MINISTRY OF EDUCATION

DIPLOMA IN INFORMATION COMMUNICATION TECHNOLOGY

KENYA INSTITUTE OF CURRICULUM DEVELOPMENT
STUDY NOTES

Data Communication & Networking

MODULE III: SUBJECT NO 3

Contents

TOPIC 1: DATA COMMUNICATION AND NETWORKING

T1.1) Meaning of computer network

A **computer network** or data **network** is a telecommunications **network/link** which allows **computers** to exchange data. In **computer networks**, networked computing devices pass data to each other along **network** links (data connections). Data is transferred in the form of packets.

A ***computer network*** is a set of *computers* connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server.

T1.2) Components of computer network

Computer network components include the major parts that are needed to install a network both at the office and home level. Before delving into the installation process, you should be familiar with each part so that you could choose and buy the right component that fits with your network system.

These hardware components include **cable**, **Hub**, **Switch**, **NIC** (network interface card), **modem** and **router**. Depending on the type of network you are going to install, some of the parts can be eliminated. For example, in a wireless network you don't need cables, hubs so on.

In this article we will discuss about the main computer network components required **to install simple computer network**, often called **LAN** (local area network).

Major computer network components

Computer network requires the following devices (some of them are optional):-

- Network Interface Card (NIC)
- Hub
- Switches
- Cables and connectors
- Router
- Modem

1. Network Interface Card
Network adapter is a device that enables a computer to talk with other computer/network. Using unique **hardware addresses (MAC address)** encoded on the card chip, the data-link protocol employs these addresses to discover other systems on the network so that it can transfer data to the right destination.

There are **two types of network cards**: **wired and wireless**. The wired NIC uses cables and connectors as a medium to transfer data, whereas in the wireless card, the connection is made using antenna that employs radio wave technology. All modern laptop computers incorporated wireless NIC in addition to the wired adapter.

Network Card Speed
Network Interface card, one of the main computer network components, comes with different speeds, 10Mbps, 100Mbps, and 1000Mbps, so on. Recent standard **network cards built with Gigabit** (1000Mbps) connection speed. It also supports to connect slower speeds such as 10Mbps and 100Mbps. However, the speed of the card depends on your LAN speed.

For example, if you have a switch that supports up to 100Mbps, your NIC will also transfer a data with this same speed even though your computer NIC has still the capability to transfer data at 1000Mbps (1Gbps). In modern computers, network adapter is integrated with a computer motherboard. However if you want advanced and fast Ethernet card, you may buy and install on your computer using the **PCI slot** found on the motherboard (desktop) and **ExpressCard slots** on laptop .

2. Hub
Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer request information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.

Currently Hubs are becoming obsolete and replaced by more advanced communication devices such as **Switchs and Routers**.

3. Switch
Switch is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses **physical device addresses** in each incoming messages so that it can deliver the message to the right destination or port.

Like Hub, switch don't broadcast the received message to entire network, rather before sending it checks to which system or port should the message be sent. In other words switch connects the source and destination directly which increases the speed of the network. Both switch and hub have common features: Multiple RJ-45 ports, power supply and connection lights.

4. Cables and connectors
Cable is one way of transmission media which can transmit communication signals. The wired network typology uses special type of cable to connect computers on a network.

There are a number of solid transmission Media types, which are listed below. - **Twisted pair wire**

It is classified as Category 1, 2, 3, 4, 5, 5E, 6 and 7. Category 5E, 6 and 7 are high-speed cables that can transmit 1Gbps or more. -

Coaxial cable
Coaxial cable more resembles like TV installation cable. It is more expensive than twisted-pair cable but provide high data transmission speed.

Fiber-optic cable
It is a high-speed cable which transmits data using light beams through a glass bound fibers. Fiber-optic cable is high data transmission cable comparing to the other cable types. But the cost of fiber optics is very expensive which can only be purchased and installed on governmental level.

5. Router
When we talk about computer network components, the other device that used to **connect a LAN with an internet connection is called Router**. When you have **two distinct networks** (LANs) or want to share a single internet connection to multiple computers, we use a Router.

In most cases, recent routers also include a switch which in other words can be used as a switch. You don't need to buy both switch and router, particularly if you are installing small business and home networks.

There are two types of Router: **wired and wireless**. The choice depends on your physical office/home setting, **speed** and **cost**.

6. Modems
A modem enables you to connect your computer to the available internet connection over **the existing telephone line**. Like NIC, **Modem is not integrated with a computer motherboard**. It comes as separate part which can be installed on the PCI slots found on motherboard.

A modem is not necessary for LAN, but required for internet connection such as dial-up and DSL.

There are some types of modems, which differs in **speed and transmission rate**. Standard PC modem or Dial-up modems (56Kb data transmission speed), Cellular modem (used in a laptop that enables to connect while on the go), **cable modem (500 times faster than standard modem)** and DSL Modems are the most popular.

T1. 3) Types of computer networks

Different types of (private) networks are distinguished based on their size (in terms of the number of machines), their data transfer speed, and their reach.
Private networks are networks that belong to a single organization.

There are usually said to be three categories of networks:

- LAN (**local area network**)

- MAN (**metropolitan area network**)
- WAN (**wide area network**)

There are two other types of networks:

- **TANs (Tiny Area Network)**, which are the same as LANs but smaller (2 to 3 machines),
- and **CANs (Campus Area Networks)**, which are the same as MANs (with bandwidth limited between each of the network's LANs).

***LAN* stands for *Local Area Network*.**
It's a group of computers which all belong to the same organization, and which are linked within a small geographic area using a network, and often the same technology (the most widespread being Ethernet).

A local area network is a network in its simplest form. Data transfer speeds over a local area network can reach up to 10 Mbps (such as for an Ethernet network) and 1 Gbps (as with FDDI or Gigabit Ethernet).
A local area network can reach as many as 100, or even 1000, users.

Note
Ethernet (also known as *IEEE 802.3 standard*) is a data transmission standard for local area networks based on the following principle:

- `All machines on an Ethernet network`
- `are connected to the same communication line,`
- `made up of cylindrical cables`

FDDI (*Fiber Distributed Data Interface*) technology is network access technology over *fibre optic* type lines.

By expanding the definition of a LAN to the services that it provides, two different operating modes can be defined:

- In a "peer-to-peer" network, in which communication is carried out from one computer to another, without a central computer, and where each computer has the same role.
- in a "client/server" environment, in which a central computer provides network services to users.

MANs (*Metropolitan Area Network*s) connect multiple geographically nearby LANs to one another (over an area of up to a few dozen kilometres) at high speeds. Thus, a MAN lets two remote nodes communicate as if they were part of the same local area network.

A MAN is made from switches or routers connected to one another with high-speed links (usually fibre optic cables).

A **WAN** (**Wide Area Network or extended network**) connects multiple LANs to one another over great geographic distances.

The speed available on a WAN varies depending on the cost of the connections (which increases with distance) and may be low.

WANs operate using **routers**, which can "choose" the most appropriate path for data to take to reach a network node.

Other Types of Area Networks

While LAN and WAN are by far the most popular network types mentioned, you may also commonly see references to these others:

- **Wireless Local Area Network** - a LAN based on Wi-Fi wireless network technology
- **Metropolitan Area Network** - a network spanning a physical area larger than a LAN but smaller than a WAN, such as a city. A MAN is typically owned an operated by a single entity such as a government body or large corporation.
- **Campus Area Network** - a network spanning multiple LANs but smaller than a MAN, such as on a university or local business campus.
- **Storage Area Network** - connects servers to data storage devices through a technology like Fibre Channel.
- **System Area Network** (also known as Cluster Area Network).- links high-performance computers with high-speed connections in a cluster configuration.

T1.4) Role of computer networks

Describes why and how computer networks support successful work

Information and communication are two of the most important strategic issues for the success of every enterprise. While today nearly every organization uses a substantial number of computers and communication tools (telephones, fax, personal handheld devices), they are often still isolated. While managers today are able to use the newest applications, many departments still do not communicate and much needed information cannot be readily accessed.

To overcome these obstacles in an effective usage of information technology, computer networks are necessary. They are a new kind (one might call it paradigm) of organization of computer systems produced by the need to merge computers and communications. At the same time they are the means to converge the two areas; the unnecessary distinction between tools to process and store information and tools to collect and transport information can disappear. Computer networks can manage to put down the barriers between information held on several (not only computer) systems. Only with the help of computer networks can a borderless communication and information environment be built.

Computer networks allow the user to access remote programs and remote databases either of the same organization or from other enterprises or public sources. Computer networks provide communication possibilities faster than other facilities. Because of these optimal information and

communication possibilities, computer networks may increase the organizational learning rate, which many authors declare as the only fundamental advantage in competition.

Besides this major reason why any organization should not fail to have a computer network, there are other reasons as well:

- cost reduction by sharing hard- and software resources
- high reliability by having multiple sources of supply
- cost reduction by downsizing to microcomputer-based networks instead of using mainframes
- greater flexibility because of possibility to connect devices from various vendors

Because of the importance of this technology, decisions of purchase, structure, and operation of computer networks cannot be left to technical staff. Management as well has a critical need for understanding the technology of computer networks.

T1.5) Network topologies

What is a Topology?

A topology is a usually schematic description of 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.

The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Physical topology should not be confused with logical topology which is the method used to pass information between workstations. Logical topology was discussed in the Protocol chapter.

Main Types of Physical Topologies

The following sections discuss the physical topologies used in networks and other related topics.

- Linear Bus
- Star
- Tree (Expanded Star)
- Considerations When Choosing a Topology
- Summary Chart

Linear Bus

A linear bus topology consists of a main run of cable with a terminator at each end (See fig. 1). All nodes (file server, workstations, and peripherals) are connected to the linear cable.

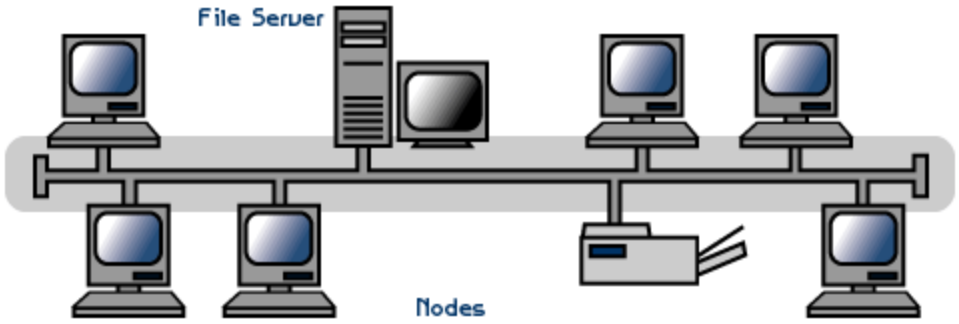


Fig. 1. Linear Bus topology

Advantages of a Linear Bus Topology

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages of a Linear Bus Topology

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.

Star

A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub, switch, or concentrator (See fig. 2).

Data on a star network passes through the hub, switch, or concentrator before continuing to its destination. The hub, switch, or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow. This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.

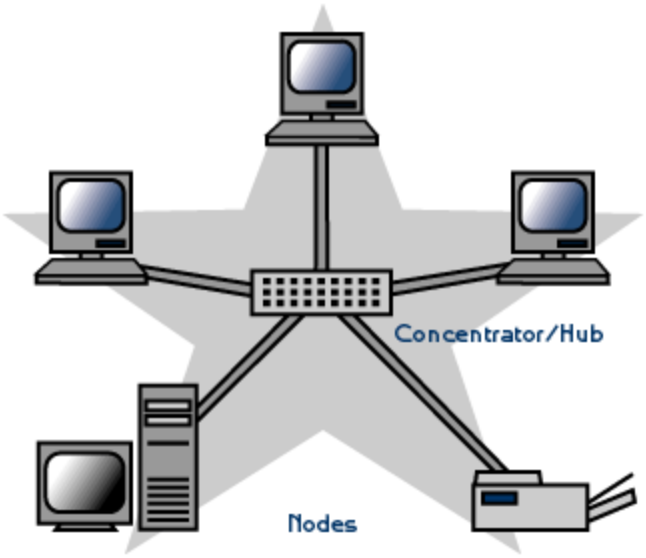


Fig. 2. Star topology

Advantages of a Star Topology

- Easy to install and wire.
- No disruptions to the network when connecting or removing devices.
- Easy to detect faults and to remove parts.

Disadvantages of a Star Topology

- Requires more cable length than a linear topology.
- If the hub, switch, or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the hubs, etc.

Tree or Expanded Star

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable (See fig. 3). Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.

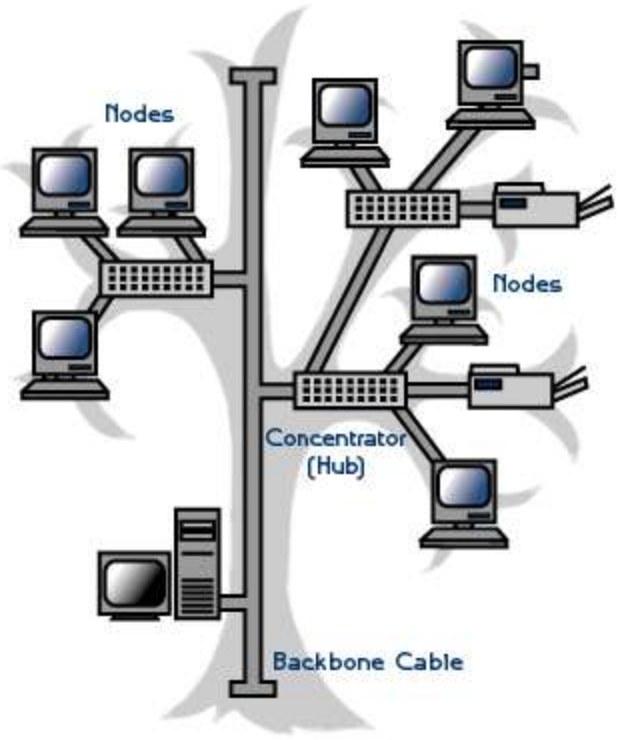


Fig. 3. Tree topology

Advantages of a Tree Topology

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

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.

5-4-3 Rule

A consideration in setting up a tree topology using Ethernet protocol is the 5-4-3 rule. One aspect of the Ethernet protocol requires that a signal sent out on the network cable reach every part of the network within a specified length of time. Each concentrator or repeater that a signal goes through adds a small amount of time. This leads to the rule that between any two nodes on the network there can only be a maximum of 5 segments, connected through 4 repeaters/concentrators. In addition, only 3 of the segments may be populated (trunk) segments if they are made of coaxial cable. A populated segment is one that has one or more nodes attached to it . In Figure 4, the 5-4-3 rule is adhered to. The furthest two nodes on the network have 4 segments and 3 repeaters/concentrators between them.

NOTE: This rule does not apply to other network protocols or Ethernet networks where all fiber optic cabling or a combination of a fiber backbone with UTP cabling is used. If there is a

combination of fiber optic backbone and UTP cabling, the rule would translate to a 7-6-5 rule.The speed of networking switches is vastly improved over older technologies, and while every effort should be made to limit network segment traversal, efficient switching can allow much larger numbers of segments to be traversed with little or no impact to the network.

Considerations When Choosing a Topology

- **Money**. A linear bus network may be the least expensive way to install a network; you do not have to purchase concentrators.
- **Length of cable needed**. The linear bus network uses shorter lengths of cable.
- **Future growth**. With a star topology, expanding a network is easily done by adding another concentrator.
- C**able type**. The most common cable in schools is unshielded twisted pair, which is most often used with star topologies.

Summary Chart

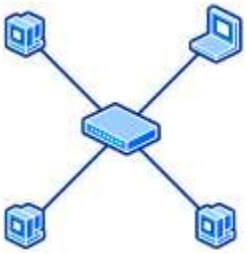
Physical Topology	Common Cable	Common Protocol
Linear Bus	Twisted Pair Coaxial Fiber	Ethernet
Star	Twisted Pair Fiber	Ethernet
Tree	Twisted Pair Coaxial Fiber	Ethernet

T1.6) Categories of computer networks

There are two different categories/architecture with which network between computers can be formed.

A network is either a peer-to-peer network (also called a workgroup) or a server-based network (also called a client/server network).

Peer-to-peer network(p2p)



In a peer-to-peer network (see Figure above), a group of computers is connected together so that users can share resources and information. There is no central location for authenticating users, storing files, or accessing resources. This means that users must remember which computers in the workgroup have the shared resource or information that they want to access. It also means that users must log on to each computer to access the shared resources on that computer.

In most peer-to-peer networks, it is difficult for users to track where information is located because data is generally stored on multiple computers. This makes it difficult to back up critical business information, and it often results in small businesses not completing backups. Often, there are multiple versions of the same file on different computers in the workgroup.

In some peer-to-peer networks, the small business uses one computer that is running a client operating system, such as Microsoft Windows 98 or Windows XP Professional, as the designated "server" for the network. Although this helps with saving data in a central location, it does not provide a robust solution for many of the needs of a small business, such as collaborating on documents.

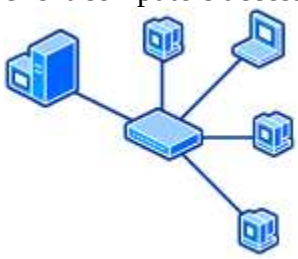
Limitation of P2P networking model:

Before deciding to implement P2P model one must know the limitations of this type. Getting to know later can be frustrating big time. It would highly be recommended to get your organizational people site together and discuss the needs. Peer to Peer looks very simple, quite cost effective and attractive, yet it can keep progress very limited.

- Peer-To-Peer networks are designed for limited number computers, it will start creating issues when exceed 15 number of computers
- High security levels can not be achieved using p2p networks, so if organization have concerns with security p2p will not be that great.
- Organizational growth will outgrow p2p networks; it will not support growing number of computers when increased above fifteen.
- Regular training is required for computer users of p2p network. p2p network is control by computers and computers are controlled by human, small mistake by one of the user can hold the work for other users on same p2p network.

Server-based network

In a server-based network, the server is the central location where users share and access network resources (see Figure below). This dedicated computer controls the level of access that users have to shared resources. Shared data is in one location, making it easy to back up critical business information. Each computer that connects to the network is called a client computer. In a server-based network, users have one user account and password to log on to the server and to access shared resources. Server operating systems are designed to handle the load when multiple client computers access server-based resources.



Windows SBS 2008 is installed and configured as the central server on a server-based network. Windows SBS 2008 provides the central point for authenticating users, accessing resources, and storing information.

Features of Server:

Servers are powerful machines when they are compared to normal desktop computers. They are meant to provide strength to computing power within the entire network. Controlling developed network can only be done by dedicated servers as they have higher specifications to support network. Servers can have better processing speed with multiple processors capability available. Server machine have higher RAM to load and execute software with ease. They have more advance network cards installed for faster data transfer. Hard drives are way bigger to store the data for entire clients. Hardware can be plugged in and plugged out while server is on, this helps network stable, and hardware like hard disk can be removed and attached accordingly.

Server Os:

Operating systems are also specially designed for servers. Server Os have much more features file serving, print serving, backing up data, enhanced security features etc. There are few major Server Os which are used commonly in servers, Windows server NT. 2000 , 2003,Linux and Novell NetWare. Windows server 2003 is more powerful and enhanced for much higher security levels, Linux servers provide the maximum security to networks.

TOPIC 2: NETWORK MEDIA

T2.1) Electrical properties of matter

Matter is defined as something that occupies space, possesses mass, offers resistance and can be felt by our senses, for example, water, metals, plants, animals, etc.

State of State?

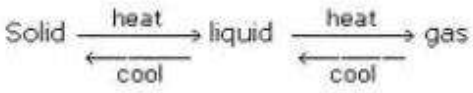
Matter exists in three physical states - Solid, Liquid and Gas. The existence of any state depends upon two main forces,

1. **Intermolecular forces :** The force which binds the constituent particles and tries to keep them close together.
2. **Thermal energy :** This is the energy which tries to keep the particles apart and makes their movement fast.

At low temperature, the thermal energy is low and intermolecular forces are strong, so the particles occupy fixed positions and can oscillate about their mean position. The compound exists in solid state.

A solid is defined as that form of matter which possesses rigidity and hence possesses a definite shape and a definite volume.

The three states are inter convertible by changing the conditions of temperature and pressure as shown below-



Properties of Solids

There are three main properties of solids which depend on their structure. The three main properties are:

1. **Electrical property**
2. **Magnetic property**
3. **Dielectric property**

Electrical properties

Solids show a wide range of electrical conductivities from 10^{-20} to 10^{7} ohm^{-1} m^{-1}. On the basis of electrical conductivity the solid can be broadly classified into three types:

Metals (conductors)

The solids which have conductivities in order of 10^4 to 10^7 ohm^{-1} m^{-1}. Metals are good conductors of electricity.

Insulators

Solids which have very low conductivity in the range 10^{-20} to 10^{-10} ohm^{-1} m^{-1}. For example wood, rubber, sulfur, phosphorus etc.

Semiconductors

Their conductivity is in between conductor and insulator up to the order of 10^{-6} to 10^4 ohm^{-1} m^{-1}.

Electrical Conductivity

Solids can conduct electrical charge due to the motion of electrons and the positive holes (electronic conductivity) or because of the motion of ions (ionic conductivity). The reason for electrical conductivity of metals is the motion of electrons and it increases by increasing the number of participating electrons in the process of conduction.

Pure ionic solids, in which conduction occurs only through the ionic motion, are termed as insulators. The defects in crystal structure increases the conductance property of semiconductor and more so with insulator. The electrical conductivity of metals, insulators and semiconductors can be explained in terms of Band Theory.

Band theory

This is based on molecular orbital theory. The molecular orbitals are formed by overlapping of atomic orbitals and the number of molecular orbitals formed are equal to the number of atomic orbitals which take part in overlapping.

In the case of metals, the atomic orbitals are very close in energy so they form a large number of molecular orbitals which are very close in energy. This set of molecular orbitals is called band which is of two types.

- **Valence band :**This is a band of lower energy
- **Conduction band :**The band of higher energy

The energy difference separating these two bands is called band gap or energy gap. These energy bands are separated by space where no energy is allowed in and are termed as forbidden bands. The top of available electron energy level at low temperature is called Fermi level.

- If the valence band is partially filled or it overlaps with higher energy or have unoccupied conduction band then the electrons can be excited from lower to higher energy level by supplying a very small amount of energy or applied electric field. Hence the metal conducts electricity and behaves as a conductor.

- If the gap between the filled valence and unfilled conduction band is large and it's not possible for electrons to jump from the valence to conduction band, then the substance has extremely low conductivity and behaves as an insulator.

- If the gap between the valence and conduction band is small and some electrons can jump from valence to conduction band, then the substance shows some amount of conductivity and behaves as a semiconductor.

Effect of temperature on conductivity

1. In the case of metals, the conductivity decreases with increase in temperature because the positive ions of metals start vibrating and produce hindrance in the flow of electrons.
2. There is no effect of temperature on the conductivity of an insulator.
3. In the case of a semiconductor, it increases by increasing the temperature as more electrons can jump from valance to conduction band.

T2.2, T2.3,T2. 4) Types of transmission media, Importance and benefits and limitations

Transmission medium

A **transmission medium** is a material substance (solid, liquid, gas, or plasma) that can propagate energy waves. For example, the transmission medium for sounds is usually air, but solids and liquids may also act as transmission media for sound.

The absence of a material medium in vacuum may also constitute a transmission medium for electromagnetic waves such as light and radio waves. While material substance is not required for electromagnetic waves to propagate, such waves are usually affected by the transmission media they pass through, for instance by absorption or by reflection or refraction at the interfaces between media.

The term transmission medium also refers to a technical device that employs the material substance to transmit or guide waves. Thus, an optical fiber or a copper cable is a transmission medium. Not only is this but also able to guide the transmission of networks.

A transmission medium can be classified as a:

- *Linear medium*, if different waves at any particular point in the medium can be superposed (**i.e.** when two waves meet they overlap and interact. Sometimes they add to make a wave bigger, sometimes they cancel each other)
- *Bounded medium*, if it is finite in extent, otherwise *unbounded medium*;
- *Uniform medium* or *homogeneous medium*, if its physical properties are unchanged at different points;
- *Isotropic medium*, if its physical properties are the same in different directions.

Transmission and reception of data is performed in four steps.

1. The data is coded as binary numbers at the sender end

2. A carrier signal is modulated as specified by the binary representation of the data
3. At the receiving end, the incoming signal is demodulated into the respective binary numbers
4. Decoding of the binary numbers is performed

Telecommunications

A physical medium in data communications is the transmission path over which a signal propagates.

Many transmission media are used as communications channel.

For telecommunications purposes in the United States, Federal Standard 1037C, transmission media are classified as one of the following:

- Guided (or bounded)—waves are guided along a solid medium such as a transmission line.
- Wireless (or unguided)—transmission and reception are achieved by means of an antenna.

Bounded/Guided Transmission Media

It is the transmission media in which signals are confined to a specific path using wire or cable. The types of Bounded/ Guided are.

1. Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 µs/km.
- Repeater spacing is 2km.

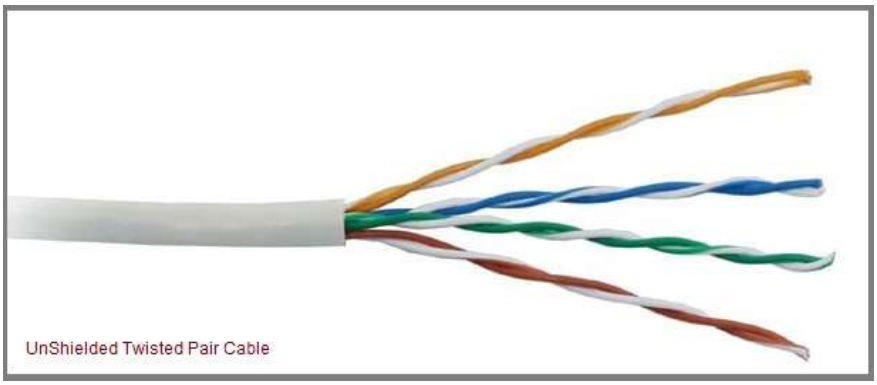
Twisted Pair is of two types :

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**

Unshielded Twisted Pair Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.

UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use **RJ-45** connector.



It can be either voice grade or data grade depending on the condition. UTP cable normally has an impedance of 100 ohm. UTP cost less than STP and easily available due to its many use. There are five levels of data cabling

Category 1	These are used in telephone lines and low speed data cable.
Category 2	These cables can support up to 4 mps implementation.
Category 3	These cable supports up to 16 mps and are mostly used in 10 mps.
Category 4	These are used for large distance and high speed. It can support 20mps.
Category 5	This is the highest rating for UTP cable and can support up to 100mps.

UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use RJ-11 connector and 4 pair cable use RJ-45 connector.

Characteristics of UTP

- low cost
- easy to install
- High speed capacity
- High attenuation
- Effective to EMI
- 100 meter limit

Advantages:

- Installation is easy
- Flexible
- Cheap
- It has high speed capacity,
- 100 meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

Disadvantages:

- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk (noise).

It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.

It is similar to UTP but has a mesh shielding that's protects it from EMI which allows for higher transmission rate.

IBM has defined category for STP cable.

Type 1	STP features two pairs of 22-AWG
Type 2	This type include type 1 with 4 telephone pairs
Type 6	This type feature two pairs of standard shielded 26-AWG
Type 7	This type of STP consist of 1 pair of standard shielded 26-AWG
Type 9	This type consist of shielded 26-AWG wire

American Wire Gauge (*AWG*) is a U.S. standard set of non-ferrous wire conductor sizes. The "*gauge*" means the diameter.

Characteristics of STP

- Medium cost
- Easy to install
- Higher capacity than UTP
- Higher attenuation, but same as UTP
- Medium immunity from EMI
- 100 meter limit

Advantages:

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission

- Increases the signalling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages:

- Difficult to manufacture
- Heavy

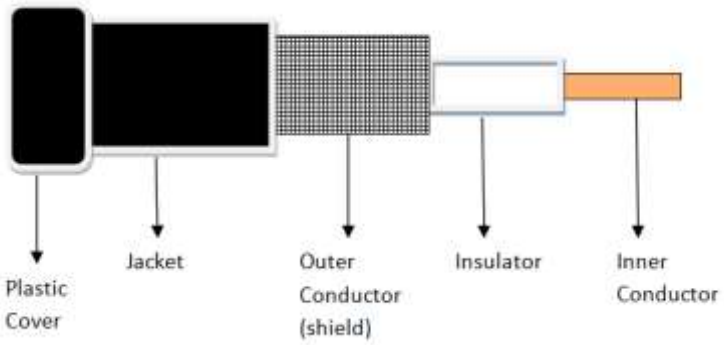
2. Coaxial Cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both.

Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

Here the most common coaxial standards.

- 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
- 50-Ohm RG-58 : used with thin Ethernet
- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.



There are two types of Coaxial cables :

Baseband: This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet.

Broadband: This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

Advantages :

- Bandwidth is high
- Used in long distance telephone lines.
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity
- Data transmission without distortion.
- The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

Disadvantages :

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

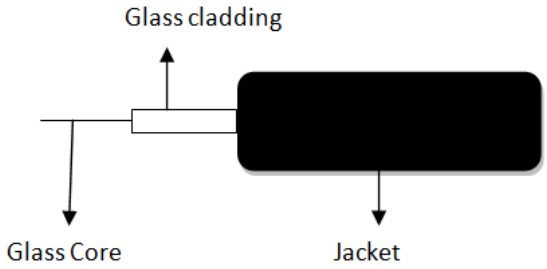
3. Fiber Optic Cable

These are similar to coaxial cable. It uses electric signals to transmit data. At the centre is the glass core through which light propagates.

In multimode fibres, the core is 50microns, and In single mode fibres, the thickness is 8 to 10 microns.

The core in fiber optic cable is surrounded by glass cladding with lower index of refraction as compared to core to keep all the light in core. This is covered with a thin plastic jacket to protect the cladding. The fibers are grouped together in bundles protected by an outer shield.

Fiber optic cable has bandwidth more than **2 gbps (Gigabytes per Second)**



Characteristics Of Fiber Optic Cable:

- Expensive
- Very hard to install
- Capable of extremely high speed
- Extremely low attenuation
- No EMI interference

Advantages:

- Provides high quality transmission of signals at very high speed.
- These are not affected by electromagnetic interference, so noise and distortion is very less.
- Used for both analog and digital signals.

Disadvantages:

- It is expensive
- Difficult to install.
- Maintenance is expensive and difficult.
- Do not allow complete routing of light signals.

UnBounded/UnGuided Transmission Media

Unguided or wireless media sends the data through air (or water), which is available to anyone who has a device capable of receiving them. Types of unguided/ unbounded media are:

- Radio Transmission
- MicroWave Transmission

1. Radio Transmission

Its frequency is between 10 kHz to 1GHz. It is simple to install and has high attenuation. These waves are used for multicast communications.

Types of Propogation

Radio Transmission utilizes different types of propogation :

- **Troposphere :** The lowest portion of earth's atmosphere extending outward approximately 30 miles from the earth's surface. Clouds, jet planes, wind is found here.
- **Ionosphere :** The layer of the atmosphere above troposphere, but below space. Contains electrically charged particles.

2. Microwave Transmission

It travels at high frequency than the radio waves. It requires the sender to be inside of the receiver. It operates in a system with a low gigahertz range. It is mostly used for unicast communication.

There are 2 types of Microwave Transmission :

1. Terrestrial Microwave
2. Satellite Microwave

Advantages of Microwave Transmission

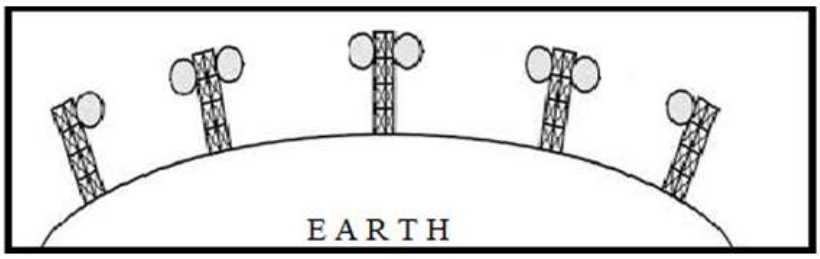
- Used for long distance telephone communication
- Carries 1000's of voice channels at the same time

Disadvantages of Microwave Transmission

- It is Very costly

Terrestrial Microwave

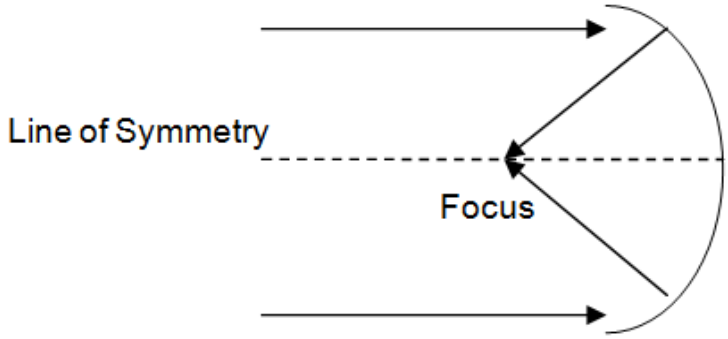
For increasing the distance served by terrestrial microwave, repeaters can be installed with each antenna .The signal received by an antenna can be converted into transmittable form and relayed to next antenna as shown in below figure. It is an example of telephone systems all over the world



There are two types of antennas used for terrestrial microwave communication :

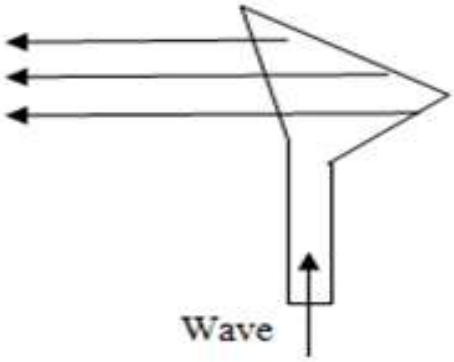
1. Parabolic Dish Antenna

In this every line parallel to the line of symmetry reflects off the curve at angles in a way that they intersect at a common point called focus. This antenna is based on geometry of parabola.



2. Horn Antenna

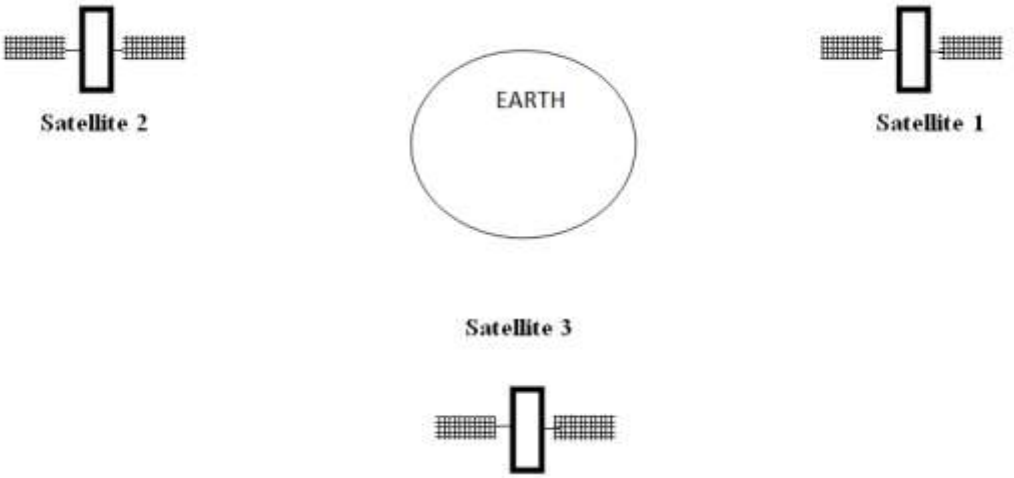
It is a like gigantic scoop. The outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by curved head.



Satellite Microwave

This is a microwave relay station which is placed in outer space. The satellites are launched either by rockets or space shuttles carry them.

These are positioned 3600KM above the equator with an orbit speed that exactly matches the rotation speed of the earth. As the satellite is positioned in a geo-synchronous orbit, it is stationery relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antenna at a fixed point in the sky.



Features of Satellite Microwave :

- Bandwidth capacity depends on the frequency used.
- Satellite microwave deployment for orbiting satellite is difficult.

Advantages of Satellite Microwave :

- Transmitting station can receive back its own transmission and check whether the satellite has transmitted information correctly.
- A single microwave relay station which is visible from any point.

Disadvantages of Satellite Microwave :

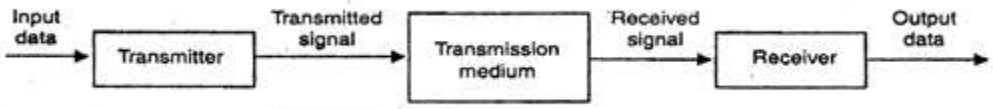
- Satellite manufacturing cost is very high
- Cost of launching satellite is very expensive
- Transmission highly depends on whether conditions, it can go down in bad weather

TOPIC 3: DATA COMMUNICATION

T3.1) Meaning of data communication

Data communication refers to the exchange of data between a source and a receiver.

The Figure is an illustration of a simple data communication system.



Simple Data Communication System

A data communication system may collect data from remote locations through data transmission circuits, and then outputs processed results to remote locations. Figure provides a broader view of data communication networks.

T3.2) Principles of data communication

a) Components of data communication system

A Communication system has following components:

1. **Message**: It is the information or data to be communicated. It can consist of text, numbers, pictures, sound or video or any combination of these.

2. **Sender**: It is the device/computer that generates and sends that message.

3. **Receiver**: It is the device or computer that receives the message. The location of receiver computer is generally different from the sender computer. The distance between sender and receiver depends upon the types of network used in between.

4. **Medium**: It is the channel or physical path through which the message is carried from sender to the receiver. The medium can be wired like twisted pair wire, coaxial cable, fiber-optic cable or wireless like laser, radio waves, and microwaves.

5. **Protocol**: It is a set of rules that govern the communication between the devices. Both sender and receiver follow same protocols to communicate with each other.

A protocol performs the following functions:

1. **Data sequencing**. It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering packets to detect loss or duplication of packets, and to correctly identify packets, which belong to same message.

2. **Data routing**. Data routing defines the most efficient path between the source and destination.

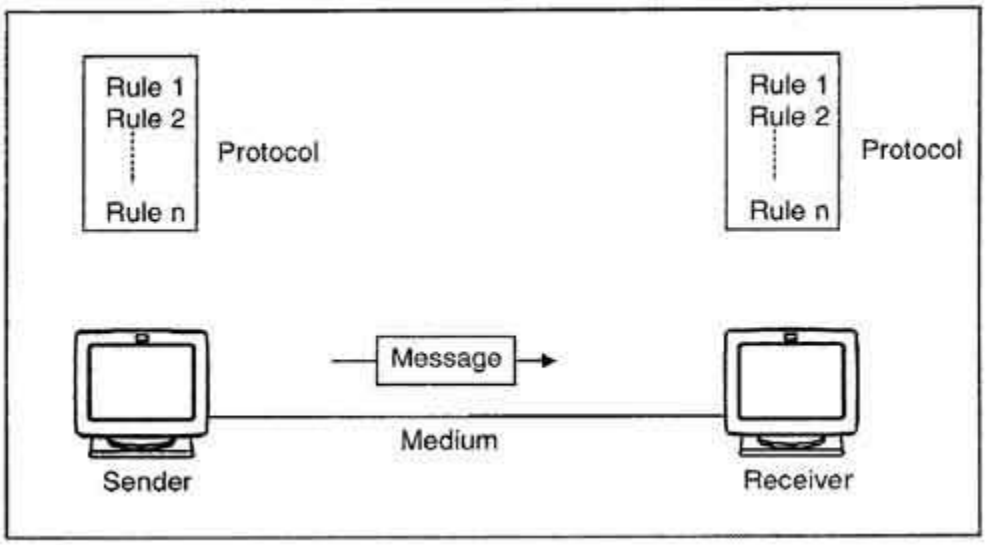
3. **Data formatting**. Data formatting rules define which group of bits or characters within packet constitute data, control, addressing, or other information.

4. **Flow control**. A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on communication lines.

5. **Error control**. These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method is to retransmit erroneous message block. In such a case, a block having error is discarded by the receiver and is retransmitted by the sender.

6. **Precedence and order of transmission**. These rules ensure that all the nodes get a chance to use the communication lines and other resources of the network based on the priorities assigned to them.

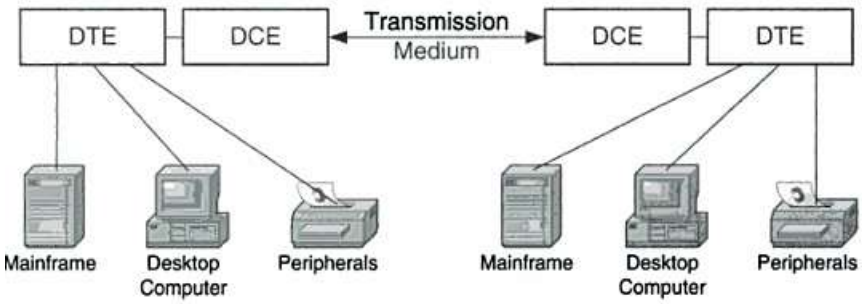
7. **Connection establishment and termination**. These rules define how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.



8. **Data security**. Providing data security and privacy is also built into most communication software packages. It prevents access of data by unauthorized users.

9. Log information. Several communication software are designed to develop log information, which consists of all jobs and data communications tasks that have taken place. Such information may be used for charging the users of the network based on their usage of the network resources.

b) Basic data communication link



Components of a basic communication link

Data Communications Equipment (DCE) can be classified as equipment that transmits or receives analogue or digital signals through a network. DCE works at the physical layer of the OSI model taking data generated by Data Terminal Equipment (DTE) and converting it into a signal that can then be transmitted over a communications link. A common DCE example is a modem which works as a translator of digital and analogue signals.

DCE may also be responsible for providing timing over a serial link. In a complex network which uses directly connected routers to provide serial links, one serial interface of each connection must be configured with a clock rate to provide synchronisation.

Other common DCE examples include:

- ISDN adapters
- Satellites (including base stations)
- Microwave stations
- NIC (network interface cards)

DCE is sometimes said to stand for **Data Circuit-terminating Equipment**.

Data Terminal Equipment (DTE) is any equipment that is either a source or destination for digital data. DTE do not generally communicate with each other to do so they need to use DCE to carry out the communication. DTE does not need to know how data is sent or received; the communications details are left to the DCE. A typical example of DTE is a computer.

Other common DTE examples include:

- Printers
- File and application servers
- PCs
- Dumb Terminals
- Routers

c) Principles of packet switching

A **packet** is a unit of data that is transmitted across a packet-switched network.

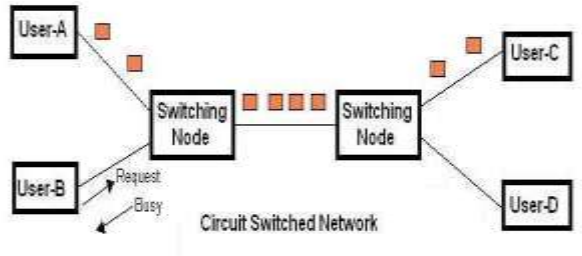
A **packet-switched** network is an interconnected set of networks that are joined by routers or switching routers. The most common packet-switching technology is TCP/IP, and the Internet is the largest packet-switched network.

Packet switching and circuit switching

These are two networking methods for transferring data between two nodes or hosts.

Circuit Switching

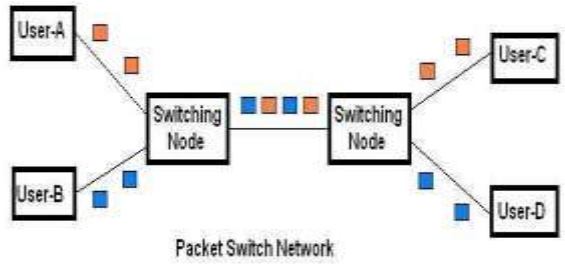
In circuit switching network dedicated channel has to be established before the call is made between users. The channel is reserved between the users till the connection is active. For half duplex communication, one channel is allocated and for full duplex communication, two channels are allocated. It is mainly used for voice communication requiring real time services without any much delay.



As shown in the figure 1, if user-A wants to use the network; it need to first ask for the request to obtain the one and then user-A can communicate with user-C. During the connection phase if user-B tries to call/communicate with user-D or any other user it will get busy signal from the network.

Packet Switching

In packet switching network unlike CS network, it is not required to establish the connection initially. The connection/channel is available to use by many users. But when capacity or number of users increases then it will lead to congestion in the network. Packet switched networks are mainly used for data and voice applications requiring non-real time scenarios.



As shown in the figure 2, if user-A wants to send data/information to user-C and if user-B wants to send data to user-D, it is simultaneously possible. Here information is padded with header which contains addresses of source and destination. This header is sniffed by intermediate switching nodes to determine their route and destination.

In packet switching, station breaks long message into packets. Packets are sent one at a time to the network. Packets are handled in two ways, viz. datagram and virtual circuit.

In **datagram**, each packet is treated independently. Packets can take up any practical route. Packets may arrive out of order and may go missing.

In **virtual circuit**, preplanned route is established before any packets are transmitted. The handshake is established using call request and call accept messages. Here each packet contains virtual circuit identifier(VCI) instead of the destination address. In this type, routing decisions for each packet are not needed.

Comparison between CS vs. PS networks

As shown above in Packet switched (PS) networks quality of service (QoS) is not guaranteed while in circuit switched (CS) networks quality is guaranteed.
PS is used for time insensitive applications such as internet/email/SMS/MMS/VOIP etc.
In CS even if user is not talking the channel cannot be used by any other users, this will waste the resource capacity at those intervals.
The example of circuit switched network is PSTN and example of packet switched network is GPRS/EDGE.

Following table summarizes difference between circuit switching and packet switching of type datagram and virtual circuit.

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

T3.3) Techniques in data communication

Digital Data Communication Techniques:

For 2 devices connected by a transmission medium to exchange data, a large degree of co-operation is necessary. Normally data is transmitted 1-bit at a time. The timing (rate, duration, spacing) of these bits have to be same for transmitter and receiver. There are only two options for transmission of bits.

1. Parallel All bits of a byte are transferred at the same time on separate parallel wires.

Synchronization between multiple bits is essential which becomes difficult over long distance. Gives huge band width but expensive. Practical only for those devices that are close to each other

2. Serial Bits transferred successively one after other. Gives low bandwidth but cheaper. Good for transmission over long distances.

Data transfer methods include many complex concepts, but we can still break down the process to a few basic types.

1. Simplex - A simplex communication system sends a message in only one direction.
2. Duplex - A half-duplex data communication system provides messages in both directions but only allows transfer in one direction at a time.
3. Full duplex - A full duplex is a communication that works both ways at the same time.

T3.4) Networking models and their importance

Network models define a set of network layers and how they interact. There are several different network models depending on what organization or company started them. The most important two are:

- **The TCP/IP Model** - This model is sometimes called the DOD model since it was designed for the department of defense It is also called the internet model because TCP/IP is the protocol used on the internet.
- **OSI Network Model** - The International Standards Organization (ISO) has defined a standard called the Open Systems Interconnection (OSI) reference model. This is a seven layer architecture listed in the next section.

Importance networking models

Network model is concerned with how different systems communicate over networks

It defines network activities into rough categories:

- Ways that applications talk to their peer applications, such as electronic mail message interchange defined by application protocols such as the Simple Mail Transfer Protocol(SMTP)

- Methods for moving bytes from network endpoint to network endpoint, using end-to-end protocols such as the Transmission Control Protocol (TCP)
- Techniques for moving (i.e., routing) packets from intermediate point (i.e., routers inside the network "cloud"
- Mechanisms for sharing a network medium, and for connecting individual device-level network interfaces to physical media.

T3.5) OSI model and different layers

Importance and illustration of ISO Model

International Standards Organization/Open System Interconnection **(ISO/OSI) model** is a standard reference model for communication between two end users in a network. It can be helpful to have a basic understanding of how your network works in order to troubleshoot future problems.

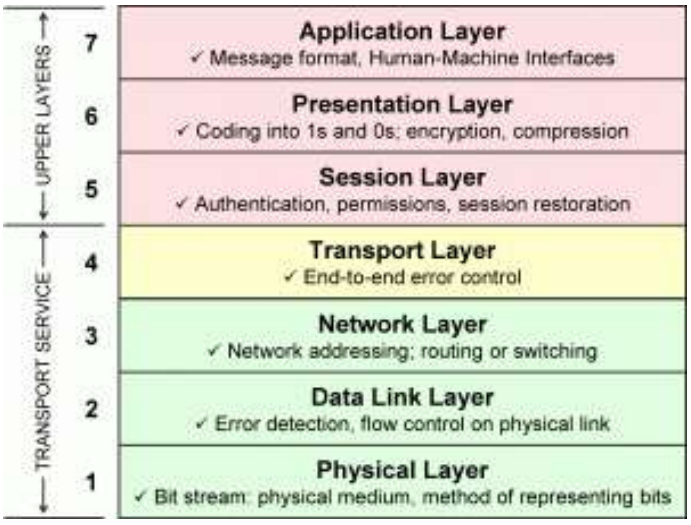
It would be difficult to overstate the importance of the OSI model. Virtually all networking vendors and users understand how important it is that network computing products adhere to and fully support the networking standards this model has generated. When a vendor's products adhere to the standards the ISO model has generated, connecting those products to other vendors' products is relatively simple. Conversely, the further a vendor departs from those standards, the more difficult it becomes to connect that vendor's products to those of other vendors.

In addition, if a vendor were to depart from the communication standards the model has engendered, software development efforts would be very difficult because the vendor would have to build every part of all necessary software, rather than being able to build on the existing work of other vendors.

The first two problems give rise to a third significant problem for vendors: a vendor's products become less marketable as they become more difficult to connect with other vendors' products.

Thus, the ISO model defines a networking framework for implementing protocols according to **seven layers**. Each layer is functionally independent of the others, but provides services to the layer above it and receives services from the layer below it.

The layers are in two groups. **The upper four layers** are used whenever a message passes from or to a user. **The lower three layers** are used when any message passes through the host computer. Messages intended for this computer pass to the upper layers. Messages destined for some other host are not passed up to the upper layers but are forwarded to another host.



The seven ISO layers are explained in more detail below:

Layer 7— The application layer: This is the layer at which communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. (This layer is not the application itself, although some applications may perform application layer functions). It represents the services that directly support applications such as software for file transfers, database access, email, and network games.

Layer 6—The presentation layer: This is a layer, usually part of an operating system, that converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text). This layer also manages security issues by providing services such as data encryption and compression. It's sometimes called the syntax layer.

Layer 5—The session layer: This layer allows applications on different computers to establish, use, and end a session/connection. This layer establishes dialog control between the two computers in a session, regulating which side transmits, and when and how long it transmits.

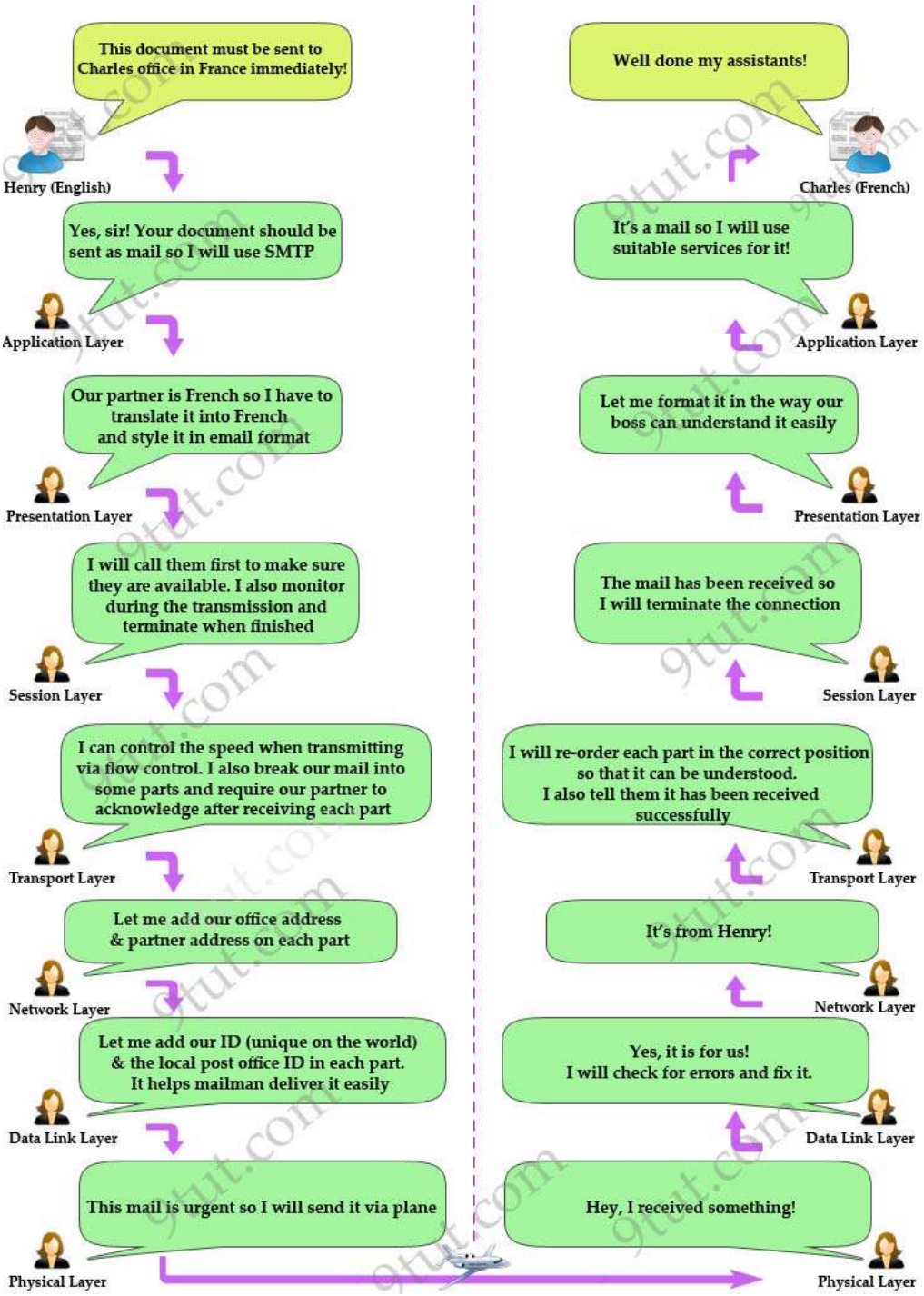
Layer 4—The transport layer: This layer handles error recognition and recovery, manages the end-to-end control (for example, determining whether all packets have arrived) and error-checking. It ensures complete data transfer.

Layer 3—The network layer: This layer handles the routing of the data, addresses messages and translates logical addresses and names into physical addresses. It also determines the route from the source to the destination computer and manages traffic problems (flow control), such as switching, routing, and controlling the congestion of data packets.

Layer 2—The data-link layer: This layer package raw bit from the Physical layer into frames (logical, structures packets for data). It is responsible for transferring frames from one computer

to another, without errors. After sending a frame, it waits for an acknowledgment from the receiving computer.

Layer 1—The physical layer: This layer transmits bits from one computer to another and regulates the transmission of a stream of bits over a physical medium. This layer defines how the cable is attached to the network adapter and what transmission technique is used to send data over the cable.



OSI 7 layer illustration diagram

Besides, the principles that led to these 7 layers were the following:

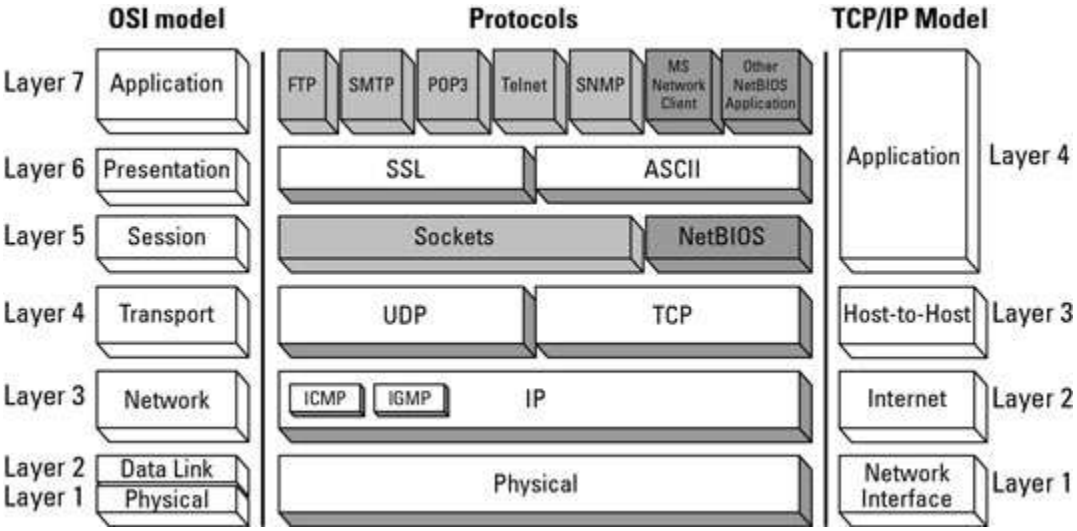
Every time a new level of abstraction for a layer is necessary; every layer has well defined functions, the functions of each layer must be chosen in the objective of the international standardization of protocols. Boundaries between layers must be chosen so as to minimize the flows of data through interfaces.

The low layers (1, 2, 3 and 4) are necessary to the routing of information between the two concerned ends and depend on the physical medium. The higher layers (5, 6 and 7) are responsible for the data processing relative to the management of exchanges between information processing systems. In addition, layers 1 to 3 intervene between close machines, but not between ending machines that can be separated by several routers. On the contrary, layers 4 to 7 intervene only between distant hosts.

TCP/IP and OSI Network Model Comparisons

The OSI model and the TCP/IP models were both created independently. The TCP/IP network model represents reality in the world, whereas the OSI mode represents an ideal. With that said, the TCP/IP network model matches the standard layered network model as it should.

The following figure shows the relationship between the OSI model and the TCP/IP model.



The TCP/IP network model has four basic layers:

- **Network interface (layer 1):** Deals with all physical components of network connectivity between the network and the IP protocol
- **Internet (layer 2):** Contains all functionality that manages the movement of data between two network devices over a routed network
- **Host-to-host (layer 3):** Manages the flow of traffic between two hosts or devices, ensuring that data arrives at the application on the host for which it is targeted
- **Application (layer 4):** Acts as final endpoints at either end of a communication session between two network hosts

T3.6) T7.2) Standards for Ethernet

Physical Ethernet Standards

Have I said that ethernet is the most popular LAN protocol? Ethernet started in the 1970s when Xerox needed a networking system to connect personal computers. Xerox joined forces with Digital Equipment Corp. (DEC) and Intel to develop the protocol, which is why the very first ethernet standards were referred to as DIX Ethernet. This section covers the progression of ethernet standards from the earlier 10Mbps connections to the more recent 10 gigabit ethernet connections.

Each standard has a maximum connection length and speed. Individual ethernet standards also specify which cables and connectors can be used for network connectivity.

Ethernet

The IEEE 802.3 ethernet standards are covered in the following sections. The following list contains all the ethernet standards that are covered in this chapter, in order.

- 10BASE-2
- 10BASE-5
- 10BASE-T
- 10BASE-FL
- 100BaseT4
- 100BaseTX
- 100BaseFX
- 1000BaseT
- 1000BaseTX
- 1000BaseCX
- 1000BaseSX
- 1000BaseLX
- 10GbE

10BASE-2

10BASE-2 networks are connected with RG-58 coaxial cables that use Bayonet Neill Concelman (BNC) connectors. There are no other hardware devices such as hubs or switches to connect devices, just the coaxial cables. This creates a physical bus topology. An electrical signal is sent by each device that wants to transmit data on that network. If more than one device sends a signal at the same time, this causes a collision and the signal is lost. To prevent loss of data transmissions, an algorithm called *Carrier Sense Multiple Access Collision Detection (CSMA/CD)* was defined. This algorithm sends a jam signal to notify the devices that there has been a collision. The devices then halt transmission for a random back-off time. CSMA/CD must be activated for 10Base ethernet LANs that are connected with a hub.

The name 10BASE-2 breaks down as follows:

- **10**—10Mbps data transmission speed

- **Base**—Represents *baseband*, the signaling mode where the media can only send one signal per wire at a time
- **2**—Actually refers to 185m or the maximum segment length (where 185 is rounded up to 200 and 2 is a multiple of 100m)

NOTE

So what you can see from the naming scheme is that the first number represents the speed, the word base means the baseband signaling mode, and the last helps you determine the type of cable used.

10BASE-5

10BASE-5 has the same characteristics as 10BASE-2, but with a maximum segment length of 500m. The 5 is also a multiple of 100m.

10BASE-T

10BASE-T has a maximum segment length of 100m and has a 10Mbps data transmission speed. 10BASE-T can use Category 3, 4, or 5 unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cables for connectivity. If you recall, UTP is the more common and cost-effective solution. STP has an additional shield that provides additional reduction of interference and attenuation, but it is also the more expensive solution. The following cables can be used with a 10BASE-T connection:

- **Category 3**—Data cable that can handle speeds up to 10Mbps.

  Although it is faster than the Cat2 cable, this was quite popular until network speeds surpassed the 10Mbps threshold.

- **Category 4**—Data cable that can handle speeds up to 16Mbps and is meant to be used with token ring LANs.
- **Category 5**—Data cable that can handle speeds up to 100Mbps and is currently the most popular cable selection.

10BASE-FL

10BASE-FL also has a 10Mbps data transmission speed, but it runs over fiber-optic cables. This option allows for a maximum segment length up to 2km.

Table 3.4 compares the 802.3 ethernet characteristics, listing the key characteristics of each specification.

Table 3.4 Summary of Ethernet 802.3 Characteristics

Standard	Speed	Maximum Distance	Media Type	Connector Used
10BASE-2	10Mbps	185m	RG-58 coaxial	BNC

10BASE-5	10Mbps	500m	RG-58 coaxial	BNC
10BASE-T	10Mbps	100m	Category 3, 4, or 5 UTP or STP	RJ-45
10BASE-FL	10Mbps	Up to 2km	Fiber-optic	SC or ST

As you can see, the early standards are all limited to 10Mbps. More recent ethernet specifications allow for faster data transmission speeds and are more popular for today's networks.

Fast Ethernet

Fast Ethernet was derived for networks that needed speeds in excess of 10Mbps. The IEEE 802.3u defines standards for 100BaseT4, 100BaseTX, and 100BaseFX. You may also hear them collectively referred to as 100BaseX. Based on what you learned from the 10Base naming scheme, you would be correct to infer that the 100 represents 100Mbps. Also, all three standards are baseband like the 10Mbps family of protocols.

NOTE

Fast Ethernet is defined in the IEEE 802.3u standard.

100BaseT4

100BaseT4 has the same characteristics as 100BaseTX except that it can use Category 3, 4, or 5 UTP or STP cables.

100BaseTX

100BaseTX, like 10BASE-T, uses either UTP or STP. Category 5 UTP cable is used with this implementation. 10BASE-T has a maximum segment length of 100m.

100BaseFX

100BaseFX uses either single-mode or multimode fiber-optic cables to connect. Multimode (MM) fiber set for half-duplex can reach a distance of 412m. Single-mode (SM) fiber set for full-duplex can reach a distance of 10,000m. SC or ST connectors can be used. The drawback, as mentioned before with fiber implementations, is the high overhead.

- **Multimode (MM) fiber**—This is generally used for shorter distances and is ideal for a campus-sized network. MM also has a larger diameter of optical fiber than SM fiber.
- **Single-mode (SM) fiber**—This mode is used to span longer distances. SM also allows for a higher data rate than MM and faster data transmission speeds.

REVIEW BREAK

Table 3.5 compares Fast Ethernet 802.3u standards.

Table 3.5 Comparison of Fast Ethernet 802.3u Characteristics

Standard	Speed	Maximum Distance	Media Type	Connector Used
100BaseT4	100Mbps	100m	Category 3, 4, or 5 UTP or STP	RJ-45
100BaseTX	100Mbps	100m	Category 5 UTP or STP	RJ-45
100BaseFX	100Mbps	412m with half-duplex MM fiber	Fiber-optic	SC or ST
		10,000m with full-duplex SM fiber		

Gigabit Ethernet

Gigabit Ethernet standards all have a data transmission speed of 1000Mbps (1Gbps) and use a baseband signaling mode. Gigabit Ethernet can be broken down into two IEEE standards, 802.3ab or 1000BaseT and 802.3z or 1000BaseX.

1000BaseT 802.3ab

1000BaseT or 1000BaseTX is defined by the 802.3ab standard and can reach a maximum total distance per segment of 75m. This standard uses a minimum of Category 5 UTP cable with an RJ-45 connector.

- **Category 5e**—Data cable that can handle speeds up to 1Gbps; a popular choice for Gigabit Ethernet networks.
- **Category 6**—Cable that was created to exceed speeds of 1Gbps.

Table 3.6 summarizes the primary points of interest that are relevant for the 1000BaseT standard.

Table 3.6 Summary of Gigabit Ethernet 802.3ab Characteristics

Standard	Speed	Maximum Distance	Media Type	Connector Used
1000BaseT or 1000BaseTX	1000Mbps or 1Gbps	75m	Category 5 UTP or higher	RJ-45

1000BaseX 802.3z

1000BaseX is the collective name for 802.3z standards 1000BaseCX, 1000BaseSX, and 1000BaseLX that have the following characteristics respectively:

- **1000BaseCX**—1000BaseCX is the unique standard in this family because it uses shielded copper wire cable with a 9-pin shielded connector instead of fiber-optic cable for connectivity. The maximum total distance per segment is a mere 25m.

- **1000BaseSX—**1000BaseSX transmits short-wavelength laser over fiber-optic cable. Either 50-micron or 62.5-micron (diameter) MM fiber can be used with this option. Lengths may vary depending on the type of MM fiber and duplex chosen for each connection as follows:
    - Half-duplex 62.5-micron MM fiber connections can reach a maximum segment length of 275m.
    - Half-duplex 50-micron MM fiber connections can reach a maximum segment length of 316m.
    - Full-duplex 62.5-micron MM fiber connections can reach a maximum segment length of 275m.
    - Full-duplex 50-micron MM fiber connections can reach a maximum segment length of 550m.

  As you can see, the 50-micron MM fiber can offer longer segment distances. The 62.5-micron MM fiber reaches the same maximum segment length of 275m regardless of the duplex.

- **1000BaseLX—**1000BaseLX transmits long-wavelength laser over fiber-optic cable. Either 50-micron or 62.5-micron (diameter) MM fiber can be used with this option. SM fiber can also be used with 1000BaseLX, which differentiates this standard from 1000BaseSX. The same MM fiber length restrictions apply based on the implementation of half- or full-duplex. The following lengths apply when SM fiber is used:
    - Half-duplex SM fiber connections can reach a maximum segment length of 316m.
    - Full-duplex SM fiber connections can reach a maximum segment length of 5000m.

  Using full-duplex SM fiber allows for a huge increase in distance. As you can imagine, this is also the more expensive option.

Table 3.7 compares Fast Ethernet 802.3z standards.

Table 3.7 Comparison of Gigabit Ethernet 802.3z Characteristics

Standard	Speed	Maximum Distance	Media Type	Connector Used
1000BaseCX	1000Mbps or 1Gbps	25m	Shielded copper wire	9-pin shielded connector
1000BaseSX	1000Mbps or 1Gbps	275m with half or full-duplex 62.5-micron MM fiber	MM fiber-optic	SC or ST
		316m with half-duplex 50-micron MM fiber		
		550m with full-duplex 50-micron MM fiber		
1000BaseLX	1000Mbps or 1Gbps	275m with half- or full-duplex 62.5-micron MM fiber	MM or SM fiber-optic	SC or ST

		316m with half-duplex 50-micron MM fiber or SM fiber		
		550m with full-duplex 50-micron MM fiber		
		5000m with full-duplex SM fiber		

10-Gigabit Ethernet (10GbE)

You guessed it: 1Gbps just wasn't a fast enough option. Actually, it is just the nature of technology to constantly strive for faster speeds. Yet another new standard was defined by IEEE and labeled 802.3ae. Earlier in this chapter you saw 10BASE-2, which has data transmission speeds of 10Mbps. 10-Gigabit Ethernet transmits data at 10,000Mbps. That is quite an upgrade! IEEE 802.3ae uses 62.5-micron MM, 50-micron MM, or SM fiber-optic cabling for connectivity and a baseband signaling mode.

NOTE

All of the ethernet standards, regardless of their speed, use the same 802.3 MAC and 802.2 LLC headers and trailers.

Long Reach Ethernet

Cisco Long Reach Ethernet (LRE) was developed to provide broadband service over existing telephone-grade or Category 1, 2, or 3 wiring. Speeds vary between 5–15Mbps and can reach a maximum segment length of up to 5000m. Cisco LRE may be a viable networking solution for a LAN or MAN that already has Category 1/2/3 cabling installed. A hotel could benefit from Cisco LRE to provide high-speed Internet or video conferencing solutions to their clientele.

NOTE

Broadband is a signaling method that supports various frequencies such as audio and video.

T3.7) Networking components as they map to OSI models

Major computer network components

Computer network requires the following devices (some of them are optional):-

- Network Interface Card (NIC)
- Hub
- Switches
- Cables and connectors
- Router

- Modem

1. Network Interface Card
Network adapter is a device that enables a computer to talk with other computer/network. Using unique **hardware addresses (MAC address)** encoded on the card chip, the data-link protocol employs these addresses to discover other systems on the network so that it can transfer data to the right destination.

There are **two types of network cards**: **wired and wireless**. The wired NIC uses cables and connectors as a medium to transfer data, whereas in the wireless card, the connection is made using antenna that employs radio wave technology. All modern laptop computers incorporated wireless NIC in addition to the wired adapter.

Network Card Speed
Network Interface card, one of the main computer network components, comes with different speeds, 10Mbps, 100Mbps, and 1000Mbps, so on. Recent standard **network cards built with Gigabit** (1000Mbps) connection speed. It also supports to connect slower speeds such as 10Mbps and 100Mbps. However, the speed of the card depends on your LAN speed.

For example, if you have a switch that supports up to 100Mbps, your NIC will also transfer a data with this same speed even though your computer NIC has still the capability to transfer data at 1000Mbps (1Gbps). In modern computers, network adapter is integrated with a computer motherboard. However if you want advanced and fast Ethernet card, you may buy and install on your computer using the **PCI slot** found on the motherboard (desktop) and **ExpressCard slots** on laptop .

2. Hub
Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer request information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.

Currently Hubs are becoming obsolete and replaced by more advanced communication devices such as **Switchs and Routers**.

3. Switch
Switch is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses **physical device addresses** in each incoming messages so that it can deliver the message to the right destination or port.

Like Hub, switch don't broadcast the received message to entire network, rather before sending it checks to which system or port should the message be sent. In other words switch connects the source and destination directly which increases the speed of the network. Both switch and hub have common features: Multiple RJ-45 ports, power supply and connection lights.

4. Cables and connectors
Cable is one way of transmission media which can transmit communication signals. The wired network typology uses special type of cable to connect computers on a network.

There are a number of solid transmission Media types, which are listed below. - **Twisted pair wire**

It is classified as Category 1, 2, 3, 4, 5, 5E, 6 and 7. Category 5E, 6 and 7 are high-speed cables that can transmit 1Gbps or more. -

Coaxial cable
Coaxial cable more resembles like TV installation cable. It is more expensive than twisted-pair cable but provide high data transmission speed.

Fiber-optic cable
It is a high-speed cable which transmits data using light beams through a glass bound fibers. Fiber-optic cable is high data transmission cable comparing to the other cable types. But the cost of fiber optics is very expensive which can only be purchased and installed on governmental level.

5. Router
When we talk about computer network components, the other device that used to **connect a LAN with an internet connection is called Router**. When you have **two distinct networks** (LANs) or want to share a single internet connection to multiple computers, we use a Router.

In most cases, recent routers also include a switch which in other words can be used as a switch. You don't need to buy both switch and router, particularly if you are installing small business and home networks.

There are two types of Router: **wired and wireless**. The choice depends on your physical office/home setting, **speed** and **cost**.

6. Modems
A modem enables you to connect your computer to the available internet connection over **the existing telephone line**. Like NIC, **Modem is not integrated with a computer motherboard**. It comes as separate part which can be installed on the PCI slots found on motherboard.

A modem is not necessary for LAN, but required for internet connection such as dial-up and DSL.

There are some types of modems, which differs in **speed and transmission rate**. Standard PC modem or Dial-up modems (56Kb data transmission speed), Cellular modem (used in a laptop that enables to connect while on the go), **cable modem (500 times faster than standard modem)** and DSL Modems are the most popular.

T3.8) TCP models and functions of different layers

Overview of the TCP/IP Networking Model

Transmission Control Protocol/Internet Protocol (TCP/IP). The first part: TCP is a main protocol that runs under Transport Layer 4 of TCP/IP Model; IP is another main protocol that runs under Network Layer 3 of TCP/IP Model, hence, called TCP/IP Network Model – they just picked its name based on these protocols. Both of them combined; refer to the whole suite or Networking Model that is used today for Network communication. *OSI is similar to TCP/IP and used globally as reference Model since it has 7 layers vs. 5 Layers used by TCP/IP Model. But remember, we configure IPv4 or IPv6 stack on the Network devices instead of OSI stack.*

The TCP/IP Networking Model both defines and references a large collection of protocols that allow components to communicate. To help people understand a networking model (such TCP/IP and OSI Models), each model broken down to something called *Layers*. Each layer includes protocols and standards that relate to that category of functions and TCP/IP has two models as shown below.

The original TCP/IP Network Model started with 4 Layers

4. Application

3. Transport

2. Internet

1. Link Layer

The second version of TCP/IP became 5 layers: changed the name of Internet Layer to Network layer and divided the link Layer to 2 layers

5. Application

4. Transport

3. Network

2. Data-Link

1. Physical

T3.9) Comparison between OSI model and TCP model

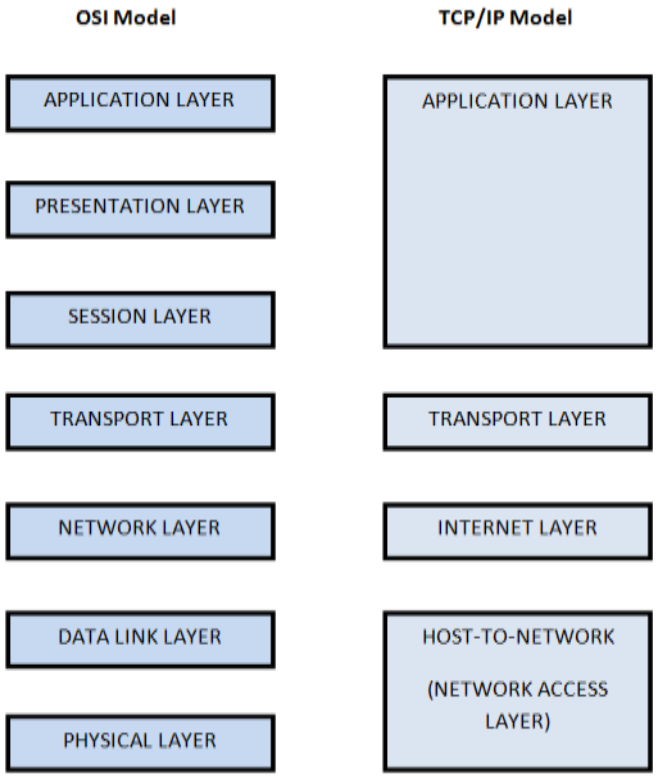
Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below.

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol /

	Internet Protocol)
1. OSI provides layer functioning and also defines functions of all the layers.	1. TCP/IP model is more based on protocols and protocols are not flexible with other layers.
2. In OSI model the transport layer guarantees the delivery of packets	2. In TCP/IP model the transport layer does not guarantees delivery of packets.
3. Follows horizontal approach	3. Follows vertical approach.
4. OSI model has a separate presentation layer	4. TCP/IP does not have a separate presentation layer
5. OSI is a general model.	5. TCP/IP model cannot be used in any other application.
6. Network layer of OSI model provide both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols in the model	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.	9. In TCP/IP it is not clearly separated its services, interfaces and protocols.
10. It has 7 layers	10. It has 4 layers

Diagrammatic Comparison between OSI Reference Model and TCP/IP Reference Model



TOPIC 4: NETWORK CONNECTIONS AND PROTOCOLS

T4.1) Transport protocols

Transport layer provides end-to-end or host-to-host communication services for applications within a layered architecture of network components and protocols. The transport layer provides services such as connection-oriented data stream support, reliability, flow control, and multiplexing.

The best-known transport protocol is the Transmission Control Protocol (TCP). It lent its name to the title of the entire Internet Protocol Suite, *TCP/IP*. It is used for connection-oriented transmissions, whereas the connectionless User Datagram Protocol (UDP) is used for simpler messaging transmissions. TCP is the more complex protocol, due to its stateful design incorporating reliable transmission and data stream services. Other prominent protocols in this group are the Datagram Congestion Control Protocol (DCCP) and the Stream Control Transmission Protocol (SCTP).

Transmission Control Protocol (TCP) is a core protocol of the Internet Protocol Suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as *TCP/IP*. TCP provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating over an IP network. TCP is the protocol that major Internet applications such as the World Wide Web, email, remote administration and file transfer rely on.

User Datagram Protocol (UDP) uses a simple connectionless transmission model with a minimum of protocol mechanism. It has no handshaking dialogues, and thus exposes any unreliability of the underlying network protocol to the user's program. There is no guarantee of delivery, ordering, or duplicate protection. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram.

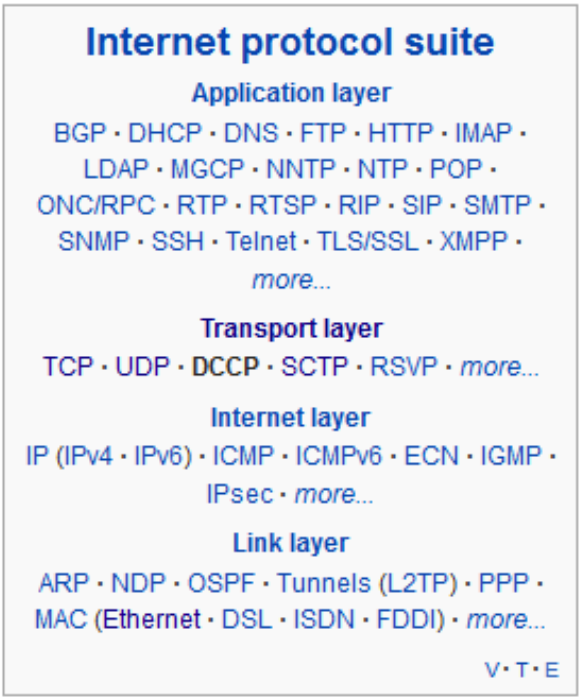
Stream Control Transmission Protocol (SCTP) is a transport-layer protocol, serving in a similar role to the popular protocols TCP and UDP. It provides some of the same service features of both: it is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP.

Datagram Congestion Control Protocol (DCCP) is a message-oriented transport layer protocol. DCCP provides a way to gain access to congestion control mechanisms without having to implement them at the application layer. It allows for flow-based semantics like in TCP, but does not provide reliable in-order delivery. Sequenced delivery within multiple streams as in the SCTP is not available in DCCP.

T4.2) Other protocols

- RIP

- BGP
- OSPF



Open Shortest Path First (**OSPF**) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008).

OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks. Intermediate System to Intermediate System (IS-IS), another link-state dynamic routing protocol, is more common in large service provider networks. The most widely used exterior gateway protocol is the Border Gateway Protocol (BGP), the principal routing protocol between autonomous systems on the Internet.

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. The protocol is often classified as a path vector protocol but is sometimes also classed as a distance-vector routing protocol. Makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and is involved in making core routing decisions.

Note

1. **Exterior gateway protocol (EGP)** is a routing protocol used to exchange routing information between autonomous systems. While as **Interior gateway protocol (IGP)** is a type of protocol used for exchanging routing information between gateways (commonly routers) *within* an autonomous system (for example, a system of corporate local area networks).

autonomous system (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the Internet.

Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination.

2. **Path vector protocol** is a computer network routing protocol which maintains the path information that gets updated dynamically. Updates which have looped through the network and returned to the same node are easily detected and discarded. It is different from the distance vector routing and link state routing. Each entry in the routing table contains the destination network, the next router and the path to reach the destination.

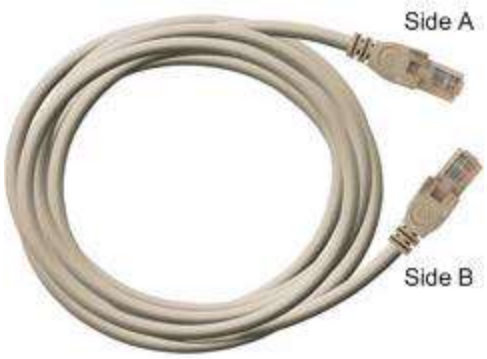
   Distance-vector routing protocol is one of the two major classes of intra domain routing protocols, A distance-vector routing protocol requires that a router inform its neighbors of topology changes periodically.
   Link-state routing protocols are one of the other main classes of routing protocols link-state protocol is performed by every *switching node* in the network (i.e., nodes that are prepared to forward packets; in the Internet, these are called routers). The basic concept of link-state routing is that every node constructs a *map* of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical *path* from it to every possible destination in the network. The collection of best paths will then form the node's routing table.

T4.3) Network connectivity

What are Straight and Crossover cable

Common Ethernet network cable are straight and crossover cable. This Ethernet network cable is made of 4 pair high performance cable that consists twisted pair conductors that used for data transmission. Both end of cable is called RJ45 connector.
The cable can be categorized as **Cat 5, Cat 5e, Cat 6 UTP cable**. Cat 5 UTP cable can support 10/100 Mbps Ethernet network, whereas Cat 5e and Cat 6 UTP cable can support Ethernet network running at 10/100/1000 Mbps. You might heard about Cat 3 UTP cable, it's not popular anymore since it can only support 10 Mbps Ethernet network.

Straight and crossover cable can be Cat3, Cat 5, Cat 5e or Cat 6 UTP cable, the only difference is each type will have different wire arrangement in the cable for serving different purposes.



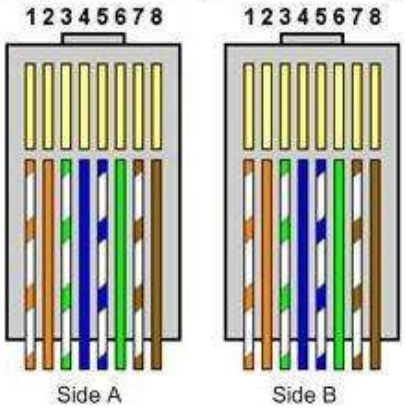
Straight Cable

You usually use straight cable to connect different type of devices. This type of cable will be used most of the time and can be used to:

1) Connect a computer to a switch/hub's normal port.
2) Connect a computer to a cable/DSL modem's LAN port.
3) Connect a router's WAN port to a cable/DSL modem's LAN port.
4) Connect a router's LAN port to a switch/hub's uplink port. (normally used for expanding network)
5) Connect 2 switches/hubs with one of the switch/hub using an uplink port and the other one using normal port.

If you need to check how straight cable looks like, it's easy. **Both side (side A and side B) of cable have wire arrangement with same color**. Check out different types of straight cable that are available in the market here.

Pin ID	Side A	Side B
1	Orange-white	Orange-white
2	Orange	Orange
3	Green-white	Green-white
4	Blue	Blue
5	Blue-white	Blue-white
6	Green	Green
7	Brown-white	Brown-white
8	Brown	Brown



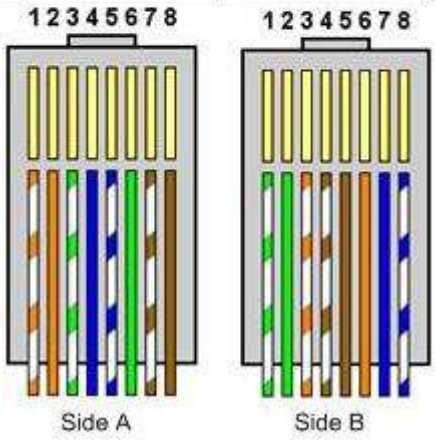
Crossover Cable

Sometimes you will use crossover cable, it's usually used to connect same type of devices. A crossover cable can be used to:

1) Connect 2 computers directly.
2) Connect a router's LAN port to a switch/hub's normal port. (normally used for expanding network)
3) Connect 2 switches/hubs by using normal port in both switches/hubs.

In you need to check how crossover cable looks like, **both side (side A and side B) of cable have wire arrangement with following different color** . Have a look on these crossover cables if you plan to buy one.

Pin ID	side A	side B
1	Orange-white	green-white
2	Orange	green
3	green-white	orange-white
4	blue	brown-white
5	blue-white	Brown
6	green	orange
7	brown-white	Blue
8	brown	blue-white

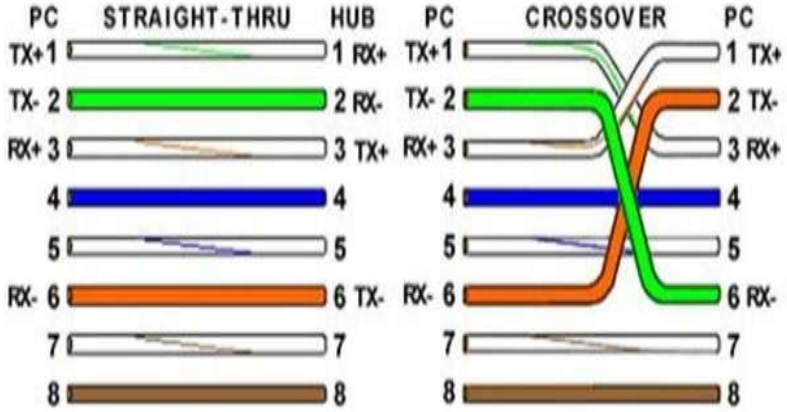


In case you need to make a crossover cable yourself! You can use this crimper to do it.

Lastly, if you still not sure which type of cable to be used sometimes, **try both cables and see which works**.

Note: If there is **auto MDI/MDI-X** feature support on the switch, hub, network card or other network devices, you don't have to use crossover cable in the situation which I mentioned above. This is because crossover function would be enabled automatically when it's needed.

Basic Theory:



TOPIC 5: LOCAL AREA NETWORK

T5.1) Meaning of local area network

A local area network (LAN) is a computer network within a small geographical area such as a home, school, computer laboratory, office building or group of buildings.

A LAN is composed of inter-connected workstations and personal computers which are each capable of accessing and sharing data and devices, such as printers, scanners and data storage devices, anywhere on the LAN. LANs are characterized by higher communication and data transfer rates and the lack of any need for leased communication lines.

T5.2,T5.3) LAN protocols and LAN transmission methods and Access methods

LAN Protocols

Protocols used in a LAN includes: Ethernet/IEEE 802.3, Token Ring/IEEE 802.5, and Fiber Distributed Data Interface (FDDI).

More on protocols

Network Protocol - Types of Network Protocols

Network Protocol is a set of rules that governs the communications between computers on a network.

Network Protocol & Types

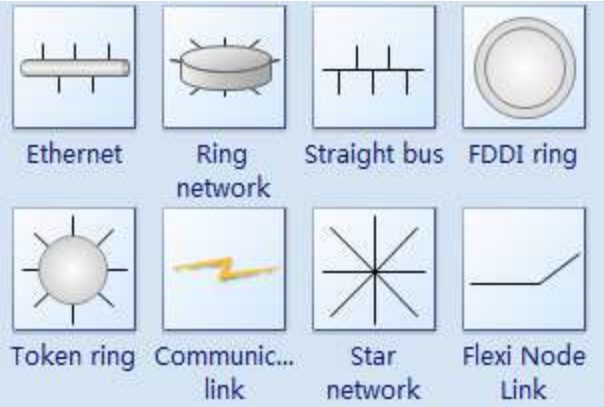
Rules of Network Protocol include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer.

Types of Network Protocols

The most common network protocols are:

1. Ethernet
2. Local Talk
3. Token Ring
4. FDDI
5. ATM

The followings are some commonly used network symbols to draw different kinds of network protocols.



Ethernet
The Ethernet protocol is by far the most widely used one. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other nodes have already transmitted 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. A collision occurs when this happens. Each computer then backs off and waits a random amount of time before attempting to retransmit. With this access method, it is normal to have collisions. However, the delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network.

The Ethernet protocol allows for linear bus, star, or tree topologies. Data can be transmitted over wireless access points, twisted pair, coaxial, or fiber optic cable at a speed of 10 Mbps up to 1000 Mbps.

Fast Ethernet
To allow for an increased speed of transmission, the Ethernet protocol has developed a new standard that supports 100 Mbps. This is commonly called Fast Ethernet. Fast Ethernet requires the application of different, more expensive network concentrators/hubs and network interface cards. In addition, category 5 twisted pair or fiber optic cable is necessary. Fast Ethernet is becoming common in schools that have been recently wired.

Local Talk
Local Talk is a network protocol that was developed by Apple Computer, Inc. for Macintosh computers. The method used by Local Talk is called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). It is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. Local Talk adapters and special twisted pair cable can be used to connect a series of computers through the serial port. The Macintosh operating system allows the establishment of a peer-to-peer network without the need for additional software. With the addition of the server version of AppleShare software, a client/server network can be established.

The Local Talk protocol allows for linear bus, star, or tree topologies using twisted pair cable. A primary disadvantage of Local Talk is low speed. Its speed of transmission is only 230 Kbps.

Token Ring
The Token Ring protocol was developed by IBM in the mid-1980s. The access method used involves token-passing. In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next. If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the data is captured by the receiving computer. The Token Ring protocol requires a star-wired ring using twisted pair or fiber optic cable. It can operate at transmission speeds of 4 Mbps or 16 Mbps. Due to the increasing popularity of Ethernet, the use of Token Ring in school environments has decreased.

FDDI
Fiber Distributed Data Interface (FDDI) is a network protocol that is used primarily to interconnect two or more local area networks, often over large distances. The access method used by FDDI involves token-passing. FDDI uses a dual ring physical topology. Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new complete ring. A major advantage of FDDI is high speed. It operates over fiber optic cable at 100 Mbps.

ATM
Asynchronous Transfer Mode (ATM) is a network protocol that transmits data at a speed of 155 Mbps and higher. ATM works by transmitting all data in small packets of a fixed size; whereas, other protocols transfer variable length packets. ATM supports a variety of media such as video, CD-quality audio, and imaging. ATM employs a star topology, which can work with fiber optic as well as twisted pair cable.

ATM is most often used to interconnect two or more local area networks. It is also frequently used by Internet Service Providers to utilize high-speed access to the Internet for their clients. As ATM technology becomes more cost-effective, it will provide another solution for constructing faster local area networks.

Gigabit Ethernet
The most latest development in the Ethernet standard is a protocol that has a transmission speed of 1 Gbps. Gigabit Ethernet is primarily used for backbones on a network at this time. In the future, it will probably also be used for workstation and server connections. It can be used with both fiber optic cabling and copper. The 1000BaseTX, the copper cable used for Gigabit Ethernet, became the formal standard in 1999.

Compare the Network Protocols

Protocol	Cable	Speed	Topology
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps	Linear Bus, Star, Tree

Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star
LocalTalk	Twisted Pair	.23 Mbps	Linear Bus or Star
Token Ring	Twisted Pair	4 Mbps - 16 Mbps	Star-Wired Ring
FDDI	Fiber	100 Mbps	Dual ring
ATM	Twisted Pair, Fiber	155-2488 Mbps	Linear Bus, Star, Tree

Media-Access Methods

LAN protocols typically use one of two methods to access the physical network medium: carrier sense multiple access collision detect (CSMA/CD) and token passing.

In the **CSMA/CD** media-access scheme, network devices contend for use of the physical network medium. CSMA/CD is therefore sometimes called contention access. Examples of LANs that use the CSMA/CD media-access scheme are Ethernet/IEEE 802.3 networks, including 100BaseT.

In the **token-passing** media-access scheme, network devices access the physical medium based on possession of a token. Examples of LANs that use the token-passing media-access scheme are Token Ring/IEEE 802.5 and FDDI.

LAN Transmission Methods

LAN data transmissions fall into three classifications: unicast, multicast, and broadcast. In each type of transmission, a single packet is sent to one or more nodes.

1. In a **unicast** transmission, a single packet is sent from the source to a destination on a network.
2. A **multicast** transmission consists of a single data packet that is copied and sent to a specific subset of nodes on the network.
3. A **broadcast** transmission consists of a single data packet that is copied and sent to all nodes on the network.

LAN Topologies

LAN topologies define the manner in which network devices are organized. Four common LAN topologies exist: bus, ring, star, and tree. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies, for example, are commonly organized physically as a star.

- A **bus topology** is a linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations.

- A **ring topology** is a LAN architecture that consists of a series of devices connected to one another by unidirectional transmission links to form a single closed loop. Both Token Ring/IEEE 802.5 and FDDI networks implement a ring topology.
- A **tree topology** is a LAN architecture that is identical to the bus topology, except that branches with multiple nodes are possible in this case.
- A **star topology** is a LAN architecture in which the endpoints on a network are connected to a common central hub, or switch, by dedicated links. Logical bus and ring topologies are often implemented physically in a star topology.

LAN Devices

Devices commonly used in LANs include repeaters, hubs, LAN extenders, bridges, LAN switches, and routers.

- A **repeater** is a physical layer device used to interconnect the media segments of an extended network. A repeater essentially enables a series of cable segments to be treated as a single cable. Repeaters receive signals from one network segment and amplify, retime, and retransmit those signals to another network segment. These actions prevent signal deterioration caused by long cable lengths and large numbers of connected devices. Repeaters are incapable of performing complex filtering and other traffic processing. In addition, all electrical signals, including electrical disturbances and other errors, are repeated and amplified. The total number of repeaters and network segments that can be connected is limited due to timing and other issues.
- A **hub** is a physical-layer device that connects multiple user stations, each via a dedicated cable. Electrical interconnections are established inside the hub. Hubs are used to create a physical star network while maintaining the logical bus or ring configuration of the LAN. In some respects, a hub functions as a multiport repeater.
- A **LAN extender** is a remote-access multilayer switch that connects to a host router. LAN extenders forward traffic from all the standard network-layer protocols (such as IP, IPX, and AppleTalk), and filter traffic based on the MAC address or network-layer protocol type. LAN extenders scale well because the host router filters out unwanted broadcasts and multicasts. LAN extenders, however, are not capable of segmenting traffic or creating security firewalls.
- **Bridges** analyze incoming frames, make forwarding decisions based on information contained in the frames, and forward the frames toward the destination. In some cases, such as source-route bridging, the entire path to the destination is contained in each frame. In other cases, such as transparent bridging, frames are forwarded one hop at a time toward the destination.
- **Switches** are data link layer devices that, like bridges, enable multiple physical LAN segments to be interconnected into a single larger network. Similar to bridges, switches forward and flood traffic based on MAC addresses. Because switching is performed in hardware instead of in software, however, it is significantly faster. Switches use either store-and-forward switching or cut-through switching when forwarding traffic. Many types of switches exist, including ATM switches, LAN switches, and various types of WAN switches.
- **Routers** perform two basic activities: determining optimal routing paths and transporting information groups (typically called packets) through an internetwork. In the context of the routing process, the latter of these is referred to as switching. Although switching is relatively straightforward, path determination can be very complex.

TOPIC 6: WIDE AREA NETWORK

T6.1) Meaning & Types of WAN

Wide Area Network, WAN is a collection of computers and network resources connected via a network over a geographic area. Wide-Area Networks are commonly connected either through the Internet or special arrangements made with phone companies or other service providers.

Wide Area Networks can be seen as connection pipes that interconnect Local Area Networks. Usually WANs in contrast to LANs are not owned by the public; they are owned by service providers and their functionality-infrastructure is leased in order for LANs to be able to extend their expandability and make use of distant-remote services.

A number of different WAN connection types exist today. Choosing the right WAN connection type is up to you, but the information in this article will make your decision process much easier.

WAN Connection Types

Leased Line:
This is considered to be a dedicated point-to-point connection type where a permanent communication path exists between a Customer Premise Equipment (CPE) on one site and a CPE at the remote site communicating through a Data Communicating Equipment (DCE) within the providers' site. Synchronous serial lines are used for this connection and the most frequent protocols observed in these lines are **HDLC** (High-Level Data Link Control) and **PPP** (Point-to-Point Protocol). When cost in not an issue, you should use this type of connection.

Circuit Switching:
The concept of this WAN connection is based on the typical telephone switching network. A connection needs to be established prior to be able to transfer data. This type of connection is used for low bandwidth data transfers where charging is calculated based on actual connection time. **ISDN** (Integrated Services Digital Network) protocol is basically used on this connection type.

Packet Switching:
Always-on connection, where available bandwidth is shared between several users. No time-based charging. Charging is based on committed traffic rate. This type of connection is more appropriate for bursty data transfers. Special configuration is needed to support strict QoS requirements. **Frame Relay** is a packet switching connection type.

T6.2) WAN protocols

1. High Level Data Link Control (HDLC)

HDLC is a data-link layer protocol and because of the fact that there is no standard way of identifying the type of network protocol carried within the HDLC encapsulation, each vendor uses its own proprietary HDLC protocol.

Cisco uses its own HDLC implementation; therefore Cisco routers are not able to communicate with equipment running other vendors' HDLC implementation. Nevertheless, HDLC is the default encapsulation used by Cisco routers on synchronous serial links (leased line connections). When communicating with a non-Cisco device, synchronous Point-to-Point protocol (PPP) is the more feasible option to use.

On Cisco routers use the **show interface** command on serial interfaces to see the configured encapsulation method.

```
ROUTER#show interfaces serial 1/0
Serial1/0 is up, line protocol is up
  Hardware is QUICC Serial
  Internet address is 195.18.159.41/30
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec,
     reliability 255/255, txload 25/255, rxload 32/255
  Encapsulation HDLC, loopback not set
                .
                .
                .
```

To see the physical connection type used, issue the **show controllers** command:

```
ROUTER#show controllers serial 1/0
Interface Serial1/0
Hardware is Quicc 68360
DTE V.35 TX and RX clocks detected.
idb at 0x62132190, driver data structure at 0x62139C04
WIC interrupt reg = F
                .
                .
                .
```

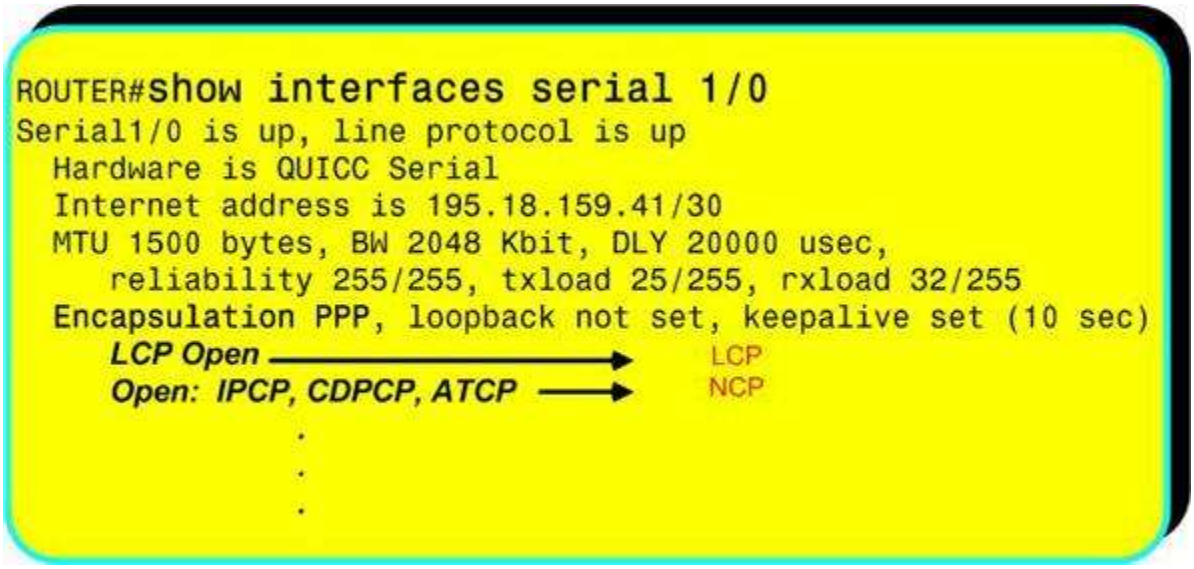
2. Point-to-Point Protocol (PPP)

PPP data link protocol is used on serial connections between dissimilar routers, for example a Cisco router and a non-Cisco router. PPP is designed to allow the simultaneous use of multiple network layer protocols and also supports two types of hostname authentications **CHAP** (Challenge Handshake Authentication Protocol) and **PAP** (Password Authentication Protocol).

PPP uses the services of the HDLC protocol for encapsulating datagrams over serial links. Moreover, it uses two additional control protocols to support its operation:

- **Link Control Protocol** (LCP) provides the means for configuring, establishing, maintaining and terminating the PPP connection. Among other things, LCP handles PPP authentication methods, error detection, compression techniques, support for multilink etc.
- **Network Control Protocol** (NCP) provides the means for encapsulating multiple network layer protocols across the PPP data link.

Use the show interface command to verify PPPs operation.



Notice from the output of the **show interface serial 1/0** command the PPP encapsulation type. Also, notice that LCP is Open meaning is being running and maintaining the PPP connection. Finally, the last line is associated with the NCP. It shows that IP, CDP and AppleTalk are open.

3. Frame Relay

Frame Relay is a packet-switched technology. No connection setup phase takes place prior to data transmission. Moreover, the network infrastructure is shared among different users in contrast to leased line connections where the whole amount of bandwidth is always dedicated to the corresponding user. The main characteristics of Frame Relay technology are presented below:

- Contract terms are signed between the customer and service provider. Mainly the contract consists of a so-called Committed Information Rate (CIR) which is the amount of bandwidth the service provider has contractually guaranteed to provide to the customer at all times. The later may use more bandwidth if the network infrastructure is not congested, however this excess traffic is not guaranteed at all.
- Big money saved for both customer and service provider. The customer makes use of this packet switched technology at much lower price compared to the leased line option. From the other hand, the service provider does not have to install and maintain a huge number of leased line connections which always consume the whole bandwidth tube even if they are not really used.
- Frame Relay on Cisco routers is configured on serial interfaces. Unlike HDLC or PPP, configuring Frame Relay is achieved by specifying the appropriate encapsulation type among Cisco and IETF (Internet Engineering Task Force). The default encapsulation used for Frame Relay on Cisco routers is you guess correctly Cisco of course.
- Frame Relay uses what is called virtual circuits to route data across the service providers infrastructure towards the other communicating end. Service providers mainly use Permanent Virtual Circuits (PVCs) within their network to route packets forth and back. The PVCs once created remain operating as long as the customer pays the bill.
- PVCs are identified by the use of Data Link Connection Identifiers (DLCIs) which are typically assigned by the provider to end devices. These identifiers have only local significance in the sense that they are used to identify a specific data link and not the entire virtual circuit end-to-end. According to the DLCIs values assigned to the customers, the service provider is able to route packets appropriately.

4. Integrated Services Digital Network (ISDN)

ISDN is a Circuit Switched technology that is designed to run over existing telephone networks. It is a fully digital technology end-to-end. It consists of a number of protocols for transferring data, voice and video over the traditional telephone system. ISDN has the following major characteristics:

- Faster data transmission compared with analog modem connection.
- Perfect candidate for establishing a backup connection to a leased line connection.
- Comes with two flavors:
    - ISDN Basic Rate Interface (BRI) service also known as 2B+D consists of two data channels (B channels) that operate at 64 Kbps each and a single signaling channel (D channel) that operates at 16kbps.
    - ISDN Primary Rate Interface (PRI) also known as 23B+D in North America and Japan and 30B+D in Europe. In the case of 23B+D, it consists of 23 data channels operating at 64kbps each and one signaling channel operating at 64kbps as well.
- To be able to connect a Cisco router to the ISDN network you can either use a router with a built-in NT1 (U) interface (ISDNs two wire connection that runs into the home or office) or use an ISDN terminal adapter (TA) along with your routers serial interface

TOPIC 7: ETHERNET TECHNOLOGY

T7.1) Ethernet technology

Ethernet is a technology originally developed by Xerox, which acts as a sort of traffic cop for movement of data on a LAN (local area network) which consists of numerous computers (called Nodes) on the network, all of which can send or receive data. If two people try to send data at the same time on their computers the data could "crash" into each other causing havoc, so the Ethernet device won't let someone send data if someone else is already doing so.

Ethernet is a family of frame-based computer networking technologies for local area networks (LANs). The name comes from the physical concept of the ether. It defines a number of wiring and signaling standards for the physical layer, through means of network access at the Media Access Control (MAC)/Data Link Layer, and a common addressing format.

T7.2) Ethernet standards

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.

Ethernet, 802.3 is defined under a number of IEEE standards, each reflecting a different flavour of Ethernet. One of the successes of Ethernet has been the way in which it has been updated so that it can keep pace with improving technology and the growing needs of the users.

As a result of this the IEEE standards committee for Ethernet has introduced new standards to define higher performance variants. Each of the Ethernet IEEE 802.3 standards is given a different reference so that it can be uniquely identified.

In addition to this the different IEEE 802.3 standards may be known by other references that reflect the different levels of performance. These are also defined below.

There is a convention for describing the different forms of Ethernet. For example 10Base-T and 100Base-T are widely seen in the technical articles and literature. The designator consists of a three parts:

- The first number (typically one of 10, 100, or 1000) indicates the transmission speed in megabits per second.
- The second term indicates transmission type: BASE = baseband; BROAD = broadband.
- The last number indicates segment length. A 5 means a 500-meter (500-m) segment length from original Thicknet. In the more recent versions of the IEEE 802.3 standard, letters replace numbers. For example, in 10BASE-T, the T means unshielded twisted-pair cables. Further numbers indicate the number of twisted pairs available. For example in 100BASE-T4, the T4 indicates four twisted pairs.

The Ethernet IEEE 802.3 standards are continually being updated to ensure that the generic standard keeps pace with constant advance of technology and the growing needs of the users. As a result, IEEE 802.3, Ethernet is still at the forefront of network communications technology, and it appears it will retain this position of dominance for many years to come. In addition to the different IEEE 802.3 standards, the terminology used to define the different flavors is also widely used for defining which Ethernet variant is used.

IEEE 802.3 standards

The IEEE 802.3 standard references all include the IEEE 802.3 nomenclature as standard. Different releases and variants of the standard are then designated by different designated letters after the 802.3 reference, i.e. IEEE 802.3*. These are defined in the table below.

Standard Supplement	Year	Description
802.3a	1985	10Base-2 (thin Ethernet)
802.3c	1986	10 Mb/s repeater specifications (clause 9)
802.3d	1987	FOIRL (fiber link)
802.3i	1990	10Base-T (twisted pair)
802.3j	1993	10Base-F (fiber optic)
802.3u	1995	100Base-T (Fast Ethernet and auto-negotiation)
802.3x	1997	Full duplex
802.3z	1998	1000Base-X (Gigabit Ethernet)
802.3ab	1999	1000Base-T (Gigabit Ethernet over twisted pair)
802.3ac	1998	VLAN tag (frame size extension to 1522 bytes)
802.3ad	2000	Parallel links (link aggregation)
802.3ae	2002	10-Gigabit Ethernet
802.3as	2005	Frame expansion
802.3at	2005	Power over Ethernet Plus

Ethernet standards supplements and releases

New technologies are being added to the list of IEEE 802.3 standards to keep pace with technology.

TOPIC 8: NETWORK TROUBLE SHOOTING

T8.1) Meaning and importance of network trouble shooting

Network troubleshooting is the collective measures and processes used to identify, diagnose and resolve problems and issues within a computer network.

It is a systematic process that aims to resolve problems and restore normal network operations within the network.

Some of the processes within network troubleshooting include but are not limited to:

- Finding and resolving problems and establishing Internet/network connection of a computer/device/node
- Configuring a router, switch or any network management device
- Installing cables or Wi-Fi devices
- Updating firmware devices on router switch
- Removing viruses
- Adding, configuring and reinstalling a network printer

Key Benefits/importance of Network Monitoring

1. Reliability: Network monitoring keeps track of mission-critical appliances and software, and notifies your network administrator before issues become user-impacting problems. For example, network monitoring can let you know if a server fails, if a service stops responding or if you are in danger of running out of disk space. This ensures a proactive approach to dealing with issues, as opposed to waiting for your end users to call with a problem.

2. Stay in the know: Network monitoring systems will alert the IT administrator of performance issues or failure events by sending a variety of alerts to computers, pagers or mobile devices. This allows your IT administrator to be aware of issues regardless of where they are. Animate Inc. and LexCloud.ca monitors your respective systems 24/7 so that your firm has peace of mind after hours.

3. Capacity: Having a thorough understanding of how your devices are being used allows you to proactively identify areas that require additional disk space and roll out extra capacity in a controlled manner.

4. Troubleshooting: With network monitoring you can quickly identify the device that is causing the problem, thereby limiting your downtime and the time wasted trying to diagnose the issue. Rather than waiting for an end user to report a problem and then troubleshooting, network monitoring allows the support team to detect, diagnose and fix a problem before users are aware of it.

5. Track trends: Problems that occur intermittently or at certain peak times may be hard to pin point in the moment, but ongoing network monitoring reports allow you to understand key trends in the performance and general health of your network.

6. Plan for upgrades and changes: If a device is constantly running near its limit, this may be the time to make a change. Network monitoring applications allow you to track this type of data and plan ahead to make appropriate changes with ease.

7. Show others what is happening: Reports and statistics on network health and activity are great tools for proving adherence to a service level agreement or demonstrating why a specific device needs fixing or replacing.

8. Know when to apply your disaster recovery solutions: Without network monitoring, major problems may go undetected. With the extra notice afforded by proper monitoring, you can implement your disaster recovery protocols in time to prevent downtime and/or system failures. Examples of this include uninterrupted power supply batteries during an outage, backup completion status and the ability to predict hard drive failure.

9. Ensure security systems are operating properly: Without network monitoring, there is no way to ensure that expensive and mission critical security systems are performing their functions. One example you may not be familiar with is your firewall, which protects your data and allows for secure internet connectivity. Animate Inc. and LexCloud.ca frequently identify and fix problems with client firewalls before anyone at the firm notices these problems.

10. Save money: Reduce downtime and investigation time, as fewer hours worked means less money spent when problems occur and greater productivity across your organization.

11. Increase profits: Avoiding financial losses caused by undetected system failures is the ultimate result of being able to proactively point out and deal with network issues. All of your mission-critical services will run smoothly more of the time with a monitoring service, which gives you more time to run your firm.

T8.2) Methods of network trouble shooting

Connectivity testing with Ping, Telnet, Tracert and PathPing:
All of the following command line tools are accessed from the command prompt. You can open a command prompt window by selecting Start | All Programs | Accessories | Command Prompt.

You can also open the command prompt window by selecting Start | Run - and then entering CMD.EXE into the dialog box and pressing the Enter key or the OK button.

Each tool in this KB is given only a very basic overview and usage description. We would suggest that you research each of these in more detail to learn about advanced usage.

PING :
The ping command is a very simple connectivity testing tool. Ping verifies connectivity by

sending Internet Control Message Protocol (ICMP) echo packets to a host and listening for an echo reply.

The ping command waits for each packet sent and prints the number of packets transmitted and received. Each received packet is validated against the sent packet. The default setting will send four echo packets containing 64 bytes of data. You can use the ping utility to test both the host name and IP address of the host for DNS resolution. A successful IP ping and failed host name ping could indicate name resolution issues.

Usage:

In a command prompt window, enter Ping followed by the Fully Qualified Domain Name (FQDN) or IP address of the server you want to test. You may wish to use the –t command line switch to send continuous echo requests to a host.

Ping 123.123.123.123

Common usage examples might be to test for a server to be restarted and start responding again. You may wish to use the –t command line switch to send continuous echo requests:

Ping 123.123.123.123 –t

Another example may be to test what IP address is returned by a specific record or service lookup:

Ping mail.domain_name.com
Ping www.domain_name.com

TELNET:
Telnet comes from the combination of the words telephone and network. It was originally designed to allow for command line remote management over slower connection types. RFC 854 states: " The purpose of the TELNET Protocol is to provide a fairly general, bi-directional, eight-bit byte orientated communications facility. "

It is a TCP based protocol that can also be used to test a variety of services for connectivity. You can use it to test for SMTP, SQL or Remote Desktop connectivity. This is a good test to use for service or port blocks resulting from a firewall configuration.

Usage:

In a command prompt, enter TELNET, followed by the Fully Qualified Domain Name (FQDN) or IP address of the server you want to connect to - and then the port that the service uses.

TELNET 123.123.123.123 5678

The following is a list of common protocols and ports of interest:

FTP	21
SMTP	25
SQL	1433
RDP	3389

The response of a successful connection will be different for each service, but a failed connection will always respond with a variation of the following message: "Could not open connection to the host, on port n: Connect failed"

When testing your mail connection with Telnet, you will want to reference the mail record for the domain:

TELNET mail.yourdomain.com 25

TRACERT:
Tracert is the Windows implementation of the trace route tool that originated on UNIX and Cisco systems. Tracert is a Windows command-line tool that displays the path a packet takes to reach a destination from the machine that it is executed on. It does this by sending Internet Control Message Protocol (ICMP) echo request messages to the destination. It does this by incrementally increasing the Time To Live (TTL) values to find the path taken to the destination address. The path is displayed as a list in the order of which it heard back from each node that it passed through on its way to the destination.

When you run tracert, the top line shows the destination of the trace. It also lets us know that it stops if it reaches a maximum of 30 hops. Next you will see each hop it takes to reach the destination. The number of hops will go in order numerically from 1 to 30 depending on the path to the destination. Following this tracert will normally include at least 4 pieces of information for each hop; the number of the hop, the Round Trip Time (RTT is displayed in milliseconds or ms) it takes to get from the interface of the current hop and then back again to your machine, the IP address of the interface for that hop and the hostname corresponding to the IP address of the hop. The default is to send out 3 packets to each hop. This is done in case a packet is lost and allows you to get an idea of whether or not there is a variance in the time for a specific hop.

A high number on the first external hop from your machine is a good indication of possible Local Area Network (LAN) issues.

An asterisk (*) indicates an echo request that was lost. These can be the result of security implementations of firewalls or Access Control List (ACL's). Additionally, routers may be configured not to respond to this type of traffic. You may see a row of three asterisks with no IP address or hostname. The trace may then continue responding normally again and display the destination results.

Usage:

In a command prompt window, enter TRACERT followed by the Fully Qualified Domain Name (FQDN) or IP address of the server you want to test. You may wish to use the –d command line switch to prevent Tracert from resolving the name of the nodes from the IP address in the trace route.

TRACERT 123.123.123.123

You can see the output results in the following example:

Tracing route to 123.123.123.123 over a maximum of 30 hops:

1	<1 ms	<1 ms	<1 ms	111.111.111.111
2	<1 ms	<1 ms	<1 ms	222.222.222.222
3	1 ms	1 ms	1 ms	111.222.111.222
4	1 ms	1 ms	12 ms	222.111.222.111
5	*	*	*	Request timed out.
6	14 ms	13 ms	13 ms	123.123.123.123

Trace complete.

Additionally, you can use external tools such as www.traceroute.org or other ‘looking glass’ type sites to verify traces from different geographic locations throughout the world. You may want to select multiple sites to test connectivity to your server.

PATHPING:

PathPing is a utility that combines many of the features of Ping and Tracert into one tool. You can use it to verify connectivity to a host as well as see if you are taking an optimal path to a remote host or suffering from a bottleneck somewhere in the connection route. The final output provides statistics on the latency (packet loss) by sending multiple echo requests over a period of time to each node between the local and remote host.

Initially, PathPing will produce results are similar to Tracert; you will see the hop number followed by the IP address or node name. PathPing will then compute the statistics (the time this takes depends on the number of hops) for each node in the connection route. After the computation is complete, the window will display the following information for each node: Hop number, Round Trip Time (RTT), percent of packets Lost and Sent for Source to Here, the Address of the node at that hop and the percent of packets Lost and Sent from This Node/Link to the next node. You can see the output results in the following example:

	Source to Here		This Node/Link	
Hop	RTT	Lost/Sent = Pct	Lost/Sent = Pct	Address (Node)
0				111.111.111.111/
			0/100 = 0%	|
1	30ms	0/100 = 0%	0/100 = 0%	222.222.222.222/
			0/100 = 0%	|
2	30ms	0/100 = 0%	0/100 = 0%	111.222.111.222/

```
                                  33/100 = 33%      |
3       30ms   0/100 = 0%          0/100 =  0%       222.111.222.111/
                                  0/100 =  0%       |
0       30ms   0/100 = 0%          0/100 =  0%       123.123.123.123
```

Trace complete.

The “Source to Here” – is the first set of statistic after the hop number is equivalent to if you pinged the node directly.

The “This Node/Link” is the set of statistic before the pipe and is the column you want to pay the most attention to. This will show you the statistics for the links between the nodes.

In the above example, the link between 111.222.111.222 and 222.111.222.111 is dropping 33 percent of the packets. The router at hop 3 is dropping packets addressed to it, but this loss does not affect their ability to forward traffic.

A 0/100 = 0% means that out of 100 packets, none were lost. A low single digit loss 1% or 2% is common, but anything higher is an indication of

Usage:

In a command prompt window, enter PathPing followed by the Fully Qualified Domain Name (FQDN) or IP address of the server you want to test. You may wish to use the –n command line switch to prevent PathPing from resolving name from the IP address of the nodes in the connection route.

PATHPING –n 123.123.123.123

PathPing offers slightly more accurate output over Tracert because it provides averages based on multiple echo requests. One disadvantage to PathPing is that it can take longer to return results.

Final note:

All of these Windows utilities are based on ICMP echo request over TCP/IP - otherwise known as ping packets. Many firewalls block ICMP traffic - so you may not get the response although the site is up and responsive. Access rules can cause false negatives with the reporting of from these network tools.

TOPIC 9: NET WORK SECURITY

T9.1) Network security

Network security consists of the policies adopted to prevent and monitor authorized access, misuse, modification, or denial of a computer network and network-accessible resources.

Network security involves the authorization of access to data in a network, which is controlled by the network administrator.

Importance Of Network Security For Business Organization:

- **To Protect Company's Assets**- This can be considered as the primary goal of securing the computers and computer networks. The assets mean the information that is stored in the computer networks, which are as crucial and valuable as the tangible assets of the company. The computer and network security is concerned with the integrity, protection and safe access of the confidential information. It also involves the accessibility of information in a meaningful manner.

- **To Comply with Regulatory Requirements and Ethical Responsibilities-** It is the responsibility of every organization to develop procedures and policies addressing the security requirements of every organization. These policies work for the safety and security of any organization and are compulsory for any organization working on computers. Protection of company's assets would mean that it is protected from liability addressing to the ethical responsibilities of an organization.

- **For Competitive Advantage-** Developing an effective security system for networks will give the organization a competitive edge. In the arena of Internet financial services and e-commerce, network security assumes prime importance. The customers would avail the services of internet banking only if the networks are secured.

Data, Vulnerabilities, and Countermeasures

Although viruses, worms, and hackers monopolize the headlines about information security, risk management is the most important aspect of security architecture for administrators. A less exciting and glamorous area, risk management is based on specific principles and concepts that are related to asset protection and security management.

An *asset* is anything of value to an organization. By knowing which assets you are trying to protect, as well as their value, location, and exposure, you can more effectively determine the time, effort, and money to spend in securing those assets.

A *vulnerability* is a weakness in a system or its design that could be exploited by a threat. Vulnerabilities are sometimes found in the protocols themselves, as in the case of some security weaknesses in TCP/IP. Often, the vulnerabilities are in the operating systems and applications.

Written security policies might also be a source of vulnerabilities. This is the case when written policies are too lax or are not thorough enough in providing a specific approach or line of conduct to network administrators and users.

A *threat* is any potential danger to assets. A threat is realized when someone or something identifies a specific vulnerability and exploits it, creating exposure. If the vulnerability exists theoretically but has not yet been exploited, the threat is considered latent. The entity that takes advantage of the vulnerability is known as the threat agent or threat vector.

A *risk* is the likelihood that a particular threat using a specific attack will exploit a particular vulnerability of a system that results in an undesirable consequence. Although the roof of the data center might be vulnerable to being penetrated by a falling meteor, for example, the risk is minimal because the likelihood of that threat being realized is negligible.

NOTE

If you have a vulnerability but there is no threat toward that vulnerability, technically you have no risk.

An *exploit* happens when computer code is developed to take advantage of a vulnerability. For example, suppose that a vulnerability exists in a piece of software, but nobody knows about this vulnerability. Although the vulnerability exists theoretically, there is no exploit yet developed for it. Because there is no exploit, there really is no problem yet.

A *countermeasure* is a safeguard that mitigates a potential risk. A countermeasure mitigates risk either by eliminating or reducing the vulnerability or by reducing the likelihood that a threat agent will be able to exploit the risk.

T9.2) Security techniques

Different types of Network Security

1. Encryption

Wi-Fi Protected Access (WPA)

WPA encrypts information, and checks to make sure that the network security key has not been modified.

WPA also authenticates users to help ensure that only authorized people can access the network.

There are two types of WPA authentication: **WPA** and **WPA2**.
WPA is designed to work with all wireless network adapters, but it might not work with older routers or access points.
WPA2 is more secure than WPA, but it will not work with some older network adapters.
WPA is designed to be used with an 802.1X authentication server, which distributes different

keys to each user. This is referred to as WPA-Enterprise or WPA2-Enterprise.
It can also be used in a pre-shared key (**PSK**) mode, where every user is given the same password. This is referred to as **WPA-Personal** or **WPA2-Personal**.

Wired Equivalent Privacy (WEP)

WEP is an older network security method that is still available to support older devices, but it is no longer recommended.
When you enable **WEP**, you set up a network security key. This key encrypts the information that one computer sends to another computer across your network. However, WEP security is relatively easy to crack.

802.1X authentication

802.1X authentication can help enhance security for 802.11 wireless networks and wired Ethernet networks. **802.1X** uses an authentication server to validate users and provide network access. On wireless networks, **802.1X** can work with WEP or WPA keys. This type of authentication is typically used when connecting to a workplace network.

2. MAC Address

A Media Access Control address is a unique identifier assigned to network interfaces for communications on the physical network segment. Can be described as Ethernet hardware address (EHA), hardware address or physical address. It is assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, the card's read-only memory, or some other firmware mechanism.

The advantage to MAC filtering is that there is no attachment cost to devices that connect to the network. The policy is set on a router or switch, and the equipment attached either is permitted or it is not. The person attaching the equipment has nothing to do.

The disadvantage to MAC filtering is that it is easy to spoof due to the broadcast nature of LAN and WLAN, an advisory can sit on the wire and just listen to traffic to and from permitted MAC addresses. Then, the advisory can change his MAC address to a permitted one, and in most cases obtain access to the network.

3. Authentication

One-factor authentication – this is “something a user knows.” The most recognized type of one-factor authentication method is the password.

Two-factor authentication – in addition to the first factor, the second factor is “something a user has.” Examples of something a user has are a device that generates a pre-determined code, a

signed digital certificate or even a bio-metric such as a fingerprint.

Three-factor authentication – in addition to the previous two factors, the third factor is "something a user is." Examples of a third factor are all bio-metric such as the user's voice, hand configuration, a fingerprint, a retina scan or similar.

The advantage of using a 3 factor authentication is that it's made reassuringly sure that the person who is authenticating is the person who is authenticating through multiple layers of security. The disadvantage is that there is a possibility that the person trying to authenticate loses first or the second authentication, the process can also take time.

4. Firewall
Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. It may be hardware or software.

The advantage of a firewall is that the user can monitor incoming and outgoing security alerts and the firewall company will record and track down an intrusion attempt depending on the severity. Some firewalls can detect viruses, worms, Trojan horses, or data collectors.

The disadvantage of firewalls is that they offer weak defense from viruses so antiviral software and an IDS (intrusion detection system) which protects against Trojans and port scans should also complement your firewall in the layering defense. A firewall protection is limited once you have an allowable connection open. This is where another program should be in place to catch Trojan horse viruses trying to enter your computer as unassuming normal traffic.

5. Physical Security
Something that is physically in the way of someone breaking into a system. E.g. a door, or walls, or security guards.

T9.3) Security threats and other network vulnerabilities

Common Network Security Threats

Three common factors emerges when dealing with network security, these are vulnerability, threat, and attack.

Vulnerabilities
An experienced hacker knows that every network or device has a certain degree of vulnerability or weakness, and they take advantages of each security weakness or loophole to exploit the

network. A A Computer network hackers work round the clock in search of unsecured networks or devices to exploit. These includes routers, switches, desktops, servers, and even security devices.

They use variety of tools, programs and scripts to accomplish these threats. The primary network vulnerabilities or weaknesses are:

Technological, Configuration and Security policy weaknesses,

Technological weaknesses: as mentioned earlier, every computer network and device has an inherent security weakness. These include TCP/IP protocol (HTTP, FTP, SMTP, SNMP) on which the Internet was designed, operating system (Unix, Linux, Mac OS, Windows OS, and network equipment weaknesses (Routers, Firewalls, Switches etc.)

Configuration weaknesses: incorrect configuration or application of security software or firewall devices due to laxity can help to compromise a network. These includes unsecured user accounts information or passwords, system accounts information or passwords, misconfigured internet services, unsecured default settings within products, misconfigured network equipments – ACLs or routing protocols. All of the above enable the creation of security holes that every experienced hacker is looking out for.

Security policy weaknesses: Every organization must have a security policy that governs and maintains how the network or company information should be used. Security risks to the network exist if users do not follow the security policy. Security weaknesses emerge when there is no clear cut or written security policy document. A security policy meets these goals:

i. To Inform users, staff, and managers of their obligatory requirements for protecting technology and information assets
ii. Specifies the mechanisms through which these requirements can be met
iii. Provides a baseline from which to acquire, configure, and audit computer systems and networks for compliance with the policy

Types of Network Attacks

There are four primary types of attacks, they are:

i. Reconnaissance
ii. Access
iii. Denial of Service
iv. Worms, Viruses, and Trojan Horses

1. Reconnaissance

Reconnaissance attack is a kind of information gathering on network system and services. This enables the attacker to discover vulnerabilities or weaknesses on the network. It could be likened to a thief surveying through a car parking lot for vulnerable – unlocked - cars to break into and steal.

Reconnaissance attacks can consist of:

a. Internet information lookup
b. Ping sweeps
c. Port scans
d. Packet sniffers

Network intruders can use Internet tools, such as the **nslookup** and **whois** utilities, to easily determine the IP address space assigned to a given organization or network. After finding out the IP address, the intruder can then ping the publicly available IP addresses to identify the addresses that are active.

There are automate ping sweep tool which an attacker can use, such as **fping** or **gping**, these tools methodically pings all network addresses in a given range or subnet. This is like to going through a section of a telephone directory and calling each number to know who answers.

When the attacker discovers active IP addresses, the intruder or attacker uses a port scanner (**Nmap** or **Superscan -**software designed to search a network host for open ports) to determine which network services or ports are active on the active IP addresses. The port scanner queries the ports to determine the application or operating system (OS) type and version, running on the targeted host. Based on the information gathered, the intruder can determine if a possible vulnerability or weakness that can be exploited exists.

Packet sniffing or Network snooping are common terms for eavesdropping. The information gathered by eavesdropping can be used to pose other attacks to the network.

A common method for eavesdropping on communications on a network is to capture TCP/IP or other protocol packets and decode the contents using a protocol analyser or similar tools such as wireshark. After packets are captured, they can be examined for vulnerable information.

An intruder to eavesdrop on a management protocol called SNMP can use protocol analyser or wireshark.

SNMP provides a means for network devices to collect information about their status and to send it to an administrator. An intruder could eavesdrop on SNMP versin1 queries and gather valuable information on network devices configuration.

2. Network Access Attacks

Technology is forever evolving, so is hacking! It might come as a surprise to many that, as one wakes up in the morning and prepares for work, gets to the office and spends nine to twelve hour working; the same way a professional hacker spends all day modifying hacking techniques and looking for networks to exploit!

Firstly, for an attacker to gain access to a system network, the intruder has to find out the vulnerabilities or weaknesses in the network authentication, FTP and web services. Finding and

exploiting these vulnerabilities will enable the attacker to gain access to web account and other confidential or sensitive information.

Types of access attacks

1. Password attack
2. Trust Exploitation
3. Port Redirection
4. Man-in-the middle attack

Password Attacks

A Network attacker uses packet sniffer tools to obtain user accounts and passwords information. Normally we log in and out of a system using authentication passwords to shared resources in a router or server, an attacker also repeatedly attempts to log in to a shared resource or to gain unauthorised access to an organisation's network; this can also be referred to as dictionary or brute force attacks. To carry out this type of attacks, the intruder can use tools like the **L0phtCrackor Cain.**

These software or programs repeatedly attempt to log in as a user using words derived from a dictionary. Most dictionary attacks often succeed because network users often choose simple and short passwords, single words that are easy to predict.

Another password attack method uses what is called rainbow tables. A rainbow table is precompiled series of passwords, which is constructed by building chains of possible plain text passwords. Each chain is developed by starting with a randomly selected "guess" of the plain text password then sequentially applies variations on it. The attack software will apply the passwords in the rainbow table until it at a possible password. To conduct a rainbow table attack, attackers can use a tool such as L0phtCrack.

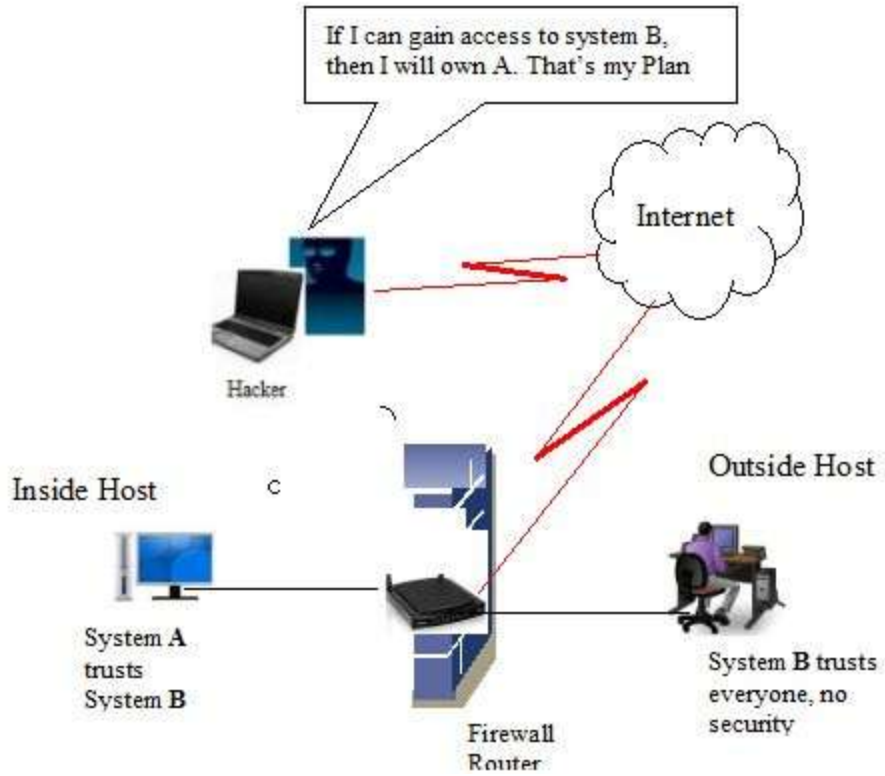
A brute-force attack tool is more sophisticated because it searches in detail using combinations of character sets to work out every possible password made up of those characters. The only disadvantage is that it takes much time to complete this type of attack. Brute-force attack tools have been known to solve simple passwords in less than a minute. Longer, more complex passwords may take days or weeks to resolve.

Solutions to Password Attacks

1. Educating users to use complex password.
2. Restricting the number of failed login attempts.

Network Attack: Trust Exploitations Attack

The goal of a trust exploitation attacker is to compromise a trusted host, using it to stage attacks on other hosts in a network. If a host in a network of a company is protected by a firewall (inside host), but is accessible to a trusted host outside the firewall (outside host), the inside host can be attacked through the trusted outside host.



Solutions

Trust exploitation-based attacks can be controlled through strict protocols on trust levels within a network, for example, private VLANs can be deployed in public-service segments where multiple public servers are available.

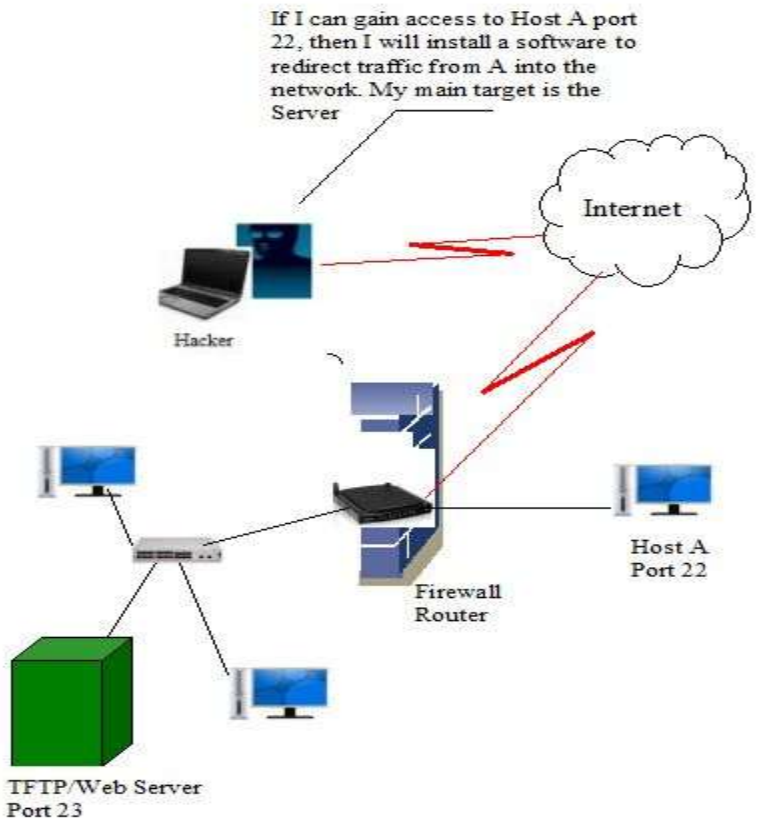
Systems on the outside of a firewall should never be totally trusted by systems on the inside of a firewall. Such trust should be limited to specific protocols and should be authenticated by something other than an IP address.

Port Redirection Attack

A port redirection attack is another type of attack based on trust exploitation. The attacker uses a compromised host to gain access through a firewall that would otherwise be blocked.

Look at it this way; the host on the outside can get to the host on the public services segment, but not the host on the inside. If an intruder is able to compromise the host on the public services segment, the attacker could install software to redirect traffic from the outside host directly to the inside host.

Although neither communication violates the rules implemented in the firewall, the outside host has now achieved connectivity to the inside host through the port redirection process on the public services host. An example of a tool that can provide this type of access is Netcat.



Solution

Port redirection can be controlled primarily through the use of proper trust models. Antivirus software or a host-based intrusion detection system (IDS) can help detect an attacker and prevent installation of such utilities on a host.

Man-in-the-Middle Attack

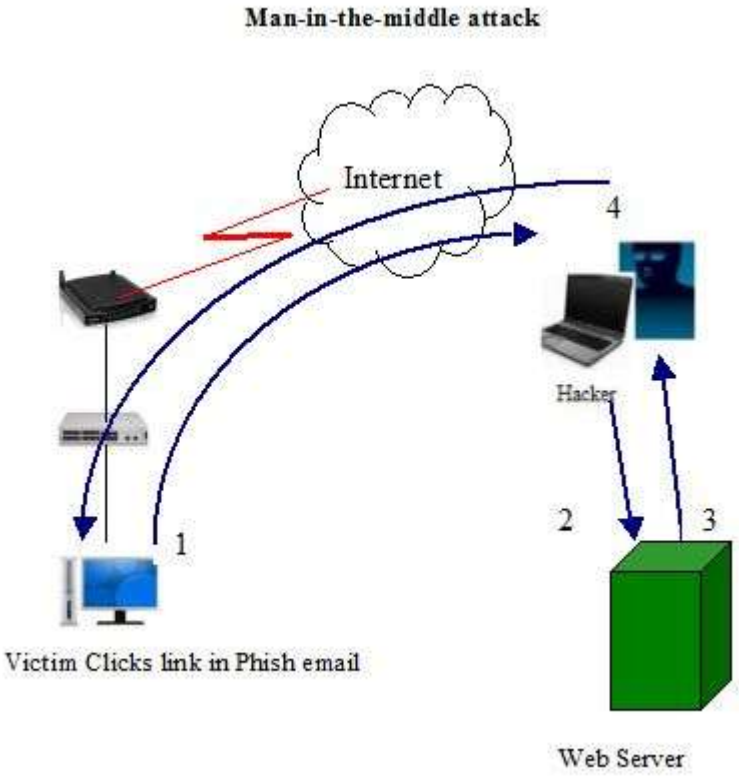
A man-in-the-middle (MITM) attack is implemented by intruders that manage to position themselves between two legitimate hosts. The attacker may allow the normal communication between hosts to occur, but manipulates the conversation between the two.

There are many ways that an attacker gets position between two hosts. A very good example is called the transparent proxy. The attacker prey on their victims by sending a phising email or by defacing a legitimate website.

When the victim loads the URL of a defaced webpage, the attackers URL is added to the front of it.

For example: let say http://www.ocbtc.com/ is a legitimate URL. But when website's URL is hacked it becomes http://www.theattacker.com/http://www.ocbtc.com/

If an intruder manages to get into a strategic position, they can steal information, take control of an ongoing session to gain access to private network resources, conduct DoS attacks, corrupt transmitted data, or introduce new information into network sessions.



1. When a victim requests a webpage, the host of the victim makes the request to the host of the attacker's.
2. The attacker's host receives the request and fetches the real page from the legitimate website.
3. The attacker can alter the legitimate webpage and apply any transformations to the data they want to make.
4. The attacker forwards the requested page to the victim.

Solutions

One of the ways to control Man-in-the-middle (MITM) attack is by using VPN tunnels, this allow the attacker to see only the encrypted, unreadable text. These can be especially useful in Wide Area Networks.

In Local Area Networks, attackers use hacking tools such as, ettercap and ARP poisoning. One of the ways to control this type of attack is by configuring port security on LAN switches.

3. Denial of Service (DoS) Attacks

DoS attack prevents authorized users from using services by consuming system resources. Most times DoS attack is regarded as trivial but in a sense it is a consequentially threat. DoS can cause

potential damage to networks. Not only are they easy to execute, but its among the most difficult to eliminate. DoS attacks deserve special attention from network security administrators.

There are different types of DoS attacks. The following are some examples of common DoS threats:

Ping of Death
A ping of death attack gained prominence in the late 1990s. Then were the older operating systems, which were not as secured as the recent ones. Ping of death type of attack took advantage of vulnerabilities or loop holes in older operating systems, what it does was to modified the IP portion of a ping packet header to indicate that there is more data in the packet than there actually was. A ping is normally 64 or 84 bytes, while a ping of death could be up to 65,536 bytes. Sending a ping of this size may crash an older target computer. Most networks are no longer susceptible to this type of attack.

SYN Flood
A SYN flood attack exploits the TCP three-way handshake. It involves sending multiple SYN requests (1,000+) to a targeted server. The server replies with the usual SYN-ACK response, but the malicious host never responds with the final ACK to complete the handshake. This ties up the server until it eventually runs out of resources and cannot respond to a valid host request.

Other types of DoS attacks include:

i. **E-mail bombs** - Programs send bulk e-mails to individuals, lists, or domains, monopolizing e-mail services.

ii. **Malicious applets** - These attacks are Java, JavaScript, or ActiveX programs that cause destruction or tie up computer resources.

Distributed DoS
This type of attack is executed by flooding network links with illegitimate data. This data can overwhelm an Internet link, thereby enabling legitimate traffic to be dropped.
Solution
DoS and DDoS attacks can be controlled by the implementation of special anti-spoof and anti-DoS Access Control Lists.
ISPs can also implement traffic rate, limiting the amount of unnecessary traffic that crosses network segments. A common example is to limit the amount of ICMP traffic that is allowed into a network, because this traffic is used only for problem-solving purposes.

4. Malicious Code Attacks

Worm, Virus, and Trojan horse attacks constitute a potential threat to end-user workstations.

Worms

A worm executes code and installs copies of itself in the memory of the infected computer, which can, in turn, infect other hosts on the network. The structure of a worm attack is as follows:

- **Creating loopholes**- A worm installs itself by exploiting known vulnerabilities in systems, such as naive end users who open unverified attachments in e-mails.
- **Parasitic ability**- After gaining access to a host, a worm copies itself to that host and then selects new targets.
- **Payload**-Once a host is infected with a worm, the attacker has access to the host, often as an authorised user. Attackers could use a local exploit to escalate their privilege level to administrator.

Solution

1. Contain the spread of the worm in and within the network. Sort out parts of the network that are not infected.

2. Start patching all systems and, if possible, scanning for vulnerable systems.

3. Scan and locate each infected workstations inside the network. Disconnect, remove, or block infected machines from the network.

4 Clean and patch each infected system. Some worms may require complete core system reinstallations to clean the system.

Viruses

A virus is malicious software that is attached to another program file so that they can spread from one machine to another. For your machine to be infected, you must have or had run an infected program or software.

Viruses are potential threats to machines and the entire network, they don't only constitute a strain or nuisance; but are like a time bomb that could destroy all files or contents in your hard drive.

A virus normally requires a delivery mechanism-a vector-such as a zip file or some other executable file attached to an e-mail, to carry the virus code from one system to another. The key element that distinguishes a computer worm from a computer virus is that human interaction is required to facilitate the spread of a virus.

Trojan Horses

A Trojan is a software or program that has a hidden agenda! It is a program written to look like something else. When a software or program that contains Trojan virus is run on your computer, it is doing something else different from what it is meant to do.

For example, you install oe download a free game or software from the Internet, while you are busy running or playing the game; the Trojan horse mails a copy of itself to every address in your address book. The other users receive the game and play it, thereby spreading the Trojan horse to the addresses in each address book.

Most Trojan horse creates loopholes or backdoor program on user systems, attackers can use the program to cause mouse cursors to disappear or use it to install keystroke loggers (programs that record all user keystrokes) to capture sensitive information.

Solution

1. The effective use of antivirus software at the user level, and potentially at the network level. Antivirus software can detect most viruses and many Trojan horse applications and prevent them from spreading in the network.

2. Keep your antivirus software and network operating systems (OS) up to date. Be updated with the latest developments in these sorts of attacks so as to not be caught unawares.

As the type of threats, attacks, and exploits grows, various terms have been used to describe the individuals involved. Some of the most common terms are as follows:

i. White hat- These are network attackers who looks for vulnerabilities in systems or networks and then reports these vulnerabilities to the owners of the system so that they can be fixed. They are ethically opposed to the abuse of computer systems. A white hat generally focuses on securing IT systems.

ii. Hacker- This is a general term that is used to describe a computer programming expert. These are normally used in a negative way to describe an individual that attempts to gain unauthorized access to network resources with malicious intent.

iii. Black hat or Cracker- The opposite of White Hat, this term is used to describe those individuals who use their knowledge of computer systems and programming skills to break into systems or networks that they are not authorized to use, this of course is done usually for personal or financial gain.

iv. Phreaker- This terms is often used to describe an individual who manipulates the phone network in a bid to perform a function that is not allowed. The phreaker breaks into the phone network, usually through a payphone, to make free or illegal long distance calls.

v. Spammer- This is often used to describe the persons who sends large quantities of unsolicited e-mail messages. Spammers often use viruses to take control of home computers and use them to send out their bulk messages.

vi. Phisher- Uses e-mail or other means to trick others into providing sensitive information, such as credit card numbers or passwords. A phisher masquerades as a trusted party that would have a legitimate need for the sensitive information.

TOPIC 10: NETWORK DESIGN

T10.1) Meaning of network design

Network design refers to the planning of the implementation of a computer network infrastructure.

Network design involves evaluating, understanding and scoping the network to be implemented. The whole network design is usually represented as a network diagram that serves as the blueprint for implementing the network physically. Typically, network design includes the following:

- Logical map of the network to be designed
- Cabling structure
- Quantity, type and location of network devices (router, switches, servers)
- IP addressing structure
- Network security architecture and overall network security processes

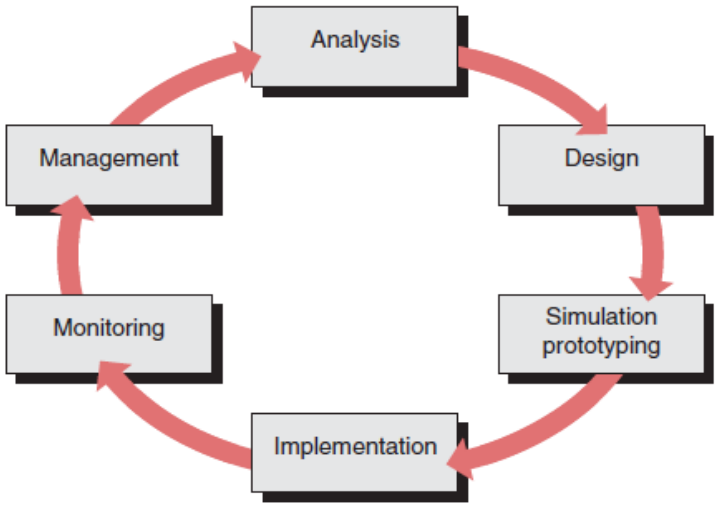
T10.2) Computer development life cycle

The **systems development life cycle** (**SDLC**), also referred to as the **application development life-cycle**, is a term used in systems engineering, information systems and software engineering to describe a process for planning, creating, testing, and deploying an information system. The systems development life-cycle concept applies to a range of hardware and software configurations, as a system can be composed of hardware only, software only, or a combination of both

THE NETWORK DEVELOPMENT LIFE CYCLE

The key model behind the network design process is known as the **network development life cycle (NDLC)** as illustrated in Figure below. The word "cycle" is a key descriptive term of the network development life cycle as it clearly illustrates the continuous nature of network development. A network designed "from scratch" clearly has to start somewhere, namely with an analysis phase.

Existing networks, however, are constantly progressing from one phase to another within the network development life cycle.



Network Design may be fitted in the Overall Scheme of Things as below of the above development stages

The top-down model and the network development life cycle	
Top-Down Model	**Information Systems Development Process**
Business	Strategic business planning Business processing re engineering
Applications	Systems development life cycle Systems analysis and design Application development life cycle
Data	Database analysis and design Database distribution analysis
Network	Network Development Life Cycle Network analysis and design
Technology	Physical network design Network implementation Technology analysis

The Network Development Life Cycle detailing

Category	**Questions/Issues**
People	• Number of total employees

	• Number of employees performing each business function as listed in strategic information system design • Feeling about the "new" system • Key political situations • Number of network-oriented/technically-oriented employees • Training needs
Hardware-Software	• Current level of computerization
Media	• Current applications software • Current networking status • Local phone company • Availability of data services from local phone company • Software performance requirements ❍ Maximum time for customer look-up ❍ Maximum time for part number or pricing look-up ❍ Maximum time for order entry • How "mission-critical" is each application? • Must backup systems be ready at a moment's notice?
Data	• Number of customers • Number of inventory items • Number of open orders • Need for sharing data with other locations, regional offices, corporate headquarters • Special security needs for data or transmission
Network	• Current network configuration • Network traffic volumes • Network protocols • Network monitoring and management technology • Current problems with network to be corrected • Expected growth of network, traffic volume, user community
Physical Plant	• What is the condition of each remote site? • Will additional electrical, heating, data wiring, space, or security systems be required at any sites to accommodate the new systems?

T10.3) Hardware and Software selection criteria

Hardware and Software Selection

There is a bewildering array of IT hardware, software, and services available to businesses today. But lines of business managers typically don't have the background, the time, or the inclination to educate themselves on all the features, pros and cons of alternative solutions to their business problems.

In fact, too often, the way that new technology comes into an organization is like this:

- Somebody goes to a trade show
- A vendor gloms onto them and, of course, has the answer to all their problems
- The vendor pitches to an ad hoc procurement team, which vows to research alternatives and perhaps even issue a Request For Proposal (RFP)
- Due to the press of business, the process is short-circuited and the decision comes down to "Can we afford what the vendor is selling?" rather than "Is this the right solution of the many alternatives we've researched?"
- The purchase is made and never evaluated to see if it a) solved the problem and b) delivered true ROI

It doesn't have to be that way for your business. These can assist at any stage of your procurement process, from developing business requirements, to creating and managing RFPs, to evaluating and managing vendors.

Here are typical hardware and software selection criteria statements:

Hardware Selection Criteria

- Hardware must support current software as well as software planned for procurement over the next planning interval [*year, 18 months, three years*]
- Hardware must be compatible with existing or planned networks
- Hardware must be upgradeable and expandable to meet the needs of the next planning interval
- Hardware warranties must be of an appropriate length
- Hardware maintenance must be performed by [*local/remote vendor, in-house personnel*]
- Whenever feasible, hardware standards will dictate procurement of like brands and configurations to simplify installation and support
- Routine assessments of installed infrastructure will feed an upgrade/replace decision process

Software Selection Criteria

- Software must be compatible with current and future hardware over the next planning interval
- Software maintenance and warranties must be of appropriate length and cost
- Sotware help desk must be maintained by [*vendor, third party, in-house personnel*]
- Software must be standardized throughout the business to improve purchasing power, simplify training, and facilitate support
- Software must comply with current standards set by technology leadership
- Software must support and enhance business goals

In addition to these hardware and software selection criteria, You should evaluate the proposed vendors on several criteria, including:

Stability — Vendor's attributes such as length of operations, size of customer base, size of income and revenue, company size, leadership, stock history and more can affect a technology purchasing decision

Proven Track Record — A vendor's experience not only in the broader market but in your business' specific industry can be key

Business Model Fit — If the vendor is offering, for example, software as a service, but your business isn't always Internet-connected, this business model mismatch could rule out the vendor

Mature Technology — You want to see continuity in the vendor's offerings. If the vendor has been through a series of acquisitions and is just now integrating new technology with an old line of business, you may want to obtain assurances on the longevity of the vendor's solution.

Service Level Agreements — Unfortunately, most vendor Service Level Agreements (SLAs) aren't worth the paper they are printed on. We'll help you understand the vendor's SLA and negotiate a service level partnership instead.

TOPIC 11: TCP/IP PROTOCALS

T11.1) Meaning of TCP/IP concepts

TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet.

TCP is a **connection-oriented** protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages. It determines how to break application data into packets that networks can deliver, sends packets to and accepts packets from the network layer, manages flow control, and—because it is meant to provide error-free data transmission—handles retransmission of dropped or garbled packets as well as acknowledgement of all packets that arrive.

Internet Protocol (IP) is the Internet Protocol. It is a mechanism by which packets may be routed between computers on a network-of-networks. **IP** allows computers to be connected using various physical media, ranging from modems to Ethernet cabling, fiber-optic cables and even satellite and radio links.

IP is designed to be robust, and to gracefully handle the loss of some connections. Individual packets of data are routed by hosts with little knowledge of the overall network structure - just a few local routing rules.

As its name implies, the global Internet is constructed using the IP network protocol.

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.

TCP/IP is responsible for full-fledged data connectivity and transmitting the data end-to-end by providing other functions, including addressing, mapping and acknowledgment. TCP/IP contains four layers, which differ slightly from the OSI model.

Note
TCP/IP is not a single networking protocol - it is a suite of protocols named after the two most important protocols or layers within it - TCP and IP.

As with any form of communication, two things are needed: a message to transmit and the means to reliably transmit the message. The TCP layer handles the message part. The message is broken down into smaller units, called packets, which are then transmitted over the network. The packets are received by the corresponding TCP layer in the receiver and reassembled into the original message.

The IP layer is primarily concerned with the transmission portion. This is done by means of a unique IP address assigned to each and every active recipient on the network.

TCP/IP is considered a stateless protocol suite because each client connection is newly made without regard to whether a previous connection had been established.

T11.2) Types of data flow

The way in which data is transmitted from one place to another is called *data transmission mode*. It is also called the *data communication mode*. It is indicates the direction of flow of information. Sometimes, data transmission modes are also called *directional modes*.

Types of Data Transmission Modes
Different types of data transmission modes are as follows:

1. Simplex mode
2. Half-duplex mode
3. Full-duplex mode

1- Simplex Mode

In simplex mode, data can flow in only one direction. In this mode, a sender can only send data and cannot receive it. Similarly, a receiver can only receive data but cannot send it. Data sent from computer to printer is an example of simplex mode.
In simplex mode, it is not possible to confirm successful transmission of data. It is also not possible to request the sender to re-transmit information. This mode is not widely used. However, this mode is used in business field at certain point-of-sale terminals. The other examples of simplex communication modes are Radio and T.V transmissions.

Figure: Simplex Mode

2- Half-Duplex Mode

In half-duplex mode, data can flow in both directions but only in one direction at a time. In this mode, data is sent and received alternatively. It is like a one-lane bridge where two-way traffic must give way in order to cross the other.
The Internet browsing is an example of half duplex mode. The user sends a request to a Web server for a web page. It means that information flows from user's computer to the web server. Web server receives the request and sends data of the requested page. The data flows the Web server to the user's computer. At a time a user can a request or receive the data of web page.

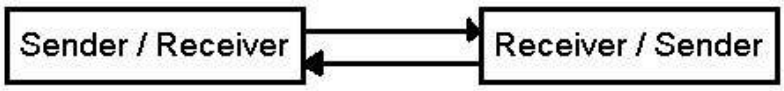


Figure: Half-Duplex Mode

3- Full-Duplex Mode

In full duplex-mode, data can flow in both directions at the same time. It is the fastest directional mode of data communication. The telephone communication system is an example of full-duplex communication mode. Two persons can talk at the same time. Another example of fully-duplex mode in daily life is automobile traffic on a two-lane road. The traffic can move in both directions at the same time.

Figure: Full-Duplex Mode

TOPIC 12: COMMUNICATION SOFTWARE

T12.1) Meaning of terms (computer software and network software)

Computer software or simply **software** is any set of machine-readable instructions that directs a **computer**'s processor to perform specific operations. **Computer software** contrasts with **computer** hardware, which is the physical component of **computers**.

Networking software, in the most basic sense, is software that facilitates, enhances or interacts with a computer network.

One type of networking software allows computers to communicate with one another, while another type of networking software provides users access to shared programs. Networking software is a key component of today's computer networks, including the Internet. Understanding the types of networking software is the first step in understanding how your computer network really works.

T12.2) Different types of communication software

Communication software is an application or program designed to pass information from one system to another. Such software provides remote access to systems and transmits files in a multitude of formats between computers. Communication software forms a part of communication systems with software components classified according to functions within the Open Systems Interconnection Model (OSI Model). The best defined examples of communication software are file transfer protocol (FTP), messaging software and email.

Types of communication software

1. ***File Transfer Protocol* (*FTP*)** is a client-server standard used to *transfer* files between computers over the Internet using control and data channels.
2. ***Software*** to send text ***messages*** to mobile phones and wireless devices. Network *messaging* and standalone text *messaging* solutions for businesses.

Messaging Software

Wireless Messaging includes: WAP, other wireless messaging applications
Mail Server Software includes: SMTP, POP, mail server software and email management
E-Mail Client Software includes: email client software and email addons
Voice Mail includes: voice messaging, ivr, messaging retrieval, and other voice messaging software.
Paging / SMS Software includes: text messaging, numeric paging, SMS applications and more
Unified Messaging includes: forwarding to multiple devices, unified messaging accross multiple devices.
Telephony Software includes: voice over IP, tty, video conferencing and more
Instant Messaging includes: chat, instant messaging and remote messaging software

Programming Toolsincludes: SDK's, messaging api's, components and general messaging development tools
Message Board Software includes: newsgroups and web based message boards
Bulk Email Software includes: mass mail, group e-mails, list server software, newsletter management & bulk email software
Featured Messaging Software includes: messaging software featured from each messaging category
PopUp Killer Software includes: software that stops or filters annoying popups
Spam Killer Software includes: email filtering and anti-spam software

3. An ***email client***, email reader or more formally mail user agent (MUA) is a computer program used to access and manage a user's email.
   I.e. MS Outlook, third bird etc.

T12.3) Types of network software

In addition to protocols, there are many other types of network software.

1. There are network operating systems, sometimes known as NOS. A network operating system provides a framework for computers to understand one another, and from which the computers can run shared applications. Examples of network operating systems include .Net and Novell Netware.
2. Shared network applications are another type of computer networking software. These are applications that are stored on a central server, but run from the individual client computers. Examples include certain types of database applications such as Oracle.
3. There are also client-server network programs. These network programs have a component that's stored on the server, and a component that's stored on the client workstation. Microsoft Exchange is an example of this type of network program.

TOPIC 13: INTERNET

T13.1) Meaning and importance of internet

Definition of Terms

The Internet is a global network connecting millions of computers. More than 190 countries are linked into exchanges of data, news and opinions

The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers).

Is Web and Internet the Same?

The *Internet* is **not** synonymous with *World Wide Web*. The Internet is a massive network of networks, a networking infrastructure. It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet. The World Wide Web, or simply Web, is a way of accessing information over the medium of the Internet. It is an information-sharing model that is built on top of the Internet.

The World Wide Web is a system of Internet servers that support specially formatted documents.

The Internet is Decentralized

Unlike online services, which are centrally controlled, by design, the Internet is decentralized. Each Internet computer, called a *host*, is independent. Operators can choose which Internet services to use and which local services to make available to the global Internet community. Remarkably, this anarchy by design works exceedingly well. There are a variety of ways to access the Internet. Most online services offer access to some Internet services. It is also possible to gain access through a commercial Internet Service Provider (ISP).

Who Owns the Internet?

No one actually owns the Internet, and no single person or organization controls the Internet in its entirety. The Internet is more of a concept than an actual tangible entity, and it relies on a physical infrastructure that connects networks to other networks.

Importance of the internet to your organisation

What does your organisation do?

Broadly, i think one could classify your organisation's jobs into something like this:

- "Communication"
  with other organisations, with your members, with your staff, with your supporters and donors.
  some great ways: letters, phone calls, faxes, meetings
  additional ways: email, messenger, web pages, mail lists, web site message boards

- "Publishing" your message to the world.
  some great ways: books, journals, brochures, press releases, workshops, conferences, lectures.
  additional ways: website with conference proceedings, PDF files of your publications, blogs, newsfeeds
- "Customer support"
  the people you are helping through your organisation.
  Nothing is better than people with people: interviews, workshops, conferences, classes.
  additional ways can help them when you aren't there: email, messenger, web pages, mail lists, web site message boards. With video-conferencing, podcasting and other great web tools, you can even have workshops and classes online.
- "Research"
  on the news, issues, papers and literature relevant to your cause.
  some great ways: books, magazines, journals, papers
  additional ways: websites, search engines to find materials world-wide, mail lists

What's the advantage of these "additional internet ways"? They just look confusing so far.

Yes, they do look confusing, probably because they are new to you. Books and paper looked very confusing to you when you first started to read — you just don't remember because it was a loooong time ago!

- Increase credibility
  These days, if a company or an organisation doesn't have a website, it doesn't exist.
  The more information and services an organisation provides online, the more professional it appears to the public.
- Increase exposure
  When journalists, researchers, etc want to find out about something these days, they don't write letters asking for brochures — they search on the web, and subscribe to newsfeeds.
  They can get information any time of day or night, and easily save it and sort through it.
- Greater quantity and quality of inquiries
  Quantity: People can contact you easily and immediately, through your email address on your site, or even better, through a form on your site.
  Quality: When people contact you, they have already searched for your information at least once already. So they have already shown they are interested, and through your website they are already informed.
- Increase donations and sales.
  Donating or ordering directly from a website can be as easy as typing in a card number and clicking a button.
- Reduce cost per contact.
  The ultimate cost of doing "business" on the Internet is much lower than by print brochures and letters by post.
- Increased access to your information.
  The information you supply is available to the world 24 hours a day, seven days a week.
  It is easily findable through internet search sites, unlike a brochure that can slip underneath a pile of other literature never to be seen again!
  With a website, you can easily keep your information always current and up-to-date.
- Gain full access to a seemingly infinite supply of current information.

As well as current events and blogs, information about almost any subject is available in depth and up to date. This is incredibly valuable for every subject you can imagine. Almost every college and government research organization is on the Internet, along with libraries, educational institutions, associations, and many commercial directories and sites,

- Maintain information that's "up to the minute" accurate.
  With printed materials, the information you deliver can be out of date even before you get it back from the printer. Often, providing updated materials involves throwing out old materials that you had paid for. Materials on the internet however, can be brought up to date immediately at little cost. Also, because there is only one copy people are referring to, you can know that your readers are seeing current information — and not an out-dated brochure, that they forgot to replace with the new copy you mailed to them at your expense!
- Save on printing costs.
  You can reduce your printed materials to shorter brochures and pamphlets, and in them refer the reader to the wealth of information available 24 hours a day on your site.
- Reduce phone usage and staff load.
  By having information on your website, available to the entire world, 24 hours a day, you can greatly reduce the time your staff must spend on the phone or answering letters or emails, providing this same information.
- Reduce postage, express mail and courier service, and phone costs.
  Using email and mail lists, you can send large amounts of information to many people, for little or no cost.
- Increase your "green rating".
  By using electronic media instead of print whenever possible, you reduce the amount of paper, ink, and related materials you consume and discard — helping our poor over-worked planet (and ultimately ourselves, since that planet is where we have to live!).

And this list mostly concerns using websites and email. I haven't even started on the possibilities of online forums, blogs, wikis, video conferencing...

TOPIC 14: EMERGING TRENDS

T14.1) Emerging trends in networking

Networking technologies emerging in the enterprise: We look at the latest networking technologies on offer, and those being adopted in the enterprise

The networking world has always had a tendency to get carried away with new trends and technologies.

Many of these technologies are simply re-inventions with new names, which forget to focus on the basics of efficiently running a corporate network.

Whether that network now resides in the physical corporate offices, some other datacentre or public/private cloud is largely irrelevant.

What is important is to see the take-up of new, relevant technologies that improve networking beyond where it is today.

Here, we look at a few examples of these technologies.

We also look at what some of the more established suppliers are doing to re-invent their offerings.

1. Clouds of virtualisation

One area that – partly as a result of the cloud and virtualisation – has been a focal point is the convergence of networking and storage. While the big names – including Dell, IBM, Cisco, EMC and HP – have all been majorly involved, there has been plenty of activity beyond these incumbents.
Cirba, for instance, has focused on optimizing input/output (I/O) with respect to virtualisation management systems and deployment. The supplier argues companies often do not consider I/O when deploying virtual machines (VMs), which can result in uneven loads across physical hosts. When network-attached storage (NAS) or other storage technologies send disk I/O across the network, Cirba models combine I/O to intelligently balance workloads and minimize the stress points that can otherwise occur. The net effect is safely increasing VM density while at the same time minimizing the risk of contention for resources.

Another move – again a factor in the cloud–plus–virtualisation combination – is from virtualized (hardware-to-software) systems. For example, Avere has just introduced a virtual NAS product that provides the ability to deploy and scale compute in the cloud while using both on-premise and cloud-based storage resources. The idea is to connect the dots between the compute cloud, storage cloud and on-premise storage, without sacrificing performance, worrying about security or seeing IT overspends. This is a software-only product that runs in the compute cloud alongside applications, providing low-latency access to the active data and enabling applications to run at maximum performance.

Pluribus Networks is another company looking to bring all network and compute elements together, using distributed-network hypervisor operating system Netvisor for the convergence of compute, network, storage and virtualisation. It is based on open-compute and open-networking technologies and is aimed at enabling enterprises to better support application performance service-level agreements (SLAs) while reducing operating expenditure and capital expenditure, as well as accelerating service-deployment velocity.

One of many examples of the current move from IT-centric to customer-focused products comes in the form of Virtual Instruments' VirtualWisdom4 infrastructure performance management platform for physical, virtual and cloud-computing environments. The technology was recently introduced to the Morrisons supermarket chain.

The retailer's head of storage, Simon Close, says: "The Virtual Instrument platform has evolved from an engineering-type system to something more customer-focused." Morrisons was keen to consolidate down from a large number of storage suppliers to a single supplier and single SAN environment, with VirtualWisdom plumbed in the middle of it to ensure and assure application and data performance and response times, as well as availability.

2. Traditional tools go modern

Another transitioning technology is the application delivery controller (ADC). According to CTO of ADC provider jetNexus, Greg Howett, gone are the days when these appliances were all hardware devices, designed to be configured and managed by specialist systems engineers. "Load balancers are an essential requirement to everyday application stacks such as Microsoft Exchange and Lync, web-based customer relationship management (CRM) and enterprise resource planning (ERP) applications, as well as external customer-facing websites. Therefore it's essential load balancers are easy to deploy, simple to configure and straightforward to manage," he says. Not only is the graphical user interface (GUI) designed for IT administrators to use, but the product sells almost exclusively as a virtual appliance – a pure software appliance.This switch in terms of moving the network to the users, rather than the engineers, has also been mirrored by Sunrise Software in the latest release of its IT service management (ITSM)application, Sostenuto. Again, the interface is designed for IT administrators – not IT professionals – to use, while fairly radical features (certainly for network management tools) such as gamification have been introduced.

3. Re-managing the network

The changing shape of the corporate network has also meant a change in the way it is managed, with performance and application management becoming increasingly prevalent. Network management is being re-invented. For instance, Sideband Networks' XRE/vXRE system for network performance management correlates live traffic with logged network traffic, giving a single point of management – regardless of wired/wireless or local area network (LAN)/wide area network (WAN) characteristics. The system provides analytics of network traffic up to 40Gbps, addressing both physical and virtual planes, and delivers intelligence that notifies with real-time alerts and actions for network issues. So it combines being a dynamic network discovery tool for network mapping with the ability to drill down into the network performance.

4. Emerging SDN market

Software-defined networking (SDN) seems as where all the traditional startup venture capital money is, with several companies vying to come out on top in the SDN controller market, with Plexxi and other pure-play SDN companies pushing standards and adoption. At the same time, the major suppliers are funding a variety of spin-ins, such as Cisco's Insieme, to accelerate innovation that is often difficult for established suppliers. As a result, there's still lots of bleeding-edge technology and supplier-specific approaches in the market, and a de-facto standard has yet to be chosen by admins on the ground. For network-management software suppliers, the plus point is it will be easy to extend current systems with SDN once standards are determined by the market of actual installations.

5. Advances in wireless

Wireless is another area of recent innovation – beyond the basic Institute of Electrical and Electronic Engineers (IEEE) standards implementations. This is with respect to two particular aspects – bring-your-own-device (BYOD) technology and Wi-Fi in the cloud.

The former has meant real wireless, wire-like infrastructures really have had to be put into place. Wi-Fi technology company Xirrus, for example, has an array-based system designed to effectively replace a wired network – after all, a network of iPads and smartphones renders an Ethernet switch redundant. This means the size of Wi-Fi deployments is increasing enormously.

While often it's the bigger, established suppliers which validate a new (or re-invented) technology area, it's the smaller, more nimble players which populate it in the first place. We have a number of new players in various market segments – including cloud, virtualisation, application management and others – leading the way in getting actual products out to the user. So, while some of the giants of networking are talking the talk – regarding SDN and cloud, for example – it's actually the newbies which are more focused on actually delivering the product.

Communication and media technology and application services – network trend and possible implications may sum up as below

1. An **accelerating pace of change** driven by overlapping development in technology, connections between people, database and objects
2. **Diversity in the development of physical infrastructure** including broadband, digital broadcasting, smart radio system, sensors networks, mesh networks, efficiency techniques in multimedia transmission, location sensing and context-aware technologies, intelligent transport systems and satellite services.
3. Continuing **spread of distributed connectivity** through integration of information processing beyond the desktop into everyday objects and activities
4. **Enhanced content and network management capabilities** driven by developments in deep packet inspection and content filtering technologies, coupled with the need to improve e-security, identity management, intellectual property protection and energy efficiency.

5. The **emerging social web** acting both as a platform and database enabling, innovation and creativity by users and service providers
6. **Continuing scientific and technological innovation**, which in combination are driving advances in computing power, display technologies, artificial intelligence and nanotechnology.

T14.2) Challenges of emerging trends in networking

With each passing year, the security threats facing computer networks have become more technically sophisticated, better organized and harder to detect. At the same time, the consequences of failing to block these attacks have increased. In addition to the economic consequences of financial fraud, we are seeing real-world attacks that impact the reliability of critical infrastructure and national security. With these observations in mind, here are five key challenges that computer security professionals face as we move into 2013.

- ***State-sponsored espionage and sabotage of computer networks***

Current security technologies and best practices are not effective at preventing sophisticated, targeted attacks from being successful. This fact was underlined earlier this year when a malicious program called Flame was discovered after evading detection by anti-virus software for years. Similarly, a recent study by Symantec Research Labs identified 18 undisclosed security vulnerabilities that were used to target computer networks in the wild for up to 30 months before they were discovered. The consequences of missing these attacks can be significant, as demonstrated by the Shamoon malware that recently hit several companies in the oil and energy sector. Shamoon erases data and renders machines unbootable.

New strategies are clearly needed to fight advanced attacks. Looking for known malware and attacks that target known vulnerabilities is not effective in this context because we don't know exactly where the next vulnerability will be found or what the next attack will look like. Instead, we need to develop tactics that focus on the behavior of software, systems and actors on the network. By investigating both specific, suspicious behaviors that we know to be associated with malicious activity, as well as general anomalous behaviors that are unusual or unexpected, we can uncover evidence of attack activity even when we are not exactly sure what to look for at the outset.

- ***Monster DDoS attacks***

Distributed denial-of-service attacks have become increasingly popular with attackers, and the size of the attacks keeps getting larger. The DDoS mitigation firm Prolexic reported an 88% increase in the number of DDoS attacks launched in Q3 2012 versus a year earlier, with substantial increases in both the duration of the attacks as well as the amount of bandwidth involved. Furthermore, early this fall, the websites of several large U.S. financial firms were disrupted by a DDoS attack that reportedly exceeded 60 Gbps – much larger than the typical 5-10 Gbps attack.

The time to prepare for a DDoS attack is not the day that one's website goes down. Firms that are effective at protecting their networks against these incidents have: Assessed the risk of several different kinds of DDoS attack scenarios well in advance; developed processes for

responding in the event that one of those scenarios occurs; and have tested those processes with real drills in order to ensure that they work as expected when needed. Getting this right is a top priority for any firm with a large Internet presence in 2013.

- ***The loss of visibility and control created by IT consumerization and the cloud***

When workloads move into the cloud, organizations lose control over who can access the computer systems that those workloads are running on. They also often lose visibility into what resources were accessed, when they were accessed and from where. The providers of cloud services and technology tell us not to worry about all of that, but seasoned IT security professionals know better. And this problem isn't limited to the cloud. With bring-your-own-device (BYOD) programs, IT is losing control over the software load, configuration and patch level of network endpoints. IPv6 is going to create its own visibility gaps, beginning with vulnerability assessment, as large address ranges are more difficult to scan.

Organizations have to start demanding their network visibility back. There is no reason that new information technologies cannot be designed with the capability of providing security controls and audit trails to people who need them. The best approach to providing those basic capabilities might be different than in legacy systems, but at the end of the day, it is not impossible to solve these problems. It is all a matter of exposing the right information and regaining control in the right way.

- ***The password debacle***

2012 was rife with large disclosures of passwords and password hashes from major websites that were breached, including Zappos, LinkedIn, eHarmony, Last.fm, Yahoo Voice and Formspring. In addition, attackers are constantly scanning the Internet for exposed, password-protected services like Secure Shell (SSH) and Remote Desktop Protocol (RDP). Accounts on these services are subject to brute-force cracking, and have a tendency to show up on the black market.

The fact is that passwords, as a security technology, are reaching the end of their useful life. Moving to a world where alternative authentication systems are the norm is incredibly difficult, and as a consequence we are entering into a period of time when we are going to have to continue to rely on a security control that doesn't work. Encouraging users to pick longer passphrases, and proactively auditing networks for weak passwords are steps that can be helpful during this time. Increasingly, we are going to see attackers entering networks with legitimate access credentials without ever having to fire an exploit that would trigger an intrusion detection system. We need to be prepared for this type of attack activity.

- ***The insider threat***

The insider threat has traditionally been viewed as a high-consequence but low-frequency risk, and many IT organizations have found it challenging to develop effective programs that manage that risk. Even the concerns that were raised over WikiLeaks have failed to create much of a response, because security professionals don't agree on the right approach. However, some good answers have finally started to appear.

For years, researchers at the CERT Insider Threat Center at Carnegie Mellon's Software Engineering Institute have been collecting and studying data on real-world insider incidents. This

year, they published a book cataloging the results of their research, called The CERT Guide to Insider Threats. This book is an invaluable guide to establishing effective processes for managing the risk of insider attacks, and it should be on every security professional's wish list this year. In general, the insider threat drives home the point that perimeter defenses are no longer enough. IT organizations also need to be able to see into their internal networks to identify suspicious activity.

In a recent public comment, former U.S. Cybersecurity Czar Howard Schmidt spoke of the important role that security professionals are playing in keeping infrastructure up and running. "Security professionals day after day, not withstanding disruptions, still keep the machine running," he said. "We are able to do online banking and shopping most of the time – and it's a direct result of the security professionals…" To be sure, 2013 promises to be another challenging year for those professionals, but being adequately prepared to address the above threats will help keep businesses running and critical infrastructure secure.

T14.3) Coping with challenges of emerging trends in networking

New Technology

Technology advances rapidly and shows up in media on all sides. This means users, managers at all levels and even competitors pressure IT staff to implement this new technology just because it is new. The real challenge is deciding which of these new technologies will work to the best interest of advancing the organization and which is better to avoid for now.

Organizational priorities and long-term goals tend to remain relatively static. Technology has become much more fluid and changes more rapidly. IT management must evaluate the organizational value each technology offers to determine when and if it is a good fit.

New technologies such as cloud, big data, virtualization and mobility all become tools for experienced IT managers who understand their organization's priorities. Since every organization is different, the IT value of each new technology will vary with the organization's strategic goals.

To address this issue:

To make the most of any new technology, an IT manager needs a solid understanding of the organization and the challenges its users and markets face. Prior to jumping into a new trend in technology, IT managers must ask one question: "How does this help us address our current challenges or meet our strategic goals?"

Cloud

Many organizations have yet to make cloud plans. They choose to keep their data and applications in-house and manage everything themselves.

With the advances of cloud offerings and to future-proof the network, preparing the organization for a potential future cloud move is simple common sense. For example, what happens when organizational management decides to set up an internal cloud solution. Maybe that is a step toward moving applications and data off-site.

The main point: You must create portable applications today that won't hold your company back in the future, whatever that may hold.

To address this issue:
This comes down to software and hardware architecture. New applications must be built using an open architecture that lets them run on any platform or with any database. Doing so means the organization's applications will run on the in-house servers, an in-house cloud or in an external cloud. The extra benefit is that any move to a cloud-based solution can be completed without new applications.

Big Data Analytics

Data is projected to grow by 800 percent in the next five years. The big challenge is that more than 80 percent of it unstructured. Unstructured data varies in its formats, including plain text, email, blog, formatted document, standard and non-standard image, video, voice, animation, sensor input and web search logs. Unstructured data is growing faster than structured data. As a relatively new and untapped source of organizational insight, unstructured data analytics has the potential to reveal more important information interrelationships that were previously very difficult or impossible to determine.

Part of that unstructured data includes data from communities, groups and social networks outside the organization known as "the collective". Data mining the collective is a great way to understand the organization's market and customers.

To address this issue:
To provide the best value to the organization, big data analytics requires new approaches to capturing, storing and analyzing data. The massive amount and growth of unstructured data rapidly outpaces traditional solutions and calls for new volume handling. Big data is collected from new sources. Traditional data management processes fall short in coping with the variable nature of big data. New analytics offer methods to process the variety. Data is generated in real time and the demands call for usable information to be ready as needed. Solutions like 100 GB Ethernet, parallel- processing, and SSDs (Solid State Drives) offer good response times.

Virtualization

Virtualization continues to expand from desktops to servers to switches, routers and firewalls. Virtualization will provide a much higher level of control of these devices rather than saving money. In fact, the organization's infrastructure will require larger servers, more VM licenses, and emulation software in addition to the continuing cost of desktop licenses.

A virtualized data center requires many of the same management tasks that also must be performed in the physical server environment. These tasks need to be extended into the virtualized environment as well as also integrated with the existing workflow and management processes.

One example is that IT organizations must be able to automatically discover both the physical and the virtual environment and have an integrated view of both environments available for monitoring and managing. That view of the combined virtual and physical server resources needs to stay current as VMs move from one host to another. The view must also be able to indicate which resources are involved in the case of fault or performance issues.

To address this issue:

The Distributed Management Task Force (DMTF) set its Virtualization Management (VMAN) standard. That includes a set of specifications to address the management lifecycle of a virtual environment. VMAN's Open Virtualization Format (OVF) specification provides a standard for describing virtual machines and applications for deployment across various virtualization platforms. VMAN's profiles now standardize many aspects of the operational management of a mixed vendor virtualized environment.

BYOD and BYOA

For years, IT has controlled user's devices. With the advent of smartphones and tablets, that has changed. Users now bring in their own devices without IT's knowledge. They use them for both personal and work-related tasks. IT's initial plan was to attempt to maintain control. The facts are clear: Controlling user-owned devices in an organization's network is nearly impossible.

When a user brings their own device, they will also bring their own applications that they have grown used to using. That is a plus for productivity and a challenge for IT security. IT managers and CIOs will need to decide what to secure: the network infrastructure or the organization's data.

Suggestions:

Controlling users' mobile devices, is a losing battle. IT staff, even with automation, can't possibly monitor every device that links to the network. The solution moves to controlling data access. First, secure the data on servers. Then provide users access to that data in the form of mobile web apps. This lets them access the data on any server they are authorized to access, but doesn't store any data on the mobile device.

Shadow IT

IT continues to have a poor image inside organizations. Whether it be slow response times, dictatorial actions, or software challenges, many IT departments are facing users' preference of going to intra-department super users for help. Add the easily available cloud software and services, organizations see users and groups head toward bypassing the IT department altogether. They find and purchase third party SaaS (Software as a Service) packages to meet their needs.

Other departments like sales, marketing, accounting, etc. are considering independent arrangements with outside IT service providers.

To address this issue:
When end users and managers are less satisfied with the service and support they receive from IT, they begin to look for other options. The solution is less about controlling an emerging Shadow IT. It's really about training the IT department to better communicate with and support the needs of the organization.

Boomers

Starting in this year, about 10,000 baby boomers will become eligible to retire every day for the next 15 to 20 years in North America. A lot of those potential retirees are IT people who have years of both IT and organization-specific knowledge and experience.

The entry-level people coming into the workforce are much more loyal to themselves, what they know and in some cases, to their peers than to the organization. They arrive with different skill sets and new ways of looking at and using technology.

To address this issue:
To deal with retirements and the possibility that younger workers may stay less time, there are two basic alternatives. One choice is a mentoring program so those people who need to be replaced can share their knowledge with their potential replacement in sufficient time to complete the exchange smoothly before retirement. Another solution is giving newer IT workers projects outside of their comfort zone, more training and other opportunities to learn something different and as a result become less vertically focused. As they complete these projects they move to other new areas and projects.

Interoperability

Users and customers are more demanding of the products on their desktops and mobile devices. It all comes down to communicating with each another. Systems need to send and receive data that will be compatible on all user platforms.

Open applications and systems built on open standards are the way of the future. Development efforts must focus on the system or application itself as well as how that system/application works with others.

Tips to address this issue:
At the most basic level, developers must avoid proprietary architecture and use only open architecture and frameworks that communicate easily with other systems.

User Systems

Desktops, laptops, notebooks, tablets and smartphones are already an integral part of many users lives. In some cases, it has become increasingly difficult to draw the line between them. Will tablets replace laptops and notebooks? Will desktops go the way of the dinosaurs?

Tablets and smartphones already perform many tasks previously completed by desktops. That means organizations must adapt to a multiple user systems. These days, internal users and customers may access organizational data and applications via many different methods depending on their current location.

To address this issue:
IT managers must develop applications that adjust to the device the users have available. Some will turn to responsive design that creates a more fluid display to adjust to the screen size variations. Others use the adaptive approach that designs the display to match the desired screen size.

Energy Efficiency

According to most estimates, a 25,000 square foot data center will use about $4 million in energy this year. At that rate, a savings of just a few percent can make a big difference to an IT budget. With an increasing trend of expanding green initiatives and alternate sources of energy, organizations are working on ways to improve energy monitoring and efficiency.

There's an emerging market of tools for energy monitoring and efficiency. More than 25 vendors have entered this market. These tools monitor consumption at the device level and, in some cases, at the application level.

To address this issue:
Resources and tools are readily available to help IT and data center managers benchmark energy use, monitor ongoing trends, identify any savings opportunities, and adopt the most energy efficient practices. Projects funded by the U.S. Department of Energy's (DOE's) Advanced Manufacturing Office (AMO) can strongly improve energy efficiency in both IT and telecommunications.

Creating value

This is a recurring IT issue. It's now a priority. IT departments must focus on improving service to the organizational user and to the organization's departmental needs. To do so, IT managers must remove any non-essential activities that are in the way.

That means a different way of outsourcing non-core activities to keep the focus on value creation. This outsourcing means moving as many services to the cloud as possible. Why own or maintain software or hardware? Small or mid-sized firms can easily rely on the cloud for standardized services.

To address this issue:
This is relatively simple. Ask, "Does this task/activity improve our organization's core priorities?" If not, figure out how to eliminate that function and focus on the mission-critical tasks.

Social Networks

Customers, suppliers and others are currently talking about every organization on some form of social media. This may include Twitter, Facebook, Foursquare, LinkedIn and YouTube. At minimum, IT and marketing departments need to monitor and participate in those conversations. Semantic analysis tools can help companies mine that social dialog to shape new product and upgrades, improve customer service, sales and marketing initiatives.

To address this issue:
Establish a social presence and determine what is being shared. The biggest challenge here is the struggle with shifting from providing a platform to sell products and services to delivering strong customer solutions.