TVET CERTIFICATE III in COMPUTER SYSTEM TECHNOLOGY

INTRODUCTION TO COMPUTER NETWORKS

COSIC301

Introduce computer networks

Competence

Learning hours

 **40**

Credits:4

Sector: ICT

Sub-sector: Computer maintenance

Module Note Issue date: October, 2020

Purpose statement

This core module describes the skills, knowledge and attitude required to describe the purpose and functions of various network devices and protocols. The learner will be able to select the components required to meet a network specification, Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network, describe the purpose and basic operation of the protocols in the OSI and TCP models, the components required for network and Internet communications, Explain the technology and media access control method for Ethernet networks, network segmentation and basic traffic management concepts, implement an IP addressing scheme and IP Services to meet network requirements in a medium-size Enterprise branch office network, describe the operation and benefits of using private and public IP addressing. At the end the learner will have a strong foundation and an understanding of basic network functions, standards, and protocols.

Table of Contents

Total Number of Pages: 96

Learning Unit 1-Introduce Network Concepts

LO 1.1 – Describe Network concepts and technologies

Content/Topic 1: Description of computer network

A. Definition of computer network

1. **computer network**, often simply referred to as a network, is a collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information.
2. A computer network is a group of computers that shares information across wireless or wired technology.
3. A computer network is any set of computers or devices connected to each other with the ability to exchange data.

B. Elements of network

The modern data network has become a critical asset for many industries. Most basic data networks are designed to connect users and enable them to access various resources, like the Internet and other computers connected to the network. Networks are comprised of four basic elements: hardware, software, protocols and the connection medium. All data networks are comprised of these elements, and cannot function without them.

1. Hardware

The backbone of any network is the hardware that runs it. Network hardware includes network cards, routers or network switches, modems and Ethernet repeaters. Without this hardware, computers have no means of accessing a network. Network cards give computers direct access to network media and enable them to connect to other equipment, including routers, switches, modems and repeaters. Routers or switches allow a single network connection from a modem to be divided between several computers. Repeaters refresh the network signal between Ethernet cable segments, allowing Category 5 cables to reach beyond their 300-foot maximum length without signal loss.

2. Software

In order for the hardware to interact with the network, it needs software to issue commands. The primary form of networking software is protocols -- software that instructs network devices on how to connect to

the network and how to interact with one another. Other examples of networking software include connection monitoring software, networking clients and other tools designed to further facilitate your computer's ability to connect to the network.

3. Client Devices

Client devices are the computers and mobile devices connected to the network. Client devices are vital components of a network, as without clients requiring access the network is essentially pointless. In order to classify as a client device, a computer or mobile device must be able to connect to the network and utilize it. Depending on the network, client devices may also require specialized software to establish a connection.

4. Connection Media

Without connections, a network cannot function. The medium used to connect the nodes of a network varies with the type of network. Wired networks will often use network cables like Category 5 Ethernet cables, while wireless networks make direct connections between devices using radio signals as the medium.

Summary

Basic elements of a computer network include the following:

- **Hardware**
  - Network devices (Ex: Router, Switch, …).
  - Network Cables (Coaxial cables, Twisted pair cables, Fiber optic cable).
  - End devices.
- **Software** (Ex: Internetwork Operating System).
- **Protocols** (TCP, HTTP, …).

The interrelationship of these basic elements constitutes the infrastructure of the network.

A network infrastructure is the topology in which the nodes of a local area network (LAN) or a wide area network (WAN) are connected to each other. These connections involve equipment like routers, switches, bridges and hubs using cables (copper, fiber, and so on) or wireless technologies (Wi-Fi).

C. Network benefits:

Main benefits of networks include:

- **File sharing** – you can easily share data between different users, or access it remotely if you keep it on other connected devices.

- **Resource sharing** – using network-connected peripheral devices like printers, scanners and copiers, or sharing software between multiple users, saves money.
- **Sharing a single internet connection** – it is cost-efficient and can help protect your systems if you properly secure the network.
- **Increasing storage capacity** – you can access files and multimedia, such as images and music, which you store remotely on other machines or network-attached storage devices.

Networking computers can also help you **improve communication**, so that:

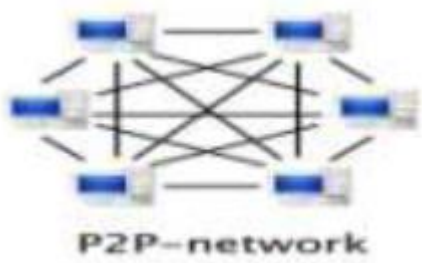
- staff, suppliers and customers can share information and get in touch more easily
- your business can become more efficient - eg networked access to a common database can avoid the same data being keyed multiple times, saving time and preventing errors
- staff can deal with queries and deliver a better standard of service as a result of sharing customer data

Content/topic 2: Distinguishing between network classification

A. Classifying network by components roles

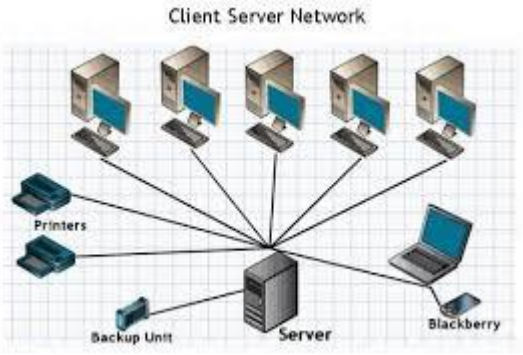
1. Peer to peer network

A **peer-to-peer** (**P2P**) **network** is created when two or more PCs are connected and share resources without going through a separate server computer



2. Client/server network

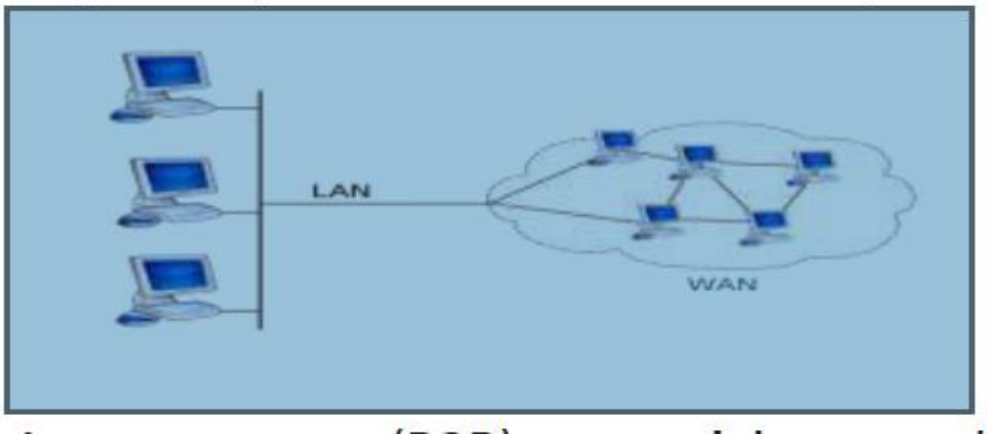
Client/server network. A computer **network** in which one centralized, powerful computer (called the **server**) is a hub to which many less powerful personal computers or workstations (called **clients**) are connected.



B. Classifying network by geographical area

1. WAN (Wide Area Network)

A **wide area network**, or **WAN**, occupies a very large area, such as an entire country or the entire world.



2. LAN

A local area network is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building

3. MAN

A metropolitan area network (MAN) is a computer network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (**LAN**) but smaller than the area covered by a wide area network (WAN).

Content/topic 3: Introduction to network technologies

A. **IEEE802.3 Ethernet**

Definition for Ethernet

IEEE stand for Institute of Electrical and Electronics Engineers

Ethernet is a system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems

Ethernet is the most widely used local area network (LAN) technology, that defines wiring and signaling **standards** for the physical layer of TCP/IP. **Ethernet** was originally standardized as IEEE 802.3 with a data transmission rate of 10 Mb/s.Is LAN and Ethernet the same?

Ethernet is a type of network used extensively for setting up **LAN**. **LAN** port means your Local Area Network port which invariably ends up being an **Ethernet** port. So for all practical purpose **LAN** port is the **same** as **Ethernet** port. The connector used is RJ45.

IEEE 802.3 is a working group and a collection of **Institute of Electrical and Electronics Engineers**(IEEE) standards produced by the working group defining the physical layer and data link layer's media access control (MAC) of wired Ethernet. This is generally a local area network (LAN) technology with some wide area network (WAN) applications. Physical connections are made between nodes and/or infrastructure devices (hubs, switches, routers) by various types of copper or fiber cable.

B. IEEE802.5 Token ring

"A **token ring** network is a local area network (LAN) in which all computers are connected in a **ring** or star topology and a bit- or **token**-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time.

PACKET

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, Graphics Interchange Format file, Uniform Resource Locator request, and so forth) is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination.

In IEEE 802.5, the token passing scheme is used in place of Carrier Sense Multiple Access with Collision Detection (CSMA/CD) on a ring topology local area network (LAN). A token is circulated around a network. The computer that has possession of the token has the right to transmit packets for a certain period of time. If that computer has no packets to transmit then the token is passed to the next computer. Only one computer at a time can transmit packets so this helps to avoid collision problems.

C. IEEE802.8 Fiber optic

The **Fiber Optic Technical Advisory Group** was to create a LAN standard for fiber optic media used in token passing computer networks like**FDDI**. This was part of the**IEEE 802** group of standards.

Fiber Distributed Data Interface (**FDDI**) is a standard for **data transmission in a local area network**

D. IEEE802.11 Wireless

IEEE 802.11 is part of the IEEE 802 set of LAN protocols, and specifies the set of media access control (MAC) and *physical layer* (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication in various frequencies, including but not limited to 2.4, 5, and 60 GHz frequency bands.

LO1.2- Describe Network topology

Content/Topic1: Description of Network topology

A. **Definition of topology**

- Is the way in which constituent parts are interrelated or arranged?
- Network topology is the interconnected pattern of network elements. A network topology may be physical, mapping hardware configuration, or logical, mapping the path that the data must take in order to travel around the network.

- A network topology is the arrangement of a network, including its nodes and connecting lines. There are two ways of defining network geometry: the physical topology and the logical (or signal) topology.

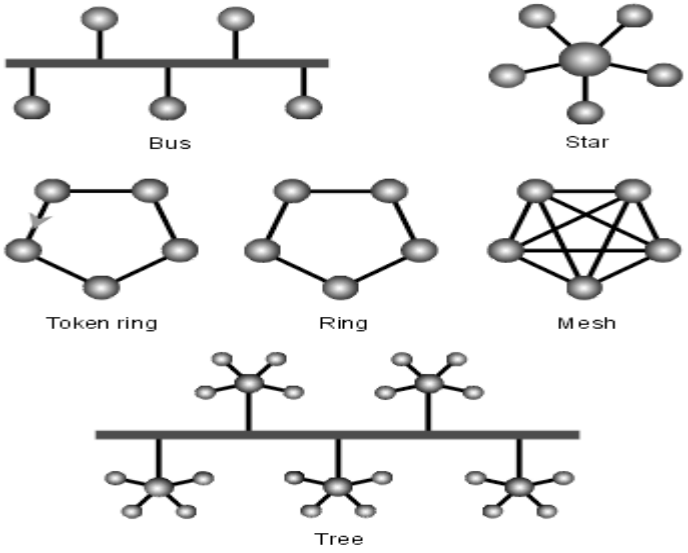
1. **Logical**

   Logical (or signal) topology refers to the nature of the paths the signals follow from node to node. In many instances, the logical topology is the same as the physical topology. But this is not always the case. For example, some networks are physically laid out in a star configuration, but they operate logically as bus or ring networks.

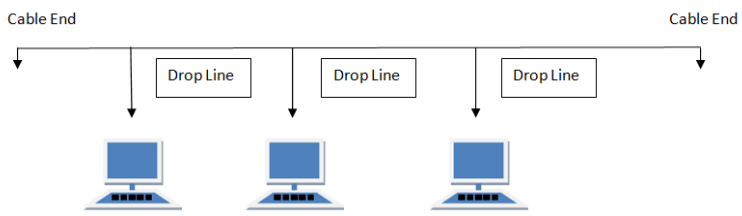
2. **Physical**

   The physical topology of a network is the actual geometric layout of workstations. There are several common physical topologies, as described below and as shown in the illustration.

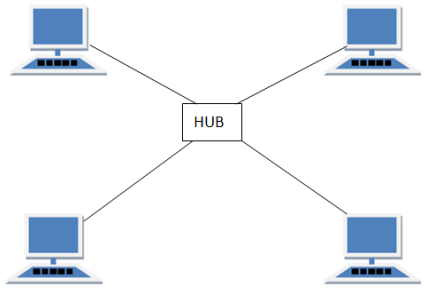
Types of network topology



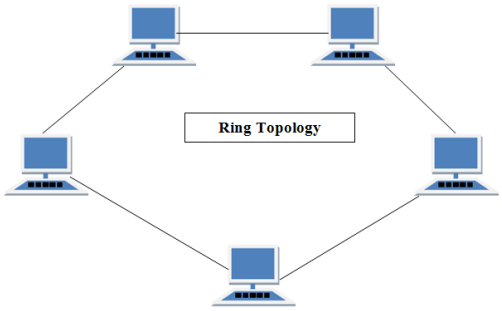
✓ **In the bus network topology**, every workstation is connected to a main cable called the bus. Therefore, in effect, each workstation is directly connected to every other workstation in the network.



- ✓ **In the star network topology**, there is a central computer or server to which all the workstations are directly connected. Every workstation is indirectly connected to every other through the central computer.

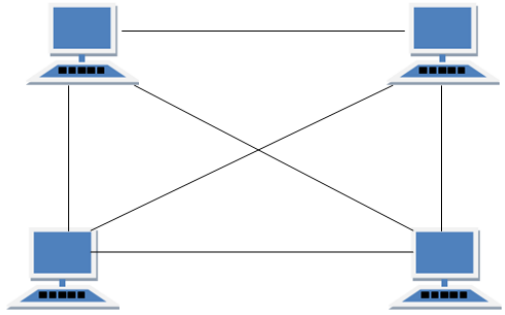


- ✓ **In the ring network topology**, the workstations are connected in a closed loop configuration. Adjacent pairs of workstations are directly connected. Other pairs of workstations are indirectly connected, the data passing through one or more intermediate nodes.

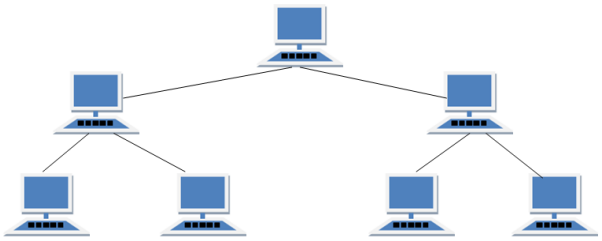


If a Token Ring protocol is used in a star or ring topology, the signal travels in only one direction, carried by a so-called token from node to node.

- ✓ **The mesh network topology** employs either of two schemes, called full mesh and partial mesh. In the full mesh topology, each workstation is connected directly to each of the others. In the partial mesh topology, some workstations are connected to all the others, and some are connected only to those other nodes with which they exchange the most data.



✓ **The tree network topology** uses two or more star networks connected together. The central computers of the star networks are connected to a main bus. Thus, a tree network is a bus network of star networks.



Content/ Topic 2: Identification of advantages and disadvantages of topology

Bus topology

1. **Advantages** of bus topology:
    b. Easy to implement and extend
    c. Well suited for temporary networks that must be set up in a hurry
    d. Typically the cheapest topology to implement
    e. Failure of one station does not affect others

2. **Disadvantages** of bus topology:
    f. Difficult to administer/troubleshoot
    g. Limited cable length and number of stations
    h. A cable break can disable the entire network; no redundancy
    i. Maintenance costs may be higher in the long run
    j. Performance degrades as additional computers are added

B. Star topology

1. **Advantages of star topology**
    a. Easy to add new stations
    b. Easy to monitor and troubleshoot
    c. Can accommodate different wiring

2. **Disadvantages of star topology**

- Failure of hub cripples attached stations
- More cable required (more expensive to wire a building for networking)

C. Token ring and ring topology

1. Advantages of ring topology

- Growth of system has minimal impact on performance
- All stations have equal access

2. Disadvantagesof ring topology

- Most expensive topology
- Failure of one computer may impact others
- Complex

D. Mesh topology

1. **Advantage of Mesh Topology**

The arrangement of the network nodes is such that it is possible to transmit data from one node to many other nodes at the same time.

2. **Disadvantage of Mesh Topology**

The arrangement wherein every network node is connected to every other node of the network, many of the connections serve no major purpose. This leads to the redundancy of many of the network connections.

E. Tree Topology

1. Advantages of a Tree Topology

- ✓ Point-to-point wiring for individual segments.
- ✓ Supported by several hardware and software venders.

2.Disadvantages of a Tree Topology

- ✓ Overall length of each segment is limited by the type of cabling used.
- ✓ If the backbone line breaks, the entire segment goes down.
- ✓ More difficult to configure and wire than other topologies.

L.O1.3-Study network devices, components and their functions

Content/Topic 1: Network devices classification

A. Interconnection devices

Many interconnection devices are required in a modern network, from the interface that allows a single computer to communicate with other computers via a LAN cable or a telephone line, to the large and complex switching devices that interconnect two or more entire networks. The main categories of interconnection device used in computer networks are listed below:

1. Network Interface Card (NIC)
2. Repeater
3. Hub
4. Bridge

B. Access devices

When used in broadband a NAD (Network Access Device) is a term to describe all the subscriber equipment required to make a connection to a wide area network (WAN) from a local area network (LAN). The NAD normally includes a router, modem and a monitored power supply. Most NAD's have the ability to report power failures and automatically reconnect themselves back to the network when disconnected.

In residential and business networks, Network Access Devices that are commonly seen include Wireless Access Points and Ethernet switches.

C. End devices

The network devices that people are most familiar with are called ***end devices***, or hosts. These devices form the interface between users and the underlying communication network.

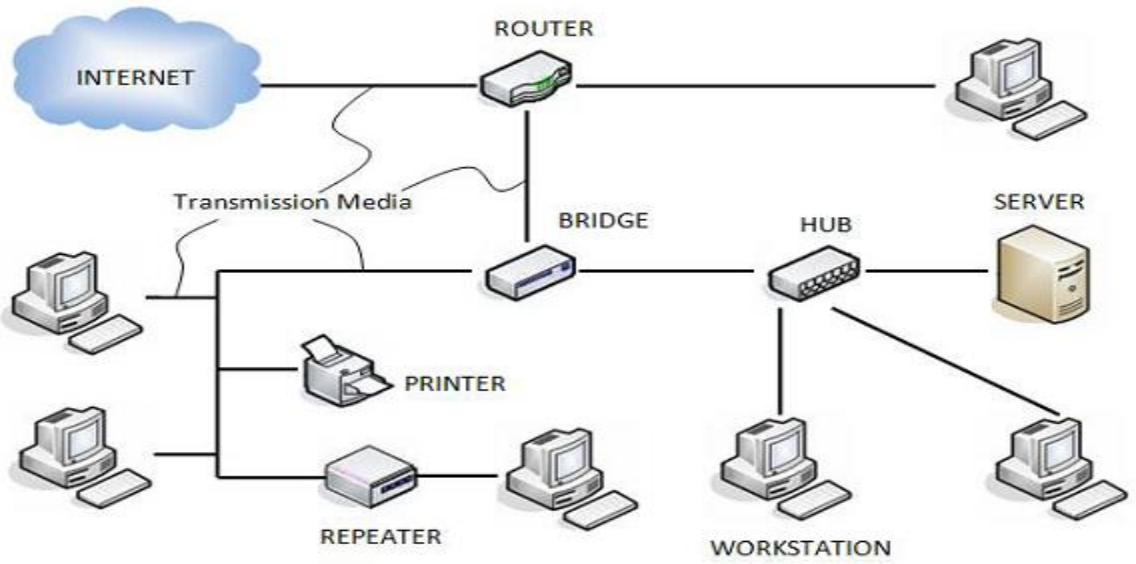
Some examples of end devices are:

1. Computers (work stations, laptops, file servers, web servers)
2. Network printers
3. Security cameras
4. Mobile handheld devices (such as smartphones, tablets, PDAs, and wireless debit/credit card readers and barcode scanners)

Content/Topic 2: Network components

- **Computer networks components** comprise both physical parts as well as the software required for installing computer networks, both at organizations and at home.

The following figure shows a network along with its components −



COMPUTER NETWORK COMPONENTS

✓ Hardware Components

- **Servers** −Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they give user accesses to the network resources. Servers can be of various kinds: file servers, database servers, print servers etc.
- **Clients** − Clients are computers that request and receive service from the servers to access and use the network resources.
- **Peers** − Peers are computers that provide as well as receive services from other peers in a workgroup network.
- **Transmission Media** − Transmission media are the channels through which data is transferred from one device to another in a network. Transmission media may be guided media like coaxial cable, fibre optic cables etc; or maybe unguided media like microwaves, infra-red waves etc.
- **Connecting Devices** − Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are:

a. Routers

b. Bridges

c. Hubs

d. Repeaters

e. Gateways

f. Switches

✓ Software Components

- **Networking Operating System** − Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc.
- **Protocol Suite** − A protocol is a rule or guideline followed by each computer for data communication. Protocol suite is a set of related protocols that are laid down for computer networks. The two popular protocol suites are −
  - a. OSI Model (Open System Interconnections)
  - b. TCP / IP Model

Media

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

Message

A message is a buffer of text data sent to a user or application on the network

Protocol

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

D. Devices

They allow the network resources to be shared among computers.

1. Router

Routers are the most intelligent among all the network devices. They can be programmed to use the most efficient route to transmit the data to the desired computers. They operate on the Network Layer 3 of OSI model and can route data packets from one network to another based on their IP address. Also they don't forward broadcasts by default.

Routers make each of its port into a separate segment and a separate collision domain. Thus routers have many segments and many collision domains. The routers can separate broadcast domains unlike switches that create separate collision domains but same broadcast domains.

By default, routers break the broadcast domains and keep all devices separate on a segment from other segments. This means if messages are sent on a segment, the devices on that segment will be able to get that broadcast message and not all other segments of the same network. The functions of a router are: Path selection, Packet filtering, Packet switching, and Internetworking. The routers perform packet switching and internetworking using logical addressing and packet filtering using access lists. Routers use routing tables or map of the internetwork to make path selection and send data packets to remote networks

2. **Hubs**

A hub a very basic network device that connects all the computers together in a network. It sends all the network data to all the computers connected to it, without using any intelligence of its own. Each port on the hub is on the same network segment. Thus a hub has one segment and one collision domain. The job of a hub is simply sending out anything that comes to it to other computers connected to it.

Every computer connected to hub can see every other computer on the hub. With the increase in the number of ports in a hub network, the possibility of collision also increases. A hub operates on the Network Layer 1 of the OSI model and can only detect basic network errors such as network collisions

3. **Switch**

Switches do same what a hubs do but they do it intelligently. They learn the MAC address of the requester and the port or the location of the device which responded to the request almost instantly. The first time, a request received by a switch is sent to all the computers connected to it. However, as soon as the request is responded by a computer, the switch learns the network location of the port that responded to the request and the Mac address of the source computer to handle the similar subsequent requests.

For example, consider computers called CompA, CompB, and CompC are connected to a switch. When a message destined for CompA is received by the switch, it broadcasts the message to all the computers. Now as soon as CompA responds to the message, the switch learns the path and sends all messages destined for CompA to CompA only.

It does this by remembering the MAC address of the originator of the request and then it sends the response from CompA to the same MAC address (originator of the request) only. Thus all subsequent messages received from the same source for the same destination are delivered to the same source and the destination computers only.

Switches operate on the Network Layer 2 of the OSI model and create many collision domains on the same segment. The switches make each port its own collision domain.

4. **NIC**

A network card, network adapter, or NIC (network interface card) is a piece of computer hardware designed to allow computers to physically access a networking medium. It provides a low-level addressing system through the use of MAC addresses.

5. **Repeater**

A repeater is an electronic device that receives a signal, cleans it of unnecessary noise, regenerates it, and retransmits it at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable that runs longer than 100 meters. A repeater with multiple ports is known as a hub. Repeaters work on the Physical Layer of the OSI model. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row (e.g. Ethernet's 5-4-3 rule).

Today, repeaters and hubs have been made mostly obsolete by switches (see below).

6. **Firewall**

A firewall is an important aspect of a network with respect to security. It typically rejects access requests from unsafe sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in 'cyber' attacks for the purpose of stealing/corrupting data, planting viruses, etc.

7. **Access points**

Access points are wireless network devices that are used to provide wireless access to a wired network. The access points are similar to hubs because the RF frequency they use on the wireless side is a shared media. It then further shares the frequency with all the computers accessing it just like a hub. The access points have one segment and one collision domain.

8. **Antenna**

An antenna is a transducer that converts radio frequency (RF) fields into alternating current or vice versa. There are both receiving and transmission antennas for sending or receiving radio transmissions. Antennas play an important role in the operation of all radio equipment. They are used in wireless local area networks, mobile telephony and satellite communication.

9. **Gateways**

Operates at or above the OSI transport layer and links LANs or networks that employ different architectures and use dissimilar protocols. Enable communications between two different types of networked systems.

A gateway is a node (router) in a computer network, a key *stopping point* for data on its way to or from other networks. Thanks to gateways, we are able to communicate and send data back and forth. The Internet wouldn't be any use to us without gateways (as well as a lot of other hardware and software).

In a workplace, the gateway is the computer that routes traffic from a workstation to the outside network that is serving up the Web pages. For basic Internet connections at home, the gateway is the Internet Service Provider that gives you access to the entire Internet.

Router: The routers are used to create internetworks. They use routing tables or map of the internetworks to make path selection and send data packets to other networks.

Hubs: Hubs operate on the same network segment they cannot divide a network.

Bridge: A Bridge has just 2 interface devices. It can connect only two networks that do not communicate very often.

The switches and bridges can create LANs and separate collision domains but they cannot be used to create separate LANs.

Learning Unit 2-Apply network protocols

LO 2.1. Describe Network Protocols

Content/Topic1: Introduction to network protocols

A. Definition

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

Network protocols are grouped such that each one relies on the protocols that underlie it sometimes referred to as a protocol stack.

B. Types of most common network protocols

1. NetBEUI

NetBIOS (Network Basic Input/Output System)

NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a local area network (LAN). It was created by IBM for its early PC Network, was adopted by Microsoft, and has since become a de facto industry standard. NetBIOS is used in Ethernet and Token Ring networks and, included as part of NetBIOS Extended User Interface (NetBEUI), in recent Microsoft Windows operating systems. It does not in itself support a routing mechanism so applications communicating on a wide area network (WAN) must use another "transport mechanism" (such as Transmission Control Protocol) rather than or in addition to NetBIOS.

2.NetBEUI (NetBIOS Extended User Interface) is a new, extended version of NetBIOS, the program that lets computers communicate within a local area network.

Pronounced *net-booey,* NetBEUI is short for ***NetB****ios* ***E****xtended* ***U****ser* ***I****nterface.* It is an enhanced version of the NetBIOSprotocol used by network operating systems such as LAN Manager, LAN Server, Windows for Workgroups, Windows 95 and Windows NT.

Netbeui was originally designed by IBM for their Lan Manager server and later extended by Microsoft and Novell.

3. TCP/IP

- TCP stands for “Transmission Control Protocol”

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

- IP stands for Internet Protocol

Internet Protocol (IP) is the principal set of digital message formats and rules for exchanging messages between computers across a single network or a series of interconnected networks, using the Internet Protocol Suite(often referred to as TCP/IP).

- TCP/IP

The Transmission Control Protocol/Internet Protocol(TCP/IP) is the language a computer uses to access the Internet. It consists of a suite of protocols designed to establish a network of networks to provide a host with access to the Internet.

4. **Apple talk**

AppleTalk is a discontinued proprietary suite of networking protocols developed by Apple Inc. for their Macintosh computers. AppleTalk includes a number of features that allow local area networks to be connected with no prior setup or the need for a centralized router or server of any sort. Connected AppleTalk-equipped systems automatically assign addresses, update the distributed namespace, and configure any required inter-networking routing.

AppleTalk was released in 1985, and was the primary protocol used by Apple devices through the 1980s and 1990s. Versions were also released for the IBM PC and compatibles and the Apple IIGS. AppleTalk support was also available in most networked printers (especially laser printers), some file servers, and a number of routers.

The rise of TCP/IP during the 1990s led to a reimplementation of most of these types of support on that protocol, and AppleTalk became unsupported as of the release of Mac OS X v10.6 in 2009. Many of AppleTalk's more advanced autoconfiguration features have since been introduced in Bonjour, while Universal Plug and Play serves similar needs.

5. **Novell NetWare(IPX/SPX)**

- ✓ **IPX/SPX** stands for **Internetwork Packet Exchange/Sequenced Packet Exchange**. IPX and SPX are networking protocols used primarily on networks using the NovellNetWareoperating systems.

- ✓ **NetWare** is a discontinued computer network operating system developed by Novell, Inc. It initially used cooperative multitasking to run various services on a personal computer, using the IPX network protocol.

- ✓ **Network operating system definitions**:

- A specialized operating system for a network device such as a router, switch or firewall.
- An operating system oriented to computer networking, to allow shared file and printer access among multiple computers in a network, to enable the sharing of data, users, groups, security, applications, and other networking functions, typically over a local area network (LAN), or private network. This sense is now largely historical; as common operating systems generally now have such features included.

Content/Topic2: Description of IP terminologies

A. Definition

- ✓ **IP** Stands for "**Internet Protocol**." IP provides a standard set of rules for sending and receiving data over the Internet. It allows devices running on different platforms to communicate with each other as long as they are connected to the Internet.

In order for an Internet-connected host to be recognized by other devices, it must have an IP address. This may be either an IPv4 or IPv6 address, but either way it uniquely defines a device on the Internet.

The Internet Protocol also provides basic instructions for transferring packets between devices. However, it does not actually establish the connection or define the ordering of the packets transmitted. These aspects are handled by the Transmission Control Protocol, which works in conjunction with the Internet Protocol to transfer data between systems on the Internet. For this reason, connections between Internet-connected systems are often called "**TCP/IP**" connections.

B. Two Types of IP

1. IPv4

IPv4 addresses are 32 bits long (four **bytes**). An example of an IPv4 address is **216.58.216.164**,

The maximum value of a 32-bit number is 2^{32}, or 4,294,967,296. So the maximum number of IPv4 addresses, which is called its address space, is about **4.3 billion**. In the 1980s, this was sufficient to address every networked device, but scientists knew that this space would quickly become exhausted. Technologies like NAT have delayed the problem by allowing many devices to use a single IP address, but a larger address space is needed to serve the modern Internet.

2. IPv6

IPv6 is also called IP next generation, or IPng, in honor of the favorite television show of most Internet gurus, Star Trek: The Next Generation.

IPv6 offers several advantages over IPv4, but the most important is that it uses 128 bits for Internet addresses instead of 32 bits. The number of host addresses possible with 128 bits is a number so large that it would have made Carl Sagan proud. It doesn't just double or triple the number of available addresses, or even a thousand-fold or even a million-fold. Just for the fun of it, here is the number of unique Internet addresses provided by IPv6:

340,282,366,920,938,463,463,374,607,431,768,21 1,456

This number is so large it defies understanding. If the IANA had been around at the creation of the universe and started handing out IPv6 addresses at a rate of one per millisecond - that is, 1,000 addresses every second - it would now, 15 billion years later, have not yet allocated even 1 percent of the available addresses.

The transition from IPv4 to IPv6 has been a slow one. IPv6 is available on all new computers and has been supported on Windows since Windows XP Service Pack 1 (released in 2002). However, most Internet service providers (ISPs) still base their service on IPv4. Thus, the Internet will continue to be driven by IPv4 for at least a few more years.

LO 2.2. Describe Network standards

Content/Topic1: Network standards

A. Importance of standards

Standards provide people and organizations with a basis for mutual understanding, and are used as tools to facilitate **communication**, **measurement**, **commerce** and **manufacturing**.

Standards are everywhere and play an important role in the economy, by:

- facilitating business interaction
- enabling companies to comply with relevant laws and regulations

- speeding up the introduction of innovative products to market

providing interoperability between new and existing products, services and processes.

B. Internet standards

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

C. Types of standards

1. De Facto standards

A de facto standard is something that is used so widely that it is considered a standard for a given application although it has no official status.

Here are a few examples of de facto standards:

- **The QWERTY keyboard layout** is the standard pattern in countries that use a Latin-based alphabet.
- **Microsoft's Windows operating system**, along with commonly used business applications such as Microsoft Word and Excel, has long been the de facto standard for business and home users.

2. De Jure standards

A de jure standard is a technology, method or product that has been officially endorsed for a given application.

De jure, from Medieval Latin, means *from law*. The term refers not only to legally protected or enforced standards but also to those that have been endorsed by an official standards organization, such as ANSI (American National Standards Institute) or IETF (Internet Engineering Task Force).

Examples of de jure standards include:

- **ASCII (American Standard Code for Information Interchange),** the most common **format** for text files in computers and on the Internet.
- **SCSI (Small Computer System Interface),** a set of ANSI standard electronic interfaces that allow personal computers to communicate with peripheral hardware.
- **TCP/IP (Transmission Control Protocol/Internet Protocol)** is the IETF-endorsed standard communication language or protocol of the Internet.

De facto standards contrast with de jure standards, which have official status as confirmed by a standards organization.

D. Standards organizations

There are a number of well-known international **organizations** that play an important role in the development of open **networking standards**. Some of the most important of these are ISO, ANSI, ITIC, IEEE, EIA/TIA, ITU-T and ETSI.

1. ISO

ISO (International Organization for Standardization) is a worldwide federation of national standards bodies.

ISO is a nongovernmental organization that comprises standards bodies from more than 160 countries, with one standards body representing each member country. The American National Standards Institute (ANSI) for example, represents the United States.

2. Popular standards

Some of the most popular ISO standards for information technology include:

Open Systems Interconnection **(OSI):** Computer manufacturers and telecommunications providers developed this universal reference model for communication protocols in 1983, and ISO later adopted it as a standard.

3. IEEE

Stands for the "Institute of Electrical and Electronics Engineers" and is produced "I triple E." The IEEE is a professional association that develops, defines, and reviews electronics and computer science standards. Its mission is "to foster technological innovation and excellence for the benefit of humanity."

While the Institute of Electrical and Electronics Engineers is based in the United States, IEEE standards often become international standards. Below are a few examples of technologies standardized by the IEEE.

- IEEE 1284 (Parallel Port) – an I/O interface used by early desktop PCs
- IEEE 1394 (Fire wire) – a high-speed interface designed for external hard drives, digital video cameras, and other A/V peripherals
- IEEE 802.11 (Wi-Fi) – a series of Wi-Fi standards used for wireless networking
- IEEE 802.16 (WiMAX) – a wireless communications standard for transferring cellular data

4. ANSI

The acronym **ANSI** stands for **American National Standards Institute**, an organization that has been around for about a century. What is ANSI? Think of it as a large number of expert volunteers getting together as committees under an umbrella term. They come together to establish a set of common guidelines (expectations) for just about anything we depend on, so people can smoothly conduct business and communicate with one another. ANSI doesn't actually make the standards, but it is an umbrella under which standards are made.

ANSI's standard, Z535, looks more broadly at safety and accident prevention information. ANSI Z535 includes six specific standards, which are:

- **ANSI Z535.1** - Safety colors
- **ANSI Z535.2** - Environmental and facility safety signs
- **ANSI Z535.3** - Criteria for all safety symbols
- **ANSI Z535.4** - Product safety signs and labels
- **ANSI Z535.5** - Safety tags and barricade tape
- **ANSI Z535.6** - Product safety information used in manuals and other materials

5. ITU-Formally CCITT

Formerly known as **CCITT**, **ITU** (**International Telecommunication Union**) is the committee of the United Nations that was founded on May 17, 1865. Its job is to make sure all telecommunications devices (e.g., telephones, fax machines, and modems) can "talk to" each other, no matter what company makes them or in what country they're used.

6. EIA

The **Electronic Industries Alliance** (**EIA**; until 1997 **Electronic Industries Association**) was a standards and trade organization composed as an alliance of trade associations for electronics manufacturers in the United States. They developed standards to ensure the equipment of different manufacturers was compatible and interchangeable.

7. Telcodia

The Telcordia Software Module of ITEM ToolKit calculates the reliability prediction of electronic equipment based on the Telcordia (Bellcore) TR-332 and SR-332 standards. These standards use a series of models for various categories of electronic, electrical and electro-mechanical components to predict steady-state

failure rates which environmental conditions, quality levels, electrical stress conditions and various other parameters affect.

The Telcordia standard also documents a recommended method for predicting serial system hardware reliability. It contains instructions for suppliers to follow when providing predictions of their device, unit, or serial system reliability. It can also be used directly by telecommunications service providers for product reliability evaluation

L.O: 2. 3- Identify and apply Network media and connectors

Content/Topic1: Introduction to network media

A. Definition

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

Means used to transport information fall into two main categories: wired means which uses cables and hertzian means or wireless which don't use cables.

B. Types of media

1. Logical (wireless)

- ✓ **Hertian** support (Wireless)

Wireless methods do not use electrical (cables) or optical (fiber optics) conductors. It uses the earth's electromagnetic frequency spectrum. There are three main types of wireless media: radio wave, microwave, and infrared.
Wireless signals are electromagnetic waves that can travel through the vacuum of outer space and through a medium such as air.

Wireless communication uses radio frequencies (RF) or infrared (IR) waves to transmit data between devices on a LAN. For wireless LANs, a key component is the wireless hub, or access point, used for signal distribution.

To receive the signals from the access point, a PC or laptop must install a wireless adapter card (wireless NIC).
Some common applications of wireless data communication include the following:
• Accessing the Internet using a cellular phone
• Establishing a home or business Internet connection over satellite
• Beaming data between two hand-held computing devices
• Using a wireless keyboard and mouse for the PC.
Advantages and disadvantages of wireless LAN

- ✓ **Benefits of Wireless LAN**

The popularity of wireless LANs is a testament primarily to their convenience, cost efficiency, and ease of integration with other networks and network components. The majority of computers sold to consumers today come pre-equipped with all necessary wireless LAN technology.

✓ **The benefits of wireless LANs include:**

- **Convenience** - The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment (home or office). With the increasing saturation of laptop-style computers, this is particularly relevant.
- **Mobility** - With the emergence of public wireless networks, users can access the internet even outside their normal work environment. Most chain coffee shops, for example, offer their customers a wireless connection to the internet at little or no cost.
- **Productivity** - Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place. For a business, this implies that an employee can potentially be more productive as his or her work can be accomplished from any convenient location.
- **Deployment** - Initial setup of an infrastructure-based wireless network requires little more than a single access point. Wired networks, on the other hand, have the additional cost and complexity of actual physical cables being run to numerous locations (which can even be impossible for hard-to-reach locations within a building).
- **Expandability** - Wireless networks can serve a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients would require additional wiring.
- **Cost** - Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated to running physical cables. Wi-Fi chipset pricing continues to come down, making Wi-Fi a very economical networking option and driving inclusion of Wi-Fi in an ever-widening array of devices.

✓ **Disadvantages of Wireless LAN**

Wireless LAN technology, while replete with the conveniences and advantages described above, has its share of downfalls. For a given networking situation, wireless LANs may not be desirable for a number of reasons. Most of these have to do with the inherent limitations of the technology.

- **Security** - Wireless LAN transceivers are designed to serve computers throughout a structure with uninterrupted service using radio frequencies. Because of space and cost, the "antennas" typically present on wireless networking cards in the end computers are generally relatively poor. In order to properly receive signals using such limited antennas throughout even a modest area, the wireless LAN transceiver utilizes a fairly considerable amount of power. What this means is that not only can the wireless packets be intercepted by a nearby adversary's poorly-equipped computer, but more importantly, a user willing to spend a small amount of money on a good quality antenna can pick up packets at a remarkable distance; perhaps hundreds of times the radius as the typical user. In fact, there are even computer users dedicated to locating and sometimes even hacking into wireless networks, known as wardrivers. On a wired network, any adversary would first have to overcome the physical limitation of tapping into the actual wires, but this is not an issue with wireless packets. To combat this consideration, wireless network users usually choose to utilize various encryption technologies available such as WPA. Some of the older encryption methods, such as WEP, are known to have weaknesses that a dedicated adversary can compromise.
- **Range** - The typical range of a common 802.11g network with standard equipment is on the order of tens of meters. While sufficient for a typical home, it will be insufficient in a larger structure. Range varies with frequency band, as Wi-Fi is no exception to the physics of radio wave propagation. To obtain additional range, repeaters or additional access points will have to be

purchased. Costs for these items can add up quickly. Other technologies are in the development phase, however, which feature increased range, hoping to render this disadvantage irrelevant.

- **Reliability** - Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects (such as multipath, or especially in this case Rician fading) that are beyond the control of the network administrator. In the case of typical networks, modulation is achieved by complicated forms of phase-shift keying (PSK) or quadrature amplitude modulation (QAM), making interference and propagation effects all the more disturbing. As a result, important network resources such as servers are rarely connected wirelessly. Also, many 2.4 GHz 802.11b and 802.11g Access points default to the same channel, contributing to congestion on certain channels.
- **Speed** - The speed on most wireless networks (typically 1-108 Mbps) is reasonably slow compared to the slowest common wired networks (100Mbit/s up to several Gbit/s). There are also performance issues caused by TCP and its built-in congestion avoidance. For most users, however, this observation is irrelevant since the speed bottleneck is not in the wireless routing but rather in the outside network connectivity itself. For example, the maximum ADSL throughput (usually 8Mbit/s or less) offered by telecommunications companies to general-purpose customers is already far slower than the slowest wireless network to which it is typically connected. That is to say, in most environments, a wireless network running at its slowest speed is still faster than the internet connection serving it in the first place. However, in specialized environments, the throughput of a wired network might be necessary. Newer standards such as 802.11n are addressing this limitation and will support peak throughputs in the range of 100-200 Mbit/s.
- **Energy** - Power consumption is fairly high compared to some other standards, making battery life and heat a concern.

✓ **(Infrared, Bluetooth, Wifi, Line of sight)**

Wireless LANs – Wireless local area network use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. An example of open-standards wireless radio-wave technology is IEEE 802.11.

✓ **Infrared**

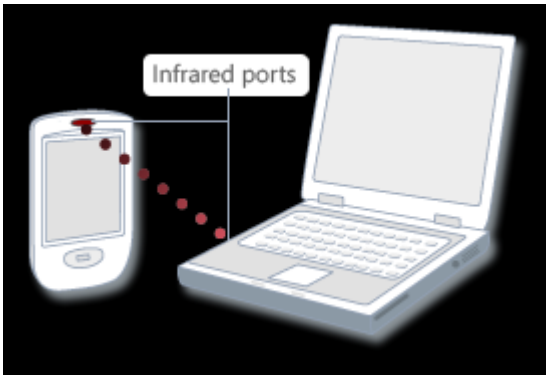
- **Infrared signals are** used for short-range wireless communication in a closed area (not more than 10 meters) using line-of-sight propagation. Theline-of-sight propagation limits the physical positioning of communicating devices. This technology is used to connect various computing devices such as handheld computers. They can transfer files and other digital data bidirectional. Computer infrared adapters both transmit and receive data through ports on the rear or side of a device.

Unlike WIFI and Bluetooth technologies, infrared network signals cannot penetrate walls or other obstructionsand work only in the direct line of sight.

- **Working Principle**

An infrared connection is communication between an infrared receiver and emitter. The infrared emitter sends pulses of infrared light to the receiver. Infrared light is used because it has less problems with interference than other types of light in the visible spectrum. Usually, there are only two devices in the connection, but the system still needs a computer name and a common protocol. The computer name is

needed in case there are multiple devices in the range of the connection. This way, the right devices can be selected for the connection. The use of the protocol has to be explained with the way the devices recognize the infrared signal. A chip inside the device analyses the infrared pulses that come in to detect any patterns. If a pattern is recognized, the appropriate action is executed. In computing devices, these patterns are binary codes. If the infrared light of the emitter is activated, it is sending a binary 1 and if it is off it is sending a 0. The protocol ensures that both devices use the same frequency and packet length for the codes to avoid miscommunication.



- **Performance**

Slow speed(IrDA-SIR)-up to 115 Kps

Medium speed(IrDA-MIR)-up to 1.15 Mbps

Fast speed(IrDA-FIR)-up to 4 Mps

- **Advantages of infrared networking**

- Transmission speeds up to 16 Mbit/s.

- The technology uses a little amount of energy.

- The directed transmission is safe, while it uses a short range direct line of sight signal which is not diffused.

- The infrared technology has been available for a long time, which means that the technology is well developed and that there is a lot of knowledge.

- No cables are needed to enable the connection.

- **Disadvantages of infrared networking**

- The connection is restricted to a small range, with a maximum area depending on the used equipment. (0.3 meters for directed signals and up to five meters for diffused infrared)

- The signal can be of bad quality or can be interrupted due to a wrong angle, distance, noise, heat or light waves.

- Primarily only usable for a connection between two devices.

✓ **Bluetooth**

Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions in the ISM band from 2400-2480 MHz) from fixed and mobile devices, creating personal area networks (PANS) with high levels of security. It has been created by telecoms vendor Ericsson in 1994. It was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. Examples of use:

- Wireless control of and communication between a Bluetooth mobile phone and a handsfree headset.
- Wireless control of and communication between a Bluetooth mobile phone and a Bluetooth compatible car stereo system.
- Wireless Bluetooth headset and intercom.
- Wireless communication with PC input and output devices, the most common being the mouse, keyboard and printer.
- Transfer of files, contact details, calendar appointments, and reminders between devices with OBEX.
- GPS receivers
- Medical equipment
- Bar code scanners
- Traffic control devices
- For low bandwidth applications where higher USB bandwidth is not required and cable-free connection desired.
- Wireless bridge between two industrial Ethernet.

✓ **Wifi(Wireless Fidelity)**

Wi-fi is a mechanism that allows electronic devices to exchange data wiresslly over computer network. A device enabled with wi-fi such as a personal computer, video game console, Smartphone, tablet or digital audio player, can connect to a network resource such as the internet via a wireless network access point. The access point or hotspot has a range of about 20 meters indoors and greater range outdoors. Hotspot coverage can comprise an area as small as a single room signals or a large area, as much as many square miles, covered by multiple overlapping access points.

- **Uses**

To connect to a Wi-Fi LAN, a computer has to be equipped with a wireless network interface controller. The combination of computer and interface controller is called a station. All stations share a single radio frequency communication channel. Transmissions on this channel are received by all stations within range.

The hardware does not signal the user that the transmission was delivered and is therefore called a best-effort delivery mechanism. A carrier wave is used to transmit the data in packets, referred to as "Ethernet frames". Each station is constantly tuned in on the radio frequency communication channel to pick up available transmissions.

A Wi-Fi-enabled device can connect to the Internet when within range of a wireless network connected to the Internet.

- **Advantages**

- Wi-Fi allows cheaper deployment of local area networks (LANs). Also spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs.
- Manufacturers are building wireless network adapters into most laptops. The price of chipsets for Wi-Fi continues to drop, making it an economical networking option included in even more devices.
- Products designated as "Wi-Fi Certified" by the Wi-Fi Alliance are backwards compatible. Unlike mobile phones, any standard Wi-Fi device will work anywhere in the world.
- The current version of Wi-Fi Protected Access encryption (WPA2) as of 2010 is widely considered secure, provided users employ a strong passphrase. New protocols for quality-of-service (WMM) make Wi-Fi more suitable for latency-sensitive applications (such as voice and video); and power saving mechanisms (WMM Power Save) improve battery operation.

- **Disadvantage**

Due to reach requirements for wireless LAN applications, Wi-Fi has fairly high power consumption compared to some other standards.

- **Range**

Wi-Fi networks have limited range. A typical wireless access point using 802.11b or 802.11g with a stock antenna might have a range of 32 m indoors and 95 m outdoors. IEEE 802.11n, however, can exceed that range by more than two times. Range also varies with frequency band. Wi-Fi in the 2.4 GHz frequency block has slightly better range than Wi-Fi in the 5 GHz frequency block which is used by 802.11a. On wireless routers with detachable antennas, it is possible to improve range by fitting upgraded antennas which have higher gain. Outdoor ranges can be improved to many kilometers through the use of high gain directional antennas at the router and remote device(s). In general, the maximum amount of power that a Wi-Fi device can transmit is limited by local regulations, such as FCC Part 15 in the US.

- ✓ **Line of sight**

Line-of-sight propagation refers to electro-magnetic radiation or acoustic wave propagation. Electromagnetic transmission includes light emissions traveling in a straight line. The rays or waves may be diffracted, refracted, reflected, or absorbed by atmosphere and obstructions with material and generally cannot travel over the horizon or behind obstacles.

Microwave system uses very high frequency radio signals to transmit data through space. The transmitter and receiver of a microwave system should be in line-of-sight because the radio signal cannot bend. With microwave very long distance transmission is not possible. In order to overcome the problem of line of sight and power amplification of weak signal, repeaters are used at intervals of 25 to 30 kilometers between the transmitting and receiving end.

Line of sight is used in microwave communication systems which to transmit information from one place to another without interruption, and have clear reproduction at the receiver.Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do.microwaves are limited to line of sight propagation. Their disadvantages is that they cannot pass around hills or mountains as lower frequency radio waves can.

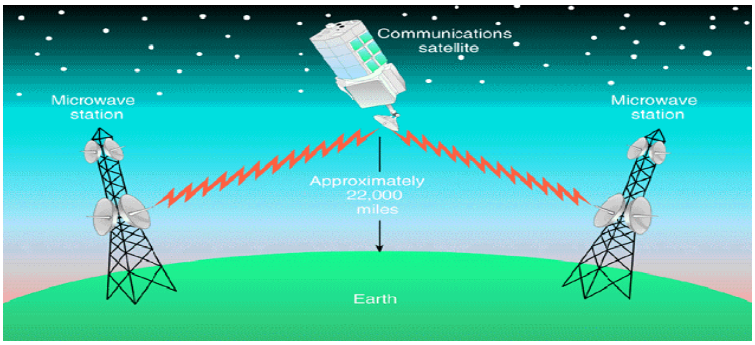
Microwave radio transmission is commonly used in point-to-pointcommunication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

- ✓ **Satellite, line of sight**

  - **Satellite**

- Communications satellites are relay stations that receive signals from one earth station and rebroadcast them to another

- They use microwave radio signals



The satellites are stationed in space, typically 35,400 km (22,000 mi) (for geosynchronous satellites) above the equator. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.

- ✓ **Line of sight**

Line-of-sight propagation
(above 30 MHz)

- ✓ **Transmitting terrestrial**

Terrestrial microwave

– Terrestrial microwaves use Earth-based transmitter and receiver. The equipment looks similar to satellite dishes. Terrestrial microwaves use low-gigahertz range, which limits all communications to line-of-sight. Path between relay stations spaced approx, 48 km (30 mi) apart.

Bands

Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3–30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30–300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz–3 MHz	Sky	AM radio
HF (high frequency)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3–30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30–300 GHz	Line-of-sight	Radar, satellite

2. Physical

Wired means use Ethernet cables and network adapters. This allows connecting two computers using an Ethernet crossover cable. It may also require a central device like hub, switch or router to accommodate more computers.

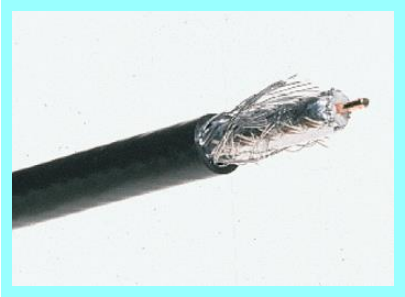
✓ **Coaxial**

- A coaxial cable or coax, is a cable which consists of an inner conductor wire surrounded by insulation, called the dielectric.
- The dielectric is surrounded by a conductive shield, which is surrounded by a non-conductive jacket. Coaxial cable has better data transmission rate than twisted pair

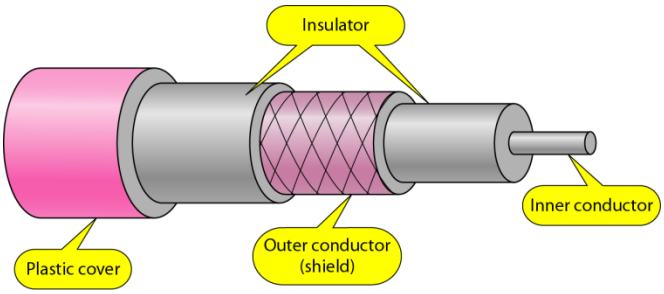
Coaxial cabling is the primary type of cabling used by the cabletelevision industry and is also widely used for computer networks.

Although more expensive than standard telephone wire, it is much less susceptible to interference and can carry much more data.

Note: The shield minimizes electrical and radio frequency interference.



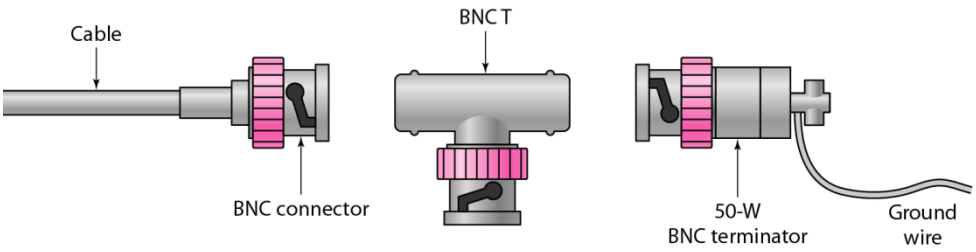
It consists of a hollow outer cylindrical conductor that surrounds a single inner wire conductor.



- **Categories of coaxial cables**

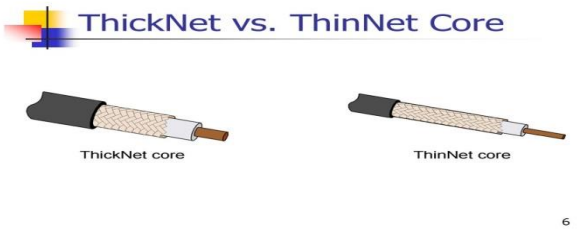
Category	Use
RG-59	Cable TV
RG-58	Thin Ethernet
RG-11	Thick Ethernet

BNC



The following summarizes the features of coaxial cables:
Speed and throughput—10 to 100 Mbps
Average cost per node—Inexpensive
Media and connector size—Medium
Maximum cable length—500 m (medium)

- **Thinnet Vs Thicknet coaxial cable**



Ethernet based LANs using thick cable for inter-connection is referred as Thicknet. While ethernet systems using thinner coaxial cable is referred as Thinnet.

Thicknet is also referred as 10Base5 systems, where 10 means 10Mbps speed. Base means baseband and 5 denotes 500meter max. distance between nodes/repeaters. RG-8/U cable is used as thick cable in thicknet based LAN network.

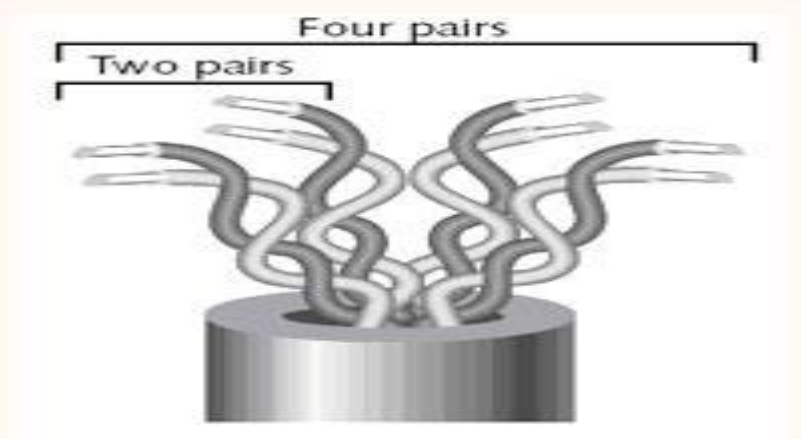
Thinnet is also referred as 10Base2, where 2 denotes 200 m max. distance between two nodes or repeaters. RG-58/U is used as thin cable in thinnet based LAN network.

- ✓ **Twisted pair**

- **UTP, STP**

- **Twisted pair cable**

Twisted pair(TP) cable is similar to telephone wiring and consists of color-coded pairs of insulated copper wires. The more twists per inch in a pair of wires, the more resistant the pair will be to all forms of noise. Higher-quality, more expensive twisted-pair cable contains more twists per foot. The number of twists per meter or foot is known as the twist ratio.



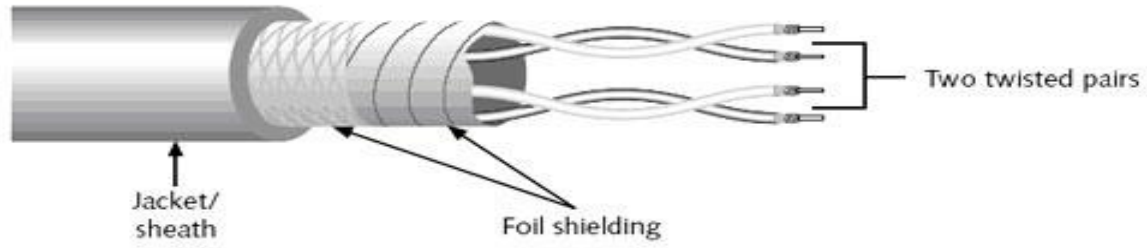
Twisted-pair cable is the most common form of cabling found on LANs today. It's inexpensive, flexible, and easy to install, and it can span a significant distance before requiring a repeater (though not as far as coaxial). Twisted-pair cable easily accommodates several different topologies, although it is most often implemented in star or star-hybrid topologies

One drawback to twisted-pair is that, because of its flexibility, it is more prone to physical damage than coaxial cable. All twisted-pair cable falls into one of **two categories:**

- Shielded twisted-pair (STP)
- Unshielded twisted-pair (UTP).

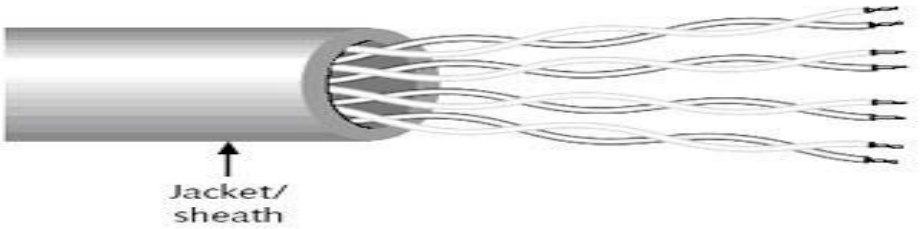
- **Shielded twisted-pair (STP)**

As the name implies, shielded twisted-pair (STP) cable consists of twisted wire pairs that are not only individually insulated, but also surrounded by a shielding made of a metallic substance such as foil. Some STP uses a braided metal shielding. The shielding acts as a barrier to external electromagnetic forces, thus preventing them from affecting the signals traveling over the wire inside the shielding. The shielding may be grounded to enhance its protective effect.



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

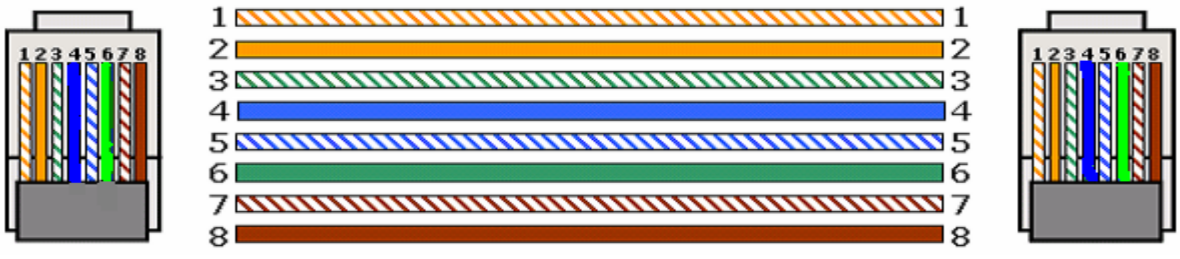
Unshielded twisted-pair (UTP) cabling consists of one or more insulated wire pairs encased in a plastic sheath. As its name implies, UTP does not contain additional shielding for the twisted pairs. As a result, UTP is both less expensive and less resistant to noise than STP



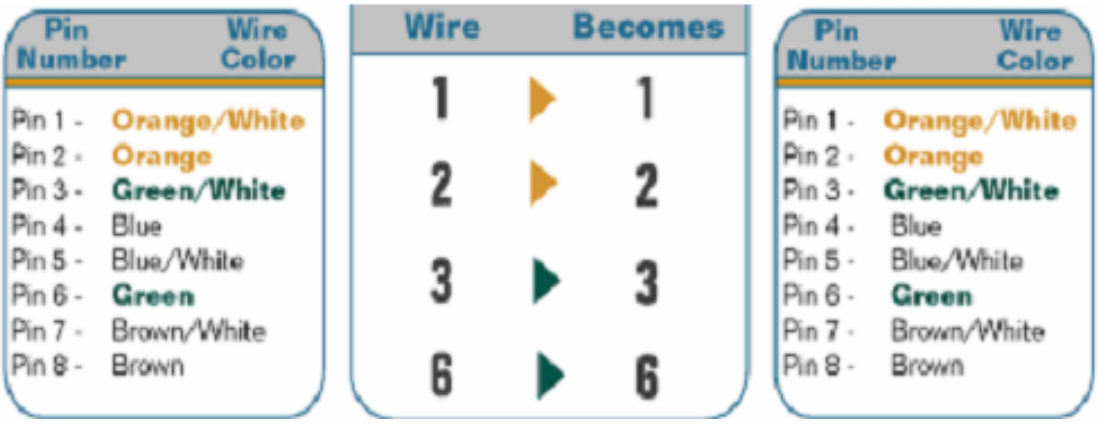
- **UTP Types**

	UTP CAT 1/2/3/4/5/6
Cat 1	Data Rate upto 1 Mbps - Telephone Line
Cat 2	Data Rate upto 4 Mbps - Token Ring
Cat 3	Data Rate upto 10 Mbps - Token Ring & 10 Base - T
Cat 4	Data Rate upto 16 Mbps - Token Ring
Cat 5	Data Rate upto 100 Mbps Ethernet - 16 for Token
Cat 5e	Data Rate upto 1000 Mbps Ethernet
Cat 6	Data Rate upto 1000 Mbps Ethernet

- ✓ **UTP cabling**
- ✓ **UTP straight through cable**



2)Coaxial cable



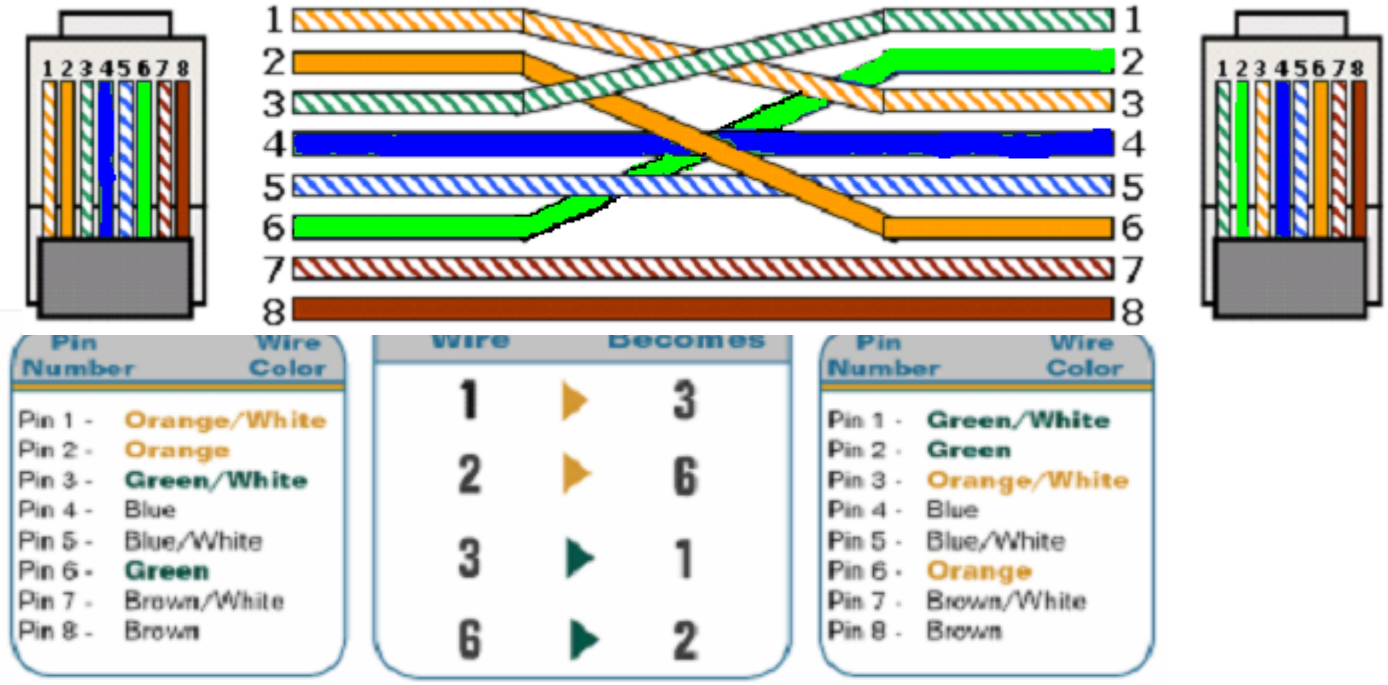
In a UTP implementation of a straight-through cable, the wires on both cable ends are in the same order.

You can determine that the wiring is a straight-through cable by holding both ends of the UTP cable side by side and seeing that the order of the wires on both ends is identical

You can use a straight-through cable for the following tasks

- Connecting a router to a hub or switch
- Connecting a server to a hub or switch
- Connecting computer to a hub or switch

✓ **UTP Crossover Cable**



In the implementation of a crossover, the wires on each end of the cable are crossed

Transmit to receive and receive to Transmit on each side, for both tip and ring

Notice that pin 1 on one side connects to pin 3 on the other side, and pin 2 connects to pin 6 on the opposite end

You can use a crossover cable for the following tasks:

- Connecting switch to switch
- Connecting hubs to switch
- Connecting a hub to another hub
- Connecting router to router
- Connecting router to computer
- Connecting computer to computer
- **UTP cable connectors**
- RJ-11 – Defined for telephone connectors
- RJ-45 – Defined for UTP connectors

RJ 11 RJ 45

- ✓ **Fiber optic**

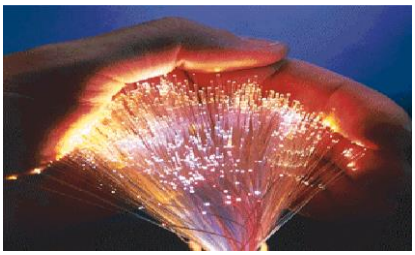
Fiber optic cable is considered the default choice for connections involving high speed [large bandwidth requirements like video, large database systems], long distances and interconnecting networks. It costs more than either twisted pair or coax, and requires special connectors and jointing methods.

Fiber optics has several advantages over traditional metalcommunications lines:

- Fiber optic cables have a much greater bandwidth than metal cables. This means that they can carry more data
- Fiber optic cables are less susceptible than metal cables to interference
- Fiber optic cables are much thinner and lighter than metal wires
- Data can be transmitted digitally (the natural form for computer data) rather than analogically.

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

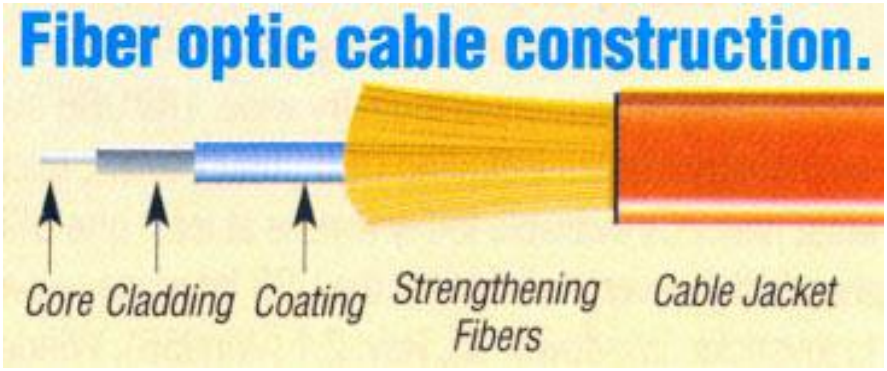
Fiber optics is a particularly popular technology for local-area networks. In addition, telephone companies are steadily replacing traditional telephone lines with fiber optic cables. In the future, almost all communications will employ fiber optics.



Fiber-optic cable is a networking medium capable of conducting modulated light Transmission.

The features of fiber-optic cable systems are,

- expensive
- used for backbones [linking LANs together]
- high capacity [100Mbps]
- immune to electromagnetic interference
- low loss
- difficult to join
- connectors are expensive
- long distance



- **Types of fiber optic cables**
- Single Mode
- Multi-Mode

✓ **Multimode fiber**

Multi-mode consists of a core of glass surrounded by another kind of glass with a different refractive index. Multimode fiber is characterized by the bandwidth-distance product which tells how far a signal can be transmitted before it becomes too spread out. A typical value is 200 MHz-km.

Multi-mode fiber optic cables are used in campus. The fiber inside buildings is 160 MHz-km and the fiber outside buildings is 200 MHz-km bandwidth-distance product. Multi-mode fiber can carry data up to about 100 Mb/s for about 2000 meters. Either a light emitting diode or a laser can drive multi-mode fiber.

- **Single mode fiber**

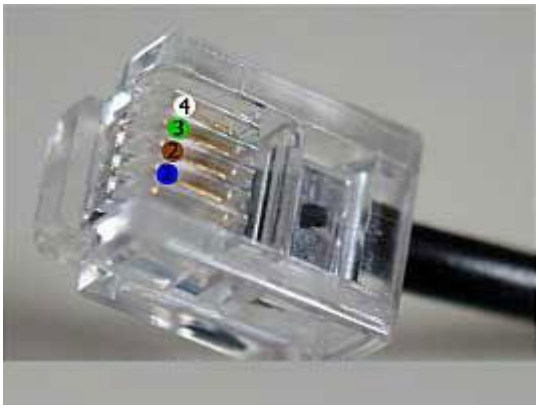
Single-modefiber optic cable consists of a smaller glass fiber than multi-mode fiber. Single mode fiber can transmit data for longer distances at higher rates than multi-mode fiber. A laser drives single mode fiber

Content/Topic2: Description of Types of network connectors

1. **RJ45,RJ11**

✓ **RJ-11 (Registered Jack)**

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



✓ **RJ-45 (Registered Jack)**

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

2. **BNC**

The Bayonet Neill-Concelman Connector (BNC connector) is a type of coaxial RF (Radio frequency) electrical connector that is used in place of coaxial connectors. A BNC connector connects various radio frequencies up to 3GHz and voltages under 500V DC and are used in electronic architectures such as audio, video and networking.

3. **USB (**Universal Serial Bus)

Universal Serial Bus, or USB, is a computer standard designed to eliminate the guesswork in connecting peripherals to a PC. It is expected to replace serial and parallel ports. A single USB port can be used to connect up to 127 peripheral devices, such as mice, modems, keyboards, digital camera's, printers, scanners, MP3 players and many more. USB also supports Plug-and-Play installation and hot plugging.

- USB 1.1 standard supports data transfer rates of 12 Mbps.
- USB 2.0 (Also referred to as Hi-Speed USB) specification defines a new High-speed transfer rate of 480 Mb/sec.

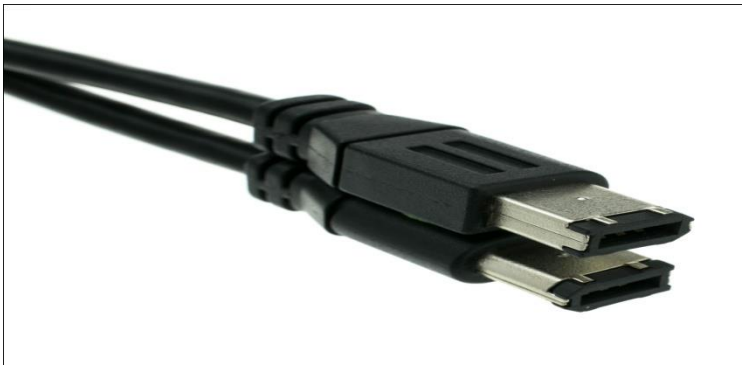
USB 2.0 is fully compatible with USB 1.1 and uses the same cables and connectors. USB has with two connector types. The first is Type A (on the right), This connector connects to the PC's USB port. The Type B (on the left) connector and is for connecting to the relevant peripheral. Whereas the type A connector is truly standard, the Type B connector could be changed in size etc. with individual peripherals meaning they require their own unique cables.

4. **Fire wire**

FireWire is Apple Computer's version of a standard, IEEE 1394, High Performance Serial Bus, for connecting devices to your personal computer. FireWire provides a single plug-and-socket connection on which up to 63 devices can be attached with data transfer speeds up to 400 Mbps (megabits per second). The standard

describes a serialbus or pathway between one or more peripheral devices and your computer's microprocessor. Many peripheral devices now come equipped to meet IEEE 1394

In time, IEEE 1394 implementations are expected to replace and consolidate today's serial and parallel interfaces. The first products to be introduced with FireWire include digital cameras, digital video disks (DVDs), digital video tapes, digital camcorders, and music systems.



Fire wire 400 6 Pin cable, IEEE-1394a

5. **VGA**

A VGA cable is used to connect an analog PC monitor to a PC or laptop. VGA cables utilize an HD15 connector (male or female depending on the equipment being attached) to connect the monitor and PC/laptop. L-com offers a very extensive selection of off the shelf VGA cable assemblies and can custom manufacture VGA video cable assemblies to your exact specifications.

HD15 Connector Configuration

Typical VGA Cable

6. **BNC-T**

A **tee connector** is an electrical connector that connects three cables together. It is usually in the shape of a capital T. It is usually used for coax cables and the three connector points can be either female or male gender, and could be different or the same standard, such as F type, BNC or N type.

Tee connectors can be used to split radio frequency power from a cable into two. They can be used to attach a piece of electronic test equipment. T connectors were much used on co-axial 10M Ethernet networks.

7. F type

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

8. RS-232

In telecommunications, **RS-232**, **Recommended Standard 232**[1] is a standard introduced in 1960[2] for serial communication transmission of data. It formally defines the signals connecting between a *DTE* (*data terminal equipment*) such as a computer terminal, and a *DCE* (*data circuit-terminating equipment* or *data communication equipment*), such as a modem.

C. Advantages and disadvantages of media

Advantages of a Wireless Network over Wired

- As I mentioned in the introduction, the main advantage of a wireless network over a wired one is that users can move around freely within the area of the network with their laptops, handheld devices etc and get an internet connection.
- Users are also able to share files and other resources with other devices that are connected to the network without having to be cabled to a port.
- Not having to lay lots of cables and put them through walls etc. can be a considerable advantage in terms of time and expense. It also makes it easier to add extra devices to the network, as no new cabling is needed.
- If you are a business such as a café, having a wireless network that is accessible to customers can bring you extra business. Customers generally love wireless networks because they are convenient.
- Wireless networks can sometimes handle a larger amount of users because they are not limited by a specific number of connection ports.
- Instant transfer of information to social media is made much easier. For instance, taking a photograph and uploading it to Facebook can generally be done much quicker with wireless technology.

C. Disadvantages of a Wireless Network

- It can require extra costs and equipment to set up, although increasingly routers have built-in wireless capability, as do devices such as laptops, handheld devices, modern DVD players, and TVs.
- Setting up a wireless network can sometimes be difficult for people who are not experienced with computers. (Although there are issues with setting up a wired network too, off course!)
- File-sharing transfer speeds are normally slower with wireless networks than they are with cabled. The speeds can also vary considerably according to your location in relation to the network.
- The general speed of a wireless connection is also usually much slower than a wired one. The connection also gets worse the farther you are from the router, which can be a problem in a large building or space.
- Wireless connections can be obstructed by everyday household items and structures such as walls, ceilings, and furniture.
- Wireless networks are generally less secure. There can also be problems with neighbors stealing bandwidth, if the network hasn't been set up to be password protected. Information is also less secure too and can be easier to hack into.

D. ACCESS METHODS

1. **CSMA/CA** Carrie Sense Multiple Access with collision Avoid is a protocol that allows multiple accesses method in which carrier sensing used, but nodes attempt to avoid collision by transmitting only when the channel is sensed to be "unused" when they do transmit, nodes transmit their packet data in its entirety. Is also a protocol for carrier transmission in 802.11 networks?

- Carrier-Sense: This means the NIC (or network interface card) on each computer on the network "listens" and senses whether there is traffic on the cable before sending.
- Carrier-Sense: This means the NIC (or network interface card) on each computer on the network "listens" and senses whether there is traffic on the cable before sending.

- Multiple Access: This means all computers have access to the cable at any given time (making this a contention method of access control)
- Multiple Access: This means all computers have access to the cable at any given time (making this a contention method of access control)
- Collision Detection: This means that ***collisions*** may occur, if two computers send data at exactly the same time--but the NICs of the sending computers will detect that a collision has occurred so they can re-send their data

✓ **Advantages of CSMA/CA**

- Effective; Avoids data collisions.
- Reliable; Intent signals are sent until the cable is clear so that data will travel and reach its destination safely.

✓ **Disadvantages of CSMA/CA**

- Relatively slow; A signal of intent must be sent *every* time a computer wants to transmit causing signal traffic.
- Inappropriate for large/active networks; The slowdown increases, as the network grows larger.
- Limited; suffers from same distance limitations as CSMA/CD since it must listen for the signals of intent.

2. **CSMA/CD** Carrie Sense Multiple Access with collision detection is a media access control method used most especially in early Ethernet technology for local area networking. It user carrier sensing schema in which a transmitting station detects collisions by sensing transmission from other station while transmitting a frame.

✓ **Advantages of CSMA/CD**

- Reliable; Collisions are detected and packets are re-sent, so no data is lost.
- Relatively fast; A computer does not have to wait its "turn" to transmit data.

✓ **Disadvantages of CDMA/CD**

- Limited to 2500 meters/11/2 mile; the collision detection mechanism restricts the length of cable segment that can be used.
- Inappropriate for large/active networks; Collisions slow the network and clog bandwidth with retransmissions.

✓ **<u>Summary</u>**

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a modification of CSMA in which each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear. Sometimes two computers attempt to transmit at the same instant. When this happens, a collision occurs. Each computer then backs off and waits a random amount of time before attempting to retransmit.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. This removes the possibility for collisions to occur.

3. **Token Passing** in telecommunication, token passing is a channel access method where a signal called token passed between nodes that authorizes the node to communicate.

✓ **Advantages of Token Passing**

- Non-contention method; Computers do not compete for access to the cable. Each computer will get its "turn" as the token comes around the network.
- Effective; Collisions are prevented altogether.
- Reliable; the maximum amount of time before a given computer will be able to transmit can be calculated.

✓ **Disadvantages of Token Passing**

- Slow; a large amount of network bandwidth is consumed in the process.
- Costly; Implementation is expensive due to the media and equipment used.

Summary

CSMA/CD (Carrier Sense Multiple Access/Collision Detection)

In CSMA/CD (Carrier Sense Multiple Access/Collision Detection) Access Method, every host has equal access to the wire and can place data on the wire when the wire is free from traffic. When a host want to place data on the wire, it will “sense” the wire to find whether there is a signal already on the wire. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted, to avoid collision again.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

In CSMA/CA, before a host sends real data on the wire it will “sense” the wire to check if the wire is free. If the wire is free, it will send a piece of “dummy” data on the wire to see whether it collides with any other data. If it does not collide, the host will assume that the real data also will not collide.

Token Passing

In CSMA/CD and CSMA/CA the chances of **collisions** are there. As the number of hosts in the network increases, the chances of **collisions** also will become more. In token passing, when a host want to transmit data, it should hold the token, which is an empty packet. The token is circling the network in a very high speed. If any workstation wants to send data, it should wait for the token. When the token has reached the workstation, the workstation can take the token from the network, fill it with data, mark the token as being used and place the token back to the network.

LEARNING UNIT 3 - Apply IP addressing (IP v4)

L O 3.1- Describe IP addressing concepts

Content/Topic1: Introduction to IP address

A. Definition

1. **An IP address** is a logical address for a network adapter. The IP address uniquely identifies computers on a TCP/IP network.

An IP address can be private - for use on a local area network (LAN) - or public - for use on the Internet or other wide area network (WAN).

Internet Protocol (IP) technology was developed in the 1970s to support some of the first research computer networks. Today, IP has become a worldwide standard for home and business networking as well. Our network routers, Web browsers, email programs, instant messaging software - all rely on IP or other network protocols layered on top of IP.

An IP address is a number that uniquely identifies every host on an IP network. IP addresses operate at the Network layer of the TCP/IP Network protocol stack, so they are independent of lower-level Data Link layer MAC addresses, such as Ethernet MAC addresses.

2. Address Space

A protocol like IPv4 that defines addresses has an **address space.** An address space is the total number of addresses used by the protocol. If a protocol uses b bits to define an address, the address space is 2^b because each bit can have two different values (0 or 1).

IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than four billion). Theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet.

The address space of IPv4 is 2^{32} or 4,294,967,296.

3. IPv4 Addressing Notation

An IPv4 address consists of four bytes (32 bits). These bytes are also known as octets. Octets can take any value between 0 and 255.

For readability purposes, humans typically work with IP addresses in a notation called **dotted decimal**. This notation places periods between each of the four numbers (octets) that comprise an IP address. For example, an IP address that computers see as

00001010 00000000 00000000 00000001

is written in dotted decimal as10.0.0.1Because each byte contains 8 bits, each octet in an IP address ranges in value from a minimum of 0 to a maximum of 255. Therefore, the full range of IP addresses is from**0.0.0.0** through **255.255.255.255**. That represents a total of 4,294,967,296 possible IP addresses.

B. IP addressing classification

IP addresses, when started a few decades ago, used the concept of classes. This architecture is called **class full addressing.**
IP address classes include:

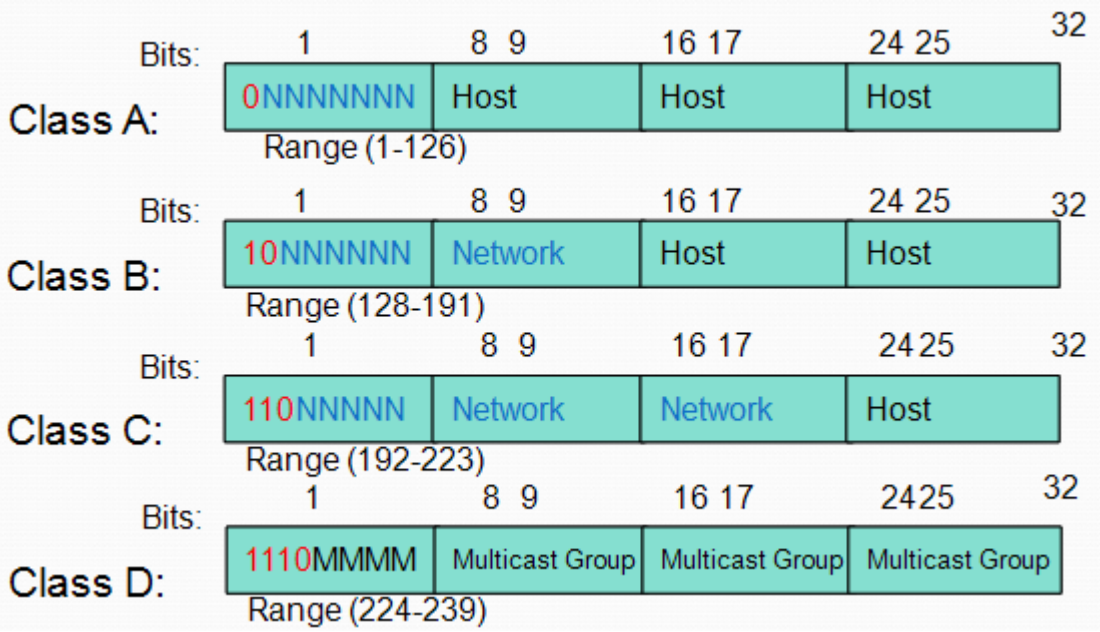
a. Class A

b. Class B

c. Class C

d. Class D: multicast

E. Class E: reserved



Class A

This class is assigned to very large Networks, such as major international companies.

Class A licenses assigns numbers to be used in the first octet (leftmost) of the address, which becomes the network address.

The other three octets on the right of the IP can be used for host addresses that identify each host on this network.

Example:

If a company assigns 87 as its class A network address, then 87 is issued as the first octet for every host on that network.

Example of IP addresses for hosts on this network are 87.0.0.1, 87.0.0.2, 87.0.0.3 etc.

NET HOST OR NODE

87.0.0.2

The last octet does not use 0 or 255 as a value. Example, 87.0.0.0 or 87.0.0.255 are not valid on class A.

The number of hosts in class A are approximately 16,000

i.e.

87.255 * 255 * 254 = 16,516.350

Class B

Class B is used for the medium sized networks.

The class B license assigns a number for each of the first two left most octets, leaning the last two octets for host addresses.

The possible number of hosts in class B are about 65,000.

I.e. 255 * 255 = 65,536

The first octet for class B license is between 128 and 191, which gives about 63 different values for a class B first octet.

The second number can be between 0 and 255.

There are approximately 16,000 networks in

class B.

L.e 63 * 255 = 16,128

Example:

Suppose a company assigned an IP address 135.18 as the network address for its class B license. The first octets for all the networks will be 135.18 and the last two octets are used for host addresses.

Example:

NET	HOST OR NODE
135.18	.0.1

Class c addresses are commonly used for small to mid- size networks.

A class C license assigns three octets as the network addresses and can have 254 host addresses.

The three first octets are assigned to the Network ID

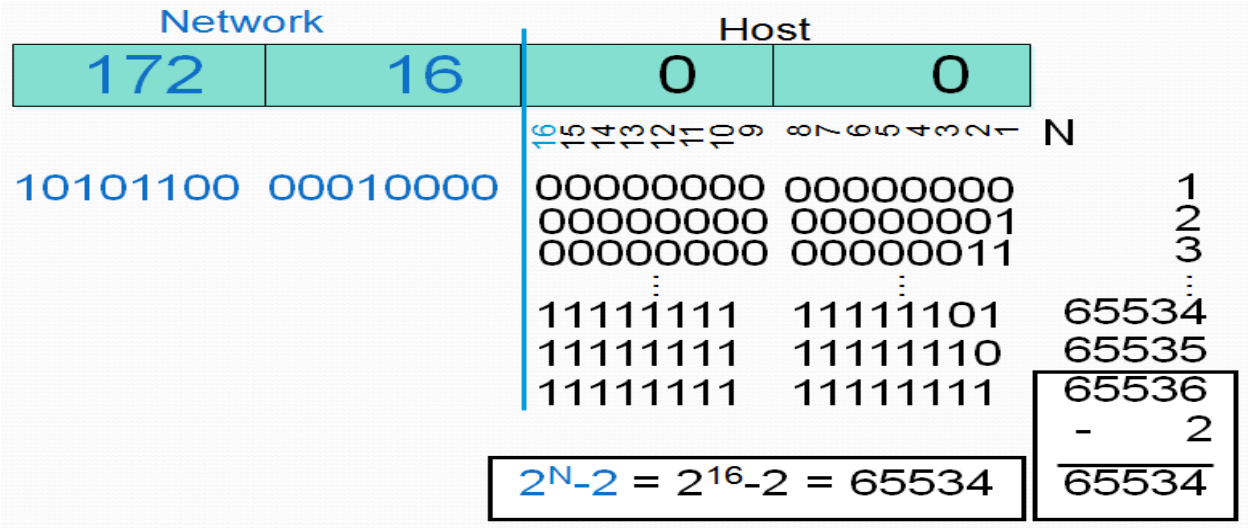
The first number of the class C is between 192 and 254.

Example:

A company can be assigned a class C license for its network with a network address of 200.80.15. Some of the IP addresses in such a network are

200.80.15.1, 200.80.15.0,200.80.15.0 etc.

Determining Available Host Addresses



IP Address Classes Exercise

Address	Class	Network	Host
10.2.1.1			
128.63.2.100			
201.222.5.64			
192.6.141.2			
130.113.64.16			
256.241.201.10			

Content/Topic2: IP addresses grouping

A. **IP protocols enforce the following grouping concept**

All hosts in the same **group** must not be separated by an **IP** router. A corollary to the **grouping** concept is this: Hosts separated by an **IP** router must be in separate groups. Without sub netting, the smallest **group** is a single, entire Class A, B, or C network number.

B. IP Grouping Concepts and Sub netting

The creators of the Internet realized the impracticality of the original network-numbering conventions early on. Computing history shows many examples of people being unable to conceive the idea that computing technology would grow as fast as it has. Needless to say, the Internet would have run out of

Class A, B, and C networks long ago if additional addressing features had not been created. Sub netting provided the first significant addressing feature that conserved the global IP address space.

IP sub netting creates vastly larger numbers of smaller groups of IP addresses, compared with simply using Class A, B, and C conventions. The Class A, B, and C rules still exist—but now, a single Class A, B, or C network can be subdivided into many smaller groups. Sub netting treats a subdivision of a single Class A, B, or C network as if it were a network itself. By doing so, a single Class A, B, or C network can be subdivided into many non-overlapping subnets.

The needs for sub netting are both technical and administrative, as documented in the following list:

• All organizations connected to the Internet (and not using IP address translation) are required to use IP networks registered with the NIC.

• IP protocols enforce the following grouping concept: All hosts in the same group must not be separated by an IP router.

• A corollary to the grouping concept is this: Hosts separated by an IP router must be in separate groups.

• Without sub netting, the smallest group is a single, entire Class A, B, or C network number.

• Without sub netting, the NIC would be woefully short of assignable networks.

• With sub netting, the NIC can assign one or a few network numbers to an organization, and then the organization can subdivide those networks into subnets of more usable sizes.

c. Rules for Grouping IP Addresses

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

Content/Topic3: IP addressing scheme and subnet masks

A. IP addressing scheme

The IP header has 32 bits assigned for addressing a desired device on the network. An IP address is a unique identifier used to locate a device on the IP network. To make the system scalable, the address structure is subdivided into the *network* ID and the *host* ID. The network ID identifies the network the device belongs to; the host ID identifies the device. This implies that all devices belonging to the same network have a single network ID. Based on the bit positioning assigned to the network ID and the host ID, the IP address is further subdivided into classes A, B, C, D (multicast), and E (reserved), as shown in Figure1.

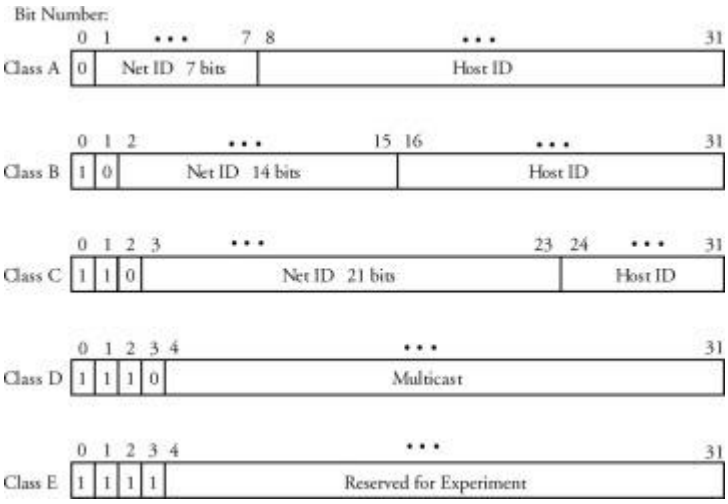


Figure1. Classes of IP addresses

Consider the lengths of corresponding fields for each class shown in this figure1:

- Class A starts with 0 followed by 7 bits of network ID and 24 bits of host ID.
- Class B starts with 10 followed by 14 bits of network ID and 16 bits of host ID.
- Class C starts with 110 followed by 21 bits of network ID and 8 bits of host ID.
- Class D starts with 1110 followed by 28 bits. Class D is used only for multicast addressing by which a group of hosts form a multicast group and each group requires a multicast address. Chapter 6 is entirely dedicated to multicast techniques and routing.
- Class E starts with 1111 followed by 28 bits. Class E is reserved for network experiments only.

For ease of use, the IP address is represented in *dot-decimal* notation. The address is grouped into four dot-separated bytes. For example, an IP address with 32 bits of all 0s can be shown by a dot-decimal form of 0.0.0.0 where each 0 is the representation of 00000000 in a logic bit format.

A detailed comparison of IP addressing is shown in the Table 1.1. Note that in this table, each of the "number of available network addresses" and the "number of available host addresses per network" has already been decreased by 2. For example, in class A, the size of the network ID field is indicated in the table to be $N = 7$; however, the number of available network addresses is presented as $2^N - 2 = 128 - 2 = 126$. The subtraction of 2 adjusts for the use of the all-bits-zero network ID (0 in decimal) and the all-bits-one network ID (127 in decimal). These two network IDs, 0 and 127, are reserved for management and cannot be available for any other use. The same argument is true for the number of available host addresses, where with the size of the host ID field indicated as $N = 24$, we can have $2^N - 2 = 16,777, 216 - 2 = 16,777, 214$ host addresses per network available for use. The last two columns of the table show the start address and the end address of each class, including the reserved addresses explained earlier.

Table 1.1 Comparison of IP addressing schemes

Class	Bits to Start	Size of Network ID Field	Size of Host ID Field	Number of Available Network Addresses	Number of Available Host Addresses per Network	Start Address	End Address
A	0	7	24	126	16,777,214	0.0.0.0	127.255.255.255
B	10	14	16	16,382	65,534	128.0.0.0	191.255.255.255
c	110	21	8	2,097,150	254	192.0.0.0	223.255.255.255
D	1110	N/A	N/A	N/A	N/A	224.0.0.0	239.255.255.255
E	1111	N/A	N/A	N/A	N/A	240.0.0.0	255.255.255.255

Example. A host has an IP address of 10001000 11100101 11001001 00010000. Find the class and decimal equivalence of the IP address.

Solution. The host's IP address belongs to class B, since it starts with 10. Its decimal equivalent is 136.229.201.16.

C. Subnet Addressing and Masking

The concept of sub netting was introduced to overcome the shortcomings of IP addressing. Managing a large number of hosts is an enormous task. For example, a company that uses a class B addressing scheme can support up to 65,535 hosts on one network. If the company has more than one network, a multiple-network address scheme, or *subnet scheme*, is used. In this scheme, the host ID of the original IP address is subdivided into *subnet ID* and *host ID*, as shown in Figure 2.

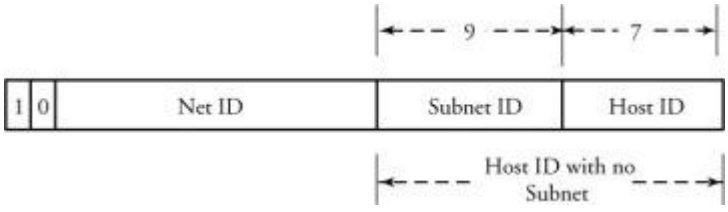


Figure2. A subnet ID and host ID in class B addressing

Depending on the network size, different values of subnet ID and host ID can be chosen. Doing so would prevent the outside world from being burdened by a shortage of new network addresses. To determine the sub netting number, a subnet *mask*—logic AND function—is used. The subnet mask has a field of all 0s for the host ID and a field of all 1s for the remaining field.

Example. Given an IP address of 150.100.14.163 and a subnet mask of 255.255.255.128, determine the maximum number of hosts per subnet.

Solution. Figure shows the details of the solution. Masking 255.255.255.128 on the IP address results in 150.100.14.128. Clearly, the IP address 150.100.14.163 is a class B address. In a class B address, the lower 16 bits are assigned to the subnet and host fields. Applying the mask, we see that the maximum number of hosts is $2^7 = 128$.

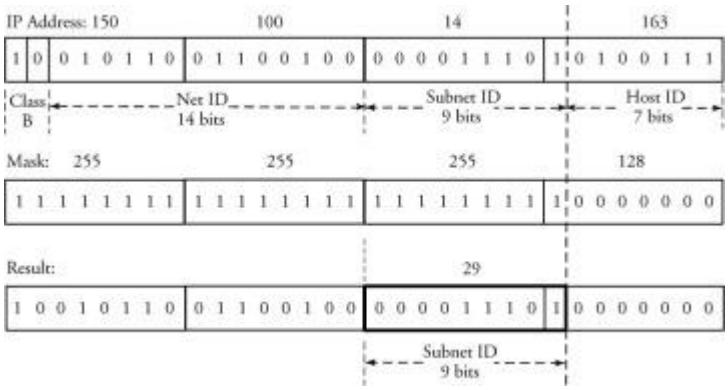


Figure 3. An example of subnet and masking

Example. A router attached to a network receives a packet with the destination IP address 190.155.16.16. The network is assigned an address of 190.155.0.0. Assume that the network has two subnets with addresses 190.155.16.0 and 190.155.15.0 and that both subnet ID fields have 8 bits. Demonstrate the details of routing the packet.

Solution. When it receives the packet, the router determines to which subnet the packet needs to be routed, as follows: The destination IP address is 190.155.16.16, the subnet mask used in the router is 255.255.255.0, and the result is 190.155.16.0. The router looks up its routing table for the next subnet corresponding to the subnet 190.155.16.0, which is subnet 2. When the packet arrives at subnet 2, the router determines that the destination is on its own subnet and routes the packet to its destination.

Content/Topic4: Examining the prefix length and Public and private addresses

- **Examining the prefix length**

The **prefix length** is the number of bits set to 1 in the subnet mask. It is written in "slash notation", a "/" followed by the number of bits set to 1. For example, if the subnet mask is 255.255. 255.0, there are 24 bits set to 1 in the binary version of the subnet mask, so the **prefix length** is 24 bits or /24.

The prefix length is another way of expressing the subnet mask. The prefix length is the number of bits set to 1 in the subnet mask. It is written in "slash notation", a "/" followed by the number of bits set to 1. For example, if the subnet mask is 255.255.255.0, there are 24 bits set to 1 in the binary version of the subnet mask, so the prefix length is 24 bits or /24. The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address.

Networks are not always assigned a /24 prefix. Depending on the number of hosts on the network, the prefix assigned may be different. Having a different prefix number changes the host range and broadcast address for each network.

D. Public and private addresses

1. **Private** IP **address** is used with a local network and
2. **public** IP **address** is used outside the network. **Public** IP **address** is provided by ISP, Internet Service Provider. ... **Private** IP **Address** is used to communicate within the network. **Public** IP **Address** is used to communicate outside the network.

Private IP Address and Public IP Address are used to uniquely identify a machine on the internet. Private IP address is used with a local network and public IP address is used outside the network. Public IP address is provided by ISP, Internet Service Provider.

Following are the important differences between Private IP Address and Public IP Address.

Sr. No.	Key	Private IP Address	Public IP Address
1	Scope	Private IP address scope is local to present network.	Public IP address scope is global.
2	Communication	Private IP Address is used to communicate within the network.	Public IP Address is used to communicate outside the network.
3	Format	Private IP Addresses differ in a uniform manner.	Public IP Addresses differ in varying range.
4	Provider	Local Network Operator creates private IP addresses using network operating system.	ISP, Internet Service Provider controls the public IP address.
5	Cost	Private IP Addresses are free of cost.	Public IP Address comes with a cost.
6	Locate	Private IP Address can be located using ipconfig command.	Public IP Address needs to be searched on search engine like google.
7	Range	Private IP Address range:	Except private IP Addresses, rest IP addresses are public.

Sr. No.	Key	Private IP Address	Public IP Address
		10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255	
8	Example	Private IP Address is like 192.168.11.50.	Public IP Address is like 17.5.7.8.

L.O 3.2: Apply IPv4 assignment

Content/Topic1: Introduction to IPv4

A. IPv4

1. **Internet Protocol Version 4 (IPv4)** is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. **IPv4** is a connectionless protocol used in packet-switched layer networks, such as Ethernet. ... **IPv4** is defined and specified in IETF publication RFC 791.

Internet Protocol version 4 (**IPv4**) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks. IPv4 was the first version deployed for production on SATNET in 1982 and on the ARPANET in January 1983. It still routes most Internet traffic today,[1] despite the ongoing deployment of a successor protocol, IPv6.

IPv4 uses a 32-bit address space which provides 4,294,967,296 (2^{32}) unique addresses, but large blocks are reserved for special networking methods.

2. History

The IP layer was originally separated in the v3 of the TCP for design improvement, and stabilized in version 4.

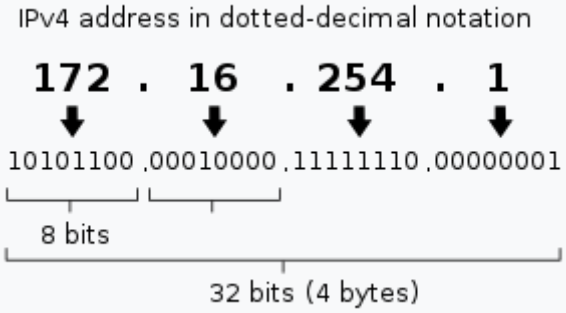
IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980). In March 1982, the US Department of Defense declared TCP/IP as the standard for all military computer networking.

3. Purpose

The Internet Protocol is the protocol that defines and enables internetworking at the internet layer of the Internet Protocol Suite. In essence it forms the Internet. It uses a logical addressing system and performs *routing*, which is the forwarding of packets from a source host to the next router that is one hop closer to the intended destination host on another network.

IPv4 is a connectionless protocol, and operates on a best-effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).

4. Addressing



Decomposition of the quad-dotted IPv4 address representation to its binary value

IPv4 uses 32-bit addresses which limits the address space to 4294967296 (2^{32}) addresses.

IPv4 reserves special address blocks for private networks (~18 million addresses) and multicast addresses (~270 million addresses).

5. Address representations

IPv4 addresses may be represented in any notation expressing a 32-bit integer value. They are most often written in dot-decimal notation, which consists of four octets of the address expressed individually in decimal numbers and separated by periods.

For example, the quad-dotted IP address *192.0.2.235* represents the 32-bit decimal number 3221226219, which in hexadecimal format is 0xC00002EB. This may also be expressed in dotted hex format as 0xC0.0x00.0x02.0xEB, or with octal byte values as 0300.0000.0002.0353.

CIDR notation combines the address with its routing prefix in a compact format, in which the address is followed by a slash character (/) and the count of leading consecutive *1* bits in the routing prefix (subnet mask).

Other address representations were in common use when classful networking was practiced. For example, the loopback address *127.0.0.1* is commonly written as *127.1*, given that it belongs to a class-A network with eight bits for the network mask and 24 bits for the host number. When fewer than four numbers are specified in the address in dotted notation, the last value is treated as an integer of as many bytes as are required to fill out the address to four octets. Thus, the address *127.65530* is equivalent to *127.0.255.250*.

6. Allocation

In the original design of IPv4, an IP address was divided into two parts: the network identifier was the most significant octet of the address, and the host identifier was the rest of the address. The latter was also called the *rest field*. This structure permitted a maximum of 256 network identifiers, which was quickly found to be inadequate.

To overcome this limit, the most-significant address octet was redefined in 1981 to create *network classes*, in a system which later became known as classful networking. The revised system defined five classes. Classes A, B, and C had different bit lengths for network identification. The rest of the address was used as previously to identify a host within a network. Because of the different sizes of fields in different classes, each network class had a different capacity for addressing hosts. In addition to the three classes for

addressing hosts, Class D was defined for multicast addressing and Class E was reserved for future applications.

Dividing existing classful networks into subnets began in 1985 with the publication of RFC 950. This division was made more flexible with the introduction of variable-length subnet masks (VLSM) in RFC 1109 in 1987. In 1993, based on this work, RFC 1517 introduced Classless Inter-Domain Routing (CIDR), which expressed the number of bits (from the most significant) as, for instance, /24, and the class-based scheme was dubbed *classful*, by contrast. CIDR was designed to permit repartitioning of any address space so that smaller or larger blocks of addresses could be allocated to users. The hierarchical structure created by CIDR is managed by the Internet Assigned Numbers Authority (IANA) and the regional Internet registries (RIRs). Each RIR maintains a publicly searchable WHOIS database that provides information about IP address assignments.

7. Special-use addresses

The Internet Engineering Task Force (IETF) and IANA have restricted from general use various reserved IP addresses for special purposes. Notably these addresses are used for multicast traffic and to provide addressing space for unrestricted uses on private networks.

B. Anatomy of IPv4 address

The **IPv4 address** is a 32-bit number that uniquely identifies a network interface on a machine. An **IPv4 address** is typically written in decimal digits, formatted as four 8-bit fields separated by periods. Each 8-bit field represents a byte of the **IPv4 address**.

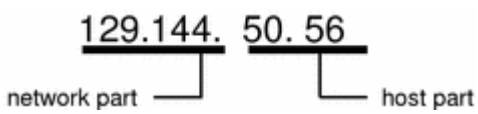
1. Parts of the IPv4 Address

Each network running TCP/IP must have a unique network number, and every machine on it must have a unique IP address. It is important to understand how IP addresses are constructed before you register your network and obtain its network number.

The IPv4 address is a 32-bit number that uniquely identifies a network interface on a machine. An IPv4 address is typically written in decimal digits, formatted as four 8-bit fields separated by periods. Each 8-bit field represents a byte of the IPv4 address. This form of representing the bytes of an IPv4 address is often referred to as the **dotted-decimal format**.

The bytes of the IPv4 address are further classified into two parts: the network part and the host part. The following figure shows the component parts of a typical IPv4 address, 129.144.50.56.

Figure 7-3 Parts of an IPv4 Address



2. Network Part

This part specifies the unique number assigned to your network. It also identifies the class of network assigned.

3. Host Part

This is the part of the IPv4 address that you assign to each host. It uniquely identifies this machine on your network. Note that for each host on your network, the network part of the address will be the same, but the host part must be different.

4. Subnet Number (Optional)

Local networks with large numbers of hosts are sometimes divided into subnets. If you choose to divide your network into subnets, you need to assign a **subnet number** for the subnet. You can maximize the efficiency of the IPv4 address space by using some of the bits from the host number part of the IPv4 address as a network identifier. When used as a network identifier, the specified part of the address becomes the subnet number. You create a subnet number by using a net mask, which is a bit mask that selects the network and subnet parts of an IPv4 address.

Content/Topic2: Assigning IP addresses

A. Introduction on how to assigning IP addresses

If you configure the networking software on your host for standalone operation (for instance, to be able to run the INN net news software), you can safely skip this section, because you will need an IP-address just for the loopback interface, which is always 127.0.0.1.

Things are a little more complicated with real networks like Ethernets. If you want to connect your host to an existing network, you have to ask its administrators to give you an IP-address on this network. When setting up the network all by yourself, you have to assign IP-addresses yourself as described below.

Hosts within a local network should usually share addresses from the same logical IP-network. Hence you have to assign an IP-network address. If you have several physical networks, you either have to assign them different network numbers, or use sub-netting to split your IP-address range into several subnetworks.

If your network is not connected to the Internet, you are free to choose any (legal) network address. You only have to make sure to choose one from classes A, B, or C, else things will most likely not work properly. However, if you intend to get on the Internet in the near future, you should obtain an official IP-address *now*. The best way to proceed is to ask your network service provider to help you.

To operate several Ethernets (or other networks, once a driver is available), you have to split your network into subnets. Note that sub-netting is required only if you have more than one *broadcast network*; point-to-point links don't count. For instance, if you have one Ethernet, and one or more SLIP links to the outside world, you don't need to subnet your network.

As an example, the brewery's network manager applies to the NIC for a class B network number, and is given 191.72.0.0. To accommodate the two Ethernets, she decides to use eight bits of the host part as additional subnet bits. This leaves another eight bits for the host part, allowing for 254 hosts on each of the subnets. She then assigns subnet number 1 to the brewery, and gives the winery number 2. Their respective network addresses are thus 191.72.1.0 and 191.72.2.0. The subnet mask is 255.255.255.0.

V lager, which is the gateway between the two networks, is assigned a host number of 1 on both of them, which gives it the IP-addresses 191.72.1.1 and 191.72.2.1, respectively.

Note that in this example I am using a class B network to keep things simple; a class C network would be more realistic. With the new networking code, sub-netting is not limited to byte boundaries, so even a class C network may be split into several subnets. For instance, you could use 2 bits of the host part for the net mask, giving you four possible subnets with 64 hosts on each.

B. Methods of assigning IP address

There are two **methods of assigning IP address** to your devices and computers. Either a **static** or dynamic **IP address** is **assigned** to a device when it connects to the internet. This goes the same way when we host your dedicated server

This section discusses methods of assigning IP addresses to end systems and explains their influence on administrative overhead. Address assignment includes assigning an IP address, a default gateway, one or more domain name servers that resolve names to IP addresses, time servers, and so forth. Before selecting the desired IP address assignment method, the following questions should be answered:

■ How many devices need an IP address?

■ Which devices require static IP address assignment?

■ Is IP address renumbering expected in the future?

■ Is the administrator required to track devices and their IP addresses?

■ Do additional parameters (default gateway, name server, and so forth) have to be configured?

■ Are there any availability issues?

■ Are there any security issues?

Static Versus Dynamic IP Address Assignment Methods

Following are the two basic IP address assignment strategies:

1. **Static**: An IP address is statically assigned to a system.

The network administrator configures the IP address, default gateway, and name servers manually by entering them into a special file or files on the end system with either a graphical or text interface. Static address assignment is an extra burden for the administrator

—especially on large-scale networks

— who must configure the address on every end system in the network.

2. **Dynamic**: IP addresses are dynamically assigned to the end systems.

Dynamic address assignment relieves the administrator of manually assigning an address to every network device. Instead, the administrator must set up a server to assign the addresses. On that server, the administrator defines the address pools and additional parameters that should be sent to the host (default gateway, name servers, time servers, and so forth). On the host, the administrator enables the host to acquire the address dynamically; this is often the default. When IP address reconfiguration is needed, the administrator reconfigures the server, which then performs the host-renumbering task. Examples of available address assignment protocols include Reverse Address Resolution Protocol, Boot Protocol, and DHCP. DHCP is the newest and provides the most features.

3. When to Use Static or Dynamic Address Assignment

To select either a static or dynamic end system IP address assignment method or a combination of the two, consider the following:

■**Node type**: Network devices such as routers and switches typically have static addresses. End-user devices such as PCs typically have dynamic addresses.

■ The number of end systems: If there are more than 30 end systems, dynamic address assignment is preferred. Static assignment can be used for smaller networks.

■ **Renumbering**: If renumbering is likely to happen and there are many end systems, dynamic address assignment is the best choice. With DHCP, only DHCP server reconfiguration is needed; with static assignment, all hosts must be reconfigured.

■ **Address tracking**: If the network policy requires address tracking, the static address assignment method might be easier to implement than the dynamic address assignment method. However, address tracking is also possible with dynamic address assignment with additional DHCP server configuration.

■**Additional parameters**: DHCP is the easiest solution when additional parameters must be configured. The parameters have to be entered only on the DHCP server, which then sends the address and those parameters to the clients.

■ **High availability**: Statically assigned IP addresses are always available. Dynamically assigned IP addresses must be acquired from the server; if the server fails, the addresses cannot be acquired. To ensure reliability, a redundant DHCP server is required.

■**Security**: With dynamic IP address assignment, anyone who connects to the network can acquire a valid IP address, in most cases. This might be a security risk. Static IP address assignment poses only a minor security risk.

- ✓ **Automatic method**: most networks today have a DHCP server that automatically assigns IP addresses to connected devices.
- ✓ **Static addressing method:** A permanent numeric identification assigned by the network administrator to a node in a TCP/IP network.

An IP address is statically assigned to a system. The network administrator configures the IP address, default gateway, and name servers manually by entering them into a special file or files on the end system with either a graphical or text interface. Static address assignment is an extra burden for the administrator —especially on large-scale networks
— who must configure the address on every end system in the network.

3.Dynamic method: IP addresses are dynamically assigned to the end systems. Dynamic address assignment relieves the administrator of manually assigning an address to every network device. Instead, the administrator must set up a server to assign the addresses. On that server, the administrator defines the address pools and additional parameters that should be sent to the host (default gateway, name servers, time servers, and so forth). On the host, the administrator enables the host to acquire the address dynamically; this is often the default. When IP address reconfiguration is needed, the administrator reconfigures the server, which then performs the host-renumbering task. Examples of available address assignment protocols include Reverse Address Resolution Protocol, Boot Protocol, and DHCP. DHCP is the newest and provides the most features.

C. IP addressing modification

Many people think that changing their IP address will somehow hide them on the internet.

However, this isn't necessarily the case. Your ISP keeps track of who is assigned to which IP address, so even if they change your IP, you're still connected to your ISP, and they still know who you are. There's really no escaping.

1. **How to change your IP address?**

- Go somewhere else. The simplest **way to change** the **IP address** of your device is to switch to a different network.
- **Reset** your modem. When you **reset** your modem, this will also **reset** the **IP address**. ...
- Connect via Virtual Private Network (VPN). ...
- Use a proxy server. ...
- Contact your ISP.

D.IP broking and firewalls

1.IP Blocking IP address

IP address blocking is a configuration of a network service that blocks requests from hosts with certain IP addresses. IP address blocking is commonly used to protect against brute force attacks and to prevent access by a disruptive address.

- **How to Block an IP Address?**

Just as it would have been in the Wild West, it's important to learn how to protect yourself from external threats. The basic security offered by internet servers can ward off some infiltration attempts, but often crafty criminals slip through the cracks.

Learning how to identify and block the IP address of an online pest is perhaps the best way to improve your security on the internet.

Ultimately, blocking an IP address allows administrators and website owners to control website traffic.

The process of blocking an IP address—or several—changes depending on the operating system that's being used.

While there are several different operating systems, the most common are Windows and Mac. We'll cover the steps for blocking an IP address using both of these systems, which achieve the same goal through slightly different means.

- **Why Block an IP Address?**

There are several reasons a business, educational institution, or internet user would attempt to block an IP address. In general, the most common reasons are:

- ✓ **Blocking Bots, Spammers, and Hackers:** When bots, spammers, and hackers attempt to infiltrate your website, it can put a heavy strain on your bandwidth and decrease the speed with which you and other users can access your website. If you run a business online, this can be detrimental to sales.
- ✓ **Limiting Website Access:** Many academic institutions and businesses use IP blocking to limit the websites that students or employees can visit. The goal is typically to increase productivity by limiting distractions.

- ✓ **Protecting Data:** Hackers often attempt to infiltrate websites to steal data or other important information. That information can be used to blackmail or otherwise undermine a company.
- ✓ **Maintaining Confidentiality:** Many academic institutions and companies who keep sensitive records—like transcripts, health records, etc.—are regularly targeted by hackers. Identifying threatening IP addresses and placing them on a blacklist is an essential step to keep those records safe and confidential.

This list should only be seen as the tip of the iceberg. There are countless reasons that an individual or organization might want to block certain IP addresses, and there should be no underestimating how malicious certain internet hackers can be.

2.**FIREWALLS**

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

- **How does a firewall work?**

Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

- **Types of firewalls**

Firewalls can either be software or hardware, though it's best to have both. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications, while a physical firewall is a piece of equipment installed between your network and gateway.

Packet-filtering firewalls, the most common type of firewall, examine packets and prohibit them from passing through if they don't match an established security rule set. This type of firewall checks the packet's source and destination IP addresses. If packets match those of an "allowed" rule on the firewall, then it is trusted to enter the network.

Packet-filtering firewalls are divided into two categories: state full and stateless. Stateless firewalls examine packets independently of one another and lack context, making them easy targets for hackers. In contrast, state full firewalls remember information about previously passed packets and are considered much more secure.

While packet-filtering firewalls can be effective, they ultimately provide very basic protection and can be very limited—for example, they can't determine if the contents of the request that's being sent will adversely affect the application it's reaching. If a malicious request that was allowed from a trusted source

address would result in, say, the deletion of a database, the firewall would have no way of knowing that. Next-generation firewalls and proxy firewalls are more equipped to detect such threats.

- ✓ **Next-generation firewalls (NGFW)** combine traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems, anti-virus, and more. Most notably, it includes deep packet inspection (DPI). While basic firewalls only look at packet headers, deep packet inspection examines the data within the packet itself, enabling users to more effectively identify, categorize, or stop packets with malicious data.

- ✓ **Proxy firewalls** filter network traffic at the application level. Unlike basic firewalls, the proxy acts an intermediary between two end systems. The client must send a request to the firewall, where it is then evaluated against a set of security rules and then permitted or blocked. Most notably, proxy firewalls monitor traffic for layer 7 protocols such as HTTP and FTP, and use both statefull and deep packet inspection to detect malicious traffic.

- ✓ **Network address translation (NAT) firewalls** allow multiple devices with independent network addresses to connect to the internet using a single IP address, keeping individual IP addresses hidden. As a result, attackers scanning a network for IP addresses can't capture specific details, providing greater security against attacks. NAT firewalls are similar to proxy firewalls in that they act as an intermediary between a group of computers and outside traffic.

- ✓ **Statefull multilayer inspection (SMLI) firewalls** filter packets at the network, transport, and application layers, comparing them against known trusted packets. Like NGFW firewalls, SMLI also examine the entire packet and only allow them to pass if they pass each layer individually. These firewalls examine packets to determine the state of the communication (thus the name) to ensure all initiated communication is only taking place with trusted sources.

Content/Topic3: Testing IP addresses

How to test a Public IP Address in Connect?

Introduction

Being able to test a client's public IP address is extremely important, to ensure that the service is working correctly before the client moves in and to determine if an issue reported by the client (slow or lack of internet) is related to the client's equipment.

Testing

You will require the following:

- ✓ A laptop an Ethernet cable
- ✓ The switch and port number that the client's public IP is assigned to
- ✓ The client's public IP information (found on the 2nd page of the service guide exported from Connect).

- Click on the Start Menu, and type in Network, and click on Network Connections.
- Ensure WIFI is disabled (if enabled by right clicking on WIFI and selecting disable.
- Right click on Ethernet adaptor, then click Properties.
- Within Ethernet Properties, scroll down to Ethernet Protocol Version 4, and select Properties.

- Then in the new window, select the User the following IP address option, and Use the following DNS server addresses.
- Please enter the client's Public IP, Subnet Mask, Default Gateway and DNS settings into their respective fields.

- Plug the laptop into the allocated switch port.
- Open a browser and try to get online.

Note:
If this procedure has been followed as a result of a client raising an issue with their Public IP port, please advise the client that the port has been successfully tested and suggest the client do the following:

- Restart their router
- Check their WAN interface network settings (they may need to have their 3rd party IT support do this).

E. Diagnostic tools

1. **Diagnostic Tool** is a fast and simple **tool**, which allows users of Control Techniques' drives to quickly solve any error codes that the drive may show.
2. **best network diagnostic tools:**

- **Solar Winds Network Configuration Manager:** An essential system security and administration tool that automatically checks on device settings. The NCM will gather all device configurations, allow the creation of standard settings, and ensure that any unauthorized changes are immediately rolled back.
- **Solar Winds Port Scanner:** Check the TCP and UDP port status (open, closed, or filtered) of the IP addresses on your network devices to ensure that you don't have unattended ports open. Great for resolving IP conflicts and can be run from the command line with the option to export results to file.
- **Data dog Network Performance Monitoring:** A cloud-based network monitoring and management service that includes troubleshooting tools.
- **Solar Winds RMM:** A remote monitoring and management tool that enables central IT departments to manage networks on several remote sites.
- **Paessler Network Troubleshooting with PRTG**: Infrastructure management system that includes port monitoring.
- **Ping**: Simple command-line utility that checks on the speed of connections.
- **Tracert**: Free command-line utility that lists the probable hops to a network or internet destination address.
- **Ipconfig**: This command-line tool reports the IPv4 and IPv6 addresses, subnets, and default gateways for all network adapters on a PC.
- **Netstat**: This tool displays active connections on your computer.
- **Nslookup**: Available for Windows, Unix, Linux, and Mac OS, this tool gives you DNS server diagnostics.
- **Speed and up/down test sites**: A list of websites that will test your internet connections.
- **Sysinternals**: Set of Microsoft tools for Windows that help troubleshoot and configure Active Directory.
- **Wireshark**: Free packet sniffer that will help you analyze traffic flows.
- **Nmap**: security and monitoring tool that needs a companion utility, Zenmap, as a user interface.

L.O. 3.3: Apply IPv4 Sub netting

Content/Topic1: Calculation of IP addresses

A. Sub-netting

Sub netting is a logical subdivision of an IP **network.** Sub netting is the practice of dividing a **network** into two or more **networks.**

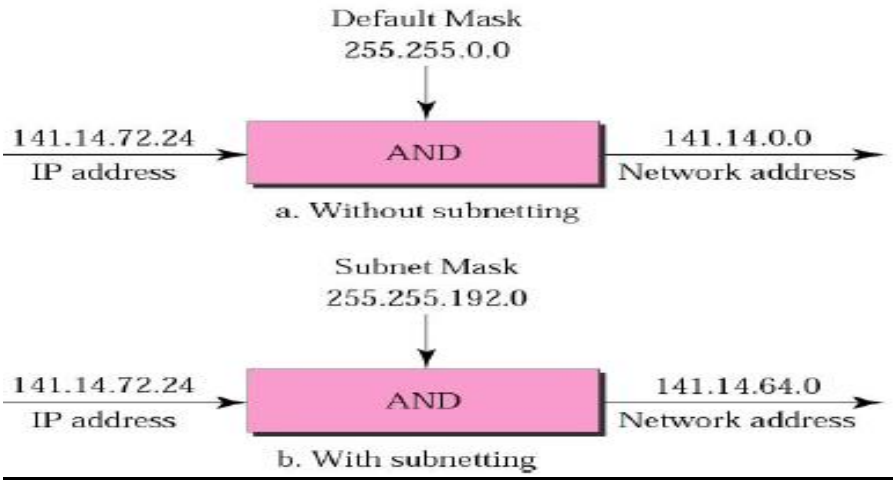
i. Understanding Sub netting

Why subnet?

- ✓ Divide larger network intosmaller network.
- ✓ Limit layer 2 and layer 3 broadcasts totheir subnet.
- ✓ Better management of traffic.

- Sub netting is used to break the network into small groups, more efficient subnets to prevent excessive rates of Ethernet packet collision in a large network.
- Applying a subnet mask to an IP address allows you to **identify the network and node parts of the address**. The network bits are represented by the **ones in the mask**, and the node bits are represented by the **zeros** which are identical to the subnet length.
- In order to subnet a network, extend the natural mask using some of the bits from the host ID portion of the address to create a subnetwork ID. For example, given a Class C network of 204.17.5.0 which has a natural mask of 255.255.255.0, you can create subnets in this manner:

ii. Default mask and subnet mask



iii. Sub netting a Class C Address: The Fast Way!

When you've chosen a possible subnet mask for your network and need to determine the number of subnets, valid hosts, and broadcast addresses of a subnet that the mask provides, all you need to do is answer five simple questions:

- **How many subnets does the chosen subnet mask produce?**
- **How many valid hosts per subnet are available?**
- **What are the valid subnets?**
- **What's the broadcast address of each subnet?**
- **What are the valid hosts in each subnet?**

At this point, it's important that you both understand and have memorized your powers of 2. Please refer to the sidebar "Understanding the Powers of 2" earlier in this chapter if you need some help. Here's how you get the answers to those five big questions:

_ ***How many subnets?*** 2^x = number of subnets. *x* is the number of masked bits, or the 1s. For example, in 11000000, the number of 1s gives us 2^2 subnets. In this example, there are 4 subnets.

_ ***How many hosts per subnet?*** $2^y - 2$ = number of hosts per subnet. *y* is the number of unmasked bits, or the 0s. For example, in 11000000, the number of 0s gives us $2^6 - 2$ hosts. In this example, there are 62 hosts per subnet. You need to subtract 2 for the subnet address and the broadcast address, which are not valid hosts.

_ ***?*** 256 – subnet mask = block size, or increment number. An example would be 256 – 192 = 64. The block size of a 192 mask is always 64. Start counting at zero in blocks of 64 until you reach the subnet mask value and these are your subnets. 0, 64,128,192. Easy

What's the broadcast address for each subnet? Now here's the really easy part. Since we counted our subnets in the last section as 0, 64, 128, and 192, the broadcast address is always the number right before the next subnet. For example, the 0 subnet has a broadcast address of 63 because the next subnet is 64. The 64 subnet has a broadcast address of 127 because the next subnet is 128. And so on. And remember, the broadcast address of the
last subnet is always 255.

What are the valid hosts? Valid hosts are the numbers between the subnets, omitting the all 0s and all 1s. For example, if 64 is the subnet number and 127 is the broadcast address, then 65–126 is the valid host range—it's *always* the numbers between the subnet address and the broadcast address.

iv. Formula for calculating subnets

- **Use this formula to calculate the number of subnets**:

2^n where n = the number of bits borrowed

In this example, the calculation looks like this:

2^1 = 2 subnets

- **The number of hosts:**

To calculate the number of hosts per network, we use the formula of 2^n - 2 where n = the number of bits left for hosts.

Applying this formula, (2^7 - 2 = 126) shows that each of these subnets can have 126 hosts.

For each subnet, examine the last octet in binary. The values in these octets for the two networks are:

Subnet 1: 00000000 = 0
Subnet 2: 10000000 = 128

B. Classless Inter-Domain Routing (CIDR)

Another term you need to familiarize yourself with is *Classless Inter-Domain Routing (CIDR)*.
It's basically the method that ISPs (Internet service providers) use to allocate a number of addresses to a company, a home—a customer. When you receive a block of addresses from an ISP, what you get will look something like this: 192.168.10.32/28. This is telling you what your subnet mask is. The slash notation (/) means how many bits are turned on (1s). Obviously, the maximum could only be /32 because a byte is 8 bits and there are 4 bytes in an IP address: (4*8 = 32). But keep in mind that the largest subnet mask available (regardless of the class of address) can only be a /30 because you've got to keep at least 2 bits for host bits. Take, for example, a Class A default subnet mask, which is 255.0.0.0. This means that the first byte of the subnet mask is all ones (1s), or 11111111. When referring to a slash notation, you need to count all the 1s bits to figure out your mask. The 255.0.0.0 is considered a /8 because it has 8 bits that are 1s—that is, 8 bits that are turned on. A Class B default mask would be 255.255.0.0, which is a /16 because 16 bits are ones (1s): 11111111.11111111.00000000.00000000.
Table below has a listing of every available subnet mask and its equivalent CIDR slash notation.

v. TABLE: CIDR Values

Subnet Mask	CIDR Value
255.0.0.0	/8
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12

255.248.0.0	/13
255.252.0.0	/14
255.254.0.0	/15
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

The /8 through /15 can only be used with Class A network addresses. /16 through /23 can be used by Class A and B network addresses. /24 through /30 can be used by Class A, B, and C network addresses. This is a big reason why most companies use Class A network addresses.

vi. Sub netting Class C Addresses

In a Class C address, only 8 bits are available for defining the hosts. Remember that subnet bits start at the left and go to the right, without skipping bits. This means that the only Class C subnet masks can be the following:

```
Binary     Decimal  CIDR
------------------------
00000000 = 0        /24
10000000 = 128      /25
11000000 = 192      /26
11100000 = 224      /27
11110000 = 240      /28
11111000 = 248      /29
11111100 = 252      /30
```

We can't use a /31 or /32 because we have to have at least 2 host bits for assigning IP addresses to hosts. In the past, I never discussed the /25 in a Class C network.

vii. Sub netting a Class C Address: The Fast Way!

When you've chosen a possible subnet mask for your network and need to determine the number of subnets, valid hosts, and broadcast addresses of a subnet that the mask provides, all you need to do is answer five simple questions:

- How many subnets does the chosen subnet mask produce?
- How many valid hosts per subnet are available?
- What are the valid subnets?
- What's the broadcast address of each subnet?
- What are the valid hosts in each subnet?

Here's how you get the answers to those five big questions:

- ***How many subnets?*** 2^x = number of subnets. *x* is the number of masked bits, or the 1s. For example, in 11000000, the number of 1s gives us 2^2 subnets. In this example, there are 4 subnets.

- ***How many hosts per subnet?*** $2^y - 2$ = number of hosts per subnet. *y* is the number of unmasked bits, or the 0s. For example, in 11000000, the number of 0s gives us $2^6 - 2$ hosts. In this example, there are 62 hosts per subnet. You need to subtract 2 for the subnet address and the broadcast address, which are not valid hosts.

- ***What are the valid subnets?*** 256 – subnet mask = block size, or increment number. An example would be 256 – 192 = 64. The block size of a 192 mask is always 64. Start counting at zero in blocks of 64 until you reach the subnet mask value and these are your subnets. 0, 64, 128, 192.

- ***What's the broadcast address for each subnet?*** Now here's the really easy part. Since we counted our subnets in the last section as 0, 64, 128, and 192, the broadcast address is always the number right before the next subnet. For example, the 0 subnet has a broadcast address of 63 because the next subnet is 64. The 64 subnet has a broadcast address of 127 because the next subnet is 128. And so on. And remember, the broadcast address of the last subnet is always 255.

- ***What are the valid hosts?*** Valid hosts are the numbers between the subnets, omitting the all 0s and all 1s. For example, if 64 is the subnet number and 127 is the broadcast address, then 65–126 is the valid host range—it's *always* the numbers between the subnet address and the broadcast address.

Practice Example 1: 255.255.255.128 (/25)

Since 128 is 10000000 in binary, there is only 1 bit for subnetting and 7 bits for hosts. We're going to subnet the Class C network address 192.168.10.0.

192.168.10.0 = Network address
255.255.255.128 = Subnet mask
Now, let's answer the big five:

- *How many subnets?* Since 128 is 1 bit on (**1**0000000), the answer would be $2^1 = 2$.
- *How many hosts per subnet?* We have 7 host bits off (1**0000000**), so the equation would be $2^7 - 2 =$ 126 hosts.
- *What are the valid subnets?* 256 – 128 = 128. Remember, we'll start at zero and count in our block size, so our subnets are 0, 128.
- ***What's the broadcast address for each subnet?*** The number right before the value of the next subnet is all host bits turned on and equals the broadcast address. For the zero subnet, the next subnet is 128, so the broadcast of the 0 subnet is 127.

- ***What are the valid hosts?*** These are the numbers between the subnet and broadcast address. The easiest way to find the hosts is to write out the subnet address and the broadcast address. This way, the valid hosts are obvious. The following table shows the 0 and128 subnets, the valid host ranges of each, and the broadcast address of both subnets:

Subnet	0	128
First host	1	129
Last host	126	254
Broadcast	127	255

viii. Sub netting Class B Addresses

Before we dive into this, let's look at all the possible Class B subnet masks first. Notice that we have a lot more possible subnet masks than we do with a Class C network address:

```
255.255.0.0     (/16)
255.255.128.0   (/17)
255.255.192.0   (/18)
255.255.224.0   (/19)
255.255.240.0   (/20)
255.255.248.0   (/21)
255.255.252.0   (/22)
255.255.254.0   (/23)
255.255.255.0     (/24)
255.255.255.128   (/25)
255.255.255.192   (/26)
255.255.255.224   (/27)
255.255.255.240   (/28)
255.255.255.248   (/29)
255.255.255.252   (/30)
```

We know the Class B network address has 16 bits available for host addressing. This means we can use up to 14 bits for sub netting (because we have to leave at least 2 bits for host addressing). Using a /16 means you are not sub netting with class B, but it is a mask you can use. The process of sub netting a Class B network is pretty much the same as it is for a Class C, except that you just have more host bits and you start in the third octet.

Practice Example 1: 255.255.128.0 (/17)

172.16.0.0 = Network address
255.255.128.0 = Subnet mask

- ***Subnets?*** $2^1 = 2$ (same as Class C).
- ***Hosts?***215 – 2 = 32,766 (7 bits in the third octet, and 8 in the fourth).
- ***Valid subnets?*** 256 – 128 = 128. 0, 128. Remember that sub netting is performed in the third octet, so the subnet numbers are really 0.0 and 128.0, as shown in the next table. These are the exact numbers we used with Class C; we use them in the third octet and add a 0 in the fourth octet for the network address.

- ***Broadcast address for each subnet?***
- *Valid hosts?*

The following table shows the two subnets available, the valid host range, and the broadcast address of each:

Subnet	0.0	128.0
First host	0.1	128.1
Last host	127.254	255.254
Broadcast	127.255	255.255

ix. Sub netting Class A Addresses

Class A sub netting is not performed any differently than Classes B and C, but there are 24 bits to play with instead of the 16 in a Class B address and the 8 in a Class C address.

Let's start by listing all the Class A masks:

```
255.0.0.0      (/8)
255.128.0.0    (/9)
255.192.0.0    (/10)
255.224.0.0    (/11)
255.240.0.0    (/12)
255.248.0.0    (/13)
255.252.0.0    (/14)
255.254.0.0    (/15)
255.255.0.0    (/16)
255.255.128.0    (/17)
255.255.192.0    (/18)
255.255.224.0    (/19)
255.255.240.0    (/20)
255.255.248.0    (/21)
255.255.252.0    (/22)
255.255.254.0    (/23)
255.255.255.0    (/24)
255.255.255.128    (/25)
255.255.255.192    (/26)
255.255.255.224    (/27)
255.255.255.240    (/28)
255.255.255.248    (/29)
255.255.255.252    (/30)
```

Remember, we're going to do this the same way as a Class B or C subnet. It's just that, again, we simply have more host bits and we just use the same subnet numbers we used with Class B and C, but we start using these numbers in the second octet.

Practice Example 1: 255.255.0.0 (/16)

Class A addresses use a default mask of 255.0.0.0, which leaves 22 bits for subnetting since you must leave 2 bits for host addressing. The 255.255.0.0 mask with a Class A address is using 8 subnet bits.

- ***Subnets?*** $\mathbf{2^8}$= 256.
- ***Hosts?*** $\mathbf{2^{16} - 2}$ = 65,534.
- ***Valid subnets?*** What is the interesting octet? 256 – 255 = 1. 0, 1, 2, 3, etc. (all in the second octet). The subnets would be 10.0.0.0, 10.1.0.0, 10.2.0.0, 10.3.0.0, etc., up to 10.255.0.0.
- ***Broadcast address for each subnet?***
- ***Valid hosts?***
  The following table shows the first two and last two subnets, valid host range, and broadcast addresses for the private Class A 10.0.0.0 network:

x. Calculate Binary to decimal conversion

In the binary system there are only 1s and 0s. Depending on their position in the octet, they get different values. Each position is a power of 2. To get the decimal number you have to sum up that number.

1	1	1	1	1	1	1	1
2^7 = 128	2^6 = 64	2^5 = 32	2^4 = 16	2^3 = 8	2^2 = 4	2^1 = 2	2^0 = 1

C. **VLSM:**

1. **VLSM** stands for Variable Length Subnet Mask where the subnet design uses more than one mask in the same network which **means** more than one mask is used for different subnets of a single class A, B, C or a network. It is used to increase the usability of subnets as they can be of variable size.

2. **The Main Purpose of Vlsm?**

VLSM provides many benefits for real networks, mainly related to how you allocate and use your IP address space. Because a mask defines the size of the subnet (the number of host addresses in the subnet), **VLSM** allows engineers to better match the need for addresses with the size of the subnet.

3. **Procedure of implementing VLSM**

In VLSM, subnets use block size based on requirement so sub netting is required multiple times. Suppose there is an administrator that has four departments to manage. These are sales and purchase department with 120 computers, development department with 50 computers, accounts department with 26 computers and management department with 5 computers.
If the administrator has IP 192.168.1.0/24, department wise IPs can be allocated by following these steps:

- For each segment select the block size that is greater than or equal to the actual requirement which is the sum of host addresses, broadcast addresses and network addresses. Make a list of subnets possible:

SLASH NOTATION	HOSTS/SUBNETS
/24	254
/25	126
/26	62
/27	30
/28	14
/29	6
/30	2

table – possible subnets list

- Arrange all the segments in descending order based on the block size that is from highest to lowest requirement.

- Sales and Purchase: 120
- Development: 50
- Accounts: 26

Management: 5

- The highest IP available has to be allocated to highest requirement so the sales and purchase department gets 192.168.1.0/25 which has 126 valid addresses that can easily be available for 120 hosts. The subnet mask used is 255.255.255.128

- The next segment requires an IP to handle 50 hosts. The IP subnet with network number 192.168.1.128/26 is the next highest which can be assigned to 62 hosts thus fulfilling the requirement of development department. The subnet mask used is 255.255.255.192
- Similarly, the next IP subnet 192.168.1.192/27 can fulfill the requirements of accounts department as it has 30 valid hosts IP which can be assigned to 26 computers
  The mask used is 255.255.255.224
- The last segment requires 5 valid hosts IP which can be fulfilled by the subnet 192.168.1.224/29 which has the mask as 255.255.255.248 is chosen as per the requirement. The IP with the mask 255.255.255.240 could be chosen but it has 14 valid hosts IPs and the requirement is less in comparison so the one that is comparable with the requirement is chosen. Thus there is less IP wastage in VLSM as compared to FLSM.

4. Advantages of VLSM over FLSM

- In Fixed length subnet mask sub netting (FLSM), all subnets are of equal size and have equal number of hosts but in VLSM the size is variable and it can have variable number of hosts thus making the IP addressing more efficient by allowing a routed system of different mask length to suit requirements.
- In FLSM there is a wastage of IP addresses but in VLSM there is a minimum wastage of IP addresses.
- FLSM is preferred for private IP addresses while for public IP addresses VLSM is the best option.

Learning unit 4: Document the Work Done

L.O4.1: Document the review process

Content/Topic1: Description the review process of document

A. Review of user manual and previous report

A great user manual educates people about a product, while also teaching them how to use product features effectively. As an author, your ultimate goal is comprehension—you want readers to easily be able to read, reference, and absorb information.

General guidelines for user manuals

- ✓ Provide a real (physical) user manual with the product.
- ✓ Make sure the instructions actually map on to the product in all respects.
- ✓ Include a one-page quick start guide.
- ✓ Present instructions as step-by-step procedures.
- ✓ Tell the user what functions there are, and what they are for — not just how to use them... but avoid marketing waffle (they already bought the product!)
- ✓ Ensure that the writers are part of the product design team.
- ✓ Write the user manual in synch with the product's development timeline — not under pressure of shipping deadlines.
- ✓ Make sure the writers have the product, understand the product, and actually use the product as they write.
- ✓ Consider the needs of disabled users (i.e., low vision, colour-blind) and provide alternative manuals in Braille, large print, audio etc.
- ✓ User-test the product and the user manual with real users (including disabled users).

B. Suggestion of solutions on problems found

Here are seven-steps for an effective problem-solving process.

1. Identify the issues.

- Be clear about what the problem is.
- Remember that different people might have different views of what the issues are.
- *Separate the listing of issues from the identification of interests (that's the next step!).*

2. Understand everyone's interests.

- This is a critical step that is usually missing.
- Interests are the needs that you want satisfied by any given solution. We often ignore our true interests as we become attached to one particular solution.
- The best solution is the one that satisfies everyone's interests.
- This is the time for active listening. Put down your differences for a while and listen to each other with the intention to understand.
- *Separate the naming of interests from the listing of solutions.*

3. List the possible solutions (options)

- This is the time to do some brainstorming. There may be lots of room for creativity.
- *Separate the listing of options from the evaluation of the options.*

4. Evaluate the options.

- What are the pluses and minuses? Honestly!
- *Separate the evaluation of options from the selection of options.*

5. Select an option or options.

- What's the best option, in the balance?
- Is there a way to "bundle" a number of options together for a more satisfactory solution?

6. Document the agreement(s).

- Don't rely on memory.
- Writing it down will help you think through all the details and implications.

7. Agree on contingencies, monitoring, and evaluation.

- Conditions may change. Make contingency agreements about foreseeable future circumstances (If-then!).
- How will you monitor compliance and follow-through?
- Create opportunities to evaluate the agreements and their implementation. ("Let's try it this way for three months and then look at it.")

Effective problem solving does take some time and attention more of the latter than the former. But less time and attention than is required by a problem not well solved. What it really takes is a willingness to

slow down. A problem is like a curve in the road. Take it right and you'll find yourself in good shape for the straightaway that follows. Take it too fast and you may not be in as good shape.

C. Description of solution implementation

1. Definition

Implementation is the culmination of all your work in solving a problem and requires careful attention to detail. There are three basic stages involved:

- ✓ planning and preparing to implement the solution
- ✓ implementing and monitoring the action
- ✓ reviewing and analyzing the success of the action.

2. Planning and preparation

Planning and preparation **is** *the key to successful implementation.* The more important the problem, or the more complex the actions required to solve it, the more thorough your planning and preparation needs to be to ensure success.

These questions highlight the main features of planning and preparation, which involve:

- ✓ constructing a plan of action
- ✓ the actions required
- ✓ scheduling the actions
- ✓ the resources required
- ✓ measures to counter adverse consequences
- ✓ management of the action
- ✓ reviewing the plan

✓ selecting, briefing and training those involved.

- **Constructing a plan of action**

Basically***,*** *the plan of action describes what actions are required and how they will be implemented to ensure success****.*** Unless the problem is simple or routine, you need to construct a detailed plan of action.

This involves systematically identifying and recording the following elements:

✓ ***The actions required***

These must be identified fully and precisely, otherwise the results expected will not be achieved. The expected effects of these actions must also be identified, so that you will know when they have been carried out successfully. This part of the plan can be constructed as follows:

- state your objective
- list the individual goals in the order in which they must be achieved to reach that objective
- identify what actions are required to achieve each goal, determine the sequence in which they need to be carried out, and record them
- define, in measurable terms, what a successful outcome will be for each action and add the details to the plan.

✓ ***Scheduling the* actions**

To create *a time schedule* for the actions, first you identify the time required to complete each action. By representing this information on the diagram you can calculate at what stage, relative to the starting time, each action will commence and finish, and determine the total time required to achieve the objective. Simple plans can be represented by a chart which uses bars to show the sequence and duration of the actions.

More complex plans require a more flexible structure, like a chain diagram or flow chart. Diagrams help you to arrange the actions in a way which makes the best use of time and other resources. In drawing up a schedule. it's important not to be over-optimistic in the time you allow for each action. Additional time is required to accommodate delays and unforeseen obstacles, particularly with actions which must be completed on time or which are susceptible to delays.

✓ ***The resources required***

For each action the resources required have to be precisely defined along a number of parameters, including the type, amount and when they are required. Each resource is considered individually:

Time is sometimes overlooked but it can be a key resource in some situations. These can be defined by answering some simple questions.

- What time is available before the deadline for achieving each action/goal/the overall objective?
- Are these timings compatible?
- Whose time is required?
- Will this time be spent within normal working hours?

Manpower may come from within and outside the organization and can be defined by answering these questions

- How many people will be required?
- What skills, qualities and knowledge will they need to carry out the actions required of them?
- When and where will they be required?
- Will they be available when and where required?
- Will they be available for the length of time required?
- What briefing and training will they need to be able to carry out their tasks effectively?

Money can be defined by answering the questions

- How much will be needed?
- In what form? (eg cash, cheque, foreign currency)
- How will it be acquired? (eg loan, grant, endowment)
- What will be the source? (eg profits, merchant bank, local or central government)
- How will it be used and is this compatible with the source? (eg if it's a development grant does the plan use it appropriately?)
- When and where will it be required?
- Will it be available when and where required?
- Does it need to be repaid, and when?
- Will it be recouped, how, and when? (eg through increased profits)
- Will there be additional cost in using this money? (eg interest or handling charges)
- Have the costs of all other resources been included?

Materials may fall into a number of categories, including consumables, raw materials, and equipment (for temporary or permanent use). The material requirements can be defined by answering the questions

- What type of materials will be required?
- If capital equipment is required, how will it be financed? (eg lease, loan)
- What are the specifications of the materials required? (eg quality, size)
- What wastage is likely to occur?
- In what quantities are they required?
- When and where will they be required?
- Will they be available when and where required?
- Will transport be required?

- What handling (human and mechanical) will be required?
- Will storage space be required, where, how much, for how long, and will it be available?

Space can be defined by answering these questions

- What space will be required?
- How much space will be required?
- Where will the space be required?
- Does it have to be of a particular type (eg covered, with amenities) or with particular dimensions?
- How long will the space be required?

Information may form a part of the manpower resource (eg expert advice or skills) but it can also be a resource in its own right (eg renting a mailing list for a direct mail campaign). To define this resource, you need to answer these questions

- What specific information will be required?
- Is this information available from within the organization or does it have to be bought-in?
- Where specifically is it available?
- When and where will it be required?
- Will it be available when and where required?
- How long will it be required?

When you are calculating the resources required to implement a solution it's vital not to under-estimate. A shortage could disrupt implementation completely and possibly incur heavy penalties, eg having to pay a consultant for doing nothing while he's waiting for the installation of a piece of equipment. Sometimes you may have to adapt your plan of action to suit the availability of resources.

Once you have made a complete list of the resource requirements, draw up a schedule of resources, showing how and when they will be requested, from whom, and when and where they are to be delivered.

- ✓ ***Measures to counter adverse consequences***

These have to be included in the plan. Although you have considered the areas of risk and possible side-effects when constructing and evaluating your solution, and adapted it to try to minimize the adverse consequences, you need to identify everything that could go wrong during implementation and devise countermeasures. This includes even minor problems such as a key person being sick.

The steps involved are similar to those used to evaluate and minimize the risks associated with the solution, only more detailed.

There are certain features of a plan of action which can make it more susceptible to something going wrong. To identify these and make provision in your plan to deal with them, you should examine your plan step-by-step and follow these stages:

- ***identify everything that could go wrong****;* look for areas where, for example,

- timing is crucial (eg with delays, could a deadline be missed?)

- a slippage in timing could bring subsequent actions into conflict (eg so that they simultaneously require the same resource)

- two or more activities coincide (eg will they interfere with each other?)

- there is no way of predicting what may happen (eg because of lack of knowledge or experience)

- there is heavy reliance on facilities or equipment (eg could they fail?) ,

- there is heavy reliance on the cooperation and efforts of people (eg will they perform as required?)

- all available resources in a particular category are being used (eg could an unexpected event require their more urgent use elsewhere?)

- external factors could affect the actions required (eg withdrawal of labour in a national dispute) or the effectiveness of the results (eg a change in market needs)

- ***analyze and evaluate the consequences****,* eg .

- what are the effects if this happens?

- how serious are they?

- what is their relative seriousness?

- what is the probability of them happening (low, medium or high)?

- *define how you could recognize trouble* as early as possible, eg through the detection of unexpected changes in predicted events

- *devise countermeasures* where possible, either to prevent the cause of trouble or minimize its effects
- *incorporate* the method of recognition and the appropriate countermeasure into your plan.

Adverse consequences which have the highest probability of occurring combined with the greatest seriousness should be tackled first and every effort made to ensure that provision is made in your plan to counter them effectively. Even if time is short and it requires extensive work, you can only afford to omit minor adverse consequences with a low probability of occurrence. Although problems may not arise during Implementation, if they do your plan must contain appropriate countermeasures which can be taken without jeopardizing the rest of the plan.

✓ ***Management of the action***

Unless the solution is very simple or routine you must specify how the implementation will be monitored and controlled. This enables the manpower to be appropriately led and managed, their progress to be measured at specific intervals, and appropriate action to be taken to correct any variance from the plan. The following steps help to identify how to manage the implementation:

- identify actions which require on-the-job supervision and monitoring (eg where individuals have no previous experience of the actions required of them)
- identify the stages at which progress should be measured (eg upon completion of individual goals or major activities; at critical phases)
- specify exactly what results are expected to have been achieved at these stages
- specify how and by whom the actual results will be measured
- ensure that appropriate measures to correct any variance between the expected and the actual results are specified in the plan.

The stages you identify for measuring progress are, in effect, ***deadlines for achieving specific results***. These must be stated as a specific time or date in the overall time schedule. Unspecific or woolly deadlines make implementation difficult to manage and can lead to disaster. The frequency of measuring progress is dependent upon a number of factors:

- what is practical (eg economical and not interfering significantly with progress)
- the rate at which the situation is likely to change (eg major building works compared with delicate negotiations over a couple of days)
- the seriousness of potential variances from the plan

- Provision should also be made to monitor the solution once it has been implemented, so that any unforeseen adverse consequences arising in the long term can be detected. For example, has a change in the system created a bottleneck in processing work, or resulted in undue pressure on one individual or department?

✓ ***Reviewing the plan***

Finally, you need to check the plan to ensure that

- the actions listed will achieve the various goals and the overall objective
- your time schedule is workable and can accommodate unexpected delays
- your estimation of resources is accurate
- the plan for managing the action will enable it to be kept on course.
- Drawing up a plan of action is the most crucial stage in ensuring efficient implementation and it must be accurate and thorough. This plan provides a blueprint for the remaining stages of implementation.

✓ **Selecting, briefing and training those involved**

Your plan of action provides most of the information you require at this stage.

This situation is very similar to having to get your solution implemented successfully. You need to go through the following stages:

- select indjviduals with the appropriate skills, qualities and knowledge required to carry out the various actions effectively
- brief these people. so that they know and understand what they are required to do
- give training, if necessary, to individuals who do not meet the exact requirements for carrying out their assigned tasks effectively.

Selection involves comparing the skills, qualities and knowledge required for specific tasks with those available amongst individual members of the workforce. By identifying the ideal attributes for carrying out each action effectively - both what is required and what is to be avoided - you can construct a model of the ideal candidate. Selection then consists of finding the best match to this ideal amongst members of the workforce.

Once you have selected appropriate individuals you need to draw up a list of what actions each is required to carry out, the results they will be expected to achieve, and what responsibilities they have for achieving these results.

Frequently there will be at least some aspects of your plan for which the individuals available are not ideally suited. If the discrepancy is large it may be necessary to buy in manpower with the appropriate attributes. However, frequently the shortfall can be overcome by careful briefing or specific training.

Briefing is often the final step before a plan is implemented. As in any other type of communication, it must be planned and executed carefully to ensure that it's effective. The following steps will help you to brief people effectively:

- give individuals reasonable advance warning of what will be required of them
- prepare your briefing carefully so that it is clear, comprehensive and can be understood easily by everyone
- after the briefing, check that everyone has understood what they are required to do by asking them to repeat your instructions.

Your instructions should ***state clearly the responsibilities of each individual and the scope of their authority in carrying out their task***. It's important to give a level of authority which enables individuals to use their initiative and not be bound rigidly to the plan. For example, if they foresee a problem arising they need the freedom to act immediately if necessary.

The way you communicate your message is very important. Some individuals may have a different view of the situation and different attitudes to your own, particularly if they have not been involved in finding and evaluating solutions.

Training can be expensive and time-consuming. If people with the appropriate skills are not readily available you need to compare the advantages and disadvantages of training them or buying-in the necessary skills, eg training may provide individuals with skills which are of value in other aspects of their work; hiring a consultant may create a valuable business contact.

Once people have been briefed on what they are required to do and other appropriate resources have been arranged, the plan of action can be implemented.

✓ Implementing and monitoring the action

Once action has been initiated, it has to be supervised and monitored to ensure that the plan is followed accurately, implementing corrective action when necessary. The details of this stage are specified in the plan of action.

Supervising the action ensures that individuals carry out their tasks efficiently according to the plan.

Monitoring progress enables you to identify whether or not the results being achieved are meeting the planned requirements, and if not, why not. A decision can then be made on the action required to put the plan back on course. Reviewing the overall achievement once the plan has progressed significantly will indicate how well it is achieving the objective. If there are major discrepancies it suggests that the plan is inadequate and needs to be revised.

Taking corrective action may involve implementing the appropriate countermeasure laid down in the plan, or taking unplanned action to counter unforeseen problems. For example, if time. has been lost in completing one activity, other activities may have to be completed more quickly than planned in order to meet a deadline. Minor problems which are unlikely to recur may not require any action. Major faults in the plan may make it necessary to abandon implementation if no appropriate corrective action is possible.

These three processes must be maintained until the plan is completed.

- ✓ **Reviewing and analyzing the outcome**

When the plan has been completed and the solution implemented it is important to measure and analyze its success. This tells you whether the solution has been effective in solving the problem and how useful it will be in solving similar problems in the future. There are three stages

- measure the success of the solution by comparing the outcome of the action with the expected results
- analyze any discrepancy to identify the reasons for it
- take further action if necessary.

- ✓ **Remember**

- The more important them. problem, or the more complex the actions required to solve it, the more planning and preparation you need to do.
- Action must be monitored to ensure that it is being carried out effectively and having the desired effects; if not, corrective action must be taken.
- Once the action is completed, the outcome must be measured to check that it has provided an effective solution; if not, further action may be required.

D. Description of procedures of the task accomplished

3. What is a procedure?

The idea of what a procedure is, changes depending on who you ask. To many, a procedure is a set of detailed instructions that tell the reader how to complete a task.

4. How to write an effective procedure?

Now we're getting into the meat of the topic – learning how to write a procedure. Any of you who've read our other posts on documenting processes and recording standard operating procedures will know much of this already, but to summarize you need to:

1. Meet with the teams responsible for the procedure
2. Start with a short introduction
3. Make a list of required resources
4. Document the current procedure
5. Add supporting media
6. Include any relevant resources
7. Check the procedure is accurate
8. Test in a controlled environment
9. Make improvements if necessary
10. Deploy

E. Tools equipment and materials used

Explain clearly a proper selection of tools and equipment you have used in your installation, and how they work.

F. Technical journal and Recommendation report

- **Technical journal** is a multidisciplinary **journal** in the field of engineering science and technology that offers platform for researchers, engineers and scientists to publish their original and to date research of high scientific value.

The **journal** is being published electronically as well as in print form.

Technical Journal introduces its readers to all the latest technologies, products, and solutions to any problems to be occurred.

- **Recommendation report**

recommendation report proposes a solution to a problem or evaluates possible solutions and recommends one. Before proposing or recommending a solution, the **report** needs to identify the problem. Think about the various problems you encounter every day or read about in the paper.

3. Report: A report is a document that presents information in an organized format for a specific audience and purpose. Although summaries of reports may be delivered orally, complete reports are almost always in the form of written documents.

L.O 4.2: Report the procedures of the task accomplished are in place and used

Content/Topic1: Description Report the procedures of the task accomplished are in place and used

A. Review of user manual and previous report

The User Manual contains all essential information for the user to make full use of the information system. This manual includes a description of the system functions and capabilities, contingencies and alternate modes of operation, and step-by-step procedures for system access and use. Use graphics where possible. The manual format may be altered if another format is more suitable for the particular project.

B. Suggestion of solutions on problems found

The User Manual contains all essential information for the user to make full use of the information system. This manual includes a description of the system functions and capabilities, contingencies and alternate modes of operation, and step-by-step procedures for system access and use. Use graphics where possible. The manual format may be altered if another format is more suitable for the particular project.

1. Cable Problem: Cables that connect different parts of a network can be cut or shorted. A short can happen when the wire conductor comes in contact with another conductive surface, changing the path of the signal. Cable testers can be used to test for many types of cable problems such as:
Cut cable, incorrect cable connections, Cable shorts, Interference level, Connector Problem

2. Connectivity Problem: A connectivity problem with one or more devices in a network can occur after a change is made in configuration or by a malfunction of a connectivity component, such as hub, a router or a Switch.

3. Excessive Network Collisions: These often lead to slow connectivity. The problem can occur as a result of bad network setup/plan, a user transferring a lot of information or jabbering network card.

NB: A jabbering Network card is a network card that is stuck in a transmit mode. This will be evident because the transmit light will remain on constantly, indicating that the Network card is always transmitting.

4. Software Problem: Network problems can often be traced to software configuration such as DNS configuration, WINS configuration, the registry etc.

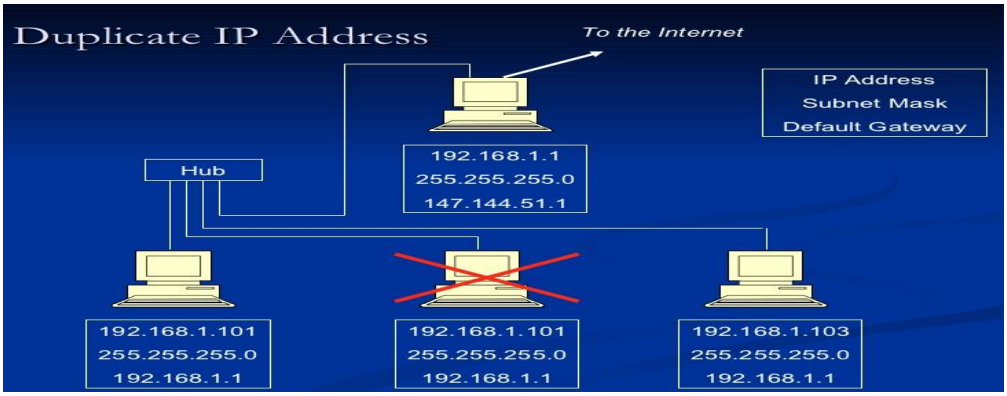
5. Duplicate IP Addressing: A common problem in many networking environments occurs when two machines try to use the same IP address. This can result in intermittent communications.

C. Description of solution implementation

In today's world, every organization relies upon a good and hassle free **Computer Network** to maintain a good flow of data or information exchange. A Computer Network is the cornerstone of every organization used to share or exchange information which can be a image, text, video, sound clip or any other type of media or file. But it's very embarrassing when we face some technical problems in our network which hampers our work. Here I am sharing some common network issues and some steps to come up with those issues.

1. Duplicate IP Address

Sometimes, more than one PC is trying to use same IP address by manual confirmation mistake, this can cause network issue with the parent network of computer or also it can intermittent network communications.



Duplicate IP Address

Solution: – Always try to find and assign a unique IP address for your PC or every computer system.

2. NIC got damaged or not placed well

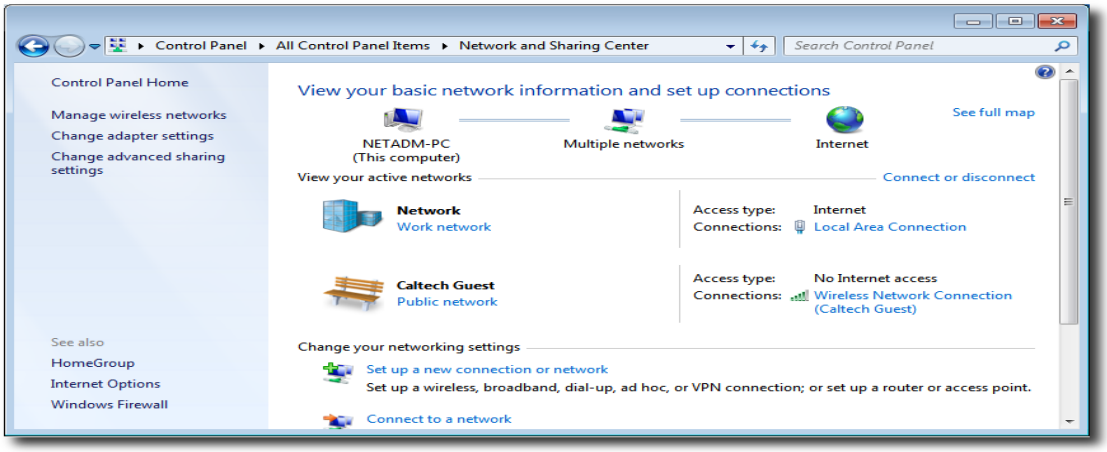
NIC (Network Interface Card) is the most vital component of computer network is responsible for creating a temporary connection of your computer to a computer network.


Damaged NIC

Solution: – For NIC issue check your NIC to find whether it is good or damaged or installed properly or not. And you can also do ping the computers and analyze the problem and change the settings according to your problems or requirements.

3. No Network Access Issue

Sometimes we see "**No Network Access**" icon in our working computers or either we see a HTTP 504 web server error code.

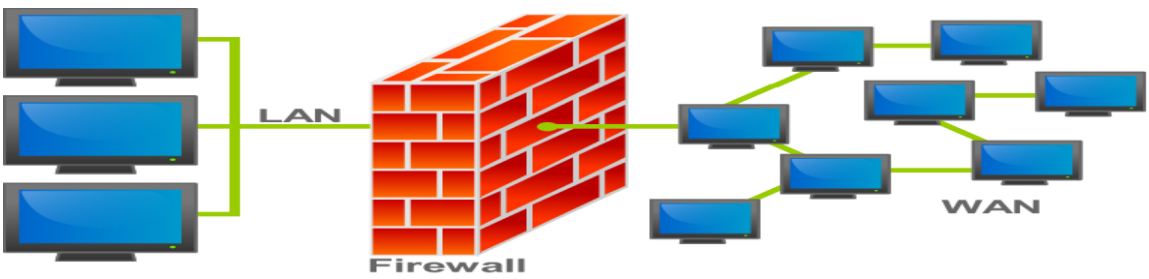


No Network Access

Solution: – To solve this problem, check each and every component and wires are connected properly and if not then connect it properly or reset all the connections. You can also check the Hub or Router settings and if anything wrong is there just correct it or else you can restart the whole setup or connection.

4. Check Firewall Restrictions or Settings

Sometimes, Firewall will restrict and disallow the network access or file sharing between the computers in your network. That's due to firewall restrictions which encounters no network issue or deny the network communication. Firewalls are responsible to protect your PC from threats or malware which can be come into your PC over internet or other network sources.



Firewall Restrictions

Solution: – Change your computer's firewall settings and enable it for accessing network sharing and services. Then you'll be able to connect, share and receive files, data or other media files from your networking system.

5. Slow Internet or Network Speed

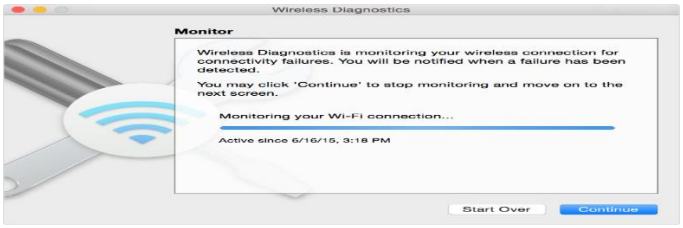
You noticed some glitches in speed like slow internet or data transmission over the network then most of time usually people thought that they've excesses the data limit. This is also true but sometimes, it causes due to improper planning of network which causes the slower internet speed or data transmission over the network.

slow internet connection

Solution: – Make sure that all the peripherals are connected and working properly. Use file compression technologies to reduce the burden of bulky files on network. Find and analyze the users to allocate network bandwidth according to the user's needs to avoid excessive use of bandwidth or network space. And check your network card, is it updated or working properly or not, if anything is wrong then correct or replace it for a smoother networking performance.

6. Regular drops of network

You have noticed regular network connection failures or drops in network connections. Some physical damage of cables or wrong setup of network peripherals might be responsible for this.



Network Drops

Solution: – Check and identify the faulty areas, and if you see any cut or noise in cables then cut or replace it. Check to ensure the correct setup of routers, hubs and other network peripherals, and if anything is wrong there just correct it for a smooth networking experience.

D. Description of procedures of the task accomplished

For an implementation process to be successful, many tasks between different departments need to be accomplished in sequence. Companies strive to use proven methodologies and enlist professional help to guide them through the implementation of a system but the failure of many implementation processes often stems from the lack of accurate planning in the beginning stages of the project due to inadequate resources or unforeseen problems that arise.

E. Tools equipment and materials used

Equipment and Accessories	Tools	Materials
LAN Card	Screwdriver(standard)	Software applications
UPS	Screwdriver(Philips)	Network OS Software
Server	Long nose pliers	RJ 45
24 port-hub	Mechanical pliers	UTP Cat 5 cable
Modem	Allen wrench	Motherboard's manual and
Fax machine	Multitester	installer
PC Video camera	Crimping tools	Sound device driver
USB External CD writer	Soldering iron (30 watts)	installer
USB scanner	Wire stripper	
USB printers	LAN Tester Anti-static wrist	
USB Flash Drive	wrap	
	Device drivers/installers	

LAN CARD
It is a network interface card. This is a computer circuit board or card that is installed in a computer so that it can be connected to a network.

SERVER
It is a part of a network. It is a special computer that users on the network can access to carry out a particular job.

HUB/PORT
It is a connector on the back of a computer or other device. A port is either a serial port or a parallel port.

MODEM
The modem is a device that allows a given computer to share data or otherwise a device which let computers exchange information

CANNER
It is an input device that read text or illustration printed on paper, translates the information into a form that a computer can use

FLAT SCREW DRIVER
It is used to drive or fasten negative slotted screws

USB
Universal Serial Bus, a hardware interface for low-speed peripherals such as the keyboard, mouse, joystick, scanner, printer and telephony devices.

PRINTER
It is a piece of hardware that produces a paper copy (also known as 'hardcopy') of the information generated by the computer.

RAM
Random Access Memory, is a primary memory. This memory is used inside the computer to hold programs and data while it is running.

BIOS
Basic Input / Output System, chip that controls the most basic functions of the computer and performs a self-test every time you turn it on.

FLASH DRIVE
RAM that can retain data without electrical power. It is widely used for BIOS chips and for digital camera and digital music storage

VIDEO CAMERA
A camera using videotape: a camera that records onto videotape

LONG NOSE PLIERS
It is used for holding, bending and stretching the lead of electronics component or connecting wire.

SOLDERING IRON
It is used to join two or more metal conductors with the support of soldering lead melted around it.

DESOLDERING TOOL
It is used to unsolder unwanted parts or component in the circuit with the support of soldering pencil.

PHILIPS SCREW DRIVER
It is used to drive or fasten positive slotted screws.

LAN TESTER
For RJ11,12,45 & BNC w/ Remote Unit This ergonomic tester is designed to test most network cable wiring. You can either conduct an auto or manual test.

UTP

Unshielded Twisted Pair, is a popular type of cable used in computer networking that consists of two

shielded wires twisted around each.

F. Technical journal and recommendation report

1. Technical journal

In the modern high performance computing systems, innovative as well as hi-tech research is required to address the challenges in the networking. The Journal of Networking Technology will act as a platform to

publish and disseminate the cross cutting research in networking systems. The journal solicits original research in the following but not limited areas.

Computer network components
Network architecture and design
Digital networks
Broadband networks
Internet and Web Technology
Sensor networks
Adhoc networks
Mobile and wireless networks
Data networks
Next generation networks
Optical networks
Neural networks
Signal processing
Satellite communication

2. Recommendation report

Basic Network Recommendations

- ✓ **Correct User Rights**

Administrator rights should be granted with caution. Users who have administrator rights can potentially do things that could be seriously damaging. They can, and do, unintentionally make changes that decrease the level of network security. They can also be tricked into running malware, which would run with the user's administrator privileges.

If they are careless about protecting their authentication details, their user-name and password may be stolen. This may allow unauthorized third parties to log in and carry out damaging actions, intentionally or accidentally. For better security, make sure that users have a privilege level which is appropriate for the tasks they carry out and minimize the number of users that have administrator privileges.

- ✓ **Only Download from Trusted Websites**

You should determine who has a genuine business need to download files and applications from a website. Use web filtering to restrict this to people with a genuine requirement and ensure that the select few are educated in how to download files safely. Files can often be downloaded from multiple locations on the Internet, but not all locations are equally secure. Make sure that your users can only download from trusted sites, such as primary source websites rather than file-sharing or generic websites.

- ✓ **Review Network Shares**

Carry out an audit of network shares. Users should only have access to files and folders that they need as part of their day-to-day work. You should also be aware that a lot of malware can spread via networks. This is typically due to there being little or no security on network shares. Remove access to unnecessary shares and secure the others and their contents to limit network-aware malware from spreading.

- ✓ **Restrict Network Connections**

When a computer connects to a network, it can adopt that network's security settings for that specific session. If the network is outside the administrator's control, the security settings may be weak and put the computer at risk. Restrict users from connecting computers to unapproved networks. In most instances users only need to connect to the main company network.

- ✓ **Change Your Default IP Range**

Networks typically use standard IP ranges, like 10.1.x.x or 192.168.x.x. This standard approach means machines configured to look for this range could accidentally connect to a network outside your control. Change the default IP range so that computers are less likely to find a similar range. You should also consider adding firewall rules, which allows only approved users to connect.

- ✓ **Review Open Ports**

You should periodically audit the open ports on your network and block all unused ones. If you leave them open for long periods of time without surveying them, you increase the chance of letting in intruders. If ports are left open, Trojans and Worms may use them to communicate with unauthorized third-parties.

- ✓ **Audit the Entry Points to Your Network**

Networks undergo frequent change, so it is very important to review all the routes into your organization's infrastructure on a regular basis. For each means of entry, consider how to best secure the routes to stop unwanted files and applications entering undetected or sensitive information leaking out.

- ✓ **Network Segmentation**

There are a number of advantages to segmenting your network.
Improved security comes from the fact that broadcasts will be contained to local network and internal network structure will not be visible from outside. If an attacker gains unauthorized access to a network, segmentation or "zoning" can provide effective controls to limit further movement across the network.
Improved performance can be achieved, because on a segmented network there are fewer hosts per subnetwork, thus minimizing local traffic. It can also help to containing network problems, limiting the effect of local failures on other parts of network.
When business critical systems are affected, they can slow business processes significantly. To help protect them, consider having them on a different network from the one used for day-to-day activities.

- ✓ **Resist the Temptation to Live Test**

Although most software developers are good people and rigorously test their software before releasing it, they are unlikely to have your infrastructure's exact configuration and setup. To ensure that a new software version or update does not cause problems, test it on a virtual system and check its effects before deploying to the real live network.

- ✓ **Block Unused USB Ports**

Many devices, when connected to a USB port, can be automatically detected and mounted as a drive. USB ports may also allow attached devices to auto-run stored software. Users are often unaware that even the safest and most trusted devices can potentially introduce malware onto their computer. To prevent any accidents, it is much safer to disable all unused ports.

L.O 4.3: Write the technical journal and recommendation

Content/Topic1: Review of user manual and previous report

- **Report:** A report is a document that presents information in an organized format for a specific audience and purpose. Although summaries of reports may be delivered orally, complete reports are almost always in the form of written documents.

- **The main advantages of report writing?**

1. **Report gives consolidated and updated information.**

A report provides consolidated, factual and an up-to-date information about a particular matter or subject. Information in the report is well organized and can be used for future planning and decision making.

2. **Report as a means of internal communication.**

A report acts as an effective means of communication within the organization. It provides feedback to employees. It is prepared for the information and guidance of others connected with the matter/ problem.

3. **Report facilitates decision making and planning**

Report provide reliable data which can be used in the planning and decision making process. It acts as a treasure house of reliable information for long term planning and decision making.

4. **Report discloses unknown information**

Reports provide information, which may not be known previously. The committee members collect data, draw conclusions and provide information which will be new to all concerned parties. Even new business opportunities are visible through unknown information available in the reports.

2. **Report gives Information to employees**

Reports are available to managers and departments for internal use. They are widely used by the departments for guidance. Report provide a feedback to employees and are useful for their self-improvement.

3. **Report gives reliable permanent information**

The information provided by a report is a permanent addition to the information available to the office. We have census reports (prepared since last 100 years) which are used even today for reference purpose.

4. **Report facilitates framing of personnel policies**

Certain reports relating to employees are useful while preparing personnel policies such as promotion policy, training policy and welfare facilities to employees.

5. **Report gives information to shareholders**

Some company reports are prepared every year for the benefit of shareholders. Annual report for example, is prepared and sent to all shareholders before the AGM. It gives information about the progress of the company.

6. **Report gives information to the Registrar**

Annual report and annual accounts are sent to the Registrar every year for information. Such reports enable the government to keep supervision on the companies.

7. **Report solves current problems**

Reports are useful to managers while dealing with current problems faced by the company. They provide guidance while dealing with complicated problems.

8. **Report helps directors to take prompt decisions**

Company reports relate to internal working of the company and are extremely useful to directors in decision making and policy framing. Reports give reliable, updated and useful information in a compact form.

- **Report Writing Format**

Here are the main sections of the standard report writing format:

- **Title Section** – This includes the name of the author(s) and the date of report preparation.

- **Summary** – There needs to be a summary of the major points, conclusions, and recommendations. It needs to be short as it is a general overview of the report. Some people will read the summary and only skim the report, so make sure you include all the relevant information. It would be best to write this last so you will include everything, even the points that might be added at the last minute.

- **Introduction** – The first page of the report needs to have an introduction. You will explain the problem and show the reader why the report is being made. You need to give a definition of terms if you did not include these in the title section, and explain how the details of the report are arranged.

- **Body** – This is the main section of the report. There needs to be several sections, with each having a subtitle. Information is usually arranged in order of importance with the most important information coming first.

- **Conclusion** – This is where everything comes together. Keep this section free of jargon as most people will read the Summary and Conclusion.

- **Recommendations** – This is what needs to be done. In plain English, explain your recommendations, putting them in order of priority.

- **Appendices** – This includes information that the experts in the field will read. It has all the technical details that support your conclusions.

Remember that the information needs to be organized logically with the most important information coming first.

- Pointers to score high in Report Writing

1. **Use names and pronouns**
2. **Limit yourself to one idea per sentence.**

Short, straightforward sentences are easy to read, understand and save time for everyone. You will appreciate this time-saving tip when you are reviewing a report to prepare for an important business meeting. Also, the longer a sentence is, the more likely you are to make an error.

Short sentence and its structure in English generally begin with a noun, and the grammar is simple. Complicated sentences, on the other hand, require complicated punctuation, and they open the door to sentence errors.

Try to limit yourself to three commas per sentence. If a sentence has more than three commas, it's probably too complicated to be read easily, and it may contain usage or punctuation errors.

3. **Be as clear and specific as possible.**

"Contacted" is vague: Did you visit, phone, or email the witness? "Residence" is just as confusing: House, apartment or mobile home? Always strive for clarity.

4. **Use simple language.**

"Since" is easier to understand (and write)

5. **Stick to observable facts.**

Conclusions, guesses, hunches, and other thought processes do not belong in a report.

6. **Write in paragraphs.**
7. **Use active voice.**
8. **Use bullet style.**

- **Sample of Report**

Typical structure template for writing a committee report:

1. **Members to which the report is meant for**
    - [Name, institution, location, Chair]
    - [Name, institution, location, member]
2. **[Date, Time, and Location]**
    - [Provide simple documentation of any meetings of the committee or subset of the committee, in whatever mode and format, e.g., in person, conference call, etc.]
3. **Purpose**
    - [Here you mention the purpose of the report in a brief. This enables the reader to understand the purpose behind writing the format.]
4. **Issues** [Write different issues as sub headings and explain their highlights in bullet points below the respective sub headings]

- Current Status
- Accomplishments / Issue 1
- Future Goals

5. **Near-Term Plans / Main Body of the Report**
6. **Informal Recommendation(s)**

References

1. Network topology. (2010, February 8). In Wikipedia, The Free Encyclopedia. Retrieved February 9, 2010, from http://en.wikipedia.org/w/index.php?title=Network_topology&oldid=342762416

2. Mitchell, B. (2010). Introduction to Client Server Networks. Retrieved March 1, 2010, from About.com: http://compnetworking.about.com/od/basicnetworkingfaqs/a/client-server.htm

3. Dionys, D. (2008). How to Make a Network Cable? Unpublished. Produced for the VVOB Program in Zambia 2008-2013. For more information about VVOB seewww.vvob.be