****

Department of Electronics and Communication Engineering

University College of Engineering, Osmania University, Hyderabad



**REPORT ON SUMMER INTERNSHIP 2021**

Topic - Designing a Campus Area Network

Submitted to:

Prof.P.Koti Lakshmi

Prof.P.Naveen Kumar

Submitted by:

Megha Mallela – 100518735024

Mitta Sai Ruthvik Reddy – 100518735025

Nirali Nallapuri – 100518735030

TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
| **S.NO** | **TOPIC** | **PAGE NUMBER** |
| 1 | INTRODUCTION | 3 |
| 2 | OBJECTIVES | 8 |
| 3 | VLAN | 14 |
| 4 | INTERNET CONNECTIVITY | 18 |
| 5 | CONCLUSION | 26 |

**Title**

**Design of campus area network using Virtual Local Area Network(VLAN) with Physical Network Security Implementation and connectivity of Internet with wired and wireless access.**

**Chapter 1: ABSTRACT**

We did our summer internship at Bharat Sanchar Nigam Limited, a government-owned telecommunications service provider. Their primary service is to provide fixed telephone lines and mobile telephony services on GSM and CDMA platforms.

The main aim was to establish communication within a particular department and also to establish inter-departmental communication.

One of the ways to execute this is to use a local area network (LAN) connection. A local area network includes all the user devices, servers, switches, routers, cables, and wireless access points in one location. It connects all the devices in the same broadcast domain. The idea we adopted was to use a virtual local area network (VLAN) connection. We established communication by virtual local area network (VLAN) and provided Internet connection for wired and wireless access.

We used a virtual local area network instead of a local area network to reduce the number of switches. Without VLANs, a switch considers all its interfaces to be in the same broadcast domain. When a broadcast frame enters one switch port, the switch forwards that frame out to all other ports. So, to create two different LAN broadcast domains needs two Ethernet LAN switches. With VLANs, a switch can configure interfaces into separate broadcast domains.

We implemented this project using the Cisco packet tracer, a [cross-platform](https://en.wikipedia.org/wiki/Cross-platform) visual [simulation](https://en.wikipedia.org/wiki/Simulation) tool designed by [Cisco Systems](https://en.wikipedia.org/wiki/Cisco_Systems) to create [network topologies](https://en.wikipedia.org/wiki/Network_topologies) and imitate modern [computer networks](https://en.wikipedia.org/wiki/Computer_networks). The software allows users to simulate the configuration of Cisco routers and switches using a simulated command-line interface.

**1.1. About the organization:**

* Bharat Sanchar Nigam Limited is a government-owned telecommunications service provider headquartered in New Delhi, India.
* It is under the ownership of the Department of Telecommunications, Ministry of Communications, Government of India.
* Regional Telecom Training Centre has been established in Hyderabad by the Department of Telecommunications to impart training to their staff.

They also offer internships to the second year or third year B.Tech students to familiarize themselves in the fields of Communication.



**1.2. Introduction:**

A LAN includes all the user devices, servers, switches, routers, cables, and wireless access points in one location. A LAN includes all devices in the same broadcast domain. A broadcast domain includes the set of all LAN-connected devices so that when any of the devices sends a broadcast frame, all the other devices get a copy of the frame. So, from one perspective, a LAN and a broadcast domain as being the same thing. Without VLANs, a switch considers all its interfaces to be in the same broadcast domain. That is, for one switch, when a broadcast frame entered one switch port, the switch forwarded that broadcast frame out all other ports. With that logic, to create two different LAN broadcast domains needs two different Ethernet LAN switches.

With support for VLANs, a single switch can accomplish the same goals of the design to create two broadcast domains—with a single switch. With VLANs, a switch can configure some interfaces into one broadcast domain and some into another, creating multiple broadcast domains. These individual broadcast domains created by the switch are called virtual LANs (VLAN).

Designing campus LANs to use more VLANs, each with a smaller number of devices, often helps improve the LAN in many ways. For example, a broadcast sent by one host in a VLAN will be received and processed by all the other hosts in the VLAN—but not by hosts in a different VLAN. Limiting the number of hosts that receive a single broadcast frame reduces the number of hosts that waste effort processing unneeded broadcasts. It also reduces security risks, because fewer hosts see frames sent by anyone host.   
These are just a few reasons for separating hosts into different VLANs.

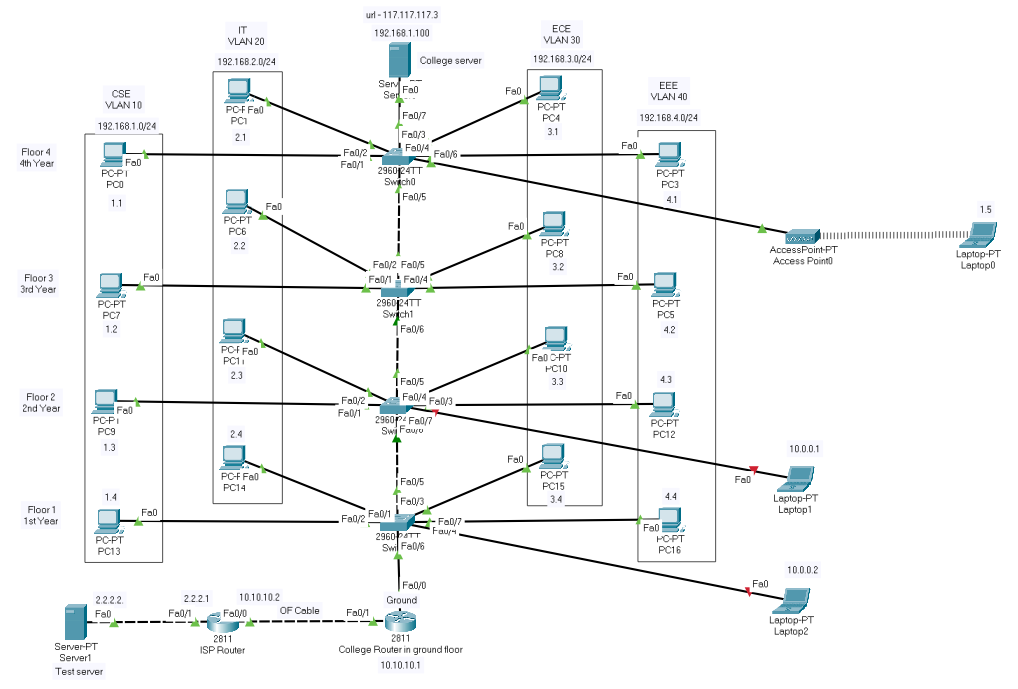
The following list summarizes the most common reasons for choosing to create smaller broadcast domains (VLANs):

* To reduce CPU overhead on each device by reducing the number of devices that receive each broadcast frame.
* To reduce security risks by reducing the number of hosts that receive copies of frames that the switches flood (broadcasts, multicasts, and unknown unicasts)
* To improve security for hosts that send sensitive data by keeping those hosts on a separate VLAN
* To create more flexible designs that group users by department, or by groups that work together, instead of by physical location
* To solve problems more quickly, because the failure domain for many problems is the same set of devices as those in the same broadcast domain.

**1.3. Project Description**

In this Project, the trainee should design a college campus area Network with VLANs with different Hosts and Departments as per the following requirement.

1. College campus is a (Ground + 4 ) 5 Floor building.
2. Ground Floor has 100Mbps connectivity to ISP for Internet with a CISCO 2811 Router with a single LAN port.
3. The first, second, Third, and Fourth floors have Hosts belonging to CSC/IT//ECE/EEE departments related to I year, II year, III Year, and Final year students' classrooms. Each Floor has a switch connecting these hosts.
4. Switch from the top floor is connected directly to its next floor switch and finally, from the First-floor switch, a cable is extended to the ground floor to the LAN port of CISCO Router 2811.
5. The administrator has been asked to configure the departments in different VLAN domains and also instructed that communication between the departments is also required.
6. The administrator has been asked to place an Access point for wireless connectivity with a security password from the Fourth Floor on need basis
7. The administrator has been asked to create security credentials for login to the Router and Switches such that the authorized person only logs in.
8. The administrator has been asked to make sure that if anyone connects a PC in the vacant ports of the switch on any floor they should not be connected to Network.
9. The administrator has been asked to allocate 40 Mbps bandwidth to the CSC department, 30 Mbps bandwidth to the IT department, 20 Mbps bandwidth for the ECE department & 10 Mbps bandwidth to the EEE department for Internet access.
10. ISP has given the 10.10.10.0/30 subnet to the college and asked the administrator to configure the WAN link IP 10.10.10.1 at the College side WAN interface on the Router. The Internet IP pool given to the college by ISP is 117.117.117.0/29.
11. The administrator has been instructed to make sure that all computers available on the campus should be connected to the Internet (except 192.168.2.3)
12. The administrator has been asked to put the college website IP as 117.117.117.3 and this website has to be accessed from the Internet.  
     (Please Take any Class C, IP Pool s for the LAN networks connectivity)
13. DHCP Protocol and Configuration of DHCP on CISCO Router for automatic assignment of IP addresses.
14. Configuration of DNS entries for browsing using URL.



THIS IS THE DESIGNED NETWORK

**Chapter 2: Objectives**

→ Networks

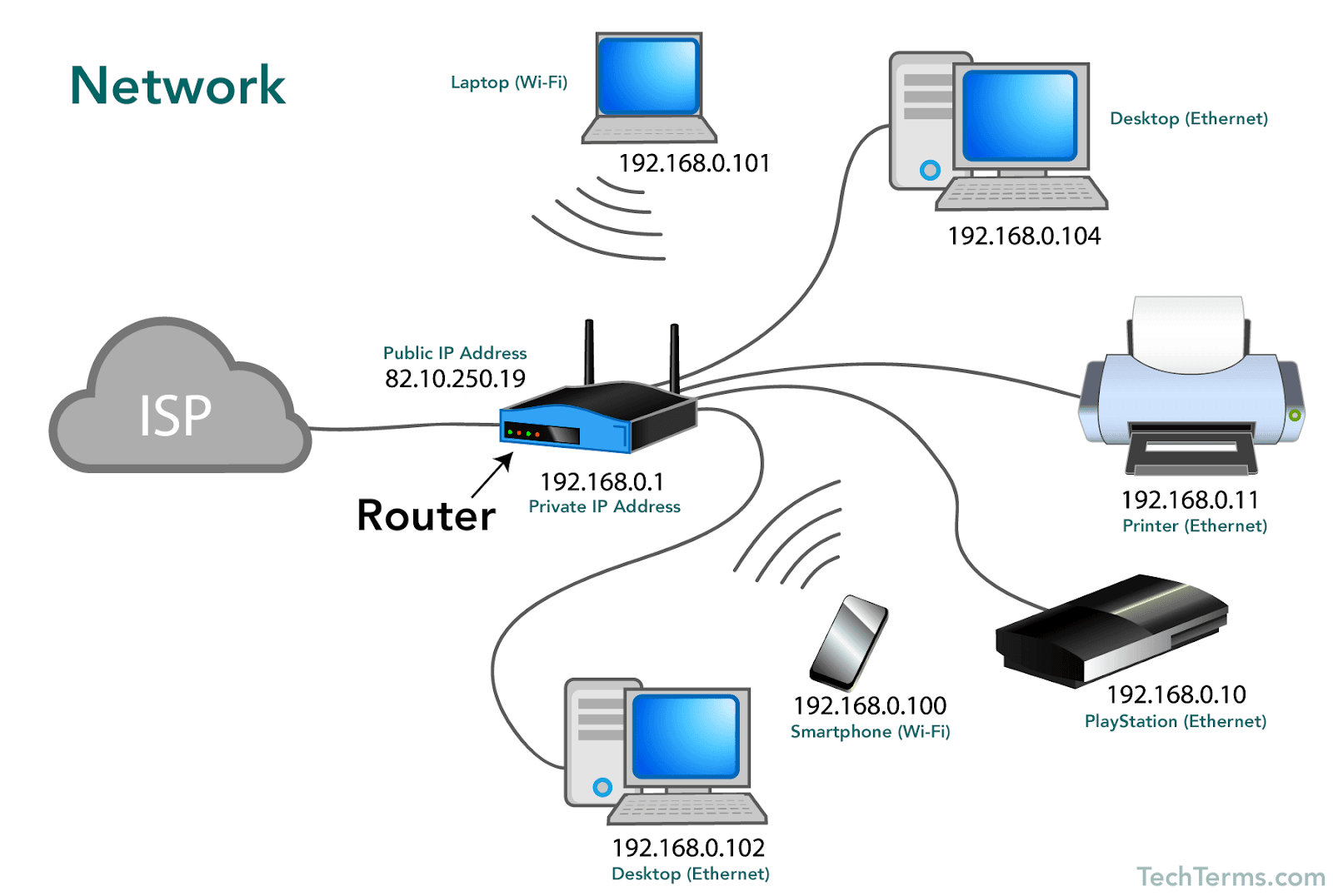
→ Types of networks

→ IP Addressing

→ Wireless connectivity

→ DNS Server

→ Working of a campus area network using VLAN



**What is a Computer Network?**

A computer network is a set of [computers](https://en.wikipedia.org/wiki/Computer) sharing resources located on or provided by [network nodes](https://en.wikipedia.org/wiki/Node_(networking)). The computers use common [communication protocols](https://en.wikipedia.org/wiki/Communication_protocol) over [digital](https://en.wikipedia.org/wiki/Digital_signal) [interconnections](https://en.wikipedia.org/wiki/Interconnection) to communicate with each other. These interconnections are made up of [telecommunication network](https://en.wikipedia.org/wiki/Telecommunication_network) technologies, based on physically wired, optical, and wireless radio-frequency methods that may be arranged in a variety of [network topologies](https://en.wikipedia.org/wiki/Network_topology).

The nodes of a computer network may include [personal computers](https://en.wikipedia.org/wiki/Personal_computer), [servers](https://en.wikipedia.org/wiki/Server_(computing)), [networking hardware](https://en.wikipedia.org/wiki/Networking_hardware), or other specialized or general-purpose [hosts](https://en.wikipedia.org/wiki/Host_(network)). They are identified by [network addresses](https://en.wikipedia.org/wiki/Network_address) and may have [hostnames](https://en.wikipedia.org/wiki/Hostname). Hostnames serve as memorable labels for the nodes, rarely changed after initial assignment. Network addresses serve for locating and identifying the nodes by communication protocols such as the [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol).

Computer networks may be classified by many criteria, including the [transmission medium](https://en.wikipedia.org/wiki/Transmission_medium) used to carry signals, [bandwidth](https://en.wikipedia.org/wiki/Bandwidth_(computing)), [communications protocols](https://en.wikipedia.org/wiki/Communications_protocol) to organize network traffic, network size, the topology, [traffic control](https://en.wikipedia.org/wiki/Network_traffic_control) mechanism, and organizational intent.

Computer networks support many [applications](https://en.wikipedia.org/wiki/Application_software) and [services](https://en.wikipedia.org/wiki/Network_service), such as access to the [World Wide Web](https://en.wikipedia.org/wiki/World_Wide_Web), [digital video](https://en.wikipedia.org/wiki/Digital_video), [digital audio](https://en.wikipedia.org/wiki/Digital_audio), shared use of [application and storage servers](https://en.wikipedia.org/wiki/File_server), printers, and [fax machines](https://en.wikipedia.org/wiki/Fax), and use of [email](https://en.wikipedia.org/wiki/Email) and [instant messaging](https://en.wikipedia.org/wiki/Instant_messaging) applications.

**2.1. Types of networks**

Some of the different types of networks are :

→ Local area network

→ Wide area network

→ Metropolitan area network

**2.2. What is a LAN?**

A local area network (LAN) is a collection of devices connected in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.

Regardless of size, a LAN's single defining characteristic is that it connects devices that are in a single, limited area. In contrast, a [wide area network](https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html) (WAN) or metropolitan area network (MAN) covers larger geographic areas. Some WANs and MANs connect many LANs.

**What’s in a LAN?**

A LAN comprises cables, access points, switches, routers, and other components that enable devices to connect to internal servers, web servers, and other LANs via wide area networks.

The rise of virtualization has also fueled the development of virtual LANs, which enable network administrators to logically group network nodes and partition their networks without a need for major infrastructure changes.

For example, in an office with multiple departments, such as accounting, IT support, and administration, each department's computers could be logically connected to the same switch but segmented to behave as if they are separate.

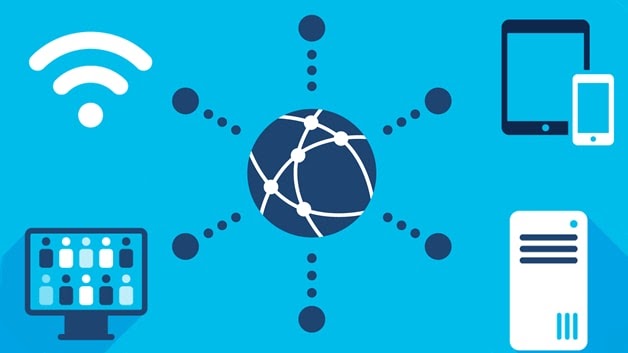
**Benefits of a LAN:**

The advantages of a LAN are the same as those for any group of devices networked together. The devices can use a single Internet connection, share files, print to shared printers, and be accessed and even controlled by one another.

LANs were developed in the 1960s for use by colleges, universities, and research facilities (such as NASA), primarily to connect computers to other computers. It wasn't until the development of Ethernet technology (1973, at Xerox PARC), its commercialization (1980), and its standardization (1983) that LANs started to be used widely.

While the benefits of having devices connected to a network have always been well understood, it wasn't until the wide deployment of Wi-Fi technology that LANs became commonplace in nearly every type of environment. Today, not only do businesses and schools use LANs, but also restaurants, coffee shops, stores, and homes.

Wireless connectivity has also greatly expanded the types of devices that can be connected to a LAN. Now, nearly everything imaginable can be "connected," from PCs, printers, and phones to smart TVs, stereos, speakers, lighting, thermostats, window shades, door locks, security cameras--and even coffeemakers, refrigerators, and toys.



A LAN NETWORK

**2.3. What is a MAN?**

A metropolitan area network (MAN) is a computer network that is larger than a single building local area network ([LAN](https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN)) but is located in a single geographic area that is smaller than a wide area network ([WAN](https://www.techtarget.com/searchnetworking/definition/WAN-wide-area-network)). Generally, it is several LANs interconnected by dedicated [backbone](https://www.techtarget.com/searchnetworking/definition/backbone) connections. It may also refer to public use networking infrastructure in a municipality or region.

**MAN for organizations:**

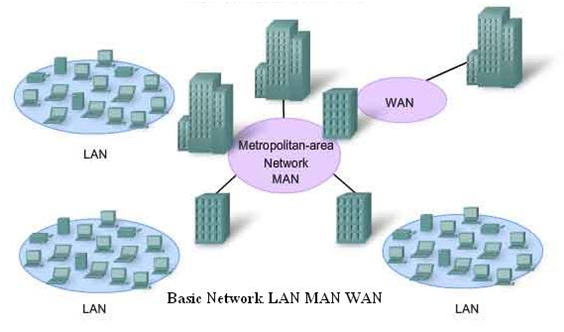
A metropolitan area network traditionally refers to a private data network used by a single organization in several buildings or by several organizations interconnected in the same geographic vicinity. It is larger than a LAN in a single building but not large enough to be considered a WAN. The size usually ranges from 5 kilometers to 50 km. If all the buildings are on a single piece of contiguous property, it may also be considered a [campus network](https://www.techtarget.com/searchnetworking/definition/campus-network).

Generally, a MAN is small enough that dedicated point-to-point, or backbone, data connections are established between buildings or to a hosted colocation (colo) data center. These backbone connections can use a variety of link technologies, including Ethernet runs, leased Dark fiber or private fiber, point-to-point Wi-Fi, wireless LAN ([WLAN](https://searchmobilecomputing.techtarget.com/definition/wireless-LAN)), millimeter-wave (MM wave) radio, and microwave radio links or private [5G](https://www.techtarget.com/searchnetworking/definition/5G) networks. Public internet routed links, such as through a virtual private network (VPN) or public cloud, would not be considered part of a MAN but may be included in a MAN diagram for simplicity. A well-designed system will have redundant links between locations.

**Advantages and Disadvantages of MAN:**

The primary advantage of a MAN over a WAN is the high bandwidth enabled by the dedicated links of a metropolitan area network. This application of a MAN provides higher speed, from 1 gigabit per second to 100 Gbps, and lower latency than would be possible over a WAN. Since the organization maintains control of the connection, it can apply traffic shaping and increased security.

Disadvantages of a MAN over a WAN include potentially higher costs, greater complexity, and additional logistics required to maintain the links. A well-designed MAN will also have redundant connections, requiring at least two connections per building.

.

Network of LAN, WAN, and MAN

**2.4. What is a WAN?**

A wide area network (also known as WAN), is a large network of information that is not tied to a single location. WANs can facilitate communication, the sharing of information, and much more between devices from around the world through a WAN provider.

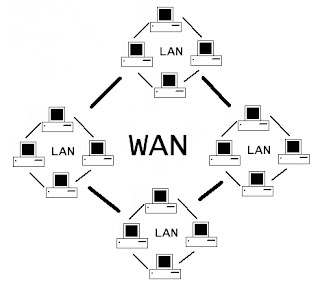
WANs can be vital for international businesses, but they are also essential for everyday use, as the internet is considered the largest WAN in the world. Keep reading for more information on WANs, their use, how they differ from other networks, and their overall purpose for businesses and people, alike.

### What Is the Purpose of a WAN Connection?

If WAN connections didn’t exist, organizations would be isolated to restricted areas or specific geographic regions. LANs would allow organizations to work within their building, but growth to outside areas — either different cities or even different countries — would not be possible because the associated infrastructure would be cost-prohibitive for most organizations.

As organizations grow and become international, WANs allow them to communicate between branches, share information and stay connected. When employees travel for work, WANs allow them to access the information they need to do their job. WANs also help organizations share information with customers, as well as partner organizations, such as B2B clients or customers.

However, WANs also provide an essential service to the public. Students at universities might rely on WANs to access library databases or university research. And every day, people rely on WANs to communicate, bank, shop, and more.



WAN NETWORK

## Chapter 3: VLAN

## 3.1. What is VLAN?

**VLAN** is a custom network that is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as a Virtual Local Area Network.

## 3.2. How does a VLAN work?

Here is a step by step process of how a VLAN works:

* VLANs in networking are identified by a number.
* A Valid range is 1-4094. On a VLAN switch, you assign ports with the proper VLAN number.
* The switch then allows data, which needs to be sent between various ports having the same VLAN.
* Since almost all networks are larger than a single switch, there should be a way to send traffic between two switches.
* One simple and easy way to do this is to assign a port on each network switch with a VLAN and run a cable between them.

## 3.3. Advantages of VLAN:

Here are the important pros/benefits of VLAN:

* It solves a broadcast problem.
* VLAN reduces the size of broadcast domains.
* VLAN allows you to add an additional layer of security.
* It can make device management simple and easier.
* You can make a logical grouping of devices by function rather than location.
* It allows you to create groups of logically connected devices that act like they are on their network.
* You can logically segment networks based on departments, project teams, or functions.
* VLAN helps you to geographically structure your network to support the growing companies.
* Higher performance and reduced latency.
* VLANs provide increased performance.
* Users may work on sensitive information that must not be viewed by other users.
* VLAN removes the physical boundary.
* It lets you easily segment your network.

## 3.4. Disadvantages of VLAN

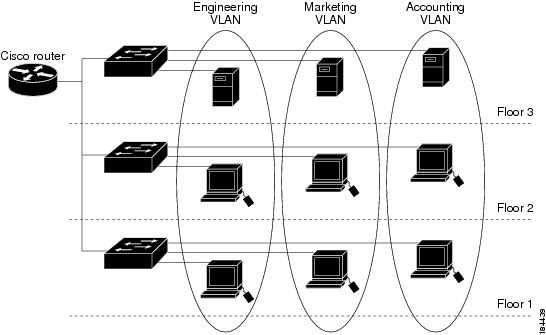
Here are the important cons/ drawbacks of VLAN:

* A packet can leak from one VLAN to another.
* An injected packet may lead to a cyber-attack.
* The threat in a single system may spread a virus through a whole logical network.
* You require an additional router to control the workload in large networks.
* You can face problems in interoperability.
* A VLAN cannot forward network traffic to other VLANs.

## 3.5. Application/Purpose of VLAN

Here are the important uses of VLAN:

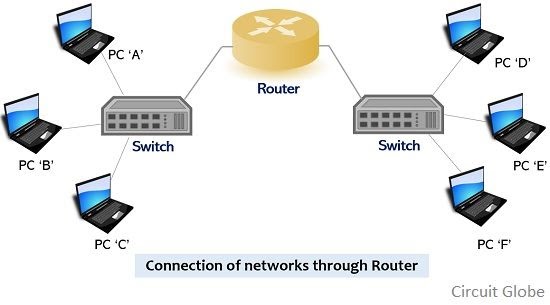
* VLAN is used when you have 200+ devices on your LAN.
* It is helpful when you have a lot of traffic on a LAN.
* VLAN is ideal when a group of users need more security or is being slowed down by many broadcasts.
* It is used when users are not on one broadcast domain.
* Make a single switch into multiple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



**VLAN NETWORK**

**Switch vs router**

| **S.No.** | **Router** | **Switch** |
| --- | --- | --- |
| 1. | The main objective of the router is to connect various networks simultaneously. | While the main objective of the switch is to connect various devices simultaneously. |
| 2. | It works in the network layer. | While it works in the data link layer. |
| 3. | A router is used by LAN as well as MAN. | While the switch is used by only LAN. |
| 4. | Through the router, data is sent in the form of a packet. | While through switch data is sent in the form of packet and frame. |
| 5. | There is less collision take place in the router. | While there is no collision taking place in the full-duplex switch. |
| 6. | The router is compatible with NAT. | While it is not compatible with NAT. |
| 7. | The types of routing are Adaptive and Non-adaptive routing. | The types of switching are Circuit, Packet, and Message Switching. |



**Chapter 4: INTERNET CONNECTIVITY**

**4.1. IP ADDRESSING**

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.

IP addresses are not random. They are mathematically produced and allocated by the [Internet Assigned Numbers Authority](https://www.iana.org/) (IANA), a division of the [Internet Corporation for Assigned Names and Numbers](https://www.icann.org/) (ICANN). ICANN is a non-profit organization that was established in the United States in 1998 to help maintain the security of the internet and allow it to be usable by all. Each time anyone registers a domain on the internet, they go through a domain name registrar, who pays a small fee to ICANN to register the domain.

**4.2. Classful addressing**

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

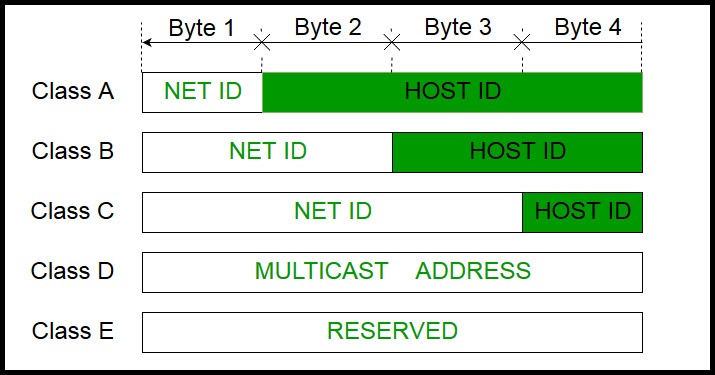
* Class A
* Class B
* Class C
* Class D
* Class E

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 an IP address to each device that is connected to its network.



**Class A:**

IP addresses 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 the 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 subtracted 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 is assigned to the networks that range 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 are used to determine the host in any network. The default subnet 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 addresses 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 is always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID are used to determine the host in any network. The default subnet 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 D:**

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

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

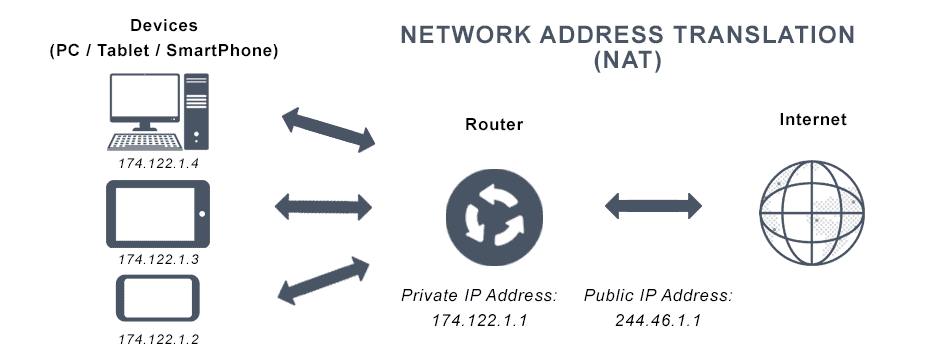
**Class E:**

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E range from 240.0.0.0 – 255.255.255.254. This class doesn’t have any subnet mask. The higher-order bits of the first octet of class E is always set to 1111.

## 4.3. NAT:

Network Address Translation (NAT) conserves IP addresses by enabling private IP networks using unregistered IP addresses to go online. Before NAT forwards packets between the networks it connects, it translates the private internal network addresses into legal, globally unique addresses.

NAT configurations can reveal just one IP address for an entire network to the outside world as part of this capability, effectively hiding the entire internal network and providing additional security. Network address translation is typically implemented in remote-access environments, as it offers the dual functions of address conservation and enhanced security.



**4.4. ACL:**

Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

1. The set of rules defined are matched serial wise i.e matching starts with the first line, then 2nd, then 3rd, and so on.
2. The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.
3. There is an implicit deny at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

**Types of ACL –**   
There are two main different types of Access-list namely:

1. **Standard Access-list –**   
   These are the Access-list that are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don’t distinguish between the IP traffic such as TCP, UDP, HTTPS, etc. By using numbers 1-99 or 1300-1999, the router will understand it as a standard ACL and the specified address as the source IP address.
2. **Extended Access-list –**   
   These are the ACL that uses source IP, Destination IP, source port, and Destination port. These types of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.

Also, there are two categories of access-list:

1. **Numbered access-list –** These are the access list that cannot be deleted specifically once created i.e if we want to remove any rule from an Access-list then this is not permitted in the case of the numbered access list. If we try to delete a rule from the access list then the whole access list will be deleted. The numbered access list can be used with both standard and extended access lists.
2. **Named access list –** In this type of access list, a name is assigned to identify an access list. It is allowed to delete a named access list, unlike numbered access list. Like numbered access lists, these can be used with both standards and extended access lists.

**4.5. DHCP:**

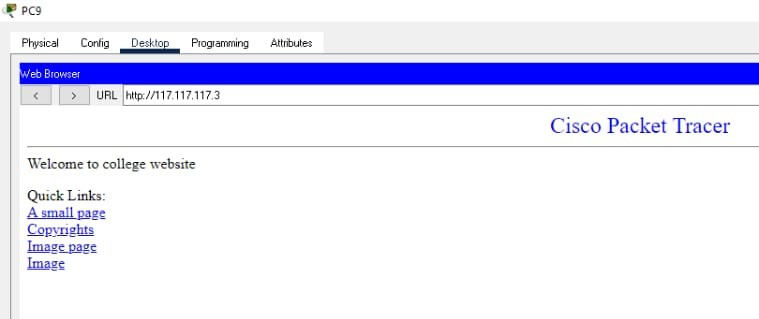
The **Dynamic Host Configuration Protocol** (**DHCP**) is a [network management protocol](https://en.wikipedia.org/wiki/Network_protocol) used on [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP) networks for automatically assigning [IP addresses](https://en.wikipedia.org/wiki/IP_address) and other communication parameters to devices connected to the network using a [client-server](https://en.wikipedia.org/wiki/Client%E2%80%93server) architecture.[[1]](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#cite_note-TechTarget-1)

The technology eliminates the need for individually configuring network devices manually, and consists of two network components, a centrally installed network DHCP [server](https://en.wikipedia.org/wiki/Server_(computing)) and client instances of the protocol [stack](https://en.wikipedia.org/wiki/Stack_(abstract_data_type)) on each computer or device. When connected to the network, and periodically thereafter, a client [requests](https://en.wikipedia.org/wiki/Request%E2%80%93response) a set of parameters from the DHCP server using the DHCP protocol.

DHCP can be implemented on networks ranging in size from [residential networks](https://en.wikipedia.org/wiki/Home_network) to large [campus networks](https://en.wikipedia.org/wiki/Campus_network) and regional ISP networks.[[2]](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#cite_note-2) Many [routers](https://en.wikipedia.org/wiki/Router_(computing)) and [residential gateways](https://en.wikipedia.org/wiki/Residential_gateway) have DHCP server capability. Most residential network routers receive a [unique](https://en.wikipedia.org/wiki/Universally_unique_identifier) IP address within the ISP network. Within a local network, a DHCP server assigns a local IP address to each device.

DHCP services exist for networks running [Internet Protocol version 4](https://en.wikipedia.org/wiki/IPv4) (IPv4), as well as version 6 ([IPv6](https://en.wikipedia.org/wiki/IPv6)). The IPv6 version of the DHCP protocol is commonly called [DHCPv6](https://en.wikipedia.org/wiki/DHCPv6).

**COLLEGE WEBSITE**



## 4.6. What is DNS?

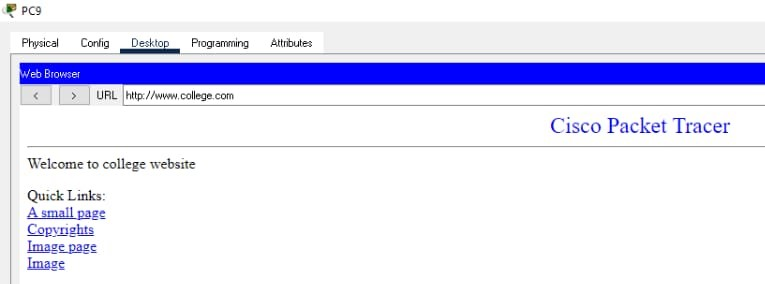
The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through [domain names](https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/), like nytimes.com or espn.com. Web browsers interact through [Internet Protocol (IP)](https://www.cloudflare.com/learning/network-layer/internet-protocol/) addresses. DNS translates domain names to [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/) so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address that other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

**How does DNS work?**

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.

To understand the process behind the DNS resolution, it’s important to learn about the different hardware components a DNS query must pass between. For the web browser, the DNS lookup occurs "behind the scenes" and requires no interaction from the user’s computer apart from the initial request.



COLLEGE WEBSITE USING DNS

**Chapter 5: Conclusion**

The Future of Virtual Local Area Network is wide open to companies that operate on a wide-scale to small Companies. The VLAN will help in the reduction of traffic, increase security, be cost-effective and make it easier for the IT department to manage better security and Management in the organization

During this internship, we learned about

* Different concepts like networks, types of networks, IP address, and internet connectivity.
* Implementation of a computer network using new software – cisco packet tracer.
* Advantages of VLAN over LAN

This was a great opportunity for us to get to know how an external organization works and the technologies being adopted.