**CT043-3-1 : Introduction to Networking**

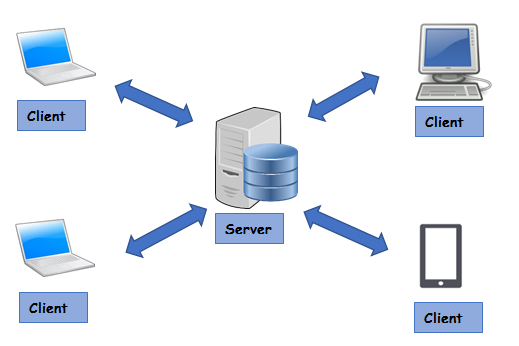
**Chapter 1.**

1. Differentiate between Host and P2P

|  |  |
| --- | --- |
| Host/ client sever | P2p |
| 1.In Client-Server Network, Clients and server are differentiated, Specific server and clients are present.  2. Client-Server Network focuses on information sharing. | 1. In Peer-to-Peer Network, Clients and server are not differentiated  2. While Peer-to-Peer Network focuses on connectivity. |

1. What do you understand by Client and Server?

Ans.Client-server denotes a relationship between cooperating programs in an application, composed of clients initiating requests for services and servers providing that function or service



3.Explain in details about End Devices and Intermediary Devices

1. End device

A source or destination device in a networked system. For example, a user's PC is an end device, and so is a server. Network switches, routers and other equipment work in between to enable messages to travel from one end device to the other. See edge router.

2.I*ntermediary Device*

*I*ntermediary Device is any networking device positioned between a Remote Access Service (RAS) server and a RAS client. Intermediary devices are third-party devices for performing security-related tasks such as authentication, encryption, and other functions.

4. Describe about LAN and WAN Networks.

**Local Area Networks (LAN)**

Local Area Network (LAN) is a computer network, which is limited to a small office, single building, multiple buildings inside a campus etc. Typically, a Local Area Network (LAN) is a private network owned and maintained by a single organization.

Below image shows a small Local Area Network (LAN) connected together using a Network Switch.

## Wide Area Networks (WAN)

A Wide Area Network (WAN) spans over multiple geographic locations, which is composed of multiple LANs. It is nearly impossible for a small to medium organization (except Network Service Providers) to pull network cables between their two offices in two different countries located 1000s of kilometers away. Network Service Providers (also called as ISPs) provide the connectivity solutions for Wide Area Networks (WAN).

5. write a short note on

**1.Fault tolerance:** Fault tolerance refers to the ability of a system (computer, network, cloud cluster, etc.) to continue operating without interruption when one or more of its components fail.

6. Explain what do you understand by BYOD? How can this help with our learning?

The latest IT trend in town, BYOD or Bring Your Own Device, is a practice where employees are encouraged to make use of their personal devices to access enterprise systems and data. Being a small part of the larger trend of ‘IT consumerization’ – where hardware and software of the customer are allowed into organizational premises – BYOD is a movement that affects each individual in the company, from the CEO to the hourly worker.

1. Employee Satisfaction:

When you allow employees to bring their own set of devices they may have invested in rather than the ones chosen by the IT department, they are satisfied at some level – and you know how important it is to keep employees satisfied. 60% of users are said to give more importance to their mobile phones than even to a cup of coffee.

2. Cost Savings:

Cost cutting is a major consideration for most enterprises. With a BYOD policy in place, there is a shift of costs from employers to employees, resulting in savings.

3. Increased Productivity and Innovation:

There is a positive correleation between the comfort-level of employees and their productivity. With their own devices, employees get comfortable and master their use.

7.Differentiate between intranet, extranet and internet.

**1. Internet :**  
The network formed by the co-operative interconnection of millions of computers, linked together is called Internet. Internet comprises of :

* **People :** People use and develop the network.
* **Resources :** A collection of resources that can be reached from those networks.
* **A setup for collaboration :** It includes the member of the research and educational committees worldwide.

**2. Intranet :**  
It is an internal private network built within an organization using Internet and World Wide Web standards and products that allows employees of an organization to gain access to corporate information.

**3. Extranet :**  
It is the type of network that allows users from outside to access the Intranet of an organization.

8.What Is Cloud Computing?

Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software.

9. What is a Security Threat?

Security Threat is defined as a risk that which can potentially harm computer systems and organization. The cause could be physical such as someone stealing a computer that contains vital data. The cause could also be non-physical such as a virus attack.

How can we ,minimize it

**1. Protect the physical location of your data**

#### ****Educate employees about security measures****

#### ****3. Implement best practices for password security.****

#### ****4. Install user action monitoring software****

Chapter 2.

1. Define the following terms:

**a. IOS Access**

## IOS (Internetwork Operating System)?

IOS is an operating system developed by Cisco Systems for its line of routers and access servers to provide a standard way to configure these devices.

**b. running configuration**

A running **configuration** resides in a device's RAM, so if a device loses power, all configured commands will be lost.

**c. startup configuration**

A startup configuration is stored in the nonvolatile memory of a device, which means that all **configuration** changes are saved even if the device loses power.

1. **Explain he following configuration and sub configuration modes:**

**a. Global configuration mode**

**b. Line configuration mode**

**c. Interface configuration mode**

1. **Global configuration mode**

* Global Configuration mode mode allows users to modify the running system configuration. From the Privileged mode a user can move to configuration mode by running the "configure terminal" command from privileged mode. To exit configuration mode, the user can enter "end" command or press Ctrl-Z key combination.

1. **line configuration mode**

* Line configuration mode commands allow you to configure the virtual terminal line settings. To configure the virtual terminal line settings and access line configuration mode, use the line vty command in configuration mode. The CLI prompt changes to (config-line).

**C. Interface configuration mode**

* To enter interface configuration mode, enter the interface configuration command. Interface configuration From global configuration mode, specify an interface by entering the interface command followed by an interface identification. To exit to privileged EXEC mode, enter the end command, or press Ctrl-Z.

**4. What are ports and interfaces? Explain with examples**

**PORT**

Ans. >> In computer networking, a port is a communication endpoint. At the software level, within an operating system, a port is a logical construct that identifies a specific process or a type of network service. A port is identified for each transport protocol and address combination by a 16-bit unsigned number, known as the port number.

**Interface**s

In computing, a network interface is a software or hardware interface between two pieces of equipment or protocol layers in a computer network.

A network interface will usually have some form of network address. This may consist of a node identifier and a port number or may be a unique node ID in its own right.

**5.How can we use telnet and ping command in Networking?**

## ANs.>> Ping Specific Port using telnet

**The easiest way to ping a specific port is to use the telnet command followed by the**[**IP address**](https://devconnected.com/how-to-get-your-ip-address-on-linux/)**and the port that you want to ping.**

You can also specify a domain name instead of an IP address followed by the specific port to be pinged.

$ telnet <ip\_address> <port\_number>

$ telnet <domain\_name> <port\_number>

The “telnet” command is valid for **Windows**and **Unix**operating systems.

**6. What is IP address? What are its types? Explain the need for using IP address.**

Ans.>> IP address stands for internet protocol address; it is an identifying number that is associated with a specific computer or computer network. When connected to the internet, the IP address allows the computers to send and receive information.

There are four types of IP addresses:

* public
* private
* static
* dynamic

Need to using IP address

* An internet protocol (IP) address allows computers to send and receive information.
* An IP address allows information to be sent and received by the correct parties, which means they can also be used to track down a user's physical location.

Chapter 3.

1. Discuss about the network protocol requirement in details.

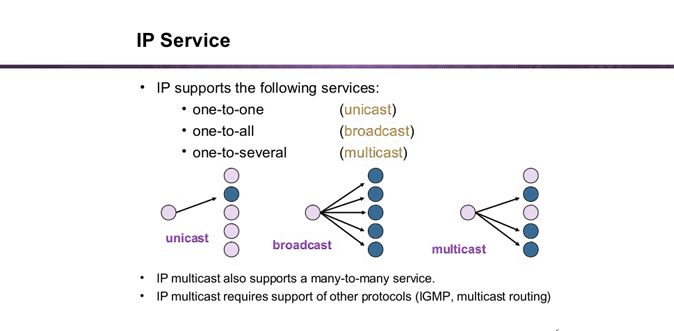
Network protocols are sets of established rules that dictate how to format, transmit and receive data so computer network devices -- from servers and routers to endpoints -- can communicate regardless of the differences in their underlying infrastructures, designs or stand Support for network protocols can be built into software, hardware or both.

1. Illustrate the following with example and a figure.

Unicast: from one source to one destination i.e. One-to-One

Broadcast: from one source to all possible destinations i.e. One-to-All

Multicast: from one source to multiple destinations stating an interest in receiving the traffic i.e. One-to-Many



5.Explain different layers of OSI model and the function associated with each layer

**OSI model**

The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system.

**Physical Layer**

The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device. It can include specifications such as voltages, pin layout, cabling, and radio frequencies. At the physical layer, one might find “physical” resources such as network hubs, cabling, repeaters, network adapters or modems.

**Data Link Layer**

At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer.

The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

**Network Layer**

The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

**Transport Layer**

The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol.

**Session Layer**

The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and termined at layer 5. Session layer services also include authentication and reconnections.

**Presentation layer**

The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it at times also called the syntax layer. This layer can also handle the encryption and decryption required by the application layer.

Application Layer

At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resource availability, and synchronizes communication.

**6. Explain in details about the different protocols used in TCP/IP models.**

## Four Layers of TCP/IP model

In this TCP/IP tutorial, we will learn about different TCP/IP layers

Four Layers of TCP/IP model

In this TCP/IP tutorial, we will learn about different TCP/IP layers

**Application Layer**

Application layer interacts with an application program, which is the highest level of OSI model. The application layer is the OSI layer, which is closest to the end-user. It means the OSI application layer allows users to interact with other software application.

The function of the application Layers are:

**Transport Layer**

Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system. It is hosted using single or multiple networks, and also maintains the quality of service functions.

**Internet Layer**

An internet layer is a second layer of TCP/IP layes of the TCP/IP model. It is also known as a network layer. The main work of this layer is to send the packets from any network, and any computer still they reach the destination irrespective of the route they take.

**The Network Interface Layer**

Network Interface Layer is this layer of the four-layer TCP/IP model. This layer is also called a network access layer. Its helps you to defines details of how data should be sent using the network.

. Define the following terms:

* **Protocol Data Unit**
* In telecommunications, a protocol data unit (PDU) is a single unit of information transmitted among peer entities of a computer network.
* **Segments**
* a network segment is an electrical connection between networked devices using a shared medium.
* **Packets**
* In networking, a packet is a small segment of a larger message. Data sent over computer networks\*, such as the Internet, is divided into packets. These packets are then recombined by the computer or device that receives them.

**Frame**

* A frame is a digital data transmission unit in computer networking and telecommunication.

**Bits**

* A bit (short for binary digit) is the smallest unit of data in a computer. A bit has a single binary value, either 0 or 1.

Chapter 4

1. Describe in brief about physical layer components.

* The physical layer defines the relationship between a device and a transmission medium, such as a copper or optical cable. This includes the layout of pins, voltages, cable specifications, hubs, repeaters, network adapters, host bus adapters (HBA used in storage area networks) and more.

3. Describe in brief the characteristics and types of copper cabling.

* Cooper Cabling is one of the two basic types of physical cabling media (the other being glass or fiber-optic cabling). Copper cabling is cheap and flexible, but it is susceptible to electromagnetic interference (EMI).

1. UTP Copper Cabling

UTP cabling of category 6 grade is the most commonly used copper cabling in networking environments today. Category 6 cabling (CAT6 cabling) comes in either solid core or stranded cabling.

5. Explain the characteristics and types of fiber optics cable.

* Extremely high throughput.
* Very high resistance to noise.
* Excellent **security**.
* Ability to carry signals for much longer distances before requiring repeaters than copper cable.
* Industry standard for high-**speed** networking.

Chapter 5

* 1. What is Data Link layer? Explain in brief the function of data link sub layers.
* The data link layer is the protocol layer in a program that handles the moving of data into and out of a physical link in a network.

The data link layer has three main functions:

It handles problems that occur as a result of bit transmission errors.

It ensures data flows at a pace that doesn't overwhelm sending and receiving devices.

It permits the transmission of data to Layer 3, the network layer, where it is addressed and routed.

3. Explain various types of WAN Topologies.

**WAN Topologies**

Interconnecting multiple sites across WANs can involve a variety of service provider technologies and WAN topologies. Common WAN topologies are

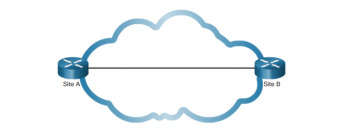
Point-to-point topology

Hub-and-spoke topology

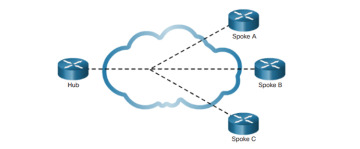
Full mesh topology

Dual-homed topology

* + 1. **Point-to- point topology**

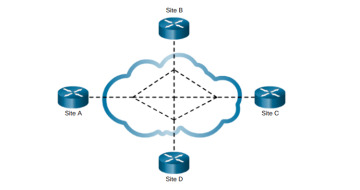
****A point-to-point topology, as shown in Figure, employs a point-to-point circuit between two endpoints. Typically involving dedicated leased-line connections like a T1 or an E1 line, a point-to-point connection provides a Layer 2 transport service through the service provider network. Packets sent from one site are delivered to the other site and vice versa. A point-to-point connection is transparent to the customer network, as if there was a direct physical link between two endpoints.

* 1. **hub-and- spoke**



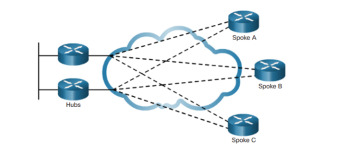
If a private network connection between multiple sites is required, a point-to-point topology with multiple point-to-point circuits is one option. Each point-to-point circuit requires its own dedicated hardware interface that will require multiple routers with multiple WAN interface cards. This interface can be expensive. A less expensive option is a point-to-multipoint topology, also known as a hub-and-spoke topology.

* 1. **Full mesh**



One of the disadvantages of hub-and-spoke topologies is that all communication has to go through the hub. With a full mesh topology using virtual circuits, any site can communicate directly with any other site. The disadvantage here is the large number of virtual circuits that need to be configured and maintained. Figure 1-4 displays a sample full mesh topology consisting of four routers connected to each other across a WAN cloud.

* 1. **Dual-homed Topology**



A dual-homed topology provides redundancy. As shown in Figure 1-5, the spoke routers are dual-homed and redundantly attached to two hub routers across a WAN cloud. The disadvantage to dual-homed topologies is that they are more expensive to implement than a single-homed topology. The reason is that they require additional networking hardware, like additional routers and switches.

* 1. **Explain various types of LAN Topologies.**

Gseometric representation of how the computers are connected to each other is known as topology. There are five types of topology – Mesh, Star, Bus, Ring and Hybrid.

Types of Topology

There are five types of topology in computer networks:

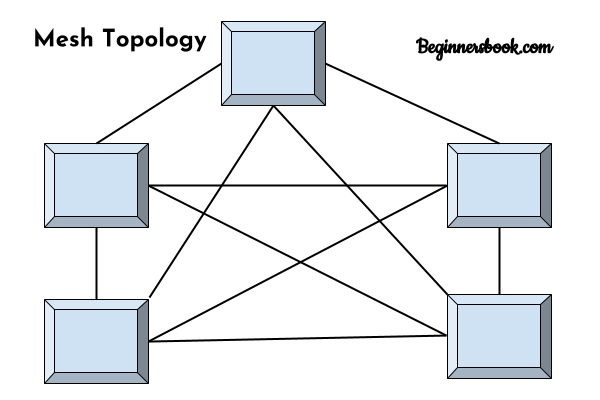
Types of Topology

1. Mesh Topology

2. Star Topology

3. Bus Topology

4. Ring Topology



**Mesh Topology**

In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated it means that the link only carries data for the two connected devices only. Lets say we have n devices in the network then each device must be connected with (n-1) devices of the network. Number of links in a mesh topology of n devices would be n(n-1)/2.

Advantages of Mesh topology

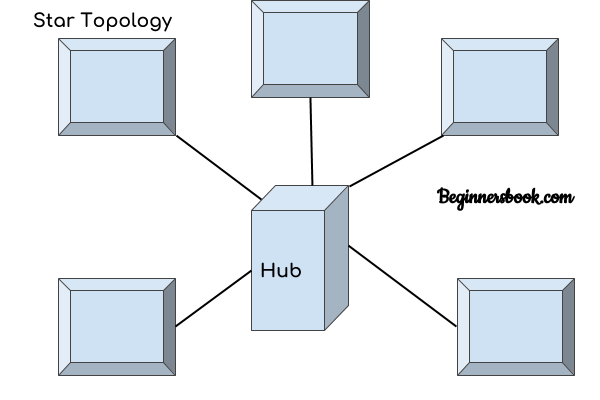
1. No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.

2. Mesh topology is reliable and robust as failure of one link doesn’t affect other links and the communication between other devices on the network.

3. Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.

4. Fault detection is easy.

## Star Topology

  
In star topology each device in the network is connected to a central device called hub. Unlike Mesh topology, star topology doesn’t allow direct communication between devices, a device must have to communicate through hub. If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.

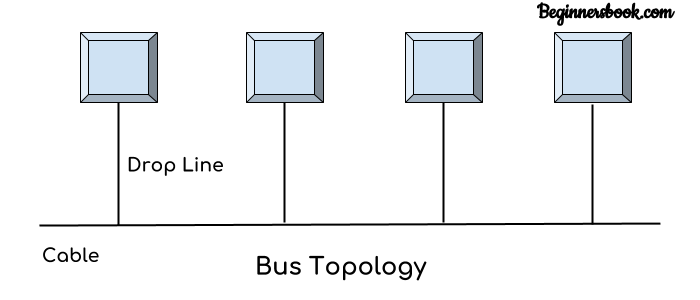
### Advantages of Star topology

1. Less expensive because each device only need one I/O port and needs to be connected with hub with one link.  
2. Easier to install  
3. Less amount of cables required because each device needs to be connected with the hub only.  
4. Robust, if one link fails, other links will work just fine.  
5. Easy fault detection because the link can be easily identified.

### Disadvantages of Star topology

1. If hub goes down everything goes down, none of the devices can work without hub.  
2. Hub requires more resources and regular maintenance because it is the central system of star topology.

## Bus Topology

  
In bus topology there is a main cable and all the devices are connected to this main cable through drop lines. There is a device called tap that connects the drop line to the main cable. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

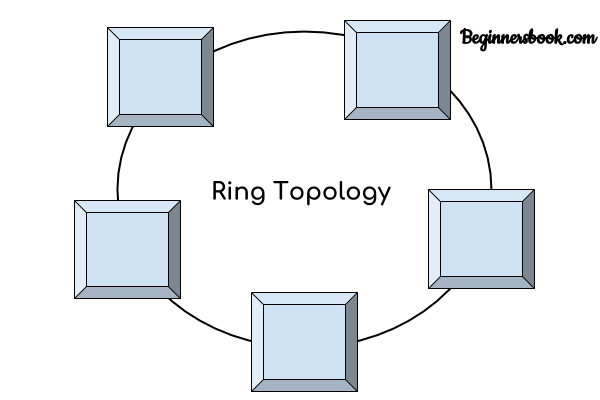
### Advantages of bus topology

1. Easy installation, each cable needs to be connected with backbone cable.  
2. Less cables required than Mesh and star topology

### Disadvantages of bus topology

1. Difficultly in fault detection.  
2. Not scalable as there is a limit of how many nodes you can connect with backbone cable.

## Ring Topology

  
In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it. This structure forms a ring thus it is known as ring topology. If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

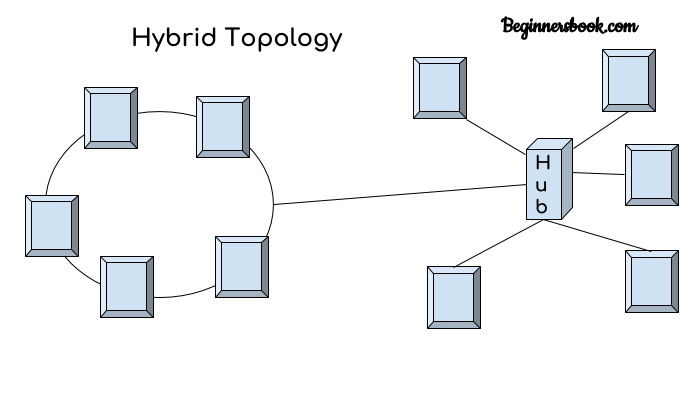
### Advantages of Ring Topology

1. Easy to install.  
2. Managing is easier as to add or remove a device from the topology only two links are required to be changed.

### Disadvantages of Ring Topology

1. A link failure can fail the entire network as the signal will not travel forward due to failure.  
2. Data traffic issues, since all the data is circulating in a ring.

## Hybrid topology

  
A combination of two or more topology is known as hybrid topology. For example a combination of star and mesh topology is known as hybrid topology.

### Advantages of Hybrid topology

1. We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.  
2. Scalable as we can further connect other computer networks with the existing networks with different topologies.

### Disadvantages of Hybrid topology

1. Fault detection is difficult.  
2. Installation is difficult.  
3. Design is complex so maintenance is high thus expensive.

5. Differentiate the following:

a. Half and Full Duplex Communication.

Differences Between Full and Half Duplex Systems

There are distinct differences between full and half-duplex systems. With half-duplex mode, each transmitted character is immediately displayed on a monitor. If a device is operating in full-duplex mode, transmitted data does not appear on-screen until it is received and returned. Full-duplex Ethernet does save time when compared to half-duplex because it alleviates collisions and frame retransmissions. Sending and receiving are separate functions, creating a system where there is full data capacity in each direction. In contrast, half-duplex can be used to conserve bandwidth.