Name:Soham Desai
Batch B

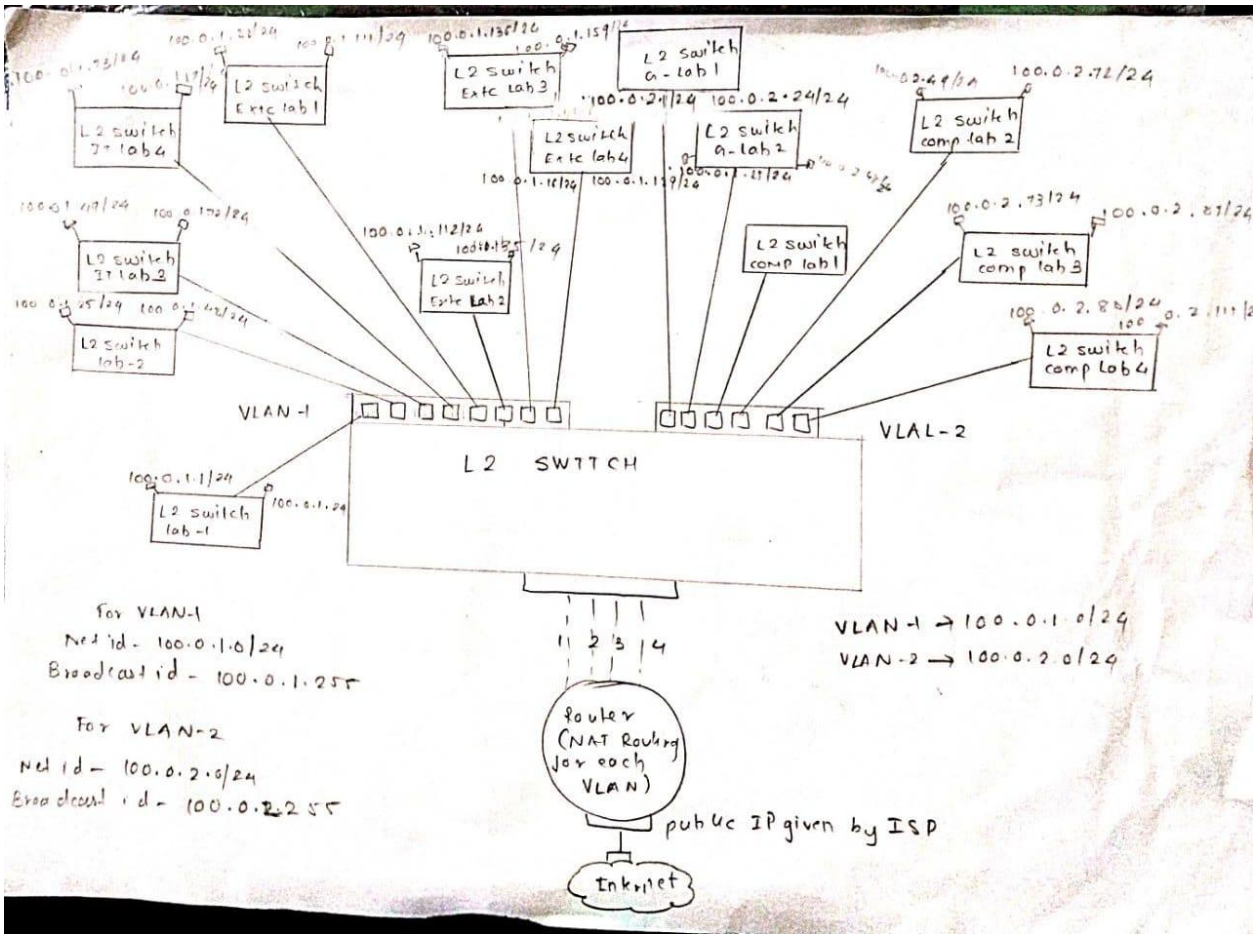
Roll no : 11
Xavier ID: 202003021

Experiment 10

Aim : Case Study: (Group Activity) Design a network for an organization using the concepts of Addressing (IP Address Assignment), Naming (DNS) and Routing.

LO 6 : Design a network for an organization using a network tool

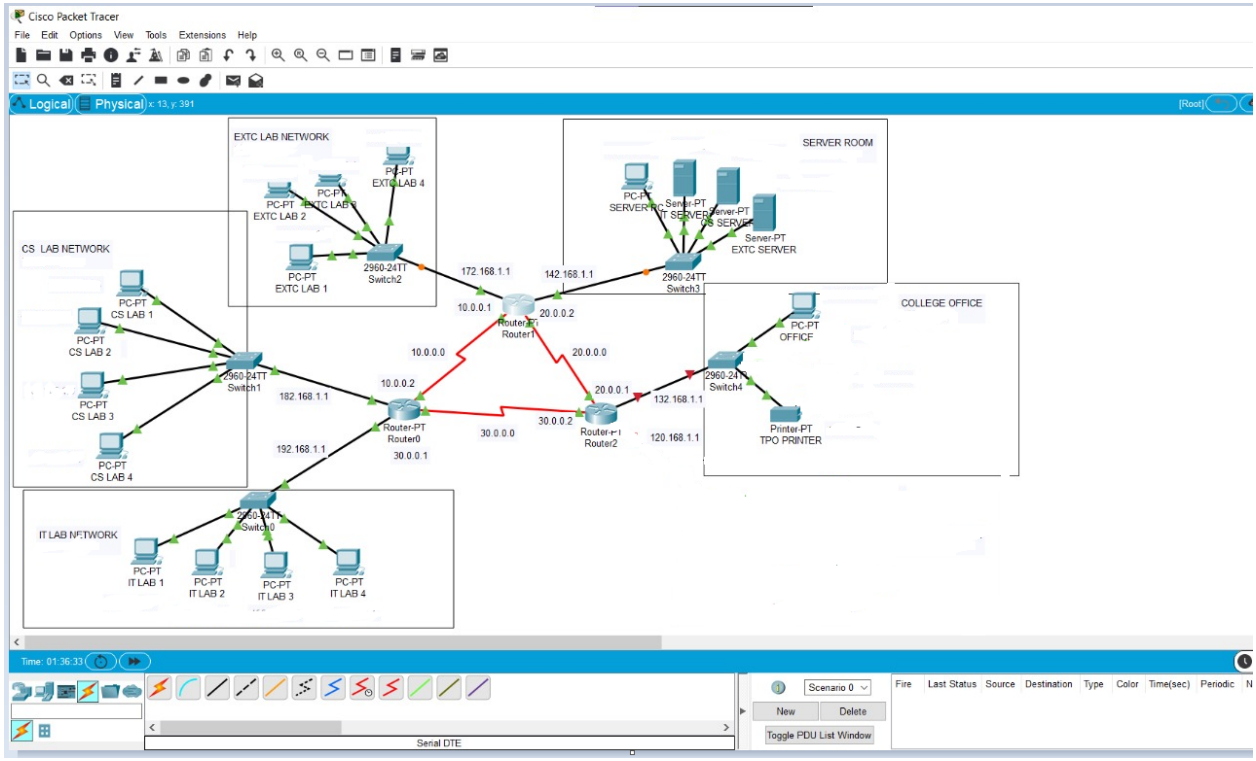
Network Design:



In our Network Design of the college we have taken two subnetworks VLAN-1 and VLAN-2 for the ground and the first floor and for second and third floor respectively

Name:Soham Desai
Batch B

Roll no : 11
Xavier ID: 202003021



This is the design of the network made and being run on the Cisco Packet Tracer and we can see that we have different switches and hubs for the respective departments.

Name:Soham Desai
Batch B
Roll no : 11
Xavier ID: 202003021

Theory:

A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs). A LAN is a group of computers and devices that share a communications line or wireless link to a server within the same geographical area.

VLANs make it easy for network administrators to partition a single switched network to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure. VLANs are often set up by larger businesses to re-partition devices for better traffic management.

VLANs are also important because they can help improve the overall performance of a network by grouping together devices that communicate most frequently. VLANs also provide security on larger networks by allowing a higher degree of control over which devices have access to each other. VLANs tend to be flexible because they are based on logical connections, rather than physical.

Ports (interfaces) on switches can be assigned to one or more VLANs, enabling systems to be divided into logical groups -- based on which department they are associated with -- and establish rules about how systems in the separate groups are allowed to communicate with each other. These groups can range from the simple and practical (computers in one VLAN can see the printer on that VLAN, but computers outside that VLAN cannot), to the complex and legal (for example, computers in the retail banking departments cannot interact with computers in the trading departments).

Each VLAN provides data link access to all hosts connected to switch ports configured with the same VLAN ID. The VLAN tag is a 12-bit field in the Ethernet header that provides support for

up to 4,096 VLANs per switching domain. VLAN tagging is standardized in IEEE (Institute of Electrical and Electronics Engineers) 802.1Q and is often called *Dot1Q*.

When an untagged frame is received from an attached host, the VLAN ID tag configured on that interface is added to the data link frame header, using the 802.1Q format. The 802.1Q frame is then forwarded toward the destination. Each switch uses the tag to keep each VLAN's traffic separate from other VLANs, forwarding it only where the VLAN is configured. Trunk links between switches handle multiple VLANs, using the tag to keep them segregated. When the frame reaches the destination switch port, the VLAN tag is removed before the frame is to be transmitted to the destination device.

Multiple VLANs can be configured on a single port using a *trunk* configuration in which each frame sent via the port is tagged with the VLAN ID, as described above. The neighboring device's interface, which may be on another switch or on a host that supports 802.1Q tagging, will need to support trunk mode configuration to transmit and receive tagged frames. Any untagged Ethernet frames are assigned to a default VLAN, which can be designated in the switch configuration.

When a VLAN-enabled switch receives an untagged Ethernet frame from an attached host, it adds the VLAN tag assigned to the ingress interface. The frame is forwarded to the port of the host with the destination MAC address(media access control address). Broadcast, unknown unicast and multicast (BUM traffic) is forwarded to all ports in the VLAN. When a previously unknown host replies to an unknown unicast frame, the switches learn the location of this host and do not flood subsequent frames addressed to that host.

The switch-forwarding tables are kept up to date by two mechanisms. First, old forwarding entries are removed from the forwarding tables periodically, often a configurable timer. Second, any topology change causes the forwarding table refresh timer to be reduced, triggering a refresh.

Name:Soham Desai
Batch B
Roll no : 11
Xavier ID: 202003021

Without VLANs, a broadcast sent from a host can easily reach all network devices. Each and every device will process broadcast received frames. It can increase the CPU overhead on each device and reduce the overall network security.
In case if you place interfaces on both switches into separate VLAN, a broadcast from host A can reach only devices available inside the same VLAN. Hosts of VLANs will not even be aware that the communication took place.

Advantages and Disadvantages of VLAN

Advantages to VLAN include reduced broadcast traffic, security, ease of administration and broadcast domain confinement.

However, a disadvantage of VLANs includes the limitation of 4,096 VLANs per switching domain creates problems for large hosting providers, which often need to allocate tens or hundreds of VLANs for each customer. To address this limitation, other protocols, like VXLAN(Virtual Extensible LAN), NVGRE (Network Virtualization using Generic Routing Encapsulation) and Geneve, support larger tags and the ability to tunnel Layer 2 frames within Layer 3 (network) packets.

Application/Purpose of VLAN

Here are the important uses of VLAN:

- VLAN is used when you have 200+ devices on your LAN.
- It is helpful when you have a lot of traffic on a LAN.
- VLAN is ideal when a group of users need more security or being slow down by many broadcasts.
- It is used when users are not on one broadcast domain.
- Make a single switch into multiple switches.

Name:Soham Desai
Batch B
Roll no : 11
Xavier ID: 202003021

Internet Protocol (IP) is a set of governing rules for data packets, data format, or datagram sent through a local network or the internet. It is a connectionless and datagram-oriented protocol as it works on a dynamic computer network. An IP works without a centralized monitor or directory and never relies on a node or link. Hence, each data packet must have the source and destination's IP address and other key information to get delivered successfully.

An IP address is an address used in order to uniquely identify a device on an IP network. The address is made up of 32 binary bits, which can be divisible into a network portion and host portion with the help of a subnet mask. The 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is converted to decimal and separated by a period (dot). For this reason, an IP address is said to be expressed in dotted decimal format (for example, 172.16.81.100). The value in each octet ranges from 0 to 255 decimal, or 00000000 - 11111111 binary.

An IP address is the identifier that enables your device to send or receive data packets across the internet. It holds information related to your location and therefore making devices available for two-way communication. The internet requires a process to distinguish between different networks, routers, and websites. Therefore, IP addresses provide the mechanism of doing so, and it forms an indispensable part in the working of the internet. You will notice that most of the IP addresses are essentially numerical. Still, as the world is witnessing a colossal growth of network users, the network developers had to add letters and some addresses as internet usage grows.

An IP address is represented by a series of numbers segregated by periods(.). They are expressed in the form of four pairs - an example address might be 255.255.255.255 wherein each set can range from 0 to 255.

IP addresses are not produced randomly. They are generated mathematically and are further assigned by the IANA (Internet Assigned Numbers Authority), a department of the ICANN.

Name:Soham Desai Roll no : 11
Batch B Xavier ID: 202003021

ICANN stands for Internet Corporation for Assigned Names and Numbers. It is a non-profit corporation founded in the US back in 1998 with an aim to manage Internet security and enable it to be available by all.

How do IP addresses work?

Sometimes your device doesn't connect to your network the way you expect it to be, or you wish to troubleshoot why your network is not operating correctly. To answer the above questions, it is vital to learn the process with which IP addresses work.

Internet Protocol or IP runs the same manner as other languages, i.e., applying the set guidelines to communicate the information. All devices obtain, send, and pass information with other associated devices with the help of this protocol only. By using the same language, the computers placed anywhere can communicate with one another.

The process of IP address works in the following way:

1. Your computer, smartphone, or any other Wi-Fi-enabled device firstly connects to a network that is further connected to the internet. The network is responsible for giving your device access to the internet.
2. While working from home, your device would be probably using that network provided by your Internet Service Provider (ISP). In a professional environment, your device uses your company network.
3. Your ISP is responsible to generate the IP address for your device.
4. Your internet request penetrates through the ISP, and they place the requested data back to your device using your IP address. Since they provide you access to the internet, ISP's are responsible for allocating an IP address to your computer or respective device.
5. Your IP address is never consistent and can change if there occurs any changes in its internal environment. For instance, if you turn your modem or router on or off, it will change your IP address. Or the user can also connect the ISP to change their IP address.

6. When you are out of your home or office, mainly if you travel and carry your device with you, your computer won't be accessing your home IP address anymore. This is because you will be accessing the different networks (your phone hotspot, Wi-Fi at a cafe, resort, or airport, etc.) to connect the device with the internet. Therefore, your device will be allocated a different (temporary) IP address by the ISP of the hotel or cafe.

Types of IP addresses

There are various classifications of IP addresses, and each category further contains some types.

Consumer IP addresses

Every individual or firm with an active internet service system pursues two types of IP addresses, i.e., Private IP (Internet Protocol) addresses and public IP (Internet Protocol) addresses. The public and private correlate to the network area. Therefore, a private IP address is practiced inside a network, whereas the other (public IP address) is practiced outside a network.

1. Private IP addresses

All the devices that are linked with your internet network are allocated a private IP address. It holds computers, desktops, laptops, smartphones, tablets, or even Wi-Fi-enabled gadgets such as speakers, printers, or smart Televisions. With the expansion of IoT (internet of things), the demand for private IP addresses at individual homes is also seemingly growing. However, the router requires a method to identify these things distinctly. Therefore, your router produces unique private IP addresses that act as an identifier for every device using your internet network. Thus, differentiating them from one another on the network.

2. Public IP addresses

A public IP address or primary address represents the whole network of devices associated with it. Every device included within with your primary address contains their own private IP address.

Name:Soham Desai Roll no : 11
Batch B Xavier ID: 202003021

ISP is responsible to provide your public IP address to your router. Typically, ISPs contains the bulk stock of IP addresses that they dispense to their clients. Your public IP address is practiced by every device to identify your network that is residing outside your internet network.

Public IP addresses are further classified into two categories- dynamic and static.

- **Dynamic IP addresses**

  As the name suggests, Dynamic IP addresses change automatically and frequently. With this types of IP address, ISPs already purchase a bulk stock of IP addresses and allocate them in some order to their customers. Periodically, they re-allocate the IP addresses and place the used ones back into the IP addresses pool so they can be used later for another client. The foundation for this method is to make cost savings profits for the ISP.

- **Static IP addresses**

  In comparison to dynamic IP addresses, static addresses are constant in nature. The network assigns the IP address to the device only once and, it remains consistent. Though most firms or individuals do not prefer to have a static IP address, it is essential to have a static IP address for an organization that wants to host its network server. It protects websites and email addresses linked with it with a constant IP address.

In reality, other versions were defined, from versions 1 to 9, but only versions 4 and 6 found widespread use. Version 1 and 2 were TCP protocol names in 1974 and ’77 to separate the IP specification at that time. Moreover, version 3 was introduced in 1978, where v3.1 was the first ever version in which TCP got separated from IP. Next, version 5 that surfaced in 1979 was the experimental protocol – Internet Stream Protocol.

IPv6 is a combination of various versions – v6, v7, v8, and v9.

Name:Soham Desai Roll no : 11
Batch B Xavier ID: 202003021

The Domain Name System (DNS) underpins the web we use every day. It works transparently in the background, converting human-readable website names into computer-readable numerical IP addresses. DNS does this by looking up that information on a system of linked DNS servers across the Internet. However, different DNS servers can behave differently in terms of speed and security. So, let's take a look at how DNS works and what you can do to make sure it's working its best for you.

Domain Names and IP Addresses

Domain names are the human-readable website addresses we use every day. For example, Google's domain name is google.com. If you want to visit Google, you just need to enter google.com into your web browser's address bar.

DNS Servers

DNS servers match domain names to their associated IP addresses. When you type a domain name into your browser, your computer contacts your current DNS server and asks what IP address is associated with the domain name. Your computer then connects to the IP address and retrieves the right web page for you.

The DNS servers you use are likely provided by your Internet service provider (ISP). If you're behind a router, your computer may be using the router itself as its DNS server, but the router is forwarding requests to your ISP's DNS servers.

Some viruses and other malware programs can change your default DNS server to a DNS server run by a malicious organization or scammer. This malicious DNS server can then point popular websites to different IP addresses, which could be run by scammers.

Name:Soham Desai Roll no : 11
Batch B Xavier ID: 202003021

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet.

In packet switching networks, routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms. Packet forwarding is the transit of network packets from one network interface to another. Intermediate nodes are typically network hardware devices such as routers, gateways, firewalls, or switches. General-purpose computers also forward packets and perform routing, although they have no specially optimized hardware for the task.

The routing process usually directs forwarding on the basis of routing tables. Routing tables maintain a record of the routes to various network destinations. Routing tables may be specified by an administrator, learned by observing network traffic or built with the assistance of routing protocols.

Routing, in a narrower sense of the term, often refers to IP routing and is contrasted with bridging. IP routing assumes that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within local area networks.

Name:Soham Desai Roll no : 11
Batch B Xavier ID: 202003021

The following protocols help data packets find their way across the Internet:

IP: The Internet Protocol (IP) specifies the origin and destination for each data packet. Routers inspect each packet's IP header to identify where to send them.

BGP: The Border Gateway Protocol (BGP) routing protocol is used to announce which networks control which IP addresses, and which networks connect to each other. (The large networks that make these BGP announcements are called autonomous systems.) BGP is a dynamic routing protocol.

The below protocols route packets within an AS:

OSPF: The Open Shortest Path First (OSPF) protocol is commonly used by network routers to dynamically identify the fastest and shortest available routes for sending packets to their destination.

RIP: The Routing Information Protocol (RIP) uses "hop count" to find the shortest path from one network to another, where "hop count" means number of routers a packet must pass through on the way. (When a packet goes from one network to another, this is known as a "hop.")

Other interior routing protocols include EIGRP (the Enhanced Interior Gateway Routing Protocol, mainly for use with Cisco routers) and IS-IS (Intermediate System to Intermediate System).