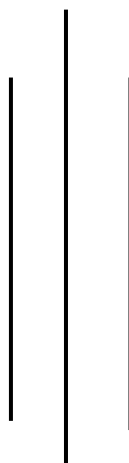


# COMPUTER SCIENCE AND MULTIMEDIA



## COLLEGE OF MANAGEMENT &IT

### BACHELOR IN COMPUTER SCIENCE



Enterprise Network Design for Leapfrog Tech

**FINAL YEAR PROJECT**

As part of The Degree BCS (Hons)

**Academic Year 2019**

College ID: udayaraj.subedi@texascollge.edu.np

Name: Udayaraj Subedi

LCID:LC00017000918

Project Supervisor: Suman Thapaliya

## Abstract

The main purpose of this project is to design a suitable network system for enterprise. Which help to provide high-quality security and availability of network. The device used in this project like firewall, router, switch, AP etc are connected with each other via ethernet/serial cable. This project introduces the high-quality network security. These security/ utilities are hardware firewalls, ACL, Port-security, SSH, Password on every mode of router and switch, password on every virtual interface as well as console, password on wireless AP etc. All of these security measures have been configured to provide the security and make a secure environment for the entire network and to prevent unauthorized to the organization network.

The protocol like STP, EtherChannel and FHRP will help to keep network up 24/7. There is different VLAN are created on switch, another most useful technology VTP is configured in my project which help system administrator to configure VLAN many switches. Port security and ACL provide security with in organization and firewall will help to filter traffic and protect from different attacks, virus, malware etc. the Network address translation will help us to mapping our private IP into Public IP. The technology like IPsec VPN will help us to get connect with a LAN from remote area in a secure way. The dynamic routing protocol like OSPF is used in this project to connect to different network and other many more technology would be used in this project which make this network fast and secure. The servers used for this network design are DHCP server and DNS servers. This presentation and design included additional components such as a web server, mail server, etc.

## Acknowledgement

I would like to express my gratitude to all who helped me directly or indirectly throughout the preparation of this document. Particularly I owe a deep sense of gratitude to my project supervisor Mr. **Suman Thapaliya** for providing his valuable guidelines. This is an indeed a great pleasure and honor submitting this document under his precious supervision.

I sincerely thank you our College Management for their guidelines and supervision during preparation of this report. I am highly obliged to university of our collage Lincoln university college for giving us the opportunity to create a project which can bring a big change in my life. I dedicate this acknowledgment to all our professors and members of our department who gave us knowledge, confidence and shared their ideas during our study in Texas Collage of Management and IT.

I am thankful to my friends with whom I have learned a lot, and last but not least I am very much thankful to my parents and families who gave me the confidence to believe in myself.

## Plagiarism Declaration

I confirm that the enclosed written work along with my topology and configuration is entirely my own. I also declare that whenever I had copied, paraphrased, summarized by providing full credit to the respective author. More than this if any other material, word, sentences found will be just a mistake. I had tried to be full open and honest.

# Table of Content

<b>Abstract.....</b>	<b>I</b>
<b>Acknowledgement .....</b>	<b>II</b>
<b>Plagiarism Declaration .....</b>	<b>II</b>
1.1 Introduction to Enterprise Network .....	1
1.2 Aim and Objective: .....	2
1.2.1 objective: .....	2
1.2.2 Aim: .....	2
1.3 Problem Definition.....	3
<b>Chapter 2: Introduction to Computer Network.....</b>	<b>5</b>
1.1 Computer Network.....	5
1.2 Networking Device .....	6
1.2.1 Modem .....	6
1.2.2 RJ45 Connector.....	6
1.2.3 Ethernet Card .....	6
1.2.4 Router.....	7
1.2.5 Switch.....	7
1.2.6 Firewall .....	7
1.2.7 Wi-Fi Card .....	7
1.3 Network Topology .....	8
1.3.1 Bus Topology:.....	8
1.3.2 Star Topology:.....	8
1.3.3 Ring Topology: .....	8
1.3.4 Tree Topology:.....	8
1.3.5 Mesh Topology: .....	9
<b>Chapter 3: Switching .....</b>	<b>12</b>
1.1 VLAN.....	12
1.1.1 Configure VLAN on L2 Switch.....	13
1.1.2 Assign Port on VLAN.....	14
1.1.3 Trunking.....	14

1.2 VTP Domain .....	15
1.3 EtherChannel.....	16
1.4 Switch Security: .....	18
1.4.1 Port Security.....	18
1.5 Spanning Tree Protocol.....	21
<b>Chapter 4: Routing .....</b>	<b>22</b>
1.1 Static routing .....	22
1.2 Default routing .....	24
1.3 Dynamic Routing .....	25
1.4 OSPF (Open Shortest Path First) .....	26
<b>Chapter 5: Firewall .....</b>	<b>28</b>
1.1 Introduction .....	28
1.2 Type of firewall.....	30
1.3 Working of Firewalls .....	32
1.4 Advantages of Network Firewall .....	32
<b>Chapter 6: Configuration .....</b>	<b>35</b>
6.1 Router Configuration.....	35
6.3 Switch Configuration .....	43
6.4 Firewall Configuration .....	49
<b>Chapter 7: Testing / Conclusion .....</b>	<b>53</b>
<b>Referance .....</b>	<b>58</b>

## Table of Figure

Figure 1: Topology.....	4
Figure 2: Basic Diagram Computer Network .....	5
Figure 3: OSI.....	9
Figure 4: VLAN .....	12
Figure 5: Configure VLAN on switch .....	13
Figure 6: Assign port on VLAN 10 .....	14
Figure 7: trunking.....	15
Figure 8: Configure VTP .....	15
Figure 9: EtherChannel .....	16
Figure 10: Etherchannel Configuration.....	17
Figure 11: Port Security .....	18
Figure 12: Portsecurity-Configuration .....	19
Figure 13: Spanning Tree Protocol .....	21
Figure 14: Basic topology for implement static route.....	23
Figure 15: Static Route Configuration .....	24
Figure 16: Default Routing .....	24
Figure 17: Dynamic routing.....	25
Figure 18 : Firewall Operation.....	28
Figure 19: Firewall Topology With DMZ .....	29

## **Chapter 1: Introduction**

### **1.1 Introduction to Enterprise Network**

An enterprise network is an enterprise's communication backbone that helps to connect computer and related devices across departments and workgroup networks, facilitating insight and data accessibility. An enterprise network reduces communication protocols, facilitating system and devices interoperability, as well as improved internal and external enterprise data network. An enterprise network is also known as corporate network. The key purpose of an enterprise network is to eliminate isolate users and workgroups all the system should be able to communicate and provide and retrieve satisfactory performance, reliability and security.

Enterprise computing models are developed for this purpose facilitating the exploration and improvement of established enterprise communication protocols and strategies. It includes local area network and wide area network, depending on operational and departmental requirement.

An enterprise network can integrate all the system include all device like smart phones and tablets and all operating system. A tightly integrated enterprise network effectively combines and uses different devices and system communication protocols.

## 1.2 Aim and Objective:

### 1.2.1 objective:

The major objective of this network design is to allow only the genuine users to access the network and prevent the intruders from accessing it. Reduce network failure by using technology like FHRP, STP and EtherChannel. Provide Security by using ACL, Port Security and Firewall. Fast resource sharing, highly available data and proper utilization of Devices and technology.

### 1.2.2 Aim:

The main scope of My project is to help to improve the network performance easy and fast to access data and provide security for enterprise network.

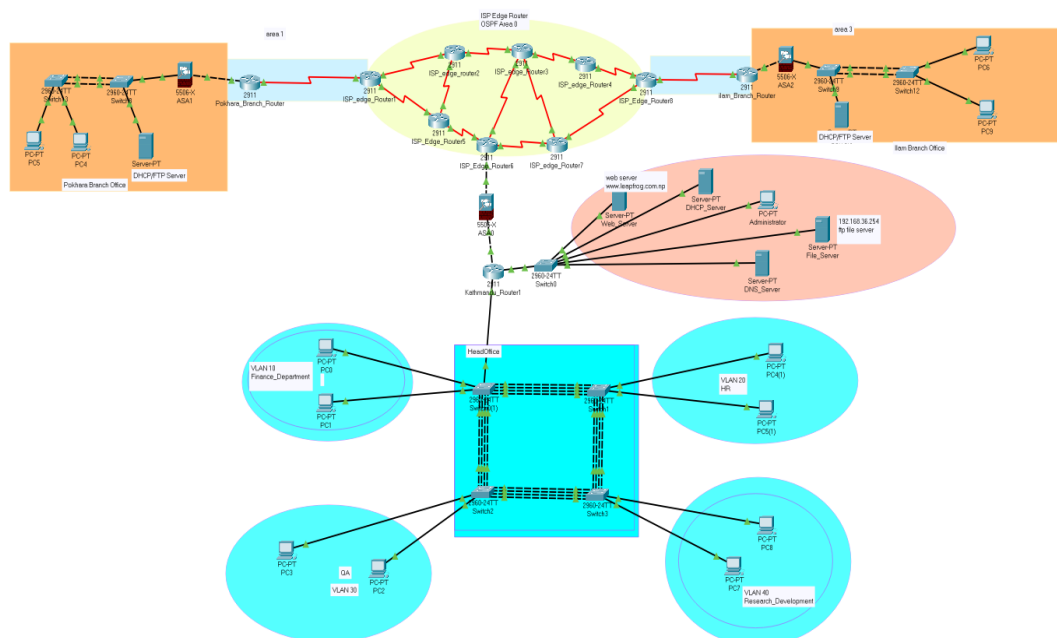
- a. Identifies all network resources and their required security.
- b. A solid security policy, Detect and monitor suspicious activity.
- c. Analyze network and maintain quality of service.
- d. Maintains redundant network and easily expandable network.



### 1.3 Problem Definition

There were many issues that have been solved technically. The first concern was security, the second concern was quality and the third concern was safety. In the security centered analysis, the enterprise network provides security services like packet filtering, access control list, port security, MAC flooding, ARP spoofing, DOS etc, so that may be some people who cannot be trusted to connect to the inside network. However, there are many technologies to prevent people who are planning terrorist attack from having access to the sensitive department in the network.

Improving the performance of any network needs a high quality of techniques and services that help to improve the general function of the network. Enterprise networks need to have a high quality of services that should be presented immediately in order to keep the network activities on track. In this section the quality of network services has been provided by new techniques to improve the quality of services. When network devices communicate with many other devices, the workload required of the CPUs on the devices can be burdensome. As such the modular nature of the hierarchical design model is to enable accurate capacity planning within each layer of the hierarchy, thus reducing wasted bandwidth. Network management responsibility and network management system should be distributed to the different layers of modular network architecture to control management costs.



*Figure 1: Topology*

## Chapter 2: Introduction to Computer Network

### 1.1 Computer Network

A computer network is a group of computer systems and other hardware computing devices connected through communication channels to enable communication between a wide range of users to share resources. In other word Computer network is interconnection of computing device that can able to exchange resources with each other. Different networking device like router, switch, AP, server etc. are connected with the help guided/unguided media. Every device follows the rules called communication protocol to transmit data and resources over physical or wireless technology. Each device on a network is connected with each other and they all are identify uniquely with the help of internet protocol address. (wiki, n.d.)

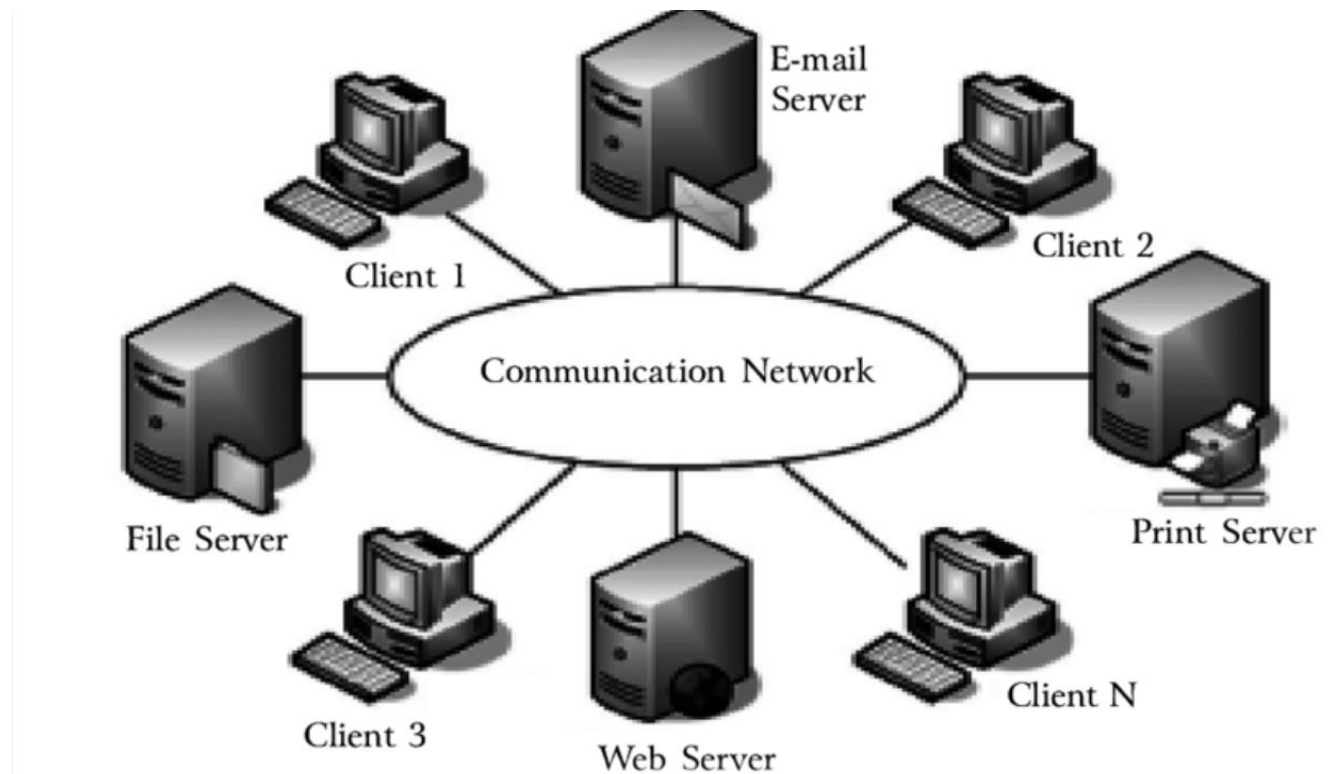


Figure 2: Basic Diagram Computer Network

## 1.2 Networking Device

Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called network devices. These devices transfer data in a fast, secure and correct way over same or different networks. Network devices may be inter-network or intra-network. Some devices are installed on the device, like NIC card or RJ45 connector, whereas some are part of the network, like router, switch, etc. Let us explore some of these devices in greater detail. (Melnick, 2019)

### 1.2.1 Modem

Modem is a device that enables a computer to send or receive data over telephone or cable lines. The data stored on the computer is digital whereas a telephone line or cable wire can transmit only analog data.

### 1.2.2 RJ45 Connector

RJ45 is the acronym for Registered Jack 45. RJ45 connector is an 8-pin jack used by devices to physically connect to Ethernet based local area networks (LANs). Ethernet is a technology that defines protocols for establishing a LAN. The cable used for Ethernet LANs are twisted pair ones and have RJ45 connector pins at both ends. These pins go into the corresponding socket on devices and connect the device to the network.

### 1.2.3 Ethernet Card

Ethernet card, also known as network interface card (NIC), is a hardware component used by computers to connect to Ethernet LAN and communicate with other devices on the LAN. The earliest Ethernet cards were external to the system and needed to be installed manually. In modern computer systems, it is an internal hardware component. The NIC has RJ45 socket where network cable is physically plugged in.

#### 1.2.4 Router

A router is a network layer hardware device that transmits data from one LAN to another if both networks support the same set of protocols. So a router is typically connected to at least two LANs and the internet service provider (ISP). It receives its data in the form of packets, which are data frames with their destination address added. Router also strengthens the signals before transmitting them. That is why it is also called repeater.

#### 1.2.5 Switch

Switch is a network device that connects other devices to Ethernet networks through twisted pair cables. It uses packet switching technique to receive, store and forward data packets on the network. The switch maintains a list of network addresses of all the devices connected to it. On receiving a packet, it checks the destination address and transmits the packet to the correct port. Before forwarding, the packets are checked for collision and other network errors. The data is transmitted in full duplex mode.

#### 1.2.6 Firewall

A firewall is a security device that helps us prevent unauthorized access. This is a set of rules that we define and protect ourselves from device abuse or get rid of the hacker somehow. There are two types of firewalls such as hardware and software firewall.

#### 1.2.7 Wi-Fi Card

Wi-Fi is the acronym for wireless fidelity. Wi-Fi technology is used to achieve wireless connection to any network. Wi-Fi card is a card used to connect any device to the local network wirelessly. The physical area of the network which provides internet access through Wi-Fi is called Wi-Fi hotspot. Hotspots can be set up at home, office or any public space. Hotspots themselves are connected to the network through wires.

### 1.3 Network Topology

Network topology refers to the geometric arrangement of links and nodes in a computing network. Alternately, network topology may describe how the data is transferred between these nodes. There are two types of network topologies: physical and logical. Physical topology emphasizes the physical layout of the connected devices and nodes, while the logical topology focuses on the pattern of data transfer between network nodes.

#### 1.3.1 Bus Topology:

All the devices/nodes are connected sequentially to the same backbone or transmission line. This is a simple, low-cost topology, but its single point of failure presents a risk.

#### 1.3.2 Star Topology:

All the nodes in the network are connected to a central device like a hub or switch via cables. Failure of individual nodes or cables does not necessarily create downtime in the network but the failure of a central device can. This topology is the most preferred and popular model.

#### 1.3.3 Ring Topology:

All network devices are connected sequentially to a backbone as in bus topology except that the backbone ends at the starting node, forming a ring. Ring topology shares many of bus topology's disadvantages so its use is limited to networks that demand high throughput.

#### 1.3.4 Tree Topology:

A root node is connected to two or more sub-level nodes, which themselves are connected hierarchically to sub-level nodes. Physically, the tree topology is similar to bus and star topologies; the network backbone may have a bus topology, while the low-level nodes connect using star topology.

### 1.3.5 Mesh Topology:

The topology in each node is directly connected to some or all the other nodes present in the network. This redundancy makes the network highly fault-tolerant but the escalated costs may limit this topology to highly critical networks.

## 1.4 OSI Reference Model

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s. The modern Internet is not based on OSI, but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.

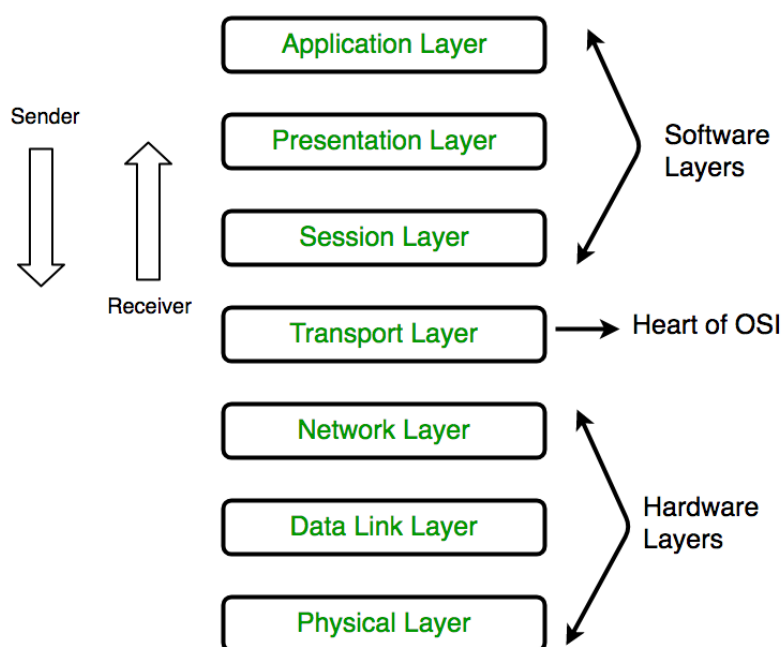


Figure 3: OSI

## 7. Application Layer

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

## 6. Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

## 5. Session Layer

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

## 4. Transport Layer

The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

## 3. Network Layer

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.



## 2. Data Link Layer

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

## 1. Physical Layer

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

## Chapter 3: Switching

### 1.1 VLAN

Virtual LANs (VLANs) provide segmentation and organizational flexibility in a switched network. A group of devices within a VLAN communicate as if each device was attached to the same cable. VLANs are based on logical connections, instead of physical connections. VLANs allow an administrator to segment networks based on factors such as function, team, or application, without regard for the physical location of the users or devices. Each VLAN is considered a separate logical network. Devices within a VLAN act as if they are in their own independent network, even if they share a common infrastructure with other VLANs. Any switch port can belong to a VLAN.

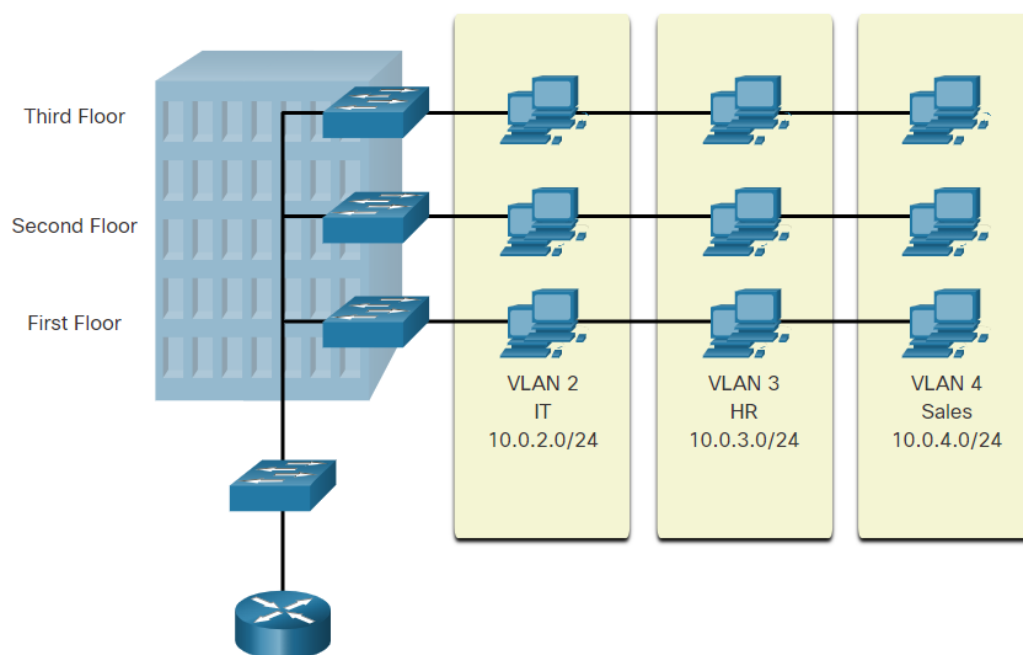


Figure 4: VLAN

### 1.1.1 Configure VLAN on L2 Switch

To configure VLAN we have to access the console of switch. Here we are using packet tracer so I am going to open packet tracer and access the console of packet tracer and in order to create VLAN I am going to follow the following commands:

```
Switch>enable
```

```
Switch# configure terminal
```

```
Switch(config)# VLAN 10
```

```
Switch(config-vlan)# name VLAN10
```

```
Switch(config-vlan)#end
```

To verify we can go back to privileges mode and hit following command

```
Switch# show VLAN brief
```

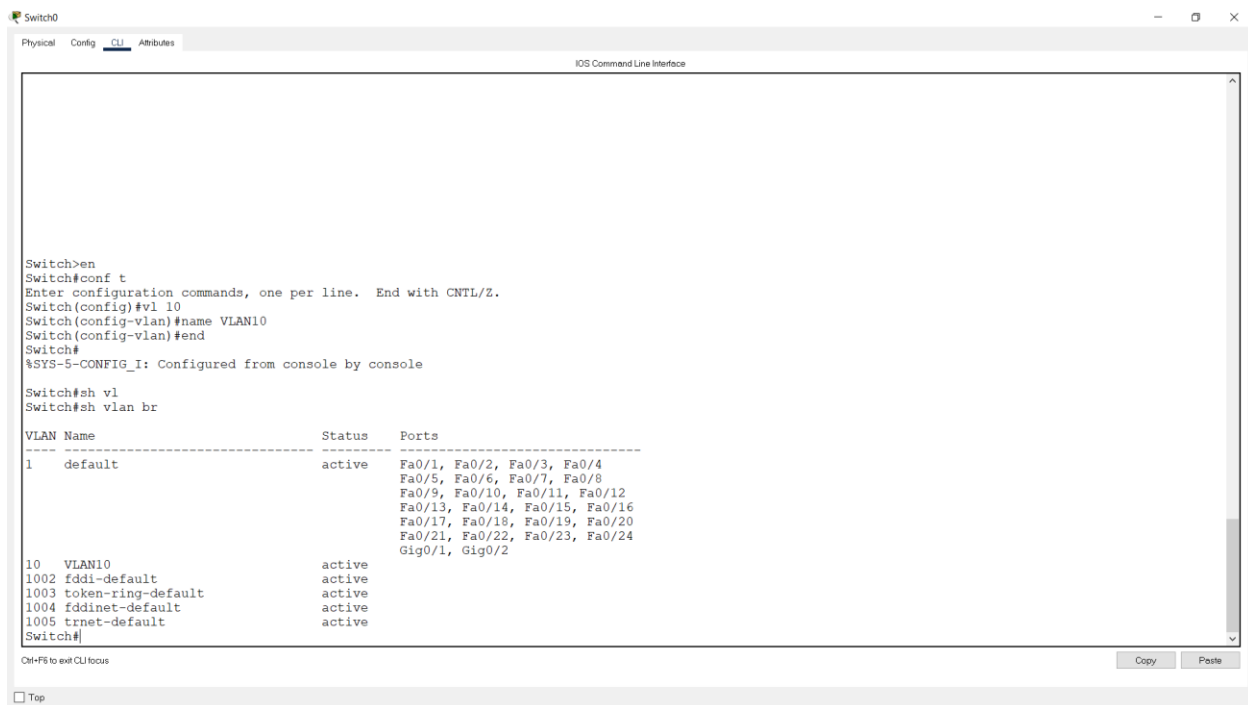


Figure 5: Configure VLAN on switch

### 1.1.2 Assign Port on VLAN

The VLAN is created on switch but if we connect pc with switch then the pc still connected with VLAN 1 which is default VLAN that can not be delete or edit. We have to assign each port on specific VLAN. Here just for example I am going to assign fastEthernet 0/10 port with VLAN 10. To do so we have to follow the following command:--

```
Switch# configure terminal
```

```
Switch(config)# interface fa0/10
```

```
Switch(config-if)# switchport mode access
```

```
Switch(config-if)# switchport access VLAN 10
```

Now fa0/10 is assigned to VLAN 10. We can verify it by fire command show VLAN brief from privilege mode

```
Switch# show vl br
```

```
Switch(config)#int range fastEthernet 0/1-10
Switch(config-if-range)#sw
Switch(config-if-range)#switchport ma
Switch(config-if-range)#switchport mo
Switch(config-if-range)#switchport mode ac
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#sw
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#do sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10	VLAN10	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10
1002	fdi-default	active	
1003	token-ring-default	active	
1004	fdiinet-default	active	
1005	trnet-default	active	

```
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#
```

Figure 6: Assign port on VLAN 10

### 1.1.3 Trunking

Let's assume we have two switch. Each switch have VLAN 10. If switch 1 VLAN 10 want to communicated with switch 2 VLAN 10 then they will not communicate without making the link trunk. We have to go to that interface to which two switch are connected and fire following commands:

```
S1(config)#interface fa0/0
```

```
S1(config-if)# switchport mode trunk
```

```
S2(config)#interface f0/0
```

```
S2(config-if)# switchport mode trunk
```

```
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#int fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
```

*Figure 7: trunking*

## 1.2 VTP Domain

A enterprise network has many switch. Creating VLAN on every switch one by one is bit work overhead and hard to manage for network engineering so network engineer use vtp to create VLAN on multiple switch from one switch. We create a vtp domain on one switch set its password and set the mode as server. And we have to go to other switch, simply add the vtp domain and password, set mode as client and boom, We do not have to create VLAN on that switch. But make sure the link between vtp server switch and vtp client switch is in trunking mode. Lets see how It is done in cisco switch:

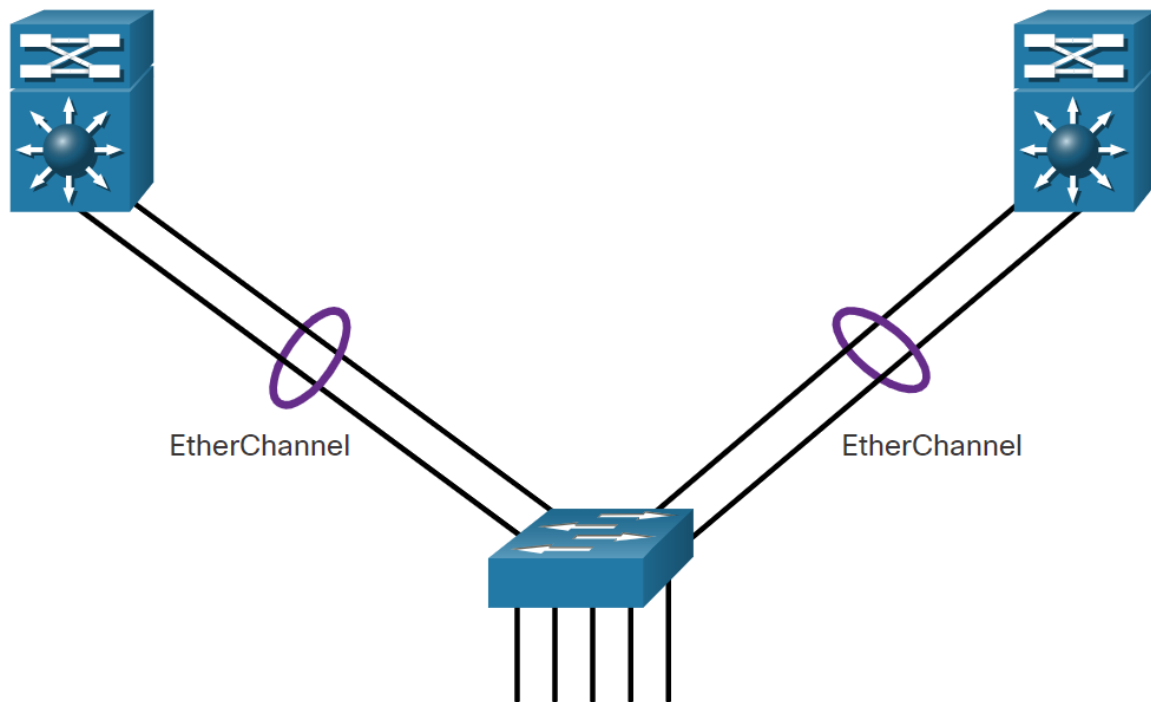
```
VTP_Server(config)#
VTP_Server(config)#
VTP_Server(config)#
VTP_Server(config)#vtp domain vtpserver
Domain name already set to vtpserver.
VTP_Server(config)#vtp password cisco
Password already set to cisco
VTP_Server(config)#vtp mode client
Device mode already VTP CLIENT.
VTP_Server(config)#
```

*Figure 8: Configure VTP*

```
VTP_Client(config)#
VTP_Client(config)#
VTP_Client(config)#
VTP_Client(config)#vtp domain vtpserver
Domain name already set to vtpserver.
VTP_Client(config)#vtp password
% Incomplete command.
VTP_Client(config)#vtp password cisco
Password already set to cisco
VTP_Client(config)#vtp mode client
Device mode already VTP CLIENT.
VTP_Client(config)#
```

### 1.3 EtherChannel

EtherChannel aggregates links between devices into bundles. These bundles include redundant links. STP may block one of those links, but it will not block all of them. With EtherChannel your network can have redundancy, loop prevention, and increased bandwidth. EtherChannel technology was originally developed by Cisco as a LAN switch-to-switch technique of grouping several Fast Ethernet or Gigabit Ethernet ports into one logical channel. When an EtherChannel is configured, the resulting virtual interface is called a port channel. The physical interfaces are bundled together into a port channel interface, as shown in the figure.



*Figure 9: EtherChannel*

```
Switch-1#  
Switch-1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch-1(config)#interface range fastethernet 0/1-4  
Switch-1(config-if-range)#channel-group 1 mode auto  
Switch-1(config-if-range)#  
Switch-1(config-if-range)#do wr  
Building configuration...  
[OK]  
Switch-1(config-if-range)#
```

---

```
Switch-2(config)#  
Switch-2(config)#  
Switch-2(config)#  
Switch-2(config)#interface range fastethernet 0/1-4  
Switch-2(config-if-range)#channel-group 1 mode desi  
Switch-2(config-if-range)#channel-group 1 mode desirable  
Switch-2(config-if-range)#do wr  
Building configuration...  
[OK]  
Switch-2(config-if-range)#
```

---

*Figure 10: Etherchannel Configuration*

## 1.4 Switch Security:

An important part of your responsibility as a network professional is to stay the network secure. Most of the time we only consider security attacks coming from outside the network, but threats can come from within the network in addition. These threats can range anywhere from an employee innocently adding an Ethernet switch to the company network so that they can have more ports, to malicious attacks caused by a disgruntled employee. It's your job to stay the network safe and ensuring that business operations continue uncompromised.

### 1.4.1 Port Security

Port security limits the amount of valid MAC addresses allowed on a port. It allows an administrator to manually configure MAC addresses for a port or to allow the switch to dynamically learn a limited number of MAC addresses. When a port configured with port security receives a frame, the source MAC address of the frame is compared to the list of secure source MAC addresses that were manually configured or dynamically learned on the port.

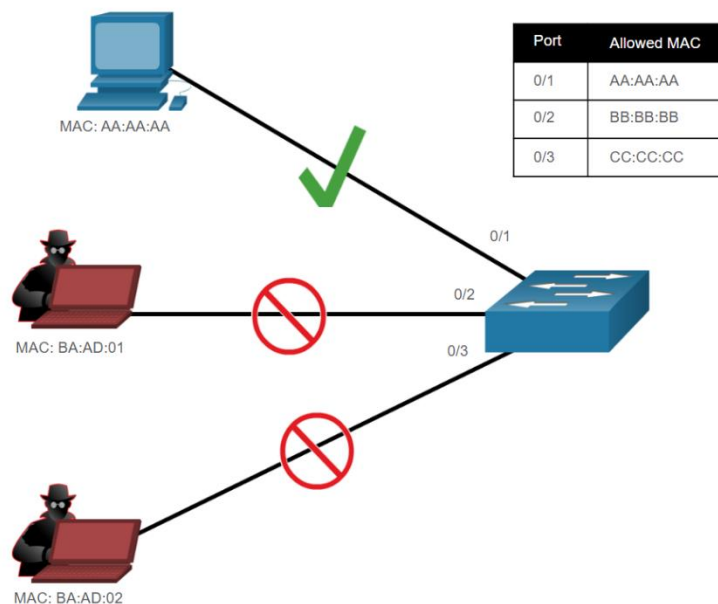


Figure 11: Port Security



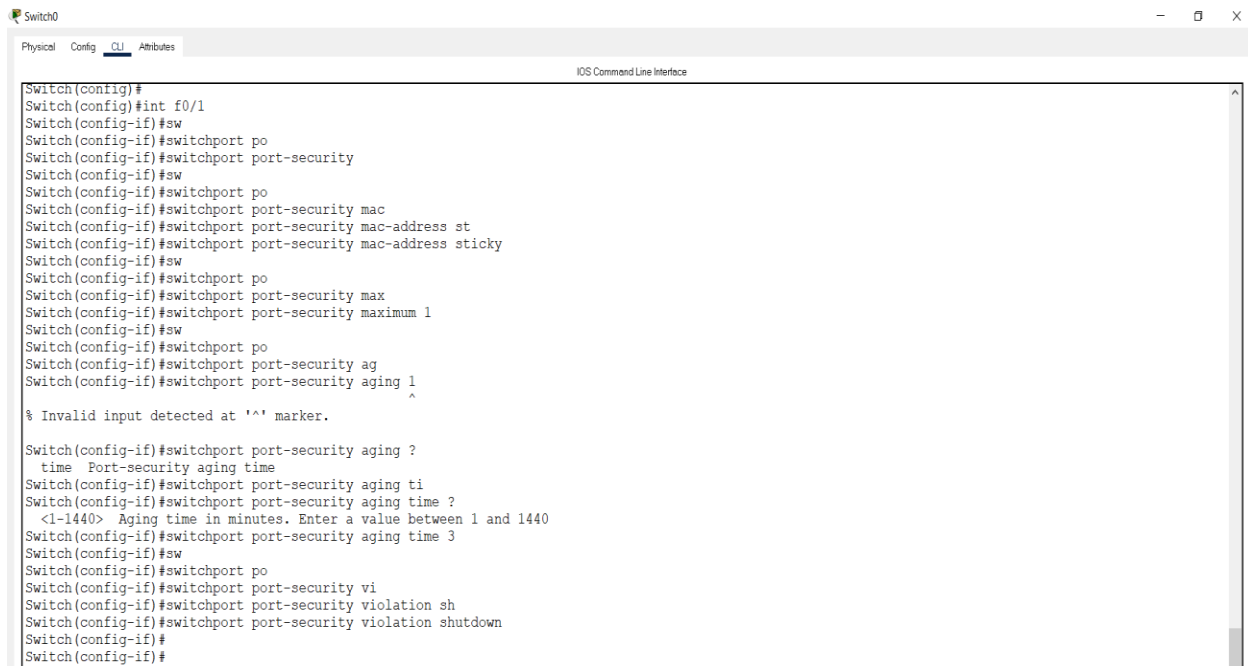


Figure 12: Portsecurity-Configuration

### 1.4.2 Mitigate VLAN attack

A VLAN hopping attack can be launched in one of three ways:

- a. Spoofing DTP messages from the attacking host to cause the switch to enter trunking mode. From here, the attacker can send traffic tagged with the target VLAN, and the switch then delivers the packets to the destination.
- b. Introducing a rogue switch and enabling trunking. The attacker can then access all the VLANs on the victim switch from the rogue switch.
- c. Another type of VLAN hopping attack is a double-tagging (or double-encapsulated) attack. This attack takes advantage of the way hardware on most switches operate.

Use the following steps to mitigate VLAN hopping attacks:

Step 1: Disable DTP (auto trunking) negotiations on non-trunking ports by using the switchport mode access interface configuration command.

Step 2: Disable unused ports and put them in an unused VLAN.

Step 3: Manually enable the trunk link on a trunking port by using the switchport mode trunk command.

Step 4: Disable DTP (auto trunking) negotiations on trunking ports by using the switchport nonegotiate command.

Step 5: Set the native VLAN to a VLAN other than VLAN 1 by using the switchport trunk native vlan vlan\_number command.

### 1.4.3 DHCP Mitigate Attack

The goal of a DHCP starvation attack is to create a Denial of Service (DoS) for connecting clients. DHCP starvation attacks require an attack tool such as Gobbler. Recall that DHCP starvation attacks can be effectively mitigated by using port security because Gobbler uses a unique source MAC address for each DHCP request sent. However, mitigating DHCP spoofing attacks requires more protection. Gobbler could be configured to use the actual interface MAC address as the source Ethernet address, but specify a different Ethernet address in the DHCP payload. This would render port security ineffective because the source MAC address would be legitimate. Use the following steps to enable DHCP snooping:

Step 1. Enable DHCP snooping by using the IPDHCP snooping global configuration command.

Step 2. On trusted ports, use the IPDHCP snooping trust interface configuration command.

Step 3. Limit the number of DHCP discovery messages that can be received per second on untrusted ports by using the IPDHCP snooping limit rate interface configuration command.

Step 4. Enable DHCP snooping by VLAN, or by a range of VLANs, by using the IPDHCP snooping vlan global configuration command.

## 1.5 Spanning Tree Protocol

Spanning Tree Protocol (STP) is a loop-prevention network protocol that allows for redundancy while creating a loop-free Layer 2 topology. IEEE 802.1D is the original IEEE MAC Bridging standard for STP.

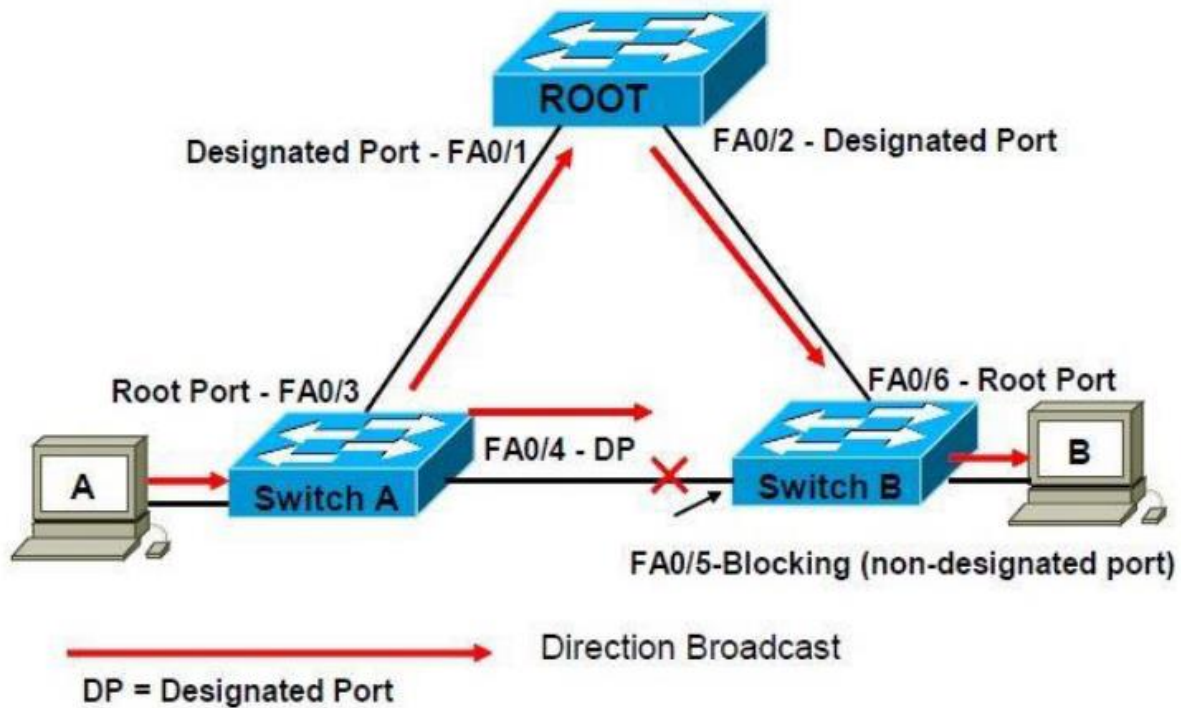


Figure 13: Spanning Tree Protocol

## Chapter 4: Routing

A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router. Router works at the network layer in the OSI model and internet layer in TCP/IP model. It is a networking device that forwards the packet based on the information available in the packet header and forwarding table. The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted. The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination. The routing algorithm initializes and maintains the routing table for the process of path determination.

### 1.1 Static routing

Static routing is a process in which we have to manually add routes to the routing table.

Advantages –

- No routing overhead for router CPU which means a cheaper router can be used to do routing.
- It adds security because an only administrator can allow routing to particular networks only.
- No bandwidth usage between routers.

Disadvantage –

- For a large network, it is a hectic task for administrators to manually add each route for the network in the routing table on each router.
- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology

## Configuration static routing

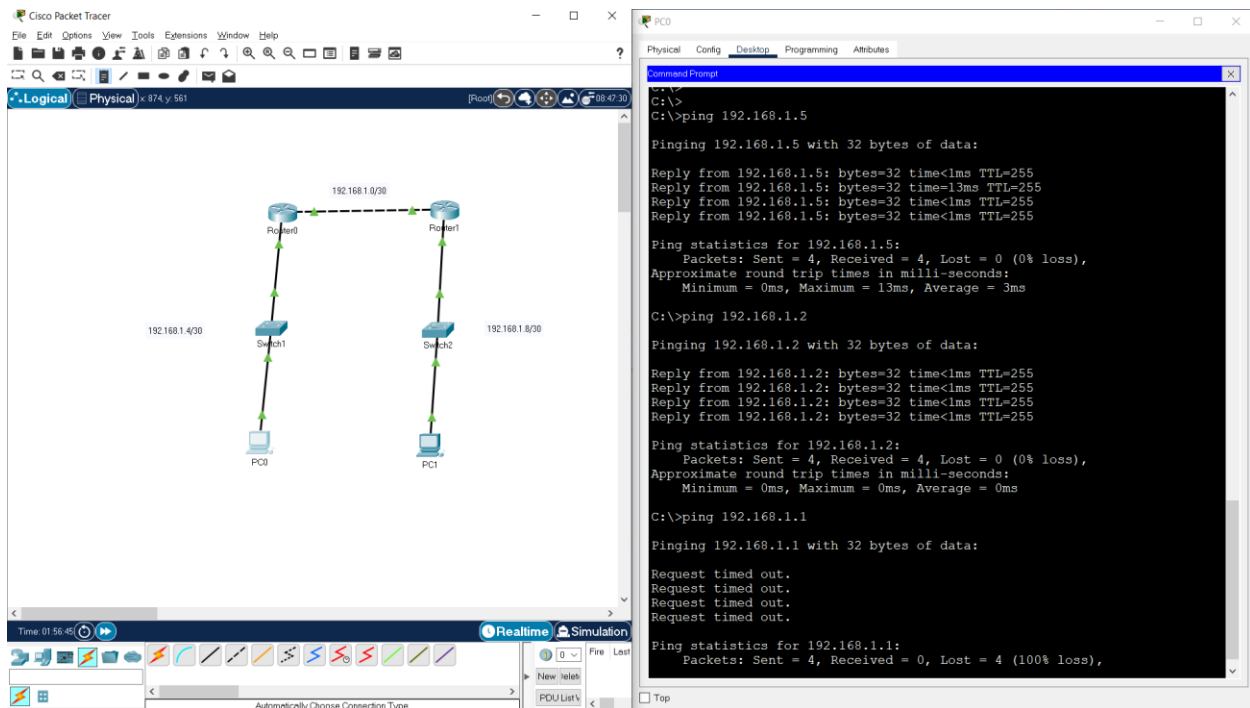


Figure 14: Basic topology for implement static route

Here pc 0 can only ping directly connected network. Here 192.168.1.1 is not directly connected with pc 0 so we have to add route to reach that network.

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.1.8 255.255.255.252 192.168.1.1
Router(config)#
  
```

```

Router2(config)#ip route 192.168.1.4 255.255.255.252 192.168.1.2
Router2(config)#
  
```

```

-----
Router#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

    1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    C       1.1.1.0/30 is directly connected, GigabitEthernet0/0
    L       1.1.1.1/32 is directly connected, GigabitEthernet0/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
    C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
    L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
    O       192.168.2.0/24 [110/2] via 1.1.1.2, 00:02:11, GigabitEthernet0/0

```

Figure 15: Static Route Configuration

## 1.2 Default routing

This is the method where the router is configured to send all packets towards a single router (next hop). It doesn't matter to which network the packet belongs, it is forwarded out to the router which is configured for default routing. It is generally used with stub routers. A stub router is a router that has only one route to reach all other networks.

### Configuration:

```

Router>
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.1
Router(config)#sh ip route
      ^
% Invalid input detected at '^' marker.

Router(config)#do sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

```

Figure 16: Default Routing

### 1.3 Dynamic Routing

Dynamic routing is known as a technique of finding the best path for the data to travel over a network in this process a router can transmit data through various different routes and reach its destination on the basis of conditions at that time of communication circuits. Dynamic routers are smart enough to take the best path for data based on the condition of the present scenario at that time of the network. In case one section fails in the network to transfer data forward dynamic router will use its algorithm (in which they use routing protocols to gather and share information of the current path among them) and it will re-route the previous network over another network in real-time. And this amazing capability and functionality to change paths in real-time over the network by sharing status among them is the key functionality of Dynamic Routing. OSPF (open shortest path first) and RIP are some protocols used for dynamic routing.

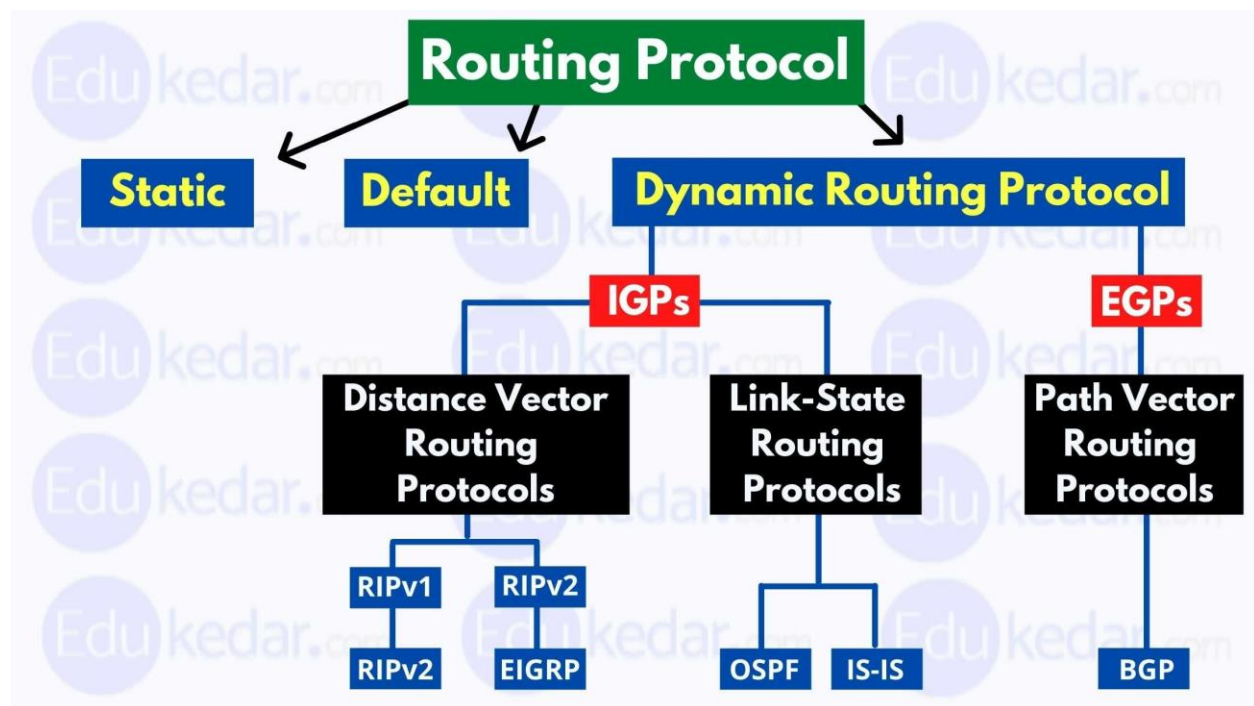


Figure 17: Dynamic routing

## 1.4 OSPF (Open Shortest Path First)

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 of 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:

- 2 A neighbor table – contains a list of all neighboring routers.
- 3 A topology table – contains a list of all possible routes to all known networks within an area.
- 4 A routing table – contains the best route for each known network.

## Chapter 5: Firewall

### 1.1 Introduction

A firewall is one of the most effective security tools available for protecting users from external threats. A firewall protects computers and networks by preventing undesirable traffic from entering internal networks.

Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access. For example, the top topology in the figure illustrates how the firewall enables traffic from an internal network host to exit the network and return to the inside network. The bottom topology illustrates how traffic initiated by the outside network (i.e., the internet) is denied access to the internal network. (cisco, n.d.)

### Firewall Operation

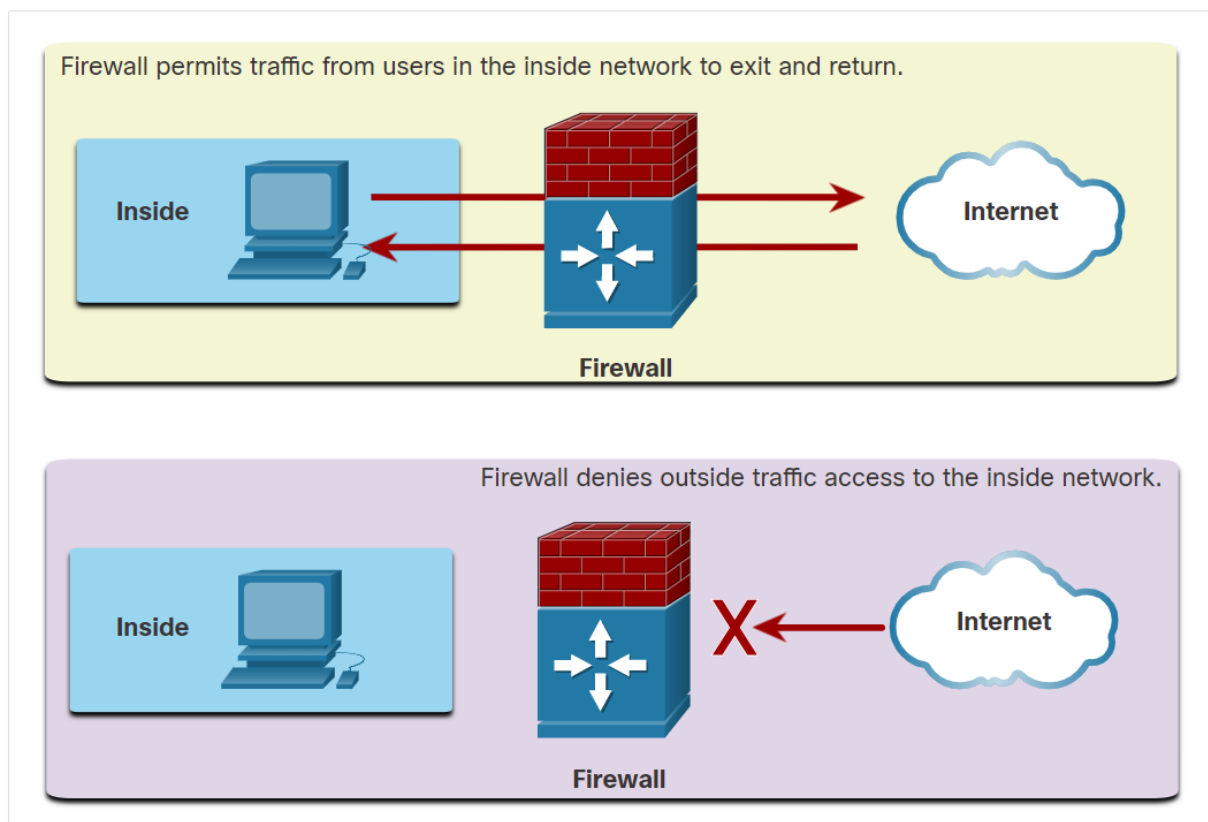
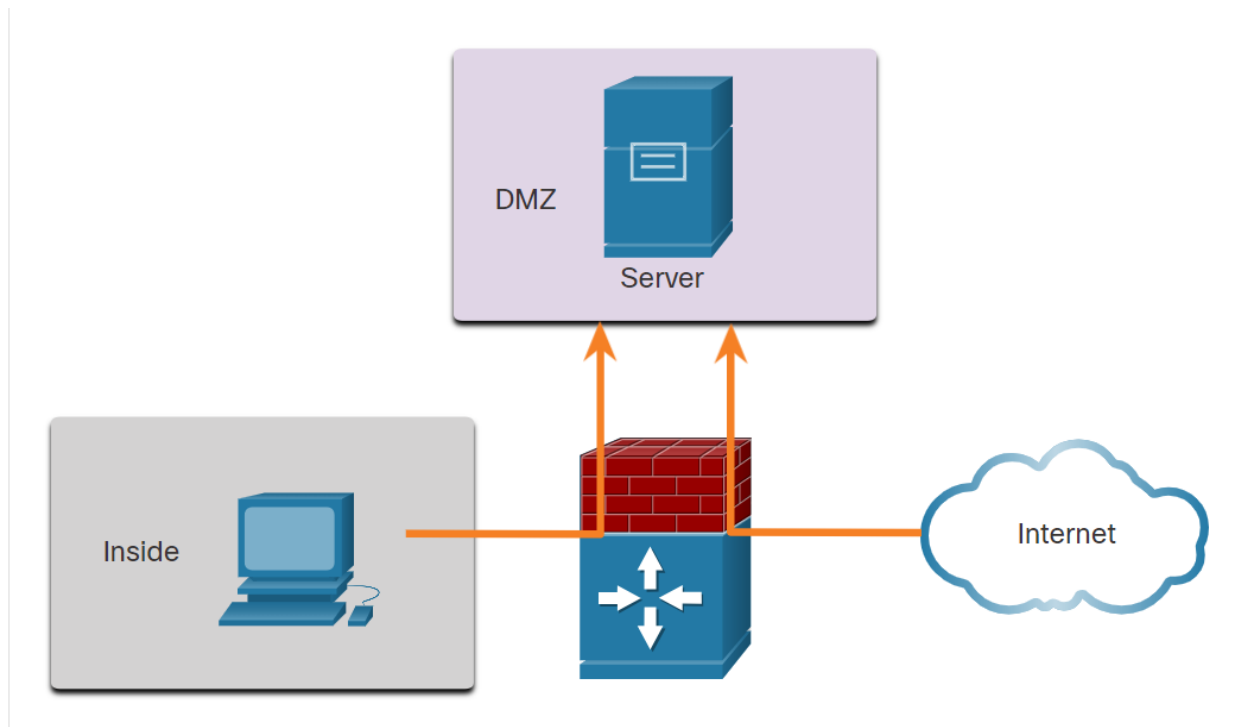


Figure 18 : Firewall Operation

A firewall could allow outside users-controlled access to specific services. For example, servers accessible to outside users are usually located on a special network referred to as the demilitarized zone (DMZ), as shown in the figure. The DMZ enables a network administrator to apply specific policies for hosts connected to that network.



*Figure 19: Firewall Topology With DMZ*

## 1.2 Type of firewall

Firewall products come packaged in various forms. These products use different techniques for determining what will be permitted or denied access to a network. They include the following: (geeksforgeeks, 2021)

### 1. Packet Filters

It is a technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols, and ports. This firewall is also known as a static firewall.

### 2. Stateful Inspection Firewalls –

It is also a type of packet filtering which is used to control how data packets move through a firewall. It is also called dynamic packet filtering. These firewalls can inspect that if the packet belongs to a particular session or not. It only permits communication if and only if, the session is perfectly established between two endpoints else it will block the communication.

### 3. Application Layer Firewalls –

These firewalls can examine application layer (of OSI model) information like an HTTP request. If finds some suspicious application that can be responsible for harming our network or that is not safe for our network then it gets blocked right away.

### 4. Next-generation Firewalls –

These firewalls are called intelligent firewalls. These firewalls can perform all the tasks that are performed by the other types of firewalls that we learned previously but on top of that, it includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.

## 5. Circuit-level gateways –

A circuit-level gateway is a firewall that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security and works between an Open Systems Interconnection (OSI) network model's transport and application layers such as the session layer.

## 6. Software Firewall –

The software firewall is a type of computer software that runs on our computers. It protects our system from any external attacks such as unauthorized access, malicious attacks, etc. by notifying us about the danger that can occur if we open a particular mail or if we try to open a website that is not secure.

## 7. Hardware Firewall –

A hardware firewall is a physical appliance that is deployed to enforce a network boundary. All network links crossing this boundary pass-through this firewall, which enables it to perform an inspection of both inbound and outbound network traffic and enforce access controls and other security policies.

## 8. Cloud Firewall –

These are software-based, cloud-deployed network devices. This cloud-based firewall protects a private network from any unwanted access. Unlike traditional firewalls, a cloud firewall filters data at the cloud level.

## 1.3 Working of Firewalls

Firewalls can control and cover the quantum of incoming or outgoing traffic of our network. The data that comes to our network is in the forms of packets (a small unit of data), it's tough to identify whether the packet is safe for our network or not, this gives a great chance to the hackers and interferers to bombard our networks with colorful contagions, malware, spam, etc.

A network firewall applies a certain set of rules on the incoming and gregarious network traffic to examine whether they align with those rules or not. If it matches – also the business will be allowed to pass through your network. If it doesn't match – also the firewall will block the business. This way, the network remains safe and secure. (geeksforgeeks, 2021)

## 1.4 Advantages of Network Firewall

### 1. Monitor network traffic:

A network firewall observer and analyzes traffic by examining whether the traffic or packets passing through our network is safe for our network or not. By doing so, it keeps our network down from any vicious content that can harm our network.

### 2. Halt Hacking

In a society where everyone is connected to technology, it becomes more important to keep firewalls in our network and use the internet safely.

### 3. Stops viruses

Viruses can come from anywhere, similar as from an insecure website, from a spam communication, or any trouble, so it becomes more important to have a strong defense system (i.e. firewall in this case), a contagion attack can fluently shut off a whole network. In such a situation, a firewall plays a vital part.

#### 4. More security

still, contagion-free, spam-free terrain so network firewall will give better security to our network, if it's about monitoring and assaying the network from time to time and establishing a malware-free.

#### 5. Increase privacy

By guarding the network and furnishing better security, we get a network that can be trusted.

### 1.5 Disadvantages of Network Firewall

#### 1. Cost:

Depending on the type of firewall, it can be expensive, generally, the tackle firewalls are more expensive than the software ones.

#### 2. Restricts Users:

Restricts users can be a disadvantage for large associations, because of its tough security medium. A firewall can circumscribe the workers to do a certain operation indeed though it's a necessary operation.

#### 3. Issues with the speed of the network:

Since the firewalls have to cover every packet passing through the network, this can decelerate down operations demanded to be performed, or it can simply lead to decelerating down the network.

#### 4. Maintenance:

Firewalls bear nonstop updates and maintenance with every change in the networking technology. As the development of new contagions is adding continuously that can damage your system.



## Chapter 6: Configuration

In this chapter I am going to configure the topology. Each step and all the configuration done in topology are documented in this chapter.

### 6.1 Router Configuration

#### 1. Pokhara Branch Router

##### 1.1 Configure router name, banner and console password

```
Router(config)# hostname Pokhara_Branch_Router
Pokhara_Branch_Router(config)# line console 0
Pokhara_Branch_Router(config-line)# password cisco
Pokhara_Branch_Router(config-line)# login
Pokhara_Branch_Router(config-line)# motd-banner #Unauthorized access prohibited#
Pokhara_Branch_Router(config)# enable password cisco
```

##### 1.2 Assign IP address on interface.

Pokhara_Branch_Router	Gig0/1	10.10.0.0	10.10.0.1	255.255.0.0
Pokhara_Branch_Router	Gig0/0	100.10.1.148/30	100.10.1.149	255.255.255.252

Interface gigabitether 0/0 is connected with firewall of Pokhara branch and serial interface is connected with ISP.

##### 1.3 Command to configure ip address

```
Pokhara_Branch_Router(config)# interface <interface name>
Pokhara_Branch_Router(config-if)# ip address <ip address> <subnet mask>
```

### 1.3 Configuring static route toward firewall

```
Pokhara_Branch_Router(config)# ip route 10.10.0.0 255.255.0.0 100.10.1.150
```

## 2. ISP Edge Router 1

### 2.1 Configure router name, banner and console password

```
Router(config)# hostname ISP_Edge_Router1
ISP_Edge_Router1(config)# line console 0
ISP_Edge_Router1(config-line)# password cisco
ISP_Edge_Router1(config-line)# login
ISP_Edge_Router1(config-line)# motd-banner #Unauthorized access prohibited#
ISP_Edge_Router1(config)# enable password cisco
```

### 2.2 Assign IP address on interface

ISP_Edge_Router1	Se0/1/0	100.10.1.0/30	100.10.1.2	255.255.255.252
ISP_Edge_Router1	Se0/2/0	100.10.1.4/30	100.10.1.5	255.255.255.252
ISP_Edge_Router1	Se0/1/1	100.10.1.8/30	100.10.1.9	255.255.255.252

### 2.3 Command to configure ip address

```
ISP_Edge_Router1(config)# interface <interface name>
ISP_Edge_Router1(config-if)# ip address <ip address> <subnet mask>
```

### 1.2 Configuring OSPF

```
ISP_Edge_Router1(config)# router ospf 1
ISP_Edge_Router1(config-router)# network 100.10.1.4 0.0.0.3 area 0
ISP_Edge_Router1(config-router)# network 100.10.1.0 0.0.0.3 area 1
ISP_Edge_Router1(config-router)# network 100.10.1.8 0.0.0.3 area 0
```

## 3. ISP Edge Router 2

### 3.1 Configure router name, banner and console password

```
Router(config)# hostname ISP_Edge_Router2
ISP_Edge_Router2(config)# line console 0
ISP_Edge_Router2(config-line)# password cisco
ISP_Edge_Router2(config-line)# login
ISP_Edge_Router2(config-line)# motd-banner #Unauthorized access prohibited#
ISP_Edge_Router2(config)# enable password cisco
```

### 3.2 Assign ip address on interface

ISP_Edge_Router2	Se0/2/1	100.10.1.4/30	100.10.1.6	255.255.255.252
ISP_Edge_Router2	Se0/1/1	100.10.1.12/30	100.10.1.13	255.255.255.252
ISP_Edge_Router2	Se0/1/0	100.10.1.16/30	100.10.1.17	255.255.255.252

### 2.3 Command to configure ip address

```
ISP_Edge_Router2(config)# interface <interface name>
ISP_Edge_Router2(config-if)# ip address <ip address> <subnet mask>
```

### 1.2 Configuring OSPF

```
ISP_Edge_Router2(config)# router ospf 1
ISP_Edge_Router2(config-router)# network 100.10.1.12 0.0.0.3 area 0
ISP_Edge_Router2(config-router)# network 100.10.1.16 0.0.0.3 area 0
ISP_Edge_Router2(config-router)# network 100.10.1.4 0.0.0.3 area 0
```

## 4. ISP Edge Router 3

### 4.1 Configure router name, banner and console password

```
Router(config)# hostname ISP_Edge_Router3
ISP_Edge_Router3(config)# line console 0
ISP_Edge_Router3(config-line)# password cisco
ISP_Edge_Router3(config-line)# login
ISP_Edge_Router3(config-line)# motd-banner #Unauthorized access prohibited#
ISP_Edge_Router3(config)# enable password cisco
```

#### 4.2 Assigning IP address on interface

ISP_Edge_Router3	Se0/1/0	100.10.1.12/30	100.10.1.14	255.255.255.252
ISP_Edge_Router3	Se0/1/1	100.10.1.20/30	100.10.1.21	255.255.255.252
ISP_Edge_Router3	Se0/2/1	100.10.1.24/30	100.10.1.25	255.255.255.252
ISP_Edge_Router3	Se0/2/0	100.10.1.28/30	100.10.1.29	255.255.255.252

#### 4.3 Command to configure ip address

```
ISP_Edge_Router3(config)# interface <interface name>
```

```
ISP_Edge_Router3(config-if)# ip address <ip address> <subnet mask>
```

#### 4.4 Configuring OSPF

```
ISP_Edge_Router3(config)# router ospf 1
```

```
ISP_Edge_Router3(config-router)# network 100.10.1.12 0.0.0.3 area 0
```

```
ISP_Edge_Router3(config-router)# network 100.10.1.20 0.0.0.3 area 0
```

```
ISP_Edge_Router3(config-router)# network 100.10.1.24 0.0.0.3 area 0
```

```
ISP_Edge_Router3(config-router)# network 100.10.1.28 0.0.0.3 area 0
```

### 5. ISP Edge Router 4

#### 5.1 Configure router name, banner and console password

```
Router(config)# hostname ISP_Edge_Router4
```

```
ISP_Edge_Router4(config)# line console 0
```

```
ISP_Edge_Router4(config-line)# password cisco
```

```
ISP_Edge_Router4(config-line)# login
```

```
ISP_Edge_Router4(config-line)# motd-banner #Unauthorized access prohibited#
```

```
ISP_Edge_Router4(config)# enable password cisco
```

#### 5.2 Assign IP Address on Interface

ISP_Edge_Router4	Se0/1/0	100.10.1.20/30	100.10.1.22	255.255.255.252
ISP_Edge_Router4	Se0/1/1	100.10.1.32/30	100.10.1.33	255.255.255.252

### 5.3 Command to configure ip address

```
ISP_Edge_Router4(config)# interface <interface name>
```

```
ISP_Edge_Router4(config-if)# ip address <ip address> <subnet mask>
```

### 5.4 Configuring OSPF

```
ISP_Edge_Router4(config)# router ospf 1
```

```
ISP_Edge_Router4(config-router)# network 100.10.1.32 0.0.0.3 area 0
```

```
ISP_Edge_Router4(config-router)# network 100.10.1.20 0.0.0.3 area 0
```

## 6. ISP Edge Router 5

### 6.1 Configure router name, banner and console password

```
Router(config)# hostname ISP_Edge_Router4
```

```
ISP_Edge_Router5(config)# line console 0
```

```
ISP_Edge_Router5(config-line)# password cisco
```

```
ISP_Edge_Router5(config-line)# login
```

```
ISP_Edge_Router5(config-line)# motd-banner #Unauthorized access prohibited#
```

```
ISP_Edge_Router5(config)# enable password cisco
```

### 6.2 Assign IP address on interface

ISP_Edge_Router5	Se0/1/0	100.10.1.8/30	100.10.1.10	255.255.255.252
ISP_Edge_Router5	Se0/1/1	100.10.1.16/30	100.10.1.18	255.255.255.252
ISP_Edge_Router5	Se0/2/0	100.10.1.120/30	100.10.1.121	255.255.255.252

### 6.3 Command to configure ip address

```
ISP_Edge_Router5(config)# interface <interface name>
```

```
ISP_Edge_Router5(config-if)# ip address <ip address> <subnet mask>
```

### 6.4 Configuring OSPF

```
ISP_Edge_Router5(config)# router ospf 1
```

```
ISP_Edge_Router5(config-router)# network 100.10.1.8 0.0.0.3 area 0
```

```
ISP_Edge_Router5(config-router)# network 100.10.1.16 0.0.0.3 area 0
```

```
ISP_Edge_Router5(config-router)# network 100.10.1.120 0.0.0.3 area 0
```

## 7. ISP Edge Router 6

### 7.1 Configure router name, banner and console password

```
Router(config)# hostname ISP_Edge_Router4
```

```
ISP_Edge_Router6(config)# line console 0
```

```
ISP_Edge_Router6(config-line)# password cisco
```

```
ISP_Edge_Router6(config-line)# login
```

```
ISP_Edge_Router6(config-line)# motd-banner #Unauthorized access prohibited#
```

```
ISP_Edge_Router6(config)# enable password cisco
```

### 7.2 Assign IP address on interface.

ISP_Edge_Router6	Se0/2/1	100.10.1.36/30	100.10.1.38	255.255.255.252
ISP_Edge_Router6	Se0/1/1	100.10.1.40/30	100.10.1.41	255.255.255.252
ISP_Edge_Router6	Se0/2/0	100.10.1.28/30	100.10.1.30	255.255.255.252
ISP_Edge_Router6	Se0/1/0	100.10.1.48/30	100.10.1.49	255.255.255.252

### 6.3 Command to configure ip address

```
ISP_Edge_Router6(config)# interface <interface name>
```

```
ISP_Edge_Router6(config-if)# ip address <ip address> <subnet mask>
```

### 6.4 Configuring OSPF

```
ISP_Edge_Router6(config)# router ospf 1
```

```
ISP_Edge_Router6(config-router)# network 100.10.1.48 0.0.0.3 area 0
```

```
ISP_Edge_Router6(config-router)# network 100.10.1.36 0.0.0.3 area 0
```

```
ISP_Edge_Router6(config-router)# network 100.10.1.40 0.0.0.3 area 0
```

```
ISP_Edge_Router6(config-router)# network 100.10.1.28 0.0.0.3 area 0
```

## 7. ISP Edge Router 7

### 7.1 Configure router name, banner and console password

```
Router(config)# hostname ISP_Edge_Router4
```

```
ISP_Edge_Router7(config)# line console 0
ISP_Edge_Router7(config-line)# password cisco
ISP_Edge_Router7(config-line)# login
ISP_Edge_Router7(config-line)# motd-banner #Unauthorized access prohibited#
ISP_Edge_Router7(config)# enable password cisco
```

## 7.2 Assign IP address on interface.

ISP_Edge_Router7	Se0/1/1	100.10.1.48/30	100.10.1.50	255.255.255.252
ISP_Edge_Router7	Se0/2/0	100.10.1.24/30	100.10.1.26	255.255.255.252
ISP_Edge_Router7	Se0/2/1	100.10.1.52/30	100.10.1.53	255.255.255.252
ISP_Edge_Router7	Se0/1/0	100.10.1.56/30	100.10.1.57	255.255.255.252

## 7.3 Command to configure ip address

```
ISP_Edge_Router7(config)# interface <interface name>
ISP_Edge_Router7(config-if)# ip address <ip address> <subnet mask>
```

## 7.4 Configuring OSPF

```
ISP_Edge_Router7(config)# router ospf 1
ISP_Edge_Router7(config-router)# network 100.10.1.52 0.0.0.3 area 0
ISP_Edge_Router7(config-router)# network 100.10.1.56 0.0.0.3 area 0
ISP_Edge_Router7(config-router)# network 100.10.1.48 0.0.0.3 area 0
ISP_Edge_Router7(config-router)# network 100.10.1.24 0.0.0.3 area 0
```

## 8. ISP Edge Router 8

### 8.1 Configure router name, banner and console password

```
Router(config)# hostname ISP_Edge_Router4
ISP_Edge_Router8(config)# line console 0
ISP_Edge_Router8(config-line)# password cisco
ISP_Edge_Router8(config-line)# login
```

```
ISP_Edge_Router8(config-line)# motd-banner #Unauthorized access prohibited#
```

```
ISP_Edge_Router8(config)# enable password cisco
```

## 8.2 Assign IP address on interface.

ISP_Edge_Router8	Se0/1/0	100.10.1.32/30	100.10.1.34	255.255.255.252
ISP_Edge_Router8	Se0/2/1	100.10.1.60/30	100.10.1.61	255.255.255.252
ISP_Edge_Router8	Se0/1/1	100.10.1.56/30	100.10.1.58	255.255.255.252

## 8.3 Command to configure ip address

```
ISP_Edge_Router8(config)# interface <interface name>
```

```
ISP_Edge_Router8(config-if)# ip address <ip address> <subnet mask>
```

## 8.4 Configuring OSPF

```
ISP_Edge_Router8(config)# router ospf 1
```

```
ISP_Edge_Router8(config-router)# network 100.10.1.32 0.0.0.3 area 0
```

```
ISP_Edge_Router8(config-router)# network 100.10.1.56 0.0.0.3 area 0
```

```
ISP_Edge_Router8(config-router)# network 100.10.1.60 0.0.0.3 area 0
```



## 6.3 Switch Configuration

### 1 Switch-1

#### 1.1 Basic Configuration

```
Switch(config)# hostname Switch-1
Switch-1(config)# line console 0
Switch-1(config-line)# password cisco
Switch-1(config-line)# login
Switch-1(config-line)# motd-banner #Unauthorized access prohibited#
Switch-1(config)# enable password cisco
```

#### 1.2 Creating VLANs

```
Switch-1(config)# vlan 10
Switch-1(config-vlan)# name Developer_Department
```

```
Switch-1(config)# vlan 20
Switch-1(config-vlan)# name Account_Department
```

```
Switch-1(config)# vlan 30
Switch-1(config-vlan)# name HR_Department
```

```
Switch-1(config)# vlan 40
Switch-1(config-vlan)# name Business_Department
```

#### 1.3 Assigning Interface on vlan

```
Switch-1(config)# interface range fastethernet 0/10-20
Switch-1(config)# switchport mode access
Switch-1(config)# switchport access vlan 10
```

#### 1.4 configure EtherChannel

```
Switch-1(config)# interface range fastethernet 0/1-4
Switch-1(config-if)# channel-group 1 mode desirable
Switch-1(config)# interface range fastethernet 0/5-8
Switch-1(config-if)# channel-group 2 mode desirable
```

#### 1.5 Configure Trunking

```
Switch-1(config)# interface port-channel 1
Switch-1(config-if)# switchport mode trunk
```

```
Switch-1(config)#int fastethernet 0/9  
Switch-1(config-if)#switchport mode trunk
```

### 1.6 Configuring Port Security

```
Switch-1(config)# interface range fastethernet 0/10-20  
Switch-1(config-if)# switchport port-security  
Switch-1(config-if)# switchport port-security violation shutdown  
Switch-1(config-if)# switchport port-security mac-address sticky  
Switch-1(config-if)# switchport port-security maximum 1
```

### 1.7 Configure Spanning Tree Protocol

```
Switch-1(config)# spanning-tree mode rapid-pvst  
Switch-1(config)# spanning-tree vlan 10 root primary
```

## 2 Switch-2

### 2.1 Basic Configuration

```
Switch(config)# hostname Switch-2  
Switch-2(config)# line console 0  
Switch-2(config-line)# password cisco  
Switch-2(config-line)# login  
Switch-2(config-line)# motd-banner #Unauthorized access prohibited#  
Switch-2(config)# enable password cisco
```

### 2.2 Creating VLANs

```
Switch-2(config)# vlan 10  
Switch-2(config-vlan)# name Developer_Department
```

```
Switch-2(config)# vlan 20  
Switch-2(config-vlan)# name Account_Department
```

```
Switch-2(config)# vlan 30  
Switch-2(config-vlan)# name HR_Department
```

```
Switch-2(config)# vlan 40
```

```
Switch-2(config-vlan)# name Business_Department
```

### 2.3 Assigning Interface on vlan

```
Switch-2(config)# interface range fastethernet 0/10-20
```

```
Switch-2(config)# switchport mode access
```

```
Switch-2(config)# switchport access vlan 20
```

### 2.4 configure EtherChannel

```
Switch-2(config)# interface range fastethernet 0/1-4
```

```
Switch-2(config-if)# channel-group 1 mode auto
```

```
Switch-2(config)# interface range fastethernet 0/5-8
```

```
Switch-2(config-if)# channel-group 2 mode auto
```

### 2.5 Configure Trunking

```
Switch-2(config)# interface port-channel 1
```

```
Switch-2(config-if)# switchport mode trunk
```

### 2.6 Configuring Port Security

```
Switch-2(config)# interface range fastethernet 0/10-20
```

```
Switch-2(config-if)# switchport port-security
```

```
Switch-2(config-if)# switchport port-security violation shutdown
```

```
Switch-2(config-if)# switchport port-security mac-address sticky
```

```
Switch-2(config-if)# switchport port-security maximum 1
```

### 2.7 Configure Spanning Tree Protocol

```
Switch-2(config)# spanning-tree mode rapid-pvst
```

```
Switch-1(config)# spanning-tree vlan 20 root primary
```

### 3 Switch-3

#### 3.1 Basic Configuration

```
Switch(config)# hostname Switch-3
Switch-3(config)# line console 0
Switch-3(config-line)# password cisco
Switch-3(config-line)# login
Switch-3(config-line)# motd-banner #Unauthorized access prohibited#
Switch-3(config)# enable password cisco
```

#### 3.2 Creating VLANs

```
Switch-3(config)# vlan 10
Switch-3(config-vlan)# name Developer_Department
```

```
Switch-3(config)# vlan 20
Switch-3(config-vlan)# name Account_Department
```

```
Switch-3(config)# vlan 30
Switch-3(config-vlan)# name HR_Department
```

```
Switch-3(config)# vlan 40
Switch-3(config-vlan)# name Business_Department
```

#### 3.3 Assigning Interface on vlan

```
Switch-3(config)# interface range fastethernet 0/10-20
Switch-3(config)# switchport mode access
Switch-3(config)# switchport access vlan 30
```

#### 3.4 configure EtherChannel

```
Switch-3(config)# interface range fastethernet 0/1-4
Switch-3(config-if)# channel-group 1 mode auto
Switch-3(config)# interface range fastethernet 0/5-8
```

```
Switch-3(config-if)# channel-group 2 mode auto
```

### 3.5 Configure Trunking

```
Switch-3(config)# interface port-channel 1
```

```
Switch-3(config-if)# switchport mode trunk
```

### 3.6 Configuring Port Security

```
Switch-3(config)# interface range fastethernet 0/10-20
```

```
Switch-3(config-if)# switchport port-security
```

```
Switch-3(config-if)# switchport port-security violation shutdown
```

```
Switch-3(config-if)# switchport port-security mac-address sticky
```

```
Switch-3(config-if)# switchport port-security maximum 1
```

### 3.7 Configure Spanning Tree Protocol

```
Switch-3(config)# spanning-tree mode rapid-pvst
```

```
Switch-1(config)# spanning-tree vlan 30 root primary
```

## 4 Switch-4

### 4.1 Basic Configuration

```
Switch(config)# hostname Switch-4
```

```
Switch-4(config)# line console 0
```

```
Switch-4(config-line)# password cisco
```

```
Switch-4(config-line)# login
```

```
Switch-4(config-line)# motd-banner #Unauthorized access prohibited#
```

```
Switch-4(config)# enable password cisco
```

### 4.2 Creating VLANs

```
Switch-4(config)# vlan 10
```

```
Switch-4(config-vlan)# name Developer_Department
```

```
Switch-4(config)# vlan 20
```

```
Switch-4(config-vlan)# name Account_Department
```

```
Switch-4(config)# vlan 30
```

```
Switch-4(config-vlan)# name HR_Department
```

```
Switch-4(config)# vlan 40
```

```
Switch-4(config-vlan)# name Business_Department
```

#### 4.3 Assigning Interface on vlan

```
Switch-4(config)# interface range fastethernet 0/10-20
```

```
Switch-4(config)# switchport mode access
```

```
Switch-4(config)# switchport access vlan 40
```

#### 4.4 configure EtherChannel

```
Switch-4(config)# interface range fastethernet 0/1-4
```

```
Switch-4(config-if)# channel-group 1 mode desirable
```

```
Switch-4(config)# interface range fastethernet 0/5-8
```

```
Switch-4(config-if)# channel-group 2 mode desirable
```

#### 4.5 Configure Trunking

```
Switch-4(config)# interface port-channel 1
```

```
Switch-4(config-if)# switchport mode trunk
```

#### 4.6 Configuring Port Security

```
Switch-4(config)# interface range fastethernet 0/10-20
```

```
Switch-4(config-if)# switchport port-security
```

```
Switch-4(config-if)# switchport port-security violation shutdown
```

```
Switch-4(config-if)# switchport port-security mac-address sticky
```

```
Switch-4(config-if)# switchport port-security maximum 1
```

#### 4.7 Configure Spanning Tree Protocol

```
Switch-4(config)# spanning-tree mode rapid-pvst
```

```
Switch-1(config)# spanning-tree vlan 40 root primary
```

#### 5. Administration Switch

Fastethernet 0/4	Web server	80.80.80.80	vlan 80
Fastethernet 0/1	DHCP server	50.20.1.1	vlan 1
Fastethernet 0/3	file server	50.20.1.10	vlan 1
Fastethernet 0/5	DNS server		

#### 6.4 Firewall Configuration

##### 1. Pokhara Firewall

```
Pokhara_firewall(config)# interface vlan 1
```

```
Pokhara_firewall(config-if)# nameif inside
```

```
Pokhara_firewall(config)# security level 100
```

```
Pokhara_firewall(config)# ip address 100.10.1.249 255.255.255.252
```

```
Pokhara_firewall(config)# no shutdown
```

```
Pokhara_firewall(config)# interface vlan 2
```

```
Pokhara_firewall(config-if)# nameif outside
```

```
Pokhara_firewall(config)# security level 0
```

```
Pokhara_firewall(config)# ip address 100.10.1.1 255.255.255.252
```

```
Pokhara_firewall(config)# no shutdown
```

```
Pokhara_firewall(config)# interface ethernet0/0
```

```
Pokhara_firewall(config)#switchport access vlan 1
```

```
Pokhara_firewall(config)#interface ethernet 0/1
```

```
Pokhara_firewall(config)#switchport access vlan 2
```

```
Pokhara_Firewall(config)#object net
Pokhara_Firewall(config)#object network inside-net
Pokhara_Firewall(config-network-object)#subnet 10.10.10.0 255.255.255.0
Pokhara_Firewall(config-network-object)#nat (inside,outside) dynamic interface
Pokhara_Firewall(config-network-object)#exit
Pokhara_Firewall(config)#class-map inspect
Pokhara_Firewall(config)#class-map inspect
Pokhara_Firewall(config-cmap)#class-map inspecion_default
Pokhara_Firewall(config-cmap)#match default-inspection-traffic
Pokhara_Firewall(config-cmap)#exit
Pokhara_Firewall(config)#policy-map global_policy
Pokhara_Firewall(config-pmap)#class inspecion_default
Pokhara_Firewall(config-pmap-c)#inspect icmp
Pokhara_Firewall(config-pmap-c)#exit
Pokhara_Firewall(config)#service-policy global_policy global
Pokhara_Firewall(config)#exit
```

## 2. Ilam Firewall

```
Ilam_Firewall(config)# interface vlan 1
Ilam_Firewall(config-if)# nameif inside
Ilam_Firewall(config)# security level 100
Ilam_Firewall(config)# ip address 20.10.10.1 255.255.255.252
Ilam_Firewall(config)# no shutdown
Ilam_Firewall(config)# interface vlan 2
Ilam_Firewall(config-if)# nameif outside
Ilam_Firewall(config)# security level 0
Ilam_Firewall(config)# ip address 100.10.1.245 255.255.255.252
Ilam_Firewall(config)# no shutdown
Ilam_Firewall(config)# interface ethernet0/0
```



```
Ilam_Firewall(config)#switchport access vlan 1
Ilam_Firewall(config)#interface ethernet 0/1
Ilam_Firewall(config)#switchport access vlan 2
Ilam_Firewall(config)#route outside 0.0.0.0 0.0.0.0 100.10.1.246
Ilam_Firewall(config)#object network inside-net
Ilam_Firewall(config-network-object)#subnet 20.10.10.0 255.255.255.0
Ilam_Firewall(config-network-object)#nat (inside,outside) dynamic interface
Ilam_Firewall(config-network-object)#exit
Ilam_Firewall(config)#class-map inspect
Ilam_Firewall(config)#class-map inspect
Ilam_Firewall(config-cmap)#class-map inspecion_default
Ilam_Firewall(config-cmap)#match default-inspection-traffic
Ilam_Firewall(config-cmap)#exit
Ilam_Firewall(config)#policy-map global_policy
Ilam_Firewall(config-pmap)#class inspecion_default
Ilam_Firewall(config-pmap-c)#inspect icmp
Ilam_Firewall(config-pmap-c)#exit
Ilam_Firewall(config)#service-policy global_policy global
Ilam_Firewall(config)#exit
```

### 3. Kathmandu Firewall

```
Kathmandu_Firewall(config)# interface vlan 1
Kathmandu_Firewall(config-if)# nameif inside
Kathmandu_Firewall(config)# security level 100
Kathmandu_Firewall(config)# ip address 100.10.1.38 255.255.255.252
Kathmandu_Firewall(config)# no shutdown
Kathmandu_Firewall(config)# interface vlan 2
Kathmandu_Firewall(config-if)# nameif outside
Kathmandu_Firewall(config)# security level 0
```

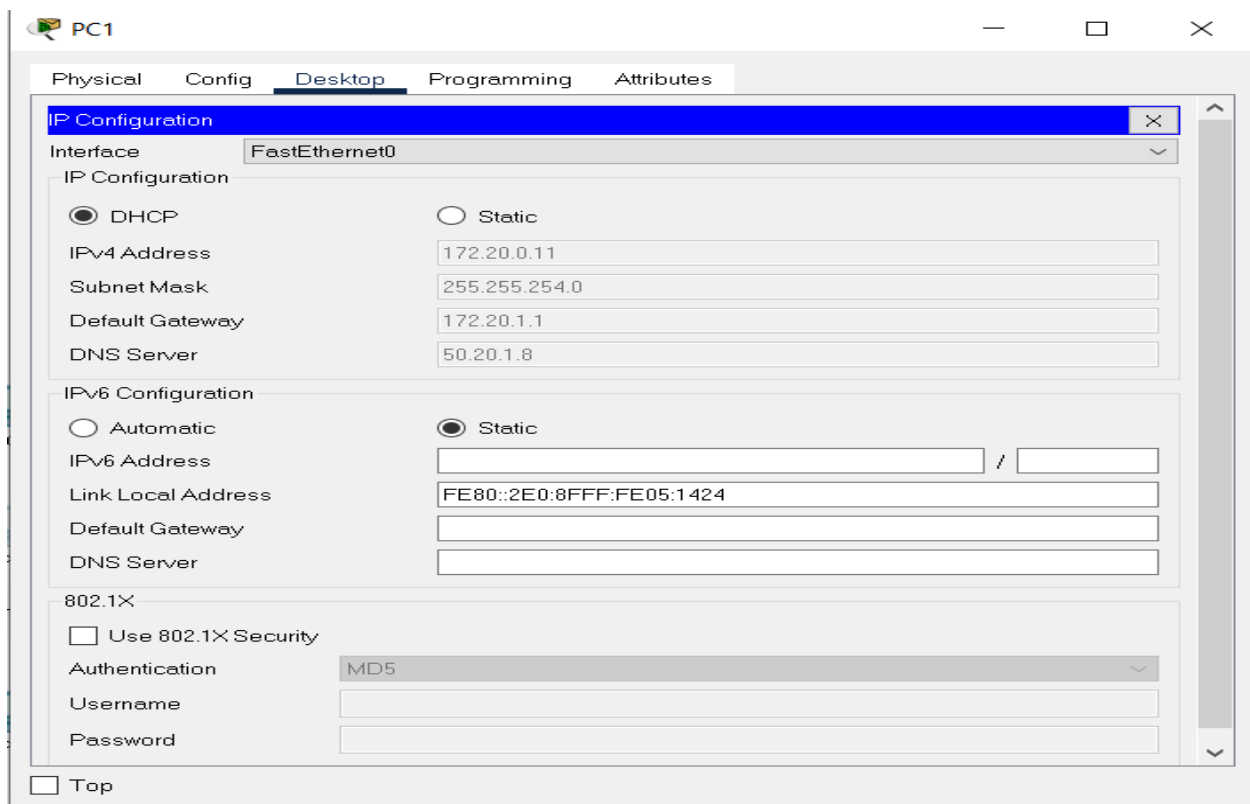
```
Kathmandu_Firewall(config)# ip address 100.10.1.34 255.255.255.252
Kathmandu_Firewall(config)# no shutdown
Kathmandu_Firewall(config)# interface ethernet0/0
Kathmandu_Firewall(config)#switchport access vlan 1
Kathmandu_Firewall(config)#interface ethernet 0/1
Kathmandu_Firewall(config)#switchport access vlan 2
Kathmandu_Firewall(config)#route outside 0.0.0.0 0.0.0.0 100.10.1.246
Kathmandu_Firewall(config)#object network inside-net
Kathmandu_Firewall(config-network-object)#subnet 172.20.0.0 255.255.254.0
Kathmandu_Firewall(config-network-object)#subnet 172.20.3.0 255.255.254.0
Kathmandu_Firewall(config-network-object)#subnet 172.20.5.0 255.255.254.0
Kathmandu_Firewall(config-network-object)#subnet 172.20.7.0 255.255.254.0
Kathmandu_Firewall(config-network-object)#subnet 50.20.1.0 255.255.255.0
Kathmandu_Firewall(config-network-object)#nat (inside,outside) dynamic interface
Kathmandu_Firewall(config-network-object)#exit
Kathmandu_Firewall(config)#class-map inspectKathmandu_Firewall(config)#class-map inspect
Kathmandu_Firewall(config-cmap)#class-map inspecion_default
Kathmandu_Firewall(config-cmap)#match default-inspection-traffic
Kathmandu_Firewall(config-cmap)#exit
Kathmandu_Firewall(config)#policy-map global_policy
Kathmandu_Firewall(config-pmap)#class inspecion_default
Kathmandu_Firewall(config-pmap-c)#inspect icmp
Kathmandu_Firewall(config-pmap-c)#exit
Kathmandu_Firewall(config)#service-policy global_policy global
Kathmandu_Firewall(config)#exit
```

## Chapter 7: Testing / Conclusion

In conclusion, This Project is designed for a most popular it company of Nepal however it could be used by any organization who is seeking for advance and improvised topology then old one which had low speed not proper connection between server and client. The protocol like STP, EtherChannel and FHRP will help to keep network up 24/7. Port security and ACL provide security with in organization and firewall will help to filter traffic and protect from different attacks, virus, malware etc. the Network address translation will help us to mapping our private IP into Public IP. The technology like IP Sec VPN will help us to get connect with a LAN from remote area in a secure way. The dynamic routing protocol like OSPF is used in this project to connect to different network and other many more technology would be used in this project which make this network fast and secure.

This is just Some of the Result of my configuration, there is much more configuration than this file. I haven't included all of them, you can find full configuration on packet tracer file.

### DHCP



## Console, login password and banner

```
ISP_Edge_Router6
Physical Config CLI Attributes
IOS Command Line Interface

unauthorized access prohibited
User Access Verification
Password:
Password:
Password:
% Bad passwords

Press RETURN to get started!
unauthorized access prohibited
User Access Verification
Password:
ISP_Edge_Router6>en
Password:
ISP_Edge_Router6#
ISP_Edge_Router6#
ISP_Edge_Router6#
ISP_Edge_Router6#
ISP_Edge_Router6#
ISP_Edge_Router6#
ISP_Edge_Router6#
Ctrl-F6 to exit CLI focus
Copy Paste
```

## Routing Table of OSPF

```
ISP_Edge_Router6#
ISP_Edge_Router6#
ISP_Edge_Router6#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

100.0.0.0/8 is variably subnetted, 18 subnets, 2 masks
O IA 100.10.1.0/30 [110/192] via 100.10.1.122, 00:13:39, Serial0/1/1
O 100.10.1.4/30 [110/192] via 100.10.1.29, 00:13:39, Serial0/2/0
O [110/192] via 100.10.1.122, 00:13:39, Serial0/1/1
O 100.10.1.8/30 [110/128] via 100.10.1.122, 00:13:54, Serial0/1/1
O 100.10.1.12/30 [110/128] via 100.10.1.29, 00:13:39, Serial0/2/0
O 100.10.1.16/30 [110/128] via 100.10.1.122, 00:13:54, Serial0/1/1
O 100.10.1.20/30 [110/128] via 100.10.1.29, 00:13:39, Serial0/2/0
O 100.10.1.24/30 [110/128] via 100.10.1.50, 00:13:39, Serial0/1/0
O [110/128] via 100.10.1.29, 00:13:39, Serial0/2/0
C 100.10.1.28/30 is directly connected, Serial0/2/0
L 100.10.1.30/32 is directly connected, Serial0/2/0
O 100.10.1.32/30 [110/192] via 100.10.1.50, 00:13:39, Serial0/1/0
O [110/192] via 100.10.1.29, 00:13:39, Serial0/2/0
C 100.10.1.48/30 is directly connected, Serial0/1/0
L 100.10.1.49/32 is directly connected, Serial0/1/0
O 100.10.1.56/30 [110/128] via 100.10.1.50, 00:13:54, Serial0/1/0
O 100.10.1.60/30 [110/192] via 100.10.1.50, 00:13:39, Serial0/1/0
O IA 100.10.1.120/30 is directly connected, Serial0/1/1
L 100.10.1.121/32 is directly connected, Serial0/1/1
C 100.10.1.132/30 is directly connected, GigabitEthernet0/0
L 100.10.1.133/32 is directly connected, GigabitEthernet0/0

ISP_Edge_Router6#
ISP_Edge_Router6#
ISP_Edge_Router6#
Ctrl-F6 to exit CLI focus
Copy Paste
```

Switch1

Physical Config CLI Attributes

IOS Command Line Interface

```

switch-2#show
switch-2#show
switch-2#show ethe
switch-2#show etherchannel
switch-2#show etherchannel
switch-2#show etherchannel

    Channel-group listing:
    -----

Group: 1
-----
Group state = L2
Ports: 4 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP

Group: 2
-----
Group state = L2
Ports: 4 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP
switch-2#
switch-2#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
      (Count)      (Count)      (Count)
-----
Fa0/10      2          2          0          Shutdown
Fa0/11      2          2          0          Shutdown
Fa0/12      2          0          0          Shutdown
Fa0/13      2          1          0          Shutdown
Fa0/14      2          0          0          Shutdown
Fa0/15      2          0          0          Shutdown
Fa0/16      2          0          0          Shutdown
Fa0/17      2          0          0          Shutdown
Fa0/18      2          0          0          Shutdown
Fa0/19      2          0          0          Shutdown
Fa0/20      2          0          0          Shutdown
-----
switch-2#

```

OH-F6 to exit CLI focus

Copy Paste

☐ Top

```

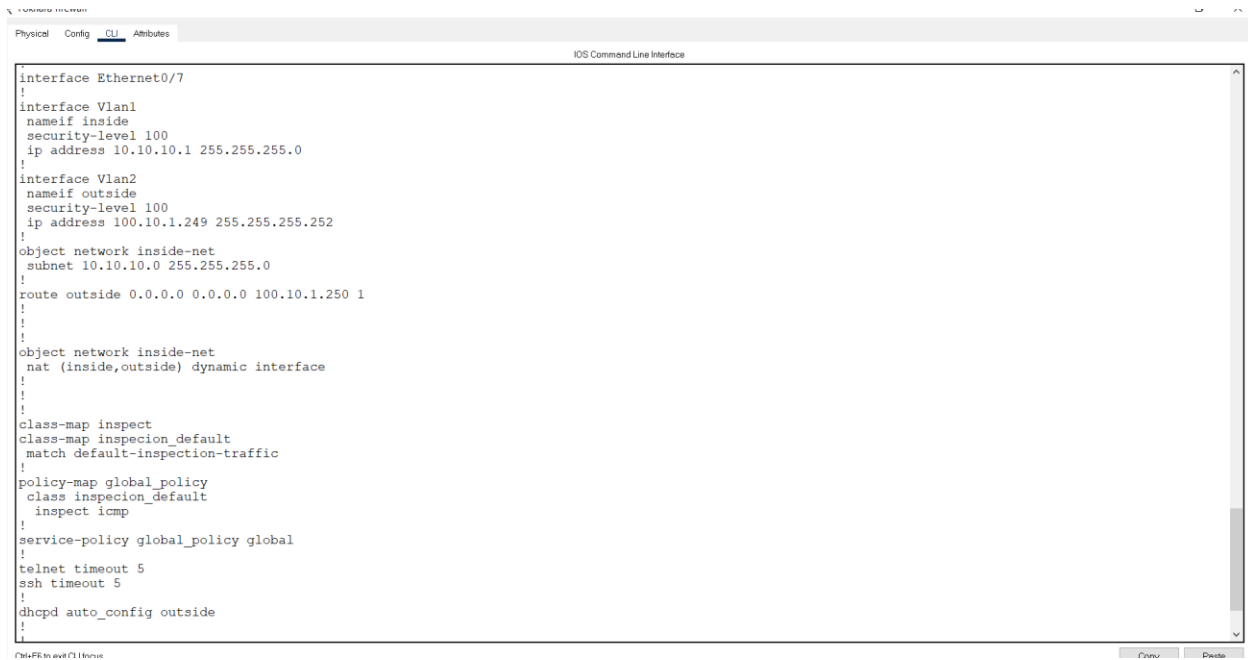
Password:
switch-1#
switch-1#
switch-1#
switch-1#sh vl br

```

VLAN	Name	Status	Ports
1	default	active	Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10	Finance_Department	active	Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20
20	HR	active	
30	QA	active	
40	Research_Development	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	
switch-1#			

Ctrl-F8 to exit CLI focus

## Firewall



```

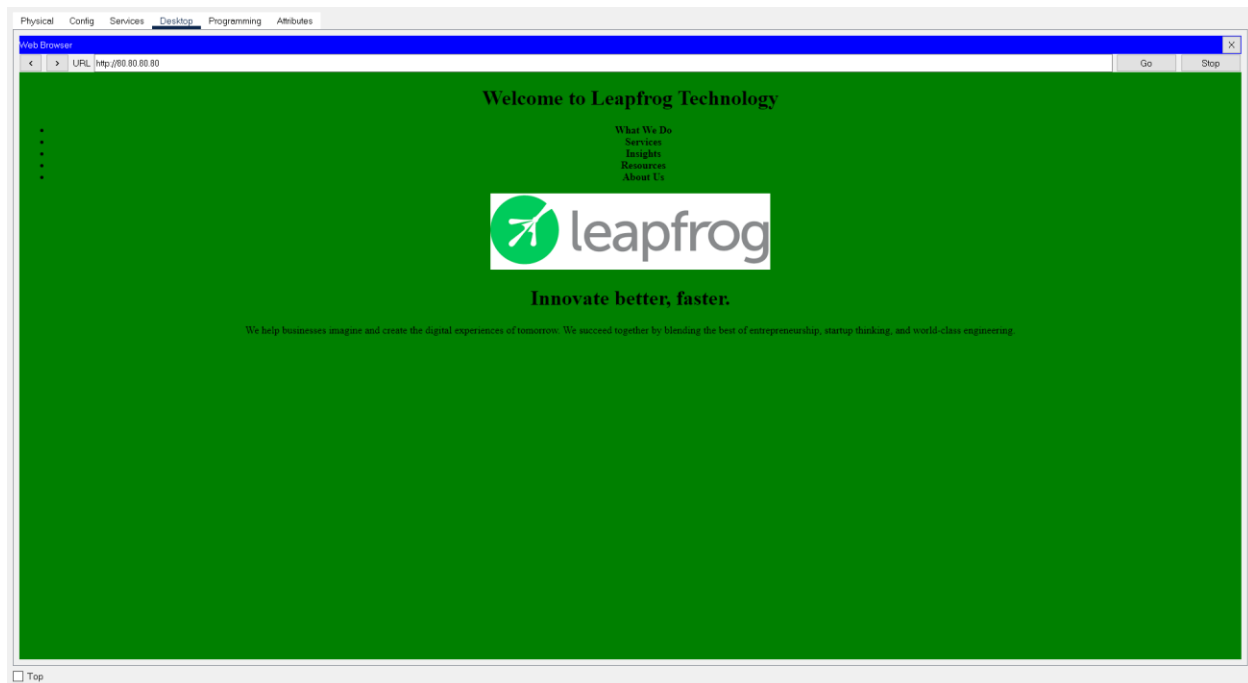
IOS Command Line Interface

Physical  Config  CLI  Attributes

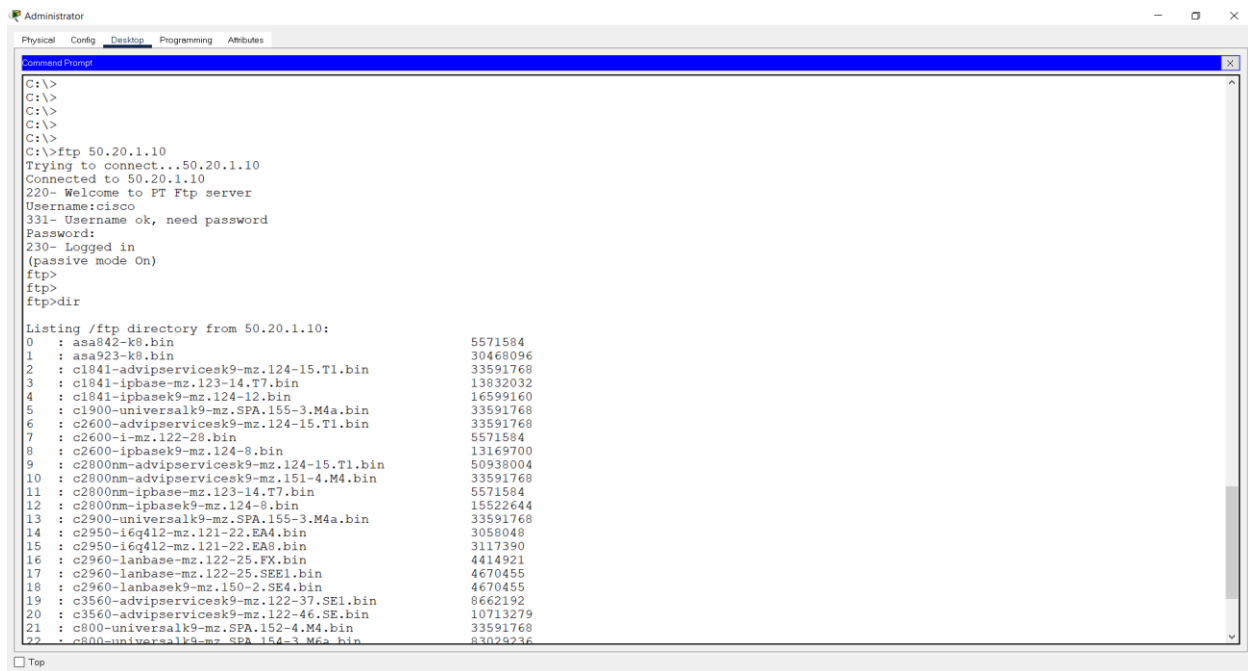
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 100
 ip address 100.10.1.249 255.255.255.252
!
object network inside-net
 subnet 10.10.10.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 100.10.1.250 1
!
!
!
object network inside-net
 nat (inside,outside) dynamic interface
!
!
!
class-map inspect
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
  inspect icmp
!
service-policy global_policy global
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!

```

## Web Server



## FTP



```
Administrator
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>ftp 50.20.1.10
Trying to connect...50.20.1.10
Connected to 50.20.1.10
220- Welcome to FT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
ftp>
ftp>dir

Listing /ftp directory from 50.20.1.10:
 0 : asa842-k8.bin                      5571584
 1 : asa923-k8.bin                      30468096
 2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
 3 : c1841-ipbase-mz.123-14.T7.bin       13832032
 4 : c1841-ipbasek9-mz.124-12.bin        16599160
 5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
 6 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
 7 : c2600-i-mz.122-28.bin              5571584
 8 : c2600-ipbasek9-mz.124-8.bin         13169700
 9 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin     5571584
12 : c2800nm-ipbasek9-mz.124-8.bin       15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin     3058048
15 : c2950-i6q412-mz.121-22.EA8.bin     3117390
16 : c2960-lanbase-mz.122-25.FX.bin      4414921
17 : c2960-lanbase-mz.122-25.SEE1.bin    4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin    4670455
19 : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
20 : c3560-advipservicesk9-mz.122-46.SE.bin 10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin 33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin 83029236

Top
```

## Reference

- cisco. (n.d.). *network security*. Retrieved from netacad.com:  
<https://contenthub.netacad.com/itn/16.3.6>
- geeksforgeeks*. (2021, 05 12). Retrieved from geeksforgeeks.com:  
<https://www.geeksforgeeks.org/types-of-network-firewall/>
- Melnick, J. (2019, janary 8). *blog.netwrix.com*. Retrieved from  
<https://blog.netwrix.com/2019/01/08/network-devices-explained/>
- wiki*. (n.d.). Retrieved from [https://en.wikipedia.org/wiki/Computer\\_network](https://en.wikipedia.org/wiki/Computer_network)
- (Ref 5) Topology -- from Wolfram MathWorld. (n.d.).  
<Http://Mathworld.Wolfram.Com/Topology.Html>. Retrieved August 17, 2021, from  
<https://mathworld.wolfram.com/Topology.html>
- (Ref 6) Contributor, S. (2021, April 2). What is Network Topology? Best Guide to Types & Diagrams - DNSstuff. Software Reviews, Opinions, and Tips - DNSstuff.  
<https://www.dnsstuff.com/what-is-network-topology>
- (Ref 7) Wikipedia contributors. (2021, August 9). Network topology. Wikipedia.  
[https://en.wikipedia.org/wiki/Network\\_topology](https://en.wikipedia.org/wiki/Network_topology)
- (Ref 8) What Is Network Topology? (2021, May 25). Cisco.  
<https://www.cisco.com/c/en/us/solutions/automation/network-topology.html>
- (Ref 9) What is a firewall? Firewalls explained and why you need one. (n.d.). Norton. Retrieved August 17, 2021, from <https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html#:~:text=A%20firewall%20is%20a%20security,private%20data%20on%20your%20computer.>
- (Ref 10) Improving Resiliency of Network Topology with Enhanced Evolving Strategies. (2006, September 1). IEEE Conference Publication | IEEE Xplore.