INITIATIVES DON BOSCO
INSTITUT DON BOSCO KABARONDO TSS
TEL: 0788670647/0790909669
B.P: 50 Kibungo
Email: dbtikabarondo@gmail.com

Module: GENBN401_ BASICS OF NETWORKING

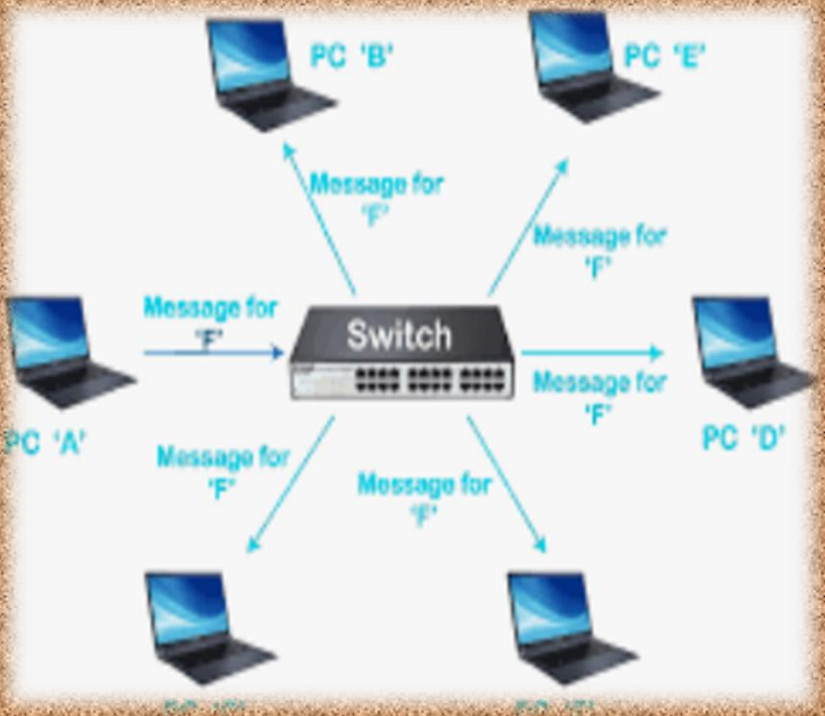
COMPETENCE: BASICS OF NETWORKING

RQF Level: 4

CREDIT: 7

SECTOR: ICT

TRADE: SOD



PURPOSE OF THE MODULE:

This module Describes the skills, Knowledge and attitude required to Perform basic Networking. This module intended to prepare students Pursuing TVET in Level 4 Software Development. At the end of this module, the students will be able to Establish network media connectivity, Perform Basic Network Configuration, Maintain Network system.

Your network is proportional to your net worth !

Table of Contents

LEARNING OUTCOME 1 ESTABLISH NETWORK MEDIA CONNECTIVITY

Indicative content 1.1 – Identification of Network requirements.

Topic1. Description of Network concepts and Technologies

A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes.

- **Elements of Network**

The modern data network has become a critical asset for many industries. Most basic data networks are designed to connect users and enable them to access various resources, like the Internet and other computers connected to the network. Networks are comprised of four basic elements: **hardware, software, protocols and the connection medium.**

1. Hardware

The backbone of any network is the hardware that runs it. Network hardware includes network cards, routers or network switches, modems and Ethernet repeaters. Without this hardware, computers have no means of accessing a network.

2. Software

Network software is a foundational element for any network. This type of software helps administrators deploy, manage and monitor a network. The traditional networks are made up of specialized hardware, such as routers and switches that bundle the networking software into the solution.

3. Protocols

There are some defined rules and conventions for communication between network devices. These are called Protocols. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into sent and received messages.

Protocols may be of 3 types:

1. Internet Protocols
2. Wireless Network Protocols
3. Network Routing Protocols

4. Transmission medium:

The means through which we send our data from one place to another is known as Transmission medium.

Signals are used to represent data by computers and other telecommunication devices. The signals (i.e., data or information) are transmitted in the form of electromagnetic energy from one device to another. These signals travel through vacuum, air or other transmission mediums to move from one point to another (from sender to receiver).

Transmission medium is of two types:

(i) Wired or Guided: For example, Twisted Pair Cable, Coaxial Cable and Optical Fiber Cable.

(i) Wireless or Unguided: For example, Radio waves, Microwaves and Infrared.

❖ Classification of network

✓ Classifying network by components roles

Based on network components, there two classification of computer network which are the following:

1. **Client-Server Network:** This model is broadly used network model. In Client-Server Network, Clients and server are differentiated, specific server and clients are present. In Client-Server Network, Centralized server is used to store the data because its management is centralized. In Client-Server Network, Server respond the services which is request by Client.

2. Peer-to-Peer Network: This model does not differentiate the clients and the servers, in this each and every node is itself client and server. In Peer-to-Peer Network, Each and every node can do both request and respond for the services.

The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN and WAN are the three major types of the network designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover.

✓ Classifying network by geographical area

1. **Local Area Network (LAN) –**LAN or Local Area Network connects network devices in such a way that personal computer and workstations can share data, tools and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol.

Data transmits at a very fast rate as the number of computers linked are limited. By definition, the connections must be high speed and relatively inexpensive hardware (Such as hubs, network adapters and Ethernet cables). LANs cover smaller geographical area (Size is limited to a few kilometers) and are privately owned. One can use it for an office building, home, hospital, schools, etc.

2. **Metropolitan Area Network (MAN) –**MAN, or Metropolitan Area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need a high-speed connectivity. Speeds of MAN ranges in terms of Mbps.

The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN is moderate. Devices used for transmission of data through MAN are: Modem and Wire/Cable. Examples of a MAN are the part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

3. **Wide Area Network (WAN) –**WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LANs via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive.

There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long distance transmission, the noise and error tend to be more in WAN.

- **Benefits of Network**

Setting up a computer network is a fast and reliable way of sharing information and resources within a business. It can help you make the most of your IT systems and equipment.

Advantages of computer networking

Main benefits of networks include:

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

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

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

Cost benefits of computer networking

Storing information in one centralized database can also help you reduce costs and drive efficiency**.** For example:

- staff can deal with more customers in less time since they have shared access to customer and product databases
- you can centralize network administration, meaning less IT support is required
- you can cut costs through sharing of peripherals and internet access

You can reduce errors and improve consistency by having all staff work from a single source of information. This way, you can make standard versions of manuals and directories available to them, and back up data from a single point on a scheduled basis, ensuring consistency

Disadvantages

1. Purchasing the network cabling and file servers can be expensive.
2. Managing a large network is complicated, requires training and a network manager usually needs to be employed.

3. If the file server breaks down the files on the file server become inaccessible. Email might still work if it is on a separate server. The computers can still be used but are isolated.
4. Viruses can spread to other computers throughout a computer network.
5. There is a danger of hacking, particularly with wide area networks. Security procedures are needed to prevent such abuse, eg a firewall.

❖ **Application of network**

A network application is a software program or service that relies on network resources to perform specific functions, enabling communication, data sharing, and collaboration among devices connected to a network.

○ **Types of Network Applications**

There are several types of network applications, each designed to serve specific purposes and meet diverse communication and data-sharing needs:

1. **Web Browsers:**

   Examples: Google Chrome, Mozilla Firefox, Microsoft Edge
2. **Email Clients:**

   Examples: Microsoft Outlook, Apple Mail, Gmail
3. **File Transfer Protocols:**

   Examples: FTP (File Transfer Protocol), SFTP (Secure File Transfer Protocol)
4. **Messaging Apps:**

   Examples: WhatsApp, Slack, Microsoft Teams
5. **Video Conferencing Tools:**

   Examples: Zoom, Microsoft Teams, Cisco Webex
6. **Remote Desktop Applications:**

Examples: TeamViewer, AnyDesk, Remote Desktop Protocol (RDP)

○ **Network Applications**

1. **Network Architecture and Topology:** Network architecture defines the design and layout of the network, including its physical and logical structure. Topology refers to the arrangement of network elements and their interconnections. Common topologies include star, mesh, and hybrid.

2. **OSI Model and TCP/IP:** The OSI (Open System Interconnection) h`

model provides a framework for understanding network interactions in seven layers, from the physical layer to the application layer.

3. **Network Security:** Ensuring the security of network applications involves implementing firewalls, encryption (SSL/TLS), and authentication mechanisms to protect data and prevent unauthorized access.

4. **Data Transfer and Latency:** Efficient data transfer is critical for network performance. Protocols like TCP and UDP manage data transmission, balancing reliability and speed.

5. **API and Interconnection:** APIs (Application Programming Interfaces) enable different software applications to communicate and share data seamlessly.

6. **Network Services and IoT:** Network services include DNS, DHCP, and other essential services that support the functionality of network applications.

7. **Case Studies and Metrics:** Analyzing case studies provides insights into practical applications and challenges in networking.

8. **Cloud Services and AWS (AWS stands for Amazon web services):** Cloud providers like AWS offer scalable network services that support modern applications.

❖ **Network Technology**

Networking technology allows for the exchange of data between large and small information systems used primarily by businesses and educational institutions. **Network technicians,** also known as network engineers or specialists, are responsible for the configuration, installation and troubleshooting of the technology used to transmit digital information, including audio, visual and data files.

1. **IEEE802.3 Ethernet**

Ethernet Operation

Ethernet is the most widely used LAN technology used today.
Ethernet operates in the data link layer and the physical layer. It is a family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards. Ethernet supports data bandwidths of:

- 10 Mb/s

- 100 Mb/s
- 1000 Mb/s (1 Gb/s)
- 10,000 Mb/s (10 Gb/s)
- 40,000 Mb/s (40 Gb/s)
- 100,000 Mb/s (100 Gb/s)

Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies. For the Layer 2 protocols, as with all 802 IEEE standards, Ethernet relies on the two separate sub layers of the data link layer to operate, the Logical Link Control (LLC) and the MAC sub layers.

2. **IEEE 802.5 Token ring**

The foundation of a token ring is the IEEE 802.5 network of the "Institute of Electrical and Electronics Engineers" from 1985, in which all participants of the "Local Area Network" (LAN) are connected to form a logical ring. Usually, token ring topologies have a transmission speed of 4 or 16 Mbit/s, but in theory speeds of 100 Mbit/s or 1 Gbit/s are also possible.

A token ring works somewhat differently to other ring topologies, which is why it's said that this technology is based only logically on a ring topology. The token ring topology uses **Mult station Access Units (MAUs),** which allow a star-shaped connection of the connections involved. The distributor is a node that is connected to all computers on the network. There is no direct connection between the individual computers.

3. **Token passing**

To avoid chaos(disorder), the token passing procedure is used. This method ensures that not all participants send data to the network at the same time.

4. **IEEE802.8 Fiber optic**

This is the technology of IEEE that introduced the use of Fiber Optic cable that enables an Internet service provider to provide higher bandwidth speeds and support more services such as Internet, phone, and TV in large distance.

5. **IEEE802.11 Wireless**

802.11 and 802.11x refers to a family of specifications developed by the IEEE for **w**ireless **LAN** (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

❖ **Network topology types**

A network topology is the physical and logical arrangement of nodes and connections in a network.

A **network topology** is the basic design of a computer network. It is very much like a map of a road. It details how key network components such as nodes and links are interconnected.

A topology of a network is key to determining its performance. Network topology is the way a network is arranged, including the physical or logical description of how links and nodes are set up to relate to each other.

1. Types of Network Topology

The way a network is arranged can make or break network functionality, connectivity, and protection from downtime. Ask yourself a question "**What is network topology**?" This question can be answered with an explanation of the **two categories** in the network topology.

1. **Physical** – The physical network topology refers to the actual connections (wires, cables, etc.) of how the network is arranged. Setup, maintenance, and provisioning tasks require insight into the physical network.
2. **Logical** – The logical network topology is a higher-level idea of how the network is set up, including which nodes connect to each other and in which ways, as well as how data is transmitted through the network. Logical network topology includes any virtual and cloud resources.

✓ **Types of Physical Network Topology**

There are **six types** of topologies in computer networks:

1. BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.

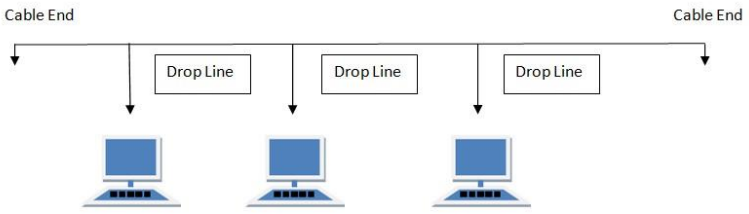


Fig.1: Bus topology

Features of Bus Topology

1. It transmits data only in one direction.

2. Every device is connected to a single cable

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to another network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

2. RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.

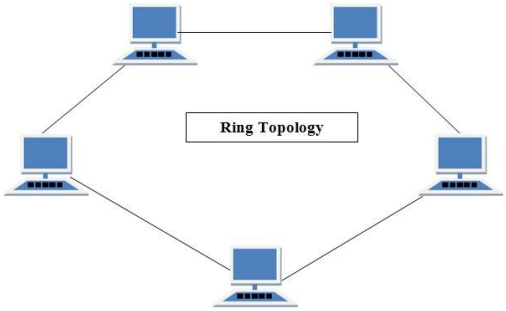


Fig.2: Star topology

Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them.

4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node. **Advantages of Ring Topology**
5. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
6. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

3. **STAR Topology**

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

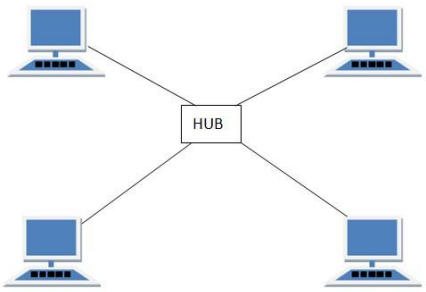


Fig.3: Star topology

Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fiber or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.

4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails, then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

4. MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other.

Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are:

1. Routing (disorder)
2. Flooding (order)

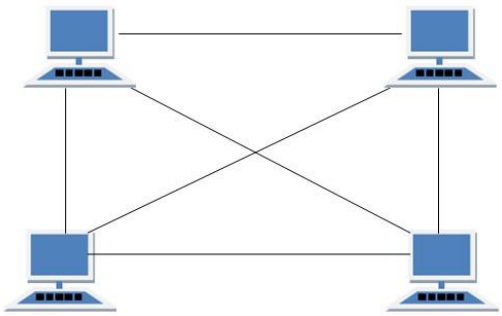


Fig.4: Mesh topology

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology

1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration are difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

5. TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

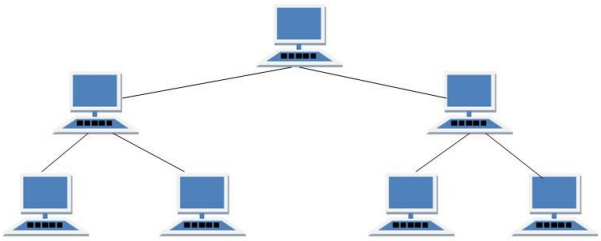


Fig.5: Tree topology

Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

- ✓ Heavily cabled.
- ✓ Costly.
- ✓ If more nodes are added maintenance is difficult.
- ✓ Central hub fails, network fails.

6. HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example, if in an office in one department ring topology is used and, in another star, topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

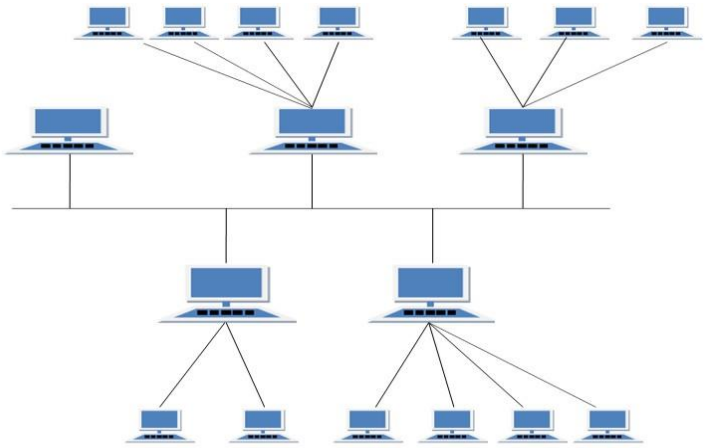


Fig.6: Hybrid topology

Features of Hybrid Topology

1. It is a combination of two or more topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

1. Reliable as Error detecting and troubleshooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

❖ Identification of Network devices, Components and their Functions

✓ Classification of network device

There are three classes of network devices which are:

1. Interconnection devices
2. Access devices

3. End devices

1. Interconnection devices

Interconnection device is any device that can enable computers to exchange data on a network.

a. **Repeater**

Repeaters are non-intelligent network devices that receive a signal through one port. They regenerate that signal and then transmit the signal again on all remaining ports.

Figure 1. Repeater

b. **Bridge**

Unlike repeaters, a bridge can extend the capacity as well as the length of a network because each port on a bridge has a MAC (Media Access Control) address. They are used to connect two or more LANs of the same type, e.g. Ethernet to Ethernet.

c. **Switch**

The switch has replaced a lot of hubs and bridges in Local Area Networks as it's considered a more intelligent device, improving network performance and reducing the chances of errors occurring on a network. A switch keeps a record of all MAC address connected to it so it can then identify which device is connected to which port. When a frame is received, it then looks at the destination MAC address and knows exactly which port to send the data on to. It doesn't just send the data out on all ports like a hub does.

Figure 2. switch

d. **Router**

If a network has a number of sub-networks (segments) that use different networking protocols and architectures, it requires a sophisticated device to manage the data flow. This device is known as a router which determines how incoming packets get to destination networks in the most efficient way possible. Routers can communicate information about their network with routers on different networks and they store information in a routing table.

Figure 3. Router

2. Access devices

Network access device is any device that help a user (end device) to get connected on a network.

a. Network Interface Card (NIC)

A NIC is also known as a network adapter. Any device that wants to communicate and send / receive data must have a NIC installed. They are usually located in a computer's expansion slot, similar to how you'd see a graphics card or sound card installed.

Figure 4. NIC

b. Hub

Hubs are used in Ethernet networks to connect multiple Ethernet devices together, forming a network segment (group of computers that is a portion of a network). A hub, like a repeater has no intelligence so simply broadcasts all network data across all ports. However, most hubs can detect basic errors such as collision and because every computer connected to the hub has its own dedicated connection to the hub, this means that if there is a connection failure, it only affects a single device and not the entire hub and all of its associated connections / devices.

Figure 5.Hub

c. Access point

An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.

Figure 6. Access Point

3. End devices

Network devices that people are most familiar with are called end devices. All computers connected to a network that participate directly in network communication are classified as hosts. These devices form the interface between users and the underlying communication network.

Some examples of end devices are:

- computers (workstations, laptops, file servers, and web servers)
- network printers
- VoIP phones
- Telepresence endpoints
- security cameras
- Mobile handheld devices (smartphones, tablets, PDAs, and wireless debit/credit card readers and barcode scanners) sensors such as thermometers, weight scales etc...

❖ **Description of network components**

Network components are used to provide services and processes.

Devices and media are the physical elements, or hardware, of the network. Hardware is often the visible components of the network platform such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices. Occasionally, some components may not be so visible. In the case.

Here are the main categories of network components:

1. Media

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

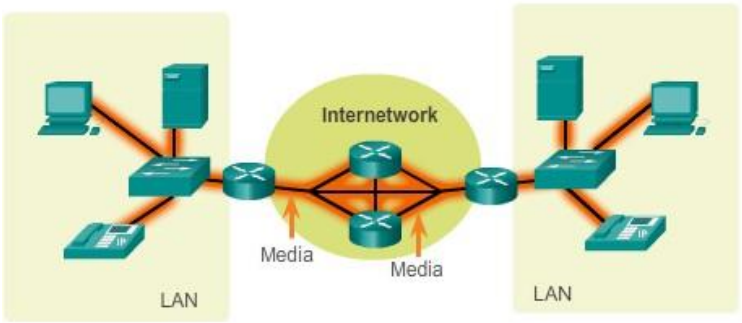


Fig.8: Network component/ Media

2. **Message**

In general, a message is any grouping of information at the application layer (layer 7) of the Open Systems Interconnection (OSI) reference model that is exchanged between applications for various purposes.

3. **Protocol**

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network.

4. **Devices**

The devices which are used for communication between different hardware's used in the computer network are known as network devices. These devices are also known as physical devices, networking hardware, and network equipment otherwise computer networking devices. In a computer network, each network device plays a key role based on their functionality, and also works for different purposes at different segments.

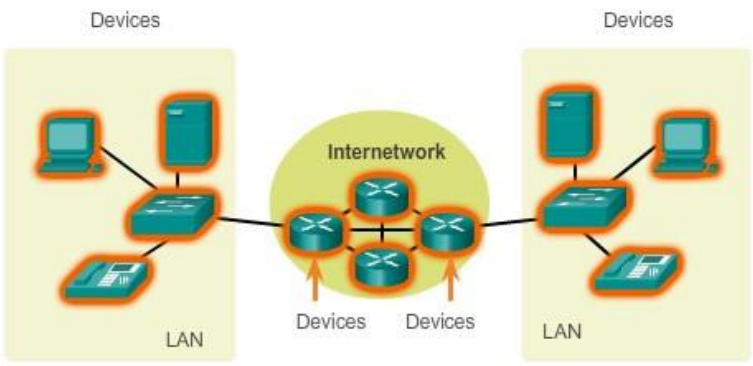


Fig.7: Network component/ Device

Here are the common network devices:

1. **Router**
2. **Hubs**
3. **Switch**
4. **NIC**
5. **Repeater**

6. **MAU:** A media access unit (MAU), also known as a multi-station access unit (MAU or MSAU), is a device to attach multiple network stations in a star topology as a token ring network, internally wired to connect the stations into a logical ring (generally passive i.e. non-switched and unmanaged; however managed token ring MAUs do exist in the form of CAUs, or Controlled Access Units).
7. **Firewall:** A firewall is a security device such as computer hardware or software that can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on your computer.

   Not only does a firewall block unwanted traffic, it can also help block malicious software from infecting your computer.

8. **Access points:** While an access point (AP) can technically involve either a wired or wireless connection, it commonly means a wireless device. An AP works at the second OSI layer, the Data Link layer, and it

can operate either as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another.

9. **Antenna:** Also called an aerial, an antenna is a conductor that can transmit, send and receive signals such as microwave, radio or satellite signals. A high-gain antenna increases signal strength, where a low-gain antenna receives or transmits over a wide angle.

10. **Gateways:** Gateways normally work at the Transport and Session layers of the OSI (Open System Interconnection) model.

Topic 2. Network materials

- **Network Cables (twisted, coaxial and Fiber optic)**

1. Twisted

These are a type of guided media. It was invented by Alexander Graham Bell. Twisted pair cables have two conductors that are generally made up of copper and each conductor has insulation. These two conductors are twisted together, thus giving the name twisted pair cables.

Twisted Pair Cables are further of two types:

1. **Unshielded Twisted Pair Cables (UTP):**

These are a pair of two insulated copper wires twisted together without any other insulation or shielding and hence are called unshielded twisted pair cables. They reduce the external interference due to the presence of insulation.

Advantages

1. These cables are cost-effective and easy to install owing to their compact size.
2. They are generally used for short-distance transmission of both voice and data.
3. It is less costly as compared to other types of cables.

Disadvantages

1. The connection established using UTP is not secure.
2. They are efficient only for a distance up to 100 meters and have to be installed in pieces of up to 100 meters.
3. These cables have limited bandwidth.

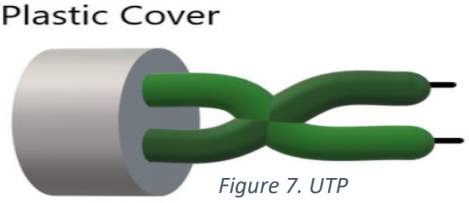


Figure 7. UTP

2. **Shielded Twisted Pair Cables (STP):**

These types of cables have extra insulation or protective covering over the conductors in the form of a copper braid covering.

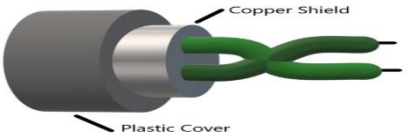


Figure 8. STP

Advantages

1. They are generally used for long-distance communication and transmission and are installed underground.
2. The protective shield prevents external electromagnetic noise penetration into the cable.
3. They have a higher bandwidth as compared to UTP.

Disadvantages

1. These cables are very expensive.
2. They require a lot of maintenance which increases the cost more.
3. These can be installed underground only.
4. The length of the segment is similar to UTP for these cables.

2. **Coaxial Cable**

It is a type of guided media made of Plastics, and copper wires which transmit the signal in electrical form rather than light form. Coaxial cable is also known as coax.

Structure of Coaxial Cable

1. Copper conductor
2. Insulator
3. Braided mesh
4. Protective plastic layer

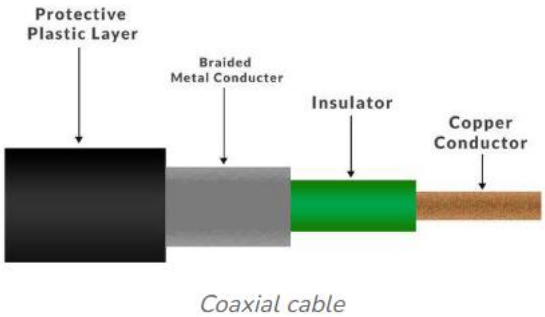


Figure 9. Coaxial cable

3. What Is Fiber Optic Cable?

Fiber optic cable, also known as **optical fiber** cable, is a type of Ethernet cable which consists of one or more optic fibers that are used to transmit data.

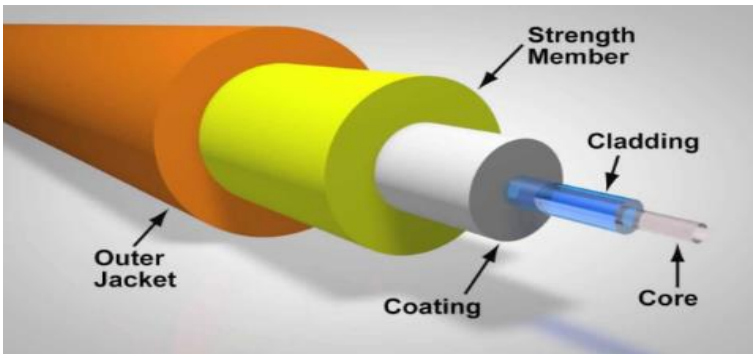


Figure 10.Fiber Optic Cable

- **Network switch trunking (Flexible, plastic, timber and stainless steel)**

1. **Network truncking** is a technique to combine multiple physical links into a single logical link, enhancing bandwidth, redundancy, and load balancing.
   Cable trunking is a type of cable management system that is used to organize and protect cables and wires.

Figure 11. Trunking

❖ **Description of network connector's types**

A variety of connectors are used with the associated network media. Media connectors attach to the transmission media and allow the physical connection into the computing device. It is necessary to identify the connectors associated with the specific media. The following sections identify the connectors and associated media.

1. **BNC (Bayonet Neill-Concelman) Connectors:** BNC connectors are associated with coaxial media and 10Base2 networks. BNC connectors are not as common as they once were, but still are used on some networks, older network cards, and older hubs. Common BNC connectors include a barrel connector, T-connector, and terminators.

Fig.16: Two terminators (top and bottom) and two T-connectors (left and right)

2. **RJ11connectors:** RJ (Registered Jack) -11 connectors are small plastic connectors used on telephone cables. They have capacity for six small pins. However, in many cases, not all the pins are used. For example, a standard telephone connection only uses two pins, while a cable used for a DSL modem connection uses four.

RJ-11 connectors are somewhat similar to RJ-45 connectors, which are discussed next, though they are a little smaller. Both RJ-11 and RJ-45 connectors have small plastic flange on top of the connector to ensure a secure connection. Figure 5 shows two views of an RJ-11 connector.

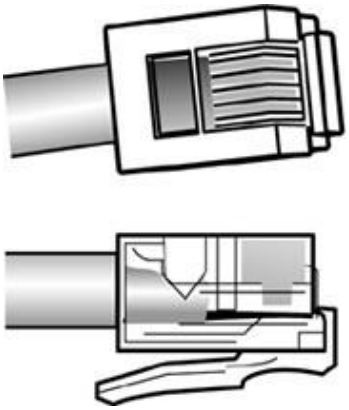


Fig.17: RJ-11 connectors

3. **RJ-45 Connectors:** RJ-45 connectors are the ones you are most likely going to encounter in your network travels. RJ-45 connectors are used with twisted-pair cabling, the most prevalent network cable in use today. RJ-45 connectors resemble the aforementioned RJ-11 phone jacks, but support up to eight wires instead of the six supported by RJ-11 connectors. RJ-45 connectors are also larger. Figure 6 shows the RJ-45 connectors.

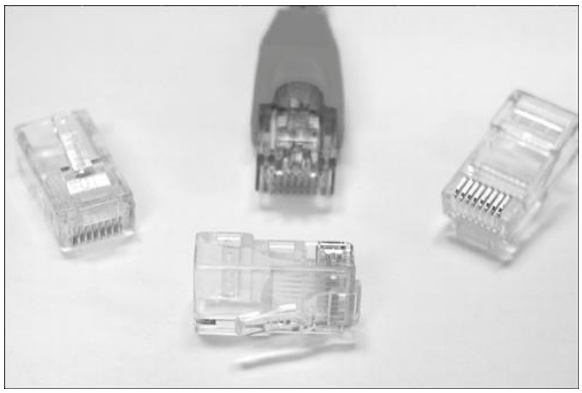


Fig.18: RJ-45 connectors

4. **F-Type connectors:** F-Type connectors are screw on connections used for attaching coaxial cable to devices. In the world of modern networking, F-Type connectors are most commonly associated with connecting Internet modems to cable or satellite Internet provider's equipment. However, they are also used for connecting to some proprietary peripherals.

F-Type connectors have a 'nut' on the connection that provides something to grip as the connection is tightened by hand. If necessary, this nut can be also being lightly gripped with pliers to aid disconnection.

Fig.19: An example of an F-Type connector

5. **Fiber Connectors:** a variety of connectors are associated with fiber cabling, and there are several ways of connecting these connectors. These include bayonet, snap-lock, and push-pull connectors.

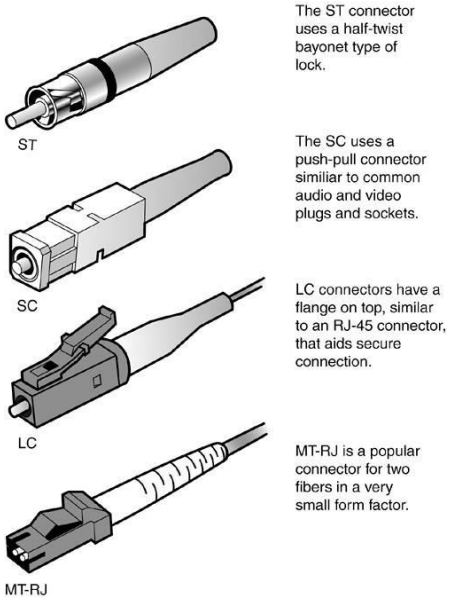


Fig.20: Different fiber connectors

6. **VGA connector:** A Video Graphics Array (VGA) connector is a standard connector used for computer video output. It is a three-row, 15-pin D-sub miniature connector referred to variously as DE-15, HD-15 or DB-15. DE-15 is the most accurate common nomenclature under the D-sub specifications: an "E" size D-sub connector, with 15 pins in three rows.

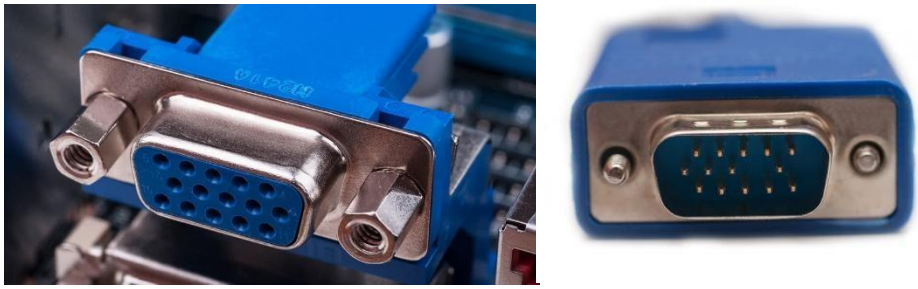


Fig.21: VGA Male and Female connectors

7. **USB connector:** A universal serial bus (USB) connector is a connector between a computer and a peripheral device such as a printer, monitor, scanner, mouse or keyboard. It is part of the USB interface, which includes types of ports, cables and connectors.
8. **Firewire Connectors:** External connector, similar to a USB port, that provides a high-speed connection between a computer and peripheral devices. Firewire was developed by Apple, Inc. and is based off the standard IEEE 1394 high performance serial bus. Firewire ports are able to transfer data at a rate of up to 400 Mbps. This technology was once standard on computers manufactured by Apple, Inc., but has since been replaced by Thunderbolt ports and later versions of USB ports.

Fig.22: Different firewire connectors

9. **Serial Port/Connector:** A serial port is an interface that allows a PC to transmit or receive data one bit at a time. It is one of the oldest types of interfaces and at one time was commonly used to connect printers and external modems to a PC. Modern serial ports are used in scientific instruments, shop till systems such as cash registers and applications like industrial machinery systems.

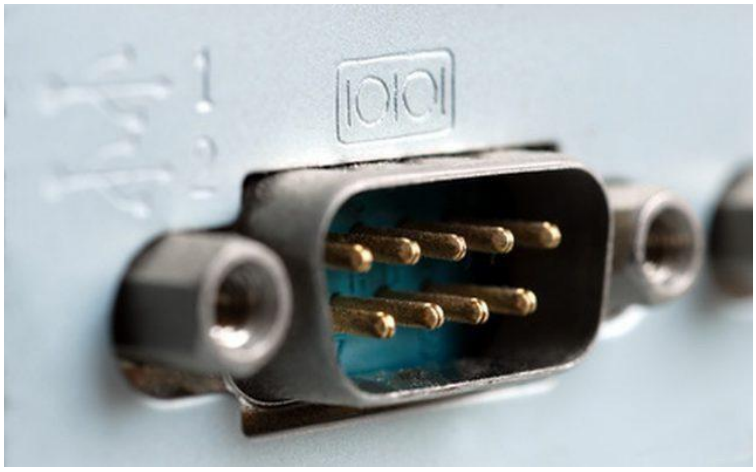


Fig.23: Serial port

MT-RG

10. **MT-RG Connector: MT-RJ** stands for Mechanical Transfer Registered Jack. **MT-RJ** is a fiber-optic Cable **Connector** that is very popular for small form factor devices due to its small size. Housing two fibers and mating together with locating pins on the plug.

Figure: Fiber optic cable connector

11. RS-232

RS232 is a standard protocol used for serial communication, it is used for connecting computer and its peripheral devices to allow serial data exchange between them. As it obtains the voltage for the path used for the data exchange between the devices. It is used in serial communication up to 50 feet with the rate of 1.492kbps.

RS-232 Connector is a type of connector used for serial communication standard that provides asynchronous and synchronous communication capabilities.

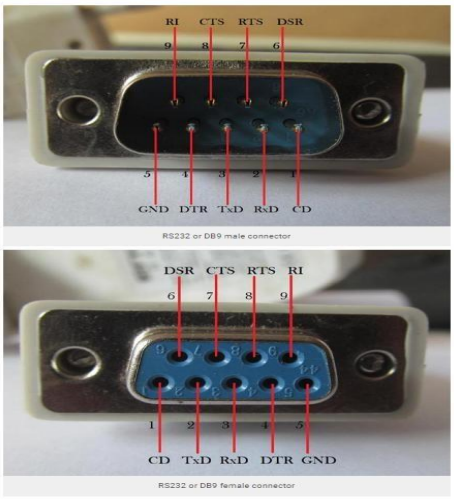


Figure: RS-232 Connector

- ❖ **Cable ties**

These are fasteners used for holding items together, primarily electrical cables and wires.

- ✓ **Types of Cable Ties**

1. Standard Cable Ties

These are the most common type of cable ties, made from durable nylon. They are available in various lengths and strengths, suitable for general-purpose use in homes, offices, and industrial settings.

2. Releasable Cable Ties

Designed for temporary applications, releasable cable ties can be easily undone (unfinished) and reused. They are ideal for situations where changes are frequent, such as in networking setups.

3. Heavy-Duty Cable Ties

These cable ties are built to handle heavy loads and extreme conditions. Made from stronger materials, they are used in demanding environments like construction sites and automotive industries.

4. Stainless Steel Cable Ties

Resistant to corrosion and high temperatures, stainless steel cable ties are perfect for harsh environments. They are commonly used in marine, aerospace, and industrial applications.

5. Colored and UV Resistant Cable Ties

Colored cable ties aid in organization by allowing easy identification of cables. UV-resistant ties are specially treated to withstand prolonged exposure to sunlight, making them ideal for outdoor use.

6. Specialty Cable Ties

These include ties with specific features, such as marker ties for labelling, push-mount ties for securing to panels, and double-headed ties for securing two bundles simultaneously.

- ✓ **Applications of Cable Ties**

1. Home and Office Organization
2. Electrical and Networking
3. Industrial and Construction
4. Gardening and Outdoor Use

- ✓ **How to Choose the Right Cable Tie**

1. Material Considerations
2. Size and Strength
3. Environmental Factors

- ✓ **Best Practices for Using Cable Ties**

1. Proper Installation Techniques
2. Safety Tips

- **Cable clip**

It is a device that manages wires and cables and secures them to a fixed point on a surface, like a wall, ceiling or floor. A wide range of cable clips is available to control cables of all sizes and shapes, in almost any number, in both home and industrial applications.

Figure 12. Cable Clips

- **Cable Sockets**

A socket is an opening that fits another specific device with matching pins or other connectors

- **Wall plug**

It is an electrical outlet permanently mounted on a wall.

Figure 13. Wall Plug

Topic 3. Networking Tools

- **Cutting Tools**

Cable-cutting tools are designed for accurately cutting cables and wires in various applications, such as electrical work, telecommunications, networking, and home improvement projects.

Handheld Wire Rope & Cable Cutter

Round Cable Strip & Ring Tool, 4.5 - 29 mm OD

3/4" COAX Cable Cutter

Long Nose Telecom Pliers

6.25" Telecom Diagonal Cutting Pliers

Tabbing Shears

6" Heavy Duty Diagonal Cutting Pliers

6 1/4" PRO Drywall Saw, Multipurpose Cutting Tool

100 Pair Cable Cutter for Large Diameter Cables

Professional Network Technicians Scissors

❖ **Stripping tools**

A cable stripper, also known as a wire stripper, is a hand-held networking tool used to remove the outer insulation layer from an electrical wire or cable without damaging the inner conductor.

1. Punch-Down Tool

A punch-down tool, also known as Krone tool, is a networking tool used to punch wires into a connection block, keystone jack, or patch panel.

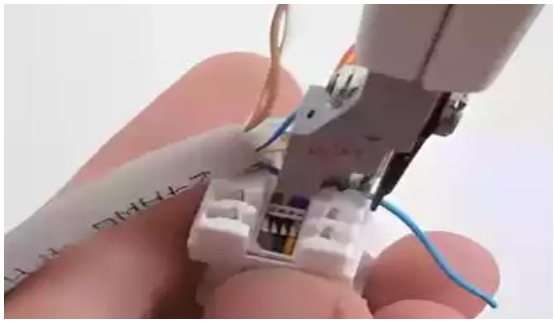


Figure 14. Punch-Down

2. Cable Stripper

A cable stripper, also known as a wire stripper, is a hand-held networking tool used to remove the outer insulation layer from an electrical wire or cable without damaging the inner conductor.

Figure 15. Cable Stripper

❖ **Drilling Tools**

In networking, “drilling tools” can refer to various software and hardware tools used for testing, troubleshooting, and maintaining network infrastructure.

Figure 16.Home Drilling tool

❖ **Fixing Tool**

1. **A tone generator** is a networking device used to identify and trace the path of a network cable.

Figure 17. Toner Generator

2. A **screwdriver** set is a collection of screwdrivers in various sizes and shapes that are used to loosen or tighten screws.

Figure 18.Screwdrivers

3. **A cable tie,** also known as a zip tie or tie-wrap, is a type of fastener used to secure and organize wires, cables, and other components in a network installation.

Figure 19. Cable tie

❖ **Patching tools**

1. Cable Crimper

A cable crimper, also called a wire crimper, is a hand-held tool used to join two or more Ethernet cables or wires together by crimping a metal connector onto the ends of the wires.

Figure 20. crimper

2. **Krone Punch Down Tool**

It is also a common type of punch down tool used for wiring installations such as standard Ethernet keystone jacks, mount boxes, and patch panels. Krone punch down tool is great for installing and terminating Cat3, Cat5, Cat6, and the above network cables.

Figure 21. Keystone Jack Termination tool

❖ **Crimping (pressing) tool**

A crimping tool is a handy device that allows you to create secure connections between wires and connectors.

The following image shows a crimping device equipped with a wire-stripper and wire-cutter.

Figure 22.Crimper

❖ **Testing tool**

1. Time domain reflectometer

This device is used to measure the length of a network cable as well as the breaks in the cable.

Figure 23. Time domain reflectometer

2. **Tone generator and the probe**

This device is used to trace the unlabeled network cables.

Figure 24. Tone generator and the probe

3. **Basic cable tester**

If you can't afford a network cable certifier, you can buy and use this device to manage your network cables. Besides certifying the cable installation, this device provides all remaining functionalities of a network cable certifier. It can test cable length, cross talk, and breaks in the cable. It can also check whether the connectors on both ends of a network cable are properly attached or not.

Figure 25. Basic cable tester

4. **Cable certifier**

This device thoroughly tests a network cable and certifies that the cable installation meets a special wiring standard such as Cat 5e, Cat 6, Cat 6a, and so on. This device can check and test total segment length, crosstalk, noise, wire map, resistance, impedance, and the capability to transfer data at the maximum frequency rated for the cable.

Figure 26. Cable certifier

Topic 4. Equipment

- **Computer**

It is an electronic device a machine capable for solving the problems and manipulating data.

Figure 27.Computer

❖ **Inverter**

Inverters in networking typically refer to devices that convert direct current (DC) to alternating current (AC). This conversion is essential for various applications, including renewable energy systems and industrial automation.

Figure 28. Power Inverter

❖ **UPS (Uninterruptible Power Supply)**

UPS is a type of power supply system with an integrated battery, and in the absence of primary mode or when power is shut down, the battery is used for the power source.

Figure 29. UPS

❖ **Switch**

The **Switch** is a network device that is used to segment the networks into different subnetworks called subnets or LAN segments. It is responsible for filtering and forwarding the packets between LAN segments based on MAC address.

Figure 30.Switch

❖ **Glue gun**

A hot **glue gun** is a hand-held device that uses a heating element to heat and melt solid glue. Once the adhesive has melted, it can be directed out of the gun's nozzle and then onto a given object.

Figure 31. Glue gu

❖ **Rack**

A **network rack** is a metal frame chassis that holds, stacks, organizes, secures and protects various computer network and server hardware devices.

Figure 32. Network Rack

❖ **Bracket**

In computing, a bracket is a punctuation mark used to enclose groups of characters, such as code statements or mathematical expressions.

There are several types of brackets used in computing, including parentheses **()**, square brackets **[]**, and curly brackets **{}**. Each type of bracket has a different use and meaning in programming.

- **Patch panel**

A patch panel is **a device that connects cables in a network cabling system.**

Figure 33.Patch Panel

- **Repeaters**

Repeaters are defined as a networking device that is used to amplify and generate the incoming signal.

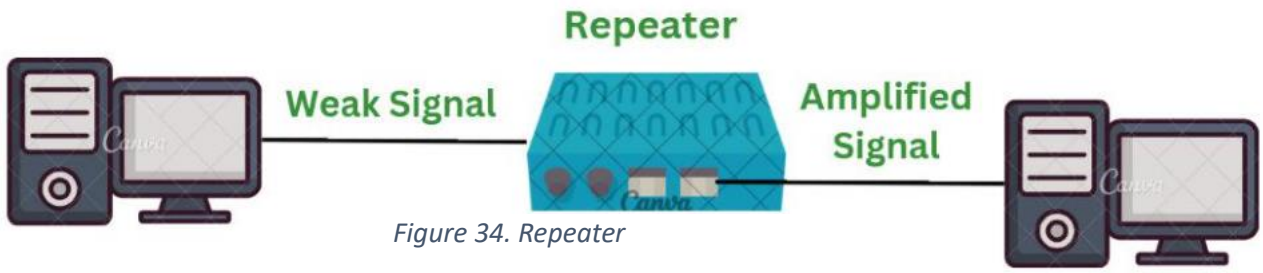


Figure 34. Repeater

- **Regenerator**

Regenerator is a repeater, that takes an optical signal and regenerates (increases the strength) it.

Indicative Content 2. Termination of Network cables

Topic1. Network cables installation types.

1. **Open wire installation**

Open wire was an early transmission technology in telecommunication, first used in telegraphy. It consisted of pairs of electric wire strung on a pole line between communities, towns, and cities.

2. **Aerial Installation**

An aerial installation in networking refers to the use of existing electrical poles and towers to run fiber cables directly to a new building. This method is cost-effective and practical when supporting infrastructure already exists in the area.

3. **Above-Grounds Conduits installation**

In the context of the Internet, a conduit is a means of transmitting data from one device or network to another. It can be thought of as a pipeline or a pathway through which data flows.

An electrical conduit is a tube used to protect and route electrical wiring in a building or structure. Electrical conduit may be made of metal, plastic, fiber, or fired clay.

4. **Underground installation**

In areas where space for cables is limited and crunched, especially the urban regions, underground laying of cables is an efficient method. Telecommunications or electric power can be transmitted through underground cables.

5. **Underwater installation**

Underwater networking involves the deployment of communication systems beneath the water's surface.

6. **Built in installation**

In networking, built-in installation typically refers to the process of integrating network components directly into the infrastructure of a building.

7. **Semi built in installation**

In networking semi-built-in installation typically refers to the process of integrating network components after finishing the infrastructure.

Topic 2. Network cables Trunking materials

Cable trunking is a way of hide and protecting wires. Cable is trunked by

1. **Plastic**
2. **Wood**

- **Stainless:** It is an alloy of iron that is resistant to rusting and corrosion.
- **Cable termination**

Cable Termination is the connection of the wire or fiber to a device, such as equipment, panels or a wall outlet, which allows for connecting the cable to other cables or devices.

1. **Twisted-pair cabling** is a type of cabling used for telephone communications and most modern Ethernet networks
2. **Fiber-optic cabling** is widely used for high-speed Ethernet links over relatively long distances1. It uses glass or plastic fiber as a medium through which light is "guided" to the other end of the link.
3. **Coaxial network cabling** is used for transmitting electrical signals, primarily radio frequency (RF) signals, with minimal signal loss and interference.
4. **Shielded twisted pair (STP)** is a special kind of copper telephone and local area network (LAN) wiring used in some business installations. It adds an outer covering or shield that function as a ground to ordinary twisted pair wiring.

- **Connection of Network Media**

1. **Labels** need to identify all cables, connecting hardware, and associated physical locations (building, room, cabinet, rack, port, telecommunications spaces, etc.)
2. **Tagging**, also known as Frame Tagging, is a method developed by Cisco to help identify packets travelling through trunk links.
3. **Patching** in networking typically refers to the use of patch panels. These are hardware devices that organize and connect various network cables.

4. **Provide us build design**

Network design, sometimes known as network topology, is the physical, virtual, and logical arrangement of infrastructure in an IT network.

Learning outcome 2: PERFORM BASIC NETWORK CONFIGURATION

Indicative Content 1. Classification of IP Addresses

Topic1. Types of IP Addresses

Types of IP Addresses

1. **Private IP Addresses**

A private IP address is an address which is reserved for use only within private/local network and cannot be seen outside the private networks. These private addresses are translated at the company's firewall into an external (public) IP address, which will be some address that does 'not' fall within the range of Private ones. (e.g., home or office).

Ranger of private IP address

Class A: 10.0.0.0/8=10.0.0.0 – 10.255.255.255

Class B: 172.16.0.0/12=172.16.0.0 – 172.31.255.255

Class C: 192.168.0.0/16=192.168.0.0 – 192.168.255.255

2. **Public IP-address**

It is public global addresses that are used in the Internet. A public IP address is an IP address that is used to access the Internet. Public (global) IP addresses are routed on the Internet, unlike private addresses.

Note: All servers and sites on the Internet use public IP addresses (for example, google.com — 172.217.22.14, Google's DNS server — 8.8.8.8).

3. **IPv4**: The original version, represented in dotted-decimal notation (e.g., 192.168.1.1). It uses 32-bit addresses, allowing for about 4.3 billion unique addresses.
4. **IPv6:** The newer version, designed to replace IPv4.
5. **Static IP:** An IP address that doesn't change. It's manually assigned and remains constant over time2.

6. **Dynamic IP:** Assigned by a DHCP server and can change over time. Most home networks use dynamic IP addresses2.
7. **Local Host IP:** Also known as the loopback address, typically 127.0.0.1 for IPv4, used for testing and network diagnostics3.
8. **Broadcast IP:** Used to send data to all possible destinations in a network (e.g., 192.168.1.255 for IPv4)3.

All of the public IP-addresses in the Internet are unique to their host or server and cannot duplicate assignment.

Topic 2. Types of IP address

There are two main versions of IP addresses:

1. **IPv4 (Internet Protocol version 4):**

Format: 32-bit address.

Notation: Four decimal numbers separated by periods, e.g., 192.168.1.1.

Address Space: Approximately 4.3 billion unique addresses.

Usage: IPv4 is the most commonly used version of IP addresses. Due to the growing number of devices, IPv4 addresses are becoming scarce.

2. **IPv6 (Internet Protocol version 6):**

Format: 128-bit address.

Notation: Eight groups of four hexadecimal digits separated by colons, e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Address Space: Approximately 340 undecillion (3.4 x 10^38) unique addresses.

Usage: IPv6 was developed to address the limitations of IPv4, particularly the shortage of addresses. It also includes improvements in routing, network autoconfiguration, and security.

The transition from IPv4 to IPv6 is ongoing, but IPv4 is still widely used. IPv6 adoption is increasing as more devices come online and the limitations of IPv4 become more pressing.

Topic 2: Classification of IP Address

Classification

Released in 1981, RFC 790 and RFC 791 describe how IPv4 network addresses were initially allocated based on a classification system. In the original specification of IPv4, the authors established the classes to provide three different sizes of networks for large, medium, and small organizations. As a result, class A, B, and C addresses were defined with a specific format for the high order bits. High order bits are the far-left bits in a 32-bit address.

As shown in the figure:

Class A addresses begin with 0 - Intended for large organizations; includes all addresses from 0.0.0.0 (**0**0000000) to 127.255.255.255 (**0**1111111). The 0.0.0.0 address is reserved for default routing and the 127.0.0.0 address is reserved for loopback testing.

Class B addresses begin with 10 - Intended for medium-to-large organizations; includes all addresses from 128.0.0.0 (**10**000000) to 191.255.255.255 (**10**111111).

Class C addresses begin with 110 - Intended for small-to-medium organizations; includes all addresses from 192.0.0.0 (**110**00000) to 223.255.255.255 (**110**11111).

The remaining addresses were reserved for multicasting and future uses.

Class D Multicast addresses begin with 1110 - Multicast addresses are used to identify a group of hosts that are part of a multicast group. This helps reduce the amount of packet processing that is done by hosts, particularly on broadcast media (i.e., Ethernet LANs). Routing protocols, such as RIPv2, EIGRP, and OSPF use designated multicast addresses (RIP = 224.0.0.9, EIGRP = 224.0.0.10, OSPF 224.0.0.5, and 224.0.0.6).

Class E Reserved IP addresses begin with 1111 - These addresses were reserved for experimental and future use.

High Order Bits

Class	High Order Bits	Start	End
Class A	0xxxxxxx	0.0.0.0	127.255.255.255
Class B	10xxxxxx	128.0.0.0	191.255.255.255
Class C	110xxxxx	192.0.0.0	223.255.255.255
Class D (Multicast)	1110xxxx	224.0.0.0	239.255.255.255
Class E (Reserved)	1111xxxx	240.0.0.0	255.255.255.255

Figure 35. Ip address classes

Indicative content.2 Calculation of IP addresses subnet masks

Topic1. Introduction to subnet masks

- **Subnet masks**

A subnet mask refers to a range of IP addresses used to create multiple sub-networks within an extensive network.

Subnetting is the process of diving a network into small networks and is a common task on IPV4 networks.

- **Benefits of subnetting**

Here are three reasons why you may want to use sub-netting:

1. **Conservation of IP addresses:** Imagine having a network of 20 hosts. Using a Class C network will waste a lot of IP addresses (254-20=234). Breaking up large networks into smaller parts would be more efficient and would conserve a great number of addresses.

2. **Reduced network traffic:** The smaller networks that created the smaller broadcast domains are formed, hence less broadcast traffic on network boundaries.
3. **Simplification**: Breaking large networks into smaller ones could simplify fault troubleshooting by isolating network problems down to their specific existence.

Topic2. Binary Numbering System

In the binary numbering system, the radix is 2. Therefore, each position represents increasing powers of 2. In 8-bit binary numbers, the positions represent these quantities:

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

The base 2 numbering system only has two digits: 0 and 1.

When we interpret a byte as a decimal number, we have the quantity that position represents if the digit is a 1 and we do not have that quantity if the digit is a 0, as shown in Figure 1.

Figure 2 illustrates the representation of the decimal number 192 in binary. A 1 in a certain position means we add that value to the total. A 0 means we do not add that value. The binary number 11000000 has a 1 in the 2^7 position (decimal value 128) and a 1 in the 2^6 position (decimal value 64). The remaining bits are all 0 so we do not add the corresponding decimal values. The result of adding 128+64 is 192, the decimal equivalent of 11000000.

Here are two more examples:

Example 1: An octet containing all 1s: 11111111

A 1 in each position means that we add the value for that position to the total. All 1s means that the values of every position are included in the total, therefore, the value of all 1s in an octet is 255.

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

Example 2: An octet containing all 0s: 00000000

A 0 in each position indicates that the value for that position is not included in the total. A 0 in every position yields a total of 0.

0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0

A different combination of ones and zeros will yield a different decimal value.

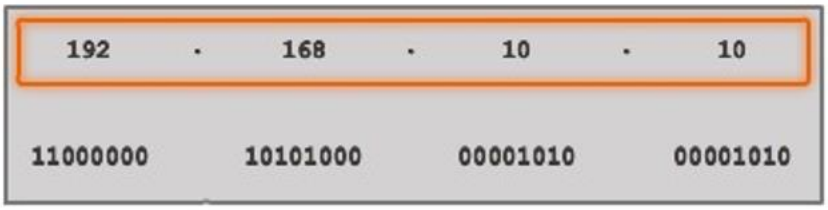


Figure 36. Ip address to buinary

192.168.10.10 is an IP address that is assigned to a computer.

Topic 3. The types of subnetting

Subnetting is a technique used in networking to divide a large network into smaller, more manageable sub-networks or subnets. This helps in efficient IP address management, reduces broadcast traffic, and enhances security. **There are several types of subnetting and subnetting strategies:**

1. Fixed-Length Subnet Mask (FLSM)

Description: All subnets have the same size, meaning each subnet has the same number of IP addresses.

Example: If you have a Class C network and create 4 subnets, each subnet would have the same number of addresses, typically determined by dividing the available address space equally.

2. Variable-Length Subnet Mask (VLSM)

Description: Subnets can have different sizes. This allows for more efficient use of IP addresses by allocating more addresses to larger subnets and fewer addresses to smaller ones.

Example: In a network, you might allocate a larger subnet for a department with many devices and a smaller subnet for a department with fewer devices.

3. Classful Subnetting

Description: Subnetting done according to the original classful network boundaries (Class A, B, C). This is the traditional method and often used in older systems.

Example: A Class B network (e.g., 172.16.0.0/16) might be divided into multiple Class C-sized subnets (e.g., 172.16.1.0/24, 172.16.2.0/24, etc.).

4. Classless Inter-Domain Routing (CIDR)

Description: An extension of subnetting that allows for more flexible IP address allocation by using variable-length subnet masks, not tied to classful boundaries. CIDR uses notation like /24 to specify the subnet mask.

Example: A network might be represented as 192.168.0.0/22, which allows for a more flexible division of IP address space compared to traditional classful subnetting.

5. Super netting (Aggregation)

Description: The reverse of subnetting. It involves combining multiple contiguous subnets into a single larger network to reduce the size of routing tables.

Example: Instead of advertising several Class C networks, you might aggregate them into a single Class B network for routing purposes.

6. Subnetting for Special Cases

Private Networks: Reserved IP ranges (e.g., 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) often use subnetting to manage internal networks efficiently.

Subnetting for IP Address Conservation: In scenarios where IP addresses are limited, subnetting helps in maximizing the efficient use of available addresses.

Key Considerations:

Subnet Mask: Determines the boundary between the network and host portions of an IP address.

Network Design: The choice of subnetting strategy depends on the network's size, requirements, and the number of hosts needed in each subnet.

Understanding these types of subnetting allows network administrators to design efficient and scalable networks.

Topic 4. Logical bitwise and Operation

We can join two statements by “AND” operand. It is also known as a conjunction. Its symbolic form is “∧ “. In this operator, if anyone of the statement is false, then the result will be false. If both the statements are true, then the result will be true. It has two or more inputs but only one output.

Input A	**Input B**	**A^B**
1	**1**	**1**
1	**0**	**0**
0	**1**	**0**
0	**0**	**0**

Indicative content 3. Assigning IP Address

Topic 3.1. Static

An IP address is a unique series of numbers that identifies each device on a local network or the internet. An IP address can be dynamic or static.

A static IP address can be very useful in some cases, and can even improve your security. If you want to set up a local server or improve your internet speeds, configuring a static IP address on different devices is a very simple process.

How to set a static IP address on Windows 10

Assigning a static IP to your Windows 10 device is much easier than on your router. Just follow these instructions:

1. **Go to Settings.** Press the Windows key, type “Settings,” and press Enter.
2. Click **Network and Internet** and then **Network and Sharing Center**.
3. Click **Change adapter settings** on the left pane.
4. Right-click your network connection and select **Properties**.
5. Highlight **Internet Protocol Version 4 (TCP/IPv4)** and click on **Properties**.
6. Fill in the **IP address, Gateway, Network prefix length, and DNS** fields.
7. Click **OK** to save your changes, then click OK again to exit the properties menu

How to set a static IP address on Windows 11

The steps for Windows 11 are very similar to those on Windows 10:

1. **Open Settings.** Click on the Start menu, select Settings, or press Windows + I on your keyboard.
2. **In the Settings menu, click on Network & Internet.**
3. **Choose the network you are connected to.** If you are using Wi-Fi, click on “Wi-Fi” and then select your network. For a wired connection, click on “Ethernet” and then on your network connection.
4. **Edit IP Assignment.** Scroll down and click on “Hardware properties.” Then, find the “IP assignment” section and click the “Edit” button.
5. **Change to Manual.** In the “Edit IP settings” window, change the setting from “Automatic (DHCP)” to “Manual.” Toggle on the “IPv4” switch to enable manual IP configuration.

6. **Fill in the IP address, Gateway, Network prefix length, and DNS fields.**

7. **Click Save to apply your settings.**

How to set a static IP address on macOS

To configure a static IP on your Mac, follow these steps:

1. Click on the **Apple menu** in the top left corner of your screen and select **System Preferences**.

Topic 3.2. Dynamic

A dynamic IP address is assigned automatically to a node or connection of a network like your computer, laptop, or smartphone. It is automatically assigned using a DHCP (**Dynamic Host Configuration Protocol**) server.

Topic 3.2. Automatic

Automatic Private IP Addressing, also known as APIPA or Auto IP, is a method of **automatically assigning IP addresses** to networked computers and printers.

Indicative Content 4. Configuration of Basics Network Device.

Topic 4.1. Device Configuration Modes

- ✓ **Configure a Switch with Initial Settings**

After a Cisco switch is powered on, it goes through the following five-step boot sequence:

Step 1: First, the switch loads a power-on self-test (POST) program stored in ROM.

POST checks the CPU subsystem. It tests the CPU, DRAM, and the portion of the flash

device that makes up the flash file system.

Step 2: Next, the switch loads the boot loader software. The boot loader is a small

program stored in ROM that is run immediately after POST successfully completes.

Step 3: The boot loader performs low-level CPU initialization. It initializes the CPU

registers, which control where physical memory is mapped, the quantity of memory, and its speed.

Step 4: The boot loader initializes the flash file system on the system board.

Step 5: Finally, the boot loader locates and loads a default IOS operating system

software image into memory and gives control of the switch over to the IOS.

- ✓ **Router configuration**

If the router has antennas and they're separate from the router box, you'll need to install them. In addition, you should extend the antennas before beginning the setup process.

Router setup steps

Step 1: Decide where to place the router

Step 2: Connect to the Internet

Step 3: Configure the wireless router gateway

Step 4: Connect gateway to router

Step 5: Use app or web dashboard

Step 6: Create a username and password

Step 7: Update the router's firmware

Step 8: Create a Wi-Fi password

Step 9: Use auto-configuration tools where possible

Step 10: Set up security

2. Host name

A hostname is a unique label given to a specific machine or device on a network.

Example: In the URL **“www.example.com”, “www”** is the hostname.

3. Banner message

A banner is a text displayed by a host that provides details such as the type and version of software running on the system or server.

4. **Reload device**

" Reload " to **"restart"** the device.

5. **Configure port**

Port is a logical address of a 16-bit unsigned integer that is allotted to every application on the computer that uses the internet to send or receive data.

6. **Configure Device passwords**

How to set router password?

1. Locate your router’s IP address.
2. Enter the IP address into your browser’s address bar.
3. Log in using your default admin username and password.
4. Oppen wireless or wireless property page

7. **Save configuration**

To ensure that your configurations are saved correctly in Cisco routers and switches, follow this step-by-step guide carefully. Each step can be crucial in avoiding configuration losses and ensuring the stability of your network environment.

Step 1: Enter Privileged EXEC Mode

First, connect to your device and access the console. Once in, you need to enter Privileged EXEC mode. Typically, you can enter this mode by typing enable in the user EXEC mode prompt. This mode allows you to execute all commands and can make global configuration changes.

Use the command **show running-config**.

To permanently save the changes you've made in the running configuration to the startup configuration, use the **copy running-config startup-config command**. This command is straightforward yet vital, as it ensures that your changes are not lost if the device is rebooted.

Indicative content 4. Testing network Interconnection

Topic 1. Physical testing

Physical testing in networking involves evaluating the physical components and infrastructure of a network to ensure they are functioning correctly and efficiently

Topic 2. Unit testing

Unit testing is the process of testing small isolated portions of a software application called units**.**

Topic 3. Integration testing

Integration testing focuses on verifying the communication between two or more units of an application.

LEARNING OUTCOME 3: MAINTAIN NETWORK SYSTEM

Indicative content 3.1. Perform preventive maintenance.

Topic 1. Hardware preventive maintenance

8. Schedule regular cleaning
9. Setting of preventive measures
10. Check physical Equipment condition.
11. Check environment condition.

Topic 2. Software preventive maintenance

1. Regular change of network device credentials
2. Network monitoring software Licensing /Application
3. Updating and Upgrading network monitoring software and device firmware

Indicative content 3.2. Perform corrective maintenance.

Topic1. Hardware corrective maintenance

1. Identification of common problem and their causes
2. Repair/Replace damaged equipment.

Topic 2. Software corrective maintenance

1. Troubleshoot network configuration.
2. Check network status
3. Update network configuration

Indicative content 3.3. Troubleshooting network

Topic 3.3.1. Introduction to troubleshooting

Network troubleshooting is the act of discovering and correcting problems with connectivity, performance, security, and other aspects of networks.

Topic 3.3.2. Troubleshoot process

1. Collecting Network System information
2. Analyzing current Network Status
3. Identification of common problem
4. Implementation of solution

Indicative content 3.4. Elaboration (Explanation) of maintenance report

Topic 3.4.1. The ways of reporting

- ✓ **Oral reporting:**

It is defined as the process of transmitting information or ideas verbally from one person or group to another.

- ✓ **Written report**

It is a document that describe the status, performance, issues, or recommendations of a network system.

- ✓ **Video reporting**

Video reporting encompasses the creation of video records or recordings with the intention of capturing, preserving, and sharing specific content.

Topic 3.4.2. Report elements

1. Used Tools, materials, and Equipment.
2. Status after maintenance

3. Update us built design.
4. Recommendation

References

1. Dordal, P. L. (2020). An Introduction to Computer Network. Chicago.
2. Malay Kumar Kundu, D. P. (2014). Advance Computing Networking and Informatics. Canberra.
3. Olivier, B. (2011). Computer Networking: Principles, Protocols and Practice.
4. Rackly, S. (2007). Wireless Network Technology. Oxford.
5. Reid, A. (2007). WAN Technologies, CCNA4 Companion Guid. India.
6. Sosinsky, B. (2009). Networking Bible. Indianapolis: Wiley publication Inc.