A

Mini Project Report

On

BIGBULL

BANK OF INDIA

Submitted in partial fulfillment of the requirements
of the degree of

Bachelor of Engineering

Group Members

Parth Pravin Shah (119IT3345A)

Jay Ashok Patel (119IT3216A)

Omkar Uday Mahadik (119IT3251A)

Ritik Prakash Singh (119IT3356A)

Under the Guidance of:

Prof. Swati Sinha

Department of IT Engineering

Mahatma Gandhi Mission's College of Engineering & Technology
Kamothe, Navi Mumbai – 410 209

Academic Year: 2021-22

CERTIFICATE

This is to certify that the mini project entitled **"BIGBULL BANK OF INDIA"**is a bonafide work of **PARTH PRAVIN SHAH (119IT3345A), JAY ASHOK PATEL (119IT3216A), OMKAR UDAY MAHADIK (119IT3251A), RITIK PRAKASH SINGH (119IT3356A)**submitted to the University of Mumbai in partial fulfillment of the requirement for the award of the degree of **"Undergraduate"** in **"Information Technology".**

Prof. Dr. Swati Sinha

(Project Guide)

(External Examiner)

Dr. Swati Sinha

(H. O. D. It Dept)

Dr. Geeta Lathkar

Director

DECLARATION

We declare that this written submission represents our ideas in our own words and where others ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

_____

(Signature)

Date:

Place: Kamothe

ACKNOWLEDGEMENT

The success and final outcome of this project required a lot of guidance and assistance from many people and we are extremely fortunate to have got this all along the completion of our project work. Whatever we have done is only due to such guidance and assistance and we would not forget to thank them.

It is matter of great pleasure for us to submit the project report on **"BIGBULL BANK OF INDIA"** as a part of our curriculum.

First and foremost, we would like to thank to our Director **Dr.Geeta Lathkar**, for giving us an opportunity to do the project work. We would like to thank our H.O.D **Swati Sinha** and Project **Guide Prof. Swati Sinha** for the valuable guidance and advice. He inspired us greatly to work in this project. Her willingness to motivate us contributed tremendously to our project and last but notthe least a special thanks goes to my team members, who helped me to assemble theinformation and gave suggestions to complete our project.

TABLE OF CONTENTS

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.

BigBull Bank is setting up a new 3-storey branch in Mumbai, Maharashtra IN. It is planning to have 6 departments allocated on their new branch. BigBull Bank proposed to have departments of internal IT supports, ATM services, consumer banking, investment banking, loans and insurance. All their departments network is separated but able to communicate with each other using an internal chatting system using a port. BigBull Bank prefer the branch to have a balance between network performance network performance, security and cost effectiveness.

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.

2.0 Site to Site VPN

A site-to-site virtual private network (VPN) is a connection between two or more networks, such as a corporate network and a branch office network. Many organizations use site-to-site VPNs to leverage an internet connection for private traffic as an alternative to using private MPLS circuits to Site VPN.

2.1 NAT/PAT

Network Address Translation (NAT) and Port Address Translation (PAT) are the protocols used to map the unregistered private (inside local) address of an internal network to a registered public (inside global) address of an external network before transferring the packet. The main difference between them is that NAT is used to map public IP addresses to private IP addresses, it could be a one-to-one or many-to-one relation. On the other hand, PAT is a type of NAT where the multiple private IP addresses are mapped into a single public IP (many-to-one) by using ports.

1.9 OBJECTIVES

Below are the main goals of the network being to achieve several operational objectives which are:

- Every department network is separated. All staffs can communicate through emails.
- There should be a guest Wi-Fi is provided to customers. This is an isolated network isolated with only web browsing capabilities.
- The IT department consists of a small team that the staffs are mainly performing operational tasks instead of planning and implementations. Your team is required to provide detail documentations so that the IT staffs can troubleshoot their systems with references.
- Your team are working to strike a balance between network performance, security and cost effectiveness so that your team can close this deal.
- The Branch Should Have a Communication with the Headquaters i.e in Delhi & the communication should be secured.
- NAT/PAT implementation in the branch.
- Additional Server farm for the branch office of bank.

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

i. 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.

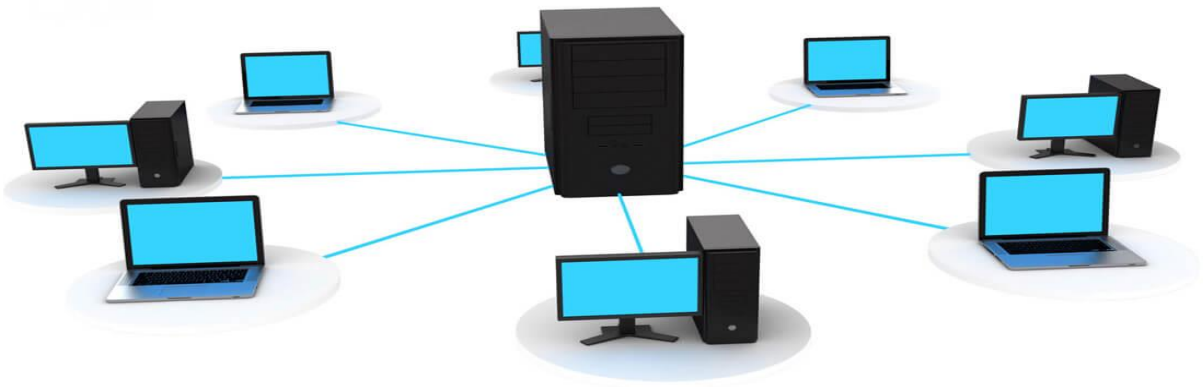


Figure 3.1 Server Based Network

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.

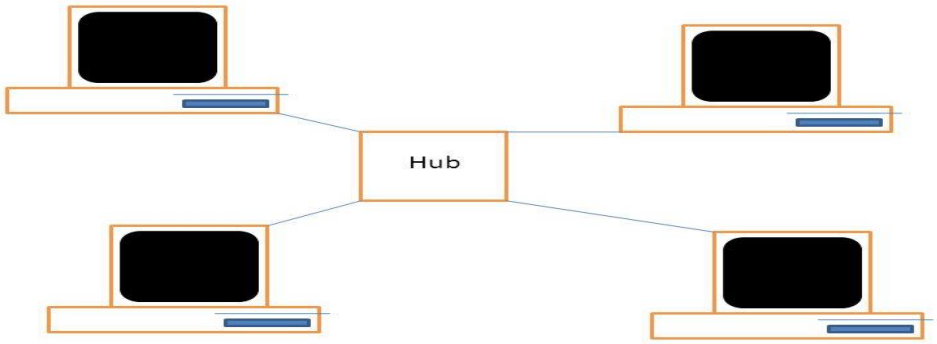


Figure 3.2 P2P Network workgroup

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.

i. Send documents upstairs to your office printer while sitting on the couch with your Laptop. Upload photos from your phone to your desktop computer.
ii. 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.

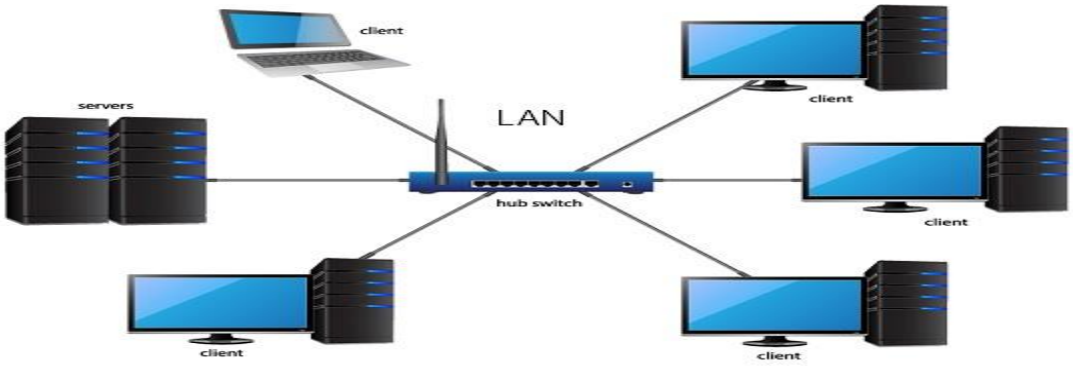


Figure 3.3 Local Area Network (LAN)

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.

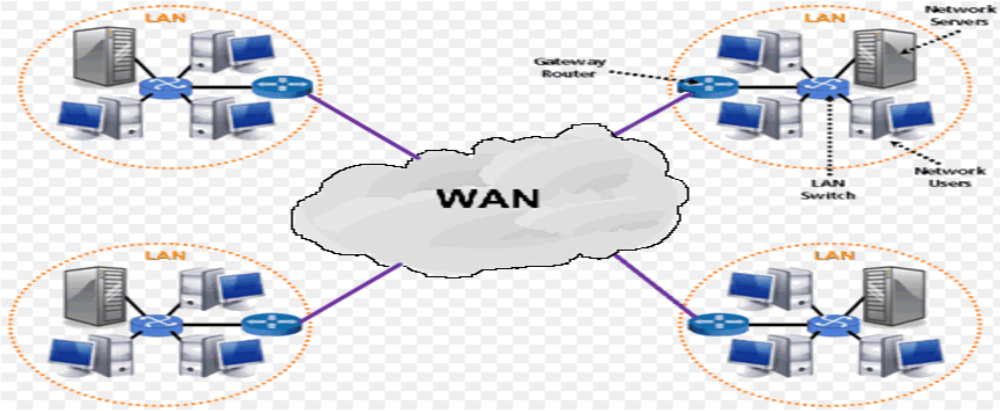


Figure 3.4 Wide Area Network

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.

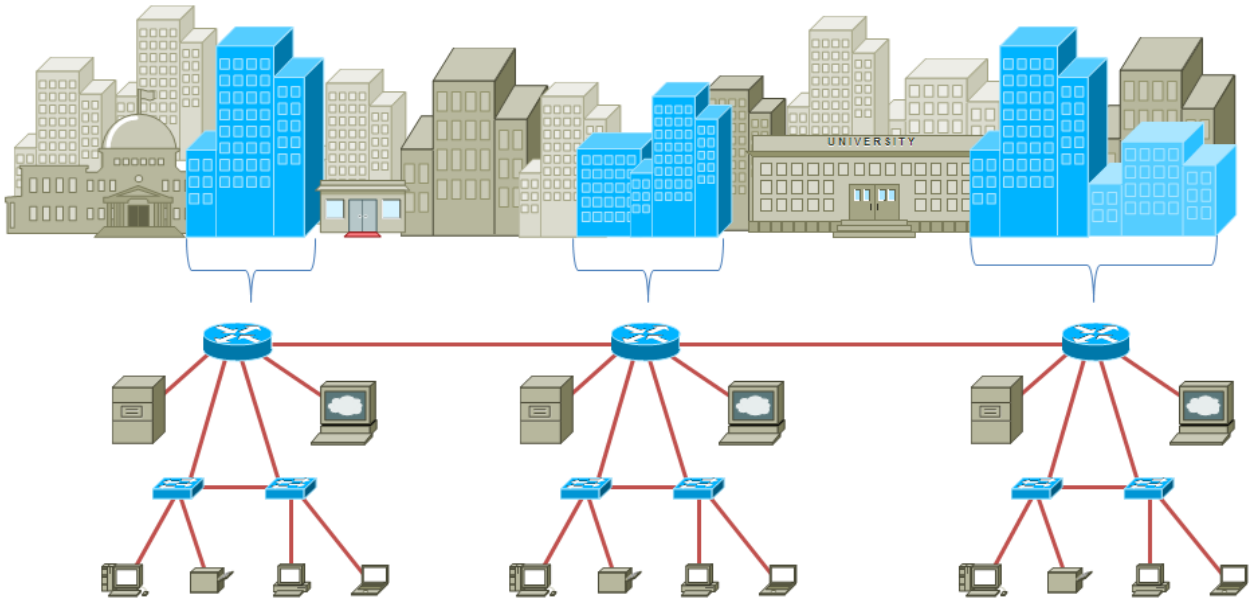


Figure 3.5 Metropolitan Area Network (MAN)

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 NETWORK 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.

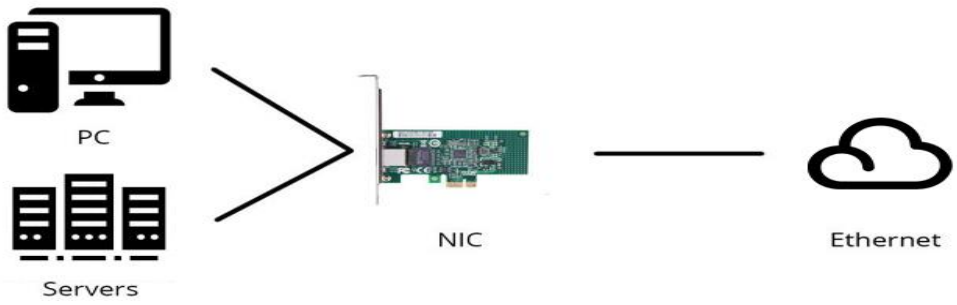


Figure 3.6 Network Interface Controller

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.

i. 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.

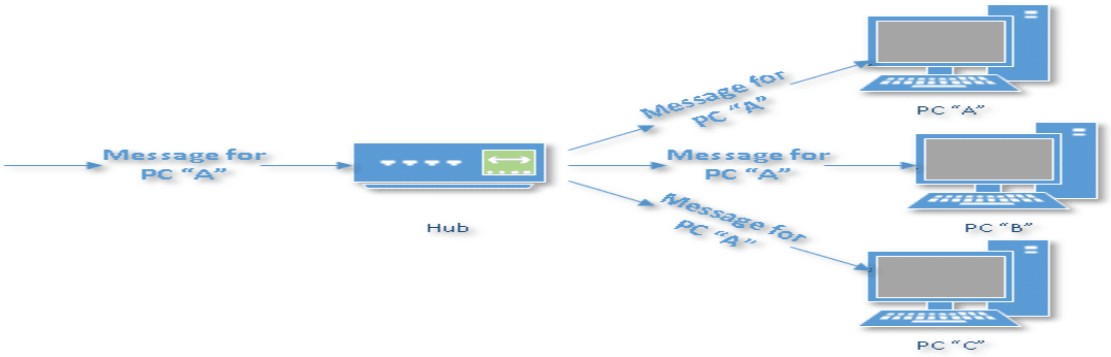


Figure 3.7 Layer 1 HUB

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

ii. 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

iii. 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

iv. 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.

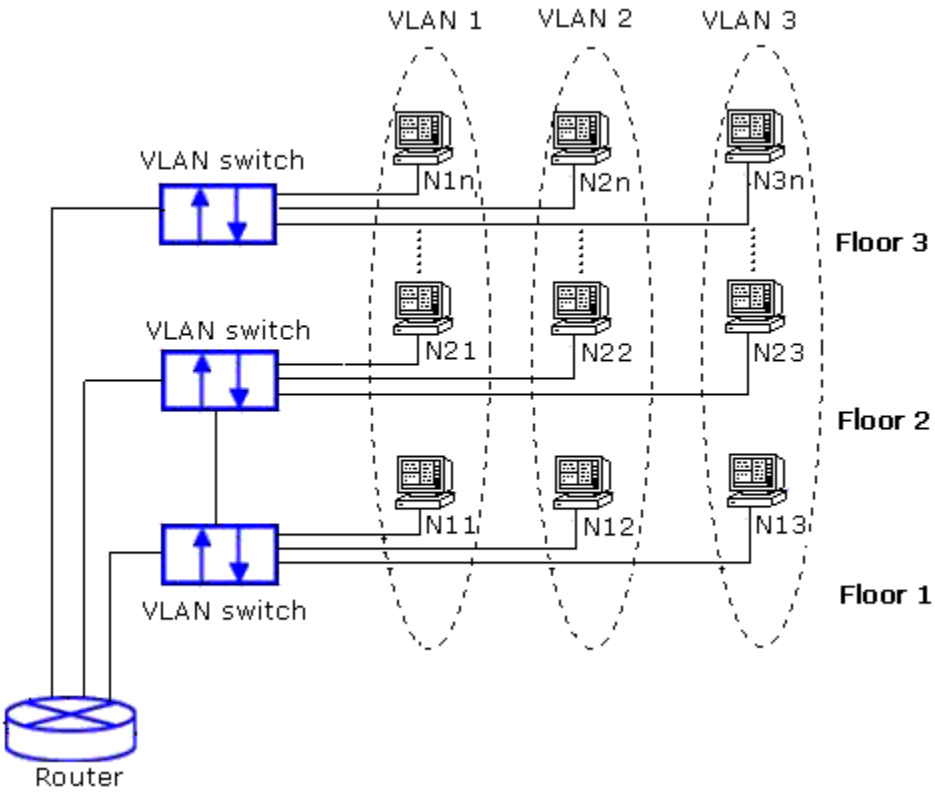


Figure 4.1 VLAN

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

i. 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

ii. 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

iii. 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.

iv. VLAN become great asset in providing security to our network plus saving lot of expenditure by providing virtual isolation in networks.

v. 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.

vi. 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.

vii. 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...

viii. 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.

ix. 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

i. 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.

ii. 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.

iii. Performance - Splitting up a switch into VLANs allows for multiple broadcast domains which reduces unnecessary traffic on the network and increases network performance.

iv. 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:

i. VLAN ID
ii. VLAN name
iii. 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.

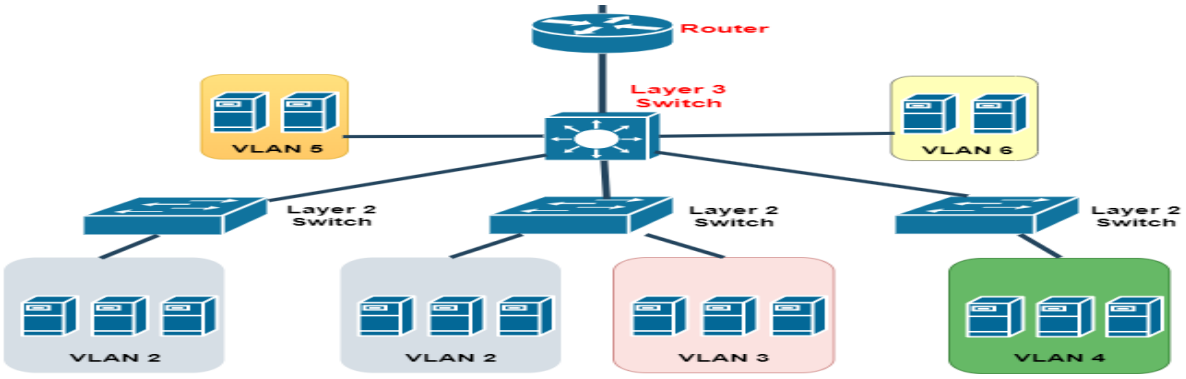


Figure 4.2 Different VLANs Works

CHAPTER-5

ROUTING

5.1 OSPF (OPEN SHORT PATH FIRST) ROUTING

- OSPF is a standardized Link-State routing protocol, designed to scale efficiently to support larger networks.

OSPF adheres to the following Link State characteristics:

• OSPF employs a hierarchical network design using Areas.

• OSPF will form neighbor relationships with adjacent routers in the same Area.

• Instead of advertising the distance to connected networks, OSPF advertises the status of directly connected links using Link-State Advertisements (LSAs).

• OSPF sends updates (LSAs) when there is a change to one of its links, and will only send the change in the update. LSAs are additionally refreshed every 30 minutes.

• OSPF traffic is multicast either to address 224.0.0.5 (all OSPF routers) or 224.0.0.6 (all Designated Routers).

• OSPF uses the Dijkstra Shortest Path First algorithm to determine the shortest path.

• OSPF is a classless protocol, and thus supports VLSMs.

Other characteristics of OSPF include:

• OSPF supports only IP routing.

• OSPF routes have an administrative distance is 110.

• OSPF uses cost as its metric, which is computed based on the

bandwidth of the link. OSPF has no hop-count limit.

The OSPF process builds and maintains three separate tables:

• A neighbor table – contains a list of all neighboring routers.

• A topology table – contains a list of all possible routes to all known networks within an area.

• A routing table – contains the best route for each known network.

OSPF Neighbors

OSPF forms neighbor relationships, called adjacencies, with other routers in the same Area by exchanging Hello packets to multicast address 224.0.0.5.

Only after an adjacency is formed can routers share routing information.

Each OSPF router is identified by a unique Router ID. The Router ID can be determined in one of three ways:

• The Router ID can be manually specified.

• If not manually specified, the highest IP address configured on any

Loopback interface on the router will become the Router ID.

• If no loopback interface exists, the highest IP address configured on

any Physical interface will become the Router ID.

By default, Hello packets are sent out OSPF-enabled interfaces every 10

seconds for broadcast and point-to-point interfaces, and 30 seconds for nonbroadcast and point-to-multipoint interfaces.

OSPF also has a Dead Interval, which indicates how long a router will wait

without hearing any hellos before announcing a neighbor as “down.” Default

for the Dead Interval is 40 seconds for broadcast and point-to-point

interfaces, and 120 seconds for non-broadcast and point-to-multipoint

interfaces. Notice that, by default, the dead interval timer is four times the

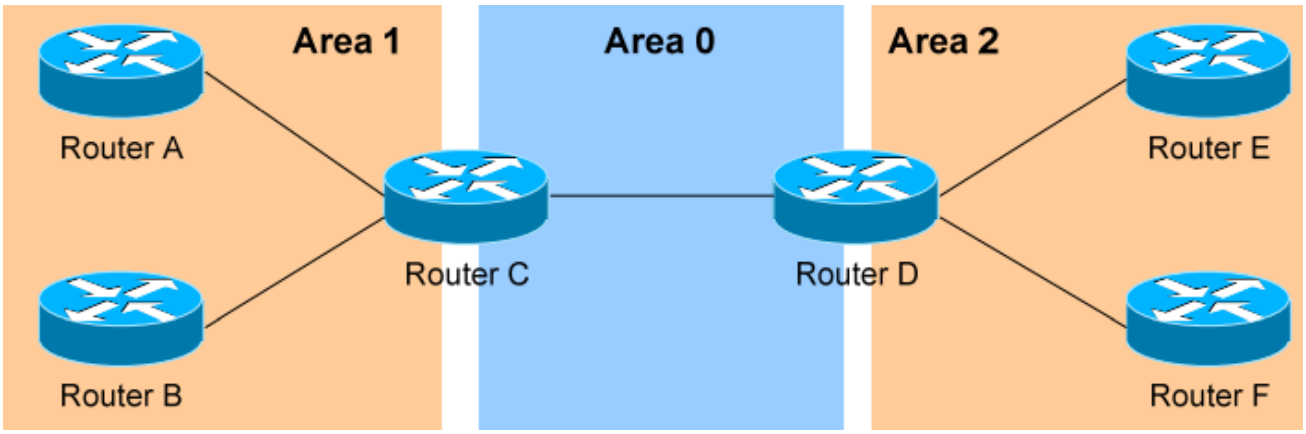
Hello interval.

These timers can be adjusted on a per interface basis:

Router(config-if)# ip ospf hello-interval 15

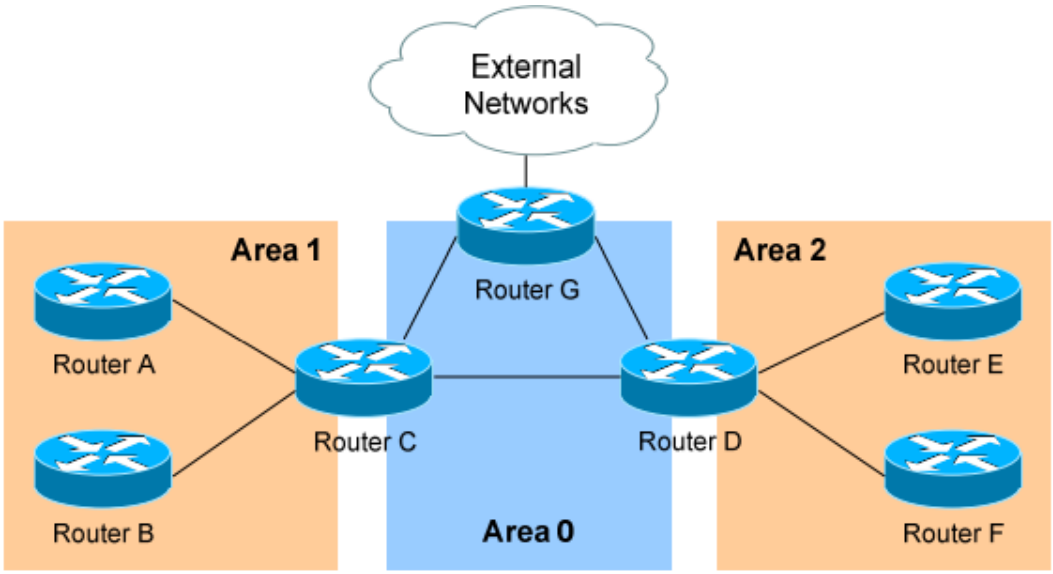
Router(config-if)# ip ospf dead-interval 60

5.1 THE OSPF HIERARCHY



OSPF is a hierarchical system that separates an Autonomous System into individual areas. OSPF traffic can either be intra-area (within one area), inter-area (between separate areas), or external (from another AS). OSPF routers build a Topology Database of all links within their area, and all routers within an area will have an identical topology database. Routing updates between these routers will only contain information about links local to their area. Limiting the topology database to include only the local area conserves bandwidth and reduces CPU loads. Area 0 is required for OSPF to function, and is considered the “Backbone” area. As a rule, all other areas must have a connection into Area 0, though this rule can be bypassed using virtual links (explained shortly). Area 0 is often referred to as the transit area to connect all other areas. OSPF routers can belong to multiple areas, and will thus contain separate Topology databases for each area. These routers are known as Area Border Routers (ABRs). Consider the above example. Three areas exist: Area 0, Area 1, and Area 2. Area 0, again, is the backbone area for this Autonomous System. Both Area 1 and Area 2 must directly connect to Area 0.

Routers A and B belong fully to Area 1, while Routers E and F belong fully to Area 2. These are known as Internal Routers. Router C belongs to both Area 0 and Area 1. Thus, it is an ABR. Because it has an interface in Area 0, it can also be considered a Backbone Router. The same can be said for Router D, as it belongs to both Area 0 and Area 2.



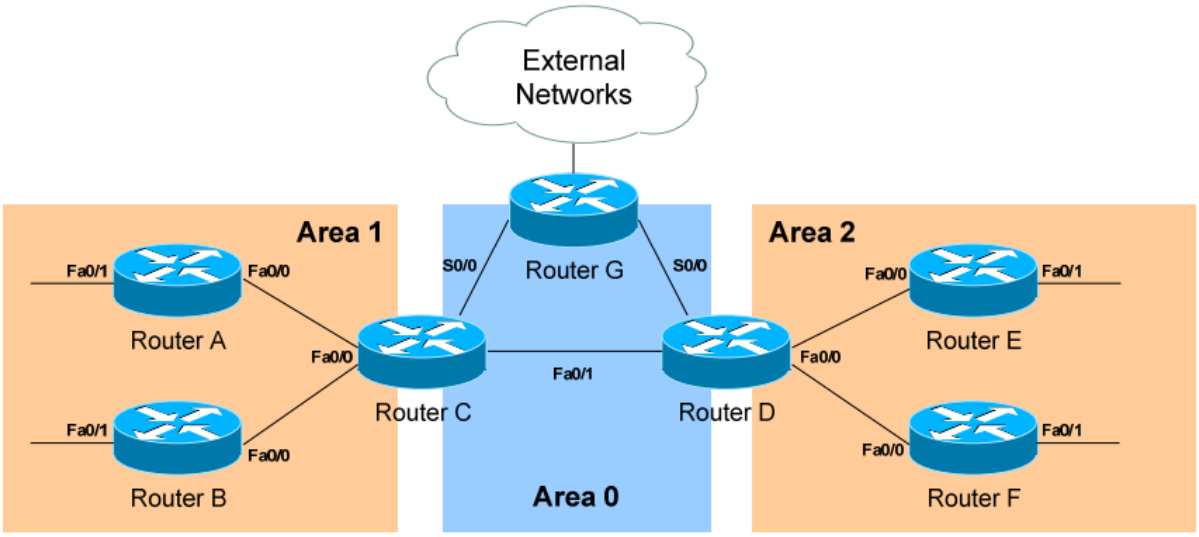
Now consider the above example. Router G has been added, which belongs to Area 0. However, Router G also has a connection to the Internet, which is outside this Autonomous System.
This makes Router G an Autonomous System Border Router (ASBR). A router can become an ASBR in one of two ways:

- By connecting to a separate Autonomous System, such as the Internet
- By redistributing another routing protocol into the OSPF process.

ASBRs provide access to external networks. OSPF defines two "types" of external routes:

- Type 2 (E2) – Includes only the external cost to the destination network. External cost is the metric being advertised from outside the OSPF domain. This is the default type assigned to external routes.
- Type 1 (E1) – Includes both the external cost, and the internal cost to reach the ASBR, to determine the total metric to reach the destination network. Type 1 routes are always preferred over Type 2 routes to the same destination. Thus, the four separate OSPF router types are as follows:
- Internal Routers – all router interfaces belong to only one Area.
- Area Border Routers (ABRs) – contains interfaces in at least two separate areas
- Backbone Routers – contain at least one interface in Area 0
- Autonomous System Border Routers (ASBRs) – contain a connection to a separate Autonomous System

5.2 LSAs & the OSPF Topology Database



Now consider the above example. Router G has been added, which belongs to Area 0. However, Router G also has a connection to the Internet, which is outside this Autonomous System. This makes Router G an Autonomous System Border Router (ASBR). A router can become an ASBR in one of two ways:

• By connecting to a separate Autonomous System, such as the Internet

• By redistributing another routing protocol into the OSPF process.

ASBRs provide access to external networks. OSPF defines two “types” of

external routes:

• Type 2 (E2) – Includes only the external cost to the destination network. External cost is the metric being advertised from outside the OSPF domain. This is the default type assigned to external routes.

• Type 1 (E1) – Includes both the external cost, and the internal cost to reach the ASBR, to determine the total metric to reach the destination network. Type 1 routes are always preferred over Type 2 routes to the same destination.

Thus, the four separate OSPF router types are as follows:

• Internal Routers – all router interfaces belong to only one Area.

• Area Border Routers (ABRs) – contains interfaces in at least two

separate areas

• Backbone Routers – contain at least one interface in Area 0

• Autonomous System Border Routers (ASBRs) – contain a

connection to a separate Autonomous System

OSPF, as a link-state routing protocol, does not rely on routing-by-rumor as RIP and IGRP do.

Instead, OSPF routers keep track of the status of links within their respective areas. A link is simply a router interface. From these lists of links and their respective statuses, the topology database is created. OSPF routers forward link-state advertisements (LSAs) to ensure the topology database is consistent on each router within an area.

Several LSA types exist:

• Router LSA (Type 1) – Contains a list of all links local to the router, and the status and "cost" of those links. Type 1 LSAs are generated by all routers in OSPF, and are flooded to all other routers within the local area.

• Network LSA (Type 2) – Generated by all Designated Routers in OSPF, and contains a list of all routers attached to the Designated Router.

• Network Summary LSA (Type 3) – Generated by all ABRs in OSPF, and contains a list of all destination networks within an area. Type 3 LSAs are sent between areas to allow inter-area communication to occur.

• ASBR Summary LSA (Type 4) – Generated by ABRs in OSPF, and contains a route to any ASBRs in the OSPF system. Type 4 LSAs are sent from an ABR into its local area, so that Internal routers know how to exit the Autonomous System.

• External LSA (Type 5) – Generated by ASBRs in OSPF, and contain routes to destination networks outside the local Autonomous System. Type 5 LSAs can also take the form of a default route to all networks outside the local AS. Type 5 LSAs are flooded to all areas in the OSPF system. Multicast OSPF (MOSPF) utilizes a Type 6 LSA, but that goes beyond the scope of this guide.

Later in this section, Type 7 NSSA External LSAs will be described in detail.

From the above example, the following can be determined:

• Routers A, B, E, and F are Internal Routers.

• Routers C and D are ABRs.

• Router G is an ASBR.

All routers will generate Router (Type 1) LSAs. For example, Router A will generate a Type 1 LSA that contains the status of links FastEthernet 0/0 and FastEthernet 0/1. This LSA will be flooded to all other routers in Area 1. Designated Routers will generate Network (Type 2) LSAs. For example, if Router C was elected the DR for the multi-access network in Area 1, it would generate a Type 2 LSA containing a list of all routers attached to it. Area Border Routers (ABRs) will generate Network Summary (Type 3) LSAs. For example, Router C is an ABR between Area 0 and Area 1. It will thus send Type 3 LSAs into both areas. Type 3 LSAs sent into Area 0 will contain a list of networks within Area 1, including costs to reach those networks. Type 3 LSAs sent into Area 1 will contain a list of networks within Area 0, and all other areas connected to Area 0. This allows Area 1 to reach any other area, and all other areas to reach Area 1. ABRs will also generate ASBR Summary (Type 4) LSAs. For example,

Router C will send Type 4 LSAs into Area 1 containing a route to the ASBR, thus providing routers in Area 1 with the path out of the Autonomous System. ASBRs will generate External (Type 5) LSAs. For example, Router G will generate Type 5 LSAs that contain routes to network outside the AS. These Type 5 LSAs will be flooded to routers of all areas.

Each type of LSA is propagated under three circumstances:

• When a new adjacency is formed.

• When a change occurs to the topology table.

• When an LSA reaches its maximum age (every 30 minutes, by

default). Thus, though OSPF is typically recognized to only send updates when a

change occurs, LSA's are still periodically refreshed every 30 minutes.

5.3 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.

5.3.1 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)

5.4 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.

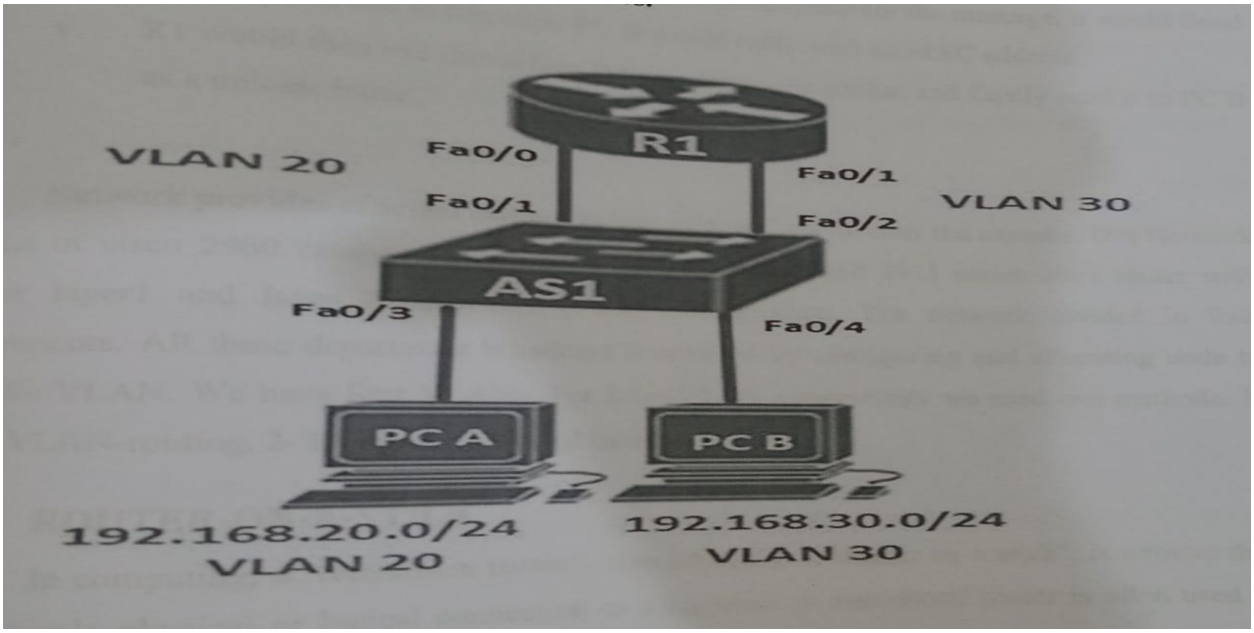


Figure 5.1 Traditional inter-vlan routing

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.

5.5 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

5.6 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

5.7 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 4321 series cisco router. The network divided in seven segments. All These segments. Broadcast is reduced by configuring and allocating node to specific VLAN. We have seven VLANS.

6.1. Network topology Diagram

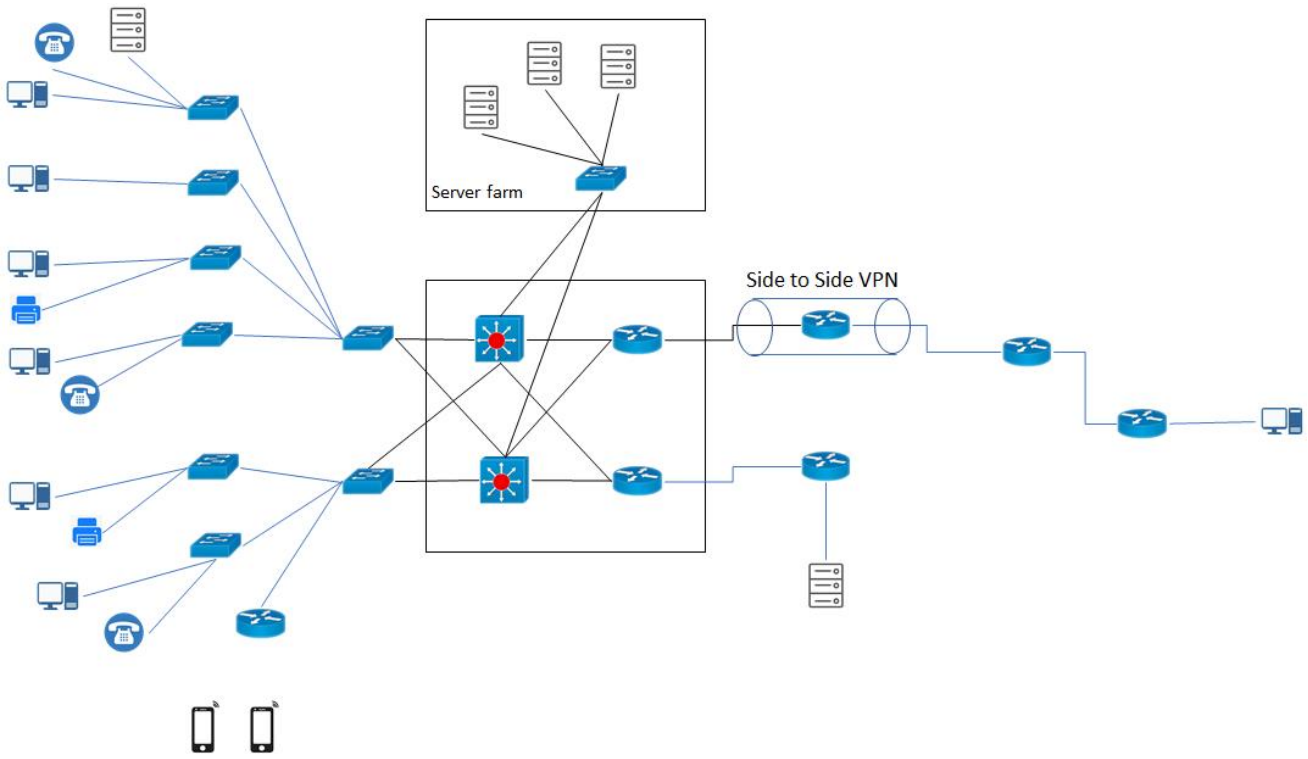
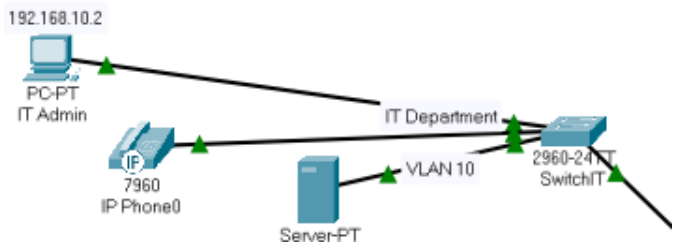


Figure 6.1 Network topology

6.2.1 Site-1 IT Department(VLAN 10)

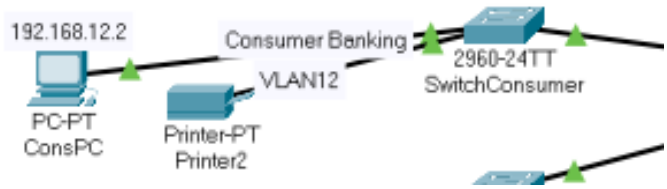


This site consists of 2 IT administrators, and 1 server. The default gateway got IT Department is 192.168.10.2. IT Department is using VLAN 10 to control access between the groups.

6.2.2 Site-2 ATM(VLAN 11)

As for site 2, this would be the ATM Department which consists 3 ATM and 1 Switch of ATM. ATM Department is using VLAN 11 to control access between the departments.

6.2.3 Site-3 Consumer Banking(VLAN 12)

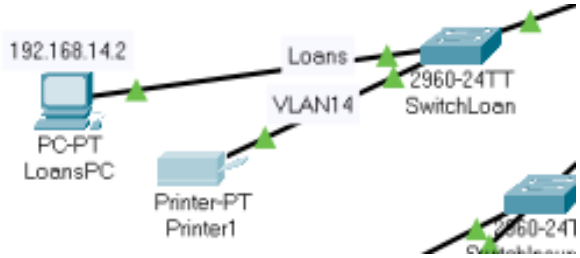


The figure above is the site dedicated for the Consumer Banking department. It consists 3 Consumer PC and 1 Switch for Consumer Department, and it's using VLAN 12 to control access between the departments.

6.2.4 Site-4 Investment Banking (VLAN 13)

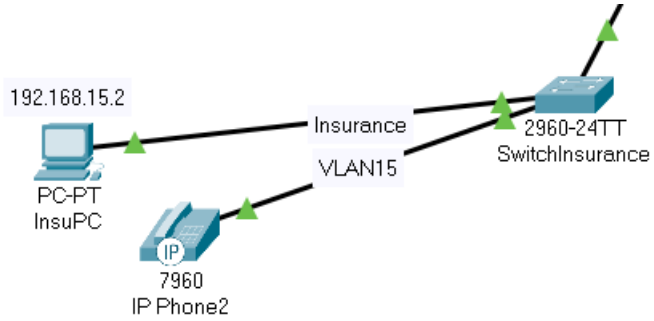
As for Site 4, This is Investment Banking which consists 3 PC of Investment and 1 switch for using VLAN 13 to control access between the department.

6.2.5 Site-5 Loans (VLAN 14)



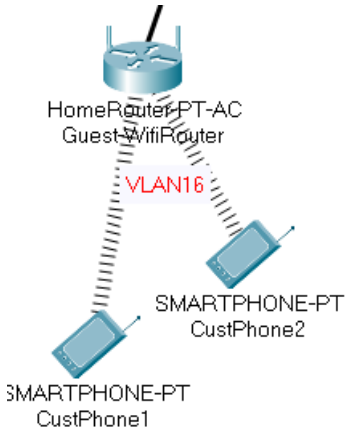
This Site 5 is for the Loans Department and its consists 3 Loans PC for staff and 1 switch for Loans Department. Its using VLAN 14 to control access between the departments.

6.2.6 Site-6 Insurance(VLAN 15)



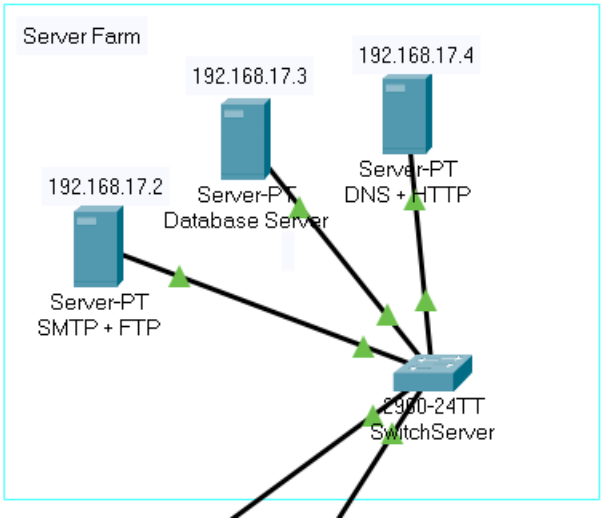
The figure above is the site dedicated for the Insurance department. It consists 3 Insurance PC for staff and 1 Switch for Insurance Department, and it's using VLAN 15 to control access between the departments.

6.2.7 Site-7 Guest-Wifi Router(VLAN 16)



As for Site 4, This is Guest Wifi Design which only consists 1 Wireless router and 1 example device of user for access into internet. Its using VLAN 16 that only allow users to access the internet.

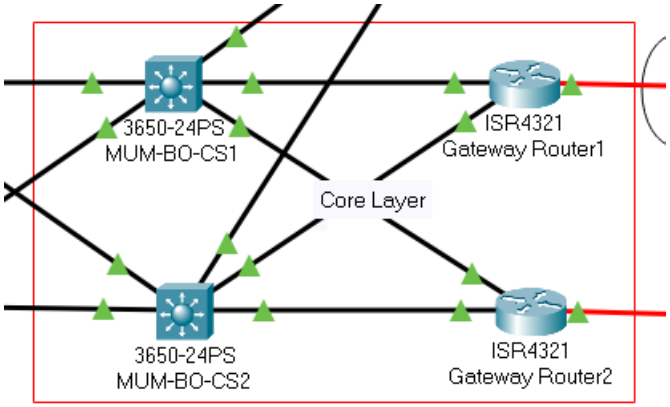
6.2.8 Site-8 Server Farm



Server Farm consist of 3 servers

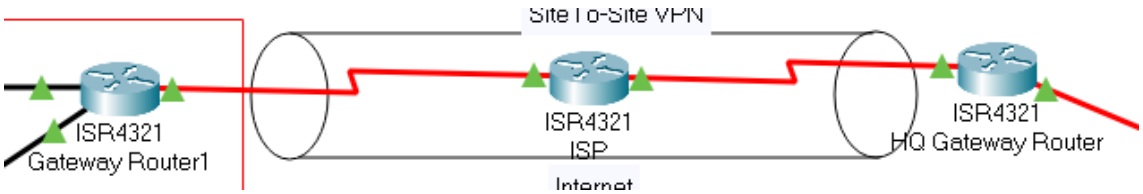
1) SMTP + FTP
2) Database Server
3) DNS + HTTP

6.2.9 Redudant Multi-Layer Switch/Router



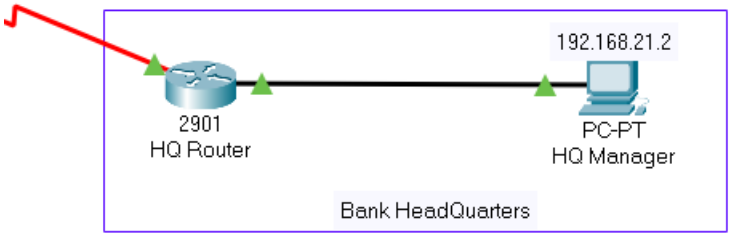
Series of Switch and Router are Configured in such a way so that if one goes down the other control the flow of network traffic.

6.2.10 Site-2-Site VPN



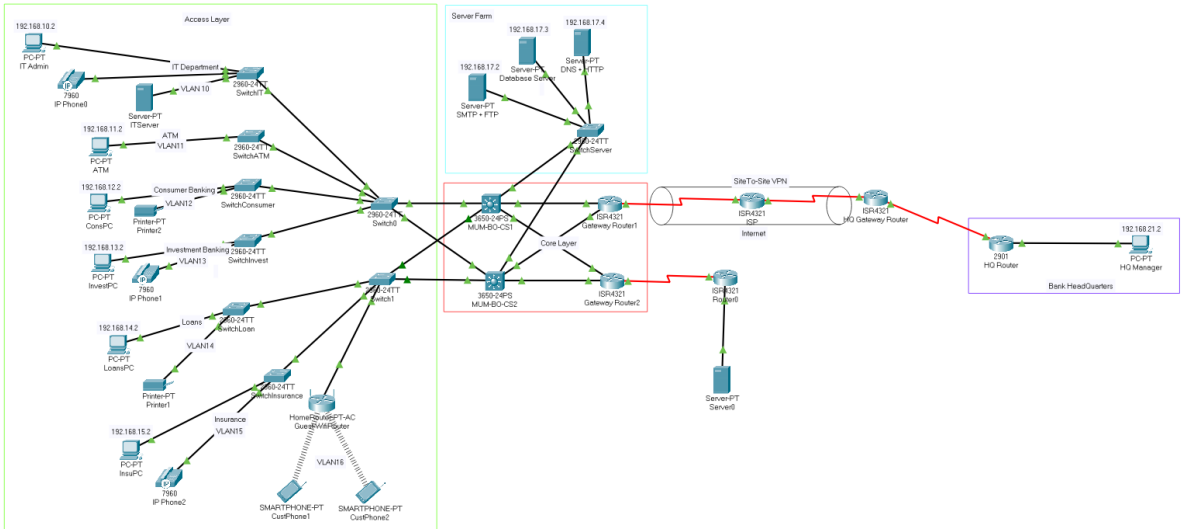
Site to Site VPN is configured and implemented from the Gateway Router to the HQ Gateway Router for Secured transmission of data packets.

6.2.11 HQ Bank



Bank HeadQuarters is added to the network design for site-2-site VPN demonstration purposes.

6.3 Design Snippet



CHAPTER-7

NETWORK DISASTER & RECOVERY PLANNING

A network disaster recovery plan includes a set of procedures required to effectively respond to a disaster that affects a network and causes its disruption. The main purpose of network disaster recovery is to ensure that services can be delivered to customers despite a disruption in network connectivity.

- **Back up network configuration files**

The main aim is to ensure that a network is restored to its normal state as rapidly as possible. That is why it is important to regularly back up network configuration files, including the initial parameters and settings for configuring network devices. Regarding this, you are advice to install third-party data protection software, which can be used to back up and recover critical data when your infrastructure is hit by a disaster.

- **Regularly test and update the plan**

By regularly testing and updating network disaster plans, it will reduce the chances of panicking when a network disaster occurs. IT recovery team will be more ready and prepared to deal with network disasters.

- **Assess potential risks and threats**

You also need to determine risks and threats which your organization is most exposed to that can disrupt your network services. After assessing potential dangers, you can come up with preventive measures to stop them from occurring to reduce the possible impact on your infrastructure.

- **Create an IT recovery team and assign responsibilities**

It is not enough to create a network disaster recovery plan; you should also decide who will implement the plan when an actual disaster strikes. So, by having an IT team recovery team will have the organization prepared for disaster recovery. Each recovery team member should be

assigned with a specific role and a unique set of responsibilities to avoid any confusion and panic during a disaster recovery event.

- **Document steps of the network disaster recovery process.**

By documenting the steps of the network disaster recovery process will avoid confusion when the actual network disaster occurs. By listing the document also helps identify the weakness of the infrastructure of the organization which indirectly reduce network disaster from occurring.

7.1 Objectives of Disaster Recovery Plan

To limit the extent of disruption and damage.

To minimize the economic impact of the interruption.

To establish an alternative means of operation in advance.

To train personnel with emergency procedures

7.2 Risk Assessments

- Identify Possible Threats A high-level risk assessment can still be done by involving the simplest network component where it can still pose a threat if it has an IP address on the network, stores any sensitive data, and/or allows users to access it over the network.

- Rate Each Risk and Impact Each risk is can be classified as low, medium or high risk. This helps to prioritize where you should focus most of your effort initially, and you work down your list to the medium and low-risk resources.

- Analyze Your Protection Firewalls and antivirus software installed on desktops. Analyze any cyber security protection in place, because it reduces risk. This step might affect your priority because you could have a high-priority item that already has the best protection. This type of resource would then be a lower priority.

7.3 Emergency Response Procedure

- Evaluate current plans, procedures and incident
- Identify hazards
- Emergency resources
- Review codes and regulations
- Training Programs
- Communication
- Write the plan

7.4 Recovery Response Procedure

Prevention

- Focuses on creating concrete plans, training, hazard response plans and exercises well ahead of a disaster to prepare your organization, through proactive planning

Preparedness

- A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action.

Mitigation

- Effort to reduce loss property by developing structural and non-structural measures that will mitigate the effects of a disaster

CHAPTER - 8

COMPONENTS & BOM

- CISCO ROUTERS
- MULTILAYER SWITCHES
- L2 SWITCHES
- PERSONAL COMPUTERS
- SERVERS
- PRINTERS
- HOME ROUTER
- IP TELEPHONES

Components	No. of Components	Total Cost
Multilayer Switch 3650-24PS	**2x**	**2,95,000**
Layer 2 Switch 2960-24TT	**9x**	**9,62,100**
Router 2911	**6x**	**20,45,230**
PC(Personal Computer):	**9x**	**2,15,618**
Servers	**5x**	**10,04,000**
Printer	**2x**	**20000**
IP Telephone	**3x**	**45000**
		43,53,330

CHAPTER – 9

REFERENCES

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

2. https://en.wikipedia.org/wiki/Wired_communication

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

16. https://www.webopedia.com