Study Unit 5

Network Hardware, Software, and Standardization

Study Session Outline

- Network Hardware,
- Software
- Standardization
- Security

Study Session Duration

This Study Session requires a 2 hours of formal study time.

You may spend an additional 2-3 hours for revision

Introduction

This study unit teaches students the components that are physical, visible, and touchable components of the Computer (Hardware) and the software alongside standardization.

Learning Outcomes of Study Unit 5

Upon completion of this study unit, you should be able to:

5.1 List various network devices and identify them

5.2 Define network software and state their areas of applications

5.3 Enumerate network protocols and state their functions

5.4 Define network standards and list them

Terminologies

Network protocols	Network standards
Network software	Standardization

5.0 Network Hardware, Software, and Standardization

This module focuses on network hardware, network software, and standardization. At the end of this module, every learner should be able to recognize devices in a computer networking area. You are also expected to state the functions of network software and list recognized industry standards in computer networking.

5.1 Network Hardware

5.1.1 Hub

Figure 5.1: Hub

Hubs are network devices that connect computers and other devices in a network. It contains multiple ports (as shown in Figure 10). When a packet arrives at a port, the hub does not send it to the destination port, rather it copies the packets to all the other ports. This limitation increases unnecessary traffic and causes collision because all the ports and devices connected to the ports are in the same collision domain.

Collision occurs when a computer is sending a packet at the same time the hub is a broadcasting packet to all the ports. This is called packet collision. Because of this limitation, only one device can send data per time. If two devices are sending packets at the same time, there will be packet collision.

The hub operates at the physical layer of the OSI layer.

5.1.2 Switch

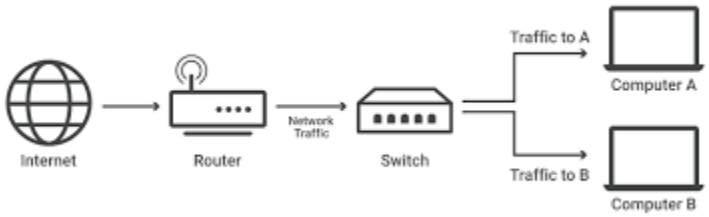


Figure 5.2: Switch [source: www.cloudfare.com]

A network switch is used for packet switching and operates at the datalink layer of the OSI model. When a packet arrives at the switch, the switch checks the destination address on the packet and uses its switching table to decide the port where the computer with the destination address is connected to. A detail operation involving a Switch is depicted in Figure 11.

Each device connected to a switch port can transfer data to any of the other ports at any time and collisions will not occur. The Switch uses Carrier Sense Multiple Access/Collision Domain (CSMA/CD) to solve the collision problems associated with hubs. When a device wants to transmit data frame, it checks whether another device is transmitting data, if the data exists on the operation, it stops transmitting the frame and waits for a time interval before resending the frame.

The switch uses MAC address of a computer to check which port a computer is connected to. Security can be provided through MAC address filtering (access can be permitted or denied using MAC address). Some switches with routing capabilities, they are called multiplayer switches.

5.1.3 Router

A router helps to send packets out of a network and receives packets into a network. It also helps a local network to connect into a public network like the internet. A router connects two different

networks together. It is responsible for allocating IP addresses to devices in a network (See Figure 5.3).

Figure 5.3: Router Image Credit: cisco.com

In data transmission out of a network, the router chooses the best path (route) to send the packets with the help of a routing table (See Figure 5.4).

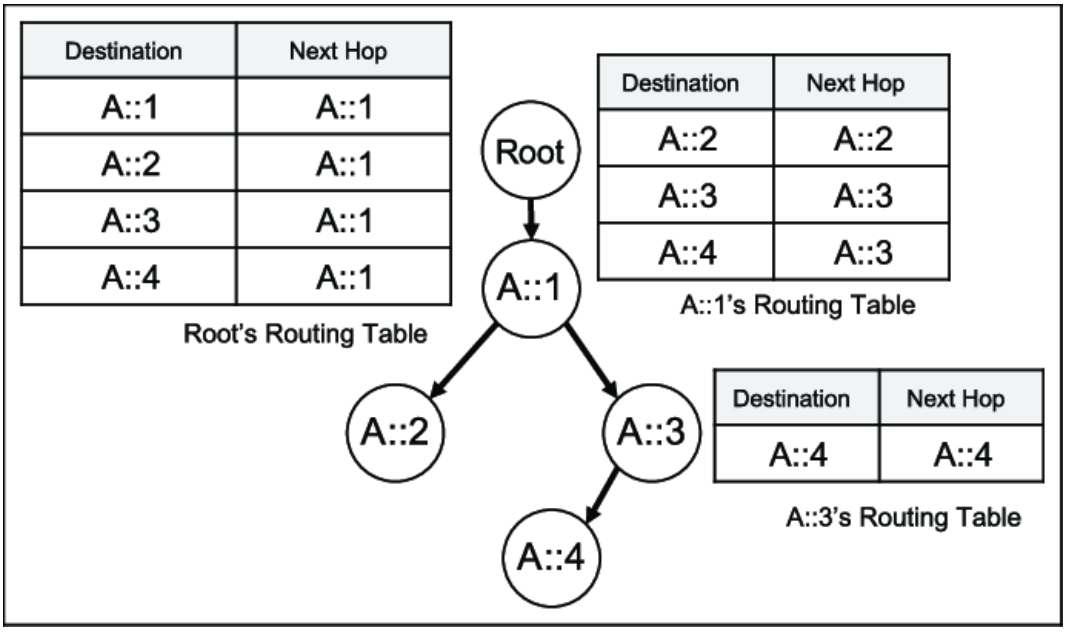


Figure 5.4: A sample routing table (Sukho, DongYeop, Kangseok, & Kim, 2018)

A router monitors every packet that enters or leaves the network. In case an unintended unsolicited packet enters a network, the router has an inbuilt firewall that filters packets coming into a network. It makes sure the destination IP addresses are inside the network.

Wireless routers use Dynamic Host Configuration Protocol (DHCP) to randomly assign IP addresses to computers and other devices connected to a network. The router determines the network bandwidth (how fast or slow a network speed/performance can be). A router operates at the third layer of the OSI model.

Figure 5.5: A Cisco Wireless Router - Image Credit Cisco.com

Further reading

www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-vs-router.html#~switches

5.1.4 Network Interface Cards (NICs)

Also called LAN card or Ethernet card. It is an inbuilt device in the computer that helps to connect to a network. Every NIC has a MAC address. The MAC address is a machine-assigned unique identifier that maps the device to a network. It is a 48-bit number used in data communication. Without the NIC, there is no MAC address.

The NIC supports the RJ-45 connector. It converts data into digital signals before transmission. It has a slot for connecting Twisted Pair Cables while the other end can be connected to a modem, switch, or Wireless router.

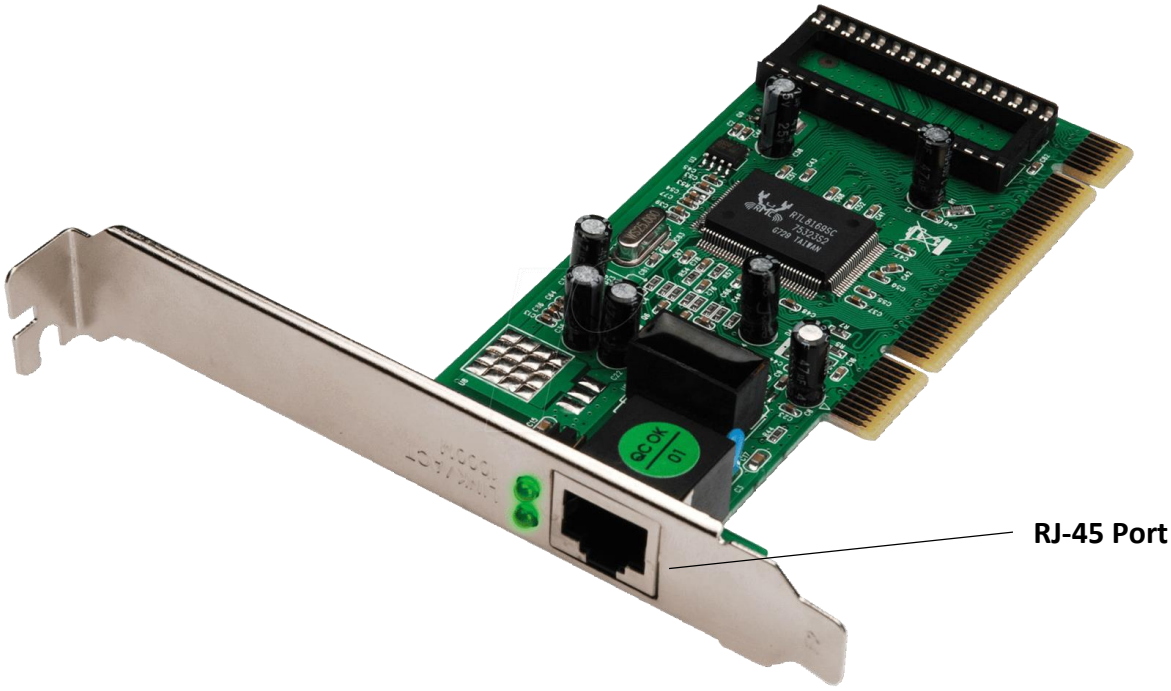


Figure 2.6: Network Interface Card. Credit - reichelt.com

Wireless network interface cards are used for wireless data communications. They are used by laptops to connect to a wireless access point (see Figure 14).

5.1.5 Bridge

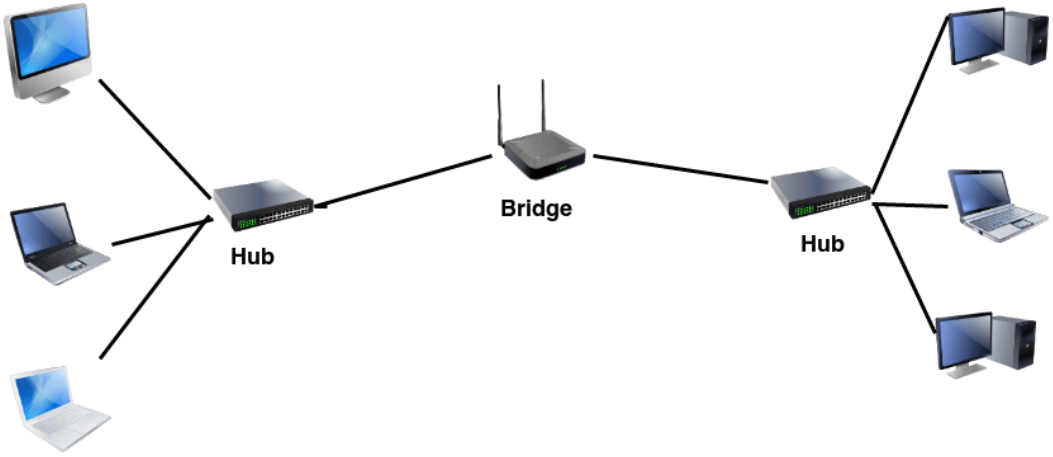


Figure 5.7: Network Bridge. (Image Credit - kencorner.com)

This is a network device that links or joins two different networks to function as a single network. From Figure 5.7, Bridging operates at the Datalink (layer 2) of the OSI model.

It connects multiple LANs to for a bigger LAN. The Bridge determines where to send the frame using a database. It can be in the same network or a connected network. If any of the network segments are wireless, it is called a Wireless Bridge.

5.1.6 Gateway

A gateway joins two networks with different protocols to communicate with each other, in the figure below, the typical example is presented. It is called a protocol converter because of its ability to provide compatibility between the different protocols used in the two different networks. It also stores information about the routing paths of the communicating networks.

Every communicating device that needs to communicate with another device outside a network must pass through a Gateway. Internal traffics inside a LAN does not pass through a Gateway. The gateway is implemented at the edge of a network. This shows that a gateway determines whether the network can communicate with each other.

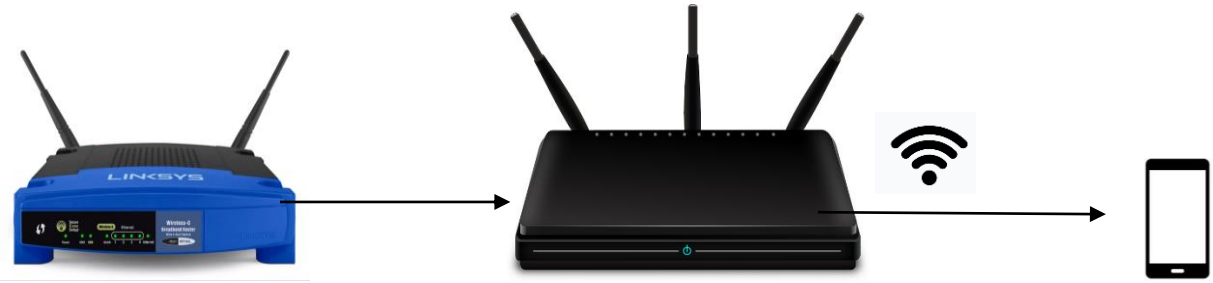
5.1.7 Modem

Refers to as Modulator-Demodulator. It helps computers to transmit data over telephone cables or telecommunications network. The data from a computer is in digital format, to transmit these data over telephone cables which uses analogue transmission, a Modem is required. A modem converts these digital signals (Modulation) into analogue signals and reconverts them (demodulation) at destination into analogue signals.

A modem can links a computer to a broadband network. Examples are dial up modem, cable modem, and DSL (Digital Subscriber Line).

5.1.8 Access Point

Access Point or Wireless Access Point is a networking device that uses Wireless LAN technology and allows users to connect to a wireless internet using their Wi-Fi. An access Point connects to a router and helps to extend the reach of a network. Access Points are used in restaurants, airports, hotels, schools, offices to extend the reach of the network.



Router **Access Point**

Figure 3: Access Points

Consider this scenario, accounts department moved to a new office, because of the distance with their former office, they do not have access to the network. You have been advised to connect them to the existing network. How can you achieve this?

5.1.9 Servers

A Server is a software or hardware that provides services to other computer/hosts called CLIENTS. Some hardware devices are dedicated servers (they are built solely as servers). A server provides range of services for the clients ranging from file services, printer services, email services, database services and other services as needed. Clients and Servers use the request-respond model – a client requests for a service, the server responds. Servers are named according to the services they provide.

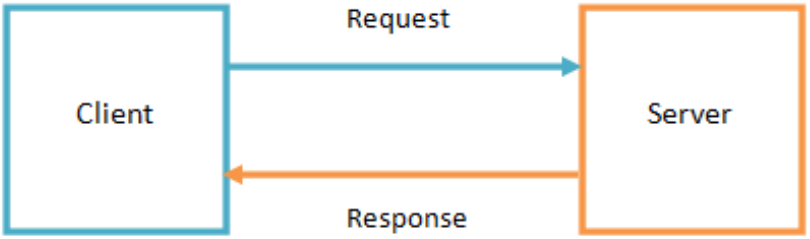


Figure 4: Client-Server process

Figure 5: Server Room with Servers

Which server provides a central access for files in a network or over the internet?

A. *Database Server*
B. *File Server*
C. *Print Server*
D. *Game servers*

5.2 Network Software

There is a wide range of software applications used in a network environment. They are used to manage, troubleshoot, and ensure the smooth operation of a computer network. Network software can also be defined as any software application that can be hosted on a network; this allows multiple users to use the software rather than a standalone software that is deployed on a personal computer that can only be accessed by a single user.

5.2.1 Network Operating Systems

Network Operating Systems (NOS) are specialized computer software that are used in workstations, personal computers, routers, switches, and other devices that are used in network management. They allow computers to share resources like files, printers, database, and internet.

5.2.2 Network Browsers

These are computer programs or software applications that allow users to access information on the World Wide Web (WWW).

A user accesses this information by typing the website address or Uniform Resource Locator (URL) e.g., www.myaddress.com on the address bar of the browser.

List three browsers you have used to access information from the internet.

Browsers retrieve data which includes text, audio, images, video, video games from web servers and displays them for the user to see. Browsers work on desktops, laptops, smartphones, and tablets. Some examples of browsers are Opera, Internet Explorer, Google Chrome, Apple Safari, Microsoft Edge, Mozilla Firefox, Apple Safari, and UC Browser.

5.3 Network Protocols

Network Protocols are a conventional rule that determine by that means data are exchanged in a computer network. It was necessary to set these protocols because network devices were produced by different manufacturers. These protocols enable devices to interact with one another. However, these protocols operate at separate layers on the OSI model

5.3.1 Application Layer Protocols

- **Domain Name System (DNS)** - this protocol maps domain names to IP address. It is regarded as the phonebook of the internet. Every website has an IP address, since it is difficult to memorize IP addresses. DNS servers convert the domain name we type on the browser's address bar to its IP address.

visit https://whatismyipaddress.com/hostname-ip to know the IP address of any website of your choice

- **Dynamic Host Configuration Protocol (DHCP)** - this protocol enables automatic assignment of IP addresses in a network. This is referred to as dynamic IP addressing. For example, when you connect to a hotspot or Wi-Fi, an IP address is automatically assigned to you. The DHCP makes this possible. If you disconnect from the network, the DHCP takes back the IP address assigned to you. This will be reassigned to a new user that connects to the network.
- **Simple Network Management Protocol (SNMP)** - permits network devices to share information within a network. A router can communicate with another network device like the switch. It also enables network monitoring and management by network administrators. This protocol helps to manage routers, switches, servers, workstations.
- **Simple Mail Transfer Protocol (SMTP)** - this protocol makes it possible to electronically transfer mails from one computer to another.
- **Hyper Text Transfer Protocol (HTTP)** - the secure HTTP is called HTTPS (secure). It allows the browser to request for text, images, audio, video from a web server. The web server is responsible for handling the request and relays the information back to the browser.
- **File Transfer Protocol (FTP)** – this protocol permits the transfer of files between a computer and a server. FTP is not secure; this allows passwords and usernames to be seen by hackers. To secure FTP, FTP secure (FTPS) is used. Another security mechanism is Secure Socket Layer (SSL certificates). TLS (Transport Layer Security) is commonly used with SSL i.e., SSL/TLS.
- **Internet Message Access Protocol (IMAP)** – permits users to retrieve email messages whenever there are from once they login to any device. It allows you to access messages on your mobile phones and computer at the same. IMAP enable operations like creation and deletion of emails.
- **Post Office Protocol (POP)** - this Protocol makes it possible for you to download all your messages on your computer. Once they are downloaded to the computer or any device, the messages are deleted from the email server.

- **Termination Emulation Protocol (TELNET)** - this Protocol allows a device to communicate with a remote device. The communication is done through the Command Line Interface (CLI) of a remote computer. This is called a Virtual terminal.

5.3.2 Transport Layer Protocols

- **Transmission Control Protocol (TCP)** - a connection-oriented protocol that ensures safe transmission of packets from one network to another. There must be a connection before data transfer. When a packet of data is sent over TCP, the recipient must always acknowledge what they received.
- **User Datagram Protocol (UDP)** - a connection less protocol that does not provide any guarantee of message delivery. UDP is suitable for purposes where error checking and correction are not necessary.

5.3.3 Network Layer Protocols

- **Internet Protocol (IPv4, IPv6)** - this protocol contains addressing information that ensure packets are delivered. For reliable delivery of data packets, IP is combined with TCP to form TCP/IP.
- **Internet Control Message Protocol (ICMP)** - this protocol is used by network devices to generate and send error messages when communicating with another IP address. For example, if a packet is too big and cannot be transmitted by a router, the router will discard the packet and send an ICMP message back to the original source that the message is too large.

5.3.4 Datalink Layer Protocol

- **Address Resolution Protocol (ARP)** - it maps the public internet address to a physical computer address (MAC addresses) in a LAN. The ARP helps the network devices to determine which computer/device in a network will receive an incoming packet. All computers have a unique MAC (Media Access Control) Address. It translates the 32 bits IP address to 48 bits MAC Address.

5.4 Network Standards

Network standards refers to rules required by different and diverse network technologies to interoperate with each other. This ensures that consumers are not locked with one manufacturer.

5.4.1 Types of Standards

- **De Facto Standards** - these are standards that are not formally approved by any standard organization. E.g., Microsoft Windows is not formally recognized by any standard organization, yet it is a standard in operating systems for microcomputers.
- **De Jure Standards** - these are standards that are formally developed or approved by a standard organization or a regulatory commission. There are many standards in use in computer networking.

5.4.2 List of Standard Organizations in Computer Networking

- International Standards Organization (ISO)
- International Telecommunication Union (ITU)
- Institute of Electronics and Electrical Engineers (IEEE)
- American National Standards Institute (ANSI)
- Internet Engineering Task Force (IETF)

5.4.3 Examples of Network Standards

- HTML, HTTP, SMTP, IMAP, TCP, IP, TCP/IP,
- **Wired Networks Standards** - Token Ring IEEE 802.5, Ethernet IEEE 802.3 (10Mbp), Fast Ethernet IEEE 802.3u (100Mbps), Gigabit Ethernet IEEE 802.3z (1,000Mbps), 10 Gigabit Ethernet IEEE 802.3ae (10,000Mbps).
- **Wireless Network Standards** - Wireless LAN IEEE 802.11.

5.5 Network Servers

Figure 6: Network Server

Network servers are computer software or hardware that provides resources, data services, repositories, storages, access, and security to other computers called CLIENTS. Client-

Server models work on a "***request-response relationship"***, the client requests for a service, then the server responds.

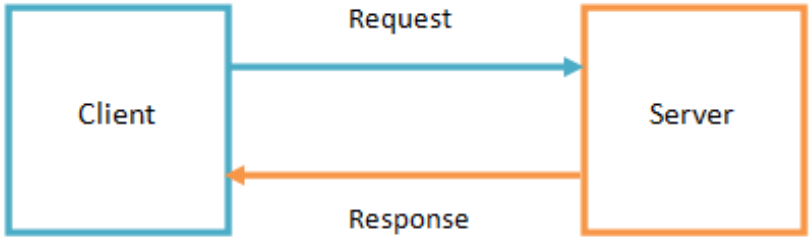


Figure 7:Client-Server Service

A server provides range of services for the clients ranging from file services, printer services, email services, database services and other services as needed. Servers are named according to the services they provide.

5.5.1 Examples of Servers in a Computer Network

Servers	Clients	Purpose
Database server e.g., Oracle Database, Microsoft SQL (Structured Query Language)	Microsoft Access,	Provides database services over a computer network
File server e.g., FTP (File Transfer Protocol) server	FTP clients	Allows for the transfer of files over the internet.
Mail server	Gmail application, Microsoft Outlook on your computer	Receives emails from client computers and sends them to the destination mail.
Web server	Web browsers	Handles client requests from the WWW
DNS (Domain Name System) server		Maps web addresses (URL) to IP addresses.

5.6 Network Security

These are measured taken to secure your network and network connectivity. Network security measures help to prevent unauthorized access and use of a network and protect the data stored on the network. Some networks like public internet access are free, while others can be restricted to external users.

3.6.1 Network Security Measures in a Local Area Network

a. **Authentication** – involves passwords, PINs (Personal Identification Numbers), secret codes, OTP (One Time Passwords).
b. **MAC filtering** – Here, the network administrator decides which device can access the network using their MAC addresses.
c. **Firewalls** – inspects inbound and outbound traffic and decides which traffic to grant or deny access based on some security rules. A firewall can decide to block traffic coming from this network 192.168.100.0/24 or traffic coming from www.google.com
d. **Frequent updates of your devices** – Frequent updates ensures the latest security updates are installed
e. **Provide frequent backup on important data** – in case of network failure, you can restore the previous data you have backed up.
f. **Physically secure your network devices** – sometimes your network can be attacked physically. An attacker can physically shutdown your network, delete important files. Always ensure that important systems are shielded from public access

5.7 Network Media

If two devices want to communicate with each other in a network, there must be a network medium. The media used for communication can be physical (guided) or wireless (unguided) (See categorization on Figure 22).

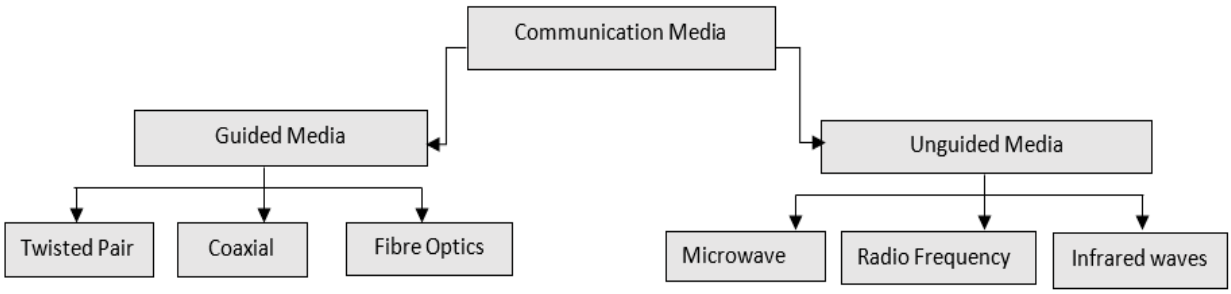


Figure 8: Network Media Categorization

5.7.1 Guided Media

Guided media uses Twisted Pair cable, Coaxial cable and fibre optics.

Twisted Pair Cables

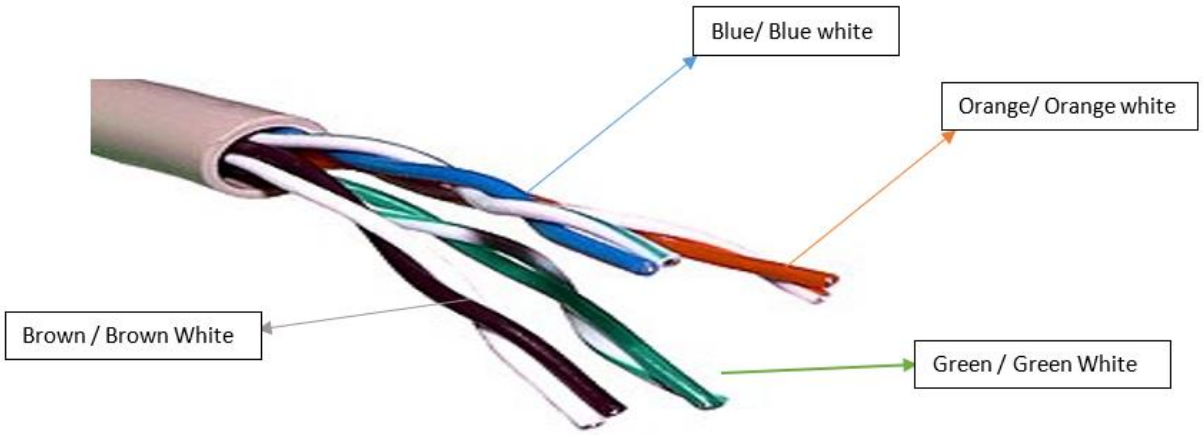


Figure 9:Twisted Pair Cables

A twisted pair cable is made of two insulated copper wires arranged in a regular helix pattern. Each wire is identified by its colour combination - a major colour and minor colour.

They are used for communication in Ethernet and telephone networks. The pairs are twisted to prevent crosstalk (unwanted transfer of signals between communication channels) as presented in Figure 23.

Crosstalk explained*- this occurs when magnetic fields are created around a network cable because of electrical current. As a result of this, two cable close to each will have a magnetic field that cancels each other. Any other outside magnetic field is also cancelled. A cable with twisted pair reduces this problem.*

Source: ciscopress.com

Types of Twisted Pa

A. **Unshielded Twisted Pair (UTP)** - does not have any physical covering that can block interference. Rather, UTP cable uses the cancellation effect created by the twisted wire pairs to reduce signal interference.

Figure 10:Unshielded Twisted pair

These are the categories of UTP Cables.

- **Category 1** - used for telephone communication. Not good for data communication.
- **Category 2** - Suitable for transmission of data at speed up to 4 Megabits per seconds (4Mbps).
- **Category 3** - Can transmission of data at speed up to 10Mbps.
- **Category 4** – supports transmission of data up to 16Mbps.
- **Category 5** – utilized in networks with speed up to 100Mbps.
- **Category 5e** - can support data at speed up to 1000Mbps or 1Gbps (Gigabits bits per seconds)
- **Category 6, 6a, 7** - up to 10Gbps.

B. **Shielded Twisted Pair (STP)** - uses a foil jacket to neutralize any outside interference. STP cables are used where exterior and outside cabling might be required. The shielding will protect the cable from environmental factors like sunlight, rainfall, and humidity. It is commonly used in critical network installations in big organizations.

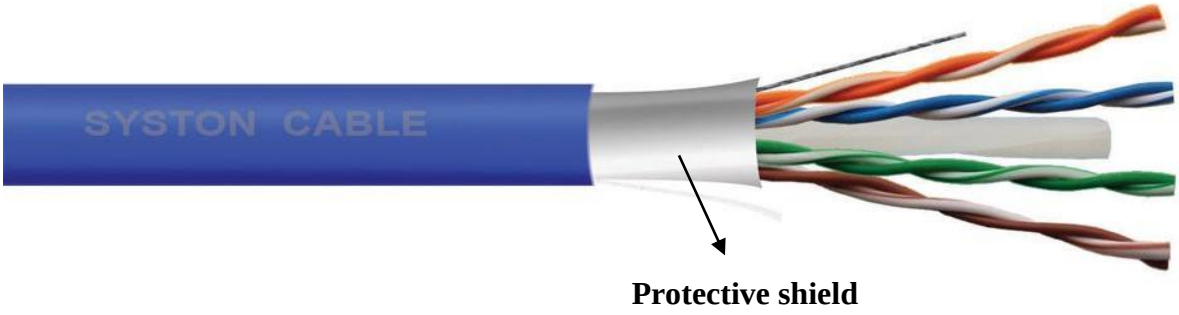


Figure 11: Syston Cable Shielded Twisted Pair

Coaxial Cables

Coaxial cables were designed to block interference unlike Twisted Pair Cables that can be affected by it. it is made up of a metallic shield located at the centre of the cable that helps to block interference. The middle core is made up an insulator cover that the inner wire from the metallic shield. It is commonly used for TV transmission. Coaxial cables are more expensive than twisted-pair cables and less cheap than fibre optics cable.

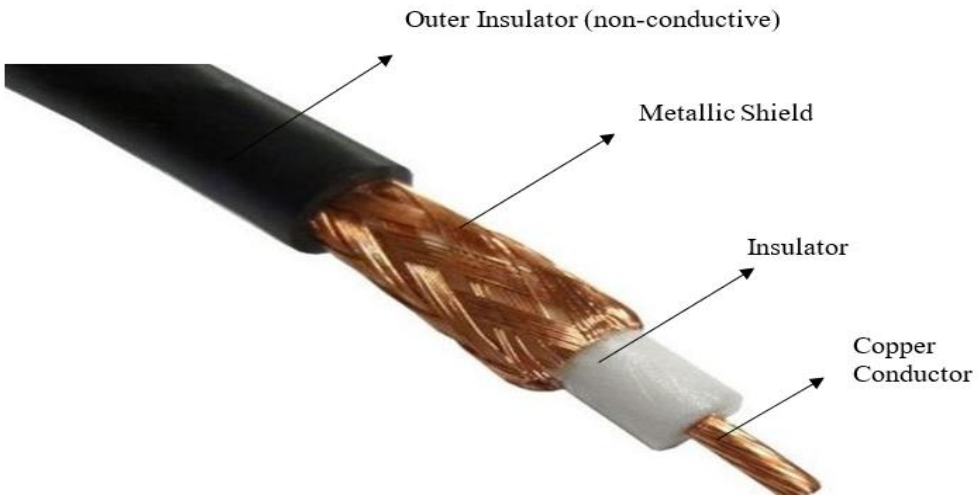


Figure 12: Coaxial Cables

Advantages of Coaxial cable:

- Allows for the transmission of data at high speed.
- It is better at blocking signal interference compared to twisted pair cable.
- It can transmit larger amount of data than twisted pair cables.

Disadvantages of Coaxial cable:

- It is costlier than twisted pair cable.
- There can be loss of signal as the cable length increases.

4.1.3 Fibre Optics

Figure 13: Fibre Optics

These cables contain as presented in Figure 27; optical fibres use light for data transmission. It has plastic coating that protects the optical fibres from high and low temperature, cold, electromagnetic interference from other types of wiring. It has the highest data transmission speed among coaxial and twisted pair cables.

Benefits of fibre optic cable over copper (Twisted and Coaxial)

- **Greater Bandwidth:** The fibre optics cable can carry larger amount of data at higher speed than coaxial and twisted pair cables.
- **Longer distances:** The fibre optics cable can carry data at a longer distance as compared to copper cable and twisted pair cables.

Cable Connectors

- **RJ-45 Connector –** used to connect a twisted pair cable to a computer. They have 8-pins that connects the 8-twisted pairs.

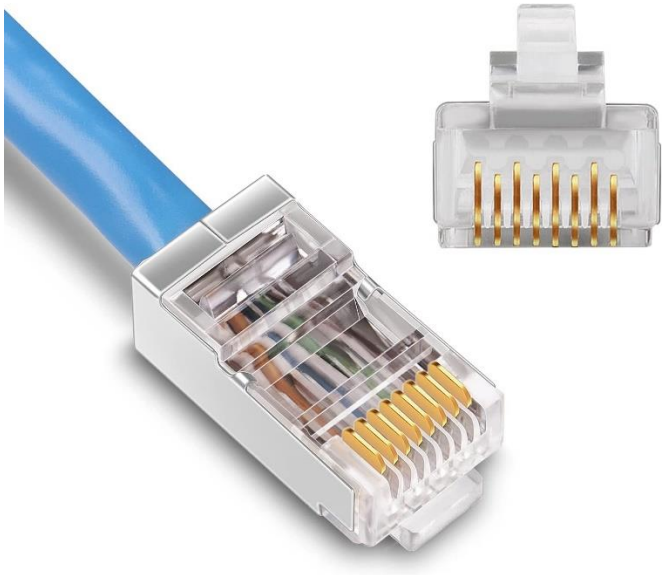


Figure 14: RJ-45 Connector. Credit - amazon.com

- **RJ-11 –** used for connecting telephone cables

Figure 15: RJ-11. Credit- indiamart.com

5.7.2 Unguided Medium

In unguided media, data is transmitted through air in form of electromagnetic waves. Unguided transmission media is divided into three categories - Radio Frequency (RF), Microwaves and Infrared Waves.

Radio Frequency (RF)

Also known as radio waves. The direction of the waves is in 360 degrees (moves in all directions). It can cover a large area and distance. This makes it suitable for Wide Area Networks (WAN). Radio waves on the other hand, have the capacity to penetrate walls in transmission, therefore it not hindered by obstacles or scintillations. Radio waves use frequencies between 3KHz (3 Kilohertz) and 1 GHz (1 Gigahertz). The Frequency Modulation (FM) radio is a good example of radio waves. Examples of data communications that uses radio waves are wireless routers, Bluetooth communications, mobile phones,

Microwaves

Figure 16:Satellite Microwave. Image Credit: https://www.technologyuk.net/

Microwaves transmit data at a frequency of 1GHz to 300GHz (example diagram in Figure 28). Unlike radio waves that transmits at all directions (omnidirectional), Microwaves transmits in a unidirectional form. Because of this, the transmitter and receiver must be in direct line of sight to each other.

A good example is the satellite antenna parabolic dish. Also, the receiver must be placed outside of the building to get a clear line of communication. Other examples are wireless LAN, cellular phones, and satellite networks.

There are two types of microwaves namely: Terrestrial and Satellite

Infrared Waves

Used for short-range communication, mostly used in TV/DVD remote controls, wireless mouse, printers, and keyboards. It operates at a frequency of 300GHz to 400GHz. It cannot penetrate walls like microwaves. Infrared waves are immune to interference.

Comparison Between Radio Waves, Microwaves and Infrared

From a detailed categorized description, Table 2 presents the properties of the Radio, Microwaves alongside the Infra-red

Table 1: Radio Waves, Microwaves and Infrared

	RADIO WAVES	MICROWAVE	INFRARED
DIRECTION	Omni-directional	Unidirectional	Unidirectional
FREQUENCY RANGE	3kHz – 1 GHz	1 GHz – 300GHz	300GHz – 400GHz
COMMUNICATION	Long distance communication	Long distance communication	Short distance communication
PENETRATION	Can penetrate walls	Cannot penetrate buildings	Cannot penetrate buildings