PDCA - 05

# VARDHAMAN MAHAVEER OPEN UNIVERSITY, KOTA

## Post Graduate Diploma in Computer Application (PGDCA)

## Computer Networking and Internet

## Course Development Committee

**Chaiman**

Prof. (Dr.) Naresh Dadhich
Vice-Chancellor
Vardhaman Mahaveer Open University Kota

**Convener / Coordinator**

Prof. (Dr.) D.S. Chauhan
Department of Mathematics
University of Rajasthan Jaipur

**Member Secretary / Coordinator**

Sh. Rakesh Sharma
Assistant Professor (Computer Application)
V.M. Open University Kota

**Members**

1. Prof. (Dr.) S.C. Jain
   Engineering College Ajmer
2. Prof. (Dr.) M.C. Govil
   M.N.I.T. Jaipur
3. Dr. (Mrs.) Madhavi Sinha
   A.I.M. & A.C.T. Jaipur

## Editing and Course Writing

**Editor**

Sh. Rajeev Srivastava
HOD (Computer Science)
LBS PG College Jaipur

**Writers**

1. Dr. S.B. Sharma
   Director, Dau Dayal Vocational Institute
   Dr. B.R. Ambedkar University Agra
2. Dr. D.K. Paliwal
   Lecturer (Institute of Basic Sciences)
   Dr. B.R. Ambedkar University Agra
3. Sh. Manoj Kumar
   Asstt. Professor (Computer Engineering)
   Rajasthan Technical University Kota
4. Ms. Poonam Kshatriya
   Sr. Lecturer (Computer Science)
   A.I.M. & A.C.T. Jaipur
5. Ms. Shweta Sharma
   Lecturer (Computer Engineering)
   Modi Institute of Technology Kota

## Course Supervision and Production

| **Director (Academic)** | **Director (Material Production & Distribution)** |
|---|---|
| Prof. (Dr.) Anam Jaitly<br>Vardhaman Mahaveer Open University,<br>Kota | Prof. (Dr.) P.K. Sharma<br>Vardhaman Mahaveer Open<br>University, Kota |

Production July 2007



Printed and published on behalf of V.M. Open University, Kota by Director (Academic).

# Index

# UNIT - I

# COMPUTER NETWORK FUNDAMENTALS

## STRUCTURE OF THE UNIT



## 1.0 OBJECTIVE:

Students who complete this unit should be able to understand the following tasks:

- Evolution of Networking
- Various types of transmission media
- Various types of inter-network connecting devices

## 1.1 INTRODUCTION

Data networks developed as a result of business applications that were written for microcomputers. The microcomputers were not connected so there was no efficient way to share data among them. It was not efficient or cost-effective for businesses to use floppy disks to share data known as Sneaker net. Sneaker net created multiple copies of the data. Each time a file was modified it would have to be shared again with all other people who needed that file. If two people modified the file and then tried to share it, one of the sets of changes would be lost. Businesses needed a solution that would successfully address the following three problems:

- How to avoid duplication of equipment and resources
- How to communicate efficiently
- How to set up and manage a network

Businesses realized that computer networking could increase productivity and save money. Networks were added and expanded almost as rapidly as new network technologies and products were introduced. The early development of networking was disorganized. However, a tremendous expansion occurred in the early 1980s.

## 1.2 DEFINITIONS

**LAN (Local Area Network)**

A high-speed, low-error data network covering a relatively small geographic area, up to a few thousand meters. LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LANs allow businesses to locally share computer files and printers efficiently and make internal communications possible. LANs manage data, local communications, and computing equipment. LAN standards specify cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies.

LANs consist of the following components:

- Computers
- Network interface cards
- Peripheral devices
- Networking media
- Network devices

**MAN (Metropolitan Area Network)**

A MAN usually consists of two or more LANs in a common geographic area. A network that spans a metropolitan area. Generally, a MAN spans a larger geographic area than a LAN, but a smaller geographic area than a WAN. For example, a bank with multiple branches may utilize a MAN. Typically, a service provider is used to connect two or more LAN sites using private communication lines or optical services. A MAN can also be created using wireless bridge technology by beaming signals across public areas. Wireless bridge technologies that send signals across public areas can also be used to create a MAN.

**WAN (Wide Area Network)**

A WAN is a data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs. WANs interconnect LANs, which then provide access to computers or file servers in other locations. Because WANs connect user networks over a large geographical area, they make it possible for businesses to communicate across great distances. WANs allow computers, printers, and other devices on a LAN to be shared with distant locations. WANs provide instant communications across large geographic areas.

Collaboration software provides access to real-time information and resources and allows meetings to be held remotely. WANs have created a new class of workers called telecommuters. These people never have to leave their homes to go to work.

WANs are designed to do the following:

- Operate over a large and geographically separated area

- Allow users to have real-time communication capabilities with other users
- Provide full-time remote resources connected to local services
- Provide e-mail, Internet, file transfer, and e-commerce services

Some common WAN technologies include the following:

- Integrated Services Digital Network (ISDN)
- Digital subscriber line (DSL)
- Frame Relay
- T1, E1, T3, and E3
- Synchronous Optical Network (SONET)

**The Internet and Beyond**

More than just a technology, the Internet has become a way of life for many people, and it has spurred a revolution of sorts for both public and private sharing of information. The most popular source of information about almost anything, the Internet is used daily by technical and non-technical users alike.

**The Internet: The Largest Network of All**

With the meteoric rise in demand for connectivity, the Internet has become a major communications highway for millions of users. It is a decentralized system of linked networks that are worldwide in scope. It facilitates data communication services such as remote log-in, file transfer, electronic mail, the World Wide Web and newsgroups. It consists of independent hosts of computers that can designate which Internet services to use and which of their local services to make available to the global community.

Initially restricted to military and academic institutions, the Internet now operates on a three-level hierarchy composed of backbone networks, mid-level networks and stub networks. It is a full-fledged conduit for any and all forms of information and commerce. Internet websites now provide personal, educational, political and economic resources to virtually any point on the planet.

**Intranet: A Secure Internet-like Network for Organizations**

With advancements in browser-based software for the Internet, many private organizations have implemented *intra*nets. An intranet is a private network utilizing Internet-type tools, but available only within that organization. For large organizations, an intranet provides easy access to corporate information for designated employees.

**Extranet: A Secure Means for Sharing Information with Partners**

While an intranet is used to disseminate confidential information *within* a corporation, an *extra*net is commonly used by companies to share data in a secure fashion with their business partners. Internet-type tools are used by content providers to update the extranet. Encryption and user authentication means are provided to protect the information, and to ensure that designated people with the proper access privileges are allowed to view it.

Self learning Exercises :

1. The performance of a data communication network depends on:

   (a) the number of users (b) the transmission media

   (c) the hardware and software (d) all of the above

2. The information to be communicated in a data communication system is the:

(a) medium (b) protocol

(c) message (d) transmission

3. The world's largest network that provides communication to people around the world:

(a) LAN (b) Intranet

(c) Internet (d) WAN

## 1.3 APPLICATIONS

Computer Networking has become more and more a part of our daily lives. The exchange of information and sharing of devices in this digital world can only be accomplished by networking. It has evolved from being something only useful to businesses, to being a necessity to home users. Computer networking has expanded it uses in many positive ways and continues to do so.

**Interactive Multimedia Networking**

Applications that require real-time interaction among their users are gaining importance and diffusion as computer networks become more powerful and ubiquitous. Many such applications impose very stringent requirements on the network; among the applications today widely deployed, video-conferencing is the most demanding. In order for the participants in a videoconference call to interact naturally, the end-to-end delay should be below human perception; even though an objective and unique figure cannot be set, 100 ms is widely recognized as the desired one way delay requirement for interaction. Since the global propagation delay can be about 100 ms, the actual end-to-end delay budget available to the system designer (excluding propagation delay) can be no more than 10 ms.

**E-Com (Electronic Commerce)**

This covers the electronic business transactions over network Electronic Commerce (EC) conducted on the Internet and World Wide Web (WWW). After an introduction to the Internet and WWW, during which the benefits of using these infrastructures for EC are highlighted, the importance of authentication, confidentiality, integrity and non-repudiability in any business transaction will be handled and extrapolated to EC on the Internet/WWW. The importance of digital signatures and digital identities are major issues, as well as the public key infrastructure on which such signatures and identities are based. The role of Certification Authorities in certifying digital identities is an important issue. Several Internet security protocols like Secure Sockets Layer (SSL) and Secure Hyper Text Transport protocol (SHTTP) as well as the secure payment protocol SET participates, showing how the discussed security technologies are used in these protocols. Different implementations for electronic cash as well as some legal and policy aspects concludes the EC.

Today, E-mail and Internet access are as important to your business as your phone, or any other revenue-producing asset. Innovative network peripherals, powerful administrative tools and thorough management of these growing networks are a requirement to keep your networks available, reliable and secure. Many companies offer for industry-leading solutions from building the backbone of your workgroup or enterprise WAN to connectivity from your home offices or between your satellite sites.

**Enterprise Management**

Enterprise management solutions generally do more than optimize infrastructure, availability and performance. Companies provide solutions that put you in control and allow you to focus on improving your business' efficiency and increasing customer satisfaction. This allows you a greater (ROI) return on investment.

**Network Systems**

In today's challenging economic environment, IT managers increasingly have to do more with constrained resources. For the enterprise network manager, this means looking for smarter ways to use the network while managing the demands of users, applications and limited budgets. Companies offer a unique blend of practical and innovative technologies and way of combining them that provides you with high-value, leading-edge solutions designed for the realities of business and the Internet.

## 1.4 TRANSMISSION MEDIA

Whatever type of network is used, some type of network media is needed to carry signals between computers. Two types of media are used in networks: cable-based media, such as twisted pair, and the media types associated with wireless networking, such as radio waves, microwaves and Infrared waves.

In networks using cable-based media, there are three basic choices:

- Twisted pair
- Coaxial
- Fiber-optic

Twisted-pair and coaxial cables both use copper wire to conduct the signals electronically; fiber-optic cable uses a glass or plastic conductor and transmits the signals as light.

For many years, coaxial was the cable of choice for most LANs. Today, however (and for the past 10 years), twisted pair has proved to be far and away the cable media of choice, thus retiring coax to the confines of storage closets. Fiber-optic cable has also seen its popularity rise but because of cost has been primarily restricted to use as a network backbone where segment length and higher speeds are needed. That said, fiber is now increasingly common in server room environments as a server to switch connection method, and in building to building connections in what are termed as metropolitan area networks (MANs).

Copper cable is used in almost every LAN. Many different types of copper cable are available. Each type has advantages and disadvantages. Proper selection of cabling is key to efficient network operation. Since copper uses electrical currents to transmit information, it is important to understand some basics of electricity.

### 1.4.1 Magnetic Media

All matter is composed of atoms. The Periodic Table of Elements lists all known types of atoms and their properties. The atom is comprised of three basic particles:

- **Electrons** – Particles with a negative charge that orbit the nucleus
- **Protons** – Particles with a positive charge
- **Neutrons** – Neutral particles with no charge

The protons and neutrons are combined together in a small group called a nucleus. Atoms, are groups of atoms called molecules, can be referred to as materials. Materials are classified into three groups based on how easily free electrons flow through them.

The basis for all electronic devices is the knowledge of how insulators, conductors, and semiconductors control the flow of electrons and work together. The materials through which current flows vary in their resistance to the movement of the electrons. The materials that offer very little or no resistance are called conductors. Those materials that do not allow the current to flow, or severely restrict its flow, are called insulators. The amount of resistance depends on the chemical composition of the materials.

All materials that conduct electricity have a measure of resistance to the flow of electrons through them. These materials also have other effects called capacitance and inductance that relate to the flow of electrons. Impedance includes resistance, capacitance, and inductance and is similar to the concept of resistance.

Attenuation is important in relation to networks. Attenuation refers to the resistance to the flow of electrons and explains why a signal becomes degraded as it travels along the conduit.

Electrical insulators are materials that are most resistant to the flow of electrons through them. Examples of electrical insulators include plastic, glass, air, dry wood, paper, rubber, and helium gas. These materials have very stable chemical structures and the electrons are tightly bound within the atoms.

Electrical conductors are materials that allow electrons to flow through them easily. The outermost electrons are bound very loosely to the nucleus and are easily freed. At room temperature, these materials have a large number of free electrons that can provide conduction. The introduction of voltage causes the free electrons to move, which results in a current flow.

Semiconductors are materials that allow the amount of electricity they conduct to be precisely controlled. Examples include carbon (C), germanium (Ge), and the alloy gallium arsenide (GaAs). Silicon (Si) is the most important semiconductor because it makes the best microscopic-sized electronic circuits. Silicon is very common and can be found in sand, glass, and many types of rocks.

Voltage is sometimes referred to as electromotive force (EMF). EMF is related to an electrical force, or pressure, that occurs when electrons and protons are separated. The force that is created pushes toward the opposite charge and away from the like charge. This process occurs in a battery, where chemical action causes electrons to be freed from the negative terminal of the battery. The electrons then travel to the opposite, or positive, terminal through an external circuit. The electrons do not travel through the battery. Remember that the flow of electricity is really the flow of electrons. Voltage can also be created in three other ways. The first is by friction, or static electricity. The second way is by magnetism, or an electric generator. The last way that voltage can be created is by light, or a solar cell.

The purpose of the physical layer is to transport a raw bit stream from one machine to another. Various physical media can be used for the actual transmission. Each one has its own niche in terms of bandwidth, delay, cost, and ease of installation and maintenance. Media are roughly grouped into guided media, such as copper wire and fiber optics, and unguided media, such as radio and lasers through the air.

Magnetic media, commonly called as copper wire media, is term referring to the transmission of audio/video, analog/digital data on a magnetised medium, in form of voltage pulses.

Cables have different specifications and expectations. Important considerations related to performance are as follows:

- What speeds for data transmission can be achieved? The speed of bit transmission through the cable is extremely important. The speed of transmission is affected by the kind of conduit used.
- Will the transmissions be digital or analog? Digital or baseband transmission and analog or broadband transmission require different types of cable.
- How far can a signal travel before attenuation becomes a concern? If the signal is degraded, network devices might not be able to receive and interpret the signal. The distance the signal travels through the cable affects attenuation of the signal. Degradation is directly related to the distance the signal travels and the type of cable used.

The following Ethernet specifications relate to cable type:

- 10BASE-T
- 10BASE5
- 10BASE2

10BASE-T refers to the speed of transmission at 10 Mbps. The type of transmission is baseband, or digitally interpreted. The T stands for twisted pair.

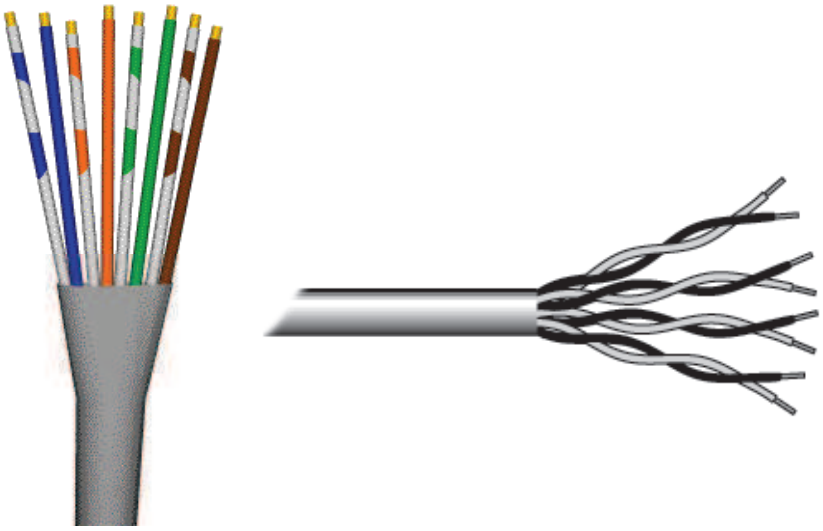
10BASE5 refers to the speed of transmission at 10 Mbps. The type of transmission is baseband, or digitally interpreted. The 5 indicates that a signal can travel for approximately 500 meters before attenuation could disrupt the ability of the receiver to interpret the signal. 10BASE5 is often referred to as Thicknet. Thicknet is a type of network and 10BASE5 is the cable used in that network.

10BASE2 refers to the speed of transmission at 10 Mbps. The type of transmission is baseband, or digitally interpreted. The 2, in 10BASE2, refers to the approximate maximum segment length being 200 meters before attenuation could disrupt the ability of the receiver to appropriately interpret the signal being received. The maximum segment length is actually 185 meters. 10BASE2 is often referred to as Thinnet. Thinnet is a type of network and 10BASE2 is the cable used in that network.

### 1.4.2 Twisted Pair

Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. To reduce crosstalk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Each connection on twisted pair requires both wires. Since some telephone sets or desktop locations require multiple connections, twisted pair is sometimes installed in two or more pairs, all within a single cable. For some business locations, twisted pair is enclosed in a shield that functions as a ground. This is known as shielded twisted pair (STP). Ordinary wire to the home is unshielded twisted pair (UTP).

**UTP :**



UTP cables are made up of pairs of copper wires twisted together. The twisting serves an important purpose – it helps to eliminate electromagnetic interference (EMI). EMI is a common problem on networks using copper wire. Signals from one wire pair might interfere with another (referred to as crosstalk), while powerful external electrical devices may also impact transmission capabilities. When using UTP cables, a common mistake is to unravel the twisting too far – this will certainly degrade signal strength and make the wires more prone to interference.

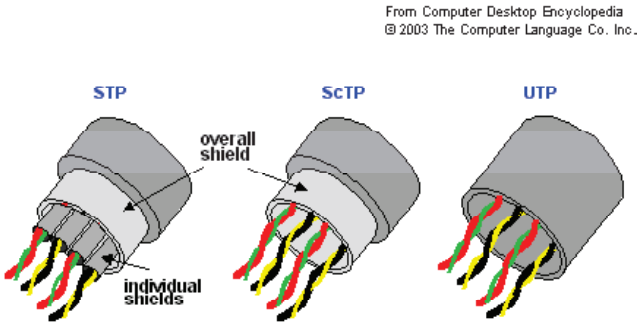
UTP cable has many advantages. It is easy to install and is less expensive than other types of networking media. In fact, UTP costs less per meter than any other type of LAN cabling. However, the real advantage is the size. Since it has such a small external diameter, UTP does not fill up wiring ducts as rapidly as other types of cable. This can be an extremely important factor to consider, particularly when a network is installed in an older building. When UTP cable is installed with an RJ-45 connector, potential sources of network noise are greatly reduced and a good solid connection is almost guaranteed.

There are some disadvantages of twisted-pair cabling. UTP cable is more prone to electrical noise and interference than other types of networking media, and the distance between signal boosts is shorter for UTP than it is for coaxial and fiber optic cables. Twisted pair cabling was once considered slower at transmitting data than other types of cable. This is no longer true. In fact, today, twisted pair is considered the fastest copper-based media..

The category of the cabling defines how many wire pairs you'll find in a given cable. Voice grade cable, also known as Category (or simply 'Cat') 3, uses only two pairs and is used for telephone service and 10Mb Ethernet. Cat 5 wiring, on the other hand, uses 4 wire pairs and is the minimum required for 100Mb Fast Ethernet. For the most part, buildings today are usually pre-wired for Cat 5, although Cat 3 may still be found in older environments. You may also come across what is known as Cat 5E – this version of Cat 5 simply has more twists per inch of wiring, providing better resistance to EMI and higher transmission capabilities.

**STP :**

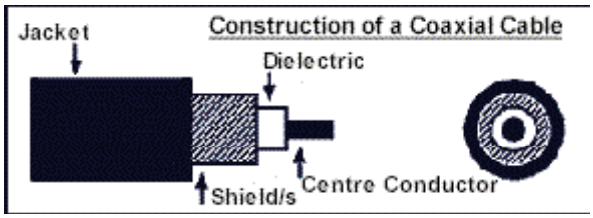
Twisted pair cables are often shielded in attempt to prevent electromagnetic interference (EMI). Because the shielding is made of metal, it may also serve as a ground. However, usually a shielded or a screened twisted pair(ScTP) cable has a special grounding wire added called a drain wire. This shielding can be applied to individual pairs, or to the collection of pairs. When shielding is applied to the collection of pairs, this is referred to as screening. The shielding must be grounded for the shielding to work.




STP cable combines the techniques of cancellation, shielded, and twisted wires. Each pair of wires is wrapped in metallic foil. The two pairs of wires are wrapped in an overall metallic braid or foil. It is usually 150-ohm cable. As specified for use in Token Ring network installations, STP reduces electrical noise within the cable such as pair to pair coupling and crosstalk. STP also reduces electronic noise from outside the cable such as electromagnetic interference (EMI) and radio frequency interference (RFI). STP cable shares many of the advantages and disadvantages of UTP cable. STP provides more protection from all types of external interference. However, STP is more expensive and difficult to install than UTP. A variation of STP, known as ScTP for "screened twisted pair" or FTP for "foil twisted pair," uses only the overall shield and provides more protection than UTP, but not as much as STP.

### 1.4.3 Coaxial Cable

Coaxial cable (or "coax) is the most common cable used for transmitting video signals. The name "coaxial" refers to the common axis of the two conductors.




The dielectric is surrounded by foil shield/s and/or copper braid/s which form the outer conductor and also shield against The outer conductor/shield is encased in a PVC jacket. Most coaxial cables for video applications have a nominal impedance of 75 ohms. Their differing electrical and physical characteristics make it important to select the correct type of cable to suit the application.

A coaxial cable has a solid copper or copper-clad-steel centre conductor surrounded by a non-conductive dielectric insulating material. The center conductor can also be made of tin plated aluminium cable allowing for the cable to be manufactured inexpensively. Over this insulating material is a woven copper braid or metallic foil that acts as the second wire in the circuit and as a shield against for the inner conductor. This second layer, or shield also reduces the amount of outside electromagnetic interference. Covering this shield is the cable jacket.

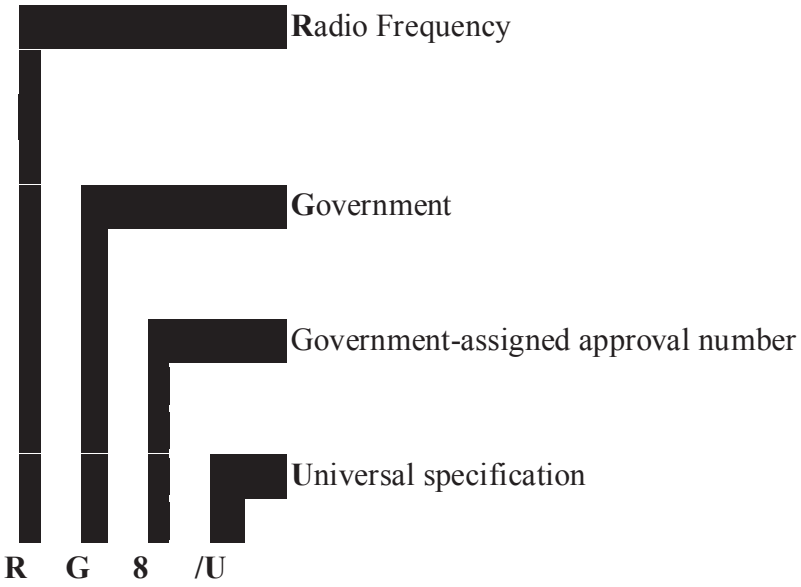
For LANs, coaxial cable offers several advantages. It can be run longer distances than shielded twisted pair, STP, unshielded twisted pair, UTP, and screened twisted pair, ScTP, cable without the need for repeaters. Repeaters regenerate the signals in a network so that they can cover greater distances. Coaxial cable is less expensive than fiber-optic cable and the technology is well known. It has been used for many years for many types of data communication such as cable television.

It is important to consider the size of a cable. As the thickness increases, it becomes more difficult to work with a cable. Remember that cable must be pulled through conduits and troughs that are limited in size. Coaxial cable comes in a variety of sizes. The largest diameter was specified for use as Ethernet backbone cable since it has greater transmission lengths and noise rejection characteristics. This type of coaxial cable is frequently referred to as Thicknet. This type of cable can be too rigid to install easily in some situations. Generally, the more difficult the network media is to install, the more expensive it is to install. Coaxial cable is more expensive to install than twisted-pair cable.

In the past, Thinnet coaxial cable with an outside diameter of only 0.35 cm was used in Ethernet networks. It was especially useful for cable installations that required the cable to make many twists and turns. Since Thinnet was easier to install, it was also cheaper to install. This led some people to refer to it as Cheapernet. The outer copper or metallic braid in coaxial cable comprises half the electric circuit. A solid electrical connection at both ends is important to properly ground the cable. Poor shield connection is one of the biggest sources of connection problems in the installation of coaxial cable. Connection problems result in electrical noise that interferes with signal transmission. For this reason Thinnet is no longer commonly used nor supported by latest standards, 100 Mbps and higher, for Ethernet networks.

**Types of Coax :**

Coaxial cables that conform to U.S. Government specifications are identified with an RG designation. The meaning of the individual components of the designation are:




If the letters **A**, **B** or **C** appear before the slash (/) it indicates a specification-modification or revision. As an example, RG 8/U is superseded by RG 8A/U.

The three most commonly used coaxial cable types for video applications are RG59/U, RG6/U and RG11/U.

**RG59/U** is available with either solid copper or copper-clad-steel centre conductor. It's suitable for basic analog TV antenna feeds in residential applications and for basic CCTV systems over short cable runs. The copper-clad-steel type has high tensile strength and should be used when terminating the cable with F-Type connectors.

**RG6/U Quad-shield** is the minimum requirement under the latest Australian Standard for digital TV antenna cabling and for all TV antenna cabling for apartments/units (MATV). It is also used for the distribution of Cable TV (CATV) and Satellite TV (SATV) in residential or commercial premises. It features a copper-clad-steel inner conductor. Single-shield, dual-shield and tri-shield versions of RG6/U are available but do not provide adequate EMI shielding.

**RG11/U Quad-shield** is used for the same applications as RG6/U for either backbone cabling or for long distribution runs. It features a copper-clad-steel inner conductor.

**Choosing the correct cable :**

Use the table below to determine which cable should be used for your application.

| | | |
|---|---|---|
| **Analog TV** | **RG59/U** | Acceptable performance on cable runs <225 metres |
| | **RG6/U** | Gives superior performance on cable runs <225 metres.Used for cable runs >225 metres but <545 metres. |
| | **RG11/U** | For cable runs greater than 545 metres. |
| **CCTV** | **RG59/U** | Acceptable performance on cable runs <225 metres |
| | **RG6/U** | Gives for superior performance on cable runs <225 metres.Used for cable runs >225 metres but <545 metres. |
| | **RG11/U** | For cable runs greater than 545 metres. |
| **DTV, CATV, SATV, MATV** | **RG6/U** **RG11/U** | Standard cable for these applications Recommended for long cable runs and for backbone cabling. |

**Coaxial Connectors**

| | |
|---|---|
|  | **BNC connector** are bayonet type connectors, commonly used in CCTV systems. They are the most suitable connector for use with RG59/U cable. BNC connectors are specified by IEC standard IEC60169-8. The argument, over what the "BNC" in "BNC connector" means, will go on forever. It has been variously defined as: British Navy Connector, Bayonet Node Connector, Bayonet Nut Coupling, Baby Neil Connector, etc. The two Amphenol engineers who invented the BNC connector were named Paul Neil and Carl Concelman. It therefore seems logical that the "true" meaning of the "BNC" acronym is perhaps "Bayonet **N**eil-**C**oncelman". |
|  | **F-Type connectors** are used for CATV, SATV and Digital TV in conjunction with either RG6 or RG11 cables. The copper-clad-steel inner conductor of the cable forms the inner "pin" of the connector. Although "twist-on" type connectors are available, they do not produce a reliable connection in comparison to a crimp-type connector that has been terminated with a good-quality ratchet crimping tool. F-type connectors are also known as F-81 connectors and are specified by IEC standard IEC60169-24.<br>F-type connectors are named according to the type of cable or the application that they have been designed for as shown in the table below. |

| Connector Name | Application / Description |
|---|---|
| F-59A male<br>F-6 (F-56)<br>F-11 | F-connector that seizes the outer braid and jacket of an RG-59, RG-6 (RG-56) or RG-11 coaxial cable. The cable's centre conductor extends through the connector to form the centre contact. |
| F-61 | An equipment or panel-mounted F-connector (usually female) with soldered cable connections. A 3/8" ( 32 pitch) thread is provided to accept the connector nut of the male connector. |
| F-71 | A male/male F-connector. |
| F-81A | female/female F-connector used to couple two male-ended cables together for in-line or wall-plate applications. |

**PAL (Belling Lee) connectors** are a push-on connector that have been traditionally used for TV antenna wall plates and connections. With the exception of TV/VCR hook-ups, PAL connectors are being replaced by F-Type connectors as required for CATV, SATV and DTV. PAL connectors are specified by IEC standard IEC60169-2.

**Adaptors.** Where BNC connectors are required with RG6/U coaxial cable, it is recommended that an F-Type plug be crimped to the RG6/U and an F-Type to BNC adaptor used.

### 1.4.4 Fiber Optics

Optical fiber is the most frequently used medium for the longer, high bandwidth, point-to-point transmissions required on LAN backbones and on WANs. Optical media uses light to transmit data through thin glass or plastic fiber. Electrical signals cause a fiber-optic transmitter to generate the light signals sent down the fiber. The receiving host receives the light signals and converts them to electrical signals at the far end of the fiber. However, there is no electricity in the fiber-optic cable. In fact, the glass used in fiber-optic cable is a very good electrical insulator.

The part of an optical fiber through which light rays travel is called the core of the fiber. Light rays can only enter the core if their angle is inside the numerical aperture of the fiber. Likewise, once the rays have entered the core of the fiber, there are a limited number of optical paths that a light ray can follow through the fiber. These optical paths are called modes. If the diameter of the core of the fiber is large enough so that there are many paths

that light can take through the fiber, the fiber is called "multimode" fiber. Single-mode fiber has a much smaller core that only allows light rays to travel along one mode inside the fiber.

**Properties of light rays:**

When electromagnetic waves travel out from a source, they travel in straight lines. These straight lines pointing out from the source are called rays. Think of light rays as narrow beams of light like those produced by lasers. In the vacuum of empty space, light travels continuously in a straight line at 300,000 kilometers per second. However, light travels at different, slower speeds through other materials like air, water, and glass. When a light ray called the incident ray, crosses the boundary from one material to another, some of the light energy in the ray will be reflected back. That is why you can see yourself in window glass. The light that is reflected back is called the reflected ray.

The light energy in the incident ray that is not reflected will enter the glass. The entering ray will be bent at an angle from its original path. This ray is called the refracted ray. How much the incident light ray is bent depends on the angle at which the incident ray strikes the surface of the glass and the different rates of speed at which light travels through the two substances.

The bending of light rays at the boundary of two substances is the reason why light rays are able to travel through an optical fiber even if the fiber curves in a circle.

The optical density of the glass determines how much the rays of light in the glass bends. Optical density refers to how much a light ray slows down when it passes through a substance. The greater the optical density of a material, the more it slows light down from its speed in a vacuum. The index of refraction is defined as the speed of light in vacuum divided by the speed of light in the medium. Therefore, the measure of the optical density of a material is the index of refraction of that material. A material with a large index of refraction is more optically dense and slows down more light than a material with a smaller index of refraction.

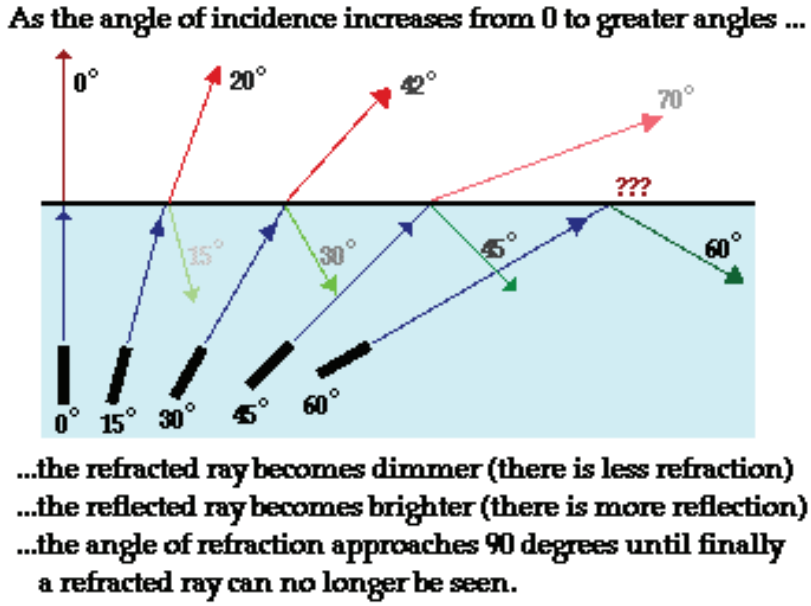
For a substance like glass, the Index of Refraction, or the optical density, can be made larger by adding chemicals to the glass. Making the glass very pure can make the index of refraction smaller. The next lessons will provide further information about reflection and refraction, and their relation to the design and function of optical fiber

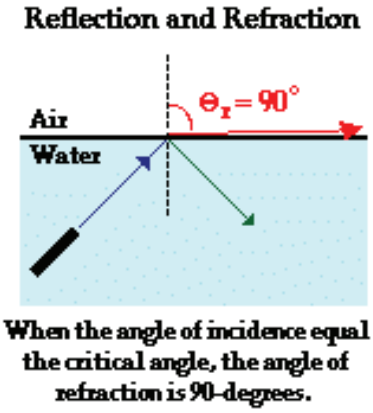
**An overview of reflection:**

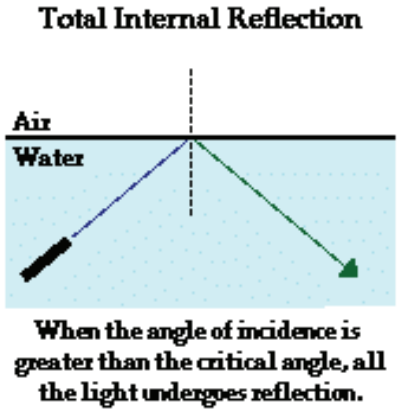
When a ray of light (the incident ray) strikes the shiny surface of a flat piece of glass, some of the light energy in the ray is reflected. The angle between the incident ray and a line perpendicular to the surface of the glass at the point where the incident ray strikes the glass is called the angle of incidence. The perpendicular line is called the normal. It is not a light ray but a tool to allow the measurement of angles. The angle between the reflected ray and the normal is called the angle of reflection. The Law of Reflection states that the angle of reflection of a light ray is equal to the angle of incidence. In other words, the angle at which

a light ray strikes a reflective surface determines the angle that the ray will reflect off the surface.

These principles are depicted in the diagram below.




**An overview of refraction**:

When a light strikes the interface between two transparent materials, the light divides into two parts. Part of the light ray is reflected back into the first substance, with the angle of reflection equaling the angle of incidence. The remaining energy in the light ray crosses the interface and enters into the second substance.

If the incident ray strikes the glass surface at an exact 90-degree angle, the ray goes straight into the glass. The ray is not bent. However, if the incident ray is not at an exact 90-degree angle to the surface, then the transmitted ray that enters the glass is bent. The bending of the entering ray is called refraction. How much the ray is refracted depends on the index of refraction of the two transparent materials. If the light ray travels from a substance whose index of refraction is smaller, into a substance where the index of refraction is larger, the refracted ray is bent towards the normal. If the light ray travels from a substance where the index of refraction is larger into a substance where the index of refraction is smaller, the refracted ray is bent away from the normal.

Consider a light ray moving at an angle other than 90 degrees through the boundary between glass and a diamond. The glass has an index of refraction of about 1.523. The diamond has an index of refraction of about 2.419. Therefore, the ray that continues into the diamond will be bent towards the normal. When that light ray crosses the boundary between the diamond and the air at some angle other than 90 degrees, it will be bent away from the normal. The reason for this is that air has a lower index of refraction, about 1.000 than the index of refraction of the diamond.

**Total internal reflection as it relates to optical media**

A light ray that is being turned on and off to send data (1s and 0s) into an optical fiber must stay inside the fiber until it reaches the far end. The ray must not refract into the material wrapped around the outside of the fiber. The refraction would cause the loss of part of the light energy of the ray. A design must be achieved for the fiber that will make the outside surface of the fiber act like a mirror to the light ray moving through the fiber. If any light ray that tries to move out through the side of the fiber were reflected back into the fiber at an angle that sends it towards the far end of the fiber, this would be a good “pipe” or “wave guide” for the light waves.

The laws of reflection and refraction illustrate how to design a fiber that guides the light waves through the fiber with a minimum energy loss. The following two conditions must be met for the light rays in a fiber to be reflected back into the fiber without any loss due to refraction:

- The core of the optical fiber has to have a larger index of refraction (n) than the material that surrounds it. The material that surrounds the core of the fiber is called the cladding.
- The angle of incidence of the light ray is greater than the critical angle for the core and its cladding.

When both of these conditions are met, the entire incident light in the fiber is reflected back inside the fiber. This is called total internal reflection, which is the foundation upon which optical fiber is constructed. Total internal reflection causes the light rays in the fiber to bounce off the core-cladding boundary and continue its journey towards the far end of the fiber. The light will follow a zigzag path through the core of the fiber.

A fiber that meets the first condition can be easily created. In addition, the angle of incidence of the light rays that enter the core can be controlled. Restricting the following two factors controls the angle of incidence:

- **The numerical aperture of the fiber** – The numerical aperture of a core is the range of angles of incident light rays entering the fiber that will be completely reflected.

- **Modes** – The paths which a light ray can follow when traveling down a fiber.

By controlling both conditions, the fiber run will have total internal reflection. This gives a light wave guide that can be used for data communications.

**Self Learning Exercises :**

4 Why are pairs of wires twisted together in UTP cable :

(a) twisting of wires makes it less expensive

(b) twisting of wires makes it thinner

(c) twisting of reduces noise problems

(d) makes six pairs fit in space of four pairs

5 Which material is considered electrical semiconductor :

(a) Air (b) Silicon

(c) Glass (d) Gold

6 Which of the following are the parts of fiber optic cable :

(a) Clad (b) Braid

(c) Core (d) All of the above

## 1.5 NETWORKING ESSENTIALS

### 1.5.1 Repeaters

A repeater connects two segments of your network cable. It retimes and regenerates the signals to proper amplitudes and sends them to the other segments. When talking about, ethernet topology, you are probably talking about using a hub as a repeater. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row. Repeaters work only at the physical layer of the OSI network model.

### 1.5.2 Hubs

Hubs are actually multiport repeaters. The difference between hubs and repeaters is usually the number of ports that each device provides. A typical repeater usually has two ports. A hub generally has from 4 to 24 ports. Hubs are most commonly used in Ethernet 10BASE-T or 100BASE-T networks.

Hubs come in three basic types:

- **Passive** – A passive hub serves as a physical connection point only. It does not manipulate or view the traffic that crosses it. It does not boost or clean the signal. A passive hub is used only to share the physical media. A passive hub does not need electrical power.
- **Active** – An active hub must be plugged into an electrical outlet because it needs power to amplify a signal before it is sent to the other ports.
- **Intelligent** – Intelligent hubs are sometimes called smart hubs. They function like active hubs with microprocessor chips and diagnostic capabilities. Intelligent hubs are more expensive than active hubs. They are also more useful in troubleshooting situations.

Devices attached to a hub receive all traffic that travels through the hub. If many devices are attached to the hub, collisions are more likely to occur. A collision occurs when two or more workstations send data over the network wire at the same time. All data is corrupted when this occurs. All devices that are connected to the same network segment are members of the same collision domain.

Sometimes hubs are called concentrators since they are central connection points for Ethernet LANs.

### 1.5.3 Switches

Switches occupy the same place in the network as hubs. Unlike hubs, switches examine each packet and process it accordingly rather than simply repeating the signal to all ports. Switches map the Ethernet addresses of the nodes residing on each network segment and then allow only the necessary traffic to pass through the switch. When a packet is received by the switch, the switch examines the destination and source hardware addresses and compares them to a table of network segments and addresses. If the segments are the same, the packet is dropped ("filtered"); if the segments are different, then the packet is "forwarded" to the proper segment. Additionally, switches prevent bad or misaligned packets from spreading by not forwarding them.

Filtering of packets, and the regeneration of forwarded packets enables switching technology to split a network into separate collision domains. Regeneration of packets allows for greater distances and more nodes to be used in the total network design, and dramatically lowers the overall collision rates. In switched networks, each segment is an independent collision domain. In shared networks all nodes reside in one, big shared collision domain.

Easy to install, most switches are self learning. They determine the Ethernet addresses in use on each segment, building a table as packets are passed through the switch. This "plug and play" element makes switches an attractive alternative to hubs.

Switches can connect different networks types (such as Ethernet and Fast Ethernet) or networks of the same type. Many switches today offer high-speed links, like Fast Ethernet or FDDI, that can be used to link the switches together or to give added bandwidth to important servers that get a lot of traffic. A network composed of a number of switches linked together via these fast uplinks is called a "collapsed backbone" network.

Dedicating ports on switches to individual nodes is another way to speed access for critical computers. Servers and power users can take advantage of a full segment for one node, so some networks connect high traffic nodes to a dedicated switch port.

Full duplex is another method to increase bandwidth to dedicated workstations or servers. To use full duplex, both network interface cards used in the server or workstation, and the switch must support full duplex operation. Full duplex doubles the potential bandwidth on that link, providing 20 Mbps for Ethernet and 200 Mbps for Fast Ethernet.

**Bridge**

A bridge reads the outermost section of data on the data packet, to tell where the message is going. It reduces the traffic on other network segments, since it does not send all packets. Bridges can be programmed to reject packets from particular networks. Bridging occurs at the data link layer of the OSI model, which means the bridge cannot read IP addresses, but only the outermost hardware address of the packet. In our case the bridge can read the ethernet data which gives the hardware address of the destination address, not the IP ad-

dress. Bridges forward all broadcast messages. Only a special bridge called a translation bridge will allow two networks of different architectures to be connected. Bridges do not normally allow connection of networks with different architectures. The hardware address is also called the MAC (media access control) address. To determine the network segment a MAC address belongs to, bridges use one of:

- **Transparent Bridging** - They build a table of addresses (bridging table) as they receive packets. If the address is not in the bridging table, the packet is forwarded to all segments other than the one it came from. This type of bridge is used on Ethernet networks.
- **Source route bridging** - The source computer provides path information inside the packet. This is used on Token Ring networks.

### 1.5.4 Router

A router is used to route data packets between two networks. It reads the information in each packet to tell where it is going. If it is destined for an immediate network it has access to, it will strip the outer packet, readdress the packet to the proper Ethernet address, and transmit it on that network. If it is destined for another network and must be sent to another router, it will re-package the outer packet to be received by the next router and send it to the next router. The section on routing explains the theory behind this and how routing tables are used to help determine packet destinations. Routing occurs at the network layer of the OSI model. They can connect networks with different architectures such as Token Ring and Ethernet. Although they can transform information at the data link level, routers cannot transform information from one data format such as TCP/IP to another such as IPX/SPX. Routers do not send broadcast packets or corrupted packets. If the routing table does not indicate the proper address of a packet, the packet is discarded.

There is a device called a brouter which will function similar to a bridge for network transport protocols that are not routable, and will function as a router for routable protocols. It functions at the network and data link layers of the OSI network model.

### 1.5.5 Gateways

A gateway can translate information between different network data formats or network architectures. It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers. Most gateways operate at the application layer, but can operate at the network or session layer of the OSI model. Gateways will start at the lower level and strip information until it gets to the required level and repackage the information and work its way back toward the hardware layer of the OSI model. To confuse issues, when talking about a router that is used to interface to another network, the word gateway is often used. This does not mean the routing machine is a gateway as defined here, although it could be.

### 1.5.6 NIC (Network interface Card)

Each network card, called a network interface card **(NIC)** has a built in hardware address programmed by its manufacturer. This is a 48 bit address and should be unique for each card. This address is called a media access control **(MAC)** address.

Network Interface Cards, commonly referred to as NICs, are used to connect a PC to a network. The NIC provides a physical connection between the networking cable and the computer's internal bus. Different computers have different bus architectures. PCI bus

slots are most commonly found on 486/Pentium PCs and ISA expansion slots are commonly found on 386 and older PCs. NICs come in three basic varieties: 8-bit, 16-bit, and 32-bit. The larger the number of bits that can be transferred to the NIC, the faster the NIC can transfer data to the network cable. Most NICs are designed for a particular type of network, protocol, and medium, though some can serve multiple networks.

Many NIC adapters comply with plug-and-play specifications. On these systems, NICs are automatically configured without user intervention, while on non-plug-and-play systems, configuration is done manually through a set-up program and/or DIP switches.

Cards are available to support almost all networking standards. Fast Ethernet NICs are often 10/100 capable, and will automatically set to the appropriate speed. Gigabit Ethernet NICs are 10/100/1000 capable with auto negotiation depending on the user's Ethernet speed. Full duplex networking is another option where a dedicated connection to a switch allows a NIC to operate at twice the speed.

Self learning exercises:

7 What is the function of router?

(a) It routes traffic from one LAN segment to another

(b) It regenerates the data

(c) It transforms the data from one format to another

(d) None of the above

8 What is multiport repeater called as?

(a) Hub (b) Switch

(c) Router (d) Gateway

9 What is the Gateway?

(a) It is used to connect two totally dissimilar networks

(b) It regenerates and retransmits signals from one network to another

(c) It acts as a bridge between two networks

(d) It is used to change the format of the message

## 1.6 SUMMARY

Computer networks developed in response to business and government computing needs. Applying standards to network functions provided a set of guidelines for creating network hardware and software and provided compatibility among equipment from different companies. Information could move within a company and from one business to another.

Network devices, such as repeaters, hubs, bridges, switches and routers connect host devices together to allow them to communicate. Protocols provide a set of rules for communication.

The amount of information that can flow through a network connection in a given period of time is referred to as bandwidth. Network bandwidth is typically measured in thousands of bits per second (kbps), millions of bits per second (Mbps), billions of bits per second (Gbps) and trillions of bits per second (Tbps). The theoretical bandwidth of a network is an important consideration in network design. If the theoretical bandwidth of a network connection is known, the formula T=S/BW (transfer time = size of file / bandwidth) can be

used to calculate potential data transfer time. However the actual bandwidth, referred to as throughput, is affected by multiple factors such as network devices and topology being used, type of data, number of users, hardware and power conditions.

Intranets are only available to users who have access privileges to the internal network of an organization. Extranets are designed to deliver applications and services that are Intranet based to external users or enterprises.

## 1.7 GLOSSARY

- **Attenuation** - signal loss due to impedance
- **Backbone** - Main cable used to connect computers on a network.
- **Bandwidth** - Indicates the amount of data that can be sent in a time period. Measured in Mbps which is one million bits per second.
- **Baseband** - Data bits are defined by discrete signal changes.
- **Bridge** - Read the outermost section of data on the data packet, to tell where the message is going. It reduces the traffic on other network segments, since it does not send all packets but only sends packets intended for that segment they are attached to.
- **Broadband** - Uses analog signals to divide the cable into several channels with each channel at its own frequency. Each channel can only transmit one direction.
- **Broadcast** - A transmission to all interface cards on the network.
- **Brouter** - Will function similar to a bridge for network transport protocols that are not routable, and will function as a router for routable protocols.
- **EMI interference)** - Interference by electromagnetic signals that can cause reduced data integrity **(electromagnetic** and increased error rates on transmission channels.
- **Media** - The hardware method used to connect computers over a network. The three main types are copper cable, fiber optic cable, and wireless.
- **Protocol** - A set of standards sets of standards that define all operations within a network. There are various protocols that operate at various levels of the OSI network model such as transport protocols include TCP, SPX.
- **Repeater** - Used on a network to regenerate signals to be sent over long distances or tie computers together on a network.
- **Router** - Routes data packets between two networks. It reads the information in each packet to tell where it is going.
- **Thicknet** - Half inch rigid cable. Maximum cable length is 500 meters. Transmission speed is 10Mbps. Expensive and is not commonly used. (RG-11 or RG-8).

- **Thinnet** - Thinnet uses a British Naval Connector (BNC) on each end. Thinnet is part of the RG-58 family of cable*. Maximum cable length is 185 meters. Transmission speed is 10Mbps.
- **Token Ring** - A network architecture developed by IBM which sends tokens around a ring of computers to allow media access. Standardized to IEEE 802.5
- **Topology** - The shape of the physical connection of a network with regard to repeaters and networked computers. The three main types are ring, bus, and star.
- **VPN** - Virtual Private Networking. The function of VPN is to allow two computers or networks to talk to each other over a transport media that is not secure, but the network is made secure by VPN security protocols.

## 1.8 FURTHER READINGS

1. Data Communication & Networking - Behrouz Forouzan
2. CCNA (Cisco Certified Network Associate) First year Companion Guide - Cisco Press
3. Computer Networks – Andrew Tanenbaum; Prentice Hall India(PHI)

## 1.9 ANSWERS TO THE SELF LEARNING EXERCISES

1. d
2. c
3. c
4. c
5. b
6. d
7. a
8. a
9. a

## 1.10 UNIT END QUESTIONS

1. How do guided media differ from unguided media.
2. Name the advantages of optical fiber over twisted-pair and coaxial cable.
3. Why is coaxial cable superior to twisted pair cable?
4. What is reflection? How is total internal reflection used in fiber optics for communication?
5. What is major advantage of shielded twisted pair over un-shielded twisted Pair?
6. What is the device Router used for?
7. What is the function of Repeater?
8. Differentiate between Switch and Bridge?
9. What is the significance of NIC?
10. List out various Internet applications.