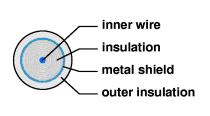
**CLASS: LOWER SIXTH**

**SUBJECT: ICT**

**DURATION: 4Hr**

1. **Coaxial cable**



To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-Neill-Concelman, or BNC connector.

* **Advantages:**
* Inexpensive
* Easy to wire
* Easy to expand
* Moderate level of EMI immunity
* **Disadvantage:**
* Single cable failure can take down an entire network

1. **Twisted pair cable**
2. **Unshielded Twisted Pair**

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. RJ stands for registered jack. There are five levels of UTP:

**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 can be connected as straight through or crossover. A straight-thru cable has identical ends. A crossover cable has different ends.

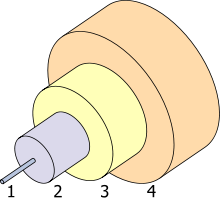
* **Advantages:**
* Easy installation
* Capable of high speed for LAN
* Low cost
* **Disadvantages :**
* Short distance due to attenuation (Signals loose power in time.)

1. **Shielded Twisted Pair**

* **Advantage**
* Faster than UTP and coaxial
* **Disadvantage**
* More expensive than UTP and coaxial
* More difficult installation
* High attenuation rate

1. **Fiber optic cable**

1. Core: 8 µm diameter.  
2. Cladding: 125 µm diameter.  
3. Buffer: 250 µm diameter.  
 4. Jacket: 400 µm diameter.

[](http://en.wikipedia.org/wiki/File:Singlemode_fibre_structure.svg)

Two types: single mode and multi-mode.



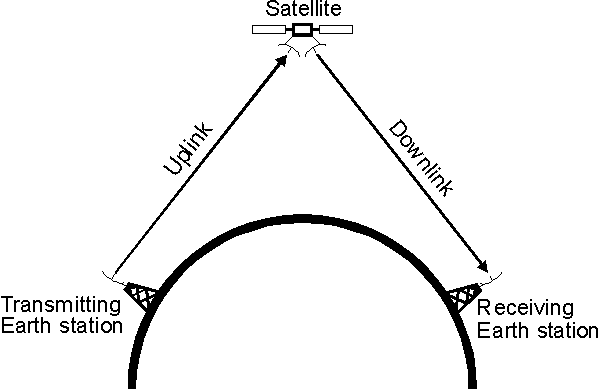
The light source can be LED (light emitting diode) or LD (laser diode)

* **Advantages**
* Fast
* Larger bandwidth
* No EMI interference, no cross-talk , no attenuation
* Impossible to tap
* **Disadvantages**
* Very costly
* Hard to install
* Requires special connection techniques (electro-optic transducers to convert from electric to optic)

1. **Unguided Media**

Unguided media do not use physical means to define the path to be taken. They provide a means for transmitting electromagnetic waves but do not guide them. They are also called unbounded media. Examples of unguided media are infrared waves, radio waves, microwaves and satellite.

* Infrared: uses transmitters/receivers (transceivers) that modulate non-coherent infrared light. Infrared signals do not penetrate walls as such transceivers must be within line-of-sight either directly or via reflection. Line of sight is a type of propagation that can transmit and receive data only where transmit and receive stations are in view of each other without any sort of an obstacle between them.
* Radio waves: radio systems transmit signals by modulation of electromagnetic waves with frequencies below that of visible light. Radio waves carry information by systematically changing some property of the radiated waves such as amplitude (AM radio), frequency (FM radio) and phase. Radiowaves are omnidirectional.This means that signals spread out in all directions and can be received by many antennas.
* Microwave: microwaves are electromagnetic radiations beyond the frequency range of radio and television. Microwaves travel in a straight line and are line-of-sight. Due to the earth’s curvature long distance microwave transmissions require directional antennas (repeaters) to be used at intervals of 25 to 30 kilometers between the transmitting and receiving end. A microwave system that uses land-based antennas is known as terrestrial microwave system.
* Satellite: the problem posed by the earth’s curvature to terrestrial microwave systems can be solved by using satellite systems. Satellite systems use communication satellites. A communication satellite is a microwave relay station placed in outer space. A microwave signal is transmitted from earth to the satellite which amplifies the signal and sends it back to earth. The earth station transmits the signal to the satellite on an up-link, on one frequency and the satellite repeats those signals on a down link which is on another frequency.

****

## Advantages of microwave systems

* No cables needed
* Multiple channels available
* Wide bandwidth

## Disadvantages

* Line-of-sight will be disrupted if any obstacle, such as new buildings, are in the way
* Signal absorption by the atmosphere. Microwaves suffer from attenuation due to atmospheric conditions.
* Towers are expensive to build
* Bluetooth
* Wi-Fi
* WiMax

1. **Transfer Checks**

Network data transmissions often produce errors, such as toggled, missing or duplicated bits. As a result, the data received might not be identical to the data transmitted, which is obviously a bad thing. Because of these transmission errors, network protocols very often use error-detection codes. Examples of error-detection codes include parity checking, checksums and cyclic redundancy checks.

* 1. **Parity Checking**

Parity checking refers to the process of using a parity bit to check that data has been transmitted accurately. A parity bit is an extra bit transmitted with a data unit that will be used to check its integrity. There are two types of parity: odd parity and even parity. In odd parity, the parity bit is added such that the total number of bits at 1, in the data unit, is an odd number. In even parity, the parity bit is added so that the total number of 1s is an even number.

Example: What are the parity bits for the following data units in odd parity?

1. 111011011 ii) 001001010 iii) 110101010

Example 2: What are the parity bits for the following data units in even parity?

1. 011010100 ii) 111001011 iii) 100111000
   1. **Checksum**

A checksum or hash sum is a count of the number of bits in a transmission unit that is included with the unit for the purpose of detecting errors that may have been introduced during transmission. The checksum or hash sum may be computed according to the number of set or unset bits in the message. On reception, the receiver applies the same checksum function/algorithm to the message. If the checksum obtained matches the one sent, the transmission is considered to be successful and error-free.

* 1. **Cyclic Redundancy Check**

A CRC is an error-detection code in which each segment of theoriginal message is combined with additional bits to make a binary number that is divisible by some previously chosen divisor.

* is the length of the message we want to send, i.e., the number of information bits.
* is the total length of the message we will end up sending the information bits followed by the check bits. Peterson and Brown call this a code polynomial.
* is the number of check bits. It is also the degree of the generating polynomial. The basic (mathematical) idea is that we're going to pick the n-k check digits in such a way that the code polynomial is divisible by the generating polynomial. Then we send the data, and at the other end we look to see whether it's still divisible by the generating polynomial; if it's not then we know we have an error, if it is, we hope there was no error.

1. **Peripheral Device Control**
2. **Buffer**

A buffer is an area of memory used to temporarily store data while it is being moved from one place to another. Buffers are used to compensate for differences in rate of flow of data or time of occurrence of events, when transferring data from one device to another. Routers use buffers to route data packets on the Internet. When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, then the packet is forwarded.

1. **Interrupt**

An interrupt is a signal to the processor emitted by hardware or software indicating an event that needs immediate attention. An interrupt alerts the processor of a high-priority condition requiring the interruption of the current task the processor is executing. Interrupts are used to handle such events as data receipt from a modem or network, or a key press or mouse movement.

1. **Polling**

Polling is the process by which the central computer or communications controller in a network, "polls" or asks each device in the network if it has a message to send and then allows each in turn to transmit data. Access and control of star network typically is maintained by a polling system.

1. **Handshaking:**

Handshaking is the process by which two devices initiate communications. It begins when one device sends a message to another device indicating that it wants to establish a communications channel. The two devices then send several messages back and forth that enable them to agree on a communications protocol.

1. **Communication Protocols**

A protocol is a set of rules and conventions that govern how devices on a network communicate. Protocols set message formats and procedures that allow machines and application programs to exchange information. These rules must be followed by each machine involved in the communication in order for the receiving host to be able to understand the message. The need for a protocol is obvious: it allows different computers from different vendors and with different operating characteristics to ‘speak the same language’. A protocol may be physical or logical.

* 1. **Physical Protocols**

Physical protocols are concerned with how a device connects to a medium. They ensure that a device connected to a medium can transmit through the medium. They make sure that the layout of pins on the connectors is the same and that devices are correctly connected and configured. Few examples of physical protocols are 802.11 for Wi-Fi connections and DSL for broadband.

* 1. **Logical Protocols**

Logical protocols are concerned with data handling. They ensure that data are in the right format for the application, the bit rates match at both ends, and the same error correction is used. Examples of logical protocols are TCP/IP, HTTP, POP3, FTP, SMTP and WAP.

* **TCP:** stands for Transmission Control Protocol. It is a connection-based Internet protocol that supports reliable data transfer connections. Data packets are verified using checksums and retransmitted if they are missing orcorrupted. The application plays no part in validating the transfer.
* **IP:** stands for Internet Protocol. It specifies the format of packets and the addressing scheme.
* **UDP:** stands for User Datagram Protocol. It is a connectionless Internet protocol that is designed for network efficiency and speed at the expense ofreliability.Data packets are sent without testing to verify whetherthey actually arrive at the destination, not whether they were corrupted in transit. It is up to the applicationto determine these factors and request retransmissions.
* **HTTP:** stands for Hypertext Transfer Protocol. It is a standard method of publishing information as hypertext in HTML format on the Internet. In other words, HTTP defines how messages are formatted and transmitted over the World Wide Web. Web addresses or URLs usually begin with http indicating that the protocol used is HTTP.
* **HTTPS:** stands for Hypertext Transfer Protocol Secure. It is the protocol used for accessing a secure web server, whereby all data transferred are encrypted.
* **POP:** stands for Post Office Protocol. It is a standard protocol for delivering e-mails to personal computers.
* **FTP:** stands for File Transfer Protocol. It is a standard for transferring files between a server and a client on a TCP/IP network.
* **SMTP:** stands for Simple Mail Transmission Protocol. It defines a basic service for electronic mails. It is used for sending e-mails between servers.
* **WAP:** stands for Wireless Application Protocol. It is a protocol which runs on mobile phones and provides a universal open standard for bringing Internet content to mobile phones and other wireless devices.

1. **Machine Identification and Communication Ports**

Every node on a network be it a server or network station has a unique identity. The type of identity a node has is determined by the protocols running on the network. Two types of addresses exist for identifying a node on a network: MAC and IP addresses.

* 1. **Media Access Control (MAC) Address**

Every node on a network has a network interface card or network adapter, which has a media access control address. MAC address is a built-in number consisting of 12 hexadecimal digits that uniquely and permanently identifies the network adapter. For example,00-14-22-DA-67-15. Under Windows, the MAC address can be displayed by typing *ipconfig/all* at a Command prompt.

* 1. **IP Address**

An IP address is a unique identifying number given to every single computer on a TCP/IP network. All computers, desktops, laptops, PDAs, phones, tablet PCs connected to the Internet, have IP addresses by which they are identified. Two versions of IP addresses are available: IPv4 that uses 32 bits and IPv6 that uses 128 bits.

An IPv4 is made up of four sets of numbers separated by periods such as 123.23.168.22. Each of the four numbers separated by periods can be any number from 0 to 255, making for a total of 4.3 billion potential IPv4 addresses (i.e.).

An IPv6 has eightsets of numbers separated by colons such as 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

IP addresses are assigned manually (by an administrator) or automatically (by DHCP or APIPA), unlike MAC addresses that are assigned during manufacture. MAC addresses are physical addresses while IP addresses are logical addresses.

* 1. **Communication Ports**

A computer has a single physical connection to the network. All data destined for a particular computer arrives through that connection. However, the data may be intended for different applications running on the computer. To identify the application for which the data is intended, communication ports are used. A communication port is a 16-bit number that identifies an application on the Internet. Popular Internet application protocols are associated with ***well-known ports*** and ***well-known services***. Examples are port 80 for accessing the World Wide Web (HTTP), port 21 for file transfer (FTP), port 25 for sending emails (SMTP) and port 110 for receiving emails (POP).

1. **The Open Systems Interconnection Model**

The Open Systems Interconnection (OSI) reference model or more commonly the OSI model is an ISO standard that defines how network communications take place. The OSI model divides network communications into seven layers. Each layer is responsible for carrying out specific functions when transmitting data on the network. The table below shows the layered architecture of the OSI reference model.

|  |  |  |
| --- | --- | --- |
| **No.** | **Layer Name** | **Examples of Protocols** |
| 7 | Application | HTTP, SMTP, FTP, TELNET |
| 6 | Presentation | XDR, ANS.1, SMB |
| 5 | Session | X.225, RPC, NetBIOS, |
| 4 | Transport | TCP, UDP, SPX, |
| 3 | Network | IP, X.25 |
| 2 | Data Link | Ethernet, Token Ring, PPP, ISDN |
| 1 | Physical | Electricity, Radio, Laser |

The OSI reference model

**Layer 7: Application**

It provides network services directly to the user’s applications such as a web browser or e-mail client. This layer is said to be “closest to the user”. Examples of protocols that operate at this layer are: TELNET, HTTP, FTP, SMTP and POP.

**Layer 6: Presentation**

The Presentation layer represents the data in a particular format to the Application layer. It defines encryption, compression, conversion and other coding functions. Examples of specifications defined at this layer are: GIF, JPEG, MPEG, MIME and ASCII.

**Layer 5: Session**

It establishes, maintains and terminates end-to-end connections (session) between two applications on two network nodes. It controls the dialogue between the source and destination nodes, which node can send when and for how long. Examples of protocols that operate on this layer are: RPC, NETBIOS and X.225

**Layer 4: Transport**

It is responsible for end-to-end delivery of entire messages. It allows data to be transferred reliably and uses sequencing to guarantee that it will be delivered in the same order it was sent. It also provides services such as error checking and flow control. Examples of protocols at this layer are: TCP, UDP, NETBEUI and SPX.

**Layer 3: Network**

It is responsible for path determination, routing, and the delivery of packets across internetworks. It is also responsible for addressing (also known as logical addressing) for example IP addressing. Examples of protocols at this layer are: IP, IPX and ICMP.

Examples of devices that operate at this level are Layer-3 switches and routers. WAPs (wireless access points) with built-in routing capabilities also act at this layer.

**Layer 2: Data Link**

It is responsible for reassembling bits taken off the wire by the physical layer to frames and makes sure they are in the correct order and requests retransmission of frames in case an error occurs. It provides error checking by adding CRC to the frame. Examples of protocols at this layer are: Ethernet, Token Ring, PPP and ISDN.

Examples of devices that operate at this layer are: switches, bridges, NICs and WAPs (Wireless Access Points).

**Layer 1: Physical**

This layer communicates directly with the communication medium. It is responsible for activating, maintaining and deactivating the physical link. It defines electrical and optical signaling, voltage levels, data transmission rates, as well as mechanical specifications such as cable lengths, and connectors, the amount of pins and their functions. Examples of devices that operate at this layer are: hubs, repeaters, and NICs.

These layers can be recalled using the following mnemonics: All People Seem To Need Data Processing. (Layers 7 - 1)

1. **The TCP/IP Protocol Suite**