

# Network security

by

Mohammed Abdalrazek Mohammed Ali

Kirolos Romany Samir Habeab

Mohammed Ali Mohammed Rizk

Ezzat Gamil Ezzat

kerelos Amin Thabet Amin

Taha Farid Taha

A thesis presented to the University of Benha  
in partial fulfilment of the requirement of the degree of  
Bachelor Degree  
in  
Electronics and Communications Engineering

**Supervised by**  
Dr. Heba-Allah Adly



## **Abstract**

A computer network, which is also referred to as a data network, constitutes a form of telecommunications infrastructure facilitating communication between computer systems. In the context of computer networks, the transmission of information occurs among interconnected computing devices. At the enterprise level, several widely prevalent network vulnerabilities include the improper installation and configuration of hardware and software, the failure to update operating systems or firmware, the misuse of hardware or software, and inadequate security protocols. These vulnerabilities can have far-reaching consequences, including breaches in confidentiality and data integrity, the unauthorized access and alteration of critical business information, and system downtime affecting business continuity. Thus, it is imperative for companies to implement comprehensive security measures to protect their networks and information assets from potential cyber threats. The absence of adequate physical security measures, employment of weak password configurations, as well as inherent deficiencies in each device's design, collectively contribute to the compromised security posture of said device. The integration of an operating system within a network infrastructure simplifies and enhances its potential for operation. There are various mechanisms that enable individuals to acquire entry too. Corporations are required to possess a server system to ensure smooth and efficient operation. The web server, like its counterparts such as the email server and FTP server, is primarily utilized for the purpose of disseminating information regarding its products and servers. The utilization of electronic mail facilitates seamless communication between employees, thus streamlining organizational operations. Alternatively, the implementation of File Transfer Protocol (FTP) enables secure sharing of files within the company, ensuring data confidentiality and integrity.

## **Acknowledgements**

We thank Allah for completing the project and we hope that it will be useful. we would like to express our deep gratitude to Dr Heba-Allah Adly, the project supervisor, for the patient guidance, enthusiastic encouragement, and useful critiques of this research work. We have been extremely lucky to have a supervisor who cared so much about our work, and who responded to our questions and queries so promptly. valuable and constructive suggestions during the planning and development of this project. His willingness to give his time so generously has been very much appreciated. Also, we would like to thank the college for providing us with laboratories that are equipped with the required tools such as computers and the Internet. We would like to thank the Discussion committee for their time and efforts. Finally, we would like to thank our families for their unconditional support.

# Contents

<b>List of Figures</b>	<b>vii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Problem Statement . . . . .	1
1.2 objectives . . . . .	2
1.3 project scope . . . . .	3
1.4 cost . . . . .	3
1.5 project parts . . . . .	3
1.6 Requirements . . . . .	4
1.7 project outcomes . . . . .	5
<b>2 Network and security background</b>	<b>7</b>
2.1 What is a computer network? . . . . .	7
2.2 Computer network types . . . . .	8
2.3 Networking Foundation . . . . .	8
2.4 Unique identifiers of network . . . . .	9
2.5 network infrastructure .....	11
2.6 Common Threats.....	13
2.7 Understanding Defense.....	16
2.8 Endpoint Security.....	16
2.9 Network security and common devices .....	17

<b>3</b>	<b>Network</b>	<b>19</b>
3.1	Network topologies .....	19
3.2	Basic configuration .....	22
3.3	Access Methods .....	23
3.4	Internet Protocol (IP) .....	25
3.5	IP Addressing Services .....	27
3.6	Routing .....	31
3.7	Switching .....	35
3.8	Domain Name Service .....	41
<b>4</b>	<b>security</b>	<b>44</b>
4.1	Introduction .....	44
4.2	Control Plane Security Controls .....	45
4.2.1	Infrastructure ACLs .....	45
4.2.2	Control Plane Policing .....	46
4.2.3	Control Plane Protection .....	47
4.3	Layer 2 & 3 Data Plane Security Controls .....	49
4.3.1	STP .....	51
4.3.2	MAC Spoofing .....	52
4.3.3	CAM flooding .....	53
4.3.4	DHCP Attacks .....	55
4.3.5	ARP Inspection .....	58
4.4	ACLs .....	60
4.5	Security devices and services .....	62
4.5.1	Firewall .....	62
4.5.2	IPS .....	64

<b>5</b>	<b>Firewall</b>	<b>66</b>
5.1	firewall zone .....	66
5.2	cisco ASA VS cisco NGFW .....	67
5.3	cisco NGFW (FTD) .....	68
5.4	FTD to FMC registration .....	69
5.5	FTD connect the inside zone with outside zone .....	70
5.6	FTD object .....	71
5.7	FTD Access control policy .....	74
5.8	FTD layer of defense .....	77
5.8.1	Cisco Firepower NGFW Prefilter Policies .....	77
5.8.2	Cisco Firepower NGFW Security Intelligence .....	79
5.8.3	Cisco Firepower NGFW Discovery Policies .....	80
5.8.4	Cisco Firepower NGFW IPS Policies .....	82
5.8.5	Cisco Firepower NGFW Malware and File Policies .....	83
<b>6</b>	<b>Servers</b>	<b>84</b>
6.1	Introduction.....	84
6.2	servers and services in proposed network.....	84
6.3	File sharing services (File Transfer Protocol).....	85
6.3.1	What is FTP (File Transfer Protocol)?.....	85
6.3.2	How does FTP work?.....	86
6.3.3	Why is FTP important and what is it used for?.....	86
6.3.4	FTP types .....	87
6.3.5	FTP security .....	88
6.3.6	FTP clients .....	89
6.3.7	FTB server in proposed network.....	89
6.4	web server .....	90
6.4.1	What is a web server? .....	90

6.4.2	How do web servers work? .....	90
6.4.3	Common and top web server software on the market .....	93
6.4.4	Web server security practices .....	94
<b>7</b>	<b>Conclusions and Future Work</b>	<b>96</b>
7.1	Future Work.....	96
<b>8</b>	<b>References</b>	<b>100</b>

# List of Figures

1.1	project topology . . . . .	6
2.1	hup. . . . .	10
2.2	bridge. . . . .	10
2.3	switch. . . . .	10
2.4	Router. . . . .	11
2.5	link. ....	11
2.6	IP address classes.....	11
2.7	hierarchical network.....	12
2.8	network and security topology in general. ....	18
3.1	types of Network Topology.....	21
3.2	mesh topology in proposed network.....	22
3.3	the ip in proposed Network.....	28
3.4	the ip in proposed Network.....	28
3.5	DHCP in proposed Network.....	29
3.6	DHCP work.....	30
3.7	excluded addresses.....	31
3.8	pools.....	31
3.9	working of DHCP in proposed network .....	31
3.10	default root.....	33



3.11 OSPF in proposed network .....	34
3.12 vlan in proposed network.....	36
3.13 configure access port.....	37
3.14 configure trunk port .....	37
3.15 configure of stp .....	38
3.16 stp.....	39
3.17 How STP works .....	39
3.18 link aggregation .....	40
3.19 the proposed network containing link aggregation .....	40
3.20 DNS working .....	41
3.21 DNS hierarchical.....	42
4.1 Identifying Network Device Planes .....	45
4.2 Infrastructure ACLs filter traffic .....	46
4.3 copp.....	47
4.4 CoPP aggregates traffic.....	48
4.5 configured traffic to CPPr .....	48
4.6 configured CPPr.....	49
4.7 OSI module .....	50
4.8 Overview of Layer 2 Data Plane Security Controls.....	50
4.9 MAC Spoofing .....	53
4.10 macof .....	54
4.11 DHCP starvation attack.....	56
4.12 DHCP Spoofing Attack.....	56
4.13 trusted port at our proposed network .....	57
4.14 ARP Inspection .....	59
4.15 ACL in proposed Network .....	61
4.16 for try the device in it2 to ping with sale in proposed Network.....	61

4.17	firewall advantage .....	63
4.18	ips handles denied traffic .....	65
5.1	Cisco Firepower NGFW Deployments .....	69
5.2	FTD Device.....	70
5.3	Add device .....	70
5.4	FTD to FMC registration .....	71
5.5	FTD NAT.....	71
5.6	ACP in FTD .....	72
5.7	OSPF with FTD .....	72
5.8	New Network Object .....	73
5.9	ACP details .....	76
5.10	ACP rule action.....	77
5.11	FTD layer of defense .....	77
5.12	Prefilter policy .....	78
5.13	Security Intelligence .....	79
5.14	Cisco Firepower NGFW Discovery Policies .....	82
6.1	FTP.....	86
6.2	FTP in proposed Network.....	89
6.3	step 1 .....	92
6.4	step 2 .....	92
6.5	step 3 .....	92
6.6	step 4 .....	92
6.7	web server in proposed network .....	93
6.8	web server in proposed network .....	95

# Chapter 1

## Introduction

### 1.1 Problem Statement

The world is now interconnected via the Internet in all fields at the personal, international, and institutional levels. Now Egypt is moving towards digital transformation and all private and public information will be managed via the Internet by the competent authorities in the country. Recently, a new kind of war emerged cyberwarfare and information warfare. And this kind clearly appeared between Russia and Ukraine, where Ukrainian banks were hacked into the network and stopped working for a while. On a small scale in companies there are some of the most common network vulnerabilities Improperly installed hardware or software operating systems or firmware that have not been updated Misused hardware or software Poor or a complete lack of physical security insecure passwords design flaws in a device's operating system or in the network, it does make it much easier and possible for them to gain access to it. the attacker achieved that by using different common of attacks:

- Ransomware: The goal of the attackers is financial gain because they hold the company's data for ransom until they are paid.
- Arp spoofing: ARP spoofing is a type of attack in which a malicious actor sends

falsified ARP (Address Resolution Protocol) messages over a local area network, this results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.

- Man-in-the-middle attack (MITM): An MITM attack intercepts a communication between two systems, the attacker inserts a device into a network that grabs packets that are streaming past.
- Distributed Denial-of-Service (DDoS) attack is a DoS attack that features a simultaneous, coordinated attack from multiple source machines. The best-known example of a DDoS attack is the "smurf" attack.
- DHCP attack: The attacker runs DHCP server software and replies to DHCP requests from legitimate clients.
- IoT-Based Attacks: are cyber-attacks that gain access to users' sensitive data with the help of any IoT device. Attackers usually install malware on the device, harm the device, or gain access to further personal data of the company.
- Password attack: The password attack is a widely utilized attack vector for the purpose of exploiting user account authentication or circumventing it altogether. In contrast
- Fragmentation attack: fragmentation attacks are a prevalent incarnation of Denial of Service (DOS) attacks where the attacker applies datagram fragmentation mechanisms to overload a network.

## 1.2 objectives

1- Design a network with all its layers and set up the basic configuration for all its devices.

2- Configure the Authentication, Authorization and Accounting (AAA) for the different

departments.

3- Use kali Linux to try the attacks and discover vulnerabilities to close it.

4- Configure layer 2 & layer 3 security configurations to avoid internal attacks on routers and switches

5- Use a next generation fire wall to secure data and avoid or eliminate the external attacks.

6- Simulate a real network company in eve-ng.

### **1.3 project scope**

We design a network and use security devices to secure it from internal and external attacks. We use simulators in our own laptops to build the project and use kali Linux for inner user and outer user to test the security.

### **1.4 cost**

The biggest advantage of our project is it is almost free and costs less if users have a laptop and the internet pay in month.

### **1.5 project parts**

- Network part consists of:
  - Core part: which is the core router of the project.
  - Distribution part: which is four routers connected directly to the core router.
  - Access part: which contains switches and end user devices.
- Security part consists of:

- NGFW (The Cisco Firepower Next-Generation Firewall) and we can configure and manage firepower with:
  - \* FTD (Firepower Threat Defense software) is a Cisco Next Generation Firewall and IPS solution for securing networks and applications. It also includes many other security features.
  - \* FMC (firepower management center) gives you the ability to configure the FTD WSA device to control web security & ESA device to control email security.
- Server's part consists of:
  - DMZ zone .
  - DHCP server.
  - DNS server

## 1.6 Requirements

To establish this network, we use a group of TOOLS:

- VMware Workstation Player .
- FileZilla.
- EVE-COMM-VM.
- It requires the internet to establish the network.
- It requires laptops or desktops with high capabilities to establish it at least 16G RAM.

## **1.7 project outcomes**

The main benefit of network includes File sharing- you can easily share data between different users or access it remotely if you keep it on other connected devices. Sharing a single internet connection - it is cost-efficient and can help protect your systems if you properly secure the network. Networking computers can also help you improve communication, so that: staff, suppliers and customers can share information and get in touch more easily. Your business can become more efficient networked access to a common database can avoid the same data being keyed multiple times, saving time and preventing errors. We establish a security system in our network that prevents different types of attacks:

- IP attacks: Man in the middle attack (MITM), IP address spoofing, Dos attack.
- DHCP Attacks: DHCP server spoofing, DHCP starvation.
- TCP Vulnerabilities: TCP SYN flooding, TCP Reset Attack.
- ICMP Vulnerabilities: Reconnaissance and scanning. ICMP based Operating System fingerprinting, Denial of service attacks.

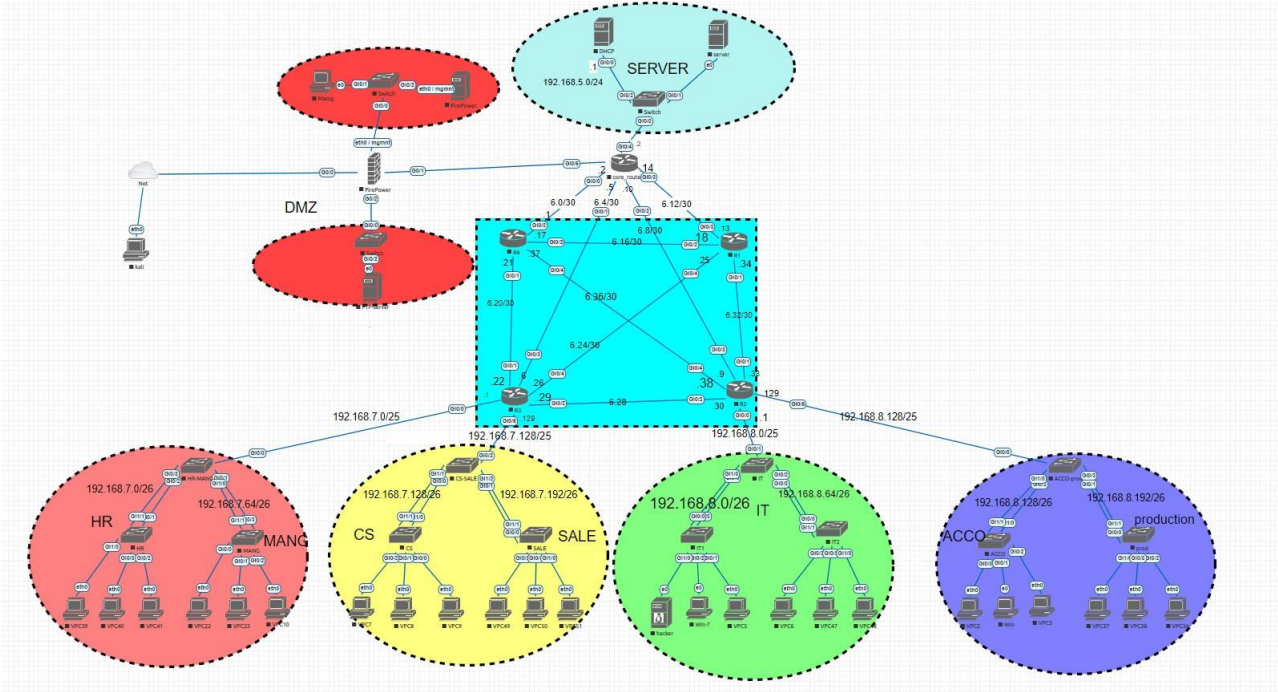


Figure 1.1: project topology



# Chapter 2

## Network and security background

For any company, a connection between all its employees is needed, a connection can be achieved by using the concept of computer networking with the aid of some routers and switches.

### 2.1 What is a computer network?

A computer network comprises two or more computers that are connected either by cables (wired) or WIFI (wireless)—with the purpose of transmitting, exchanging, or sharing data and resources. You build a computer network using hardware (e.g., routers, switches, access points, and cables) and software (e.g., operating systems or business applications). Geographic location often defines a computer network. For example, a LAN (local area network) connects computers in a defined physical space, like an office building, whereas a WAN. (Wide area network) can connect computers across continents. The internet is the largest example of a WAN, connecting billions of computers worldwide. You can further define a computer network by the protocols it uses to communicate, the physical arrangement of its components, how it controls traffic, and its purpose. Computer networks enable communication for every business, entertainment, and research purpose. The internet, online search, email, audio and video sharing, online commerce,

live-streaming, and social networks all exist because of computer networks.

## 2.2 Computer network types

As networking needs evolved, so did the computer network type that served those needs. Here are the most common and widely used. computer network types:

- LAN (local area network): A Local Area Network (LAN) serves as a means of interconnecting computers within a restricted geographic area, thereby enabling the exchange of data, files, and resources among these machines. As an illustration, a Local Area Network (LAN) may interlink all computing systems within a campus, healthcare facility, or commercial office complex. LANs are commonly operated as privately owned and managed networks.
- WAN (wide area network): The term WAN, short for wide area network, refers to a network architecture that facilitates the interconnection of computer systems over a geographically extensive environment, spanning from regional domains to intercontinental distances. The internet represents the most extensive Wide Area Network (WAN), facilitating global connectivity. A substantial number of computing machines extend across the globe. Collective or distributed ownership models are commonly observed in the management of Wide Area Networks (WAN).
- MAN (metropolitan area network): MANs are typically larger than LANs but smaller than WANs. Cities and government entities typically own and manage MANs.

## 2.3 Networking Foundation

- Hub : Hubs connect multiple computer networking devices together. A hub also acts as a repeater in that it amplifies signals that deteriorate after traveling long

distances over connecting cables.

- **Bridge:** Bridges are used to connect two or more hosts or network segments together. The basic role of bridges in network architecture is storing and forwarding frames between the different segments that the bridge connects. They use hardware Media Access Control (MAC) addresses for transferring frames.
- **Switch:** A switch is an apparatus that interconnects various devices while concurrently managing the communication between nodes in a network to guarantee the successful delivery of data packets to their intended destination. The routing function of a network device involves the mechanism by which information is transmitted between networks, whereas the switching function is concerned with the process of information interchange between nodes within a given network. Routers are networking devices, either existing as physical or virtual components, which possess the capability to transport data packets containing informational content between networks. Routers perform an analysis of data contained within packets to identify the optimal route for transmitting the information to its intended destination. Routers function to transmit data packets until they are effectively delivered to their intended recipient node.
- **links:** The most common network cable types are Ethernet twisted pair, coaxial, and fiber optic. The choice of cable type depends on the size of the network, the arrangement of network elements, and the physical distance between devices.

To work on any network some unique identifiers must be known to the network engineer.

## 2.4 Unique identifiers of network

- **Hostname:** Every device of the network is associated with a unique name, which is called hostname.



Figure 2.1: hup.



Figure 2.2: bridge.

- IP Address: IP (Internet Protocol) address is a unique identifier for each device on the Internet. Length of the IPv4 address is 32-bits. IPv6 address is 64 bits
- DNS Server: DNS stands for Domain Name System. It is a server which translates URL or web addresses into their corresponding IP addresses.
- MAC Address: MAC (Media Access Control Address) is known as a physical address is a unique identifier of each host and is associated with the NIC (Network Interface Card). General length of MAC address is: 12-digit/ 6 bytes/ 48 bits
- Port: Port is a logical channel which allows network users to send or receive data to an application. Every host can have multiple applications running. Each of these



Figure 2.3: switch.



Figure 2.4: Router.



Figure 2.5: link.

applications are identified using the port number on which they are running.

2.5 network infrastructure

Traditionally, data center network infrastructure for large companies or large computer farms was built based on a three- layer hierarchical model, which Cisco calls the “hier-

IP address classes (pre 1993 mindset)

Class A	1.0.0.1 to 126.255.255.254	16M hosts 127 networks
Class B	128.1.0.1 to 191.255.255.254	64K hosts 16K networks
Class C	192.0.1.1 to 223.255.254.254	254 hosts 2M networks
Class D	224.0.0.0 to 239.255.255.255	Multicast
Class E	240.0.0.0 to 254.255.255.254	R&D == wasted

Figure 2.6: IP address classes.

archical inter-networking model.” It consists of core layer switches which connect to distribution layer switches (sometimes called aggregation switches), which in turn connect to access layer switches. Access layer switches are frequently located at the top of a rack, so, these are also known as top-of-rack (TOR) switches. Most network infrastructure is still laid out this way today.

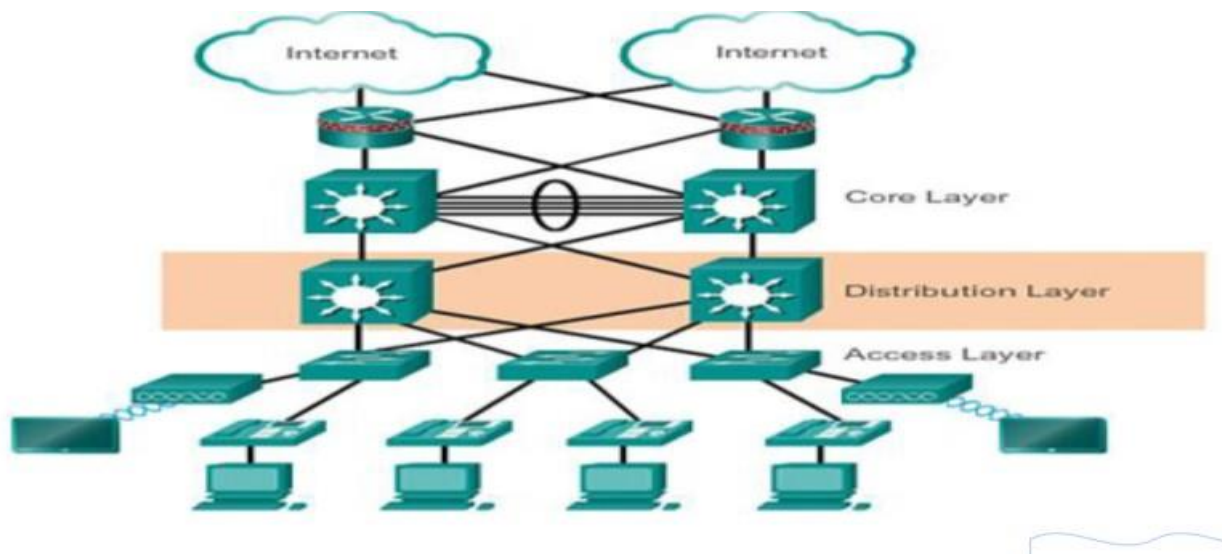


Figure 2.7: hierarchical network.

The good news with this hierarchical model is that traffic between two nodes is in the same rack, if at Layer 2 of the network stack, is sent with low latency. If the access switches are 10Gb, then the communication can have high throughput as well. Also, this type of configuration allows for a vast number of ports at the access layer and for any failure in any device the network will not stop. On the other hand, It is expensive and East – west communication, means that traffic travels to the aggregation layer and frequently to the data center core. These multiple hops, frequently across oversubscribed back planes, take a very long time – 50 microsec

- Core layer: The core layer is a high-speed switching backbone and should be designed to switch packets as fast as possible. This layer of the network should not perform any packet manipulation, such as access lists and filtering, which would slow

- down the switching of packets.
- **Distribution layer** :The distribution layer is the smart layer in the three-layer model. Routing, filtering, and QoS policies are managed at the distribution layer. Distribution layer devices also often manage individual branch-office WAN connections. This layer is also called the Workgroup layer.
  - **Access layer**: End-stations and servers connect to the enterprise at the access layer. Access layer devices are usually commodity switching platforms and may or may not provide layer 3 switching services. The traditional focus at the access layer is minimizing "cost-per-port": the amount of investment the enterprise must make for each provisioned Ethernet port. This layer, commonly referred to as the desktop layer, serves to establish connectivity between client nodes and the underlying network infrastructure. Within organizational settings, a prevalent issue pertains to network vulnerabilities arising from improperly installed components.

## 2.6 Common Threats

- **Malware** is short for malicious software. It is code or software specifically designed to damage, disrupt, steal, or inflict "bad" or illegitimate action on data, hosts, or networks. The following are types of malwares:
  - **Viruses**: A computer virus is a type of malware that propagates by inserting a copy of itself into, and becoming part of, another program. It spreads from one computer to another, leaving infections as it travels.
  - **Worms** :Computer worms are like viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to

propagate.

- Trojan Horses - It is a harmful piece of software that looks legitimate. Unlike viruses and worms, Trojan horses do not reproduce by infecting other files. They self-replicate. Trojan horses must spread through user interaction such as opening an email attachment or downloading and running a file from the internet.
- Reconnaissance Attacks: In addition to malicious code attacks, it is also possible for networks to fall prey to various network attacks. Network attacks can be classified into three major categories:
  - Reconnaissance attacks: Apart from malevolent code assaults, networks are also susceptible to several network-based assaults.
  - Access attacks: The unauthorized manipulation of data, system access, or user privileges.
  - Denial of service :The disabling or corruption of networks, systems, or services.
- Access Attacks: Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information. Access attacks can be classified into four types:
  - Password attacks: Implemented using brute force, trojan horse, and packet sniffers
  - Trust exploitation : A threat actor uses unauthorized privileges to gain access to a system, compromising the target
  - Port redirection: A threat actor uses a compromised system as a base for attacks against other targets. For example, a threat actor using SSH (port



22) to connect to a compromised host A. Host A is trusted by host B and, therefore, the threat actor can use Telnet (port 23) to access it

- Man-in-the middle :The threat actor is positioned in between two legitimate entities to read or modify the data that passes between the two parties.
- Denial of Service Attacks: Denial of service (DoS) attacks are the most publicized form of attack and among the most difficult to eliminate. However, because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators.
  - DoS attacks take many forms. They prevent authorized people from using a service by consuming system resources. To help prevent DoS attacks it is important to stay up to date with the latest security updates for operating systems and applications.
  - DoS attacks are a major risk because they interrupt communication and cause significant loss of time and money. These attacks are simple to conduct, even by an unskilled threat actor.
  - A DDoS is like a DoS attack, but it originates from multiple, coordinated sources. For example, a threat actor builds a network of infected hosts, known as zombies. A network of zombies is called a botnet. The threat actor uses a command and control (CnC) program to instruct the botnet of zombies to carry out a DDoS attack.
- Ransomware: The goal of the attackers is financial gain because they hold the company's data for ransom until they are paid.
- IoT-Based Attacks: are cyber-attacks that gain access to users' sensitive data with the help of any IoT device. Attackers usually install malware on the device, harm the device, or gain access to further personal data of the company.

- Fragmentation attack: are a common form of Denial of Service (DOS) attack, in which the perpetrator overbears a network by exploiting datagram fragmentation mechanisms.

## 2.7 Understanding Defense

The starting point for network defense is the identification of assets, vulnerabilities, and threats.

- Assets are anything of value to an organization that must be protected including servers, infrastructure devices, end devices, and the greatest asset, data.
- Vulnerabilities are weaknesses in a system or its design that could be exploited by a threat actor.
- Threats are any potential danger to an asset.

## 2.8 Endpoint Security

Endpoint, or host, is an individual computer system or device that acts as a network client. Common endpoints are laptops, desktops, servers, smartphones, and tablets. Securing endpoint devices is one of the most challenging jobs of a network administrator because it involves human nature. A company must have well-documented policies in place and employees must be aware of these rules. Employees need to be trained in proper use of the network. Policies often include the use of antivirus software and host intrusion prevention. More comprehensive endpoint security solutions rely on network access control.

## 2.9 Network security and common devices

- Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access. A firewall could allow outside user-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). The DMZ enables a network administrator to apply specific policies for hosts connected to that network.
- Types of firewalls : 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:
  - Packet filtering - Prevents or allows access based on IP or MAC addresses
  - Application filtering : Prevents or allows access by specific application types based on port numbers
  - URL filtering : Prevents or allows access to websites based on specific URLs or keywords
  - Stateful packet inspection (SPI) : Incoming packets must be legitimate responses to requests from internal hosts. Unsolicited packets are blocked unless permitted specifically. SPI can also include the capability to recognize and filter out specific types of attacks, such as denial of service (DoS).
- Various network security devices are required to protect the network perimeter from outside access. These devices could include the following:
  - Virtual Private Network (VPN) enabled router provides a secure connection to remote users across a public network and into the enterprise network. VPN services can be integrated into the firewall.

- Next-Generation Firewall (NGFW) : provides stateful packet inspection, application visibility and control, a next-generation intrusion prevention system (NGIPS), advanced malware protection (AMP), and URL filtering.
- Network Access Control (NAC) : includes authentication, authorization, and accounting (AAA) services. In larger enterprises, these services might be incorporated into an appliance that can manage access policies across a wide variety of users and device types. The Cisco Identity Services Engine (ISE) is an example of a NAC device

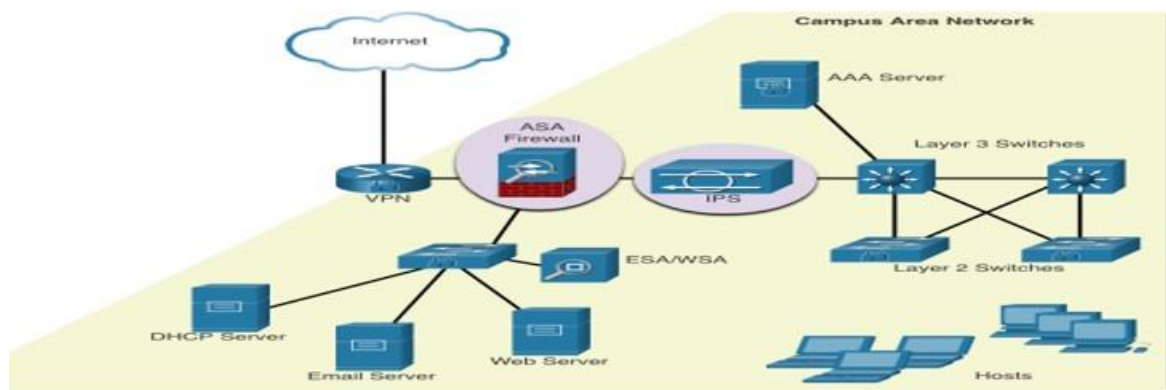


Figure 2.8: network and security topology in general.

# Chapter 3

## Network

### 3.1 Network topologies

In computer networks, there are two types of topologies, they are:

- **Physical Topology:** A physical topology describes the way in which the computers or nodes relate to each other in a computer network. It is the arrangement of various elements (link, nodes, etc.), including the device location and code installation of a computer network. In other words, we can say that it is the physical layout of nodes, workstations, and cables in the network.
- **Logical Topology:** A logical topology describes the way data flows from one Computer to another. It is bound to a network protocol and defines how data is moved throughout the network and which path it takes. In other words, it is the way in which the devices communicate internally.
  - **Bus Topology:** is the simplest kind of topology in which a common bus or channel is used for communication in the network. The bus is connected to various taps and droplines.
  - **Ring topology:** is a topology in which each computer is connected to exactly

two other computers to form the ring. The message passing is unidirectional and circular in nature.

- Star topology: is a computer network topology in which all the nodes are connected to a centralized hub. The hub or switch acts as a middleware between the nodes. Any node requesting for service or providing service, first contact the hub for communication.

- Mesh topology: is a computer network topology in which nodes are interconnected with each other. In other words, direct communication takes place between the nodes in the network. There are two types of Mesh:

Full Mesh: In which each node is connected to every other node in the network.

Partial Mesh: In which, some nodes are not connected to every node in the network.

- Tree topology: is a computer network topology in which all the nodes are directly or indirectly connected to the main bus cable. Tree topology is a combination of Bus and Star topology.
- A Hybrid topology: is a computer topology which is a combination of two or more topologies. In practical use, they are the most widely used. In proposed network, we use mesh topology. you can see all types in [fig 3.1](#)

**Why use MESH topology?** There are several reasons why mesh topology may be used:

- Fault tolerance: With a mesh topology, if one link or connection fails, data can be rerouted through another path, ensuring that the network remains operational. This makes mesh topology a highly resilient and fault-tolerant networking option.

- Scalability: Mesh networks can be easily scaled by adding more nodes to the network, without any significant impact on the performance of the network.
- Security: Mesh topology can be more secure than other types of topologies because each node can act as a relay, making it difficult for an attacker to identify and target specific nodes.
- High bandwidth: In a mesh topology, each node has its own dedicated connection to every other node, which can result in high-bandwidth connections between devices.
- Redundancy: Mesh topology provides redundancy and multiple pathways for data to travel, ensuring that data can be transmitted even if one pathway is unavailable.
- Overall, mesh topology can be an effective networking solution for organizations that require a high degree of reliability, scalability, and redundancy in their network infrastructure.

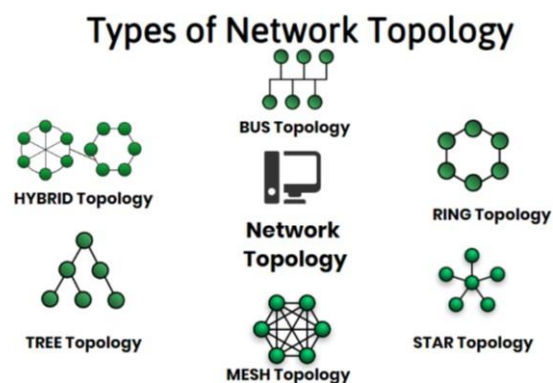


Figure 3.1: types of Network Topology.

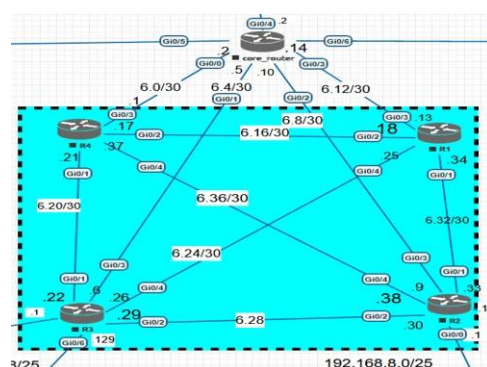


Figure 3.2: mesh topology in proposed network

## 3.2 Basic configuration

The first configuration command on any device should be to give it a unique hostname. All networking devices should limit administrative access by securing privileged EXEC, user EXEC, and remote Telnet access with passwords. In addition, all passwords should be encrypted.

### Configuration:

```
R1(config)# hostname R1
```

```
R1(config)# enable secret class
```

```
R1(config)# line console 0
```

```
R1(config-line)# password cisco
```

```
R1(config-line)# login
```

```
R1(config-line)# line vty 0 4
```

```
R1(config-line)# password cisco
```

```
R1(config-line)# login
```

```
R1(config-line)# transport input ssh
```

```
R1(config-line)# exit
```

```
R1(config)# service password encryption
```

```
R1(config)# banner motd " WARNING: Unauthorized access is prohibited "
```



```
R1(config)# exit
```

```
R1# copy running config startup config
```

### 3.3 Access Methods

Console: A physical management port used to access a device to provide maintenance, such as performing the initial configurations.

Secure Shell (SSH): Establishes a secure remote CLI connection to a device, through a virtual interface, over a network.

Telnet—Establishes an insecure remote CLI connection to a device over the network.

In the proposed network, we use Secure Shell (SSH).

- Enable SSH It is possible to configure a Cisco device to support SSH using the following steps:
  - Configure a unique device hostname. A device must have a unique hostname other than the default.
  - Configure the IP domain name. Configure the IP domain name of the network by using the global configuration mode command `ip domain name`.
  - Generate a key to encrypt SSH traffic. SSH encrypts traffic between source and destination. However, to do so, a unique authentication key must be generated by using the global configuration command `crypto key generate rsa general-keys modulus`.
  - Verify or create a local database entry. Create a local database username entry using the username global configuration command.
  - Authenticate against the local database. Use the login local line configuration command to authenticate the vty line against the local database.

- Enable vty inbound SSH sessions. By default, no input session is allowed on vty lines. You can specify multiple input protocols including Telnet and SSH using the transport input[ssh — telnet]command.

- Why use SSH?

Here are some reasons why SSH is commonly used:

- Security: SSH is designed to provide secure communication between two devices, encrypting all data transmitted over the network. This makes it a popular choice for remote access to servers and other critical systems, as it helps protect against unauthorized access and data theft.
- Remote access: SSH allows users to remotely access and manage systems from anywhere in the world if they have an internet connection and the necessary credentials.
- Versatility: SSH can be used for a wide range of tasks, including remote login, file transfers, and tunneling of other protocols. It is supported on most operating systems, including Linux, macOS, and Windows.
- Automation: SSH can be used in conjunction with automation tools, such as shell scripts and configuration management systems, to automate tasks and streamline system administration.
- Open source: SSH is an open-source protocol, which means that the source code is available for review and modification by anyone. This has helped to ensure the continued development and improvement of the protocol over time.

Overall, SSH is a widely used and trusted protocol for secure remote access and management of computer systems. It provides strong security features, is versatile, and can be easily integrated into existing workflows and automation tools, making it a valuable

tool for system administrators and developers.

Configure the Default Gateway to get access :

- The default gateway address is the IP address of the router that the host will use to access remote networks, including the internet.
- A switch must have a default gateway address configured to remotely manage the switch from another network.
- To configure an IPv4 default gateway on a switch, use: `ip default-gateway ip-address` command.

### 3.4 Internet Protocol (IP)

- The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.
- Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place.
- Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.
- IP address is a unique numerical identifier for every device or network that connects to the internet. Typically assigned by an internet service provider (ISP), there are two versions of IP:
  - IPv4: An IPv4 address is expressed as a set of four dotted decimal numbers, where each octet is separated by a period, such as 192.168.35.4.

- IPv6: An IPv6 address represents eight groups of four hexadecimal digits separated by colons, such as 2620:cc:8000:1c82:544c:cc2e:f2fa:5a9b
- The two most common types of IP addresses are:
  - Private IP addresses: Private IP addresses are non-internet facing and are only used on an internal network. Devices with private IP addresses might include computers, tablets, or smartphones.
  - Public IP addresses: Public IP addresses cover the entire network, enable a router to communicate with the internet or an outside network.
- In the proposed network IPv4 is used.
- IPv4 is divided into five classes:
  - IP v 4 Class A: The first octet has a value from 1 to 126, Network. Host. Host. Host (Network =8-bit, Host = 24 bit).
  - IP v 4 Class B: The first octet has a value from 128 to 191, Network. Network. Host. Host (Network =16-bit, Host=16bit).
  - IP v 4 Class C: The first octet has a value from 192 to 223, Network. Network. Network. Host (Network =24-bit, Host =8 bit).
  - IP v 4 Class D: The first octet has a value from 224 to 239 (Address for applications).
  - IP V 4 Class E: The first octet has a value from 240 to 254 (Address for research and military application)
- The use of the class depends on the number of hosts and the application.
- The IPv4 class C is the class used in the proposed network and uses subnet.

What is the subnetting?

A subnet, also known as a subnetwork, denotes a partitioned section of a larger

network. To be more precise, subnets are a method of logically dividing an IP network into several smaller network segments. The Internet Protocol (IP) constitutes the mechanism employed to transmit information from one computing system to another via the internet.

Every computer or host existing on the internet is assigned a distinct IP address, which serves as a unique identifier for the said entity. Organizations may opt for subnetting as a means of partitioning sizable networks into more manageable and optimized subnetworks. The objective of a subnet resides in its capability to partition a network of considerable scale into multiple, interdependent networks, thereby mitigating network congestion. By circumventing redundant routes, network speeds are elevated, as traffic is not required to traverse superfluous paths. The configuration of a valid IP is a necessary requirement for each device in an IP network, which may be facilitated through the utilization of IP Addressing Services, such as the Dynamic Host Configuration Protocol (DHCP). In the event of a small network, an administrator has the option to manually allocate an IP configuration to each device.

### **3.5 IP Addressing Services**

Each device in an IP network requires a valid IP configuration. If the network size is small, an administrator can manually provide an IP configuration to each device. But if the network size is large, assigning and managing the IP configuration on each device can be a challenging task.

Device	Interface	IP
DHCP	Loopback0	1.1.1.1/24
	Gi0/0	192.168.5.1/24
Core-router	Loopback0	2.2.2.2/24
	Gi0/0	192.168.6.2/30
	Gi0/1	192.168.6.5/30
	Gi0/2	192.168.6.10/30
	Gi0/3	192.168.6.14/30
	Gi0/4	192.168.5.2/24
R1	Gi0/5	192.168.10.1/30
	Loopback0	
	Gi0/1	192.168.6.34/30
	Gi0/2	192.168.6.18/30
	Gi0/3	192.168.6.13/30
R2	Gi0/4	192.168.6.25/30
	Loopback0	3.3.3.3/24
	Gi0/0.50	192.168.8.1/26
	Gi0/0.60	192.168.8.65/26
	Gi0/0.110	192.168.100.25/29
	Gi0/1	192.168.6.33/30
	Gi0/2	192.168.6.30/30
	Gi0/3	192.168.6.9/30
	Gi0/4	192.168.6.38/30
	Gi0/5.70	192.168.8.129/26
R3	Gi0/5.80	192.168.8.193/26
	Gi0/5.120	192.168.100.33/29
	Loopback0	4.4.4.4/24
	Gi0/0.10	192.168.7.1/26
	Gi0/0.20	192.168.7.65/26
	Gi0/0.90	192.168.100.9/29
	Gi0/1	192.168.6.22/30
	Gi0/2	192.168.6.29/30
	Gi0/3	192.168.6.6/30
	Gi0/4	192.168.6.26/30
	Gi0/5.30	192.168.7.129/26
	Gi0/6.40	192.168.7.193/26
	Gi0/6.100	192.168.100.17/29
	Loopback0	
R4	Gi0/1	192.168.6.21/30
	Gi0/2	192.168.6.17/30
	Gi0/3	192.168.6.1/30
	Gi0/4	192.168.6.37/30
FTD	eth0/mgmt	192.168.100.3/29
	Go/1	192.168.10.2/24
	Go/0	DHCP

Figure 3.3: the ip in proposed Network

FMC	eth0/mgmt	192.168.100.2/29	
HR-MANG	interface Vlan99	192.168.100.11/29	192.168.100.9
HR	interface Vlan99	192.168.100.10/29	192.168.100.9
MANG	interface Vlan99	192.168.100.12/29	192.168.100.9
CS-SALe	interface Vlan99	192.168.100.19/29	192.168.100.17
CS	interface Vlan99	192.168.100.18/29	192.168.100.17
SALE	interface Vlan99	192.168.100.20/29	192.168.100.17
IT	interface Vlan99	192.168.100.26/29	192.168.100.25
IT1	interface Vlan99	192.168.100.27/29	192.168.100.25
IT2	interface Vlan99	192.168.100.28/29	192.168.100.25
ACCO-PROD	interface Vlan99	192.168.100.34/29	192.168.100.33
ACCO	interface Vlan99	192.168.100.35/29	192.168.100.33
PROD	interface Vlan99	192.168.100.36/29	192.168.100.33
All PCs	Eth0	DHCP	
PC-mang	Eth0	192.168.100.4/29	

Figure 3.4: the ip in proposed Network

What is the DHCP:

- Dynamic Host Configuration Protocol (DHCP) is an application layer (first layer) protocol used to distribute various network configuration parameters to devices IP addresses, subnet masks, default gateways, DNS servers, etc.
- DHCP employs a client-server architecture; a DHCP client is configured to request network parameters from a DHCP server on the network. (DORA)
- A DHCP server is configured with a pool of available IP addresses and assigns one

of them to the DHCP client.

- In a network, clients and servers communicate using the following ways:
  - Unicast: Unicast is a one-to-one transmission where there is an exchange of data packets between a single source and a single destination. For example, a device with a specific IP address sends data packets to another device with a different IP address in the same or another network.
  - Broadcast: Broadcast is a type of transmission where a device transmits data packets to all devices in the same network or other networks. The first type of transmission is limited broadcasting, while the second type is direct broadcasting

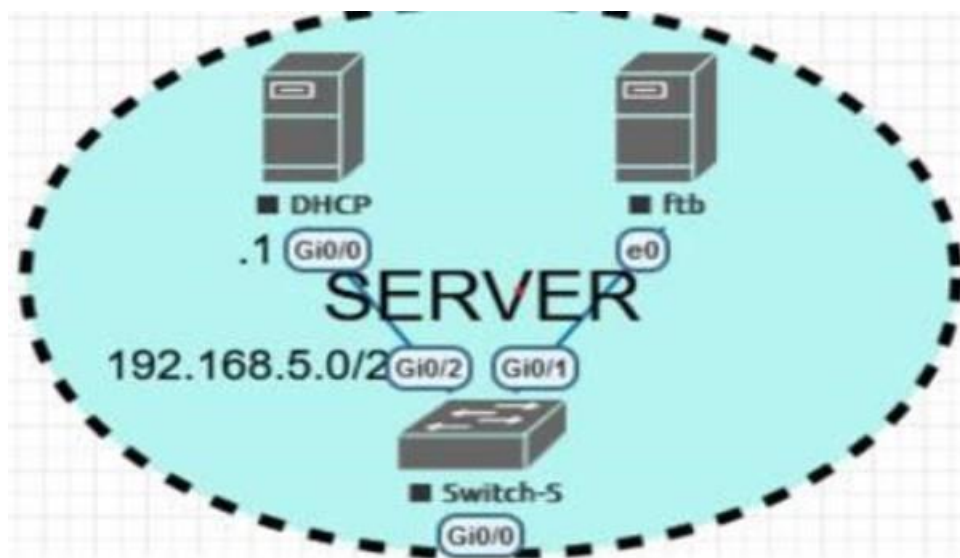


Figure 3.5: DHCP in proposed Network

The DHCP Process:

- When an IPv4, DHCP configured device boots up or connects to the network, the client broadcasts a DHCP discover (DHCPDISCOVER) message to identify any available DHCP servers on the network.

- A DHCP server replies with a DHCP offer (DHCPOFFER) message, which offers a lease to the client. Client.(If a client receives more than one offer due to multiple DHCP servers on the network, it must choose one)
- The client sends a DHCP request (DHCPREQUEST) message that identifies the explicit server and lease offer that the client is accepting.
- The server then returns a DHCP acknowledgment (DHCPACK) message that acknowledges to the client that the lease has been finalized.
- If the offer is no longer valid, then the selected server responds with a DHCP negative acknowledgment (DHCPNAK) message, and the process must begin with a new DHCPDISCOVER message.



Figure 3.6: DHCP work

Proposed network configuration :

- 1- Excluded addresses in fig 3.7:
- 2- pools in fig 3.8 .
- 3-working of DHCP in proposed network in fig 3.9.



```

ip dhcp excluded-address 192.168.7.1 192.168.7.5
ip dhcp excluded-address 192.168.7.65 192.168.7.69
ip dhcp excluded-address 192.168.7.129 192.168.7.133
ip dhcp excluded-address 192.168.7.193 192.168.7.197
ip dhcp excluded-address 192.168.8.1 192.168.8.5
ip dhcp excluded-address 192.168.8.65 192.168.8.69
ip dhcp excluded-address 192.168.8.129 192.168.8.133
ip dhcp excluded-address 192.168.8.193 192.168.8.197

```

Figure 3.7: excluded addresses

```

ip dhcp pool R3-HR
network 192.168.7.0 255.255.255.192
default-router 192.168.7.1
!
ip dhcp pool R3-MANAG
network 192.168.7.64 255.255.255.192
default-router 192.168.7.65
!
ip dhcp pool R3-CS
network 192.168.7.128 255.255.255.192
default-router 192.168.7.129
!
ip dhcp pool R3-SALE
network 192.168.7.192 255.255.255.192
default-router 192.168.7.193
!
ip dhcp pool R2-IT1
network 192.168.8.0 255.255.255.192
default-router 192.168.8.1
!
ip dhcp pool R2-IT2
network 192.168.8.64 255.255.255.192
default-router 192.168.8.65
!
ip dhcp pool R2-ACCO
network 192.168.8.128 255.255.255.192
default-router 192.168.8.129
!
ip dhcp pool R2-PROD
network 192.168.8.192 255.255.255.192
default-router 192.168.8.193
!

```

Figure 3.8: pools

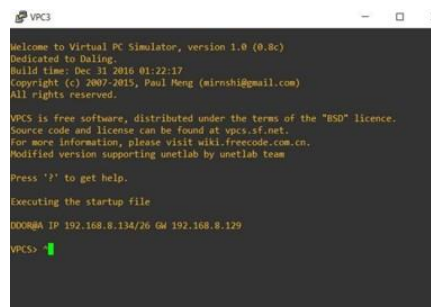


Figure 3.9: working of DHCP in proposed network

## 3.6 Routing

The process of routing involves the determination, by a router, of which interface to utilize in forwarding an IP packet to its designated destination upon receipt of the packet

via

a particular interface. The process commonly recognized as routing has been noted. The router's forwarding interface could serve as either the ultimate destination or as a network linked to a different router that functions to access the target network. In networking, it is common for a router to necessitate a distinct interface for every connected network. Nonetheless, this may not invariably be the case. The fundamental tasks of a router comprise identifying the optimal route for transmitting packets founded on the data contained in its routing table and directing packets toward their intended endpoint.

Routing is divided into two types:

- Static routing:
  - routes through a network are described by fixed paths
  - A change, such as the loss of a node, or loss of a connection between nodes, is not compensated until the admin reconfigures static routing manually again.
  - In the proposed network , Static routing commands are used to configure default route.
  - Default route :A default route is a static route that matches all packets. A single default route represents any network that is not in the routing table. Routers commonly use default routes that are either configured locally or learned from another router. The default route is used as the Gateway of Last Resort. Default static routes are commonly used when connecting an edge router to a service provider network, or a stub router (a router with only one upstream neighbor router). The used command to configure static routing as a default route can be written as : IP route 0.0.0.0 0.0.0.0 (next hop). as shown in figure [3.10](#)
- Dynamic routing

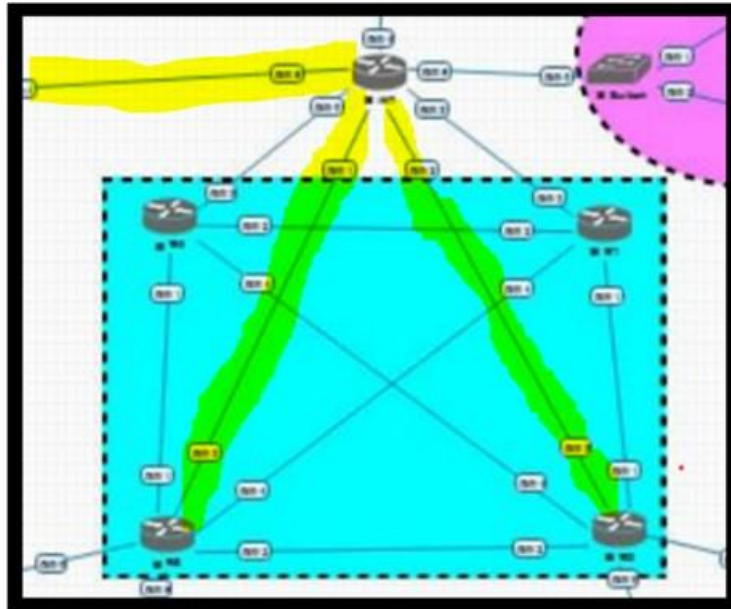


Figure 3.10: default root

- It is a technique of finding the best path for the data to travel over a network, it enables routers to select paths according to real-time logical network layout changes.
- Using dynamic routing provides some advantages:
  - \* Allows the exchange of routing information whenever the network experiences a change in topology.
  - \* Since the routes do not have to be configured manually, there is less administrative overhead and Less error-prone than static routing.
  - \* Allows scalability since there is less administrative overhead involved.
- The most popular dynamic routing protocols are (RIP, OSPF, EIGRP)
- One of the most important parameters in dynamic routing is metric.
  - \* A routing metric is calculated by routing algorithms when determining the

optimal route for sending network traffic, using many different techniques and methods based on the routing algorithms in use.

\* Some of the parameters used for calculating a routing metric are (Hop count, Path reliability, Path speed, Bandwidth,..... ).

– OSPF is the routing protocol used in the proposed networking. the advantage of OSPF is:

- \* interior gateway protocol that has been designed within a single autonomous system.
- \* based on a link-state routing algorithm(every router has a detailed map about the whole network).
- \* Administrative distance equals 110.
- \* Classless routing protocol(support VLSM).
- \* Fast convergence, secure and efficient.
- \* Its metric depends on interface bandwidth and can be calculated by :

$$\text{cost} = \frac{10^8}{\text{interface bandwidth in bps}}$$

$$\text{cumulative cost} = \text{sum of all outgoing interfaces cost in route}$$

- \* The used commands used to configure OSPF are in fig 3.11

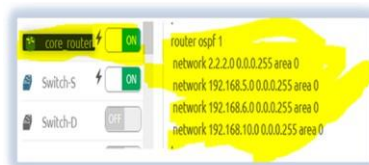


Figure 3.11: OSPF in proposed network

## 3.7 Switching

Switch Virtual Interface Configuration:

- To access the switch remotely, an IP address and a subnet mask must be configured on the SVI.
- To configure an SVI on a switch: Enter the interface vlan 1 command. Next assign an IPv4 address using the ip address ip-address subnet mask command. Finally, enable the virtual interface using the no shutdown command

VLANS:

- VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network.
- How VLAN works?
  - VLANs in networking are identified by a number.
  - A Valid range is 1-4094. On a VLAN switch, you assign ports with the proper VLAN number.
  - The switch then allows data which needs to be sent between various ports having the same VLAN.
  - Since all networks are larger than a single switch, there should be a way to send traffic between two switches.
  - One simple and easy way to do this is to assign a port on each network switch with a VLAN and run a cable between them.
  - In proposed we divide it into some branches as shown and each branch use different VLAN such as: HR take VLAN 10, and MANG take VLAN 20 and

the other vlan in fig 3.12. And management VLAN here take 99 and int's used to establish an IP connection to the switch from a workstation connected to a port in the VLAN.

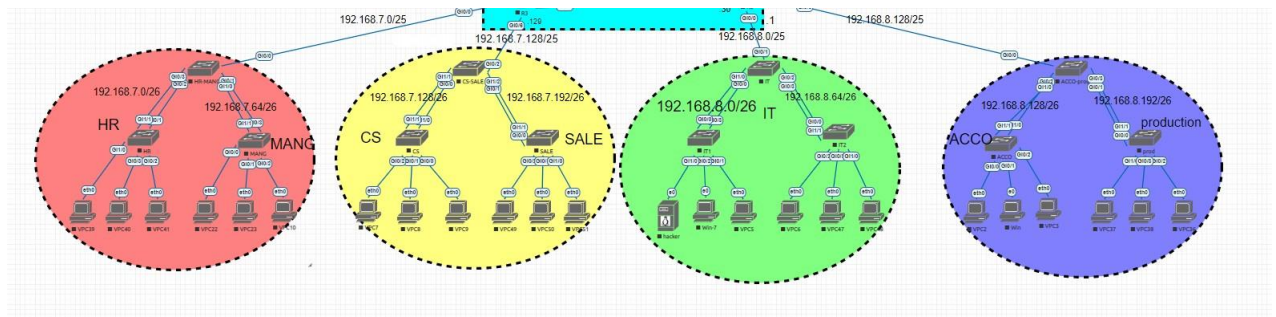


Figure 3.12: vlan in proposed network

- Some of VLAN advantages are:
  - It solves a broadcast problem.
  - VLAN reduces the size of broadcast domains.
  - VLAN allows you to add an additional layer of security.
  - It can make device management simple and easier.
  - Higher performance and reduced latency.
  - You can keep hosts separated by VLAN.
  - Users may work on sensitive information that must not be viewed by other users.
  - VLAN makes managing physical devices less complex.
  - Access port:
    - \* It is used in connecting a switch to an end device (PC, printer, laptop).
    - \* It uses an encapsulation protocol that is IEEE 802.1Q.
    - \* To designate port to access mode, use the command: (config-if) # switch port mode access.

- \* .It provides a Comparatively lower bandwidth than trunk port.
- Trunk port:
  - \* It is used in connecting Switch to switch, Switch to router or Hypervisor to switch.
  - \* It uses the encapsulation protocol: (ISL or 802.1Q)
  - \* To designate port to trunk mode, use the command: (config-if)# switch port mode trunk.
  - \* It provides high bandwidth.

To configure VLAN:

- In case of access port in fig 3.13 :
- If the interface connects between switch and switch or router 3.14 :

```
(config)#vlan 20
(config)#name (vlan 20)
(config)#int range gig 0/0-3
(config-if)#switchport mode access
(config-if)#switchport mode access VLAN 20
```

Figure 3.13: configure access port

```
(config)#int gig 0/1
(config-if)#switchport trunk encapsulation dot 1 q
Switchport mode trunk
```

Figure 3.14: configure trunk port

Spanning tree protocol(STP):

- Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on bridges and switches.
- The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network. Loops are deadly to a network.

- Spanning trees use an algorithm to search for the redundant links in the LAN and select the best paths. It is mainly used to put all links in either forwarding or blocking.
- One of the most important features of STP is Portfast:
  - Portfast feature causes a switch port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states.
  - Portfast on switch ports connected to a single workstation or server allows those devices to connect to the network immediately, instead of waiting for the port to transition from the listening and learning states to the forwarding state.
  - To configure spanning tree portfast feature enter below commands in fig 3.15:
- Spanning Tree never uses multiple links to the same destination (There is no load-sharing feature with Spanning Tree).

```
Switch# configure terminal
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
Switch(config)# show spanning-tree
```

Figure 3.15: configure of stp

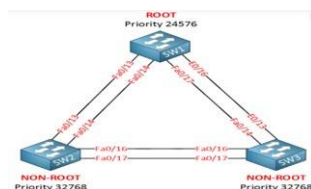


Figure 3.16: stp

How STP works?



- No need for configuration (plug & play): STP is configured automatically to the network (switch choose root and backup paths and it cannot be changed).
- Neighbor discovery: Exchange of BPDU (Bridge Protocol Data Unit) message (hello message), which is broadcasted every 2 seconds and contains (Switch ID - Accumulated Path Cost – port ID).
- Electing Root Switch: It is a switch having the least ID (we make the core switch has the least switch ID).
- Electing Root Port (RP): It is the best port on non-root switch that can reach to the root switch
- Electing Designated Port (DP): It is the best port on each link that can reach to the root switch.
- Electing Blocked Port (BP): It is the ports on each link that are neither Designated Port (DP) or Root Port RP

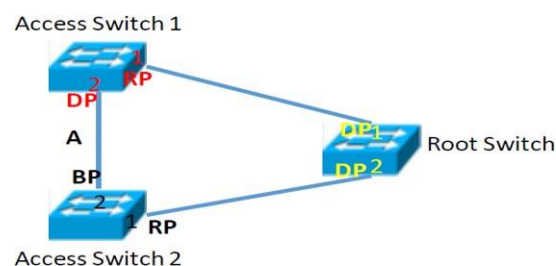


Figure 3.17: How STP works

Link aggregation:

- We need link aggregation to increase the used bandwidth between connections and more secure at failure connection it let you combine multiple ethernet links into a single logical link.
- As shown here at our proposed network and the drawing illustration how can LACP be between devices so as we said we can increase speed and can-do load balancing.
- the more we increased number of connections the more be faster and flexible

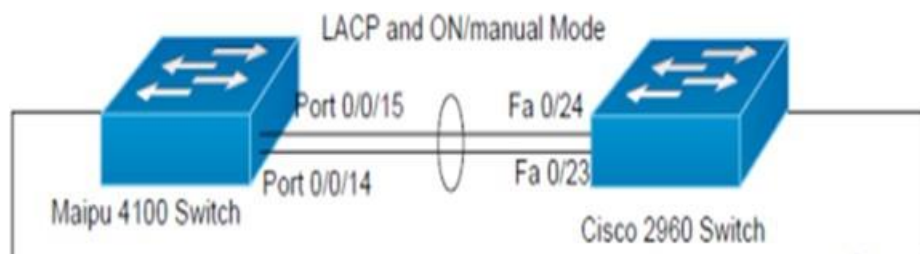


Figure 3.18: link aggregation

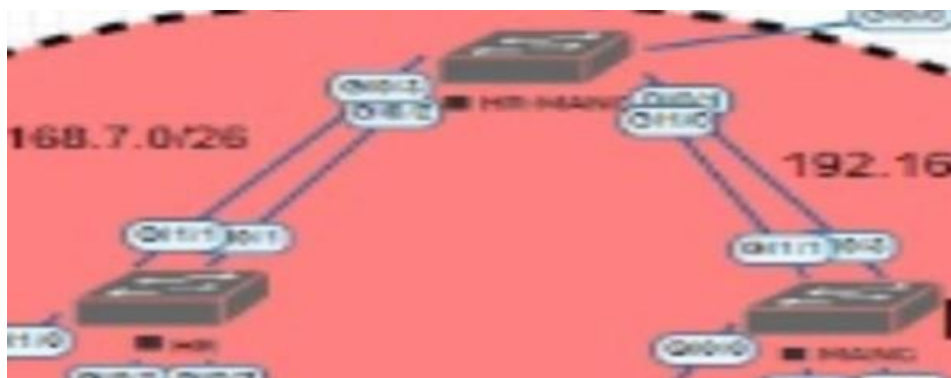


Figure 3.19: part of the proposed network containing link aggregation

### 3.8 Domain Name Service

- Domain names were created to convert the numeric IP addresses into a simple, recognizable name.
- Fully-qualified domain names (FQDNs), such as `http://www.cisco.com`, are much easier for people to remember than `198.133.219.25`. The DNS protocol defines an automated service that matches resource names with the required numeric network address. It includes the format for queries, responses, and data.

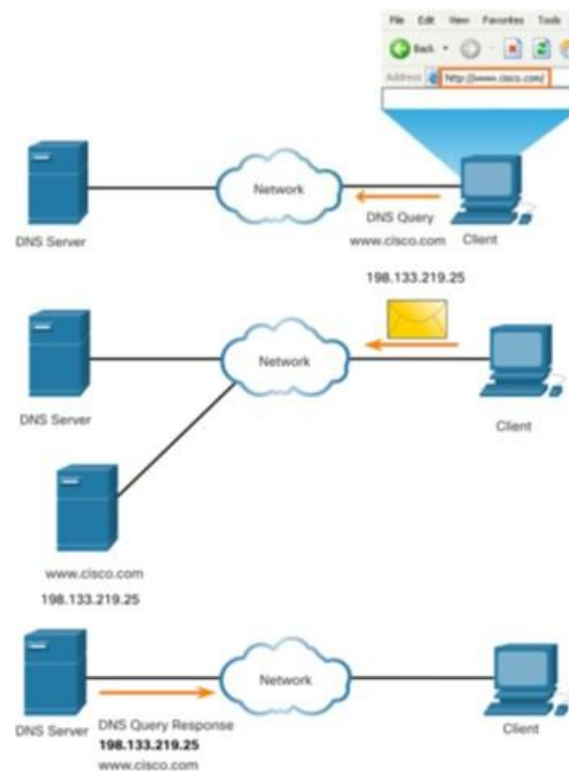


Figure 3.20: DNS working

- DNS uses a hierarchical system to create a database to provide name resolution.
- Each DNS server maintains a specific database file and is only responsible for managing name to IP mappings for that small portion of the entire DNS structure.

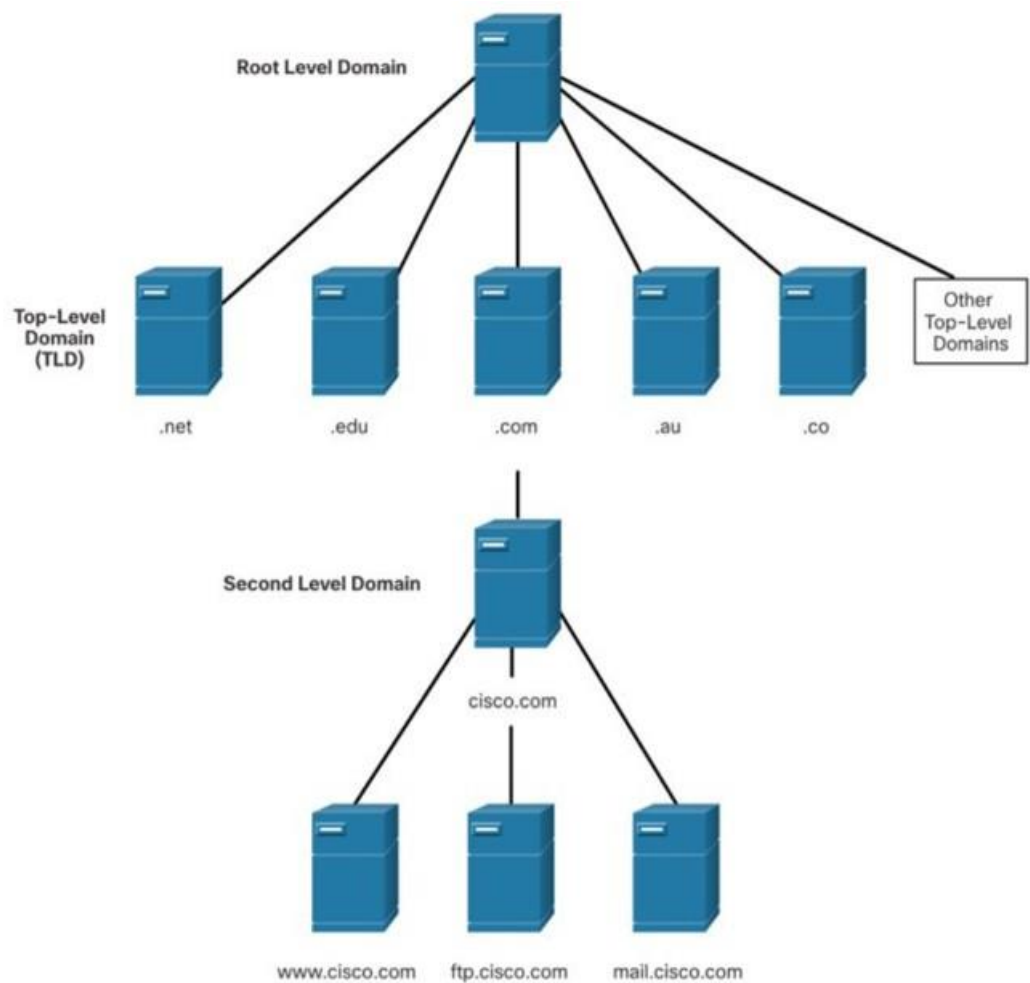


Figure 3.21: DNS hierarchical

- When a DNS server receives a request for a name translation that is not within its DNS zone, the DNS server forwards the request to another DNS server within the proper zone for translation.
- Examples of top-level domains:
  - .com-a business or industry
  - .org-a non-profit organization
  - .au-Australia

The nslookup Command:

- Nslookup is a computer operating system utility that allows a user to manually query the DNS servers configured on the device to resolve a given host name.
- This utility can also be used to troubleshoot name resolution issues and to verify the current status of the name servers.
- When the nslookup command is issued, the default DNS server configured for your host is displayed.
- The name of a host or domain can be entered at the nslookup prompt.

# Chapter 4

## security

### 4.1 Introduction

#### Identifying Network Device Planes

- Effective network security demands an integrated defense-in-depth approach.
- The first layer of a defense-in-depth strategy is the enforcement of the fundamental elements of network security.
- The security of a network device requires all three device planes to be secured.
- Configuring secure access to the network device, routing protocols, and other control features along with guaranteeing the security of the forwarded data mean to operate on three different planes: control plane, management plane, and data plane
- It is often beneficial to think of network devices in three separate contexts, as identified by their functionality planes: [fig 4.1](#)
- Data Plane functions are data switching and data routing. The data plane allows the device to forward network traffic and apply services (such as security, QoS, accounting, and optimization) to it as it is forwarded.

- Control Plane allows the device to build all of the required control structures (such as the routing table, forwarding table, and MAC address table) that will allow the data plane to operate correctly.
- Management Plane provides devices with all of the functions that administrators need to provision the configuration and monitor the operation of the device.

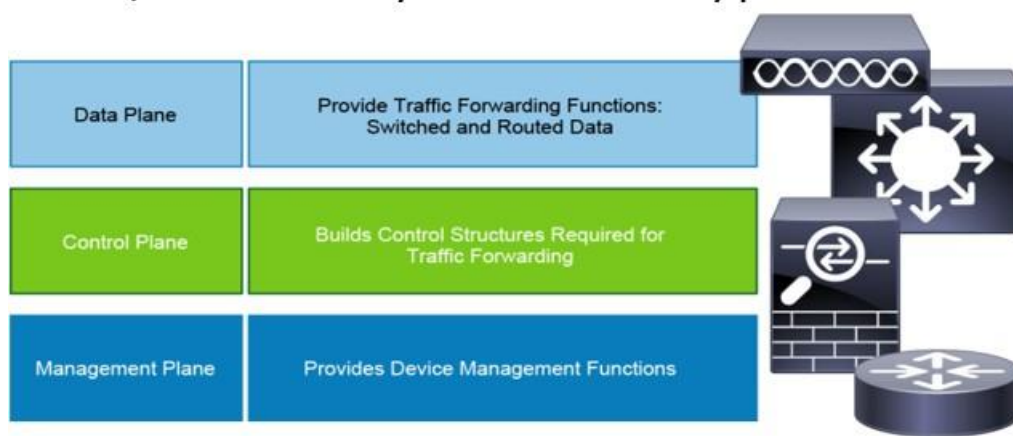


Figure 4.1: Identifying Network Device Planes

## 4.2 Control Plane Security Controls

It is divided into three mitigation techniques:

### 4.2.1 Infrastructure ACLs

- Because the CPU is shared among the three functions (control plane, management plane, slow data path), excessive traffic to one of these three functions can, by default, overwhelm the entire CPU and influence the behavior of the other two functions.
- This setup can lead to flooding attacks, in which the attacker can disable these three functions by sending a high rate of packets to the CPU.

- There are multiple possible countermeasures that guard against this threat, and one of them is the infrastructure access control list (ACL).
- Infrastructure ACLs filter traffic on the network edge of access OSI Layer 3 devices that accept IP traffic from network users or external networks. in fig  
Infrastructure ACLs are typically applied in the input direction on the interface that connects to the network users or external networks with the following policies:
- All traffic to the IP addresses of network infrastructure devices is dropped and logged.
- All other traffic is permitted and allows all transit traffic over the network.
- Also shutting down unused ports to prevent any outside access.

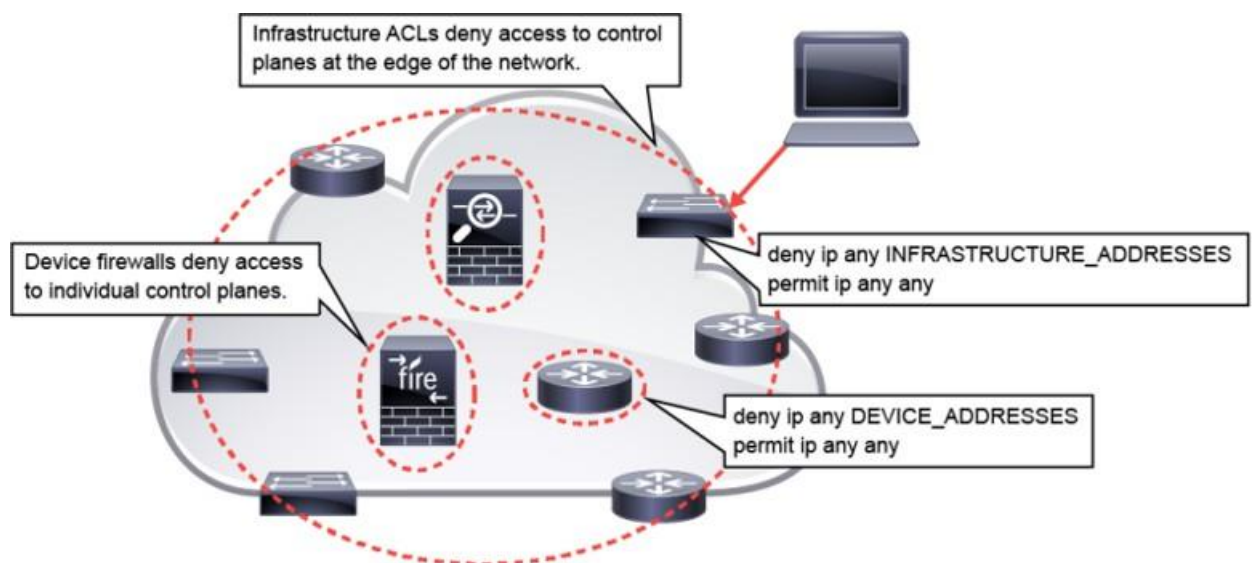


Figure 4.2: Infrastructure ACLs filter traffic

### 4.2.2 Control Plane Policing

- One more countermeasure that guards against control plane targeting threats is CoPP in fig . 4.3



- CoPP uses early rate limiting and drops traffic that is destined for the central processor of the network device by applying QoS policies to a virtual aggregate CPU- bound queue, called the "control plane interface."
- This queue receives all aggregated traffic that is destined for the control plane (which includes the routing protocols), the management plane (management processes), and the slow data plane path traffic of the network device.
- CoPP can granularly permit, drop, or rate-limit traffic to the CPU using a Modular QoS (MQC) CLI.
- Because CoPP aggregates all traffic that is forwarded to the CPU of the network device, it is independent of interfaces. fig 4.4

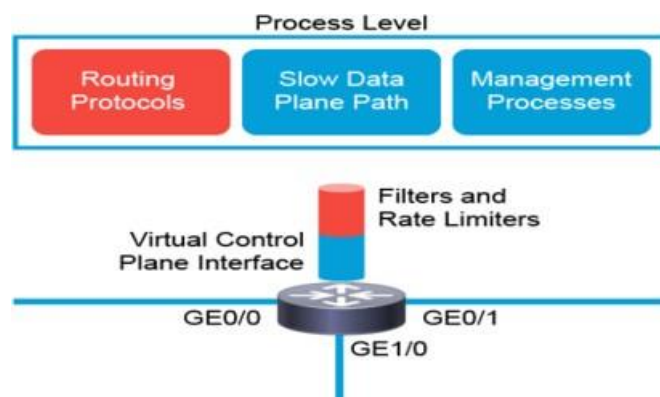


Figure 4.3: copp

### 4.2.3 Control Plane Protection

- CPPr extends the CoPP functionality by automatically classifying all CPU-bound traffic into three queues (or sub interfaces) under the aggregate control plane interface.
- Each sub interface receives and processes a specific type of CPU-bound traffic, and each sub interface has a separate traffic policy that is attached to it, which makes



Figure 4.4: CoPP aggregates traffic

the limit configuration easier.

- To configure CPPr, complete the following tasks:
  - Create traffic classes that describe valid control plane traffic.
  - Create a traffic policy that will permit, deny, or rate limit the configured traffic classes.
  - Apply the configured traffic policy to a required CPPr sub interface.

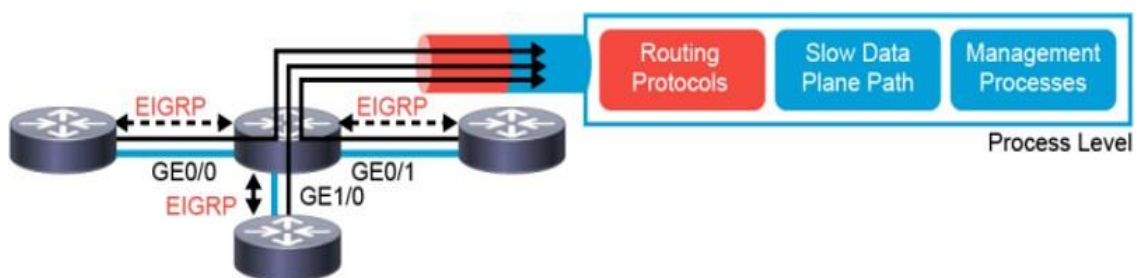


Figure 4.5: configured traffic to CPPr

- Configuration of Cpp and CPPr:

#ip access-list extended CPPR-OSPF	• Creating an access list with type extended
#permit ospf 192.168.6.0 0.0.0.255	• Ospf traffic from 192.168.6.0
#class-map CPPR-OSPF-CLASS	• Enables class map global configuration command mode used to create a traffic class.
#match access-group name CPPR-OSPF	• Specifies the match criteria for the class-map.
#policy-map CPPR-POLICY	• Enters policy map configuration mode to define a policy..
#class CPPR-OSPF-CLASS	• Enters class map configuration mode, which is used to associate a service policy with a class.
#police rate 200 pps conform-action transmit exceed-action drop	• To configure traffic policing, use the police command in policy-map class configuration mode or policy-map class police configuration mode.
#class class-default	• To configure the default traffic rate for other networks
#police rate 50 pps conform-action transmit exceed-action drop	• To configure traffic policing, use the police command in policy-map class configuration mode or policy-map class police configuration mode
#control-plane host	• applies policies to host control-plane traffic
#service-policy input control-plane-policy	• Applies the specified service policy to packets received on the control-plane.

Figure 4.6: configured CPPr

### 4.3 Layer 2 & 3 Data Plane Security Controls

Take the example of the image of a web browser and a web server communicating with each other. The two applications communicate with each other via a socket that is provided by the transport layer. Neither application is concerned with the complexity of the transport layer or any layer beneath the transport layer. Similarly, the transport layer depends on the network layer to carry packets to and from other systems based on IP addresses. The transport layer does not need to deal with the complexity of subnetting and routing. Also, the network layer depends on the data link layer to move frames between systems on the same broadcast domain, based on MAC addresses. Imagine, in this example, if Layer 2 is compromised at some point. Frames which should be passed between two neighboring routers are instead sent to a man-in-the-middle within that broadcast domain. Now, all traffic between the web browser and the web server is intercepted by man-in-the-middle, and none of the higher layers have any indication of the security breach.

Overview of Layer 2 Data Plane Security Controls. in fig 4.8

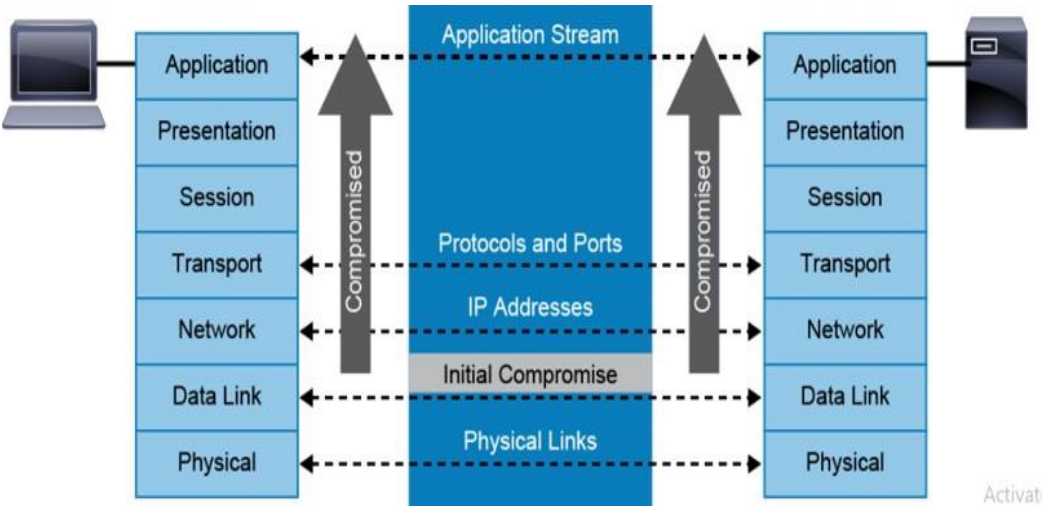


Figure 4.7: OSI module

Attack	Switched Infrastructure Countermeasure
VLAN hopping	Static access ports, disabling of Dynamic Trunking Protocol (DTP), avoidance of trunk native VLAN on access ports
STP spoofing	BPDU Guard/Root Guard
MAC spoofing	Port security
CAM flooding	Port security (MAC limit)
DHCP spoofing	DHCP snooping
DHCP starvation	Port security (MAC limit) or DHCP snooping rate limit
ARP spoofing	ARP inspection
LAN storm	Storm control

Figure 4.8: Overview of Layer 2 Data Plane Security Controls.

### 4.3.1 STP

Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on bridges and switches. The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network. Loops are deadly to a network. Spanning trees use an algorithm to search for the redundant links in the LAN and select the best paths. It is mainly used to put all links in either forwarding or blocking. After this process, all the links without a redundant link are likely to be in the forwarding state. The redundant links that were not as good as the selected links would be blocked. Spanning Tree never uses multiple links to the same destination. There is no load-sharing feature with Spanning Tree.

STP attacks:

- An attacker can exploit STP to attack a network. One of the hacking techniques is to implement a rogue switch at trunk ports and manipulate the spanning tree priority by configuring this rogue switch and giving it the lowest ID to become a root bridge. As a consequence, all the traffic will be transferred through this switch and then it will sniff all the traffic or redirect the traffic. To defend against STP attacks, you need to enable the root guard on all switch ports that you do not designate as root ports.
- BPDU attack is when an attacker attacks a device with edge ports and received by them, the device will automatically change the edge ports to non-edge ports and recalculate the spanning tree. If the bridge priority in the BPDUs sent by an attacker is higher than the priority of the root bridge, the network topology will change, thereby interrupting service traffic. To defend against BPDU attack BPDU protection is enabled on a switch, if an edge port on the switch receives a BPDU, the switch will shut down the edge port.

**STP Mitigation:**

General on switches : PortFast enables the switch to instantaneously transition from blocking state to forwarding state immediately, it is recommended on edge ports, because these ports typically do not send nor receive BPDU.

command :- spanning-tree portfast edge

On ports for protection : by command

spanning-tree bpduguard enable

spanning-tree guard root

In the proposed network STP is not used as there are no redundant paths but we added it for future if we added any redundant path.

### **4.3.2 MAC Spoofing**

MAC spoofing attacks involve the use of a known MAC address of another host to attempt to make the target switch forward frames that are destined for the remote host to the network attacker.

- By sending a single frame with the source MAC address of the other host, the network attacker overwrites the CAM table entry so that the switch forwards packets that are destined for the host to the network attacker.
- Until the host sends traffic, it does not receive any traffic. When the host sends out traffic, the CAM table entry is rewritten once more, so that it moves back to the original port.
- In the figure [4.3.2](#), traffic from Attacker 1 and Attacker 2 will be dropped at the switch because the source MAC addresses of the frames that are sent do not match the MAC addresses in the list of secured (allowed) addresses defined on the switch interfaces.

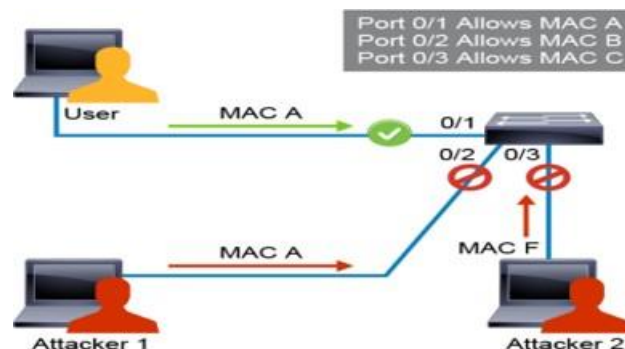


Figure 4.9: MAC Spoofing

### 4.3.3 CAM flooding

- In a MAC flooding attack (CAM table overflow attack), a network attacker can use a tool such as the macof program and flood the switch with many invalid source MAC addresses until the CAM table fills up.
- When that occurs, the switch begins to flood traffic for unknown MAC addresses to all ports because there is no room in the CAM table to learn any legitimate MAC addresses.
- The switch acts like a hub, As a result, the attacker can see all the frames that are sent from one victim host to another host without a CAM table entry.
- CAM table overflow floods traffic only within the local VLAN, so the intruder will see only traffic within the local VLAN to which the attacker is connected.
- In the figure 4.10, the macof program is running on host C.
- The macof program is one of many tools that can flood a switch with packets that contain randomly generated source and destination MAC addresses. Over a short period, the CAM table in the switch fills up until cannot accept new entries.

### Port security

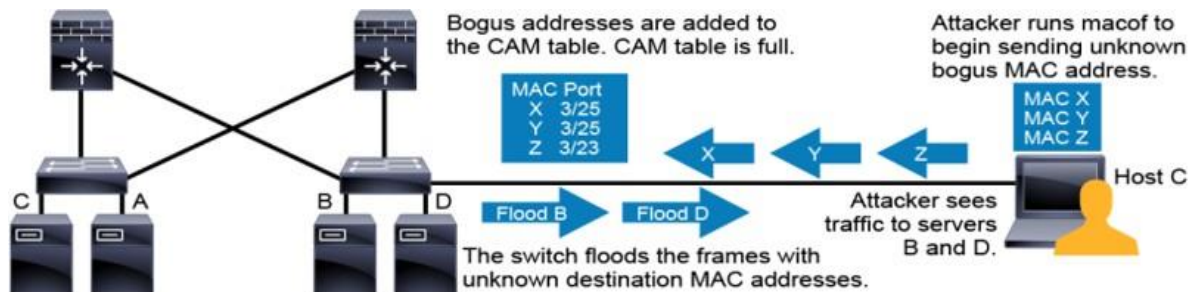


Figure 4.10: macof

- The port security feature restricts a switch port to a specific set or number of MAC addresses.
- The switch can learn these MAC addresses dynamically, or you can configure them statically on the device.
- Once an interface is configured with the port security feature, it accepts frames only from secure MAC addresses.
- When a violation occurs, the defined action applies to the interface.
- Due to these functionalities provided by the port security feature, it can be used for protection against:
  - MAC spoofing
  - MAC flooding Layer 2 attacks
- The reason for that is both these attacks operate by manipulating the MAC addresses of the frames when being sent to the switches.
- Therefore, the Port Security feature can deny any of those frames sent by the attacker with issues related to the MAC addresses.



- When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or dynamically learned on the port.
- If the arriving MAC address is on the list, it is processed normally.
- However, if the arriving MAC address is not on the list, but dynamic learning is enabled and there is room for an additional MAC address, it is added to the list and processed normally.

Configuration of port security:

- (config)# interface FastEthernet0/1
- (config-if)# switchport mode access
- (config-if)# switchport port-security
- (config-if)# switchport port-security maximum 2
- (config-if)# switchport port-security violation restrict
- (config-if)# switchport port-security mac-address sticky

To view port security settings for the switch

Switch# show port-security

#### 4.3.4 DHCP Attacks

- DHCP starvation attack is an attack that targets DHCP servers whereby forged, DHCP requests are crafted by an attacker with the intent of exhausting all available IP addresses that can be allocated by the DHCP server. Under this attack, legitimate network users can be denied service see fig 4.11.
- DHCP Spoofing Attack is when a malicious actor sets up an alternate DHCP server on a network to provide false addressing and configuration information to clients see fig 4.12.

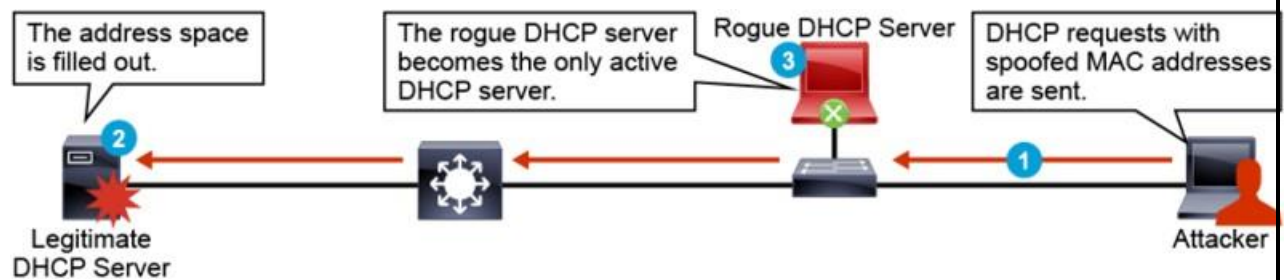


Figure 4.11: DHCP starvation attack

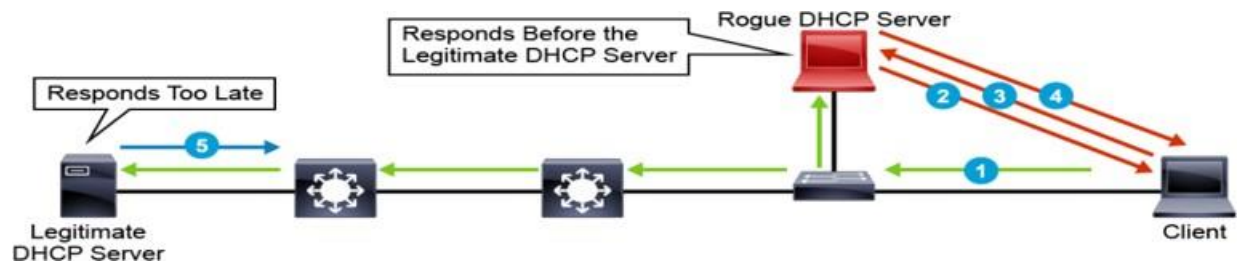


Figure 4.12: DHCP Spoofing Attack

### Mitigation

- **DHCP starvation attack** : One way to prevent a DHCP starvation attack on a network is through port security. Port security is a layer 2 traffic control feature on switches. Switches learn MAC addresses when a frame is forwarded through a switch. By using port security, a limit of the number of source MAC addresses that a port can allow can be set.
- **DHCP Spoofing Attack** : The DHCP snooping feature can be used to mitigate a DHCP server spoofing attack. With this mechanism switch ports are configured in two different states, the trusted and untrusted state. If a port is configured to be

trusted, it can receive DHCP responses. In other way, if a port is untrusted, it is not allowed to receive DHCP responses, and if a false attackers DHCP response attempts to enter an untrusted port, the port will be disabled

configured DHCP mitigation

ip dhcp snooping

interface GigabitEthernet0/0

no shutdown

switchport trunk encapsulation dot1q

switchport trunk native vlan 99

switchport mode trunk

ip arp inspection trust

negotiation auto

no cdp tlv app

channel-group 2 mode active

ip dhcp snooping trust

- The trusted port at our proposed network

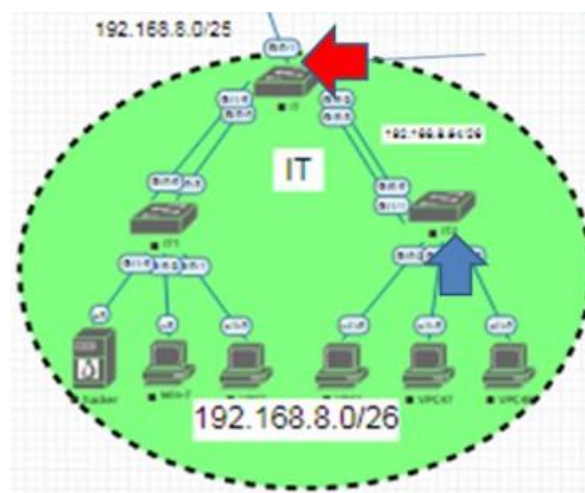


Figure 4.13: trusted port at our proposed network

### 4.3.5 ARP Inspection

- Devices that use IP addresses need ARP to map IP network addresses to MAC hardware addresses.
- Before a device sends a datagram to another device on the same subnet, it looks in its ARP cache to see if there is a MAC address that corresponds to the destination IP address.
- If there is no entry, the source device sends a broadcast ARP request to every device on the network.
- Each device compares the IP address to its own.
- The device with the matching IP address sends an ARP reply containing its MAC address.
- The source device adds the destination device MAC address to its ARP table (ARP cache) for future reference and will use that MAC address in the Layer 2 header for subsequent communication.
- ARP protocol does not provide any protection on its own.
- Therefore, the protocol itself is very susceptible to ARP attacks.
- ARP spoofing attack, also known as ARP cache poisoning target, hosts, switches, and routers that are connected to your Layer 2 network.
- This targeting is achieved by poisoning the ARP caches of systems that are connected to the subnet and by intercepting traffic that is intended for other hosts on the subnet.
- An ARP spoofing attack can result in a man-in-the-middle situation.

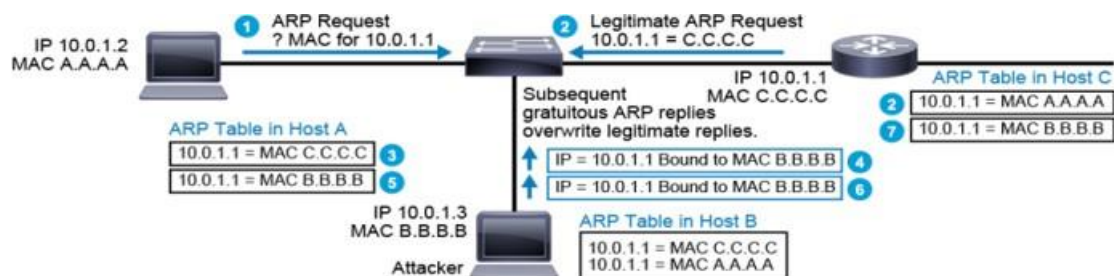


Figure 4.14: ARP Inspection

### Mitigation

- This ARP vulnerability in the infrastructure can be addressed in several ways:
  - Static ARP inspection or Dynamic ARP Inspection (DAI) enabled on network switches.
  - Static ARP entries on infrastructure devices; therefore, no use of ARP at all on critical segments.
- To prevent ARP spoofing, or poisoning, a switch can process transit ARP traffic to ensure that only valid ARP requests and responses are relayed.
- The Dynamic ARP inspection (DAI) feature of Cisco switches prevents ARP spoofing attacks by intercepting and validating all ARP requests and responses.
- Each intercepted ARP reply is verified for valid MAC-to-IP address bindings before it is forwarded.
- ARP replies with invalid MAC-to-IP address bindings are dropped.
- ARP inspection can determine the validity of an ARP reply that is based on bindings that are stored in a DHCP snooping database for DHCP-addressed hosts.

- As with DHCP snooping, ARP inspection labels all switch ports as trusted or untrusted.
- In a typical network configuration, define all access switch ports that are connected to host ports as untrusted and all switch ports that are connected to other switches as trusted.

#### Configuration

```
(config)# interface FastEthernet 0/2 (config-if) # ip dhcp snooping trust
```

```
(config)# int range gig 0/0-3
```

```
(config-if-range)# ip arp inspection limit rate 50
```

```
(config-if-range)# ip arp inspection
```

## 4.4 ACLs

Cisco ACLs use permit/deny statements. Filter packets on selected network interface. Different ACL types are used based on requirements. Max 2 ACLs allowed on Cisco interface. This would include a single IP ACL applied inbound and outbound. Cisco ACL best practices: apply extended ACLs near source, standard near destination, and order multiple statements from specific to general. Maximum two ACLs for Cisco interface. Only one ACL allowed per interface per Layer 3 protocol. Best practices for creating and applying ACLs. Admin should apply ACL closest to dest. ACL statement includes source IP and wildcard mask. One name/number is used for multiple statements in the same ACL. Older and general Standard ACLs: They may filter traffic incorrectly. Standard ACLs near destination prevent over-filtering. Apply extended ACL at source. Extended ACLs offer precise filtering options. Incl. source address, dest. address, Protocols & port numbers. Use closest extended ACLs to source to prevent filtered traffic in network. Saves bandwidth and processing at each router hop. Some ACLs have multiple statements. Statement orders crucial for ACL processing. The router cycles through

statements until a match is found, starting from the top. My pocket dropped without a match. List ACL statements from specific to general. Least specific statements first can lead to false matches. The ACL statement match does not happen. Specific ACL statements have shorter wildcard masks. Configures subnets to match. App protocols/ports are specified. The first ACL statement is more specific than the second. in proposed Network you can see the ACL in Fig 4.15.

VLAN	SPEAK
HR	ALL
MANG (GR)	HR-IT1-IT2
CS	SALE-IT1-HR
SALE	CS-IT1-HR
IT1	IT2-SALE-HR-MANG-CS
IT2	IT1-ACC-PRO-MANGE-HR
ACC	HR-IT2
PROD	HR-IT2

Figure 4.15: ACL in proposed Network

```

VPC51
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version supporting unetlab by unetlab team

Press '?' to get help.

Executing the startup file

DDORA IP 192.168.7.198/26 GW 192.168.7.193

VPCS> ping 192.168.8.70

*192.168.6.30 icmp_seq=1 ttl=254 time=16.329 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.6.30 icmp_seq=2 ttl=254 time=10.549 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.6.30 icmp_seq=3 ttl=254 time=11.726 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.6.30 icmp_seq=4 ttl=254 time=9.358 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.6.30 icmp_seq=5 ttl=254 time=14.363 ms (ICMP type:3, code:13, Communication administratively prohibited)

VPCS>

```

Figure 4.16: for try the device in it2 to ping with sale in proposed Network

## 4.5 Security devices and services

Network security consists of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. To ensure secure communications across both public and private networks, you must secure devices including routers, switches, servers, and hosts. Most organizations employ a defense-in-depth approach to security. It requires a combination of networking devices and services working together. Several security devices and services are implemented

- Firewall
- IPS

### 4.5.1 Firewall

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules. Firewalls are commonly used to protect networks from unauthorized access, malware, and other security threats. There are several types of firewalls, including:

- Packet-filtering firewalls: These firewalls examine each incoming and outgoing packet and allow or block it based on predefined rules. Packet-filtering firewalls are typically fast and easy to configure, but they provide limited security.
- Stateful firewalls: These firewalls maintain information about each network connection and use that information to make decisions about whether to allow or block traffic. Stateful firewalls are more secure than packet-filtering firewalls, as they can detect and block more advanced threats.
- Application-level gateways: These firewalls inspect the application-layer data in network traffic to ensure that only authorized traffic is allowed through. Application-



level gateways are highly secure but can be slower and more complex to set up than other firewall types.

- Next-generation firewalls: These firewalls combine the features of other firewall types and add advanced security capabilities, such as intrusion prevention, deep packet inspection, and user identification. Next-generation firewalls provide the highest level of security but can be expensive and complex to manage.

Each type of firewall has its own strengths and weaknesses, and the best type of firewall for a particular network depends on the network's security requirements and the resources available to manage the firewall. As a security engineer, it is important to understand the different types of firewalls and their capabilities to select the most appropriate firewall for your organization's needs.

<b>Allow</b> traffic from any external address to the web server.	<b>Deny</b> all inbound traffic with network addresses matching internal-registered IP addresses.
<b>Allow</b> traffic to FTP server.	<b>Deny</b> all inbound traffic to server from external addresses.
<b>Allow</b> traffic to SMTP server.	<b>Deny</b> all inbound ICMP echo request traffic.
<b>Allow</b> traffic to internal IMAP server.	<b>Deny</b> all inbound MS Active Directory queries.
	<b>Deny</b> all inbound traffic to MS SQL server queries.
	<b>Deny</b> all MS Domain Local Broadcasts.

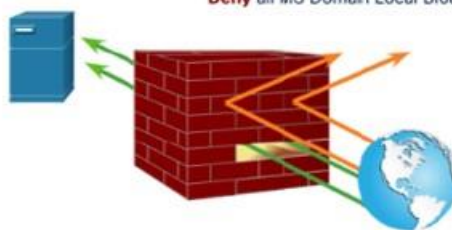


Figure 4.17: firewall advantage

### 4.5.2 IPS

An Intrusion Prevention System (IPS) is a network security device that monitors network traffic and actively prevents security threats, such as malware, viruses, and other malicious activities. IPS systems work by inspecting network traffic and comparing it against a set of pre-defined security rules. If the IPS detects any suspicious activity, it can take action to block the traffic or alert network administrators. IPS systems are designed to complement firewalls and other network security devices by providing an additional layer of security. Unlike firewalls, which primarily focus on blocking traffic based on predefined rules, IPS systems can detect and prevent more advanced threats, such as zero-day attacks, buffer overflow attacks, and SQL injection attacks. There are two types of IPS systems: network-based IPS (NIPS) and host-based IPS (HIPS). NIPS systems are placed at strategic points in a network, such as at the network perimeter or between network segments and can monitor all traffic passing through those points. HIPS systems, on the other hand, are installed on individual hosts and can monitor network traffic on that host, as well as the activities of applications running on that host. IPS systems can operate in two modes: inline mode and passive mode. In inline mode, the IPS sits between the source and destination of network traffic and can actively block traffic that violates security policies. In passive mode, the IPS is placed in a monitoring role and only alerts network administrators to potential security violations without actively blocking traffic. IPS systems use a variety of techniques to detect and prevent security threats, including signature-based detection, anomaly-based detection, and behavior-based detection. Signature-based detection involves comparing network traffic to a database of known attack signatures. Anomaly-based detection involves monitoring network traffic for unusual patterns or behaviors that may indicate an attack. Behavior-based detection involves analyzing the behavior of users and applications on the network to detect suspicious activity. in fig 4.18 shows how an IPS handles denied traffic.

- The threat actor sends a packet destined for the target laptop.

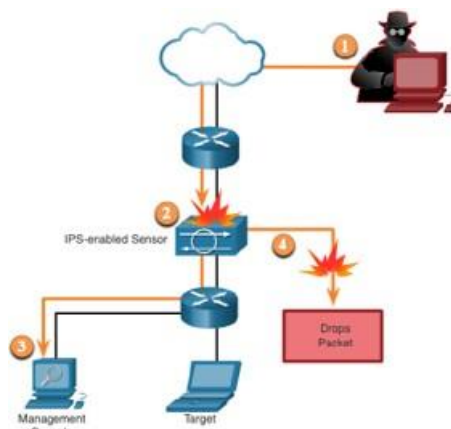


Figure 4.18: ips handles denied traffic

- The IPS intercepts the traffic and evaluates it against known threats and the configured policies.
- The IPS sends a log message to the management console.
- The IPS drops the packet.

# Chapter 5

## Firewall

### 5.1 firewall zone

- Inside zone : this is the internal network (LAN)
- outside zone : this is the public network can anyone to connect with it
- The Demilitarized Zone (DMZ) refers to a discrete physical or logical subnet that serves to segregate a local area network (LAN) from other potentially hostile external networks, such as the publicly accessible Internet. DMZs are alternatively referred to as perimeter networks or screened subnetworks in academic discourse. It is recommended that any service offered to users on the public internet be located within the DMZ network. Typically, external-facing servers, resources, and services are situated in that particular domain. Several routine services that are frequently utilized include those pertaining to web hosting, electronic messaging (email), and the domain name system. The servers and resources located in the Demilitarized Zone (DMZ) exhibit accessibility to external networks, whilst the remainder of the internal Local Area Network (LAN) remains inaccessible. This methodology confers an adjunct stratum of safeguarding to the local area network (LAN) by impeding the hacker's capability to have direct ingress to internal servers

and information from the worldwide web.

## 5.2 cisco ASA VS cisco NGFW

- Traditional firewall ASA firewall :
  - Packet Filtering with ACL
  - Stateful Inspection
  - Application Inspection
  - NAT
  - DHCP Server or Client
  - Static Routing and Routing Protocols RIP, EIGRP, OSPF
  - L3 Firewall or L2 Firewall
  - VPN Gateway (IPsec and SSL)
  - Botnet Traffic Filtering
- Cisco Firepower NGFW
  - All the ASA feature + IPS
  - provides a top-notch performance whereas ASA ranks lower in it.
  - ASA is quite expensive in comparison with Cisco FTD, which is highly affordable.
  - Cisco FTD consumes less time whereas ASA consumes more as it requires an ample amount of manual work.

## 5.3 cisco NGFW (FTD)

### Cisco Firepower NGFW Deployments

- Cisco Firepower NGFW is the Cisco next generation network security appliance, offering NGFW services such as Cisco URL Filtering, application control and visibility, advanced malware protection, and so on.
- It also offers Intrusion Prevention System (IPS) services in a single agile platform.
- The Cisco Firepower NGFW runs a unified image of Cisco FTD and Cisco ASA code to offer all the NGFW services and IPS services from Cisco Firepower plus features such as NAT, VPNs, and so on from the ASA. fig 6.3.1 Cisco Firepower NGFW Deployments

Managed by using the central Cisco Firepower Management Center (FMC) or the local Cisco Firepower Device Manager (FDM).

- Cisco FMC provides deep analytic capabilities and application programming interface (API) integration that is not provided by the Cisco FDM and FMC is supported high availability
- Both Cisco Firepower NGFW and Cisco FMC can be physical or virtual appliances.
- Physical or virtual FMCs can manage virtual or physical Cisco Firepower NGFW appliances.
- Cisco FMC can be used to manage the Cisco FTD system.
- Cisco FMC is a purpose-built network appliance that provides a centralized management console and database repository for your Cisco Firepower deployment.

- You can monitor the information that your devices report and assess and control the overall activity that occurs on your network. Cisco FMC also controls the network management features on your devices: switching, routing, NAT, VPN, and so on

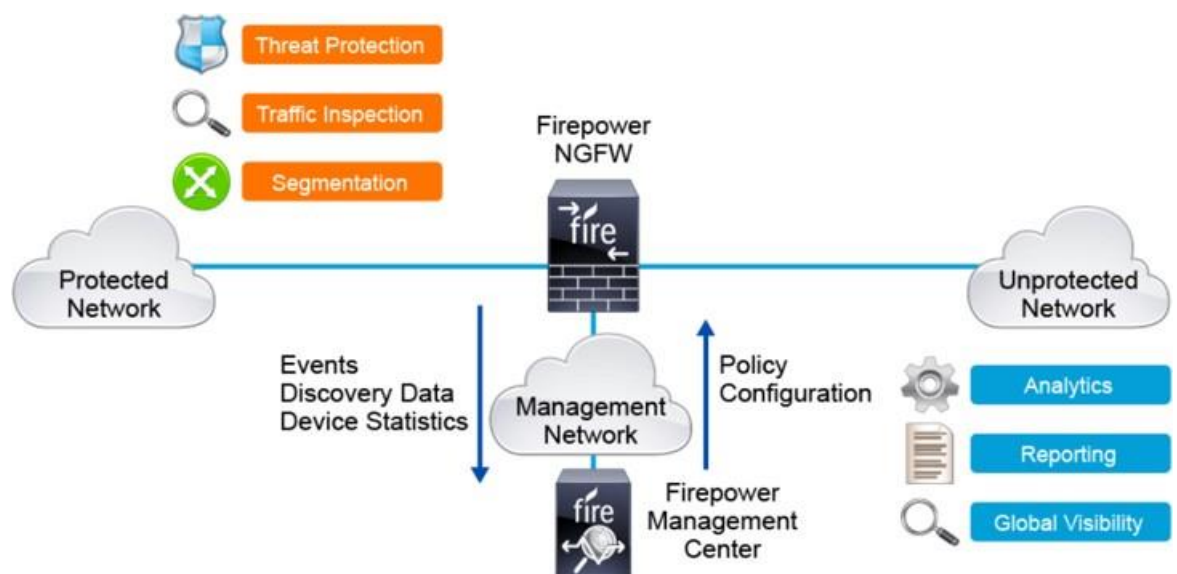


Figure 5.1: Cisco Firepower NGFW Deployments

## 5.4 FTD to FMC registration

You need to register the Cisco Firepower NGFW with Cisco FMC. Let us start the steps.

- Install FTD and FMC in eve machine after installation we give ip to FTD and FMC in proposed Network (FTD :192.168.100.3/29– FMC:192.168.100.2/29)
- In FTD write configure manger add( IP address of FMC) (registration key )
- By opening the windows in management region and writing the IP address of FMC in Google chrome or any browser and select the Devices and select add see fig ?? then choose device or group if we have more than one FTD we use group and device if one (see fig ??) in proposed Network we use group and device

- In host we write the IP address of FTD and in display name we write the name of FTD then write the registration key the same in point of 2 then choose the group if found and choose the accesses group policy if don't found we create the policy and choose the three smart licenses and register See fig 5.4



Figure 5.2: FTD Device

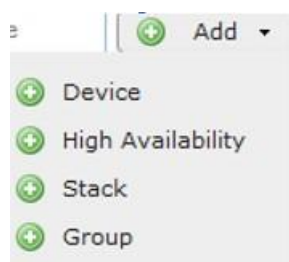


Figure 5.3: Add devices

## 5.5 FTD connect the inside zone with outside zone

- Routing: In proposed Network we use default (int g0/1 use with the internal network and g0/0 use in outside) as it we do not make routing in proposed Network
- The NAT policy: we agree for any network in inside region to convert it Ip address from private to public. See fig 5.5
- Access control policy: we determine whether the network can go outside or DMZ or deny. 5.6



**Add Device**

Host: †

Display Name:

Registration Key: \*

Group:

Access Control Policy:

**Smart Licensing**

Malware: ☐

Threat: ☐

URL Filtering: ☐

**Advanced**

Unique NAT ID: †

Transfer Packets: ☒

On Firepower Threat Defense devices version 6.2.1 onwards, AnyConnect VPN licenses can be enabled from [smart license page](#)

† Either host or NAT ID is required.

Register Cancel

Figure 5.4: FTD to FMC registration

- If you connect the FTD with router we make use OSPF to connect the router with FTD . (see fig 5.7)

Overview

Analysis

Polices

Devices

Objects

AMP

Intelligence

Deploy

System

Help

admin

Device Management

NAT

VPN

QoS

Platform Settings

FlexConfig

Certificates

NAT1

Enter Description

Save

Cancel

Policy Assignments (1)

Rules

Filter by Device

Add Rule

Original Packet

Translated Packet

#	Direction	Ty...	Source Interface ...	Destination Interface ...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											
1	➡	Dyn...	INSIDE	OUTSIDE	any-ipv4			Interface			Dns: false
▼ Auto NAT Rules											
▼ NAT Rules After											

Figure 5.5: FTD NAT

## 5.6 FTD object

Objects are reusable containers that define criteria that you want to use in policies or other settings. For example, network objects define host and subnet addresses. Or use

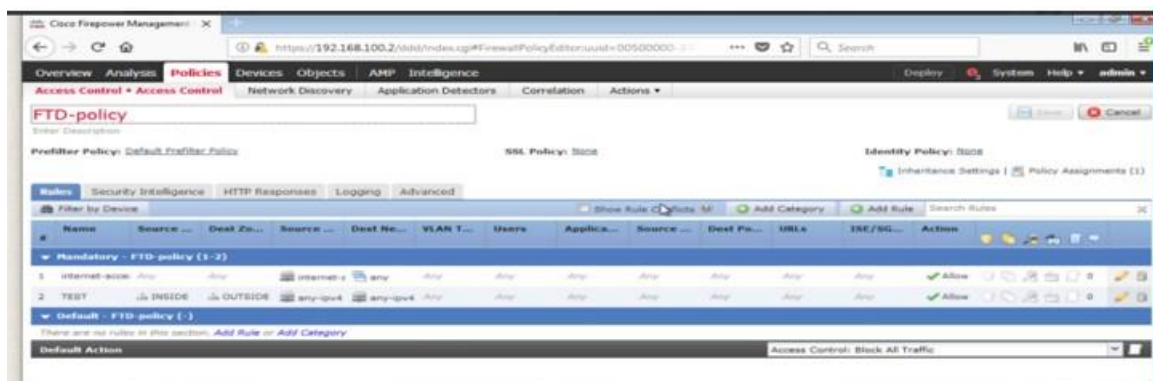


Figure 5.6: ACP in FTD



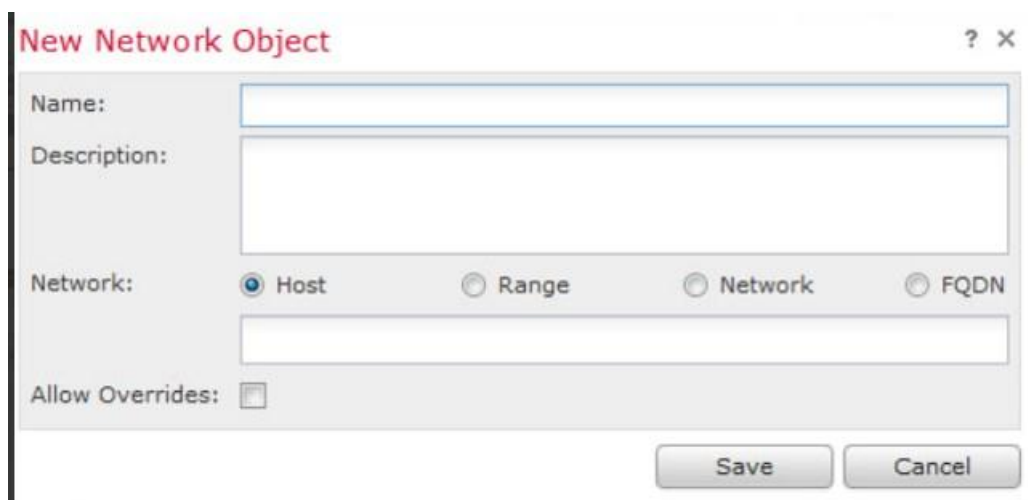
Figure 5.7: OSPF with FTD

for port or DNS object.

- Cisco FMC uses objects in various areas of your Cisco Firepower System.
- Prior to configuring different policies in Cisco Firepower, you can define certain objects that are used to label a variable, or number of variables, of a similar type.
- These objects will be referenced later in the implementation process.
- Objects are used throughout the system, with the most common use in ACP.
- Objects are containers used throughout the Cisco Firepower NGFW configuration.
- Objects are reusable configurations that associate a name with a value. When you want to use that value, use the named object instead.

For network object

- Host: if I determine one IP address
- Range: range of IP address I will do something with it
- Network: the whole network will do something with it
- FQDN: A complete designation of a network host or computer is a fully qualified domain name (FQDN) within the internet infrastructure. The precise positioning of a system within the domain name system (DNS) is facilitated by the provision of information pertaining to the hostname, the domain name, and the top-level domain (TLD). According to Figure 5. 8, the newly introduced network object FTD incorporates Access Control Policy (ACP) as a hierarchical policy-based feature that enables the specification, inspection, and logging of network traffic. It must be noted that every Cisco Firepower NGFW device that is managed is allocated a single ACP.



**New Network Object** ? x

Name:

Description:

Network: ☒ Host ☐ Range ☐ Network ☐ FQDN

Allow Overrides: ☐

Save Cancel

Figure 5.8: New Network Object

## 5.7 FTD Access control policy

Access control is a hierarchical policy-based feature that allows you to specify, inspect, and log network traffic

- Each managed Cisco Firepower NGFW device is assigned one ACP.
- ACP is the central part of configuring firewall functionality and is used to:
  - Allow or block traffic based on simple or more sophisticated traffic characteristics.
  - Send traffic to further analyses to IPS or file policy for inspection of malicious traffic.
  - Make decisions whether to log traffic as connection events.
  - Manage security intelligence, SSL decryption, authentication, and other advanced firewall and IPS settings.
- The ACP consists of rules that are processed using a top-down, first match approach.
- When traffic matches configured conditions inside a rule, the ACP applies the configured action for that rule, which can allow, block, or send traffic to further analyses.
- If traffic matches no rules, then the system applies the action defined in the default action of the ACP.
- The only exception to the first match rule is monitor action, which only logs traffic, and continues matching against the subsequent ACP rules.
- A Cisco Firepower NGFW device must have an ACP applied to perform operations, and only one ACP can be applied to a device at any given time.
- However, it is typical to create many ACPs to manage changed environments.

- ACPs use hierarchical implementation that can be used for multitenancy.
- ACPs can be nested, where descendant ACP inherits rules and settings from its direct parent policy.
- Traffic requires an ACP to proceed through the system.
- Each ACP has a name that allows unique identification inside the system.
- In proposed Network will be make 4 rules as network in inside (it1,it2,hr,manger,cs,sale) can go outside and any network in inside can connect to DMZ zone and the outside zone can connect with DMZ .
- Each ACP rule consists of:
  - Name: used to uniquely identify a rule.
  - Conditions: identify the type of traffic that the rule handles. A rule can have multiple conditions. Traffic must match all the conditions in the rule for the rule to apply to traffic.
  - Action: Each rule must have an action associated with it. The action specifies what happens with traffic that matched a rule.
  - IPS and file policy inspection settings: Influence if traffic will be sent for further analyses to IPS policy to detect malicious traffic or to file policy to detect prohibited files or malware-infected files.
  - Connection logging settings: Determine if traffic will be logged as connection events.
- ACP rule action in [5.10](#) :
  - Allow: allows matching traffic to pass. However, depending on your requirements, you can perform further inspection to inspect network traffic before

it reaches its destination. Traffic is also subject to security intelligence and network discovery.

- Trust: allows traffic to pass without further inspection of any kind, including network discovery. Based on configured conditions, the system may also skip security intelligence checks.
- Block and block with reset: deny traffic without further inspection of any kind. Block with reset also resets the connection.
- Interactive block and block with reset: deny traffic without further inspection of any kind. Block with reset rule also resets the connection. For HTTP traffic, when the system blocks a web request, a user can override the default browser or server page with a custom page that explains that the connection was denied. The system calls this custom page an HTTP response page.
- Monitor: does not affect traffic flow, matching traffic is only logged and neither permitted nor denied. Rather, traffic is matched against additional rules to determine whether to allow or block it.

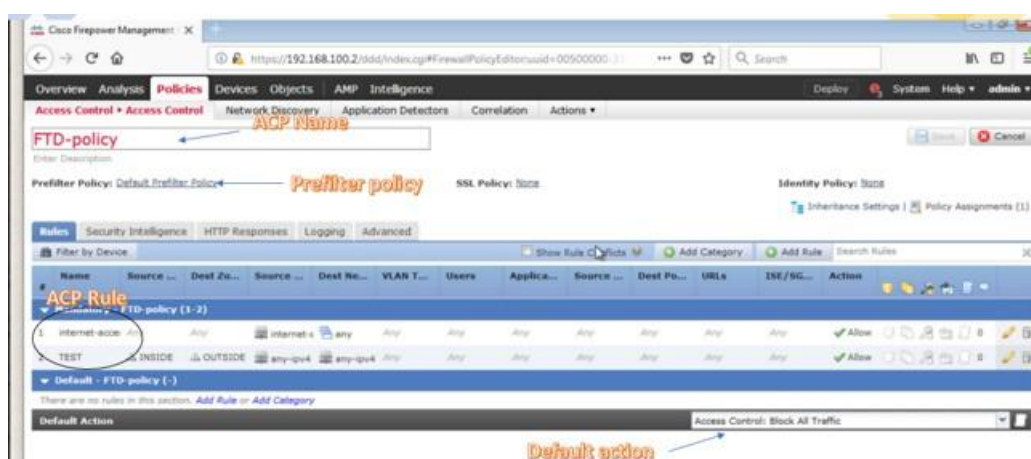


Figure 5.9: ACP details



Figure 5.10: ACP rule action

## 5.8 FTD layer of defense

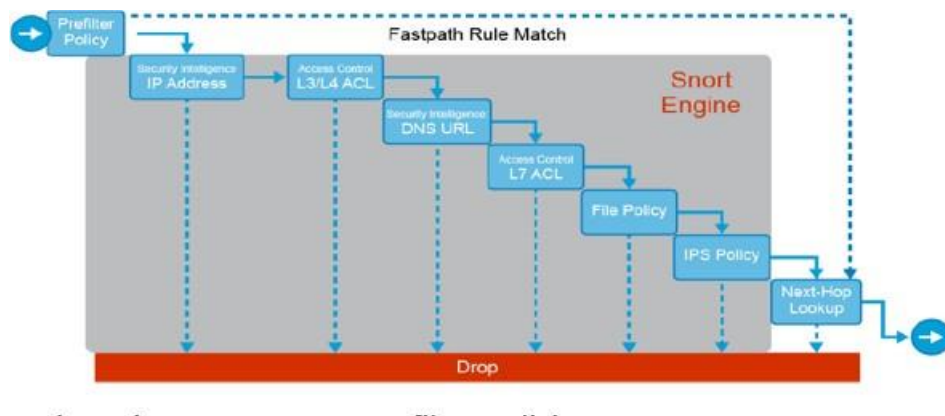


Figure 5.11: FTD layer of defense

### 5.8.1 Cisco Firepower NGFW Prefilter Policies

- Traffic arriving at Cisco Firepower NGFW device is processed by Cisco ASA and Snort engine.
- Prefilter policy is the first line of a defense inside the Cisco ASA engine which can be used to protect your network from undesired traffic.
- Prefilter policy consists of rules that are evaluated using the top-bottom approach.
- Each rule consists of simple conditions and associated actions.
- There are two reasons to use prefilter policies:



Figure 5.12: ]  
Prefilter policy

- Improves performance of Cisco Firepower NGFW system by blocking traffic early or exempting traffic from further (Snort) inspection, based on simple Layer 3 and Layer 4 conditions.
- Provide inspection for tunneled traffic based on tunnel endpoints, IP addresses, and encapsulation types. The following actions are available when configuring prefilter rules: We have three actions in prefilter
  - \* Block: discard traffic without further inspection.
  - \* Fast path: permits traffic without sending the traffic to Snort inspection.
 

On certain Cisco Firepower platforms, fast pathed flows are eligible for flow offload functionality where traffic is switched inside a network interface card.
  - \* Analyze: sends traffic to further (Snort) inspection, based on configured ACP rules.
- The policy consists of four rules:
  - \* The first rule is the prefilter rule and blocks Telnet traffic from In Zone going to Dmz Zone, based on destination TCP port. Note that a TELNET object does not represent the application, but is a port object, representing TCP port 23.
  - \* The second rule is prefilter rule and allows voice traffic from In Zone going to Dmz Zone, based on destination UDP ports. The traffic is fast pathed, thus skipping all Snort inspections.



- \* The third rule is the tunnel rule and matches GRE traffic. Traffic is sent for further analyses to ACP, where it could be matched based on inner header and inspected using Snort inspection.
- \* The last rule is the tunnel rule and immediately blocks Teredo IPv6 tunnels.

### 5.8.2 Cisco Firepower NGFW Security Intelligence



Figure 5.13: Security Intelligence

- As a first line of defense against malicious traffic, the Cisco Firepower NGFW device uses the security intelligence feature, which allows you to immediately blacklist (block) connections, based on the latest reputation intelligence, removing the need for a more resource-intensive, in-depth analysis.
- Security intelligence functionality also generates special events, called security intelligence events, when a connection matches a blacklisted object.
- Security intelligence works by matching traffic against a whitelist and a blacklist and blocking traffic to or from IP addresses, URLs, or DNS that are on the blacklist.
- The fig 6.8.3 in the Cisco Firepower NGFW processing pipeline security intelligence takes place.
- Filtering based on IP addresses takes place immediately after prefilter policies and as a first step inside an ACP.

- In case of filtering based on URLs or DNS names, the system first performs SSL decryption, since requested URLs may be sent inside an encrypted SSL session.
- Security intelligence blacklist and whitelist objects are managed inside Cisco FMC object manager.
- Security intelligence places traffic into two categories
  - Blacklist:
    - \* For traffic that is considered malicious.
    - \* Matching traffic is blocked or monitored. For blocked traffic no further inspection is performed.
  - Whitelists:
    - \* Used to override objects that appear in blacklist.
    - \* Whitelist matches do not generate events

### **5.8.3 Cisco Firepower NGFW Discovery Policies**

- Cisco Firepower Discovery is the process of collecting information about hosts and users in your environment.
- Cisco Firepower inspects the traffic passing through the Cisco Firepower NGFW to
  - discover both users and hosts. Hosts are discovered by configuring a discovery policy.
- Discovery is an integral part of the Cisco Firepower System.
- The data collected about hosts, applications, operating systems, services, users, and vulnerabilities is used throughout the system for analysis and automation of

- security protection: The network discovery policy is how you manage your discovery information.
- Upon initial setup, the network discovery policy is not configured to perform host discovery.
- A host profile provides a complete view of all the information that the system has gathered about a single host.
- Host profiles can also provide you with the following information:
  - IP address of the host.
  - The operating system running on a host.
  - The servers running on a host.
  - The clients and web applications running on a host.
  - The protocols running on a host.
  - The IOC tags on a host.
  - The VLAN tags on a host.
  - The last 24 hours of user activity on your network.
  - The most recent malware events for a host.
  - The vulnerabilities associated with a host.
  - The Nmap scan results for a host.
- Vulnerabilities are automatically assigned to a host based on the operating system, applications, and services seen on the discovered host.
- For example, Cisco Firepower NGFW detects Windows 7 on the host.
- This information on operating system will be added to the operating system section of the host profile, along with any vulnerabilities associated to that version

of Windows 7. Vulnerabilities for your host profiles come from the Vulnerability Database (VDB) in the Cisco Firepower System and are automatically populated based on what is detected on that host.

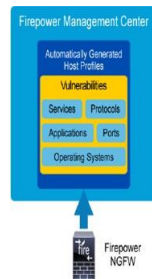


Figure 5.14: Cisco Firepower NGFW Discovery Policies

#### 5.8.4 Cisco Firepower NGFW IPS Policies

- intrusion policies are defined sets of intrusion detection and prevention configurations that inspect traffic for security violations and can block or alter malicious traffic.
- Intrusion policies are invoked by your ACP and are the system's last line of defense before traffic is allowed to its destination.
- Snort is free, open-source software that acts as a network intrusion detection system.
- Cisco Firepower technology is based on this software. An intrusion rule, also known as a Snort rule, is a specified set of keywords and arguments that the system uses to detect attempts to exploit vulnerabilities in your network.
- As the system analyzes network traffic, it compares packets against the conditions specified in each rule and triggers the rule if the data packet meets all the conditions specified in the rule. Snort rules can be created by anyone.

- Snort is a free, open-source system. You have the option to create your own Snort rules and import them into the Cisco FMC.
- The Cisco Firepower System is shipped with all available Snort rules that are regularly updated by Cisco Talos.

### **5.8.5 Cisco Firepower NGFW Malware and File Policies**

- Cisco Firepower gives you means to detect the movement of files in your networks and to take appropriate action. For example, office documents that are exchanged between users in internal
- network segments may be part of normal collaboration between co-workers, but documents that are sent to outsiders can indicate sensitive data leakage. With the file detection feature, you can choose to simply be alerted, or you can block the file and prevent it from leaving the enterprise.

# Chapter 6

## Servers

### 6.1 Introduction

A server is a computer program or a device that provides functionality for called clients which are other programs or devices. This architecture is called the client–server model. A single overall computation is distributed across multiple processes or devices. Servers can provide various functionalities called services. These services include sharing data or resources among multiple clients or performing computation for a client. Multiple clients can be served by a single server, and a single client can use multiple servers. A client process may run on the same device. It can also connect over a network to a server to run on a different device. Example of servers may include database servers, mail servers, print servers, file servers, web servers, application servers, and game servers.

### 6.2 servers and services in proposed network

In the proposed network we will use two main servers, the Web server and FTB server and talk about mail server.

- File server: Shares files and folders, storage space to hold files and folders, or both,

over a network. Networked computers are the intended clients, even though local programs can be clients.

- **Web server:** These servers host web pages. A web server is responsible for making the World Wide Web possible. Each website has one or more web servers. Their clients are computers with a web browser.
- **Mail server:** These servers make email communication possible in the same way as a post office makes snail mail communication possible. Clients of these servers are senders and recipients of email.

## **6.3 File sharing services (File Transfer Protocol)**

### **6.3.1 What is FTP (File Transfer Protocol)?**

- FTP (File Transfer Protocol) is a network protocol for transmitting files between computers over (TCP/IP) connections. Within the TCP/IP suite, FTP is considered an application layer protocol.
- In an FTP transaction, the end user's computer is typically called the local host. The second computer involved in FTP is a remote host, which is usually a server. Servers must be set up to run FTP services, and the client must have FTP software installed to access these services.
- FTP was developed to allow for data transfers between a client and a server. An FTP client is an application which runs on a computer that is being used to push and pull data from an FTP server.

### 6.3.2 How does FTP work?

- Step 1 - The client establishes the first connection to the server for control traffic using TCP port 21. The traffic consists of client commands and server replies.
- Step 2 - The client establishes the second connection to the server for the actual data transfer using TCP port 20. This connection is created every time there is data to be transferred.
- Step 3 - The data transfer can happen in either direction. The client can download (pull) data from the server, or the client can upload (push) data to the server.

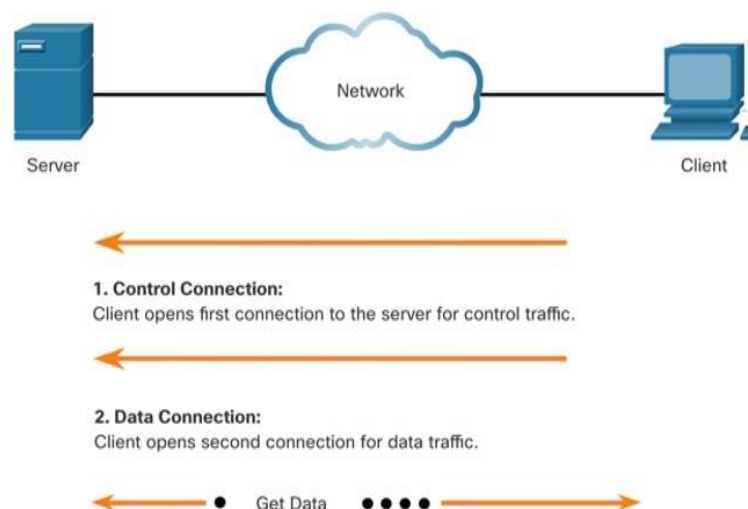


Figure 6.1: FTP

### 6.3.3 Why is FTP important and what is it used for?

- FTP is a standard network protocol that can enable expansive file transfer capabilities across IP networks. Without FTP, file and data transfer can be managed with other mechanisms – such as email or an HTTP web service – but those other options lack the clarity of focus, precision and control that FTP enables.



- The File Transfer Protocol (FTP) is frequently leveraged for transferring files from one system to another, and it boasts numerous applications that are widely utilized. Some of these include but are not limited to:
  - The process of creating a duplicate copy of digital information to protect against loss or damage is commonly referred to as backup. One possible academic rewrite of the given text is: File Transfer Protocol (FTP) can be utilized by either backup service providers or individual clients to transfer data from a source location to a remote backup server that hosts secured FTP services.
  - The process of replicating information or phenomena in scientific research is commonly referred to as replication. In a manner comparable to backup, replication entails the process of copying data from one system to another; however, it adopts a more extensive strategy to augment availability and resilience. The File Transfer Protocol (FTP) can additionally be employed to expedite this process. This study focuses on the process of accessing and loading data. FTP is a popular method employed to access shared web hosting and cloud services, typically utilized for upstreaming data onto an external system.

#### **6.3.4 FTP types**

There are several different ways an FTP server and client software can conduct a file transfer using FTP:

- Anonymous FTP: This is the most basic form of FTP. It provides support for data transfers without encrypting data or using a username and password. It works on port 21.
- Password-protected FTP: This is also a basic FTP service, but it requires the use of

a username and password, though the service might not be encrypted or secure. It also works on port 21.

- **FTP Secure (FTPS):** Sometimes referred to as FTP Secure Sockets Layer (FTP-SSL). FTPS was initially used to help enable a more secure form of FTP data transfer. It typically defaults to using port 990.
- **FTP over explicit SSL/TLS (FTPES).** This approach enables explicit TLS support by upgrading an FTP connection over port 21 to an encrypted connection. This is a commonly used approach by web and file sharing services to enable secure file transfers.
- **Secure FTP (SFTP).** This is technically not an FTP protocol, but it functions similarly. Rather, SFTP is a subset of the Secure Shell (SSH) protocol that runs over port 22. SSH is commonly used by systems administrators to access systems and applications remotely and securely, and SFTP provides a mechanism within SSH for secure file transfer.

### **6.3.5 FTP security**

FTP has also undergone several updates to enhance FTP security. These include versions that encrypt via an implicit TLS connection (FTPS) or explicit TLS connection (FTPES) or that work with SFTP. By default, FTP does not encrypt traffic, and individuals can capture packets to read usernames, passwords, and other data. By encrypting FTP with FTPS or FTPES, data is protected, limiting the ability of an attacker to eavesdrop on a connection and steal data. FTP may still be vulnerable to brute-force attacks against user/password authentication spoofing, an FTP bounce attack or a distributed denial-of-service attack.

### 6.3.6 FTP clients

FTP clients are used to uploading, downloading, and managing files on a server. FTP clients include the following:

- FileZilla: This is a free FTP client for Windows, macOS and Linux that supports FTP, FTPS and SFTP.
- Transmit: This is an FTP client for macOS that supports FTP and SSH.
- WinSCP: This is a Windows FTP client that supports FTP, SSH and SFTP.
- WS-FTP: This is another Windows FTP client that supports SSH.

### 6.3.7 FTB server in proposed network

In the proposed network we use Linux-ubuntu as an FTB server and its position in the proposed network is next to the DHCP server on the server zone in the inside zone of the firewall.

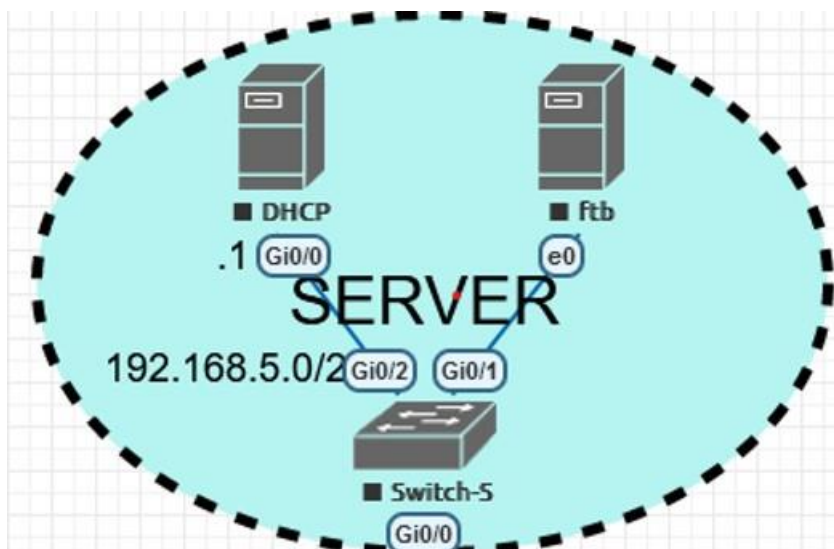


Figure 6.2: FTP in proposed Network

## **6.4 web server**

### **6.4.1 What is a web server?**

- A web server is software and hardware that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests made over the World Wide Web. The main job of a web server is to display website content through storing, processing, and delivering webpages to users. Besides HTTP, web servers also support SMTP (Simple Mail Transfer Protocol) and FTP (File Transfer Protocol), used for email, file transfer and storage.
- Web server hardware is connected to the internet and allows data to be exchanged with other connected devices, while web server software controls how a user accesses hosted file. The web server process is an example of the client/server model. All computers that host websites must have web server software.
- Web servers are used in web hosting, or the hosting of data for websites and web-based applications or web applications.

Examples of web server uses:

- sending and receiving emails.
- downloading requests for File Transfer Protocol (FTP) files; and
- building and publishing webpages.

### **6.4.2 How do web servers work?**

- Web server software is accessed through the domain names of websites and ensures the delivery of the site's content to the requesting user. The software side is also comprised of several components, with at least an HTTP server. The HTTP server can understand HTTP and URLs. As hardware, a web server is a computer that

stores web server software and other files related to a website, such as HTML documents, images, and JavaScript files.

- When a web browser, like Google Chrome or Firefox, needs a file that is hosted on a web server, the browser will request the file by HTTP. When the request is received by the web server, the HTTP server will accept the request, find the content, and send it back to the browser through HTTP.
- When a web address or Uniform Resource Locator (URL) is typed into a web browser, the web browser establishes a connection to the web service. The web service is running on the server that is using the HTTP protocol.
- To better understand how the web browser and web server interact, examine how a web page is opened in a browser.
  - Step1 see fig 6.3 The browser interprets the three parts of URL:
    - \* http (the protocol)
    - \* www.cisco.com (the server's name or Ip of the server)
    - \* index.html (the specific filename requested)
  - step2 see fig 6.4
    - \* The browser then checks with a name server to convert www.cisco.com into a numeric IP address, which it uses to connect to the server.
    - \* The client initiates an HTTP request to a server by sending a GET request to the server and asks for the index.html file.
  - Step3 see fig 6.5
    - \* In response to the request, the server sends the HTML code for this web page to the browser.
  - Step4 see fig 6.6

- \* The browser deciphers the HTML code and formats the page for the browser window.



Figure 6.3: step 1

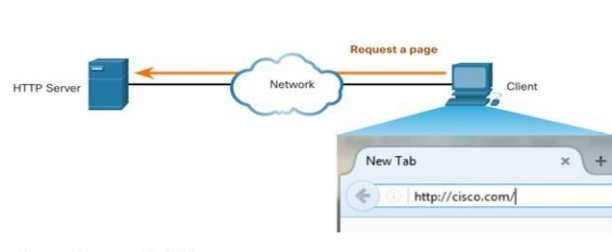


Figure 6.4: step 2

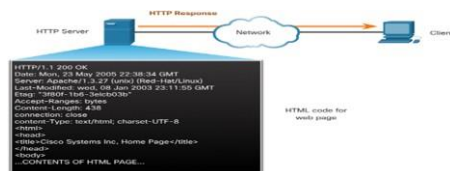


Figure 6.5: step 3

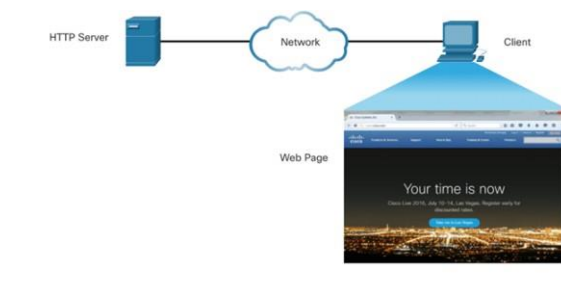


Figure 6.6: step 4



Figure 6.7: web server in proposed network

### 6.4.3 Common and top web server software on the market

There are several common web servers available, some including:

- Apache HTTP Server: Developed by Apache Software Foundation, it is a free and open-source web server for Windows, Mac OS X, Unix, Linux, Solaris, and other operating systems; it needs the Apache license.
- Microsoft Internet Information Services (IIS): Developed by Microsoft for Microsoft platforms; it is not open sourced, but widely used.
- Nginx: A popular open-source web server for administrators because of its light resource utilization and scalability. It can handle many concurrent sessions due to its event-driven architecture. Nginx also can be used as a proxy server and load balancer.
- Lighttpd: A free web server that comes with the FreeBSD operating system. It is seen as fast and secure, while consuming less CPU power.
- Sun Java System Web Server: A free web server from Sun Microsystems that can run on Windows, Linux, and Unix. It is well-equipped to handle medium to large websites.

Considerations in choosing a web server include how well it works with the operating system and other servers, its ability to handle server-side programming, security characteristics, and the publishing, search engine and site-building tools that come with it. Web servers may also have different configurations and set default values. To create high performance, a web server, high throughput, and low latency will help.

#### 6.4.4 Web server security practices

There are plenty of security practices individuals can set around web server use that can make for a safer experience. A few example security practices can include processes like:

- a reverse proxy, which is designed to hide an internal server and act as an intermediary for traffic originating on an internal server.
- access restriction through processes such as limiting the web host's access to infrastructure machines or using Secure Socket Shell (SSH).
- keeping web servers patched and up to date to help ensure the web server is not susceptible to vulnerabilities.
- network monitoring to make sure there is not any unauthorized activity.
- using a firewall and SSL as firewalls can monitor HTTP traffic while having a Secure Sockets Layer (SSL) can help keep data secure.
- The Cisco WSA solution complements the deep packet inspection and stateful filtering capabilities of the firewalls by providing additional web security features.

Web server in proposed network In the proposed network we use Linux-tiny core as a Web server and its position in the proposed network is the DMZ zone of the firewall.



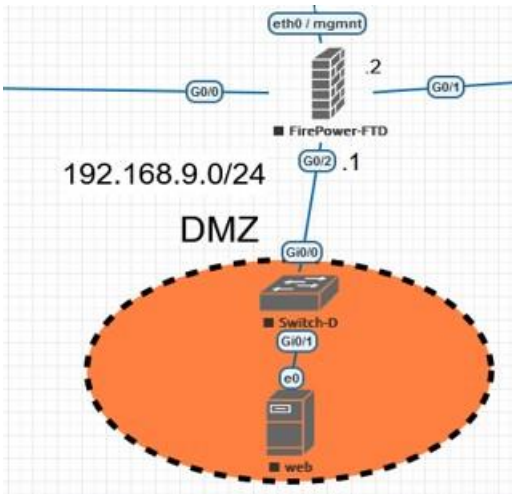


Figure 6.8: web server in proposed network

# Chapter 7

## Conclusions and Future Work

A computer network, sometimes known as a data network, is a kind of telecommunications network that enables computers to communicate with one another. Data is passed between networked computing devices . in small scale in companies there are some of the most common network vulnerabilities Improperly installed hardware or software operating systems or firmware that have not been updated Misused hardware or software Poor or complete lack of physical security insecure passwords design flaws in a device's operating system or in the network, it does make it much easier and possible for them to gain access to . companies must have the server for it . like Web server and Email server

,FTP server the web server to Announces its products and servers. Email to make the connect with employees easy .FTP for sharing the file in company with security. by making hardware and software and trying to close all vulnerabilities. the system will be saved from damage .

### 7.1 Future Work

The work presented in this thesis can only be considered preliminary, since many challenging and more important problems have not been touched upon in this thesis. At the end of the thesis, a number of problems are proposed as possible future work

related to our study.

- mail server : A mail server also known as a mail transfer agent, or MTA, mail transport agent, or mail router is an application that receives incoming email from local users and remote senders and forwards outgoing messages for delivery. A computer dedicated to running these applications is also called a mail server.
- vpn: A VPN enables remote users to securely access a private network over the internet. VPNs used for secure remote access or to connect dispersed networks. CCNA cert covers VPN basics & protocols. VPN security relies on encryption and authentication mechanisms. VPN protocols include PPTP, L2TP, OpenVPN, and IKEv2. Not recommended due to security weaknesses. L2TP offers enhanced security with improved encryption and authentication for VPN. OpenVPN is a secure and configurable open-source VPN protocol. IKEv2: fast and secure VPN protocol. VPNs use AES, DES, and 3DES encryption. AES is the top choice for VPN encryption. VPNs use 2 types of authentications: pre-shared keys and digital certificates. Simple, but insecure and vulnerable to brute-force attacks. Digital certificates use PKI to authenticate VPN. This method is secure as only trusted parties connect to the VPN. Misconfigured VPNs compromise network security.
- AAA : stands for Authentication, Authorization, and Accounting, which are three key processes in network security. Authentication is the process of verifying the identity of a user or device, while authorization is the process of granting or denying access to network resources based on the authenticated identity. Accounting is the process of recording and tracking user activity on the network for auditing and billing purposes. They can provide centralized authentication, authorization, and accounting services. AAA servers are commonly used in enterprise networks to manage user access and enforce security policies. AAA servers can also provide additional security features, such as two-factor authentication and

multi-factor authentication, to further protect network resources. AAA servers use a variety of protocols to communicate with network devices, including RADIUS (Remote Authentication Dial-In User Service), TACACS+ (Terminal Access Controller Access-Control System Plus), and Diameter. RADIUS is the most used protocol for AAA servers and is supported by a wide range of network devices and applications. AAA servers can be integrated with other network security devices, such as firewalls, VPNs, and wireless access points, to provide a centralized and consistent approach to network security. AAA servers can also integrate with identity management systems, such as Active Directory, to simplify user management and improve security.

- ESA stands for Email Security Appliance, which is a security device that protects organizations from email-borne threats, such as spam, viruses, and phishing attacks. ESA devices use a variety of techniques to identify and block malicious email traffic, including content filtering, reputation filtering, and virus scanning. ESA devices can also provide encryption and data loss prevention (DLP) capabilities to help organizations comply with regulatory requirements.
- WSA stands for Web Security Appliance, which is a security device that protects organizations from web-based threats, such as malware, viruses, and phishing attacks. WSA devices use a variety of techniques to identify and block malicious web traffic, including URL filtering, content filtering, and malware scanning. WSA devices can also provide encryption and DLP capabilities to help organizations comply with regulatory requirements.
- Network redundancy: Providing alternative paths for traffic to ensure continuous data flow in case of failure. Network uptime is the duration a network stays functional. Higher network uptime means easier, faster, and more reliable network access for customers and employees. This is vital for 24-hour organizations like

banks and hospitals. Network redundancy ensures active networks via multiple access points to data. Protects against network damage from disasters/theft. Network redundancy improves cybersecurity protection by allowing data to be securely stored for recovery after a cyberattack or disaster. Redundancy prevents downtime vulnerability during attacks.

# Chapter 8

## References

- 1- CCNA Cyber Ops (SECFND 210-250 and SECOPS 210-255) Official Cert Guide Library 1st Edition.
- 2- CCNA 200-301 Official Cert Guide, Volume 1.
- 3- CCNA 200-301 Official Cert Guide, Volume 2.
- 4- Cisco CCNP Security SCOR (350-701).
- 5- CCNP Security Securing Networks with Cisco Firepower (SNCF) 300-710.
- 6- Bonaventure, O. 2011. Computer Networking. PDF document. Available at:  
<https://www.saylor.org/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf>.
- 7- Cisco Network Academy. 2012. Network Security First-Step: Firewalls. WWW document. Available at:  
<http://www.ciscopress.com/articles/article.asp?p=1823359>.
- 8- Cisco Network Academy. 2014. Cisco Networking Academy's Introduction to Routing Concepts. WWW document. Available at:  
<http://www.ciscopress.com/articles/article.asp?p=2180208>
- 9- Cisco Network Academy. 2014. Cisco Networking Academy's Introduction to VLANs. WWW document. Available at:  
<http://www.ciscopress.com/articles/article.asp?p=2181837seqNum=4>.

10- Cisco Systems Inc. 2014. Cisco Catalyst 2960-S Series Switches. PDF document.

Available at:

[https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data\\_sheet\\_78\\_726680.pdf](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_78_726680.pdf)