPF router flood the link state advertisement (LSA) message to notify other routers about the status of link.

Then each router generate a link state database (LSDB) according to LSA.

LSDB contain detailed information about the routing in the network.

A routers in same routing area contain same LSDB.

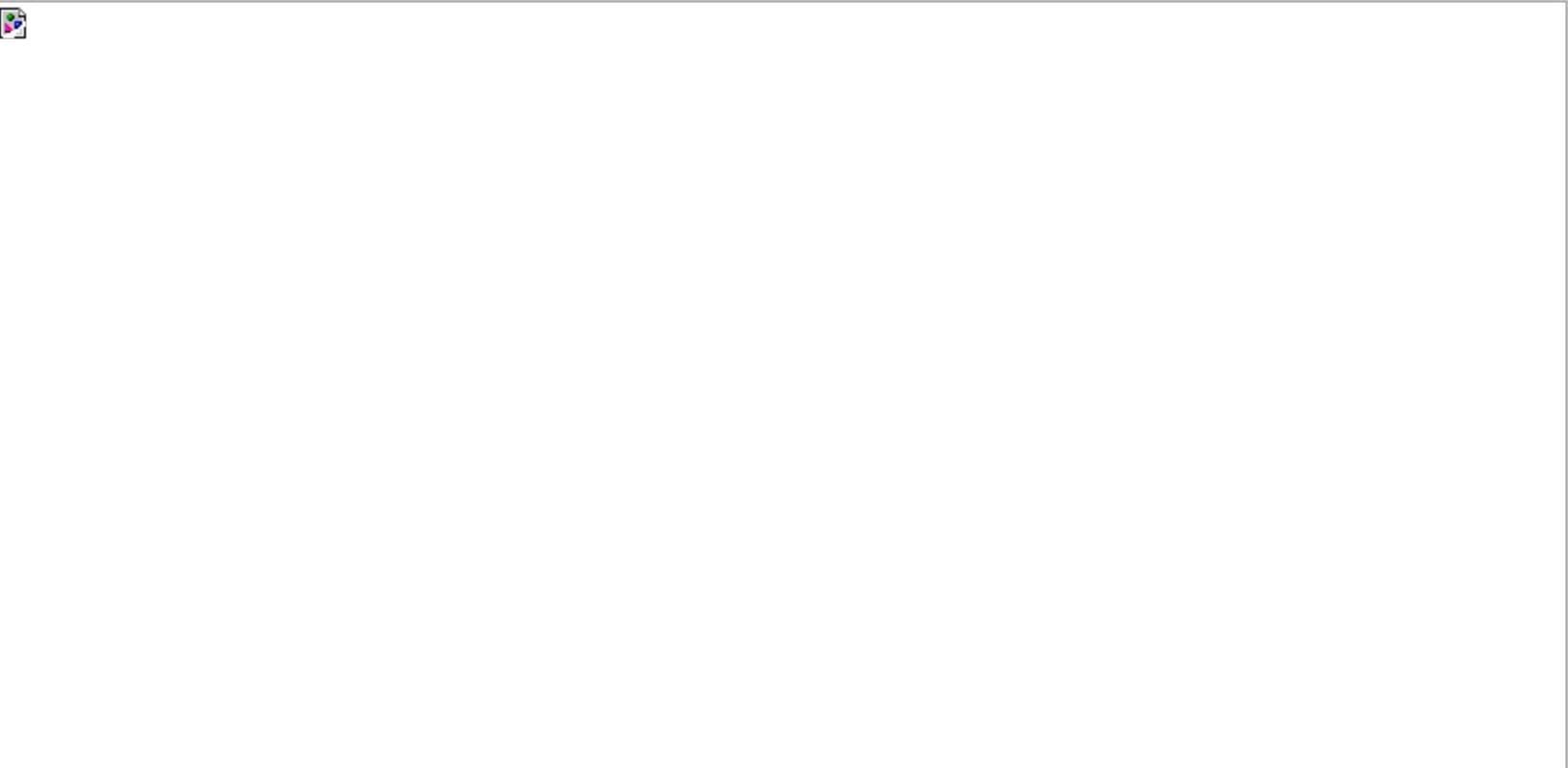
Link-state Routing protocol:

1. Open Shortest Path First:

Then based upon LSDB each routers calculate a shortest path tree with SPF algorithm.

The local router act as the root of the tree and its neighbouring routers as leaves.

Link State Routing Protocol:



Link State Routing Protocol

Part 2

Content:

1. Intermediate System - Intermediate System
 - o Types of Packets
 - o How IS-IS works?
 - o Type of Routers
2. Difference between OSPF and IS-IS

Link-state Routing protocol:

1. Intermediate System-Intermediate System:

The IS-IS protocol is a type of IP routing protocols.

It is also a type of an Interior Gateway Protocol (IGP) for the Internet.

It is used to distribute IP routing information throughout a single Autonomous System in an IP network.

In this protocol, routers exchange topology or routing information with their nearest neighbours.

It is used to calculate complete route through the AS using dijkstra algorithm.

Link-state Routing protocol:

1. Intermediate System-Intermediate System:

The complete route information is flooded in an autonomous system.

It provides a multi-level hierarchy structure for routing called "area routing," so that information about the topology will be sent to routers of the defined AS.

This enables an additional level of routing protection and a reduction in routing protocol traffic.

The all routing information exchanges can be authenticated so that only trusted routers can get the information for the AS.

Link-state Routing protocol:

1. Intermediate System-Intermediate System:

IS-IS Protocol Data Units are of four type:

- Hello – Establish and maintain adjacencies
- LSP (Link State PDU) – Advertises link-state information
- CSNP (Complete Sequence Number PDU) – An update containing the complete list of LSPs known to the router
- PSNP (Partial Sequence Number PDU) – Used to acknowledge a routing update (LSP) on point-to-point links and to request missing information about a route after receiving a CSNP

Link-state Routing protocol:

2. Intermediate System-Intermediate System:

How ISIS works?

Each IS-IS router exchange information about its local state such as interfaces, reachable neighbors and the cost of using each interface to other routers by sending a Link State PDU (LSP) message.

Each router build an identical database according to received information.

Then each router calculates its own routing table using a Shortest Path First (SPF) or Dijkstra algorithm.

Link State Routing Protocol:



Link-state Routing protocol:

Link-state databases maintained by different router:

- A L1 router maintains a database of all routers within the area.
- A L2 router maintains a database of all the areas in the autonomous system.
- A L1/L2 router maintains two separate databases—a L1 database for intra-area routing and a L2 database for inter-area routing.

Link-state Routing protocol:

Difference between OSPF and IS-IS routing protocol:

OSPF was designed according to TCP/IP model whereas ISIS was designed according to OSI model.

OSPF uses the concept of Area boundary routers (ABR) and backbone areas (Area 0) whereas ISIS uses subdomains i.e. level 1, level 2 and level 1-2.

ISIS runs on layer 2 i.e. data link layer of an OSI model where as OSPF runs at layer 3 i.e. network layer.

Hybrid Routing Protocol

Content:

1. Enhanced Interior Gateway Routing Protocol (EIGRP)

Hybrid Routing Protocol:

1. Enhanced Interior Gateway Routing Protocol (EIGRP):

EIGRP is a protocol used by routers to share routes with other routers within the same autonomous system.

EIGRP only sends incremental updates in the AS which reduce the workload on the router.

EIGRP replaced the IGRP in 1993 becoz IGRP does not support classless IPv4 addresses.

EIGRP determines the value of the path in network by using five metrics such as bandwidth, load, delay, reliability and MTU.

Hybrid Routing Protocol:

1. Enhanced Interior Gateway Routing Protocol (EIGRP):

It uses Cisco's Reliable Transport Protocol (RTP) and protocol number 88 to ensure that router updates are delivered to all neighbors routers in the network.

EIGRP can support Classless Inter-Domain Routing (CIDR) and variable length subnet masking.

It has the ability to use different authentication passwords at different times.

Hybrid Routing Protocol:

1. Enhanced Interior Gateway Routing Protocol (EIGRP):

Cisco classified EIGRP as a distance vector routing protocol, but it is said to be a hybrid routing protocol as EIGRP combines many of the features of both link-state and distance-vector routing protocols.

EIGRP used a DUAL (Diffusion Update Algorithm) algorithm to prevent looping in network.

EIGRP use these packets to exchange routing information: Hello packet, Update packet, Acknowledgement packet, Query packet, Reply packet, Request packet.

Switching

Content:

1. Switch
2. Function of switch
3. Switching Modes

Switch:

A switch is a networking device that connects devices or network elements together on a computer network.

Switch is a centralized device connected to multiple PC or nodes in a network.

Switching is a process in which switch is used to forward packet in the network.

It work at data link layer (layer 2) of the OSI model.

Some switches can also process data at the network layer (layer 3) of OSI model.

Layer 3 switches are also known as multilayer switches.

Switch:

It is a intelligent device which understand the MAC-address of the device and stores into a table called CAM (Content Addressable Memory) table.

It has the capability to do a unicast.

Switch works on a concept of CSMA/CD.

Switch port are made up of a special hardware called ASIC (Application Specific Integrated Circuit).

ASIC is an integrated embedded hardware that has a capability of switching millions of packets per second with many more features such as buffering of data packets.

Switch:

Function of switch:

1. Learning: Switch learn the MAC address of connected devices and store it in the CAM (Content Addressable Memory) table
2. Forwarding: Switch forward the packet according to the given network address in the network.
3. Preventing layer 2 switching loops: Switch is a intelligent device. So it also prevents switching loops in the network.

Switch:

Three modes of switching are:

1. Cut through:

In this mode, switch start forwarding packet before receiving complete frame.

It just check the destination address and start forwarding packet without detecting error in frames

Switch:

Three modes of switching are:

2. Store-and-forward:

The switch starts forwarding the packet after receiving complete frame.

High latency will occur and latency is decided by frame length.

Switch checks the complete frame and if error is detected then the complete frame is discarded.

Switch:

Three modes of switching are:

3. Fragment-free:

In this mode, length of received bits is described i.e. 64 bits

After receiving first 64 bits, switch start forwarding the packet without receiving complete frame.

Switch check the 64 bits for error and if error find switch will drop the packet.

This will reduce the latency in network.

Spanning Tree Protocol Part 1

Content:

1. Spanning Tree Protocol
2. How switching loop occur in network?
3. Problem caused by switching loop
4. STP terms
5. Switch Port Status

Switch

Spanning Tree protocol:

The Spanning Tree Protocol (STP) is a network protocol that builds a logical loop-free topology for any switched Ethernet local area networks. The basic function of STP is to prevent switching loops and the broadcast radiation.

Spanning tree also allows a network design to provide backup paths if any active link fails in the network.

STP was invented by Radia Perlman while working for Digital Equipment Corporation.

IEEE 802.1D is a standard of STP

Switch:

How switching loops occur in network?

- A Switching loop occurs in computer networks when there is more than one Layer 2 (OSI model) path between two endpoints or between two network switches.
- The interconnected network is design to reduce the redundancy.
- But this interconnected result into formation of loops.
- The loop creates broadcast storms as packets are forwarded by switches to every port, the switches will repeatedly re-broadcast the broadcast messages result into flooding of network.

Switch:

How switching loops occur in network?

- As Layer 2 device i.e. switch does not support a header called time to live (TTL) value, if a frame is sent into a looped topology, it can loop forever.
- The solution is to allow the formation of physical loops, but create a loop-free logical topology using spanning tree protocols (STP) on the network switches.
- Example explaining switching loop

Switch:



Switching Loop

Switch:

Problems caused by switching loops:

1. Broadcast storm:

Broadcast storm is a situation in which the packets are broadcast over a switching loop. This form an endless loop.

2. MAC address Flapping:

A loop can make a switch to receive the same broadcast message on two different ports which cause misleading entries in a switch's MAC database. This process is known as MAC address Flapping

3. Multiple frame transmission:

Switch will receive a copy of frame from two different port.

Switch:

Spanning tree protocol is used to prevent the network from switching loops

STP terms:

- Root switch: is a switch with a best bridge ID or Switch ID. All decision in the network is taken by root switch.
- Bridge ID/Switch ID: It is formed with the combination of switch priority and the switch MAC address. The switch with the lowest switch ID become the root switch in the network.

Switch:

STP terms:

- Root port: it is the nearest port from the root switch and always remain in forwarding state.
- Designated port: a designated port is one that has been determined as having the best i.e. lowest cost. A designated port will be a forwarding port.
- Alternate port: it act as backup port and it cannot forward any data to network segment it is connected to.

Switch:

STP terms:

- BPDU packet: Bridge Protocol Data Unit are used by all switch in the network to exchange information related to the selection of root bridge, root port and designated port etc.

Switch:

Switch Port Status:

- Disabled Port: only learn MAC addresses and calculate STP
- Listening Port: Receive and send BPDU packets only.
- Blocking Port: Receive and deal with BPDU packet but not send BPDU packet.
- Learning Port: Learn MAC address, calculate STP, receive and send BPDU packets
- Forwarding Port: Forward data, learn MAC address, calculate STP, receive and send BPDU packets.

Spanning Tree Protocol Part 2

Content:

1. Concept of Spanning Tree Protocol
 - o STP Convergence
 - o Four Step Decision Sequence

Switch:

Concept of Spanning Tree Protocol:

The STP run in the network by default. Whenever a loop occur in network STP make the one port of switch in blocking state.

STP convergence:

1. As STA run, it select one of the switch as **Root Switch** from the network.
2. Then **Root port** is selected on the basis of lowest cost path.
3. Then **Designated port** is selected.

Switch:

STP decisions is based on a the following sequence:

Four-Step decision Sequence

Step 1 - Lowest Bridge ID/Switch ID

Step 2 - Lowest Path Cost to reach Root switch

Step 3 - Lowest Priority of Switch

Step 4 - Lowest Port ID

Switch:



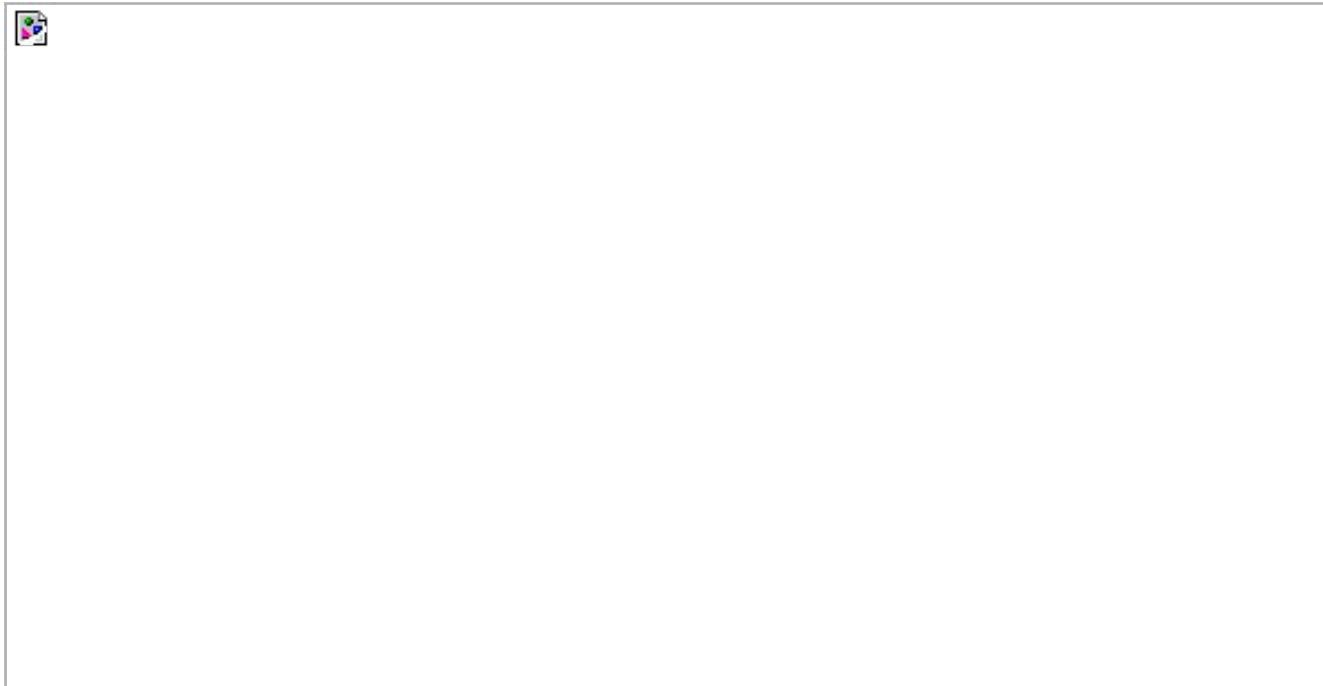
Spanning Tree Protocol

Switch:

Step 1: Selecting Root Switch:

- When the network first starts, all switches start sending the BPDU packet.
- All switch immediately begin applying the four-step sequence decision process.
- Switches need to elect a single Root Switch in the network.
- All 3 switches have the same default switch Priority value of 32,768.
- Switch with the lowest Bridge ID/Switch ID wins.
- This is known as the "Root War."

Switch:



Selecting Root Switch

Switch:

Step 2: Selecting Root port:

- After winning Root war, switches move on to selecting Root Ports.
- A switch Root Port is the port closest to the Root Switch.
- Switch use the path cost to determine closeness.
- IEEE define the cost of using every path in network.
- Every non-Root switch will select one Root Port.
- Selected switch as root port will remain in forward state.

Switch:



Selecting Root Port

Switch:

Step 3: Selecting Designated Port:

- After selecting root port, switch start finding designated port.
- Designated port is a port that has been determined as having the best i.e. lowest cost. A designated port will be a forwarding port.
- Designated port is selected by determining the lowest path cost.
- If path cost is same in links then switch repeat the four step sequence.
- In such way, ports are selected which are not in use and are put in blocking state.

Switch:



Selecting Designated Port

VLAN

Content:

1. VLAN
2. Benefits of VLAN
3. VLAN Ports
4. Type of VLAN
5. Configuring VLAN Network
6. VLAN terms
7. Advantage and Disadvantage of VLAN

VLAN:

Virtual Local Area Network is a single physical broadcast domain which is made up of two or more switches and is divided into multiple logical broadcast domain.

VLAN network is a partitioned and isolated computer network at the data link layer (OSI layer 2)

It allow network administrators to partition their networks to match the functional and security requirements of their systems.

VLAN is created using logical connection instead of Physical connection.

802.1Q is the standard which define VLAN.

VLAN:

Traffic between two VLAN cannot pass directly. Router or layer 3 device is used to interconnect two switches or VLAN.

VLAN membership can be done using software to group various host together.

VLAN ID or VID is of 12 bit it means 4094 different VLANs can be created for same network.

VLAN:



LAN Segmentation

VLAN:



VLAN Segmentation

VLAN:

Benefits of VLAN:

1. Increased Network Performance
2. Improved Network Manageability
3. Simple Software Configuration
4. Improved Security Options

VLAN

Type of VLAN ports:

1. Access Port: It is used to connect the user host or devices and it can connect to only the access link.
2. Trunk Port: It is used to connect to other switches and it can connect to only the trunk link.
3. Hybrid port: It is used to connect to either hosts or switches. It can connect to either the access link or the trunk link. A hybrid port allows frames from multiple VLANs to pass through.

VLAN:

Type of VLAN:

1. As Port Based VLANs
2. As Tagged VLANs

VLAN:

1. As Port Based VLANs:

In port-based VLANs, a single physical switch is simply divided into multiple logical switches.

As shown in the example the division of an eight-port physical switch (Switch A) into two logical switches.

VLAN:



Port based VLAN

VLAN:

Let take an example , the switch B is configured in another location with same configuration as A.

So to make communication possible between these two switch i.e switch A and switch B.

A two wires are required to connect the these two switch.

- One cable from Switch A Port 4 to Switch B Port 4 (for VLAN 1)
- One from Switch A Port 8 to Switch B Port 8 (for VLAN 2)

VLAN:



Port based VLAN

VLAN:

2. As Tagged VLAN:

In tagged VLANs, multiple VLANs can be used through a single switch port.

Tag contains the respective VLAN identifiers

These identifiers indicates that to which VLAN the frame belongs.

By checking the ethernet frames, the VLAN network is identified.

Connection of both VLANs to both physical switches done by using a single cable.

VLAN:



Tagged VLAN

Configuring a VLAN Network:

Steps to create VLAN network:

1. Log in into the switch using SSH.
2. Use CLI or GUI tool to enter the command for configuration.
3. Then define a VLAN network.
4. After creating VLAN then assign ports to the each VLAN (VLAN assignment)

VLAN:

Trunking:

It is a process transferring VLAN traffic between two or more switches.

A port is configured known as trunk port to perform trunking.

Trunk port is a port configured on switch to carry all traffic regardless of VLAN number between all switch in the LAN.

VLAN trunking Protocol:

This protocol is used to update multiple switch in the VLAN network

VLAN:

Multilayer Switch:

A switch which works at Layer 2 and Layer 3 of an OSI model is known as Multilayer switch.

It is a switch which work both as router and switch.

Type of ports are mentioned i.e. Router ports and Switch ports to differentiate the functioning of multilayer Switch.

Inter VLAN Routing:

The process of making a router work between two VLANs is called Inter VLAN Routing.

VLAN:

Advantages:

Broadcast Control

High performance network

Reduce Traffic

Security

Disadvantages:

Configuration and management of network is complex

VLAN limit - only create 4094 VLANs in one network

DNS

Content:

1. DNS
2. Naming Technology before DNS
3. DNS Server
4. DNS Terms
5. How DNS Server work?
6. Dynamic DNS Server
7. DNS Security Extension

DNS:

Domain Name System (DNS) is a powerful, extensible and flexible system used for resolving names over an entire internet.

Domain Name System is a name resolution protocol.

This protocol converts computer's name to IP addresses. DNS uses TCP port 53 and UDP port 53.

So, this makes it easier for people to remember the words rather than numbers.

For example, As we want to open a web page, we type www.google.com instead of typing its IP address as `http://216.58.196.14`

Before DNS:

Before DNS, a protocol is developed by Microsoft named as NetBIOS/NetBEUI.

This Protocol is popularized as a light and effective naming protocol.

This protocol use broadcast concept for resolving names.

Whenever a computer booted up, it broadcast its name along with its MAC address in a network.

Then every NetBIOS/NetBEUI system heard the message and stored the information in a cache.

This naming protocol works in a small network

Before DNS:

Drawback of NetBIOS/NetBEUI:

- It doesn't understand IP addresses. It only convert system name's to their MAC addresses.
- As it include broadcast concept so, it is not used in a large network.
- This protocol was only invented to share folders and printer in the network.

DNS Server:

DNS server is a collection of computers registered to join domain name system. They work as a team and collectively known as DNS root servers.

The internet name of this computer team is “.” (“dot”).

DNS servers are organized in a hierarchical form.

DNS root servers are the top level domain servers which include top level domain name such as com, org, net, edu and gov etc.

It includes a complete database of internet domain names and their corresponding IP addresses.

DNS Server:

There are 13 root servers setup by internet out of which 10 are reside in US, 1 in japan , 1 in London (UK) and 1 in sweden.

Low level DNS servers are owned by businesses and Internet service Provider (ISP).

DNS Terms:

1. Domain Namespace:

The naming system on which DNS is based is a hierarchical and imaginary tree structure called the domain namespace.

It includes all the possible names that could be used within a single system.

Each node in the DNS tree represent a DNS name.

Domain Namespace:



DNS Terms:

2. Name Server:

It include:

DNS name server: A name server is a computer that has DNS software installed on it. It is specifically designed for managing the different domain names.

Zone: is a container which holds the records of a single domain.

Record: is a line in a data contained by zone which maps an FQDN (fully qualified domain name) to an IP address.

DNS Terms:

2. Name Server:

A simple network has one DNS server for entire network.

A single domain name can use more than one DNS server. For example: google.com is a busy domain so it need multiple DNS servers to support all the incoming DNS queries.

DNS Terms:

3. Name Resolution:

Name Resolution means successfully mapping a DNS domain or hostname to an IP address.

DNS can resolve name in three ways:

- By Broadcasting (Small Network)
- By locally consulting the locally stored hosts text file.
- By contacting a DNS server.

How DNS Server works?:



How DNS Server works?

DNS act as the central part of internet, as it provide a way to match website name or computer name to their IP addresses.

1. A user type the name of website in search engine. Which generate a query and is send over the internet.
2. Let suppose the user query first goes to the recursive resolver (which is operated by its ISP)
3. The recursive resolver know where to send the query in the network.
4. Then recursive resolver talk with the root DNS server about the IP address of website.
5. Then root DNS server search for its particular top level domain(TLD) by analysing the domain name of website.

How DNS Server works?

6. Query is send to the particular TLD. where TLD servers stores the address information for second level domains within TLD.
7. Then TLD server gives the IP address of particular DNS which knows about the IP address of website to the recursive resolver.
8. Then recursive resolver sends the query to the DNS. As DNS know about the IP address of full domain. It tells the IP address of the website.
9. Recursive resolver send IP address of website to user. Thus website appears.
10. Now user can browse the website and retrieve the content using IP address

Dynamic DNS Server:

TCP/IP developed a new protocol known as Dynamic DNS (DDNS) in 1997

It is a method of automatically updating the computer IP address or namespace in the Domain Name System.

DDNS is a system that basically addresses the problem of rapid updates.

DNS Security Extension:

DNS security extension (DNSSEC) is an authentication and authorization protocol to provide security to DNS server.

The DNSSEC is a suite of Internet Engineering Task Force (IETF) specifications.

Security are added to protect DNS from unauthorized user.

DNSSEC is implemented through (Extension mechanism for DNS) EDNS

IEEE 802.11

Content:

1. Wireless Technology
2. Wireless Standard (IEEE 802.11)
 - o Working modes
 - o Radio Frequency used
 - o Spread Spectrum Techniques
 - o Channel used
 - o CSMA/CA

Wireless Technology:

Wireless Technology is a technology which uses radio waves to transmit and receive data and voice.

It is basically used for the transmission of data.

Wireless communication was developed in 19th century.

IEEE 802.11-1997 is a first wireless networking standard.

Example of wireless technology: cell phones, satellite communication, Wi-Fi, Bluetooth, Zigbee etc

Wireless Standard (IEEE 802.11):

802.11 is a wireless standard developed in 1997 by IEEE.

IEEE 802.11 standard defines two things about wireless communication:

- How wireless device communicate?

- How to make this communication secure?

It also define frequencies used by radio signals, their transmission methods and collision avoidance technique.

IEEE 802.11 is not used now as it's updated versions are developed such as IEEE 802.11g and IEEE 802.11ac etc.

IEEE 802.11

Wireless Network working modes of IEEE 802.11 standard:

1. Ad-Hoc Mode
2. Infrastructure Mode

IEEE 802.11

Ad-Hoc mode:

Ad-Hoc Mode define a direct connection of two or more devices.

It is also known as peer-to-peer mode.

Ad-Hoc network use mesh topology to connect devices in wireless network.

Ad-Hoc mode form IBSS i.e Independent Basic Service Set.

IBSS is a basic unit of organization in wireless network.

Ad-Hoc mode is used to connect devices in small network where main purpose is to transfer files and share printer.

IEEE 802.11



Ad-Hoc mode Wireless Network

IEEE 802.11

Infrastructure Mode:

Infrastructure mode use one or more WAP (Wireless Access Point) to connect the wireless devices centrally.

The configuration of this mode is similar to star topology of wired network.

Basic Service Set (BSS): BSS is an area having a single WAP and devices are connected to it.

Extended Service Set (ESS): ESS is form by extending BSS area by adding more WAP.

It provide a stable environment for permanent wireless network installation.

IEEE 802.11

Identifiers used in infrastructure mode:

1. SSID: Service Set Identifier is a standard name given to BSS or IBSS.

It is a 32 bit identification string inserted into header of each frame processed by WAP.

2. ESSID: Extended Service Set Identifier standard name given to ESS network.

Client in a ESS network will connect to a WAP having strong signal.

IEEE 802.11



Infrastructure Mode Wireless Network

IEEE 802.11

Spread Spectrum Techniques:

IEEE 802.11 use three different spread spectrum techniques:

1. Direct Sequence Spread Spectrum (DSSS)
2. Frequency Hopping Spread Spectrum (FHSS)
3. Orthogonal Frequency Division Multiplexing (OFDM)

IEEE 802.11

1. Direct Sequence Spread Spectrum:

It also known as direct sequence code division multiple access.

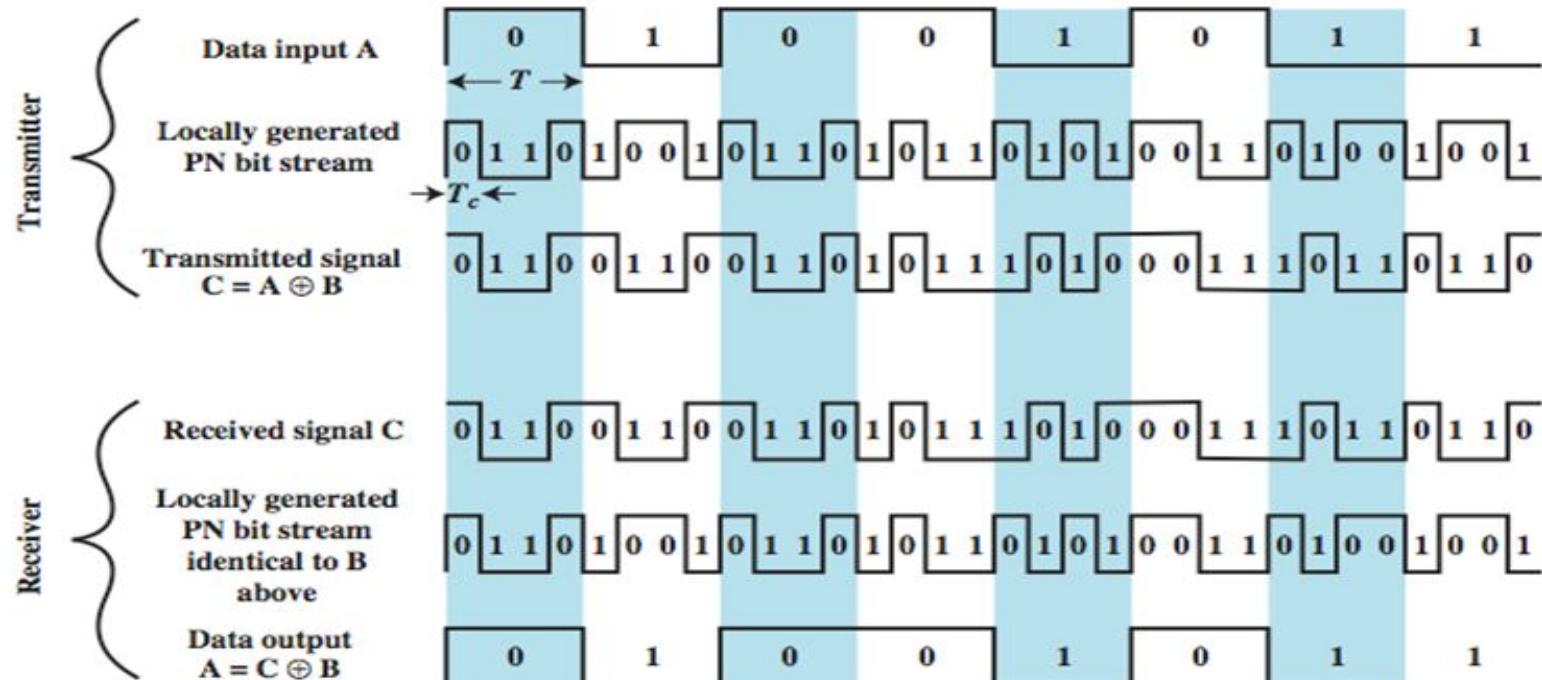
Spreading code or PN code is assigned to a every user.

Spreading codes consist of specific sequence of bits known as chips.

The PN codes are multiplexed with original message and resultant message is then transmitted.

Transmitter and receiver have same PN codes.

IEEE 802.11



Direct Sequence Spread Spectrum

IEEE 802.11

2. Frequency Hopping Spread Spectrum:

Multiple frequency is used for sending packets in the network.

Every user use different frequency at different time.

Frequency of carrier is periodically modified following a specified sequence of frequency.

This sequence is known as hopping sequence.

IEEE 802.11



Frequency Hopping Spread Spectrum

IEEE 802.11

3. Orthogonal Frequency Division Multiplexing:

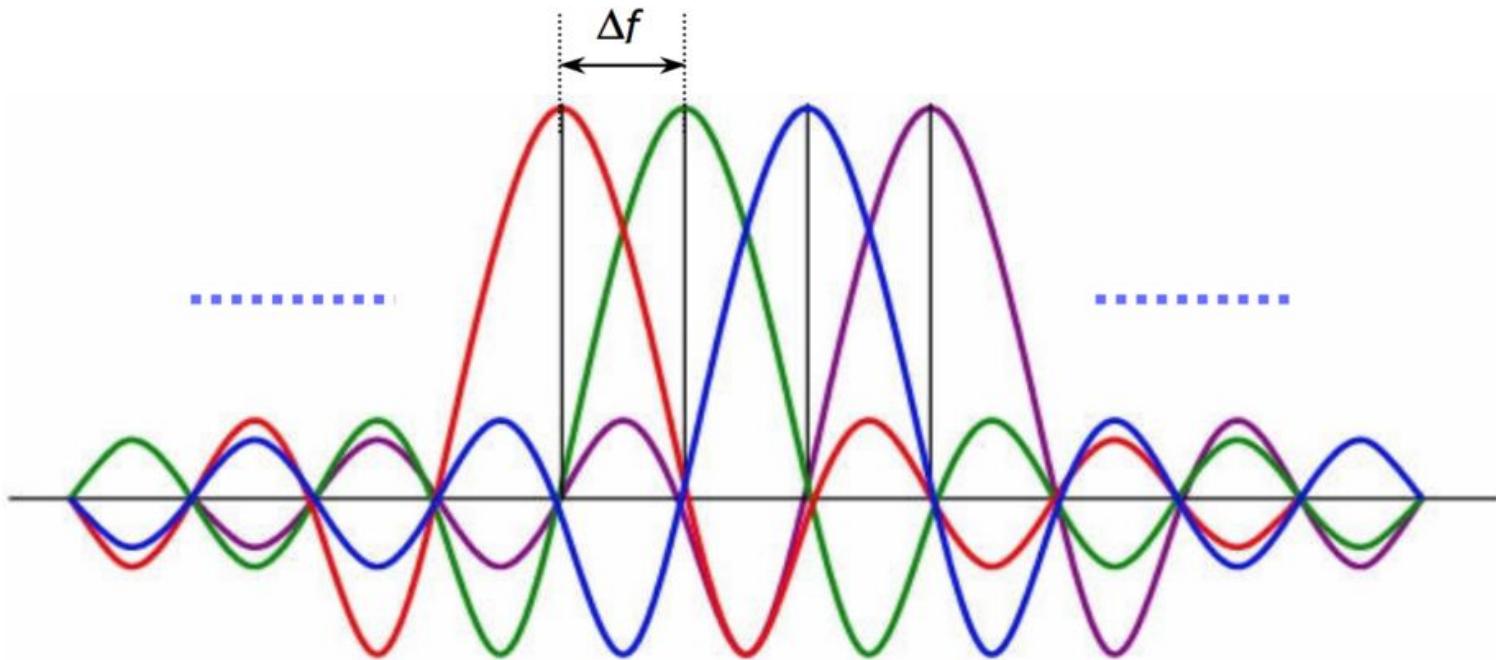
In OFDM a large no. of closely spaced orthogonal sub-carrier are used to carry data of several user.

This spacing provide the orthogonality.

Each subcarrier is modulated with a conventional modulation scheme such as quadrature amplitude modulation or phase-shift keying.

This significantly improve the spectral efficiency.

IEEE 802.11



Orthogonal Frequency Division Multiplexing

IEEE 802.11

Channels allocated for wireless network are:

1. 2.4 GHz Band it define 14 channels of 20 MHz

Most of the WAP use 1, 6 and 11 channel by default because these are non overlapping channels.

2. 5.0 GHz band define 40 different channels

It use concept of 'automatic channel switching' to reduce overlapping.

IEEE 802.11

CSMA/CA:

Wireless Network use CSMA/CA technique i.e. Carrier Sense Multiple access/Collision Avoidance.

Wireless devices doesn't detect collision in the network because:

- Wireless communication use half duplex transmission method.
- If two wireless devices packets collide, then there is no simple-to-detect electrical peaks method like there with wired network.

IEEE 802.11

CSMA/CA:

IEEE 802.11 standard define two methods for collision avoidance:

1. Distributed Coordination Function (DCF)
2. Point Coordination Function (PCF)

Wireless Standards

Content:

1. Wireless Standards
 - o IEEE 802.11
 - o IEEE 802.11b
 - o IEEE 802.11a
 - o IEEE 802.11g
 - o IEEE 802.11n
 - o IEEE 802.11ac

Wireless Standards

1. IEEE 802.11

Developed in 1997

2.4GHz frequency band is used.

Spread spectrum technique used is Direct Sequence Spread Spectrum or Frequency Hopping Spread Spectrum.

Range up to 300 feet.

Support speed up to 2mbps.

Wireless Standards:

2. IEEE 802.11b

Support data rate upto 11 mbps.

Range up to 300 feet.

Spectrum used Direct Sequence Spread Spectrum.

Use 2.4GHz frequency (interference).

It is widely adopted standard.

Wireless Standards:

3. IEEE 802.11a

Use frequency band 5.0GHz.

Support speed up to 54mbps.

Range up to 150 feet.

Spectrum used Orthogonal Frequency Division Multiplexing.

Wireless Standards:

4. IEEE 802.11g:

Frequency band used is 2.4GHz.

Orthogonal Frequency Division Multiplexing technique is used.

Its range lies up to 300 feet.

Support speed up to 54 mbps.

Compatible with IEEE 802.11b.

Wireless Standards:

5. IEEE 802.11n:

Frequency band used either 2.4GHz or 5.0 GHz.

It follows Orthogonal Frequency Division Multiplexing technique.

Speed up to 600mbps.

It transmits signal in three different ways: Legacy, Mixed and Greenfield.

Compatible with IEEE 802.11b/g/n.

It implements new features known as Multiple input multiple output (MIMO).

Wireless Standards:

6. IEEE 802.11ac:

Use 5GHz frequency band.

Spread Spectrum technique used is orthogonal frequency division multiplexing.

Support speed up to 1gbps.

Compatible with 802.11a.

It include new feature named as Multiuser MIMO (MU-MIMO).

WLAN

Content:

1. WLAN
2. Wireless Network Devices
 - o Wireless Access Point (WAP)
 - o Wireless NIC
 - o Antennas

WLAN:

A wireless local area network (WLAN) is a wireless computer network that connect two or more devices using a wireless techniques.

Its range is limited to an area such as a home, school, computer laboratory and office building.

WLANs are based on IEEE 802.11 standard.

Type of Wireless LAN:

1. Infrastructure Mode WLAN
2. Ad-Hoc Mode WLAN

WLAN:

Advantage of WLAN network:

1. Flexible Network
2. Portable
3. Offer Mobility
4. Ease of installation

Wireless Network Devices:

1. Wireless Access Point (WAP):

Wireless access points are special-purpose communication devices used in WLAN.

It act as a central transmitter and receiver of wireless radio signals.

It interconnect the wireless devices.

For example: Router

Wireless Network Devices:

2. Wireless NIC:

A wireless NIC is a network interface controller which connects to a wireless radio-based computer network.

A WNIC works on the Layer 1 and Layer 2 of the OSI Model.

This card uses an antenna to communicate via microwave radiation.

WNIC is installed within computer.

Wireless Network Devices:

3. Antennas:

Type of antenna used are:

- Omnidirectional Antenna
- Unidirectional Antenna
- Patch Antenna

Wireless Network Devices:

3. Antennas:

- Omnidirectional Antenna:

Omnidirectional Antenna radiates the radio frequencies to all the direction.

Example of omnidirectional antenna is dipole antenna which has two radiating elements that point in opposite direction.



Wireless Network Devices:

3. Antennas:

- Unidirectional Antenna:

Unidirectional antennas radiates the radio signals in particular direction.

Example of unidirectional antennas are Parabolic Antenna, Yagi Antenna (Beam Antenna), Dish Antenna etc.



Wireless Network Devices:

3. Antennas:

- Patch Antenna:

Patch Antennas are flat, plate shaped antenna that generate a half sphere beams.

This antennas are placed on walls.



Wi-Fi Security

Content:

1. Wi-Fi Protected Setup
2. Wi-Fi security
 - o MAC address Filtering
 - o Authentication
 - o Encryption

Wi-Fi Protected Setup (WPS):

Wi-Fi Protected Setup is a standard which is used to provide security to a wireless devices.

WPS adopt two method to provide security:

1. Push Button Method
2. PIN Method

Wi-Fi Security:

IEEE 802.11 uses three methods to provide security to Wi-Fi:

1. MAC Address Filtering
2. Authentication
3. Encryption

Wi-Fi Security:

1. MAC Address Filtering:

In this method, the MAC address of various devices are entered in the table of Wireless Access Point (WAP).

WAP provide service access to those devices whose MAC address is stored in WAP list.

This method is used to limit the access of their network.

Wi-Fi Security:

1. MAC Address Filtering:

WAP use ACL (Access Control list) to enable and disable the specific MAC address.

This method is enabled in small network.

MAC filtering is done on the basis of whitelist and blacklist.

Wi-Fi Security:

2. Authentication:

For providing authentication in wireless network, a standard is used named as IEEE 802.11i.

IEEE 802.11i defines both authentication and encryption using IEEE 802.11X std.

It allows the network user to create authentication using a RADIUS server and encrypt the password using Extensible Authentication Protocol (EAP).

RADIUS server stores user name and password created by the user of WAP.

Wi-Fi Security:



Authentication

Wi-Fi Security:

2. Authentication:

How user is authenticated?

1. There are 3 components in the wireless network such as
 - o Client wireless device,
 - o Network access Server(NAS) or WAP,
 - o RADIUS server
2. Client contact the WAP or NAS to provide permission to access the network.
3. Then NAS collect the username and password entered by client and contact the RADIUS server.

Wi-Fi Security:

2. Authentication:

How user is authenticated?

4. Then RADIUS server see if the client's username and password is correct or not.
5. If the entered values are correct then RADIUS server send packet back to client through the WAP with an Access Accept code.
6. Thus remote user get access to the WAP network

Wi-Fi Security:

3. Data Encryption:

Data Encryption is used to do encryption of packets floating or routed in wireless network.

Encryption is done by using private and public cryptographic keys.

Methods of Data Encryption:

1. Encryption using WEP
2. Encryption using WPA
3. Encryption using WPA2

Wi-Fi Security:

3. Data Encryption:

- Encryption using WEP:

WEP stands for Wired Equivalent Privacy.

This method is a granddaddy of wireless security.

It uses 64-, 128-bit encryption algorithm.

Drawbacks :

1. WEP requires Initialization vector.
2. Encrypted keys are both static and shared.
3. It provides authentication only on the basis of MAC address.

Wi-Fi Security:

3. Data Encryption:

- Encryption using WPA:

Was designed to overcome the limitation of Encryption using WEP.

WPA stands for Wi-Fi Protected access.

The encryption keys are dynamic and integrated.

WPA add extra layer for security called TKIP (temporal key integrity protocol)

Wi-Fi Security:

3. Data Encryption:

- Encryption using WPA2:

WPA2 stands for Wi-Fi Protected Access 2.

It completely follows IEEE 802.11i standard.

It uses Advanced Encryption Standard (AES), a 128 bit block cipher.

WPA2 encryption is done by using simple version WPA Personal Shared key (WPA-PSK or WPA2-PSK).

Installing & Troubleshooting Wi-Fi

Content:

1. Steps to install the Wi-Fi
2. Steps to troubleshoot Wi-Fi

Installing Wi-Fi:

Steps required to install Wi-Fi networks are:

1. Proper Site Survey
2. Use Wireless analyzer: generating Heat maps.
3. Detect interference Sources and find solution to reduce interference. (kill dead spots in a network)
4. Setting up of an network:
 - o Ad-Hoc mode wireless network
 - o Infrastructure mode wireless network
5. Installing Access Points (WAP) and Antennas.

Installing Wi-Fi:

Steps required to install Wi-Fi networks are:

6. Configure the Access Points:
 - a. Set its SSID (ESSID) and configure MAC address Filtering
 - b. Set up the Encryption Settings
 - c. Set Channels and frequency acc to network need
7. Configure Client
8. Adding of more WAP's (Wireless Bridge)
9. Verify the installation

Troubleshooting Wi-Fi:

Problems occur in Wi-Fi connections and solution of solving such issues:

1. Low signal/Power: If WAP signal/power quality become low. To troubleshoot this problem , solution are like
 - Covering WAP range
 - Avoid Dead zones
 - Turn up the power
 - use better antenna
 - upgrade new 802.11 standard.
2. Wrong Encryption: Entering wrong encryption key (username and password)

Troubleshooting Wi-Fi:

Problems occur in Wi-Fi connections and solution of solving such issues:

3. Problem in allocating Channels: This issue occurs when WAP is configured with 2.4GHz frequency band. If WAP channels are set using neighbouring channels. This will lead to overlapping of signals.

To solve this problem choose channel such as 1,6 and 11. Or set device to 'auto channel selection' mode.

4. Slow connection: this issue is difficult to resolve.

In this problem, device is connected to SSID or IP address of WAP but data transfer is low i.e. web page load slowly or application timeout

Troubleshooting Wi-Fi:

Problems occur in Wi-Fi connections and solution of solving such issues:

4. Slow connection: This problem occur due to:

- Overloaded WAP
- Radio frequency interference (RFI)
 - RFI from non Wi-Fi network
 - RFI from Wi-Fi network

Solution to this issue is to disconnect some devices from WAP network and reduce interference.

Troubleshooting Wi-Fi:

Problems occur in Wi-Fi connections and solution of solving such issues:

5. Unusual connection: in this issue, WAP provide a good connection but there is problem on the basis of security
 - Open network: These are the network having no encryption configured (no username and password). There's a problem with this network to how to avoid unintentional login and there is no data encryption.
 - Wrong SSID: user is attached to fake network having SSID similar to that of real network.
 - Untested Updates
 - Rogue Access Point (Rogue AP): are unauthorized access point.

Troubleshooting Wi-Fi:

Problems occur in Wi-Fi connections and solution of solving such issues:

6. Bluetooth: an amazing wireless technology with plenty of good security.

Tools used for providing security are:

- Discoverable mode
- Four digit PIN during pairing process

Attacks in Bluetooth technology:

- Bluejacking
- Bluesnarfing

Troubleshooting Wi-Fi:

Problems occur in Wi-Fi connections and solution of solving such issues:

7. War Driving and War Chalking: One of the old technology used by hacker in late 2005.

War Driving was conducted to find the wireless network using omnidirectional antennas.

When a network was found the war driver mark that place with special chalk mark to indicate other war driver about the location of SSID.

Connection in WAN

Content

1. Connection in WAN
 - T Carrier connections (T1 , T3)
 - Fiber (SDH, SONET)
 - Packet Switching Protocols (Frame Relay, ATM, MPLS)

T Carrier Connection:

T carrier:

It is a series of wideband digital data transmission formats developed by the Bell System and commonly used in North America and Japan

T carriers are the dedicated high speed line.

The basic unit of T carrier is DSO which convert the analog sound/signal into 8 bit chunks.

DSO transmission rate is 64kbps.

T Carrier Connection:

T carrier level 1:

T1 is a dedicated phone line that are leased by various offices usually on monthly basis.

T1 line use special signalling method called digital signal 1 (DS1).

DS1 is a primitive frame consist of 25 pieces i.e. 1 framing bit and 24 channels.

Each DS1 channel holds a 8 bit DSo data sample. So, framing bit (1 bit) plus data channel (24×8 bit) will give 193 bits per DS1 frame.

DS1 frame is transmitted at 8000 times/sec giving speed of 1.5mbps.

T Carrier Connection:

T Carrier level 3:

Upgrade version of T1 lines

It is also known as Digital Signal 3 (DS3) line.

It support data rate up to 45mbps.

T3 lines are consist of 672 individual DS0 channel.

It is used by ISP to connect to internet and regional telephone offices.

T Carrier Connection:



T carrier /E carrier line

T Carrier Connection:

Channel Service Unit/Digital Service Unit (CSU/DSU):

CSU/DSU is a link point which goes from phone company to a customer equipment.

It performs functions like encoding of data and also used for loopback testing.

It consists of connector used to connect leased T1 or T3 lines.

It also protects user equipment from lightning strikes and other electrical interference.

Fiber:

Fiber cables are basically designed for long distance communication.

A fiber optic cable is made from strands of glass fibers that uses pulses of light to transfer data.

First standard for Fiber optic cables are SONET and SDH.

SONET and SDH are standardized protocols that transfer multiple digital bit streams synchronously over optical fiber.

These standards replace the PDH standard used in earlier telephone system.

Fiber:

SONET:

- Developed by US through ANSI T1X1.5 committee.
- It is a subset of SDH
- Basic unit is Optical Carrier level 1 (OC1) with a speed of 51.84mbps.
- Type of optical carrier are OC-3, OC-12, OC-18, OC-24, OC-36, OC-48, OC-96 and OC-192.

SDH:

- Developed by ITU.
- Basic unit is Synchronous transfer module (STM-1) with a speed of 155.52mbps.
- Type of STM are STM-1, STM-4, STM-16 and STM-64.

Packet Switching Protocol:

Fiber cables use Packet Switching concept to route the packet in the network

First generation of packet switching protocol is X.25 developed by CCITT.

Forms of packet switching protocol are:

- Frame Relay
- Asynchronous Transfer Mode (ATM)
- Multiprotocol label Switching (MPLS)

Packet Switching Protocol:

1. Frame Relay:

Frame Relay is a fast and efficient packet switching technology with low chance of transmission errors

Design to use with T-carrier line.

Frame Relay connect local area networks (LANs) with wide-area networks (WANs).

Work at layer 2 of an OSI model.

Frame Relay was designed to transmit data as quickly as possible over low error networks

Packet Switching Protocol:

2. Asynchronous Transfer Mode (ATM):

ATM carry user traffic such as voice, video and data on one connection.

It work at Layer 2 of an OSI model.

Network technology was designed for high speed LAN but most commonly used in WAN.

Earlier it was used in SONET network but now MPLS is used.

ATM is the core protocol used in PSTN and ISDN.

Packet Switching Protocol:

2. Asynchronous Transfer Mode (ATM):

ATM can support a speed of 155.52mbps to 622.08 mbps.

ATM use asynchronous time division multiplexing.

It encode data into short and fixed length cells (53 bytes).

ATM can support different transfer speed and requirement.

Packet Switching Protocol:

3. Multiprotocol Label Switching (MPLS):

MPLS is a type of data-carrying technique used for high performance networks.

MPLS is a scalable, protocol-independent transport.

Data packets are assigned labels. Packet is routed according to assigned label rather than accessing complete network address.

It replace the frame relay and ATM method.

MPLS work at layer 2 and layer 3 of an OSI model.

Packet Switching Protocol:

3. Multiprotocol Label Switching (MPLS):

MPLS can encapsulate packets of various network protocols including T1/E1, ATM, Frame Relay, and DSL.

MPLS header consist of 4 parts:

- Label
- Cost of Service (CoS)
- Single Packet (S)
- Time to Live (TTL)

Packet Switching Protocol:

3. Multiprotocol Label Switching (MPLS):

Forwarding Equivalence Class (FEC): is a group of devices that send packet in single broadcast domain.

Label Switching Router (LSR): forward packet on the basis of MPLS label

Label Edge Router (LER): it add MPLS label to a packet that don't have a label.

Label Distribution Protocol (LDP): LSR and LER use LDP to communicate about their dynamic state.

Telephone lines & WWAN

Content:

1. Telephone Lines:
 - o Dedicated line
 - o Dial-up line
2. WWAN
3. Satellite
4. BPL

Telephone Lines:

Dedicated Lines:

Also known as non-switched line.

Permanent and hardwire connection between two endpoints.

It is a type leased line rented from telephone company.

Having no phone numbers.

Example: DSL

Dial-up Lines:

Also known as switched lines.

Temporary connection

Connection can be initiated manually or automatically.

Having phone numbers.

Example: PSTN , ISDN

Telephone Lines:

Public Switched Telephone Network (PSTN):

Old and slow technology.

Also known as Plain Old Telephone Service (POTS).

PSTN is a phone line used to connect landline phones with a baud rate of 2400.

Local Exchange Carrier (LEC) is a telephone company or exchange which connect the PSTN users with local office.

Interexchange Carrier (IXC) is exchange providing long distance service.

Telephone Lines:

Public Switched Telephone Network (PSTN):

Phone lines are used to transmit voice and data.

CCITT established standards for modems called V Standards.

V standards define the modem speed.

Current version is V.92 offering speed of 57,600bps.

ITU establish standard which define how modem compress data and perform error checking.

Telephone Lines:

Integrated Services Digital Network (ISDN):

Support Digital transmission of data and voice signals over different line.

It consist of two type of channels: Bearer Channel (B channel) and Delta channel (D channel)

Basic Rate Interface (BRI) setup contain 1 D channel and 2 B channels.

Primary Rate Interface (PRI) setup carry 23 B channels and 1 D channel over T1 line.

Service Profile Identifier (SPID) is a no. that indicate a specific ISDN line.

Telephone Lines:

Digital Subscriber Line (DSL):

DSL is a fully digital and dedicated connection.

It support both data and voice signal over same DSL line.

DSL Access Multiplexer (DSLAM) is a device that connects the multiple user to internet.

Data over cable service interface specification (DOCSIS) is a protocol that define internet access through cable modem.

Current version is DOCSIS 3.1

Telephone Lines:

Asymmetric Digital Subscriber Line (ADSL):

- Different upload and download speed.
- Less expensive
- Download speed 15 mbps and upload speed 1 mbps.
- Range of speed provided by ADSL are:

384 kbps D / 128 kbps U

1.5 mbps D / 384 kbps U

6 mbps D / 768 kbps U

Symmetric Digital Subscriber Line (SDSL):

- Same upload and download speed.
- Expensive
- Support 15 mbps speed.
- Range of speed provided by SDSL are: 192 kbps, 384 kbps, 768 kbps, 1.1 mbps and 1.5 mbps

WWAN:

It is also known as Cellular WAN (Cellular wide area network)

A WWAN use mobile telecommunication cellular network technologies such as LTE, WiMAX, UMTS, CDMA2000 and GSM to transfer data.

Cellular WAN also use Local Multipoint Distribution Service (LMDS) or Wi-Fi to provide Internet access.

These technologies are offered regionally, nationwide, or even globally by a Internet service provider.

WWAN:



WWAN:

Satellite communication:

Satellite communication is used in distant area such as hilly areas.

Satellite communication is of two type:

- One way communication
- Two way communication

Broadband over Powerline (BPL):

This service enable internet access through the electrical power grid.

Remote Access & Troubleshooting

Content:

1. Remote Access in WAN
 - o Dial up connection to internet
 - o Dial up connection to private network
 - o Dedicated connection
 - o Remote terminal
 - o VoIP
2. Troubleshooting WAN

Remote Access:

1. Dial-up connection to internet:

Old and less expensive method to access internet.

It uses dial-up method (dialing phone no.) to connect to ISP.

For dial-up connection setup, modem, telephone no., username and password, connection (PPP) and IP information is required.

This method was used in earlier days.

Remote Access:

2. Dial-up connection in Private network:

Dial-up connection is also used to connect to the private network.

This provide secure way to access the internet by private network.

For this, two systems are required:

1. Remote Access Server (RAS)
2. Client (running connection tool)

Remote Access:

3. Dedicated Connection:

It is a remote connection which is dedicated (always connected).

This connection also have a security features and high speed.

It is of two type:

1. Dedicated private connection between two location (T1 line).
2. Dedicated connection to internet (DSL or Cable Modem).

Remote Access:

4. Remote Terminal:

It provide a method to access the remote device using program.

Remote terminal are created using terminal emulation program such as telnet.

Remote terminal program require server and client to run.

Microsoft remote terminal named as Remote Desktop Connection (RDC) and using standard Remote Desktop Protocol (RDP).

RDC run over every version of windows.

Remote Access:

5. VoIP (Voice over IP):

VoIP provide a method to transmit voice call over IP network.

It work with three standards:

1. Real- time Protocol (RTP)
2. Session Initiation Protocol (SIP)
3. H.323

Troubleshooting WAN:

Troubleshooting of WAN network is done to solve issues arise in WAN connectivity:

Some of the problem are:

1. Internet connection loss
2. Interference/ Noise
3. Interface error

Virtualization

Content:

1. Virtualization
2. Hypervisor
 - o Types of Hypervisor
3. Benefits of Virtualization
4. Categories of Virtualization
5. Data storage
 - o Storage Area Network (SAN)
 - o Network Attached Storage (NAS)

Virtualization:

Virtualization is the creation of a virtual resources, such as an operating system, a server, a storage device or network resources.

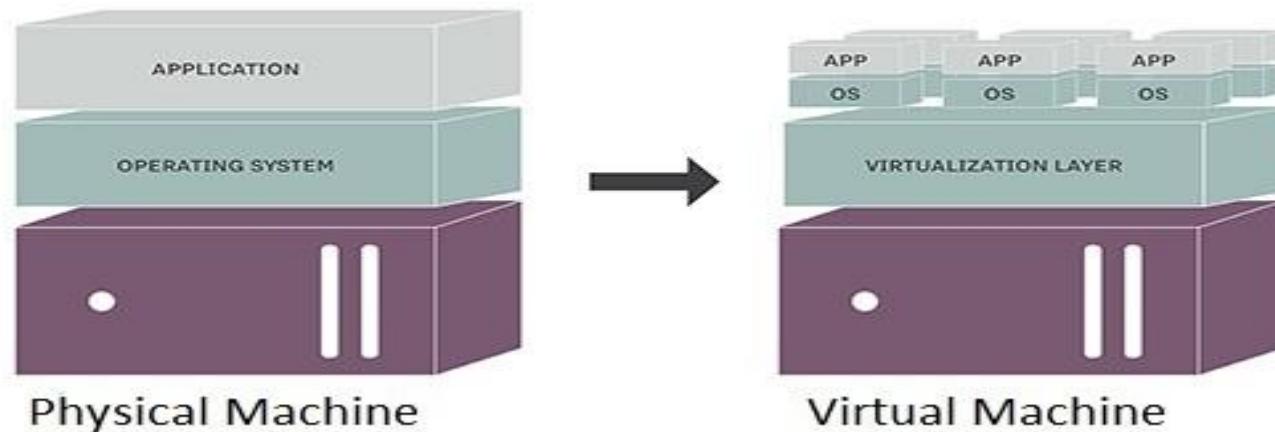
It main aim is to divides a single physical machines into multiple logical machines.

It is a process of using powerful, special software running on a physical machine to create a virtual resource same as that of real resource.

Virtualization is a fundamental part of cloud computing, especially in delivering Infrastructure as a Service (IaaS).

Example: Running both Linux and Window 7 over same PC.

Virtualization:



Hypervisor:

It is also known as Virtual Machine Monitor (VMM).

A hypervisor is computer software, firmware or hardware, that creates and runs virtual machines over a single physical machine.

It handles every input/output request of created virtual machines.

Host Machine: is a machine or computer on which a hypervisor runs one or more virtual machines.

Guest Machine: Each virtual machine is called a guest machine.

Hypervisor:

Native or Bare Metal Hypervisor:

Native Hypervisor run directly on the host's hardware to control the hardware and to manage guest operating systems.

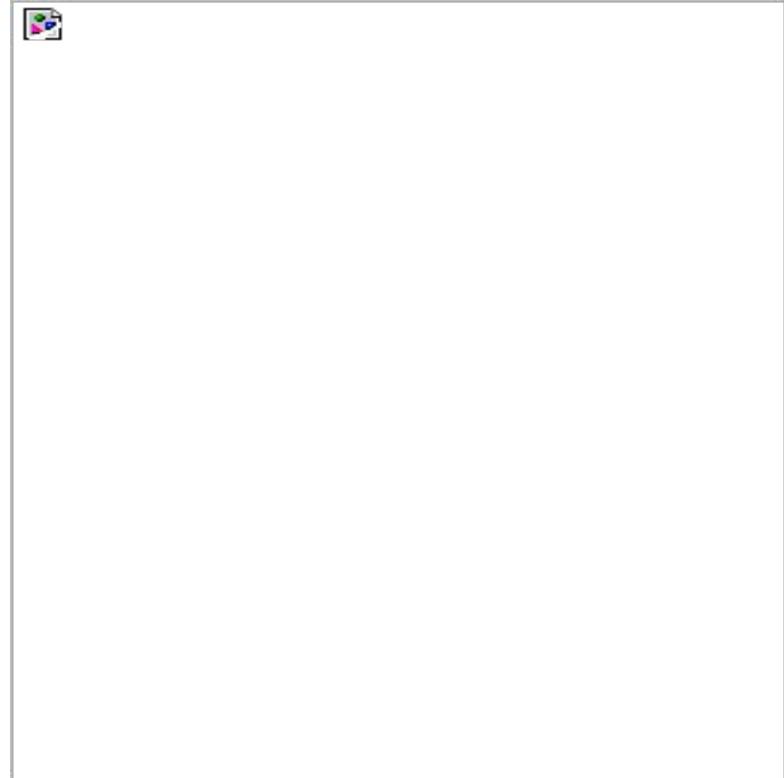
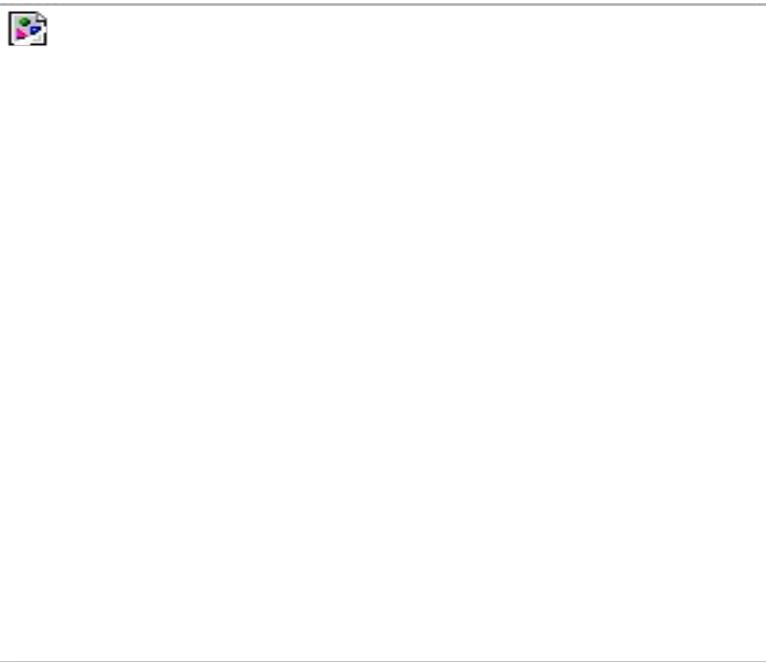
Example: Oracle VM Server for x86, Microsoft Hyper-V and VMware ESX/ESXi.

Hosted Hypervisor:

Hosted hypervisors run on a conventional operating system. A guest operating system runs as a process on the host.

Example: VMware Workstation, VMware Player, VirtualBox, QEMU.

Hypervisor:



Virtualization:

Benefits of Virtualization:

1. Workload Consolidation
2. System Duplication
3. Save Power
4. Reduce Infrastructure cost
5. Secure and reliable

Virtualization:

Basic Categories of Virtualization are:

1. Storage Virtualization
2. Network Virtualization
3. Server Virtualization
4. Application Virtualization
5. Hardware Virtualization
6. Desktop Virtualization

Data Storage:

Storage Area Network (SAN):

A storage-area network is a dedicated high-speed network that interconnects and presents shared pools of storage devices to multiple servers

It allows each server or device to access shared storage and store database.

It is assembled using three components: cabling, host bus adapters (HBAs) and switches.

Storage-area networks are managed centrally.

SAN is expensive, complex and difficult to manage technology.

Data Storage:

Storage Area Network (SAN):

SAN is access by using:

Fiber Channel (FC): is a high-speed network technology primarily used to connect computer data storage to servers. Operated at a speed of 1, 2, 4, 8, 16, 32, and 128 gbps.

Internet Small Computer System Interface (iSCSI): is a protocol used to connect storage device to server.it control data transfer over the TCP/IP. (SCSI over IP). operated at the speed of 1gbps ,10gbps 40gbps.

Data Storage:

Network Attached Storage (NAS):

Network-attached storage is also a dedicated file storage device that provides LAN nodes with file-based shared storage through a Ethernet connection.

It is configured and managed with a browser-based utility program.

Each NAS in the LAN identify as independent network node and has its own IP address.

The benefit of NAS is that it provide a ability to multiple clients on the network to can access the same file.

Cloud Computing

Content:

1. Cloud Computing
2. Types of Clouds
3. Cloud Services
4. Advantage of cloud computing.

Cloud Computing

Cloud computing is a type of internet based computing which provide the delivery of hosted services over the internet

It provide a network of remote servers to store, manage and process data over the internet.

Companies offering these computing services are called cloud providers and they charge for cloud computing services based on usage.

Example: Microsoft Window Azure, Amazon web services, Huawei GalaX cloud etc

Cloud Computing:



Cloud Computing:

Types of Cloud:

1. Public Cloud
2. Private Cloud
3. Hybrid Cloud

Cloud Computing:

1. Public Cloud:

In Public Cloud, the Service providers use the internet to make resources, such as applications and storage, for the use of the general public.

Example: Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform.

This cloud are inexpensive as compared to other clouds because user pay for the storage capacity that they used.

Limitation: Less secure and SLA specification.

Cloud Computing:

2. Private Cloud:

Private cloud is a cloud that is solely built for an enterprise.

It provides flexibility, scalability, provisioning, automation and monitoring to a enterprise.

Private cloud are not sell "as a service.

These clouds are expensive and are used by large enterprises.

The main concern for the design of Private cloud is to provide effective control of data, security and quality of service (QoS) for the company.

Example: Amazon VPC, VMware's vCloud etc

Cloud Computing:

3. Hybrid Cloud:

Hybrid Cloud is a composition of Public and Private Clouds.

Most of the enterprise use the hybrid cloud for security and control purposes because not all information is open to the public.

Hybrid cloud provide scalability and cloud-based services.

Example: Microsoft System Center, Google Cloud Platform and Rackspace.

Cloud Computing:

Cloud Services:

Cloud services are broadly divided into three categories:

1. Cloud Software as a Service (SaaS)
2. Cloud Platform as a Service (PaaS)
3. Cloud Infrastructure as a Service (IaaS)

These three models are independent of each other.

Cloud Computing:

1. Cloud Software as a Service (SaaS):

Software as a service is a way of delivering applications over the Internet—as a service.

SaaS applications are referred as Web-based software, on-demand software, or hosted software.

The provider manages access to the application, including security, availability, and performance.

SaaS customers have no hardware or software to buy, install, maintain, or update. Access to applications is easy by having internet connection.

Example: Google Apps, Salesforce, Workday, Cisco WebEx.

Cloud Computing:

2. Cloud Platform as a Service (PaaS):

In a PaaS model, a cloud provider delivers hardware and software tools needed for application development to its users as a service.

A PaaS provider hosts the hardware and software on its own infrastructure.

PaaS allows developers to frequently change or upgrade operating system features.

Users access PaaS through a Web browser.

PaaS charge for that access on a per-use basis or as a monthly fee for the access to platform.

Cloud Computing:

2. Cloud Platform as a Service (PaaS):

Example of PaaS vendors are Salesforce.com's Force.com, Google and Amazon.

PaaS platforms for development and management of software are Apper IQ, Amazon Web Services (AWS) Elastic Beanstalk, Google App Engine.

Cloud Computing:

3. Cloud Infrastructure as a Service (IaaS):

This cloud offer infrastructure resources such as hardware, software, server and storage.

Users can use these resources over internet and deploy application on them.

IaaS platforms offer highly scalable resources that can be adjusted on-demand.

IaaS customers pay on a per-use basis, typically by the hour, week or month.

Example: Amazon Web Services (AWS), Windows Azure, Google Compute Engine.

Cloud Computing:

Advantages of Cloud Computing:

1. Device and location independence
2. Multitenancy
3. Reliable
4. Network Scalability and Elasticity
5. Performance
6. Security

Basic Network Designing

Content:

1. Network Designing
 - o Steps
 - o Documentation
 - o Network components

Network Designing

Steps involve in designing of basic network:

1. Know Requirements/Need of the network
2. Type of devices require to meet those needs.
3. Material used to design the buildings
4. Understanding type of cable required
5. Wire/Wireless connectivity and Internet access
6. Dealing with computer, data and network security.

Network Designing:

Documentation is done to support configuration and maintenance of the network.

Network parts which we cover in documentation are:

- Network Diagram including floor plan
- List of assets used by company such as type of softwares and its updated version.
- IP address of every device in the network.
- Network usage policies and standards including securities.

Network Designing:

Types of Network Components:

1. Workstation
2. Servers
3. Equipment rooms
4. Peripherals

Network Designing:

1. Workstation:

A desktop computer terminal, typically networked and more powerful than a personal computer

Most of the company workers need workstation with modern OS such as window 10 or 8 and some employee need old version of OS

2. Equipment room:

Equipment room is a centralized core of the whole network.

All devices from different departments are connected in equipment room

It consist of racks and lots of patch cables

Network Designing:

3. Servers:

A server is a computer designed to process requests and deliver data to other computers over a local network or the internet.

Function of server:

- Network authentication and management
- Accounting
- Internet Service
- For web development and product testing

Network Designing:

4. Peripherals:

A peripheral device connects to a computer system to add functionality.

Examples are a mouse, keyboard, monitor, printer and scanner

Unified Communication

Content:

1. Unified communication
 - o Components
 - o Protocols
2. Related terms
 - o Medianets
 - o ICS
 - o DCS
 - o PLC
 - o SCADA

Unified Communication:

Unified Communication is a integration of real-time enterprise communication.

This technology starts with VoIP (Voice over IP network).

Other Unified communication services are:

- Instant messaging (chat)
- Presence information
- Audio, Web & Video conferencing
- Desktop and Data sharing
- Collaboration tools

Unified Communication:

Unified Communication Network Components:

1. UC devices (handle voice, video and data)
2. UC Servers (support UC provided Services)
3. UC Gateways (with extra services)

Unified Communication:

Protocols of Unified Communication:

1. SIP (Session Initiation Protocol)
2. RTP (Real-Time Protocol)
3. H.323 (used for video presentation)
4. MGCP (Media Gateway Control Protocol)

Unified Communication:

TCP ports used by every protocols:

1. SIP - TCP port 5060 and 5061
2. RTP - TCP port 5004 and 5005
3. H.323 - TCP port 1720
4. MGCP - TCP port 2427 and 2727

Unified Communication:

Terms:

1. Medianets:

A Medianet is a network optimized for rich media such as voice and video.

It also done mixing together of videos and documents, webpages, text, and many other forms of media.

It use two different fields to define Quality of Service (QoS)

- ECN (Explicit Congestion Notification): 2 bit field
- DSCP (Differentiated Services Code Point): 6 bit field

Unified Communication:

2. Industrial Control System (ICS):

Industrial control system (ICS) is a type of control systems which is associated with instruments used in industrial production.

Example: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and other smaller control system configurations such as Programmable Logic Controllers (PLC).

Industrial Control Systems are used in industries such as electrical, water, oil, gas and data.

Unified Communication:

3. Distributed Control System (DCS):

A distributed control system (DCS) is a specially designed automated control system.

It consists of geographically distributed control elements over the plant or control area.

DCS consists of a large number of local controllers in various sections of plant control area and are connected via a high speed communication network.

Unified Communication:

4. Programmable Logic Controller (PLC):

Programmable Logic Controller (PLC) is a digital computer used for the automation of various electro-mechanical processes in industries.

These controllers are specially designed to work in harsh conditions.

PLC consists of a microprocessor which is programmed using the computer language.

A visual programming language known as the Ladder Logic was created to program the PLC.

The program is written on a computer and is downloaded to the PLC via cable.

Unified Communication:

5. Supervisory Control and Data Acquisition (SCADA):

SCADA is a computer system for gathering and analyzing real time data.

SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation.

SCADA systems were first used in the 1960s.

Risk Management

Content:

1. Risk Management
 - o Change in Management
 - o Policies
 - o Patching and updating
2. User Awareness and Training

Risk Management:

Risk Management is a process to deal with attacks that occur in the network.

(IT) risk management requires companies to plan how to monitor, track, and manage security risks.

Type of risks are intentional and unintentional attacks, disasters such as earthquake, flood, meteor impact etc.

Risk Management:

Changes in Management:

The process of creating change in an organization functioning is called change management.

Change in Management is done in controlled, organized and in safe way.

These changes are done by group of peoples known as change management team.

Change in management is done two way:

- Strategic-level change
- Infrastructure level change

Risk Management:

The steps dealing with the change in management are:

1. Initiation
2. Approval
3. Implementing Change
4. Documentation

Risk Management:

Security Policies:

Security Policies are the written document that outlines the rules, laws and practices for accessing network.

Policies are made to protect the IT infrastructure.

It define what equipment they use, how they organize data and what action people take to ensure the security of the organization.

Risk Management:

Acceptable use Policy: it include

- Organization Equipment and data stored in that equipment are under the ownership of that company.
- Network access policy define who may access the network, how they access the network and what they can access like VPN policy, Password policy etc
- Organization monitor the every device by accessing it at any time.
- No one in the organization can use the company device for breaking law such as malware, hacking or spamming etc.

Risk Management:

Patching and Updating:

A patch is a piece of software which is designed to update a computer program or its supporting data, to fix or improve it.

This includes fixing security threats and other bugs, with such patches and improving its usability or performance.

Patch management is the process of using a strategy and plan of what patches should be applied to which systems at a specified time

Types of Updates are: Operating System Updates and Firmware Updates

Risk Management:

Users Awareness and Training:

Organization provide training to the end user to give them understanding of following:

1. They must read, understand and sign required security policies.
2. They must know about password skills such as complexity, sufficient length, password control etc
3. They must know how to make their devices secure from external attacks.
4. Organization also teach user how to recognize and deal with malware attack.

Security Documents

Content:

1. Security Documents
 - o Service Level Agreement (SLA)
 - o Memorandum of Understanding (MoU)
 - o Multi Source Agreement (MSA)
 - o Statement of Work (SOW)
2. Checking Network Securities

Security Documents:

Security documents are used for making deals with third party vendors.

A company use these documents to communicate, transact business and analyze its productivity.

Business documents range from brief email messages to complex legal agreements.

These documents are prepared by employees, business owner or professionals such as accountants or lawyers.

Security Documents:

Type of Security Documents are:

1. Service Level Agreement (SLA)
2. Memorandum of Understanding (MoU)
3. Multi Source Agreement (MSA)
4. Statement of Work (SoW)

Security Documents:

1. Service Level Agreement (SLA):

A service level agreement (SLA) is a contract between a service provider and the end user.

It defines the scope , quality and level of service expected from the service provider.

The basics example of SLA is SLA an Internet Service Provider (ISP) will provide to its customers.

Security Documents:

2. Memorandum of Understanding (MoU):

MoU is a document that define agreements between two parties in specific situation.

It is often used in a situation where parties either do not imply a legal commitment or in situations where the parties cannot create a legally enforceable agreement.

Many companies and government agencies use MoU's to define a relationship between departments, agencies or closely held companies.

Security Documents:

3. Multi Service Agreement (MSA):

MSA is a agreement that define the details of interoperability of a device.

This agreement is signed by manufacturer of device or hardware.

Example: companies sign agreement that their GBIC will work for both switches (Cisco or Juniper).

Security Documents:

4. Statement of Work (SoW):

A Statement of Work (SoW) is a document that defines the legal contract between Service provider and customers.

It defines specific activities, deliverables and timelines for a service or products that vendor agree to supply.

The SOW also includes detailed requirements and pricing, with standard regulatory and governance terms and conditions.

Example: Agreement between IT security company and customer.

Checking Network Securities:

1. Vulnerability Scanning:

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.

It determine where a system can be exploited and/or threatened by accessing week points.

It use software to that find out security flaws and create a database on the basis of these known flaws.

Checking Network Securities:

1. Vulnerability Scanning:

It generating a report of the findings flaws that an individual or an enterprise can use to tighten the network's security.

Most popular vulnerability scanning tools are Microsoft Baseline Security Analyzer (MBSA), Nmap, Nessus and openVAS.

Checking Network Securities:

2. Network Penetration testing:

Penetration testing (also called pen testing) is the method of testing a computer system or network to find vulnerabilities that an attacker could exploit.

Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in the system and provide solution to further harden the system.

Pen tests can be automated with software applications or they can be performed manually.

Checking Network Securities:

2. Network Penetration testing:

This process includes gathering information about the target before the test, identifying possible entry points, attempting to break in and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses.

Tools used for penetration testing are : Aircrack-ng and Metasploit

Planning & Safety

Content:

1. Planning
 - o Incidence Response Plan
 - o Disaster Response Plan
 - o Business Continuity
 - o Succession Planning
2. Computer Forensics
3. Safety Measures

Planning:

Planning in an organization is done to protect the infrastructure from damages caused by unexpected incidence, natural disasters etc.

Planning is done by making documents about how to limit the damage and how to recover from the damages.

Type of Planning:

- Incident Response Plan
- Disaster Response Plan
- Business Continuity
- Succession Planning

Planning:

1. Incident Response Plan:

Incident response is an organized plan to address and manage the damages of attack.

The goal is to handle the situation in such way that limits damage and reduces recovery time and costs.

An incident response plan provides a step-by-step process that should be followed by the IRP team, when an incident occurs.

Planning:

2. Disaster Response Plan:

A disaster recovery plan (DRP) include set of procedures to recover and protect a business IT infrastructure in the event of a disaster.

The disaster could be natural, environmental or man-made.

Man-made disasters could be intentional (terrorist attack) or unintentional (such as the breakage of a man-made dam).

This plan provide security and minimize delays in recovery.

Planning:

3. Business Continuity:

Business Continuity include the planning and preparation to ensure that an organization can continue to operations in case of serious disasters and incidence.

In Business Continuity planning, the remote sites are constructed to provide services and continue operations.

Type of secondary sites constructed are:

- Cold Site
- Warm Site
- Hot Site

Planning:

4. Succession Planning:

It is a process in which new leaders are identified and developed to replace the old leaders when they retire, leave or die.

The organization ensure that employees are recruited and developed to fill each key role in the company.

The goal of this planning to make the business continuity in case most important person left its work.

Computer Forensics:

Computer Forensics is a process of collecting, analysing and reporting on digital data in such a way that is presentable in a court of law.

It is used in detection and prevention of crime or any disputes.

Forensics is done in steps:

1. Securing Areas
2. Documenting Scene
3. Data collection

Top Computer Forensics certifications are CCE, GIAC etc

Safety Measures:

Safety Measures used to protect employee physical health are:

1. Secure installation of electrical equipment
2. Installation Safety such as hardware and racks installation
3. Emergency Procedures such as layout of building, fire exit plan, emergency alert system etc

Network Attacks

Content:

1. Attacks
2. Various type of attacks
 - o Denial of Service (DoS)
 - o Malwares
 - o Brute Force Cracking
 - o Spoofing
 - o Phishing
 - o Packet Sniffing
 - o Port Scanning
 - o Session Hijacking

Attacks:

An attack is an effort to destroy, steal or gain an unauthorized access to organization or individual asset.

Attack can be made by an insider or also done by outsider to an IT infrastructure.

It can compromises the confidentiality, Integrity and availability of the resources of an organization.

Type of attacks are like passive attack, active attack and network attack.

Attacks:

Types of attacks:

1. Denial of Services (DoS):

A DoS attack is a cyber-attack where the attacker make a machine or network resource unavailable to its intended users.

It is done by flooding a network with useless traffic temporarily or indefinitely which disrupt the services of a host connected to the internet.

It is designed to disable, shutdown or disrupt a network, website or service.

Attacks:

1. Denial of Services (DoS):

An attacker may physically interrupt the services or use software to do so.

The goal of DoS is to make server to do lot of processing and responding.

DoS is not performed by single device lot of devices are required to make this attack.

Zombie: Zombie is a computer which is controlled by the attacker.

Botnet: Botnet refers to the network of Zombie computers.

Attacks:

1. Denial of Services (DoS):

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the resources of a targeted system.

Type of DoS attacks are:

- Smurfing
- Unintentional DoS
- Plashing

Attacks:

2. Malware:

It is also known as Malicious Software.

Malware is any program or file that cause harm to the computer or other devices.

Malware includes computer viruses, worms, Trojan horses, adware and spyware.

It perform a variety of functions like stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring user's computer activity without their permission.

Attacks:

2. Malware:

Types of Malwares:

- Virus: is a malicious program that can execute itself and spreads by infecting other programs or files present in the device.
- Worms: are the type of malware that can self-replicate without a host program.
- Trojan Horse: is designed to appear as a authorized program. After installation, Trojans start executing their malicious functions.

Attacks:

2. Malware:

Types of Malwares:

- Rootkit: Its a malware which is designed to obtain administrator-level access to the victim's system
- Spyware: is designed to collect information and data on users and observe their activity without users' knowledge.

Attacks:

3. Brute Force Cracking:

Brute force cracking is a trial and error method

In this attack, attacker decode encrypted data such as passwords or Data Encryption Standard (DES) keys.

In Brute force cracking, attacker proceeds through all possible combinations of legal characters in sequence to crack the password or encrypted data.

Brute force is a time-consuming process.

Attacks:

4. Spoofing:

A spoofing attack is when an attacker or malicious program successfully acts on another person's or program behalf by impersonating data.

In this attack, the attacker pretends to be someone else or another computer, device on a network in order to trick other computers, devices or people into performing illegal actions or giving up sensitive data.

It is used to attack networks, spread malware and to access confidential information and data.

Types of spoofing attacks: ARP spoofing, DNS spoofing and IP address spoofing.

Attacks:

5. Session Hijacking:

It is also known as cookie hijacking.

Session Hijacking is the misuse of a valid computer session or session key.

In this attack, hacker gain unauthorized access to information or services in a computer system.

Example: Web developers use HTTP cookies to maintain a session on many web sites. So it can be easily stolen by an attacker using an intermediate computer or with access to the saved cookies on the user's computer.

Attacks:

6. Zero Day Attack:

Zero day attack is used to describe the threat of an unknown security flaws in a computer application.

This attack occurs if the application developers were unaware of this flaw or did not have sufficient time to patch it.

A zero day flaw is considered as an important component when designing an application to be efficient and secure.

Attacks:

7. Phishing:

Phishing is a type of social engineering attack used to obtain sensitive information or steal user data.

It include stealing of login credentials such as username and password, credit card numbers or indirectly money.

An attack can have devastating results.

Attacks:

8. Insider Attacks:

An insider attack or insider threat is a malicious attack made on a network or computer system by a person having authorized access.

Insiders can plant trojan horses or browse through the file security system. This type of attack can be extremely difficult to detect or protect against.

Trojan horses are a threat to both the integrity and confidentiality of the system.

Insiders can affect availability by overloading the system's processing or storage capacity, or by causing the system to crash.

Attacks:

9. Packet sniffing:

Packet sniffing is a network attack, where attacker captures network traffic or data at the Ethernet frame level and then analyze and retrieve the sensitive information.

Such a network attack starts with a tool such as Wireshark.

10. Port Scanning:

A port scan attack occurs when an attacker sends packets to the machine to find its destination port. The attacker use this attack to get knowledge about the operation running over operating system.

Vulnerabilities (Network)

Content:

1. Vulnerabilities:
 - o Using unencrypted channel
 - o Missing Patches
 - o Unneeded services
 - o RF Emanation
 - o Plaintext Credential

Vulnerabilities:

Vulnerability is a cyber-security that define weakness in the computer system or network.

Vulnerability is the composition of three elements:

- A flaw in system
- Access of attacker to that flaw
- Capability of attacker to exploit the flaw

Vulnerabilities:

1. Using Unencrypted Channels:

System or network using unsecured or unencrypted channel are more vulnerable to the threat or attack.

For Example:

Using HTTP instead of HTTPS for browsing

Using unsecure remote desktop such as VNC.

Vulnerabilities:

2. Missing Patches:

Missing patches or updates on a server or computer system permits the attacker an unauthenticated command prompt or other backdoor path into the web environment.

By not installing recent updates to the system cause failure of the application or also reduce the security of the system.

Patches must be installed carefully by accessing its whole information.

Vulnerabilities:

3. Unneeded Services:

Running of unnecessary services or application in the background of operating system also make system prone to threats.

These unnecessary services access the open TCP/UDP port of the system.

The attacker access these open port through different tools and cause a different malware attack.

Vulnerabilities:

4. RF Emanation:

Radio frequency can penetrate walls and spread up to long distance this is known as RF Emanation.

Attackers can tap this RF signals to steal information.

Threats can be avoided by placing some filtering between the system.

TEMPEST refers to spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations.

Vulnerabilities:

5. Cleartext Credential:

Cleartext Credential refers to the user data which is not encrypted or encoded using cryptographic keys.

Data is available in cleartext form can be read by anyone by tapping the signals or packets.

To protect the data such as username, password and credit card numbers must be encrypted before transmitting over unsecure network.

Security (Network)

Content:

1. Physical Security
2. Network Security
3. Host Security

Security:

Security is the degree of protection from harm.

It applies to any vulnerable and valuable asset such as a person, community, item, nation or organization.

Security in IT is the defense of digital data and IT assets against internal and external, malicious and accidental threats.

The defense includes detection, prevention and response to threats by using various security policies, software tools and IT services.

Security:

Types of security used to harden the network are:

1. Physical Security
2. Network Security
3. Host Security

Physical Security:

Physical security is the protection of personnel, hardware, software, networks and data from physical action.

As these threat could cause serious loss or damage to an enterprise or institution.

Physical Security includes protection from fire, flood, natural disasters, theft, vandalism and terrorism.

Physical security is obtained by:

1. Access Control
2. Monitoring by Surveillance and testing

Physical Security:

1. Access Control:

Steps for prevention and controlling access to Physical resources are:

- Lock the doors of network closet or equipment rooms and giving access keys and cards to trustworthy staff.
- Locking front door of institution or enterprise to prevent 'tailgating'. (Mantrap system is used to prevent tailgating.)
- Using Biometric authorization for opening a door or getting access to any physical resources such as fingerprint reader, facial recognition cameras, voice analyzer etc.

Physical Security:

2. Monitoring by Surveillance and testing:

Authorized peoples are kept under surveillance to prevent insider threats.

Monitoring is done using video surveillance of facilities and assets.

Two type of video surveillance is used :

- Closed Circuit Television (CCTV)
- IP cameras

Physical Security:

CCTV Camera:

1. CCTV camera are analog cameras
2. Analog camera connects over RJ Cable and does not need any network.
3. Analog camera cannot be accessed directly by mobile applications.
4. Video quality is not so good.
5. Analog cameras need hardware for recording.

IP Camera:

1. IP camera are digital cameras.
2. IP Camera needs network and connects using CAT6 Cable
3. IP Camera can be access from anywhere using the IP Address without any DVR/NVR
4. IP Cameras give better video than CCTV Camera.
5. IP Camera video can be recorded on a PC/Workstation small software.

Network Security:

Network security is a specialized field in networking that include protection of computer network infrastructure.

Network securities are designed to protect the usability and integrity of your network and data.

It includes both hardware and software technologies.

It consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification of computer network and network resources.

Network Security:

Steps involve in providing security to computer network are:

- Securing and controlling user account (Username and password)
- Installation of 'Edge' devices which work with the coordination of other devices and controllers.
- Using Posture Validation approach, in this a node or device is verify on certain conditions before it is allowed to connect to a network.
- Installing querying agents such as persistent agent and non-persistent agent.
- Testing guest or Quarantine network.

Host Security:

A host is a computer or other device that communicates with other hosts on a network.

Hosts on a network include clients and servers -- that send or receive data, services or applications.

Host security is a process of securing individual computer or device.

Technique used to secure Host are:

1. Malware and Anti-Malware.
2. Using Strong password at Host end device

Host Security:

Prevention from Malware attack:

When a malware attack occur at host end then the system become slow, application crashes out or web browser open unwanted websites.

To deal with malware attack perform these tasks:

- Installing Anti-Malware program
- Providing training to the user how to prevent the occurrence of attack and if attack occur, how to deal with it.
- Patching and updating should be done properly.

Host Security:

Anti-Malware Program:

Anti-Malware software or program protects against attack caused by many types of malware such as viruses, worms, Trojan horses, spyware and adware.

It work in two modes:

- Active seek & destroy mode: In this mode, program scan the computer boot sector & files for viruses.
- Passive entry mode (Virus Shield): It passively monitor the computer activities such as program executing or file being downloaded.

Host Security:

Types of Anti-Malware software are:

1. Host Based Anti-Malware
2. Network Based Anti-Malware
3. Cloud/Server Based Anti-Malware

Firewalls

Content:

1. Firewalls
2. Type of Firewalls
3. Implementing and Configuring Firewalls
 - ACL
 - DMZ
 - Honeypots and Honeynets

Firewalls:

A firewall is a network security system that use rules to control inbound and outbound network traffic.

It may be a hardware or software-based and act as a filter to protect internal network from unauthorized access.

It acts as a barrier between a trusted network and an untrusted network.

Firewalls are the essential tools in the fight against malicious program on the internet.

Example: ZoneAlarm, Tinywall, PeerBlock, Private eye etc

Firewalls:

Types of firewalls are:

1. Network Based Firewalls: Hardware Firewall

This type of firewall is built into the router which is placed between the LAN and unsecure internet.

Example SOHO Firewalls

2. Host-Based Firewalls: Software Firewall

The software firewall is installed in a host computer or device. It work for a individual machine.

Example: Window Firewall

Firewalls:



Firewall

Firewalls:

Implementing and Configuring Firewalls:

- Firewalls are placed between the trusted network and the internet so that it can check all the traffic flow between these two networks.
- Physical installation of firewall is same as that of installing other network elements such as routers ,switches etc.
- Example: SOHO firewalls consist of fixed number of ports and every ports have well-defined function.
- After installation, configure the firewall settings.

Firewalls:

Firewalls setting:

Access Control List (ACL):

- Configuring a firewall on the basis of traffic flow i.e. defining which traffic can flow and which traffic should not pass. This rule of traffic Control is called Access Control List.
- ACL is a rule which is applied to an interface that control traffic on the basis of source and destination address.
- It perform various other filtering also like web filtering, content filtering and port filtering.

Firewalls:

Demilitarized Zone (DMZ):

A demilitarized zone (DMZ) refers to a host or network that acts as a secure and intermediate network between an organization's internal network and the external network.

A DMZ serves as a front-line network that interacts directly with the external networks while logically separating from the internal network.

It is implemented to secure an internal network from exploitation and access by external nodes and networks.

Example: Web server, FTP server and VoIP server are placed in DMZ.

Firewalls:



Demilitarized Zone

Firewalls:

Honeypots:

A honeypot is a computer system which is similar to real system to trap cyber attackers.

It is a way to detect and study their attempts to gain unauthorized access to information system.

Honeypots network is of two type:

1. Production Honeypots
2. Research Honeypots

Firewalls:

Honeynets:

A Honeynet is a network which is set up with intentional vulnerabilities

The main purpose of a honeynet is to gather information about attackers' methods and motives.

Honeynets provide a benefit of diverting attackers from real network resources to the fake one.

A honeynet contains one or more honeypots.

Difference between honeypots and honeynets is that Honeynets usually has real applications and services so that it seems like a normal network.

SNMP & SIEM

Content:

1. SNMP

- Components
- MIB
- Versions and port number
- Functions

2. SIEM

SNMP:

Simple Network Management Protocol (SNMP) is a popular protocol for network management.

It is used for collecting information from network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.

Example: Microsoft Windows Server 2003 provides SNMP agent software that works with third-party SNMP management software.

SNMP:

SNMP-managed network consists of three components:

1. SNMP Manager
2. SNMP Agent
3. Network management station (NMS)

SNMP:

Management Information Base (MIB):

A management information base (MIB) is a description of a set of network devices that can be managed using the Simple Network Management Protocol.

SNMPv2 use MIB-II and with some additional features.

SNMP:

SNMP versions:

1. SNMP version 1 - SNMPv1
2. SNMP version 2 - SNMPv2
3. SNMP version 3 - SNMPv3

SNMP:

SNMP port numbers:

- SNMP use UDP (User Datagram Protocol) port 161 and 162 (unsecure communication).
- SNMP use UDP port adding Security Layer i.e. TLS (Transport Layer Security) 10161 and 10162.

Agent receives and listen queries on port 161 or 10161

NMS receives and listen queries on port 162 or 10162

SNMP:

SNMP functions include 8 core function, 4 the commonly used functions are:

- Get (like 'GetRequest' or 'GetNextRequest')
- Response
- Set (like 'SetRequest')
- Trap

SNMP:

How SNMP works:

1. When an SNMP manager wants to query an agent, it sends the 'GetRequest' command to agent.
2. Then agent sends the 'Response' with the requested information which is by the SNMP manager.
3. Then NMS tell the agent to make changes to the information which is queried and send 'Set' PDU.
4. Then agent make request for help by sending 'Trap' PDU to the SNMP Manager.

SIEM:

Security information and event management (SIEM) is an approach to security management.

SIEM provide an integrated view of an organization's information technology (IT) security.

It is used in large enterprise or organizations.

SIEM is an industry-standard term, with a composition of 2 term:

1. SEM (Security Event Management)
2. SIM (Security Information Management)

SIEM:

SIEM is a two part process:

SEM based on the Real-time monitoring of security events. It monitor the entire enterprise edge devices and save the database to a location that support single viewpoint review.

SIM manages the database which is reviewed and analyzed by automated and human interpreters.

Monitoring Tools

Content:

1. Monitoring Tools
 - Packet Sniffers and Packet Analyzers
 - Monitoring the performance
 - Monitoring different interface

Monitoring Tools:

1. Packet Sniffer and Analyzer:

Packet Sniffer and analyzer tool is used to diagnose network related problem.

Packet sniffers tool intercept the network traffic or packets from the wired or wireless network interface.

When the raw packet data is captured, packet analyzing software analyze it and present it in human-readable form.

Network technicians use this information to determine where a fault lies, such as determining which device failed to respond to a network request.

Monitoring Tools:

1. Packet Sniffer and Analyzer:

A good packet analyzer can file and sort a capture file and create an output to help us to do monitoring properly.

Wireshark is a powerful protocol analyzer software used to analyze network traffic.

Packet flow monitoring is also done by using NetFlow.

It contain information like source and destination address or ports, source on the device running that flow and total number of bytes of that flow.

Example: LiveAction, sFlow, IPFix etc.

Monitoring Tools:

2. Monitoring the Performance:

Performance Monitoring tools monitor the performance of the particular device.

It uses log files or baselines to define performance.

Log files store information about the performance of some particular aspect of a system.

Baseline is a log of performance indicators such as CPU utilization and other values.

Monitoring tools:

2. Monitoring the Performance:

The system which generate log files has two issues such as Security and Maintenance.

The job of providing proper security and maintenance for log files is called "*log management*".

Example of Performance Monitoring tools are Window Performance monitors (PerfMon) and Linux Syslog

Monitoring Tools:

3. Monitoring different Interfaces:

Interface Monitoring is used to monitor bandwidth and utilization of one or more interfaces or ports on one or more devices.

It consists of defining speed, duplex technique, Network utilization, packet drops etc.

Example: Cisco Network Assistant (CNA) software

Hardware Tools

Content:

1. Problem occur in network
2. Various Hardware tools
 - Cable tester
 - TDR and OTDR
 - Multimeter
 - Line tester
 - & others

Hardware Tools:

Problems occur in network are:

1. Open circuit and Short Circuit
2. Wire mapping problem
3. Crosstalk and Noise
4. Impedance mismatch

Hardware Tools:

Different hardware tools deal with these issues such as:

1. Cable tester
2. OTDR and TDR
3. Light meter
4. Cable Stripper
5. Multimeter
6. Line tester
7. Tone probes and tone generator
8. Voltage event recorder and temperature monitor
9. Others

Cable Tester

Cable tester is an electronics device used to test the continuity problem and wire mapping problem.

Common way of testing connection is continuity test and resistance test.

Example: Signal tester and optical fiber tester



TDR:

Time-domain reflectometer (TDR) is an electronic instrument that is used to locate faults in metallic cables.

It can also be used to locate discontinuities in a connections, printed circuit board and other electrical path.



OTDR:

An optical time domain reflectometer (OTDR) is an optoelectronic instrument.

It is used to locate events or faults along a fiber link.

OTDRs are mainly used in the optical fiber installation and maintenance of optical fiber network.



Light Meter:

Light meters are used to measure the amount of light loss in the optical network.

The light meter use a high powered source of light at one end and a calibrated detector at other end.

This measure the amount of light that reaches the detector.



Multimeter:

A Multimeter or Volt-Ohm meter is used to measure voltage, current and resistance.

Multimeter might be analog type multimeters or digital multimeters.

It is Hand-held devices are very useful to detect faults or provide field measurements at a high degree of accuracy.



Tone Probes:

A tone and probe kit is a useful electrical tool that is used while cable installation.

This tool is made up of two parts:

- The generator tone
- The cable probe

It work together to identify electrical circuits.



Certifiers:

A certifier is used to verify the cables that they meets its specifications such as the bandwidth and frequency.

Example: verifying CAT 5e cable meets specifications and supports speeds of 1000 Mbps, CAT 6 cable supports speeds of 10 Gbps.



Voltage Event Recorder

The Voltage Event Recorder/Temperature Monitor is used to monitor equipment rooms or server rooms over time to detect and record issues with electricity or heat respectively.



Cable Stripper:

A wire stripper is a small, hand-held device used to strip the electrical insulation from electric wires.

Wire stripper is used by rotating it around the insulation while applying pressure in order to make a cut around the insulation.



Line Tester:

Telephone line tester is a type of line fault tester with safety & multi-functions capabilities.

It also has the functions of high voltage protection and dangerous voltage warning.



Punch down Tool

A punch down tool is a hand tool used to connect network wires to a patch panel, punch down block, keystone module, or surface mount box.

It consists of a handle, a spring mechanism, and a removable slotted blade.

(When the punch down tool connects a wire, the blade cuts off the excess wire.)



Software Tools

Content:

1. Type of Software tool
 - Built-in operating system
 - Third party software tool

Software Tools:

A software tool is a computer program that software developers use to create, debug and maintain programs and applications.

Types of Software tools are:

1. Built-in operating system
2. Third Party Software tool

Software Tools:

Built-in Operating System:

1. Tracert/Traceroute command:

Traceroute/ Tracert command is used to trace all the routers between two points.

If traceroute/tracert stop at certain router, then the problem is in next router or in the connection between them.

- Tracert - Windows
- Traceroute - Linux, UNIX

Software Tools:

Built-in Operating System:

2. arp command:

arp command (address resolution protocol) is used to resolve IP address to MAC address.

It is used to view and change the ARP table on a computer.

Syntax: arp -a

Software Tools:

Built-in Operating System:

3. ipconfig/ ifconfig/ ip command:

These command are used to know about the ip setting on any device.

- ipconfig - Windows
- ifconfig - UNIX
- ip - Linux

Other related commands are ipconfig /all, ipconfig /renew etc

Software Tools:

Built-in Operating System:

4. ping/ pathping/ arping command:

ping command work over router which is used to check that the system is reachable or not.

Ping command use ICMP packet whereas arping command use ARP frames.

Microsoft has a utility called pathping with the combination of tracert and ping command functions and also add some extra functionality.

Software Tools:

Built-in Operating System:

5. nslookup/ dig command:

nslookup/ dig command is used to diagnose DNS problem.

- nslookup - all Operating System
- dig - Linux or UNIX

6. hostname command:

hostname command is used to display the name of the computer.

Software Tools:

Built-in Operating System:

7. netstat/ ss command:

netstat command display the information about active sessions and also provide statistics based on ports or protocols.

netstat consist of various command such as netstat -r, netstat -n, netstat -a etc.

ss command is powerful command used in Linux operating system.

Software Tools:

Built-in Operating System:

8. route command:

Route command is used to display and edit local system routing table.

9. mtr command:

mtr command (My Traceroute) is a powerful network diagnostic tool which combines the power of both Ping and Traceroute commands.

It enables administrator to diagnose and isolate network errors and provide helpful network status reports.

Software Tools:

Third party Software Tools:

1. Packet Sniffer (Wireshark)
2. Port Scanner (Nmap or Angry IP Scanner)
3. Throughput Testing tool (Tamosoft, NetIO GUI)
4. Looking Glass sites (at&t, Verizon)

Network Issues

Content:

1. Network Common issues
 - Problem in LAN/ WAN
 - Problem over physical device
 - Server Configuration problem
 - MTU and ISP
 - Router problem
2. Some serious network issue

Network Issues:

1. Problem in LAN/ WAN: include

Incorrect configuration of any node in LAN network.

Incorrect IP address configuration in WAN network led to problem such as router configuration issue, problem with ISP, increased frame size etc.

2. Problem over physical devices:

It define problem that can be fix at the workstation, work area or server.

It include problem like power failure, hardware failure, interferences (EMI or RFI), interface error, incorrect ip configuration etc

Network Issues:

3. Server Configuration Problem:

Misconfiguration of server setting will deny some or all access to resources over network.

It include misconfiguration of DHCP setting at server or client end or misconfiguration of DNS setting at server or client end.

To diagnose this problem use ping command or other tools.

Network Issues:

4. MTU and ISP:

When the network packets are large and are fragmented to fit into ip packet . this is known as MTU mismatch.

A method PMTU (Path MTU Discovery) is used to determine best MTU setting automatically.

PMTU runs on ICMP, where some router having firewall where they block ICMP request. This is called PMTU or MTU block hole.

To troubleshoot this problem turn off the ICMP blocking setting of firewall in router.

Network Issues:

5. Router Problem:

Problems occur in routers include use of wrong routing protocol, incorrect whitelist or blacklist of ACL, Missing IP routes etc

To troubleshoot this problem use tracert or traceroute command.

Network Issues:

Some serious network issue that should be removed are:

1. Broadcast Storm in computer network
2. Formation of Routing loops
3. Formating of Switching loops
4. Proxy ARP

Troubleshooting Network

Content:

1. Troubleshooting
2. Steps involved in troubleshooting process
 - Finding problem
 - Finding the causes
 - Plan to tackle the problem
 - Checking the functionality of system
 - Documentation about details of problem

Troubleshooting:

Troubleshooting is a method of finding the cause of a problem and correcting it.

The goal of troubleshooting is to get the equipment back into operation.

This is a very important job because the entire production operation may depend on the troubleshooter's ability to solve the problem quickly and economically.

Troubleshooting:

Steps involved in troubleshooting process are:

1. Finding problem by getting information from users, identifying symptoms and recalling if any change happen in the network.
2. Using multiple approaches to find a big problem, individually.
3. Find the cause of the problem and document it.
4. Consider multiple approaches while tackling problem such as top to down approach or divide and conquer.

Troubleshooting:

Steps involved in troubleshooting process are:

5. Then test the finding causes by analysing documents.
6. When the cause of problem is known then begin the next plan and if not then handle the job to other authorities.
7. Make a plan to properly resolve the problem and while resolving time think about the affects to network.
8. Implement the solution on network problem before the problem become intense or serious.

Troubleshooting:

Steps involved in troubleshooting process are:

9. After troubleshooting the network, make it run to check the system functionality and also apply measures to prevent the same problem in future.
10. Make proper documents of finding causes, solutions to the problems and the result of applied solutions for future reference.

Internet of Things (IoT)

Content:

1. Internet of Things
2. Problem faced by IoT
3. IEEE 1905.1

Internet of Things:

The Internet of Things (IoT) define the internetworking of physical devices, vehicles and buildings that feature an IP address for internet connectivity for collecting and exchanging data.

It encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities.

Examples of Internet of Things include connected security systems, thermostats, cars, electronic appliances, lights in household and commercial environments, alarm clocks and speaker systems.

Internet of Things:

Problem faced by IoT:

1. Errors
2. Security
3. Multiple connectivity
4. Power or Battery life
5. Data management and Traffic flow

Internet of Things:

IEEE 1905.1:

IEEE 1905.1 is a hybrid networking standard which define a flexible integrity of various wired and wireless technologies.

It include technologies such as Wi-Fi, Ethernet, MoCA and HomePlug (HD-PLC).

The IEEE 1905.1 Standard Working Group is sponsored by the IEEE Power Line Communication Standards Committee (PLCSC)

The benefits of 1905.1 technology include simple setup, configuration and operation of home networking devices using heterogeneous technologies

Internet of Things:

MoCA:

Multimedia over Coax (MoCA) provide networking over existing coaxial wires.

This technology was used by verizon to provide video, phone and internet service.

HomePlug (IEEE 1901):

HomePlug (HD-PLC) provide high speed home networking through an existing power infrastructure.

It target broadband applications such as IPTV, gaming, and Internet content.

Internet of Things:

nVoy:

nVoy is a Wi-Fi trademark and become the dominant brand name for IEEE 1905.1.

It covers a variety of IEEE 802.11 standard.

nVoy certified networking devices to create a single network for devices using various technology such as ethernet, wi-fi, MoCA and HomePlug.

