CHAPTER 1

INTRODUCTION

Computer networks are a system of interconnected computers for the purpose of sharing digital information. A computer network is basically a set of devices connected through links. The simplest network is a combination of two computers connected by a cable. The network can share information easier and faster. Data is easy to back up as all the data is stored on the file server. A large network is complicated; therefore, it may require training and network management. Viruses can spread to other computers throughout a computer network. The project focuses on creating a model of the university's internal networking system (Intranet). An Intranet is a closed network used for sharing data, simplifying communication, providing collaboration tools, running operational systems, and offering other IT services within Campus. Its goal is to create a digital community and promote communication within the Campus. Intranets are built using LAN (Local Area Network), PTP (Point to Point Network) and WAN (Wide Area Network) technologies.

This Campus infrastructure was set up using devices like Firewall, Switches, Monitor, Customer Premises Equipment (CPE), CCTV, Servers and Access Point (AP) to share information and computing resources across campus networks. This project includes services like Internet access, Web Hosting, Domain Name System (DNS), and Monitoring System.

1.1 Objectives of the Project

A private network is constructed in this system. The main objectives of this project are listed below:

- To focus on creating a private network for internal use,
- To design easily information exchange and enhance communication within the campus,
- To know how to configure Firewall, Switches, CPE, CCTV, Zabbix, Server and Access Point, and
- To provide Internet access, Web hosting, DNS and Monitoring System.

1.2 Project Overview

In this project, Chapter 1 introduces the system and describes the objective of the project. Chapter 2 describes all of the theoretical backgrounds for the system. Chapter 3 includes the Project Design Diagram, requirements, and activities of the project. Chapter 4 includes Project Implementation. Chapter 5 includes a Conclusion and Further Extensions.

CHAPTER 2

THEORETICAL BACKGROUND

This chapter describes all of the theories needed to construct an intranet, monitoring and used for virtualization.

2.1 Theory Background of Intranet

The intranet is a private network. Its purpose is to build an online community and encourage communication within an organization. Therefore, everyone can easily access important information, links, applications, and others. An intranet may also consist of many interlinked local area networks (LANs) and leased lines connecting to wide area network resources.

2.1.1 Virtual Local Area Network (VLAN)

VLAN stands for Virtual Local Area Network and it is a common OSI layer 2 (Data Link Layer). A network is logically divided into logical network segments or virtual LANs. Each network segment (VLAN) is isolated from other segments (VLANs) and has its own broadcast domain. A VLAN is used to divide a large broadcast domain into multiple smaller broadcast domains. Management VLAN and default VLAN are used in this system.

2.1.2 VLAN Trunking Protocol (VTP)

VTP is a protocol used to distribute and synchronize identifying information about VLANs configured throughout a switched network. Configurations made to a single VTP server are propagated across trunk links to all connected switches in the network. VTP enables switched network solutions to scale to large sizes by reducing the manual configuration of the network. There are four VTP modes. They are client mode, server mode, and transparent mode. There are some requirements for VTP to communicate VLAN information between switches. These are:

- The VTP version must be the same as the configuration on the switches.
- VTP domain name must be the same on the switches.
- One of the switches must be a server.
- Authentication should match if applied.

2.1.3 Inter-VLAN Routing

Inter-VLAN routing is the ability to route or send traffic between VLANs that are normally blocked by default. Switches and VLAN work at the MAC address Layer (Layer 2). Traffic cannot be routed between VLANs at Layer 2 based on MAC addresses. There are two main ways to accomplish inter-VLAN routing:

- The router on a stick model and
- Layer 3 switch inter-VLAN routing.

Generally, a Layer 3 switch will be better performance and less latency than the router on a stick because the routing is handled in hardware instead of software with the Layer 3 switch vs the router.

2.1.4 Types of Switch Ports

A switch port can be in one of two modes: access and trunk. The access port can be assigned to a single VLAN. This type of interface is configured on switch ports that are connected to end devices. The trunk port is connected to another switch. This type of interface can carry traffic of multiple VLANs, thus enabling you to extend VLANs across your entire network.

2.1.5 EtherChannel

EtherChannel is a port link aggregation technology or port-channel architecture used primarily on Cisco switches. It allows the grouping of several physical Ethernet links to create one logical Ethernet link for the purpose of providing fault-tolerance and high-speed links between switches, routers, and servers. EtherChannel is primarily used in the backbone network, but can also be used to connect end-user machines.

2.1.6 Point to Point

A direct connection between two devices is known as point-to-point (P2P) communication. This can be accomplished by a variety of wired and wireless channels, including serial cables, fiber optics, and radio frequencies. Establishing a temporary communication link or connecting two places are common uses for this technique. Point-to-point communication is ideal for applications that demand high reliability and performance in a controlled environment since it is essential in scenarios where assured bandwidth and minimal latency between two endpoints are required. Despite its restricted scalability, its simple design provides strong security and efficiency, making

it essential for establishing direct and secure communication channels in a variety of technological domains.

2.2 Theory Background of Virtualization

Virtualization is the creation of a virtual version of something, such as an operating system (OS), a server, a storage device or network resources. Virtualization uses software that simulates hardware functionality to create a virtual system. This practice allows IT organizations to operate multiple operating systems, more than one virtual system, and various applications on a single server.

2.2.1 Virtual Private Server (VPS)

A virtual private server, also known as a VPS, acts as an isolated, virtual environment on a physical server, which is owned and operated by a cloud or web hosting provider. VPS hosting uses virtualization technology to split a single physical machine into multiple private server environments that share the resources.

2.3 Monitoring

It enables network administrators to detect potential problems early through customizable alerts and detailed data analysis, ensuring optimal network performance and reduced downtime. We used Zabbix tool for monitoring.

2.3.1 About of Zabbix

Zabbix is an open-source monitoring tool designed to track the performance and availability of IT infrastructure, including servers, networks, and applications. It provides real-time monitoring, alerting, and data visualization through dashboards and reports. Zabbix supports a wide range of data collection methods and can be easily integrated with third-party systems. It is scalable, suitable for both small and large environments, and is widely used for proactive monitoring to ensure system reliability and performance.

2.3.2 Zabbix Support

Zabbix support in a Zabbix server includes both official and community resources to ensure effective monitoring. Official support offers paid services with technical assistance, troubleshooting, and. Community support is available through

forums and user groups. Zabbix also provides extensive documentation and supports various protocols like SNMP and IPMI, along with integration through APIs and Zabbix agents. Paid support guarantees timely help, while the community and documentation help with best practices and troubleshooting.

2.3.3 SNMP

SNMP (Simple Network Management Protocol) is a widely used protocol in network management that allows administrators to monitor and control network devices such as routers, switches, and servers. It operates by using a centralized SNMP manager, which communicates with SNMP agents installed on the managed devices. These agents collect data and store it in a structured database called the Management Information Base (MIB), with each piece of data identified by a unique Object Identifier (OID). SNMP supports various operations like polling for data, sending alerts (traps) when specific events occur, and setting configurations on devices. There are three versions of SNMP—v1, v2c, and v3—with SNMPv3 offering enhanced security features. SNMP is crucial for effective network performance monitoring, fault detection, and remote management, although it can present challenges in terms of security and complexity in large networks.

2.3.4 Zabbix Agent

The Zabbix Agent is a key component of the Zabbix monitoring system, which is designed to gather data from the monitored hosts and send it to the Zabbix Server for processing. Installed on each device or server that needs to be monitored, the agent collects detailed metrics such as CPU usage, memory consumption, disk space, and network traffic. It can perform both passive checks, where the server requests data, and active checks, where the agent sends data to the server periodically. The Zabbix Agent is highly configurable, allowing for custom monitoring of specific applications, services, or scripts. This makes it an essential tool for maintaining the performance, availability, and health of IT infrastructure in a Zabbix-managed environment.

2.3.5 SMTP

SMTP (Simple Mail Transfer Protocol) is the standard protocol used for sending emails across the Internet. It defines how email messages are sent from a mail client (such as Outlook or Gmail) to a mail server. Then it relayed from one server to another

until it reaches the recipient's mail server. SMTP is primarily used for sending outgoing emails from a client to a server or from one server to another. It does not handle the retrieval of emails; that task is managed by protocols like IMAP or POP3. SMTP typically uses port 25 for standard communication, but ports 587 or 465 are often used for sending emails securely via encryption (TLS/SSL).

2.3.6 IMAP

IMAP (Internet Message Access Protocol) is a standard protocol used for retrieving and managing email messages from a mail server. Unlike POP3 (Post Office Protocol version 3), which downloads emails and often removes them from the server, IMAP allows users to access and manage their emails directly on the server, providing more flexibility and synchronization across multiple devices.

CHAPTER 3

PROJECT DESIGN AND REQUIREMENTS

This chapter describes the designs to achieve the desired project goals and requirements to implement this project.

3.1 Smart Campus Infrastructure

A Smart campus infrastructure was built through this network trainer board. This network trainer board was divided into four parts with two sites, such as server and client. The first is the server area where networks can be accessed, distributed, and controlled. The second area is the classroom area in which students and teachers can access the necessary internet connection for teaching and learning from the distributed network. The third area is the monitoring area in which networks traffic and devices' utilizations can manage and troubleshoot. And, the last area is client area where it is difficult to provide ethernet or fiber cable.

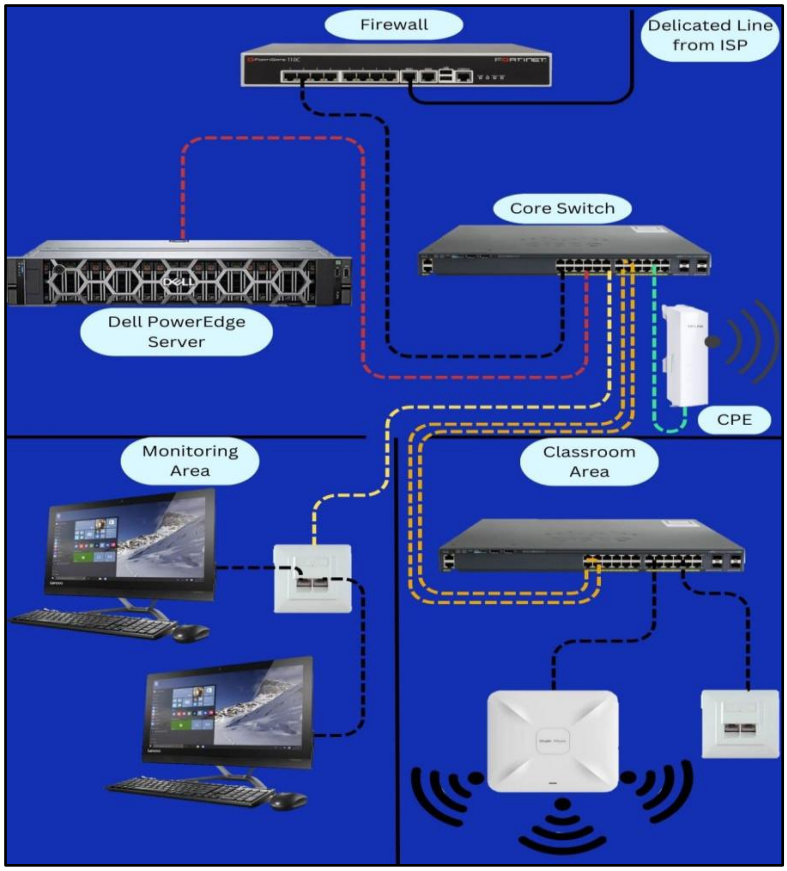


Figure 3.1(a) Physical Diagram of Server Site area in Smart Campus Infrastructure

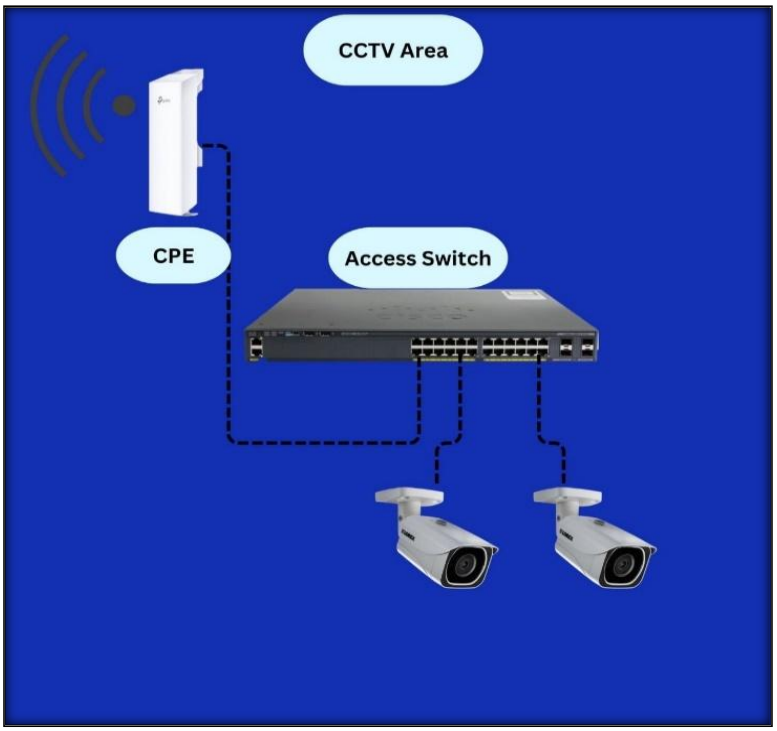


Figure 3.1(b) Physical Diagram of Client Site in Smart area Campus Infrastructure

Figure 3.1(a) and (b) express the actual physical arrangement of the network devices. Firewall, Core Switch, Access Switch, Server, Closed-circuit Television (CCTV), Monitor, and Access Point are used in this system. A firewall is used not only to connect the internal network and the external network but also to monitor incoming and outgoing network traffic and permit or block data packets based on a set of security rules. A Core Switch is used to route network traffic and switch data at the core layer of the network. Access Switches are used to ensure the routing of data to access devices. A Server is used to provide services. Access Points are used to extend the wireless coverage of an existing network and increase the number of users that can connect to it. Closed-circuit Television (CCTV) is used to record images, and videos and to keep track of what is happening at a time. In this project, Monitor are used to record security video and observe network traffic and devices' status. And, CPE are used to acts as the receiver and transmitter, enabling direct communication between two locations.

There are some processes in designing Smart Campus Infrastructure:

- Accessing an internet connection from ISP to Local Area Network using Fiber Optic Cable or Microwave,
- Managing Local Area Networks including VLANs, and providing services,
- Distributing network connections from the server area to other areas for the influence of intranet access in the Campus area,

- Accessing distributed network connections from the server area and providing services to end devices,
- Monitoring network traffic and devices' utilization within the whole system.

These processes are designed in detail as shown in figure 3.2.

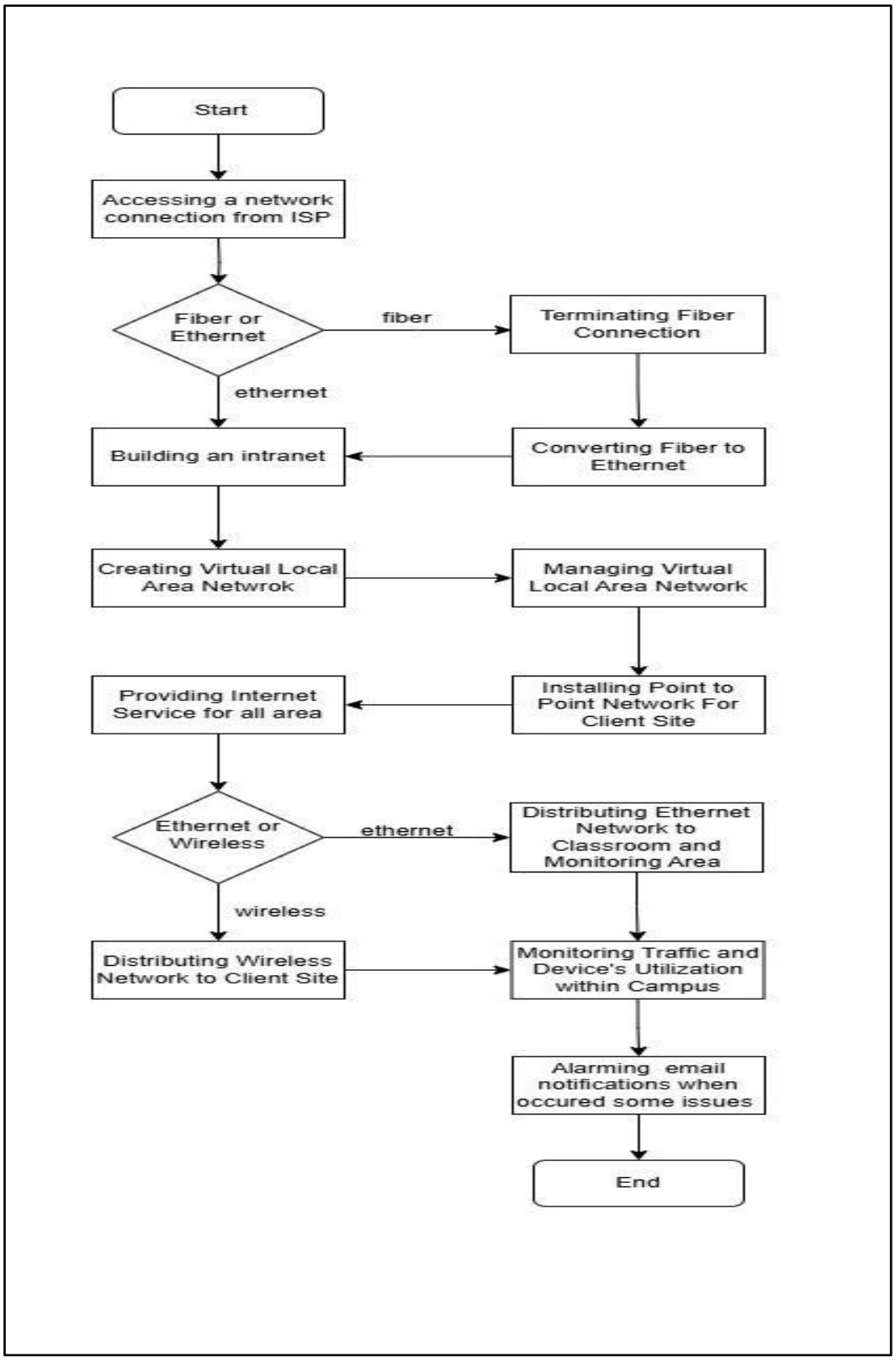


Figure 3.2(a) Flowchart of Server Site area

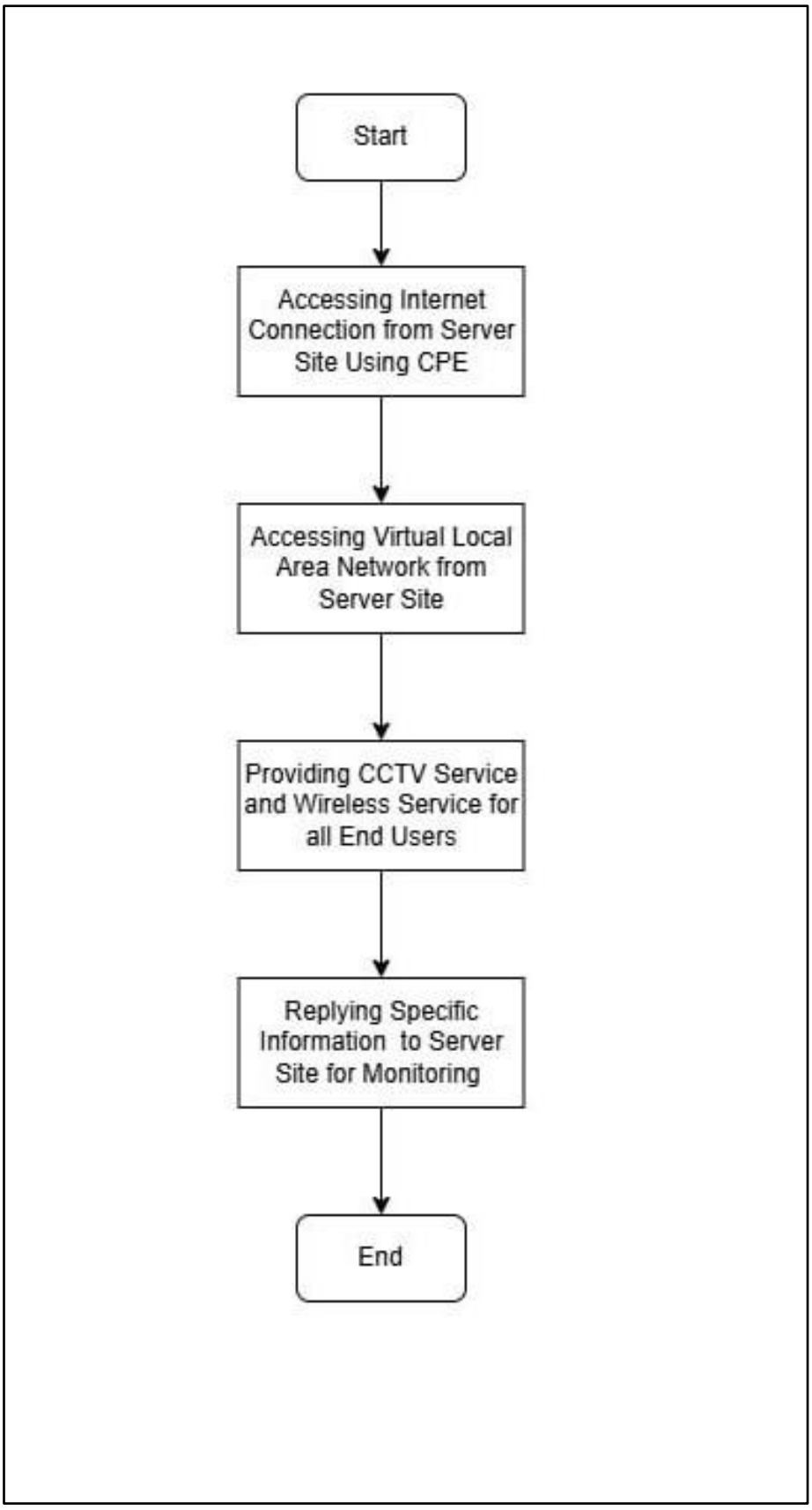


Figure 3.2(b) Flowchart of Client Site area

3.2 Project Schedule

No	Works Done	1st week	2nd week	3rd week	4th week	5th week	6th week	7th week	8th week	9th week
1	Resource Allocation									
2	Hardware Testing									
3	Device Configuration									
4	Project Board Creation									
5	Device Installation									
6	Testing									
7	Modifying Project									
8	Server Installation									
9	Testing Services									
10	Documentation									

Figure 3.3 Gantt Chart

Figure 3.3 presents overview activities of the project, “Smart Campus Infrastructure”.

In the first two weeks of our project duration, we studied the necessary theory for the project and discussed resource needs with colleagues. We identified the resources needed for each activity and resource type. We collected the necessary devices and accessories for the project from the hardware lab and server room.

In third week, we checked whether each collected item is working properly such as Switches, firewalls, servers, CPE, CCTV, and adapters.

In fourth week, we configured the network devices mentioned above.

In fifth and sixth weeks, we drew the design of the system with Drawio. Then, we created a network trainer board by identifying the position of the devices on the board. And then, we installed the devices on the network trainer board. After the equipment had been installed, we checked these devices over and over again that are actually working.

In seventh and eighth weeks, we modify the project and start the server installation and testing services.

In the last week, we prepared our system documentation.

3.3 Hardware Requirements

The required devices in this system are switches, routers, firewalls, servers, CCTV, and access points. The detailed information on these devices is as follows.

3.3.1 Firewall

Figure 3.4 FortiGate 110C

Figure 3.4 describes a Firewall FortiGate 110C that is used for security. A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. It typically establishes a barrier between a trusted network and an untrusted network, such as the Internet. It combines firewall, IPSec and SSL VPN, intrusion prevention, antivirus, antimalware, antispam, P2P security, and web filtering to identify numerous types of threats from a single device.

3.3.2 Core Switch

Figure 3.5 WS-C 3650-24TS-S v04

Figure 3.5 shows the Cisco Catalyst 3650 Series Switch. This is used as a core switch for this system. The data routed and switched by the core switch is carried forward to the bottom layers of the network such as the distribution and access layers. This means the performance of the entire network relies on the data routed and switched by the core switch. WS-C 3650-24TS-S integrates with 24 Ethernet ports and 4 x 1G SFP uplink ports in the IP Base feature set.

3.3.3 Access Switch (Classroom)

Figure 3.6 WS-C 2960-24TS-S v04

Figure 3.6 shows the Cisco Catalyst 2960 Series Switch. This is used as a distribution switch for this system. These switches are installed at the distribution layer of the hierarchy network. These switches bridge the core layer and access layer. The main responsibility of these switches is to ensure the routing of data to correct devices in the access layer. Cisco Catalyst 2960 series switches support these common features such as authentication, access control, security policy administration, multiple Fast or

Gigabit Ethernet performance options, power management, and scalable network management.

3.3.4 Access Switch (CCTV site)

Figure 3.7 WS-C2960G-48TC-L 48 Port

Figure 3.7 shows the Cisco Catalyst 2960 Series Switch. This is used as a distribution switch for this system. These switches are installed at the distribution layer of the hierarchy network. These switches bridge the core layer and access layer. The main responsibility of these switches is to ensure the routing of data to correct devices in the access layer. Cisco Catalyst 2960 series switches support these common features such as authentication, access control, security policy administration, multiple Fast or Gigabit Ethernet performance options, power management, and scalable network management.

3.3.5 Server

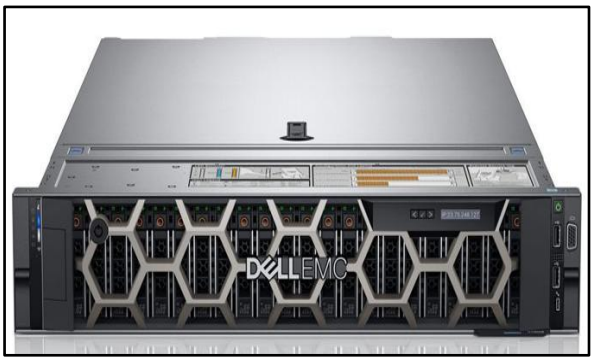


Figure 3.8 Dell PowerEdge R740 Server

Figure 3.8 shows the Server that is used for virtualization in this system. A server is a computer program or device that provides a service to another computer program and its user, also known as the client. In a data center, the physical computer that a server program runs on is also frequently referred to as a server. Dell PowerEdge

R740 servers were designed to accelerate application performance by leveraging accelerator cards and storage scalability.

3.3.6 Console Cable

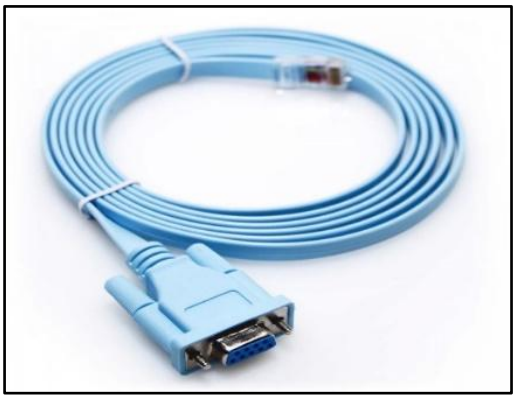


Figure 3.9 Console Cable

Figure 3.9 shows the Console cables also known as Cisco cables, rollover cables and, management cables. They connect Cisco networking devices to terminals or PCs for configuration.

3.3.7 Ruijie | Reyee RG-RAP 2260

Figure 3.10 Ruijie | Reyee RG-RAP 2260

Figure 3.10 shows Ruijie | Reyee RG-RAP2260(G), it is a high-performance ceiling-mounted wireless access point designed for indoor environments, offering robust specifications for enterprise networks. It supports the latest Wi-Fi 6 (802.11ax) standard, providing speeds up to 3.55 Gbps across both 2.4GHz and 5GHz bands. The device is equipped with 4 spatial streams and MU-MIMO technology, allowing simultaneous communication with multiple clients, enhancing network efficiency. It has dual-band support, a Gigabit Ethernet port, and PoE (Power over Ethernet) for flexible installation. The RG-RAP2260(G) is ideal for high-density environments like

schools and offices, with advanced security features and easy cloud-based management via the Ruijie Cloud platform.

3.3.8 TP-Link CPE 210

Figure 3.11 TP-Link CPE 210

The TP-Link CPE210 is a cost-effective, high-performance wireless CPE (Customer Premises Equipment) designed for point-to-point and point-to-multipoint applications. It operates on the 2.4GHz band and provides up to 300Mbps of wireless throughput, making it ideal for establishing stable and reliable connections over distances of up to 5 kilometers (3 miles). Featuring a 12dBi directional antenna, the CPE210 is optimized for long-range coverage and minimal signal interference. Its robust weatherproof design ensures reliable performance in various outdoor environments, while its flexible mounting options and easy-to-configure settings make it a practical solution for extending network connectivity or bridging remote locations.

3.3.9 Power over Ethernet (PoE) Adapter

Figure 3.12 Ubiquiti POE Adapter

Figure 3.12 shows an adapter that can power UniFi PoE devices with wireless mesh applications, or offload PoE switch power dependencies.

3.3.10 Adapter (12V 1A)

Figure 3.13 Adapter(12V 1A)

Figure 3.13 shows 12V 1A adapter provides a reliable and steady power supply for low-power electronic devices. Its compact design makes it easy to use and store while ensuring efficient performance.

3.3.11 Network Camera

Figure 3.14 Hikvision DS-2CD2T43G0-I5

The Hikvision DS-2CD2T43G0-I5 is a high-resolution 4MP outdoor security camera designed to deliver clear and detailed surveillance footage. It features a 4mm fixed lens for a broad field of view and is equipped with infrared LEDs for effective night vision up to 50 meters. With its IP67 weatherproof rating, the camera is durable and reliable in various environmental conditions. Additionally, it includes advanced image enhancement technologies like WDR and 3D DNR to ensure high-quality footage even in challenging lighting situations, making it a versatile choice for both residential and commercial security needs.

3.4 Addressing Table

Table 1 Addressing Table

Serial No	Type	Host-name	Interface	VLAN	IP Address	Subnet Mask
1	Firewall (FortiGate 110C)	FW	Wan 1		192.168.20.88 (DHCP)	255.255.252.0
			Switch port 1		10.10.11.89	255.0.0.0
2	Core Switch (WS-C 3650-24TS-S v04)	CoSW	G1/0/1		10.10.11.254	255.0.0.0
				VLAN 7	7.10.10.2	255.0.0.0
				VLAN 10	10.10.10.2	255.0.0.0
				VLAN 20	20.10.10.2	255.0.0.0
				VLAN 30	20.10.10.2	255.0.0.0
			MGMT		192.168.1.1	255.255.255.0
3	Access Switch for Classroom (WS-C 3650-48TS-S v04)	AccSW1			10.10.11.254	255.0.0.0
				VLAN 30	30.10.10.4	255.0.0.0
			MGMT		192.168.1.1	255.255.255.0
4	Access Switch for CCTV (WS - C 3650-48TS-S v04)	AccSW2		VLAN 20	20.10.10.4	255.0.0.0
			MGMT		192.168.1.1	255.255.255.0

3.5 Estimated Cost List

Table 2 Estimated Cost

No	Device Model	Qty	Price (USD)	Total Price (USD)
1	FortiGate 110C	1	6300	6300
2	WS-C 3650-24TS-S	1	4500	4500
3	WS-C 3650-48TS-S	1	4800	4800
4	Reyee RAP-2260	2	300	600
5	Hikvision CCTV	1	200.61	200.61
6	cat 6 RJ 45 modular plug (100pcs)	1	20	20
7	pro cat 6 cable 304M Network cable box	1	200.59	200.59
8	TRENDnetRJ-11/RJ-45 Crimp/Cut/Strip Tool	1	30.5	30.5
9	RJ 45 cable tester	1	11	11
10	RJ45 Cat 6 outlet keystone faceplate	2	15.45	30.9
11	Electric Wire	8m	3.5	24
12	Electric Drill Set	1	30	30
13	Dell Power Edge R740	1	45000	65000
14	Lenovo 22” Monitor	2	150	300
Total				**81747.6**

3.6 Software Requirements

The software required for this system are GNS 3 for network simulation, Ruijie Cloud for Access Point configuration, Linux Server for monitoring, Hik-Connect for CCTV, VMware ESXi for server virtualization, and Microsoft Windows Server 2022 for Web Hosting, DHCP and DNS Service.

3.6.1 Graphical Network Simulator 3

GNS3 (Graphical Network Simulator 3) is a network simulation software used by network professionals, students, and engineers to design, configure, test, and troubleshoot complex network topologies. GNS3 allows users to simulate real network devices such as routers, switches, and firewalls in a virtual environment. This is useful for learning, testing configurations, and preparing for certifications like Cisco CCNA or CCNP. The following links are used to install and guide GNS3 Software.

GNS3 Documentation | GNS3 Documentation

GNS3 | The software that empowers network professionals

3.6.2 Linux Server (Ubuntu Server)

A Linux server is a powerful, versatile system used to provide various services and functions in IT infrastructure. Its primary role is to host applications and services in a reliable, secure, and scalable manner. And, it is versatile and robust platforms used across many industries for a variety of essential services, including hosting websites, applications, databases, and managing network functions securely and efficiently.

https://ubuntu.com/download/server

Ubuntu Server documentation | Ubuntu

3.6.3 VMware ESXi

VMware ESXi, also called VMware ESXi Server, is a bare-metal hypervisor developed by VMware for vSphere. ESXi is one of the primary components in the VMware infrastructure software suite. ESXi is a Type 1 hypervisor, meaning it runs directly on system hardware without the need for an OS. Hypervisors help run multiple VMs efficiently on a physical server. The following links are used to install and guide VMware ESXi Software.

https://customerconnect.vmware.com/downloads/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/6_5

https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-B64AA6D3-40A1-4E3E-B03C-94AD2E95C9F5.html

3.6.4 Microsoft Windows Server 2022

Windows Server is a group of operating systems designed by Microsoft that supports enterprise-level management, data storage, applications, and communications. It was specifically developed to serve as a platform for running networked applications. The following links are used to install and guide Windows Server.

Windows Server 2022 | Microsoft Evaluation Center

Windows Server documentation | Microsoft Learn

3.6.5 Ruijie Cloud

Ruijie Cloud is a cloud-based network management platform designed for managing, monitoring, and configuring network devices, primarily those from Ruijie Networks. It provides a centralized, scalable solution for IT administrators to oversee and control network infrastructures. It also helps simplify network management, increases efficiency, and provides enhanced visibility for IT administrators, particularly in environments with multiple sites or large numbers of devices.

Log in to Ruijie Cloud (ruijienetworks.com)

Ruijie | Reyee —— Redefine Your Easy Network (youtube.com)

3.6.6 Hik-Connect

Hik-Connect is a cloud-based service provided by Hikvision, designed to facilitate the remote access and management of Hikvision video surveillance devices. Hik-Connect enhances the usability and functionality of Hikvision's video surveillance systems by offering convenient remote access, comprehensive device management, and robust alerting and notification features, all through an easy-to-use cloud platform.

https://www.hik-connect.com

Hik-Connect - Software – Hikvision

CHAPTER 4

IMPLEMENTATION OF SMART CAMPUS INFRASTRUCTURE

This chapter describes the implementation process to the completion of this University Campus Intranet.

4.1 Configuring Network Devices

Network configuration is the process of setting a network's controls, flow and operation to support the network communication of the Smart Campus Infrastructure. We used all of user name and password within this project are "wkmy" and "*123*wkmy#". The following configurations are used in this project.

4.1.1 Configuring FortiGate Firewall

```
FortiFirewall-VM64 # config system admin

FortiFirewall-VM64 (admin) # edit admin

FortiFirewall-VM64 (admin) # set password *123*wkmy#

FortiFirewall-VM64 (admin) # next

FortiFirewall-VM64 (admin) # end
exit

FortiFirewall-VM64 login: admin
Password:
Welcome!

FortiFirewall-VM64 # _
```

Figure 4.1 Configuring username and password for FortiGate Firewall.

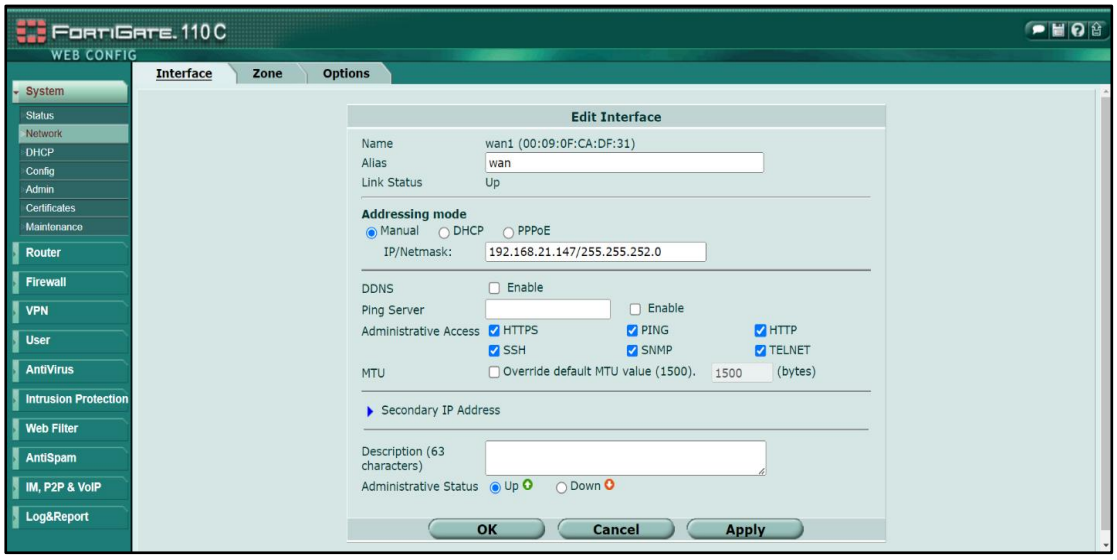


Figure 4.2 Assigning public IP for Intranet in FortiGate Firewall.

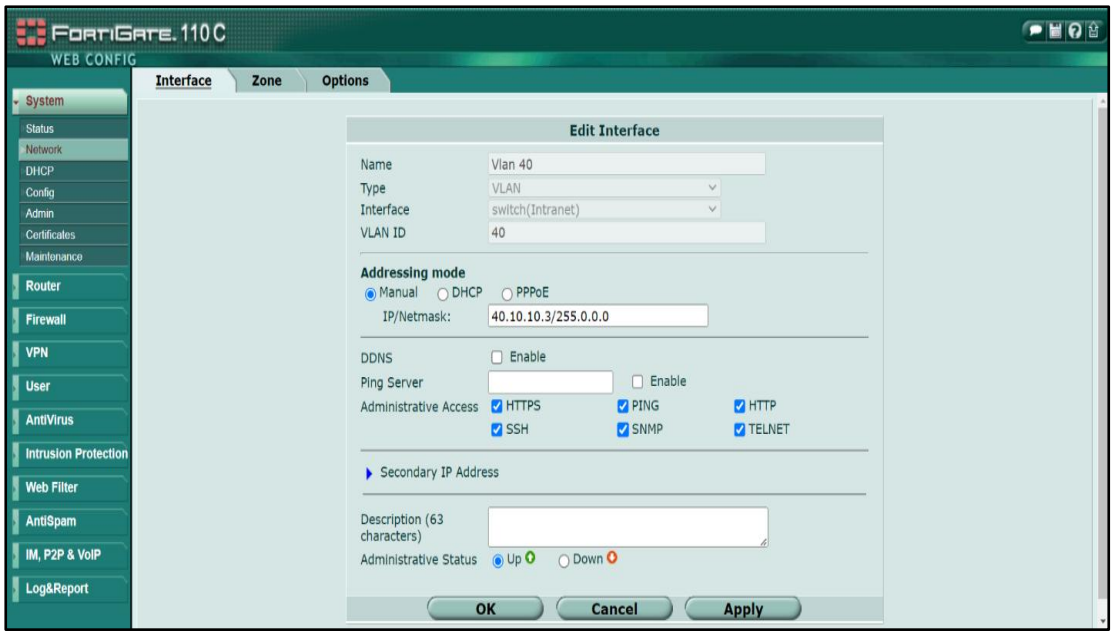


Figure 4.3 Configuring VLAN Interface in FortiGate Firewall

In figure, to create a VLAN on a FortiGate firewall using the web UI, follow these steps:

Step-1: Open a web browser and log in to the FortiGate firewall's web interface to login.

Step-2: Navigate to VLAN Settings:

- Go to the “Network section” in the left-hand menu.
- Click on “Interfaces”.

Step-3: Add a New VLAN:

- Click the “Create New button”.
- Select “Interface” from the dropdown menu.

Step-4: Configure VLAN Settings:

- Type: Select “VLAN”.
- Name: Enter a “descriptive name” for the VLAN.
- VLAN ID: Enter the “VLAN ID” (a number between 1 and 4094).
- Interface: Choose the “physical interface” to which the VLAN will be associated.
- Addressing Mode: Set to either “Manual or DHCP” depending on your network setup. If Manual, specify the IP address and subnet mask.

Step-5: Apply and Save:

- Click “OK” to save the VLAN configuration.

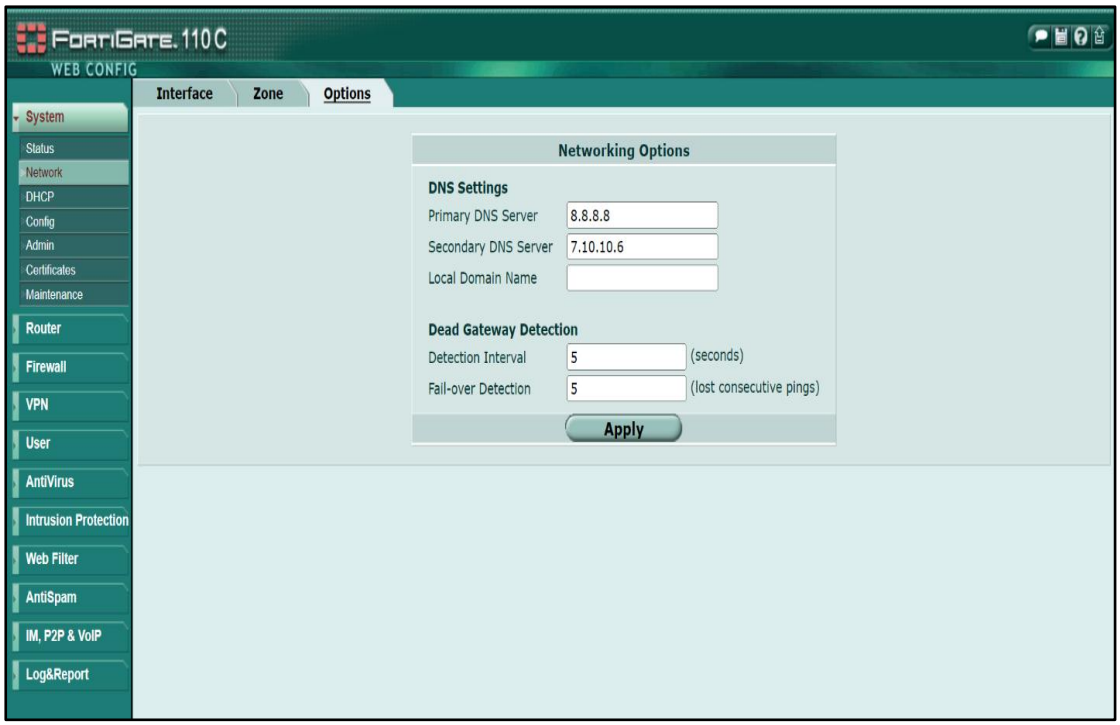


Figure 4.4 Configuring DNS Setting

Figure 4.5 Routing to Internet in FortiGate Firewall

Figure 4.5 shows configuring to control how network traffic is directed between different networks or subnets. Routes define the path that data packets take to reach their destination and are crucial for proper network functionality.

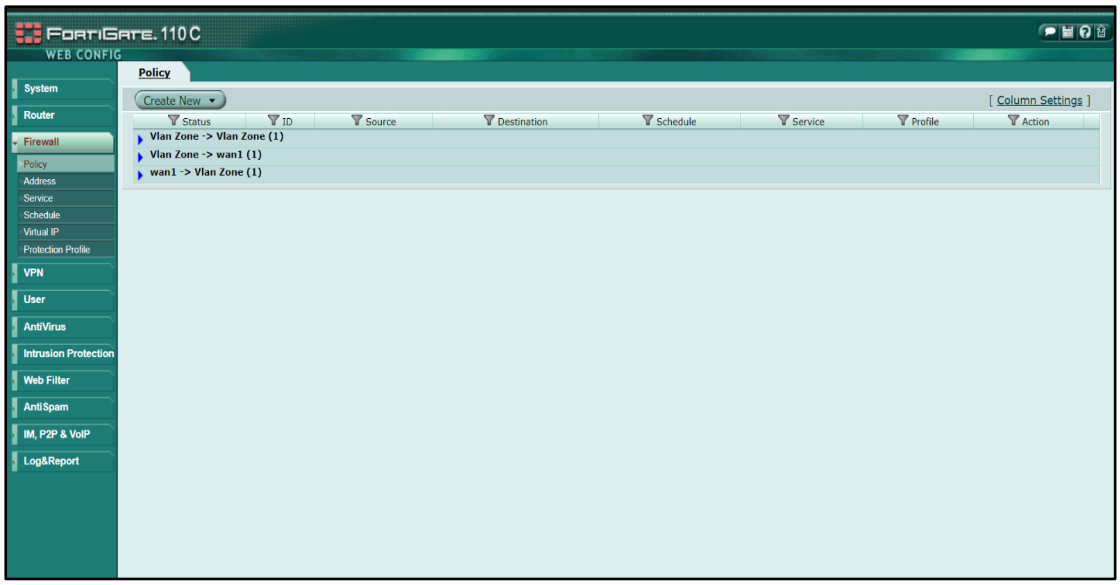


Figure 4.6 Policies control in FortiGate Firewall

Figure 4.6 shows controlling and managing the flow of traffic between different network interfaces, such as between internal networks, the DMZ, and the internet. These policies define rules that specify which traffic is allowed or denied based on various criteria.

4.1.2 Configuring Network Switches

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname CoSW
CoSW(config)#enable password *123*wkmy#
CoSW(config)#
CoSW(config)#username wkmy password *123*wkmy#
CoSW(config)#ip domain-name www.cisco.com
CoSW(config)#crypto key generate rsa
The name for the keys will be: CoSW.www.cisco.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

CoSW(config)#line vty 0 4
*Mar 1 0:5:15.662: %SSH-5-ENABLED: SSH 1.99 has been enabled
CoSW(config-line)#password *123*wkmy#
CoSW(config-line)#login local
CoSW(config-line)#transport input ssh
CoSW(config-line)#exit
CoSW(config)#
```

Figure 4.7 Configuring Hostname and password for Network Switches

Figure 4.7 shows configuring hostname and enable password for privileged mode and secure socket shell (SSH) with encryption. These commands are used in Core Switch and Distribution Switches.

```
CoSW(config)#
CoSW(config)#vlan 7
CoSW(config-vlan)#name ServerAndMonitoring
CoSW(config-vlan)#exit
CoSW(config)#vlan 10
CoSW(config-vlan)#name AccessPoint
CoSW(config-vlan)#exit
CoSW(config)#vlan 20
CoSW(config-vlan)#name CCTV
CoSW(config-vlan)#exit
CoSW(config)#vlan 30
CoSW(config-vlan)#name Classroom
CoSW(config-vlan)#exit
CoSW(config)#
```

Figure 4.8 Configuring VLAN for each area

```
CoSW(config)#int vlan 7
CoSW(config-if)#
%LINK-5-CHANGED: Interface Vlan7, changed state to up

CoSW(config-if)#ip address 7.10.10.2 255.0.0.0
CoSW(config-if)#ip helper-address 7.10.10.6
CoSW(config-if)#exit
CoSW(config)#int vlan 10
CoSW(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

CoSW(config-if)#ip address 10.10.10.2 255.0.0.0
CoSW(config-if)#ip helper-address 7.10.10.6
CoSW(config-if)#exit
CoSW(config)#int vlan 20
CoSW(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

CoSW(config-if)#ip address 20.10.10.2 255.0.0.0
CoSW(config-if)#ip helper-address 7.10.10.6
CoSW(config-if)#exit
CoSW(config)#int vlan 30
CoSW(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

CoSW(config-if)#ip address 30.10.10.2 255.0.0.0
CoSW(config-if)#ip helper-address 7.10.10.6
CoSW(config-if)#exit
```

Figure 4.9 Configuring VLAN interface, IP Address and IP helper-address for DHCP

```
CoSW(config)#
CoSW(config)#interface fa0/1
CoSW(config-if)#switchport mode trunk
CoSW(config-if)#switch trunk allowed vlan all
CoSW(config-if)#exit
CoSW(config)#interface port-channel 2
CoSW(config-if)#exit
CoSW(config)#interface range fa0/23-24
CoSW(config-if-range)#channel-group 2 mode active
```

Figure 4.10 Configuring trunk port and EtherChannel

4.1.3 Configuring CPE Access Point for Point to Point

At first, login as username “admin” and password “admin123” via web broswer.

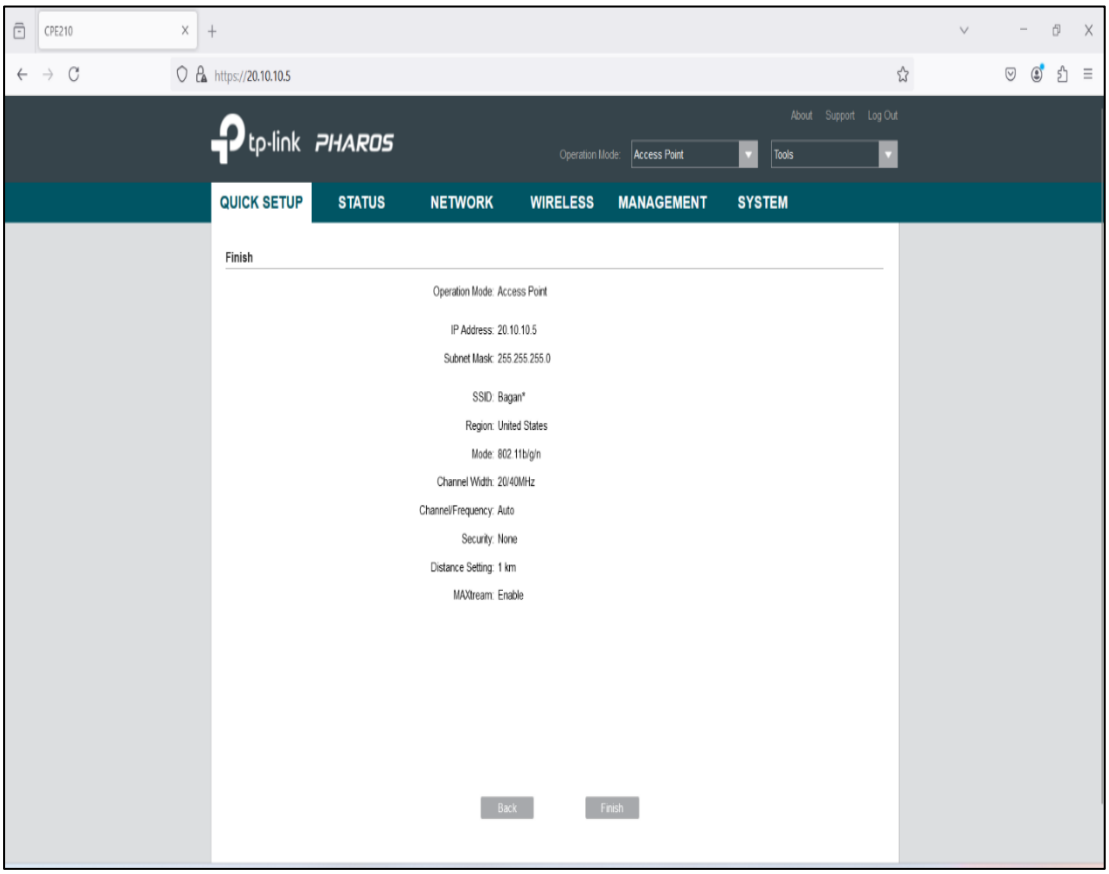


Figure 4.11 Configuring CPE (Server Site)

In the Configuring CPE (Server Site), the admin can do the following steps.

Step-1: Mode Selection:

- The admin clicks “navigates to Wireless”. Then he must choose “Operation Mode”.
- Set the first CPE to Access Point.

Step-2: Wireless Settings:

- Set the Channel Width to 20 MHz (for better stability).
- Choose a channel, or leave it on Auto.
- Set a SSID (network name).

Step-3: Security:

- Enable WPA2-PSK security and set a strong password.

Step-4: Save the settings and reboot the device if prompted.

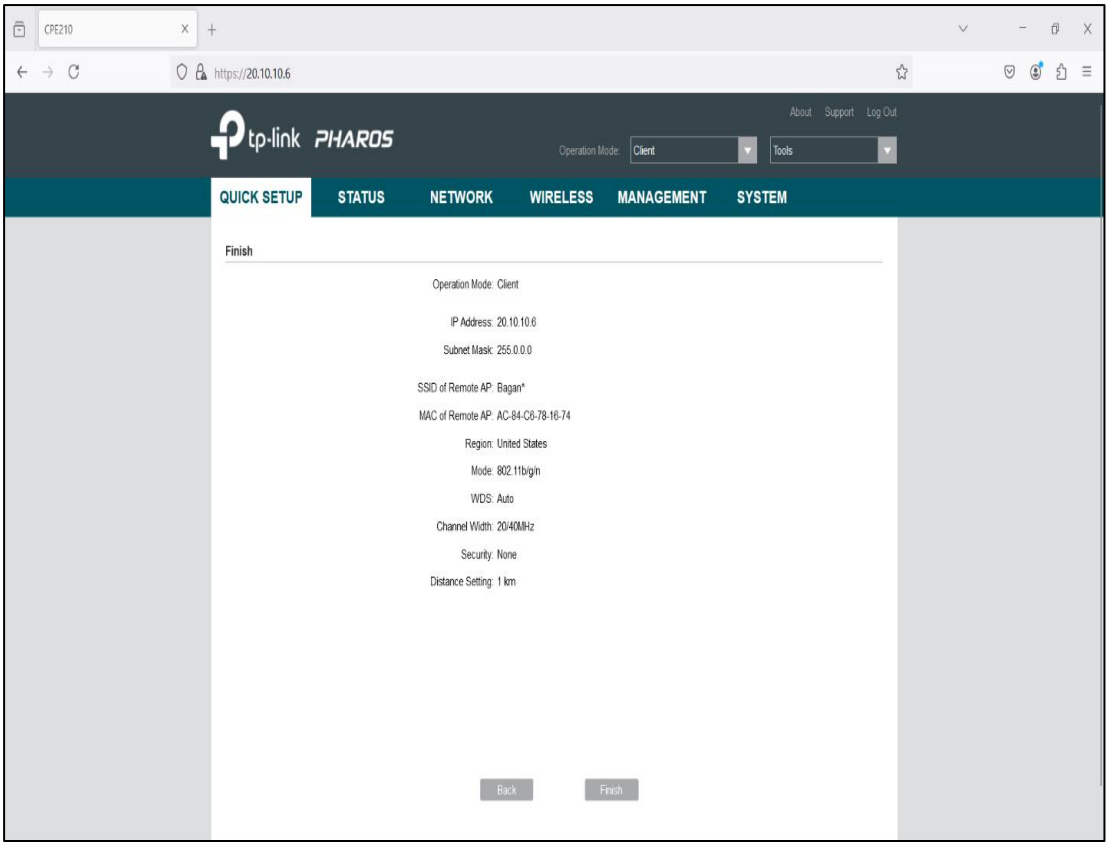


Figure 4.12 Configuring CPE (Client Site)

In the Configuring CPE (Client Site), the admin can do the following steps.

Step-1: Mode Selection:

- On the second CPE, set the Operation Mode to Client.

Step-2: Wireless Settings:

- Under Wireless Settings, click on Survey to find the Access Point (SSID) you just configured.
- Select the correct SSID and connect.

Step-3: Security:

- Enter the same WPA2-PSK password used in the Access Point setup.

Step-4: Save the settings and reboot.

4.1.4 Configuring Hikvision DS-2CD2T43G0-I5

Firstly, type default IP of Hikvision DS-2CD2T43G0-I5 via the search bar of web browser and login as default username and password.

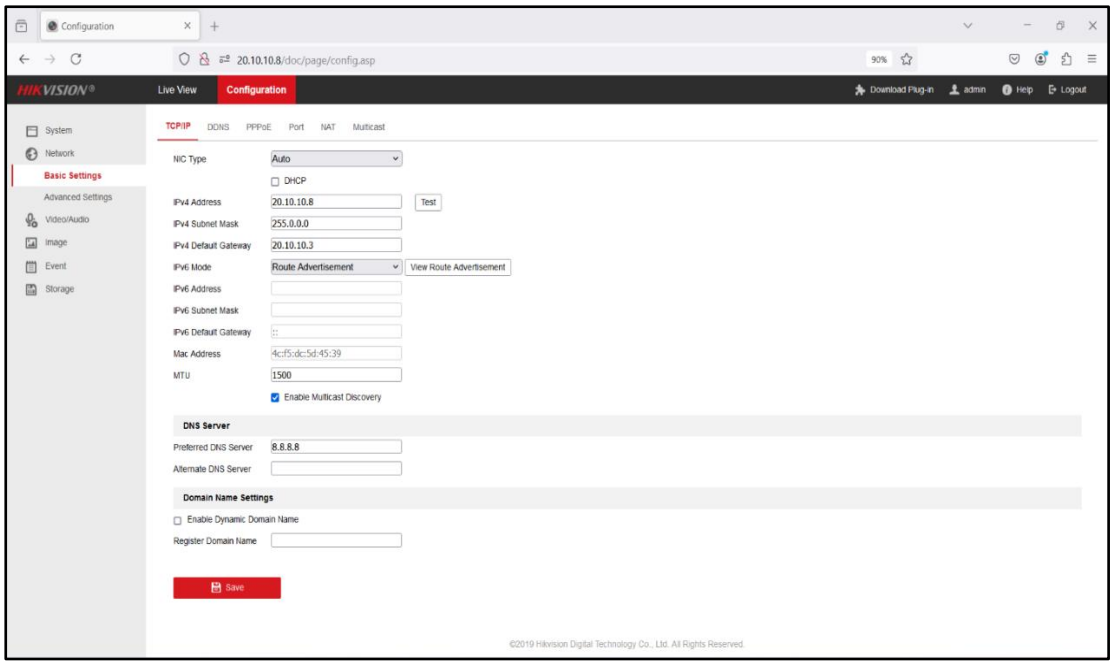


Figure 4.13 Configuring Hikvision Network Camera

4.2 Installation of Windows Server and Hosting a welcome web page

The following steps are how to make web hosting on Dell PowerEdge R740.

Step 1: Installing VMware ESXi on Dell PowerEdge R740,

Step 2: Accessing VMware ESXi using VSphere Client,

Step 3: Installing Windows Server 2022 on VMware ESXi.

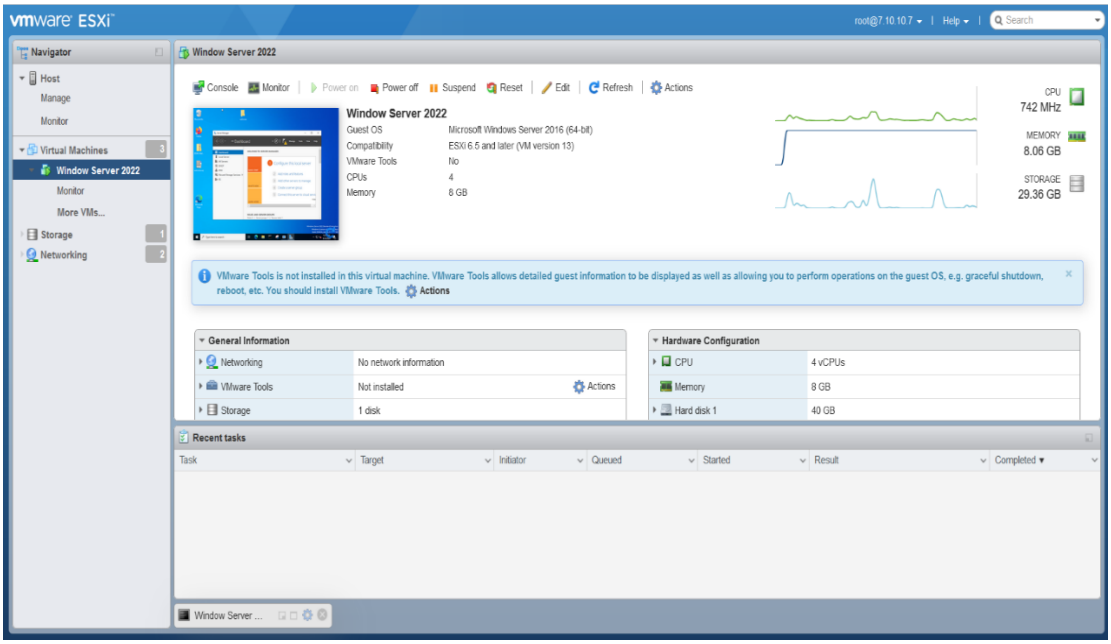


Figure 4.14 Accessing Windows Server 2022 in VMware ESXi

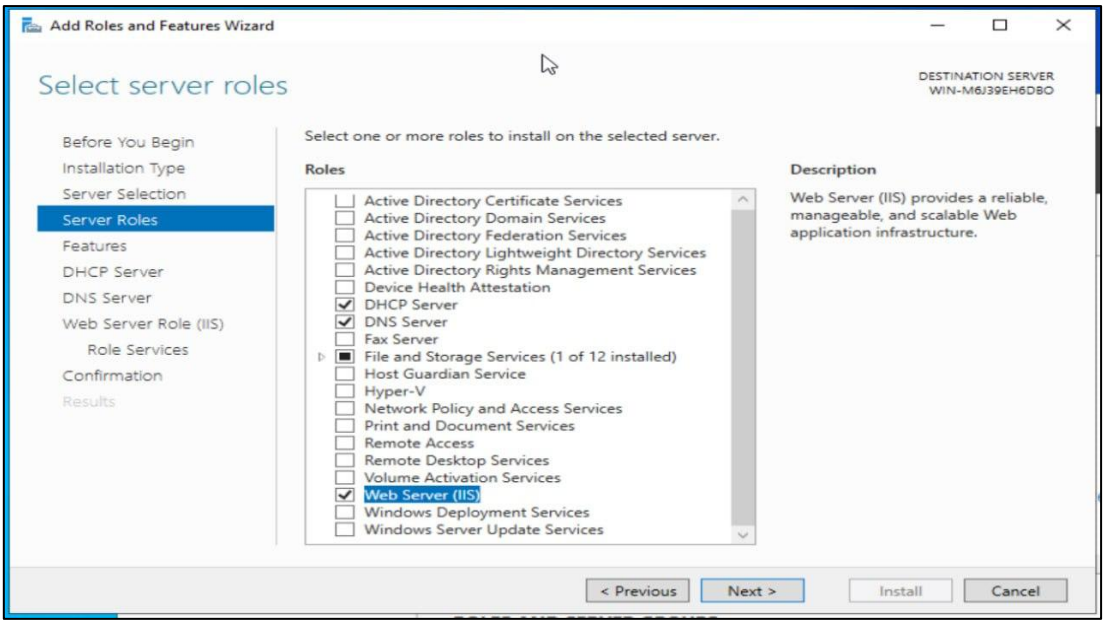


Figure 4.15 Adding Roles and Features in Windows Server 2022

4.2.1 Configuring DHCP Server

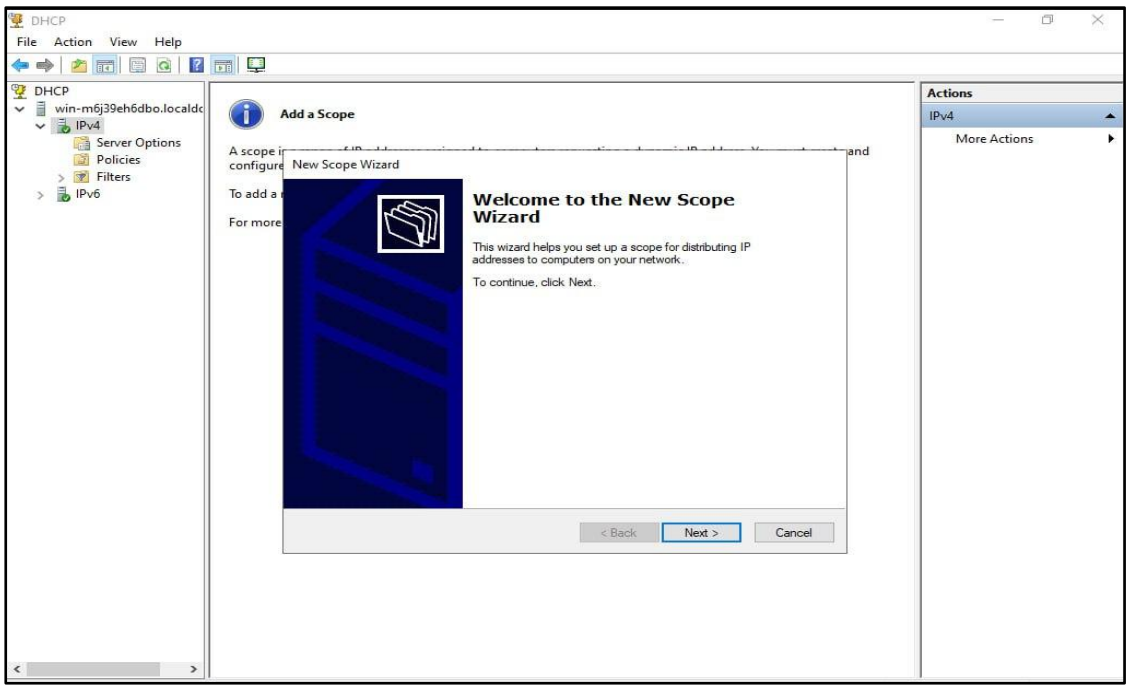


Figure 4.16(a) Configuration of DHCP Server

In the Configuring of DHCP Server, the admin can do the following steps.

Step-1: Create a new DHCP Scope:

- Click “Next” on the Welcome screen.
- “Scope Name” provides a name and description for your scope and click “Next”.

- “IP Address Range” defines the IP range that will be used by the DHCP server. Provide the start and end IP addresses, then click “Next”.
- “Length and Subnet Mask” enters the subnet length or mask, and click “Next”.
- “Add Exclusions and Delay”: If there are any IP addresses within the range that you want to exclude (for example, reserved IPs), add them here. Click “Next”.
- “Lease Duration” sets the lease duration (default is 8 days). Click “Next”.
- “Configure DHCP Options” can either configure DHCP options now or later. For now, select “Yes “and click “Next”.

Step-2: Configure DHCP Options:

- “Router (Default Gateway)” provides the default gateway address for your network and click “Next”.
- “The domain name and DNS server IP addresses” for your network is extended in “Domain Name and DNS Servers”. Click “Next”.
- “WINS Servers”: If you’re using WINS, add the IP addresses of WINS servers. Otherwise, click “Next”.
- Click “Finish” after reviewing your configuration.

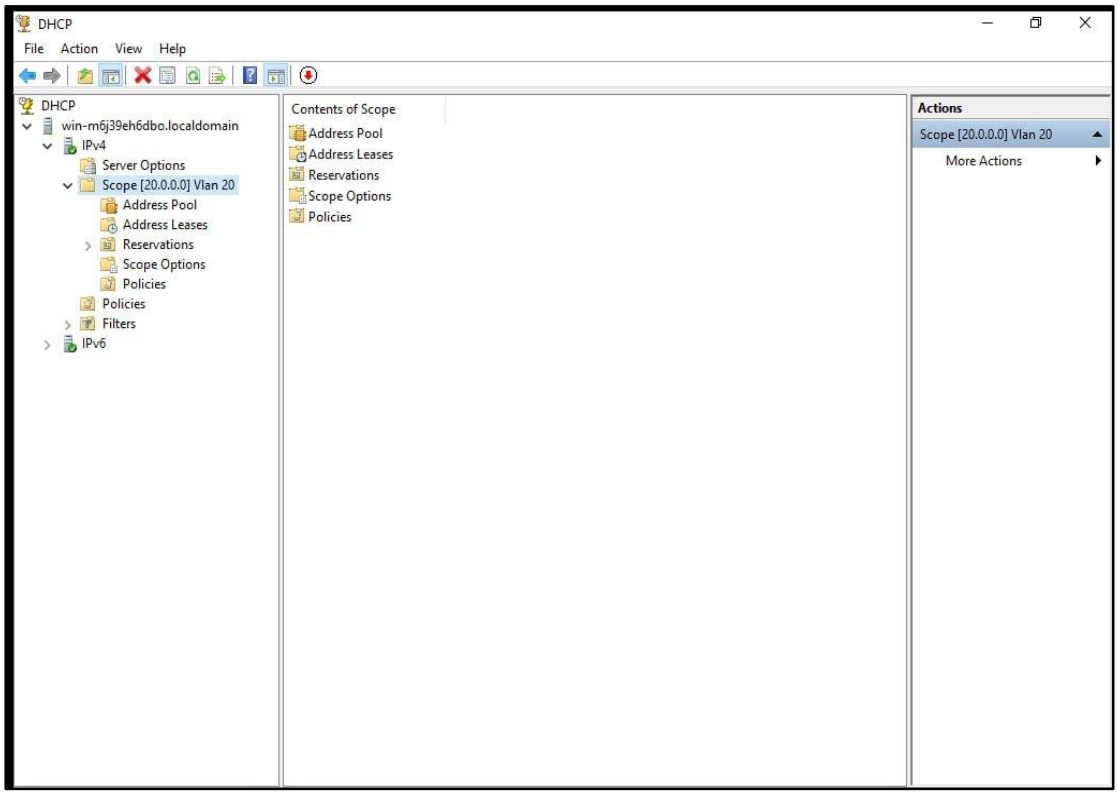


Figure 4.16(b) Configuration DHCP Server

4.2.2 Configuring DNS Server

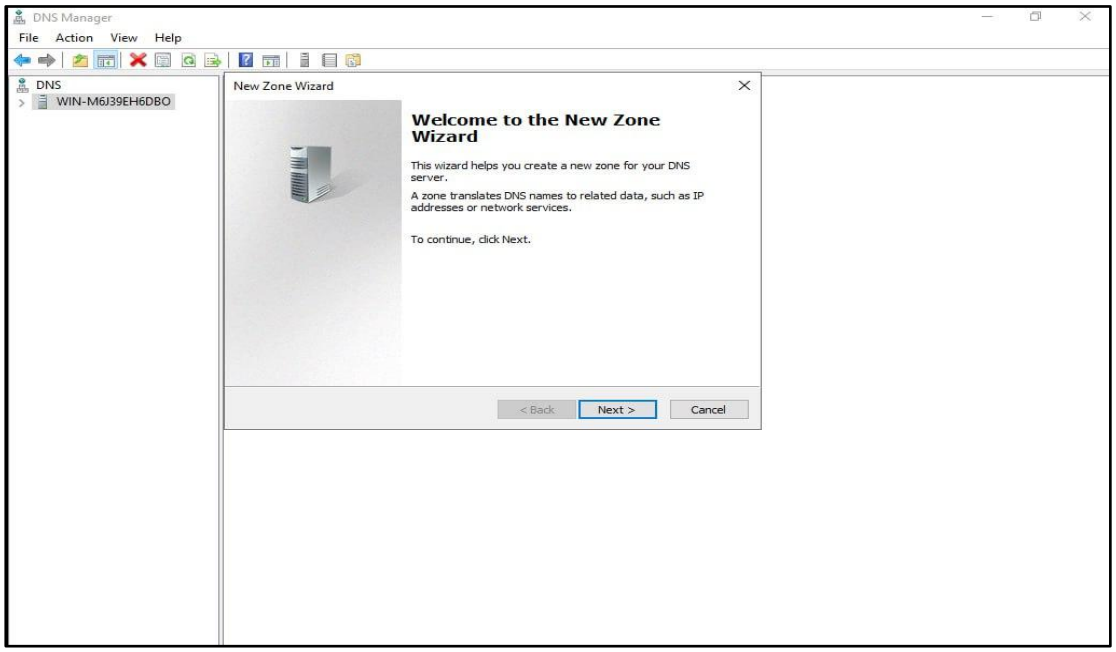


Figure 4.17(a) Configuration DNS Server

In the Configuring of DNS Server, the admin can do the following steps.

Step 1: Configure Forward Lookup Zones

A Forward Lookup Zone allows DNS to map domain names to IP addresses.

1. Create a Forward Lookup Zone:
   - Expand the server node and right-click “Forward Lookup Zones”.
   - Select “New Zone”.
2. New Zone Wizard:
   - The admin chooses “Primary Zone” (stores zone data locally) in “Zone Type” and click Next.
   - The admin enters “domain name” (for example, welcome.com) in “Zone Name”.
   - The admin selects “Create a new file” with this file name (the default is fine) in “Zone File”.
   - The admin chooses the “update method” for DNS records in “Dynamic Updates”.
   - Allow only secure dynamic updates (recommended if the server is part of a domain).
   - Allow both nonsecure and secure dynamic updates (less secure).

- Do not allow dynamic updates (if you want to manually manage DNS entries).
- Click “Finish” to complete the forward lookup zone creation.

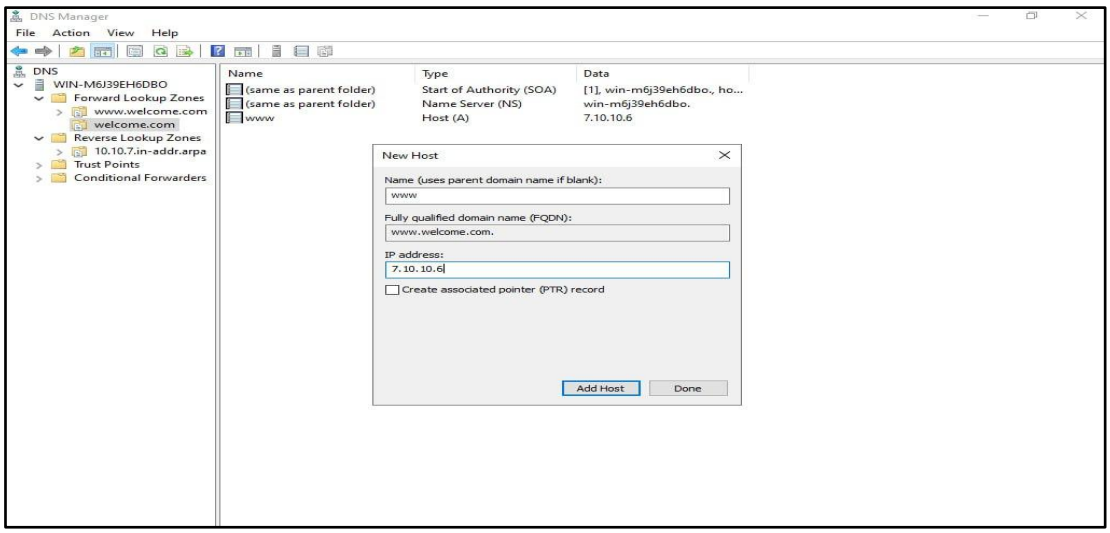


Figure 4.17(b) Configuration of DNS Server

3. Add DNS Records:
   - To add an A (Host) record (maps a domain name to an IP address), press right-click the newly created forward lookup zone and select “New Host” (A or AAAA).
   - Enter the “hostname” (for example, www.welcome.com) and the IP address (for example, 7.10.10.6).
   - Click “Add Host” and then “OK”.

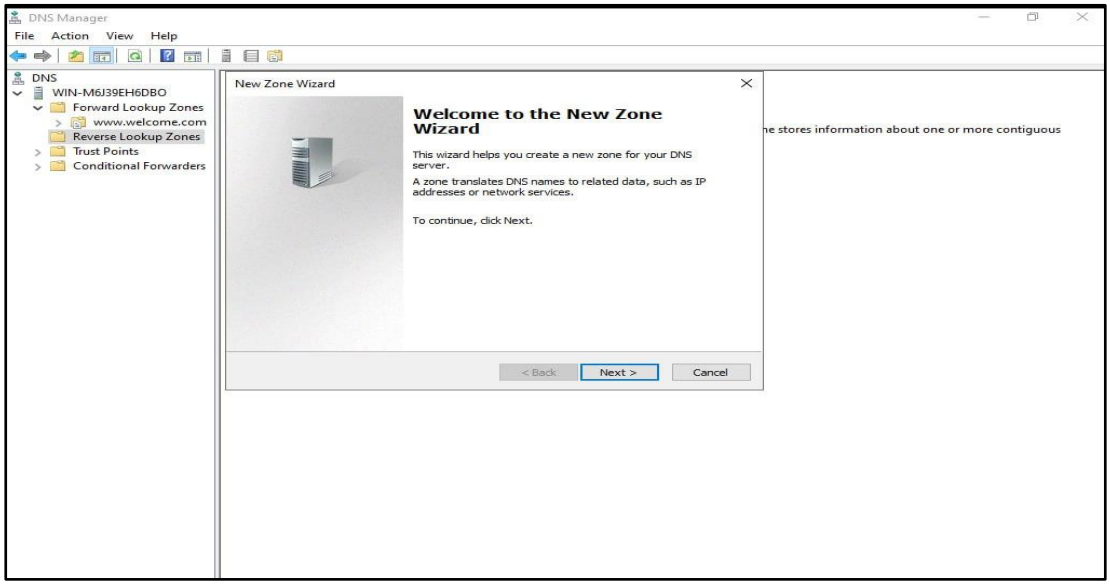


Figure 4.17(c) Configuration of DNS Server

Step 2: Configure Reverse Lookup Zones

A Reverse Lookup Zone allows DNS to map IP addresses to domain names.

1. Create a Reverse Lookup Zone:
    - Right-click “Reverse Lookup Zones” in DNS Manager and select “New Zone”.
2. New Zone Wizard:
    - The admin chooses Primary Zone in “Zone Type” and click “Next”.
    - The admin enters the network ID in “Network ID” (for example, 192.168.1 for an IP range like 192.168.1.0/24).
    - The admin accepts the default zone file name in “Zone File”.
    - The admin chooses the “dynamic update” option and click “Next”.
    - Click “Finish” to complete the reverse lookup zone creation.
3. Add PTR Records:
    - Right-click “reverse lookup zone” and select “New Pointer (PTR)”.
    - In the Host IP Number field, enter “the last octet of the IP address” (for example, 10 for 192.168.1.10).
    - In the Host Name field, enter “the fully qualified domain name” (for example, www.example.com).
    - Click “OK”.

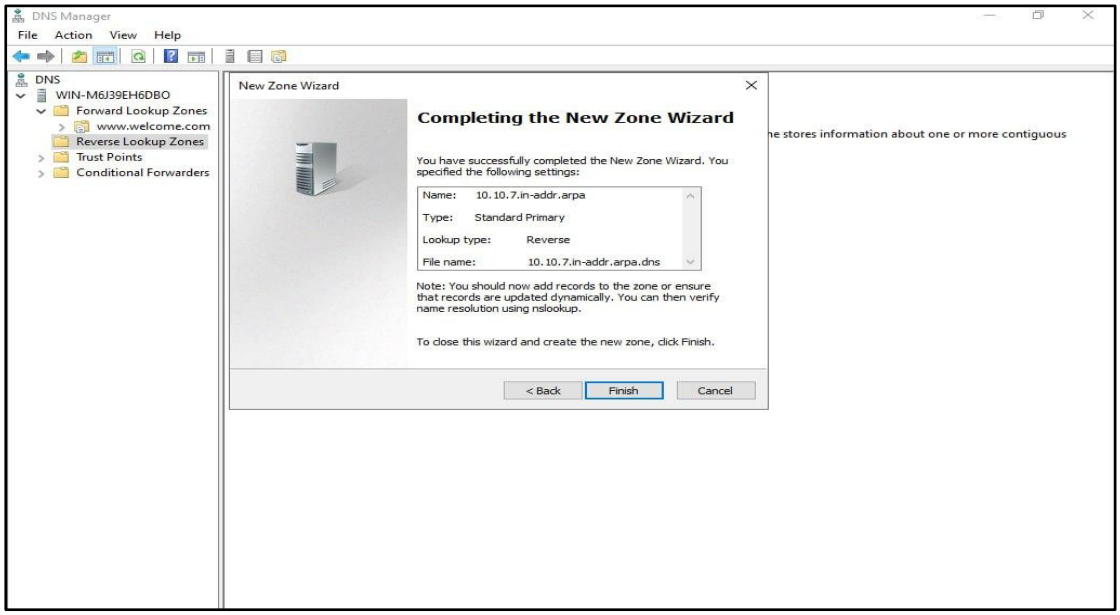


Figure 4.17(d) Configuration of DNS Server.

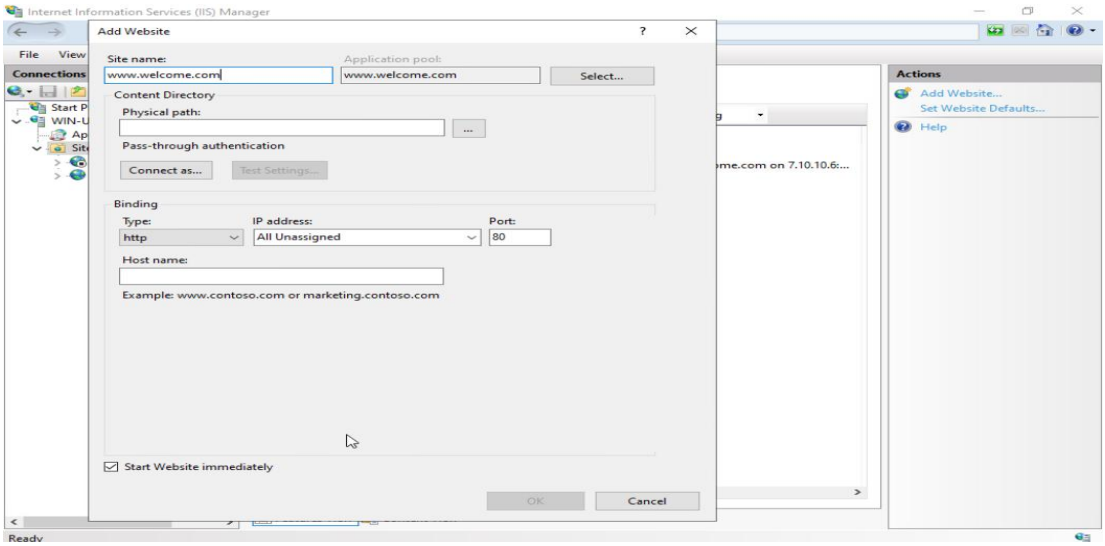


Figure 4.18 Adding a New Website Using IIS Manager

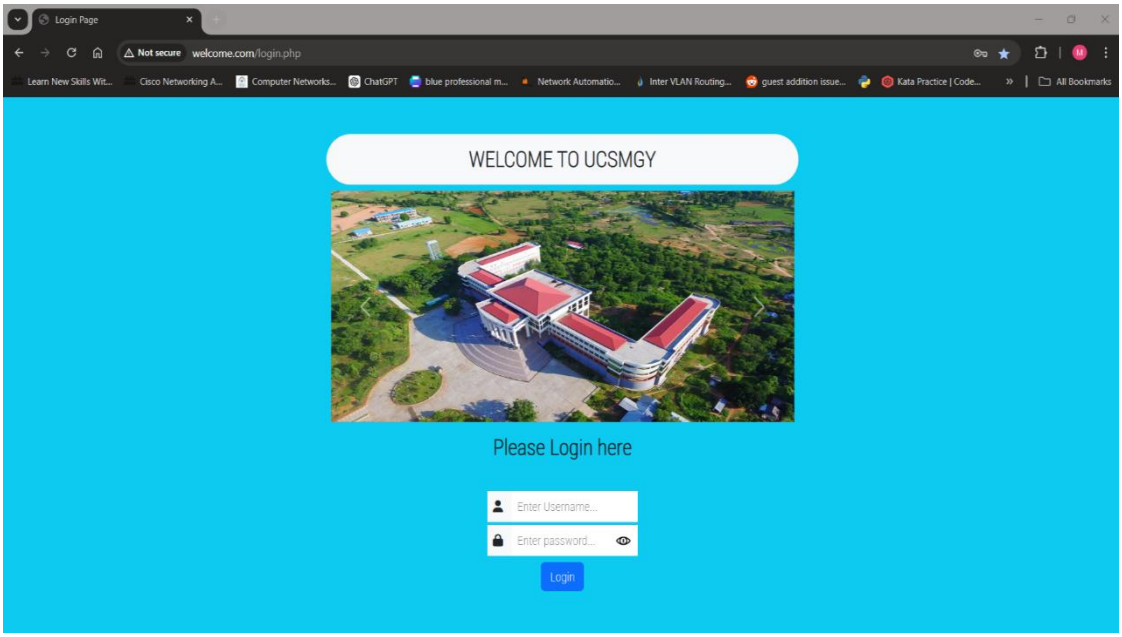


Figure 4.19 Testing Website Using Domain Name

4.3 Zabbix Server Installation on Ubuntu Server

The following steps are how to install Ubuntu Server on Dell PowerEdge R740.

Step 1: Installing VMware ESXi on Dell PowerEdge R740.

Step 2: Accessing VMware ESXi using VSphere Client.

Step 3: Installing Ubuntu Server on VMware ESXi and then Zabbix server install on Ubuntu Server.

- wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-6+ubuntu24.04_all.deb
- sudo dpkg -i zabbix-release_6.0-6+ubuntu24.04_all.deb

- sudo apt update
- sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
- sudo mysql -uroot -p
- mysql>create database zabbix character set utf8mb4 collate utf8mb4_bin;
  mysql>create user zabbix@localhost identified by 'password';
  mysql>grant all privileges on zabbix. * to zabbix@localhost;
  mysql>set global log_bin_trust_function_creators = 1;
  mysql> quit;
- /etc/zabbix/zabbix_server.conf (DBPassword=password)
- systemctl restart zabbix-server zabbix-agent apache2
- systemctl enable zabbix-server zabbix-agent apache2
- show ip addr

Insert the Ubuntu server IP in the web.

For example,7.10.10.8/Zabbix

4.3.1 Monitoring Window Server

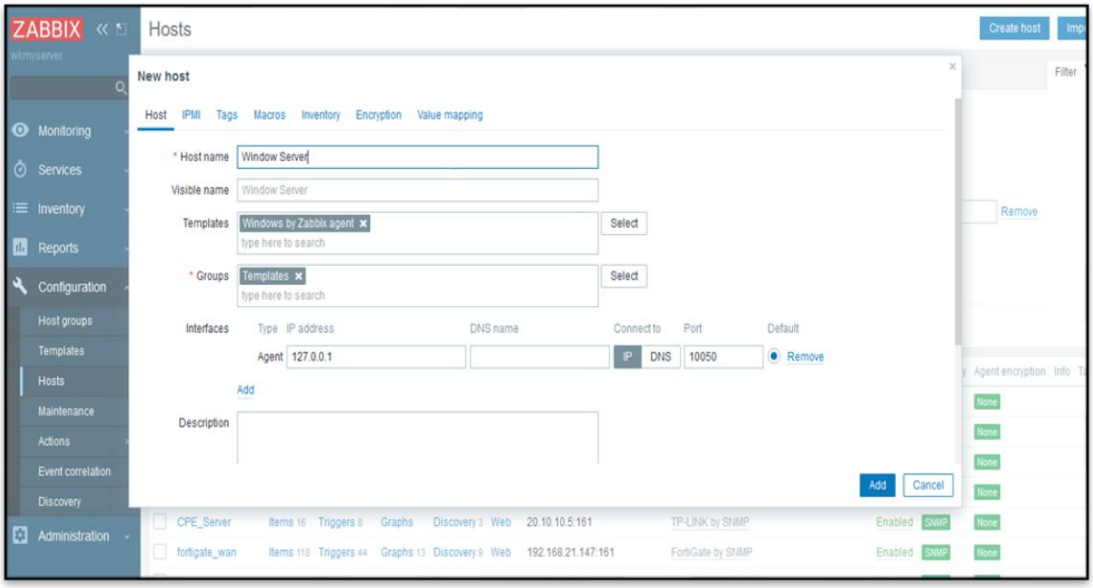


Figure 4.20 Windows Server monitoring.

To monitor the Windows server, we need to install the Zabbix Agent.

Step-1: Link to download the Zabbix agent.

https://cdn.zabbix.com/zabbix/binaries/stable/6.0/6.0.33/zabbix_agent-6.0.33-windows- amd64-openssl.msi

Step-2: We need to create the host in Zabbix.

Step-3: Add the host name and select the templates. Under the templates network device, select window by Zabbix agent.

Step-4: Click add, and then select agent. In the IP address blank, add the Zabbix server IP.

4.3.2 Monitor FortiGate Firewall

The admin clicks “Enable SNMP” checkbox on the FORTIGATE web. Go to “config” page to select the SNMP and add a community name.

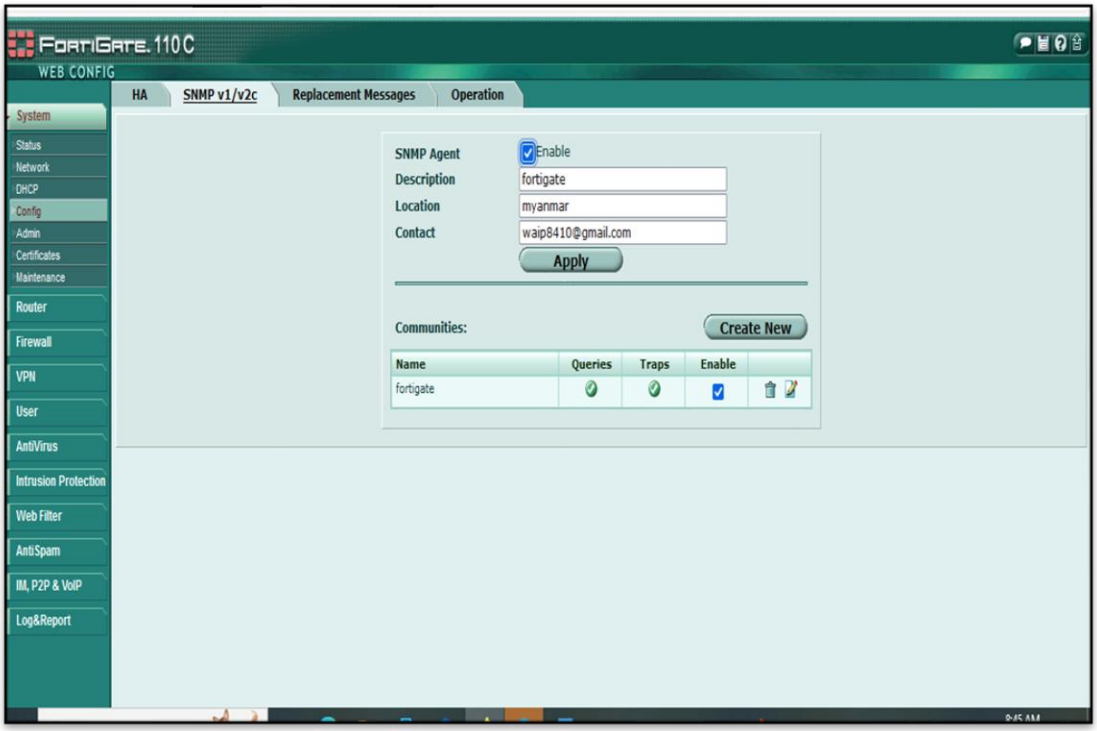


Figure 4.21(a) Configuring SNMP Agent in FortiGate Firewall.

Create Host for FortiGate Firewall

Step-1: Add the host name and select the templates.

- Under the templates network device, select FORTIGATE by SNMP.

Step-2: Click add, and then select SNMP.

- In the IP address blank, add the “FORTIGATE IP”.
- “Community name” in FotiGate must be added in the SNMP community blank.

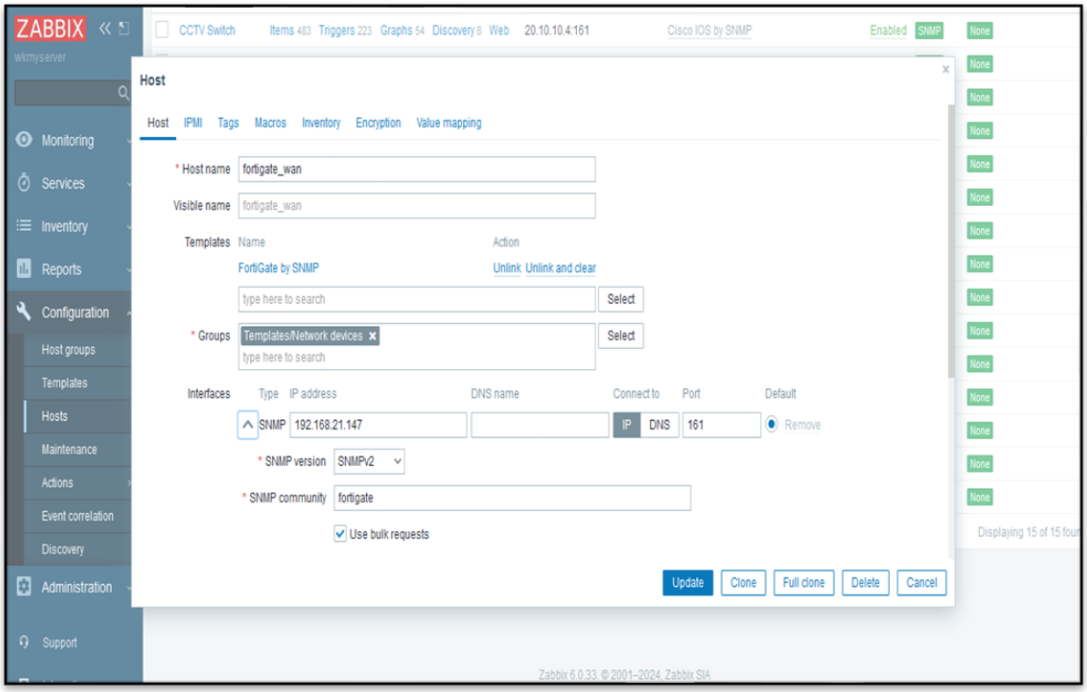


Figure 4.21(b) Creating host for FortiGate Firewall in Zabbix Server

4.3.3 Monitoring Network Switches

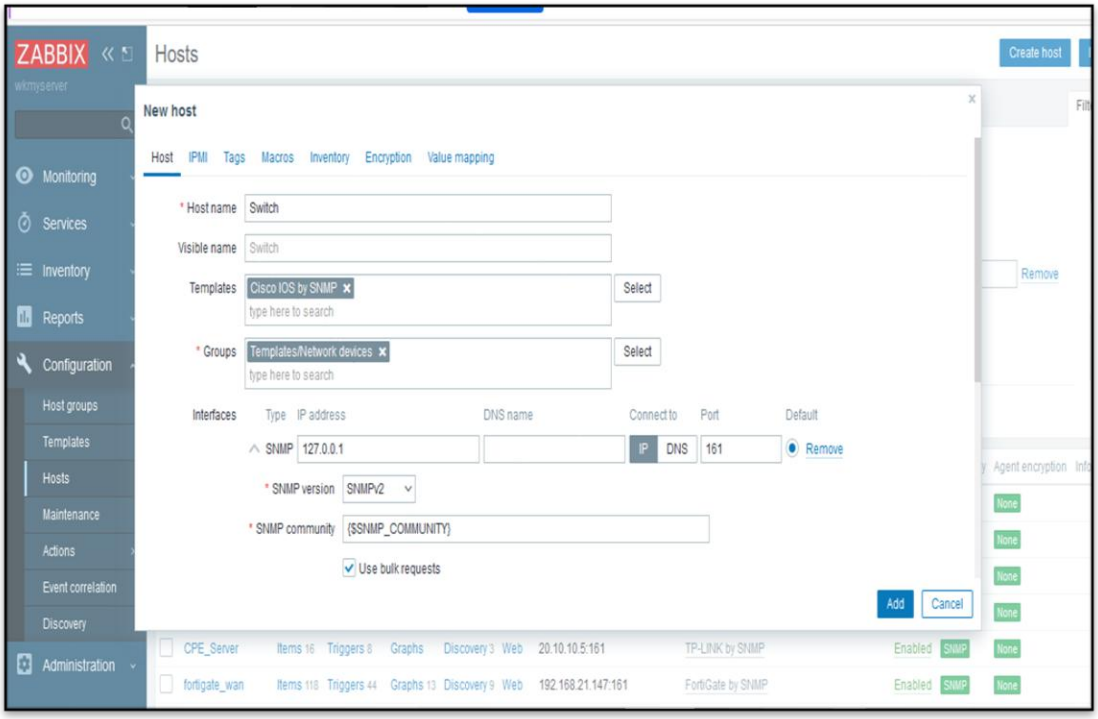


Figure 4.22 Creating host for Network Switches in Zabbix Server

In the Creating host for Network Switches in Zabbix Server, the admin can do the following steps.

Step-1: We need to enable the SNMP in the Cisco switch.

SNMP - server community name (for example, public).

SNMP - server host 192.168.1.4(switch ip) version 2c public (community name) UDP-port 161

Step-2: We need to create the host in Zabbix.

Step-3: Add the host name and select the templates. Under the templates network device, select Cisco IOS by SNMP.

Step-4: Click “add”, and then select “SNMP”. In the IP address blank, add the “Switch IP”.

Step-5: “Community name” have in switch must be added in the SNMP community blank.

4.3.4 Monitor TP-Link CPE 210

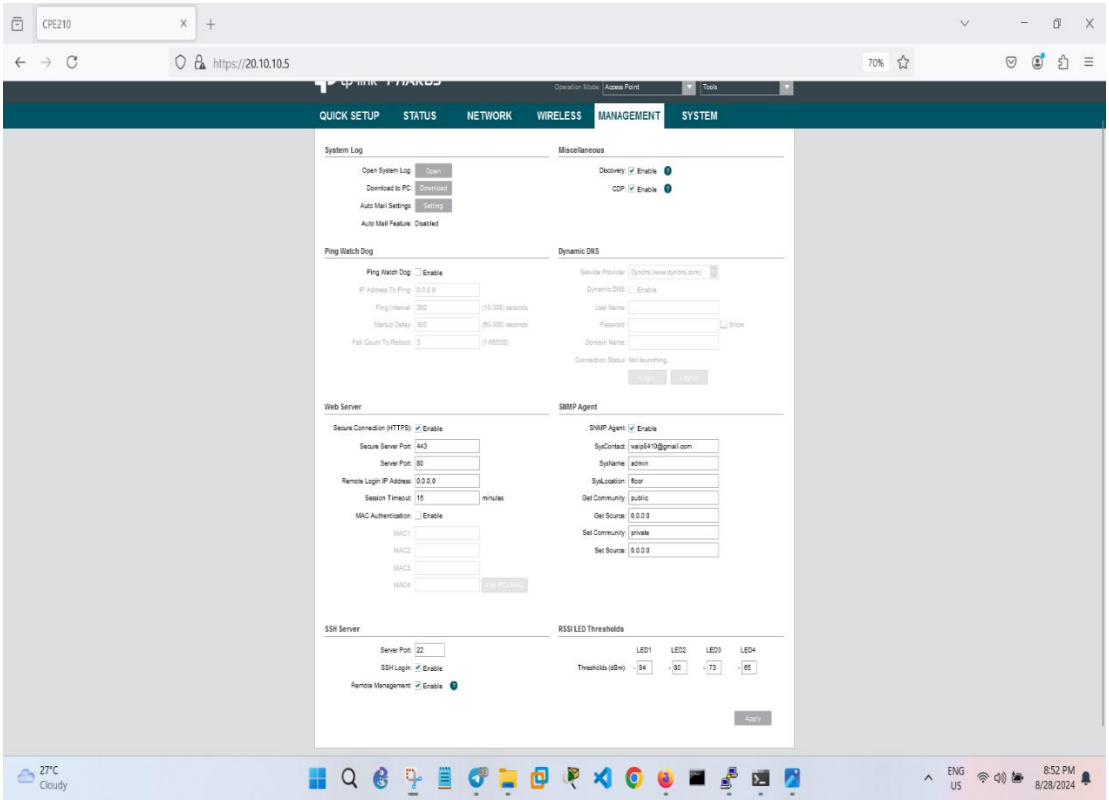


Figure 4.23 Configuring SNMP Agent in TP-Link CPE 210

In the Configuring SNMP Agent in TP-Link CPE 210, the admin can do the following steps.

- The admin clicks “Enable SNMP of TP-link CPE” checkbox.
- Go to the web with the IP of CPE.
- Click the management and select the SNMP agent.
- Fill in the IP of the zabbix server and add the community name.

4.3.5 Create Host for TP-Link CPE 210 in Zabbix Server

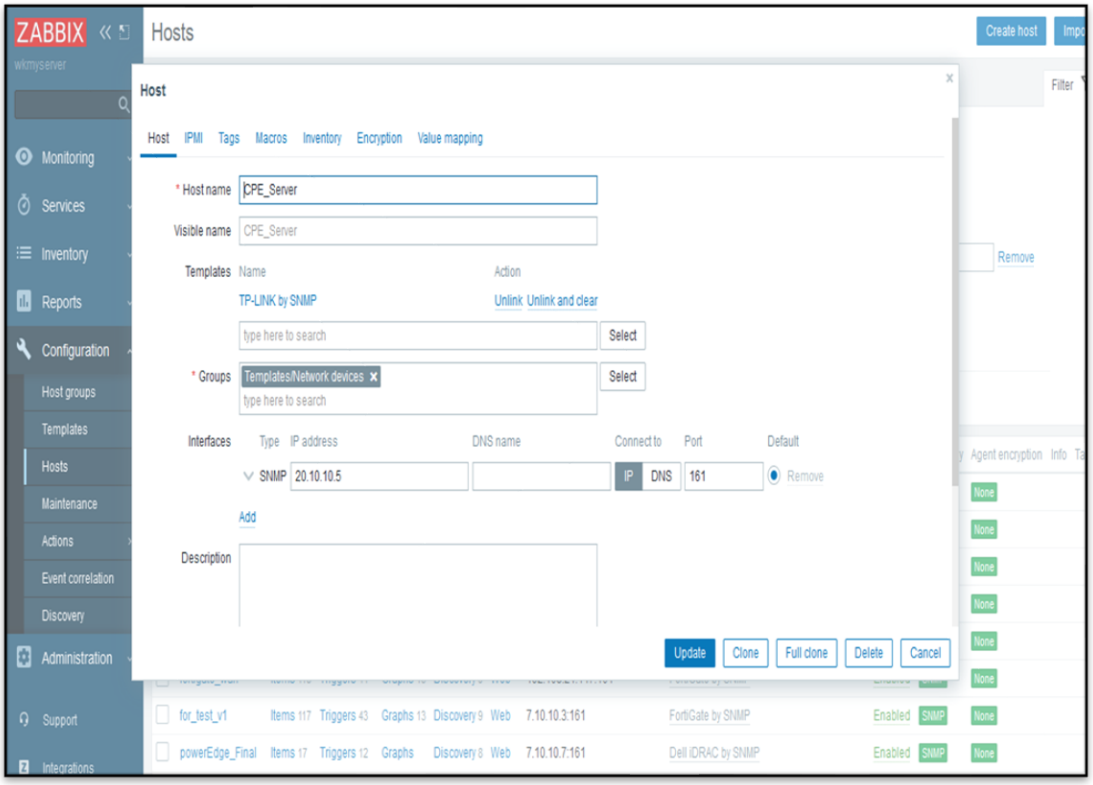


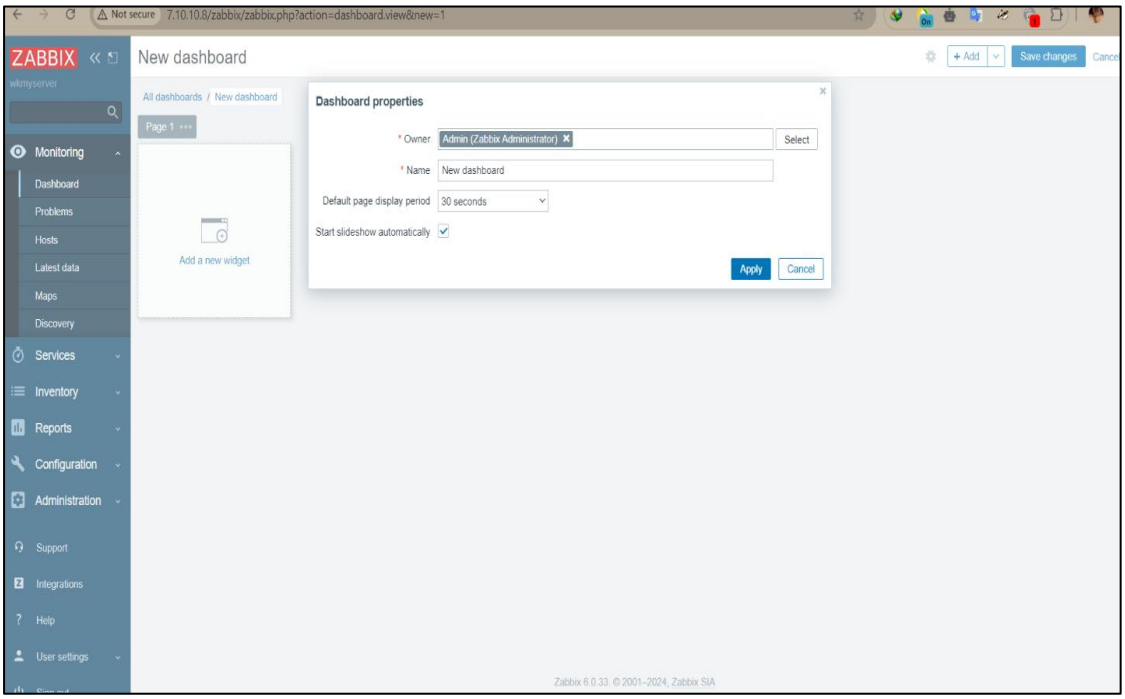
Figure 4.24 Creating host for TP-Link CPE 210 in Zabbix Server

In the Creating host for TP-Link CPE 210 in Zabbix Server, the admin can do the following steps.

- Add the host name and select the templates.
- Under the template network device, select TP-Link by SNMP.
- Click add, and then select SNMP.
- In the ip address blank, add the CPE IP.
- "Community name" have in CPE must be added in the SNMP community blank.

4.3.6 Create Dashboard for all Network Devices

Step-1: In the monitoring, click Dashboard and create dashboard.



Figurer 4.25(a) Creating Dashboard for all Network Devices

Step-2: Click Right click and create widget for device.

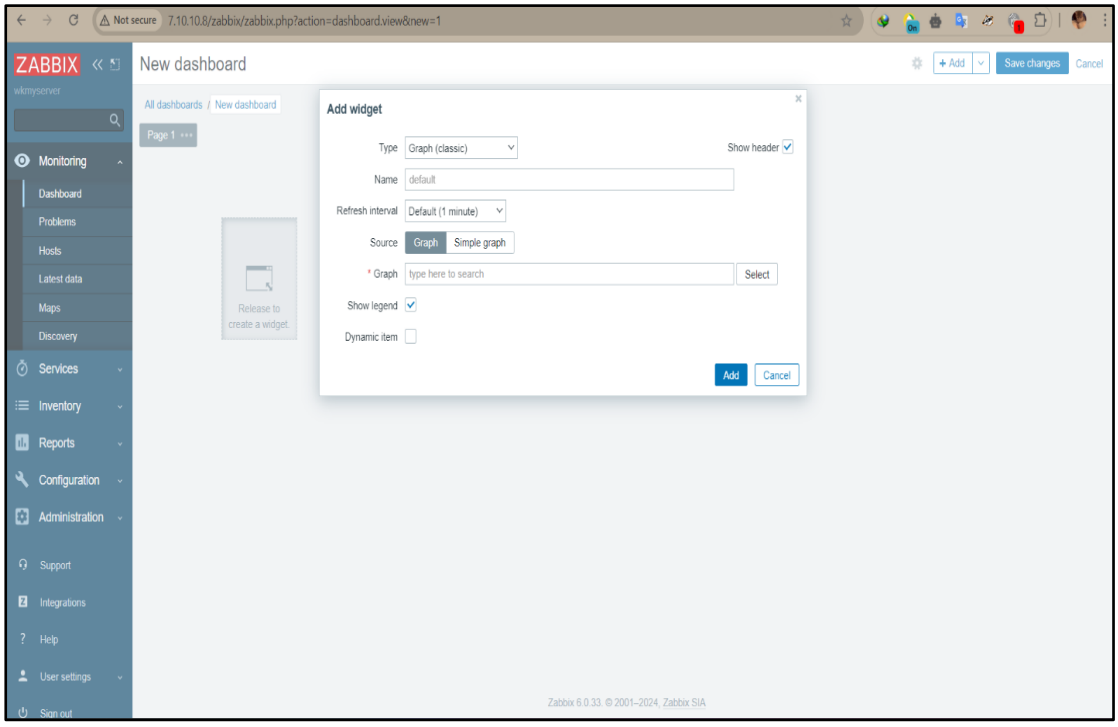


Figure 4.25(b) Creating Dashboard for all Network Devices

Step-3: In the Host field select the host device you want to create.

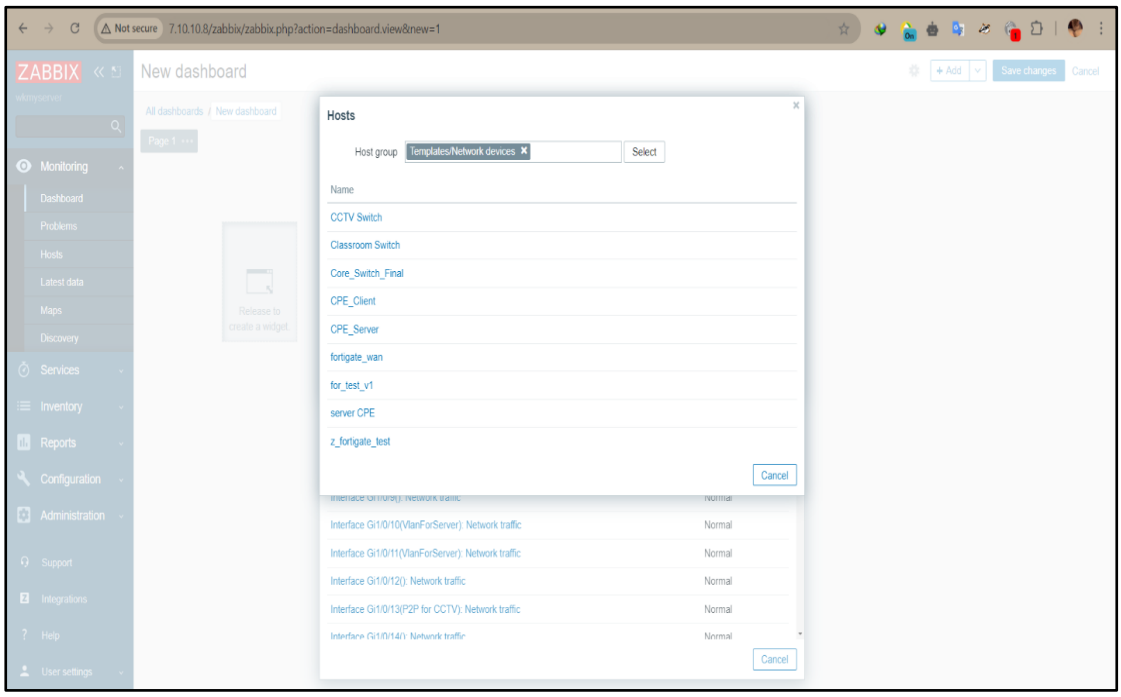


Figure 4.25(c) Creating Dashboard for all Network Devices

Step-4: In the Host filed select the status you want to monitor.

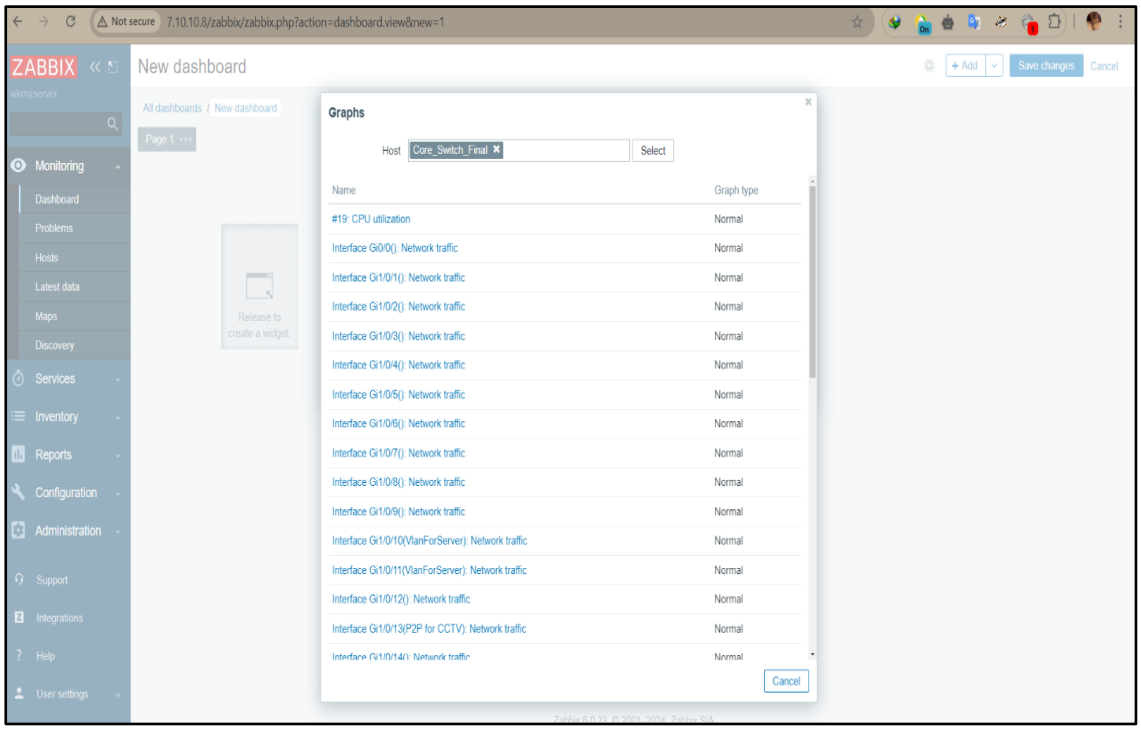


Figure 4.25(d) Creating Dashboard for all Network Devices

4.3.7 Main Dashboard for all Network Devices

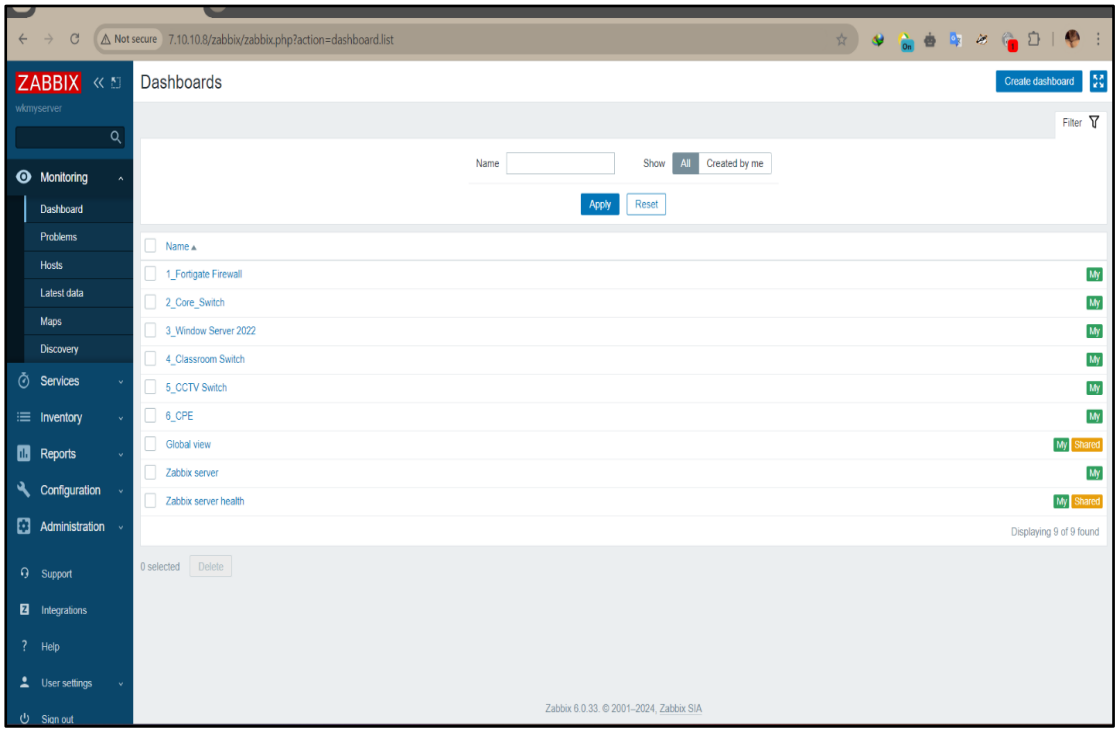


Figure 4.26 Overview Dashboard of all network devices

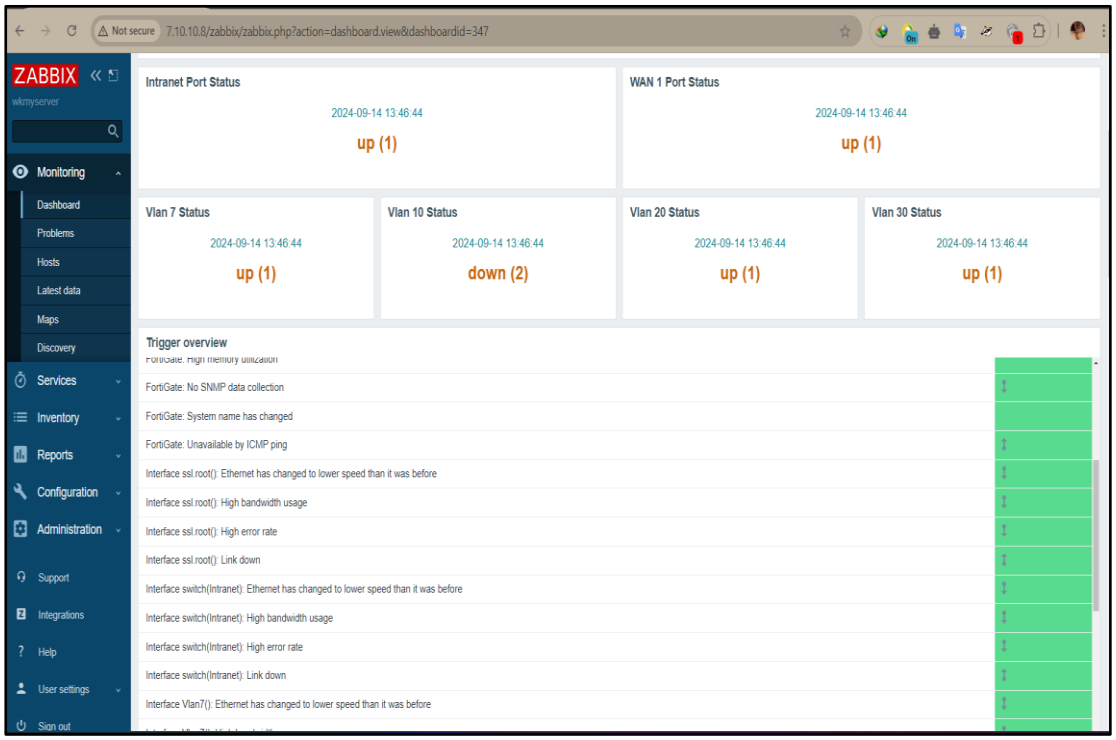


Figure 4.27 FortiGate Firewall Dashboard

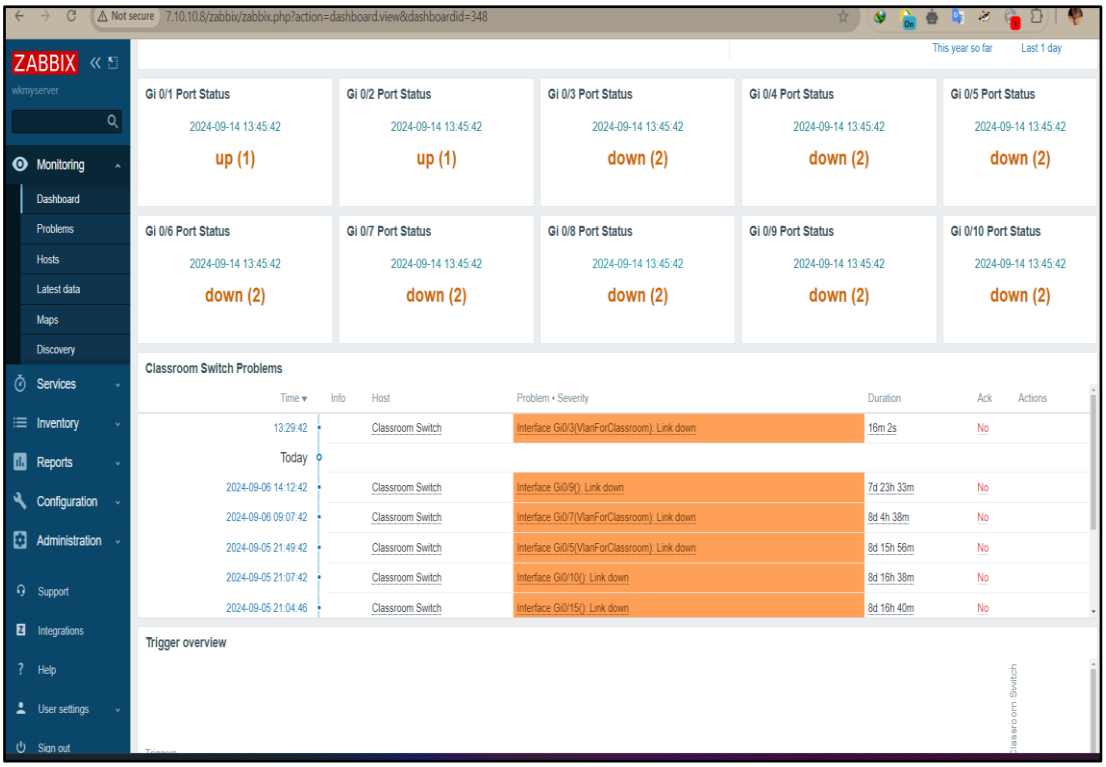


Figure 4.28 (a) Network Switches Dashboard

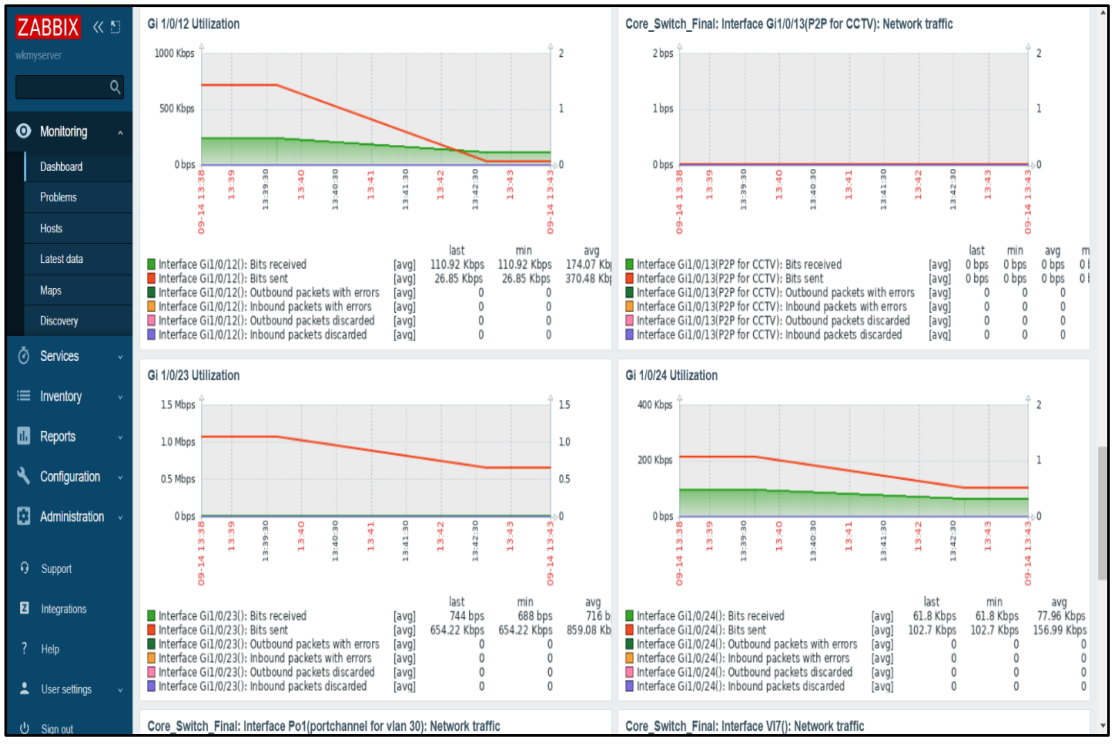


Figure 4.28 (b) Network switches Dashboard

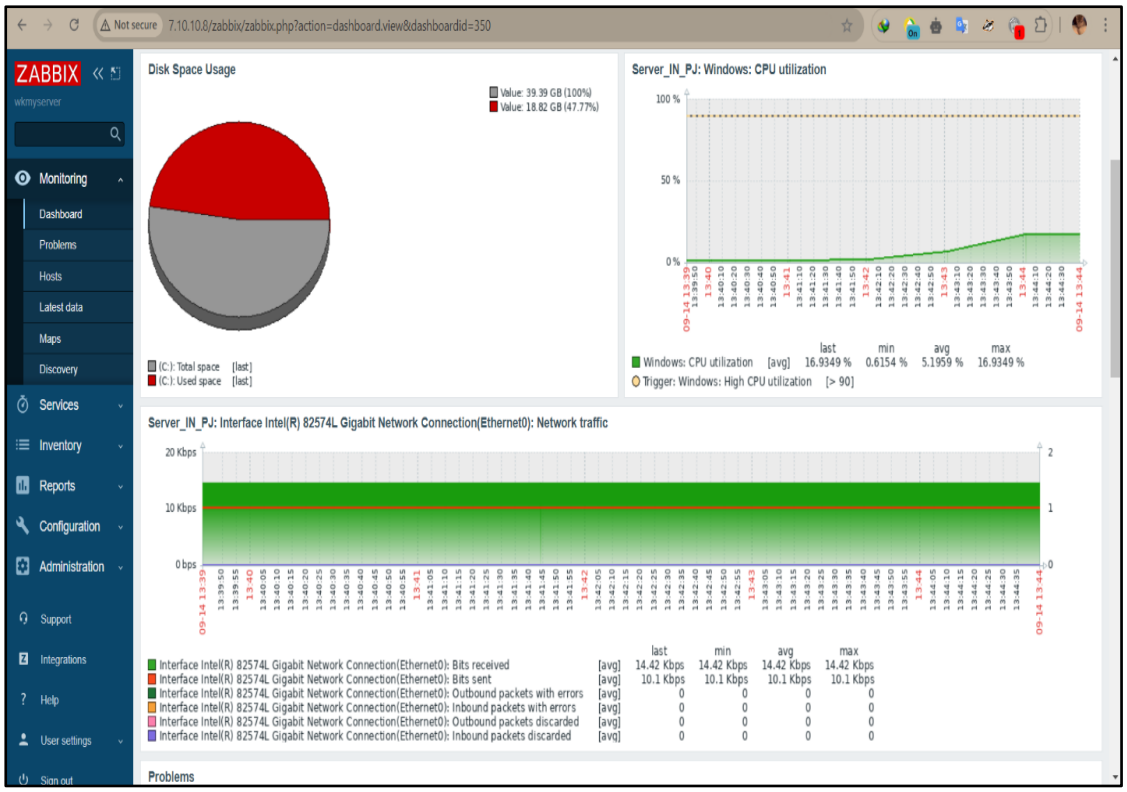


Figure 4.29 Server Dashboard

CHAPTER 5

CONCLUSION

This system establishes a network that can provide internet service and it is used in real life. Therefore, this project describes how to configure monitoring tools and networking devices such as Firewalls, Switches, Ruijie AP, Servers, and CCTV to construct a private network. This Intranet can improve communication, information sharing, and collaboration on a university campus. The project expresses the usage and specification of the devices to facilitate choosing network devices. Moreover, it can provide the services available on the server such as Web Hosting Service, Domain Name System (DNS) Service, and Dynamic Host Configuration Protocol (DHCP) Service. By using this system, the university will reduce high latency and can quickly troubleshoot about intranet and internet. It took nine weeks to complete the project. The estimated cost of this project is 81747.6 USD. All of these devices are offered by the Faculty of Computer Systems and Technologies of our university.

5.1 Further Extensions

In the Smart Campus Infrastructure, the following services can be extended.

- Private Cloud service using Dell PowerEdge R740
- File collection and sharing service using Synology
- CCTV control and monitoring service using NVR
- Web monitoring services using Zabbix

REFERENCES

[1] James F. Kurose, Keith W. Ross, "Computer Networking A Top-Down Approach", 6th edition

[2] Todd Lammle, "CompTIA Network+ Study Guide Exam N10-007", 4th edition

[3] Glen E. Clarke, "CompTIA Network+ Certification Study Guide", 4th edition

[4] https://www.router-switch.com/Price-cisco-switches_c2

[5] https://www-cloud.cisco.com/site/us/en/products/networking/index.html

[6] https://dl.ubnt.com/qsg/UAP-AC-LITE/UAP-AC-LITE_EN.html

[7] https://www.dahuasecurity.com/products/All-Products

[8] https://docs.fortinet.com/document/fortigate/hardware/fortigate-110c-quickstart-guide

[9] https://www.vmware.com/products/esxi-and-esx.html

[10] https://www.dell.com/en-us/shop/scc/sc/servers

[11] https://technoland.com.mm/product-category/networking

[12] https://ict.com.mm/collections/

[13] https://www.netacad.com/courses