Unit 1(S1)

What is a Router?

The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. There are some popular companies that develop routers; such are **Cisco**, **3Com**, **HP**, **Juniper**, **D-Link**, **Nortel**, etc. Some important points of routers are given below:

- A router is used in **LAN** (Local Area Network) and **WAN** (Wide Area Network) environments. For example, it is used in **offices** for connectivity, and you can also establish the connection between distant networks such as from **Bhopal** to delhi.
- It shares information with other routers in networking.
- It uses the routing protocol to transfer the data across a network.
- Furthermore, it is more **expensive** than other networking devices like switches and hubs.

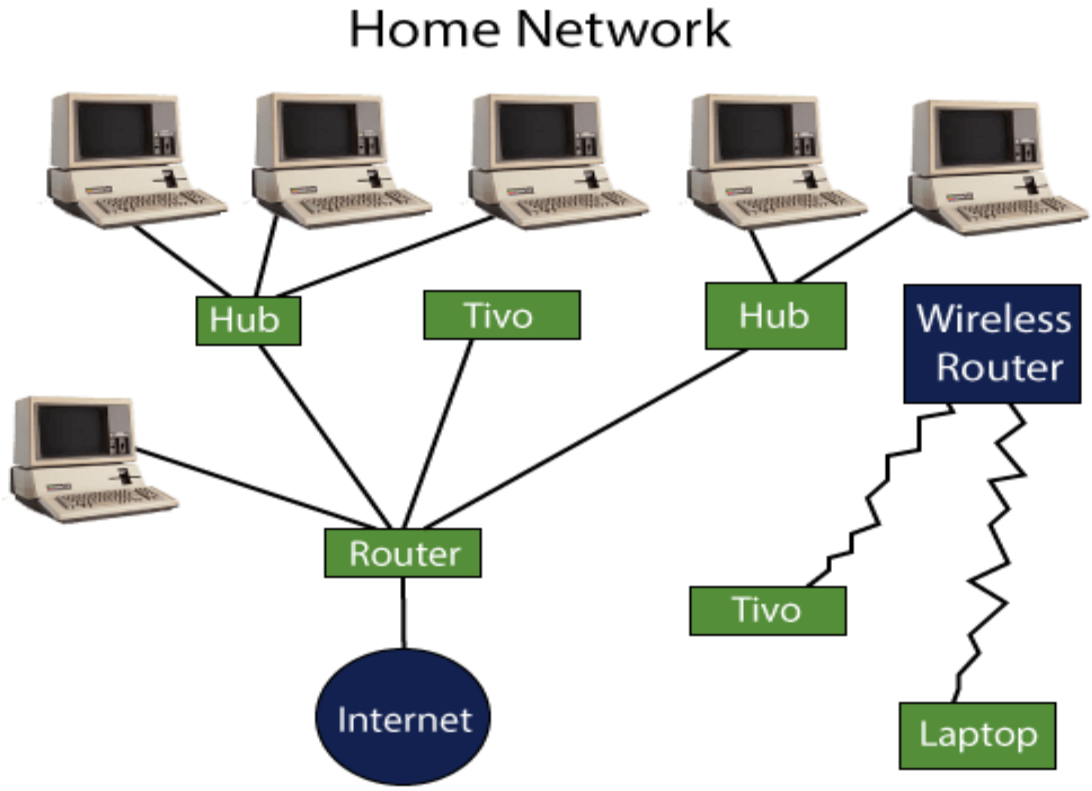
A router works on the **third layer** of the OSI model, and it is based on the IP address of a computer. It uses protocols such as ICMP to communicate between two or more networks. *It is also known as an **intelligent device** as it can calculate the best route to pass the network packets from source to the destination automatically.*

A virtual router is a software function or software-based framework that performs the same functions as a physical router. It may be used to increase the reliability of the network by virtual

router redundancy protocol, which is done by configuring a virtual router as a default gateway. A virtual router runs on commodity servers, and it is packaged with alone or other network functions, like load balancing, firewall packet filtering, and wide area network optimization capabilities.

Why Routers?

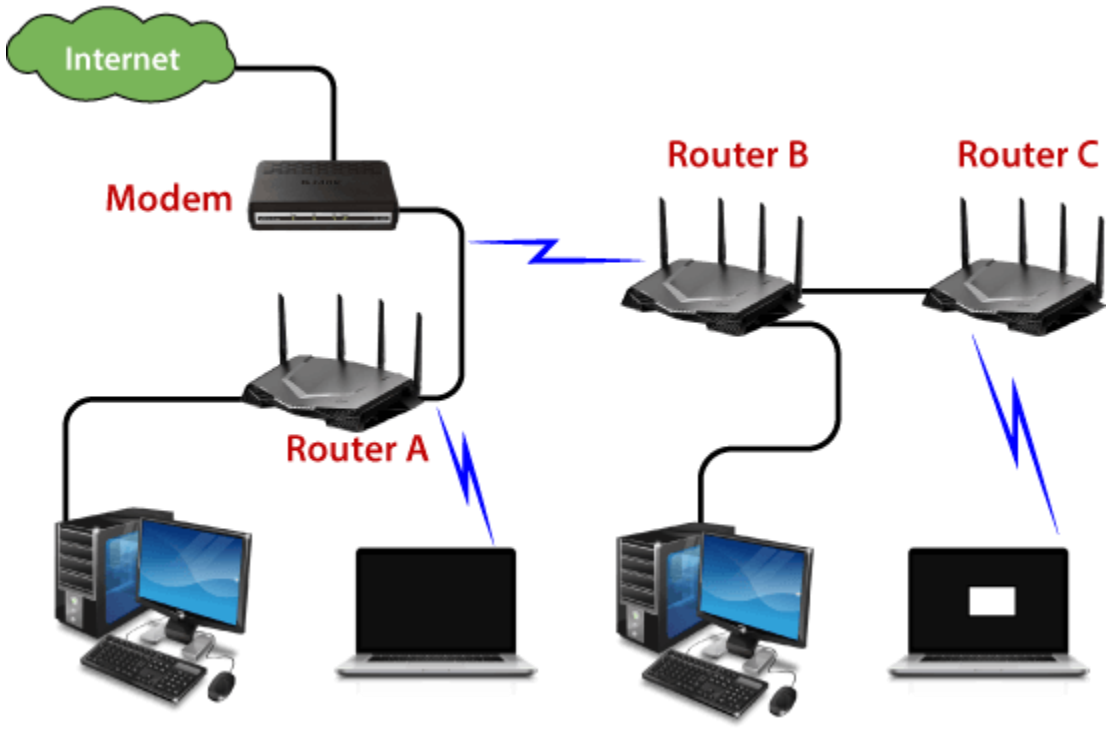
A router is more capable as compared to other network devices, such as a hub, switch, etc., as these devices are only able to execute the basic functions of the network. For example, a hub is a basic networking device that is mainly used to forward the data between connected devices, but it cannot analyze or change anything with the transferring data. On the other hand, the router has the capability to analyze and modify the data while transferring it over a network, and it can send it to another network. For example, generally, routers allow sharing a single network connection between multiple devices.



How does Router work?

A router analyzes a destination IP address of a given packet header and compares it with the routing table to decide the packet's next path. The list of routing tables provides directions to transfer the data to a particular network destination. They have a set of rules that compute the best path to forward the data to the given IP address.

Routers use a **modem** such as a cable, fiber, or DSL modem to allow communication between other devices and the internet. Most of the routers have several ports to connect different devices to the internet at the same time. It uses the **routing tables** to determine where to send data and from where the traffic is coming.



A routing table mainly defines the default path used by the router. So, it may fail to find the best way to forward the data for a given packet. For example, the office router along a single default path instructs all networks to its internet services provider.

There are two types of tables in the router that are **static and dynamic**. The static routing tables are configured manually, and the dynamic routing tables are updated automatically by dynamic routers based on network activity.

Functions of a Router:

The router basically performs two major functions:

1. Forwarding –
   Router receives the packets from its input ports, checks it header, performs some basic functions like checking checksum and then looks upto the routing table to find the appropriate output port to dump the packets onto, and forwards the packets onto that output port.

2. Routing: –
   Routing is the process by which the router ascertains what is the best path for the packet to reach the destination, It maintains a routing table which is made using different algorithms by the router only.

Features of Router

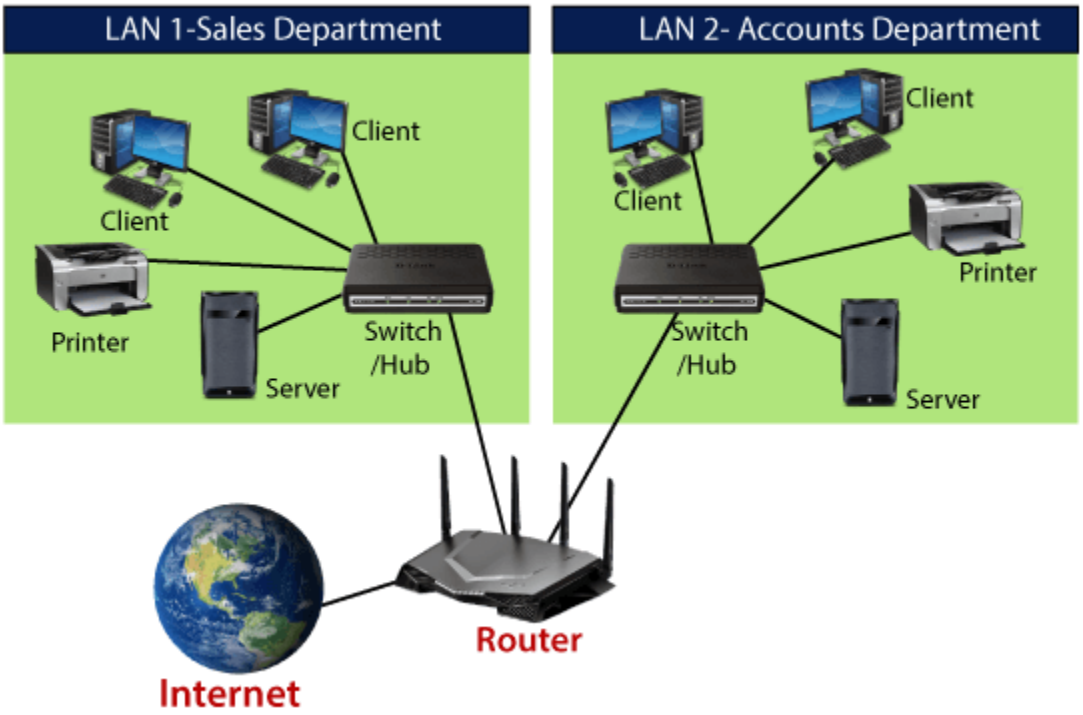
- A router works on the 3rd layer (Network Layer) of the OSI model, and it is able to communicate with its adjacent devices with the help of IP addresses and subnet.
- A router provides high-speed internet connectivity with the different types of ports like gigabit, fast-Ethernet, and STM link port.
- It allows the users to configure the port as per their requirements in the network.
- Routers' main components are central processing unit (CPU), flash memory, RAM, Non-Volatile RAM, console, network, and interface card.
- Routers are capable of routing the traffic in a large networking system by considering the sub-network as an intact network.
- Routers filter out the unwanted interference, as well as carry out the data encapsulation and decapsulation process.
- Routers provide the redundancy as it always works in master and slave mode.
- It allows the users to connect several LAN and WAN.
- Furthermore, a router creates various paths to forward the data.

Applications of Routers

There are various areas where a router is used:

- Routers are used to connect hardware equipment with remote location networks like **BSC, MGW, IN, SGSN**, and other servers.
- It provides support for a fast rate of data transmission because it uses high STM links for connectivity; that's why it is used in both wired or wireless communication.

- Internet service providers widely use routers to send the data from source to destination in the form of e-mail, a web page, image, voice, or a video file. Furthermore, it can send data all over the world with the help of an IP address of the destination.
- Routers offer access restrictions. It can be configured in a way that allows for few users to access the overall data and allows others to access the few data only, which is defined for them.
- Routers are also used by software testers for WAN communications. For example, the software manager of an organization is located in Agra, and its executive is located at a different place like Pune or Bangalore. Then the router provides the executive the method to share his software tools and other applications with the manager with the help of routers by connecting their PCs to the router using WAN architecture.
- In wireless networks, by configuring VPN in routers, it can be used in the client-server model, which allows sharing the internet, video, data, voice, and hardware resources. As shown in the below picture:



- In modern times, routers have the facility of inbuilt USB ports within the hardware. They have enough internal storage capacity. External storage devices can be used with routers to store and share data.

- Routers are used to set up the operation and maintenance center of an organization, which is known as the NOC center. All equipment at a distant location are connected by routers on optical cable at a central location, which also offer redundancy through the main link and protection link topology.

Types of Routers

There are various types of routers in networking; such are given below:

1. Wireless Router: Wireless routers are used to offer Wi-Fi connectivity to laptops, smartphones, and other devices with Wi-Fi network capabilities, and it can also provide standard ethernet routing for a small number of wired network systems.

Wireless routers are capable of generating a wireless signal in your home or office, and it allows the computers to connect with routers within a range, and use the internet. If the connection is indoors, the range of the wireless router is about 150 feet, and when the connection is outdoors, then its range is up to 300 feet.

Furthermore, you can make more secure wireless routers with a password or get your IP address. Thereafter, you can log in to your router by using a user ID and password that will come with your router.

2. Brouter: A brouter is a combination of the bridge and a router. It allows transferring the data between networks like a bridge. And like a router, it can also route the data within a network to the individual systems. Thus, it combines these two functions of bridge and router by routing some incoming data to the correct systems while transferring the other data to another network.

3. Core router: A core router is a type of router that can route the data within a network, but it is not able to route the data between the networks. It is a computer communication system device and the backbone of networks, as it helps to link all network devices. It is used by internet service providers (ISPs), and it also provides various types of fast and powerful data communication interfaces.

4. Edge router: An edge router is a lower-capacity device that is placed at the boundary of a network. It allows an internal network to connect with the external networks. It is also called as an access router. It uses an External BGP (Border Gateway Protocol) to provides connectivity with remote networks over the internet.

There are two types of edge routers in networking:

- **Subscriber edge router**
- **Label edge router**

The **subscriber edge router** belongs to an end-user organization, and it works in a situation where it acts on a border device.

The **label edge router** is used in the boundary of Multiprotocol Label Switching (MPLS) networks. It acts as a gateway between the LAN, WAN, or the internet.

5. Broadband routers: Broadband routers are mainly used to provide high-speed internet access to computers. It is needed when you connect to the internet through phone and use voice over IP technology (VOIP).

All broadband routers have the option of three or four Ethernet ports for connecting the laptop and desktop systems. A broadband router is configured and provided by the internet service provider (ISP). It is also known as a **broadband modem**, asymmetric digital subscriber line (**ADSL**), or digital subscriber line (**DSL**) modem.

Benefits of Router

There are so many benefits of a router, which are given below:

- **Security:** Router provides the security, as LANs work in broadcast mode. The information is transmitted over the network and traverses the entire cable system. Although the data is available to each station, but the station which is specifically addressed reads the data.
- **Performance enhancement:** It enhances the performance within the individual network. For example, if a network has 14 workstations, and all generate approximately the same volume of traffic. The traffic of 14 workstations runs through the same cable in a single network. But if the network is divided into two sub-networks each with 7 workstations, then a load of traffic is reduced to half. As each of the networks has its own servers and hard disk, so fewer PCs will need the network cabling system.
- **Reliability:** Routers provide reliability. If one network gets down when the server has stopped, or there is a defect in the cable, then the router services, and other networks will not be affected. The routers separate the affected network, whereas the unaffected networks remain connected, without interrupting the work and any data loss.
- **Networking Range:** In networking, a cable is used to connect the devices, but its length cannot exceed 1000 meters. A router can overcome this limitation by performing the function of a repeater (Regenerating the signals). The physical range can be as per the

requirement of a particular installation, as long as a router is installed before the maximum cable range exceeds.

Routing Protocols

Routing protocols specify a way for the router to identify other routers on the network and make dynamic decisions to send all network messages. There are several protocols, which are given below:

Open Shortest Path First (OSPF): It is used to calculate the best route for the given packets to reach the destination, as they move via a set of connected networks. It is identified by the Internet Engineering Task Force **(IETF)** as Interior Gateway Protocol.

Border Gateway Protocol (BGP): It helps manage how packets are routed on the internet via exchange of information between edge routers. It provides network stability for routers if one internet connection goes down while forwarding the packets, it can adapt another network connection quickly to send the packets.

Interior Gateway Routing Protocol (IGRP): It specifies how routing information will be exchanged between gateways within an independent network. Then, the other network protocols can use the routing information to determine how transmissions should be routed.

Enhanced Interior Gateway Routing Protocol (EIGRP): In this protocol, if a router is unable to find a path to a destination from the tables, it asks route to its neighbors, and they pass the query to their neighbors until a router has found the path. When the entry of routing table changes in one of the routers, it informs its neighbors only about the changes, but do not send the entire table.

Exterior Gateway Protocol (EGP): It decides how routing information can be exchanged between two neighbor gateway hosts, each of which has its own router. Additionally, it is commonly used to exchange routing table information between hosts on the internet.

Routing Information Protocol (RIP): It determines how routers can share information while transferring traffic among connected group of local area networks. The maximum number of hops that can be allowed for RIP is 15, which restricts the size of networks that RIP can support.

Routing algorithm

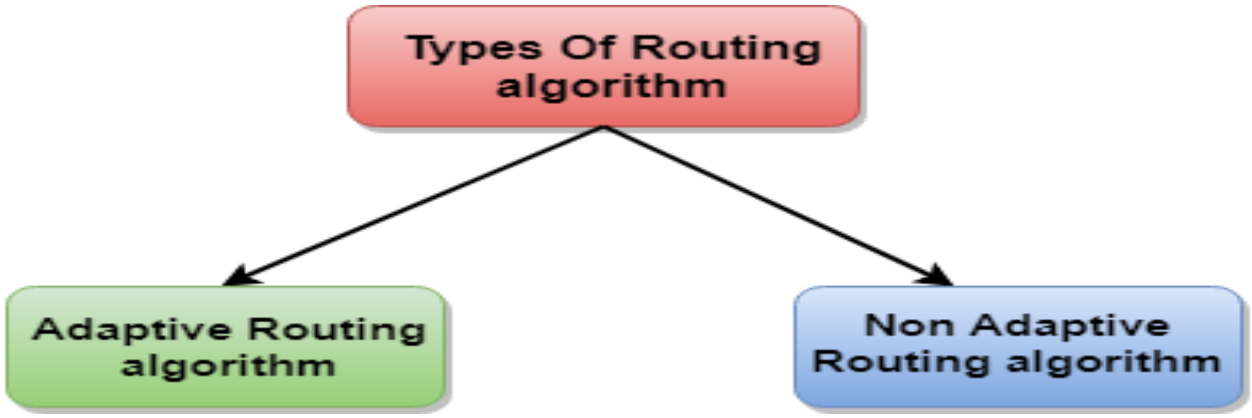
- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.

- Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of a Routing algorithm

The Routing algorithm is divided into two categories:

- Adaptive Routing algorithm
- Non-adaptive Routing algorithm



Adaptive Routing algorithm

- An adaptive routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decisions based on the topology and network traffic.
- The main parameters related to this algorithm are hop count, distance and estimated transit time.

An adaptive routing algorithm can be classified into three parts:

- **Centralized algorithm:** In the centralized method, a node has whole information regarding the network so that it can make all the decisions of routing. The main benefit of this algorithm is, it requires the only single node to keep the data of the complete network. The main drawback of this is, if the middle node goes down, then the whole network has can to be redone. Link state algorithm is referred to as a centralized algorithm since it is aware of the cost of each link in the network.
- **Isolation algorithm:** It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.
- **Distributed algorithm**: In this method, the node receives information from its neighbors and then decides to route the packets. The disadvantage is that the packet may be delayed if there is a change in between interval in which it receives information and sends the packet. A Distance vector algorithm is a decentralized algorithm as it never knows the complete path from source to the destination, instead it knows the direction through which the packet is to be forwarded along with the least cost path.

Non-Adaptive Routing algorithm

- Non Adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

The Non-Adaptive Routing algorithm is of two types:

Flooding: In case of flooding, every incoming packet is sent to all the outgoing links except the one from it has been reached. The disadvantage of flooding is that node may contain several copies of a particular packet.

Random walks: In case of random walks, a packet sent by the node to one of its neighbors randomly. An advantage of using random walks is that it uses the alternative routes very efficiently.

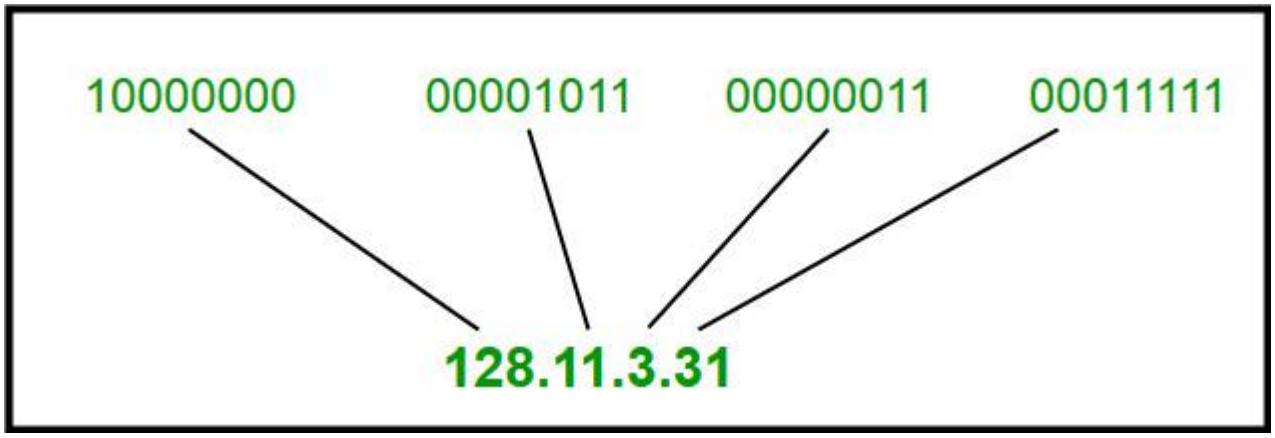
Differences b/w Adaptive and Non-Adaptive Routing Algorithm

Basis Of Comparison	**Adaptive Routing algorithm**	**Non-Adaptive Routing algorithm**
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.
Routing decision	Routing decisions are made based on topology and network traffic	Routing decisions are the static tables.
Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The Non-Adaptive Routing algorithm is used by static routing.
Complexity	Adaptive Routing algorithms are more complex	Non-Adaptive Routing algorithms are simple.

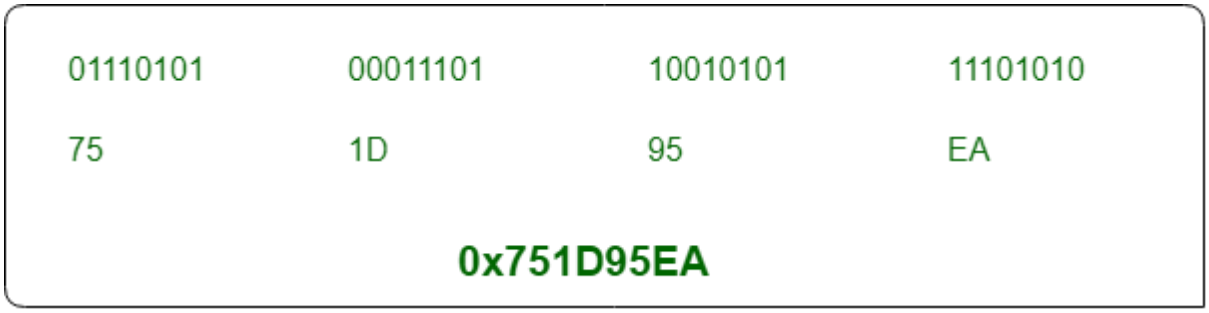
Unit 1(S2)

Introduction of Classful IP Addressing

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 2^{32}.
Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation.
Dotted Decimal Notation:



Hexadecimal Notation:



Some points to be noted about dotted decimal notation:

1. The value of any segment (byte) is between 0 and 255 (both included).
2. There are no zeroes preceding the value in any segment (054 is wrong, 54 is correct).

Classful Addressing

The 32 bit IP address is divided into five sub-classes. These are:

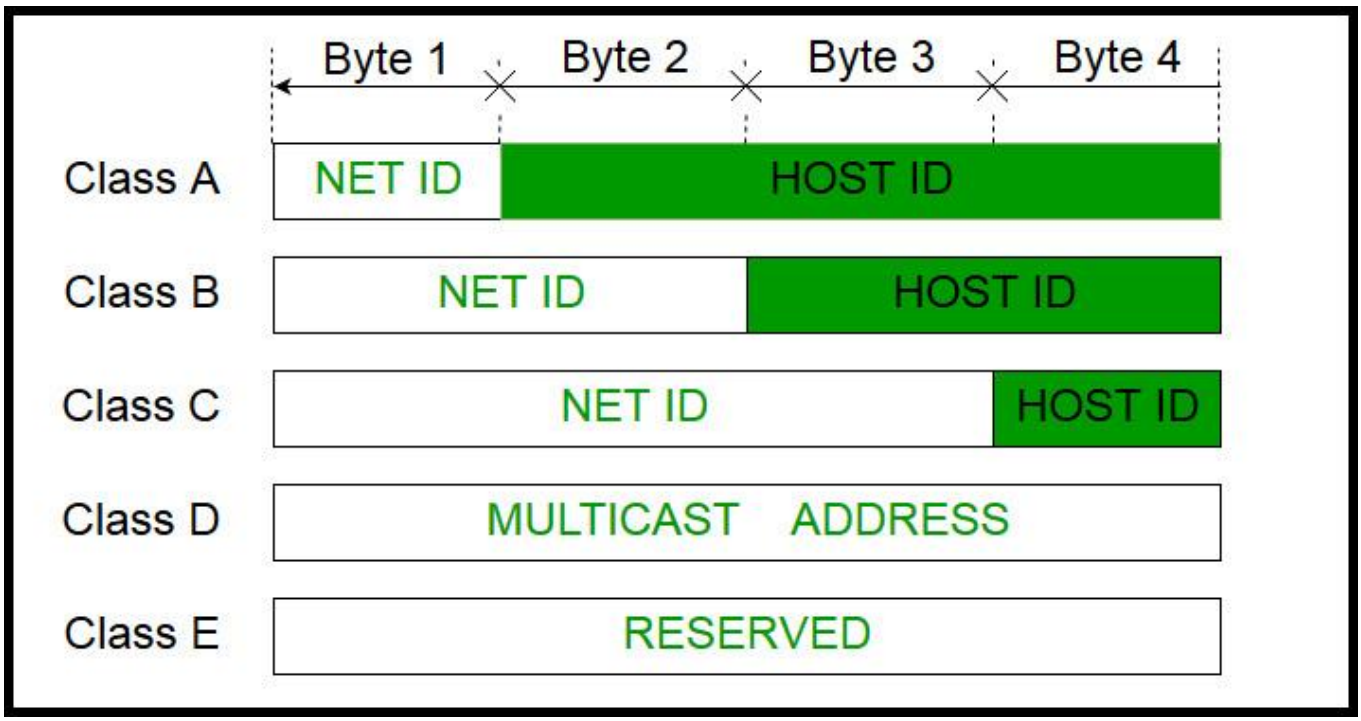
- Class A
- Class B

- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.
IPv4 address is divided into two parts:

- **Network ID**
- **Host ID**

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.



Note: IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).
Note: While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

Class A:

IP address belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:

- 2^7-2= 126 network ID(Here 2 address is subracted because 0.0.0.0 and 127.x.y.z are special address.)
- 2^24 – 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 1.x.x.x – 126.x.x.x

Class B:

IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.

Class C:

IP address belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address

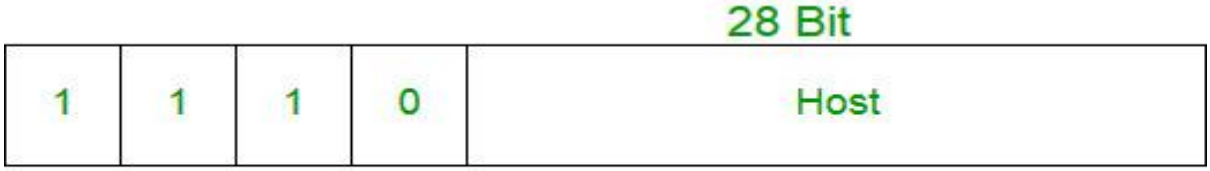
IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.

Class C

Class D:

IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.

Class D does not posses any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.



Class D

Class E:

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254. This class doesn't have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.

Range of special IP addresses:

169.254.0.0 – 169.254.0.16 : Link local addresses
127.0.0.0 – 127.0.0.8 : Loop-back addresses
0.0.0.0 – 0.0.0.8 : used to communicate within the current network.

Rules for assigning Host ID:

Host ID's are used to identify a host within a network. The host ID are assigned based on the following rules:

- Within any network, the host ID must be unique to that network.
- Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for assigning Network ID:

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Problems with Classful Addressing:

The problem with this classful addressing method is that millions of class A address are wasted, many of the class B address are wasted, whereas, number of addresses available in class C is so small that it cannot cater the needs of organizations. Class D addresses are used for multicast routing and are therefore available as a single block only. Class E addresses are reserved.

Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993. We will be discussing Classless addressing in next post.

Classless Inter-Domain Routing (CIDR):

CIDR or Class Inter-Domain Routing was introduced in 1993 to replace classfull addressing. It allows the user to use VLSM or Variable Length Subnet Masks.

CIDRnotation:

In CIDR subnet masks are denoted by /X. For example a subnet of 255.255.255.0 would be denoted by /24. To work a subnet mask in CIDR, we have to first convert each octet into its respective binary value. For example, if the subnet is of 255.255.255.0. then :

- First Octet:
  255 has 8 binary 1's when converted to binary
- Second Octet:
  255 has 8 binary 1's when converted to binary
- Third Octet:
  255 has 8 binary 1's when converted to binary
- Fourth Octet:
  0 has 0 binary 1's when converted to binary

Therefore, in total there are 24 binary 1’s, so the subnet mask is /24.

While creating a network in CIDR, a person has to make sure that the masks are contagious, i.e. a subnet mask like 10111111.X.X.X can’t exist.

With CIDR, we can create Variable Length Subnet Masks, leading to less wastage of IP addresses. It is not necessary that the divider between the network and the host portions is at an octet boundary. For example, in CIDR a subnet mask like 255.224.0.0 or 11111111.11100000.00000000.00000000 can exist.

Classless Addressing

To reduce the wastage of IP addresses in a block, we use sub-netting. What we do is that we use host id bits as net id bits of a classful IP address. We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28. Here, subnet mask is found by putting the given number of bits out of 32 as 1, like, in the given address, we need to put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be 255.255.255.240.

Some values calculated in subnetting :

1. Number of subnets : Given bits for mask – No. of bits in default mask

2. Subnet address : AND result of subnet mask and the given IP address

3. Broadcast address : By putting the host bits as 1 and retaining the network bits as in the IP address

4. Number of hosts per subnet : 2^(32 – Given bits for mask) – 2

5. First Host ID : Subnet address + 1 (adding one to the binary representation of the subnet address)

6. Last Host ID : Subnet address + Number of Hosts

Example : Given IP Address – 172.16.0.0/25, find the number of subnets and the number of hosts per subnet. Also, for the first subnet block, find the subnet address, first host ID, last host ID and broadcast address.

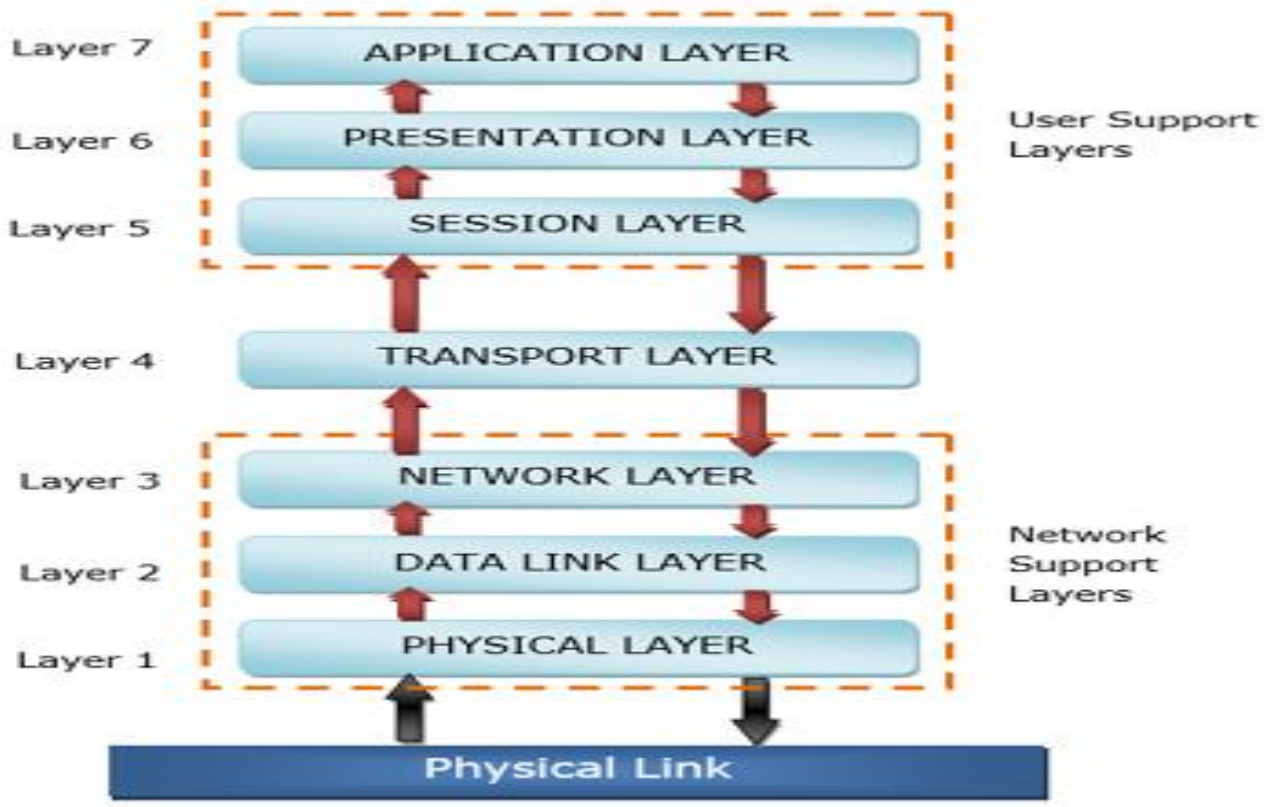
Solution : This is a class B address. So, no. of subnets = 2^(25-16) = 2^9= 512.
No. of hosts per subnet = 2^(32-25) – 2 = 2^7 – 2 = 128 – 2 = 126
For the first subnet block, we have subnet address = 0.0, first host id = 0.1, last host id = 0.126 and broadcast address = 0.127

Unit 1(S3)

OSI Reference Model

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:



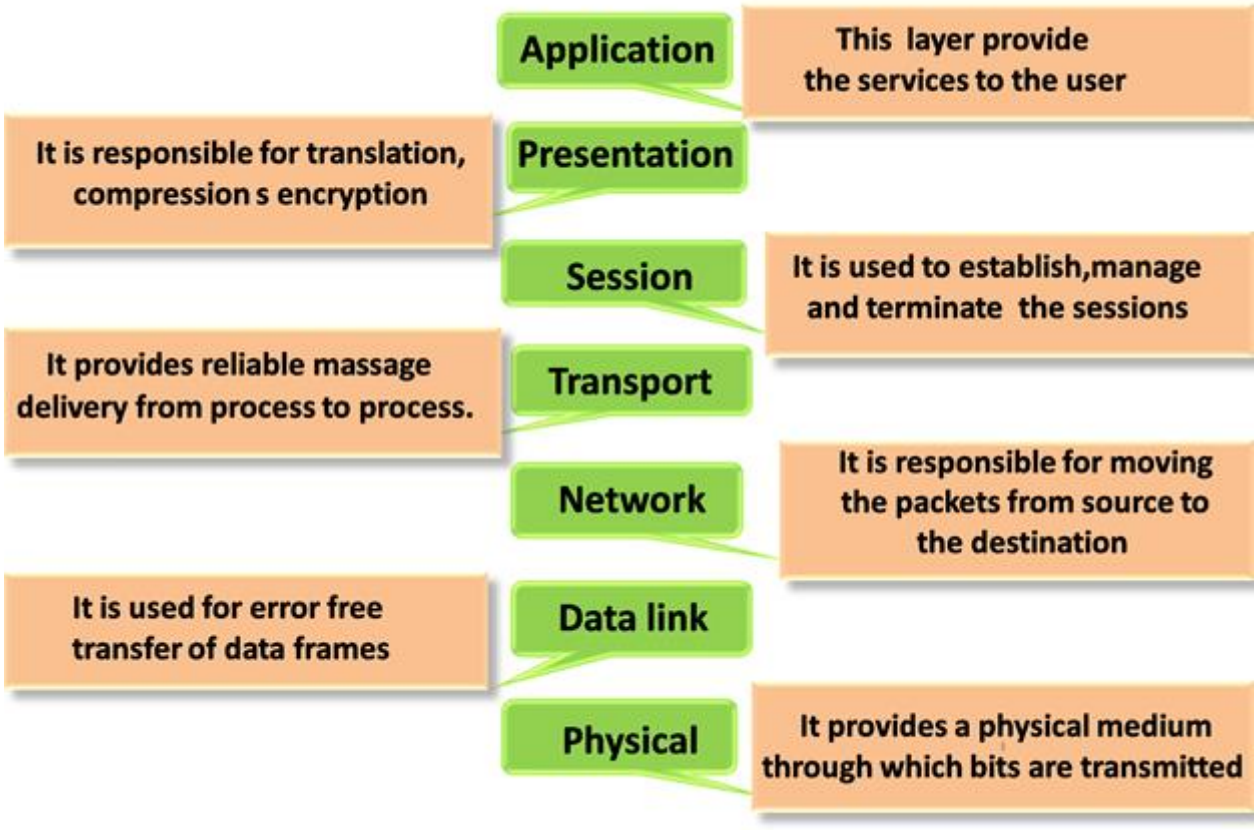
- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

Functions of the OSI Layers

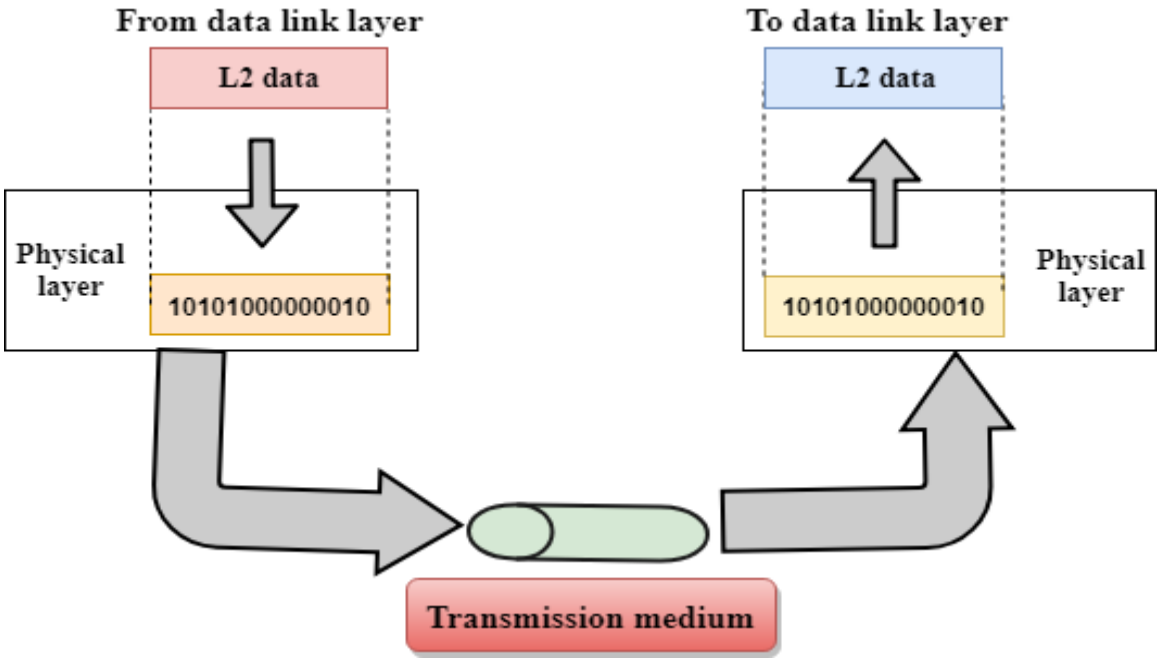
There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer

2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



Physical layer

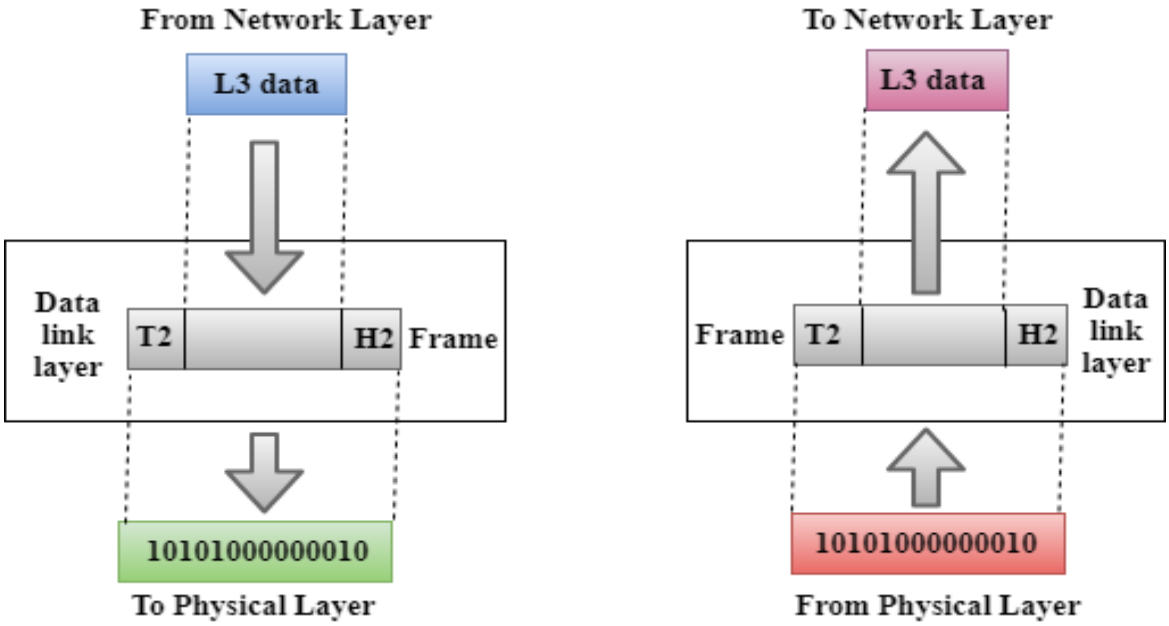


- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- **Topology:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.

Data-Link Layer



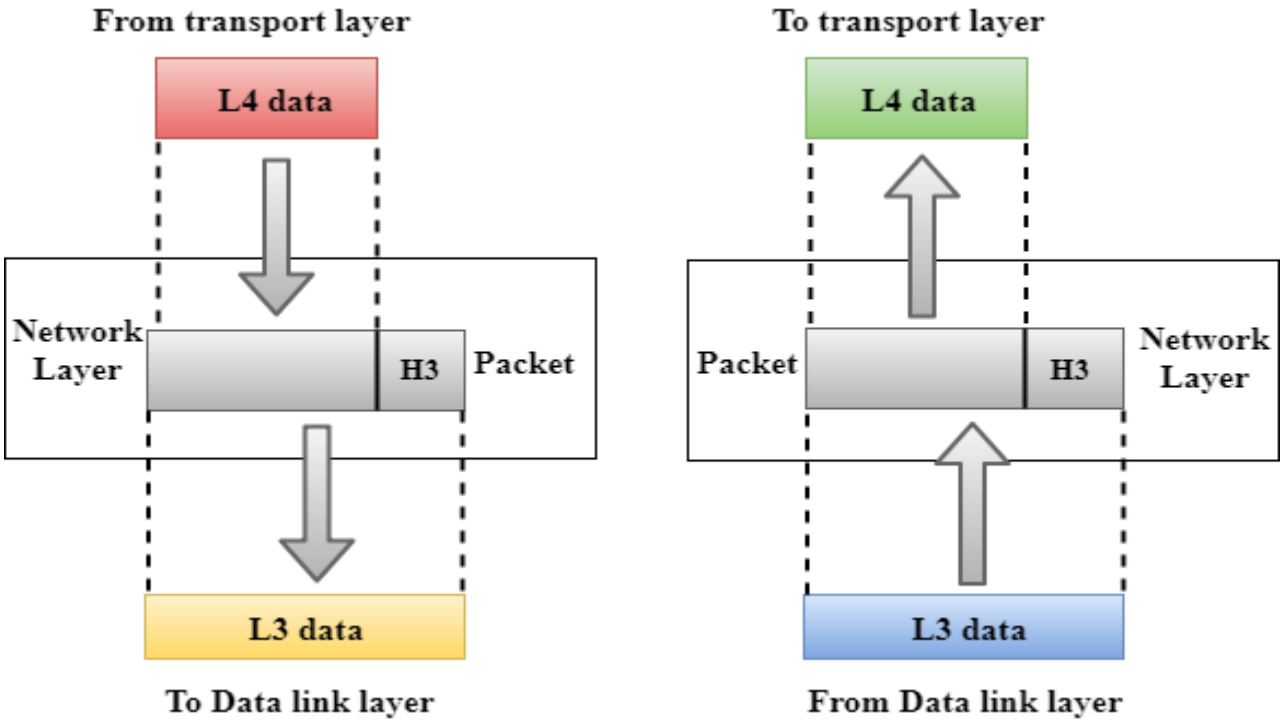
- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
    - **Logical Link Control Layer**
        - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
        - It identifies the address of the network layer protocol from the header.
        - It also provides flow control.
    - **Media Access Control Layer**
        - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
        - It is used for transferring the packets over the network.

Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

Network Layer



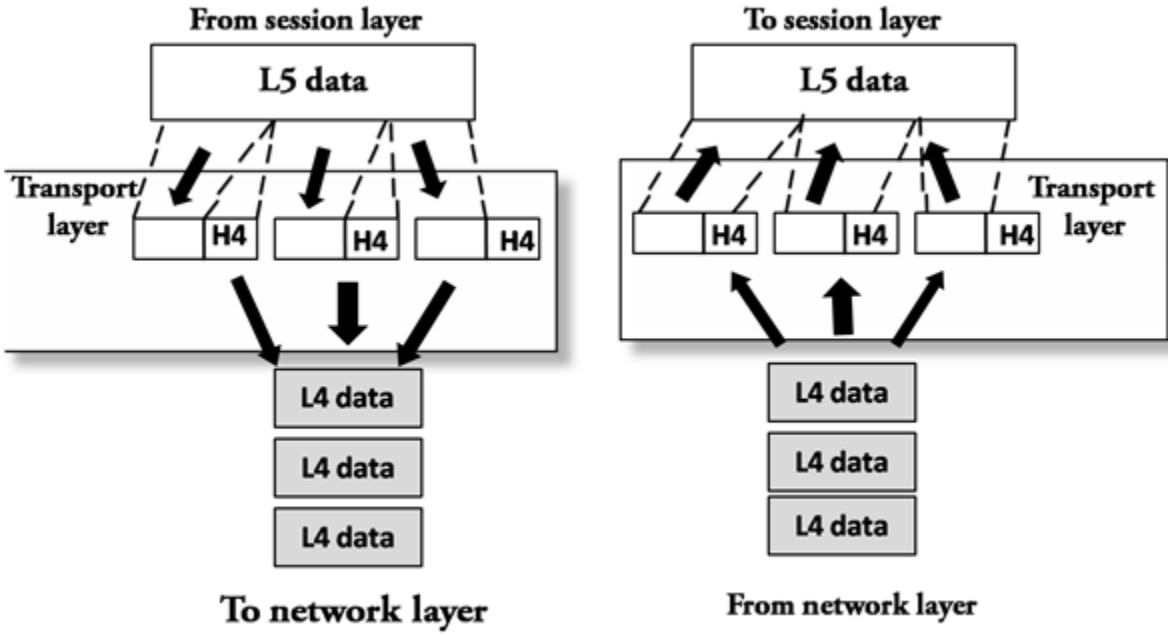
- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Transport Layer



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- **Transmission Control Protocol**
    - It is a standard protocol that allows the systems to communicate over the internet.

- It establishes and maintains a connection between hosts.
- When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

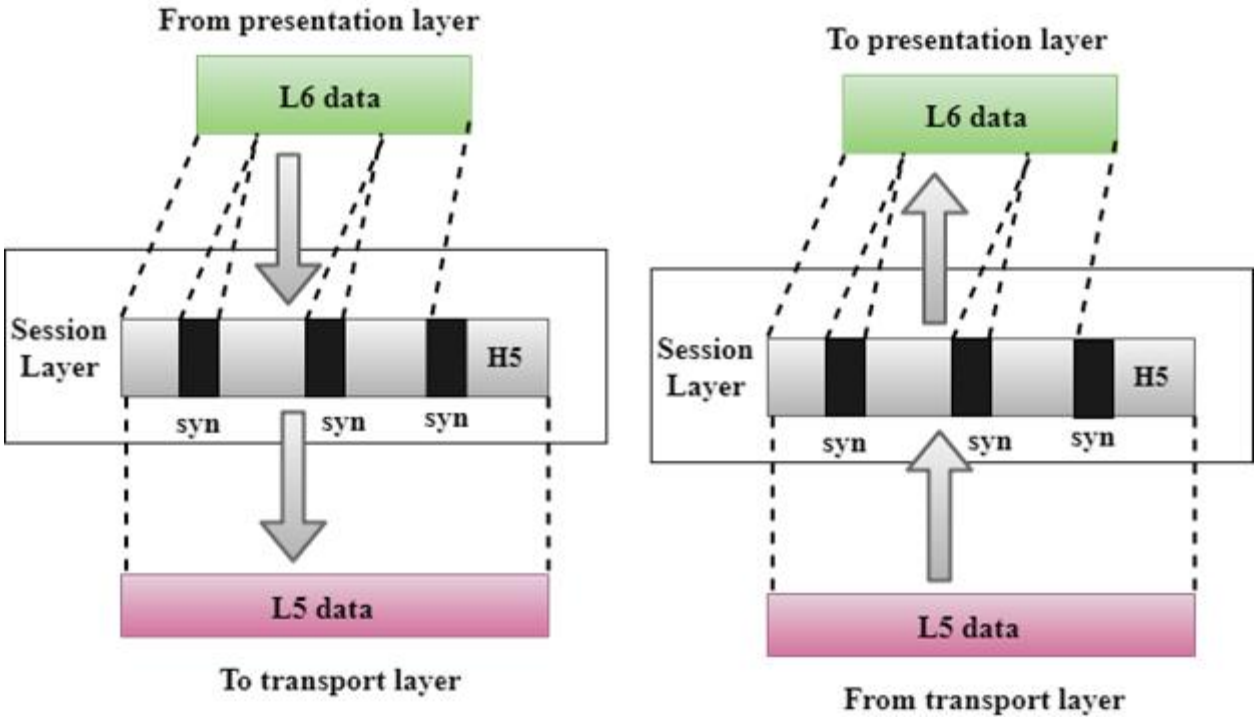
Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine

before delivering the packets. In connection-oriented service, all the packets travel in the single route.

- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer



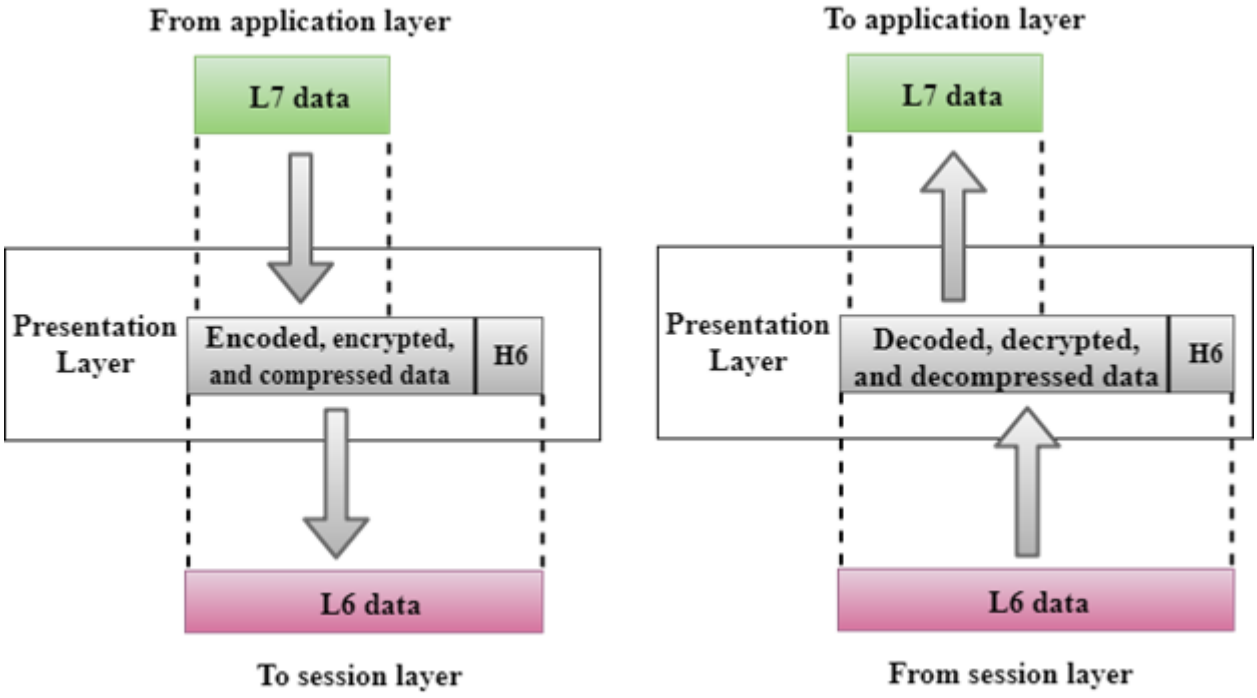
- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation Layer

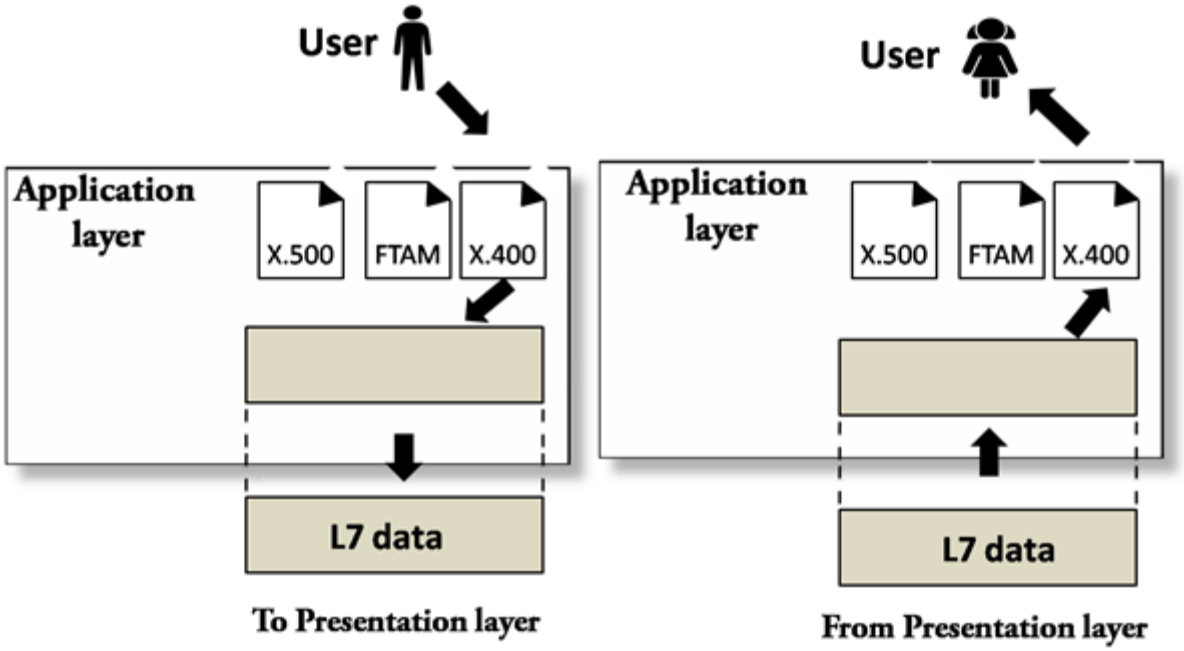


- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

Application Layer



- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Functions of Application layer:

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

IP Protocol Stack Architecture

The Internet Protocol Stack Architecture is also known as a TCP/IP protocol suite or TCP/IP model. It is one type of protocol and network model used on the internet. It consists of four layers' application layer, transport layer, internet layer, and the link layer. In this networking, the TCP and the IP layers are the most widely used protocols, so that this model named as TCP/IP model or Internet Protocol Stack Architecture.

The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer –

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has2versions:
   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host Layer –

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control

mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.

2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Application Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

The diagrammatic comparison of the TCP/IP and OSI model is as follows

TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer

OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Difference between TCP/IP and OSI Model:

TCP/IP	OSI
Implementation of OSI model	Reference model
Model around which Internet is developed	This is a theoretical model
Has only 4 layers	Has 7 layers
Considered more reliable	Considered a reference tool
Protocols are not strictly defined	Stricter boundaries for the protocols
Horizontal approach	Vertical approach
Combines the session and presentation layer in the application layer	Has separate session and presentation layer
Protocols were developed first and then the model was developed	Model was developed before the development of protocols
Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer
Protocol dependent standard	Protocol independent standard

Unit 1(S4)

Network Topology Architectures

In network designs, there are various Network topology architectures are used. In this lesson,n we will focus on rthese network topology architectures one by one.

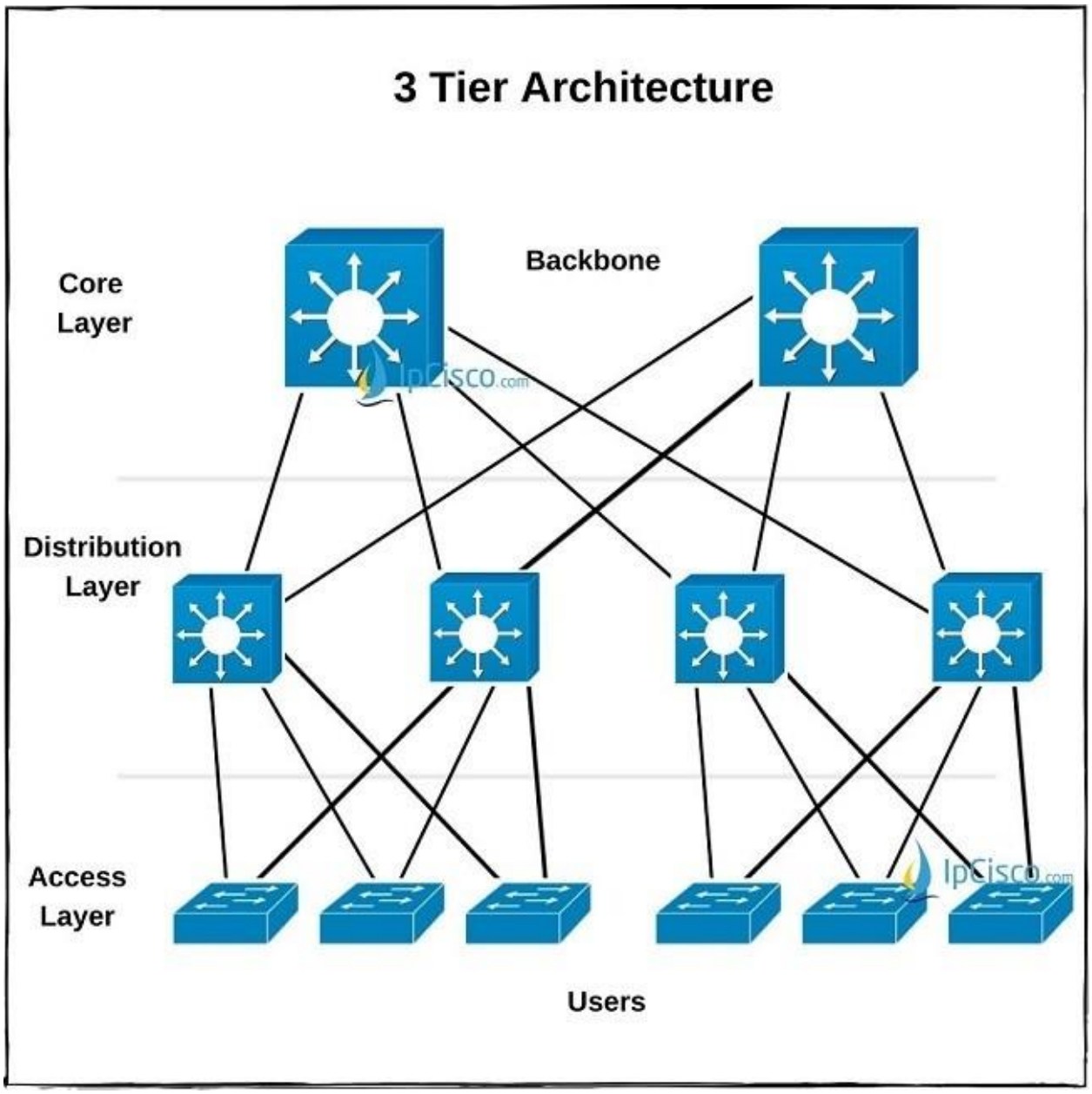
- **3 Tier Architecture**
- **2 Tier Architecture**
- **Spine Leaf Architecture**
- **WAN Arhitectures**
- **SOHO Arhitecture**
- **Cloud Arhitectures**

3 Tier Architecture

3 Tier Architecture is also called Three-Layered Hierachical Model used by large enterprises. This architecture is a scalable and resilient solution for large enterprises. 3 Tier Architecture consist of three layers. These layers are :

- **Access**
- **Distribution**
- **Core**

The logical view of a typical 3 Tier Architecture is showed below.



Each of these layers has a special duty in 3 Tier Architecture (Three-layered Hşerarchical Model). Now, let's talk about each layer's role one by one.

Access Layer

Access Layer is the lower layer of 3 Tier Architecture. It is the closes layer to the end users. In this Access Layer, Access Switches resides and uysers are connected to these switches.

In Access Layer, Network Access Policies, Layer 2 Security Mechanisms like Port Security are used. Beside, Layer 2 Loop preventation mechanims like STP, RSTP, PVST, MST are used in this layer. Another imporant and most used technolog in this layer is VLANs. With VLANs, different parts of the company is divided.

Distribution Layer

Disdtribution Layer is the middle layer of 3 Tier Architecture. This layer works as the bidge of Access Layer and Core Layer. It is the aggregation layer of all Access switches. Instead of Access layer switches, multilayer switches are used in Distribution layer.

Redundancy is used in this layer to overcome single point of failure. Multiple Multilayer switches are used as redundant in this layer. Distribution policies are also used in this layer.

Between Distribution Layer and Access Layer, Layer 2 is used. In other words the key technology between first and second layers of 3 Tier Architecture is switching. Between Distributiona and Core Layer 3 is used. In other words, the key technology between second and third layers of 3 Tier Architecture is routing. Instead of these, we can also use LAyer 3 through all these layer or we can use LAyer 2 with Virtual Port Channels(vPC).

Core Layer

Core layer is also known as Backbone Network. Core (Backbone) Layer conencts ditribution layer devices.

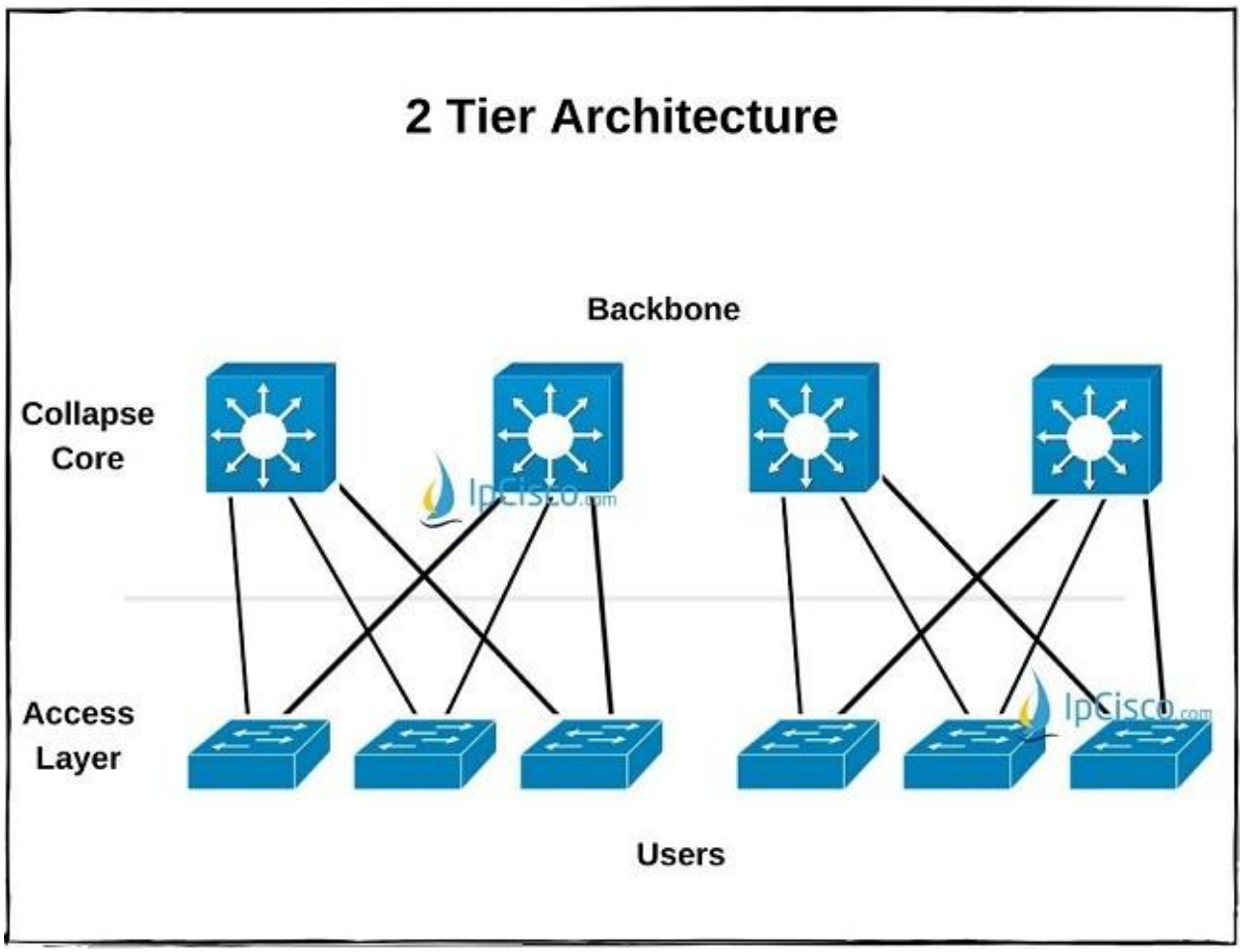
Routing protocols are used in this layer and the main duty of this layer is provifing routing between them and the distribution layer. Redundanct is also important fort his layer. So, redundant core devices are used to overcome single point of failure.

2 Tier Architecture

2 Tier Architecture is also called Two-Layerd Hierachical Model or Collapsed Core Model. This architecture is used by small enterprises that can not use 3 Tier architecture. Because, 3 Tier Architecture is a good solution but also an expensive solution. Small enterprises overcome this by combining core and distribution layer into one layer.

There are two layers in this architecture. These are :

- **Collapsed Core Layer**
- **Access Layer**



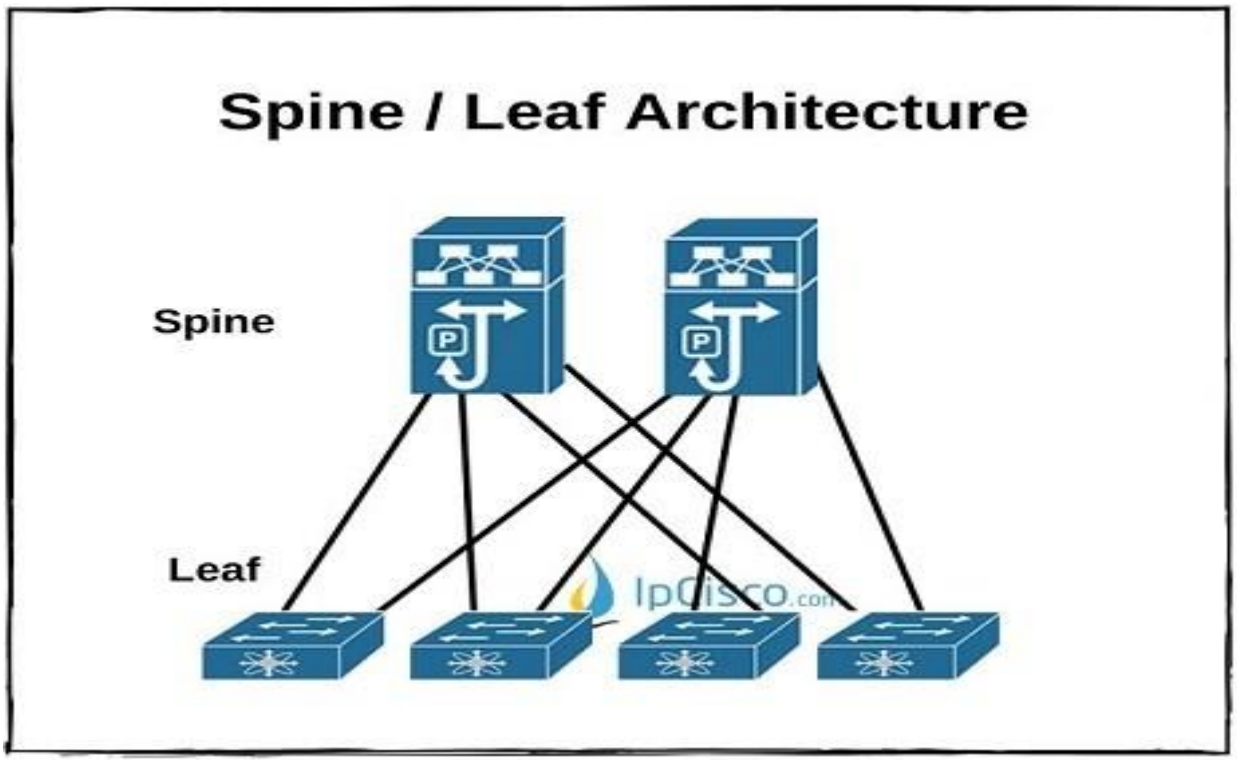
Collapsed Core Layer provides both Core and Distribution Layer duties. Distribution policies are used in this layer.

If enterprise wants to migrate to a 3 Tier Architecture, it is possible to do that with additional Core Devices.

Spine Leaf Architecture

With the new requirements to become more scalable, fast and efficient, a new datacenter design is developed. This design is replaced with three tier design that is used mostly in networking World. This technology that is also a good solution for evolving datacenters is called Spine Leaf Architecture.

Spine Leaf Architecture is the network architecture with which all the devices are the same segments away. It is the two layered architecture conssit of Spine Layer and Leaf Layer.



The Leaf Layer is the layer, consist of Access devices, swithces, servers, edge routers etc. The Spine Layer is the core layer of Spine Leaf Architecture. Routing is the first duty of Spine layer. In Spine Leaf Architecture Design, every Leaf switch is connected to all the Spine Switches.

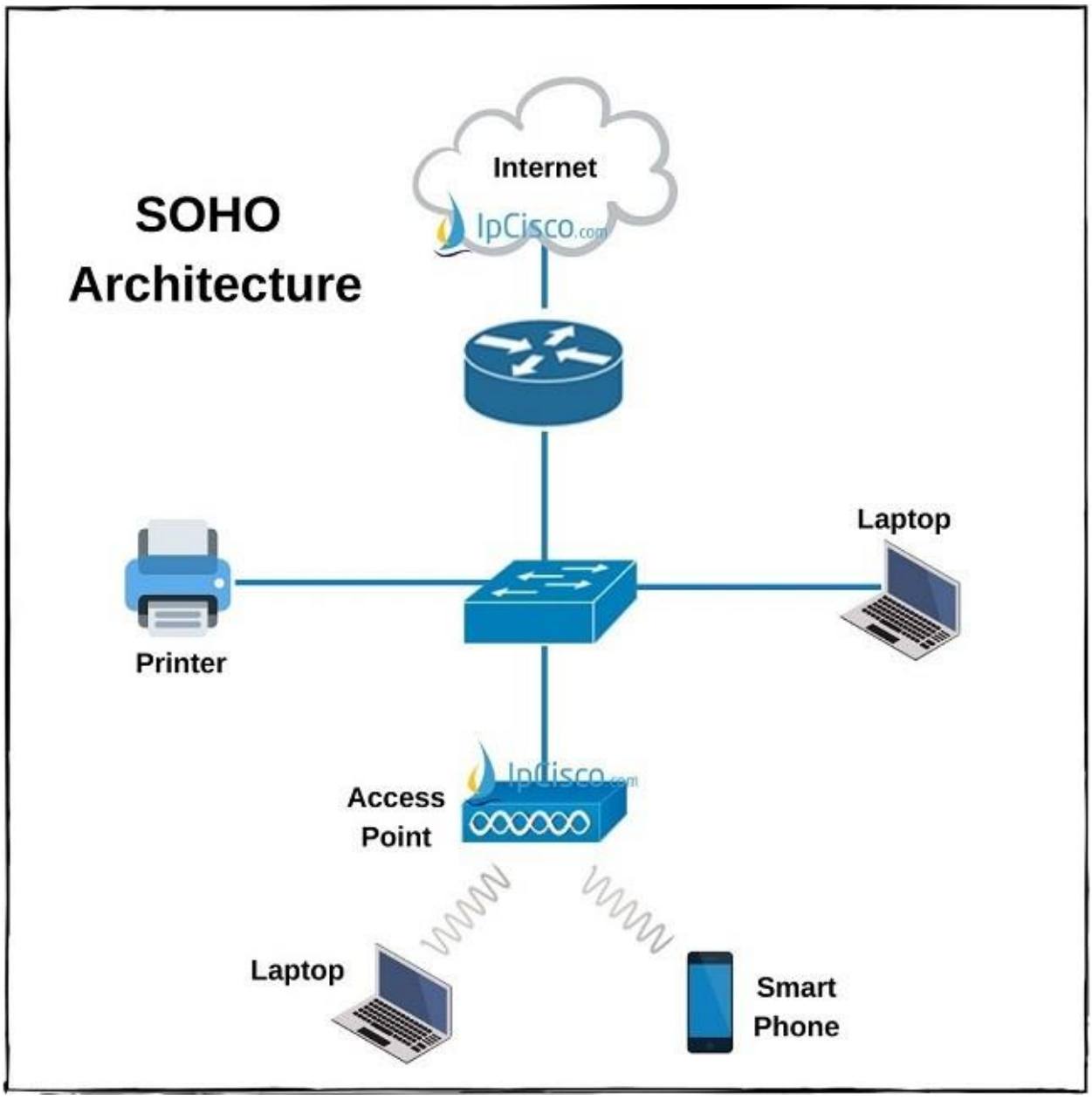
This type of network architecture is also used for spanning tree limitations. With its design, Spine Leaf Architecture provides more dynamic network than three layered architecture.

Small Office / Home Office (SOHO) Architecture

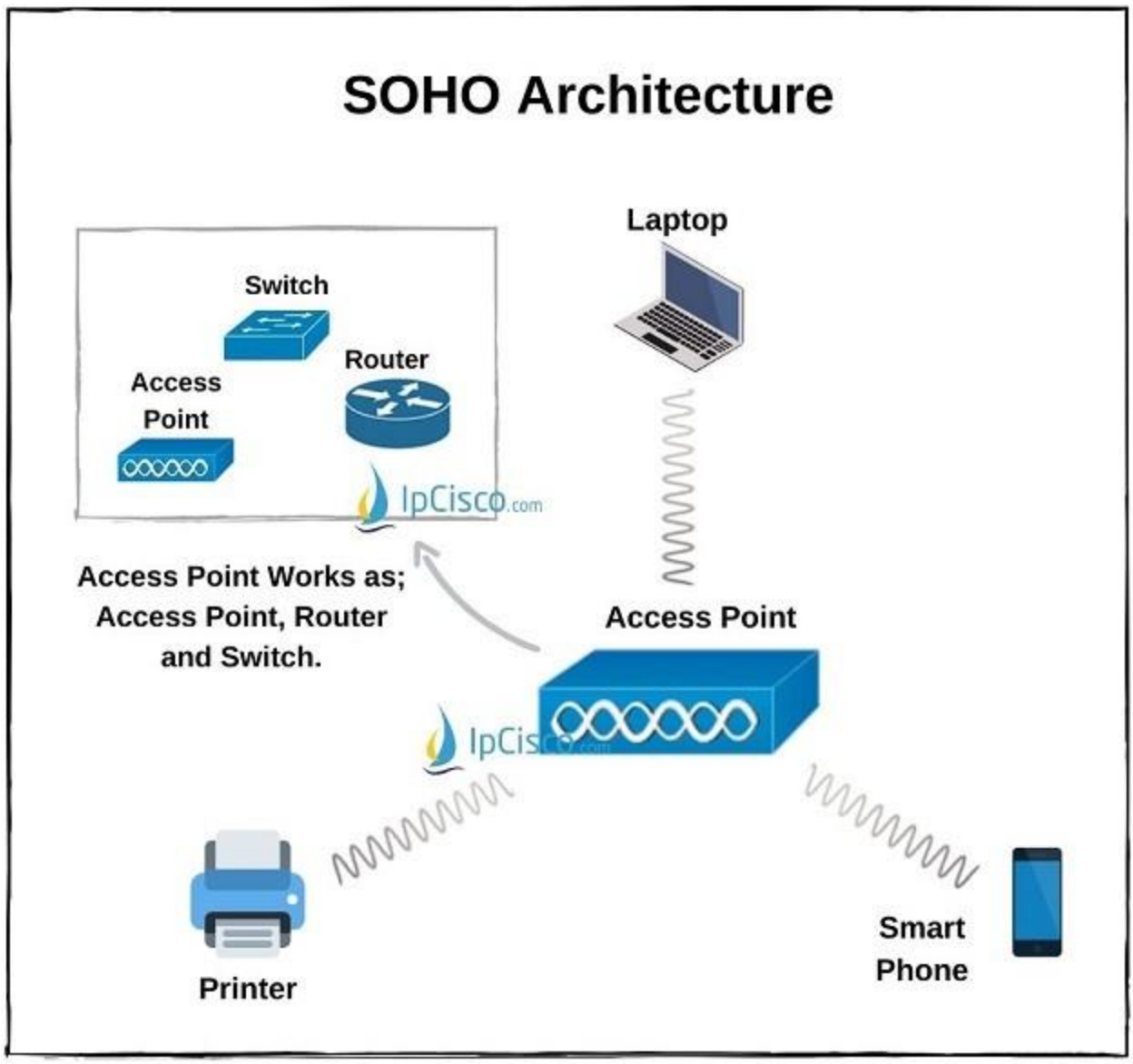
SOHO is the abbreviation of Small Office / Home Office Architectures. This architecture is the simplest network architectures that is mainly used in homes or in small enterprises as its names implies.

In SOHO architecture, there is a small switch, a router and connected access devices like PCs, printers etc. basically. The router that has routing capability provides Internet Access. The switch provides the ports to provide network access tto the end users. PCs, printers etc are the devices that is used by users. Generally one device that has both switch and router capability is used instead of two separate devices.

Ethernet technology is used to connect the devices in SOHO Architecture.Access devices are connected to the swithc or switch/router adn then they can Access Internet. Various Ethernet cables can be used to connect these devices to the network like CAT5, CAT6 cable standards.



Beside, with the wireless networking new devices has alsom added to SOHO networks like Access Points, Access Points are the devices that provide Internet Access to the access devices. To do this, they also connected to the network via Ethernet cables. These Access points can be separate devices in the network. But in today's networks, a single device is used as switch, router and access point. One device provides all these capabilities and Access devices are connected to this device to have Internet Acccess.



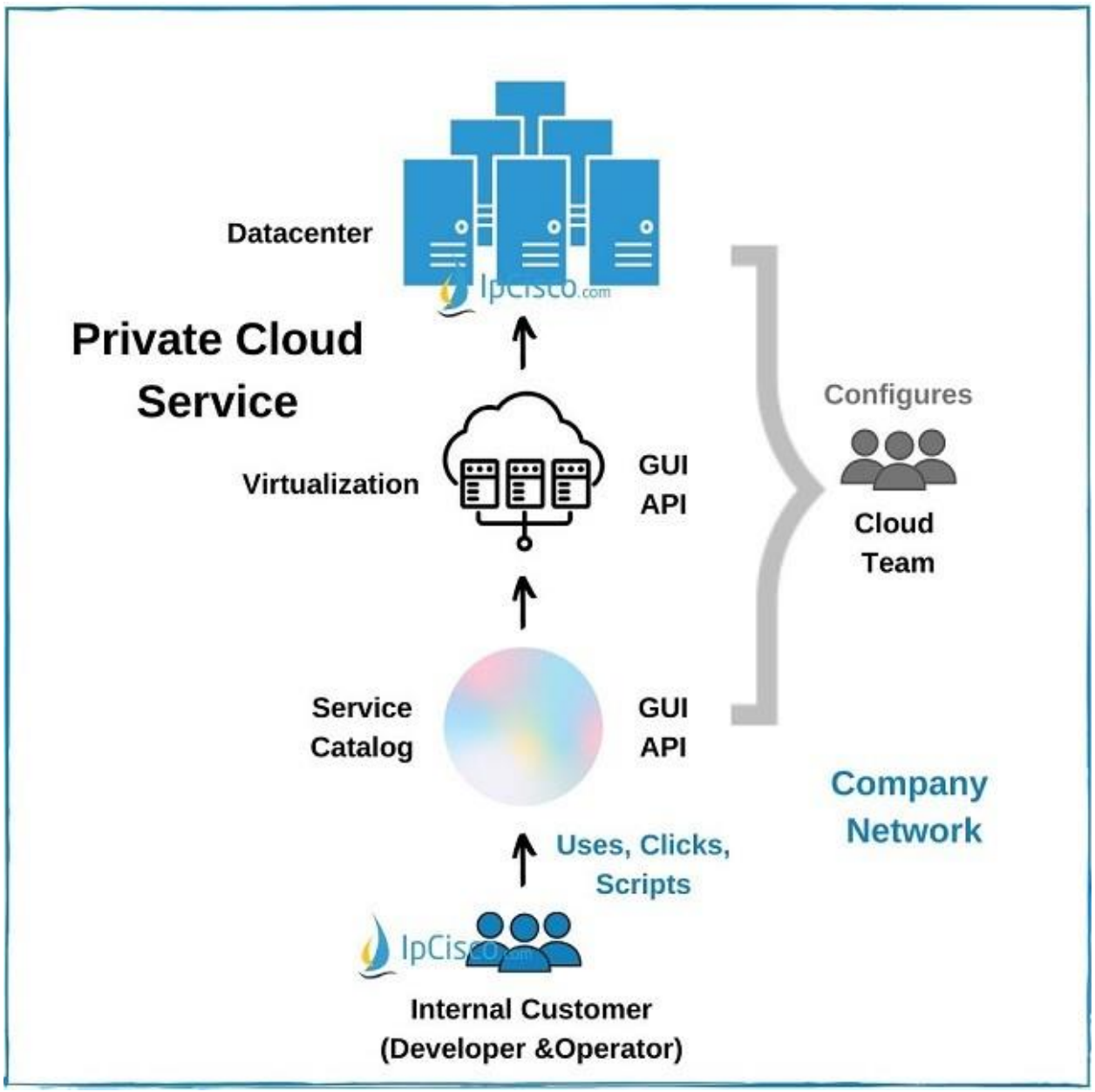
On-Premises and Cloud Architecture

Here, there are two important terms. The first one is Public Cloud. Public Cloud is the cloud service which provides cloud service to the other companies. The second one is Private Cloud (On Premises). Private Cloud is the cloud service which provides service to the local users in the same company.

Private Cloud Service

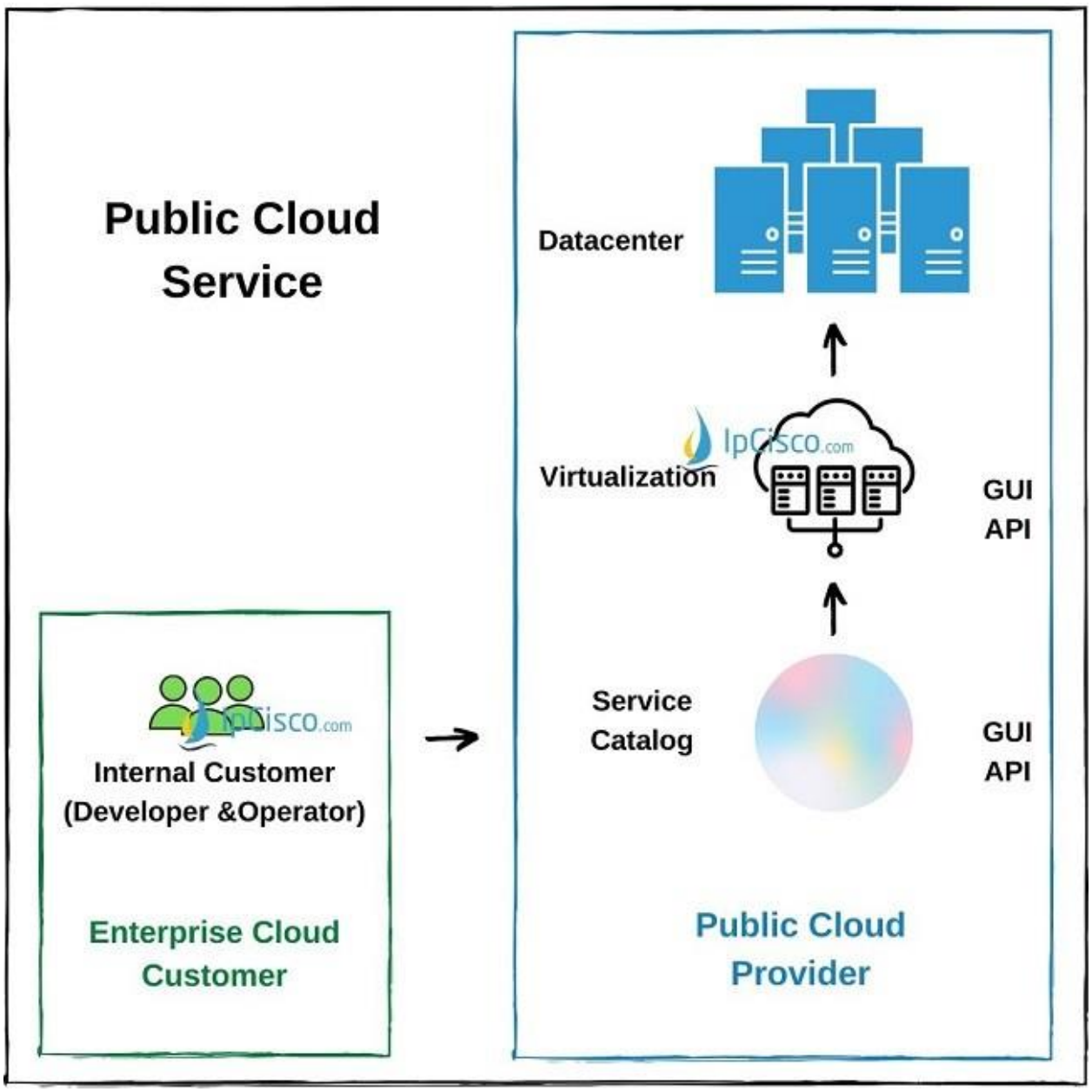
Private Cloud service or as the old name, on-premises is the cloud service that is given to own company. This service is used by the users in the same company. Employees in the company an request virtual machines for their works, developments etc. And the requested virtual devices are provided these users by cloud architecture of the company.

So how does private cloud architecture works? Here, users request cloud services form the CLous Service Catalog that is configured bu Cloud Teams before. The virtualisation softwares that are also configure by cloud teams, create virtual devices in datacenters and users can use these virtual devices for their works,d evelopments etc.



Public Cloud Service

Public Cloud Service is also defined as only cloud in old documentation. But now, the term public cloud is being used. Oublic Cloud is the cloud service that is provided by cloud service providers to the other companies. The company employeees that receive cloud services can request to create virtual devices in the cloud service provider's network.



How does Public Cloud Works? In Public Cloud Service, firstly customer selects and ask for a service in service catalog. At the provider part, the virtualization tools creates this service and customer can use this service independant from its own datacenter.

Cloud service provider has multiple options for cloud customer connections. These solutions can be VPN, Private WAN etc.

Network Management Architecture

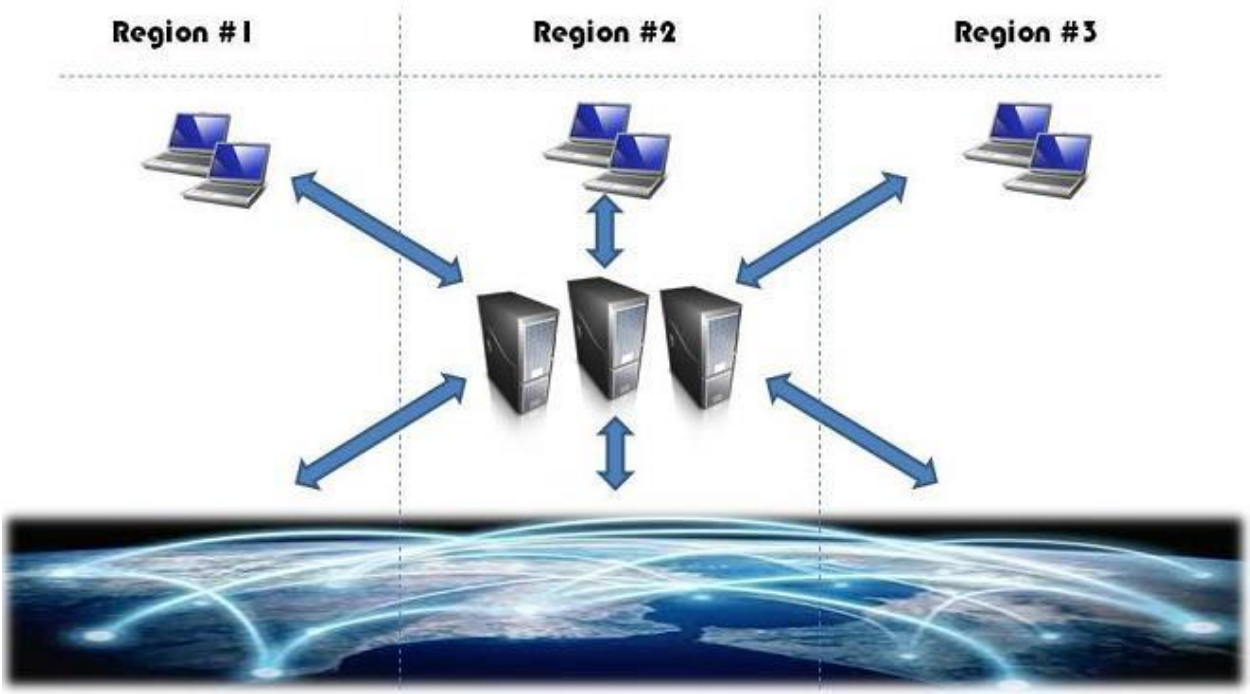
Networks are increasingly becoming complex and distributed. As a result, problems like hardware failures, performance degradation, resource allocation, bandwidth monitoring and assignment and service provisioning are harder to solve and become real challenges for Network Operation Centers (NOC). The NOC is in constant search for efficient integrated network management systems required to monitor, interpret, and control the behavior and performance of the network, its hardware devices and software resources.

This article discusses the **three network management architectures** in use today, so by reading it you will be able to understand the **differences** between each architecture, and by reading the **pros** and **cons** of each architecture you will be able to select the right solution, especially when managing a distributed network.

The three network management architectures are:

- **Centralized** Network Management
- **Distributed** Network Management
- **Hierarchical** Network Management

Centralized Network Management Architecture



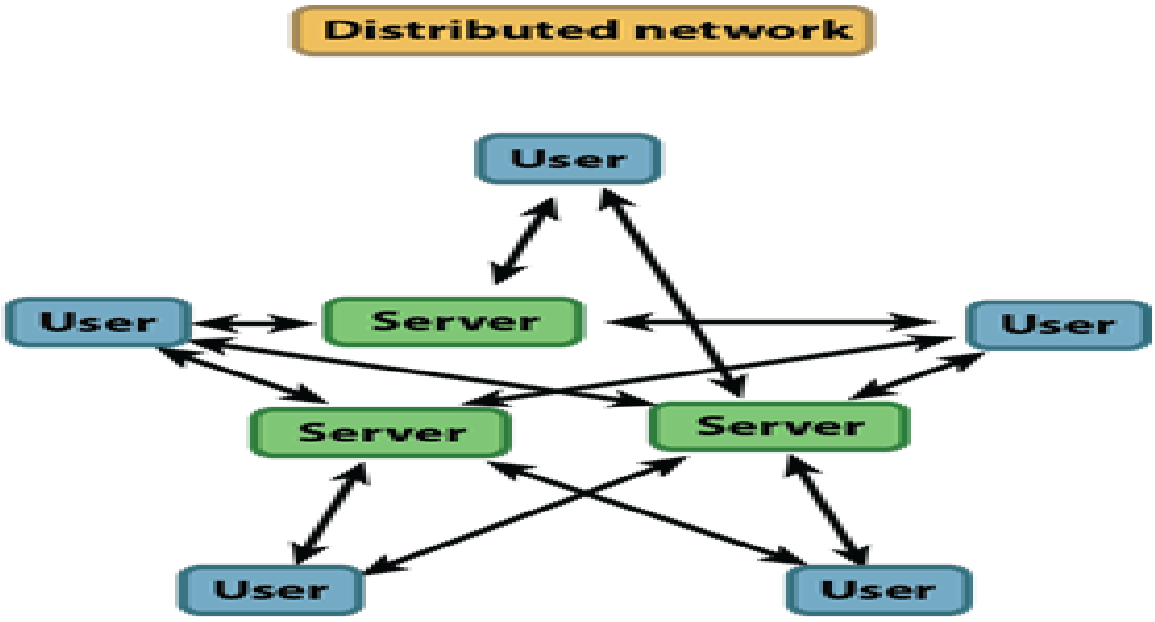
With a centralized architecture a **single management system installation** monitors the whole network. This installation may consist of one or more servers due to hardware limitations. If more than one server is used, it is considered as a centralized architecture when all servers are located at the same NOC.

As depicted in the above example diagram, with the **centralized** network management architecture, a distributed network that spans multiple geographical regions is managed from a single Network Operations Center (NOC). NOC operators from each of the regions use clients to remote connect to the centralized management servers located in another region.

With this architecture, the network management system consists of:

- **One or more NMS server(s), located in a single NOC**. The servers manage the network of the three regions, meaning that they will require Data Communications Network infrastructure (DCN) i.e., routers, switches and Ethernet connectivity from the single NOC they are installed to the remote regions where the network devices are installed to be able to establish management communication.
- **One or more clients located at all regions.** These clients communicate remotely over DCN to the central server.

Distributed Network Management Architecture

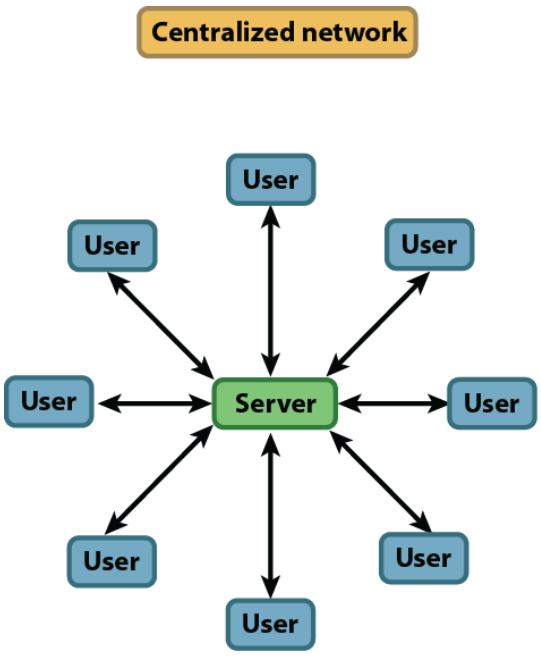


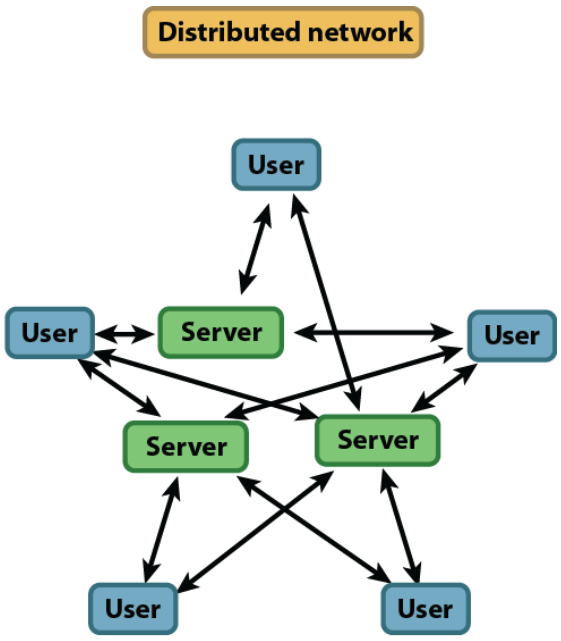
With a distributed architecture, **multiple installations of management systems** are used to monitor the whole network. Each management system is installed at a NOC that is responsible to monitor a geographical or administration region / domain, i.e. it is a *Domain Manager*.

As depicted in the above example diagram, with the **distributed** network management architecture, a distributed network that spans three regions, is managed from three NMS servers each one located at a regional Network Operating Center (NOC). NOC operators of a region use clients to locally connect to their server that manages the part of the network installed at their region.

With this architecture, the network management system consists of:

- **Three NMS servers, each located in a separate NOC**. Each server manages the (sub) network of the region it belongs, meaning that it will NOT require Data Communications Network infrastructure (DCN) i.e., routers, switches and Ethernet connectivity, from the NOC region to remote regions.
- **Clients located at all regions.** These communicate locally to their server.





Hierarchical Network Management Architecture

With a hierarchical architecture, **multiple installations of management systems** are used to monitor the whole network. Each management system is installed at a NOC that is responsible to monitor a geographical or administration region / domain, i.e. it is a *Domain Manager*. So far this is exactly the same as the distributed architecture, except that the hierarchical architecture adds an additional layer, the **Manager of Managers (MoM)**. This Manager of Managers sits at a higher level and requests information from domain managers. There is no communication between domain managers, information flow follows the hierarchy. The hierarchy can be further expanded by adding additional layers of MoMs and therefore is quite scalable.