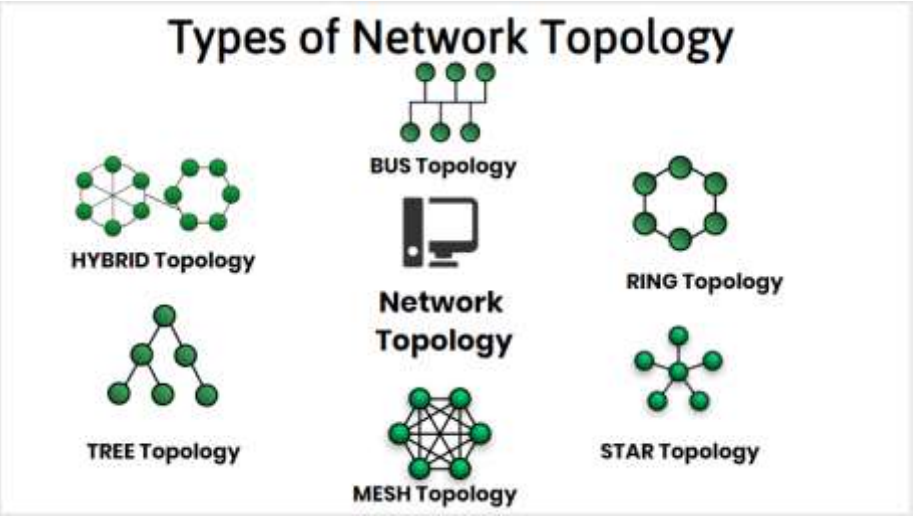
Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN

Name	**Pratik Pujari**		
UID no.	**2020300054**	**Class:**	**Comps C Batch**
Experiment No.	3		

AIM:	To find the network topologies and its commands
EXPERIMENT 1	
THEORY:	**What is Network Topology?** Network topology refers to the manner in which the links and nodes of a network are arranged to relate to each other. Topologies are categorized as either physical network topology, which is the physical signal transmission medium, or logical network topology, which refers to the manner in which data travels through the network between devices, independent of physical connection of the devices. Logical network topology examples include twisted pair Ethernet, which is categorized as a logical bus topology, and token ring, which is categorized as a logical ring topology. 

Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

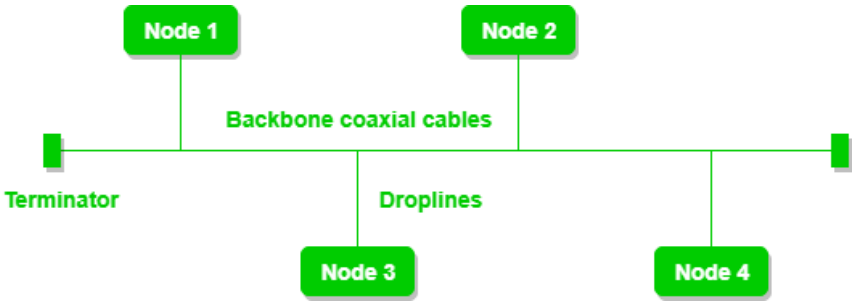
Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN

TYPES:

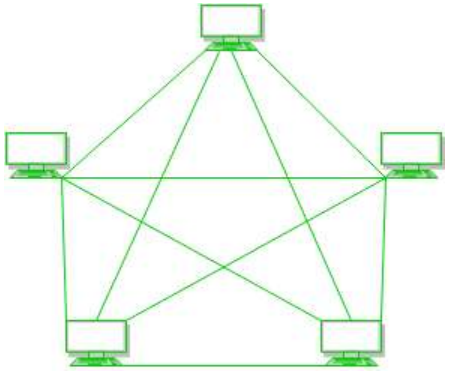
Types of Network Topology

There are several different logical and physical network topologies from which administrators can choose to build a secure, robust, and easily maintainable topology. The most popular configurations include:

- **Bus network topology** -- Also known as backbone network topology, this configuration connects all devices to a main cable via drop lines. The advantages of bus network topology lie in its simplicity, as there is less cable required than in alternative topologies, which makes for easy installation.

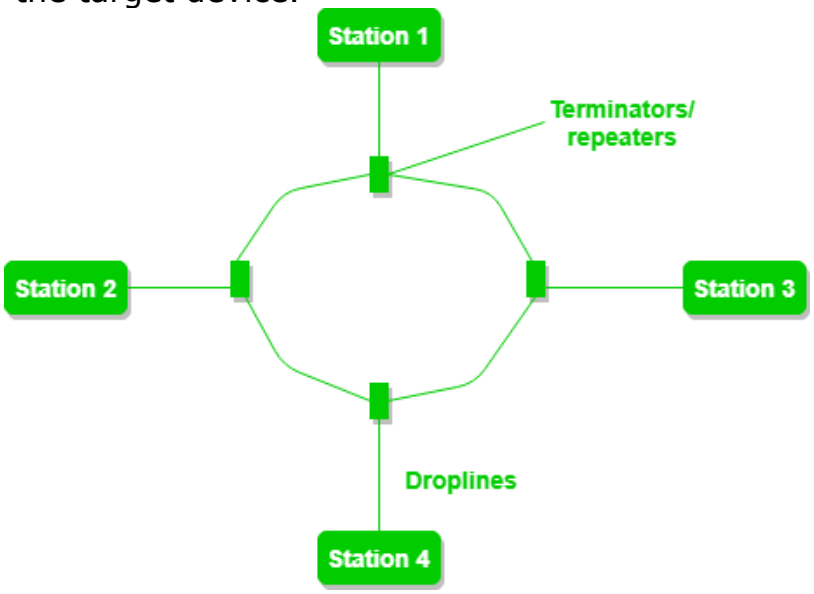


- **Mesh network topology** -- A dedicated point-to-point link connects each device on the network to another device on the network, only carrying data between two devices.

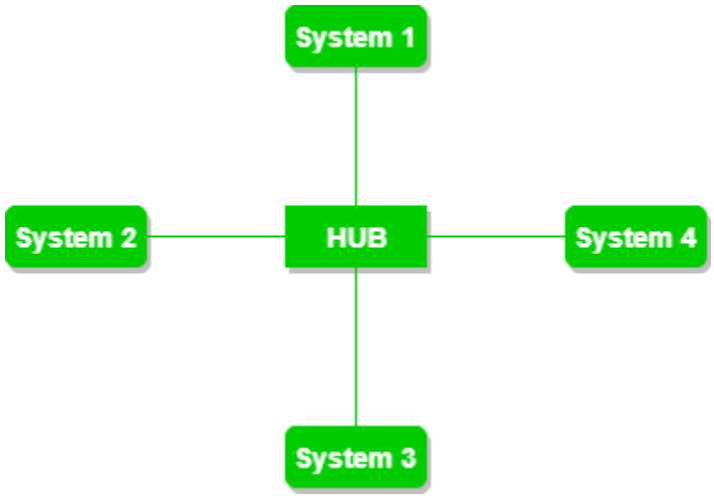


- **Ring network topology** -- Two dedicated point-to-point links connect a device to the two devices located

on either side of it, creating a ring of devices through which data is forwarded via repeaters until it reaches the target device.



- **Star network topology** -- The most common network topology, star topology connects each device in the network to a central hub. Devices can only communicate with each other indirectly through the central hub.

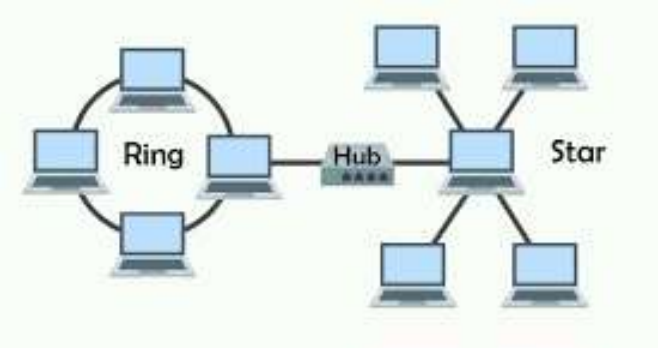


Computer Engineering Department
Engineering Department

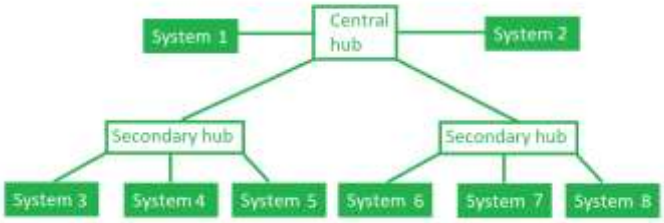
Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN

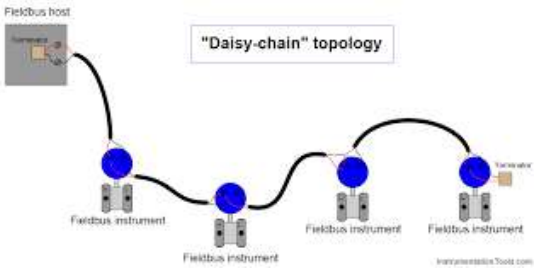
- **Hybrid network topology** -- Any combination of two or more topologies is a hybrid topology.



- **Tree network topology** -- This topology consists of a parent-child hierarchy in which star networks are interconnected via bus networks. Nodes branch out linearly from one root node, and two connected nodes only share one mutual connection.



- Daisy chain network topology -- In a daisy chain, one network node is attached to the next in a line or chain. A daisy chain topology can be linear, where the first and last two nodes are not connected, or a ring, where the first and last nodes are connected. ... A compromised network node can cut off any machines beyond that point.



Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

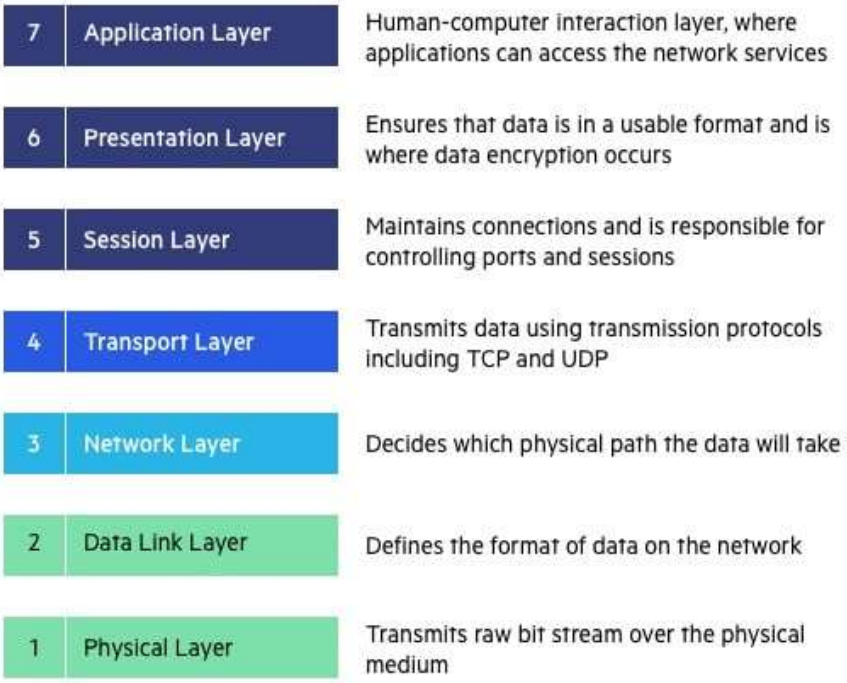
Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN

THEORY:

Network Layers



1. Physical Layer
The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

2. Data Link Layer
The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC)

3. Network Layer

	The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. **4. Transport Layer** The transport layer takes data transferred in the session layer and breaks it into "segments" on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, **5. Session Layer** The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. **6. Presentation Layer** The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer. **7. Application Layer** The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN

THEORY:	**What Is Network Hardware?** Network hardware is a set of physical or network devices that are essential for interaction and communication between hardware units operational on a computer network. These are dedicated hardware components that connect to each other and enable a network to function effectively and efficiently. Network hardware plays a key role as industries grow as it supports scalability. It integrates any number of components depending on the enterprise's needs. Network hardware helps establish an effective mode of communication, thereby improving the business standards. It also promotes multiprocessing and enables sharing of resources, information, and software with ease.
COMPONENTS:	• **Modems:** A modem enables a computer to connect to the internet via a telephone line. The modem at one end converts the computer's digital signals into analog signals and sends them through a telephone line. At the other end, it converts the analog signals to digital signals that are understandable for another computer. • **Routers:** A router connects two or more networks. One common use of the router is to connect a home or office network (LAN) to the internet (WAN). It generally has a plugged-in internet cable along with cables that connect computers on the LAN. Alternatively, a LAN connection can also be wireless (Wi-Fi-enabled), making the network device wireless. These are also referred to as wireless access points (WAPs). • **Hubs:** A hub broadcasts data to all devices on a network. As a result, it consumes a lot of bandwidth as many computers might not need to receive the broadcasted data. The hub could be useful in linking a few gaming consoles in a local multiplayer game via a wired or wireless LAN. • **Bridges:** A bridge connects two separate LAN networks. It scans for the receiving device before sending a message. This implies that it avoids unnecessary data transfers if the receiving device is not there. Moreover, it also checks to see whether the receiving device has already received the

message. These practices improve the overall performance of the network.

- **Network interface cards**: A network interface card (NIC) is a hardware unit installed on a computer, which allows it to connect to a network. It is typically in the form of a circuit board or chip. In most modern machines, NICs are built into the motherboards, while in some computers, an extra expansion card in the form of a small circuit board is added externally.
- **Network cables**: Cables connect different devices on a network. Today, most networks have cables over a wireless connection as they are more secure, i.e., less prone to attacks, and at the same time carry larger volumes of data per second.
- **Switches:** A switch is more powerful than a hub or a bridge but performs a similar role. It stores the MAC addresses of network devices and transfers data packets only to those devices that have requested Thus, when the demand is high, a switch becomes more efficient as it reduces the amount of latency.

Types of Network Switches

Here are some of the most common types of network switches, with more info on each below:

- KVM Switch
- Managed Switch
- Unmanaged Switch
- Smart Switch
- PoE Switch

KVM Switch

A KVM switch is an ideal interface for a single user that needs to control the functions of multiple computers from a single console. These devices can often be programmed with keyboard hotkeys that let you easily switch between PCs. With the addition of a KVM extender, the reach of the switch can be extended several hundred feet by transmitting DVI, VGA or HDMI video signals.

Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN

Managed Switch
A managed switch is exactly what it sounds like—a switch that requires some oversight by a network administrator. This type of switch gives you total control over the traffic accessing your network while allowing you to custom-configure each Ethernet port so you get maximum efficiency over data transfers on the network.

Unmanaged Switch
Unmanaged switches are generally made as plug-and-play devices and require little to no special installation beyond an Ethernet cable. The setup of this type of switch relies on auto-negotiation between Ethernet devices to enable communication between them.

Smart Switch
Another popular type of switch in networking is the smart switch, also referred to as an intelligent switch. These devices are a type of managed switch with only a select number of options for management. Rather than providing the full management functionality of a managed switch, a smart switch may only provide functionality to configure a handful of settings, like VLANs or duplex modes.

Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN

PoE Switch/Injector
PoE stands for power over Ethernet. A PoE switch distributes power over the network to different devices. This means any device on the network, from PCs to IP cameras and smart lighting systems, can function without the need to be near an AC access point or router, because the PoE switch sends both data and power to the connected devices.

Network Architecture: Key Components

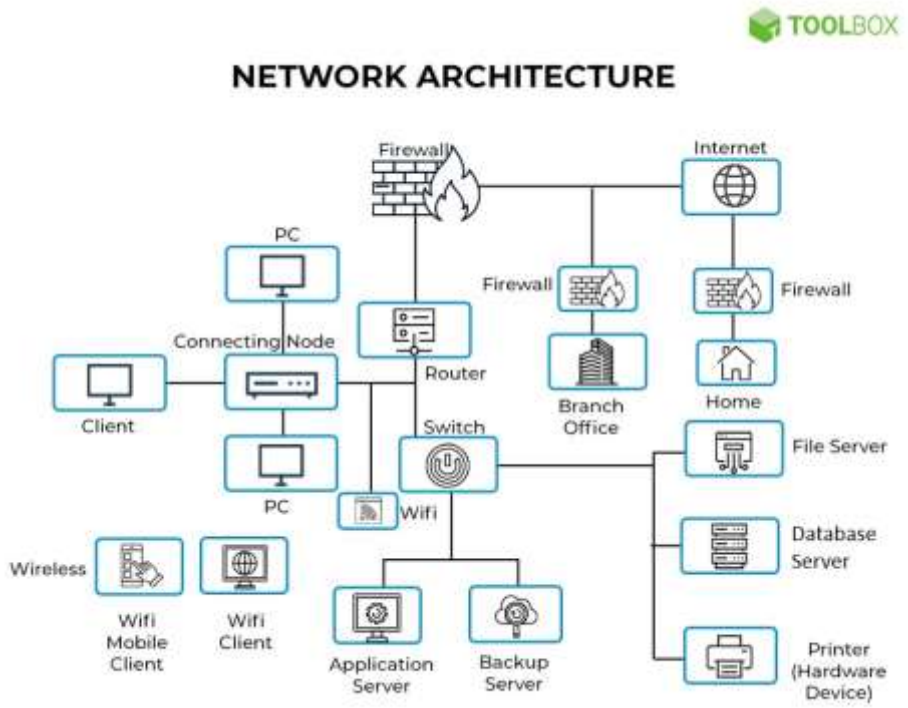
Network architecture defines the structural and logical design of a network. It constitutes hardware devices, physical connections, software, wireless networks, protocols, and transmission media. It gives a detailed overview of the whole network, which organizations use to create LAN, WAN, and other specific communication tunnels.

Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN



Network architecture can be viewed from different vantage points depending on the size and purpose of the network. WAN refers to a group of interconnected networks distributed over large distances, while LAN refers to a computer network that interconnects computers within a limited space. Therefore, the architecture of a WAN will vary from that of a LAN in a small office.

1. Hardware

Hardware refers to network devices that form the core of any network. These include user devices (laptops, PDAs, mobile phones), routers, servers, and gateways. The basic objective of any network architecture is to establish an efficient mechanism to transfer data from one hardware device to another.

2. Transmission media

	Transmission media encompasses all physical connections between network (hardware) devices. The properties of different transmission media determine the speed of data transfer from one endpoint to another. These can be wired and wireless. Wired media include physical wires or cables used for connections within a network, such as coaxial or fiber optics. On the other hand, wireless media operates on properties of microwave or radio signals, such as Wi-Fi or cellular. **3. Protocols** Protocols refer to the rules that govern data movement between network devices. Various machines on a network communicate with each other using this common protocol language. Without these protocols in place, it would be difficult for your iPhone to access a web page that is essentially stored on a Linux server. The nature of data decides the type of network protocol it needs to adopt. For example, transmission control protocol/internet protocol (TCP/IP) is used to connect to the internet, while file transfer protocol (FTP) is used for sending and receiving files to and from a server. Similarly, Ethernet protocol is used for connecting one computing device to another. **4. Topology** Network topology defines how the network is wired together and highlights the network's structure. This is important because variables such as distance between communicating devices can impact its data transfer speed, thereby affecting overall network performance.

Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

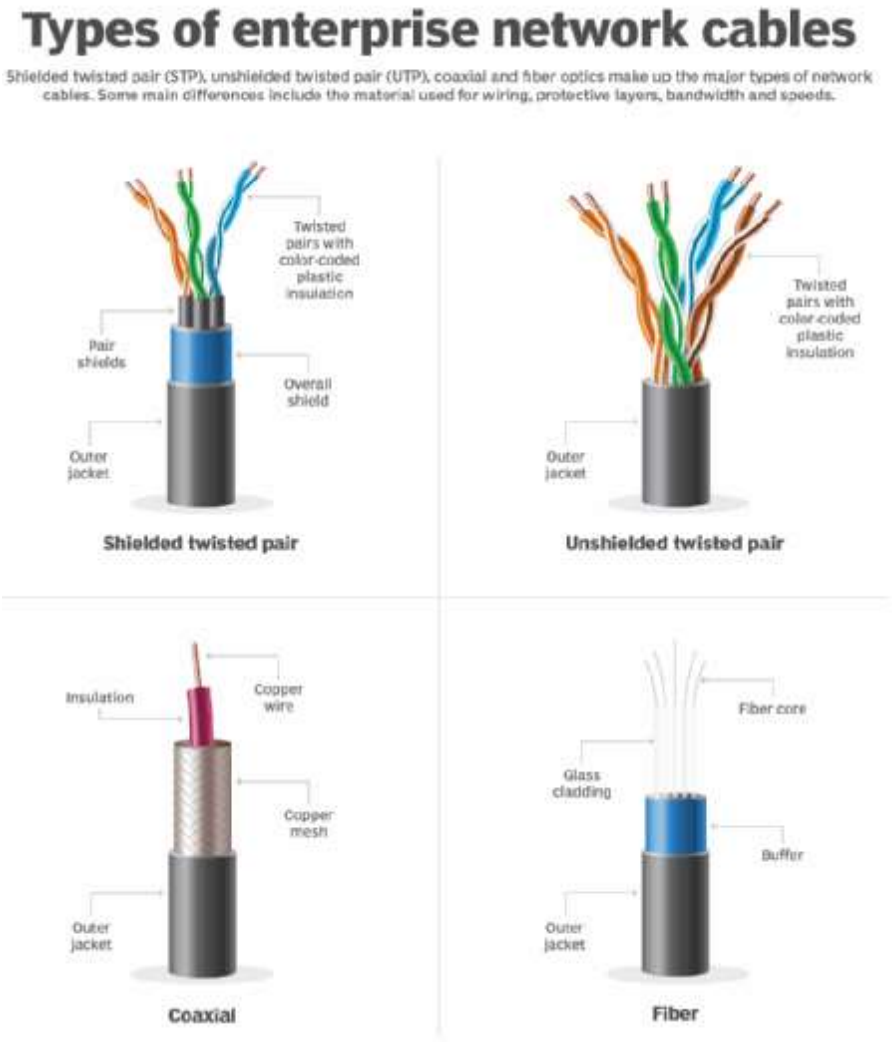
Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN

CABLES:

TYPES OF CABLES:



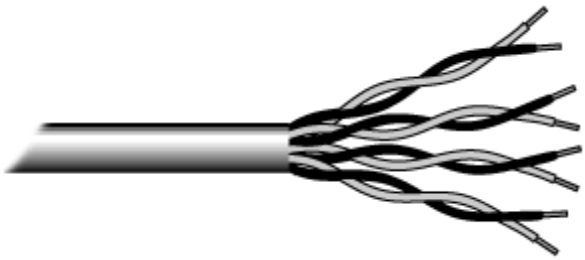
UnShielded Twisted pair Cable:

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks

Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN



The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot.

Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair)	100BaseT Ethernet
	1000 Mbps (4 pair)	Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

Shielded Twisted pair Cable:

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

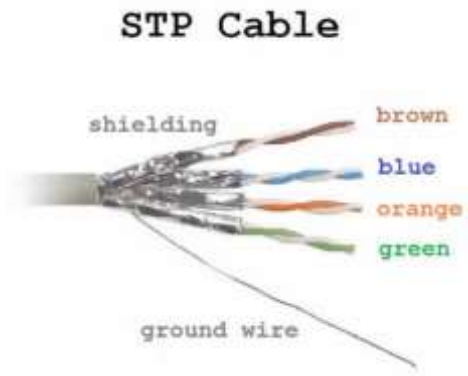
Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN

Shielded Twisted Pair (STP) Cable

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution.



Shielded twisted pair cable is available in three different configurations:

1. Each pair of wires is individually shielded with foil.
2. There is a foil or braid shield inside the jacket covering all wires (as a group).
3. There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

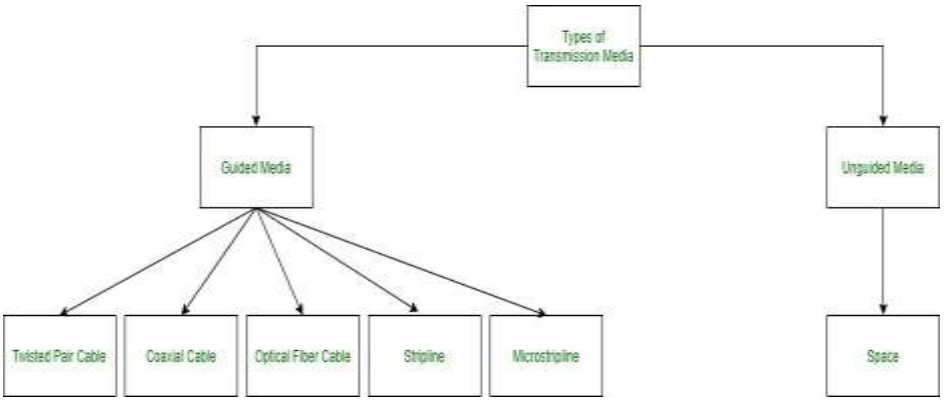
Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.
Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair.

Specification	Cable Type
10BaseT	Unshielded Twisted Pair
10Base2	Thin Coaxial
10Base5	Thick Coaxial

100BaseT	Unshielded Twisted Pair
100BaseFX	Fiber Optic
100BaseBX	Single mode Fiber
100BaseSX	Multimode Fiber
1000BaseT	Unshielded Twisted Pair
1000BaseFX	Fiber Optic
1000BaseBX	Single mode Fiber
1000BaseSX	Multimode Fiber

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another.



1. Guided Media:
It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.
Features:

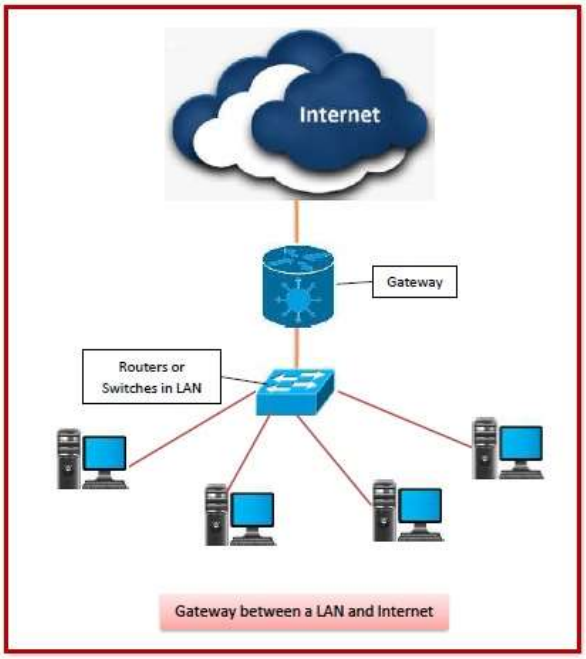
- High Speed
- Secure
- Used for comparatively shorter distances

Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN

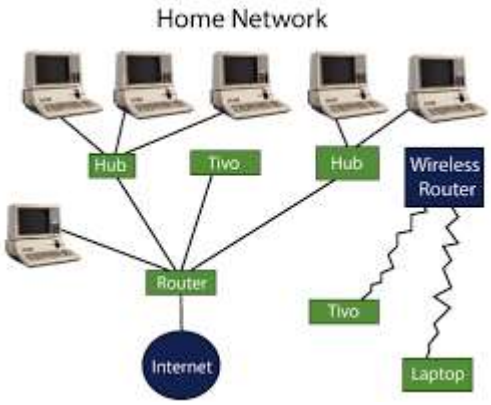
THEORY:	**GETWAYS**: A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model.  **ROUTER**:Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN



Features of Routers

- A router is a layer 3 or network layer device.
- It connects different networks together and sends data packets from one network to another.
- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
- It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.

FIREWALL: A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation

Why Do We Need Firewalls?

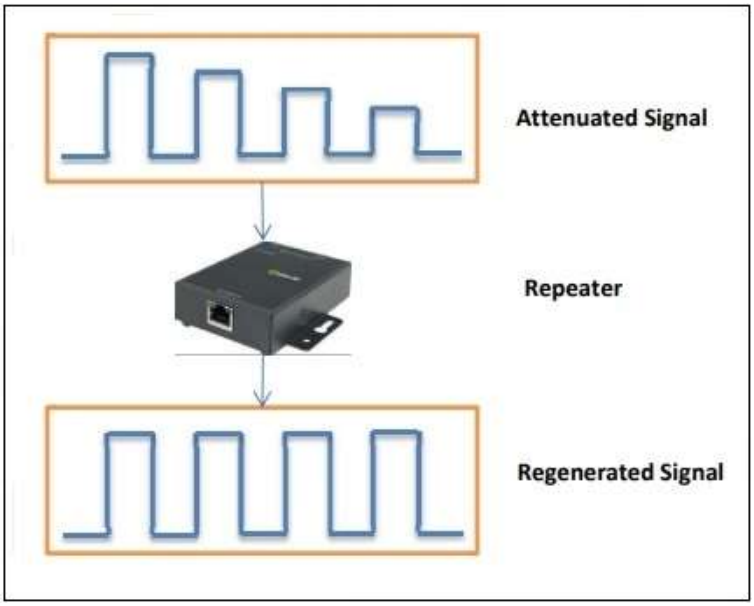
Firewalls, especially Next Generation Firewalls, focus on blocking malware and application-layer attacks. Along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls are able to react quickly and seamlessly to detect and combat attacks across the whole network.

Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN

	Types of Firewalls • **Packet filtering** A small amount of data is analyzed and distributed according to the filter's standards. • **Proxy service** Network security system that protects while filtering messages at the application layer. • **Stateful inspection** Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall. • **Next Generation Firewall** (NGFW) Deep packet inspection Firewall with application-level inspection.
THEORY:	**Repeaters:** Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters. 

Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Computer Engineering Department
Engineering Department

Academic Year: 2021-2022

Class: S.Y.B.Tech **Sem.:** 4 **Course:** CCN

Why are Repeaters needed?

When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals.

Types of Repeaters

According to the types of signals that they regenerate, repeaters can be classified into two categories −

- **Analog Repeaters** − They can only amplify the analog signal.
- **Digital Repeaters** − They can reconstruct a distorted signal.

According to the types of networks that they connect, repeaters can be categorized into two types −

- **Wired Repeaters** − They are used in wired LANs.
- **Wireless Repeaters** − They are used in wireless LANs and cellular networks.

According to the domain of LANs they connect, repeaters can be divided into two categories −

- **Local Repeaters** − They connect LAN segments separated by small distance.
- **Remote Repeaters** − They connect LANs that are far from each other.

RESULT: I learnt about the different networking hardware and networking topologies. Different types of hardware used in day-to-day life is used in networking. Learnt about the different layers of networking.