**PROJECT REPORT**

**ON**

**NETWORK DESIGN FOR AL-KHIDMAT HOSPITAL TIMERGARA**

**BY**

**MUKARAM SHAH ROLL NO: 211**

**SESSION 2017-2021**

*Project report submitted to The University of Agriculture Peshawar in partial fulfillment of the requirements for the degree of*

**BACHELOR OF SCIENCE IN COMPUTER SCIENCE**



**SUPERVISED BY**

**MS. SANA SALAH UD DIN**

**INSTITUTE OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY**

**FACULTY OF MANAGEMENT AND COMPUTER SCIENCES**

**THE UNIVERSITY OF AGRICULTURE, PESHAWAR**

**KHYBER PAKHTUNKHWA**

**JULY, 2021**

**PROJECT REPORT**

**ON**

**NETWORK DESIGN FOR AL-KHIDMAT HOSPITAL TIMERGARA**

**BY**

**MUKARAM SHAH ROLL NO: 211**

**SESSION 2017-2021**

*Project report submitted to The University of Agriculture Peshawar in partial fulfillment of the requirements for the degree of*

**BACHELOR OF SCIENCE IN COMPUTER SCIENCE**

**Approved by:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Advisor

|  |
| --- |
| Ms. Sana Salah ud Din |
| Lecturer ICS/IT |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mr. Arshad Iqbal Member

Lecturer of ICS/IT

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mr. Said Ul Abrar Member

Lecturer of ICS/IT

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dr. Asfandyar Khan HOD, ICS/IT

Assistant Professor

**INSTITUTE OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY**

**FACULTY OF MANAGEMENT AND COMPUTER SCIENCES**

**THE UNIVERSITY OF AGRICULTURE, PESHAWAR**

**KHYBER PAKHTUNKHWA**

**JULY, 2021**

**ACKNOWLEDGEMENT**

Praise be to Almighty Allah the cherisher and sustainer of the world and the Holy Prophet Muhammad (may Allah’s blessings and peace be upon him) the Final Messenger sent by Allah to the Inhabitants of Earth.

We wish to express our deepest gratitude and profound regard to our honorable and great supervisor, Miss. Sana Salah Un Din**,** Lecturer ICS/IT Institute of Computer Sciences and Information Faculty of Management and Computer Sciences, The University of Agriculture, Peshawar for her encouragement helpful suggestions and guidance during our project. Her critical insight, consistent advice, constructive criticism, personal and supervision, generated the vigor in us to complete this project.

Finally, we would like to extend thanks to all our family particularly parents for their sacrifices, understandings and being constant source of prayers and inspiration which enabled us to complete our Project work successfully.

***Mukaram shah***

**TABLE OF CONTENTS**

**Chapter No. Title Page No.**

[**CHAPTER-1** 1](#_Toc77004805)

[**INTRODUCTION** 1](#_Toc77004806)

[**1.1 OVERVIEW** 1](#_Toc77004807)

[**1.2 VLAN** 2](#_Toc77004808)

[**1.3 INTER VLAN ROUTING** 2](#_Toc77004809)

[**1.3.1 ROUTER ON A STICK** 3](#_Toc77004810)

[**1.3.2 MLS (MULTI-LAYER SWITHCH)** 3](#_Toc77004811)

[**1.4 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)** 3](#_Toc77004812)

[**1.5 TRUNK** 3](#_Toc77004813)

[**1.6 PORT SECURITY** 3](#_Toc77004814)

[**1.7 SECURE SHELL PROTOCOL (SSH)** 4](#_Toc77004815)

[**1.8 WIFI** 4](#_Toc77004816)

[**1.9 OBJECTIVES** 4](#_Toc77004817)

[**CHAPTER-2** 5](#_Toc77004818)

[**LITERATURE REVIEW** 5](#_Toc77004819)

[**2.1 OVERVIEW** 5](#_Toc77004820)

[**CHAPTER-3** 8](#_Toc77004821)

[**COMPUTER NETWORK AND NETWORK DEVICES** 8](#_Toc77004822)

[**3.1 NETWORK** 8](#_Toc77004823)

[**3.1.1 NETWORKING** 8](#_Toc77004824)

[**3.1.2 TYPES OF NETWORK** 8](#_Toc77004825)

[**I.** **SERVER BASED NETWORK** 8](#_Toc77004826)

[**II. PEER-TO- PEER NETWORK** 9](#_Toc77004827)

[**3.2 CATEGORIES OF NETWORK** 9](#_Toc77004828)

[**3.2.1 PERSONAL AREA NETWORK (PAN)** 9](#_Toc77004829)

[**3.2.2 LOCAL AREA NETWORK (LAN)** 10](#_Toc77004830)

[**3.2.3 WIDE AREA NETWORK (WAN)** 11](#_Toc77004831)

[**3.2.4 METROPOLITAN AREA NETWORK (MAN)** 12](#_Toc77004832)

[**3.3 NOTWORK DEVICES** 13](#_Toc77004833)

[**3.3.1 NIC (NETWORK INTERFACE CONTROLLER)** 13](#_Toc77004834)

[**3.3.2 SWITCH** 14](#_Toc77004835)

[**3.3.3 ROUTER** 15](#_Toc77004836)

[**3.3.4 GATEWAY** 16](#_Toc77004837)

[**3.3.5 ROUTER** 16](#_Toc77004838)

[**3.3.6 WIRELESS ACCESS POINT** 16](#_Toc77004839)

[**CHAPTER-4** 17](#_Toc77004840)

[**CONCEPTUAL STUDY OF VLAN** 17](#_Toc77004841)

[**4.1 VIRTUAL LOCAL AREA NETWORK (VLAN)** 17](#_Toc77004842)

[**4.2 PURPOSE OF VLAN** 18](#_Toc77004843)

[**4.3 BASIC PURPOSE** 19](#_Toc77004844)

[**4.4 SUPPORTED VLAN** 20](#_Toc77004845)

[**4.5 NORMAL VLAN RANGE** 20](#_Toc77004846)

[**4.6 EXTENDED VLAN RANGE** 20](#_Toc77004847)

[**4.7 HOW VLAN WORK** 21](#_Toc77004848)

[**CHAPTER-5** 22](#_Toc77004849)

[**INTER VLAN ROUTING** 22](#_Toc77004850)

[**5.1 INTRODUCTION TO INTER-VLAN ROUTING** 22](#_Toc77004851)

[**5.1.1 DEFINITION** 22](#_Toc77004852)

[**5.2 TRADITIONAL INTER-VLAN ROUTING** 23](#_Toc77004853)

[**5.3 ROUTER-ON-A-STICK** 24](#_Toc77004854)

[**5.4 SWITCH VIRTUAL INTERFACE ON MLS** 25](#_Toc77004855)

[**5.5** **ENCAPSULATION 802.1Q** 25](#_Toc77004856)

[**CHAPTER 6** 26](#_Toc77004857)

[**CONFIGURATION AND IMPLANTATION** 26](#_Toc77004858)

[**6.1. NETWORK TOPOLOGY DIAGRAM** 26](#_Toc77004859)

[**6.2 ROUTER SVI INTERFACE CONFIGURATIONS** 26](#_Toc77004860)

[**6.2.1 PRIVATE WARD SVI CONFIGURATION** 26](#_Toc77004861)

[**6.2.2 GENERAL WARD SVI CONFIGURATION** 27](#_Toc77004862)

[**6.2.3 CLINICAL WARD SVI CONFIGURATION** 27](#_Toc77004863)

[**6.2.4 ENTRANCE RECEPTION SVI CONFIGURATION** 27](#_Toc77004864)

[**6.2.5 IT DEPARTMENT INTERFACE CONFIGURATION** 28](#_Toc77004865)

[**6.3 VLAN CONFIGURATION** 29](#_Toc77004866)

[**6.3.1 VLAN CONFIGURATION** 29](#_Toc77004867)

[**6.4 DHCP POOL CONFIGURATION FOR VLANS** 30](#_Toc77004868)

[**6.4.1 PRIVATE WARD DHCP CONFIGURATION** 30](#_Toc77004869)

[**6.4.2 GENERAL WARD DHCP CONFIGURATION** 30](#_Toc77004870)

[**6.4.3** **CLINICAL WARD DHCP CONFIGURATION** 31](#_Toc77004871)

[**6.4.4 ENTRANCE RECEPTION DHCP CONFIGURATION** 31](#_Toc77004872)

[**6.4.5 IT DEPARTMENT DHCP CONFIGURATION** 31](#_Toc77004873)

[**6.5 SSH CONFIGURATION** 33](#_Toc77004874)

[**6.5.1 SSH CONFIGURATION ON MAIN ROUTER** 33](#_Toc77004875)

[**6.5.2 SSH CONFIGURATION ON SWITCH A** 33](#_Toc77004876)

[**6.5.3 SSH CONFIGURATION ON SWITCH B** 34](#_Toc77004877)

[**6.5.4 SSH CONFIGURATION ON SWITCH C** 35](#_Toc77004878)

[**6.5.5 ACCESSING SW-C THROUGH SSH FROM SW-A LAN** 36](#_Toc77004879)

[**6.6 PORT ASSIGNMENT CONFIGURATION** 37](#_Toc77004880)

[**6.6.1 SWITCH-2** 37](#_Toc77004881)

[**6.6.2 SWITCH-3** 39](#_Toc77004882)

[**6.7 PORT SECURITY CONFIGURATION** 40](#_Toc77004883)

[**6.7.1 PORT SECURITY CONFIGURATION ON SWITCH 1** 40](#_Toc77004884)

[**6.7.2 PORT SECURITY CONFIGURATION ON SWITCH 2** 42](#_Toc77004885)

[**6.7.3 PORT SECURITY CONFIGURATION ON SWITCH 3** 45](#_Toc77004886)

[**CHAPTER-7** 48](#_Toc77004887)

[**SUMMARY AND CONCLUSION** 48](#_Toc77004888)

[**7.1 SUMMARY** 48](#_Toc77004889)

[**7.2 CONCLUSION** 49](#_Toc77004890)

[**7.3 FUTURE WORK** 49](#_Toc77004891)

[**REFERENCES** 50](#_Toc77004892)

**LIST OF FIGURES**

**Figure No. Description Page No.**

[Figure 3.1 Server Based Network 8](#_Toc76074309)

[Figure 3.2 P2P Network workgroup 9](#_Toc76074310)

[Figure 3.3 Local Area Network (LAN) 10](#_Toc76074311)

[Figure 3.4 Wide Area Network 11](#_Toc76074312)

[Figure 3.5 Metropolitan Area Network (MAN) 12](#_Toc76074313)

[Figure 3.6 Network Interface Controller 13](#_Toc76074314)

[Figure 3.7 Layer 1 HUB 14](#_Toc76074315)

[Figure 3.8 Layer 3 Switch 15](#_Toc76074316)

[Figure 3.9 Cisco Router 15](#_Toc76074317)

[Figure 3.10 Wireless Access Point 16](#_Toc76074318)

[Figure 4.1 VLAN 17](#_Toc76074319)

[Figure 4.2 Different VLANs Works 21](#_Toc76074320)

[Figure 5.1 Traditional inter-vlan routing 23](#_Toc76074321)

[Figure 6.1 Network topology 26](#_Toc76074322)

[Figure 6.2 Router routing Table 28](#_Toc76074323)

[Figure 6.3 Vlan Database of switch-2 29](#_Toc76074324)

[Figure 6.4 Vlan Database of switch-3 30](#_Toc76074325)

[Figure 6.5 Dhcp Database on Router 32](#_Toc76074326)

[Figure 6.6 OT PC belongs to vlan 22 32](#_Toc76074327)

[Figure 6.7 SSH Access from command prompt 37](#_Toc76074328)

[Figure 6.8 switch-1 data base of port security 41](#_Toc76074329)

[Figure 6.9 switch-2 Database of port security 44](#_Toc76074330)

[Figure 6.10 switch-3 data base of port security 47](#_Toc76074331)

# **CHAPTER-1**

# **INTRODUCTION**

## **1.1 OVERVIEW**

In contrast to the network of yesterday that were based on collapsed backbones. Today network design is characterized by a flatter architecture. In LAN communication take place on the basis on the basis of mac addresses, which learned by address resolution protocol for these purpose every device broadcast first in whole network. This processes make the whole network slow. The best solution for these problems is VLAN. VLAN divide the actual broadcast domain into small logical domain. It actually a logically grouping of network users and resources connected to administratively defined ports on a switch. Implementation and configuration of vlan make possible to reduce the broadcast, that concern and specific group nodes broadcast restrict to its own VLAN. Host in same vlan can communicate freely, but the communication of different VLAN hosts requires a layer 3 device. Different VLANs host can communicate with the technique called inter-vlan routing, inter-vlan routing can be achieved with help of router on a stick and switch virtual interface methodologies. In our project we will describe, implement and configure VLAN and inter-vlan routing.

In which we the hospital network in different wards. Every wards has its own VLAN. After their proper logical grouping we will intercommunicate all wards with the help of router on a stick. In fact, communication between different machines on a local area network is governed by the physical architecture. Using virtual networks (VLANs) it is possible to be free of the limitations of the physical Segmentation based on a grouping together of machines using criteria (mac addresses, port numbers, protocol, etc.). Many architectures use virtual LANs, on their switches, to separate subnets from each other on the same network infrastructure. It is commonly assumed that virtual LNAs are fully isolated from each other. During the black-hat conference 2002, a presentation from Sean Connery (CISCO) demonstrated ways of sending packets across VLANs.

The reason that this is possible is apparently that vlans were not designed for security but are used to enforce it. It is up to the administrator to ensure that the infrastructure cannot be easily abused to compromise the network or data within. As it seems possible to send packets across VLANs. The origin of this technology or how it evolved is somewhat vague. According to Some network specialists, the idea came mostly from network hardware manufactures. Supposedly, it was inspired by the growing implementation of LAN technology in computing Environments and was seen as a way to extend the influence their devices had on these networks.

The adoption of new VLAN-based technology allegedly attempts to retain core Ethernet features while attempting to anticipate future growths in multipoint networks applications like gaming, Private LANs and others.

From an end user point of view, the introduction and implementation vlan technology in General is a welcome improvement to legacy networks protocols. Considering that in older Network environments, the use of geographical locations substantially limited the distance in Type of topologies that can be implemented.

## **1.2 VLAN**

A virtual local area network (VLAN) is a logical group of workstations, servers and network Devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to changes in network requirements and relocation of workstations and server nodes. Higher-end switches allow the functionality and implementation of VLANS. The purpose of Implementing a VLAN is to improve the performance of a network or apply appropriate security Features.

## **1.3 INTER VLAN ROUTING**

Inter vlan routing can be refer as a path to forward traffic different vlan by Implementing a router in the network. The user devices in the VLANs forward traffic to the router then router forwards the traffic to the destination network of the vlan configured on the switch. Inter vlan routing done with two techniques.

## **1.3.1 ROUTER ON A STICK**

Router-on-a-stick is the method in which different VLANs communicate each other in which one physical interface divided into sub interface. Each Vlan is assigned to separate sub-interface each sub-interface is configured as trunk link.

## **1.3.2 MLS (MULTI-LAYER SWITHCH)**

Multi-layer switch is also known is Layer 3 switch. It is also used for forwarding traffic between different Vlan. In MLS we make SVI to each Vlan and assign IP address to each SVI.

## **1.4 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)**

Dynamic Host Configuration Protocol (DHCP) is a networking protocol that you commonly use every day on almost all of your devices. If you don't have to set a static IP address for your devices, odds are they are set with DHCP, DHCP is not just for IP address, subnet mask, and Gateway, however. DHCP provides information you typically don't look at, for example: NTP servers, DNS servers, FTP and configuration servers for devices such as desk phones, and many other services that can be set using custom option sets.

## **1.5 TRUNK**

A trunk port is a port that is assigned to carry traffic for all the VLANs that are accessible by a

Specific switch, a process known as trunking. Trunk ports mark frames with unique identifying

Tags - either 802.10 tags or Inter Switch Link (ISL) tags as they move between switches Therefore, every single frame can be directed to its designated VLAN.

## **1.6 PORT SECURITY**

It is also called L-2 security because L-2 security using Mac-address. It is used to control users on network. If we want to particular end device connect to particular switch port. When we apply port security on switch port by giving Mac-address of end device, so then only this device connect to this switch port.

## **1.7 SECURE Shell Protocol (SSH)**

The Secure Shell Protocol is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH.

## **1.8 WIFI**

Wi-Fi is the name of a wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections.

## **1.9 OBJECTIVES**

The main objectives and purpose of our work is to provide the basic of LAN Switching. Minimizing the irrelevant broadcast, Our Study is based on to achieve the basic, implementation, configuring and troubleshooting of the following technique and terminologies

1. Perform basic configuration tasks on a switch. Traffic flow in LAN environment.
2. Understanding the basic of VLANs.
3. Assignment of specific device to a particular VLAN.
4. How trunk work
5. Implementation Secure Shell Protocol SSH
6. Provide secure Network

# **CHAPTER-2**

# **LITERATURE REVIEW**

## **2.1 OVERVIEW**

A comprehensive discussion of LAN Switching is beyond the scope of this work However, Derfler and Freed (1096) usefully define many of the terms used in discussing networks. "A local area network (LAN) is -1 group of computers typically connected by no more than 1,000 feet of cable, which interoperate and allow people to share resources. A NIC (or LAN adapter) is the device which packages data for transmission and acts as a gatekeeper to control access to the shared network cable. Network interface cards break data streams into packets, which are reassembled at the destination. Bridges segment LANs or join LANs together: they act lo control traffic by learning the station address of each machine on the networks in question, and only send a packet across the bridge if the destination of the packet is a station on the other side.

Routers function similarly to bridges, but look at the network address of packets and use different routing protocols to send the packet to its destination efficiently". Henry and De Libero (1996) describe the use of switching to divide the network into smaller segments, switching helps to reduce the number of nodes trying to use the same network segment, resulting in lower congestion on each segment". In switched hubs or bridges, each node can have its own network segment, and therefore have access to all of the network bandwidth of the segment. Switching bridges can look deep into a packet and use protocol information and the like to provide a level of filtering and prioritization". (Henry and De Libero, 1996).

"The evolution of the local area network (LAN) has followed a logical progression of improvements to tackle one problem at a time. LAN switches have essentially replaced repeating hubs in business environments". Conceptual software driven special application of LAN switches, called Virtual LANS (VLANs), was introduced in the mid-nineties with a lot of hype. They promised cost effective router-like benefits with the added advantage of reduced system administration costs. As we approached and then entered into the 21st century, other technological advances challenged the VLAN, and ultimately displaced it. This paper builds the case for VLANs and then examines some of these alternate technologies. Since VLAN technology is relatively new, and is different from vendor lo vendor, it is not surprising that there is sparse mention of the technology in the literature. Virtual local area networks address and attempt to solve many of the issues and problems facing network administrators, particularly on large, enterprise-wide networks. Some common issues include network utilization, particularly collisions and broadcasts, and network security. In addition, administrators want to reduce the amount of time and resources required to perform -moves, adds, and changes to the workstations on a network; such activities often take up a disproportionate amount of an administrator's time and resources. VLANs offer additional advantages besides breaking up the broadcast domain. One widely touted advantage is simplified stem administration functions, particularly related to office moves and employee relocations.

Layer 2 switch linked to router via trunk. Router interface, typically Fast Ethernet, subdivided into logical sub interfaces, one per VLAN. If a switch supports multiple VLANs but has no Layer 3 capability to route packets between those VLANs, the switch must be connected to a device external to the switch that possesses this capability. This setup is not a high performance solution but it is quite simple. It just needs a single trunk link between the switch and the router. This single physical link should be Fast Ethernet or greater, although 802.1Q is supported on some 10-Mb Ethernet interfaces. The figure shows a configuration where the router is connected to a core switch using a single 802.1Q trunk link. This configuration is commonly referred to as router-on-a-stick. The router can receive packets on one VLAN, for example on VLAN 10, and forward them to another VLAN, for example on VLAN 20.

To support 802.1Q trunking, subdivide the physical router interface into multiple, logical, addressable interfaces, one per VLAN. The resulting logical interfaces are called sub interfaces. Assume that client PC-1 needs to send traffic to server PC-2. Because the hosts are on different VLANs, transferring this traffic requires a Layer 3 device. In this example, an external router connects to the switch via an Q trunk—a router-on-a-stick. The frame is transmitted by the source device and enters the switch where it is associated with a specific VLAN.

The switch determines (from the destination MAC address) that the frame must be forwarded across a trunk link. It adds an 802.1Q tag to the frame header and forwards to the router. Based on the 802.1Q tag received, the router accepts the packets from VLAN10 on its sub interface in that VLAN. The router performs Layer 3 processing based on the destination network address. Because the destination network is associated with a VLAN accessed over the trunk link, the router adds the appropriate 802.1Q tag to the frame header. The router then routes the packet out the appropriate sub interface on VLAN20.The switch removes the 802.1Q tag from the frame. The switch determines from the destination MAC address that the frame will be transmitted through an access mode port in VLAN 20, so the frame is transmitted as an untagged Ethernet frame. External Router: Advantages and Disadvantages every method of inter-VLAN routing has it advantages and disadvantages. The following are the advantage of the router-on-a-stick method: It works with any switch that supports VLANs and trunking because Layer 3 services are not required on the switch. Many switches do not contain Layer 3 forwarding capability, especially switches used at the access layer of a hierarchical network. If using Local VLANs, mostly none of the switches at the access layer have Layer 3 forwarding capability.

Depending on the network design, it might be possible to have no Layer 3-capable switches at all. The implementation is simple. Only one switch port and one router interface require configuration. If the switch enables all VLANs to cross the trunk (the default), it literally takes only a few commands to configure the switch. The router provides communication between VLANs. If the network design includes only Layer 2 switches, this makes the design and troubleshooting traffic flow simply because only one place in the network exists where VLANs inter-connect.

The following are some of the disadvantages of using the external router for inter-VLAN routing: The router is a single point of failure. A single traffic path may become congested. With a router-on-a-stick model, the trunk link is limited by the speed of the router interface shared across all trunked VLANs. Depending on the size of the network, the amount of inter-VLAN traffic, and the speed of the router interface, congestion could result with this design. Latency might be higher as frames leave and re-enter the switch chassis multiple times and the router makes software-based routing decisions. Latency increases any time traffic must flow between devices. Additionally, routers make routing decisions in software, which always incurs a greater latency penalty than switching with hardware.

# **CHAPTER-3**

# **COMPUTER NETWORK AND NETWORK DEVICES**

## **3.1 NETWORK**

Network is a set of devices connected by communication links. A node can be a computer, printer, or any other device capable of sending and or receiving data. A group of computer and other devices join together through some transmission medium is called computer network.

## **3.1.1 Networking**

The concept of connected computer sharing resources is called networking. Computer network that is part of network can share the following, data, messages, graphics, printers modem, fax machines and other hardware resources.

## **3.1.2 Types of Network**

There are two main types of the network

### **Server Based Network**

A Server-based network is a network in which network security and storage are maintain with one or more servers centrally. In this type of network special computers called servers, handle network tasks such as user authentication, storing data, managing printers, and running applications such as database and e-mail programs.

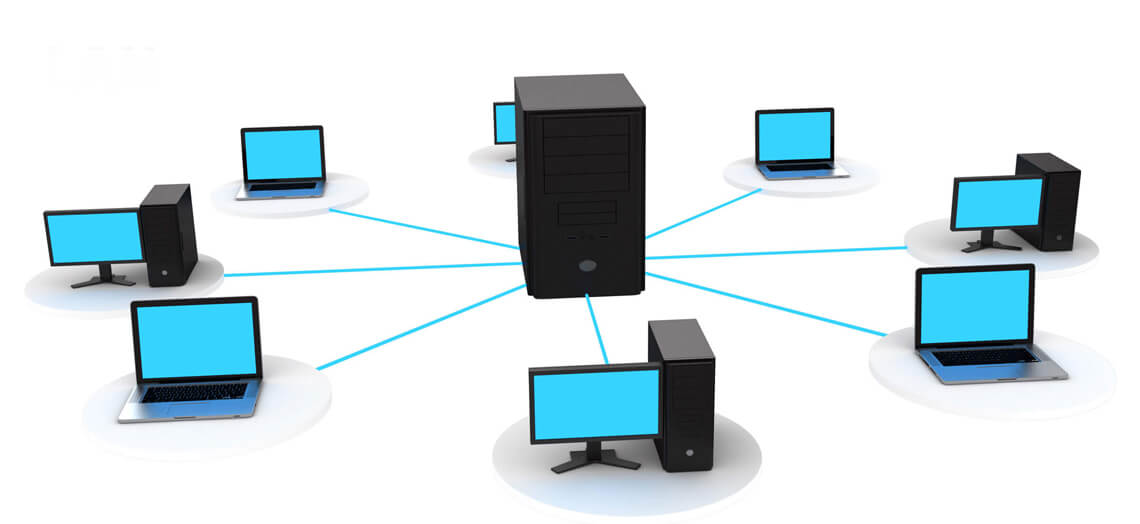


Figure 3.1 Server Based Network

### **ii. Peer-to- peer Network**

Also called P2P Network." In a P2P network, the "peers" are computers which are connected to

Each other through the wire/internet. Files can be shared directly between systems on the network without the central servers to be needed. In other words, each computer on a P2P network becomes a file server as well as a client.

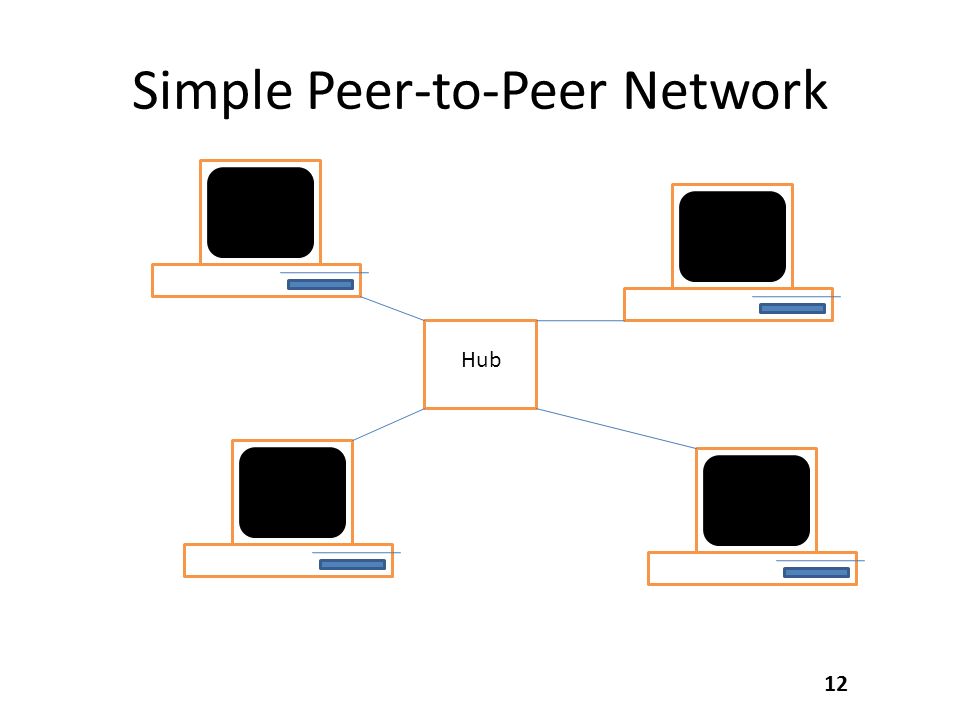


Figure 3.2 P2P Network workgroup

## **3.2 CATEGORIES OF NETWORK**

Today when we speak we are generally referring the three types of network,

## **3.2.1 PERSONAL AREA NETWORK (PAN)**

A personal area network is a technology that could enable wearable computer devices to communicate with other nearby computers, PAN is a computer network that is configured around a person within a single building. This may be in a small office or residence. A typical PAN includes one or more computers, phones, peripherals, video game console, and other personal entertainment devices. When more people use the same network within their home, sometimes the network is defined as a home network or HAN. In a very typically configuration, the residence has a single wired Internet connection connected to the modem. Therefore, this modem provides wired and wireless connectivity for multiple devices. A network is usually managed as a single computer, but it can be accessed from any device.

1. Send documents upstairs to your office printer while sitting on the couch with your

Laptop. Upload photos from your phone to your desktop computer.

1. Watch movies on TV from online streaming services.

## **3.2.2 LOCAL AREA NETWORK (LAN)**

According to local or LAN network consists of a computer network at a single site and is typically a single office building LANs are very useful for resource sharing such as data storage and printers. LANs can be built with relatively inexpensive hardware such as hubs. Network adapters, and Ethernet cables.

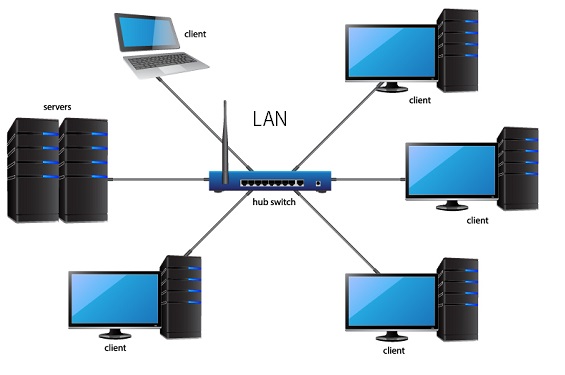


Figure 3.3 Local Area Network (LAN)

The smaller LAN can only be used by few devices, but a large LAN can accommodate thousands of computers. LANs typically use wired connections to improve speed und security, but wireless connections can also be part of a LAN. Define the features of the high speed LAN and relatively low costs.

LANs are typically used in a single site where people have to share resources unlike the outside world. Imagine an office building where everyone should be able to access tiles on a central server or printer documents to one or more central printer. This task can be performed by easily to anyone who work in the same office. But you probably do not want someone coming out of the office to send documents from your phone to the printer. If your local area network (LAN), is completely wireless, your network is called local wireless network (WLAN). Most LANS connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to wocess data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending email or engaging in chat sessions,

LANs are capable of transmitting data at very fast rates, much faster than data can be transmitted

Over a telephone line; but the distances are limited and there is also a limit on the number of computers that can be attached to a single LAN.

## **3.2.3 WIDE AREA NETWORK (WAN)**

A geographic network WAN is communications network. A large network area is simply a LAN or a LAN in a network WAN network connect to the LAN on the other side of the building to the world or the world. WANs features slow data rates and longer distances.

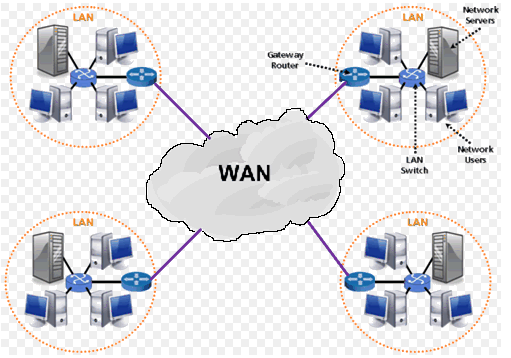


Figure 3.4 Wide Area Network

Computers connected to a geographic networks or often connected through a public network. Such as a telephone system. You can also connect via a dedicated line or satellite. The largest existing WAN is the internet. Some internet segments. Such VPN base, extranet, or themselves WANs. Finally, many WANs are companies or research networks that used leased lines. Numerous WANs have been implemented, including public packet networks, larger corporate networks, military networks, banking networks, mobile brokerage networks and aviation reservation networks.

An organization that support WAN using internet protocol is called network service provider (NSP). These form the core of the internet. Connecting a WAN NSP using in internet packet switched linked (also known as a "peering point") form a global communication infrastructure. When network (geographic network) typically used different network equipment in are much more expensive than local networks. Common technologies commonly found in wide area network (WAN) include SONET, Frame relay, and ATM.

## **3.2.4 METROPOLITAN AREA NETWORK (MAN)**

MAN stand for metropolitan area network and is one of many type of network. People are relatively new kind of network. MAN is bigger than the local network and as the name implies, it covers the area of single city, MAN does not extend beyond nearly 100 kilometres and often includes a combination of different hardware and transmission media. It can be a single network, such as a cable TV network, or you can connect multiple LANs to a larger network to share resources from LAN to LAN and from device to device.

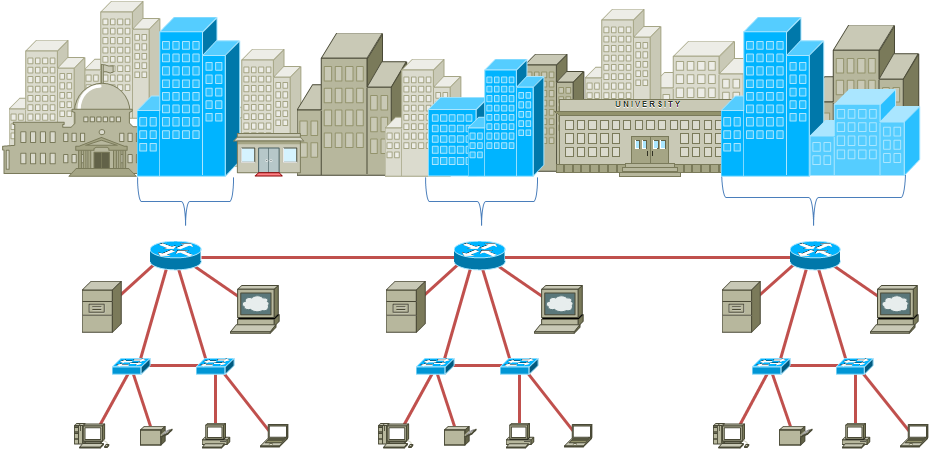


Figure 3.5 Metropolitan Area Network (MAN)

A MAN can be a single network it covers the whole city or several LANs group. This way, resources can be share from LAN to LAN and from computer to computer, MAN is typically on by large company to interconnect various point through the city.

MAN two most important components are safety and standardization Security is the important because information is share between different systems. Standardization is needed to insure reliable data communication. Typically, MAN used large backbone technologies such as fiber optics links, to connect inter multiple local network and provide uplink servers for geographic and internet networks.

## **3.3 NOTWORK DEVICES**

In network we have type of devices for reaching from one side into another side this are divided into another side parts which are discussed below A group of computer and other devices joint together through some transmission medium is called network. The concept of connected computer sharing resources is called Networking. Computer Network that is a part of network can share the following

• Data

• Message

• Graphics

• Printer

• Modem, fax and other hardware resources

## **3.3.1 NIC (Network Interface Controller)**

This device is used to provide interface between system and network. It also provides the MAC address (Media Access Control) which is unique. It can be found 100mpbs up to 100mbps in markets. There are 3 types of addresses the name address, the logical address and the MAC address. The software which converts or translate the name add to logical/IP add is known as DNS (Domain Name System) and the software which is used to convert or translate the logical/IP add to MAC add is known as ARP (Address Resolution Protocol). It connects our PC to the network via Twisted Pair Cable having RJ-45 connector.

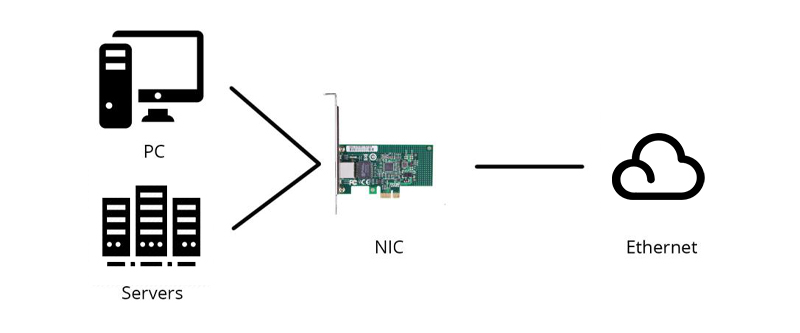


Figure 3.6 Network Interface Controller

## **3.3.2 Switch**

It is an electronic network device which is used to connecting two or more hosts which change data packets between thein. Switch is categorized into 4 types of switches technology. They are called Layer 1, Layer 2. Layer 3 and Layer 4.

1. **Layer 1**

Layer 1 switch is called HUB (Hybrid Universal Broadcast). It is a non-intelligent device because it has no capability of remembering wildernesses. Layer I switch is also called broadcast device because it copies the frame and then distributes it to all connected devices.

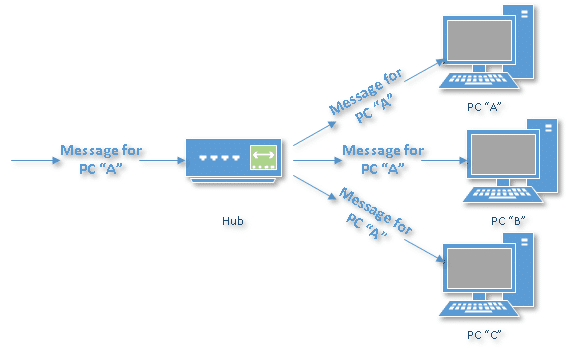


Figure 3.7 Layer 1 HUB

Broadcast consumes bandwidth. It makes the network congested collision is the main problem of Layer 1.

1. **Layer 2**

It is an intelligent device which addresses. Intelligent is due to its processor. It has its own operating system and RAM. It understands the MAC addresses and also port security option is available in Layer 2. It can avoid collision but facing difficulties in stopping broadcasting. Three steps are involved in Layer 2.

• Learning

• Listening

• Filtering

• Forwarding

1. **Layer 3**

It can understand both MAC and IP. However its shape is same as Layer 2. It can make decision either on IP or on MAC. IP broadcast request is killed in Layer 3. Its cost is high as compare to Layer 2 and Layer 1.



Figure 3.8 Layer 3 Switch

1. **Layer 4**

It can understand MAC, IP and application more intelligently. Its decision and processing power is very well as compare to other layers.

## **3.3.3 Router**

A router is an electronic device that forwards data packets between network devices. A router is connected at least two or more networks, commonly two LANs or WANs or a LAN and its Internet Service Provider’s (ISP's) network. Routers are placed at gateways, the places where two or more networks connect.

1. Router attributes
2. Layer-3 device.
3. Can read IP and MAC address.
4. Build MAC Table and Routing table.
5. Breakup broadcast and collision domain.
6. Do Internetwork communication,
7. Packet switching/filtering,
8. Path selection



Figure 3.9 Cisco Router

## **3.3.4 Gateway**

A gateways as the name pests, is a passage to communicate two networks together that may work upon different networking models Gateway essentially work as the messenger agents that lake data from one system, interpret it, and toward to another system. Gateway are also called protocol translator and can work at any network layer. Gateways are generally more complex than router and switch.

## **3.3.5 Router**

Router is also called bridging router, it is a device which hybrid features of both bridge and router. It can work with at data link layer or either at network layer. Working as a router, it is enable of routing packets at different network and working as bridge, it is enable of filtering local area network traffic.

## **3.3.6 Wireless Access Point**

Wireless access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. The AP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself.



Figure 3.10 Wireless Access Point

# **CHAPTER-4**

# **CONCEPTUAL STUDY OF VLAN**

## **4.1 VIRTUAL LOCAL AREA NETWORK (VLAN)**

A VLAN is a switched network that is logically segmented by function, project team, or, application without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch module port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router, as shown below. Because a VLAN is considered a separate logical network, it contains its own bridge MIB information and support its own implementation of spanning tree.

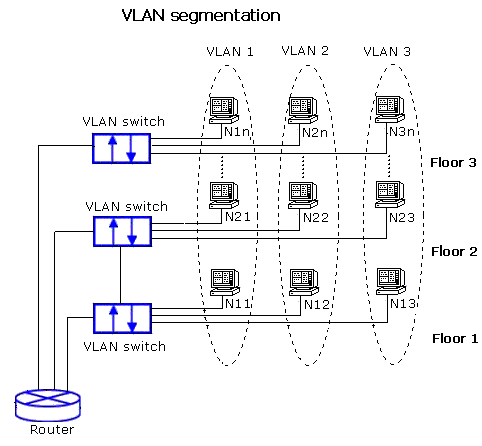


Figure 4.1 VLAN

VLANs are often associated with IP sub networks. For example, all the end stations in a particular IP subnet belong to the same VLAN, Interface VLAN membership on the switch module is assigned manually on an interface-by-interface basis. When you assign switch module prefaces to VLANs by using this method, it is known as interface-based.

## **4.2 PURPOSE OF VLAN**

Following point explain and make a good sense for the view understand the purpose of VLAN

1. A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible
2. Restrict to unauthorized user we create a VLAN suppose that u have3 Labe 11, 12, 13 and every Labe has50 pc mean total150 pc, if u want to no can access any data to our neighbour then we create3 different VLAN here nobody can access any other lab data without give trunk command
3. By default the only one VLAN in switch creating VLAN help us for differentiate the network and security for the users. We are made the VLAN for different wards to avoid conflict.
4. VLAN become great asset in providing security to our network plus saving lot of expenditure by providing virtual isolation in networks.
5. VLAN allows several networks to work virtually as a LAN. One of the most beneficial Elements of a VLAN is that it removes latency in the network, which saves network resources and increases network efficiency.
6. VLAN is a logically broadcast domain.by which we can assign multiple broadcast Domain in single switch means multiple network is running on single switch.
7. When we assign a switch-port in single VLAN that port is known as access Assign multiple VLAN on single switch-port that port is known as trunk...
8. VLAN is logically dividing a switch into 2 or more subnet using VLAN we can connect Different subnets into a single switch and it act as2 secrete switch. So we can avoid Wastage of switch ports.
9. is simple just understood that VLAN is used to create multiple broadcast domain specially used on L2 switches, because if you keep your computers more than 500 in one broadcast domain the performance will be worst every time when any broadcast packets arrive on the switch it will float to all the computers on the same network broadcast domain network so it will be much better if you create multiple broadcast domain and put them each on different network segment and use router to communicate each other. Broadcast packet will not reach to other VLAN (broadcast domain.

## **4.3 BASIC PURPOSE**

Following are the basic purpose for which we used the VLAN option in network

1. Security - Security is an important function of VLANs. A VLAN will separate data that could sensitive from the general network. Thus allowing sensitive or confidential data to traverse the network decreasing the change that users will gain access to data that they are not authorized to see. Example: An HR Dept.'s computers/nodes can be placed in one VLAN and an Accounting Dept.'s can be place in another allowing this traffic to completely separate. This same principle can be applied to protocol such as NFS, CIFS, replication, VMware (Motion) and management.
2. Cost - Cost savings can be seen by eliminating the need for additional expensive network equipment. VLANs will also allow the network to work more efficiently and command better use of bandwidth and resources.
3. Performance - Splitting up a switch into VLANs allows for multiple broadcast domains which reduces unnecessary traffic on the network and increases network performance.
4. Management: VLANs allow for flexibility with the current infrastructure and for simplified administration of multiple network segments within one switching environment,

## **4.4 SUPPORTED VLAN**

VLANs are identified with a number from 1 to 4094. VLAN IDs 5002 through 1005 are reserved for Token Ring and FDDI VIANS, VLAN IDs greater than 1005 are extended-range VLANs and are not stored in the VLAN database.

Although the switch module supports a total of 1005 (normal-range and extended-range) VLANS, the number of routed ports, SVIs, and other configured features affects the use of the switch module hardware.

The switch module supports per-VLAN spanning-tree plus (PVST+) or rapid PVST+ with a maximum of 128 spanning-tree instances. One spanning-tree instance is allowed per VLAN.

## **4.5 NORMAL VLAN RANGE**

Normal-range VLANs arc VLANs with VLAN IDs 1 to 1005. You can add, modify or

Remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to

1005 are automatically created and cannot be removed.)

Configurations for VLAN IDs 1 to 1005 are written to the file VLAN.dat (VLAN database), and

You can display them by entering the show VLAN privileged EXEC command. The VLAN.dat file is stored in flash memory,

You can set the parameters when you create a new normal-range VLAN or modify an existing

VLAN in the VLAN database:

1. VLAN ID
2. VLAN name
3. VLAN type (Ethernet, Fiber Distributed Data Interface (FDDI], FDDI network entity title [NET], TrBRF, or TrCRF, Token Ring, Token Ring-Net)

## **4.6 EXTENDED VLAN RANGE**

You can create extended-range VLANs (in the range 1006 to 4094) providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any switch port commands that allow VLAN IDs. Extended-range VLAN configurations are not stored in the VLAN database, but they are stored in the switch.

Module running configuration file, and you can save the configuration in the start-up figuration file by using the copy running-configuration start up-configuration privileged EXEC command

## **4.7 HOW VLAN WORK**

VLAN is a set of set stations and the switch ports that connect them. You can have different reasons for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Adding virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast. Like a router, it partitions the network Intel logical segments, which provides better administration, security, and management of multicast traffic.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station might omit the tag, or the

VLAN portion of the tag, in which case the first switch port to receive the packet can either

Reject it or insert a tag using its default VLAN ID. A given port can handle traffic for more than

De VLAN, but it can support only one default VLAN ID.

The Private Edge VLAN feature lets you set protection between ports located on the switch. This means that a protected port cannot forward traffic to another protected port on the same switch. The feature does not provide protection between ports located on different switches.

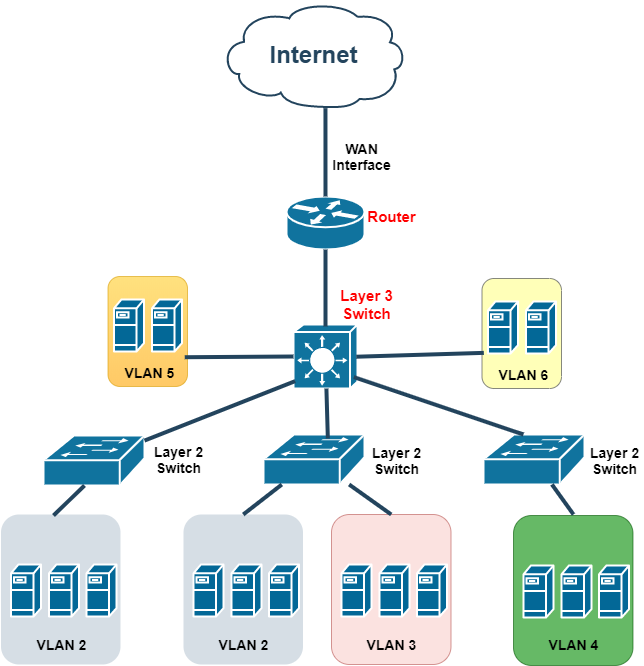


Figure 4.2 Different VLANs Works

# **CHAPTER-5**

# **INTER VLAN ROUTING**

## **5.1 INTRODUCTION TO INTER-VLAN ROUTING**

When we learnt about VLANs, we said that each VLAN is usually on its own subnet, switches mainly operate at layer 2 of the osi model and therefore they do not examine the logical addresses. Therefore, user nodes located on different VLANs cannot communicate by default. In many cases, we may need connectivity between users located on different VLANs. The way this can be accomplished is through inter-VLAN routing. In this course, we will look at one type of inter-VLAN routing, which is through the use of a router.

## **5.1.1 DEFINITION**

Inter-VLAN routing can be defined as a way to forward traffic between different VLAN by implementing a router in the network. As we learnt previously, VLANs logically segment the switch into different subnets, when a router is connected to the switch, an administrator can configure the router to forward the traffic between the various VLANs configured on the switch. The user nodes in the VLANs forwards traffic to the router which then forwards the traffic to the destination network regardless of the VLAN configured on the switch.

Information destined for PC B, leaves PC A with the VLAN 20 tag, when it gets to R1, the router, changes the format of this message from VLAN 20, to VLAN 30, it then sends it back to the switch and the switch finally sends the message to its intended recipient PC B.

There are three ways in which inter-VLAN routing can be accomplished.

* Traditional inter-VLAN routing
* Router-on-a-stick
* Multi-Layer switch (MLS)

## **5.2 TRADITIONAL INTER-VLAN ROUTING**

In this type of inter-VLAN routing, a router is usually connected to the switch using multiple interfaces. One for each VLAN. The interfaces on the router are configured as the default gateways for the VLANs configured on the switch. The ports that connect to the router from the switch are configured in access mode in their corresponding VLANs.

When a user node send a message to a user connected to a different VLAN, the message moves from their node to the access port that connects to the router on their VLAN. When the router receives the packet, it examines the packet's destination IP address and forwards it to the correct network using the access port for the destination VLAN. The switch now can forward the frame to the destination node since the router changed the VLAN information from the source VLAN to the destination VLAN.

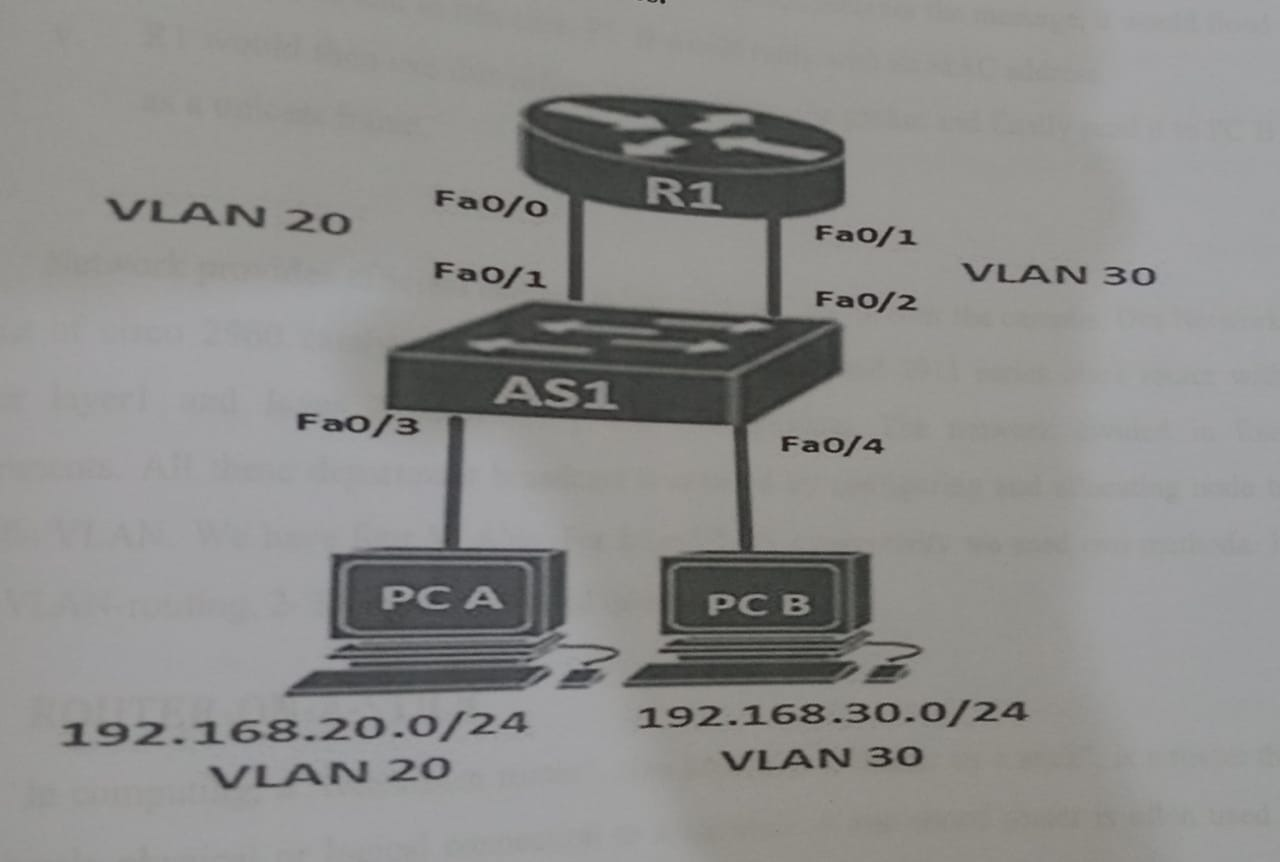
In this form of inter-VLAN routing, the router has to have as many LAN interfaces as the number of VLANs configured on the switch. Therefore, if a switch has LO VLANs, the router should have the same number of LAN interfaces.

Figure 5.1 Traditional inter-vlan routing

IPC A in VLAN 20. Wanted to send a message to PCB in VLAN 30, the steps it would take are

Shown below

* PC A would check whether the destination IPv4 address is in its VLAN if it is not, it would need to forward the traffic to its default gateway which is the ip address on Fa0/0 on R1
* PC A then sends an ARP request to AS so as to determine the physical address of Fa0/0 on RI. Once the router replies, PC A can send the frame to the router as a unicast message, since ASI has F0/0 MAC address, it can forward the frame directly to R1.
* When the router receives the frame, it compares the destination IP address by referring to its routing table so as to know to which interface it should send the data towards the destination node.
* The router then sends an ARP request out the interface connected to the destination VLAN in this case out Fab', when the switch receives the message, it would flood it to its ports and in this case, PCB would reply with its MAC address.
* R1 would then use this information to frame the packet and finally send it to PCB as a unicast frame.

## **5.3 ROUTER-ON-A-STICK**

In computing, a "one-armed router", also known as a "router on a stick", is a router that has a single physical or logical connection to a network. A one-armed router is often used to forward traffic between locally attached hosts on separate logical routing domains or to facilitate routing table

Administration, distribution and relay. One-armed routers that perform traffic forwarding are often implemented on virtual local area networks (VLAN). They would use a single Ethernet network interface port that is part of two or more Virtual LANs, enabling them to be joined. A VLAN allows multiple virtual LANs to coexist on the same physical LAN. This means that two machines attached to the same switch cannot send Ethernet frames to each other even though they pass over the same wires. If they need to communicate, there a router must be placed between the two VLANs to forward packets, just as if the two LANs were physically isolated.

The only difference is that the router in question may contain only a single Ethernet NIC that is part of both VLANs. Hence, "one- armed". While uncommon, hosts on the same physical medium may be assigned with addresses and to different networks. A one-armed router could be assigned addresses for each network and be used to forward traffic between locally distinct networks and to remote networks through another gateway

## **5.4 SWITCH VIRTUAL INTERFACE ON MLS**

A switched virtual interface (SVI) is a VLAN of switch ports represented by one interface to a routing or bridging system. There is no physical interface for the VLAN and the SVI provides the Layer 3 processing for packets from all switch ports associated with the VLAN. There is one-to-one mapping between a VLAN and SVI, thus only a single SVI can be mapped to a VLAN. By default, an SVI is created for the default VLAN (VLANI) to permit remote switch administration. An SVI cannot be activated unless associated with a physical port

## **5.5 ENCAPSULATION 802.1Q**

* It is an IEEE Standard.
* 802.1q supports 4096 Vlans.
* IN 802.1q encapsulation process, a 4 byte tag is inserted into original frame and FCS (Frame Check Sequence) is re-calculated.
* 802.1q does not tag frames from native Vlans.

# **CHAPTER 6**

# **CONFIGURATION AND IMPLANTATION**

Our Network consist of cisco 2960 catalyst switch, and 2621 series cisco router. The network divided in five segments. All These segments. Broadcast is reduced by configuring and allocating node to specific VLAN. We have five VLANS. For inter-vlan we have used router on stick method.

## **6.1. Network topology Diagram**

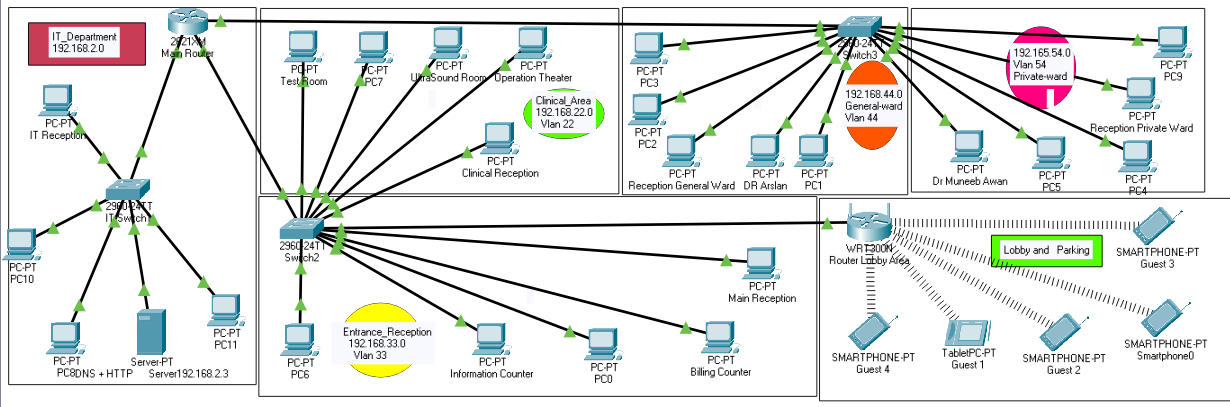


Figure 6.1 Network topology

## **6.2 Router SVI interface configurations**

## **6.2.1 Private ward SVI configuration**

Main-Router>enable

Password:

Main-Router#config t

Main-Router(config)#interface fastethernet 1/0

Main-Router(config)#no ip address

Main-Router(config)#no shutdown

Main-Router(config)#exit

Main-Router(config)#interface fastEthernet 1/0.54

Main-Router(config-subif)#encapsulation dot1Q 54

Main-Router(config-subif)#ip address 192.168.54.100 255.255.255.0

Main-Router(config-subif)#no shutdown

## **6.2.2 General ward SVI configuration**

Main-Router>enable

Password:

Main-Router#config t

Main-Router(config)#interface fastethernet 1/0

Main-Router(config)#no ip address

Main-Router(config)#no shutdown

Main-Router(config)#exit

Main-Router(config)#interface fastEthernet 1/0.44

Main-Router(config-subif)#encapsulation dot1Q 44

Main-Router(config-subif)#ip address 192.168.44.100 255.255.255.0

Main-Router(config-subif)#no shutdown

## **6.2.3 Clinical ward SVI configuration**

Main-Router>enable

Password:

Main-Router#config t

Main-Router(config)#interface fastethernet 0/1

Main-Router(config)#no ip address

Main-Router(config)#no shutdown

Main-Router(config)#exit

Main-Router(config)#interface fastEthernet 0/1.22

Main-Router(config-subif)#encapsulation dot1Q 22

Main-Router(config-subif)#ip address 192.168.22.100 255.255.255.0

Main-Router(config-subif)#no shutdown

## **6.2.4 Entrance Reception SVI configuration**

Main-Router>enable

Password:

Main-Router#config t

Main-Router(config)#interface fastethernet 0/1

Main-Router(config)#no ip address

Main-Router(config)#no shutdown

Main-Router(config)#exit

Main-Router(config)#interface fastEthernet 0/1.33

Main-Router(config-subif)#encapsulation dot1Q 33

Main-Router(config-subif)#ip address 192.168.33.100 255.255.255.0

Main-Router(config-subif)#no shutdown

## **6.2.5 IT Department interface configuration**

Main-Router>enable

Password:

Main-Router#config t

Main-Router(config)#interface fastethernet 0/0

Main-Router(config-subif)#ip address 192.168.2.100 255.255.255.0

Main-Router(config-subif)#no shutdown

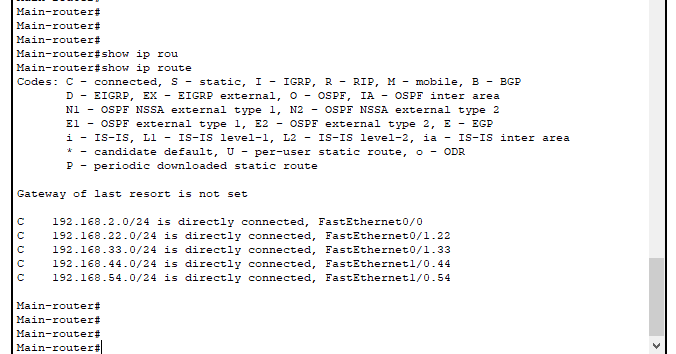


Figure 6.2 Router routing Table

# **6.3 VLAN Configuration**

**Configuration of vlan 22 and 33:**

SWITCH-2(config)#

SWITCH-2(config)#vlan 33

SWITCH-2(config-vlan)#name Clinical

SWITCH-2(config-vlan)#

SWITCH-2(config-vlan)#exit

SWITCH-2(config)#vlan 33

SWITCH-2(config-vlan)#name Entrance Reception

SWITCH-2(config-vlan)#

SWITCH-2(config-vlan)#exit

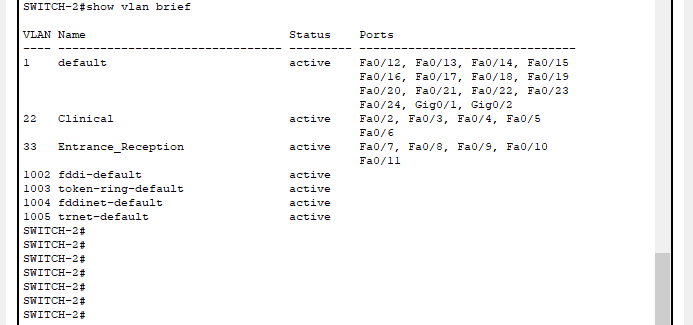


Figure 6.3 Vlan Database of switch-2

# **6.3.1 VLAN Configuration**

**Configuration of vlan 44 and 54:**

SWITCH-2(config)#

SWITCH-2(config)#vlan 44

SWITCH-2(config-vlan)#name General

SWITCH-2(config-vlan)#

SWITCH-2(config-vlan)#exit

SWITCH-2(config)#vlan 54

SWITCH-2(config-vlan)#name private

SWITCH-2(config-vlan)#

SWITCH-2(config-vlan)#exit

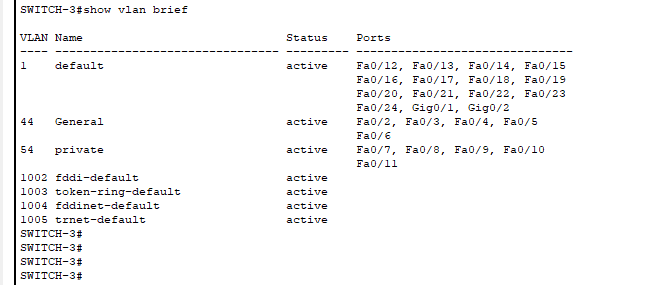


Figure 6.4 Vlan Database of switch-3

# **6.4 Dhcp pool configuration For Vlans**

## **6.4.1 Private ward Dhcp configuration**

Main-Router>enable

Password:

Main-Router#config t

Main-Router(config)#Ip dhcp pool vlan54

Main-Router(config)#Network 192.168.54.0 255.255.255.0

Main-Router(config)#ip default-router 192.168.54.100

Main-Router(config)#dns-server 192.168.2.250

## **6.4.2 General ward Dhcp configuration**

Main-Router>enable

Password:

Main-Router#config t

Main-Router(config)#Ip dhcp pool vlan44

Main-Router(config)#Network 192.168.44.0 255.255.255.0

Main-Router(config)#ip default-router 192.168.44.100

Main-Router(config)#dns-server 192.168.2.250

## **6.4.3** **Clinical ward Dhcp configuration**

Main-Router>enable

Password:

Main-Router#config t

Main-Router (config) #Ip dhcp pool vlan22

Main-Router (config) #Network 192.168.22.0 255.255.255.0

Main-Router (config) #ip default-router 192.168.22.100

Main-Router (config) #dns-server 192.168.2.250

## **6.4.4 Entrance Reception Dhcp configuration**

Main-Router>enable

Password:

Main-Router#config t

Main-Router(config)#Ip dhcp pool vlan33

Main-Router(config)#Network 192.168.33.0 255.255.255.0

Main-Router(config)#ip default-router 192.168.33.100

Main-Router(config)#dns-server 192.168.2.250

## **6.4.5 IT Department Dhcp configuration**

Main-Router>enable

Password:

Main-Router#config t

Main-Router(config)#Ip dhcp pool IT

Main-Router(config)#Network 192.168.2.0 255.255.255.0

Main-Router(config)#ip default-router 192.168.2.100

Main-Router(config)#dns-server 192.168.2.250

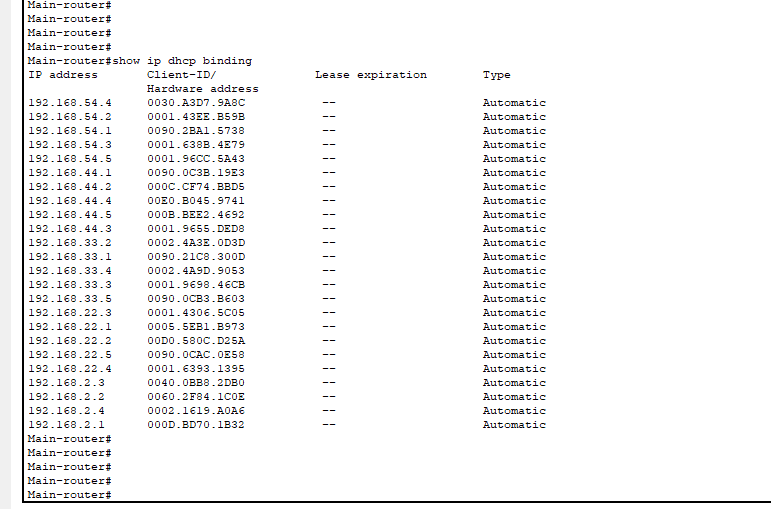


Figure 6.5 Dhcp Database on Router

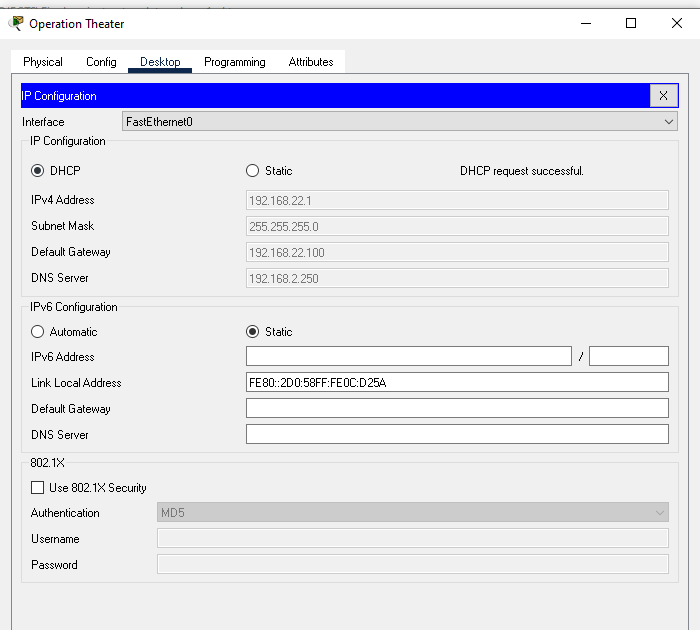


Figure 6.6 OT PC belongs to vlan 22

# **6.5 SSH Configuration**

## **6.5.1 SSH Configuration on Main router**

Router>

Router>enable

Router#config t

Router(config)#username admin password admin

Router(config)#hostname Main-router

Main-router(config)#ip domain-name test.local

Main-router(config)#ip ssh version 2

Please create RSA keys (of at least 768 bits size) to enable SSH v2.

Main-router(config)#crypto key generate rsa general-keys

The name for the keys will be: Main-router.test.local

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

\*Mar 1 0:11:14.467: %SSH-5-ENABLED: SSH 2 has been enabled

Main-router(config)#line vty 0 4

Main-router(config-line)#transport input ssh

Main-router(config-line)#login local

Main-router(config-line)#

Main-router(config-line)#exit

Main-router(config)#

Main-router(config)#

## **6.5.2 SSH Configuration on Switch A**

Switch>enable

Switch#

Switch#config t

Switch(config)#interface vlan 1

Switch(config-if)#ip address 192.168.2.101 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#

%LINK-5-CHANGED: Interface Vlan1, changed state to up

Switch(config-if)#

Switch(config-if)#exit

Switch(config)#enable password admin

Switch(config)#username admin password admin

Switch(config)#hostname SW-A

SW-A(config)#ip domain-name testswitch.local

SW-A(config)#ip default-gateway 192.168.2.100

SW-A(config)#ip ssh version 2

Please create RSA keys (of at least 768 bits size) to enable SSH v2.

SW-A(config)#crypto key generate rsa general-keys

The name for the keys will be: SW-A.testswitch.local

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SW-A(config)#li

\*Mar 1 0:3:51.472: %SSH-5-ENABLED: SSH 2 has been enabled

SW-A(config)#line vty 0 4

SW-A(config-line)#transport input ssh

SW-A(config-line)#login local

SW-A(config-line)#exit

## **6.5.3 SSH Configuration on Switch B**

Switch>enable

Switch#

Switch#config t

Switch(config)#interface vlan 22

Switch(config-if)#ip address 192.168.22.101 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#

%LINK-5-CHANGED: Interface Vlan22, changed state to up

Switch(config-if)#

Switch(config-if)#exit

Switch(config)#enable password admin

Switch(config)#username admin password admin

Switch(config)#hostname SW-B

SW-B(config)#ip domain-name testswitch.local

SW-B(config)#ip default-gateway 192.168.22.100

SW-B(config)#ip ssh version 2

Please create RSA keys (of at least 768 bits size) to enable SSH v2.

SW-B(config)#crypto key generate rsa general-keys

The name for the keys will be: SW-B.testswitch.local

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SW-A(config)#li

\*Mar 1 0:3:51.472: %SSH-5-ENABLED: SSH 2 has been enabled

SW-B(config)#line vty 0 4

SW-B(config-line)#transport input ssh

SW-B(config-line)#login local

SW-B(config-line)#exit

## **6.5.4 SSH Configuration on Switch C**

Switch>enable

Switch#

Switch#config t

Switch(config)#interface vlan 54

Switch(config-if)#ip address 192.168.54.101 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#

%LINK-5-CHANGED: Interface Vlan54, changed state to up

Switch(config-if)#

Switch(config-if)#exit

Switch(config)#enable password admin

Switch(config)#username admin password admin

Switch(config)#hostname SW-C

SW-B(config)#ip domain-name testswitch.local

SW-B(config)#ip default-gateway 192.168.54.100

SW-B(config)#ip ssh version 2

Please create RSA keys (of at least 768 bits size) to enable SSH v2.

SW-B(config)#crypto key generate rsa general-keys

The name for the keys will be: SW-C.testswitch.local

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SW-A(config)#li

\*Mar 1 0:3:51.472: %SSH-5-ENABLED: SSH 2 has been enabled

SW-B(config)#line vty 0 4

SW-B(config-line)#transport input ssh

SW-B(config-line)#login local

SW-B(config-line)#exit

### **6.5.5 Accessing SW-C through SSH from SW-A LAN**

Here we will access SW-c through SSH from SW-A Lan we will open command prompt in any of the SW-A Lan PC and enter the following commands 192.168.54.101 is the ip address of SSH Access switch c.

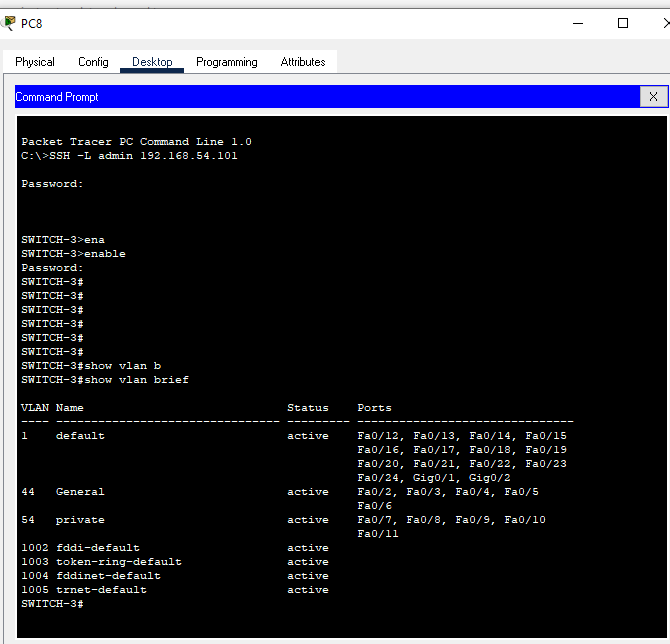


Figure 6.7 SSH Access from command prompt

# **6.6 PORT ASSIGNMENT CONFIGURATION**

### **6.6.1 SWITCH-2**

!

SWITCH-2(config)#Interface FastEthernet0/2

SWITCH-2(config)#Switchport access vlan 22

SWITCH-2(config)#Switchport mode access!

SWITCH-2(config)#Interface FastEthernet0/3

SWITCH-2(config)#Switchport access vlan 22

SWITCH-2(config)#Switchport mode access

!

SWITCH-2(config)#Interface FastEthernet0/4

SWITCH-2(config)#Switchport access vlan 22

SWITCH-2(config)#Switchport mode access

SWITCH-2(config)#Interface FastEthernet0/5

SWITCH-2(config)#Switchport access vlan 22

SWITCH-2(config)#Switchport mode access

!

SWITCH-2(config)#Interface FastEthernet0/6

SWITCH-2(config)#Switchport access vlan 22

SWITCH-2(config)#Switchport mode access

!

SWITCH-2(config)#Interface FastEthernet0/7

SWITCH-2(config)#Switchport access vlan 33

SWITCH-2(config)#Switchport mode access

!

SWITCH-2(config)#Interface FastEthernet0/8

SWITCH-2(config)#Switchport access vlan 33

SWITCH-2(config)#Switchport mode access

!

SWITCH-2(config)#Interface FastEthernet0/9

SWITCH-2(config)#Switchport access vlan 33

SWITCH-2(config)#Switchport mode access

!

SWITCH-2(config)#Interface FastEthernet0/10

SWITCH-2(config)#Switchport access vlan 33

SWITCH-2(config)#Switchport mode access

!

SWITCH-2(config)#Interface FastEthernet0/11

SWITCH-2(config)#Switchport access vlan 33

SWITCH-2(config)#Switchport mode access

### **6.6.2 SWITCH-3**

SWITCH-3(config)#Interface FastEthernet0/2

SWITCH-3(config)#Switchport access vlan 44

SWITCH-3(config)#Switchport mode access

!

SWITCH-3(config)#Interface FastEthernet0/3

SWITCH-3(config)#Switchport access vlan 44

SWITCH-3(config)#Switchport mode access

!

SWITCH-3(config)#Interface FastEthernet0/4

SWITCH-3(config)#Switchport access vlan 44

SWITCH-3(config)#Switchport mode access

!

SWITCH-3(config)#Interface FastEthernet0/5

SWITCH-3(config)#Switchport access vlan 44

SWITCH-3(config)#Switchport mode access

!

SWITCH-3(config)#Interface FastEthernet0/6

SWITCH-3(config)#Switchport access vlan 44

SWITCH-3(config)#Switchport mode access

!

SWITCH-3(config)#Interface FastEthernet0/7

SWITCH-3(config)#Switchport access vlan 54

SWITCH-3(config)#Switchport mode access

!

SWITCH-3(config)#Interface FastEthernet0/8

SWITCH-3(config)#Switchport access vlan 54

SWITCH-3(config)#Switchport mode access

!

SWITCH-3(config)#Interface FastEthernet0/9

SWITCH-3(config)#Switchport access vlan 54

SWITCH-3(config)#Switchport mode access

!

SWITCH-3(config)#Interface FastEthernet0/10

SWITCH-3(config)#Switchport access vlan 54

SWITCH-3(config)#Switchport mode access

!

SWITCH-3(config)#Interface FastEthernet0/11

SWITCH-3(config)#Switchport access vlan 54

SWITCH-3(config)#Switchport mode access

# **6.7 PORT SECURITY CONFIGURATION**

### **6.7.1 Port security configuration on switch 1**

!

SWITCH-1(config)#interface FastEthernet0/2

SWITCH-1(config)#switchport mode access

SWITCH-1(config)#switchport port-security

SWITCH-1(config)#switchport port-security mac-address sticky

SWITCH-1(config)#switchport port-security violation restrict

!

SWITCH-1(config)#interface FastEthernet0/3

SWITCH-1(config)#switchport mode access

SWITCH-1(config)#switchport port-security

SWITCH-1(config)#switchport port-security mac-address sticky

SWITCH-1(config)#switchport port-security violation restrict

!

SWITCH-1(config)#interface FastEthernet0/4

SWITCH-1(config)#switchport mode access

SWITCH-1(config)#switchport port-security

SWITCH-1(config)#switchport port-security mac-address sticky

SWITCH-1(config)#switchport port-security violation restrict

!

SWITCH-1(config)#interface FastEthernet0/5

SWITCH-1(config)#switchport mode access

SWITCH-1(config)#switchport port-security

SWITCH-1(config)#switchport port-security mac-address sticky

SWITCH-1(config)#switchport port-security violation restrict

!

SWITCH-1(config)#interface FastEthernet0/6

SWITCH-1(config)#switchport mode access

SWITCH-1(config)#switchport port-security

SWITCH-1(config)#switchport port-security mac-address sticky

SWITCH-1(config)#switchport port-security violation restrict

!

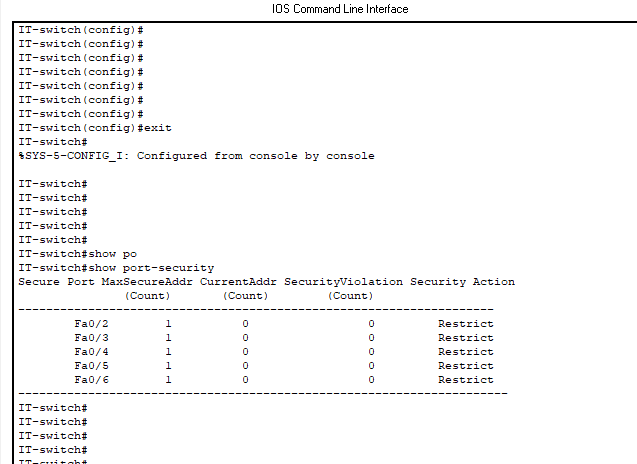


Figure 6.8 switch-1 data base of port security

### **6.7.2 Port security configuration on switch 2**

SWITCH-2(config)#interface FastEthernet0/2

SWITCH-2(config)#switchport mode access

SWITCH-2(config)#switchport port-security

SWITCH-2(config)#switchport port-security mac-address sticky

SWITCH-2(config)#switchport port-security violation restrict

SWITCH-2(config)#switchport port-security mac-address sticky 0001.6393.1395

!

SWITCH-2(config)#interface FastEthernet0/3

SWITCH-2(config)#switchport mode access

SWITCH-2(config)#switchport port-security

SWITCH-2(config)#switchport port-security mac-address sticky

SWITCH-2(config)#switchport port-security violation restrict

SWITCH-2(config)#switchport port-security mac-address sticky 0005.5EB1.B973

!

SWITCH-2(config)#interface FastEthernet0/4

SWITCH-2(config)#switchport mode access

SWITCH-2(config)#switchport port-security

SWITCH-2(config)#switchport port-security mac-address sticky

SWITCH-2(config)#switchport port-security violation restrict

SWITCH-2(config)#switchport port-security mac-address sticky 0001.4306.5C05

!

SWITCH-2(config)#interface FastEthernet0/5

SWITCH-2(config)#switchport mode access

SWITCH-2(config)#switchport port-security

SWITCH-2(config)#switchport port-security mac-address sticky

SWITCH-2(config)#switchport port-security violation restrict

SWITCH-2(config)#switchport port-security mac-address sticky 00D0.580C.D25A

!

SWITCH-2(config)#interface FastEthernet0/6

SWITCH-2(config)#switchport mode access

SWITCH-2(config)#switchport port-security

SWITCH-2(config)#switchport port-security mac-address sticky

SWITCH-2(config)#switchport port-security violation restrict

SWITCH-2(config)#switchport port-security mac-address sticky 0090.0CAC.0E58

!

SWITCH-2(config)#interface FastEthernet0/7

SWITCH-2(config)#switchport mode access

SWITCH-2(config)#switchport port-security

SWITCH-2(config)#switchport port-security mac-address sticky

SWITCH-2(config)#switchport port-security violation restrict

SWITCH-2(config)#switchport port-security mac-address sticky 0001.9698.46CB

!

SWITCH-2(config)#interface FastEthernet0/8

SWITCH-2(config)#switchport mode access

SWITCH-2(config)#switchport port-security

SWITCH-2(config)#switchport port-security mac-address sticky

SWITCH-2(config)#switchport port-security violation restrict

SWITCH-2(config)#switchport port-security mac-address sticky 0090.21C8.300D

!

SWITCH-2(config)#interface FastEthernet0/9

SWITCH-2(config)#switchport mode access

SWITCH-2(config)#switchport port-security

SWITCH-2(config)#switchport port-security mac-address sticky

SWITCH-2(config)#switchport port-security violation restrict

SWITCH-2(config)#switchport port-security mac-address sticky 0090.0CB3.B603

!

SWITCH-2(config)#interface FastEthernet0/10

SWITCH-2(config)#switchport mode access

SWITCH-2(config)#switchport port-security

SWITCH-2(config)#switchport port-security mac-address sticky

SWITCH-2(config)#switchport port-security violation restrict

SWITCH-2(config)#switchport port-security mac-address sticky 0002.4A3E.0D3D

!

SWITCH-2(config) # interface FastEthernet0/11

SWITCH-2(config)# switchport mode access

SWITCH-2(config)#switchport port-security

SWITCH-2(config)#switchport port-security mac-address sticky

SWITCH-2(config)#switchport port-security violation restrict

SWITCH-2(config)#switchport port-security mac-address sticky 0002.4A9D.9053

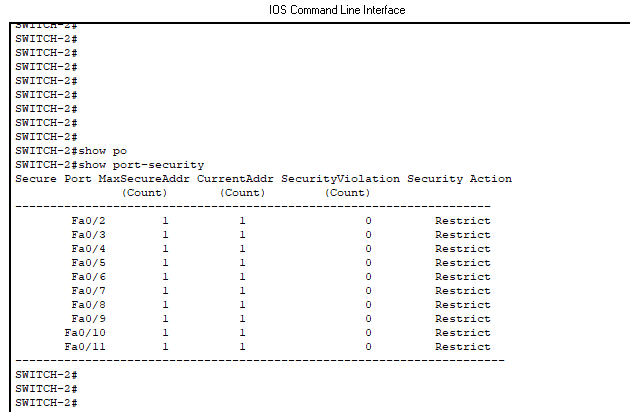


Figure 6.9 switch-2 Database of port security

### **6.7.3 Port security configuration on switch 3**

!

SWITCH-3(config)#interface FastEthernet0/2

SWITCH-3(config)#switchport mode access

SWITCH-3(config)#switchport port-security

SWITCH-3(config)#switchport port-security mac-address sticky

SWITCH-3(config)#switchport port-security violation restrict

SWITCH-3(config)#switchport port-security mac-address sticky 0001.9655.DED8

!

SWITCH-3(config)#interface FastEthernet0/3

SWITCH-3(config)#switchport mode access

SWITCH-3(config)#switchport port-security

SWITCH-3(config)#switchport port-security mac-address sticky

SWITCH-3(config)#switchport port-security violation restrict

SWITCH-3(config)#switchport port-security mac-address sticky 0090.0C3B.19E3

!

SWITCH-3(config)#interface FastEthernet0/4

SWITCH-3(config)#switchport mode access

SWITCH-3(config)#switchport port-security

SWITCH-3(config)#switchport port-security mac-address sticky

SWITCH-3(config)#switchport port-security violation restrict

SWITCH-3(config)#switchport port-security mac-address sticky 000C.CF74.BBD5

!

SWITCH-3(config)#interface FastEthernet0/5

SWITCH-3(config)#switchport mode access

SWITCH-3(config)#switchport port-security

SWITCH-3(config)#switchport port-security mac-address sticky

SWITCH-3(config)#switchport port-security violation restrict

SWITCH-3(config)#switchport port-security mac-address sticky 00E0.B045.9741

!

SWITCH-3(config)#interface FastEthernet0/6

SWITCH-3(config)#switchport mode access

SWITCH-3(config)#switchport port-security

SWITCH-3(config)#switchport port-security mac-address sticky

SWITCH-3(config)#switchport port-security violation restrict

SWITCH-3(config)#switchport port-security mac-address sticky 000B.BEE2.4692

!

SWITCH-3(config)#interface FastEthernet0/7

SWITCH-3(config)#switchport mode access

SWITCH-3(config)#switchport port-security

SWITCH-3(config)#switchport port-security mac-address sticky

SWITCH-3(config)#switchport port-security violation restrict

SWITCH-3(config)#switchport port-security mac-address sticky 0001.96CC.5A43

!

SWITCH-3(config)#interface FastEthernet0/8

SWITCH-3(config)#switchport mode access

SWITCH-3(config)#switchport port-security

SWITCH-3(config)#switchport port-security mac-address sticky

SWITCH-3(config)#switchport port-security violation restrict

SWITCH-3(config)#switchport port-security mac-address sticky 0001.43EE.B59B

!

SWITCH-3(config)#interface FastEthernet0/9

SWITCH-3(config)#switchport mode access

SWITCH-3(config)#switchport port-security

SWITCH-3(config)#switchport port-security mac-address sticky

SWITCH-3(config)#switchport port-security violation restrict

SWITCH-3(config)#switchport port-security mac-address sticky 0001.638B.4E79

!

SWITCH-3(config)#interface FastEthernet0/10

SWITCH-3(config)#switchport mode access

SWITCH-3(config)#switchport port-security

SWITCH-3(config)#switchport port-security mac-address sticky

SWITCH-3(config)#switchport port-security violation restrict

SWITCH-3(config)#switchport port-security mac-address sticky 0030.A3D7.9A8C

!

SWITCH-3(config)#interface FastEthernet0/11

SWITCH-3(config)#switchport mode access

SWITCH-3(config)#switchport port-security

SWITCH-3(config)#switchport port-security mac-address sticky

SWITCH-3(config)#switchport port-security violation restrict

SWITCH-3(config)#switchport port-security mac-address sticky 0090.2BA1.5738

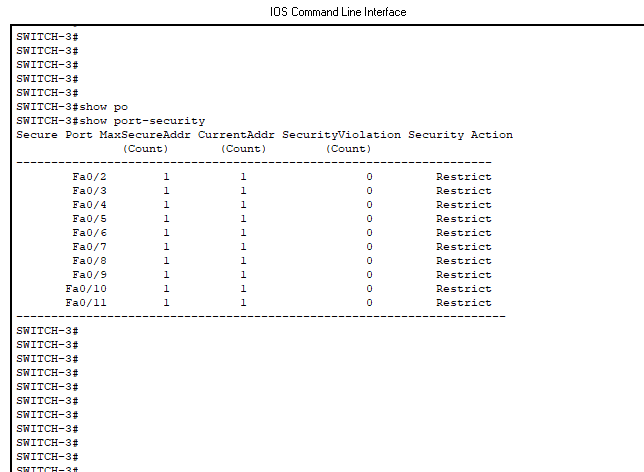


Figure 6.10 switch-3 data base of port security

# **CHAPTER-7**

# **SUMMARY AND CONCLUSION**

## **7.1 SUMMARY**

Simply we can say a network, or a computer network, is a collection of computers and other hardware are interconnected by communication channels that allow sharing of resources und information. A Network is a group of devices connected to each other. A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data. A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch module port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Different VLANs can't communicate with each other, they can communicate with the help of Layer-3 device. Hence, it is needed to connect a router to a switch, then make the sub-interface on the router to connect to the switch, establishing Trunking links to achieve communications of devices which belong to different VLANs. When using VLANs in networks that have multiple interconnected switches, you need to use VLAN trunking between the switches. With VLAN trunking, the switches tag each frame sent between switches so that the receiving switch knows to what VLAN the frame belongs. End user devices connect to switch ports that provide simple connectivity to a single VLAN each. The attached devices are unaware of any VLAN structure. By default, only hosts that are members of the same VLAN can communicate. To change this and allow inter-VLAN communication, you need a router or a layer-3 switch. We add Dynamic Host Configuration Protocol (DHCP) that we commonly use every day on almost all of your devices. Its networking protocols If you don't have to set a static IP address for your devices, they are dynamically set with DHCP, DHCP is not just for IP address, subnet mask, and Gateway, however. DHCP provides information you typically don't look at, for example: NTP servers, DNS servers, FTP and configuration servers for devices such as desk phones, and many other services that can be set using custom option sets.

## **7.2 CONCLUSION**

Our work is based on LAN switching with focus of VLAN in which we study that local Area Network (LAN) is built with the help of network switches which by default creates a single flat network with large Broadcast domain. The increase in the number of devices On LAN becomes paramour as we populate the network with more switches and workstations. Since most stations tend to be loaded with existing operating system, it results in unavoidable broadcasts being set occasionally ca the network. Unfortunately, each host on such network cannot escape from the effects generated by such uncontrollable broadcast which decreases network performance, best solution to cover these problems are VLANs. We discussed and implement every aspect of our network and also verify the result. For different VLANs communication we used router. On a router we divide one physical interface into logical sub interface to communicate different VLANs on a network. Each Vlan is assigned to separate sub-interface. Each sub-interface is configured as trunk link on a router we configured the DCHP to give the IPv4 address to the client of different VLANs member given different network, the DIICP-server configured also the client Gateway and DNS- Server. Because it is difficult to us to give static IP address to each client on a network. To secure our network from unauthorized person we used Port-Security on Switches. On a Switch second and third we applied port-security from fast Ethernet 0/2 to fast Ethernet 0/11 ports and on switch one we applied port security from fast Ethernet 0/2 to fast Ethernet 0/6 ports. And allow one mac-address for any violation we set the interface to restrict.

### **7.3 FUTURE WORK**

The future in this field is very vast that companies from large 1000+ employees to small businesses with 10+ employees. The VLAN will help reduce irrelevant broadcast, increase security, and make it easier for the IT department to manage. There can also reduction in cost to a company with the ability of employees to network together and share data without having to travel to cities with other departments””. VLAN will grow even more in the future as companies uncover more advantages in the future as companies learn more of the cost reduction possibilities and advantages of using a VLAN within the company. There will be some initial cost in the setting of the VLAN but in the long term the cost reduction will offset the expenses the company will acquire. The future looks to have more MAC-based protocol because it tends to be more supportive of sharing server resources on multiple virtual networks.

# **REFERENCES**

1. <https://www.computerhope.com/jargon/n/network.htm>

2. [https://en.wikipedia.org/wiki/Wired\_communication](https://en.wikipedia.org/wiki/Wired_communication%20)

3. <https://www.computerhope.com/jargon/t/twispair.htm>

4. <https://searchnetworking.techtarget.com/definition/shielded-twisted-pair>

**5.** <https://www.techopedia.com/definition/15981/coaxial-cable>

6. <https://computer.howstuffworks.com/fiber-optic.htm>

7. <https://www.engineersgarage.com/4g-technology/>

8. <https://searchmobilecomputing.techtarget.com/definition/personal-area-network>

9. <https://techterms.com/definition/lan>

10. <https://searchnetworking.techtarget.com/definition/metropolitan-area-network-MAN>

11. <https://www.lifewire.com/wide-arca-network-816383>

12. <https://www.ictstore.com/free-cena/inter-vlan-routing-mulilayer-switch/>

13. <https://www.cenablog.com/inter-vlan-routing/>

14. <https://www.cisco.com/c/en/us/support/docs/lan-switch/inter-vlan-routing/>

15. [https://www.telecomworld101.com/RoasS html](https://www.telecomworld101.com/RoasS%20html)

16. <https://www.webopedia.com>