



# **secured network infrastructure**

## ***graduation project***

Submitted by:

Mostafa Mohamed Mostafa	91547
Mohamed Khaled Kamal	89590
Mohamed abdelnasser Mohamed	89569
Mohamed Samir abdel salam	89913
Abdelaziz hosny abdelmagid	89751

Under supervision

Dr. Eman Salah

## Acknowledgments

Many people come to mind with gratitude to Go who Helped us complete this project.

We would like to extend our sincere thanks to our supervisor,

**Dr.Eman Salah**

We are deeply indebted to him for his valuable oversight, constant encouragement, valuable suggestions, and active assistance during this work.

Our sincerest appreciation and gratitude to our parents for their tremendous support and prepayment for us until this moment. I cannot find a suitable word to express our deep gratitude to our families who have given us such exceptional support. This thesis is a dedication to their love.

.....

Finally, to everyone who has supported us, thank you.

## Contents

Acknowledgments .....	2
List of Figures .....	7
List of Table .....	8
Abstract: .....	9
Chapter 1.....	11
Our Locations .....	11
Services Overview Troubleshooting .....	11
Cloud Backup .....	12
Detailed Service Comparison.....	12
Case Studies and Success Stories.....	13
Case Study 1: Effective Troubleshooting for a Prominent Retail Network .....	13
Case Study 2: A Financial Services Company's Dependable Cloud Backup .....	13
Chapter 2 .....	14
A Brief History of Network Technology .....	14
The Fundamentals of Networks: .....	17
Local Area Network: .....	17
What is a wide area network (WAN)?.....	20
LAN vs. WAN .....	21
Basic network components:.....	23
Types of routers: .....	24
OSI Model .....	28
Network Topology.....	31
Point to Point-to-Point topology .....	31
Mesh Topology.....	32
Star Topology .....	32
Bus Topology .....	33
Ring Topology.....	33
Tree Topology.....	34
Hybrid Topology .....	35
Chapter 3 .....	39
Introduction to Firewalls .....	39
Definition and Purpose.....	39
Historical Background.....	39
Packet Filtering Firewalls.....	40
How Packet Filtering Works .....	40

Types of Packet Filtering.....	41
Advantages and Limitations: .....	43
Stateful Inspection Firewalls .....	44
Key Features and Functionality: .....	44
Comparison with Packet Filtering Firewalls: .....	45
Proxy Firewalls.....	46
Overview and Operation: .....	46
Benefits and Drawbacks:.....	47
Next-Generation Firewalls (NGFWs) .....	48
Evolution and Features:.....	48
Integration with Advanced Security Technologies:.....	49
Introduction to Network Security.....	51
Definition and Scope of Network Security: .....	51
Common Threats and Vulnerabilities:.....	52
Network Security Measures. ....	53
Intrusion Detection Systems (IDS):.....	53
Intrusion Prevention Systems (IPS).....	54
Virtual Private Networks (VPNs):.....	55
Types of VPNs:.....	58
Access Control Lists (ACLs): .....	61
Types of Access Control Lists .....	62
Overview of Router Connections and Server Configurations .....	62
Difference Between Access Point, Station, Bridge, and Router. ....	62
Types of Router Connections.....	65
Server Configurations.....	66
Active-Active Configuration .....	66
Active-Passive Configuration.....	67
Practical Applications .....	68
How to Implement Active-Active and Active-Passive Configurations .....	68
Chapter4.....	69
Introduction.....	69
Types of Routing Protocols.....	70
Stationary Routing Protocol (Static routing) .....	71
(Default Routing Protocol) .....	71
(Dynamic Routing Protocol) .....	72
(Link state routing protocol) .....	73

How does OSPF work? .....	77
(Distance vector routing protocols ) .....	81
RIP protocol.....	84
Second type of distance vector routing protocols .....	85
Characteristics.....	86
Pretensions of IGRP .....	87
Chapter 5 ( part 1).....	88
Introduction .....	88
Uses of packet tracer.....	89
Example of simulation of packet tracer .....	90
Disadvantages of packet tracer .....	92
GNS3 (Graphical Network Simulator-3).....	93
Features of GNS3: .....	93
Example of simulation .....	95
Chapter 5(part 2).....	97
Types of Network Attacks.....	98
Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks .....	98
Man-in-the-Middle (MitM) Attacks.....	99
Phishing and Spear Phishing .....	100
SQL Injection.....	101
Cross-Site Scripting (XSS) .....	102
Malware Attacks .....	102
Insider Threats .....	104
Zero-Day Exploits .....	105
Securing Your Network .....	106
Best Practices .....	106
Tools and Technologies .....	106
Mitigation and Response Strategies .....	107
Incident Response Plan .....	107
Real-Time Monitoring .....	108
Legal and Ethical Considerations .....	108
Case Studies.....	109
Case Study 1: DDoS Attack on Dyn (2016) .....	109
Case Study 2: Equifax Data Breach (2017).....	109
Case Study 3: WannaCry Ransomware Attack (2017).....	109
Conclusion.....	110

Mechanisms of Each Attack .....	111
Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks .....	111
Man-in-the-Middle (MitM) Attacks.....	112
MitM Attack Mechanism .....	112
Phishing and Spear Phishing .....	112
Phishing Attack Mechanism.....	112
SQL Injection.....	114
SQL Injection Attack Mechanism.....	114
Cross-Site Scripting (XSS) .....	114
XSS Attack Mechanism .....	114
Zero-Day Exploits.....	115
Zero-Day Exploit Mechanism.....	115
Chapter 6 .....	117
Primary Domain Controller (PDC):.....	117
key functions for PDC: .....	117
the Interface of Server Manager in a Primary Domain Controller (PDC):.....	120
Components of Active Directory: .....	128
DHCP:.....	130
DNS (Domain Name System) server:.....	133
Remote Desktop Services (RDS): .....	144
What is the ADC?.....	149
What is the VPN:.....	158
Benefits of VPN Point-to-Point in a Domain Controller Environment: .....	159
Attack .....	163
Doing attack DDOS in server:.....	163
The attack was done .....	163
How stop the attack: .....	164
ICMP flood 10 requests only:.....	165
Limited by 10 requests: .....	165
Conclusions .....	166
Reference List.....	167

## List of Figures

Figure 1 Token Ring Topology .....	15
Figure 2 Local Area Network.....	18
Figure 3 wide area network .....	21
Figure 4 Metropolitan Area Network.....	22
Figure 5 WLAN.....	22
Figure 6 <b>hub</b> .....	23
Figure 7 switches .....	24
Figure 8 <b>Routers</b> .....	24
Figure 9 repeater.....	27
Figure 10 Bridges .....	28
Figure 11 Point-to-point topology .....	32
Figure 12 mesh topology .....	32
Figure 13 Star Topology.....	33
Figure 14 Ring Topology.....	33
Figure 15 tree Topology .....	34
Figure 16 Hybrid Topology.....	35
Figure 17Static and Dynamic Packet Filtering for FTP .....	42
Figure 18 IDS/IPS on an Enterprise Network .....	55
Figure 19 virtual private network (VPN).....	57
Figure 20 types of VPNs .....	59
Figure 21 Access Control Lists (ACLs) .....	61
Figure 22 access point .....	63
Figure 23 station.....	63
Figure 24 router .....	64
Figure 25 bridge .....	64
Figure 26 active-active configuration.....	67
Figure 27 active-passive configuration.....	67
Figure 28 routing protocols .....	70
Figure 29 Dynamic Routing Protocol.....	73
Figure 30.....	75
Figure 31.....	76
Figure 32 RIPMessage .....	82
Figure 33 RIP Protocol.....	84
Figure 34 Example of simulation of packet tracer .....	90
Figure 35 Example of simulation in GNS3 .....	95
Figure 36 Dashboard.....	120
Figure 37 Local Server.....	121
Figure 38.....	123
Figure 39 Installing service in PDC .....	123
Figure 40 Installing service in PDC .....	124
Figure 41 oracle cluster .....	125
Figure 42 local server .....	125
Figure 43 service install.....	126
Figure 44 Service installed in PDC .....	129
Figure 45 DHCP.....	132
Figure 46 Pool IP.....	133
Figure 47 DNS Security.....	136
Figure 48 Show the server is forward zone to PDC .....	136

Figure 49 ADD client to PDC.....	137
Figure 50 Create password for the client.....	137
Figure 51 Client added to PDC .....	138
Figure 52 Make a new group .....	141
Figure 53 Add Client to Group.....	141
Figure 54 Choice the client who can access to this partition .....	142
Figure 55 Give the client permission.....	142
Figure 56 GIVE access to another PC to PDC by remote management.....	145
Figure 57 Select user can admin access to PDC from his PC .....	146
Figure 58 Select user can admin access to PDC from his PC .....	146
Figure 59 Access to PDC.....	147
Figure 60 Open Server manage.....	147
Figure 61 Client PCI access to PDC .....	148
Figure 62 Client PCI access to PDC .....	148
Figure 63 Interface for Server manager for ADC.....	150
Figure 64 Making IP pool in ADC.....	151
Figure 65 Choice the range IP .....	151
Figure 66 firewall IP can access to it from browser.....	152
Figure 67 Give IP for firewall .....	152
Figure 68 Set allowances for the interface .....	153
Figure 69 Open GUI .....	153
Figure 70 GUI of firewall .....	154
Figure 71 Change IP for interface port 1 the connect to isp.....	154
Figure 72 Ping from R1 to check the connection .....	155
Figure 73 Divide the interface to VLAN.....	155
Figure 74 Make IP pool and give the range of IP .....	156
Figure 75 interface.....	156
Figure 76 Doing rip in firewall .....	157
Figure 77 The policy in firewall .....	157
Figure 78 After installing VPN give the PC access to it .....	159
Figure 79 Give the user access permission.....	160
Figure 80 Add VPN BY User.....	160
Figure 81 Connect to VPN .....	161
Figure 82 The user connected to VPN.....	161
Figure 83 The user connected to VPN.....	162

## List of Table

Table 1 Detailed Service Comparison .....	12
Table 2 compare between HUB, Switch, Router .....	30
Table 3 compare between HUB, Switch, Router .....	31
Table 4 Comparison with Packet Filtering Firewalls .....	46
Table 5 differences between the Bridge, Router, Access Point and Station.....	65
Table 6 compare between OSPF, ISIS .....	80
Table 7 compare between <b>Response, Prevention, Detection, Response</b> .....	116

## Abstract:

In the current era, networks play a crucial role in connecting various entities, including companies and their multiple subsidiaries. Different types, shapes, and sizes of networks enable seamless connectivity and consistent system operations across sites. This document explores the mechanisms that allow a company or restaurant with many branches to maintain synchronized systems, secure communications, and effectively represent the network. The focus is on understanding how these interconnected networks work, the methods used to ensure security, and the techniques used to achieve unified and efficient network management.

Network infrastructure forms the backbone of modern communication systems, facilitating the transmission of data across various devices and networks. This infrastructure encompasses a wide array of components, including routers, switches, firewalls, servers, and the physical media (cables and wireless systems) that connect them. Robust network infrastructure is critical for ensuring reliable, efficient, and secure data transfer, supporting the ever-growing demands of personal, business, and industrial applications.

The advent of advanced technologies such as 5G, fiber optics, and cloud computing has revolutionized network infrastructure, offering unprecedented speed, capacity, and flexibility. Key elements include:

1. **Routers and Switches:** These devices manage data traffic, directing packets to their destinations and ensuring efficient use of network resources.
2. **Firewalls and Security Appliances:** Essential for protecting network integrity, these devices prevent unauthorized access and mitigate cyber threats.
3. **Servers and Data Centers:** Central to storing and processing data, they enable cloud services and enterprise applications.
4. **Cabling and Wireless Technologies:** Fiber optic and Ethernet cables, along with Wi-Fi and cellular networks, form the physical and wireless media for data transmission.

Network infrastructure must be meticulously designed to handle increasing data volumes, accommodate diverse applications, and ensure high availability. Redundancy, scalability, and security are paramount considerations, particularly in critical sectors such as finance, healthcare, and telecommunications.

In today's interconnected world, ensuring the security and reliability of network infrastructures is paramount. This project aims to design and implement a robust secured network infrastructure that can withstand modern cybersecurity threats. Key objectives include establishing secure access controls, implementing encryption protocols, deploying intrusion detection systems (IDS), and conducting regular security audits. The project will leverage industry best practices and technologies to create a resilient network environment capable of protecting sensitive data and maintaining operational continuity.

Through meticulous planning and rigorous testing, the secured network infrastructure will provide a foundation for safe and efficient digital communication across organizational boundaries.

**Enhancing Network Infrastructure to Safeguard Our Digital Foundation** To protect their data and operations in the ever-changing world of cyber threats, organisations need a strong network infrastructure. This project provides a thorough plan for improving our network security posture. We suggest a multi-pronged defensive approach that includes:

**Access Control:** Putting user access management and robust authentication procedures into place. **Network segmentation:** To stop possible breaches from spreading, the network is split up into secure areas. Using intrusion detection and prevention systems (IDS/IPS) to find and stop malicious activities is known as advanced threat detection. **Vulnerability Management:** Putting in place a methodical procedure for locating, ranking, and fixing software and hardware vulnerabilities in networks.

**Data encryption:** To maintain secrecy, sensitive data should be encrypted both in transit and at rest. **Training in Security Awareness:** Informing users about online dangers and safe network operation techniques. The following goals are the focus of this project: Reduce the possibility of data breaches and illegal access. bolster our network's overall defences against cyberattacks. Verify adherence to industry security norms and guidelines.

# Chapter 1

Overview Greetings from [Company Name], your dependable resource for cutting- edge technological solutions. Our company, which has two flourishing branches in Cairo and Alexandria, is dedicated to providing outstanding services that promote commercial prosperity and operational excellence. We provide an extensive range of options, such as cloud backup, call services, and troubleshooting. We will go over the special qualities of our business, the range of services we offer, and how we professionally and knowledgeably handle a variety of business demands in this introduction.

## Our Locations

- **Cairo Branch**

Our main base of operations is our branch in Cairo, which is located in Egypt's busy city. This branch is home to a vibrant group of experts committed to offering businesses in the area excellent technical support and creative solutions.

- **Alexandria Branch**

Our presence on the Mediterranean coast is increased by our branch in Alexandria, Egypt's principal port city, which provides specialized services to cater to the unique requirements of the regional market. This department plays a critical role in guaranteeing that all of our clients, regardless of where they live, receive reliable, superior service.

## Services Overview Troubleshooting

We are aware that technical problems can cause major downtime and lost productivity in corporate operations. Our troubleshooting services are made to locate and fix technical issues fast, causing the least amount of disturbance to your company.

- 1. Hardware troubleshooting:** Physical component diagnosis and repair.
- 2. Software Troubleshooting:** Fixing problems with apps, operating systems, and software compatibility.
- 3. Network troubleshooting:** Making sure the network operates at peak efficiency and fixing connectivity problems.

# Cloud Backup

In an era where data is a critical asset, our cloud backup services provide a reliable and secure way to protect your valuable information. We offer scalable solutions that cater to businesses of all sizes, ensuring data integrity and availability.

- 1. Automated Backup Solutions:** To stop data loss, backups are scheduled and conducted automatically.
- 2. Safe Data Storage:** Making use of cutting-edge encryption techniques to protect
- 3. Disaster Recovery:** Extensive plans for quickly restoring data in the event of unanticipated circumstances.

## Detailed Service Comparison

To provide a clearer understanding of our service offerings, the following table highlights the key features and benefits of each service:

Service	Feature	Benefits
Troubleshooting	Hardware, Software, Network	Minimizes downtime, improves productivity, reduces operational costs
Cloud backup	Automated Backups, Secure Storage, Disaster Recovery	Ensures data integrity, enhances security, facilitates quick data recovery

Table 1 Detailed Service Comparison

## Case Studies and Success Stories

### **Case Study 1: Effective Troubleshooting for a Prominent Retail Network**

Client: A well-known retail business with several locations around Egypt. Problem: Regular technical problems that interfere with operations. Our troubleshooting team's solution

carried out a thorough evaluation and put in place a proactive maintenance plan. As a result, the client's downtime was reduced by 40%, which resulted in considerable cost savings and increased customer satisfaction.

### **Case Study 2: A Financial Services Company's Dependable Cloud Backup**

Client: A financial services organization in need of urgent data storage. Problem: The requirement for dependable and safe data backup options. The use of our cutting-edge encrypted automated cloud backup services is the solution. As a result, the business attained 100% data integrity and was able to quickly recover from any possible data loss occurrences.

## Chapter 2

### A Brief History of Network Technology

- **Early Influences (1950s):**

The seeds of modern networking were sown in the 1950s with the development of technologies like the Semi-Automatic Ground Environment (SAGE) system. This U.S. military radar system used one of the first commercial modems to transmit data over phone lines.

- **The First Computer Network is Born**

The first connected computer network, known as ARPANET (Advanced Research Projects Agency Network), was established in 1969, marking the beginning of modern computer networking technology. The Internet was later developed using the TCP/IP protocol suite that it implemented. The US Department of Defense's Advanced Research Projects Agency (ARPA) was responsible for developing the ARPANET. Why was it necessary for the DoD to create networked computers?

The Cold War, naturally! Maintaining communication channels in case the USSR and the USA agreed to trade nuclear weapons was the main objective of ARPANET.

Through the use of packet-switching rather than direct connections, the ARPANET completely changed communications. When data is delivered via a packet-switching network, it is formatted with the destination machine's address, sent out onto the network, and then picked up by the subsequent machine. The computer is informed where to send the packet by the address in the protocol. In this manner, even in the event that there isn't a direct link between the two devices, the information will still reach its target.

The ARPANET system continued to rely on phone lines even though it eliminated the requirement for direct connections between machines in order for them to interact. In 1972, the network between university computers at Stanford, the University of Utah, UCLA, and UCSB was enlarged to 40 nodes from its initial four nodes.

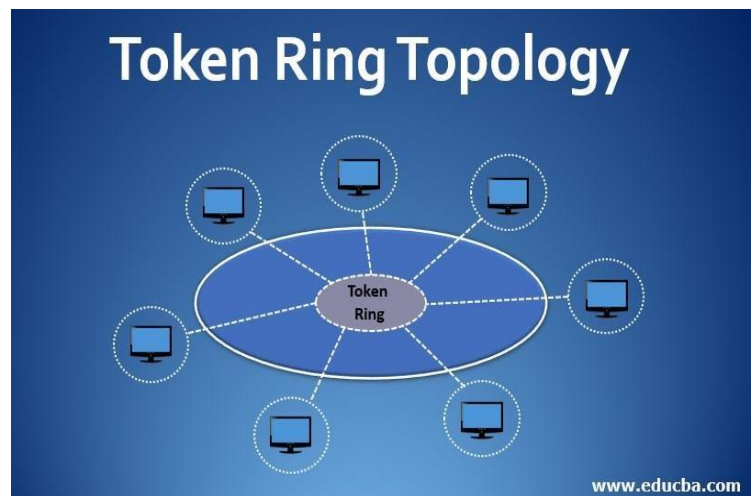
- **Attached Resource Computer NETWORK (ARCNET)**

The local area networks (LANs) communications protocol ARCNET was created in 1986 by Datapoint Corporation. In the 1980s, office automation made extensive use of this networking system, which was the first to be made commercially available. ARCNET was the first computer system that did not assume that different kinds of computer networking technologies would be connected, in contrast to prior computer systems that demanded that all networked machines be homogenous. Even though it was widely used during its heyday, ARCNET's 2.5 Mbit/s speed limit made it less dependable and adaptable than competing systems, especially Ethernet.

- **Token Ring and Network Topology**

Token ring protocols gained popularity in the 1980s, mostly as an IBM response to the new Ethernet protocol's openness. By connecting all the computers in a ring or star configuration, the local area network

(LAN) facilitates the transfer of data between hosts. By limiting who can send data on a network to hosts that have tokens and releasing tokens only after data receipt is verified, this protocol helps to avoid information packet collisions.



*Figure 1 Token Ring Topology*

In October 1985, IBM introduced their Token Ring technology, which operated at 4 Mbit/s. The ANSI/IEEE standard 802.5 was based on the star-wired physical topology that was used over shielded twisted-pair cabling. In the end, a 16 Mbit/s Token Ring was standardized, and since it was about to expire, it was raised to 100 Mbit/s. Token ring LANs were favored by many scientists over Ethernet, which was only recently invented. Nevertheless, Ethernet offered more affordable networking techniques, which contributed to the near extinction of commercial token ring systems by the 2000s.

- **Fiber Distributed Data Interface**

Optical fiber is used by the fiber distributed data interface (FDDI) to transmit data within a local area network (LAN). With speeds of up to 100 Mbit/s, it completely outperformed ARCNET. Although it employs a protocol developed from the IEEE 802.4 token bus timed token protocol rather than the IEEE 802.5 standard, FDDI is a ring-based token network. Additionally, the data network technology has a broad coverage area of up to 120 miles.

When Ethernet was still in its infancy and could only provide 10 Mbit/s in the 1990s, FDDI and its copper-based later cousin, CDDI, were widely used. However, following the 1998 release of the more affordable and faster Gigabit Ethernet, the majority of FDDI systems have been totally superseded by Ethernet.

- **The Rise of the Ethernet**

Bob Metcalfe created Ethernet at Xerox PARC in 1973, although it wasn't patented until 1975. It took a further five years to standardize the open Ethernet protocol, which became IEEE 802.3 in 1983. With initial speeds of 2.94 Mbit/s, the first Ethernet system employed coaxial cable as a shared medium. Ethernet has advanced throughout time to include switches and twisted pair or fiber optic cables, enabling a speed rise to a scorching 40 Gb/s.

When Ethernet adapted to new cable types including twisted pair and fiber optic cables, it provided a less expensive option to many earlier networking technologies. The kinds of cables they might use were restricted by other standards. Ethernet was also simpler to build since it used an open-source protocol rather than a proprietary one. Currently quite common, Ethernet is regarded as one of the key elements of the Internet as we know it.

- **Using Ethernet Cables Now**

There are numerous varieties of Ethernet cables available because Ethernet is a protocol rather than a specific sort of connection. For long-distance networking, a fiber optic variant might be your best option. Copper is needed if you need power over Ethernet (PoE). For faster speeds, you might choose Cat6 cable over Cat5e, or vice versa depending on cost.

Now that you have a basic understanding of network technology, trueCable can assist you in choosing the best Ethernet cable and configuration for your network, whether it is at home or in the workplace. Get in touch with us right now to learn more!

## **The Fundamentals of Networks:**

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be connected through cables, telephone lines, radio waves, satellites, or infrared light beams.

The two main types of networks are:

- Local Area Network (LAN)
- Wide Area Network (WAN)

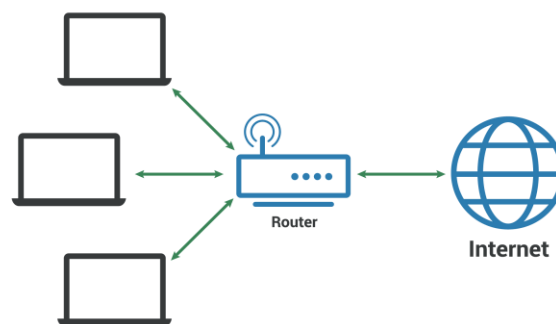
But also there are more like Metropolitan Area Networks (MAN), a Wireless LAN (WLAN), or a Wireless WAN (WWAN).

Let us break them down first

### **Local Area Network:**

A network that is contained in a small geographic region—typically within the same building—is known as a local area network (LAN). LANs are frequently used in settings like small business networks and WiFi networks at homes.

Although LANs can be fairly large, it is usually more accurate to designate them as wide area networks (WAN) or metropolitan area networks (MAN) if they occupy numerous buildings.



*Figure 2 Local Area Network*

➤ How does a LAN work?

A router serves as the hub where the majority of LANs connect to the Internet. While LANs in bigger settings may also include network switches for more effective packet delivery, home LANs typically use a single router.

LANs virtually always connect devices within the network using Ethernet, WiFi, or both. Ethernet is a physical network connection protocol that needs Ethernet cables to be used. WiFi is a radio protocol that allows users to connect to a network.

Servers, desktop and laptop computers, printers, IoT devices, game consoles, and

more can all connect to LANs. LANs are frequently used in offices to give internal staff members shared access to connected printers or servers.

### ➤ **Equipment needed for LAN**

All that is needed for the most basic Internet-connected LANs is a router and a means for computer devices to connect to it, like Ethernet cables or WiFi hotspots. For data exchange, LANs without an Internet connection require switches. For big LANs—like those in office buildings—to send data to the appropriate devices more effectively, more routers or switches may be required.

Not every LAN has an Internet connection. Actually, LANs existed before the Internet; they were initially implemented in enterprises in the late 1970s. (The network protocols used by these outdated LANs are no longer in use.) The ability for the linked devices to exchange data is the only prerequisite for setting up a LAN. This typically calls for a network switch or other piece of packet switching hardware. These days, Internet-based networking protocols (such IP) are utilized even by local area networks (LANs) that are not connected to the Internet.

### ➤ **A virtual LAN: what is it?**

Divide traffic between two networks on the same physical network by using virtual local area networks, or VLANs. Imagine putting up two different LANs in the same room, each with its own router and Internet connection. Similar to that, except instead of physically dividing them using hardware, VLANs split them electronically using software; only one router and one Internet connection are required.

Especially for very large LANs, VLANs aid in network management. Network administrators may much more simply administer the network by segmenting it. (VLANs are distinct from subnets, which are additional network subdividing techniques for increased effectiveness.)

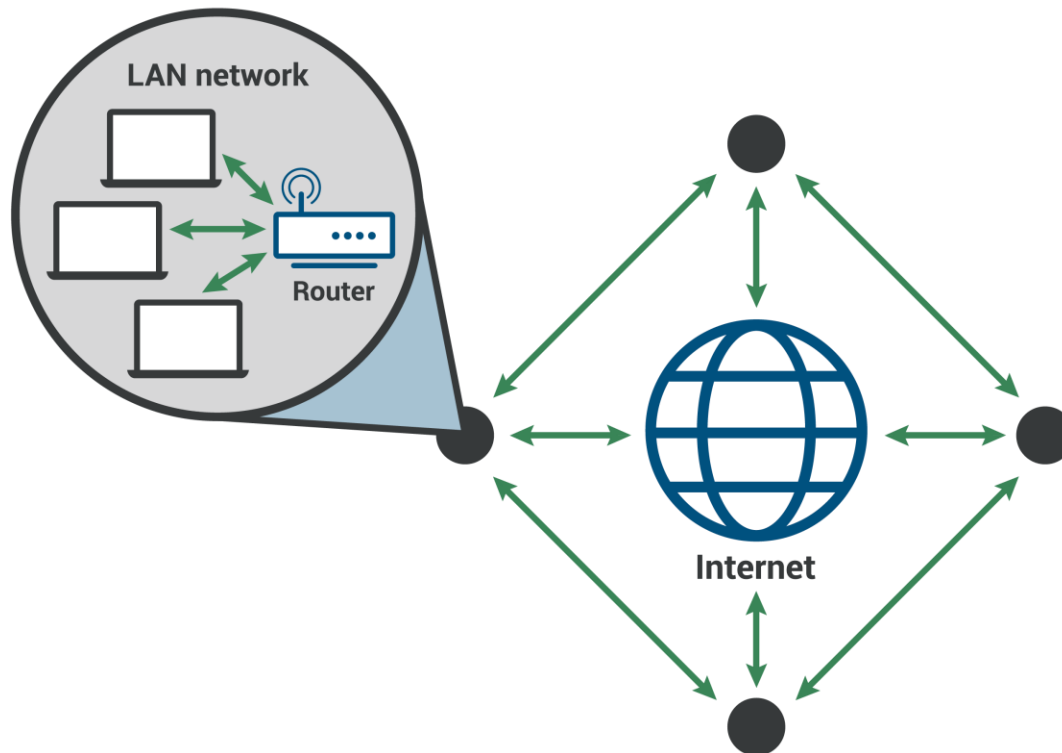
**What is a wide area network (WAN)?**

An extensive computer network that spans great distances to link groups of computers is called a wide area network (WAN). Large companies frequently utilize wide area networks, or WANs, to connect their office networks. WANs are used to connect the local area networks, or LANs, that are normally connected by each office's own LAN. There are numerous techniques to establish these lengthy connections, such as IP tunnels, VPNs, and leased lines (see below).

The concept of a wide area network (WAN) is somewhat expansive. In theory, a wide area network (WAN) is any sizable network that spans a significant

geographic area. One can think of the Internet as a WAN itself.

## WAN network



*Figure 3 wide area network*

## LAN vs. WAN

LANs normally share a single central point of Internet connectivity and are contained inside a region. Long-distance network connectivity is what WANs are made for. Usually, they consist of multiple LANs that are connected. When an organization sets up its own wide area network (WAN), it nearly always depends on network equipment that is not under its control. For instance, a business that has offices in New York and Paris will need to transport data between these locations via underwater cables that span the Atlantic Ocean.

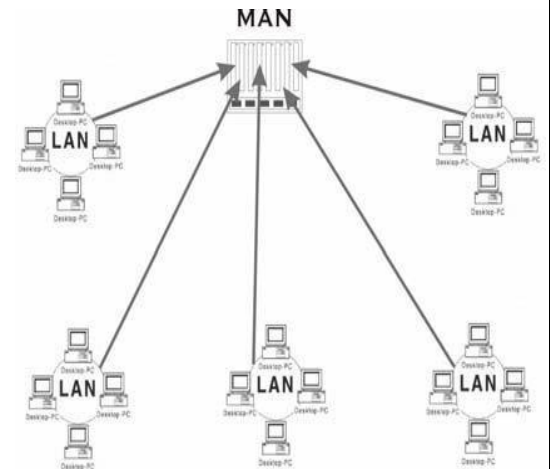
A WAN often consists of several switches and routers. A local area network (LAN) can connect to switches as well as the Internet with just one router, if that's what it needs.

### ➤ Simple brief about 'WAN' and 'WLAN'

#### 1. Metropolitan Area Network (MAN):

A MAN covers a metropolitan area, larger than a LAN but smaller than a WAN. It can encompass a city, college campus, or even a large business complex.

MANs often serve as backbones for connecting multiple LANs within a city and provide high-speed data transfer between them. They offer a middle ground between the scale of a LAN and the reach of a WAN.



*Figure 4 Metropolitan Area Network*

#### 2. Wireless LAN (WLAN):

WLAN stands for Wireless Local Area Network. It's a type of LAN that uses radio waves instead of physical cables to connect devices within a limited area, like a home, office, or school. Here's a breakdown of what WLAN offers:



*Figure 5 WLAN*

**Wireless Connectivity:** WLAN eliminates the need for cables, providing flexibility and ease of movement for devices within the network's range.

**Internet Access:** WLANs often connect to a router or access point that provides internet access to all connected devices.

Data Sharing: Devices on a WLAN can share resources like files, printers, and scanners.

WLAN is essentially what most people refer to when they say "Wi-Fi".

## Basic network components:

Connecting devices, sometimes referred to as networking devices or interconnection devices, are hardware components that link different parts of a network, enabling data to be sent and received along different routes.

Connecting devices are pivotal to your network design, each with their own specific functions:

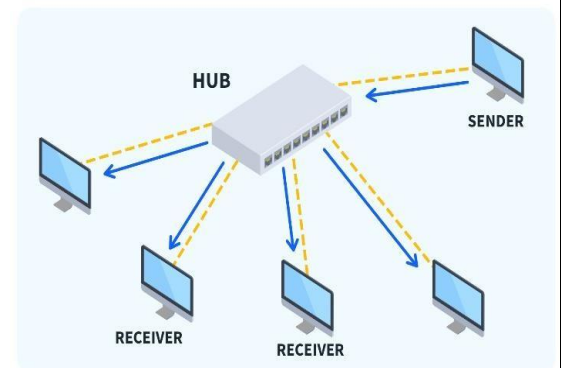
- **Hub**

This is a simple device that connects multiple devices on a network. It receives information from one connection and then sends it out to all others. In many modern networks, hubs are replaced with switches.

There are three types of hubs:

**Passive hubs or concentrators:** do not amplify or regenerate incoming signals before rebroadcasting them to the Network Hub via Allied Electronics network.

They do not improve the performance of local area networks (LANs), and may limit maximum media distances. Typically, passive hubs are connected to other devices in a star configuration.



*Figure 6 hub*

**Active hubs or multiport repeaters:** amplify the incoming electrical signals that contain data packets. They maximize network media distances and follow the same rules as repeaters. Although active hubs do not prioritize data packets, they can be configured as firewalls to examine them. Active network hubs apply retiming and resynchronization techniques if a received signal is too weak for rebroadcasting.

**Intelligent hubs:** work like active hubs and include remote management capabilities. They also provide flexible data rates to network devices.

- **Switches**

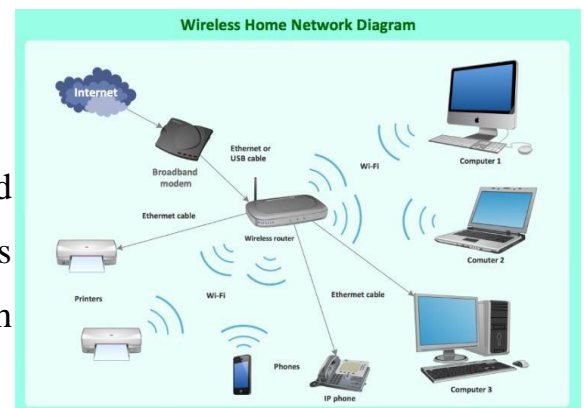
Similar to a hub, switches connect multiple devices on a network. However, they are more intelligent. They can read data packets and direct them to the right port only, reducing network traffic, and increasing security and efficiency.



*Figure 7 switches*

- **Routers**

These connect two or more different networks and direct data packets to their correct destinations across interconnected networks, often utilizing the best path to ensure efficient data delivery.



*Figure 8 Routers*

## Types of routers:

### 1. Home Routers:

- ❖ Designed for residential settings and small offices.
- ❖ Provides basic functionalities to connect multiple devices to the internet through a single internet connection.
- ❖ Often equipped with built-in wireless access points for Wi-Fi connectivity to devices within the home network.
- ❖ Easy-to-use web-based interfaces for configuration and management.

## **2. Wireless Routers:**

- ❖ Also known as Wi-Fi routers.
- ❖ Equipped with built-in wireless access points to enable devices to connect wirelessly to the network.
- ❖ Widely used in both home and small business environments.
- ❖ Provides wireless connectivity and supports multiple devices simultaneously.

## **3. Wired Routers:**

- ❖ Provides network connectivity through physical wired connections.
- ❖ Equipped with Ethernet ports to connect devices via network cables.
- ❖ Often used in environments where a stable and high-speed connection is required, such as in offices, data centers, and enterprise networks.

## **4. Core Routers:**

- ❖ High-end routers used in large-scale networks like internet service providers (ISPs) and major data centers.

- ❖ Responsible for forwarding data at the core of the network, connecting multiple high-speed data links.
- ❖ Designed for high throughput, low latency, and reliability to handle the massive traffic in backbone networks.

### **5. Edge Routers:**

- ❖ Also known as boundary routers.
- ❖ Used at the edge of a network where the network connects to external networks, such as the internet or another organization's network.
- ❖ Responsible for routing data between the local network and external networks, implementing security measures, and managing traffic entering or leaving the network.

### **6. Distribution Routers:**

- ❖ Found in large enterprise networks.
- ❖ Connects multiple local networks or segments.
- ❖ Responsible for routing traffic between different LANs, ensuring efficient data flow between different parts of the network.
- ❖ Performs tasks like VLAN segmentation and quality of service (QoS) management.

### **7. Access Routers:**

- ❖ Used in environments like office buildings and campuses.
- ❖ Provides connectivity to end-user devices within a local area network.
- ❖ Serves as a gateway between the end-user devices and the core or distribution routers in the network.

### **8. Virtual Routers:**

- ❖ Software-based routers that run on virtual machines or cloud platforms.
- ❖ Offers the same functionalities as physical routers but are more flexible and scalable.
- ❖ Commonly used in virtualized environments, data centers, and cloud computing infrastructure.

## 9. Modular Routers:

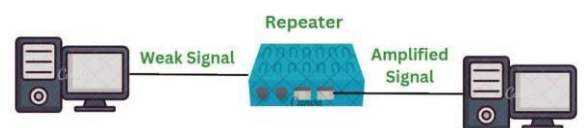
- ❖ Allows for the expansion of router capabilities through modular components or line cards.
- ❖ Interchangeable interface cards for customization based on specific networking needs.
- ❖ Often used in enterprise and data center environments.

## 10. SOHO Routers:

- ❖ Designed for small business environments and home offices.
- ❖ Offers a balance between features, price, and performance suitable for smaller networks.

### • Repeater

These boost the signal over the same network when



*Figure 9 repeater*

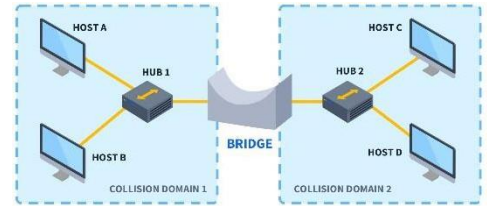
it becomes weak after traveling long distances.

### • Modems

These devices modulate and demodulate signals, converting them from digital to analog and vice versa. This enables data to be transmitted over telephone or cable lines.

- **Bridges**

They connect two separate networks, working a bit like a router but typically used for smaller networks.



*Figure 10 Bridges*

- **Gateways**

These connect two different network architectures, often different types of networks, and translate data between them.

- **Access points**

In wireless networking, these provide a point from where devices can connect to the network. They can be standalone devices or incorporated into a router or gateway.

- **NIC (Network Interface Card)**

These are used in computers to provide a network connection. They convert data from the computer into a format suitable for the network cable and vice versa. The network card handles communication between the computer and the network.

These devices are used depending upon the type and scale of the network being built, such as a small home network or large enterprise network, and provide both physical and logical connections between networked devices.

## **OSI Model**

The OSI (Open Systems Interconnection) Model is a conceptual framework that standardizes the functions of a network into seven distinct categories, also referred to as layers. It was developed by the International Organization for Standardization

(ISO) to facilitate interoperability between diverse communication systems with standard protocols.

The seven layers of the OSI Model are:

**Physical Layer (Layer 1):** This layer encompasses the physical equipment involved in data transport. It deals with the physical characteristics of the transmission medium like cables, connectors, voltages, pin layout, etc.

**Data Link Layer (Layer 2):** It provides reliable transit of data across the physical layer. It also handles error correction from the physical layer and flow control.

**Network Layer (Layer 3):** It handles routing – transmitting data sequences from one network to another.

**Transport Layer (Layer 4):** It is responsible for delivering data across network connections. It manages packet sequencing, acknowledgment, error checking, and retransmission of lost data.

**Session Layer (Layer 5):** This layer manages communication sessions, controlling the connections between computers. It establishes, maintains, and terminates connections between local and remote applications.

**Presentation Layer (Layer 6):** It works to transform data into the form that the application layer can accept. It handles data compression, encryption, and translation services.

**Application Layer (Layer 7):** This is the layer that interacts with operating system applications. It identifies communication partners and resource availability, and synchronizes communication.

OSI Model is mainly used as a point of reference for understanding how different network protocols interact and work together to provide network services. It is important to note that not all network protocols fit neatly into this model.

characteristics	HUB	Switch	Router
OSI Layer	Physical Layer (Layer 1)	Data Link Layer (Layer 2)	Network Layer (Layer 3)
Function	Receives incoming data packets and broadcasts them to all connected devices	Examines the destination MAC address of each incoming packet and forwards it to the appropriate port	Connects different network segments and routes data packets between them based on the destination IP address
Broadcast domain	Creates a single broadcast domain where all connected devices receive the same data	Creates multiple, separate broadcast domains, isolating traffic within each port	Separates network segments into different broadcast domains, dividing the network into smaller, more efficient segments
Packet Forwarding	Broadcasts all incoming packets to all connected	Forwards packets only to the relevant	Routes packets between different network segments

*Table 2 compare between HUB, Switch, Router*

	devices, without examining destination addresses	destination port based on its MAC address table	based on destination IP addresses
Network efficiency	Leads to inefficient use of network bandwidth as all devices receive all traffic	Improves network performance by reducing unnecessary traffic in other parts of the network	Enhances overall network efficiency and performance by optimizing data traffic flow between network segments
security	Provides a lower level of security as all connected devices can "see" the same traffic	Enhances security by isolating traffic within each port, creating separate broadcast domains	Improves security by separating network segments, preventing direct access between different networks

*Table 3 compare between HUB, Switch, Router*

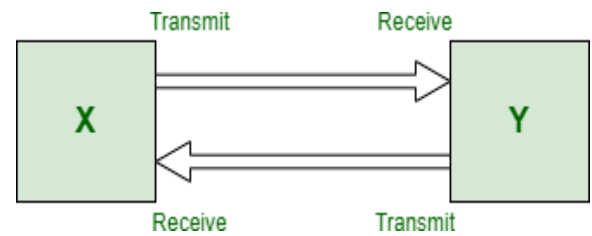
## Network Topology

### Types of Network Topology

The network arrangement comprising nodes and connecting lines via sender and receiver is referred to as Network Topology. The various network topologies are:

#### **Point to Point-to-Point topology**

Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.

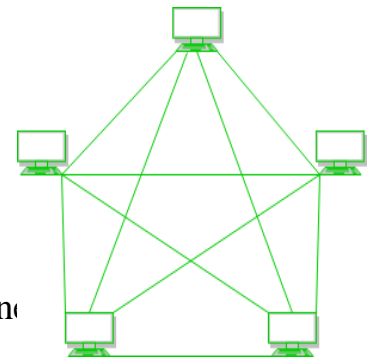


*Figure 11 Point-to-point topology*

### **Mesh Topology**

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.

In Figure: Every device is connected to another via dedicated channels. These channels are known as links.



*Figure 12 mesh topology*

Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required =  $N * (N-1)$ .

Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is  $\frac{N(N-1)}{2}$  i.e.  $\frac{N(N-1)}{2}$ . In Figure, there are 5 devices connected to each other, hence the total number of links required is  $\frac{5*4}{2} = 10$ .

### **Star Topology**

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node.

The hub can be passive, not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them.

Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.

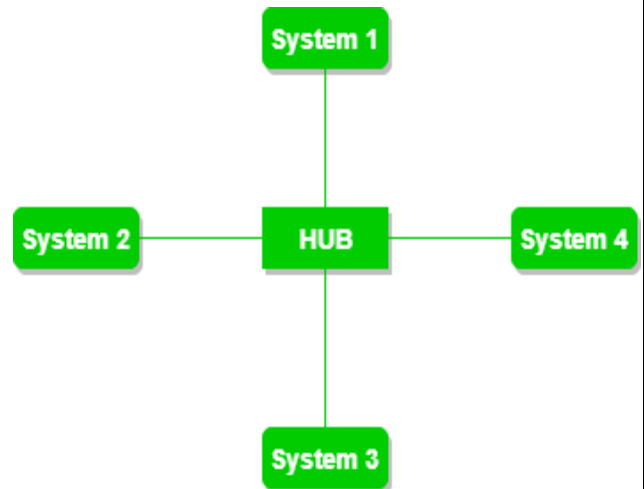
### **Bus Topology**

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.

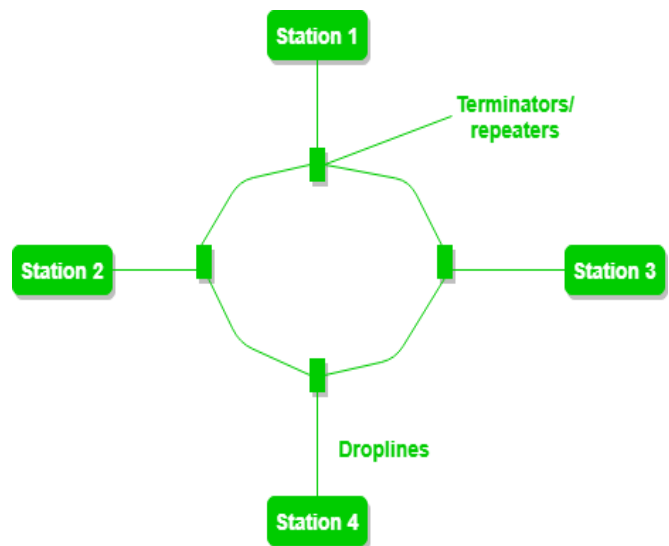
### **Ring Topology**

A Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. Several repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node.

Hence to prevent data loss repeaters are used in the network.



*Figure 13 Star Topology*

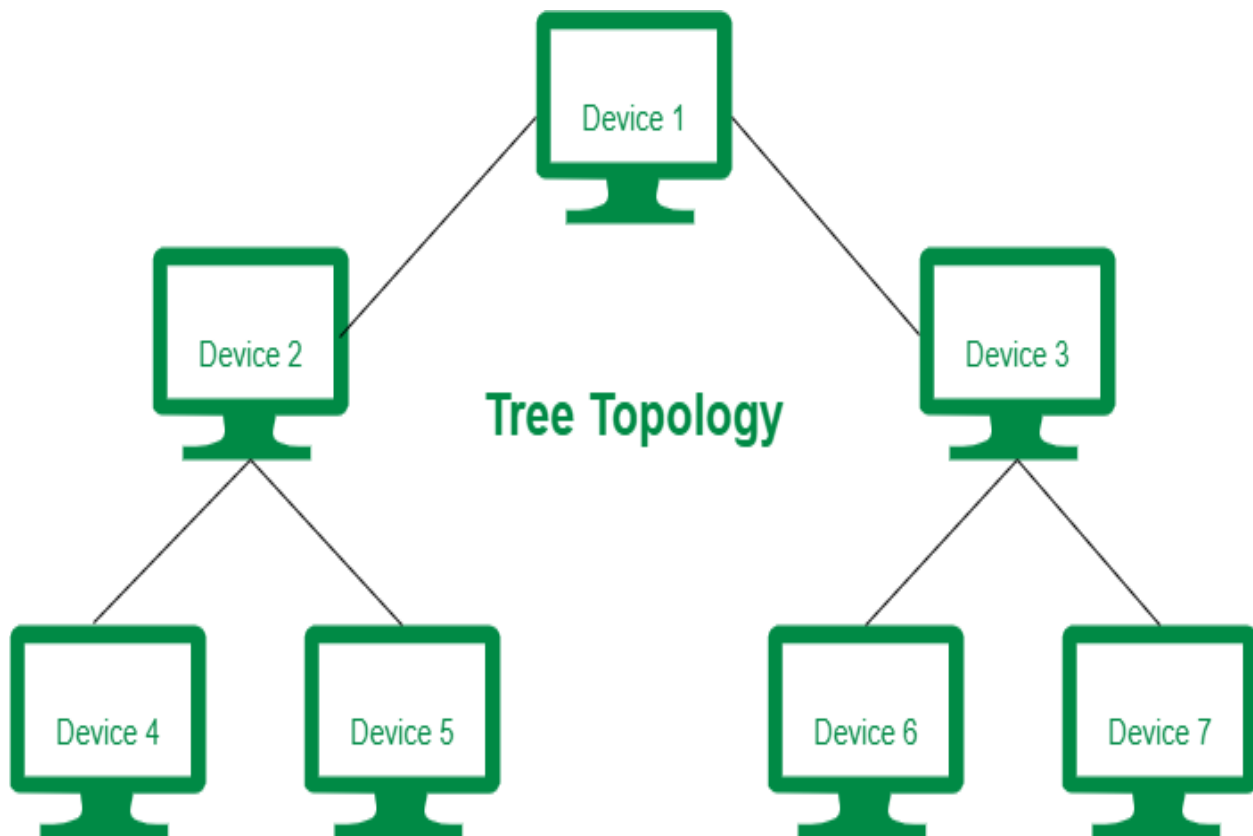


*Figure 14 Ring Topology*

The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.

### **Tree Topology**

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration ) are used.

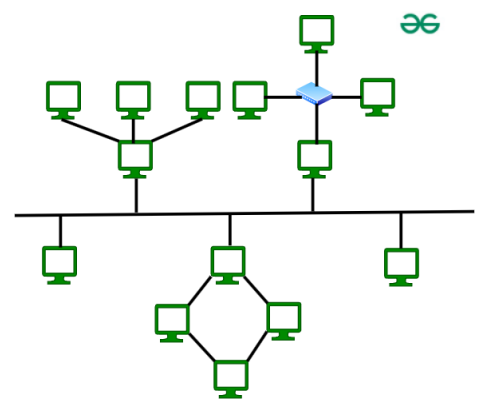


*Figure 15 tree Topology*

IN Figure: the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

### **Hybrid Topology**

This topological technology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



*Figure 16 Hybrid Topology*

## ➤ Servers

Servers are strong computers that store, manage, and distribute data within a network. They are hardware components of networks. Compared to standard personal computers, they have much more processing power, memory, and storage capacity.

Because they frequently hold sensitive data and offer essential services that must always be available, they are made to be incredibly dependable and safe.

Specialized operating systems for large user counts are frequently run on servers.

A hardware server's main job is to receive and process requests from networked computers, sometimes referred to as clients. These requests may pertain to email distribution, file retrieval and transmission, or website serving.

There are many types of servers:

**File server:** A server dedicated to storing and managing files for all users in the network.

**Web server:** Hosts websites and makes them available over the internet. **Database**

**server:** Provides database services and responds to queries from clients. **Game**

**server:** A server used for online gaming which hosts multiplayer matches. **DNS**

**server:** Translates domain names into IP addresses.

**Mail server:** Manages, stores, and transfers emails over the network.

Every server has the option of being shared (doing several jobs) or dedicated (handling only one kind of server task). Server rooms, also referred to as data centers, are designated areas where servers are kept in vast networks.

### ➤ **Clients**

Computers or other networked devices that make use of the resources and services offered by servers are known as clients. They are a type of network hardware component. The client program is the software that each client uses to communicate with the server.

The devices known as clients start communication sessions by submitting requests to servers, which reply to the clients, in a standard client-server architecture. These requests could be for services, like printing a paper, or data, like getting a web page back.

Client devices can include hardware such as printers and scanners in addition to personal computers (desktops and laptops), cellphones, and tablets. Depending on their processing capability and the proportion of the application and its data that is stored locally versus on the server, clients can also be classified as thick or thin clients.

In conclusion, clients are network endpoints that communicate with servers to gain access to common services and resources.

### ➤ **Peers**

When discussing networking, a computer or other device that is a part of a peer-to-peer (P2P) network is referred to as a "peer." In peer-to-peer networking, every peer—also referred to as a node or member—is treated equally and has the ability to communicate with other peers on the network by acting as a client or server.

Often serving as both clients and servers, peer devices allow the direct sharing of resources amongst one another, eliminating the need for a middleman server.

Examples of these resources include content, disk storage, and CPU power. Blockchain networks and file-sharing networks are two well-known examples of this.

Peers can simply be any regular computer or device that has the appropriate peer-to-peer networking software installed on it as a hardware component. The device's ability to function as a peer is provided by its software, but it may also include standard hardware parts like a CPU, memory, storage, and a network interface for network connectivity.

# Chapter 3

## Introduction to Firewalls

Firewalls are essential components of network security, acting as the first line of defense against unauthorized access and malicious traffic. Let's delve into their definition, purpose, and historical development.

### **Definition and Purpose**

A firewall is a network security device that monitors incoming and outgoing traffic flowing between a private network (like your home network) and an external network (typically the internet).

Here's a breakdown of a firewall's key purpose:

- **Traffic Inspection:** Firewalls meticulously examine incoming data packets, checking their origin, destination, type (email, web browsing, etc.), and content.
- **Rule-based Decisions:** Predefined security policies determine how the firewall treats each packet. It might allow legitimate traffic, block suspicious activity, or log information for further analysis.
- **Access Control:** By filtering traffic, firewalls restrict unauthorized access attempts to your network resources, preventing hackers and malware from infiltrating your system.

In simpler terms, imagine your home with a security guard at the entrance. The guard checks everyone entering (incoming traffic) and verifies their identity and purpose. Only authorized visitors with legitimate reasons are allowed in, while others are turned away (blocked traffic).

### **Historical Background**

The concept of a firewall has evolved over time, keeping pace with the growing complexity of network threats. Here's a glimpse into the historical journey of firewalls:

- **Early Packet Filters (1970s-1980s):** These basic firewalls simply filtered traffic based on IP addresses and port numbers, offering limited protection.
- **Proxy Servers (1980s-1990s):** Proxy servers acted as intermediaries, handling all communication between internal networks and the internet. This provided some additional security features.

- **Stateful Firewalls (1990s-present):** Stateful firewalls track the state of network connections, offering more granular control over traffic flow and improved security.
- **Next-Generation Firewalls (NGFWs) (2000s-present):** NGFWs go beyond basic packet filtering. They can analyze deeper layers of data packets, including application protocols and content, to detect and block sophisticated attacks.

Today, firewalls remain a critical security tool, constantly adapting to counter new and emerging threats in the ever-evolving digital landscape.

## Packet Filtering Firewalls

Packet filtering firewalls are the foundation of network security, offering a basic yet effective layer of protection. Let's explore how they work, their advantages, and limitations.

### How Packet Filtering Works

**Definition:** Packet filtering firewalls control network access by monitoring outgoing and incoming packets and allowing or blocking them based on a set of security rules. They operate at the network layer (Layer 3) of the OSI model.

Imagine a traffic inspector on a highway, checking each vehicle's origin, destination, and type (car, truck, etc.). Packet filtering firewalls operate similarly:

Operation:

- 1) **Packet Inspection:** Every data packet entering or leaving the network is intercepted by the firewall.
- 2) **Header Analysis:** The firewall examines the packet header, which contains information like source and destination IP addresses, port numbers, and protocol type (TCP, UDP, etc.).
- 3) **Rule Matching:** The firewall compares the packet header information against predefined security rules. These rules specify what type of traffic is allowed or blocked based on IP addresses, ports, and protocols.
- 4) **Decision and Action:** Based on the rule match, the firewall takes action:
  - **Allow:** If the packet aligns with a permit rule, it's allowed to pass through the firewall.
  - **Block:** If the packet violates a security rule, it's blocked, preventing unauthorized access.
  - **Log:** Optionally, the firewall might log information about the blocked packet for further analysis or security audits.

# Types of Packet Filtering

There are four types of packet filtering listed below:

- Dynamic packet filtering firewall
- Static packet filtering firewall
- Stateless packet filtering firewall
- Stateful packet filtering firewall

We will briefly explain each type of packet filtering firewall in the following sections.

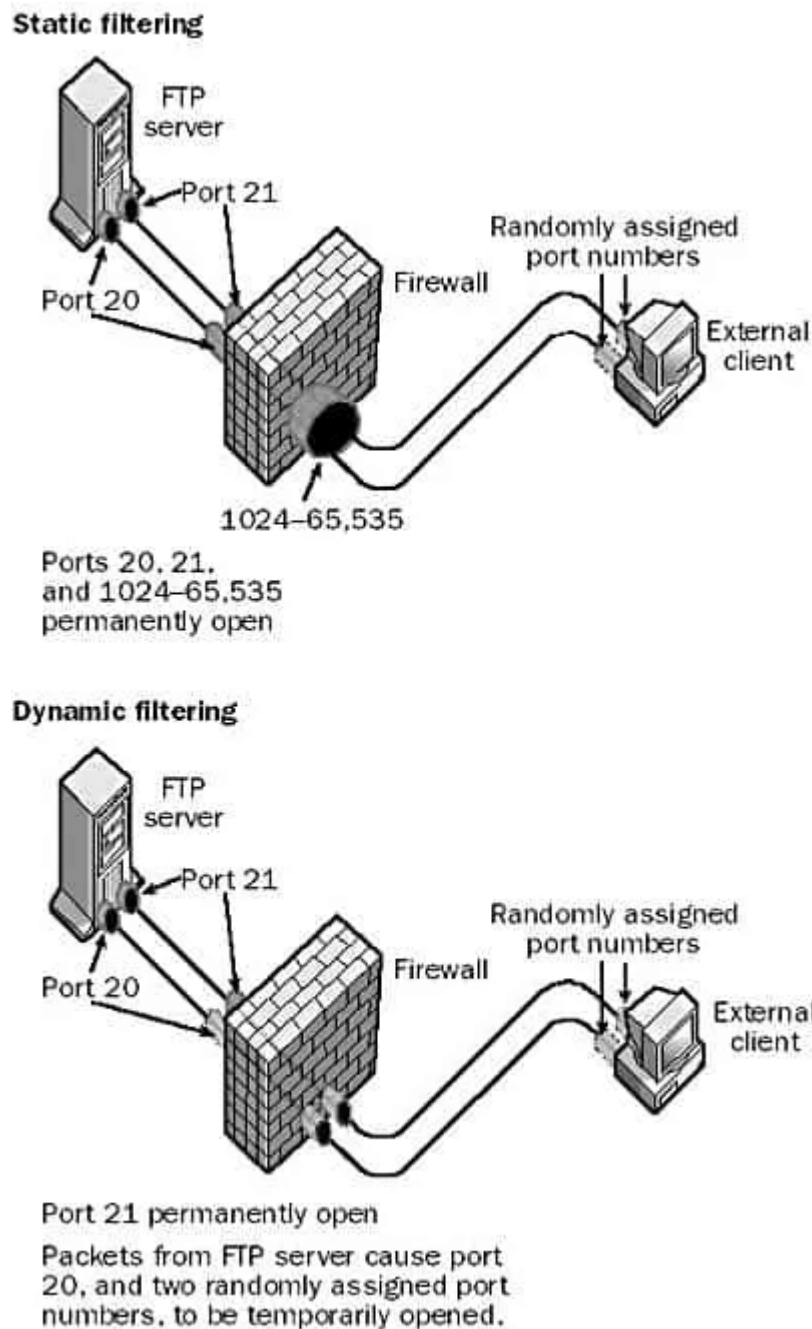
## 1) Dynamic packet filtering firewall

This form of firewall is smarter because rules can be adjusted dynamically depending on the situation, and ports are only open for a limited time before closing. Because administrators may establish customizable parameters and automate certain procedures, dynamic packet filtering firewalls are more flexible than static firewalls. Dynamic packet filtering is especially beneficial for protocols that dynamically allocate ports, such as the File Transfer Protocol (FTP). If you wish to give outside users secure access to an FTP server inside the company firewall, you need to think about the following:

- The FTP server must keep Port 21 (the FTP control port) open at all times so that it may "listen" for connection attempts from outside clients. This can be accomplished with a static filtering rule.
- Only when data will be transferred to or downloaded from the FTP server should Port 20 (the FTP data port) be opened. With static filtering, this port would have to be left open all the time, potentially opening the door to hacking efforts. This port can be opened at the start of an FTP session and then closed at the end of the session thanks to dynamic filtering.
- To create an FTP connection with the client, the FTP server assigns the client two port numbers, one for control and one for data transfer, from 1024 to 65,535 at random. Because these ports are assigned at random, there is no way to know which ports above 1024 the firewall must be able to open. If you use static filtering, you'll have to leave all ports above 1024 open all the time if you wish to allow FTP access through the firewall, which is a serious security concern. However, with dynamic filtering, you can configure firewall rules to read the packets issued by the server, dynamically open the two randomly assigned ports to allow a session to be opened, monitor the flow of packets to ensure that an unauthorized user does not attempt to hijack the session, and close the randomly assigned ports when the FTP session ends.

## 2) Static packet filtering firewall

This form of firewall requires human configuration, with the connection between the external and internal networks remaining open or closed at all times unless manually modified. Administrators can configure rules and manage ports, access control lists (ACLs), and IP addresses with these firewall types. They're usually straightforward and practical, making them a good fit for tiny applications and home or small-business networks that don't have a lot of requirements.



*Figure 17 Static and Dynamic Packet Filtering for FTP*

### 3) Stateless packet filtering firewall

Stateless packet filtering firewalls are the most common and well-known type of firewall. While they're becoming less widespread, they nevertheless serve a purpose for home internet users or service providers who deploy low-power customer-premises equipment (CPE). If users want to depart from default security settings, they must typically manually set up firewalls. Different ports and apps might pass through the packet filter thanks to manual setups.

### 4) Stateful packet filtering firewall

It employs a presettable to keep a secure connection, and packets pass through in the order that the filter rules allow. Stateful firewalls, unlike stateless packet filtering solutions, track active connections using current extensions such as transmission control protocol (TCP) and user datagram protocol (UDP) streams. Stateful firewalls can better distinguish between genuine and malicious traffic or packages by detecting the context of incoming traffic and data packets. New connections must typically introduce themselves to the firewall before being included in the list of authorized connections.

## Advantages and Limitations:

### Advantages:

- **Simplicity:** Packet filtering firewalls are relatively simple to implement and configure, especially for straightforward security policies.
- **Performance:** They typically offer high performance with low latency since they only examine the packet headers without inspecting the payload.
- **Cost-Effective:** They are less resource-intensive compared to more advanced types of firewalls, making them a cost-effective solution for basic filtering needs.
- **Basic Protection:** They provide basic protection by blocking unauthorized access and filtering out unwanted traffic based on specific criteria.

### Limitations:

- **Stateless Filtering:** Because packet filtering firewalls are stateless, they do not maintain context or track the state of connections. This makes them less effective against certain types of attacks, such as those that exploit the state of a connection (e.g., TCP SYN flood attacks).

- **Limited Visibility:** They do not inspect the payload of packets, which means they cannot detect or prevent application-layer attacks, malware, or other malicious content within the data portion of the packets.
- **Complex Rule Management:** Managing a large number of filtering rules can become complex and error-prone, especially in dynamic or large-scale network environments.
- **Lack of User Awareness:** Packet filtering firewalls do not provide any user authentication mechanisms, making it difficult to enforce user-specific security policies.

## Stateful Inspection Firewalls

Stateful inspection firewalls take network security a step further by analyzing not just the packet header but also the context of network connections. Let's delve into their key features, functionalities, and how they compare to packet filtering firewalls.

### Key Features and Functionality:

- **Definition:** Stateful inspection firewalls, also known as dynamic packet filtering firewalls, monitor the state of active connections and make decisions based on the context of the traffic rather than just individual packets.

### Key Features:

- **State Tracking:** These firewalls track the state of active connections (e.g., TCP connections) by maintaining a state table. They inspect packets within the context of these connections to ensure they are part of a legitimate session.
- **Context-Aware Filtering:** Unlike stateless packet filtering, stateful inspection considers the entire connection's state and sequence, allowing it to make more informed filtering decisions.
- **Dynamic Rule Application:** Stateful firewalls can dynamically apply rules based on the state of a connection. For example, they can allow return traffic from an established outbound connection without needing an explicit rule for the return path.
- **Enhanced Security:** By tracking state information, these firewalls can better protect against attacks such as TCP SYN floods, where the attacker tries to exhaust server resources by sending many incomplete connection requests.
- **Application Awareness:** Some stateful firewalls have basic application-layer awareness, enabling them to recognize and handle specific protocols more intelligently.

Functionality:

- **Connection Establishment:** When a connection is initiated, the firewall inspects the initial packets to determine if they match any established security rules.
- **State Maintenance:** Once a connection is established, the firewall records information about the connection in a state table, including IP addresses, port numbers, and connection state (e.g., SYN, SYN-ACK, ACK).
- **State-Based Filtering:** Subsequent packets for the same connection are allowed or blocked based on the state table entries, ensuring they are part of a valid, established connection.
- **Session Termination:** When a connection is terminated, the firewall removes the corresponding entry from the state table.

## Comparison with Packet Filtering Firewalls:

Stateful Inspection Firewalls:

- **State Awareness:** Maintain state information about active connections and use it to make filtering decisions.
- **Security:** Provide enhanced security by preventing certain types of attacks and ensuring packets are part of valid sessions.
- **Complexity:** Generally more complex than packet filtering firewalls due to state tracking and context-aware filtering.
- **Performance:** May introduce slightly more latency due to state tracking and more comprehensive inspection, but modern hardware and optimization mitigate this.

Packet Filtering Firewalls:

- **Stateless:** Do not maintain state information about connections; each packet is treated independently.
- **Basic Filtering:** Provide basic filtering based on static rules applied to packet headers (IP addresses, port numbers, protocols).
- **Simplicity:** Simpler to implement and configure, making them suitable for straightforward security policies.
- **Performance:** Typically faster with lower latency because they do not track connection states or inspect packet contents.

Comparison Table:

Feature	Packet Filtering Firewalls	Stateful Inspection Firewalls
State Tracking	No	Yes
Filtering Basis	Individual packet headers	Connection state and packet context
Security Level	Basic	Enhanced
Attack Protection	Limited (e.g., IP spoofing)	Advanced (e.g., SYN flood, session hijacking)
Complexity	Simpler	More complex
Performance	Higher performance (lower latency)	Slightly lower performance (state tracking)
Rule Management	Static rules	Dynamic rules based on connection state
Application Awareness	Limited	Basic to advanced (depending on implementation)

*Table 4 Comparison with Packet Filtering Firewalls*

## Proxy Firewalls

Proxy firewalls take a different approach to network security compared to packet filtering and stateful inspection firewalls. Let's explore how they operate, their advantages, and limitations.

### Overview and Operation:

- **Definition:** Proxy firewalls, also known as application-level gateways, act as intermediaries between end-users and the resources they access. They operate at the application layer (Layer 7) of the OSI model and can inspect, filter, and control traffic based on application-specific protocols.

Operation:

- **Intermediary Role:** A proxy firewall intercepts all requests from clients to external servers and acts on behalf of the client to communicate with the server. Similarly, it intercepts responses from the server and relays them to the client.
- **Request Handling:** When a client makes a request to an external resource, the proxy firewall examines the request, applies security policies, and then forwards the request to the destination server if it is deemed safe.
- **Response Handling:** When the server responds, the proxy firewall inspects the response, applies filtering rules, and forwards the response to the client.

- **Protocol Awareness:** Proxy firewalls understand and interpret application-layer protocols (such as HTTP, FTP, and SMTP), allowing for detailed inspection and control of the content and behavior of network traffic.
- **Caching and Content Filtering:** Proxy firewalls can cache frequently accessed content to improve performance and can also filter content based on predefined policies, such as blocking access to certain websites or types of content.

### **Benefits and Drawbacks:**

#### Benefits:

- **Enhanced Security:** By operating at the application layer, proxy firewalls can provide granular control and deep inspection of traffic, offering protection against application-specific attacks and vulnerabilities.
- **Anonymity:** Proxy firewalls can hide the internal IP addresses of clients, providing an additional layer of security by masking internal network details from external entities.
- **Content Filtering:** They can filter content based on specific criteria, such as blocking malicious websites, filtering out inappropriate content, and preventing access to unauthorized applications.
- **Logging and Monitoring:** Proxy firewalls provide detailed logging and monitoring capabilities, capturing comprehensive information about user activities, which is useful for auditing, compliance, and troubleshooting.
- **Performance Improvement:** By caching frequently accessed content, proxy firewalls can reduce bandwidth usage and improve response times for users.

#### Drawbacks:

- **Performance Overhead:** Proxy firewalls can introduce latency due to the additional processing required for deep packet inspection, content filtering, and caching. This can impact overall network performance, especially under heavy load.
- **Complex Configuration:** Setting up and maintaining a proxy firewall can be complex and time-consuming, requiring detailed knowledge of application protocols and security policies.

- **Scalability Issues:** Proxy firewalls may face scalability challenges in large, high-traffic networks due to the intensive processing demands of application-layer filtering and inspection.
- **Limited Protocol Support:** While proxy firewalls excel at inspecting and controlling traffic for supported protocols, they may struggle with newer or less common protocols, potentially requiring frequent updates and adjustments.
- **Single Point of Failure:** If a proxy firewall goes down, it can disrupt all client-server communications, making it a potential single point of failure unless redundant systems are in place.

## Next-Generation Firewalls (NGFWs)

As cyber threats become more sophisticated, traditional firewalls require additional layers of defense. Enter Next-Generation Firewalls (NGFWs), designed to address the limitations of earlier solutions. Let's explore their evolution, key features, and how they integrate with advanced security technologies.

### Evolution and Features:

Evolution:

- **Traditional Firewalls:** Initially, firewalls were simple packet filtering devices that operated primarily at the network and transport layers, inspecting packet headers to make decisions based on predefined rules.
- **Stateful Inspection Firewalls:** These introduced the concept of state tracking, allowing firewalls to maintain context about active connections and make more informed decisions.
- **Proxy Firewalls:** Operating at the application layer, proxy firewalls provided deep packet inspection and content filtering, offering enhanced security for specific applications.
- **Next-Generation Firewalls (NGFWs):** NGFWs emerged as an advanced evolution of traditional firewalls, integrating multiple security features into a single platform to address the complexities of modern network threats.

## Features:

- **Deep Packet Inspection (DPI):** NGFWs analyze the entire packet, including the payload, to detect and prevent threats embedded within the application data.
- **Intrusion Detection and Prevention Systems (IDPS):** NGFWs include built-in IDPS capabilities to detect and block suspicious activities and potential attacks in real-time.
- **Application Awareness and Control:** NGFWs can identify and control applications, regardless of port or protocol, allowing granular enforcement of security policies based on application behavior.
- **User Identity Awareness:** NGFWs integrate with user identity systems (such as LDAP, Active Directory) to apply security policies based on user roles and identities, providing personalized security measures.
- **Integrated Threat Intelligence:** NGFWs leverage up-to-date threat intelligence feeds to recognize and respond to emerging threats, providing proactive protection against new vulnerabilities.
- **SSL/TLS Decryption:** NGFWs can decrypt encrypted traffic to inspect it for malicious content, ensuring that encrypted channels are not used to bypass security measures.
- **Advanced Malware Protection:** NGFWs offer protection against advanced malware through techniques such as sandboxing, where suspicious files are executed in a controlled environment to observe their behavior.
- **Quality of Service (QoS) Management:** NGFWs can manage and prioritize network traffic, ensuring that critical applications receive the necessary bandwidth while controlling less important traffic.

## Integration with Advanced Security Technologies:

- ❖ **Endpoint Protection Platforms (EPP):** NGFWs can integrate with endpoint protection platforms to provide a comprehensive security framework, combining network-based and endpoint-based security measures.

- **Benefit:** This integration ensures coordinated defense against threats, where the firewall can block threats detected by endpoint protection software and vice versa.
- ❖ **Security Information and Event Management (SIEM):** NGFWs can feed logs and security events into SIEM systems for centralized analysis and correlation, improving threat detection and incident response.
  - **Benefit:** SIEM systems can aggregate and analyze data from multiple sources, providing a holistic view of the security landscape and enabling faster identification and mitigation of threats.
- ❖ **Threat Intelligence Platforms (TIP):** NGFWs can integrate with threat intelligence platforms to receive real-time updates about emerging threats and incorporate this intelligence into their security policies.
  - **Benefit:** Access to current threat intelligence allows NGFWs to proactively block known malicious IP addresses, domains, and other indicators of compromise.
- ❖ **Cloud Security Integration:** NGFWs can integrate with cloud security platforms to extend protection to cloud environments, ensuring consistent security policies across on-premises and cloud infrastructures.
  - **Benefit:** This integration provides visibility and control over cloud resources, helping to secure hybrid and multi-cloud deployments.
- ❖ **Network Access Control (NAC):** NGFWs can work with NAC solutions to enforce security policies based on the posture and compliance status of devices attempting to connect to the network.
  - **Benefit:** This ensures that only compliant and trusted devices can access the network, reducing the risk of compromise from vulnerable or non-compliant endpoints.
- ❖ **Advanced Threat Protection (ATP):** NGFWs can integrate with ATP solutions that use machine learning and behavioral analysis to detect and block sophisticated threats that traditional signature-based systems might miss.
  - **Benefit:** Enhanced detection capabilities provide protection against zero-day attacks and advanced persistent threats (APTs).

# Introduction to Network Security

Network security is the practice of protecting a computer network from unauthorized access, misuse, disruption, modification, or destruction. It's a crucial component of cybersecurity, ensuring the confidentiality, integrity, and availability (CIA triad) of data flowing through your network.

## **Definition and Scope of Network Security:**

Definition:

**Network Security:** Network security refers to the practices and technologies used to protect the integrity, confidentiality, and availability of data and resources as they are transmitted and stored across information networks. It involves implementing various defensive measures to safeguard against unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure of data.

Scope:

- **Data Protection:** Ensuring that data in transit and at rest is protected from unauthorized access and breaches.
- **Access Control:** Implementing mechanisms to control who can access network resources and what actions they can perform.
- **Threat Detection and Prevention:** Identifying and mitigating various forms of cyber threats and attacks.
- **Network Infrastructure Security:** Securing the underlying network infrastructure, including routers, switches, firewalls, and other devices.
- **Application Security:** Protecting applications running on the network from attacks and vulnerabilities.
- **Operational Security:** Ensuring that operational processes and procedures support and enhance network security measures.
- **Compliance and Legal Requirements:** Adhering to laws, regulations, and standards that govern data protection and privacy.

## **Common Threats and Vulnerabilities:**

### Common Threats:

- **Malware:** Malicious software, such as viruses, worms, trojans, ransomware, and spyware, that can damage or disrupt network operations.
- **Phishing:** Fraudulent attempts to obtain sensitive information, such as usernames, passwords, and credit card details, by disguising as trustworthy entities in electronic communications
- **Denial-of-Service (DoS) Attacks:** Attempts to make a network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests.
- **Man-in-the-Middle (MitM) Attacks:** Intercepting and altering communication between two parties without their knowledge.
- **SQL Injection:** Exploiting vulnerabilities in web applications by injecting malicious SQL queries to manipulate or access database information.
- **Zero-Day Exploits:** Attacks that exploit previously unknown vulnerabilities in software or hardware.
- **Insider Threats:** Threats posed by individuals within the organization who have access to network resources and misuse this access intentionally or unintentionally.

### Common Vulnerabilities:

- **Weak Passwords:** Easily guessable or common passwords that can be cracked by attackers.
- **Unpatched Software:** Software vulnerabilities that have not been addressed by applying available security patches and updates.

- **Misconfigured Devices:** Network devices that are not configured securely, leaving them open to exploitation.
- **Lack of Encryption:** Data transmitted or stored without encryption, making it vulnerable to interception and unauthorized access.
- **Insecure APIs:** Application Programming Interfaces that lack proper security measures, making them susceptible to attacks.
- **Unsecured Wi-Fi Networks:** Wireless networks that are not properly secured, allowing unauthorized access.
- **Social Engineering:** Psychological manipulation of individuals to trick them into divulging confidential information or performing actions that compromise security.

## Network Security Measures.

Network security relies on a multi-layered approach, employing various tools and techniques to safeguard your network. Here's an overview of some essential network security measures:

### **Intrusion Detection Systems (IDS):**

Intrusion detection systems (IDS) monitor enterprise networks and analyze events to detect security incidents and imminent threats. These security solutions protect businesses by proactively thwarting potential cybersecurity incidents.

An intrusion detection system is a monitoring solution that spots suspicious network incidents and sends out alerts to incident responders or security operations center (SOC) analysts. These alerts enable security personnel to investigate the detected issues and execute the appropriate countermeasures to address them before significant damage occurs.

Two main network deployment locations exist for IDS—host-based IDS (HIDS) and network-based IDS (NIDS). HIDS is deployed at the endpoint level and protects individual endpoints from threats, while NIDS solutions monitor and protect entire enterprise networks.

Apart from its deployment location, IDS also differs in terms of the methodology used for identifying potential intrusions. Signature-based IDS leverages fingerprinting to

identify known threats, such as malware. Once malicious traffic is identified, its signature is captured and added to the database. Each signature in this database is compared against network traffic in real time to detect new threats. This type of IDS is capable of detecting known threats rapidly and accurately.

False positives are extremely rare as alerts are only sent out once a known threat is detected. However, signature-based IDS solutions cannot detect unknown threats and would be helpless in the face of zero-day vulnerabilities.

On the other hand, anomaly-based IDS operates by creating a ‘normal’ network behavior model. All future network activity is compared against this behavior model, and network anomalies are highlighted as potential threats, with alerts being sent out to security personnel. This type of IDS is capable of detecting zero-day threats. However, both false positives and false negatives are possible here.

### **Intrusion Prevention Systems (IPS)**

Intrusion prevention systems (IPS) perform intrusion detection and then go one step ahead and stop any detected threats.

An intrusion prevention system is a network security hardware or software that continuously observes network behavior for threats, just like an intrusion detection system. However, IPS goes one step ahead of IDS and automatically takes the appropriate action to thwart the detected threats, including measures such as reporting, blocking traffic from a particular source, dropping packets, or resetting the connection. Some IPS solutions can also be configured to use a ‘honeypot’ (a decoy that contains dummy data) to misdirect attackers and divert them from their original targets that contain accurate data.

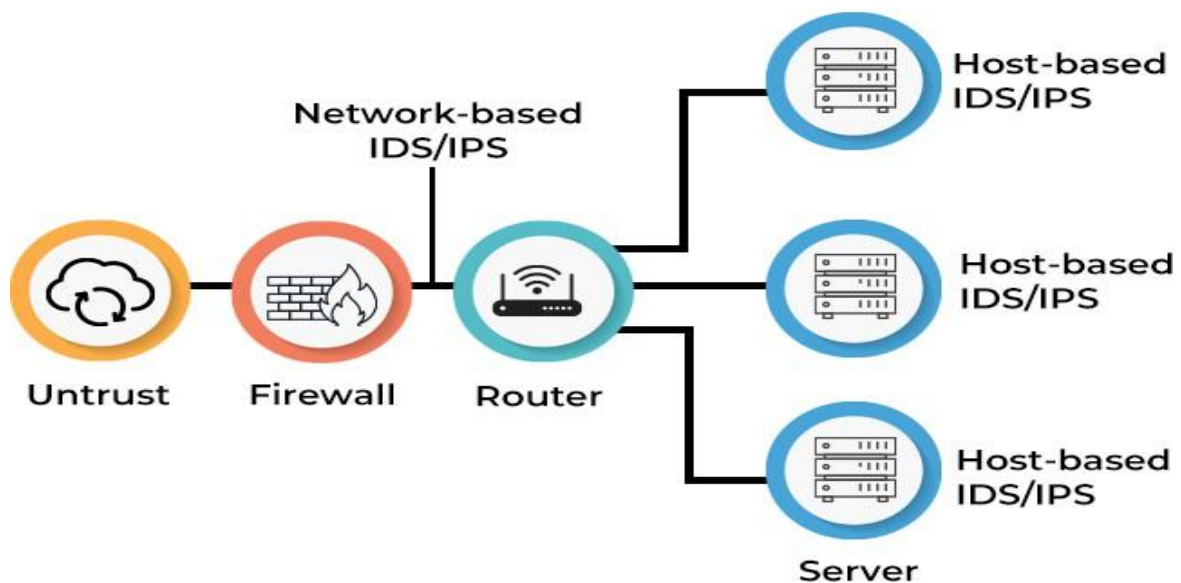
IPS is a critical component of modern-day enterprise security. This is because the organizational networks of 2022 have numerous access points and process high data volumes, thus making manually monitoring traffic and responding to threats an imposing task. Additionally, the increased popularity of cloud platforms means enterprises are operating in highly connected environments. While this has various benefits, it presents a vast attack surface and increases vulnerability if the cloud platform is not adequately secured.

As the threats faced by enterprise systems grow in number and become more sophisticated, automated security solutions such as IPS have become more vital than ever before. This network security solution allows businesses to counter threats in near real-time without stretching security teams’ capabilities. It does so by scanning high volumes of traffic without hampering network performance. Many security providers club IPS with unified threat management (UTM) or next-generation firewall (NGFW) solutions.

IPS solutions are placed within flowing network traffic, between the point of origin and the destination. IPS might use any one of the multiple available techniques to identify threats. For instance, signature-based IPS compares network activity against the signatures of previously detected threats. While this method can easily deflect previously spotted attacks, it's often unable to recognize newly emerged threats.

Conversely, anomaly-based IPS monitors abnormal activity by creating a baseline standard for network behavior and comparing traffic against it in real-time. While this method is more effective at detecting unknown threats than signature-based IPS, it produces both false positives and false negatives. Cutting-edge IPS are infused with artificial intelligence (AI) and machine learning (ML) to improve their anomaly-based monitoring capabilities and reduce false alerts.

## IDS/IPS ON AN ENTERPRISE NETWORK



*Figure 18 IDS/IPS on an Enterprise Network*

### **Virtual Private Networks (VPNs):**

A virtual private network (VPN) is a computer network that provides online privacy by creating an encrypted connection on the Internet.

The security of personal data and activities while using the Internet has always been a matter of concern. It is precisely to address this pain point that the concept of virtual private networks came about. The ambit of the technology gradually grew to accommodate the needs of businesses and corporates of varying sizes.

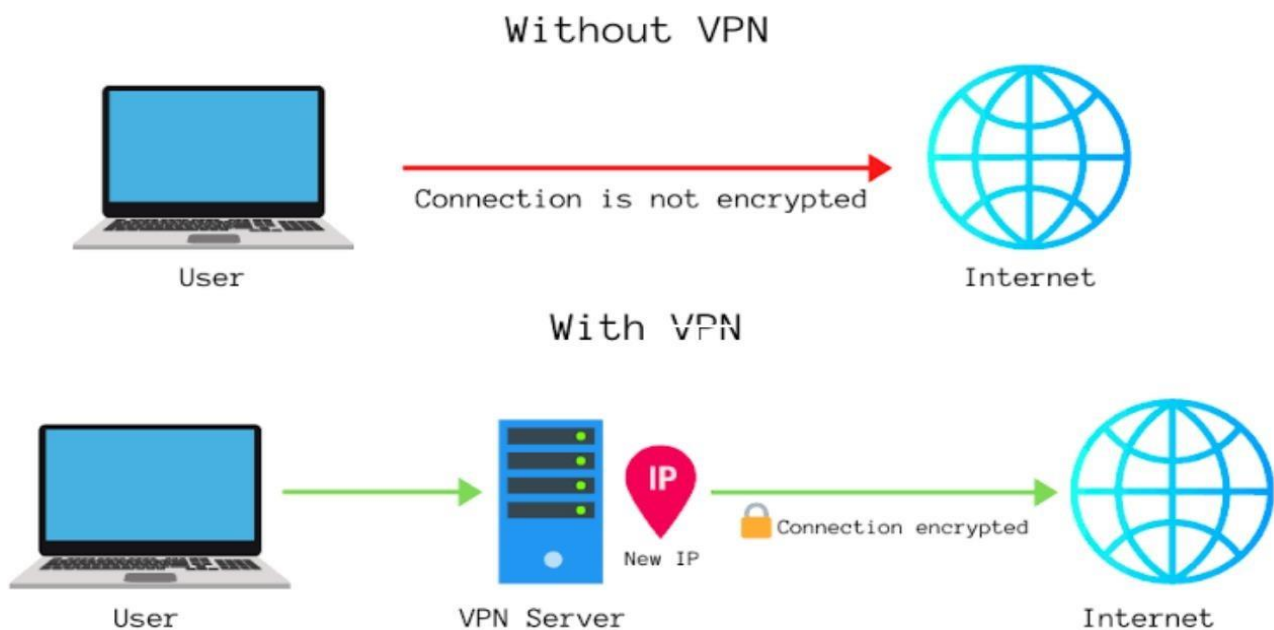
A virtual private network is a computer network that gives online privacy to a user by creating an encrypted connection from a device to a network. It uses tunneling protocols to encrypt sensitive data from a sender, transmit it, and then decrypt it at the receiver's end.

Because the user's internet protocol (IP) address is masked and untraceable during this process, it provides a high level of privacy. The most common use of VPN technology is keeping all online recreational activities of an individual untraceable, even when accessed on a private Wi-Fi network.

When used for businesses, a VPN only allows authorized personnel to access data of the organization through the Internet. With the help of a VPN, an organization with multiple offices globally can share its data with its employees, irrespective of location. This can be safely done because their IP addresses are masked, even while accessing public Wi-Fi networks. VPN significantly reduces the threat of cyber-attacks and security breaches.

A 2019 report by Knowledge Sourcing Intelligence LLP projected a CAGR growth rate of 6.39% to touch USD50.153 billion by 2024 for VPNs. The increased demand will be fueled by the need to protect against cyber-crime-related issues. Another study conducted by the University of MarylandOpens a new window concluded that hacker attacks happen at a frequency of every 39 seconds.

The CyberEdge Group 2020 Cyberthreat Defense Report revealed that 80.7% of organizations in seven major sectors had been affected by at least one successful cyberattack in 2020. VPN usage and data privacy are strongly interrelated. With VPNs making use of a separate server for Internet usage, hackers and cybercriminals can effectively be kept at bay.



*Figure 19 virtual private network (VPN)*

### Advantages and Disadvantages of Using VPN

In an article in Computer World (1997), author Bob Wallace told Tom Nolle, chief strategist at ExperiaSphere and president at CIMI Corp, that VPNs would let companies close ranks with suppliers, business partners, and remote sites around the world, and support growing legions of remote workers. Those predictions have come true to a large extent. Let's look at the advantages of a VPN.

1. Enhanced security: The fundamental functioning of a VPN strengthens the security of network traffic. It keeps all communication between remotely- located employees safe from the cybercriminals, without disturbing the flow of work. A VPN uses a range of encryption technologies like IP security (IPSec), layer 2 tunneling protocol (L2TP)/IPSec, as well as secure sockets layer (SSL) and transport layer security (TLS). All of these come together to create the tunnel through which encrypted data is passed from origin to destination points via a server.
2. Bypass geo-restrictions: Particularly in the case of personal use of a VPN, geo-restrictions can be bypassed to gain access to sites. The case in point being the scramble to access Netflix from other regions. VPN also helps to bypass censorship impositions in case of restricted sites while traveling. However, this access can be blocked if the need arises.
3. Anonymous downloads: Torrents, while usually associated with piracy, have several legitimate uses as well. Despite this, accessing Torrents can put you in trouble. VPNs can be used for access in such cases, provided they are for

legitimate causes. There are still chances of your IP address being revealed by dubious service providers.

4. **Easy file sharing:** VPNs pave the way for large networks to provide easy access to the information within a private network. It makes the management of multiple remote locations and employees easier, with access that is similar to a local intra-network. This process needs a large bandwidth. However, internet service providers (ISPs) often resort to bandwidth and data throttling to boost the Internet speed of other customers; that is, they place a cap on the amount of data and bandwidth used. VPN helps bypass these caps.

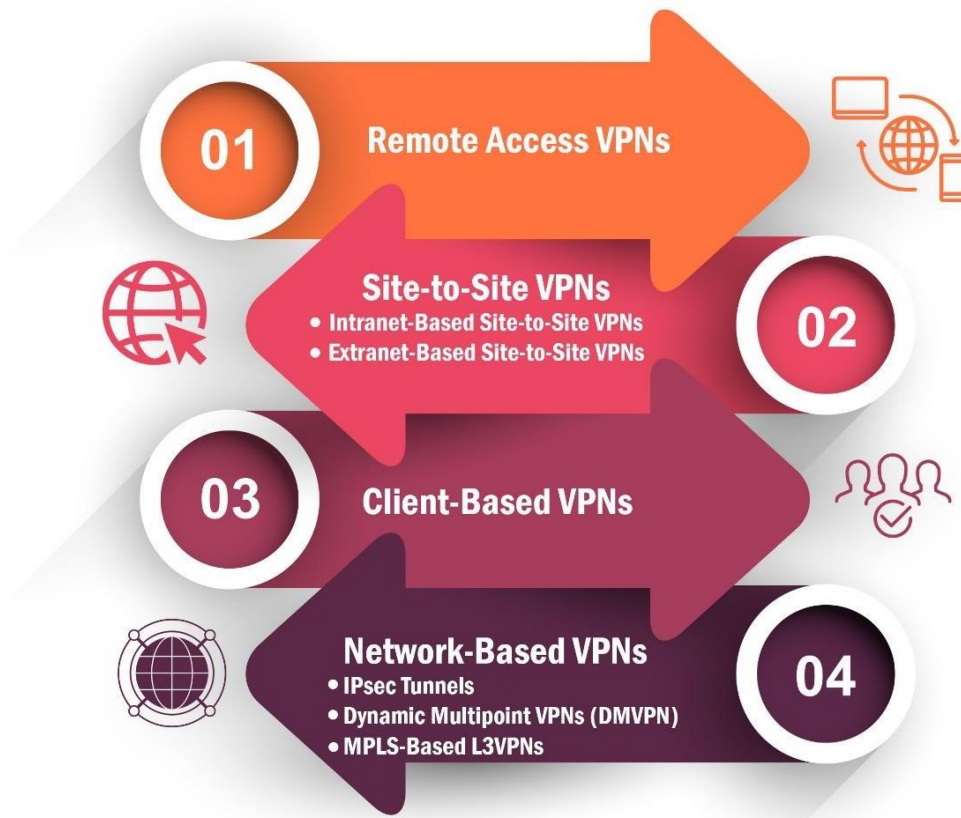
### **Disadvantages:**

1. **Speed issues:** The stronger the encryption for a VPN, the slower it becomes. This especially holds true for free VPN providers (which come with several other negative points). However, paid services can deliver good levels of encryption at decent speeds. There are several ways to boost speed, for instance, reducing the distance between the device and the VPN server location. Also, upgrading to the necessary number of servers that can take the load of a large number of people using it makes a huge difference.
2. **Increased network complexity:** If you require a high-quality VPN, the network that needs to be set up will be more complex. This comprises several network topologies, protocols as well as hardware devices. The complexity can take a while for users to understand.
3. **Security issues:** Businesses use VPNs for the primary reason of giving data access to the employees working remotely. The security of the company's network is then based on the number of users, their devices, and their access points, which reduces control of the VPN.

## **Types of VPNs:**

To find the right VPN for your business or even personal use, you must first determine what you need. The various types of VPNs include:

# TYPES OF VIRTUAL PRIVATE NETWORKS



*Figure 20 types of VPNs*

## 1. Remote access VPNs

Businesses utilize remote-access VPNs to create a secure connection between corporate networks and personal or company devices used by remote employees. Once connected, employees can access information on the company network in the same way they would if their devices were physically plugged in on office premises.

## 2. Site-to-site VPNs

Site-to-site VPNs are ideal for enterprises and businesses. They provide the ability to access and share information with a number of users based in several fixed locations.

Site-to-site VPNs are used in large-scale businesses where a multi-departmental exchange of information needs to be carried out securely and continuously. Such VPNs are not easily implemented and require a great deal of specialized equipment and complex hardware and resources. These VPNs are custom-built and may not come with the flexibility that commercial VPN services offer. Within site-to-site networks are:

- **Intranet-based site-to-site VPNs**

Intranet-based site-to-site VPN connects an organization's own networks. For instance, if a company has its headquarters in Germany and wants to set up an office in Australia. Employees in both locations will want to collaborate during the process. So, a site-to-site VPN will connect the German office local area networks (LANs) to the same wide area network (WAN) as that of Australia, and share information securely. This is an example of an intranet-based site-to-site VPN.

- **Extranet VPN site-to-site VPNs**

Extranet-based VPNs serve as a connection between two intranets that need to be connected but don't have a way of accessing each other. If two different companies want to collaborate on a project, an extranet-based VPN will be used.

### **3. Client-based VPNs**

Client-based VPNs allow users to be connected to a remote network through an application/client that manages the connection and the communication process of the VPN. For a safe connection, the software is launched and authenticated with a username and password. An encrypted link is then established between the device and the remote network.

Client-based VPNs allow users to connect their computers or mobile devices to a secure network. It's a great option for employees to access their company's sensitive information while working from home or a hotel.

### **4. Network-based VPNs**

Network-based VPNs are virtual private networks that securely connect two networks over an unsafe network. An IPsec-based WAN is an example of a network-based VPN. In this VPN, all offices of a business are connected with IPsec tunnels on the Internet.

The three common types of network VPNs include:

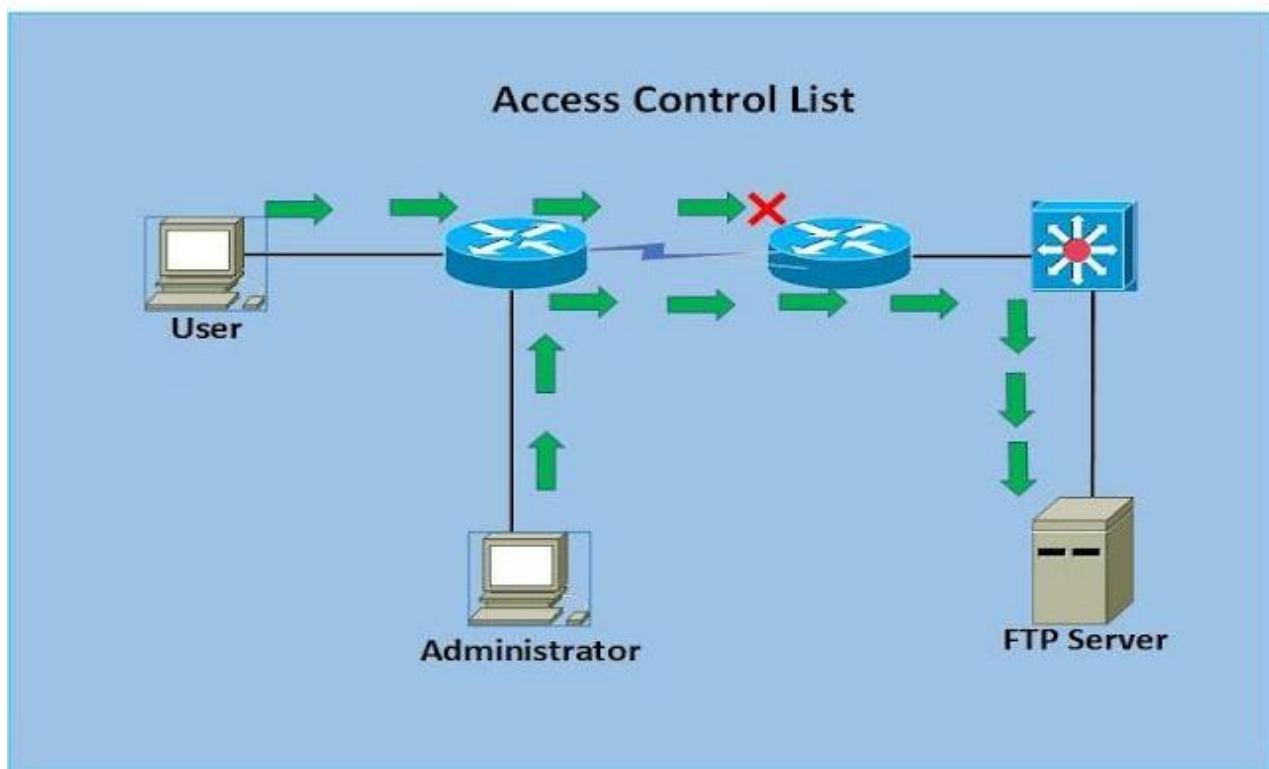
- **IPsec tunnels:** This type of approach establishes a tunnel to exchange the data between two networks in an encrypted form. IPsec tunnels can also be used to encapsulate the traffic for a single device.
- **Dynamic multipoint VPNs (DMVPN):** This type of approach allows IPsec point-to-point tunnels in a cloud of connected networks. DMVPN allows any two networks to communicate directly across the DMVPN cloud.

- **MPLS-based L3VPNs:** Multiprotocol label switched (MPLS) networks allow virtualization of networks so that users can share physical networks while staying logically separate.

## Access Control Lists (ACLs):

Access Control Lists (ACLs) are rule-based mechanisms that define who can access specific network resources and how. They can be implemented on various network devices like firewalls or routers. ACLs specify permitted or denied access based on factors like user identity, IP address, device type, or application. This allows granular control over network access, restricting unauthorized users or devices from accessing sensitive resources.

These are just some of the many network security measures available. The specific tools and techniques you use will depend on the size, complexity, and security needs of your network. By implementing a combination of these measures and following security best practices, you can significantly reduce your network's exposure to threats and vulnerabilities.



*Figure 21 Access Control Lists (ACLs)*

### **Types of Access Control Lists.**

There are two types of Access Control Lists:

#### **1. Standard ACLs**

Standard ACLs operate on the source IP address of the traffic. They are used to permit or deny traffic based on the source IP address of the packet. Standard ACLs are numbered between 1 to 99 and 1300 to 1999.

#### **2. Extended ACLs**

Extended ACLs operate on the source and destination IP addresses, protocol, and port numbers of the traffic. They are used to permit or deny traffic based on a combination of these factors. Extended ACLs are numbered between 100 to 199 and 2000 to 2699.

## **Overview of Router Connections and Server Configurations**

Router connections and server configurations are critical components of network design and operation. Routers are the devices that forward data packets between computer networks, enabling communication between devices and networks. Server configurations, on the other hand, define how servers are set up and managed to ensure availability, reliability, and performance.

## **Difference Between Access Point, Station, Bridge, and Router.**

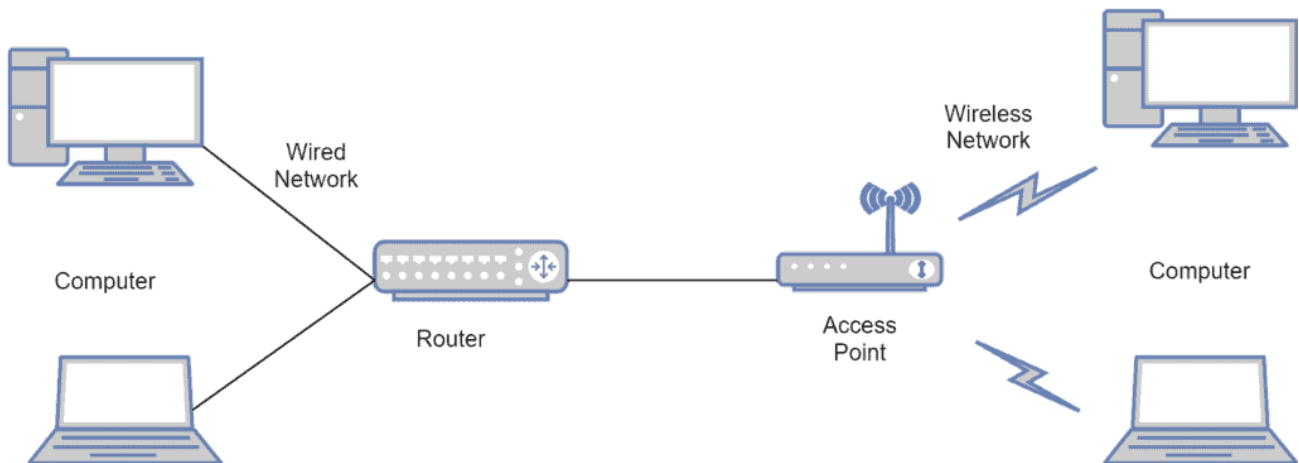
A computer network is a set of devices communicating among themselves using a wired or wireless connection. Moreover, this connection is made by combining hardware and software components.

The software components that facilitate connection are protocols and operating systems. At the same time, some of the hardware components that help make connections are router, bridge, hub, repeater, cable, and switch.

In this tutorial, we're going to emphasize the distinguishing qualities of station and router.

#### **❖ Access Point**

An access point is used to connect a wired network to a wireless one. Thus it is connected to a router by a wired connection and transmits a WiFi signal to connect other wireless devices:



*Figure 22 access point*

### ❖ Station

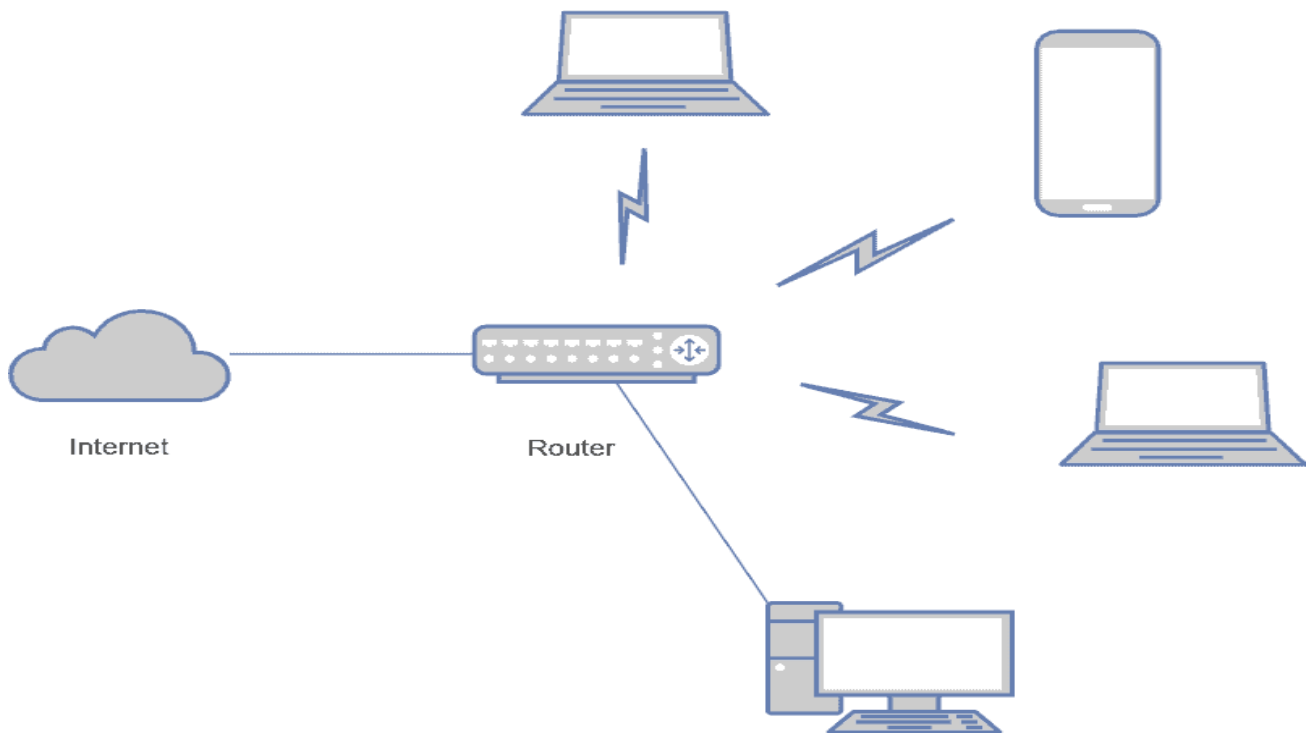
A station is a device that has access to WiFi and allows transmission and reception of data. Both the ends of data sharing is called as a station. The station is where data starts while transmission and data reach while receiving:



*Figure 23 station*

### ❖ Router

A router works at the network layer of the OSI layers. Thereby router ensures machine-to-machine transfer of data packets between source and destination:

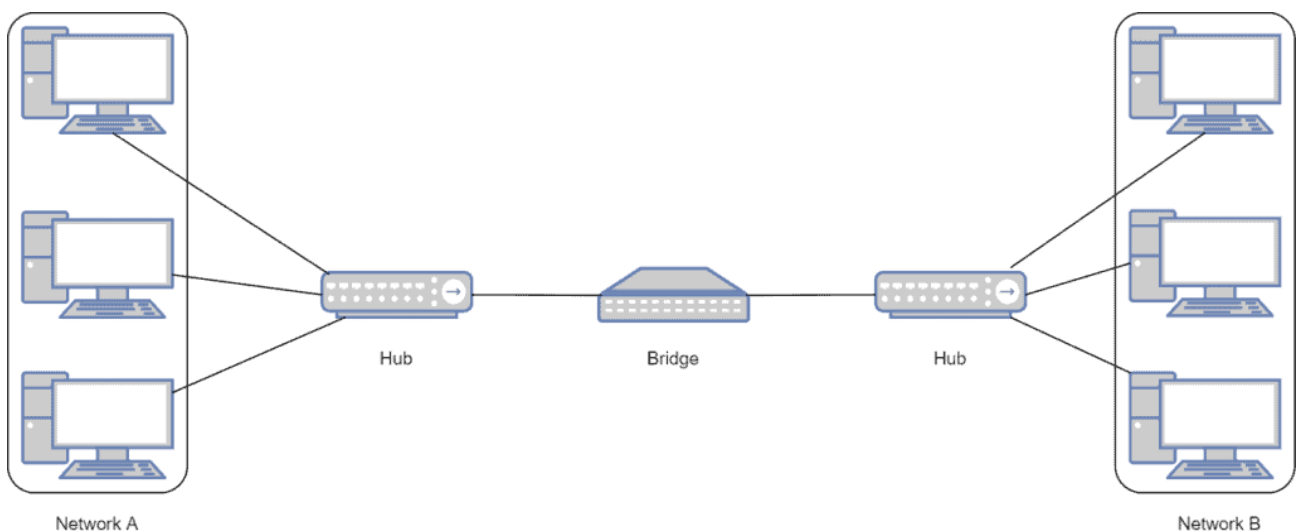


*Figure 24 router*

The router is used to read the packet's header and direct it to the destination. As the name implies, it decides the best route for transmission based on a continuously updating routing table it possesses.

### ❖ Bridge

A bridge works at the data link layer of the OSI layers. Therefore it enables the node-to-node transfer of data between source and destination. Besides acts as the connecting center of separate networks into one network:



*Figure 25 bridge*

## Variation

There are striking differences between the Bridge, Router, Access Point and Station. This section throws light on the clear-cut differences between them:

	Access Point	Station	Bridge	Router
OSI Layer	Data link	Application	Data link	Network
Connection mode	Wireless	Wireless	Wired	Wired
Protocols used	LWAPP, CAPWAP, IPP	IEEE 802.11	STP	RIP, IGRP, OSPF, EGP, EIGRP, BGP, IS-IS
Functionality	connect a wired network to a wireless network	end of the transmission or receiving having access to WIFI	connect separate networks into one network	traffic control: chooses path for data sharing
Examples of real-time brands	CISCO	Samsung, Iphone, Dell	CISCO, D-Link	CISCO

*Table 5 differences between the Bridge, Router, Access Point and Station*

## Types of Router Connections

### 1.2. Wired Connections

- **Ethernet:** The most common type of wired connection. Ethernet cables (Cat5, Cat6, etc.) connect devices to the router, providing a reliable and high-speed connection.
  - **Advantages:** High speed, low latency, stable connection.
  - **Disadvantages:** Limited mobility due to cables, installation complexity in large networks.
- **Fiber Optic:** Uses light to transmit data at very high speeds over long distances.
  - **Advantages:** Extremely high bandwidth, low latency, and long-distance capabilities.
  - **Disadvantages:** Higher cost, more delicate cables, and more complex installation.

### 9.2 Wireless Connections

Routers act as wireless access points using Wi-Fi technology to create network connections without cables. Wi-Fi utilizes radio waves to transmit data between devices and the router. Here's a breakdown of the process:

- **Standards and Protocols:** Routers adhere to specific Wi-Fi standards (like 802.11ac) that define communication protocols for data transmission.
- **Signal Transmission:** The router transmits radio waves on designated frequency bands. These waves carry encoded data packets that devices can interpret.
- **Device Connection:** Devices like laptops and smartphones search for available Wi-Fi networks and connect using a security key (password).

### Factors Affecting Wireless Performance:

- **Frequency Bands:** Wi-Fi operates on two main frequency bands:
  - **2.4 GHz:** Offers wider range but is susceptible to interference from other devices like cordless phones and Bluetooth speakers.
  - **5 GHz:** Provides faster speeds but has a shorter range and can be hindered by walls and furniture.
- **Router Placement:** The router's location significantly impacts signal strength. Ideally, place it centrally in an open area, away from obstructions like walls and metal objects.
- **Interference:** Other wireless devices and electronic appliances can create interference, weakening the Wi-Fi signal.
- **Number of Users:** The more devices connected to the network, the more it can strain bandwidth and slow down connection speeds.

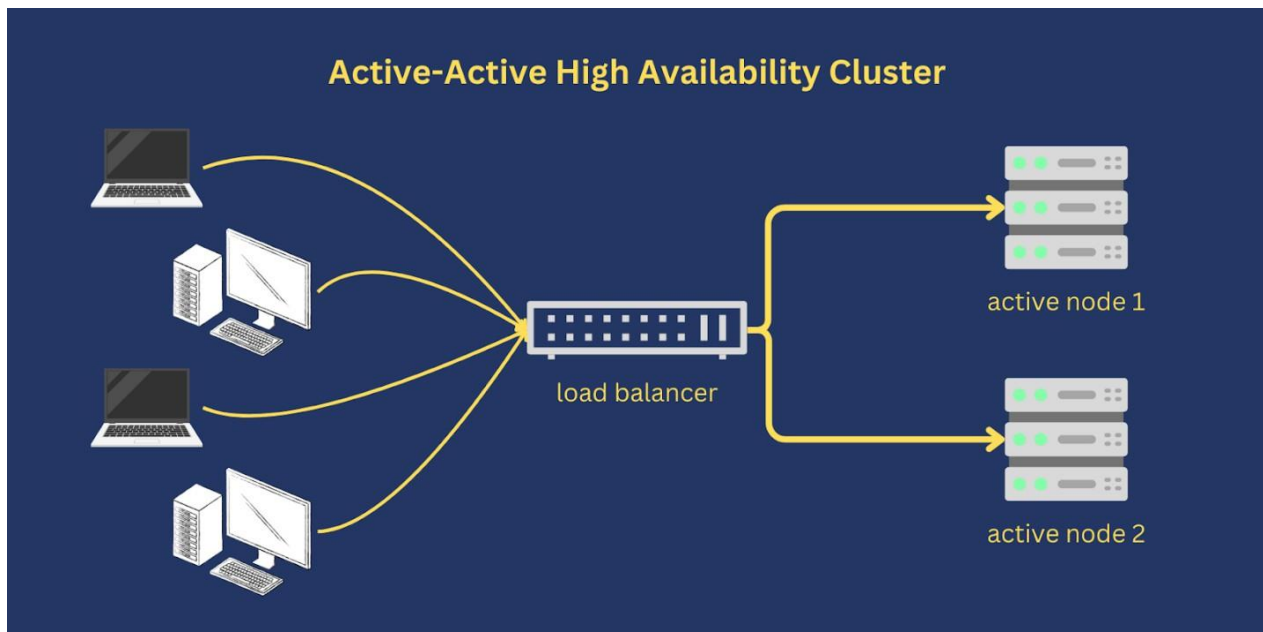
## Server Configurations

### Active-Active Configuration

An active-active configuration consists of two or more active nodes that provide similar services to multiple clients or requesting parties at the same time. For example, in a Secure File Transfer Protocol (SFTP) active-active cluster, all active servers provide SFTP services to SFTP clients. This configuration improves fault tolerance and reduces downtime since the total traffic and workload is shared across all participating nodes instead of being handled by a single node.

Since traffic is shared, each node can run at a lower capacity, avoid the risk of overload and achieve better performance. With each node capable of processing requests at a faster rate, overall traffic throughput can remain high. This can only be beneficial to end users. Your users should experience better response times and minimal, if not zero, interruptions.

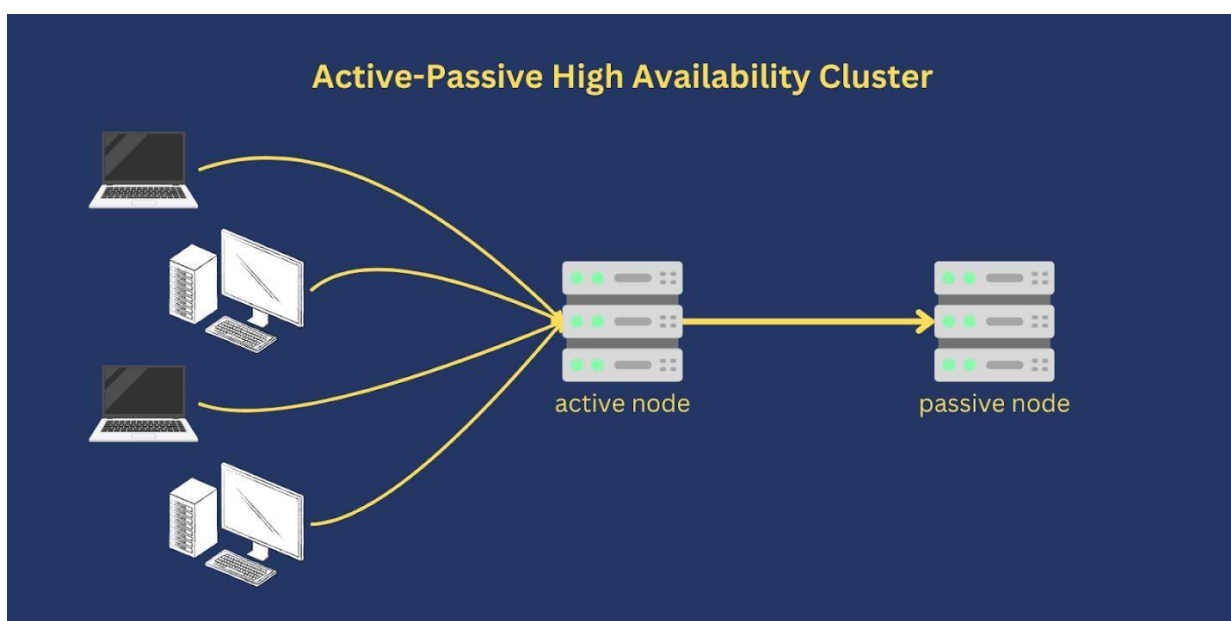
Active-active clusters are scalable. In fact, the more nodes you add to the cluster, the more effective it can be at improving throughput and user experience while reducing the risk of downtime.



*Figure 26 active-active configuration*

### **Active-Passive Configuration**

Like the active-active configuration, an active-passive configuration also consists of two or more nodes. The key difference is that, unlike active-active wherein all participating nodes are active at the same time, only one node is active in an active-passive HA cluster at any given time. All other nodes act as backups that can readily take over if the active or primary node fails.



*Figure 27 active-passive configuration*

Active-passive setups are common in disaster recovery (DR) strategies. In some DR strategies, the passive node is set up in a separate geographical location and then brought into play once the active node becomes incapacitated. You can, for example, deploy your primary node in your on-premise data center and your failover node in a cloud environment like Amazon Web Service (AWS) or Microsoft Azure.

## Practical Applications

### *How to Implement Active-Active and Active-Passive Configurations*

- **Active-Active Configuration Implementation:**
  - **Step 1:** Set up multiple servers with identical applications and data.
  - **Step 2:** Configure a load balancer to distribute incoming traffic across the servers.
  - **Step 3:** Implement data synchronization methods to ensure data consistency across all active servers.
  - **Step 4:** Monitor server performance and load to adjust the load balancing rules as needed.
  
- **Active-Passive Configuration Implementation:**
  - **Step 1:** Set up the primary (active) server with the required applications and data.
  - **Step 2:** Set up the secondary (passive) server with identical configurations but keep it in standby mode.
  - **Step 3:** Implement a failover mechanism (e.g., clustering software) to monitor the active server.
  - **Step 4:** Ensure that the passive server regularly receives updates from the active server to stay in sync.
  - **Step 5:** Test the failover process to ensure that the passive server can take over smoothly in case of a failure.

# Chapter 4

---

## *(Routing Protocols in Computer Networks)*

### Introduction

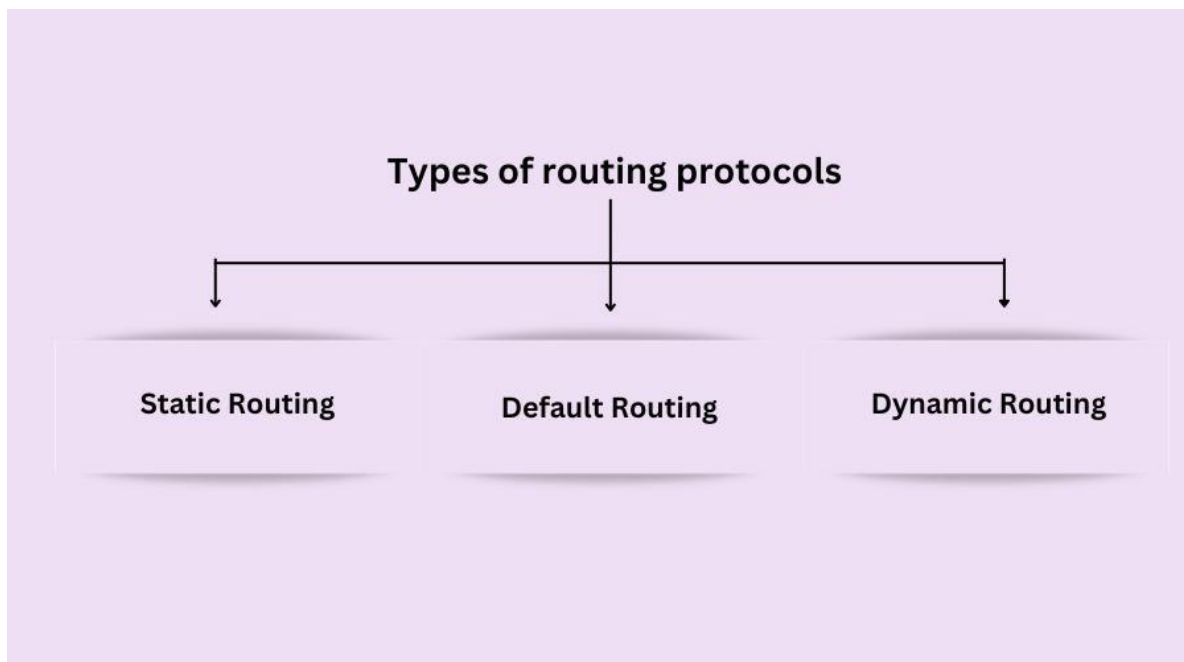
#### Routing in Computer Networks

The term "routing" comes from the word "route", which means the path used to transport data packets in computer networks. Routing is a procedure of moving data packets from one network to another by discovering the finest path from the source to the destination. The device that helps in changing the stylish path to further data packets from the source of one network to the destination of another network is called a router.

Routing protocols are the set of rules and algorithms that routers use to communicate with each other to find the most effective path to transmit data packets from a sender to a receiver. There are numerous routing protocols in computer networks, which we're going to bandy in this composition, but to understand routing protocols duly, let us first understand routing.

In computer networking, routing protocols are necessary to enable routers to share routing information and choose the optimal paths for network traffic forwarding on a dynamic basis. Through the maintenance of current routing tables that reflect the topology and connection statuses of the network, these protocols guarantee effective data transport.

In order to identify the best routes, routing protocols use a variety of techniques and metrics, including hop count, bandwidth, delay, and reliability. In order to provide dependable and effective data delivery, they constantly share routing information to adjust to network changes, such as link failures or network additions



*Figure 28 routing protocols*

## Types of Routing Protocols

There are three kinds of routing protocols in computer networks, which are given as

### **Stationary Routing Protocol (Static routing)**

It can also be called non-adaptive routing. It's a homemade configuration fashion in which the network director selects the stylish path to transfer the data packet from source to destination.

When a network director configures each router in the routing table by hand, it's called static routing. After that, the router on the data packets to the destination along the path defined by the network director.

Stationary routers are routers that employ static routing. With a wealth of advantages, static routers have been extensively used in networks moment. When there's just one route or a preferred route for business to take to reach a destination, network directors use stationary routing to specify a route. Compared to static routing, there's also dynamic routing. It's important to know the difference between these two types of routing and where are they more used.

### **(Default Routing Protocol)**

The default routing protocol can also be called the dereliction route.

When a router faces a situation where it doesn't know the destination network of a data packet, also it uses a system called "dereliction routing". It's an approach in which the router transfers all data packets to the single-hop device, anyhow of the network.

The default route is the predetermined path the router uses to shoot all data packets when encountering such a situation. When the

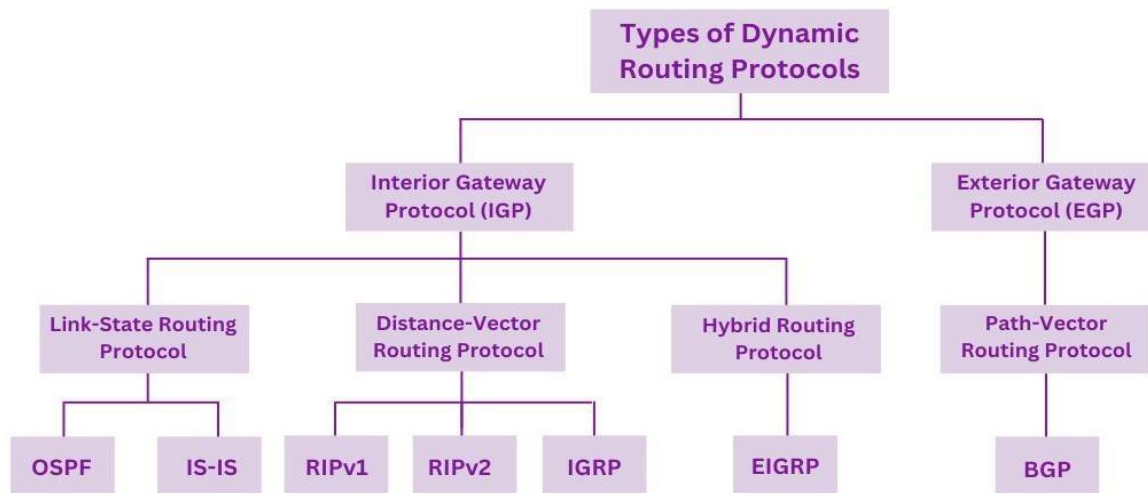
destination network is unknown to the router, also the router uses the dereliction route and sends all data packets to that route

### **(Dynamic Routing Protocol)**

It can also be called adaptive routing. It's an approach in which a router automatically finds the stylish path to transmit data packets from the sender to the receiver and puts the named path information into the routing table of each router.

The router selects the path grounded on situations of the communication circuit or the network topology. However, the

packed data is automatically acclimated on the new route to be encouraged towards the destination, If there's any loss of connection between the bumps or there's a problem with the route decided. It's ideal for larger associations where numerous routers are used. Dynamic routing protocols were designed to address the preliminarily mentioned failings of static routing similar as the need for mortal involvement to route business around failures, the mortal miscalculations made when codifying route information, and the scaling limit of the many routes one person can track in a textbook train. These benefits come at the expenditure of taking significant computing power in the routers, and the need for training network directors who specialize in reining routing algorithms.



*Figure 29 Dynamic Routing Protocol*

## (Link state routing protocol)

Open Shortest Path First( OSPF)

Open Shortest Path First( OSPF) is the most current link- state routing protocol. The OSPF Working Group of the Internet

Engineering Task Force( IETF) designed it. OSPF development began in 1987, and there are presently two active performances

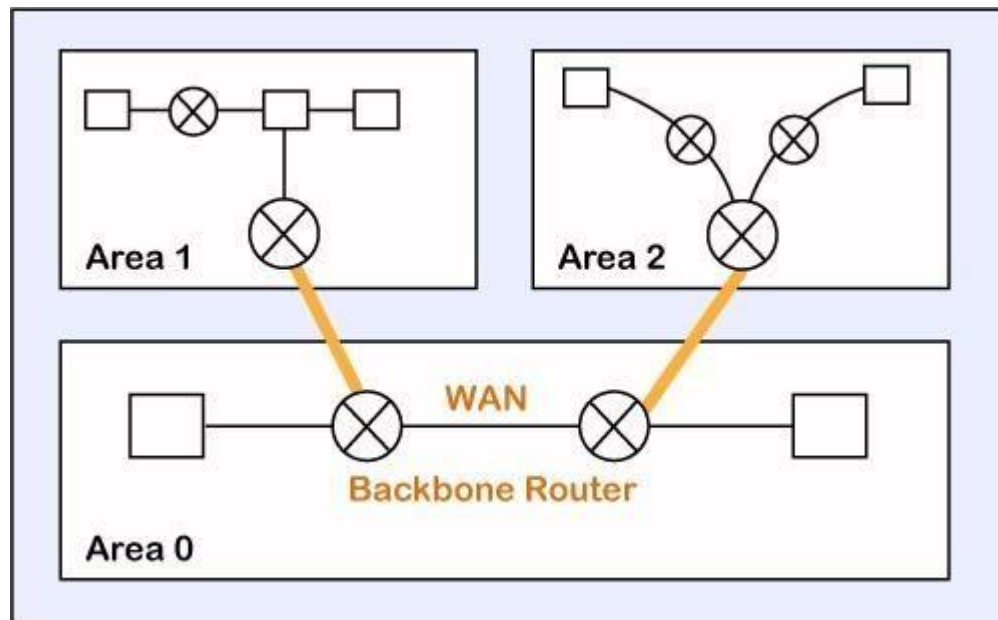
OSPFv2 OSPF for IPv4 networks( RFC 1247 and RFC 2328)

OSPFv3 is the IPv6 interpretation of OSPF( RFC 2740)

OSPFv3 now supports both IPv4 and IPv6 thanks to the Address Families functionality.

OSPF tools the link state routing algorithm and is employed in medium- to large-sized networks. OSPF is an intra domain routing protocol that only operates within a specific routing sphere. OSPF is also a hierarchical routing protocol that may be used in a single independent system. OSPF surfaced from the intermediate- system- to- system( IS- IS) routing protocol of the Open Systems Interconnection( OSI) reference model. OSPF enables multipath routing and uses one or further routing criteria , including responsibility, bandwidth, quiescence, cargo, and maximum transmission unit( MTU). Still, it also allows type- of- service( TOS) requests for business isolation, If OSPF utilizes numerous criteria .

OSPF, is a link- state, interior gateway, and cloddish protocol that uses the shortest path first( SPF) algorithm to insure effective data transmission. Internally, this type maintains multitudinous databases containing topology tables and network-wide information. Generally, the data is deduced from link state advertising transmitted by individual routers. The advertising, which resembles reports, provides thorough details of the path's length and the coffers that may be necessary.



*Figure 30*

OSPF divides the independent systems into areas where the area is a collection of networks, hosts, and routers. Like internet service providers divide the internet into a different independent system for easy operation and OSPF further divides the independent systems

into Areas. Routers that live inside the area flood the area with routing information. In Area, the special router also exists. The

special routers are those that are present at the border of an area, and these special routers are known as Area Border Routers. This router summarizes the information about an area and shares the information with other areas.

All the areas inside an independent system are connected to the backbone routers, and these backbone routers are part of a primary area. The part of a primary area is to give communication between different areas.

<b>Version(8)</b>	<b>Type(8)</b>	<b>Message (16)</b>
<b>Source IP address</b>		
<b>Area Identification</b>		
<b>Chcek sum</b>		<b>Auth.Type</b>
<b>Authentication (32)</b>		

*Figure 31*

### **OSPF Message Format**

The following are the fields in an OSPF message format:

#### **OSPF Protocol**

**Version:** It is an 8-bit field that specifies the OSPF protocol version. **Type:** It is an 8-bit field. It specifies the type of the OSPF packet.

**Message:** It is a 16-bit field that defines the total length of the message, including the header. Therefore, the total length is equal to the sum of the length of the message and header.

**Source IP address:** It defines the address from which the packets are sent. It is a sending routing IP address.

**Area identification:** It defines the area within which the routing takes place.

**Checksum:** It is used for error correction and error detection.

Authentication type: There are two types of authentication, i.e., 0 and 1. Here, 0 means for none that specifies no authentication is available and 1 means for pwd that specifies the password-based authentication.

Authentication: It is a 32-bit field that contains the actual value of the authentication data.

## **How does OSPF work?**

There are three way that can explain the working of OSPF

Step 1 The first step is to come OSPF neighbors . The two connecting routers running OSPF on the same link creates a neighbor relationship.

Step 2 The alternate step is to change database information. After getting the neighbors, the two routers change the LSDB information with each other.

Step 3 The third step is to choose the stylish route. Once the LSDB information has been changed with each other, the router chooses the stylish route to be added to a routing table grounded on the computation of SPF.

### **(Is-Is protocol)**

The IS-IS protocol is an interior gateway protocol (IGP) that uses link-state information to make routing decisions. IS-IS is a link-state IGP that uses the shortest-path-first (SPF) algorithm to determine routes. For the purpose of exchanging routing information between autonomous systems (ASes), computer networks and the Internet employ the IS-IS protocol, which stands for Intermediate System to Intermediate System. Because it functions at both the OSI layer 2 (data link layer) and layer 3 (network layer), it can be used in both LAN and WAN settings. Because of its scalability and effectiveness in managing big networks, IS-IS is frequently utilised in large service provider networks as well as in some enterprise situations.

### **(Is-Is terminology)**

An IS-IS network is made up of end systems and intermediate systems and is a single autonomous system (AS), also known as a routing domain. Network entities that send and receive packets are called end systems. Packets are sent, received, and relayed (forwarded) by intermediate systems. (A router is referred to as an intermediate system in Open System Interconnection [OSI] terminology.) Network PDUs are the name for ISO packets. Within

IS-IS, an AS can be further subdivided into areas, which are smaller groups. Administrative division of a domain into smaller areas is possible due to the hierarchical organisation of routing between areas. Configuring Level 1 and Level 2 intermediate systems completes this organisation. When a destination is outside of a defined area, Level 1 systems route in the direction of a Level 2

system. Intermediary systems at Level 2 provide routes between areas and to other Ass. No IS-IS area serves as the only backbone. IP addresses that are available within each region are shared across Level 2 and Level 1 routers, while Level 1 routers exchange routing information inside each area. Because of their special ability, IS-IS routers can function as Level 1 and Level 2 routers at the same time. They can share inter area and intra area routes with other Level 2 and Level 1 routers. The level boundaries control the link-state

update propagation. Each router in a level keeps track of every other router in the level's link-state database. The shortest path between a local router and other routers in the link-state database is then found by each router using the algorithm.

### **(Is-Is packets)**

IS-IS hello (IIH) PDUs—Broadcast to discover the identity of neighboring IS-IS systems and to determine whether the neighbors are Level 1 or Level 2 intermediate systems.

IS-IS hello PDUs establish adjacencies with other routers and have three different formats: one for point-to-point hello packets, one for Level 1 broadcast links, and one for Level 2 broadcast links. Level 1 routers must share the same area address to form an adjacency, while Level 2 routers do not have this limitation. The request for adjacency is encoded in the Circuit type field of the PDU.

Hello PDUs have a preset length assigned to them. The IS-IS router does not resize any PDU to match the maximum transmission unit

(MTU) on a router interface. Each interface supports the maximum IS-IS PDU of 1492 bytes, and hello PDUs are padded to meet the maximum value. When the hello is sent to a neighboring router, the connecting interface supports the maximum PDU size

Parameter	OSPF	ISIS
Administrative Distance	110	115
Standard	RFC 2328 (OSPFv2)	ISO 10589, RFC1195
Operating OSI Layer	OSPF operates on top of IP Layer	ISIS operates over L2
Virtual Links Supported	Yes	No
DR/BDR election	OSPF elects a DR and BDR on broadcast networks	ISIS elects a single DIS on broadcast networks
IP connectivity	OSPF requires IP connectivity between the routers to share the routing information	ISIS doesn't require IP connectivity between the routers as updates are sent via CLNS instead of IP.
Security	Prone to attack and hence requires more security overheads for protection.	Since ISIS runs on Layer 2 , hence very unlikely possibility of attack
Area/Level Types	<ul style="list-style-type: none"> <li>• Backbone Area</li> <li>• Standard Area (Non Backbone Area)</li> </ul>	Different Levels used in place of area <ul style="list-style-type: none"> <li>• Level 1</li> <li>• Level 2</li> <li>• Level 1/2 Areas</li> </ul>
Identification	OSPF uses router id to identify a router on network	ISIS uses System ID to identify a router on the network.
Table Refresh	OSPF refreshes the entire routing table after 30 minutes.	ISIS doesn't refresh the entire SPF table periodically like OSPF.
Related terms	Area,non-Backbone Area, Backbone Area,ABR,ASBR,Host	IS,Level-1,Level-2,L1/L2,Sub Domain,ES
Flexibility	Less flexible than ISIS	More flexible to use than OSPF especially in provider domain
Scalability	Less scalable than ISIS	More scalable than OSPF

*Table 6 compare between OSPF,ISIS*

## (Distance vector routing protocols )

### *The Routing Information System( RIP)*

RIP is grounded on the distance vector- grounded strategy, so we consider the entire structure as a graph where bumps are the routers, and the links are the networks.

In a routing table, the first column is the destination, or we can say that it's a network address.

The cost standard is the number of hops to reach the destination. The number of hops available in a network would be the cost. The hop count is the number of networks needed to reach the destination.

In RIP, perpetuity is defined as 16, which means that the RIP is useful for lower networks or small independent systems. The maximum number of hops that RIP can contain is 15 hops, i.e., it shouldn't have further than 15 hops as 16 is perpetuity.

The coming column contains the address of the router to which the packet is to be transferred to reach the destination.

At first we defined (Rip) in RFC 1058 as a first- generation routing protocol for IPv4. RIP is a distance- vector routing protocol that uses the metric hop count. RIP is straightforward to configure, making it an excellent option for small networks.

RIPv1 possesses the ensuing rates

The number of hops is employed as the path selection metric.

Every 30 seconds, routing updates are transmitted(255.255.255.255).

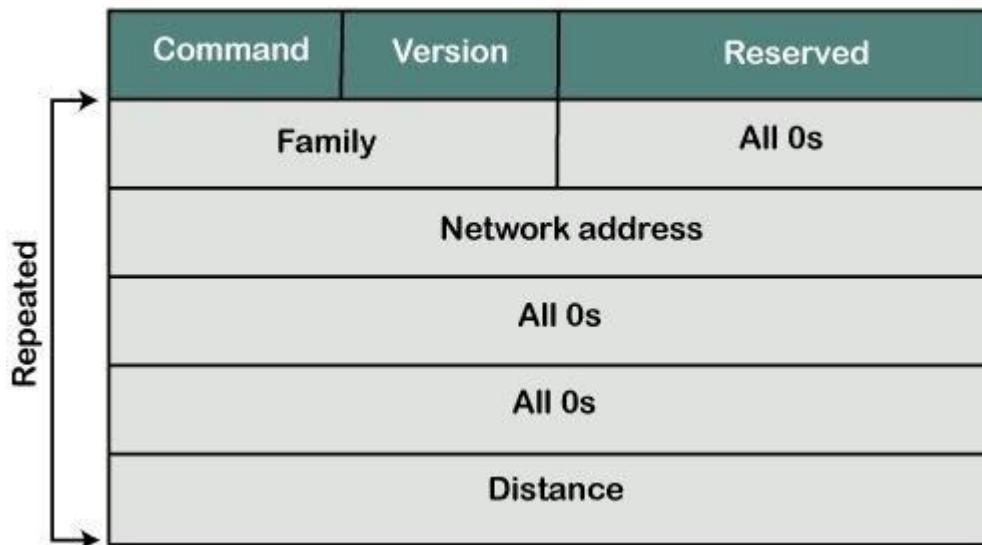
Lesser than 15 hops is considered horizonless( too far). This 15<sup>th</sup> hop router would not transmit the routing update to the following router.

In 1993, RIPv1 evolved into RIP interpretation 2, a cloddish routing protocol( RIPv2). RIPv2 brought the posterior advancements

Security It includes an authentication medium for securing routing table update dispatches between neighbors.

Cloddish routing protocol support It supports VLSM and CIDR because routing updates include the subnet mask.

### (RIP Message)



*Figure 32 RIP Message*

**RIP Message** the structure of the RIP message format. The message format is used to share information among different routers. The RIP contains the following fields in a message. **Command:** It is an 8-bit field that is used for request or reply. The value of the request is 1, and the value of the reply is 2.

**Version:** Here, version means that which version of the protocol we are using. Suppose we are using the protocol of version 1, then we put the 1 in this field.

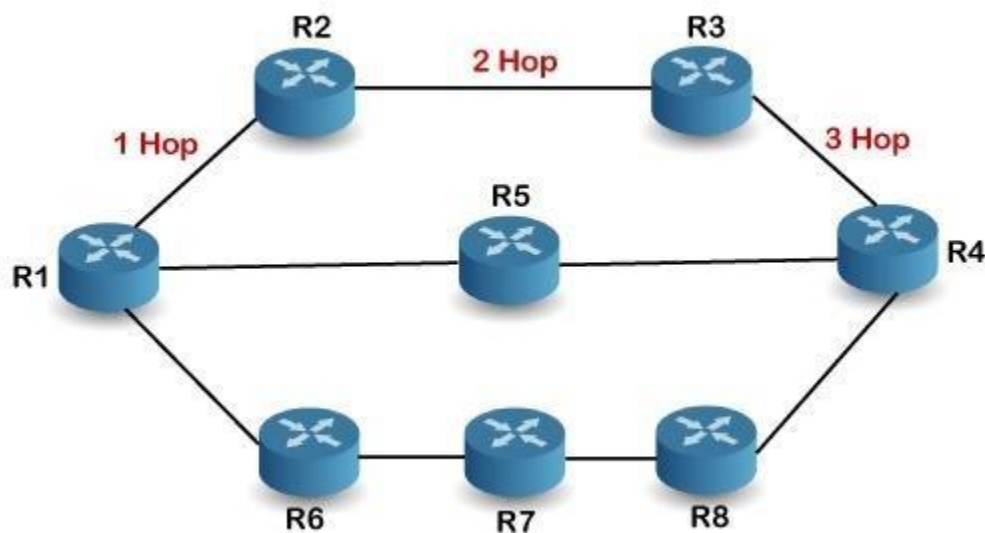
**Reserved:** This is a reserved field, so it is filled with zeroes.

**Family:** It is a 16-bit field. As we are using the TCP/IP family, so we put 2 value in this field.

**Network Address:** It is defined as 14 bytes field. If we use the IPv4 version, then we use 4 bytes, and the other 10 bytes are all zeroes.

**Distance:** The distance field specifies the hop count, i.e., the number of hops used to reach the destination.

# RIP protocol



*Figure 33 RIP Protocol*

When the router sends the packet to the network segment, then it is counted as a single hop.

## RIP Protocol

In the above figure, when the router 1 forwards the packet to the router 2 then it will count as 1 hop count. Similarly, when the router 2 forwards the packet to the router 3 then it will count as 2 hop count, and when the router 3 forwards the packet to router 4, it will count as 3 hop count. In the same way, RIP can support maximum upto 15 hops, which means that the 16 routers can be configured in a RIP.

**(This timers are used in Rip )**

RIP update timekeeper 30 sec

The routers configured with RIP shoot their updates to all the neighboring routers every 30 seconds.

#### RIP Invalid timekeeper 180 sec

The RIP invalid timekeeper is 180 seconds, which means that if the router is dissociated from the network or some link goes down, also the neighbor router will stay for 180 seconds to take the update

.However, also it'll mark the particular route as not accessible, If it doesn't admit the update within 180 seconds.

#### RIP Flush timekeeper 240 sec

The RIP flush timekeeper is 240 alternate which is nearly equal to 4 min means that if the router doesn't admit the update within 240

seconds also the neighbor route will remove that particular route from the routing table which is a veritably slow process as 4 twinkles is a long time to stay

## **Second type of distance vector routing protocols**

### **Interior gateway routing protocol**

In a host network, the Interior Gateway Routing Protocol(IGRP) is a personal distance vector routing protocol that's used to change routing information. Cisco was the bone who came up with the idea.

The Interior Gateway Routing Protocol(IGRP) regulates the transfer of routing information among linked routers in the host network or independent system. The protocol guarantees that every router's routing table is kept up to date with the most direct route available. IGRP also helps to minimize routing circles by streamlining itself in response to changes that do on the network and by enforcing error operation.

## **Characteristics**

The following are the characteristics of the IGRP( Interior Gateway Routing Protocol)

The Interior Gateway Routing Protocol(IGRP) is a distance- vector routing protocol created by Cisco.

In addition to bandwidth, detention (by dereliction), trustability, cargo, and MTU are all measured in the IGRP protocol.

It transmits updates every 90 seconds, with a hold-down time of 280 seconds between each broadcasting session.

When network changes do, touched off updates are employed to expedite the confluence process.

The IGRP router command needs the addition of an AS number.

For routers to communicate routing information, they must be in the same Associated System Number (AS).

The maximum number of hops allowed by IGRP is 255. It has a dereliction value of 100 and is frequently changed to 50 or lower.

The IGRP announcement value is 100.

## **Pretensions of IGRP**

The Interior Gateway Routing Protocol (IGRP) has two primary objects

Its primary function is to give routing information to all linked routers within its border or inside its independent system

It'll automatically modernize whenever the network topology changes.

Every 90 seconds, it sends out a notice to its neighbors to inform them of any new variations.

## **Chapter 5 ( part 1)**

(Comparison between gns3 and packet tracer )

### **Introduction**

(Packet Tracer):

Packet Tracer is a powerful network simulation tool designed by Cisco. It allows users to create, design, test and debug virtual models of computer networks. Packet Tracer is widely used in

vocational education and training to build basic networking skills, such as:

Configure network devices: such as routers, switches, and wireless access devices.

Design of network protocols: such as TCP/IP, RIP, EIGRP, and OSPF.

Network Troubleshooting: Identifying and resolving problems in networks.

Network Security: Design and implement network security solutions. Packet Tracer is compatible with Linux, macOS, and Microsoft Windows. There were additional apps available for

mobile operating systems such as iOS and Android. With Packet Tracer, users may drag and drop switches, routers, and other network device types to simulate different network topologies. A

‘cable’ item represents a physical connection between devices. To the extent necessary by the current CCNA curriculum, Packet Tracer offers basic routing with RIP, OSPF, EIGRP, and BGP in addition to a variety of simulated Application Layer protocols.

Packet Tracer now supports the Border Gateway Protocol as of version 5.3. Packet Tracer is not just a computer network simulator; it can also be used in collaborative settings.

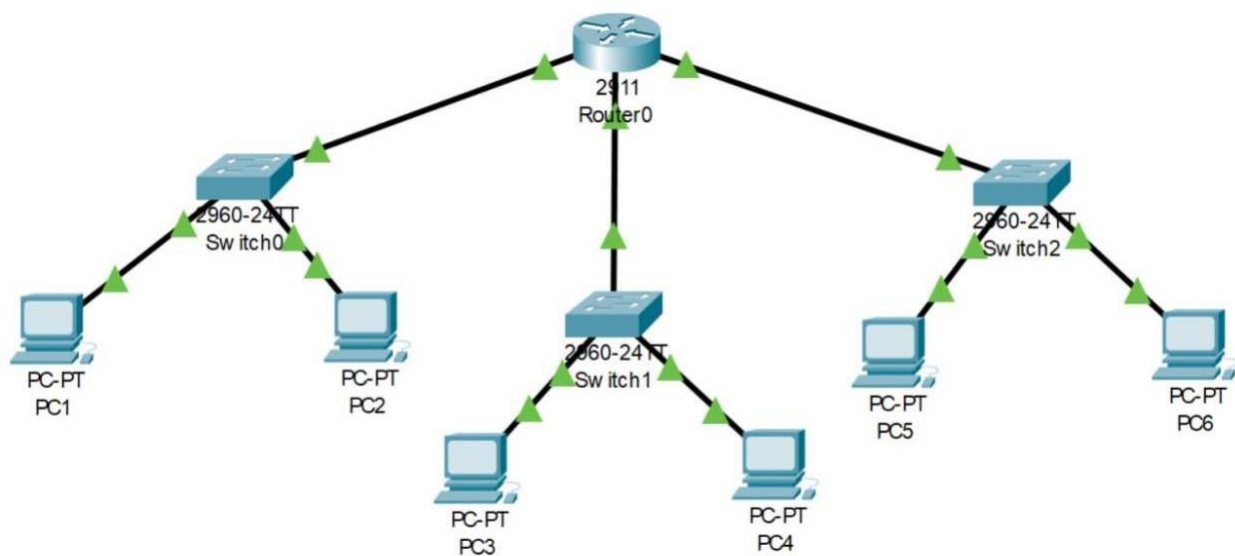
## **Uses of packet tracer**

- 1- Users can create a simulated network environment with network simulation. This allows users to connect, configure, and simulate interactions between devices such as PCs, servers, routers, and switches.
- 2-Educational Tool: To teach networking fundamentals, Packet Tracer is widely used in educational contexts, including classrooms and online courses. Without requiring actual hardware, it offers a secure environment for students to experiment with network settings and protocols.
- 3-Prototyping and Testing: Network administrators and engineers can use Packet Tracer to prototype network designs and configurations before implementing them in real-world environments. This helps in testing different scenarios and ensuring the stability and security of the network.
- 4-Packet Tracer comes with tools for debugging and resolving connectivity problems as well as for analysing packet flows and

monitoring network traffic. This aids users in honing their abilities to recognise and fix network issues.

5-Collaborative Learning: In collaborative learning environments, it enables individuals to work together on a same network project. This is very useful when managing networking labs in a classroom or working on group projects.

### **Example of simulation of packet tracer**



*Figure 34 Example of simulation of packet tracer*

### **Features:**

- **Ease of Use:** Packet Tracer has a user-friendly interface that allows users to easily design, configure, and troubleshoot networks.
- **Simulation of Network Devices:** It simulates various network devices such as routers, switches, and PCs, which helps in learning networking concepts without needing physical hardware.
- **Realistic Simulation:** It provides a fairly realistic simulation of network behaviors , allowing users to understand how data packets travel through a network.
- **Virtual Learning Environment:** Ideal for educational purposes, Packet Tracer facilitates learning networking concepts, protocols, and configurations in a controlled environment.
- **Cost-effective:** It eliminates the need for expensive physical hardware, making it accessible for students and professionals alike.
- **Supports Multiple Protocols:** It supports a wide range of protocols and technologies used in modern networks, enabling comprehensive learning and experimentation.

## **Disadvantages of packet tracer**

1-Limited Features: While Packet Tracer covers many networking concepts, it may lack some advanced features and nuances found in real-world hardware and software.

2-Simulated Environment: Since it's a simulation, it may not fully replicate all behaviors of physical networks or real-world scenarios, leading to potential gaps in understanding for complex configurations or interactions.

3-Vendor-Specific: Packet Tracer is developed by Cisco, so it primarily focuses on Cisco devices and technologies. It may not fully represent the products and configurations of other network equipment vendors.

4-Performance Differences: Simulated performance in Packet Tracer may differ from actual hardware performance, especially in large-scale or high-performance network scenarios.

5-Dependency on Updates: It requires updates from Cisco to include newer technologies and protocols, which may sometimes lag behind real-world implementations.

## **GNS3 (Graphical Network Simulator-3)**

is a powerful network simulation tool that allows users to build, design, and test complex network configurations. It's widely used by network engineers, IT professionals, and students to simulate networks using real network operating systems and software

### **Features of GNS3:**

1-Realistic Network Simulations: GNS3 can emulate a wide variety of network devices, including routers, switches, and virtual machines, running actual network operating systems (such as Cisco IOS, Juniper Junos, etc.). This makes it suitable for simulating real-world network scenarios.

2-Graphical Interface: Similar to Packet Tracer, GNS3 offers a graphical interface where users can drag and drop network devices onto a virtual topology canvas. This makes it intuitive to design and configure networks.

3-Vendor-Neutral: Unlike Packet Tracer, which is focused on Cisco technologies, GNS3 supports multiple vendors' devices and operating systems. This flexibility allows users to simulate networks with devices from different manufacturers.

4-Integration with Virtualization Platforms: GNS3 integrates with virtualization platforms like VMware and VirtualBox, enabling users to incorporate virtual machines (VMs) into their network topologies. This is useful for testing server-client interactions and complex network services.

5-Community Support and Resources: GNS3 has a large and active community of users who contribute to forums, provide tutorials, and share network configurations. This community support makes it easier for users to learn and troubleshoot network configurations

6-Advanced Network Configurations: It supports advanced networking features such as VLANs, QoS (Quality of Service),

MPLS (Multiprotocol Label Switching), and more. This makes it suitable for testing and learning complex network setups.

7-Open-Source: GNS3 is open-source software, which means it's free to download and use. This makes it accessible for students and professionals alike, without requiring expensive hardware or software licenses.

### Example of simulation

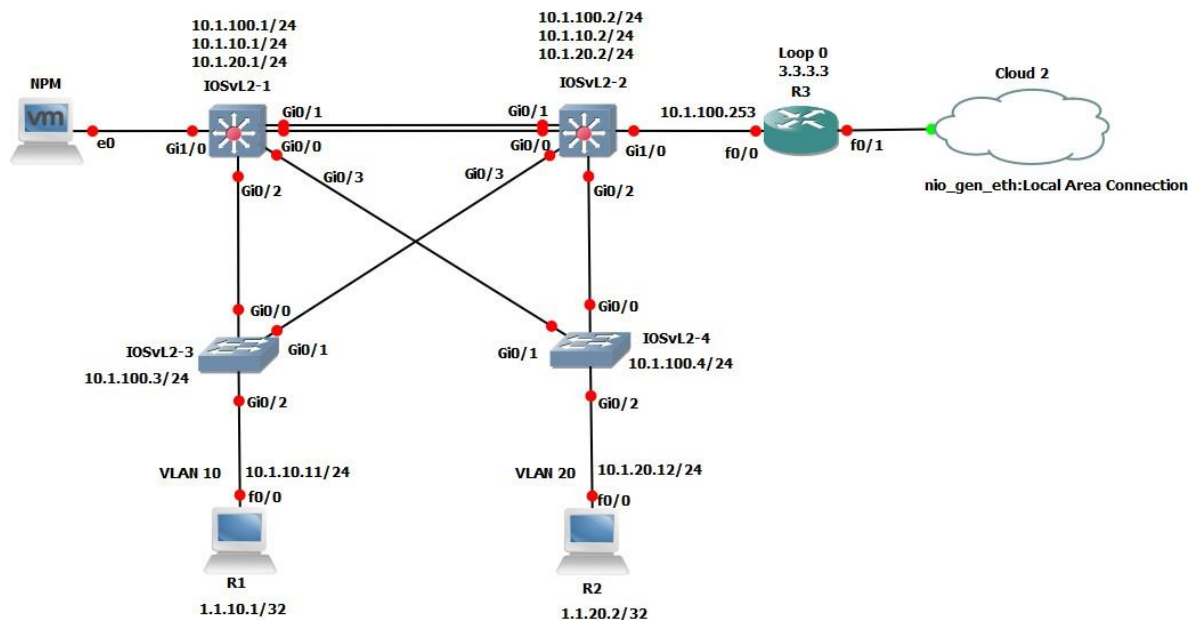


Figure 35 Example of simulation in GNS3

## **Disadvantages**

- 1- Resource Intensive: GNS3 can be demanding on computer resources (CPU, RAM), especially when running complex network simulations with multiple devices and virtual machines. This can require a powerful computer to run smoothly.
- 2- Learning Curve: Due to its advanced capabilities and flexibility, GNS3 has a steeper learning curve compared to simpler network simulation tools like Packet Tracer. Users may need to invest time in learning the interface, configurations, and troubleshooting techniques.
- 3-Complex Setup: Setting up GNS3 initially can be complex, particularly configuring the integration with virtualization software and ensuring compatibility with network operating systems. This complexity may deter some users who prefer simpler tools
- 4- Legal Considerations: Users must have legal access to the network operating systems (such as Cisco IOS) they intend to use with GNS3. Obtaining these images legally can sometimes be challenging or require additional purchases.
- 5- Limited Physical Hardware Interaction: While GNS3 excels in virtual simulations, it does not provide direct interaction with physical network hardware. This limitation may be significant for certain types of testing and configurations that require physical device interactions.

## Chapter 5(part 2)

# Types of Attacks that Can Occur on the Network

### ❖ Introduction

In the modern digital age, network security is of paramount importance. Networks are the backbone of information technology, connecting various devices and facilitating communication. However, this connectivity also exposes networks to a myriad of attacks. This chapter delves into the various types of attacks that can occur on a network, providing detailed explanations of each attack, their mechanisms, and methods to secure a network against these threats. Additionally, strategies to mitigate and respond to attacks, should they occur, are discussed comprehensively.

# Types of Network Attacks

## Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

### ➤ Explanation

A Denial of Service (DoS) attack aims to make a network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. In a Distributed Denial of Service (DDoS) attack, the incoming traffic flooding the target originates from many different sources, making it impossible to stop the attack simply by blocking a single source.

### ➤ Mechanism

DoS: The attacker uses one computer and one Internet connection to flood the targeted resource.

DDoS: The attacker uses multiple computers and Internet connections, often distributed globally in what's known as a botnet.

### ➤ Securing Your Network

Prevention: Use firewalls and intrusion detection/prevention systems (IDS/IPS). Implement rate limiting and ensure proper network redundancy.

Mitigation: Deploy anti-DDoS services, such as those provided by cloud service providers, which can absorb the malicious traffic.

### ➤ Response

During an Attack: Identify the attack early, re-route traffic, and engage with your ISP or cloud provider to filter traffic.

Post-Attack: Analyze logs to understand the attack vectors and improve defenses.

## **Man-in-the-Middle (MitM) Attacks**

### ➤ Explanation

A MitM attack occurs when an attacker secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other.

### ➤ Mechanism

The attacker inserts themselves into a conversation between two parties, either by eavesdropping or by impersonating both parties to gain access to their data.

### ➤ Securing Your Network

Prevention: Use strong encryption protocols (like SSL/TLS) for all communications. Implement mutual authentication and use secure Wi-Fi connections.

Detection: Monitor for unusual network activity and inspect SSL certificates for anomalies.

### ➤ Response

During an Attack: Terminate the session immediately and switch to a secure communication channel.

Post-Attack: Conduct a thorough security audit to identify and fix vulnerabilities that allowed the MitM attack.

# Phishing and Spear Phishing

## ➤ Explanation

Phishing involves fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity in electronic communication. Spear phishing is a more targeted version, aimed at specific individuals or organizations.

## ➤ Mechanism

Attackers send emails or messages that appear to be from legitimate sources, tricking recipients into revealing personal information such as passwords or credit card numbers.

## ➤ Securing Your Network

Prevention: Educate users about phishing tactics. Use email filtering solutions and multi-factor authentication (MFA).

- Detection: Implement anti-phishing software that can detect and block suspicious emails.

## ➤ Response

During an Attack: Quarantine the phishing emails and alert users.

Post-Attack: Change compromised credentials immediately and conduct a security review to prevent future attacks.

# SQL Injection

## ➤ Explanation

SQL Injection is a code injection technique that exploits vulnerabilities in an application's software by inserting malicious SQL statements into an entry field for execution.

## ➤ Mechanism

Attackers manipulate a web application's query parameters to execute arbitrary SQL code, which can result in unauthorized access to database information.

## ➤ Securing Your Network

Prevention: Use parameterized queries and prepared statements. Regularly update and patch your database management systems.

Detection: Implement web application firewalls (WAFs) and use continuous security monitoring.

## ➤ Response

During an Attack: Block the malicious IP address and correct the vulnerable code.

Post-Attack: Review database access controls and audit logs for unauthorized access.

## Cross-Site Scripting (XSS)

### ➤ Explanation

XSS attacks occur when an attacker injects malicious scripts into content from otherwise trusted websites. The malicious code then runs in the context of the user's browser.

### ➤ Mechanism

Attackers exploit vulnerabilities in web applications to send malicious scripts to other users. These scripts can hijack user sessions, deface websites, or redirect users to malicious sites.

### ➤ Securing Your Network

Prevention: Implement proper input validation and output encoding. Use Content Security Policy (CSP) to restrict sources of executable scripts.

Detection: Conduct regular security testing, including penetration testing and code reviews.

### ➤ Response

During an Attack: Immediately sanitize inputs and outputs to prevent script execution.

Post-Attack: Analyze the root cause and patch the vulnerability. Educate developers on secure coding practices.

## Malware Attacks

➤ Explanation

Malware, or malicious software, encompasses a variety of harmful software including viruses, worms, and Trojans, which can infiltrate and damage systems.

➤ Viruses

Viruses attach themselves to legitimate programs and spread by infecting other programs and files on the system.

➤ Worms

Worms are standalone malware that replicate themselves to spread to other computers without needing to attach to another program.

➤ Trojans

Trojans disguise themselves as legitimate software but perform malicious activities once installed, such as stealing data or providing remote access to the attacker.

➤ Securing Your Network

Prevention: Use comprehensive antivirus and anti-malware solutions. Keep systems and software updated with the latest security patches.

Detection: Employ behavior-based detection systems and regularly scan systems for malware.

➤ Response

During an Attack: Isolate the infected systems and remove the malware using appropriate tools.

Post-Attack: Restore systems from clean backups and review security policies to prevent future infections.

#### Explanation

Malware, or malicious software, encompasses a variety of harmful software including viruses, worms, and Trojans, which can infiltrate and damage systems.

## Insider Threats

#### ➤ Explanation

Insider threats involve malicious activities conducted by individuals within the organization, such as employees, contractors, or partners.

#### ➤ Mechanism

Insiders may misuse their access to steal sensitive data, disrupt operations, or facilitate external attacks.

# Zero-Day Exploits

## ➤ Explanation

Zero-day exploits take advantage of unknown vulnerabilities in software or hardware, which the vendor has not yet patched.

## ➤ Mechanism

Attackers identify and exploit vulnerabilities before developers can create fixes, leading to potentially severe damage.

## ➤ Securing Your Network

**Prevention:** Use threat intelligence services to stay informed about new vulnerabilities. Apply security patches promptly and use virtual patching solutions.

**Detection:** Deploy advanced threat detection tools and monitor for unusual network activity.

## ➤ Response

**During an Attack:** Isolate the affected systems and apply any available mitigations. Work with vendors to develop and deploy patches.

**Post-Attack:** Update all affected systems and review security practices to enhance resilience against future zero-day exploits.

# Securing Your Network

## *Best Practices*

1. Regularly Update and Patch Systems: Ensure that all software and hardware are up to date with the latest security patches.
2. Use Strong Authentication Methods: Implement multi-factor authentication (MFA) to add an extra layer of security.
3. Educate and Train Employees: Conduct regular training sessions to keep employees informed about the latest security threats and safe practices.
4. Implement Network Segmentation: Divide the network into segments to limit the spread of attacks.
5. Utilize Firewalls and IDS/IPS: Deploy firewalls and intrusion detection/prevention systems to monitor and protect the network.
6. Regular Backups: Perform regular backups of critical data and store them offline to protect against ransomware.

## Tools and Technologies

1. Firewalls: Control incoming and outgoing network traffic based on security rules.
2. Antivirus and Anti-Malware Software: Detect and remove malicious software.
3. Encryption Tools: Protect data in transit and at rest by encrypting sensitive information.
4. Security Information and Event Management (SIEM) Systems: Aggregate and analyze security data to detect and respond to threats.
5. Network Access Control (NAC): Enforce policies for device access to the network.

6. Virtual Private Network (VPN): Provide secure remote access to the network.

## Mitigation and Response Strategies

### *Incident Response Plan*

An incident response plan outlines the steps to be taken during and after a security breach. Key components include:

1. Preparation: Establish an incident response team and define roles and responsibilities.
2. Identification: Detect and confirm the occurrence of an incident.
3. Containment: Limit the scope and impact of the incident.
4. Eradication: Remove the cause of the incident.
5. Recovery: Restore affected systems and services to normal operation.
6. Lessons Learned: Analyze the incident to improve future response efforts.

## Real-Time Monitoring

Continuous monitoring of network activity can help detect and respond to threats in real-time. Tools and techniques include:

1. Intrusion Detection Systems (IDS): Monitor network traffic for suspicious activity.
2. Security Information and Event Management (SIEM): Centralize and analyze security data.
3. Endpoint Detection and Response (EDR): Monitor and protect endpoints against threats.
4. Network Traffic Analysis (NTA): Analyze network traffic patterns to identify anomalies.

## Legal and Ethical Considerations

Understanding the legal and ethical implications of network security is crucial. Key aspects include:

1. Compliance: Adhere to relevant laws and regulations (e.g., GDPR, HIPAA).
2. Privacy: Protect user data and ensure privacy policies are followed.
3. Ethical Hacking: Use ethical hacking techniques to test and improve security without causing harm.

## Case Studies

### **Case Study 1: DDoS Attack on Dyn (2016)**

In 2016, a massive DDoS attack targeted Dyn, a major DNS provider, disrupting access to many popular websites. This attack leveraged a botnet of IoT devices infected with the Mirai malware. The incident highlighted the importance of securing IoT devices and implementing robust DDoS mitigation strategies.

### **Case Study 2: Equifax Data Breach (2017)**

The Equifax data breach exposed the personal information of 147 million people. The breach was caused by a failure to patch a known vulnerability in the company's web application. This case underscores the critical need for timely patching and regular vulnerability assessments.

### **Case Study 3: WannaCry Ransomware Attack (2017)**

WannaCry ransomware exploited a vulnerability in Windows systems, encrypting data and demanding ransom payments. The attack spread rapidly, affecting organizations worldwide. It emphasized the necessity of regular backups and maintaining up-to-date systems.

## Conclusion

Network security is a complex and ever-evolving field. Understanding the various types of attacks and their mechanisms is crucial for defending against them. By implementing best

practices, leveraging appropriate tools, and preparing robust response strategies, organizations can significantly enhance their security posture and mitigate the impact of potential attacks.

This chapter provides a comprehensive overview of network attacks, prevention strategies, and response techniques. It is essential for network administrators, security professionals, and anyone involved in safeguarding digital infrastructure to stay informed and proactive in the face of ever-present cyber threats

# Mechanisms of Each Attack

## Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

### ➤ DoS Attack Mechanism

In a DoS attack, the attacker targets a specific server or network resource with the intention of overwhelming it with a flood of illegitimate requests. This can be achieved through several techniques, such as:

- ICMP Flood: Sending a high volume of ICMP (ping) requests to exhaust the target's resources.
- SYN Flood: Exploiting the TCP handshake process by sending numerous SYN requests without completing the handshake, leading to resource exhaustion.
- HTTP Flood: Sending multiple HTTP requests to a web server to overwhelm its ability to respond to legitimate traffic.

### ➤ DDoS Attack Mechanism

A DDoS attack involves multiple compromised devices, often part of a botnet, which are controlled by the attacker to target a specific resource. Common types of DDoS attacks include:

- Volume-Based Attacks: Overwhelm the target with massive amounts of traffic, measured in bits

(measured in packets per second) by exploiting weaknesses in network protocols, such as SYN floods or Ping of Death.

- Application Layer Attacks: Target specific applications or services with the intent of causing a denial of service, such as HTTP floods.

## **Man-in-the-Middle (MitM) Attacks**

### **MitM Attack Mechanism**

In a MitM attack, the attacker intercepts the communication between two parties. The primary methods include:

- Packet Sniffing: Capturing and analyzing packets traveling through a network.
- Session Hijacking: Taking control of a legitimate session between two parties.
- SSL Stripping: Downgrading HTTPS connections to HTTP to intercept unencrypted data.
- Wi-Fi Eavesdropping: Setting up a rogue Wi-Fi access point to intercept data transmitted by connected devices.

## **Phishing and Spear Phishing**

### **Phishing Attack Mechanism**

Phishing involves sending fraudulent emails or messages that appear to come from reputable sources to trick recipients into revealing sensitive information. Techniques include:

- Deceptive Phishing: Using fake websites or forms to collect user credentials.

- Smishing: Sending malicious links or requests via SMS.
- Vishing: Using voice calls to trick individuals into revealing personal information.

➤ Spear Phishing Attack Mechanism

Spear phishing targets specific individuals or organizations with personalized messages, often using information gathered from social media or other sources to increase credibility.

# SQL Injection

## *SQL Injection Attack Mechanism*

SQL injection attacks involve inserting malicious SQL queries into input fields of web applications, exploiting vulnerabilities in the application's software. Techniques include:

- Classic SQL Injection: Directly injecting SQL commands through input fields.
- Blind SQL Injection: Exploiting the database through injected queries, even when the error messages are not displayed.
- Out-of-Band SQL Injection: Using alternate channels to retrieve data from the database, often through DNS or HTTP requests.

# Cross-Site Scripting (XSS)

## *XSS Attack Mechanism*

XSS attacks occur when attackers inject malicious scripts into web pages viewed by other users. The primary types of XSS attacks are:

- Stored XSS: Malicious scripts are permanently stored on the target server, such as in a database or forum post.
- Reflected XSS: Malicious scripts are reflected off a web server and delivered to a user's browser via a malicious link.
- DOM-Based XSS: Exploits vulnerabilities in the client-side JavaScript code rather than the server-side code.

# Zero-Day Exploits

## *Zero-Day Exploit Mechanism*

Zero-day exploits target vulnerabilities that are unknown to the software vendor. Attackers use these exploits to gain unauthorized access or cause harm before the vendor can release a patch.

<b>Attack Type</b>	<b>Response</b>	<b>Prevention</b>	<b>Detection</b>	<b>Response</b>
<b>DoS/DDoS</b>	Flooding network resources	Firewalls, IDS/IPS, rate limiting	Monitoring for unusual traffic patterns	Reroute traffic, engage ISP/cloud provider, analyze logs
<b>MitM</b>	Intercepting/altering communications	SSL/TLS, mutual authentication	Inspect SSL certificates, unusual activity	Terminate session, switch to secure channel
<b>Phishing/Spear Phishing</b>	Fraudulent communication to obtain sensitive info	User education, email filtering, MFA	Anti-phishing software	Quarantine emails, change credentials, security review
<b>Malware (Viruses, Worms, Trojans)</b>	Infiltrating and damaging systems	Antivirus/anti-malware, patch updates	Behavior-based detection, regular scans	Isolate system, remove malware, restore from backups
<b>Ransomware</b>	Encrypting files and demanding ransom	Data backups, endpoint protection	IDS, monitor file activity	Disconnect systems, do not pay ransom, restore backups
<b>Insider Threats</b>	Malicious activities by insiders	Access controls, background checks	User activity monitoring, anomaly detection	Revoke access, investigate, security audit
<b>Zero-Day Exploits</b>	Exploiting unknown vulnerabilities	Threat intelligence, virtual patching	Advanced threat detection	Isolate system, apply virtual patch, permanent fix

*Table 7 compare between Response, Prevention, Detection, Response*

# Chapter 6

## Primary Domain Controller (PDC):

The PDC is a critical component within a Windows-based network that serves as the central point for managing user accounts and security. In a Windows domain, the PDC plays a pivotal role in ensuring that the network operates smoothly and securely.

In the early days of Windows NT, the concept of PDC and BDC was crucial for network management. However, with the advent of Windows 2000 and Active Directory, the role of the PDC evolved. Active Directory introduced a multi-master replication model, where all domain controllers are peers. Despite this evolution, the term PDC is still used to refer to the primary domain controller in certain contexts, particularly in mixed environments where older systems are still in use.

### key functions for PDC:

#### **1. Centralized Authentication and Security:**

The PDC is responsible for authenticating users when they log into the network. It stores user account information, such as usernames and passwords, and ensures that only authorized individuals can access the network's resources. By centralizing this authentication process, the PDC helps maintain a high level of security across the network.

#### **2. User and Group Management:**

Managing user accounts and groups is a core function of the PDC. Network administrators can create, modify, and delete user accounts, assign users to groups, and set permissions for accessing various resources. This centralized management makes it easier to enforce security policies and ensure that users have appropriate access to the tools and data they need.

### **3. Replication and Redundancy:**

In larger networks, there may be additional domain controllers, often referred to as Backup Domain Controllers (BDCs). These BDCs replicate the data from the PDC to ensure redundancy and high availability. If the PDC were to fail, a BDC can take over, minimizing downtime and maintaining network functionality.

## **What is the Server Manger?**

The Server Manager is a powerful utility provided by Microsoft within its Windows Server operating systems. It serves as the central hub for managing servers, including the Primary Domain Controller, and offers a comprehensive suite of tools and functionalities that simplify the complex task of server administration.

### **key functions for Server Manger :**

#### **1. Centralized Management Console:**

The Server Manager provides a single, unified interface for managing multiple servers within a network. For administrators of a PDC, this means having the ability to oversee and control not just the PDC itself, but also other domain controllers and member servers from one central location. This centralization enhances efficiency and simplifies the administrative workload.

## **2. Centralized Management Console:**

One of the primary functions of the Server Manager is to install, configure, and manage server roles and features. For a PDC, critical roles such as Active Directory Domain Services (AD DS) can be managed seamlessly. Administrators can add or remove roles, configure settings, and ensure that the PDC is functioning optimally to support the network's needs.

## **3. Monitoring and Performance Management:**

The Server Manager supports remote management, allowing administrators to configure and manage the PDC and other servers from remote locations. This capability is particularly valuable in distributed or large-scale environments where physical access to servers may be limited.

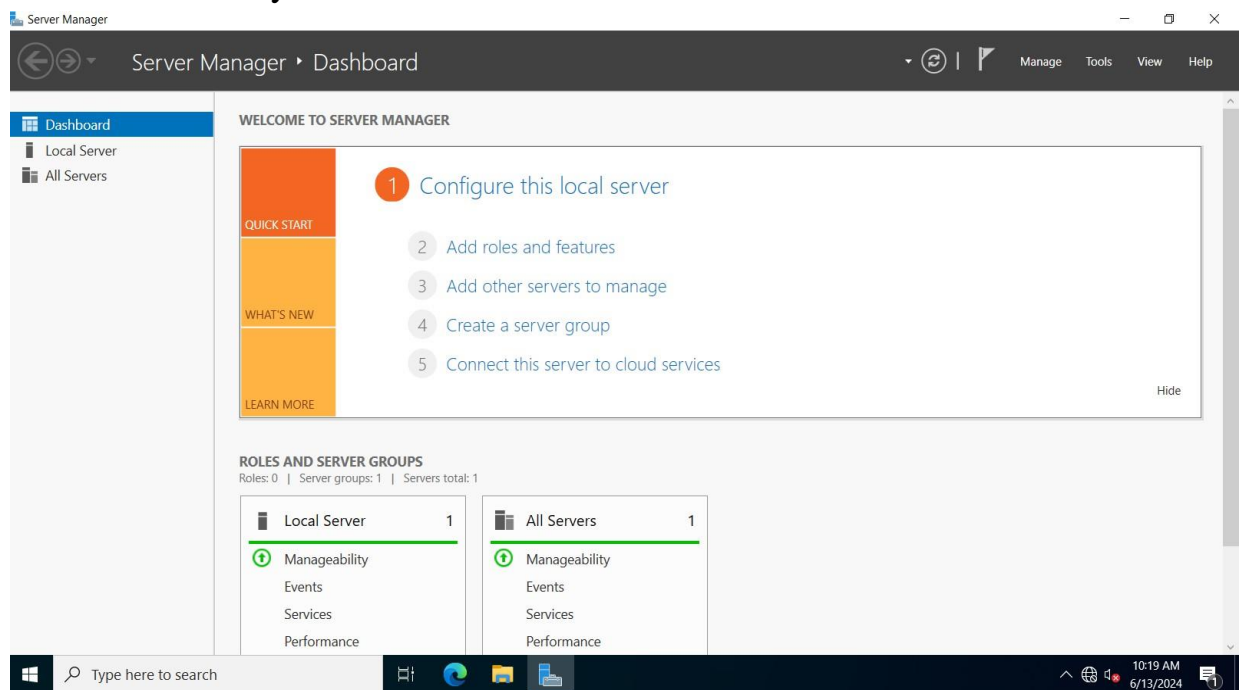
## **4. Configuration and Maintenance Tasks:**

Through the Server Manager, administrators can perform a variety of maintenance tasks such as patch management, system updates, and backup configurations. These tasks are crucial for maintaining the security and stability of the PDC and the overall network.

## the Interface of Server Manager in a Primary Domain Controller (PDC):

- **Dashboard:**

When you first open Server Manager, you are greeted by the Dashboard. This section provides a high-level overview of the server environment, including a summary of the server roles and features installed. It also displays alerts and notifications about the health and performance of the servers, helping administrators quickly identify and address any issues.

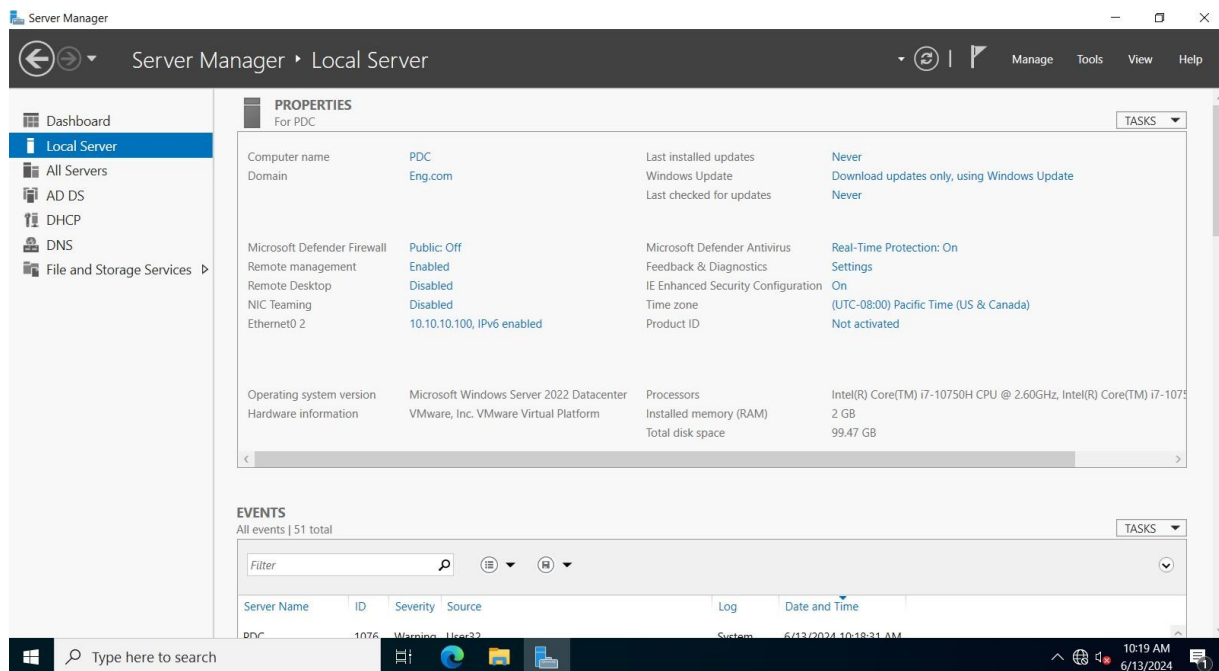


*Figure 36 Dashboard*

At the top of the Dashboard, there is a notifications area that alerts administrators to important events, warnings, and errors. This real-time feedback allows you to promptly address any issues that may arise, ensuring the continuous smooth operation of your servers.

## Local Server:

The Local Server tab focuses on the server where the Server Manager is running. Here, you can view and configure various settings such as computer name, domain membership, network settings, Windows Firewall status, and updates. This tab provides a centralized view of the local server's configuration and status.



*Figure 37 Local Server*

## Events Section:

The Events section within the Local Server tab aggregates and displays significant system events and alerts that are crucial for maintaining the server's health.

### key function:

- **Event Aggregation:**

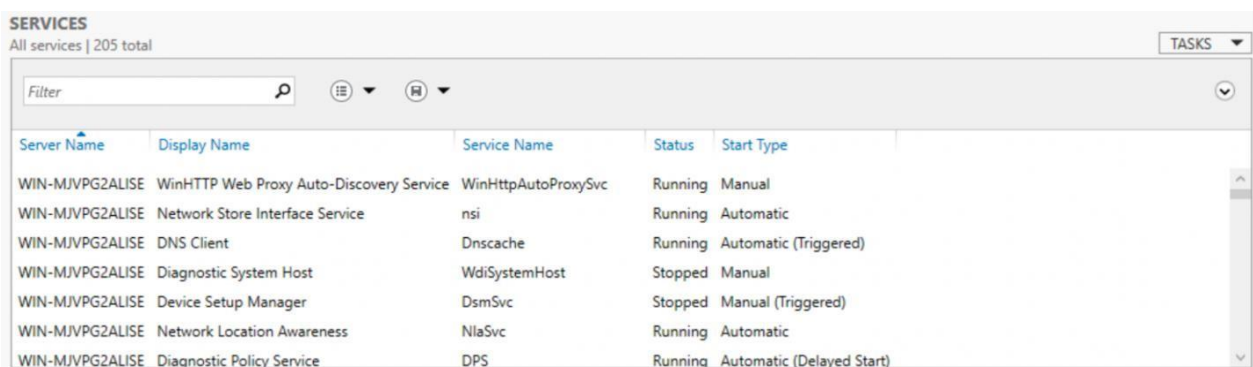
The Events section within the Local Server tab aggregates and displays significant system events and alerts that are crucial for

maintaining the server's health. Here's a detailed look at what this section entails **Events are typically categorized into three main types:**

- **Errors:** Indicate serious issues that require immediate attention, such as application crashes, hardware failures, or critical system errors.
- **Warnings:** Highlight potential problems that may not be immediately critical but could lead to issues if not addressed, such as low disk space or high CPU usage.
- **Informational Messages:** Provide information about normal operations, such as successful service starts or user logins.

## Event Details:

- Event ID: A unique identifier for the event type.
- Source: The application, service, or component that generated the event.
- Severity Level: Indicates whether the event is an error, warning, or informational message.
- Date and Time: When the event occurred.
- Description: A brief summary of the event.



The screenshot shows the Windows Services console window titled 'SERVICES' with a subtitle 'All services | 205 total'. It features a search bar and a 'Filter' button. Below is a table of services with columns for Server Name, Display Name, Service Name, Status, and Start Type.

Server Name	Display Name	Service Name	Status	Start Type
WIN-MJVPG2ALISE	WinHTTP Web Proxy Auto-Discovery Service	WinHttpAutoProxySvc	Running	Manual
WIN-MJVPG2ALISE	Network Store Interface Service	nsi	Running	Automatic
WIN-MJVPG2ALISE	DNS Client	Dnscache	Running	Automatic (Triggered)
WIN-MJVPG2ALISE	Diagnostic System Host	WdiSystemHost	Stopped	Manual
WIN-MJVPG2ALISE	Device Setup Manager	DsmSvc	Stopped	Manual (Triggered)
WIN-MJVPG2ALISE	Network Location Awareness	NlaSvc	Running	Automatic
WIN-MJVPG2ALISE	Diagnostic Policy Service	DPS	Running	Automatic (Delayed Start)

Figure 38

## Installing service in PDC:

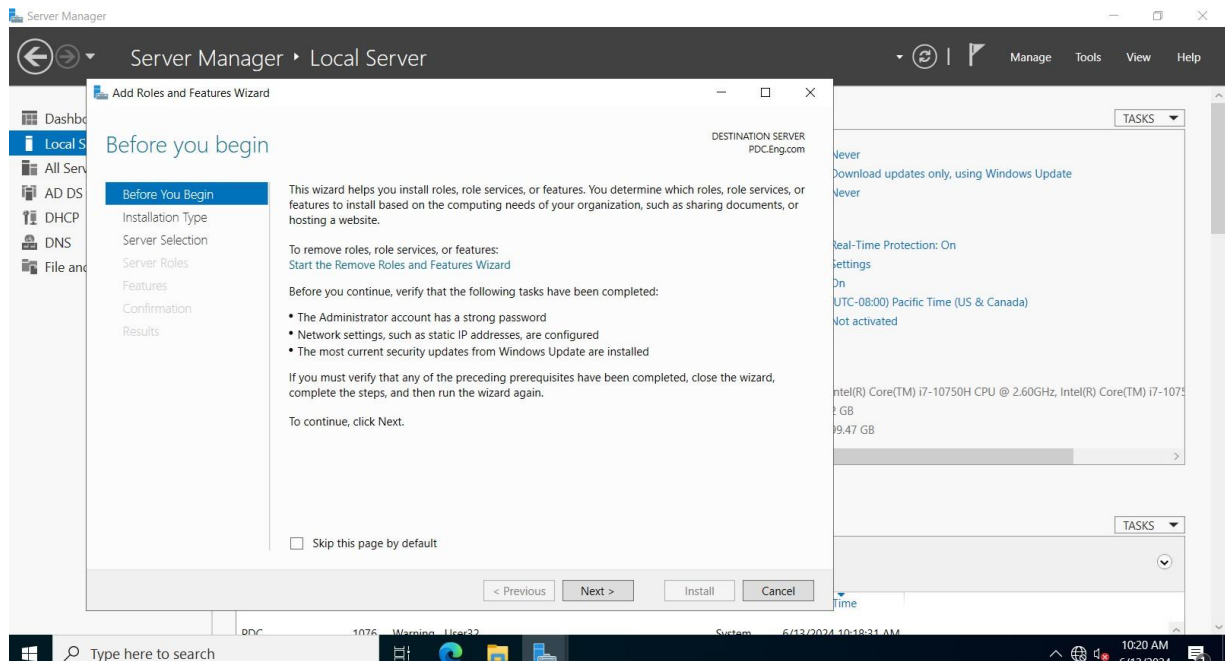
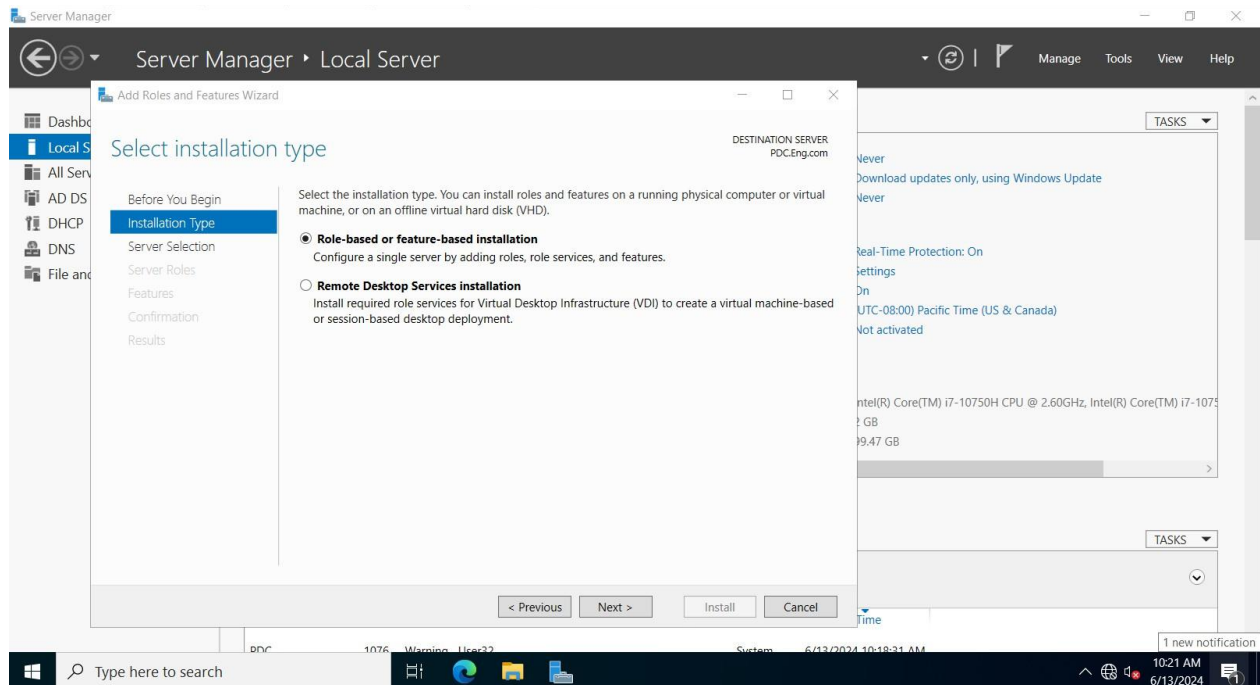


Figure 39 Installing service in PDC



*Figure 40 Installing service in PDC*

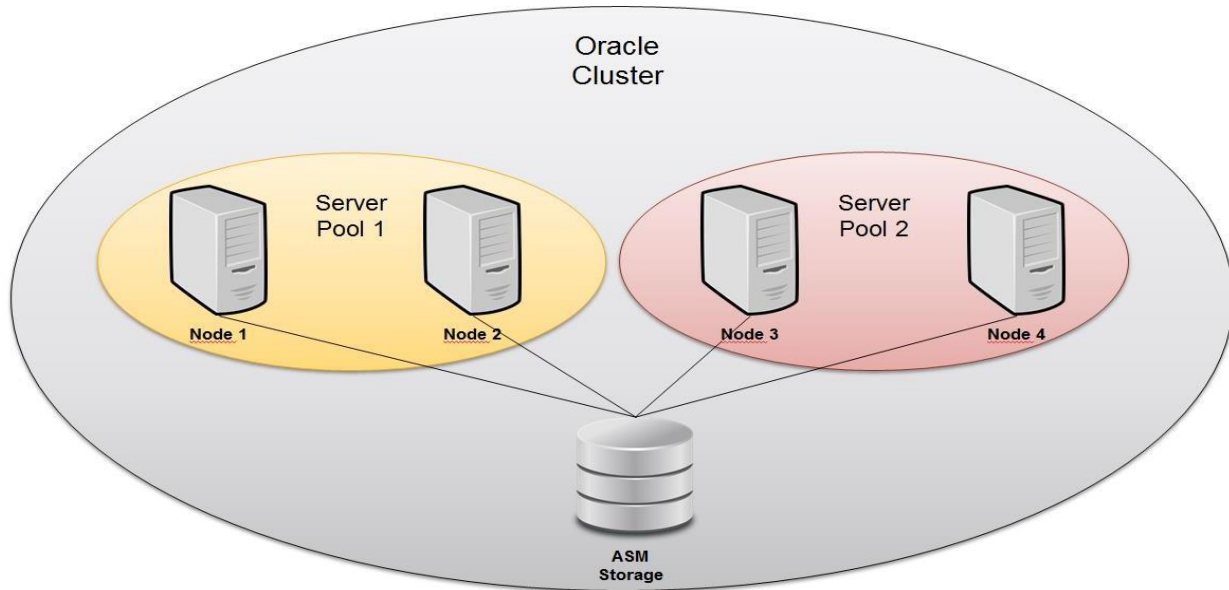
## Server pool:

server pool in the context of a local server refers to a collection of servers that are grouped together to provide high availability, load balancing, and redundancy for applications and services

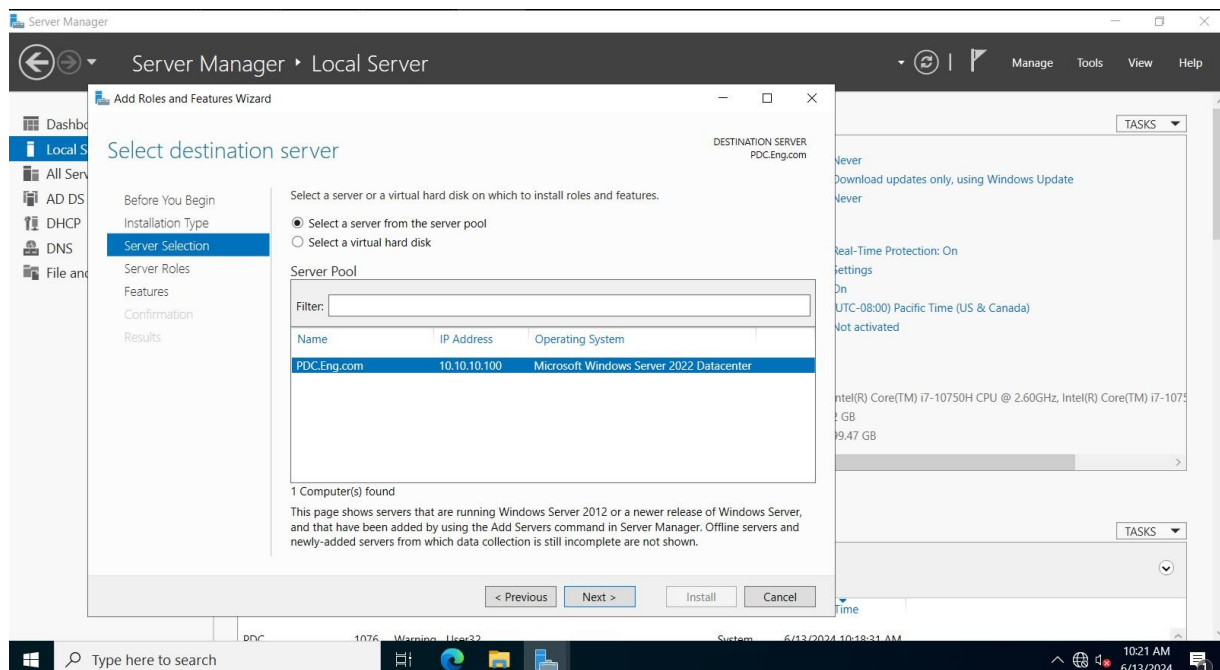
A device or software that distributes incoming network traffic across multiple servers in the server pool. This ensures no single server becomes overwhelmed with too much traffic, improving performance and reliability.

In a server pool, servers may share resources such as storage, databases, or application states to provide a seamless experience for users.

Multiple servers in the pool provide redundancy, so if one server fails, others can take over its load, ensuring continuous service availability.

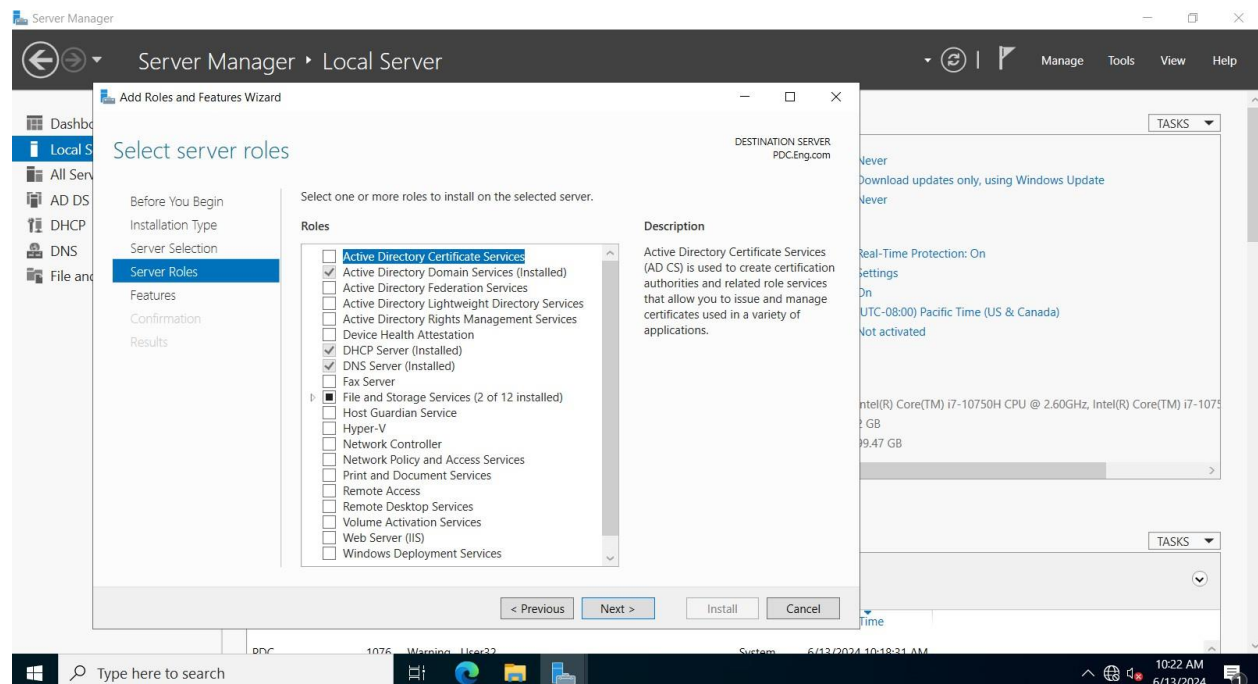


*Figure 41 oracle cluster*



*Figure 42 local server*

## Choose the service you want to install:



*Figure 43 service install*

## Active Directory Domain Services (AD DS) server:

Also called Active Directory domain controller. it is responsible for handling various functions related to identity and access management within a domain.

## Key Functions of an Active Directory Domain Services Server:

### Authentication and Authorization:

User Authentication: Verifies the identity of users trying to access the network.

Authorization: Determines what resources users can access based on their permissions.

## **Directory Services:**

User and Computer Accounts: Manages information about users, computers, and other devices on the network.

Group Policies: Allows administrators to set policies and configurations for users and computers.

Organizational Units (OUs): Helps in organizing and managing objects within the directory.

## **Replication:**

Data Synchronization: Ensures that information is consistent across multiple domain controllers within the same domain or across different domains in a forest.

## **Security:**

Single Sign-On (SSO): Enables users to access multiple resources with one set of login credentials.

Kerberos Authentication: Uses the Kerberos protocol for secure authentication.

## **Scalability and Management:**

Domain Trusts: Allows users from different domains to access resources across the domains if trust relationships are established.

Schema: Defines the types of objects and information that can be stored in the directory.

## Components of Active Directory:

1. **Domain:** The core unit of logical structure in AD. A domain can contain users, groups, computers, and other resources.
2. **Tree:** A collection of one or more domains that share a common namespace.
3. **Forest:** The top-level container in an Active Directory configuration, which can contain multiple trees. All domains in a forest share a common schema and global catalog.
4. **Global Catalog:** A distributed data repository that contains information about every object in the directory.

## How an Active Directory Domain Services Server Works:

1. **Installation:** The AD DS role is installed on a Windows Server operating system, converting it into a domain controller.
2. **Domain Controller Promotion:** After installing the AD DS role, the server is promoted to a domain controller, setting up the necessary directory services, DNS, and other components.
3. **User and Group Management:** Administrators create and manage user accounts, groups, and organizational units using tools like Active Directory Users and Computers (ADUC).
4. **Group Policy Management:** Administrators configure and apply group policies to enforce security settings, software installation, and other administrative tasks across the domain.
5. **PowerShell:** Command-line and scripting language that provides extensive capabilities for managing and automating Active Directory tasks.

## Example Scenarios:

**User Login** When a user logs into a computer joined to the domain, the domain controller authenticates the user's credentials and applies any relevant policies.

**Resource Access** When accessing network resources like shared folders or printers, the domain controller checks the user's permissions and grants or denies access accordingly.

**Policy Enforcement** Group policies configured on the domain controller are applied to users and computers to enforce security settings, software deployments, and more.

## Service installed in PDC:

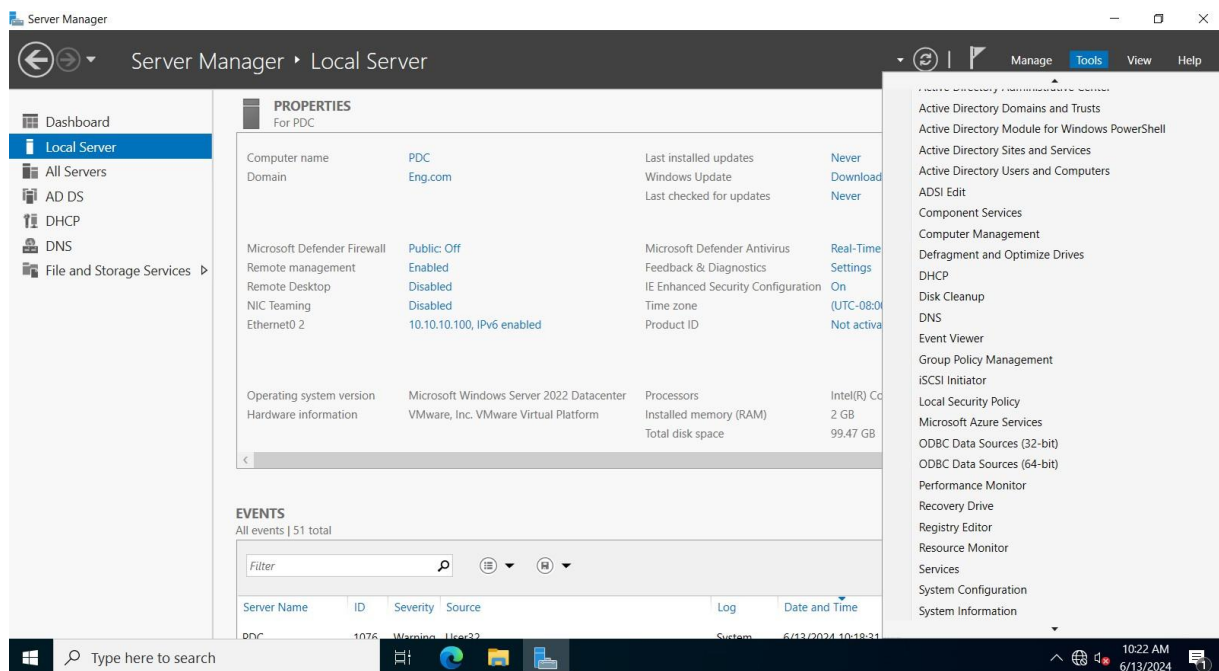


Figure 44 Service installed in PDC

## DHCP:

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring devices on IP networks. It enables devices (clients) to receive IP addresses and other necessary network configuration details (such as the default gateway and DNS server addresses) automatically from a DHCP server.

### Key Components of DHCP:

1. **DHCP Server:** The server that holds a pool of IP addresses and configuration information. It assigns IP addresses to clients and provides other network configuration settings.
2. **DHCP Client:** Any device (such as a computer, smartphone, or printer) that connects to the network and requests an IP address from the DHCP server.
3. **DHCP Lease:** The duration of time for which an IP address is assigned to a DHCP client. Leases can be renewed to keep the same IP address or can expire, making the IP address available for other devices.
4. **Scope:** A range of IP addresses that the DHCP server can assign to clients on a particular subnet.

## **How DHCP Works:**

1. Discovery: The client broadcasts a DHCPDISCOVER message to find a DHCP server.
2. Offer: The DHCP server responds with a DHCPOFFER message, offering an IP address and other configuration settings to the client.
3. Request: The client replies with a DHCPREQUEST message, indicating acceptance of the offered IP address and requesting additional configuration parameters.
4. Acknowledge: The DHCP server sends a DHCPACK message, confirming that the IP address has been assigned and providing the client with the configuration details.

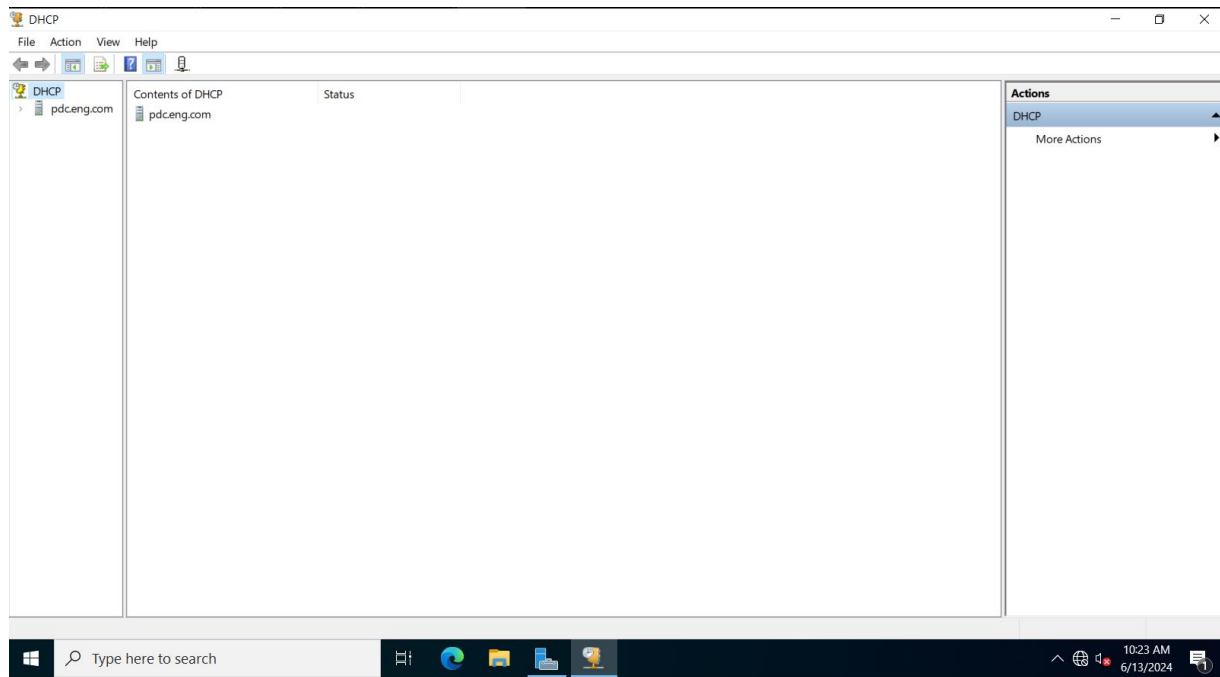
## **Advantages of DHCP:**

- Automation: Automatically assigns IP addresses and configuration settings, reducing the administrative burden.
- Flexibility: Easily accommodates new devices on the network without manual configuration.
- Consistency: Ensures that devices receive the correct network settings consistently.
- Efficiency: Frees up IP addresses when they are no longer in use, reducing the risk of address conflicts.

## DHCP can be implemented on various devices, including:

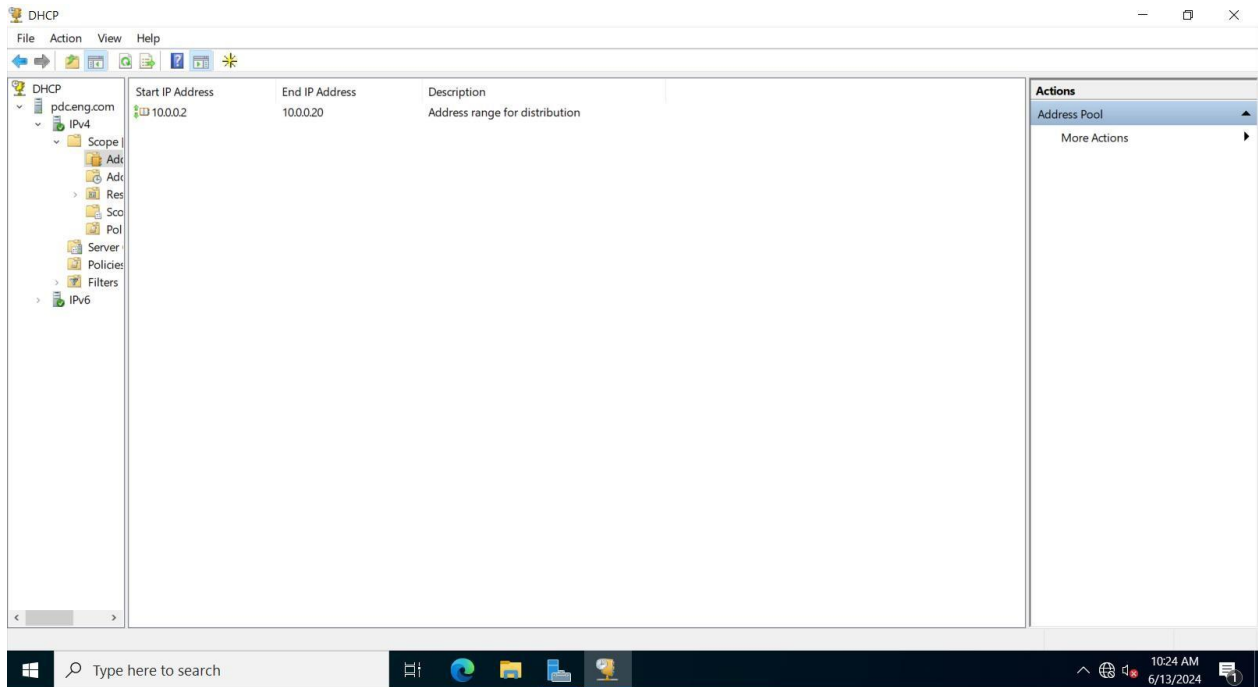
- Dedicated DHCP Servers: These are specialized servers set up to handle DHCP functions.
- Network Routers: Many home and small business routers include built-in DHCP server functionality.
- Windows Server: Windows Server operating systems have DHCP server roles that can be installed and configured.
- Linux/Unix Systems: DHCP can be set up using services like `isc-dhcp-server` on Linux-based systems.

## DHCP in PDC:



*Figure 45 DHCP*

## Pool IP in PDC:



*Figure 46 Pool IP*

## DNS (Domain Name System) server:

It is a crucial component of the internet's infrastructure. It translates human-readable domain names (like `www.example.com`) into IP addresses (like `192.0.2.1`) that computers use to communicate with each other. This process is essential because, while domain names are easy for people to remember, computers and network devices use IP addresses to locate and communicate with each other on the internet.

## Key Functions of a DNS Server

1. **Domain Name Resolution:** Converting domain names into IP addresses. When a user types a domain name into their browser, a DNS server resolves that name to the corresponding IP address.
2. **DNS Queries Handling:** Processing requests from clients (typically web browsers or other applications) and returning the appropriate IP addresses or other DNS records.
3. **Caching:** Storing previously queried DNS records for a certain period to speed up future requests for the same domain names.
4. **Zone Management:** Managing the DNS records for specific domains. This includes adding, removing, or updating records such as A (address), AAAA (IPv6 address), CNAME (canonical name), MX (mail exchange), and others.

## DNS Query Process:

1. Client Request: A user types a URL in their browser.
2. DNS Resolver: The client's device contacts a recursive DNS resolver.
3. Root Server: If the resolver does not have the cached IP address, it queries a root DNS server.
4. TLD Server: The root server responds with the address of a TLD DNS server (e.g., .com).
5. Authoritative Server: The TLD server responds with the address of the authoritative DNS server for the specific domain.

6. IP Address: The authoritative server provides the IP address of the requested domain back to the resolver, which then returns it to the client's device.

## **DNS Security:**

### **1. DNSSEC (Domain Name System Security Extensions):**

Adds security to DNS by enabling DNS responses to be verified for authenticity. It uses digital signatures to ensure that the responses have not been tampered with.

### **2. DNS over HTTPS (DoH) and DNS over TLS (DoT):**

Encrypt DNS queries and responses to enhance privacy and security by preventing eavesdropping and manipulation.

## **Example Scenario**

1. User Accesses a Website: A user enters "www.example.com" in their browser.
2. 2.DNS Resolver Query: The resolver first checks its cache. If the IP address is not cached, it starts querying the DNS hierarchy.
3. Root and TLD Servers: The resolver contacts a root server, which directs it to the .com TLD server. The TLD server then directs it to the authoritative DNS server for example.com.
4. Authoritative Response: The authoritative server for example.com returns the IP address associated with "www.example.com".

5. Accessing the Website: The resolver returns the IP address to the user's browser, which then connects to the web server at that IP address.

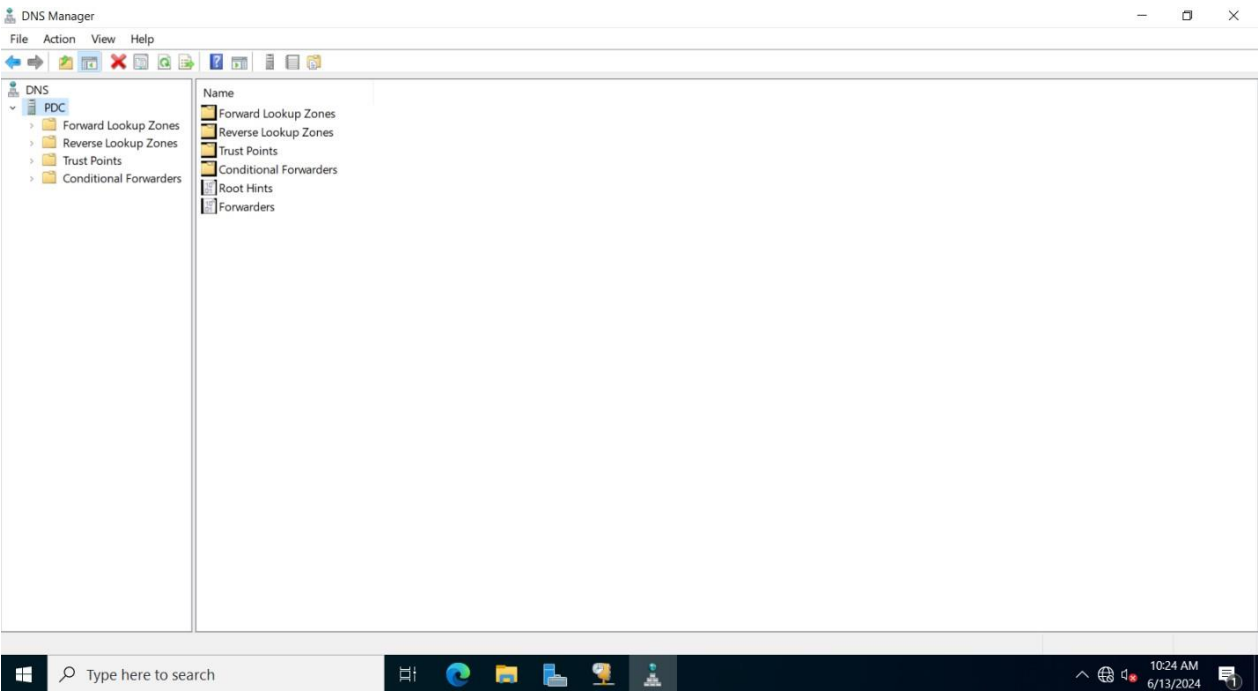


Figure 47 DNS Security

Show the server is forward zone to PDC:

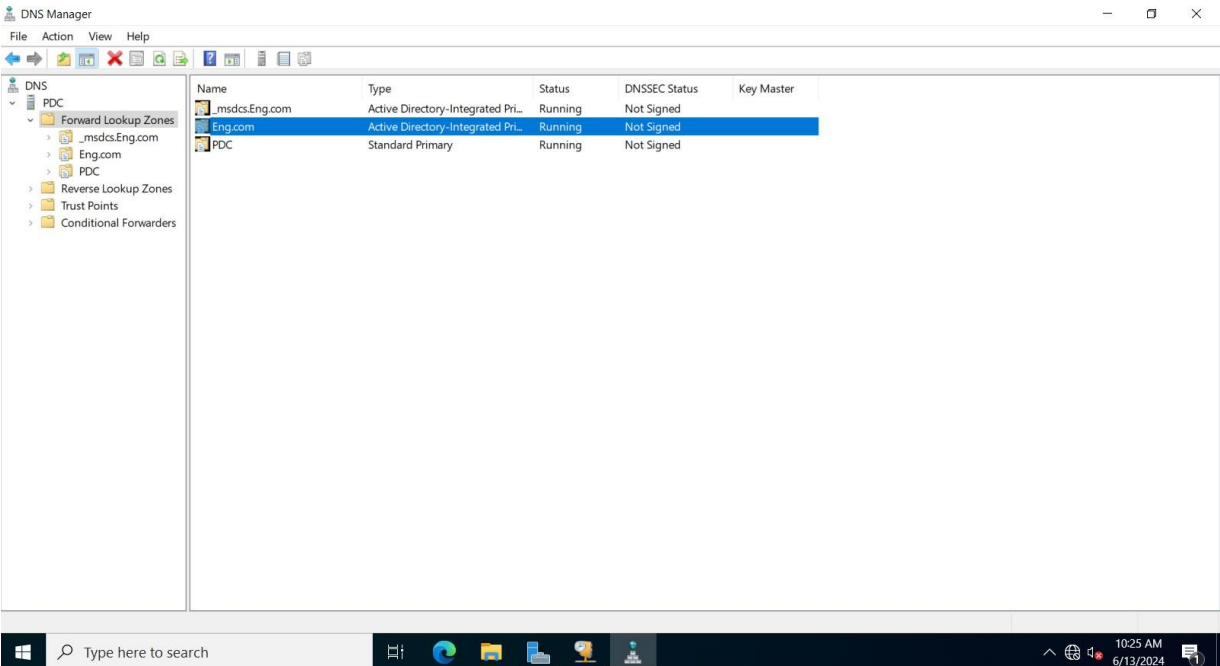
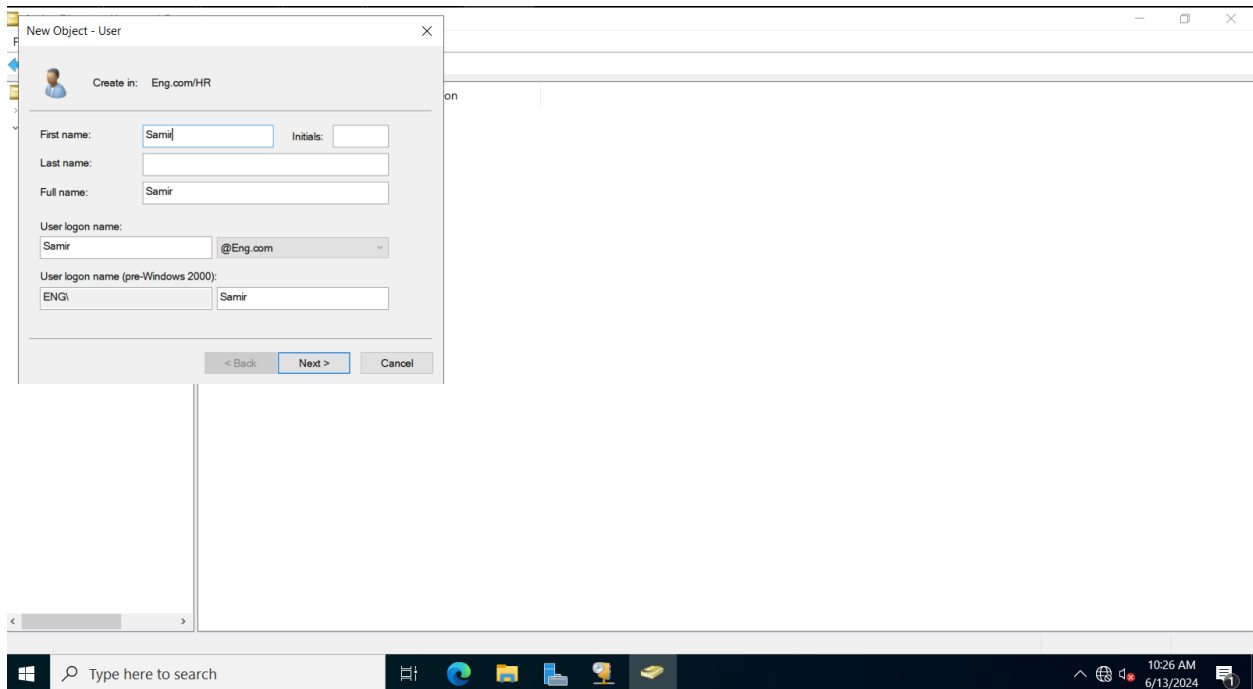


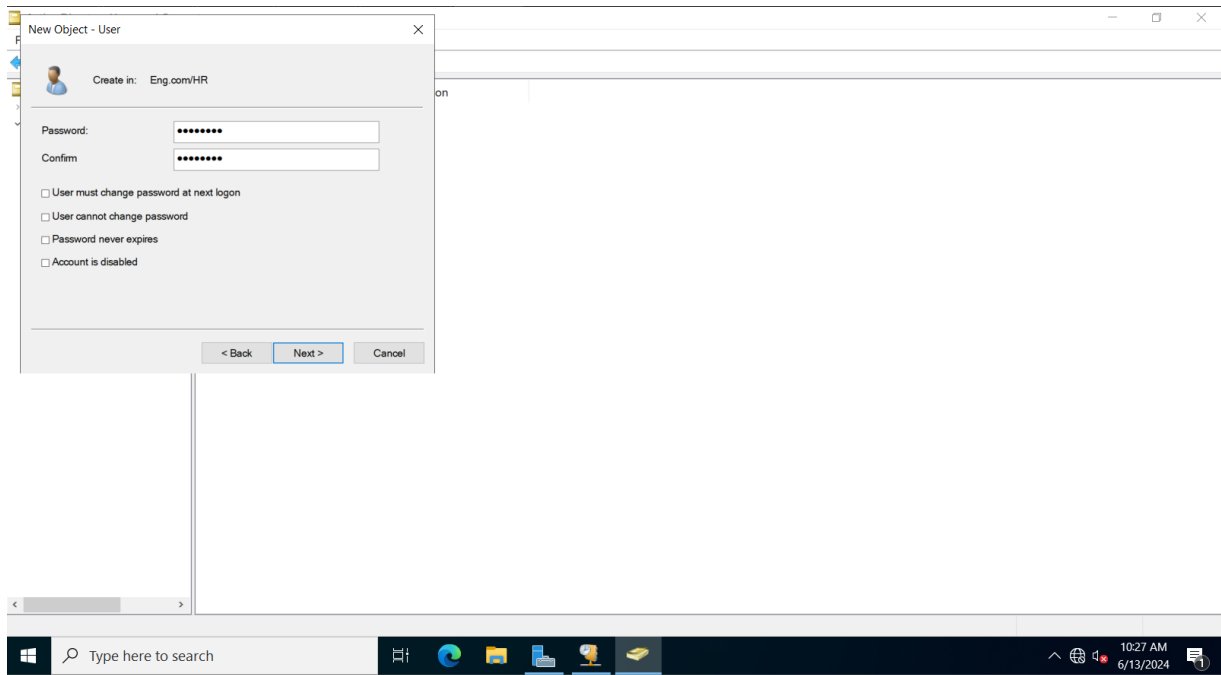
Figure 48 Show the server is forward zone to PDC

## ADD client to PDC:



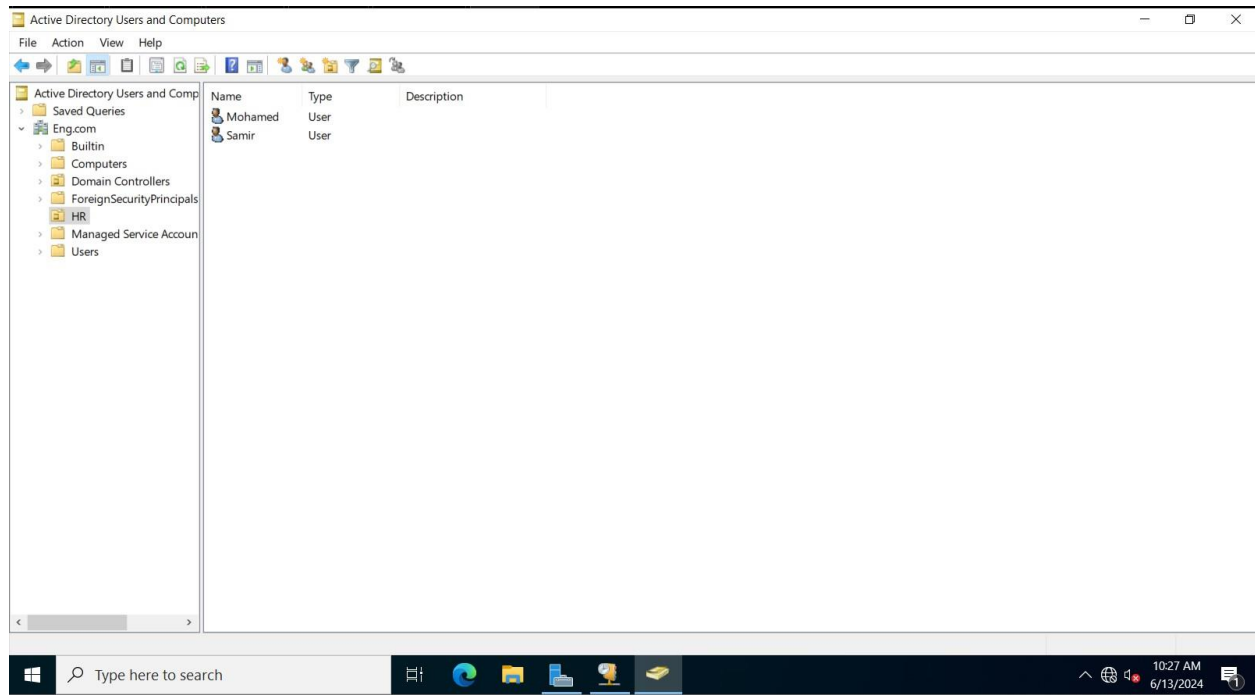
*Figure 49 ADD client to PDC*

## Create password for the client:



*Figure 50 Create password for the client*

## Client added to PDC:



*Figure 51 Client added to PDC*

## Sharing Space in a Domain Controller with Clients:

**Sharing space on a Domain Controller (DC)** involves creating and managing shared resources, such as files and folders, that users within the network can access. This is crucial for collaborative work environments, ensuring centralized storage, ease of access, and efficient management of resources.

## Importance of Sharing Space on a Domain Controller:

1. **Centralized Storage:** Provides a single location for storing files that multiple users can access.
2. **Collaboration:** Facilitates sharing and collaborative work among users.
3. **Management:** Simplifies data management and backup processes.

4. Security: Enforces centralized security policies, ensuring that only authorized users can access sensitive data.

### Concept of Sharing Space:

Sharing space on a DC means making certain files or folders available to users within the network. This involves configuring the server to allow specific users or groups to access these shared resources.

To ensure that only the right users have access to the shared resources, permissions are set. These permissions define what actions a user or group can perform on the shared files or folders, such as reading, writing, or modifying them.

## How Sharing Space is Managed

**Creating Shared Folders:** Administrators create folders on the DC that need to be shared.

**Configuring Sharing Settings:** Settings are configured to define how the folder is shared and who can access it.

**Assigning Permissions:** Specific permissions are set for different users or groups to control what they can do with the shared files.

**Accessing Shared Folders:** Users can access the shared folders from their client machines over the network.

## **Benefits:**

**Enhanced Productivity:** Employees can easily and quickly access the necessary files for their work.

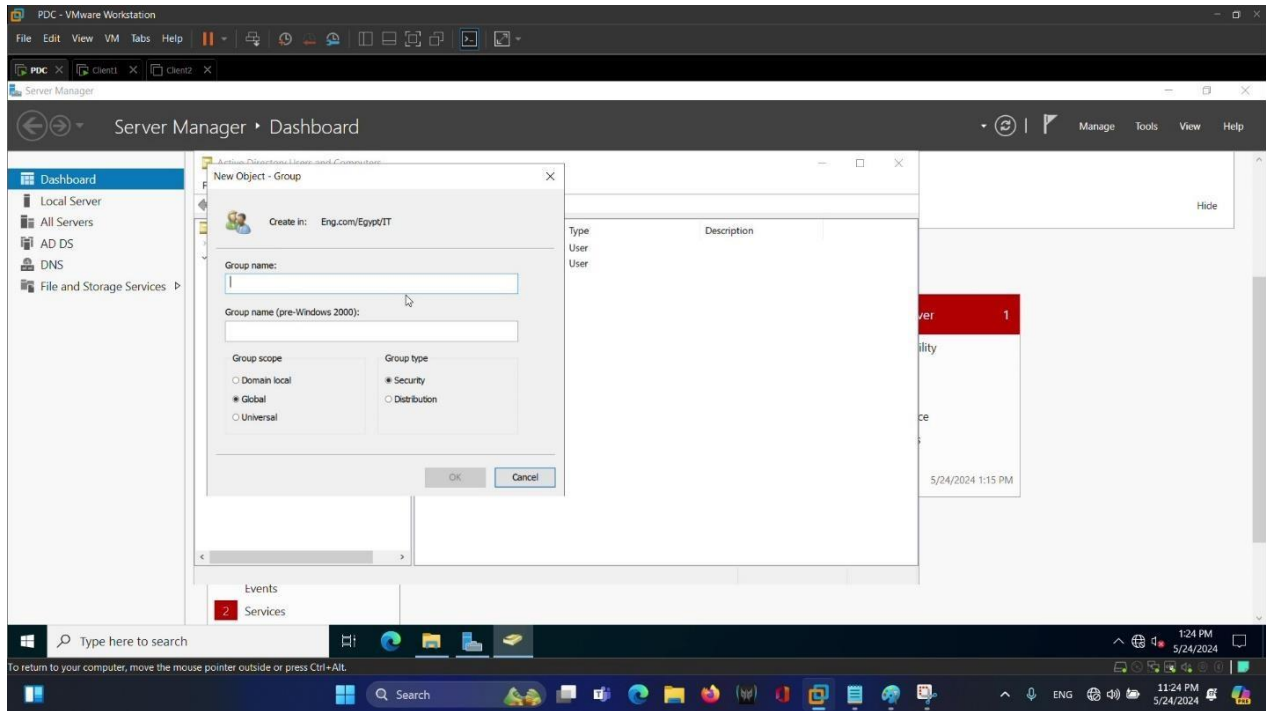
**Improved Security:** Ensures sensitive data is accessed only by authorized users.

**Better Organization:** Maintains a structured and centralized file system, simplifying management and monitoring.

## **Example:**

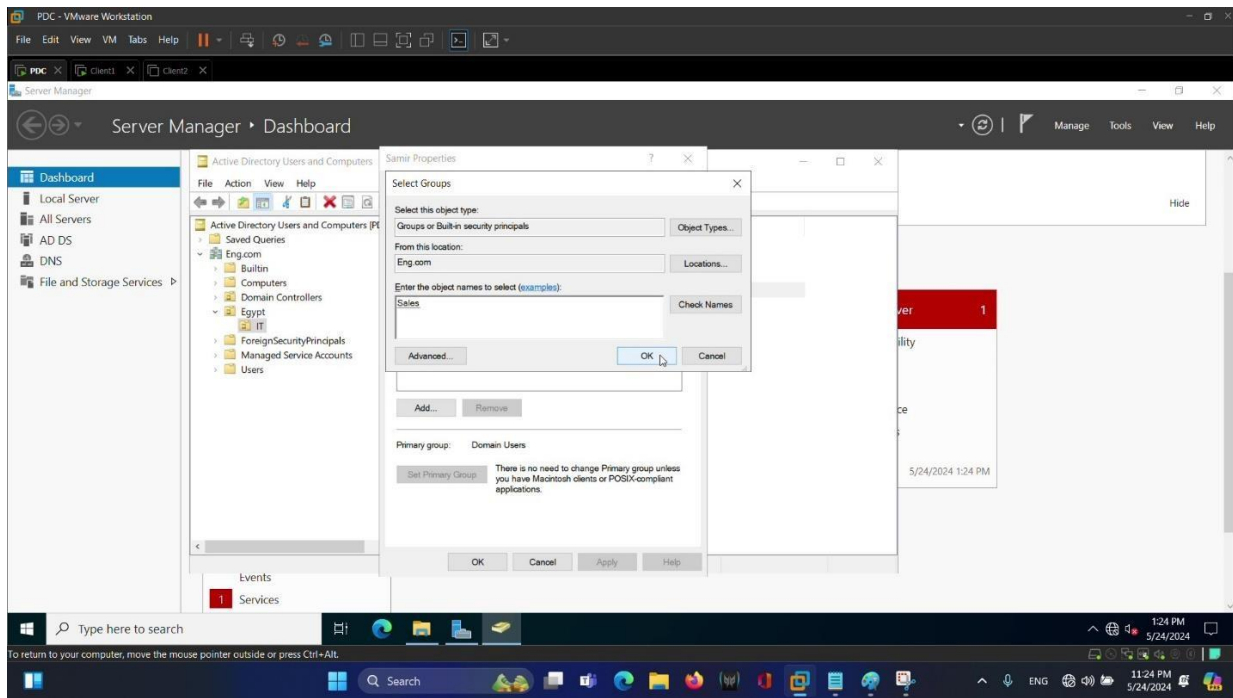
Imagine a company where multiple departments need to collaborate on projects. The IT department can set up shared folders on the domain controller for each project. Permissions can be assigned so that only team members from the relevant departments can access, edit, or view the project files. This setup not only streamlines collaboration but also secures the data by restricting access to authorized personnel.

## Make a new group:



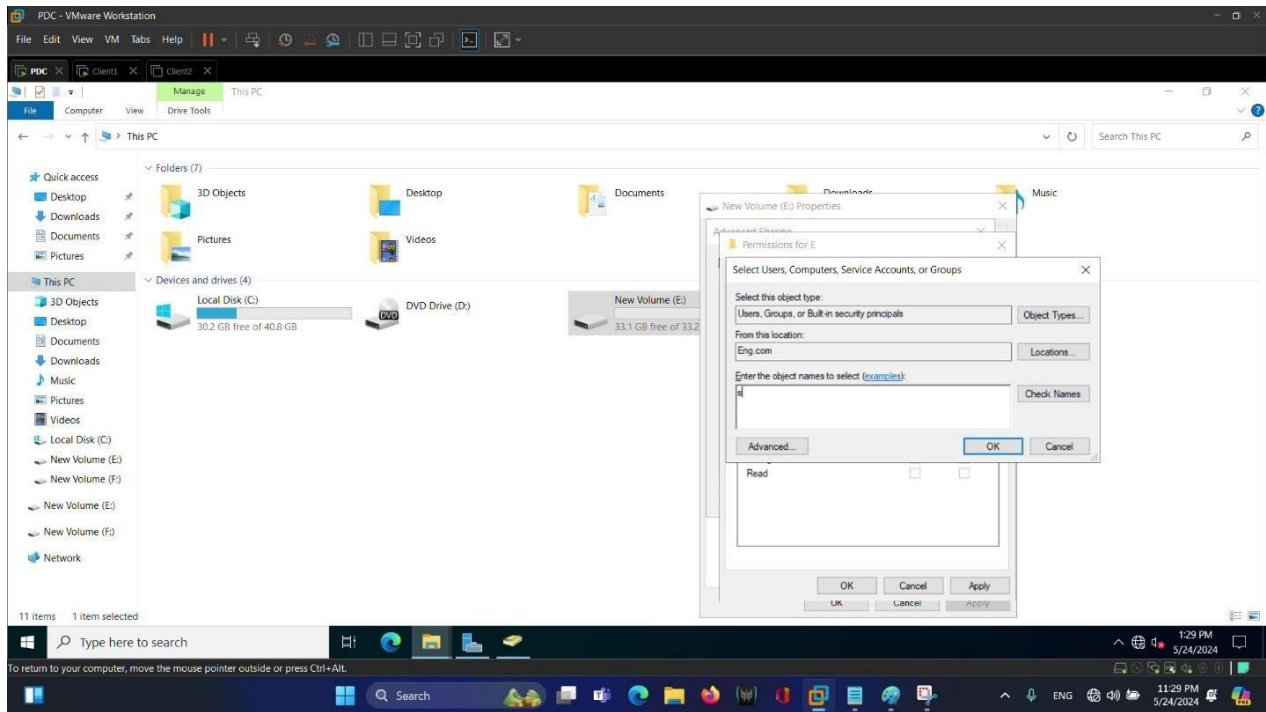
*Figure 52 Make a new group*

## Add Client to Group:



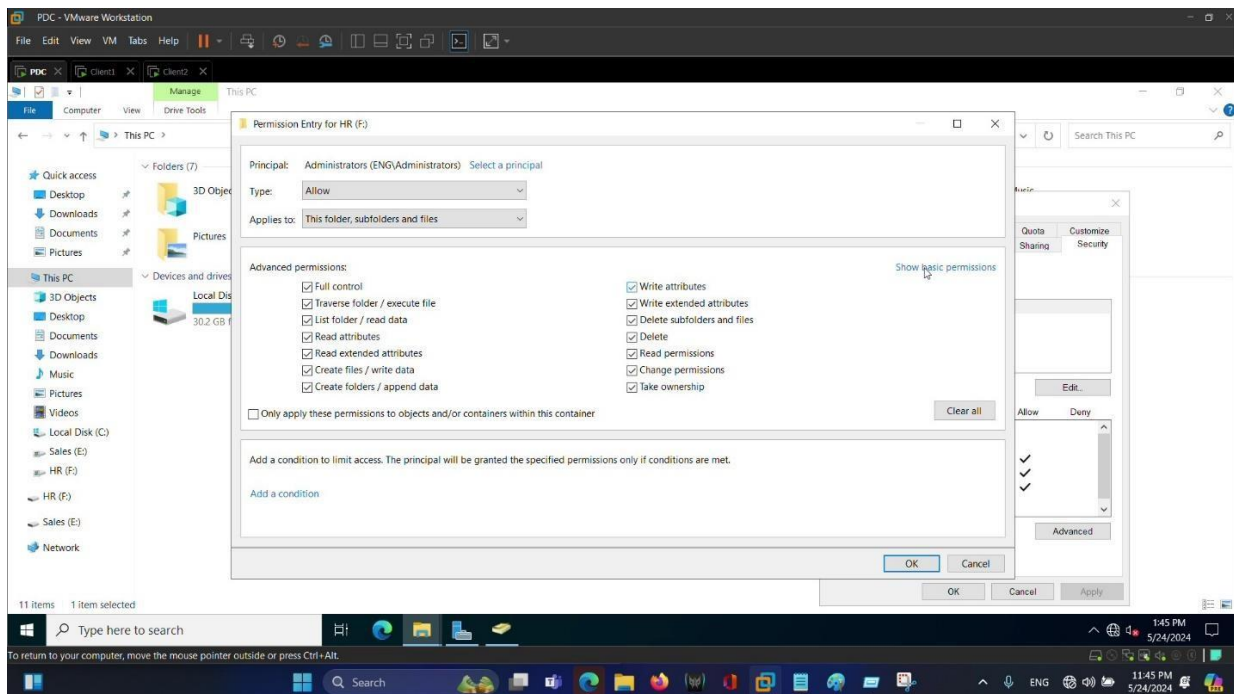
*Figure 53 Add Client to Group*

## Choice the client who can access to this partition:



*Figure 54 Choice the client who can access to this partition*

## Give the client permission:



*Figure 55 Give the client permission*

## **Remote Management in PDC (Primary Domain Controller):**

In the context of a Primary Domain Controller (PDC) refers to the ability to manage and administer the domain controller and its associated services from a remote location. This capability is crucial for administrators who need to oversee and maintain network resources without being physically present at the server's location.

### **Key Aspects of Remote Management in PDC:**

#### **1. Administration and Configuration:**

Allows administrators to perform tasks such as creating and managing user accounts, setting permissions, configuring policies, and overseeing the overall health of the domain from a remote location.

#### **2. Monitoring and Troubleshooting:**

Enables continuous monitoring of the server's performance, security logs, and event logs.

Administrators can troubleshoot issues, apply updates, and ensure the smooth functioning of the domain.

## **Benefits of Remote Management:**

### **1. Convenience:**

Administrators can manage the PDC from anywhere, reducing the need for physical presence at the server location.

### **2. Efficiency:**

Rapid response to issues and the ability to perform routine maintenance without travel delays.

### **3. Cost-Effective:**

Reduces costs associated with on-site visits and allows centralized management of multiple domain controllers.

## **Common Tools for Remote Management:**

### **Remote Desktop Services (RDS):**

Provides a graphical interface to the Windows desktop, allowing full access to the server's GUI.

#### **Windows Admin Center:**

A web-based management tool that provides a centralized interface for managing Windows servers, including PDCs.

#### **PowerShell Remoting:**

Allows administrators to run PowerShell commands and scripts on remote servers, facilitating automation and advanced management tasks.

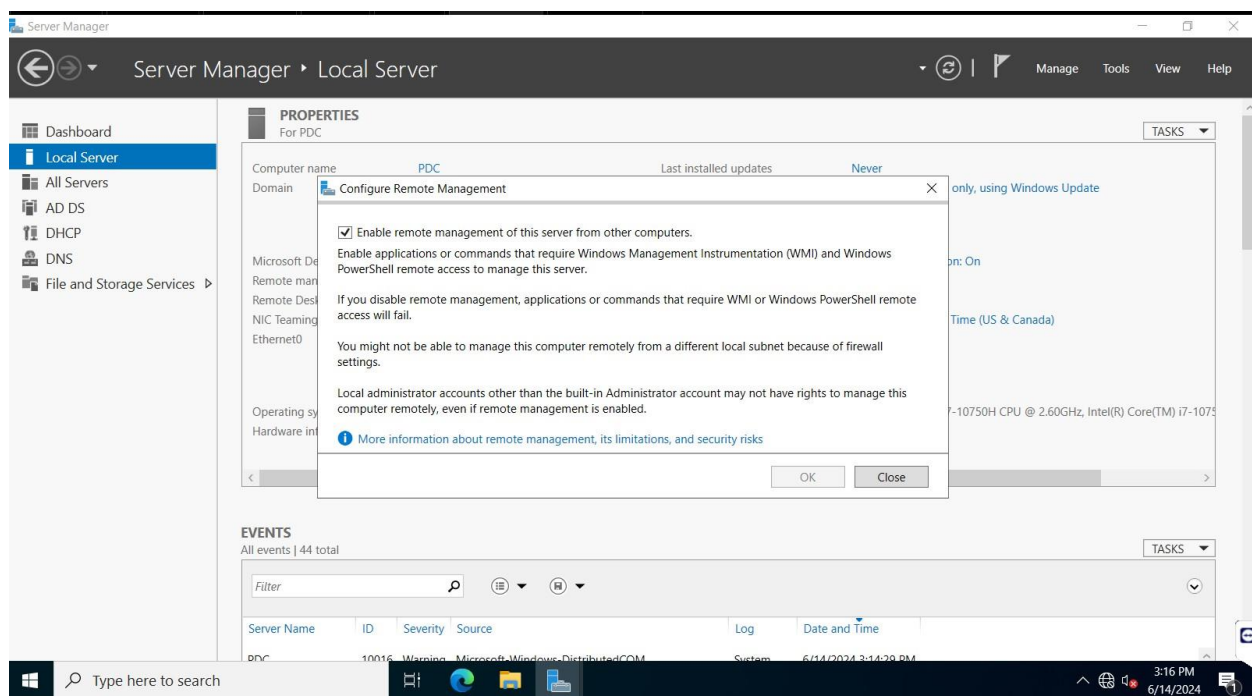
## Third-Party Tools:

Tools like TeamViewer, AnyDesk, and other remote management software can also be used, provided they meet the organization's security requirements.

## Example Scenario:

Imagine an IT administrator managing a company's PDC from a remote office. Using Remote Desktop Services, the administrator can log into the PDC's desktop environment, perform updates, configure group policies, and monitor server performance. Through PowerShell Remoting, they can automate user account creation and script routine maintenance tasks. Secure access via VPN ensures that all communication between the remote office and the PDC is encrypted, maintaining data security.

## GIVE access to another PC to PDC by remote management:



*Figure 56 GIVE access to another PC to PDC by remote management*

## Select user can admin access to PDC from his PC:

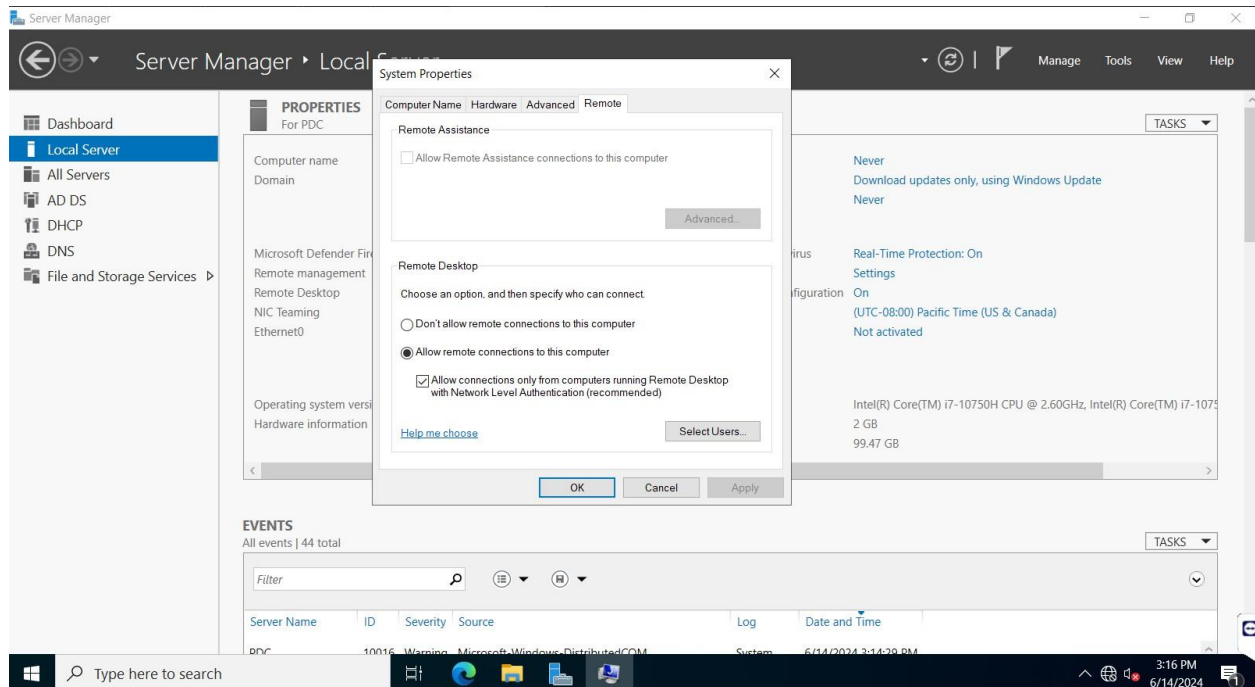


Figure 57 Select user can admin access to PDC from his PC

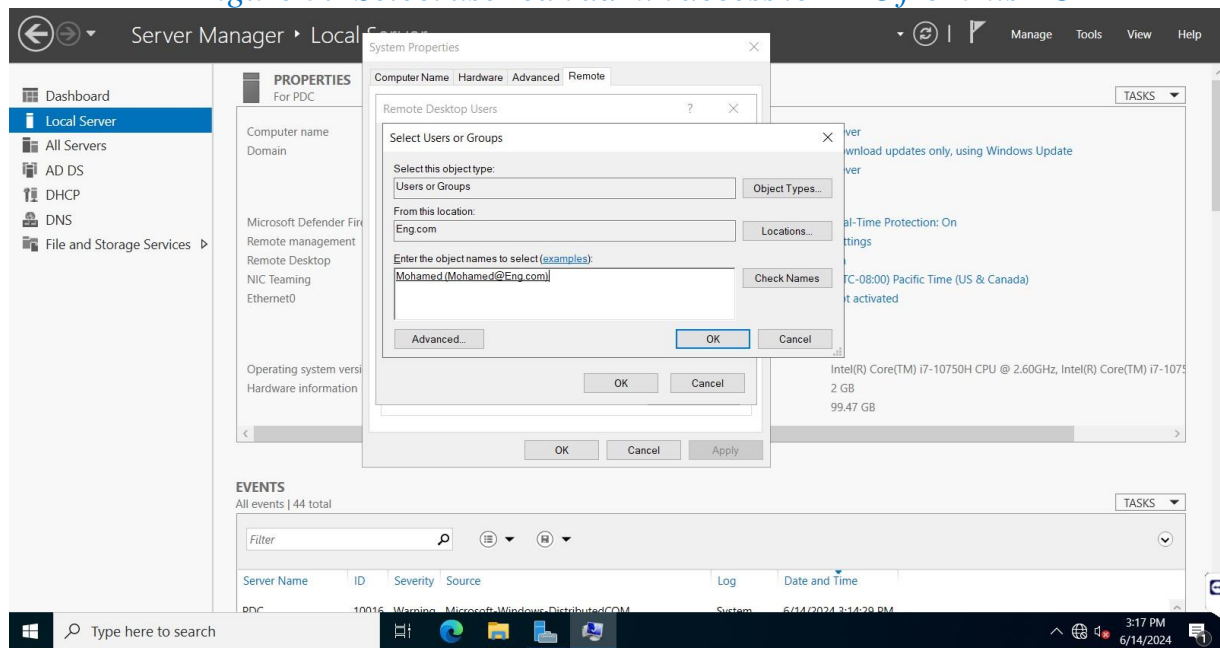
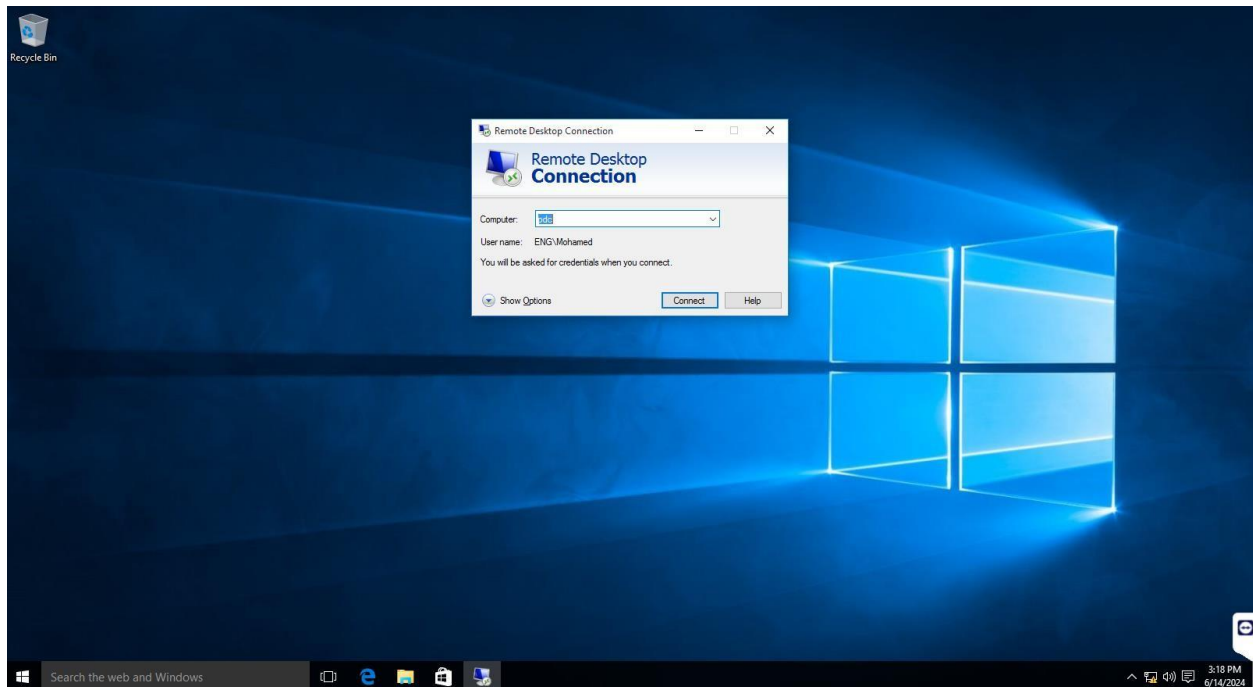


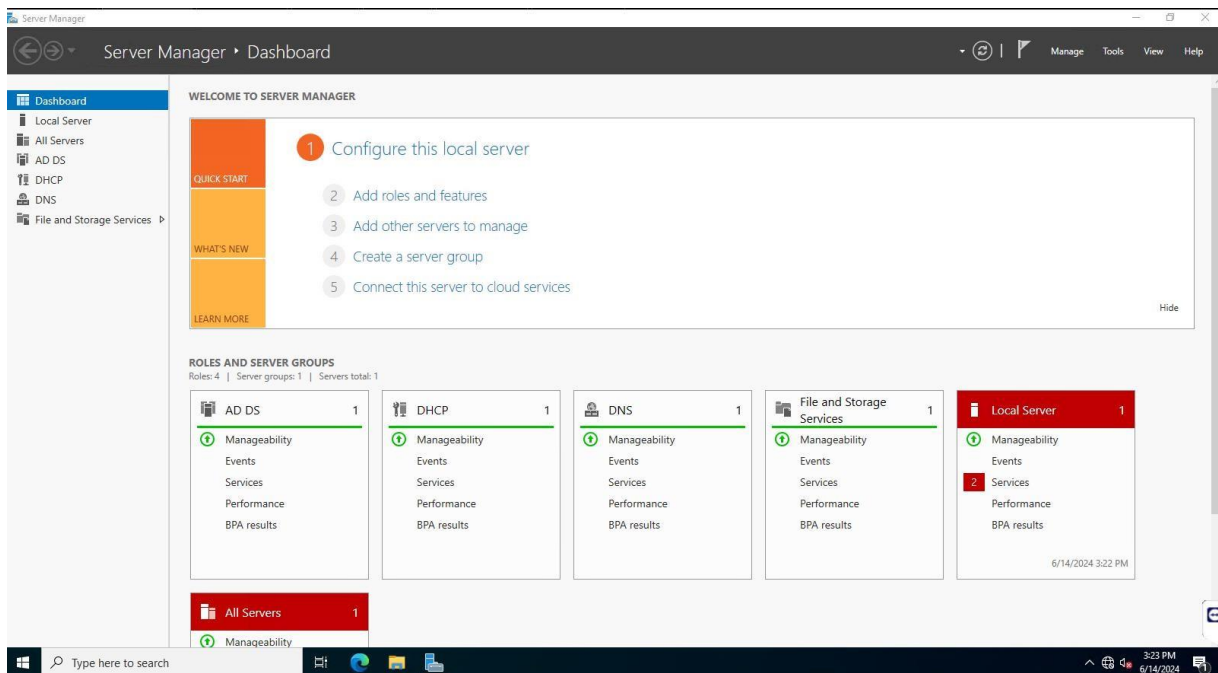
Figure 58 Select user can admin access to PDC from his PC

## Access to PDC from another PC:



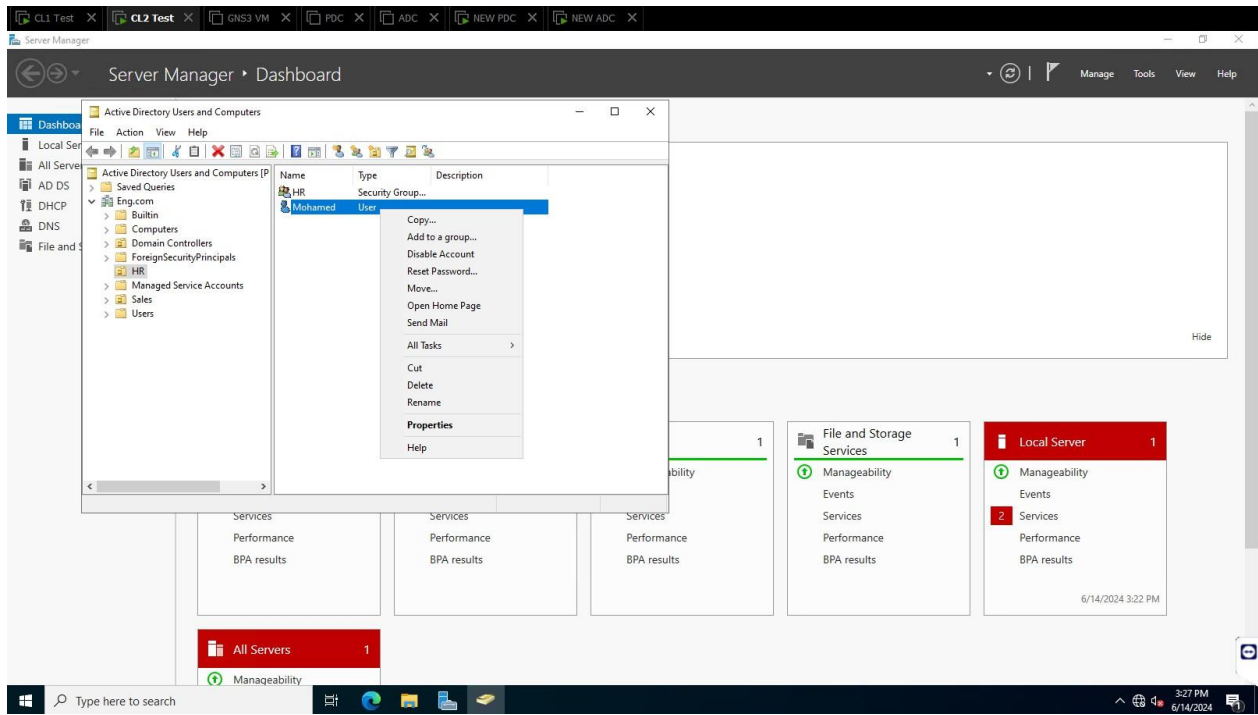
*Figure 59 Access to PDC*

## Open Server manage in PC by remote manage mint:

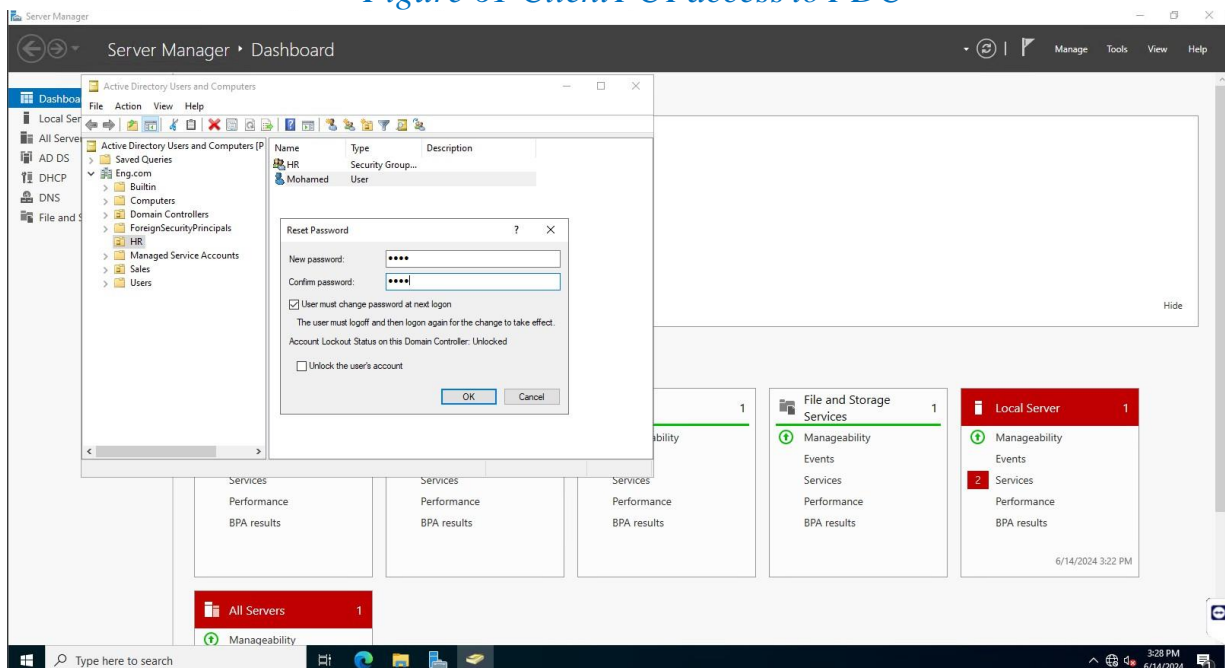


*Figure 60 OpenServer manage*

## One client Forget his Password from the Client PC I access to PDC by remote manage mint to reset his Password:



*Figure 61 Client PCI access to PDC*



*Figure 62 Client PCI access to PDC*

## What is the ADC?

An Additional Domain Controller is a server in a Windows-based network that provides redundancy, load balancing, and fault tolerance for the primary domain controller (PDC). It holds a copy of the Active Directory database and can perform all the functions of the primary domain controller.

### Functions and Benefits:

#### 1. Redundancy:

Having an ADC ensures that if the primary domain controller fails, the network can still authenticate users and provide access to resources. This improves the reliability and availability of the network.

#### 2. Load Balancing:

By distributing authentication and directory services requests across multiple domain controllers, ADCs help in balancing the load, thereby enhancing performance.

#### 3. Fault Tolerance:

ADCs provide a failover mechanism. If one domain controller goes down, the ADC can take over, minimizing downtime and maintaining network stability.

#### 4. Replication:

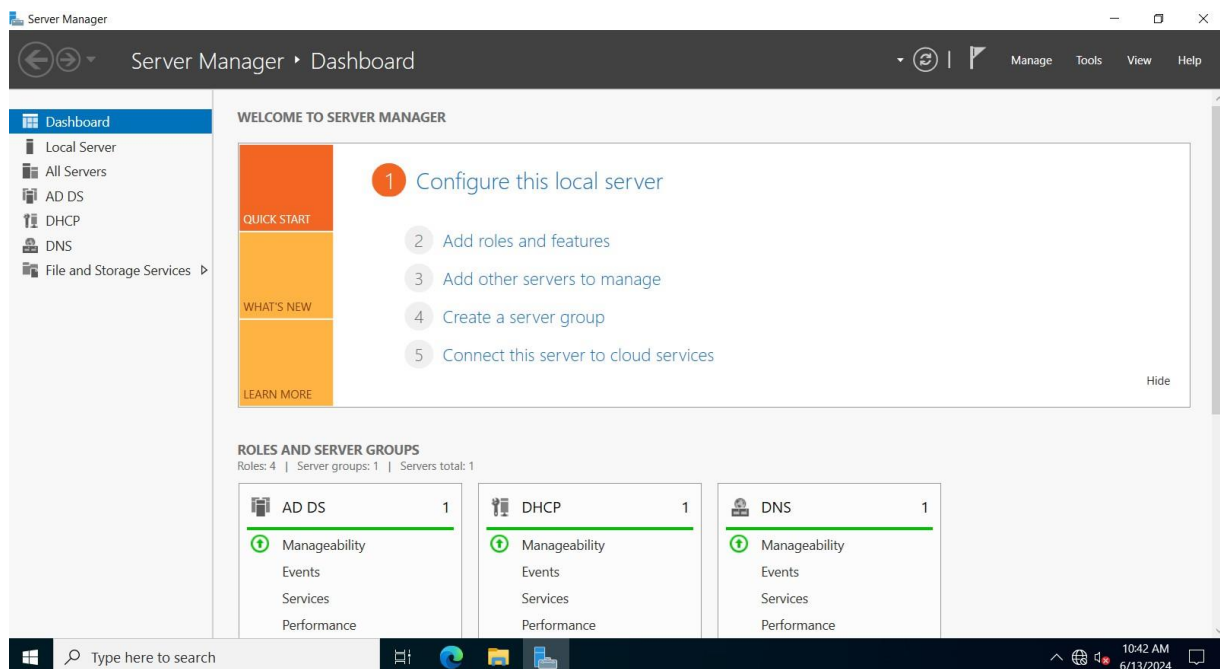
ADCs regularly replicate data with the primary domain controller and other domain controllers within the domain.

This ensures consistency and up-to-date information across the network.

#### 5. Backup:

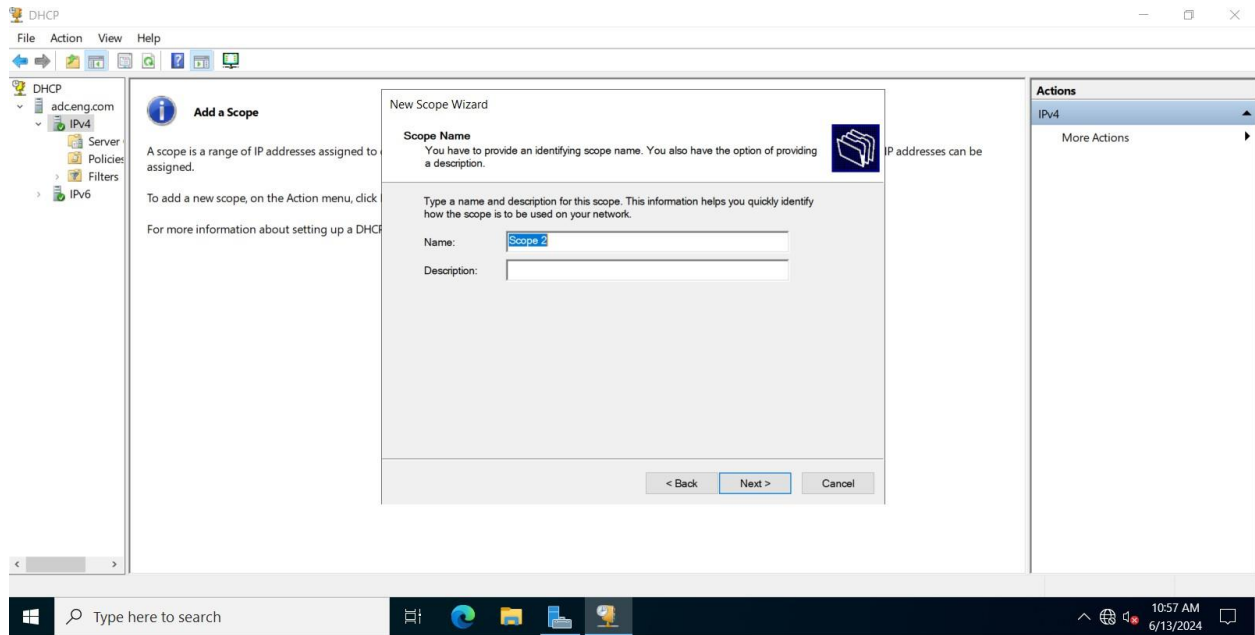
In case of corruption or loss of the Active Directory database on the primary domain controller, an ADC can provide a backup, preventing data loss.

### Interface for Server manager for ADC:



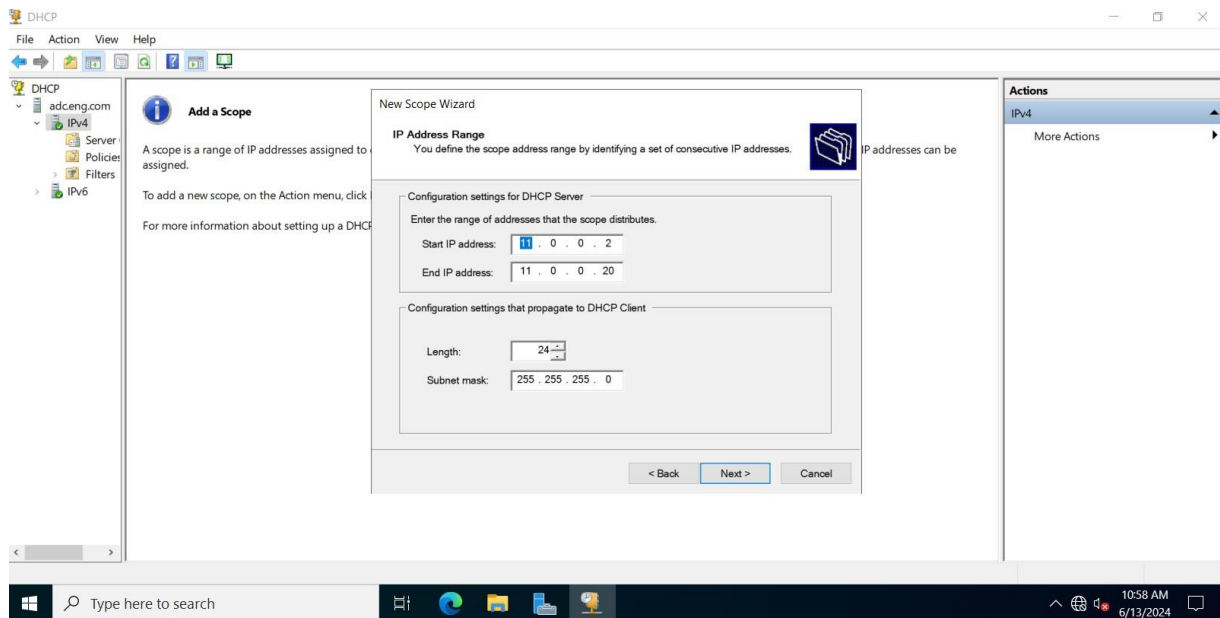
*Figure 63 Interface for Server manager for ADC*

## Making IP pool in ADC:



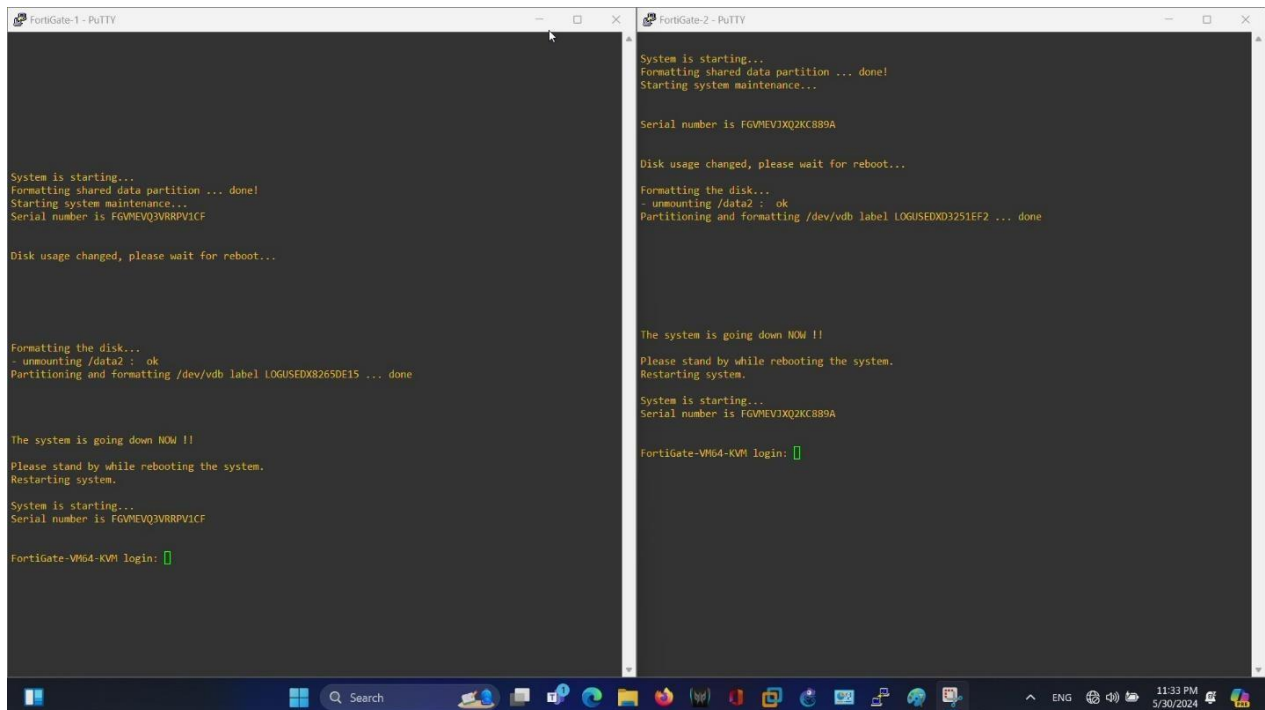
*Figure 64 Making IP pool in ADC*

## Choice the range IP:



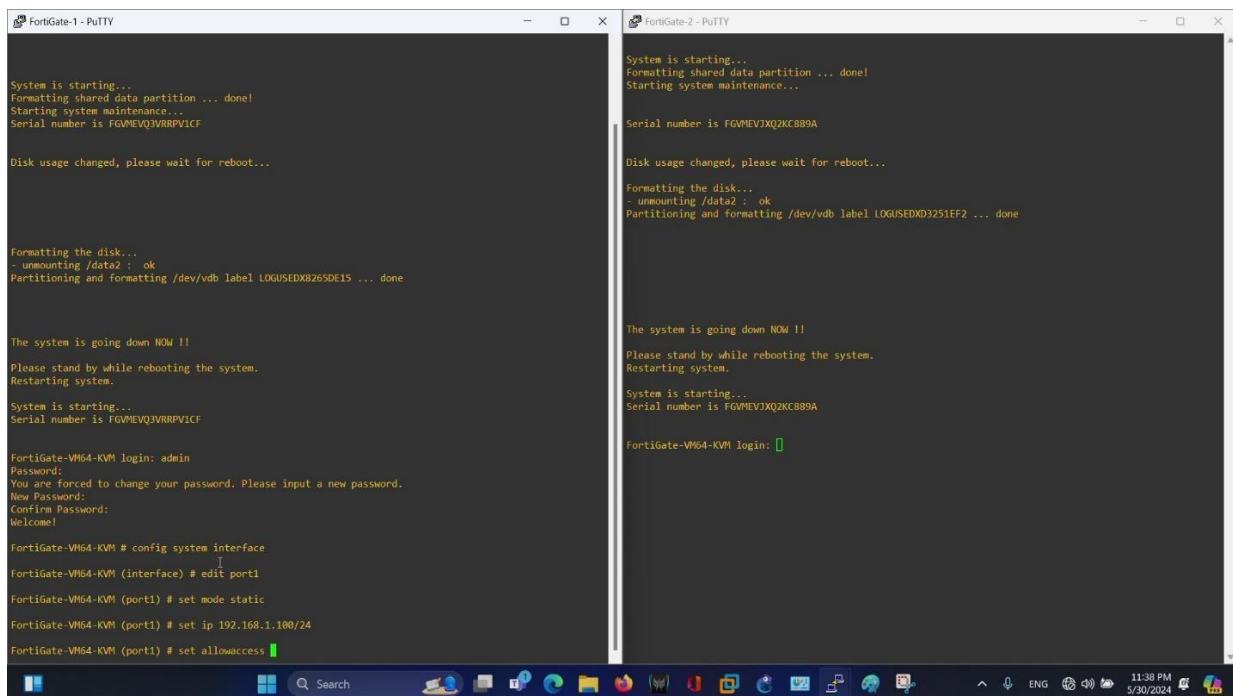
*Figure 65 Choice the range IP*

## Give firewall IP can access to it form browser:



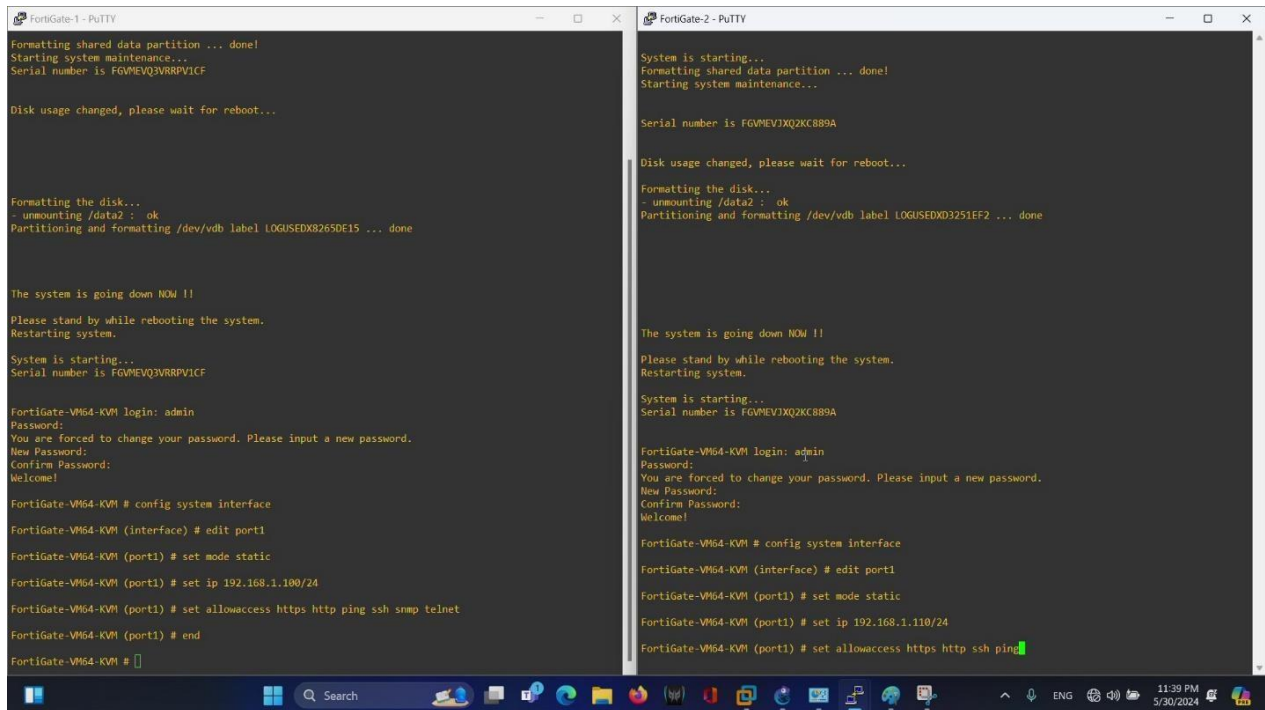
*Figure 66 firewall IP can access to it form browser*

## Give IP for firewall:



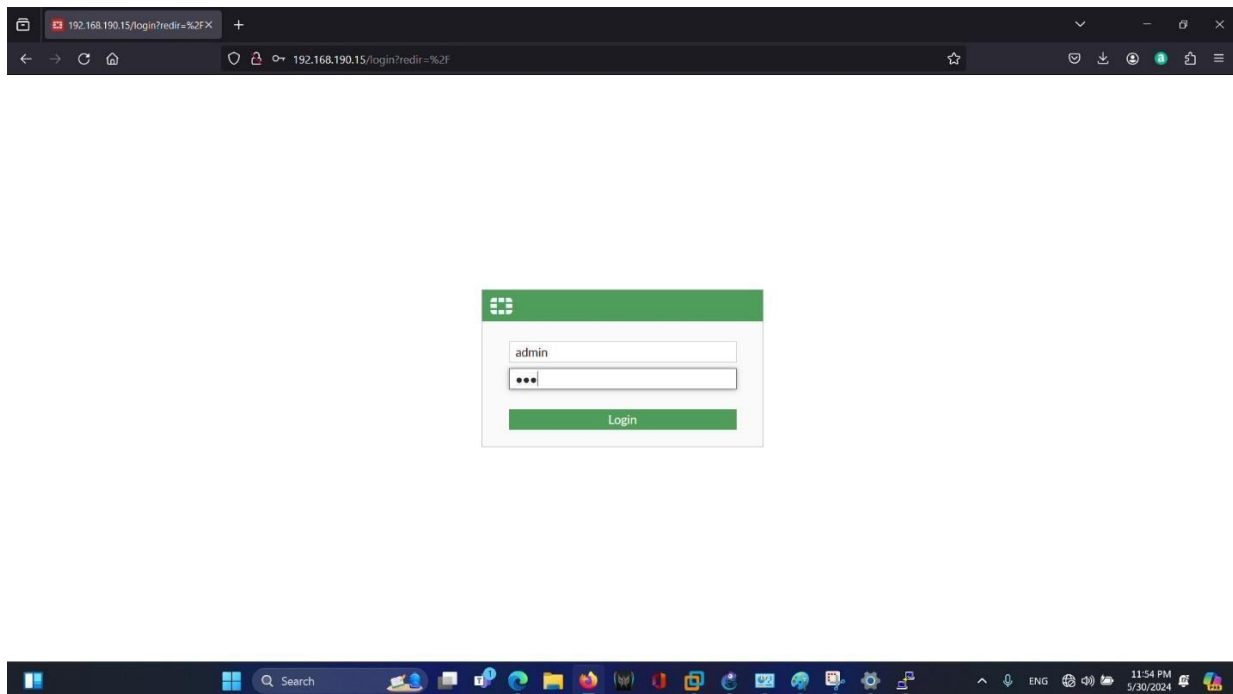
*Figure 67 Give IP for firewall*

## Set allowances for the interface:



*Figure 68 Set allowances for the interface*

## Open GUI of firewall from the browser:



*Figure 69 Open GUI*

## GUI of firewall:

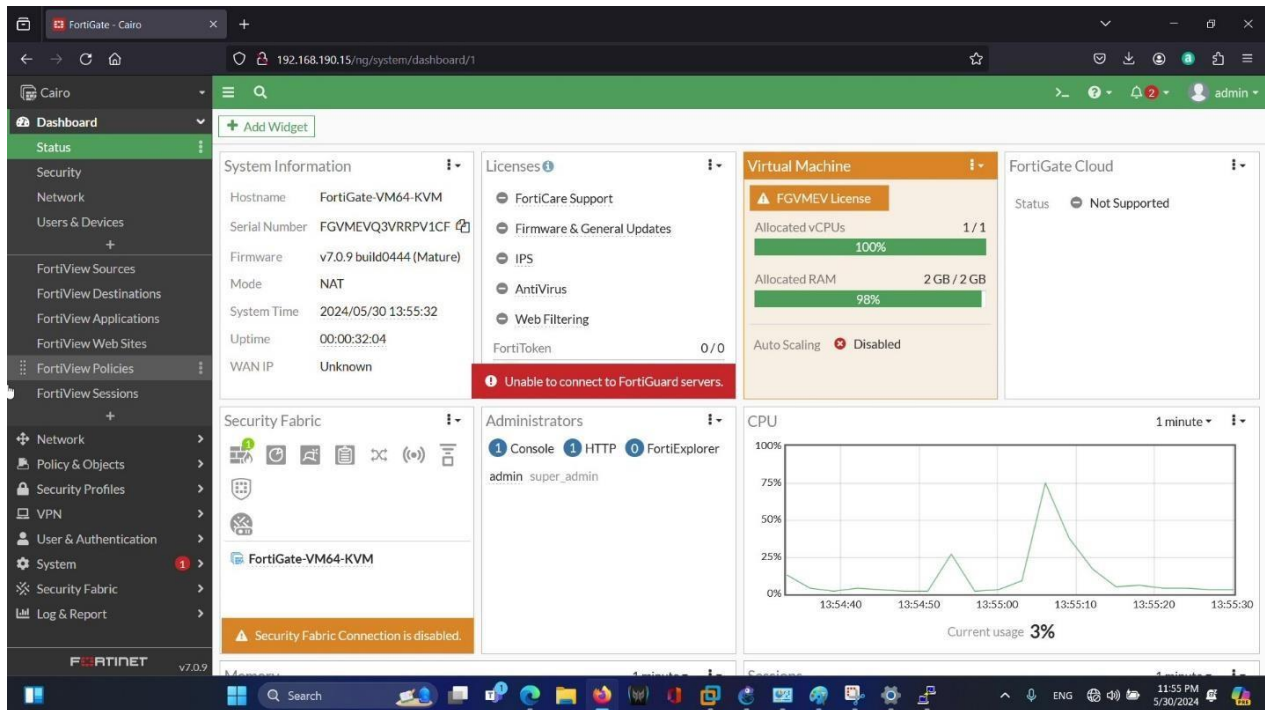


Figure 70 GUI of firewall

## Change IP for interface port1 the connect to isp :

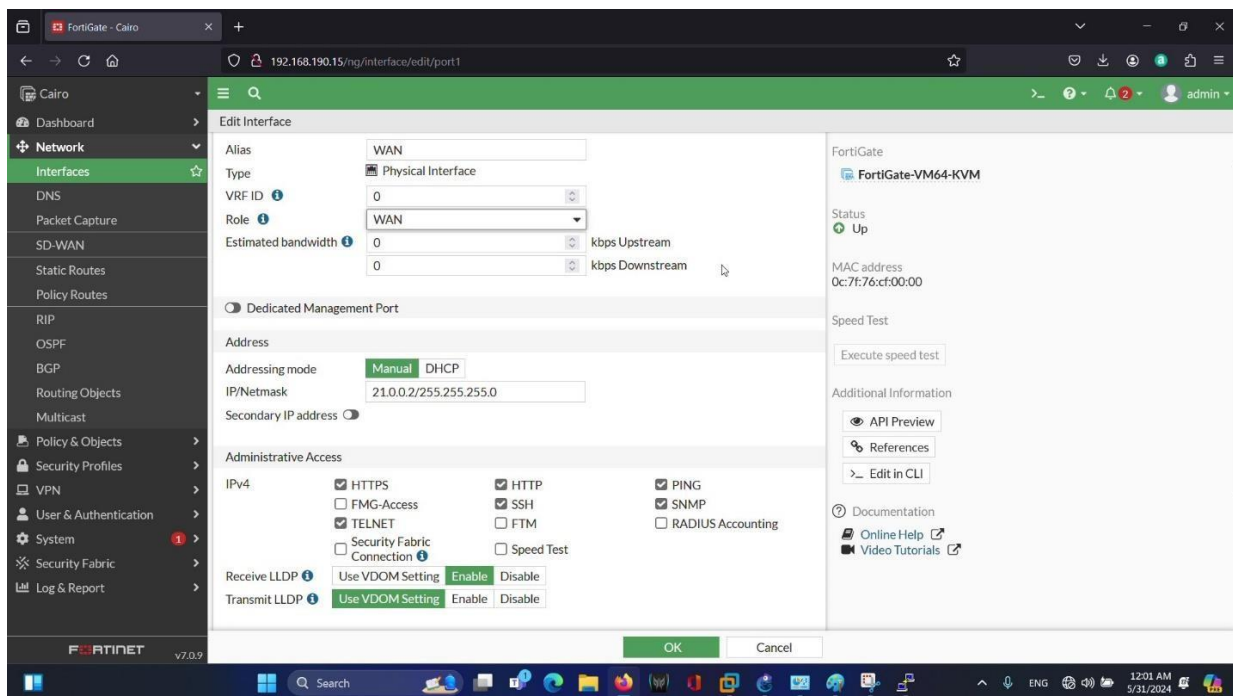
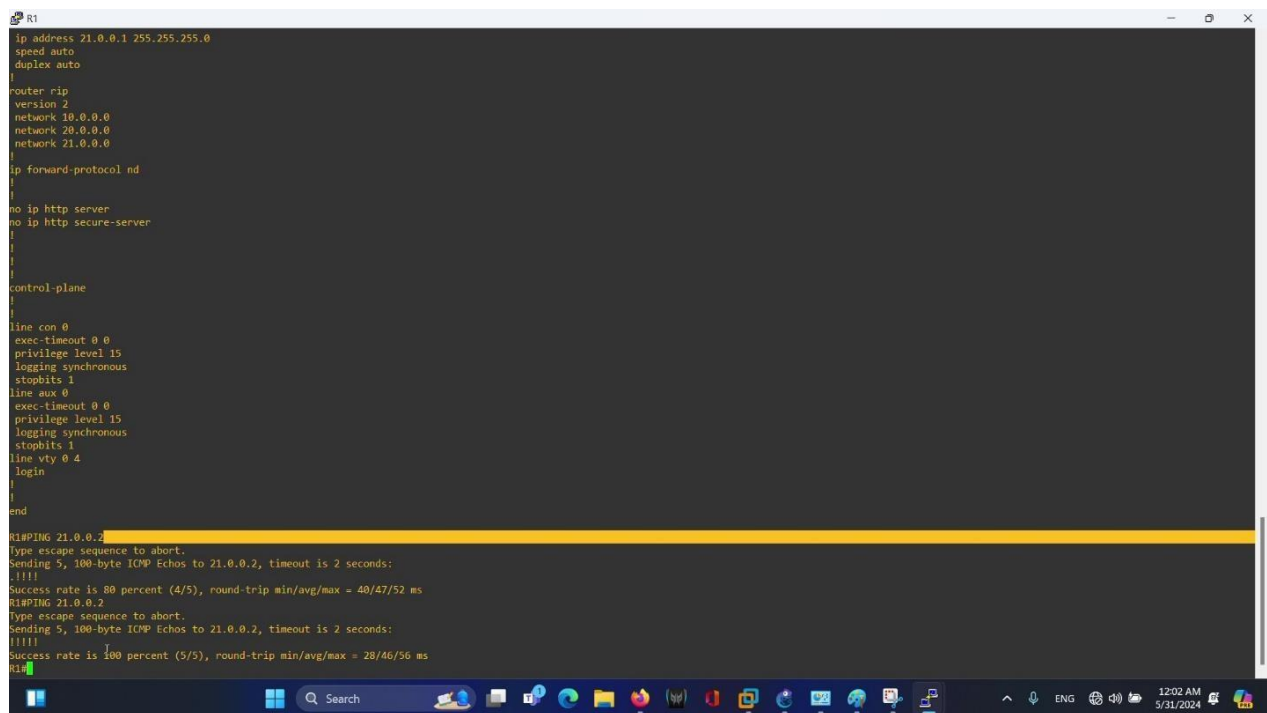


Figure 71 Change IP for interface port1 the connect to isp

## Ping from R1 to check the connection:



```
R1
ip address 21.0.0.1 255.255.255.0
speed auto
duplex auto
!
router rip
version 2
network 10.0.0.0
network 20.0.0.0
network 21.0.0.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
!
end

R1#ping 21.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 21.0.0.2, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/47/52 ms
R1#ping 21.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 21.0.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/46/56 ms
R1#
```

Figure 72 Ping from R1 to check the connection

## Divide the interface to VLAN:

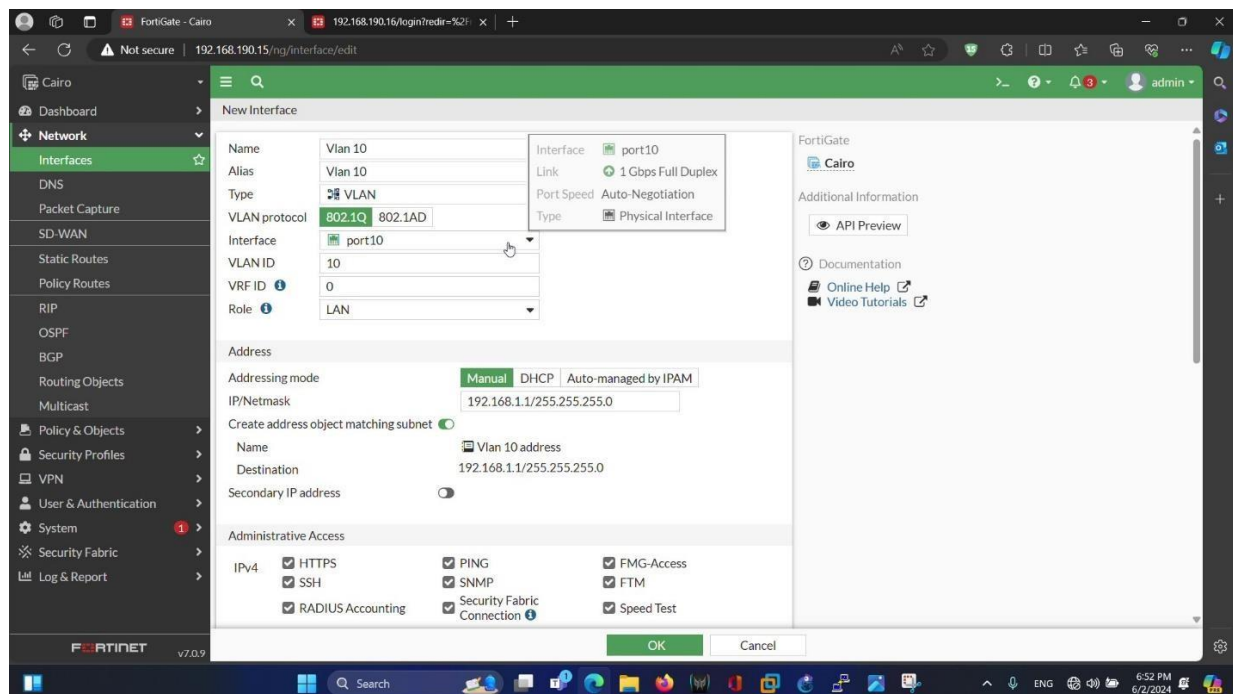


Figure 73 Divide the interface to VLAN

## Make IP pool and give the range of IP:

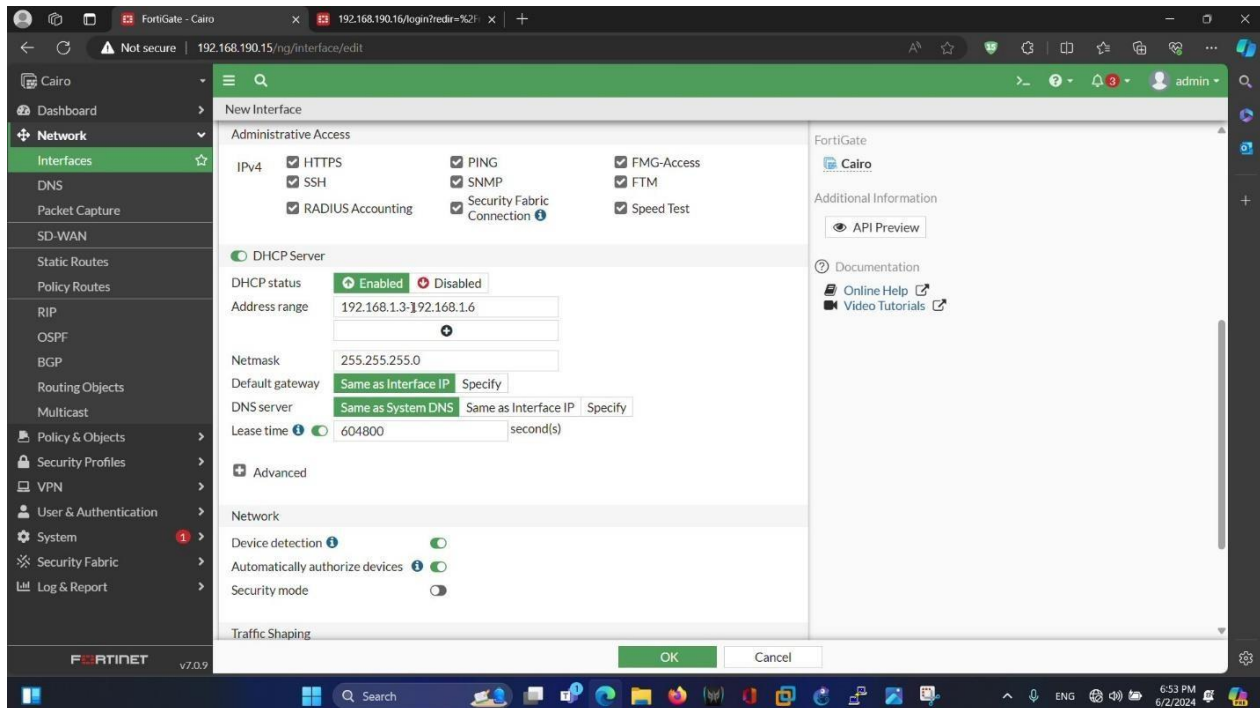


Figure 74 Make IP pool and give the range of IP

## The interface:

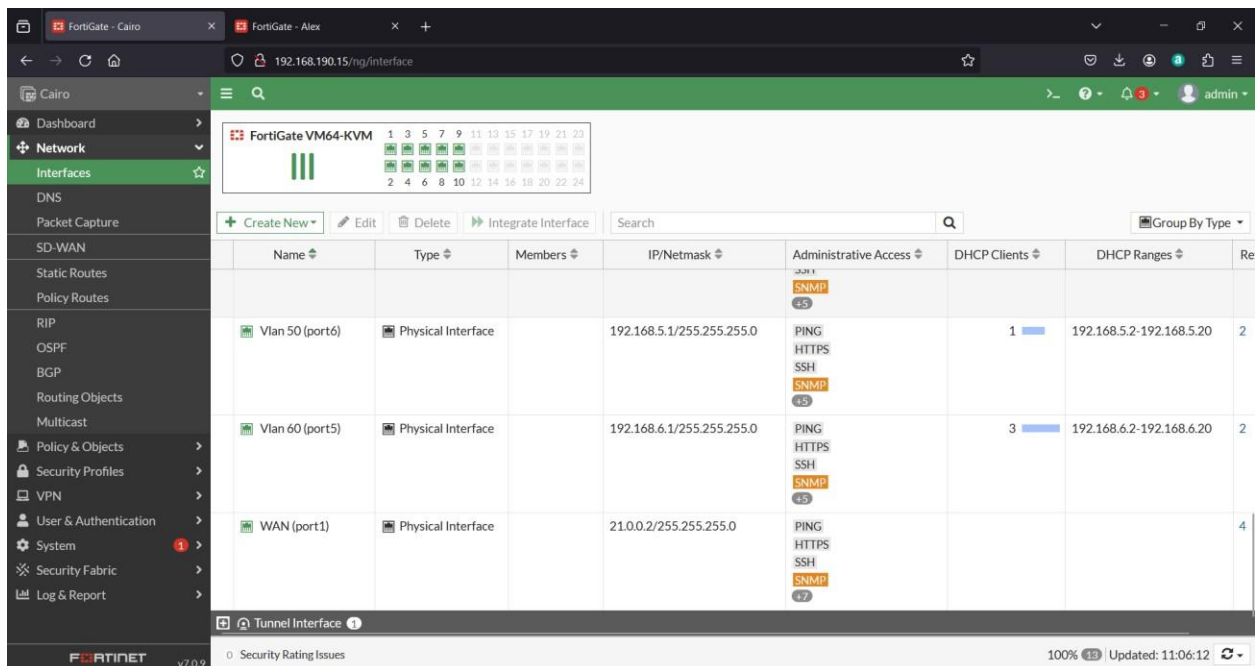


Figure 75 interface

## Doing rip in firewall:

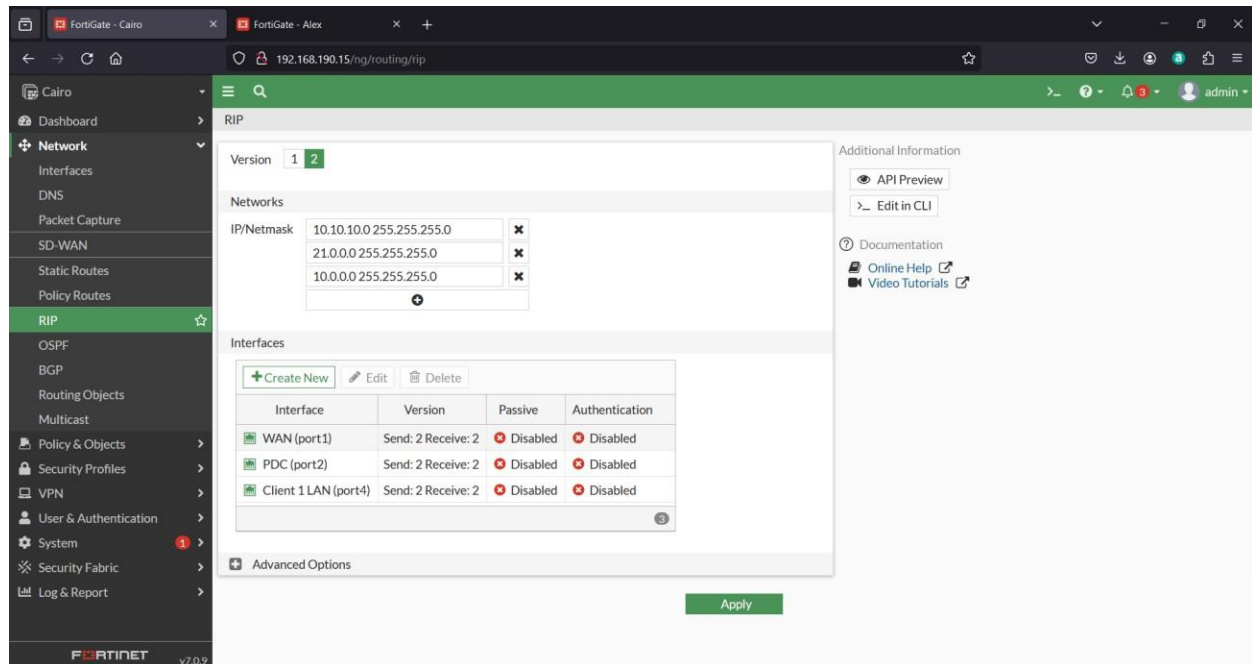


Figure 76 Doing rip in firewall

## The policy in firewall:

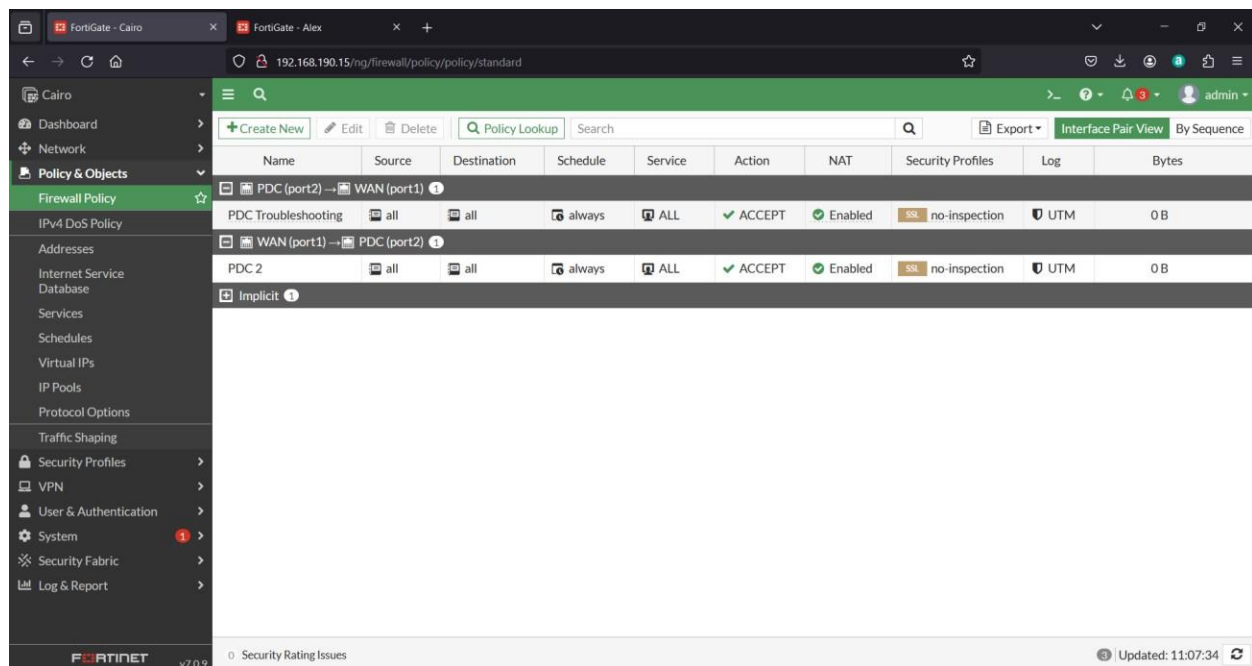


Figure 77 The policy in firewall

## What is the VPN:

VPN (Virtual Private Network) Point-to-Point setup in a domain controller context typically refers to the establishment of a secure, encrypted connection between two points (such as between two offices or a remote user and the corporate network). This setup allows remote clients or sites to securely access the resources and services within a domain as if they were physically present within the local network.

## VPN Configuration:

1. **Site-to-Site VPN:** This configuration connects two networks, such as two branch offices. It uses VPN gateways (routers, firewalls, or dedicated VPN appliances) at each end of the connection.
2. **Remote Access VPN:** This configuration allows individual clients to connect to the network. It uses VPN client software on the user's device to connect to the VPN server on the network.

## Domain Controller Integration:

1. The domain controller (DC) manages authentication and authorization within the network. For a VPN setup, the DC can authenticate remote users trying to access network resources.
2. Active Directory (AD) on the DC can be configured to handle VPN user authentication using protocols like RADIUS (Remote Authentication Dial-In User Service) and services like Network Policy Server (NPS).

## Security Considerations:

1. **Encryption:** VPNs use protocols like IPsec (Internet Protocol Security) or SSL/TLS (Secure Sockets Layer/Transport Layer Security) to encrypt the data transmitted between the points.
2. **Authentication:** Strong authentication methods, such as multi-factor authentication (MFA), can be implemented to enhance security.
3. **Access Control:** Policies can be configured on the DC and VPN servers to restrict access

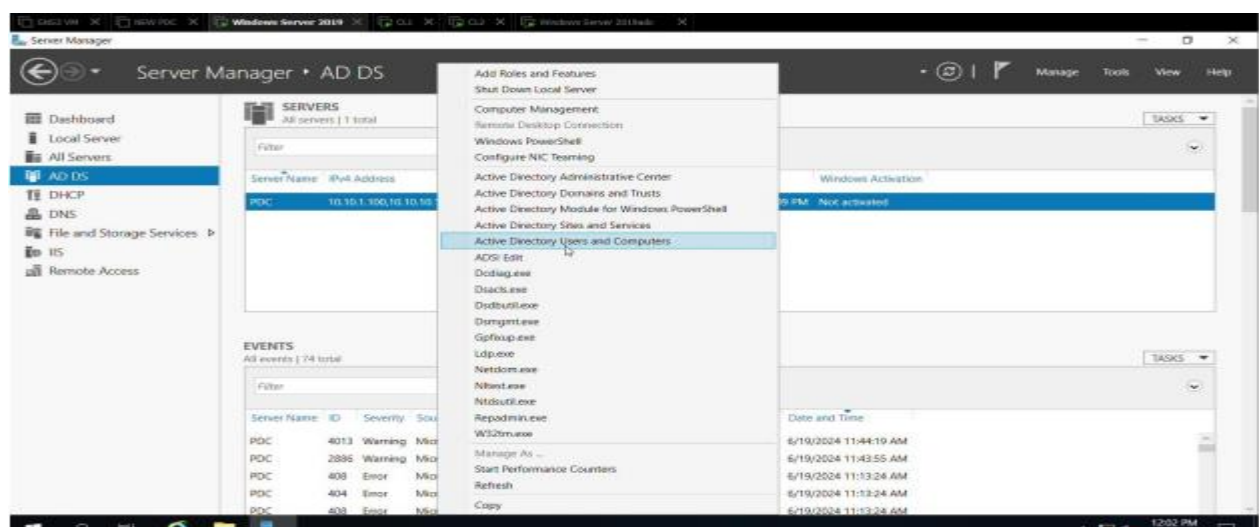
to certain resources based on user roles and groups.

## Benefits of VPN Point-to-Point in a Domain Controller Environment:

1. Enhanced Security: Encrypts data between remote points, protecting it from interception.
2. Centralized Management: The domain controller can centrally manage user authentication and access policies.
3. Remote Access: Allows employees to securely access corporate resources from remote locations.
4. Scalability: Can easily scale to accommodate additional remote users or branch offices.

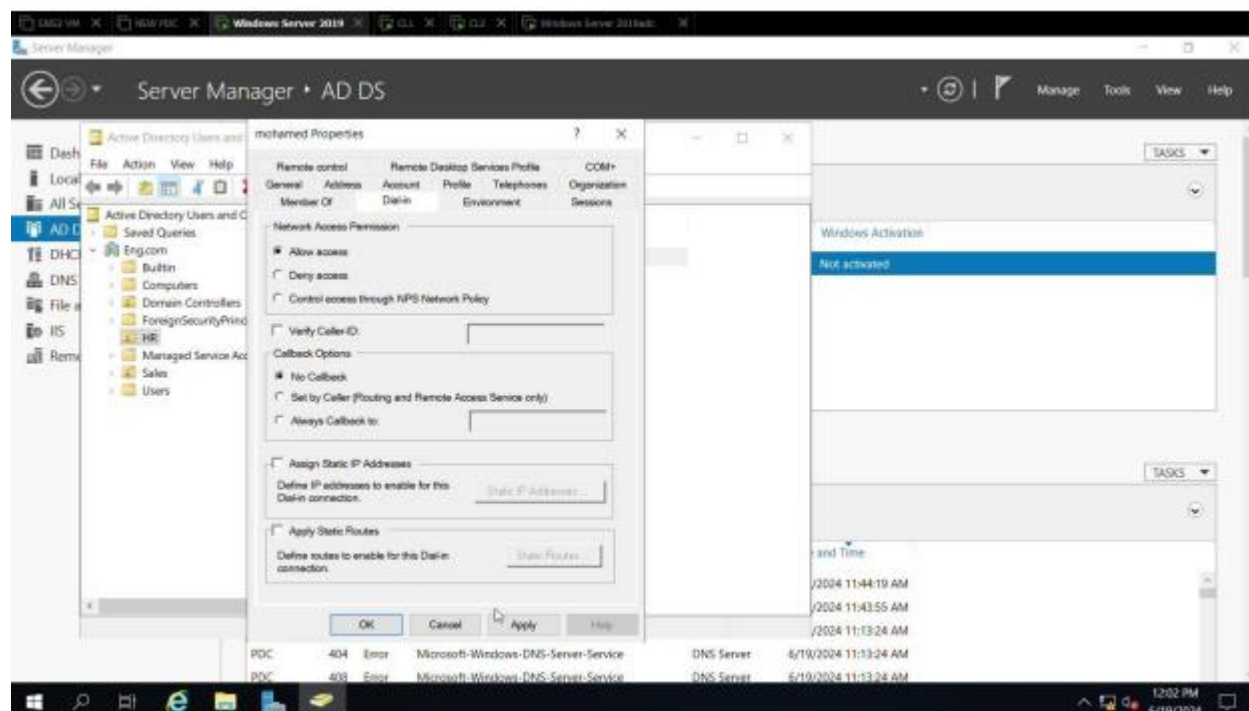
Setting up a VPN Point-to-Point connection in a domain controller environment can provide secure and efficient remote access to network resources, enhancing both productivity and security for an organization.

**After installing VPN give the PC access to it:**



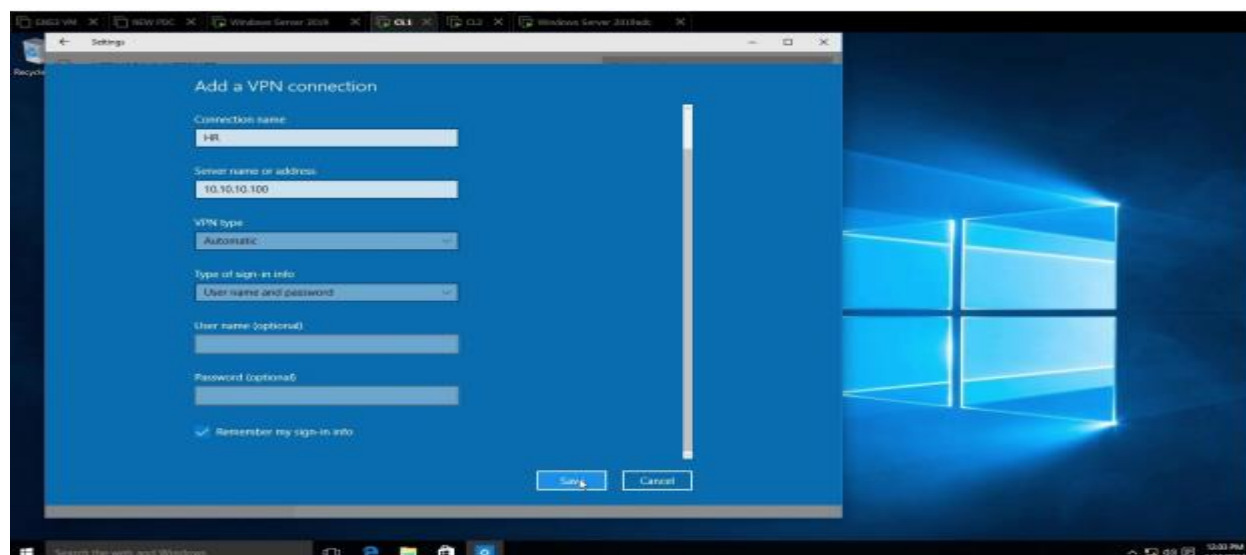
*Figure 78 After installing VPN give the PC access to it*

**Give the user access permission:**



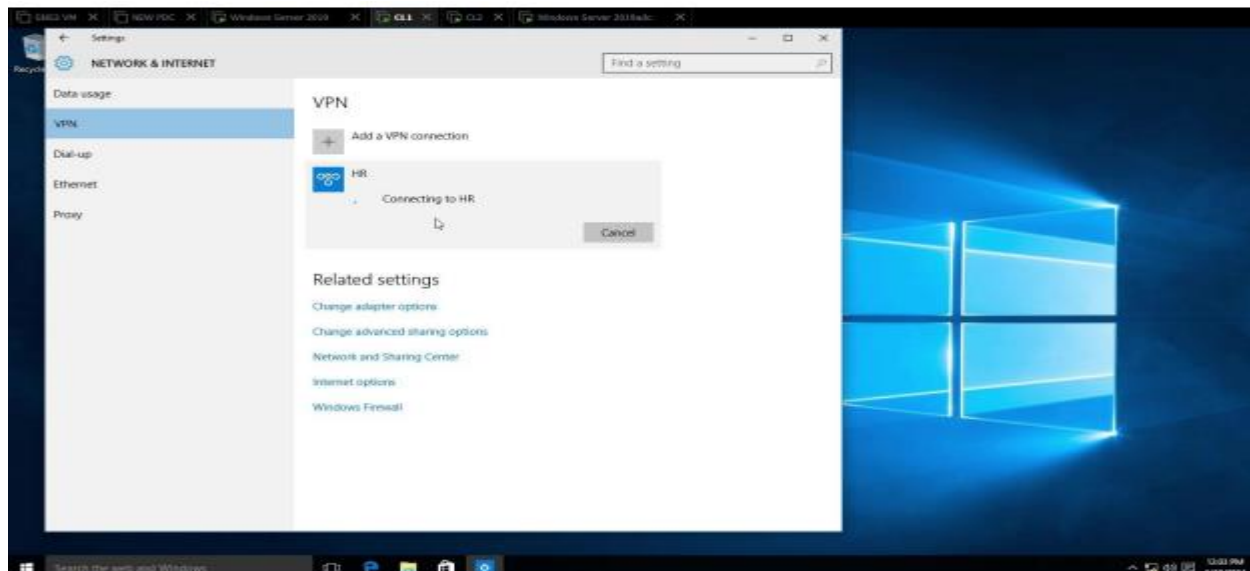
*Figure 79 Give the user access permission*

**Add VPN BY User:**



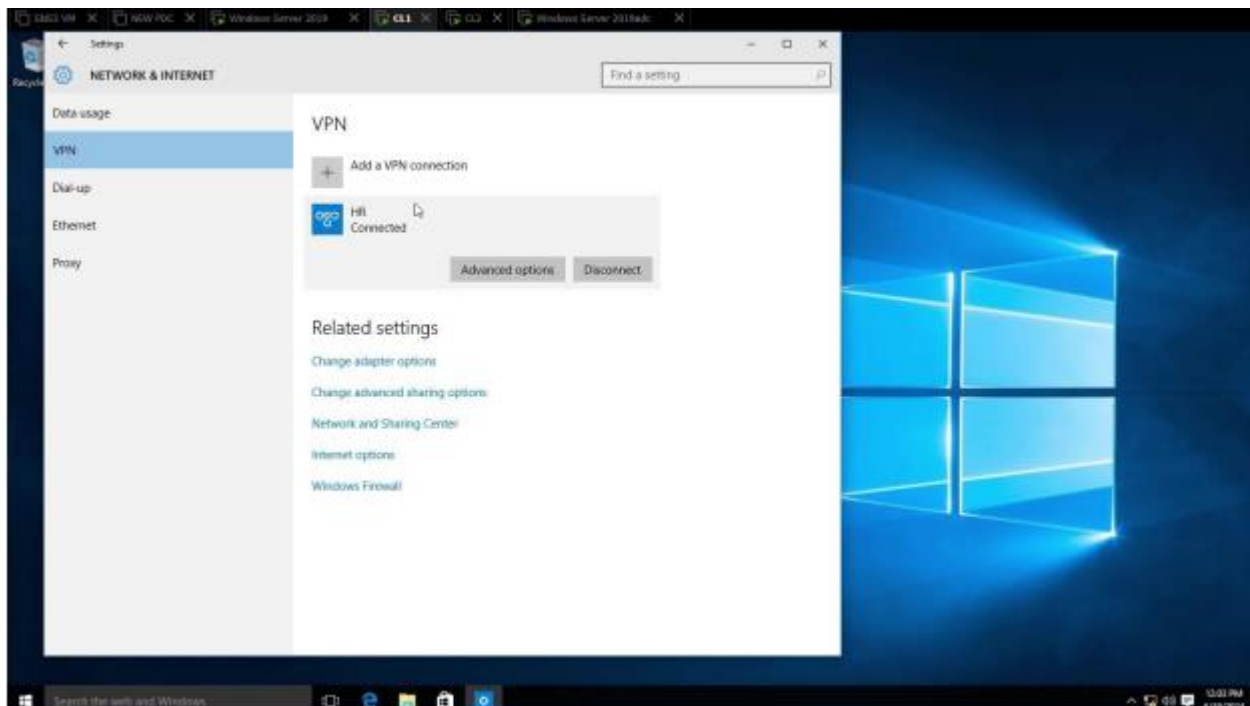
*Figure 80 Add VPN BY User*

## Connect to VPN:

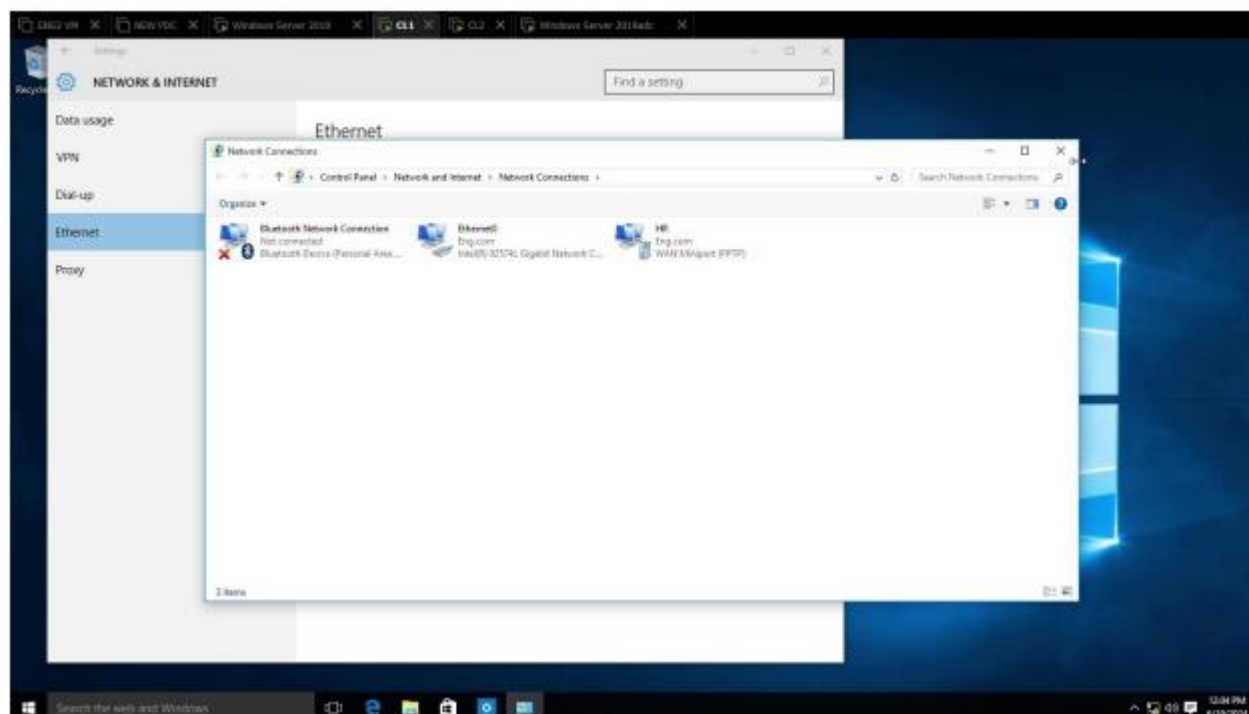


*Figure 81 Connect to VPN*

## The user connected to VPN:

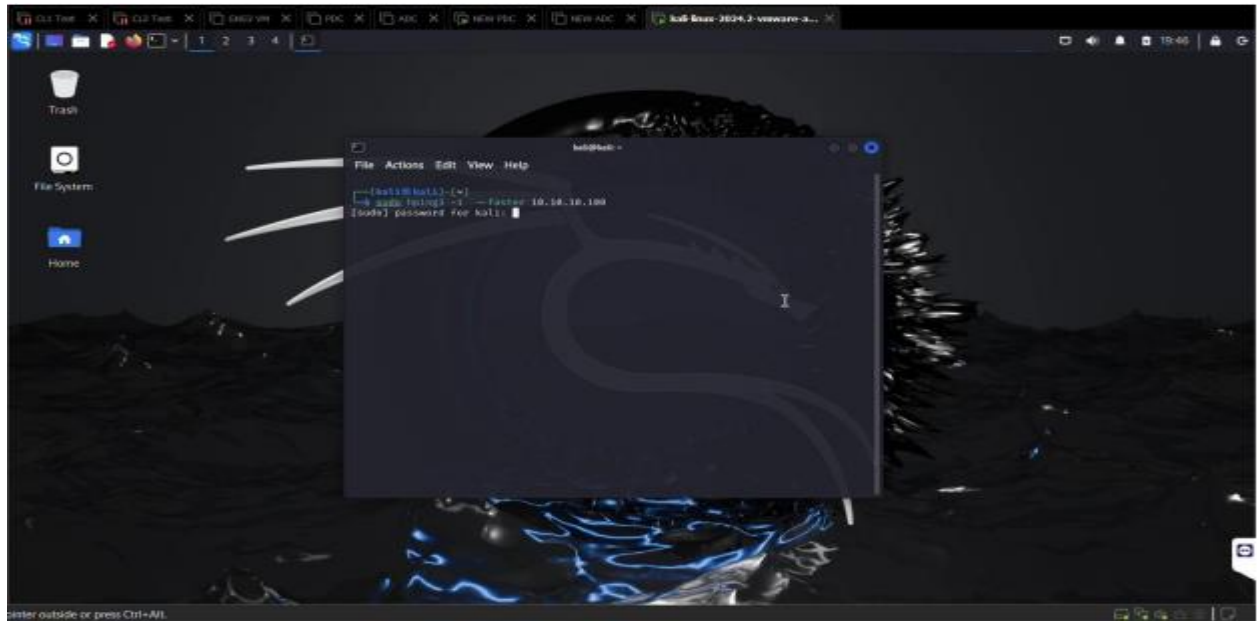


*Figure 82 The user connected to VPN*



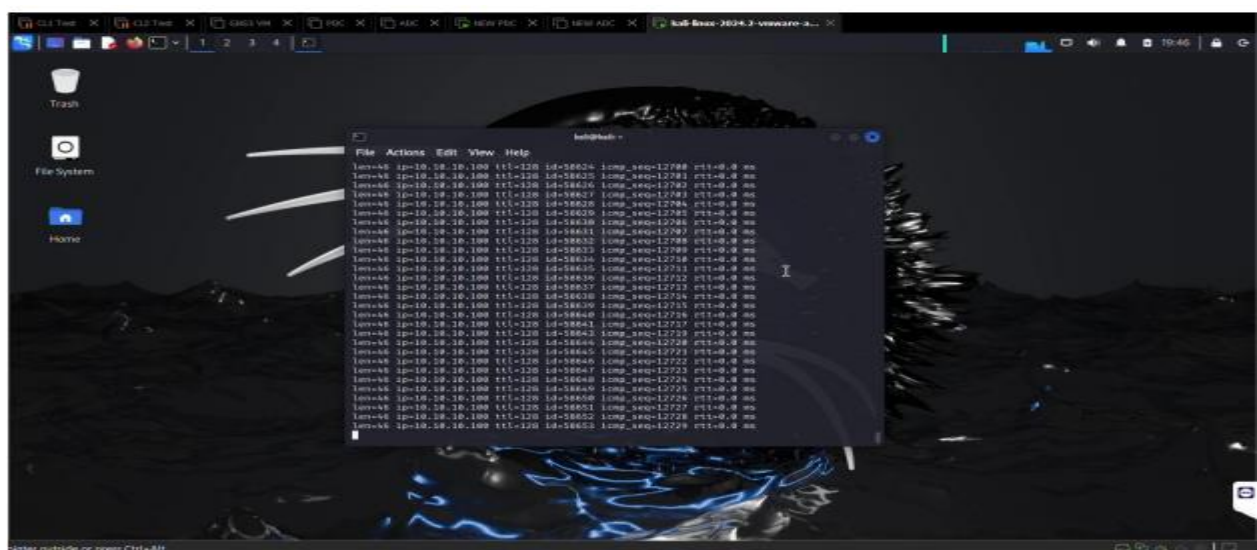
*Figure 83 The user connected to VPN*

## Doing attack DDOS in server:



*Figure 84 Doing attack DDOS in server*

## The attack was done



*Figure 85 The attack was done*

# How stop the attack:

Edit Policy

Name ⓘ

PDC-AntiDDoS

Incoming Interface

WAN (port1)

Source Address

all

+

✕

Destination Address

all

+

✕

Service

ALL

+

✕

Additional Information

API Preview

Edit in CLI

Documentation

Online Help

Video Tutorials

Consolidated Policy Configuration

L3 Anomalies

Name	Logging	Action	Threshold
ip_src_session	<input checked="" type="checkbox"/>	<div>DisableBlockMonitor</div>	4000
ip_dst_session	<input checked="" type="checkbox"/>	<div>DisableBlockMonitor</div>	4000

L4 Anomalies

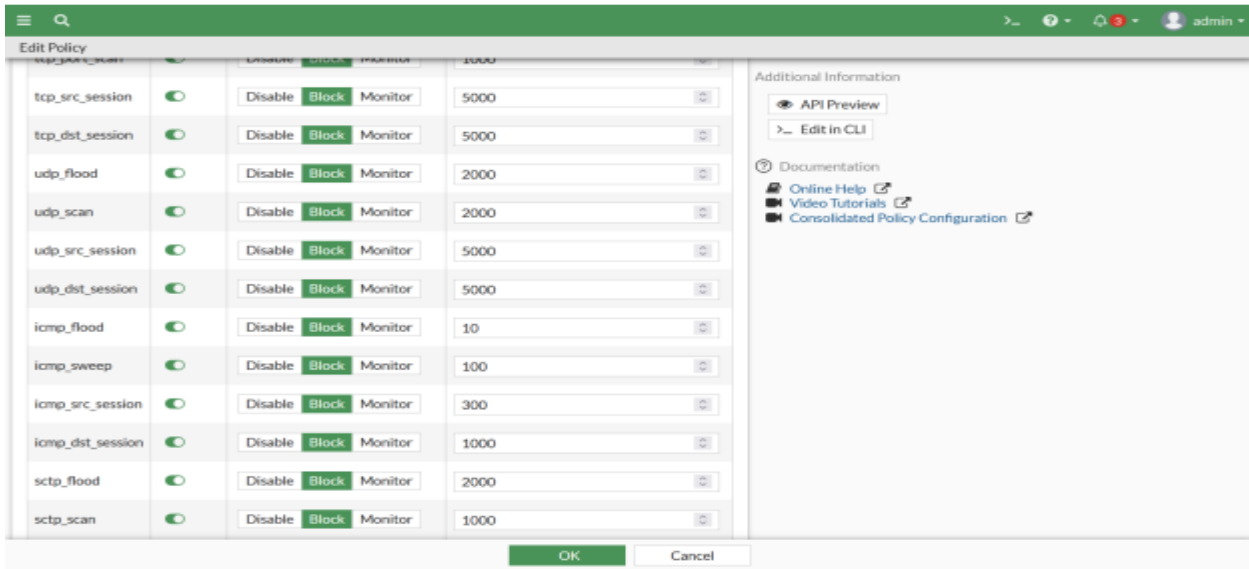
Name	Logging	Action	Threshold
tcp_syn_flood	<input checked="" type="checkbox"/>	<div>DisableBlockMonitor</div>	2000

OK

Cancel

Figure 86 How stop the attack

## ICMP flood 10 requests only:



*Figure 87 ICMP flood 10 requests only*

## Limited by 10 requests:



*Figure 88 Limited by 10 requests*

# Conclusions

In the modern era, networks are essential for the seamless operation and connectivity of companies and their subsidiaries. Through various types and configurations of networks, businesses can maintain synchronized systems and secure communications across multiple locations. This study has demonstrated the importance of understanding the underlying mechanisms that facilitate these connections. Key conclusions include:

1. **Diverse Network Structures:** The flexibility in network types, shapes, and sizes allows for tailored solutions that meet the specific needs of different organizations.
2. **Synchronized Systems:** Effective network management ensures that systems across all branches remain consistent, enabling uniform operations and streamlined processes.
3. **Secure Communication:** Advanced security protocols and encryption methods are critical in protecting data transmitted across networks, safeguarding sensitive information from potential threats.
4. **Efficient Network Management:** Utilizing modern techniques and technologies for network representation and management promotes unified control and monitoring, enhancing overall operational efficiency.

These insights underscore the pivotal role of robust and well-managed networks in achieving cohesive and secure business operations across multiple locations.

# Reference List

some references that cover these areas:

## Network Design and Configuration

### 1. Books:

- "Network Warrior" by Gary A. Donahue: This book provides practical insights into network design and configuration, including routing and switching.
- "Computer Networking: A Top-Down Approach" by James F. Kurose and Keith W. Ross: This book covers fundamental concepts of networking which are essential for designing and implementing network infrastructures.

### 2. Online Resources:

- \*Cisco Design Zone\*: Offers detailed guides and best practices for designing various types of networks.

(<https://www.cisco.com/c/en/us/solutions/enterprise/design-zone.html>)

- \*GNS3 Documentation\*: Comprehensive documentation and tutorials for using GNS3 to simulate network topologies.

[GNS3 Documentation](<https://docs.gns3.com/>)

### 3. Courses:

- Cisco Networking Academy: Provides courses on routing, switching, and network design.

[Cisco Networking Academy](<https://www.netacad.com/>)

## Network Security and Attacks

### 1. Books:

- "Network Security Essentials: Applications and Standards" by William Stallings: This book covers various aspects of network security, including attack methods and defense mechanisms.

- "Hacking: The Art of Exploitation" by Jon Erickson: Provides a deep dive into different types of attacks and how they can be executed and mitigated.

### 2. Online Resources:

- Kali Linux Documentation: Kali Linux is a popular platform for penetration testing, and its documentation includes tutorials on various attacks.

[Kali Linux Documentation](<https://www.kali.org/docs>)