FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

SEMESTER 2 SESSION 2018/2019

WORKSHOP 2
BITU 3923

BITC

FINAL REPORT

GROUP 4

PREPARED BY:

MUHAMMAD HAIKAL ASYRAF BIN NORAZMAN	(B031810124)
MEGAT MUAZAM BIN MEGAT THARIH AFENDI	(B031710049)
MUHAMMAD FIKRI ARIF BIN MOHD AMRAN	(B031710390)
SYAHRIN FANDI BIN RAZALI	(B031710022)
NURUL AQILAH BINTI ISAHAK	(B031710050)

PREPARED FOR:

TS ARIFF BIN IDRIS

ACKNOWLEDGEMENT

First and foremost, we would like to thank our supervisor of this project, TS. ARIFF BIN IDRIS for his valuable guidance and advice. He inspired us greatly to work in this project. His willingness to motivate us contributed tremendously to our project. We also would like to thank him for showing us some examples that are related to the services in our project which helped us understand our project better. This helped us complete our project on time. We would also like to thank our evaluator for this workshop, TS. DR. NAZRULAZHAR BIN BAHAMAN for taking the time to evaluate us. This evaluation gave us a deeper understanding of our services and network infrastructure.

Besides that, we would like to thank the authority of University of Technical Malaysia Melaka (UTeM) for providing us with a good environment and facilities to complete this project. Finally, an honourable mention goes to our families and friends for their understandings and supports us in completing this project. With the help of the particulars mentioned above, we completed our project successfully on time.

ABSTRACT

In this Workshop II project, we have to define, implement and manage tasks which start from selecting a leader to lead this project from the beginning until the end of this project. A task has been given to each member and we create a schedule for the task to finish on time and who will do what service. It is very important to manage and organizes every task given in order to avoid any problems and error later on. Our main objective in this Workshop II is for this project to be successful and able to go through the obstacles and challenges faced while completing the task given. Next our objective also is to have deeper understanding about the service on how it works and we are grateful to experience this as it helped us to be more prepared in our industrial training. Our group had decided to use Windows Server 2019 in server 1 (Window), Ubuntu in server 2 (Linux) and Debian in server 3 (Debian). We choose this server operating system because it has many benefits. Our group also was assigned to set up 15 services listed. The 15 services listed are Server Virtualization, DNS (IPv4 & IPv6), DHCP (IPv4 & IPv6), Network Management System, Routing & NAT, Proxy Server, AAA with radius, Secure FTP, Access Control List (ACL), Linux Email Server, Web, SSL & Virtual Hosting, IPv6 Web with IPv6 Tunneling, Active Directory, IPSec site to site tunneling and Wireless user authentication using Radius Server. During the Workshop II, we faced several problems but still managed to overcome it and make this project in time and successfully completed the services.

ABSTRAK

Dalam Projek Bengkel 2 ini, kami harus menentukan, melaksanakan dan menguruskan tugas-tugas yang telah diberikan. Kami bermula dengan memilih seorang pemimpin untuk mengetuai projek ini dari awal hingga ke akhir projek bengkel 2 ini. Setiap ahli kumpulan telah dibahagikan dengan tugas secara sama rata dan sebuah jadual telah dihasilkan di mana jadual itu digunakan untuk memastikan bahawa tugas itu disiapkan dalam masa yang ditetapkan. Setiap tugas harus diuruskan dengan sebaik mungkin untuk mengelakkan daripada menimbulkan sebarang masalah dan kesilapan.Objektif utama Bengkel 2 ini adalah untuk melaksanakan projek ini dengan jayanya dan untuk mengatasi sebarang halangan dan cabaran yang dihadapi semasa menyelesaikan tugasan yang diberikan sepanjang semester ini. Selain itu, mendapatkan pemahaman mengenai servis-servis yang perlu ada di setiap rangkaian komputer juga merupakan salah satu objektif bengkel ini. Kami sangat berterima kasih kepada pengalaman ini kerana projek ini banyak membantu kami untuk bersedia untuk latihan industri nanti. Kumpulan kami telah membuat keputusan untuk menggunakan Windows Server 2019 dalam server 1 (Window), Ubuntu dalam server 2 (Linux) and Debian dalam server 3 (Debian) . Kami memilih sistem operasi pelayan ini kerana manfaatnya. Kumpulan kami juga telah ditugaskan untuk membekalkan 15 servis kepada rangkain kami. Antara 15 servis yang disenaraikan adalah *Server Virtualization, DNS (IPv4 & IPv6), DHCP (IPv4 & IPv6), Network Management System, Routing & NAT, Proxy Server, AAA with radius, Secure FTP, Access Control List (ACL), Linux Email Server, Web, SSL & Virtual Hosting, IPv6 Web with IPv6 Tunneling, Active Directory, IPSec site to site tunneling and Wireless user authentication using Radius Server.*

TABLE OF CONTENTS

LIST OF FIGURE

LIST OF TABLE

CHAPTER 1: INTRODUCTION

1.1 Introduction

This Workshop 2 (BITU 3923) is introduced to all third year Bachelor Degree students as a platform to prepare students before undergo their Final Year Project and Industrial Training. During Workshop 2 students will work in group and they are required to develop a project based on their majoring. Workshop 2 provides an opportunity to students to practice their knowledge and experience gained from previous subjects. Students also able to develop their understanding of problem solving techniques to solve a particular problem based on their respective project.

One of the outcomes of the subject are student should be able to design the network infrastructure by using the available tools and be able to implement designated network services also to install and integrate network services infrastructure to suit the network environment while maintain and control the network services infrastructure

It will also train students to work in group and solve the problems that arise together like the actual environment in industry which emphasize on being a good team player and critical thinking. Each group will be provided with 3 servers (1 Windows and 2 Linux Distro), 2 network interface card (NIC), one Access Point, 1 router (2 FastEthernet), one Manageable Switch, one wireless router, one serial cable, UTP cable, 12 RJ-45 and 1 set of Crimping Tool.

Based on the above equipment, we are required to design, set up, maintain and monitor a network environment with basic server applications and fundamental services also the basic service that were built in this network environment. In total with 15 services will installed on the network to make sure it fulfil the question scenario requirements. We have to use three different operating system which is Microsoft Windows 2019 Server, Linux operating system that is Debian and UBUNTU.

Company Zitech is expanding with approximately 100 employees' .This Company provide server room where the main server is home and client connect to the remote site. The sites are connected with simple point to point that can be used to carry IPv6 packets between the sites. We have setup the infrastructure for company Zitech that covers all the networking functions.

1.2 Problem Statement

The following are the problem statements for the Workshop 2 project:

I. **Setting up and designing a secure network infrastructure**
   - Using all the provided network equipment's, students need to set up and design a secure network.

II. **Configure and up the services**
   - Students need to configure the 15 services and do service testing to make sure all the services work. Students must also monitor the services constantly.

III. **Installing and integrate different operating systems**
   - Students must install the different operating systems in the three servers which is Linux operating system that is Debian and UBUNTU and Windows Server 2019 and make sure that each server will be able to communicate and interact with each other.

IV. **Design a secure network infrastructure by using available tools**
   - Setup and implement the appropriate network infrastructure and network services that can fulfil the question needs and requirements.

1.3 Objective

The main objective of Workshop 2 is to build a network in difference operating system in LAN and WAN connection and develop understanding of problem solving techniques to solve a particular problem or services. Besides that, the objectives of the network development are:

- To design network infrastructure by using the available tool.
- To be able to implement designated network services.
- To be able to install and integrate network services infrastructure to suit the environment.
- To be able to maintain and control the network services infrastructure.

1.4 Project Plan

Weeks	ITEM	ACTION
2-3	**Project Proposal** Includes: 1. Executive Summary 2. Organization Chart 3. Network Design (Logical and Physical) 4. VLSM Addressing 5. Gantt charts and project distribution. **Device Collection & setup** Student must ensure that the asset collection form is signed by the Supervisor **AFTER** the proposal has been approved.	Proposal submission Bring along log book for review Device collection from designated assistant engineer.
2-5	**Progress I** Presentation of project progress: setup 8 services that consists of: 1. Inter VLAN 2. Service for video. 3. 1 service for each student	**Present *Progress I*** Bring along log book for review
6-10	**Progress II** Presentation of project progress: setup 10 services	**Present*Progress II*** Bring along log book for review
11-13	**Progress III** Presentation of project progress: setup all (100%) services. Each individual in the group is required to demonstrate their **individual** and **group task respectively** with the supervisor/evaluator	**Present Progress III** Bring along log book for review
12	**Video & Poster** Video and poster preparation involves ONE (1) services that has been set. Video and poster (softcopy) should be presented to supervisor for the purpose of updates for final exhibition at week 14	***Video & Poster submission*** Bring along log book for review
14	**Workshop II Exhibition** Video is pre-evaluated by the juries. Only poster is evaluated on by the juries on the exhibition day	***Workshop II Exhibition***
Study Week	**Final Report, Peer Assesment Report, and Log Book**	***Final Report, Peer Assesment Report, and Log Book Submission***

Table 1 Project Plan

1.5 Conclusion

The workshop II project expose the group to design, implement, install, configure, and manage the basic component of computing resources and basic services in this project. At the end of the project, we able to apply knowledge and experience from the previous subject that we have learnt such as Computer Organization, Operating System, Local Area Network, Network Analysis and Design, Wide Area Network and Network Project Management into this project. We have practice the theory of all the subject to solve the problem that we have been encountered during the development of this project.

Furthermore, it also can design the network infrastructure so that we can maintain and good network environment. We also learn how to build a security system to make sure our network is secure from hacker or unauthorized access. With the cooperation and planning of all project team members, the project that we do was able to complete on time. The Workshop II helps us to explore something new in network environment using all equipment that gives to us in any different platform operating system. This is very important because we can train our team to work not only industrial training but in the future as well.

CHAPTER 2: PROJECT REQUIREMENT

2.1 Introduction

In this workshop II, we are using 3 different operating system which are Windows Server 2019, Ubuntu 18.04 LTS and Debian 9 for setup on the servers and access point router and personal laptop. All Linux operating system doesn't require any license as it provided as open source and able download through online. The network infrastructure will be designed by using the available tools. The network to be developed will consist of three servers with combination of different platforms. Besides that, we need to setup 15 services and it will be divided among the servers. There is 15 services of computer networking. The servers will be using mainstream operating system to simulate real environment and superior services for the users. It is very important to make sure that the network system operate at the desired performance and the technologies used will be the best possible, depend on the allocated budget.

2.2 Types of operating system

An operating system is to manage the computer's memory, processes, software and hardware. To let the user gain a good experience when they operate the computer, a high-quality operating system is needed to integrate network services infrastructure to suit the network environment that have been set. The operating systems use in the project are Window Server 2019, Ubuntu 18.04 LTS amd64 (Linux) and Debian 9.

2.3 Operating system background

2.3.1 Windows Server 2019

We are choosing Windows server 2019 as one of our operating system because of its various function that might be helpful in the Workshop 2 implementation. Firstly, because it is full-function server operating system. It is automatically come with the most of the technical, security, management and administrative features such as the rewritten networking stack (native ipv6, native wireless, and speed and security improvements). Also, it improved from previous version which is consist of image-based installation, deployment, recovery, diagnostics, monitoring, event logging and reporting tools. Windows Server 2019 delivers rich web based experiences efficiently and effectively. It also, has a security improvement where by providing highest level of protection of network, data, and business.

2.3.2 Linux Ubuntu 18.04

Ubuntu 18.04 is feature that are include language settings, users, authentications, network shares, web servers and firewalls among many others. Ubuntu 18.04 is Linux distribution, Ubuntu 16.04 lays great emphasis on security also the firewall is available right from the start. Ubuntu 18.04 gives Security-Enhanced Linux feature that implements multiple security policies.

2.3.3 Debian

Debian is a Unix-like operating system consisting entirely of free software. Ian Murdock founded the Debian Project on August 16, 1993. Debian 0.01 was released on September 15, 1993 and the first stable version, 1.1, was released on June 17, 1996. The Debian Stable branch is the most popular edition for personal computers and network servers, and is used as the basis for many other Linux distributions.

Debian is one of the earliest operating systems based on the Linux kernel. The project is coordinated over the Internet by a team of volunteers guided by the Debian Project Leader and three foundational documents: the Debian Social Contract, the Debian Constitution, and the Debian Free Software Guidelines. New distributions are updated continually, and the next candidate is released after a time-based freeze.

Debian has been developed openly and distributed freely according to the principles of the GNU Project. Because of this, the Free Software Foundation sponsored the project from November 1994 to November 1995. The popular Linux operating system Ubuntu was also released based on Debian. When the sponsorship ended, the Debian Project formed the nonprofit Software in the Public Interest to continue financially supporting development. The Intel 586 (Pentium), Intel 586/686 hybrid (Pentium with MMX) and PowerPC architectures are no longer supported as of Stretch.

2.4 Operating system justification

2.4.1 Windows Server 2019

Windows Server 2019 is architecture and functionality since the code base is common, it automatically comes with most of the technical, security, management and administrative features new to Windows Operating system such as the rewritten networking stack (native IPv6, native wireless, speed and security improvements); improved image-based installation, deployment and recovery; improved diagnostics, monitoring, event logging and reporting tools. Windows Server 2019 includes an enhanced Hyper-V hypervisor (Hyper-V 2019) that provides the ability to compress virtual machines (VMs) during live migrations, automatic reallocation of memory between VMs running Linux as a guest on Hyper-V hosts, remote direct memory access (RDMA) support during live migrations, VM live cloning, and support for shared VHDX files..

Besides that, it has improved Windows Firewall with default configuration, Windows Workflow Foundation and the core kernel, memory and file system improvements. Processors and memory devices are modelled as Plug and Play devices to allow hot-plugging of these devices. This allows the system resources to be partitioned dynamically using Dynamic Hardware Partitioning which each partition has its own memory processor and I/O host bridge devices independent of other partitions.

In Windows Server 2019, there are also a lot improvements that are the reason we chosen this version as one of our server operating system such as core OS improvements, Active Directory improvements, Disk management and file storage improvements, Server Manager which gathers together all of the operations users would want to conduct on the server, such as, getting a remote deployment method set up, adding more server roles etc., and provides a consolidated, portal-like view about the status of each role and others.

2.4.2 Ubuntu 18.04

We decided to trade cutting edge software which is Ubuntu in newer version for high stability. We had chosen Ubuntu 14.04 because it is the most stable and minimize risk compared to Ubuntu 12.04 which has many bugs until now. Ubuntu 14.04 comes with new requirement which is hardware recognition and its can automatically detect our pc screen resolution, soundcard and others devices. Another reason is, Ubuntu 14.04 tries to remain pure free software. Operating system as it doesn.t include non-free components in its repositories.

In addition, Ubuntu 14.04 also respects users' freedom and privacy and doesn't track anything that users done on their PC Furthermore, Ubuntu 14.04 is supported by great documentation, a very active community and plenty of online resources and Ubuntu 14.04 came as a very stable operating system with professional appearance and easy to use.

2.4.3 Debian

Debian 9 (Stretch) was released on 17 June 2017, two years and two months after last release Debian 8 (Jessie), and contained more than 51,000 packages and the latest minor update, called a "point release", is version 9.9, released on April 27, 2019; 19 days ago. Major upgrades include the Linux kernel going from version 3.16 to 4.9, GNOME desktop version going from 3.14 to 3.22, KDE Plasma 4 was upgraded to Plasma 5, LibreOffice 4.3 upgraded to 5.2 and Qt upgraded from 4.8 to 5.7. LXQt has been added as well. The Intel 586 (Pentium), Intel 586/686 hybrid (Pentium with MMX) and PowerPC architectures are no longer supported as of Stretch.

2.5 Hardware Requirement

2.5.1 Hardware Requirements for Windows Server 2019

Component	Minimum	Recommended
Processor	1.4 Ghz	2 GHz or faster
Memory	512 MB RAM	2 GB RAM or greater
Available Disk Space	32 GB	40 GB or greater
Optical Drive	DVD-ROM drive	DVD-ROM drive
Display	Super VGA (800x600) monitor	XGA (1024x768) monitor

Table 2 hardware Requirements for Windows Server 2019

2.5.2 Hardware Requirements for Ubuntu 18.04

Component	Minimum Requirements
Processor	2 GHz dual core processor
Memory	2 GB RAM
Available disk space	25 GB of hard drive space
Display	VGA capable of 1024x768 screen resoltuion

Table 3 Hardware Requirements for Ubuntu 18.04

2.5.3 Hardware Requirements for Debian 9

Component	Minimum Requirements
Processor	1 GHz Pentium 4 processor
Memory	512 MB RAM
Available disk space	10 GB HDD
Installation Media	USB / DVD

Table 4 Hardware Requirements for Debian 9

2.6 Hardware Justification

2.6.1 Router

A router is a networking device whose software and hardware are usually forwards data packet between computer networks. Router connects two or more logical subnets, which do not necessarily maps one-to-one to the physical interfaces of the router. Router is to set IP address and to make connection between servers and client. Other than that, to route information to server. Other configuration routing we set at each server in router to make connection that we need.

2.6.2 Switch

A switch is a computer networking device that used to connect devices together on a computer network, by using a form of packet switching to forwards data to the destination device. It commonly refers to a bridge that processes and routes data at the data link layer (layer 2) of OSI Model. Other than that, the switch is used to connect all the three servers and the client and also use to connect 8 Computer to Internet. Moreover, for a configuration switch, it usually has additional features such as Command Line Interface (CLI) and has ability to display, modify, backup and restore configuration.

2.6.3 UTP Cable

UTP cable or Unshielded Twisted Pair cable is the most common cable used in computer networking. It is often used in data network for a short and medium length connection because it is relatively lower costs compared to optical fibre and coaxial cable. Other than that, unshielded twisted pair (UTP) is a type of cable that can transmit voice or data signals. In Workshop II project, we use UTP Cat 3 Cable and are given about 15 meters long UTP cable for the entire project.

2.6.4 RJ-45

RJ-45 Connectors is short for Registered Jack-45, an eight-wire connector used commonly to connect computers onto a Local Area Network (LAN), especially 9 Ethernets. It also the standard connector used for the UTP cable. It transmits information over twisted pairs or wires and RJ-45 is the connection for the cable, we use from switch to other client computer to make connection over internet once cable was plugged in switch.

2.6.5 Crimping Set Tools

A crimping tool is a tool designed to crimp or connect a connector to the end of a cable. Crimper is capable of crimping a RJ-11 (6 Pin) and RJ-45 (8 Pin) connectors and also includes a wire cutter near the handles that can be used to cut phone or CAT5 cable.

2.6.6 Wireless Router

A wireless router is a device that performs the functions of a router and also includes the functions of a wireless access point. It is used to provide access to the Internet or a private computer network. Depending on the manufacturer and model, it can function in a wired local area network, in a wireless-only LAN, or in a mixed wired and wireless network.

2.6.7 Application and Service Analysis

Each student will implement few services for BITC students, each service has function to make sure the connection of the network to fulfil the question and company specification. 15 services for the BITC student to make the connection is secure and reliable.

2.6.8 Network Interface Card (NIC)

- NIC is a circuit board or card that is installed in a computer so that it can be connected to a network.
- Network interface card provides the computer with a dedicated, full-time connection to a network.
- Network interface cards also have can supplying a basic addressing system that can be used to get data from one computer to another on the network.
- Each NIC will be used for each server and will be able to provide network communication capabilities to and from a computer.

2.7 Conclusion

As the conclusion, before installing Operating System, one should ensure that the computer meet the requirements. It is complicated for us to integrate three different types of Operating System with at least 20 different in a network infrastructure. We have to consider the demand of the operating system and decide which the best to implement is that we set to each server. Besides, we also have to state and research about the hardware requirements to make sure coincidentally of network. We have to make sure those requirements are suitable and afford to support our services for each server before we installed it. Perfect setting can make strength connection over internet.

CHAPTER 3 DESIGN

3.1 Introduction

In this workshop II, we have to define, design, implement and manage network services. Every group need to implement their own network design which is needed to be applied in real device. Stated in the requirements, that need us to design the network that include three different servers, one CISCO router, one CISCO switch and a client host for the design. Our group already designs the networks that have two clients that are from internal and external. We have been supplied with RJ-45, UTP cable, console cable and a set of crimping tools. We also required using different operating system to set the network environment. The NOS we choose to install into HP platform is Window Server 2019 and Ubuntu 18.04. Another platform we use is Debian.

3.2 Physical Design

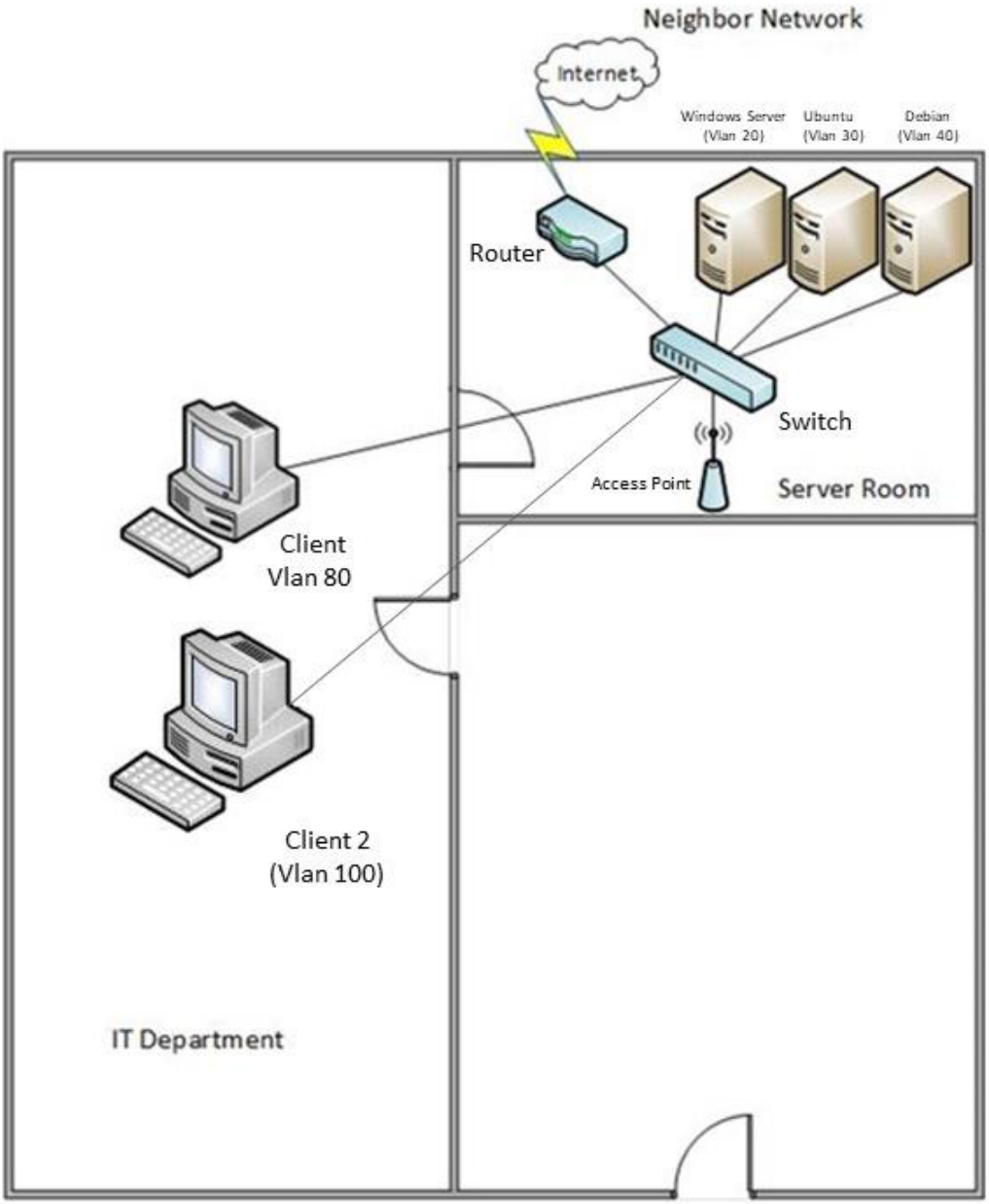


Figure 1 Physical Design

3.3 Logical Design

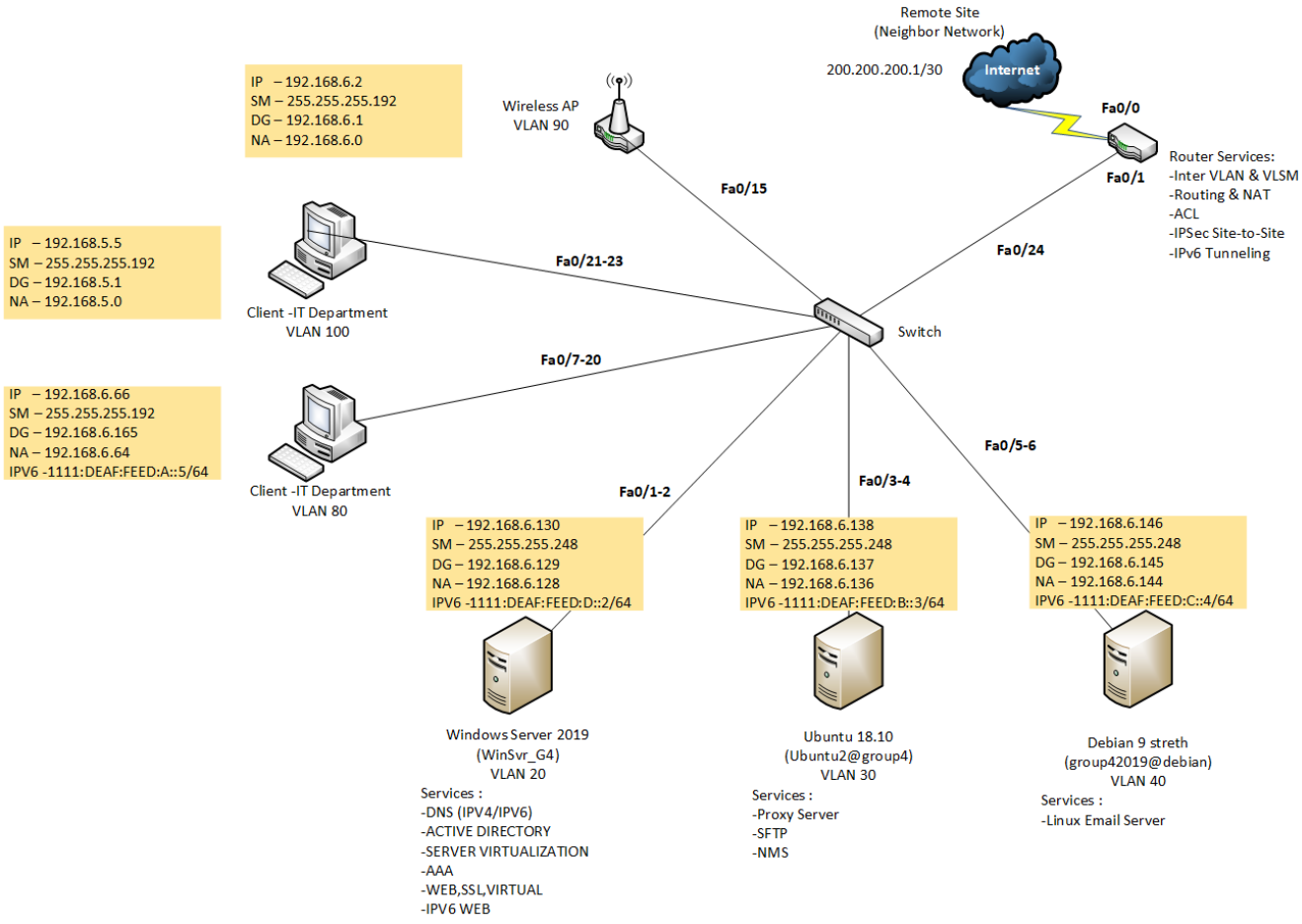


Figure 2 Logical Design

3.4 IP Addressing

3.4.1 VLAN and VLSM Addressing

Subnet	Network Address	CIDR	Subnet Mask	IP Range	Broadcast Address
VLAN 100	192.168.5.0	/26	255.255.255.192	192.168.5.1 - 192.168.5.62	192.168.5.63
VLAN 80	192.168.6.64	/26	255.255.255.192	192.168.6.65 - 192.168.6.126	192.168.6.127
VLAN 20	192.168.6.128	/29	255.255.255.248	192.168.6.129 - 192.168.6.134	192.168.6.135
VLAN 30	192.168.6.136	/29	255.255.255.248	192.168.6.137 - 192.168.6.142	192.168.6.143
VLAN 40	192.168.6.144	/29	255.255.255.248	192.168.6.145 - 192.168.6.150	192.168.6.151
Router	192.168.6.152	/30	255.255.255.252	192.168.6.153 - 192.168.6.154	192.168.6.155
Wireless AP	192.168.6.0	/26	255.255.255.192	192.168.6.1 - 192.168.6.62	192.168.6.63

Table 5 Vlan and VLSM addressing

3.5 Conclusion

Network designing is an important part while creating a network. Without network design, there is no idea on how to begin the implementation of the network. There are few main factors that need to be considered while implementing network design that include, the planning of network complexity must be in line with the network administrator, redundancy, standards and maintenances factor. All of those factors are need to ensure the network can be implementing, expandable for future implementation and easy to maintain.

After considering on those factors, we had implemented network as designed physically and go through to the next level of implementing that is planning the implementation of network services.

CHAPTER 4: SERVICES

4.1 Introduction

In this chapter, each service that was installed will be listed and explained. Explanation will include the function of the service, what are the problems that are solved by installing the service, and what type of software or package.

4.2 List of services

1. DNS (IPv4 & IPv6)
2. DHCP (IPv4 & IPv6)
3. IPv6 Web with IPv6 Tunneling
4. Web, SSL & Virtual Hosting
5. IPSec site to site tunneling
6. Active Directory
7. Server Virtualization
8. AAA with Radius
9. Secure FTP
10. Linux Email Server
11. Network Management System
12. Proxy Server
13. Wireless user authentication using Radius Server]
14. Access Control List (ACL)
15. Routing & NAT

4.3 Brief overview for services

4.3.1 DNS (IPv4 & IPv6)

The way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address. DNS are the Internet's equivalent of a phone book. They maintain a directory names and translates IP addresses. This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses. Information from all the domain name servers across the Internet are gathered together and housed at the Central Registry. Host companies and Internet Service Providers interact with the Central Registry on a regular schedule to get updated DNS information.

4.3.2 DHCP (IPv4 & IPv6)

DHCP (Dynamic Host Configuration Protocol) was developed to simplify the networking experience for users and network administrator. It provides reliable IP address configuration and reduced network administration for clients to access the network. DHCP assigns a local IP address to devices connected to the local network from DHCP address pool. Network clients will be configured automatically by the DHCP service. Besides, any modification to the IP address of the router and DNS servers can be implemented easily.

4.3.3 IPv6 Web with IPv6 Tunneling

Internet Protocol version 6 (IPv6) is the most recent version of the IP, the communication protocol that provides an identification and location system for the computers on the networks and routers traffic across the Internet. A virtual Local Area Network (LAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer. It is to subdivide a network into virtual LAN, one configure a network switch or router.

4.3.4 Web, SSL & Virtual Hosting

Secure Sockets Layer (SSL) creates an encrypted connection between the web server and the visitor's web browser allowing for private information to be transmitted without the problems of eavesdropping, data tampering or message forgery. The secure connection is made by using the certificates. SSL Certificate has a pair of public and private key that work together to establish an encrypted connection. Virtual Hosting is a method for hosting multiple domain names on a single server. This allows one server to share it resources such as memory and processor cycle without requiring all services provided to use the same host name.

4.3.5 IPSec site to site tunneling

A site-to-site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations. An example of a company that needs a site-to-site VPN is a growing corporation with dozens of branch offices around the world.

4.3.6 Active Directory

Developed for Windows Domain network, it authenticates and authorizes all users and computers by assigning and enforcing security policies. AD checks the submitted password and determines whether the user is system admin or client. Also, it allows management and storage of information, provide authentication and authorization mechanisms.

4.3.7 Server Virtualization

Server virtualization is the masking of server resources, including the number and identity of individual physical servers, processors, and operating systems, from server users. The server administrator uses a software application to divide one physical server into multiple isolated virtual environments. The virtual environments are sometimes called virtual private servers, but they are also known as guests, instances, containers or emulations.

4.3.8 AAA with Radius

Authentication is a user must gain authorization for doing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity. Authentication refers to the process of validating the identity of the user by matching the credentials supplied by the user (for example, name, and password) to those configured on the AAA server, for example, name, and password. If the credentials match, the user is authenticated and gains access to the network. If the credentials do not match, authentication fails, and network access is denied. Authorization refers to the process of determining what permissions are granted to the user. For example, the user may or may not be permitted certain kinds of network access or allowed to issue certain commands. Accounting refers to the recording of information about the resources a user consumes while they are on the network. The information gathered can include the amount of system time used, the amount of data sent, or the quantity of data received by the user during a session.

The final plank in the AAA framework is accounting, which measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

Authentication, authorization, and accounting services are often provided by a dedicated AAA server, a program that performs these functions. A current standard by which network access servers interface with the AAA server is the Remote Authentication Dial-In User Service (RADIUS).

4.3.9 Secure FTP

File Transfer Protocol (FTP) is a popular method of transferring files between two remote systems. SFTP, which stands for SSH File Transfer Protocol or Secure File Transfer Protocol is a separate protocol packaged with SSH that works in a similar way over a secure connection. It encrypts the file transfer process from start to finish with limited threat exposure for the user and proven secure method to transmit files.

Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which facilitates data access and data transfer over a Secure Shell (SSH) data stream. It is part of the SSH Protocol. This term is also known as SSH File Transfer Protocol that provides secure communications using a key-based encryption scheme. It fully encrypts the file transfer process, from start to finish with limited threat exposure for the user and proven secure method to transmit files. Ftp user may authenticate them using a clear-text-sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission, it hides username and password, and encrypts the content. SFTP is essential as a mean to transfer files between servers and client or network equipment without compromising on security and confidentiality.

4.3.10 Linux Email Server

Message transfer agent software that transfers electronic mail messages from one computer to another using client–server application architecture. An MTA implements both the client (sending) and server (receiving) portions of the Simple Mail Transfer Protocol. The major functions of an MTA are:

- Accepting messages originating from the user agent and forwarding them to their destination (other user agents)
- Receiving all messages that are transmitted from other user agents for further transmission
- Keeping track of each and every activity and analyzing and storing the recipient list to perform future routing functions
- Sending auto-responses about non-delivery when a message does not reach its intended destination

4.3.11 Network Management System

A network management system (NMS) is an application or set of applications that lets network engineers manage a network's independent components inside a bigger network management framework and performs several key functions. An NMS identifies, configures, monitors, updates and troubleshoots network devices both wired and wireless in an enterprise network. A system management control application then displays the performance data collected from each network component, allowing network engineers to make changes as needed.

Network element vendors make their performance data available to NMS software either through APIs or through a protocol such as NetFlow, a de facto industry standard originally developed by Cisco that allows NetFlow-enabled routers to transmit traffic and performance information. Network engineers use a network management system to handle a variety of operations, among them.

- Monitor performance: By collecting operating metrics through a series of physical taps, software agents or Simple Network Management Protocol interfaces, an NMS can provide the visibility necessary to determine if network elements are operating correctly.
- Detect devices: A network management system is used to detect devices on the network and to ensure the devices are recognized and configured correctly.
- Analyze performance: An NMS is used to track performance data indicators, including bandwidth utilization, packet loss, latency, availability and uptime of routers, switches and other network components.
- Enable notifications: In the event of a system disruption, an NMS will proactively alert administrators about any performance issues.

4.3.12 Proxy Server

A proxy server is computer that functions as an intermediary between a web browser and the Internet. Proxy servers help improve web performance by storing a copy of frequently used webpages. Whenever the client connects to a web proxy server and makes a request for the resources that reside on a remote server, the proxy server forwards this requests to the target server on behalf of the client, so as to fetch the requested resource and deliver it back to the client. An example of client can be a user operated computer that is connected to the Internet.

4.3.13 Wireless user authentication using Radius Server

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on local operating system or within authentication server. The authentication examples use Radius, login and Point-to-Point Protocol (PPP).For example, TACACS+ can be substituted for Radius or local authentication.

To configure AAA authentication, firstly need to define a named list of authentication methods which is in global configuration mode. Then, apply that list to one or more interfaces in interface configuration mode.

4.3.14 Access Control List (ACL)

An access control list (ACL) is a table that tells a computer operating system which access rights each user has a system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program).

4.3.15 Routing & NAT

Routing is a transit of logically addressed packets from their source toward destination through intermediate nodes. Routing is to define paths for packet transmission. Network Address Translation (NAT) translating an address used within an intranet or private network to public internet IP address. Implementation of NAT can be done in router of firewall. It helps to make sure the security of outgoing on ingoing request. Routing is the process of selecting paths in a network along which to send network traffic. Routing directs packet forwarding, the transit of logically addressed packets from their source toward their ultimate destination through intermediate nodes. The routing process directs forwarding based on routing tables which maintain a record of the routes to various network destinations. The routing service provided by the router allows a client to access and receive resources from remote networks. While NAT the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.is the act of translating an address from one to another within the packet. A router that acts as intermediary between networks performs the NAT function. One network is designated the inside network and the other is the outside. The local inside network addresses maps to one or more global outside IP addresses and un-maps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. Moreover, NAT allows network clients with private IP to communicate with public network such as the internet.

4.4 Conclusion

Each of service has their own function. Service also have different types of software or packages to be installed on the server. Service can be simple but it can be very important. The service is installed will be listed and explained. Explanation will include the functions of the services, problems solved by installing the services and the type of software used.

CHAPTER 5: INSTALLATION AND CONFIGURATION

5.1 Introduction

All the services that had been done have different methods and ways of configuration. This section will show how to install and configure all the services follow the correct setup. The configuration is to ensure the functioning of the service are successfully installed and configure.

5.2 Services Configuration and Corresponding Person-in-Charge

Service	Name
1. Server Virtualization **2.** DNS (IPv4 & IPv6) **3.** DHCP (IPv4 & IPv6)	Syahrin Fandi Bin Razali
1. Network Management System **2.** Routing & NAT **3.** Proxy Server	Nurul Aqilah Binti Isahak
1. AAA with radius **2.** Secure FTP **3.** Access Control List (ACL)	Muhammad Fikri Arif Bin Mohd Amran
1. Linux Email Server **2.** Web, SSL & Virtual Hosting **3.** IPv6 Web with IPv6 Tunneling	Megat Muazam Bin Megat Tharih Afendi
1. IPSec site to site tunnelling **2.** Active Directory **3.** Wireless user authentication using Radius Server	Muhammad Haikal Asyraf Bin Norazman

Table 6 Service Configuration and Corresponding Person in Charge

5.3 Service Installation and Configuration

5.3.1 DNS

5.3.1.1 Installation DNS

1. Start Server Manager, click the Manage menu, and then select Add Roles and Features. Click Next on the Add Roles and Features Wizard. “Before you begin” window that pops up. Select the installation type, Role-based or feature-based installation.

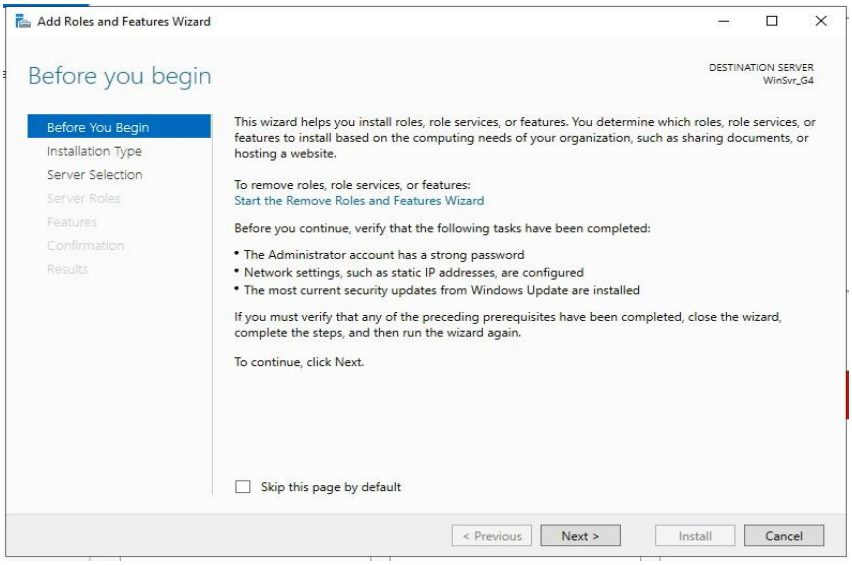


Figure 3 Add service

2. Next, select a server from the server pool to install roles and features, and click Next.

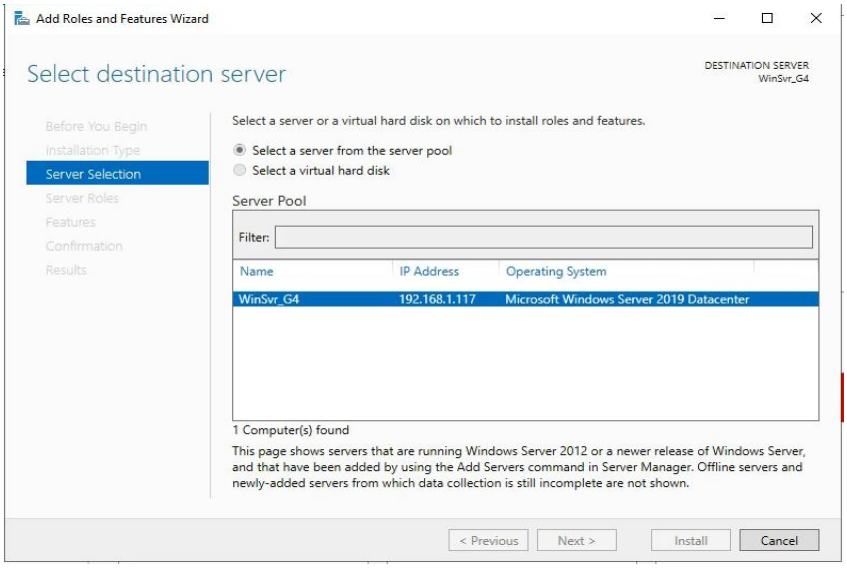


Figure 4 Select server from server pool

3. For this Features window, no need to make any changes, click Add Features.

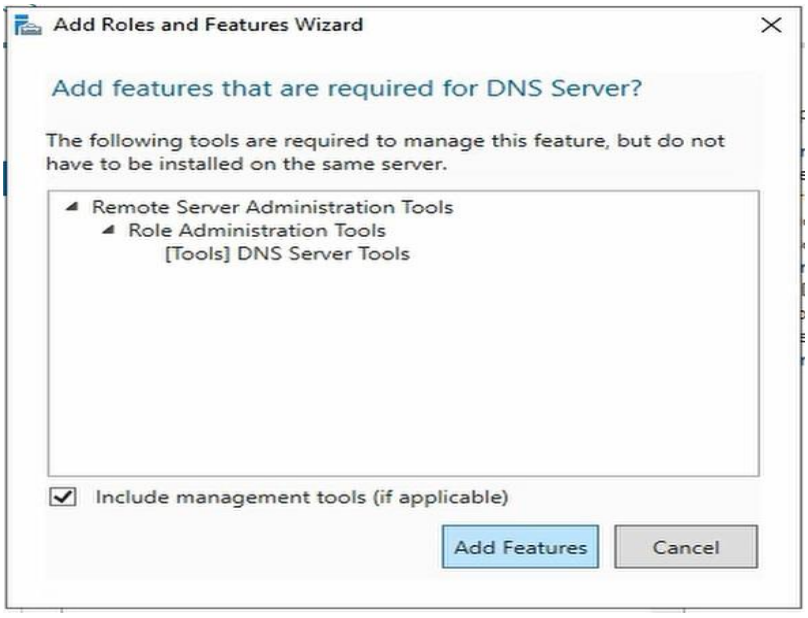


Figure 5 Add Features

4. From Server Roles lists select DNS server and click on Next.

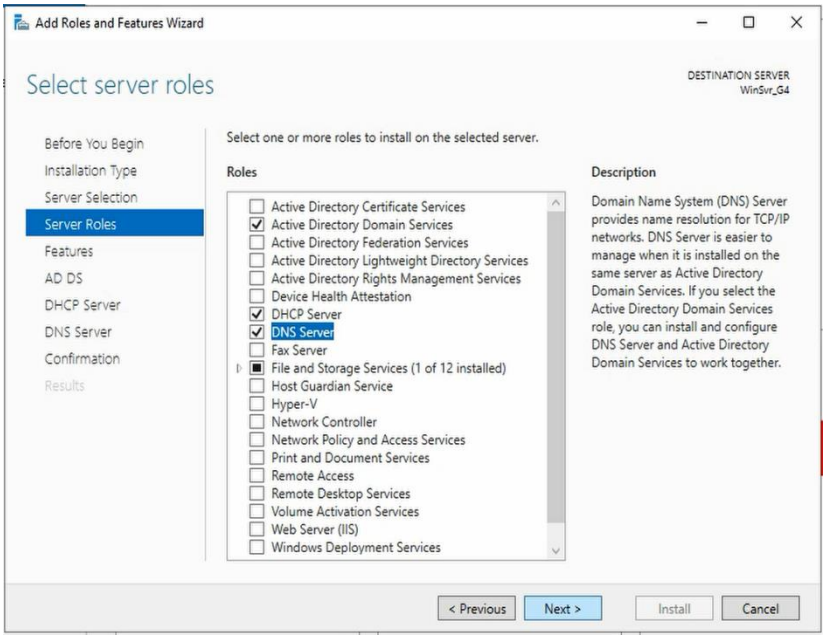


Figure 6 Choose DNS server

5. Click on Next

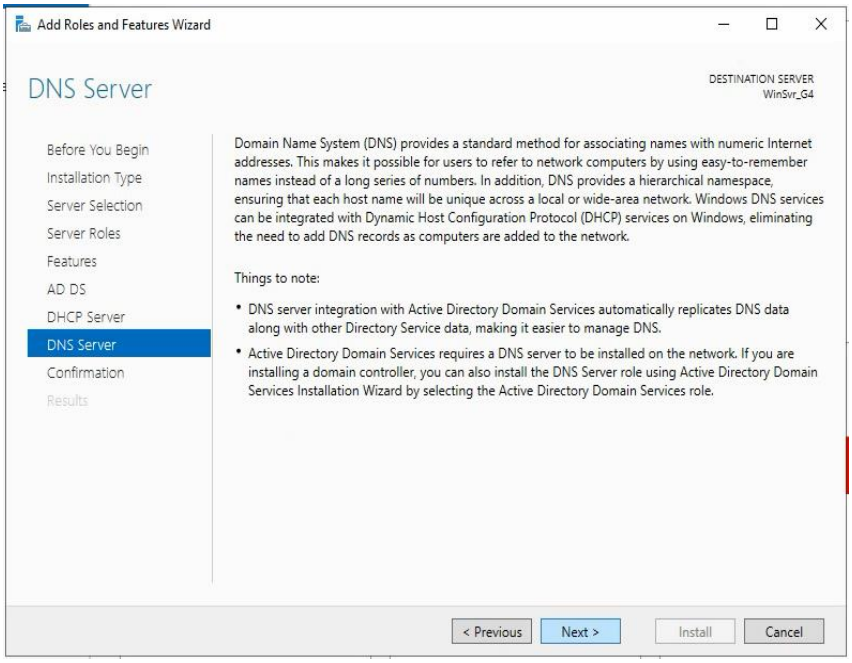


Figure 7 DNS server Information

6. To confirm installation click Install.

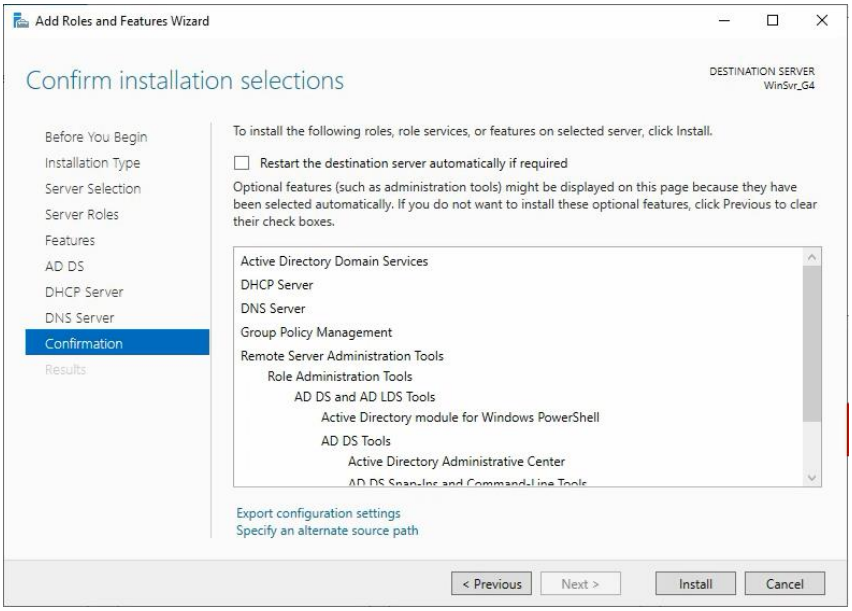


Figure 8 Installation confirmation

7. Installation process started; it may take few minutes.

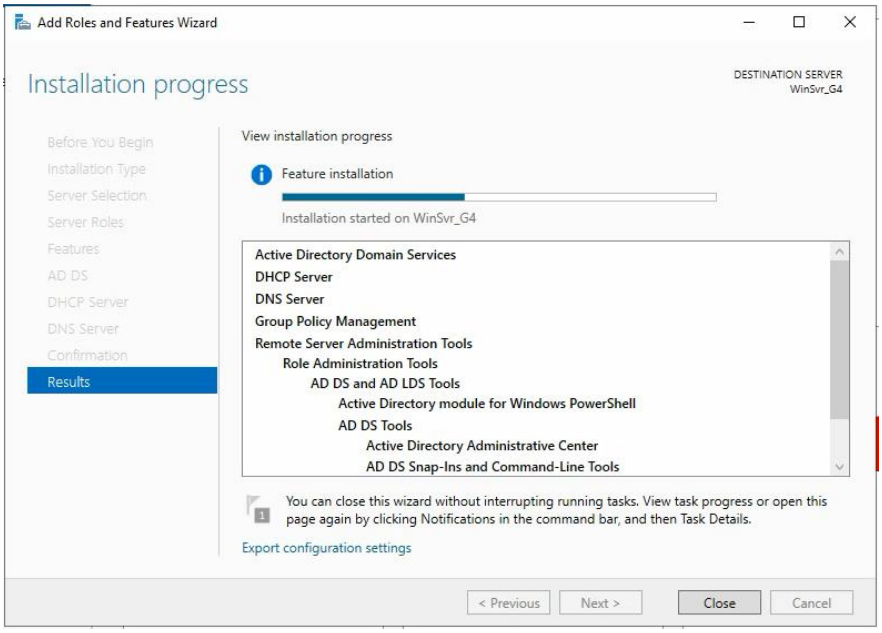


Figure 9 Installation progress

5.3.1.2 DNS IPv4 Configuration

1. Now, will configure our DNS server. Click on Tools in the upper right corner of Server Manager and click on DNS in the drop-down list.

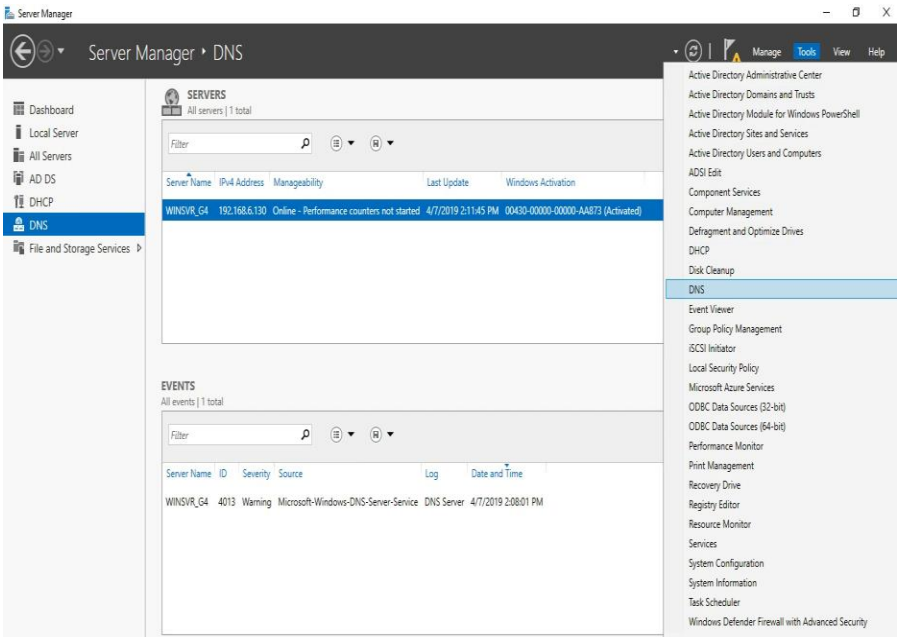


Figure 10 Tools DNS

2. Select server on the left side of DNS Manage. Right click and click on Configure a DNS Server.

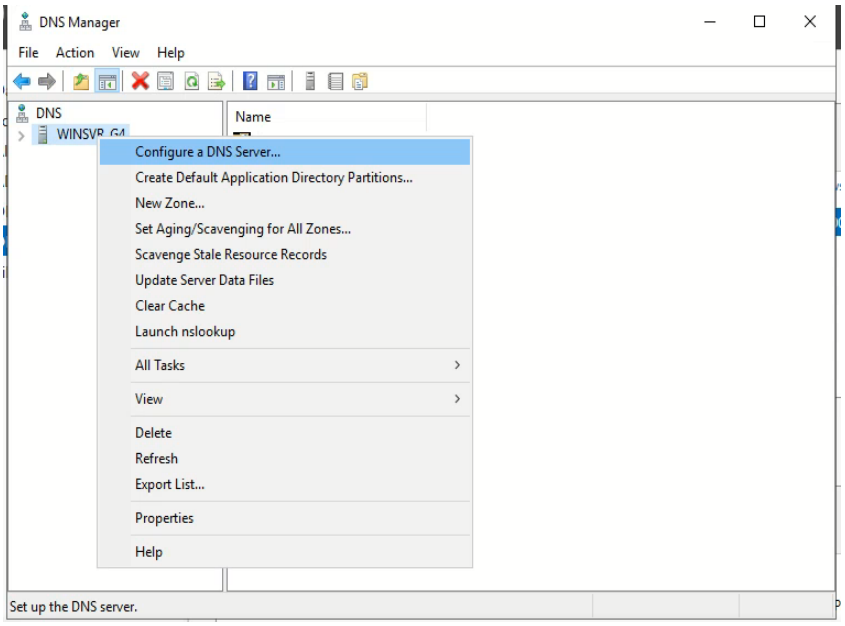


Figure 11 Configure a DNS Server

3. Choose Create forward and reverse lookup zones and click Next

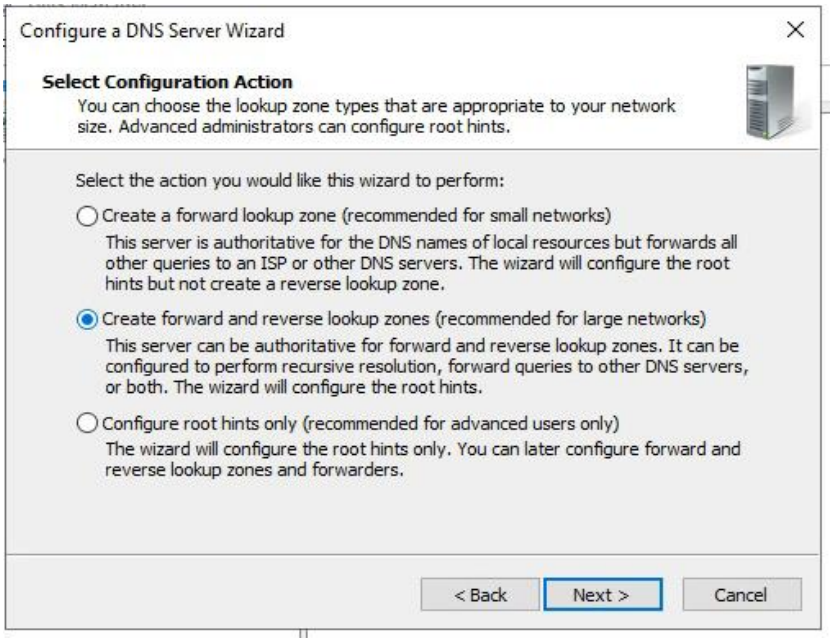


Figure 12 Create forward and reverse lookup zones

4. Choose Yes, create a forward lookup zone now and click Next

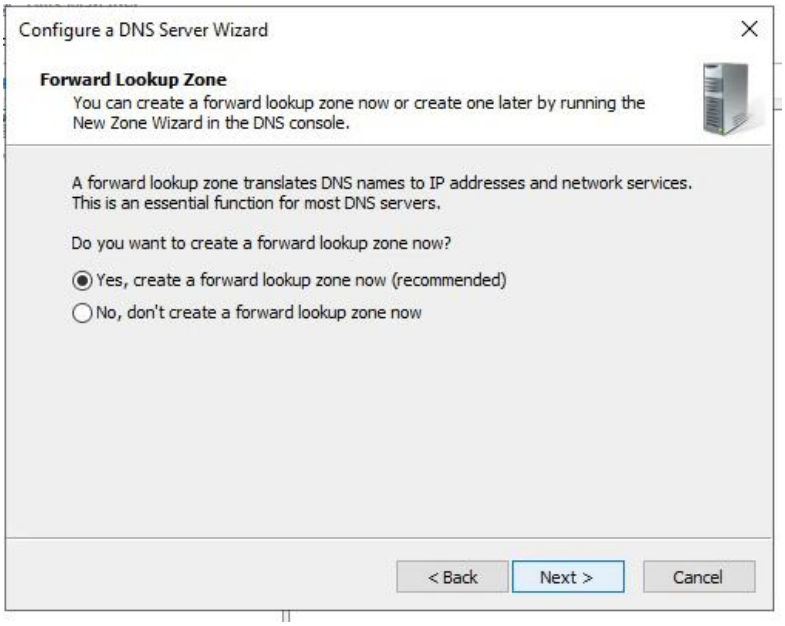


Figure 13 Forward Lookup Zone

5. In this step, the primary zone will be located in this Windows Server 2019. Choose Primary zone and click on Next to continue

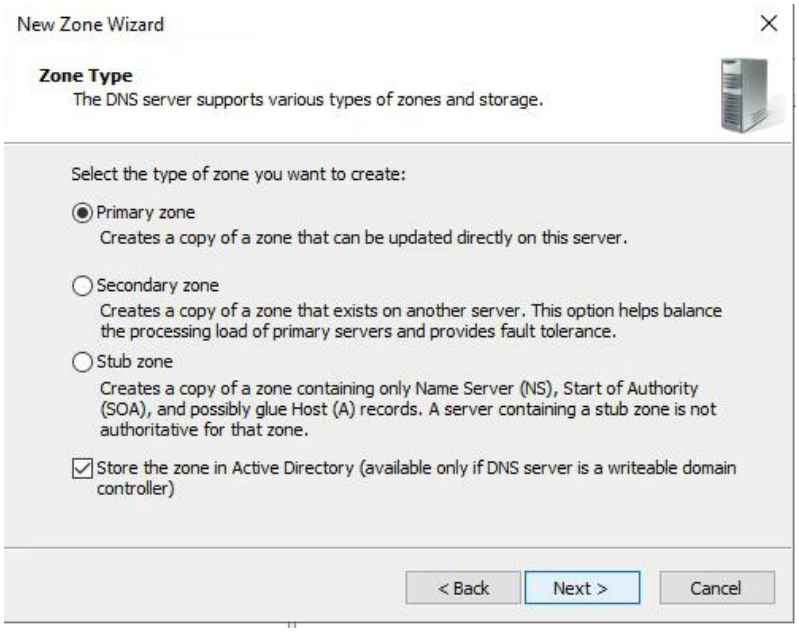


Figure 14 Choose type of zone

6. Enter any name for new zone file and click on Next button

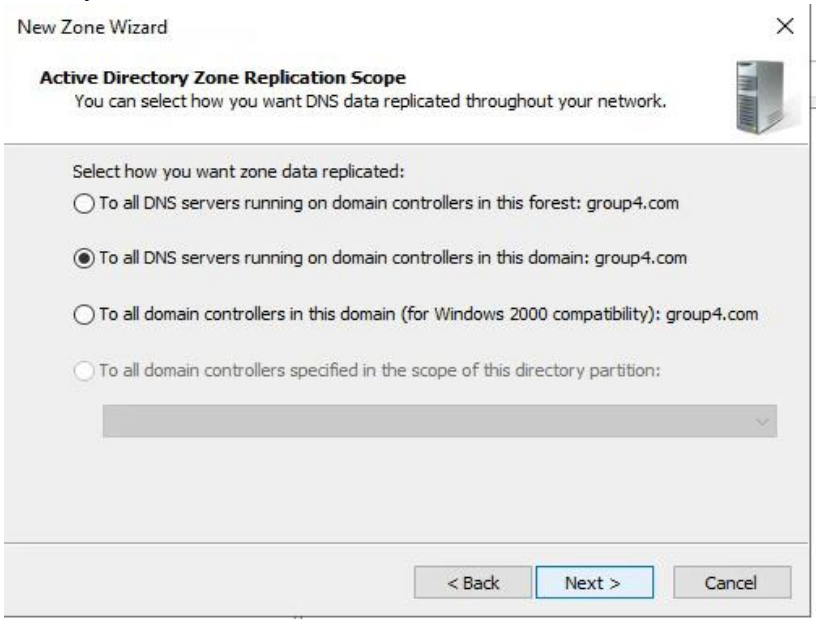


Figure 15 Select Active Directory Zone Replication Scope

7. Enter any name for new zone file and click on Next button

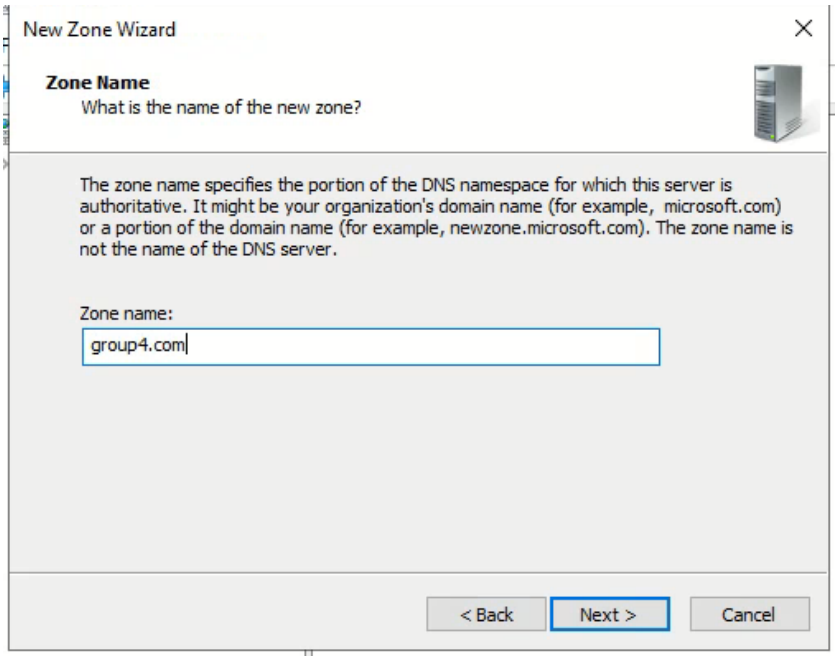


Figure 16 Name the new zone

8. Dynamic update is set to Allow both nonsecure and secure dynamic update. Then, click Next

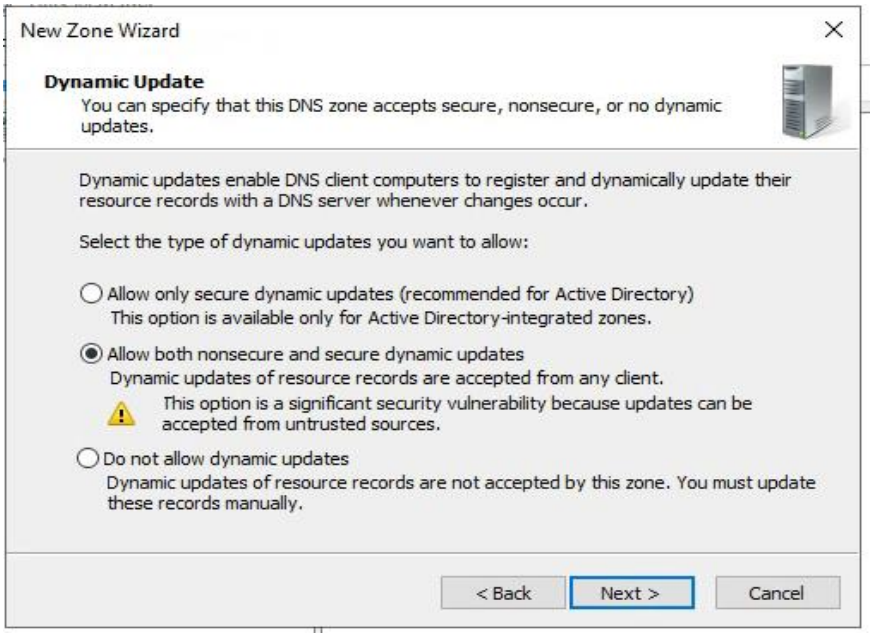


Figure 17 Dynamic update

9. So, this step is to setup reverse lookup zone. This step require to translate IP addresses to DNS names. Choose on create a reverse lookup zone now and click Next button.

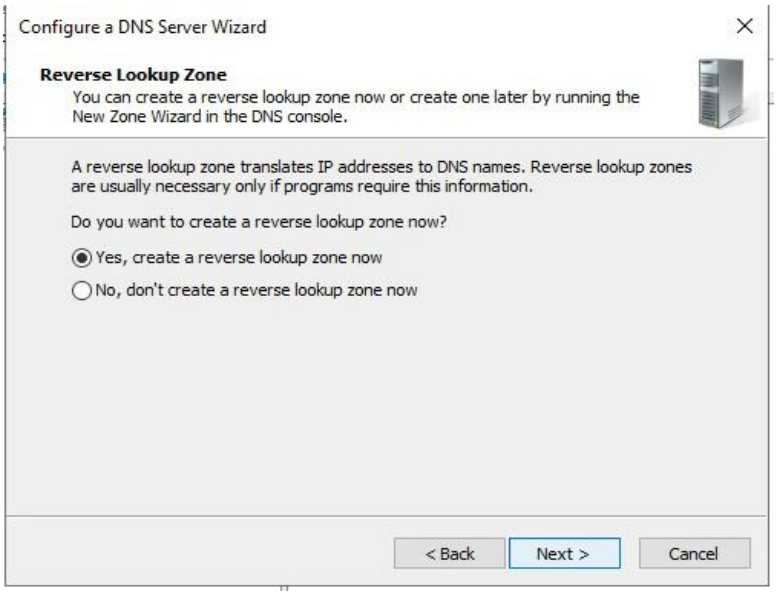


Figure 18 Creating a reverse lookup zone

10. Choose IPv4 Reverse Lookup Zone to create IPv4 addresses for reverse lookup. Then, click on Next button to continue

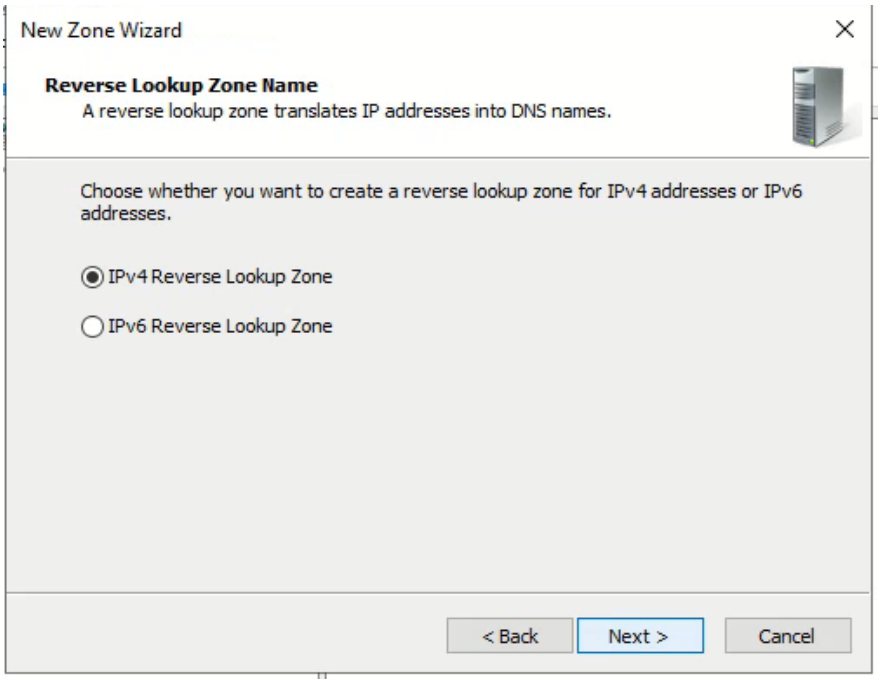


Figure 19 IPv4 reverse lookup zone

11. In Network ID field, enter the first three octets of the DNS Server IP address.

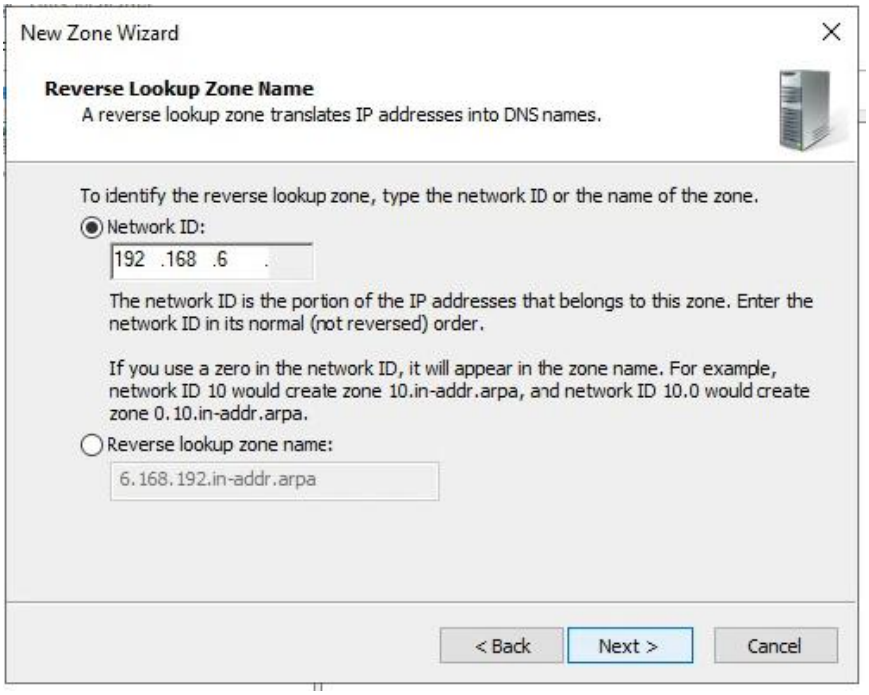


Figure 20 Reverse lookup zone name

12. Dynamic update is set to Allow both nonsecure and secure dynamic update. Then, click Next

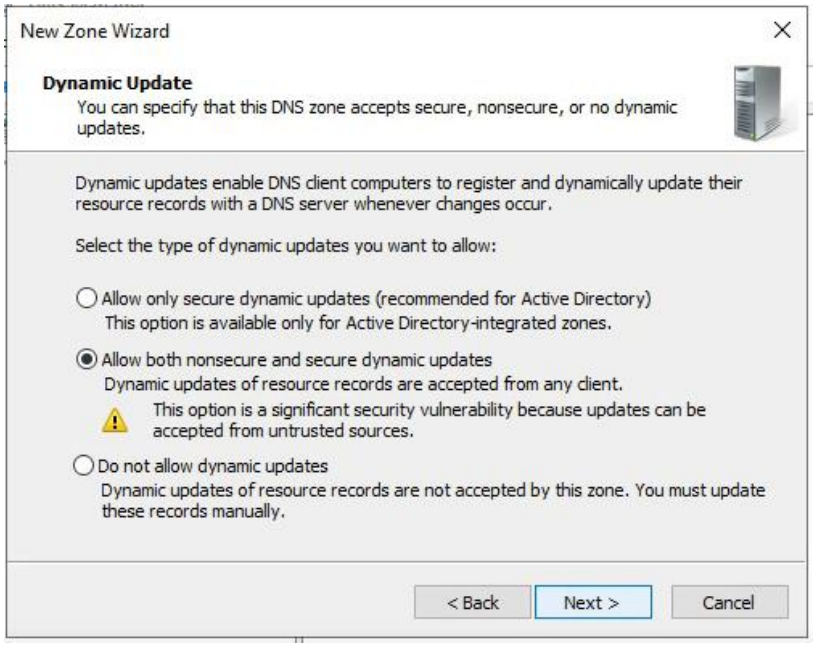


Figure 21 Dynamic update

13. Choose Yes, it should forward queries to DNS servers with the following IP addresses

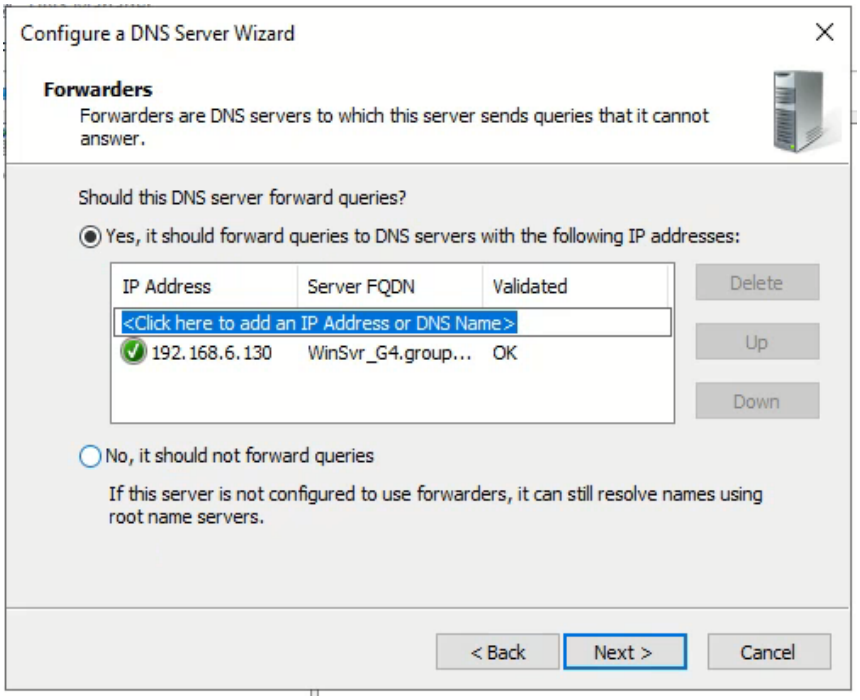


Figure 22 Forwarders to server sends queries

14. Click on Finish button and the DNS server is now configured and ready for use.

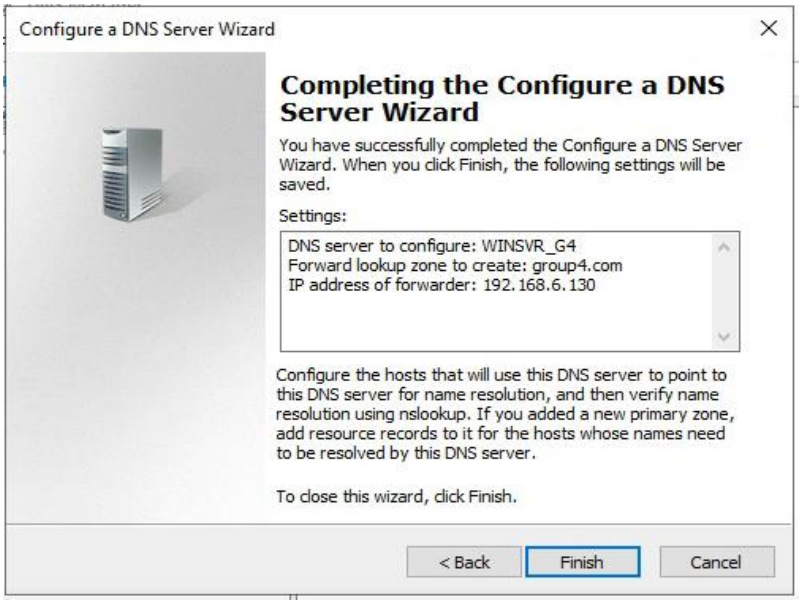


Figure 23 Completing the new zone wizard

5.3.1.2 IPv6 DNS Configuration

1. On Server Manager, select DNS. Right click on Reverse Lookup Zone and click New Zone. On the Welcome to New Wizard then click Next

Figure 24 New Zone Wizard

2. Then, choose Primary Zone. Tick on Store the zone in active AD. Then click Next

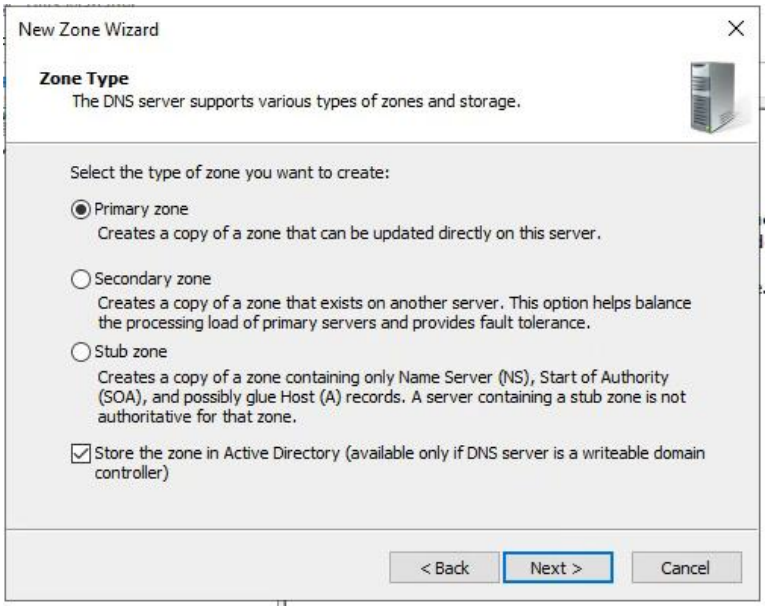


Figure 25 Choose zone type

3. Choose To all DNS servers running on domain controllers in this domain: group4.com then click Next

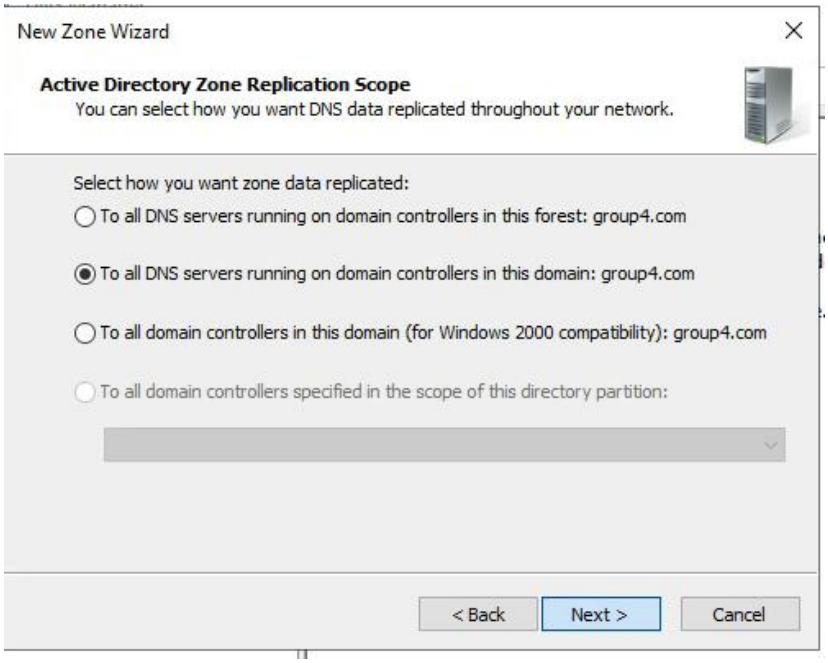


Figure 26 AD Zone Replication Scope

4. Then select IPv6 Reverse Lookup Zone then, Next

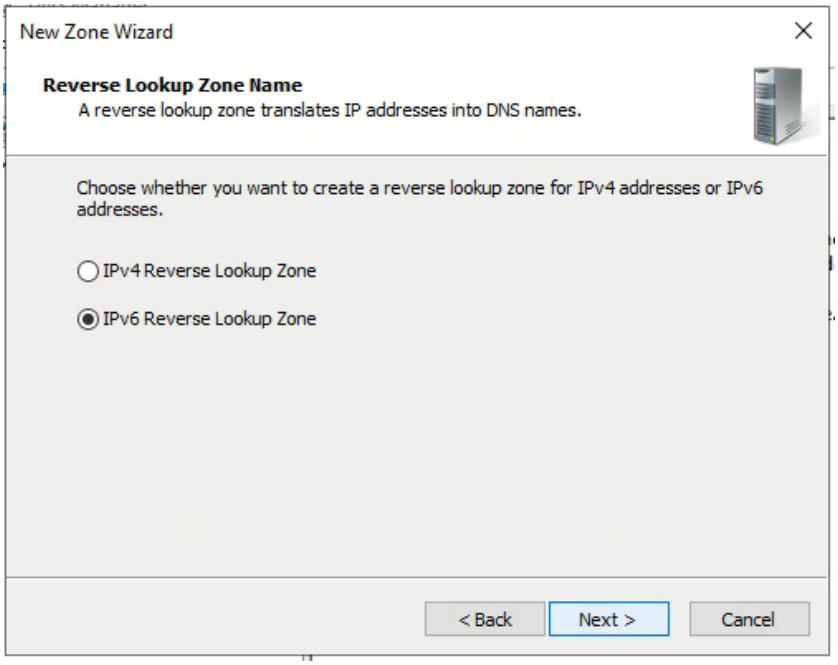


Figure 27 IPv6 Reverse Lookup Zone Name

5. Enter IPv6 Address Prefix and click Next

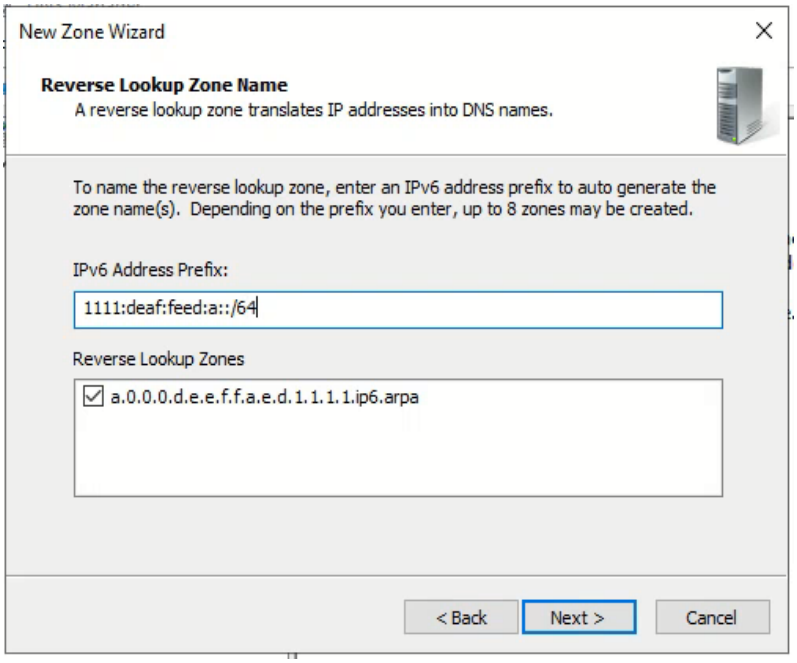


Figure 28 Enter IPv6 Prefix

6. Choose Allow both nonsecure and secure dynamic updates and proceed to Next

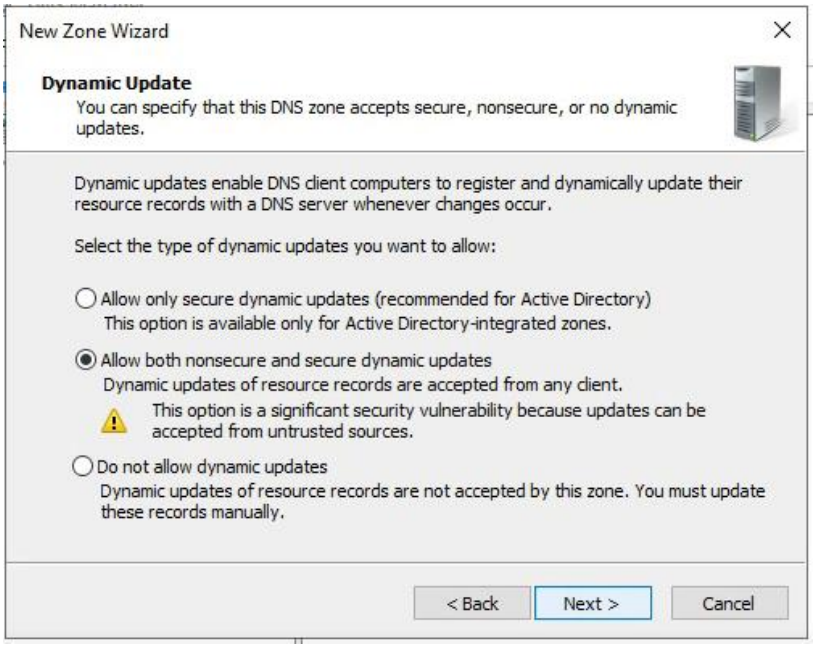


Figure 29 Dynamic Update

7. Successfully completed the New Zone Wizard. Click on Finish button

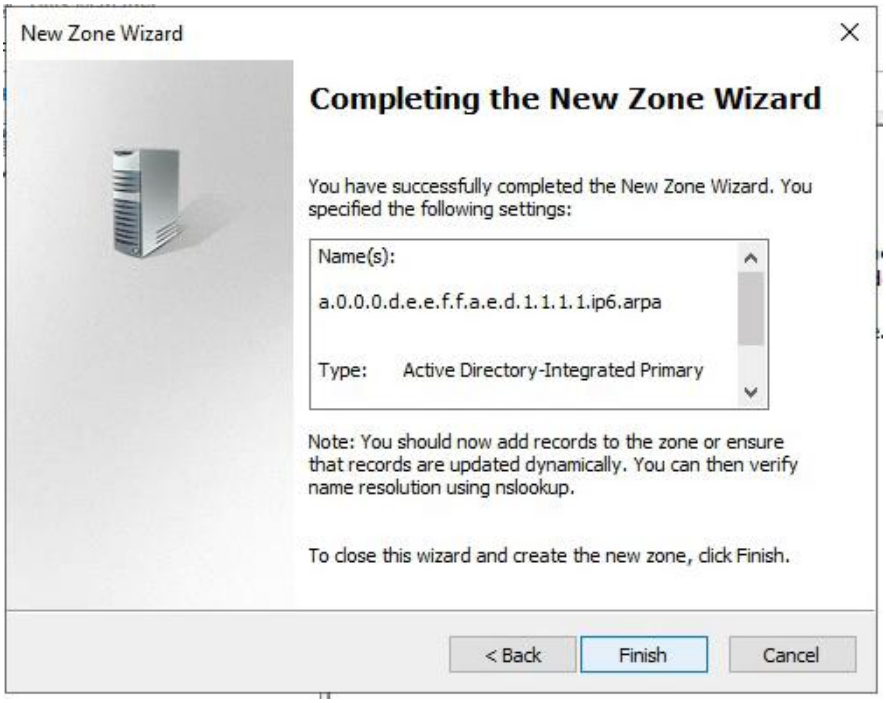


Figure 30 Completing the New Zone Wizard

5.3.2 DHCP IPV4/IPV6

DHCP (Dynamic Host Configuration Protocol) is a service that provides reliable IP address configuration and reduced network administration for clients to access the network. DHCP assigns a local IP address to devices connected to the local network from DHCP address pool. Network clients will be configured automatically by the DHCP service. Besides, any modification to the IP address of the router and DNS servers can be implemented easily.

5.3.2.1 Installation DHCP

1. In the Role Installation window select **Role-based or feature-based installation** then click **Next**.

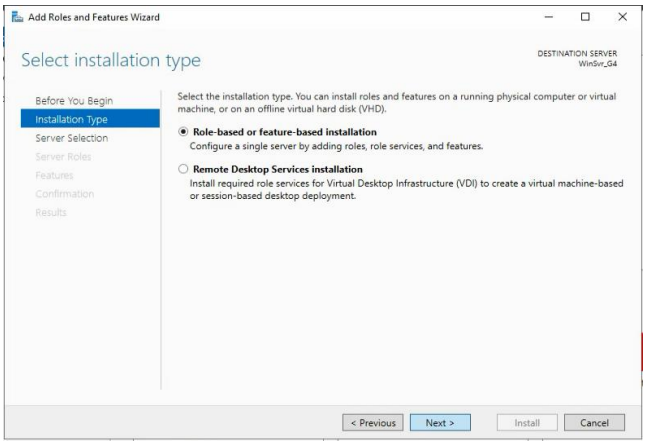


Figure 31 Installation type

2. Choose the server, want to install DHCP from the Server pool. Here, need one server and select by default.

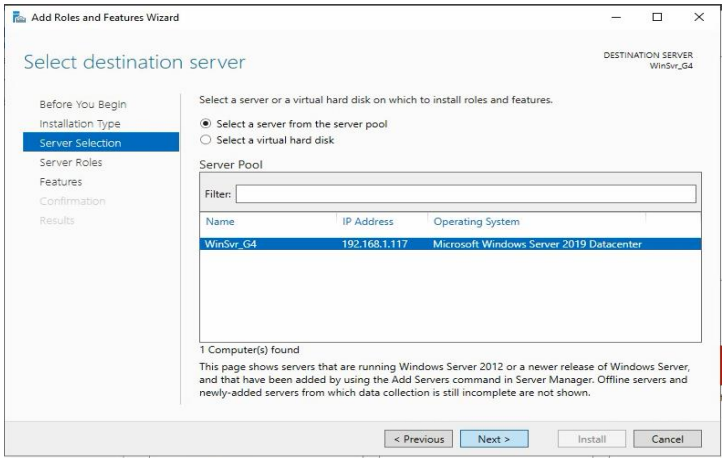


Figure 32 DHCP Server Destination Server

3. From the Roles list select DHCP Server. When the Add Roles and Features Wizard Page opened, click **Add Features** Then Click **Next**. That will install required features for DHCP Server.

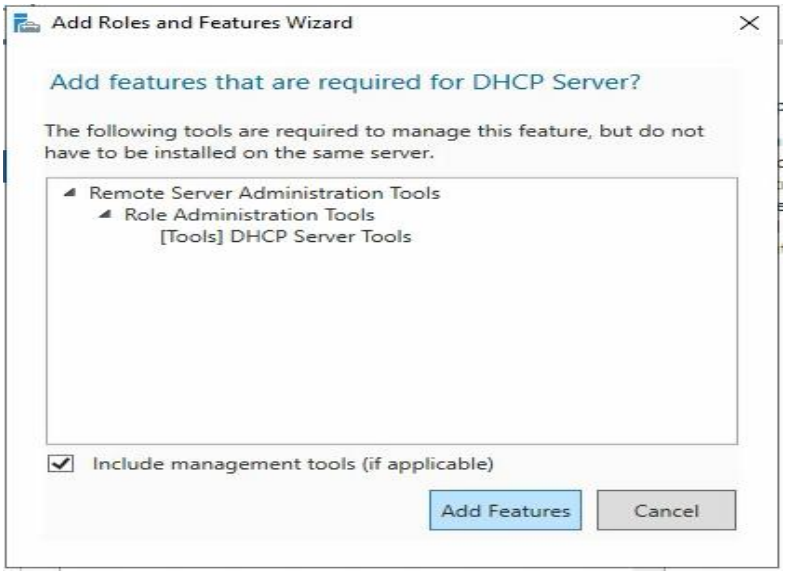


Figure 33 Add DHCP Server Role

4. In the Features window, do not change anything, just click **Next**

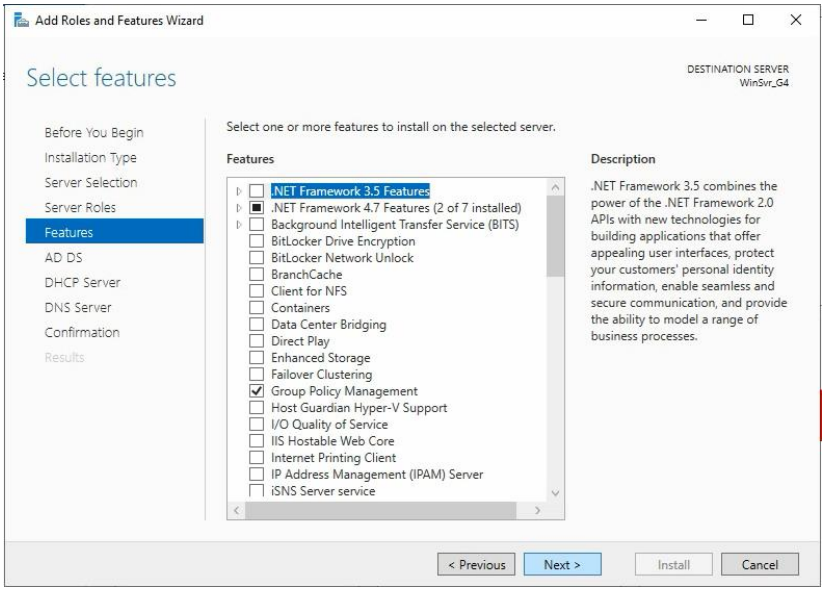


Figure 34 Windows Features

5. Once read the information about DHCP Server and click **Next** button.

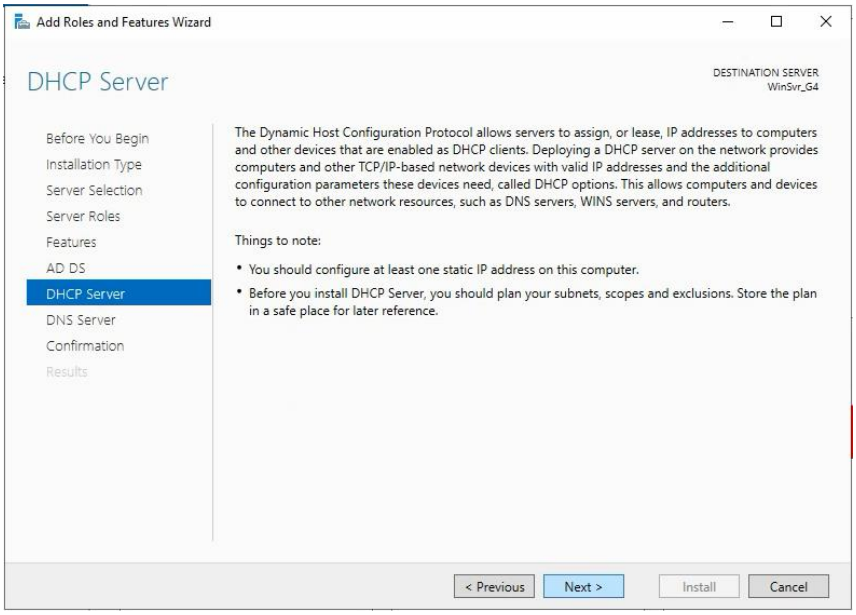


Figure 35 DHCP Server Information

6. In the Confirm Installation page, select **Restart the destination server automatically if required**. Click **Yes** the warning window and click **Install**.

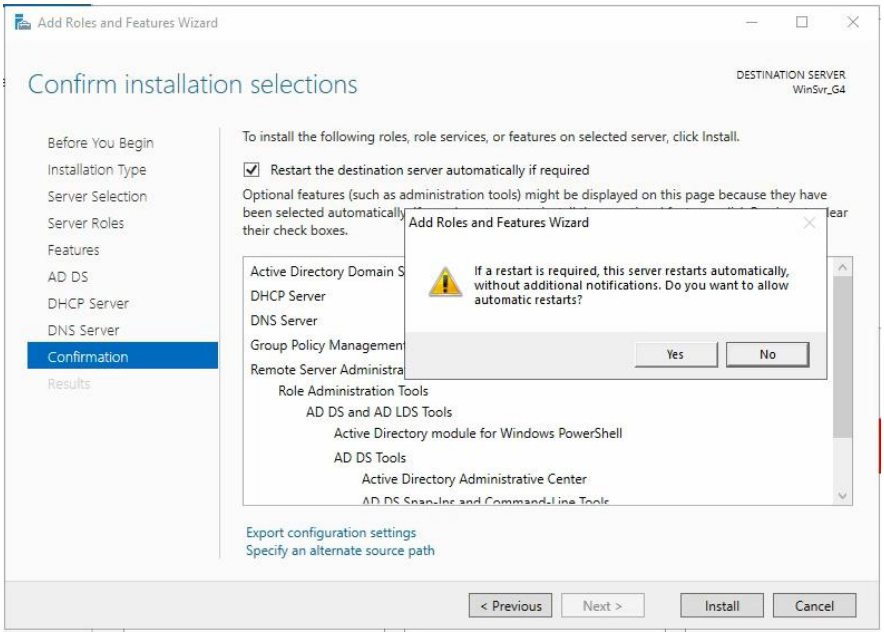


Figure 36 Restart Automatically

7. The installation will take a minute, when it has completed successfully click on notification. Then, click **Complete DHCP Configuration** link.

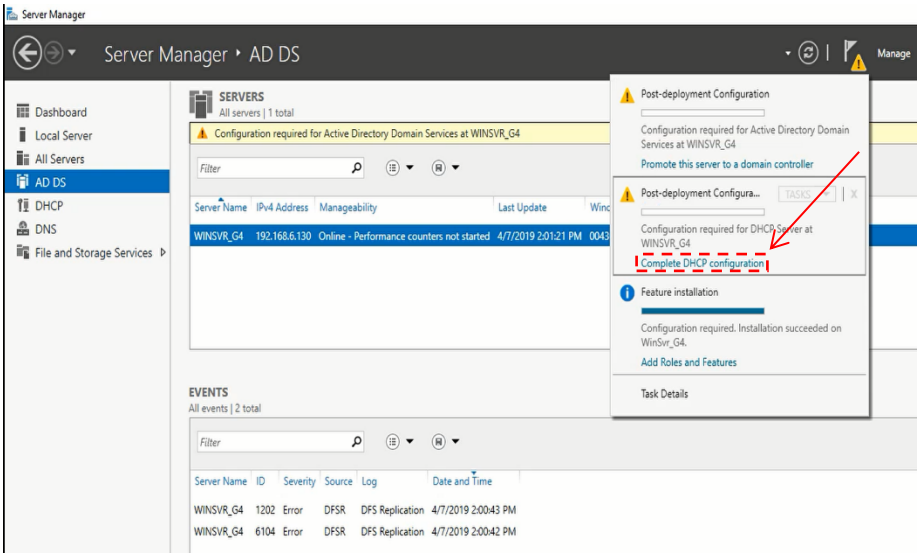


Figure 37 Configuration required for DHCP Server

8. Read DHCP Post-Install configuration wizard description and click **Next**.

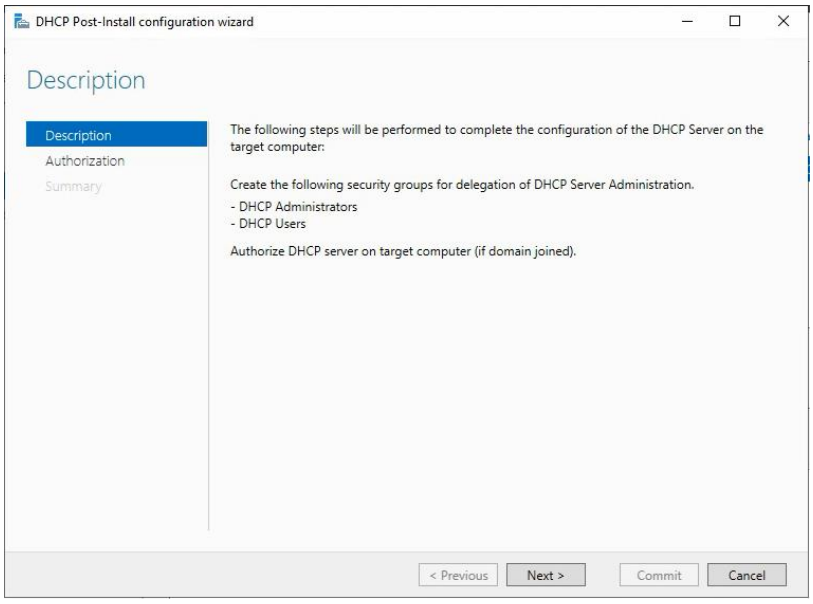


Figure 38 DHCP Post-Install

9. Set the appropriate user for management of DHCP Server. Here I leave it by default because the administrator (Group4.com) has the right privilege to perform DHCP Server configuration. Then, click on **Commit** to continue.

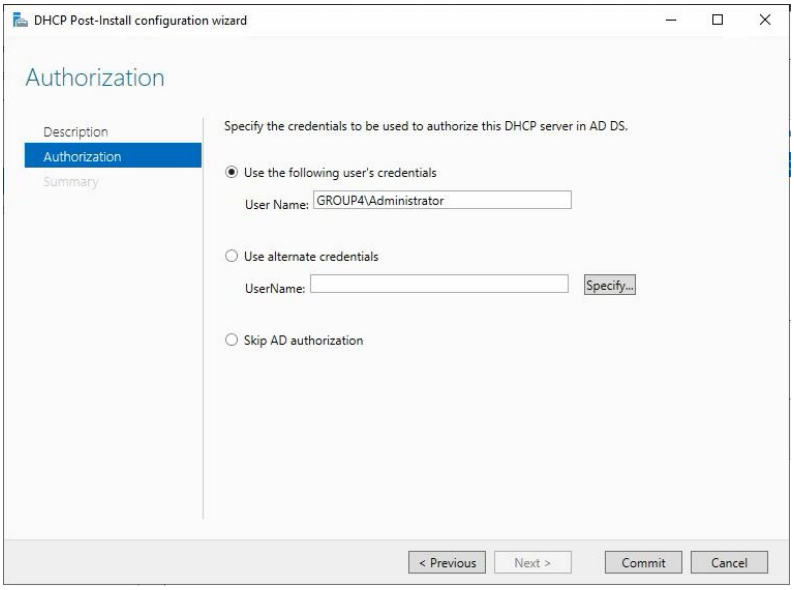


Figure 39 DHCP Authorization

10. Once DHCP Authorizing process done, click on **Close**

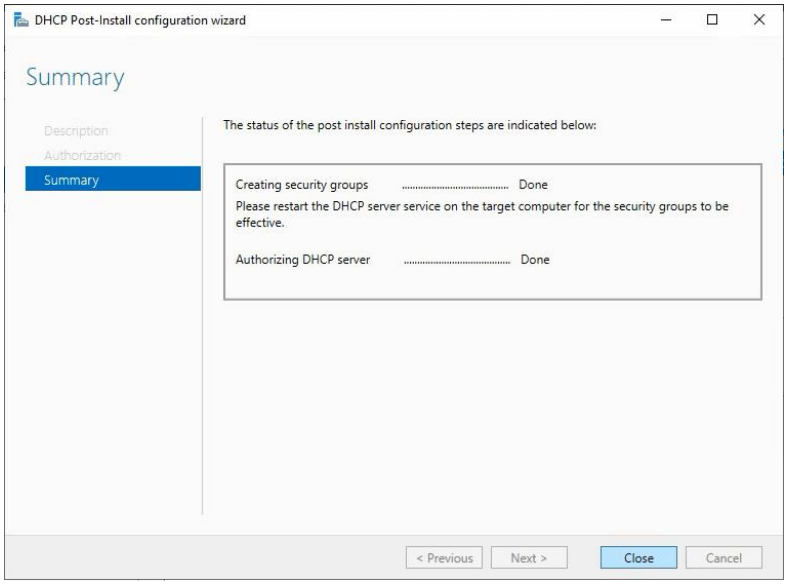


Figure 40 DHCP Summary

5.3.2.2 DHCP IPv4 Configuration

1. Open DHCP tools to create a New Scope for IPv4 Address

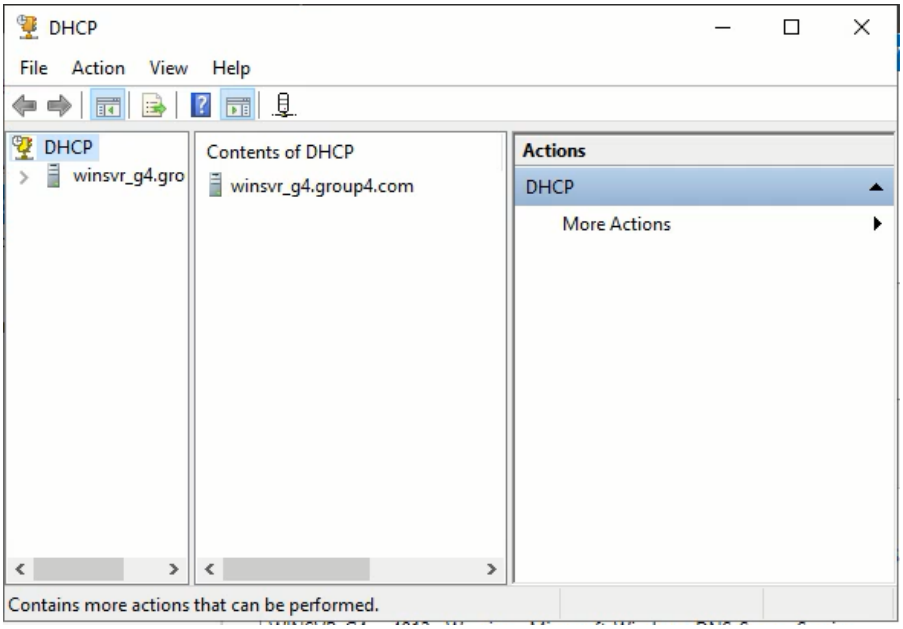


Figure 41 DHCP Tools

2. On DHCP Tools window expends the domain name and IPv4. Then, right click on the IPv4 and click **New Scope**

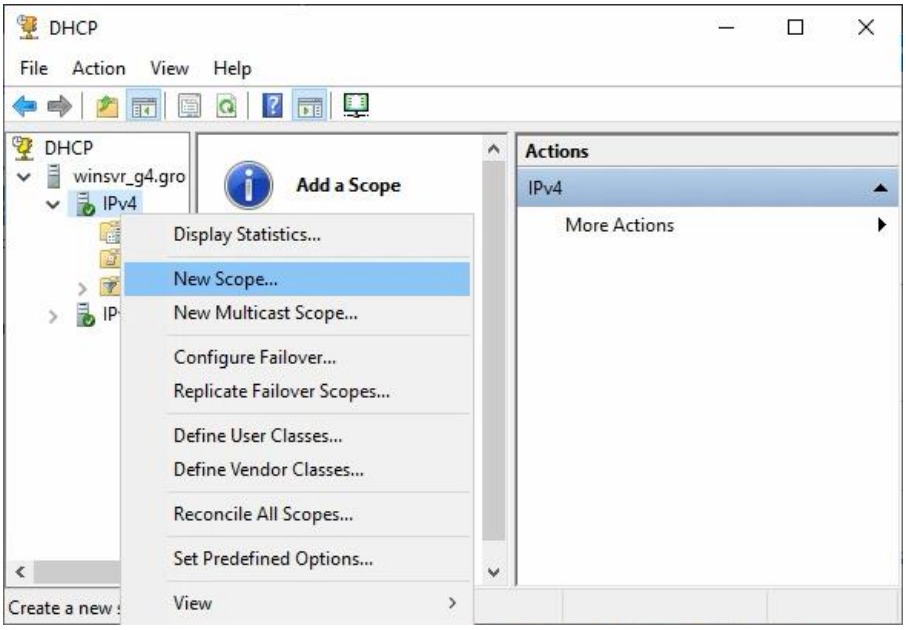


Figure 42 Create New Scope

3. Click **Next** on the New Scope Wizard page

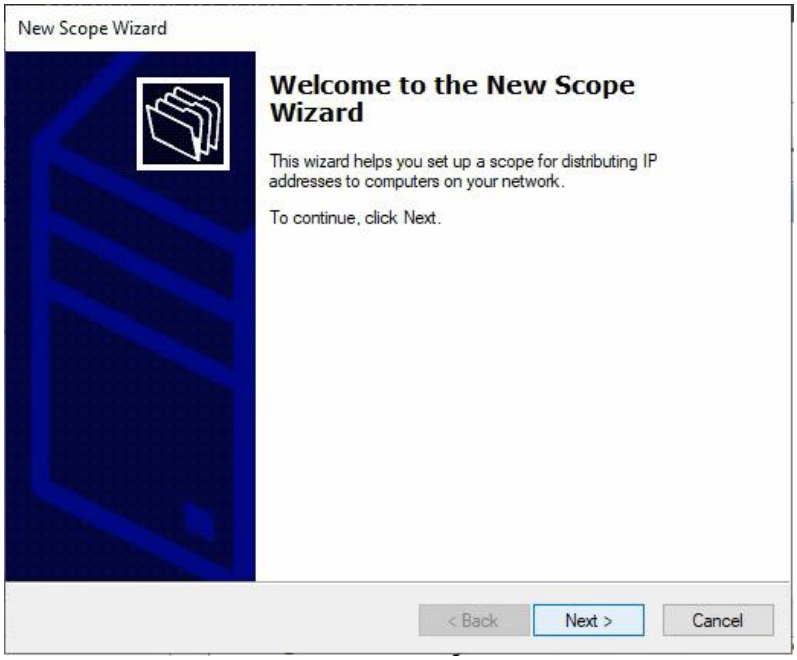


Figure 43 New Scope Wizard

4. In the scope, create a scope and write any description then click **Next**.

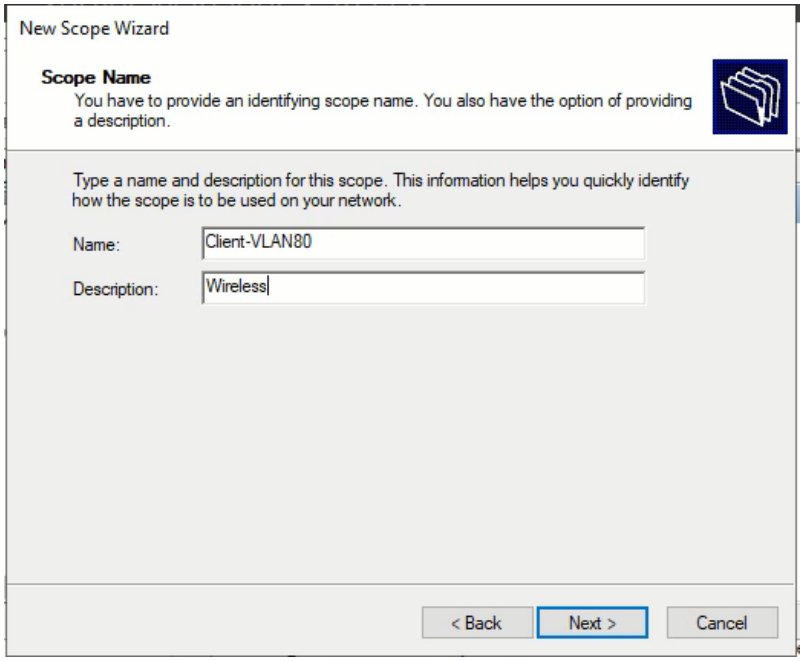


Figure 44 Scope Name and Description

5. Assign the start IP address range and the end IP address range. I need set from **192.168.1.67 to 192.168.1.126** which is a class C IP address. Leave the length 26 and click **Next**.

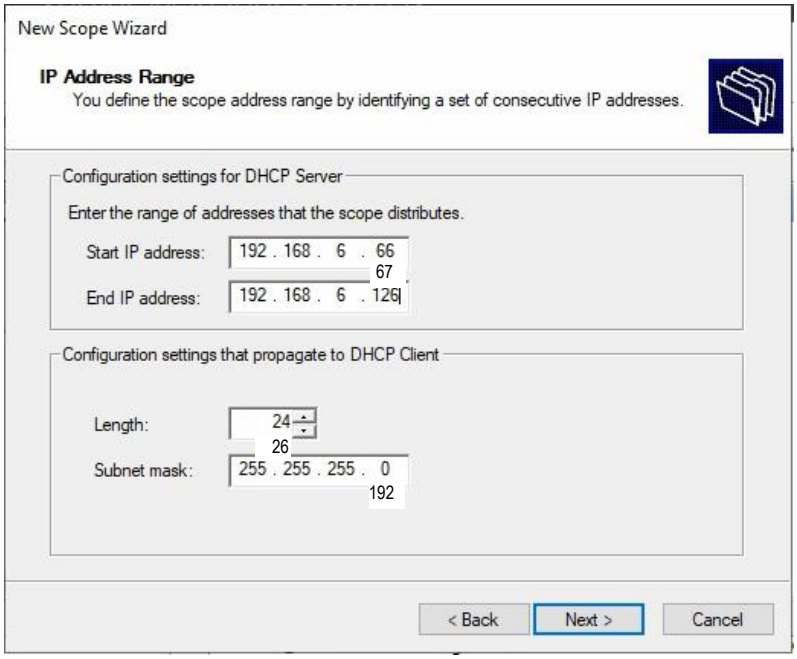


Figure 45 IP Address Range

6. Add the exclusive range prevent them from leasing to the client by DHCP Server. The IP address range which reserved is use for Network Servers and popular workstation. Just set the IP address and click Add button then click **Next**.

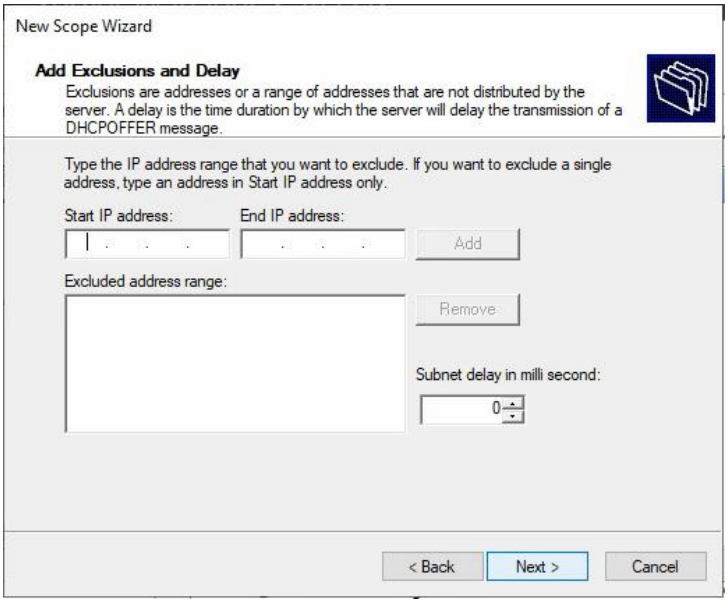


Figure 46 Add Exclusion

7. Let the Lease Duration by default and click **Next**

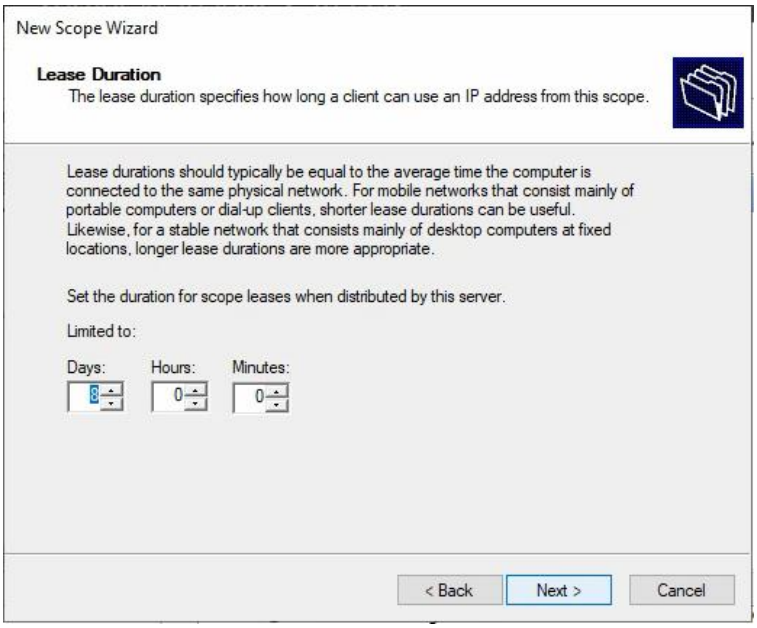


Figure 47 DHCP Lease Duration

8. Only click **Next** the Configure DHCP Options, and **Yes, I want to configure these options now** must be checked.

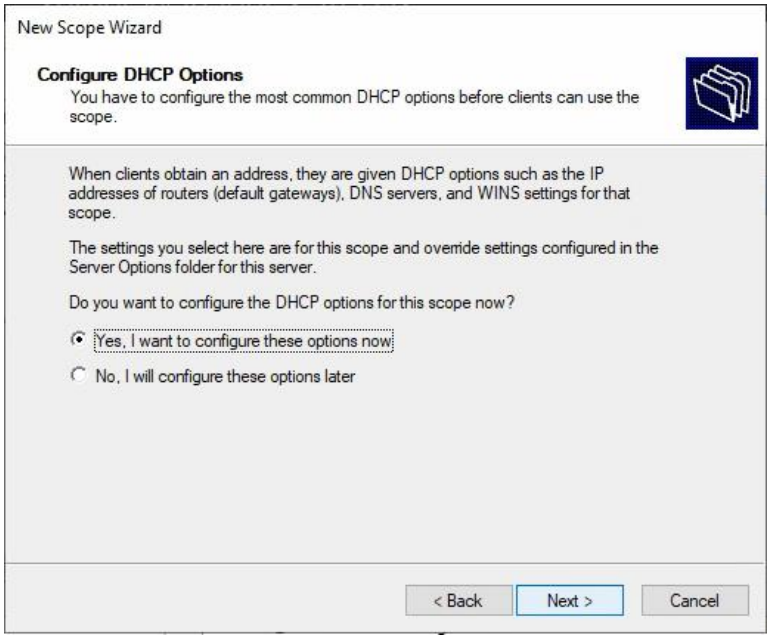


Figure 48 Configure DHCP Options

9. Set the router IP address and click Add button, then click Next.

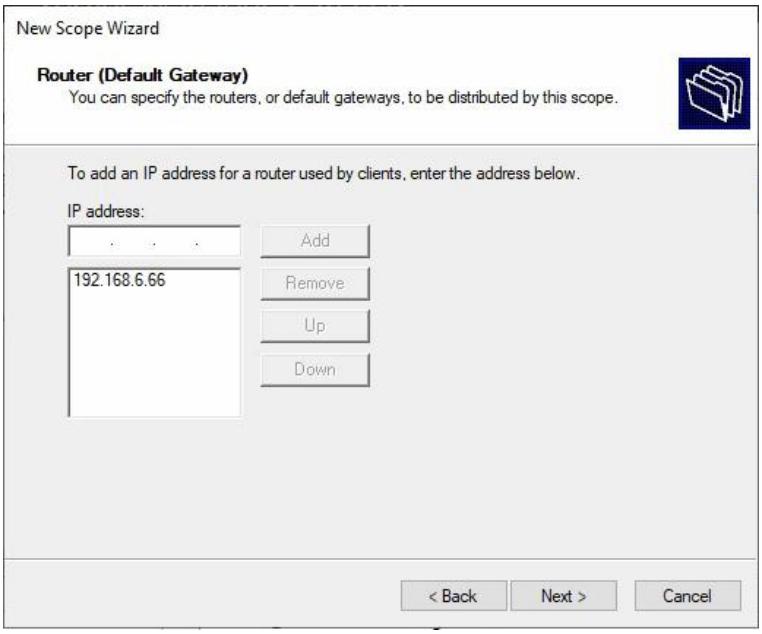


Figure 49 Router IP Address

10. Click **Next** to continue

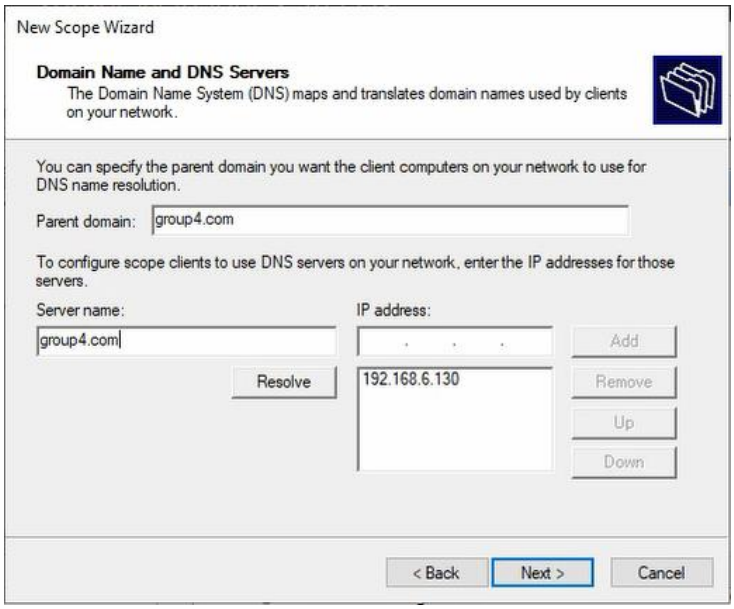


Figure 50 Domain Name and DNS Server

11. Active Scope, windows click **Next**. Be sure the **Yes, I want to active this scope now** must check.

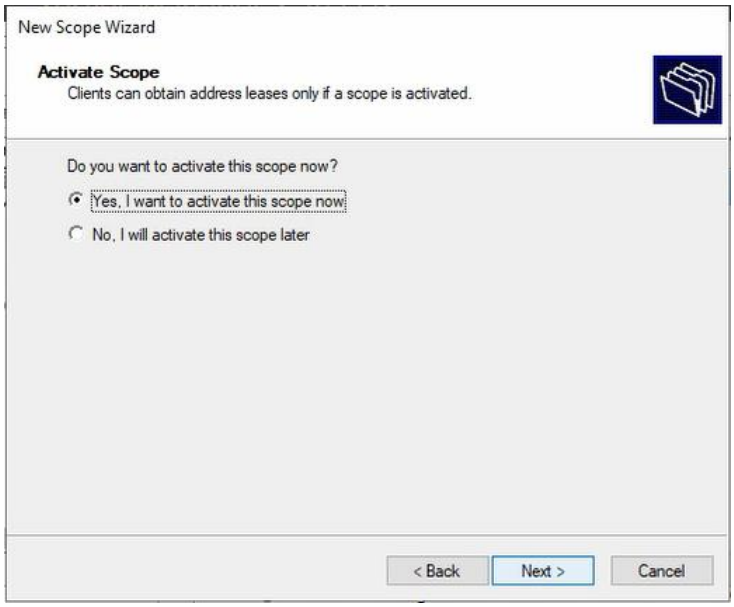


Figure 51 Activate Scope

12. Finally, click **Finish** to close and finalize the installation of DHCP Server in Windows Server 2019

Figure 52 Completing the New Scope Wizard

5.3.2.3 DHCP IPv6 Configuration

a. On router:

1. On each sub interface in the router, give the prefix of IPV6 IP address and on the Client sub interface set the IP helper-address to redirect the Client PC to the DHCP server.

```
interface FastEthernet0/0.80

 ip address 192.168.6.65 255.255.255.192
 ip helper-address 192.168.6.130
 ip nat inside
 ip virtual-reassembly
 ipv6 address 1111:DEAF:FEED:A::5/64
 ipv6 enable
 ipv6 dhcp relay destination 1111:DEAF:FEED:A::2 FastEhternet0/0.80
 ipv6 ospf area 0
```

Figure 53 Router Command

b. On Windows Server:

1. Open the DHCP services, find IPV6 on the left-panel Then, right-click and choose **new scope**.

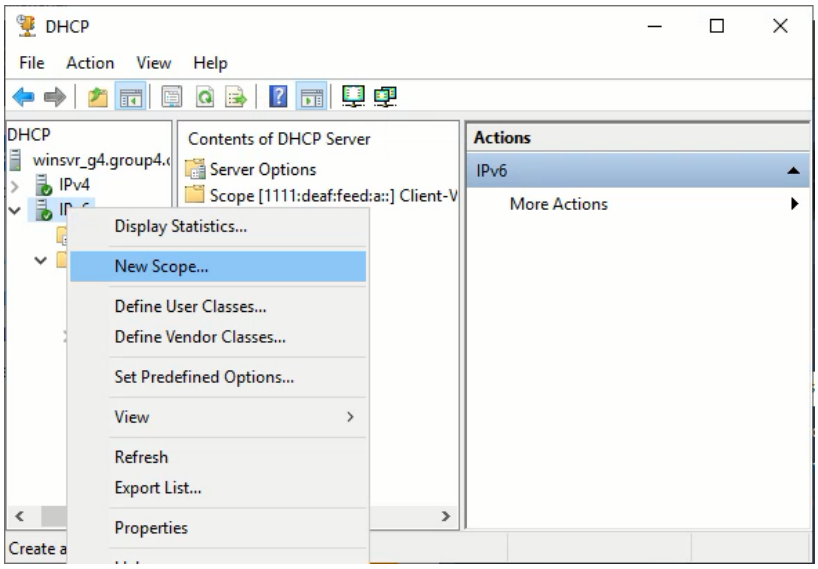


Figure 54 New IPv6 Scope

2. Click **Next** to set a new scope for IPv6

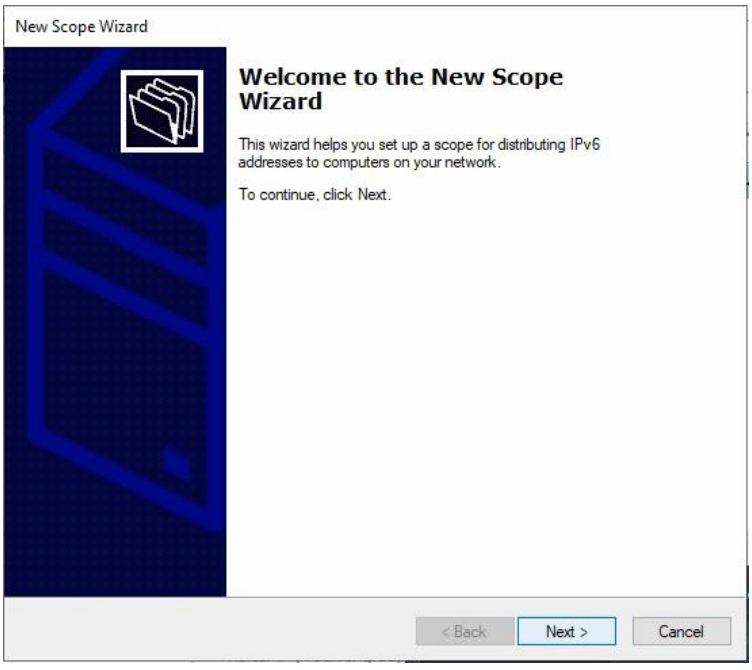


Figure 55 New Scope Wizard

3. Insert the scope name and description depend on design and planning

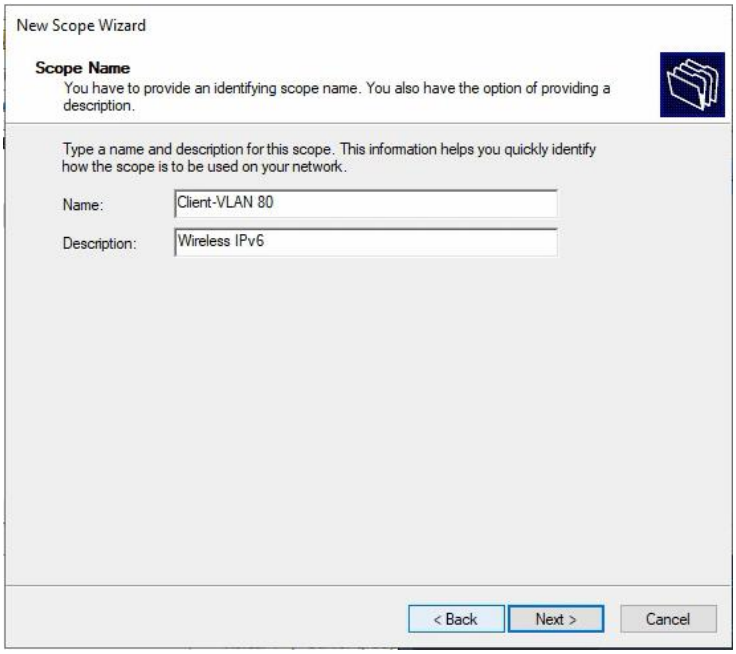


Figure 56 Scope Name and Description

4. In the scope prefix panel, insert the prefix IPv6 for the client. The prefix concept is same with subnet mask in IPv4, it determines the range of IP address and determine the subnet of the network.

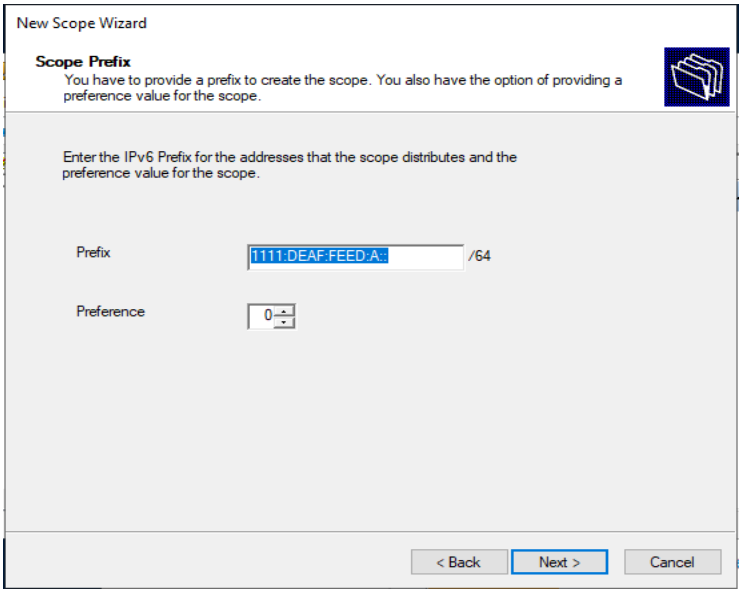


Figure 57 Scope Prefix

5. In the add exclusion tab, insert the IP address that need to be excluded (if needed).

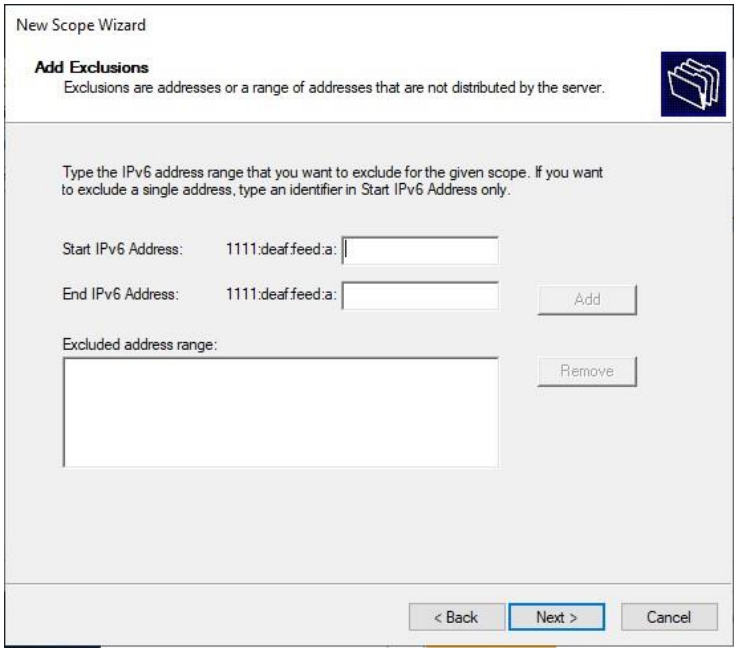


Figure 58 Add Exclusion

6. In the scope lease, insert the duration for the IP leases. Then, click **Next** to continue

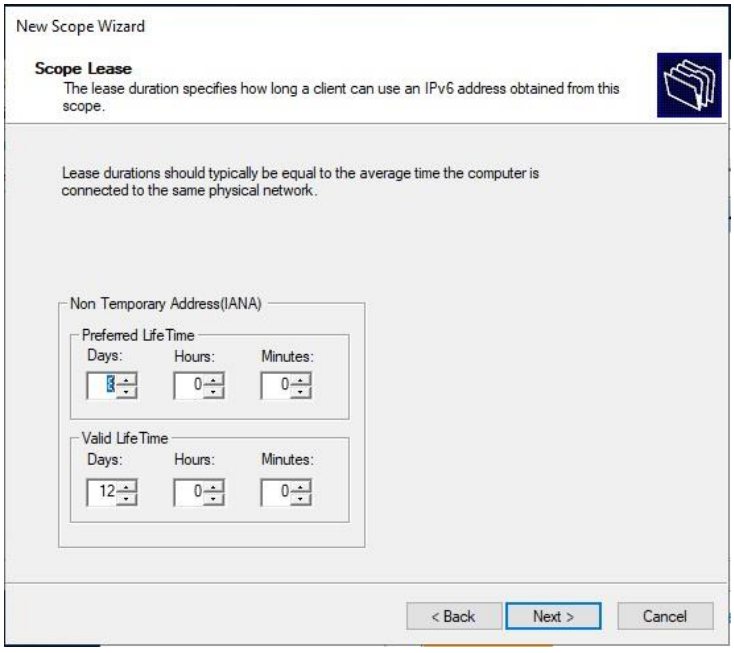


Figure 59 Scope Lease

7. Make sure to choose “Yes” for activate scope now. Then, click **Finish** to activate.

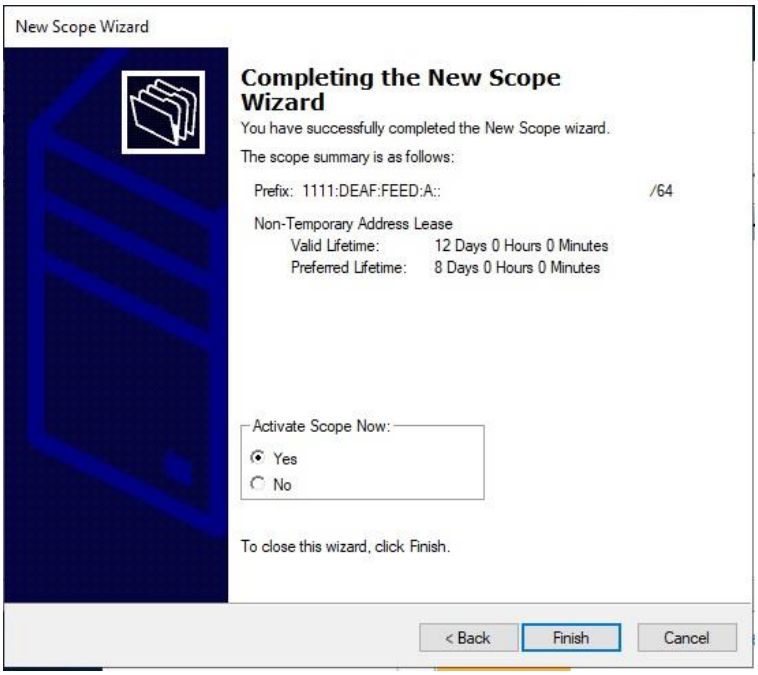


Figure 60 Completing the New Scope Wizard

5.3.3 IPv6 Web and IPv6 Tunneling

5.3.3.1 IPv6 Web

Step 1: Open IIS manager and click add website.

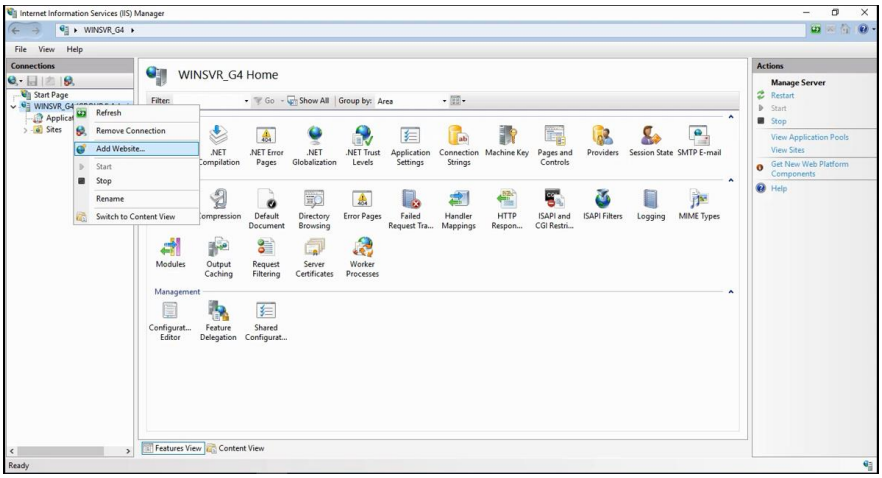


Figure 61 Server Manager Properties

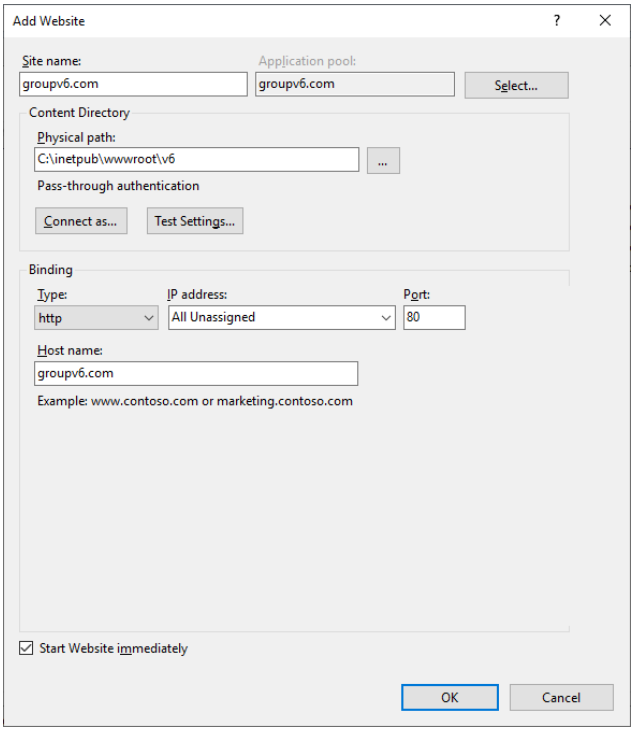


Figure 62 Enter site name, bindings, and host name then press ok

Step 2: Create default document and save as html file in the directory and Add default document that we create in IIS.

Step 3: Open DNS Manager, create new Forward Lookup Zone and add host for www.groupv6.com.

Step 4: Add new zone

Step 5 : Select zone type as primary zone

Step 6 : Choose the second choice

Step 7 : Enter zone name as www.groupv6.com

Step 8 : Choose allow both nonsecure

Step 9: Complete New Zone Creation

Step 10*:* Right click on the zone and choose new host

Step 11*:* Create static ipv6

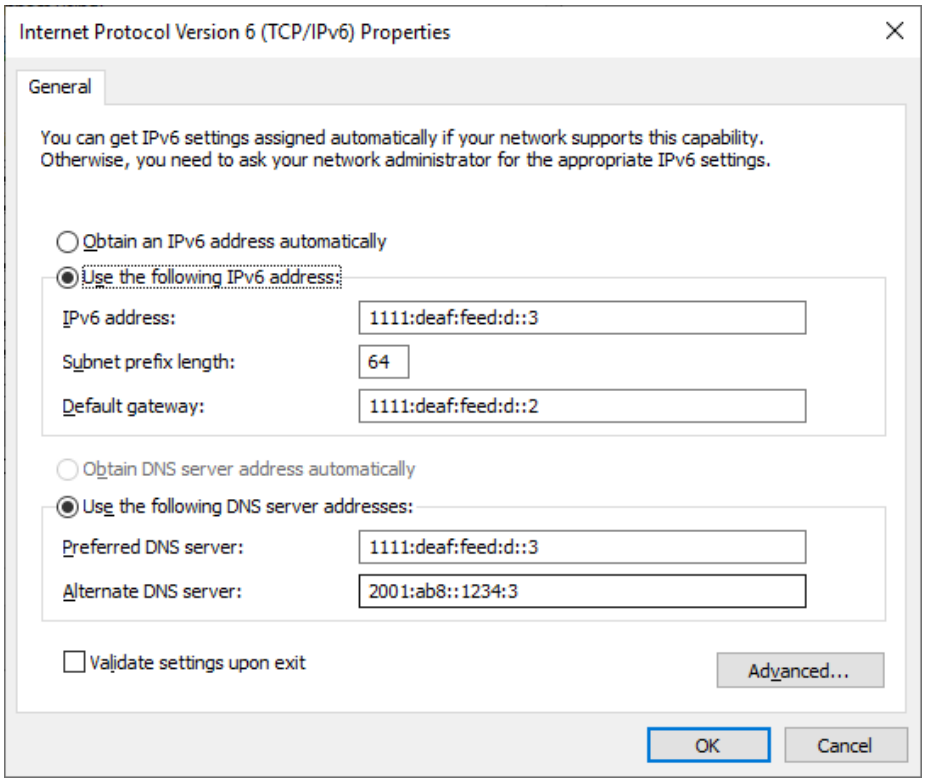


Figure 63 ipv6 static

5.3.3.2 Tunneling Configuration

Step 1: Login into router and use config terminal command to start the configuration, then define the interface tunnel number and setup an IPv6 address for the tunneling.

Step 2: Enter the interface tunnel 1

```
interface Tunnel1
 no ip address
 ipv6 address 2008:C0A8:800::9/123
 ipv6 enable
 ipv6 ospf 10 area 0
 tunnel source Serial0/2/0
 tunnel destination 200.200.200.2
 tunnel mode ipv6ip
!
```

Figure 64 ipv6 tunneling configuration

Step 3: Enter the public osfp on every vlan

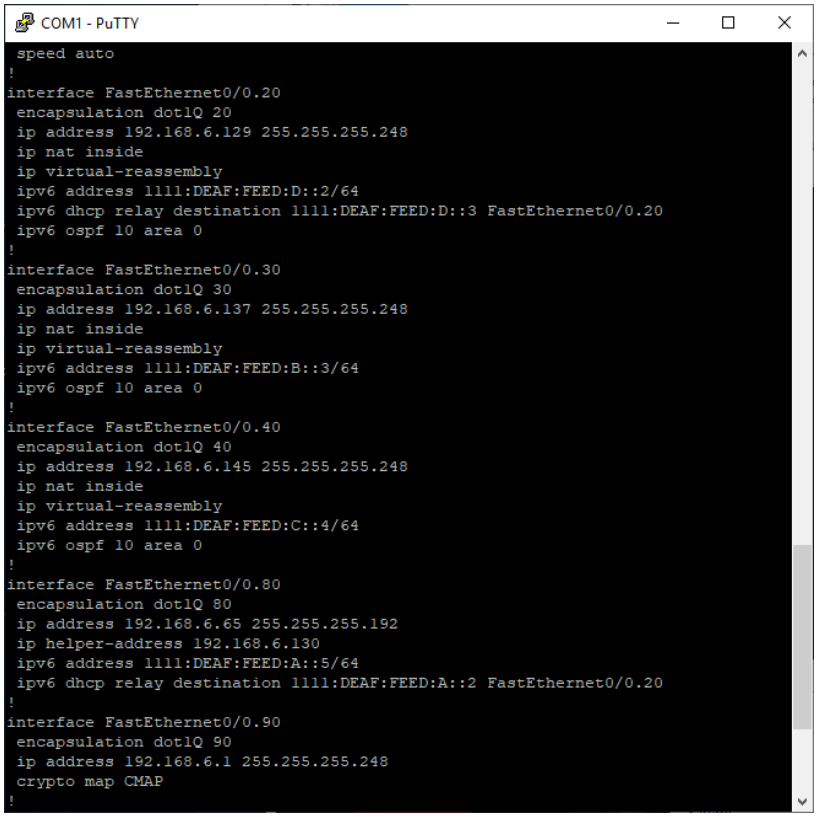


Figure 65 set ospf

5.3.4 Web, SSL and Virtual Hosting

5.3.4.1 Web Installation

1. Open the Server Manager and click Add Roles and Features

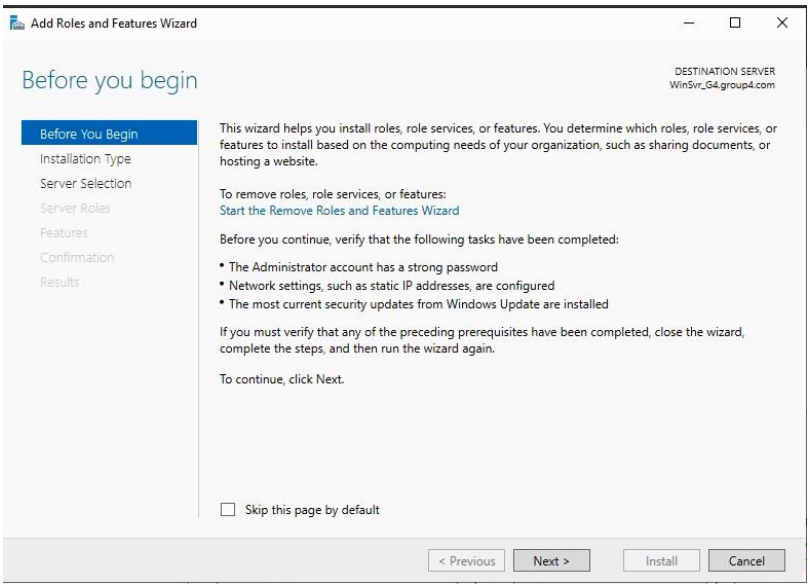


Figure 66 Add roles and features

2. On the Installation Type page, select Role-based or feature-based installation to configure a single server. Click Next.

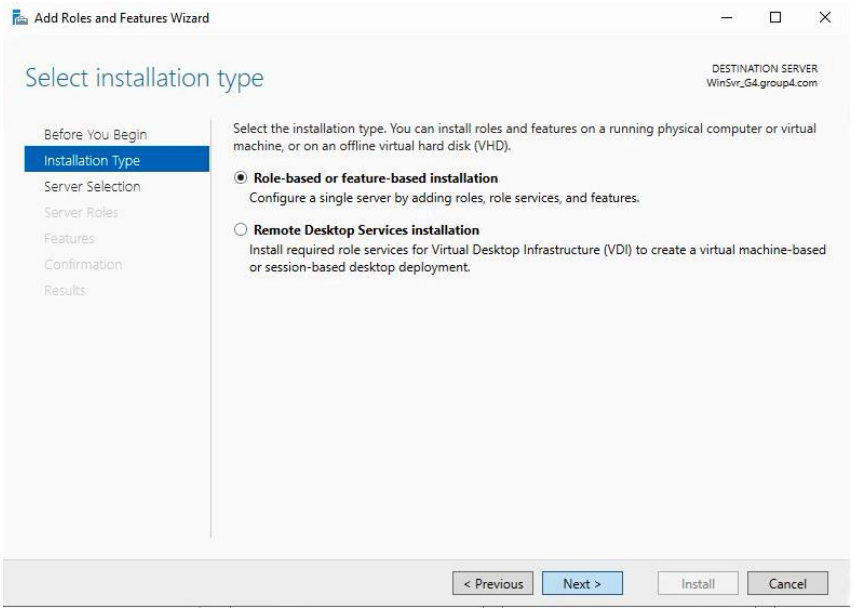


Figure 67 Select installation type

3. On the **Server Selection** page, select **Select a server from the server pool**, and then select a server; or select **Select a virtual hard disk server**, select a server to mount the VHD on, and then select a VHD file. Click **Next.**

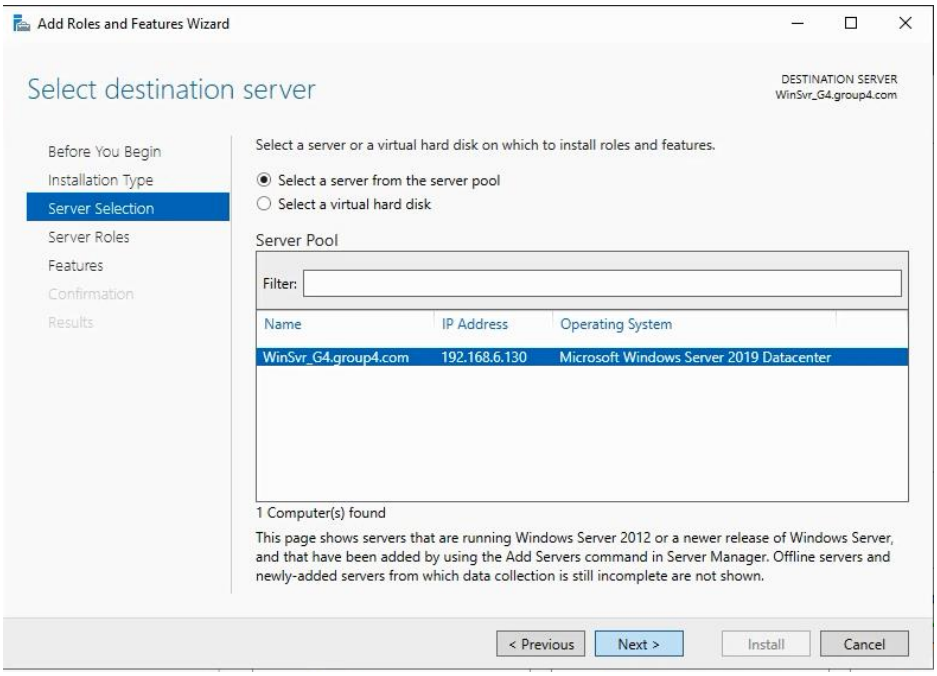


Figure 68 Select destination server

4. On the **Server Roles** page, select **web Server (IIS)**

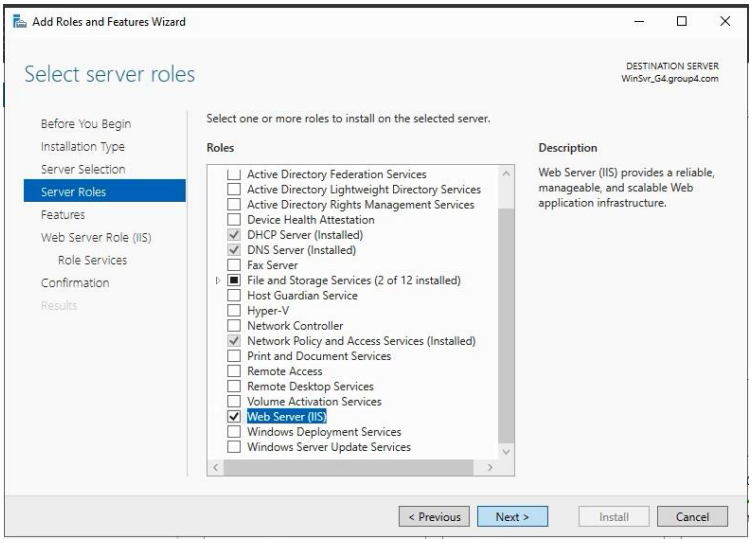


Figure 69 Select server roles

5. In the **Add Roles and Features** wizard, click **Add Features** if , want to install the IIS Management Console. If, do not want to install the Management Console, uncheck I**nclude management tools (if applicable)**, and then click **Continue.**

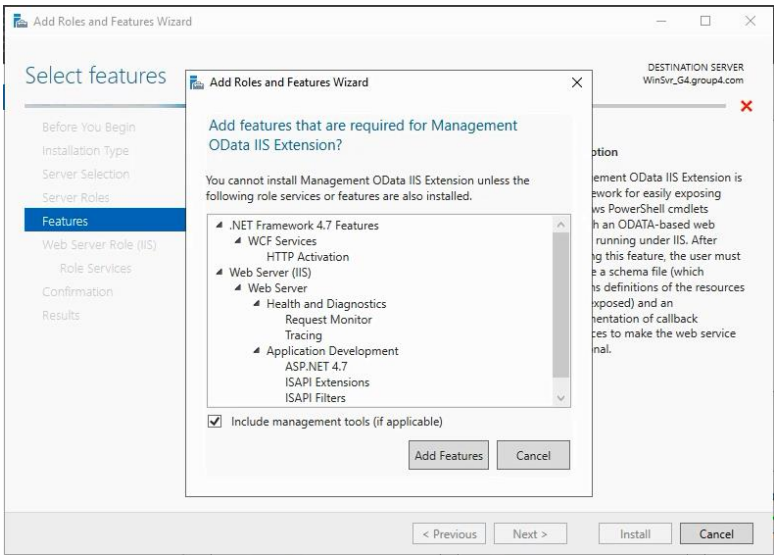


Figure 70 Include management tools if applicable

6. The Installation Progress page is displayed. , can close the wizard without interrupting running tasks. , can view task progress or open the page again by clicking Notifications in the notification area, and then clicking Task Details.

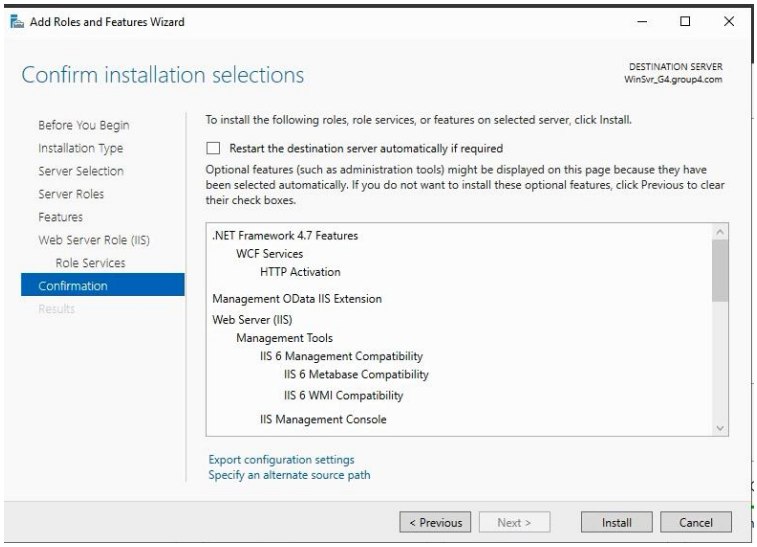


Figure 71 Installation Progress

7. On the **Results** page, verify that the installation succeeds, and then click **Close**.

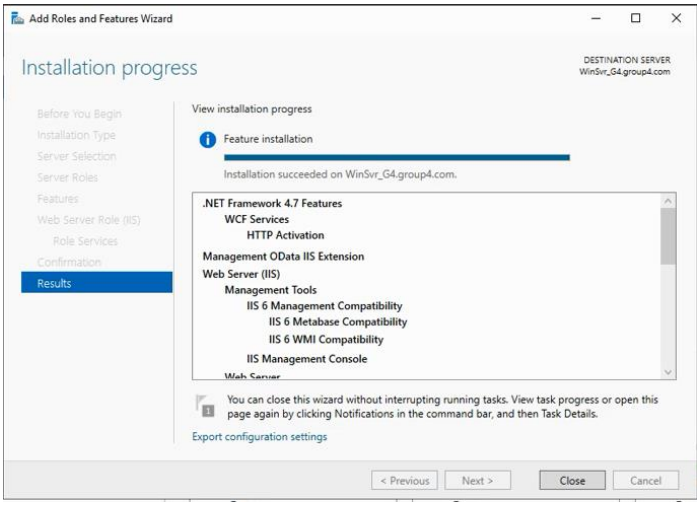


Figure 72 verify installation succeeds

5.3.4.2 Secure Socket Layer Installation and Configuration

1. In Confirm installation selections, click Install. Do not close the wizard during the installation process. When installation is complete, click **Configure Active Directory Certificate Services on the destination server**. The AD CS Configuration wizard opens. Read the credentials information and, if needed, provide the credentials for an account that is a member of the Enterprise Admins group. Click **Next**.
2. In **Role Services**, click **Certification Authority**, and then click **Next.**
3. On the **Setup Type** page**,** verify that **Enterprise CA** is selected**,** and then click **Next.**
4. In **Confirmation**, click **Configure** to apply ,r selections, and then click **Close.**
5. Open Microsoft Management Console (mmc.exe) to check if the certificate is installed.

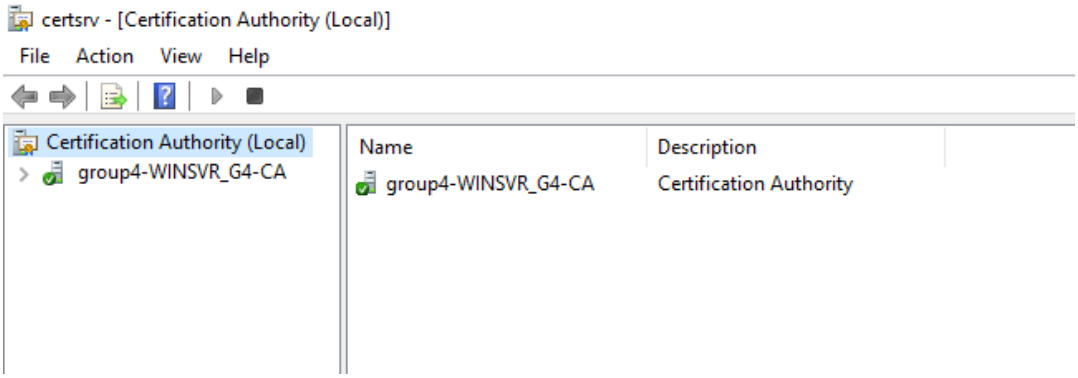


Figure 73 Certification authority

5.3.4.3 Add Website

Step 1: Open IIS manager and click add website.

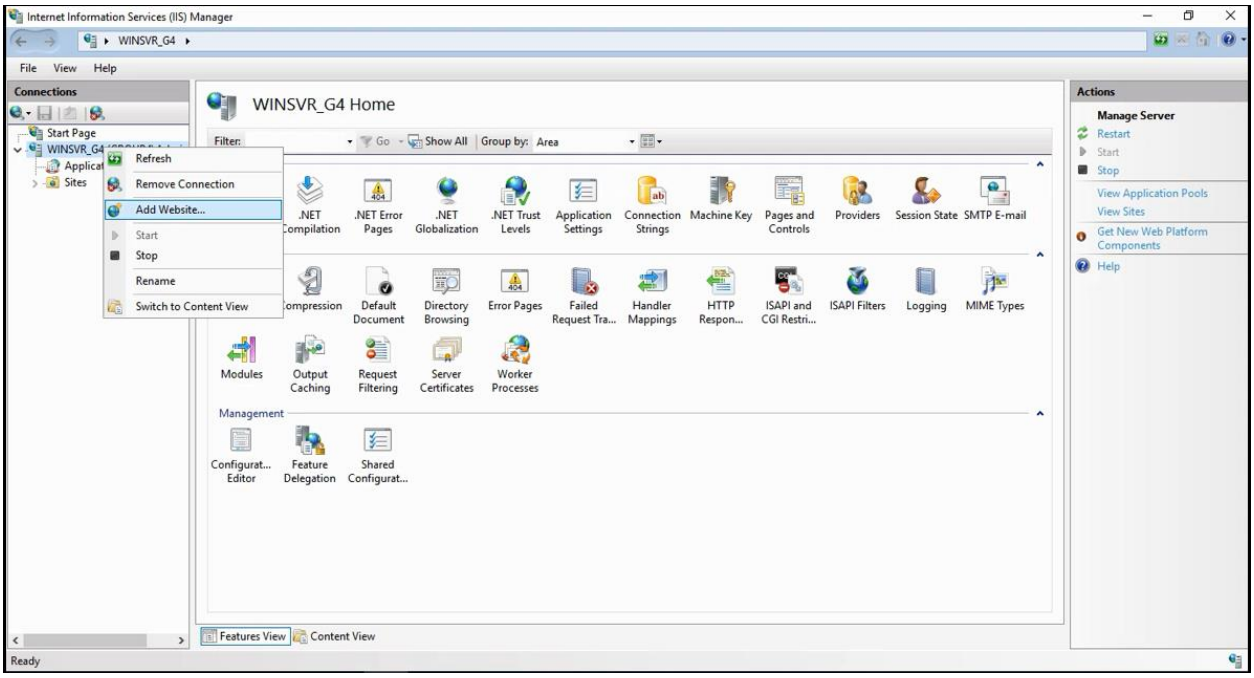


Figure 74 Server Manager Properties

Step 2: Add website for ipv4

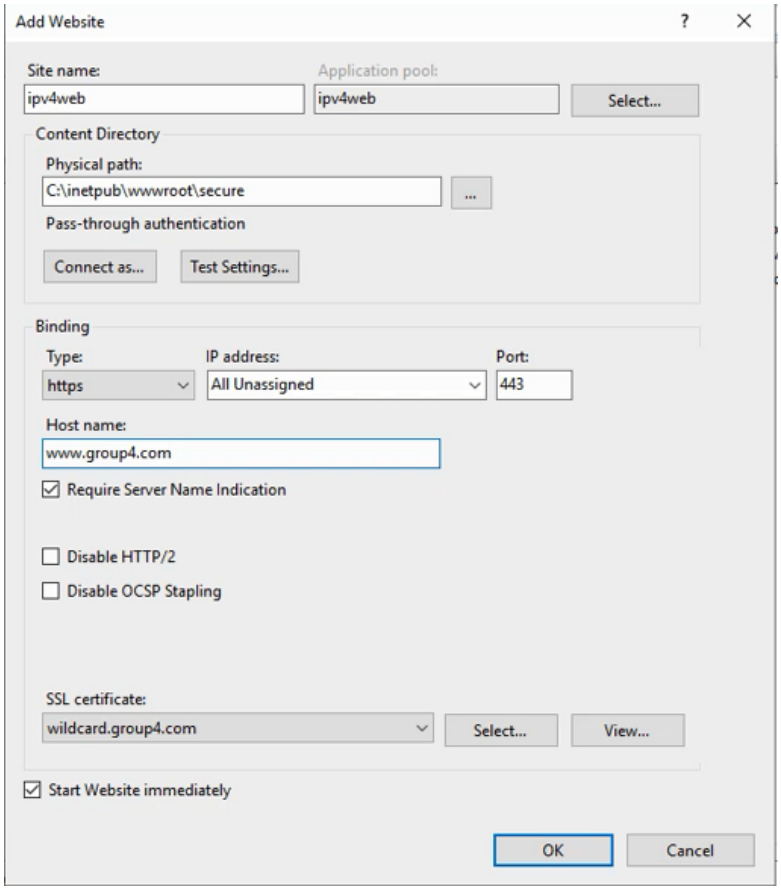


Figure 75 Enter site name, bindings, and host name then press ok.

Step 3: Create default document and save as html file in the directory and Add default document that we create in IIS.

Step 4: Open DNS manager. Then go to forward lookup zone. Find Group4.com zone. Then create new host which is www for the web.

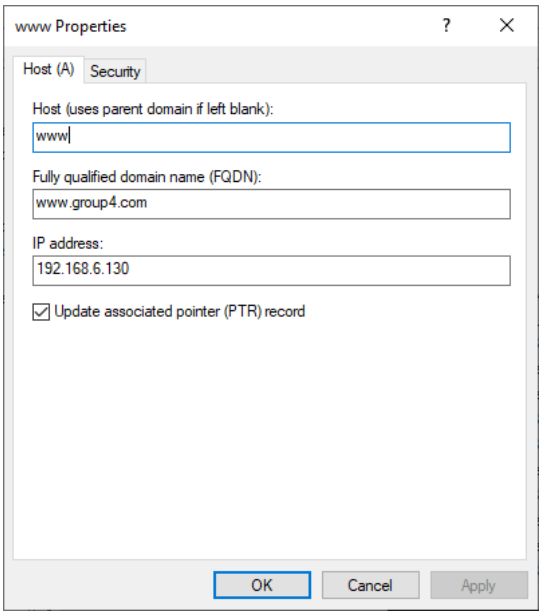


Figure 76 Create new host

Step 5: ipv4 web key bindings

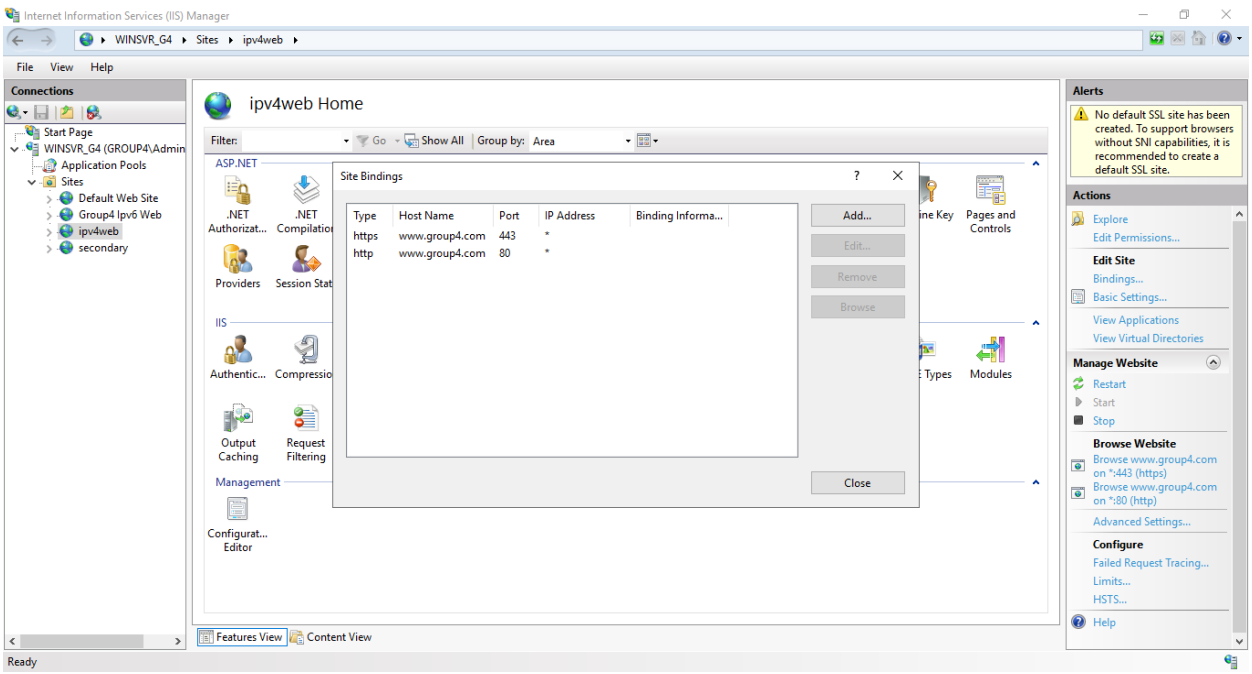


Figure 77 Key Bindings

5.3.5 Virtual Hosting

Step 1: Go to Server Manager > Tools > Internet Information (IIS) Manager and at the connection column double-click WIN to expand it. Then, right-click on Sites and select Add Website.

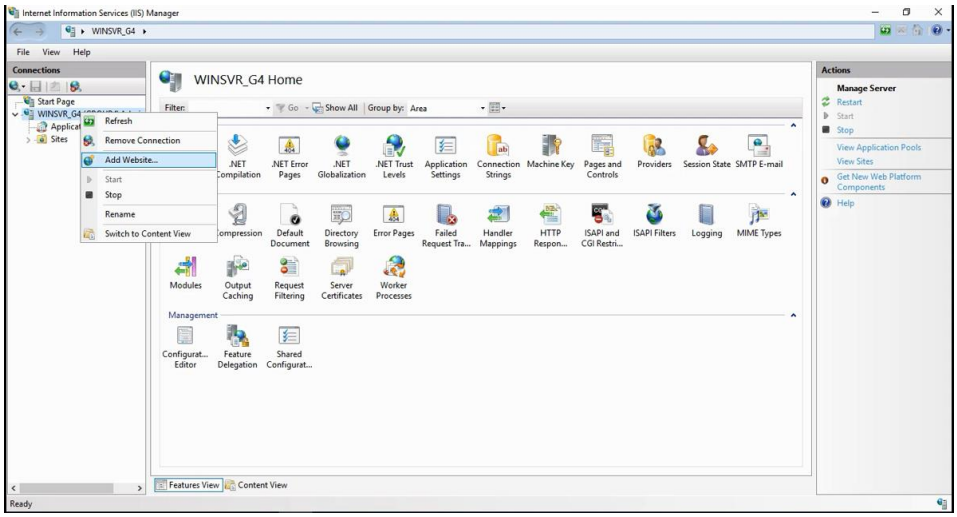


Figure 78 Add Website

Step 2: Add virtual website

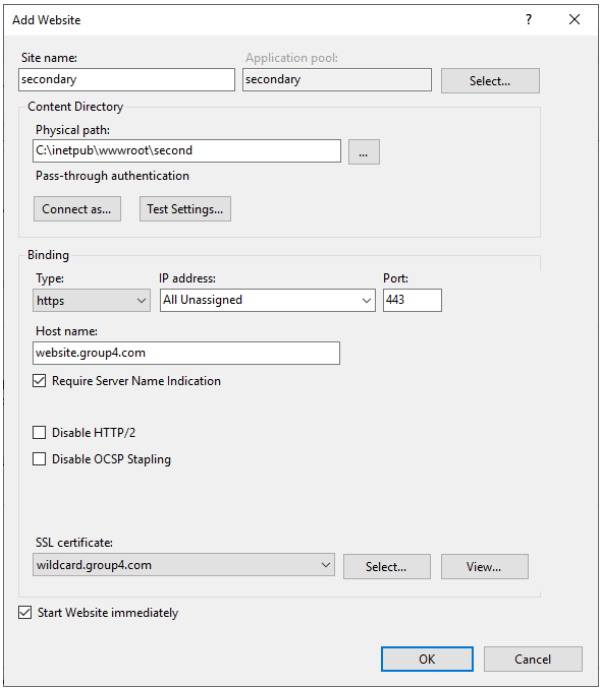


Figure 79 Enter site name, bindings, and host name then press ok

Step 3: Create the directory for the website. Then, create new html file for the site and add default document to the site.

Step 4: Open DNS Manager, create new Forward Lookup Zone and add host for website.group4.com.

Step 5: Select zone type as Primary Zone

Step 6: Choose "To all DNS servers running on domain controller this domain: group4.com"

Step 7: Enter zone name as website.group4.com

Step 8: Choose "Allow both nonsecure and secure dynamic updates"

Step 9: Complete New Zone Creation

Step 10: Right click on the zone and choose new host

Step 11: Add the host details and click add host button

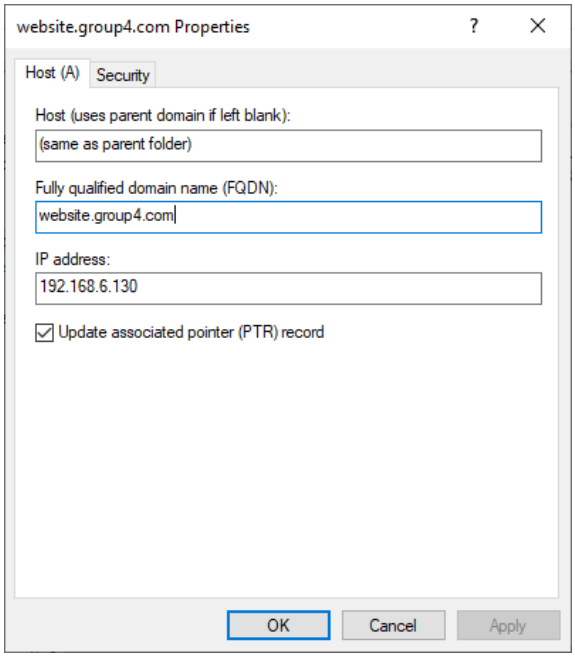


Figure 80 Create new virtual host

5.3.6 IPSec Site-To-Site Tunneling

Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data, voice and video between two sites (e.g offices or branches). The VPN tunnel is created over the Internet public network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites.

Step 1 : Create an ISAKMP phase 1 policy.

Figure 81 Create ISAKMP phase 1 policy

Step 2 : Create an encryption method to be used for Phase 1. This encryption method is to secure and encrypt our packet and connection between the tunnel.

Figure 82 Create an encryption method

Step 3: Create an hashing algorithm to be used for Phase 1.

Figure 83 Create hashing algorithm

Step 4 : Configure Pre-Shared key as the authentication method and the session key lifetime, Expressed in either kilobytes (after x-amount of traffic, change the key) or seconds. Value set is the default value.

```
R4(config-isakmp)#group 2
R4(config-isakmp)#life`
R4(config-isakmp)#lifeti
R4(config-isakmp)#lifetime 86400
R4(config-isakmp)#authentication pre-share
```

Figure 84 Configure Pre Shared Key

Step 5 : Create the pre share key authentication with our peer (Next group router). The peer's pre shared ker is set to Group4 and its public IP address is 1.1.1.2. Every time the router try to establish a tunnel with the other group router (1.1.1.2), this pre shared key will be used.

```
R4(config)#crypto isa
R4(config)#crypto isakmp key Group4 address 1.1.1.2
```

Figure 85 Define a pre shared key

Step 6 : Create an access-list and define the traffic we would like the router to pass through the VPN tunnel. In this configuration it would be traffic from one network to the other, 192.168.6.0/30 to 192.168.1.0/30.

```
R4(config)#ip access-list extended VPN-TRAFFIC
R4(config-ext-nacl)#permit ip 192.168.6.0 0.0.0.3 192.168.1.0 0.0.0.3
```

Figure 86 Create an access-list

Step 7 : Create the transform set used to protect our data. We've named this TS.

```
R4(config)#crypto ipsec transform-set TS esp-3des es
R4(config)#crypto ipsec transform-set TS esp-3des esp-md
R4(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
R4(cfg-crypto-trans)#
```

Figure 87 Create the transform set

Step 8 : Create the Crypto Map and connects the previously defined ISAKMP and Ipsec configuration together. We've named our crypto map CMAP. The ipsec-isakmp tag tells the router that this crypto map is an Ipsec crypto map.

```
R4(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R4(config-crypto-map)#set p
R4(config-crypto-map)#set p
R4(config-crypto-map)#set
R4(config-crypto-map)#set peer 1.1.1.2
R4(config-crypto-map)#set tra
R4(config-crypto-map)#set transform-set TS
R4(config-crypto-map)#matc
R4(config-crypto-map)#match add
R4(config-crypto-map)#match address VPN-TRAFFIC
```

Figure 88 Create the Crypto Map

Step 9 : Apply the crypto map to the outgoing interface of the router to another router. Here, the outgoing interface is Serial 0/2/0.

```
R4(config)#int s0/2/0
R4(config-if)#cry
R4(config-if)#crypto map CMAP
R4(config-if)#
*Jan  1 04:28:45.422: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Figure 89 Apply the crypto map to the outgoing interface

5.3.7 Active Directory (AD)

Step 1 **:** Open Server Manager in Windows Server and select Add Roles and Features Wizard.

Step 2 : Select the server from server pool that you want to install the Active Directory (AD) services.

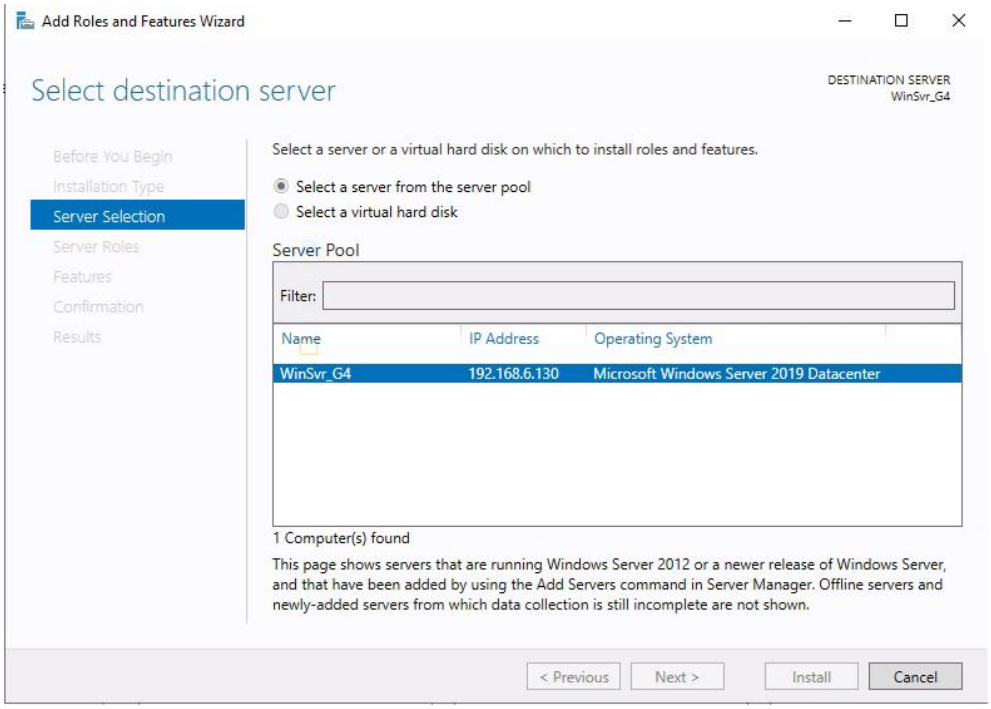


Figure 90 Select a sever from server pool

Step 3 : Select the features that you want to install with the Active Directory (AD) and then click Next > Next until it required to click Install button.

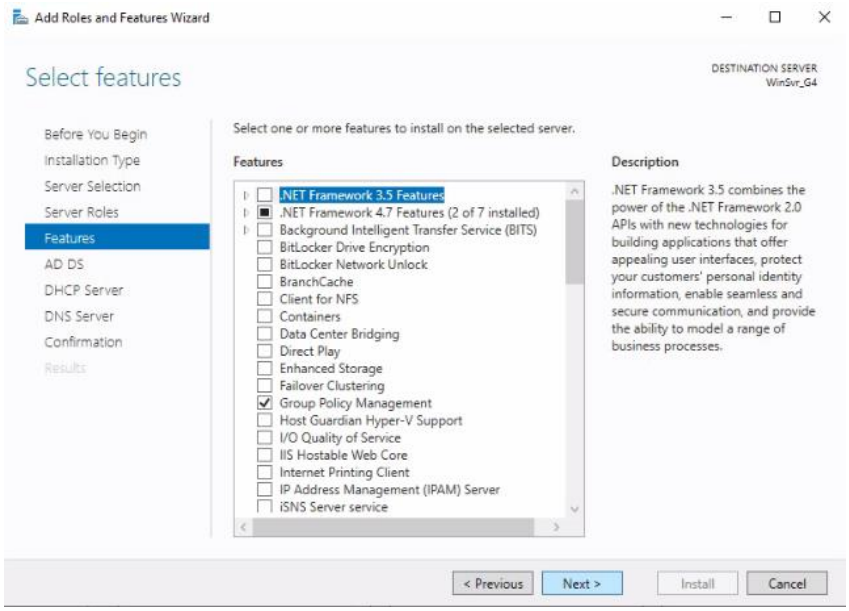


Figure 91 AD features selection

Step 4 : Then, wait until the installation finished and click Close.

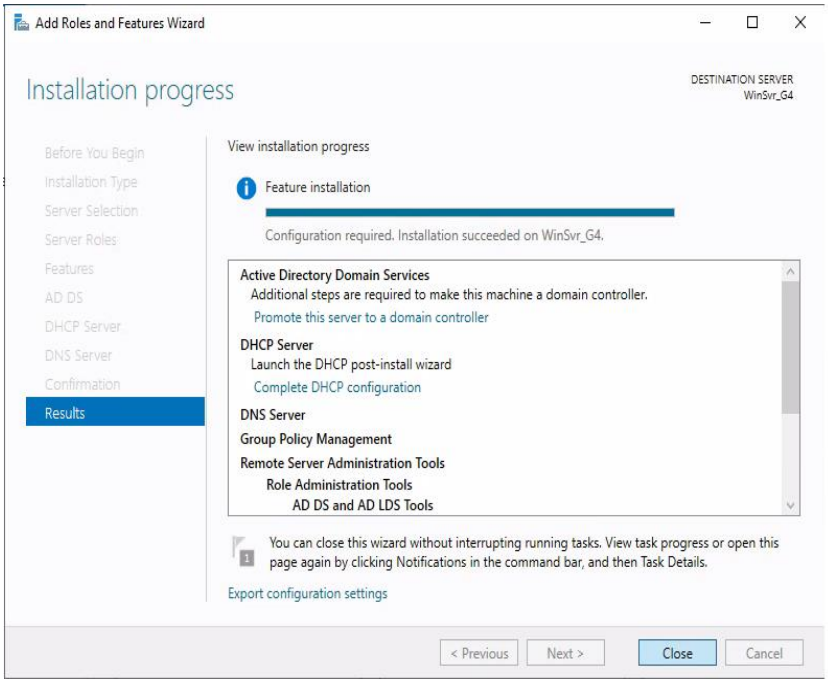


Figure 92 Installation progress for AD

Step 5 : After finish the installation, then promote this server to a domain controller.

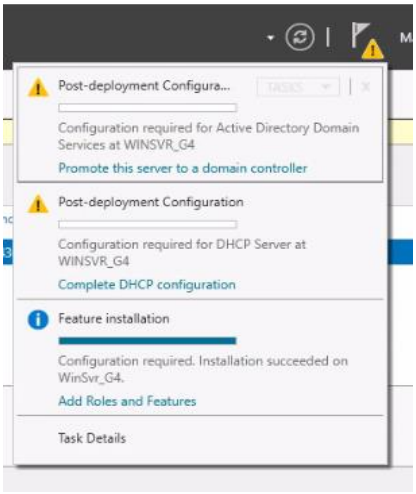


Figure 93 Promote Server to Domain Controller

Step 6 : After that, there will appear a pop up for Deployment Configuration. Then click add new forest and then enter your Root domain name.

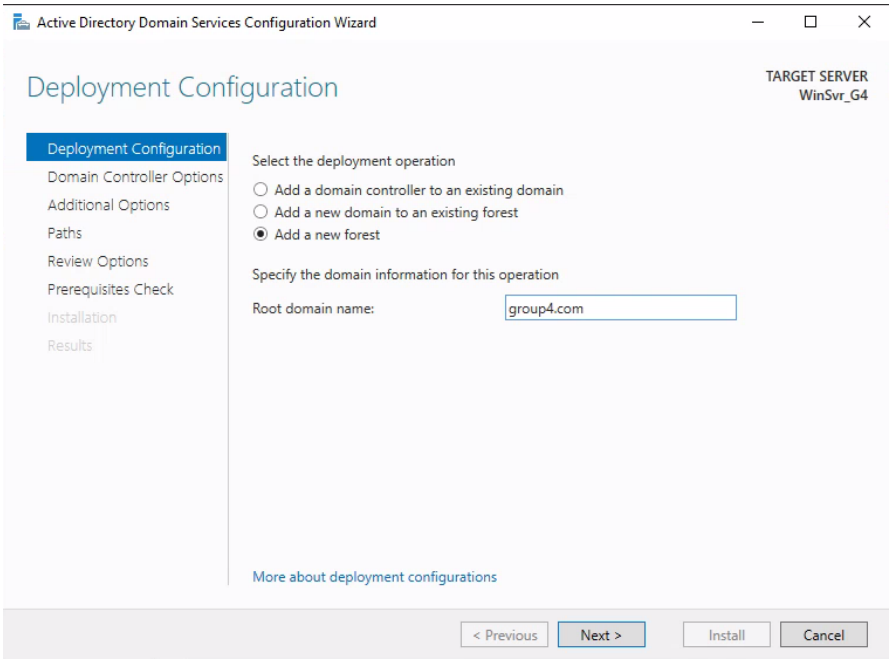


Figure 94 Add a new forest

Step 7 : Then, enter the Directory Services Restore Mode (DSRM) password and click Next.

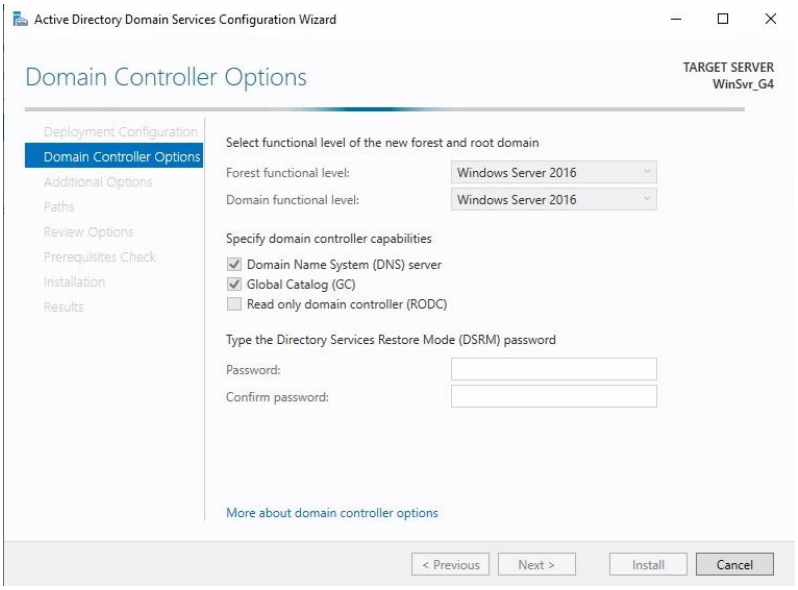


Figure 95 Enter Directory Services Restore Mode (DSRM) password

Step 8 : After that, for the DNS Options just click Next and dont select the “Create DNS delegation”.

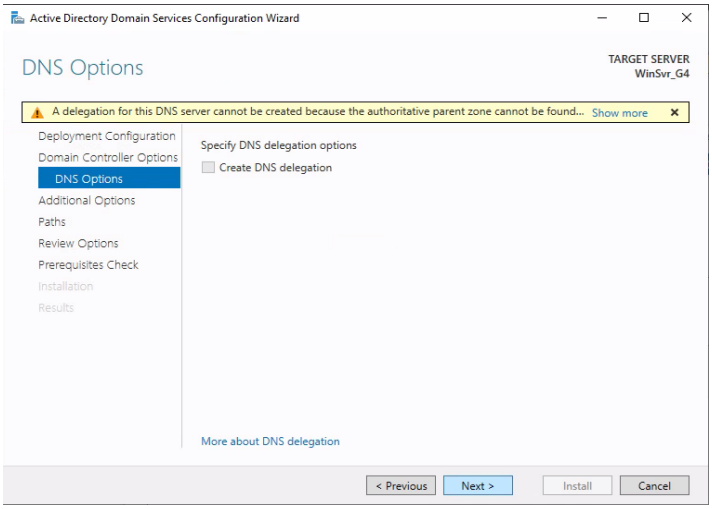


Figure 96 DNS Options

Step 9 : Next, verify the NetBIOS name assigned to the domain and chnage the name if needed.

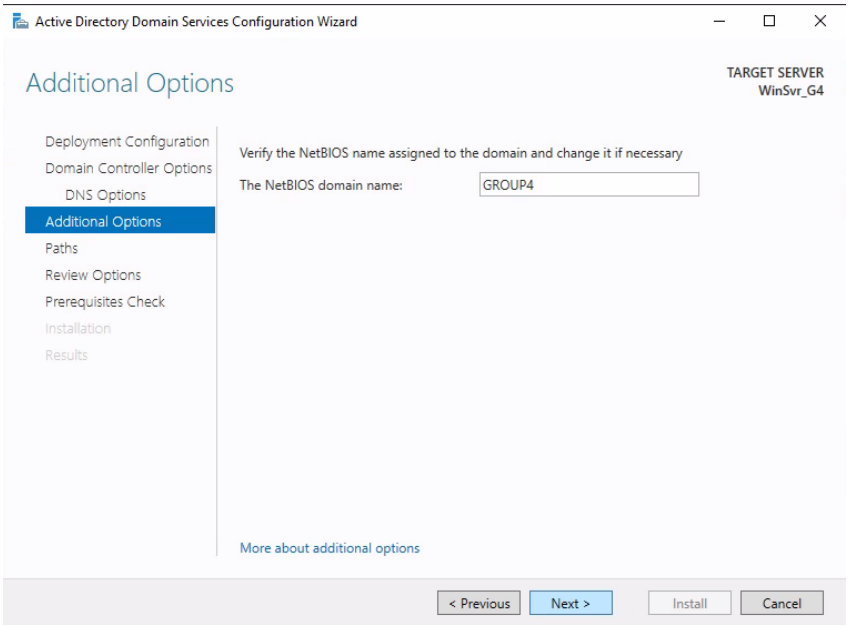


Figure 97 Verify NetBIOS name

Step 10 : Next, specify the location of the AD DS database, log files and SYSVOL.

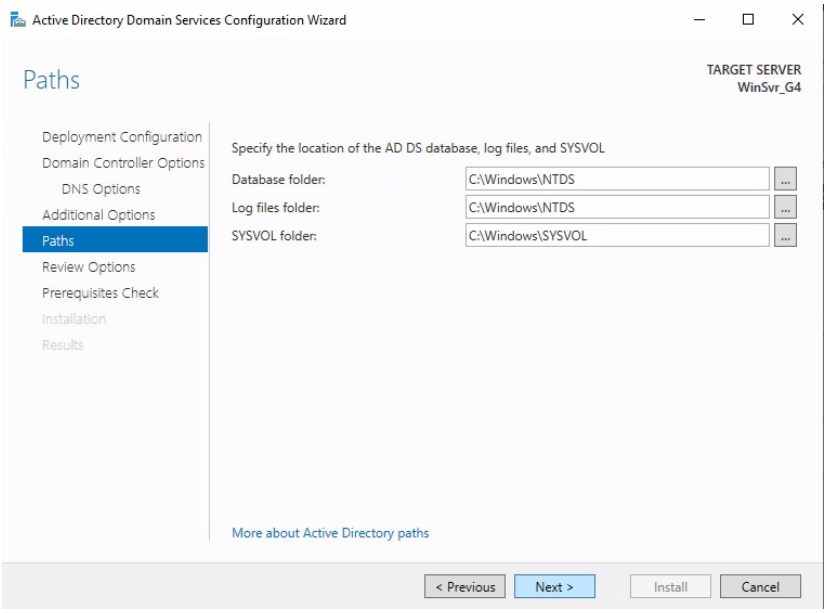


Figure 98 Specify the location of the AD DS database, log files and SYSVOL

Step 11 : Next review your options, and change it if necessary.

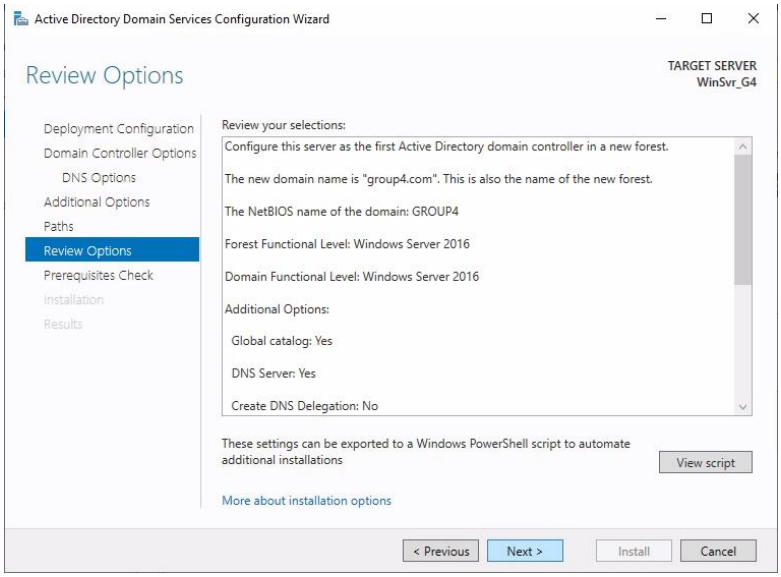


Figure 99 Review Options

Step 12 : After that, it will check the prerequisites and the click Install.

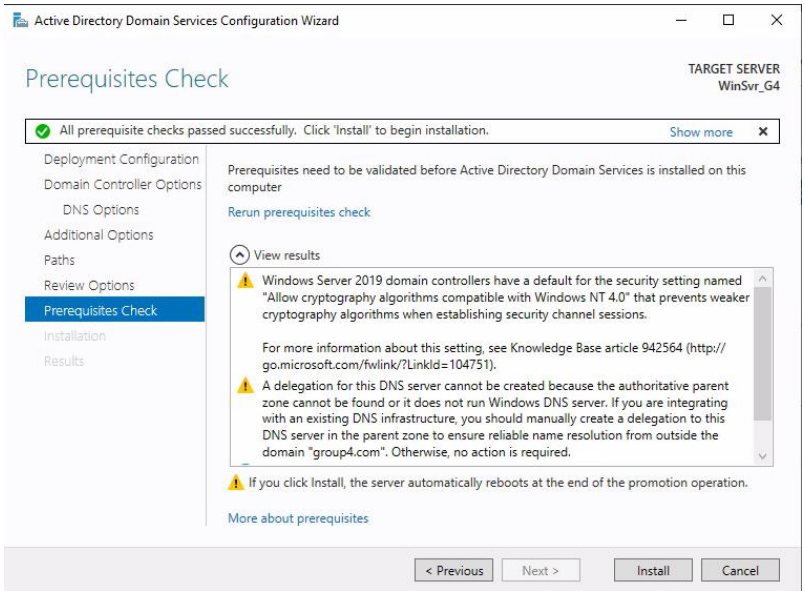


Figure 100 Prerequisites Check

Step 13 : Then, wait until the installation finished and click Close.

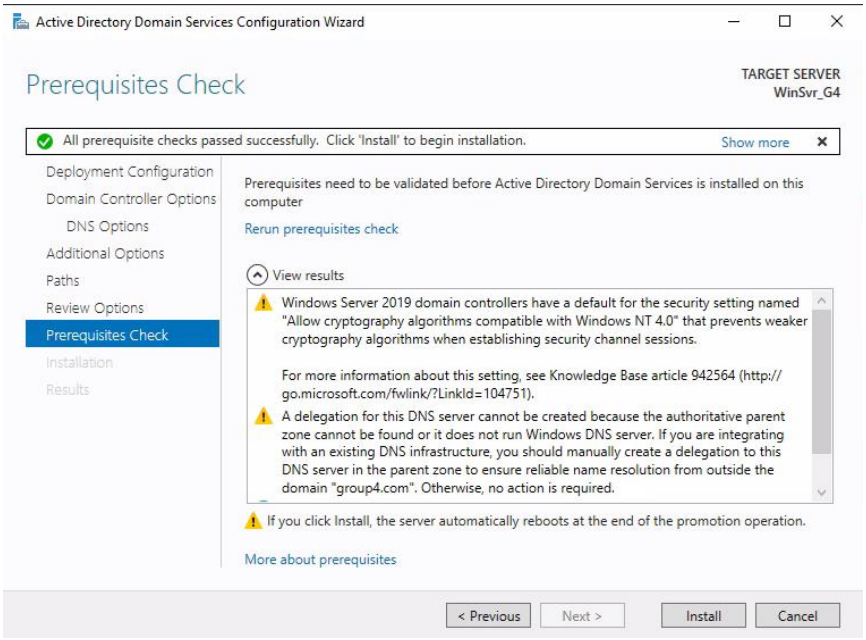


Figure 101 Installation progress for AD

Step 14 : Then, open the Active Directory Users and Computers.

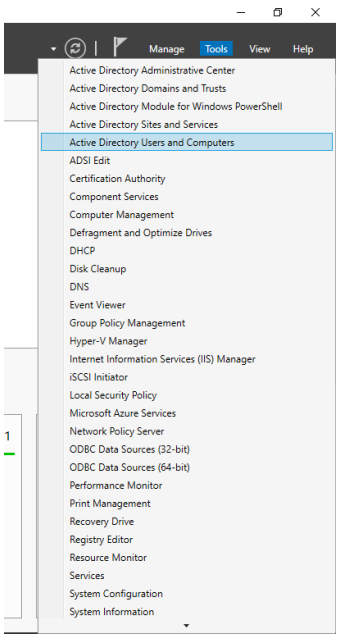


Figure 102 Active Directory Users and Computers

Step 15 : Next, create and new user named Haikal Asyraf and click Next.

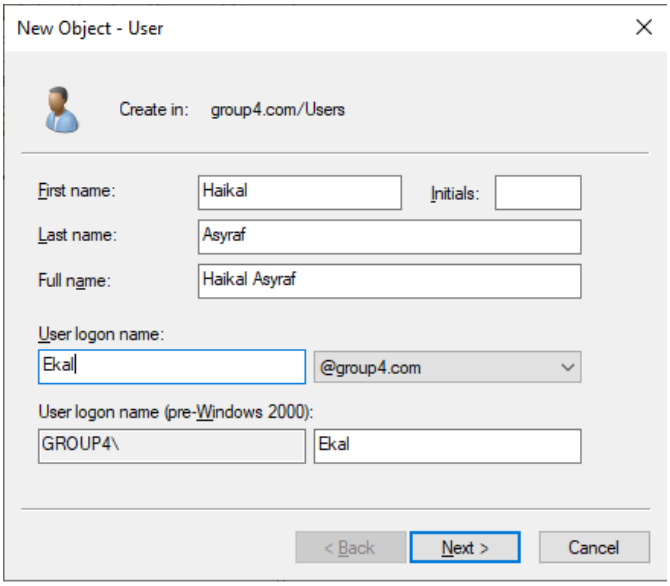


Figure 103 Create a new user

Step 16 : Then, create a password for the user and click Next.

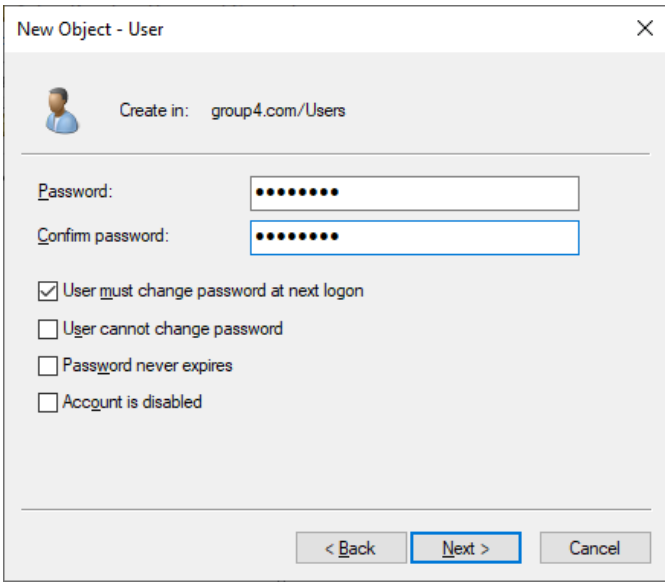


Figure 104 Create password for user

Step 17 : Then, all the user that have been created will appear in the Domain User Groups.

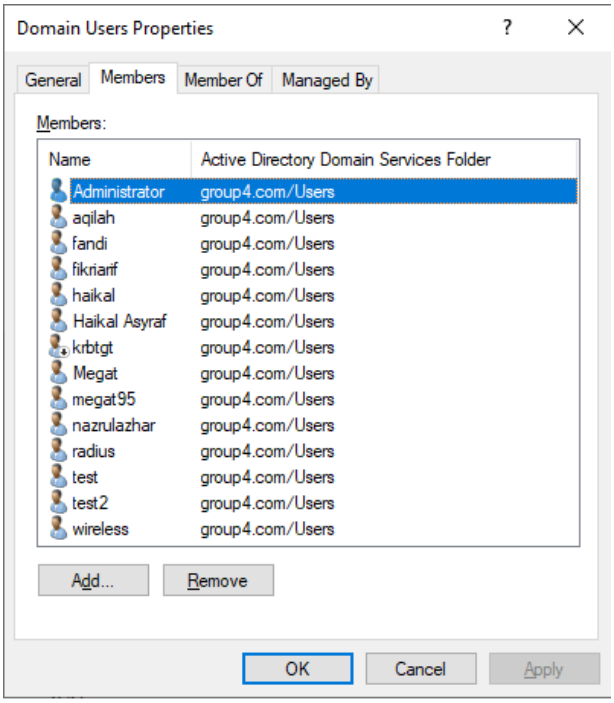


Figure 105 Domain User Groups

5.3.8 Group Policy Object (GPO)

Step 1 : Go to Icon window > Search Box > Group Policy Management.

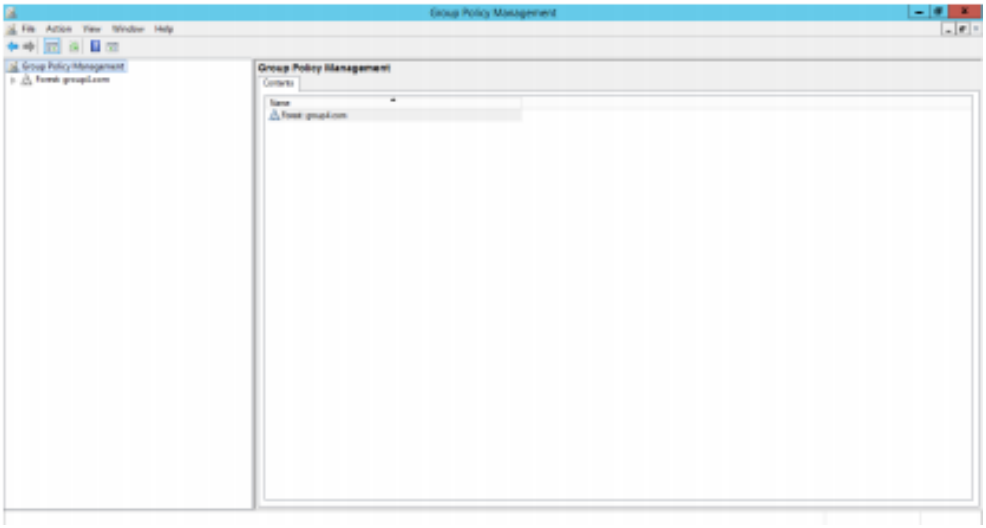


Figure 106 GPO Management Dashboard

Step 2 : Select on Forest group4.com > Domain > group4.com

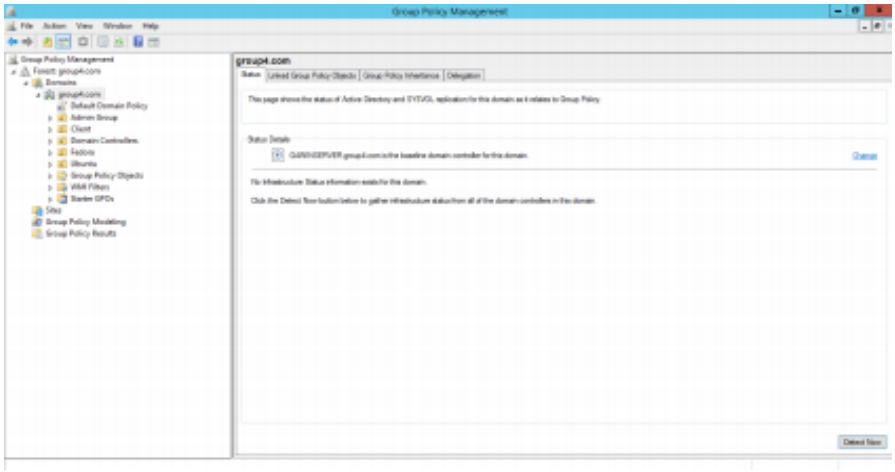


Figure 107 GPO Status

Step 3 : Right click on group4.com domain unit and select Create GPO in this domain.

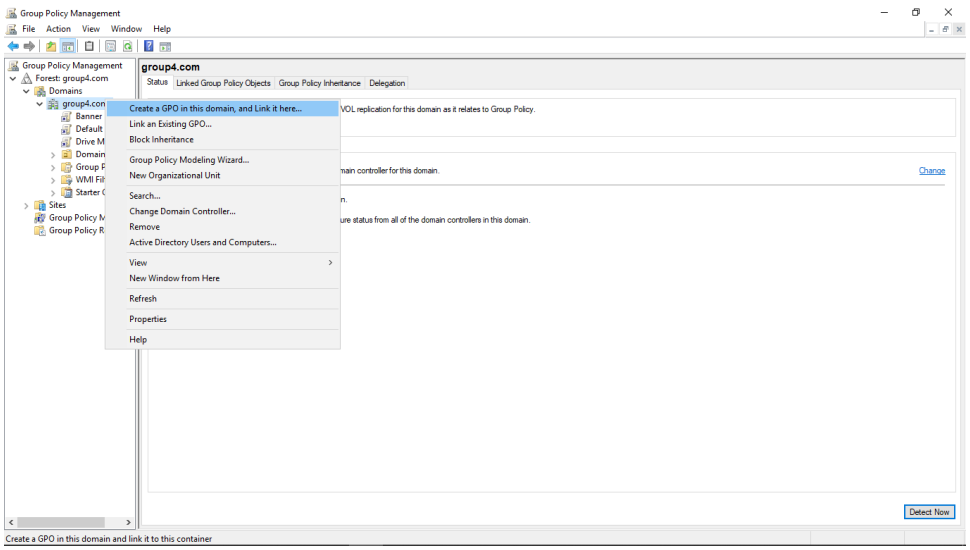


Figure 108 Create GPO in this domain

Step 4 : Insert Name (example: Banner) for the new GPO.

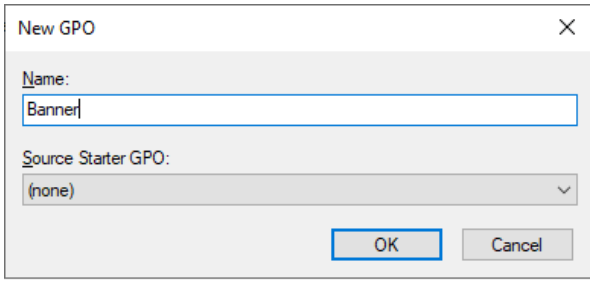


Figure 109 Creating new GPO

Step 5 : Then, right click on Banner > Edit Policy > GPO Editor.

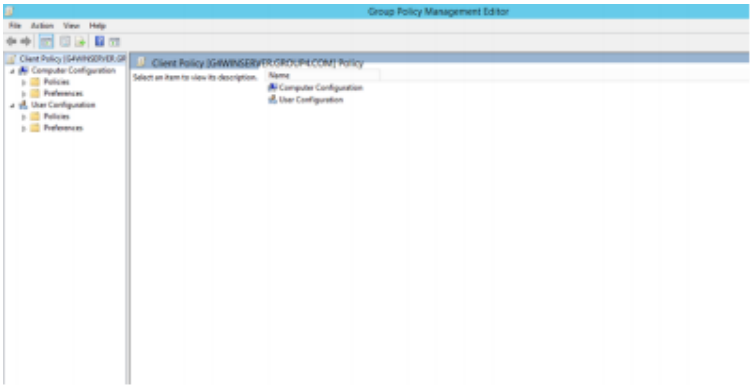


Figure 110 GPO Management Editor

Step 6 : Next click on the Computer Configuration > Windows Setting > Security Setting > Local Policies > Security Policies

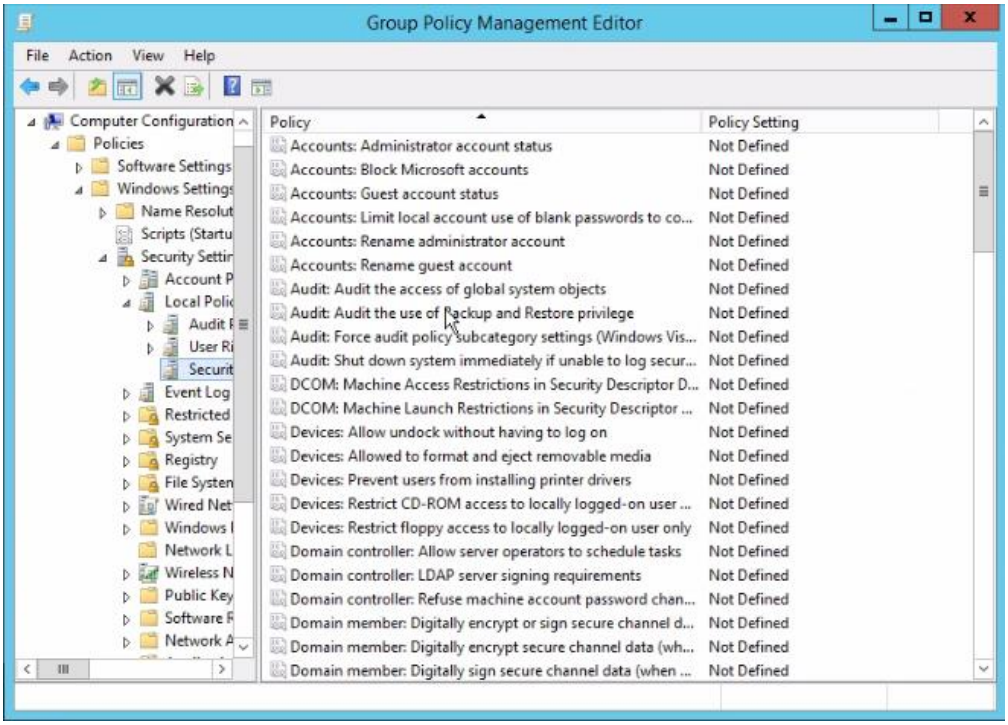


Figure 111 Personalization of GPO

Step 7 : Then, search for the Interactive logon: Message tittle for users attempting to logon policies and double-click the policies.

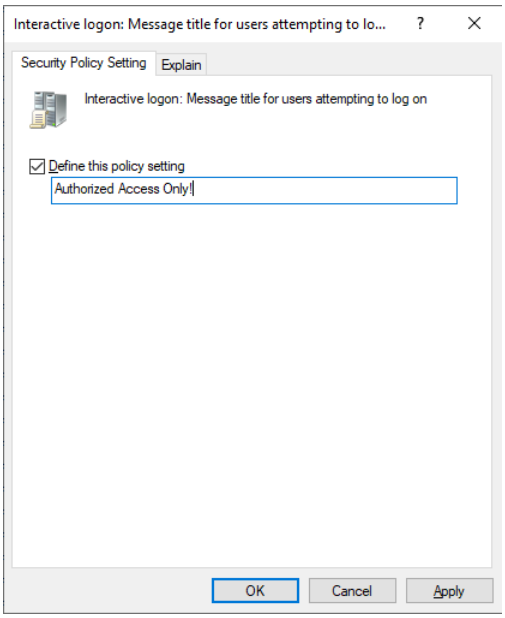


Figure 112 Define GPO policies setting

Step 8 : Next, define the next policies that is Interactive logon : Message text for users attempting to logon and enter the text for the policies.

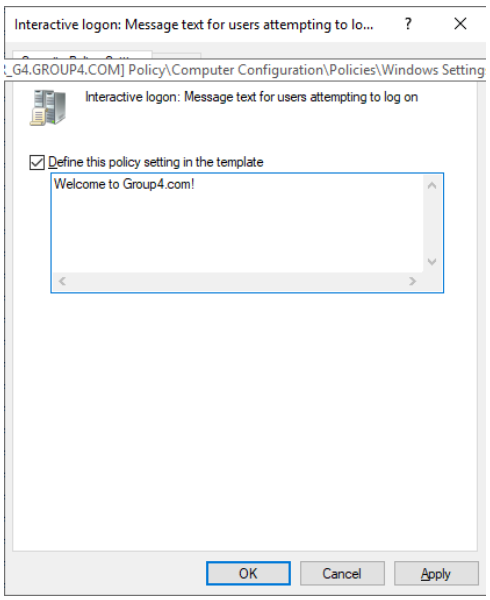


Figure 113 Define second GPO policies

Step 9 : Then, go back to GPO Management Dashboard and declare the new GPO that is named : Drive Map and click OK.

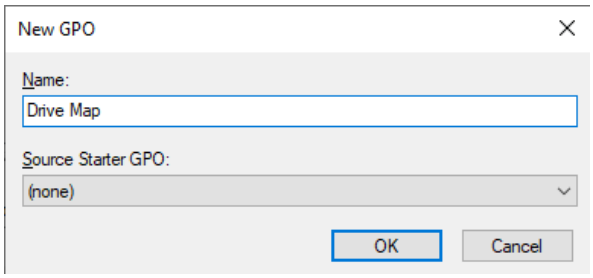


Figure 114 Creating Second GPO

Step 10 : Next, right click the Drive Maps > Edit Policy > GPO Editor > User Configuration > Preferences > Window Settings > Drive Maps.

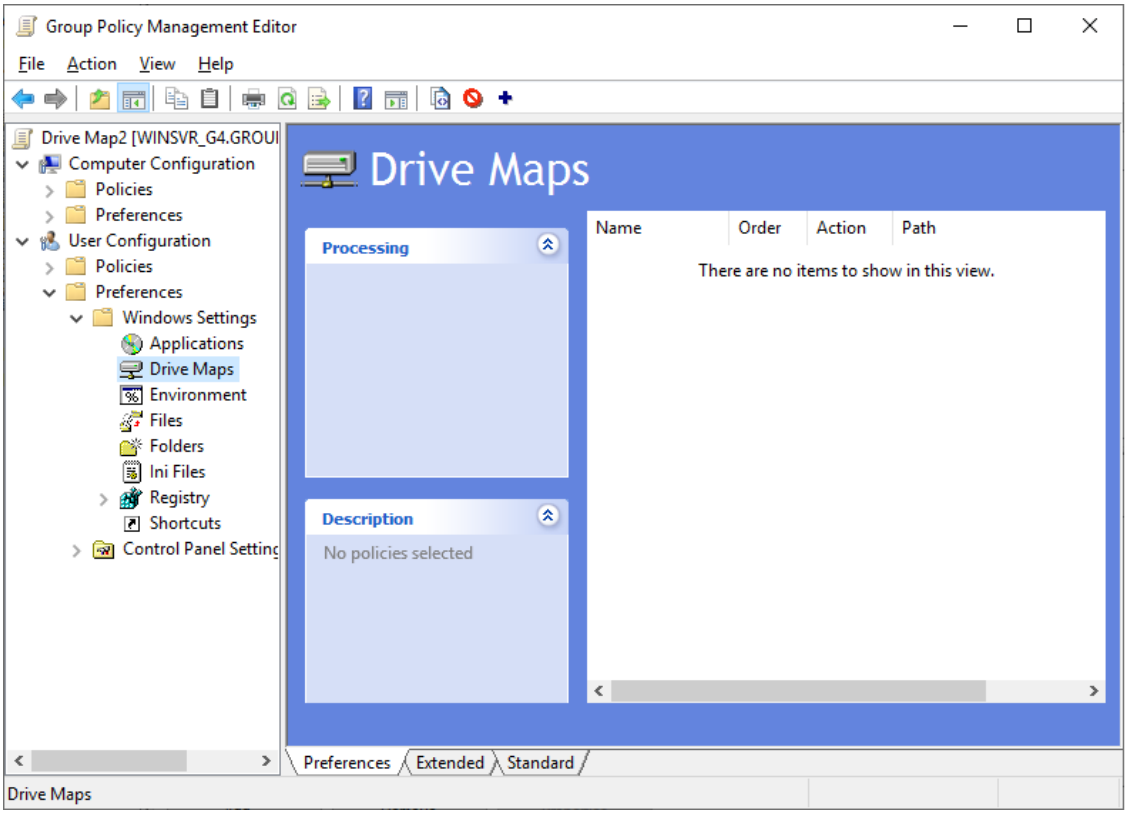


Figure 115 Creating a Drive Maps Policies

Step 11 : Then, right click on the window and click create a new drive maps. After that enter the location and the drive letter then click OK.

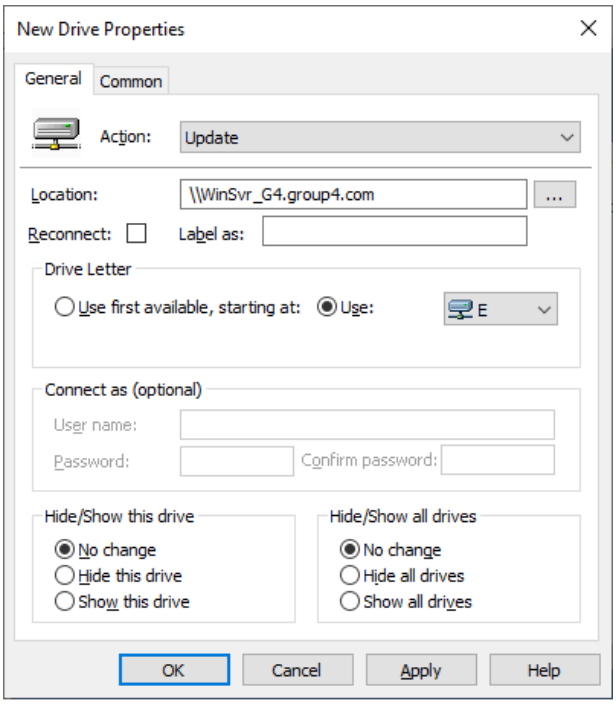


Figure 116 Configure new drive properties

Step 12 : Next, go to Server Manager > File and Storage Services > Share > New Share.

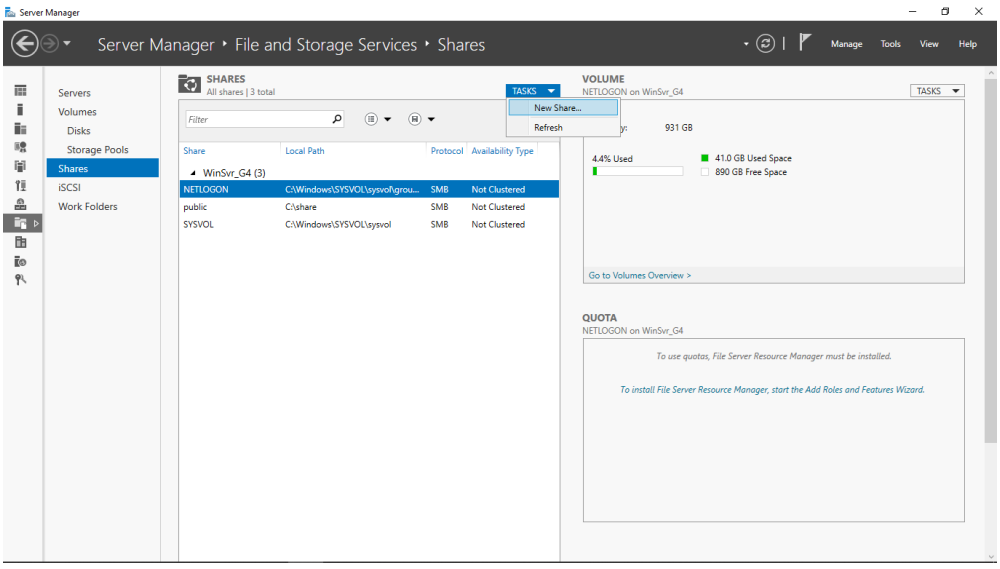


Figure 117 Creating new file shares

Step 13 : Next, choose SMB Share – Quick and the click Next

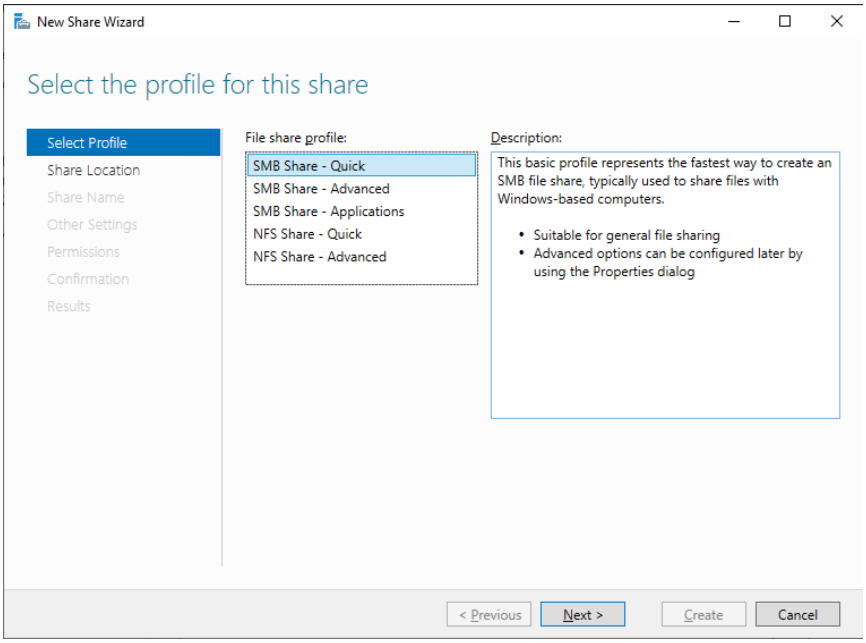


Figure 118 Choose SMB Share – Quick

Step 14 : Then, type a custom path that the file will be stored in the server.

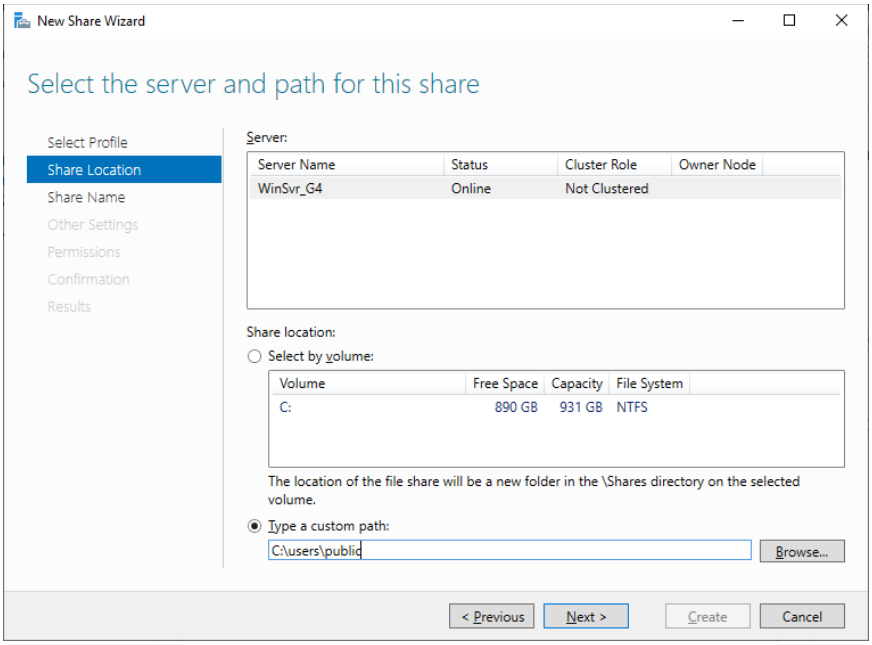


Figure 119 Select the server and path for this share

Step 15 : After that, specify the share name and verify the Local path to share is correct, then click Next.

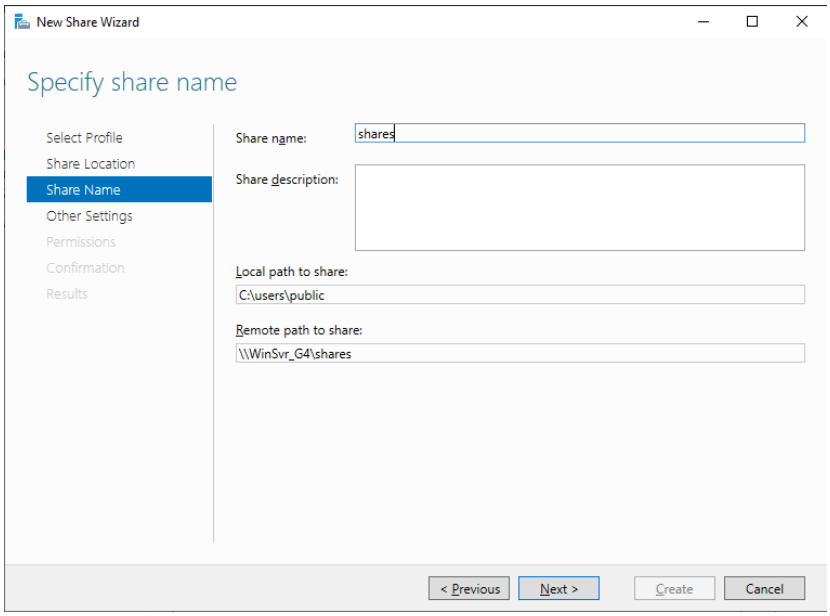


Figure 120 Specify Share Name

Step 16 : Then, confirm all the selections and if all the selections if correct then click Create.

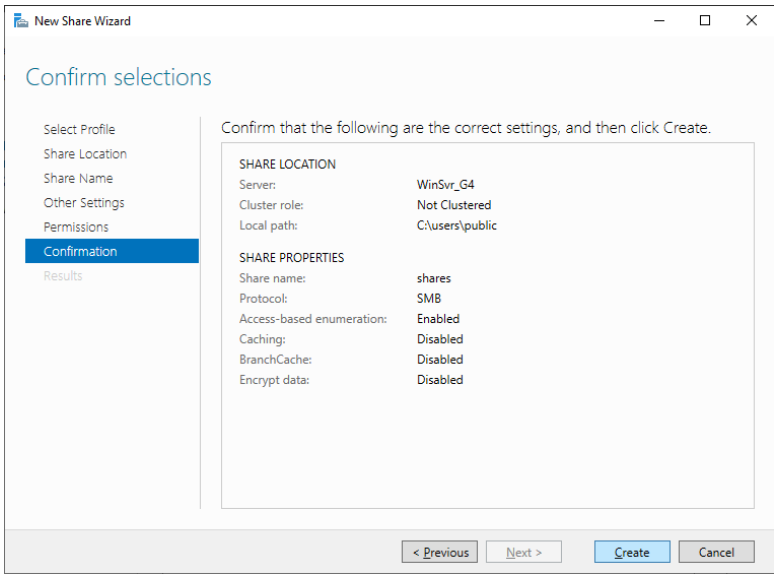


Figure 121 Confirm the File Sharing selections

5.3.9 Server Virtualization

5.3.9.1 Hyper-V Installation

1. Click **Add Roles and Features** on Server Manager

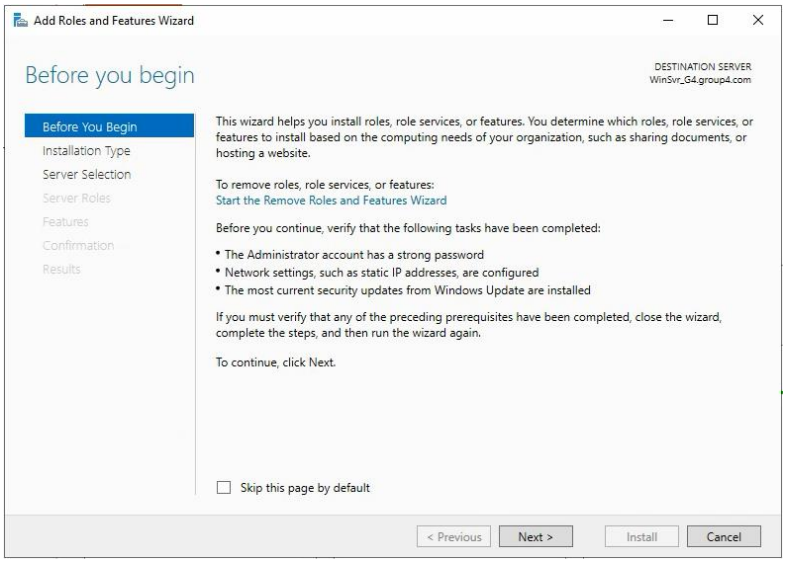


Figure 122 Add Roles Windows

2. Now select **Role-based or feature based-based** installation

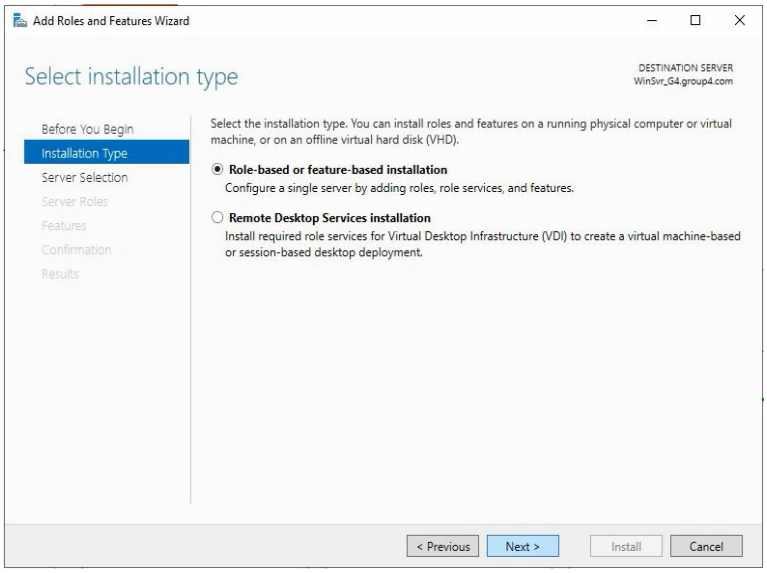


Figure 123 Select installation type

3. Choose and select the server and click **Next** button

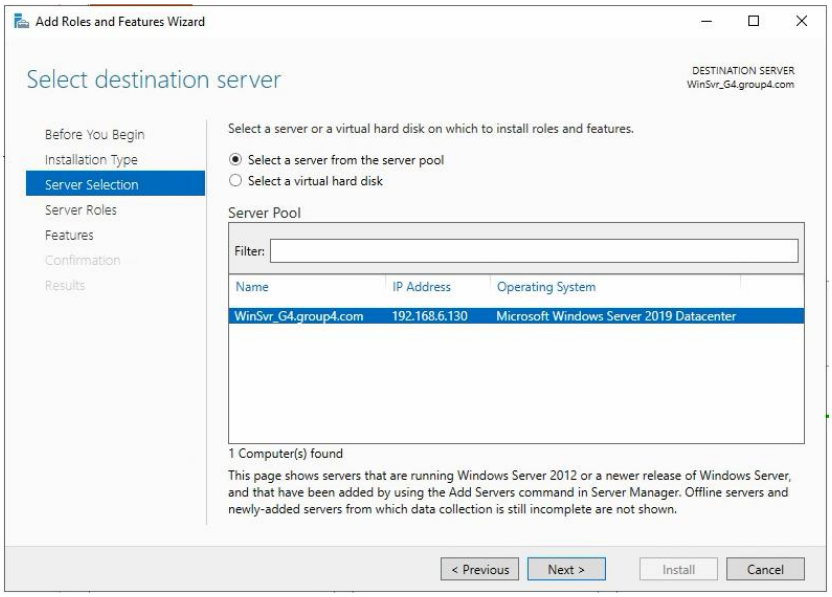


Figure 124 Select destination server

4. Choose Hyper V role and click **Next** button

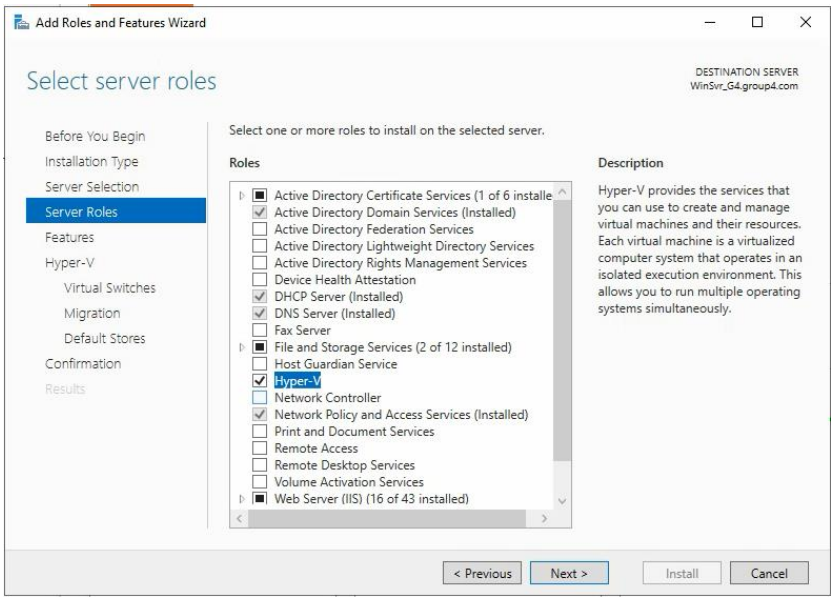


Figure 125 Select server roles

5. Click **Next** button to continue.

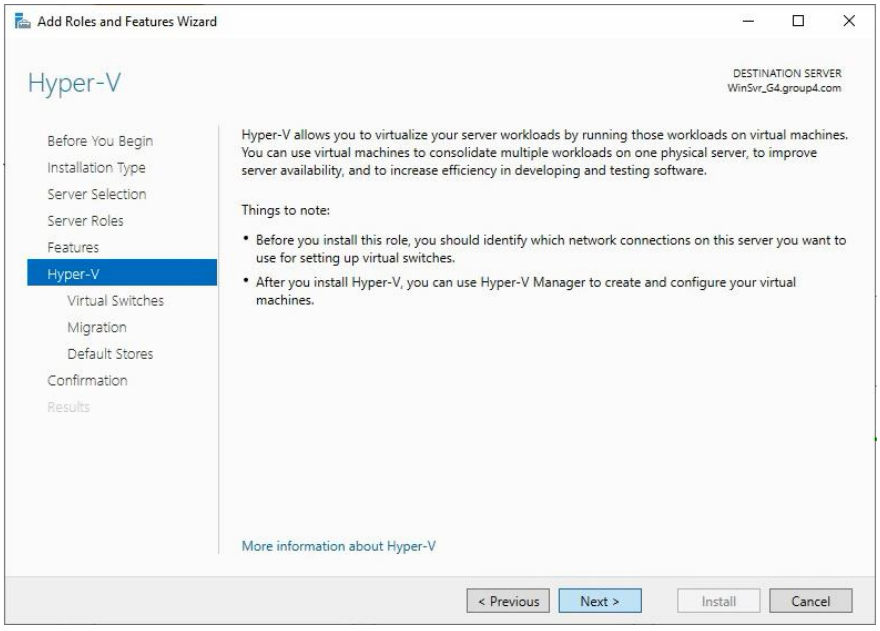


Figure 126 Select Hyper-V

6. Now select network adapter for virtual switches. Then click **Next** button.

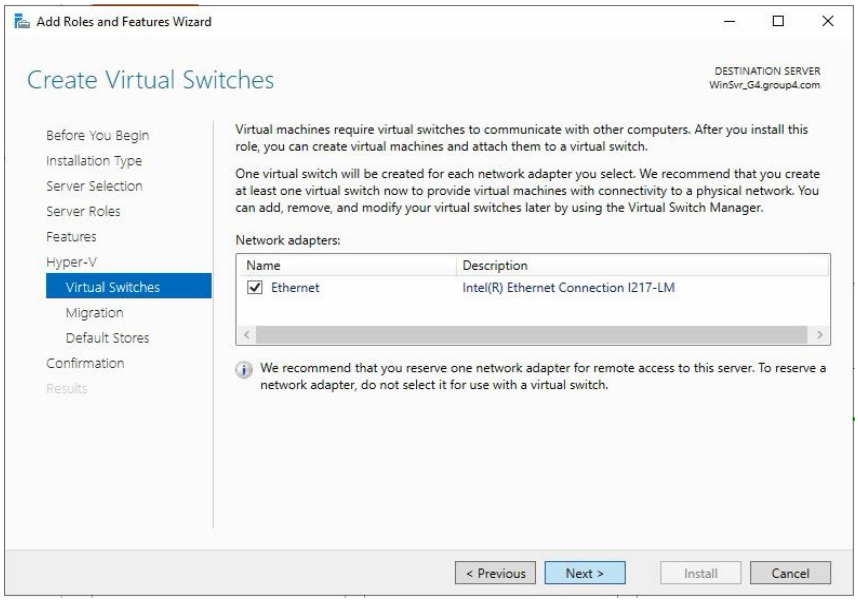


Figure 127 Create Virtual Switches

7. Here, configures the location to store Hyper V virtual hard disk files. After configuring it, click **Next** button.

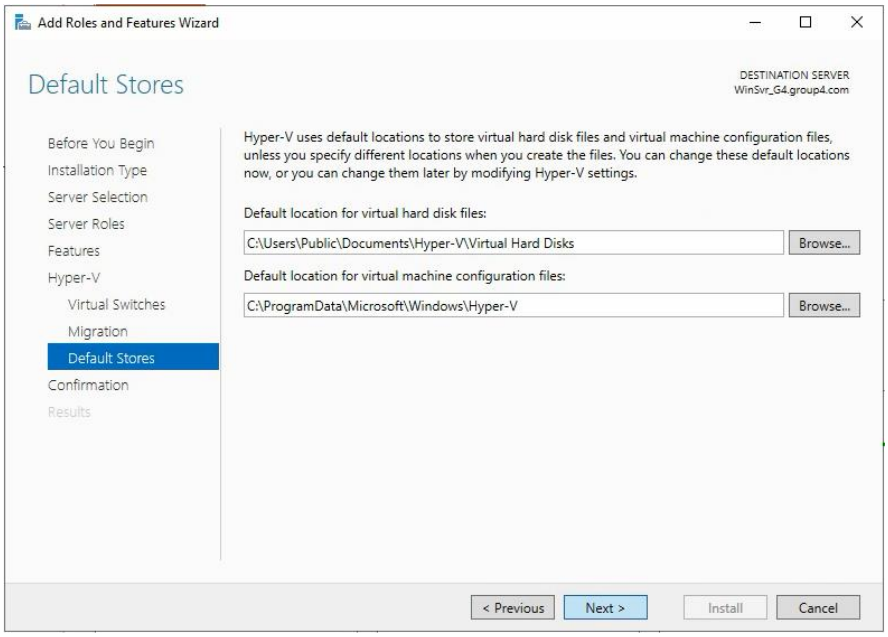


Figure 128 Default Stores

8. So now see the installation information and confirm it by clicking **Install** button.

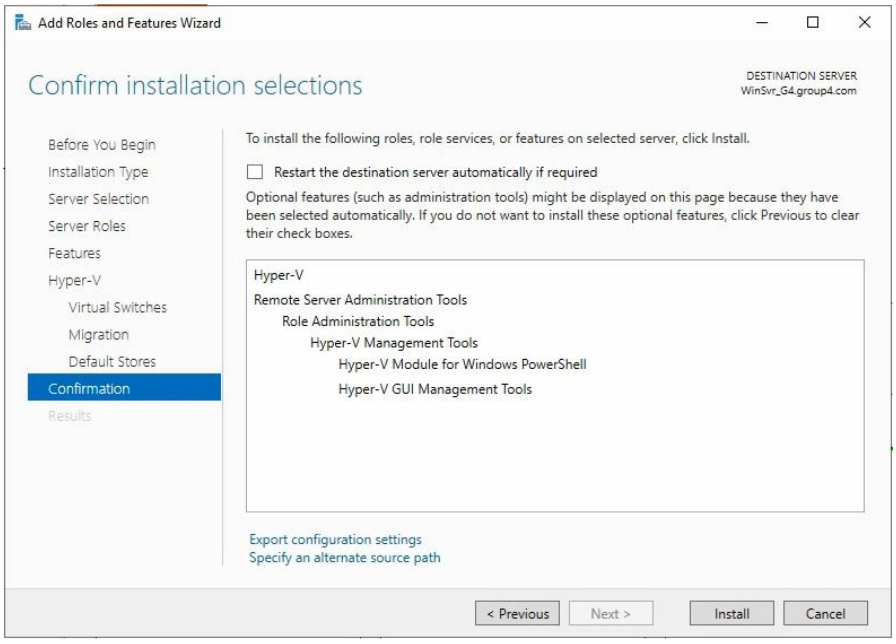


Figure 129 Confirm installation selections

9. After installation completed, click **Close** to continue. Now open Hyper V manager from start menu to configure it.

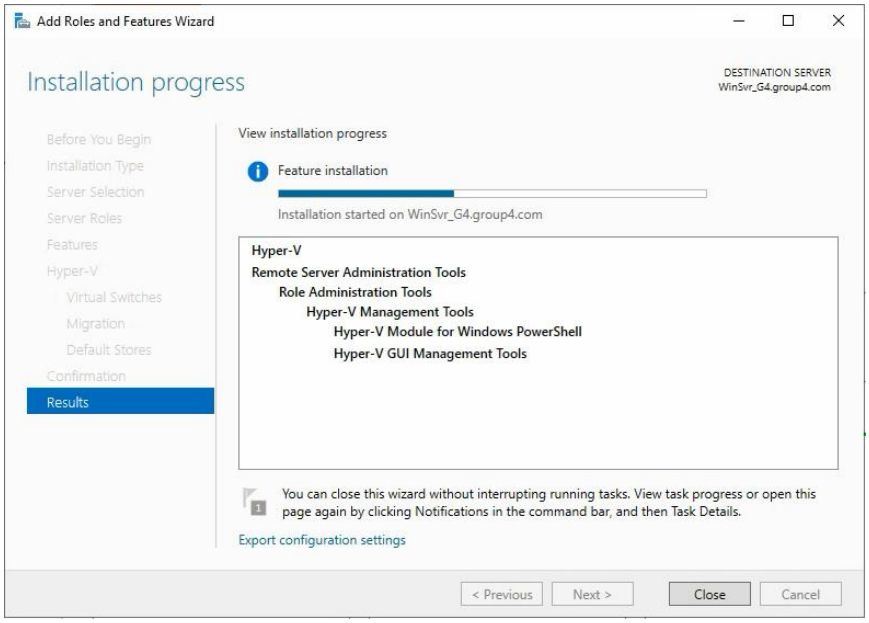


Figure 130 Installation progress

5.3.9.2 Virtual Machine Installation and Configuration

1. To create Virtual machine in Hyper-V server 2019, on right side hover a cursor to "**New**" and click on **Virtual Machine**.

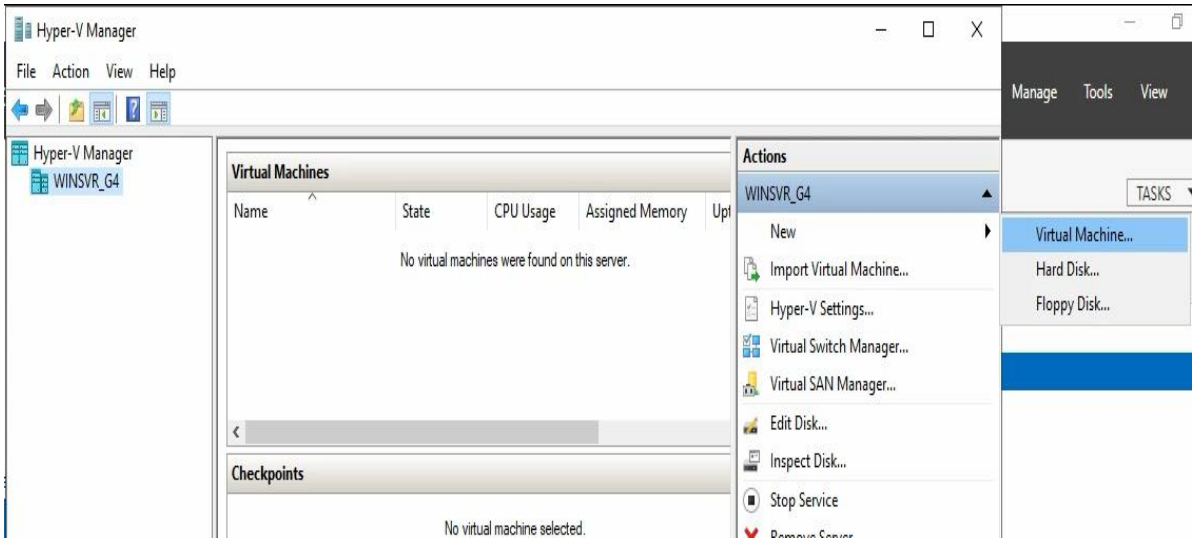


Figure 131 Create New Virtual Machine

2. Create the new virtual machine by choose a name and location for this virtual machine.

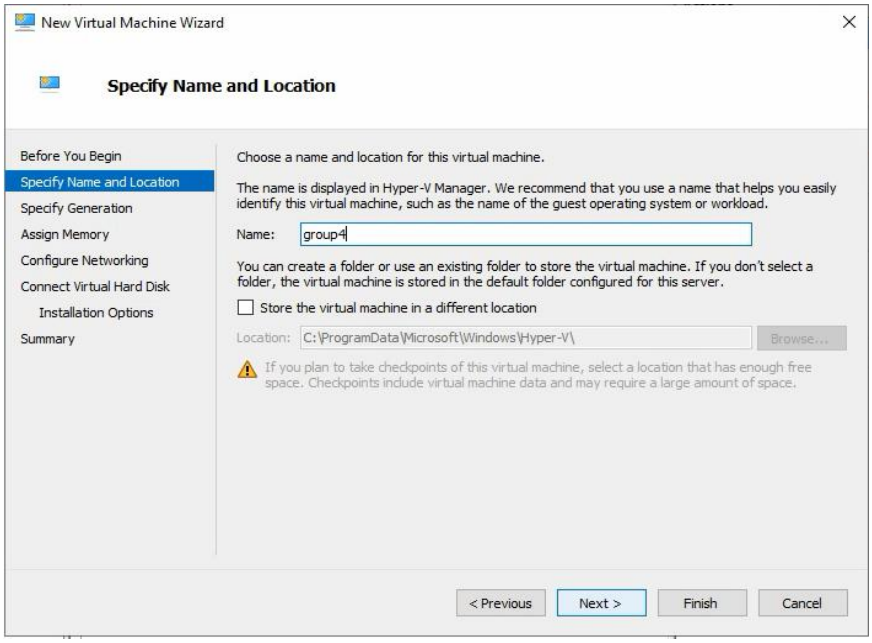


Figure 132 Specify Name and Location

3. Choose **Generation 1** for this virtual machine. This generation provides same virtual hardware to the virtual machines as in previous versions of Hyper-V. Whereas, Generation 2 provides the support for features such as SCSI boot and PXE boot using a standard network adapter. Click on next to continue.

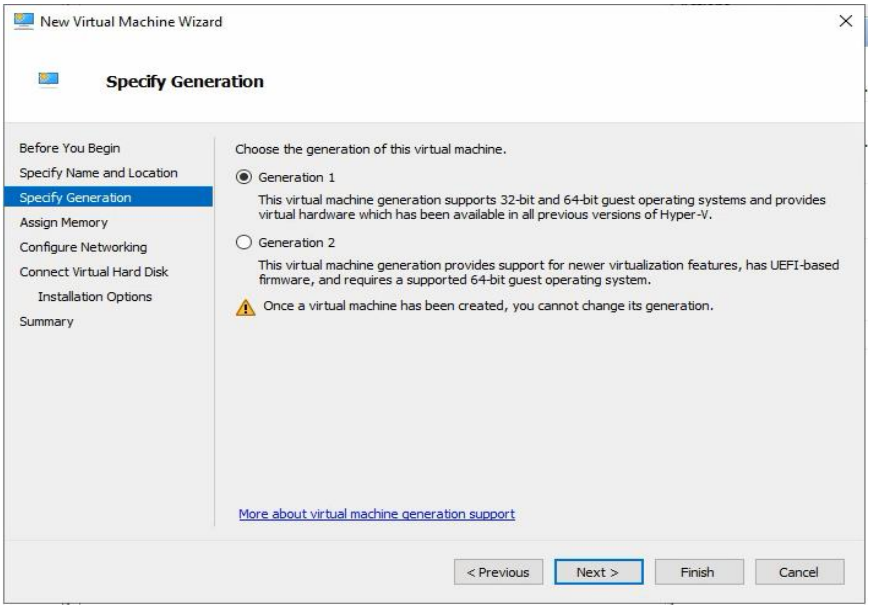


Figure 133 Specify Generation

4. On “Assign Memory” tab, set the amount of RAM in MB to allocate to this virtual machine. Click on **Next**.

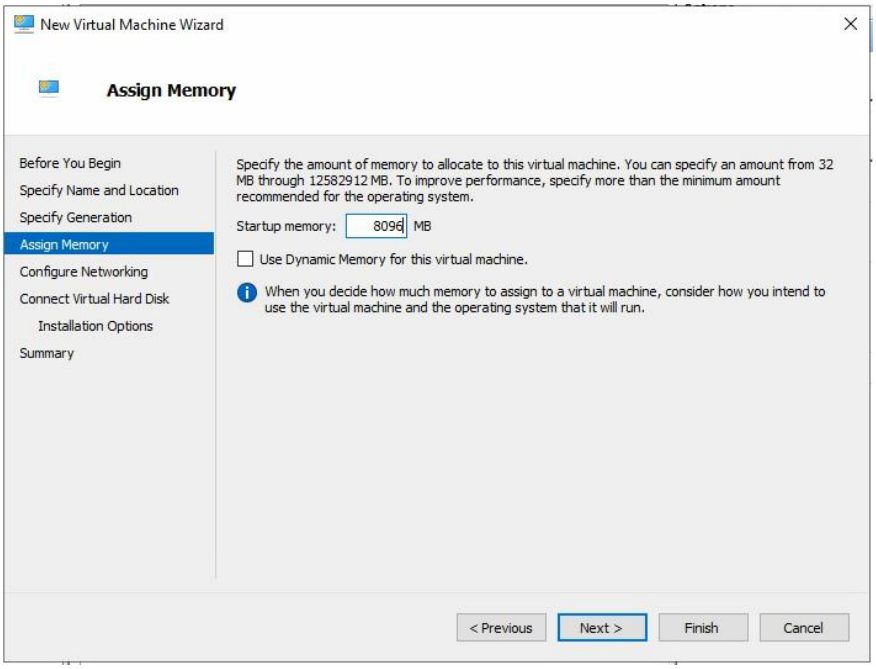


Figure 134 Assign Memory

5. On “Configure Networking” tab, select a virtual switch from the available virtual switches in the drop-down menu of connection.

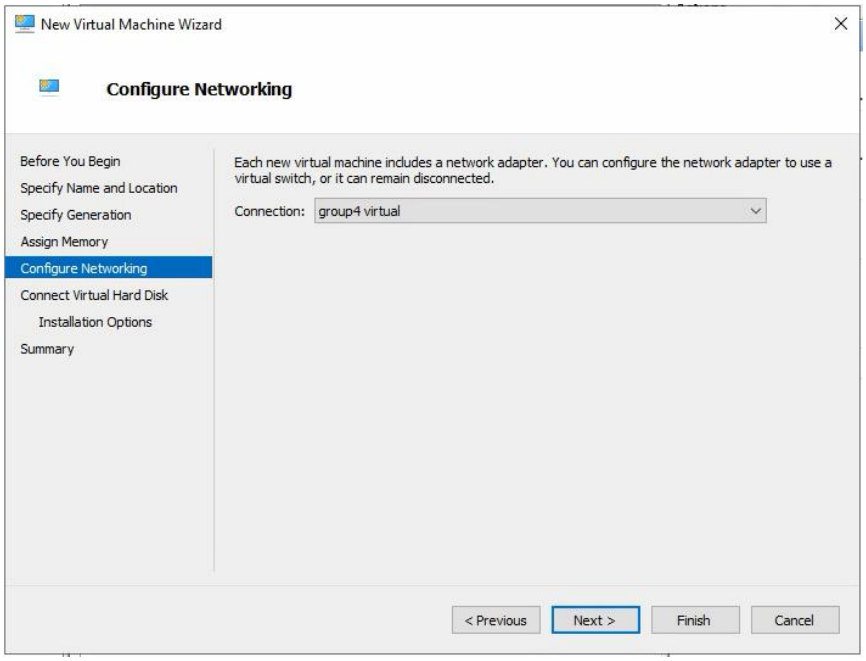


Figure 135 Configure Networking

6. Choose "**Create a virtual hard disk**". This option to create VHDX dynamically expanding virtual hard disk.

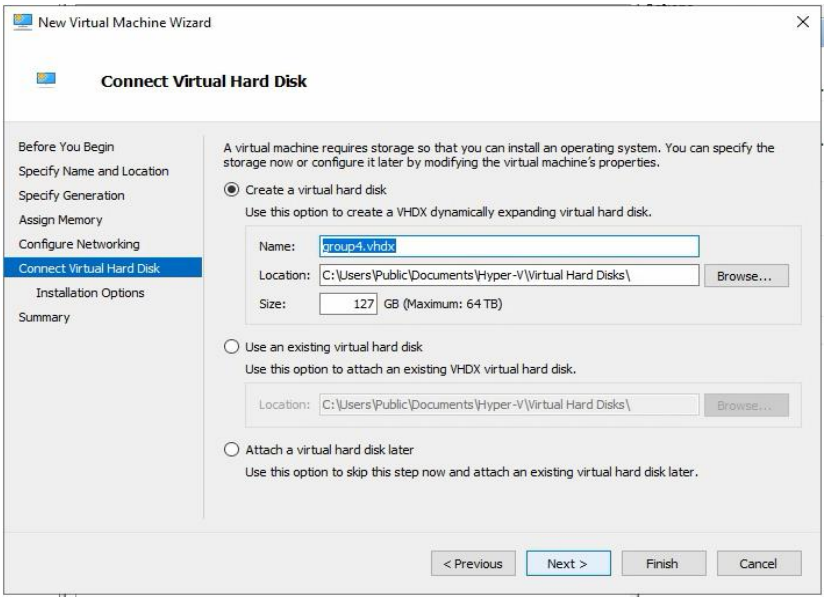


Figure 136 Connect Virtual Hard Disk

7. On "Installation Options" tab, select "**Install an operating system from a bootable image file**" to install from an ISO file. Here, will install the OS in this virtual machine through an ISO file and specified the location of ISO file here. Click on **Next** to continue the installation process.

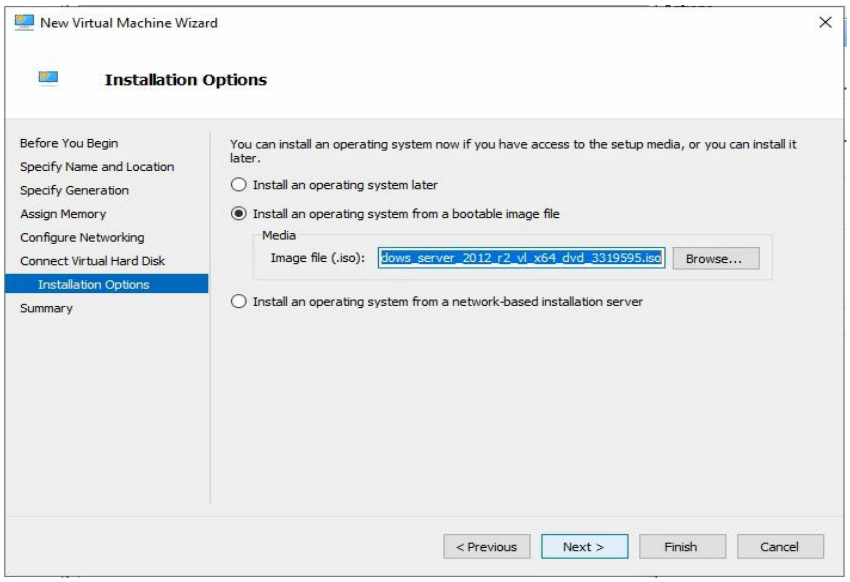


Figure 137 Installation Options

8. On “Hyper-V Manager” console, under Virtual Machines, can see that our virtual machine is listed. Right click on the virtual machine then click on **Connect** > **Start** to start the virtual machine.

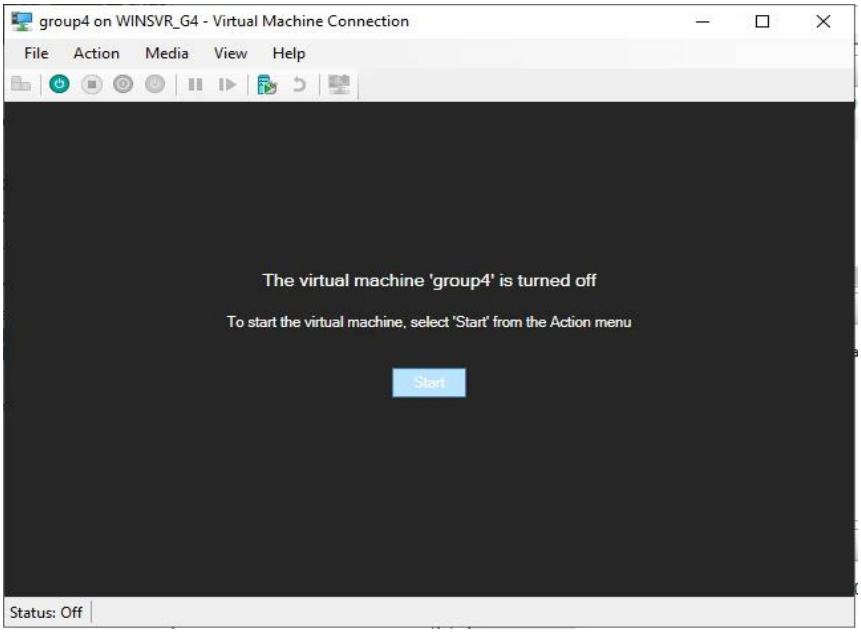


Figure 138 Virtual Machine Connection

9. Virtual Machine for Windows Server 2019 is ready to use

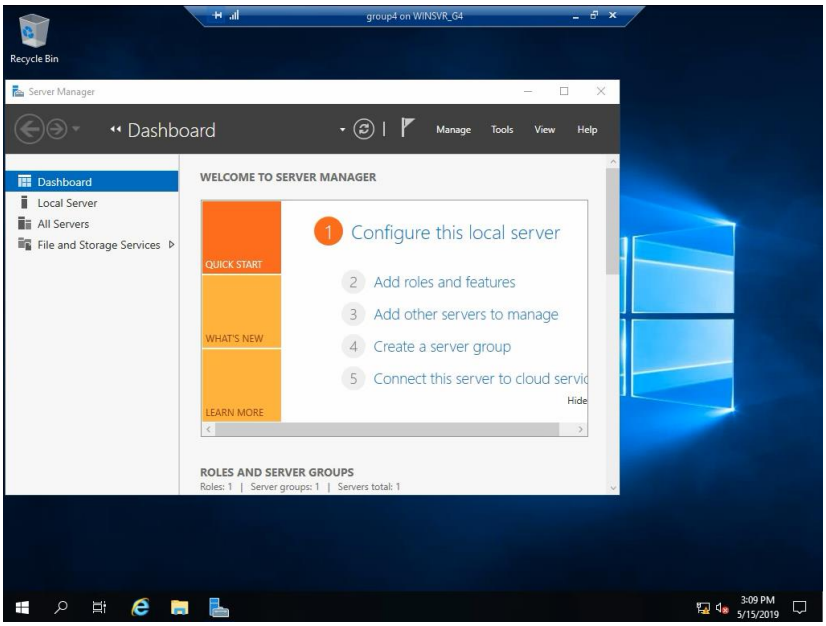


Figure 139 Group4 Virtual Machine

5.3.10 VLAN Configuration

Step 1: Create VLAN and assign port number. Enables the VLAN to be used by using switchport mode access command.

VLAN for Windows Server 2019
SW_G4 (config)#vlan 20

SW_G4 (config-vlan)#name Windows

SW_G4 (config-vlan)#exit

SW_G4 (config)#int range f0/1 - 2

SW_G4 (config-if-range)#switchport mode access

SW_G4 (config-if-range)#switchport access vlan 20

SW_G4 (config-if-range)#exit

VLAN for Ubuntu 18.04
SW_G4 (config)#vlan 30

SW_G4 (config-vlan)#name UbuntuServer

SW_G4 (config-vlan)#exit

SW_G4 (config)#int range f0/3 - 4

SW_G4 (config-if-range)#switchport mode access

SW_G4 (config-if-range)#switchport access vlan 30

SW_G4 (config-if-range)#exit

VLAN for Debian 9
SW_G4 (config)#vlan 40

SW_G4 (config-vlan)#name DebianServer

SW_G4 (config-vlan)#exit

SW_G4 (config)#int range f0/5 - 6

SW_G4 (config-if-range)#switchport mode access

SW_G4 (config-if-range)#switchport access vlan 40

SW_G4 (config-if-range)#exit

VLAN for Client

SW_G4 (config)#vlan 80

SW_G4 (config-vlan)#name Client

SW_G4 (config-vlan)#exit

SW_G4 (config)#int range f0/7 – 20

SW_G4 (config-if-range)#switchport mode access

SW_G4 (config-if-range)#switchport access vlan 80

SW_G4 (config-if-range)#exit

VLAN for Client ACL

SW_G4 (config)#vlan 100

SW_G4 (config-vlan)#name Client2

SW_G4 (config-vlan)#exit

SW_G4 (config)#int range f0/21 - 23

SW_G4 (config-if-range)#switchport mode access

SW_G4 (config-if-range)#switchport access vlan 100

SW_G4 (config-if-range)#exit

Step 2: Create trunk and from switch to router.

SW_G4 (config)#int range fa0/24

SW_G4 (config-if-range)#switchport mode trunk

SW_G4 (config-if-range)#exit

Step 3: Configure interVlan in router

R4 (config)#int f0/0.20
R4 (config-subif)#encapsulation dot1q 20
R4 (config-subif)#ip add 192.168.6.129 255.255.255.248
R4 (config-subif)#no shutdown
R4 (config-subif)#exit

R4 (config)#int f0/0.30
R4 (config-subif)#encapsulation dot1q 30
R4 (config-subif)#ip add 192.168.6.137 255.255.255.248
R4 (config-subif)#no shutdown
R4 (config-subif)#exit

R4 (config)#int f0/0.40
R4 (config-subif)#encapsulation dot1q 40
R4 (config-subif)#ip add 192.168.6.145 255.255.255.248
R4 (config-subif)#no shutdown
R4 (config-subif)#exit

R4 (config)#int f0/0.80
R4 (config-subif)#encapsulation dot1q 80
R4 (config-subif)#ip add 192.168.6.65 255.255.255.192
R4 (config-subif)#no shutdown
R4 (config-subif)#exit

R4 (config)#int f0/0.100
R4 (config-subif)#encapsulation dot1q 100
R4 (config-subif)#ip add 192.168.5.1 255.255.255.192
R4 (config-subif)#no shutdown
R4 (config-subif)#exit

5.3.11 AAA with Radius

5.3.11.1 Installation and Setup the Radius

Step 1: Add roles and features Wizard > Select Role based or feature-based installation > Click button Next. To installation new roles and feature.

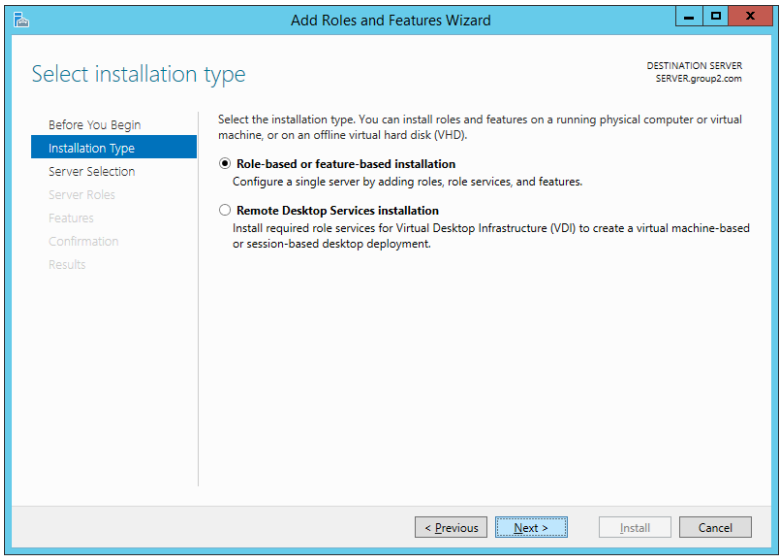


Figure 140 Add Roles and Feature Wizard

Step 2: After select a server from the server pool > Select Network Policy and Access Services.

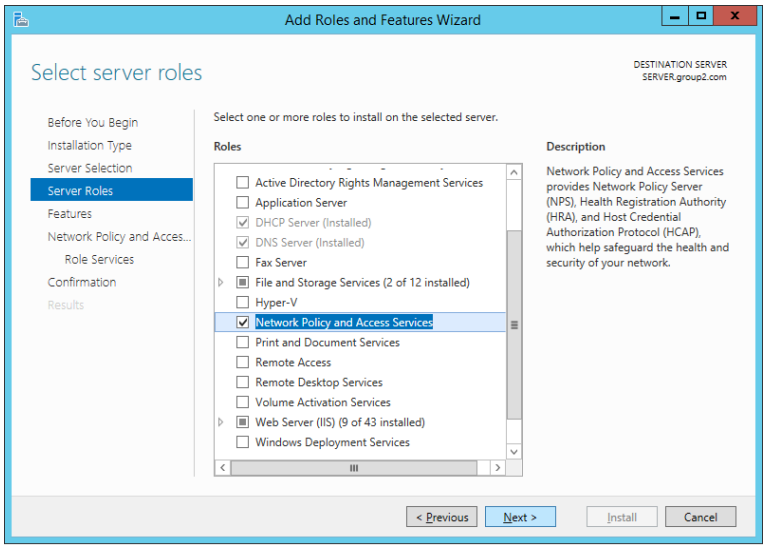


Figure 141 Add Roles new tools Network Policy and Access Services.

Step 3: Then, click Add Feature. To add new tools is Network Policy and Access Services Tools.

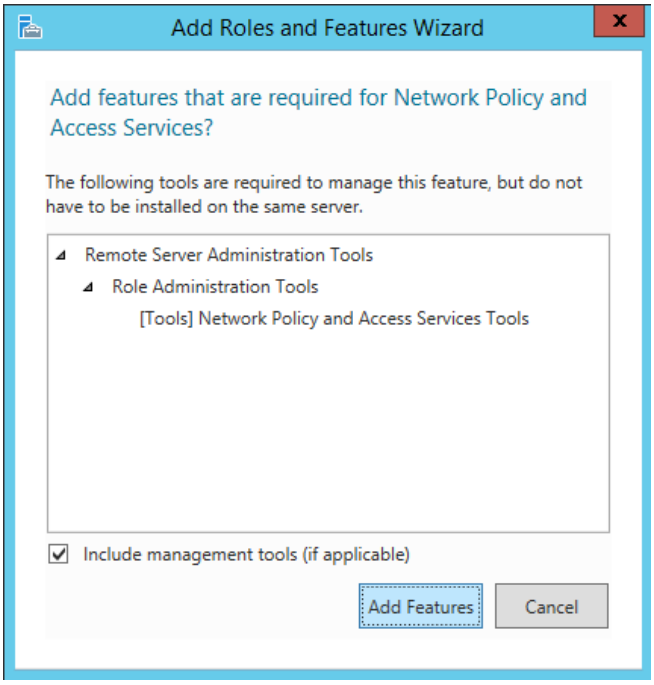


Figure 142 Add Feature Role Administration Tools

Step 4: After finish click Network Policy and Access Services > Click Next > Network Policy Server > Click Next and Click button Install to install new tools is Network Policy Server and Network Policy and Access Services.

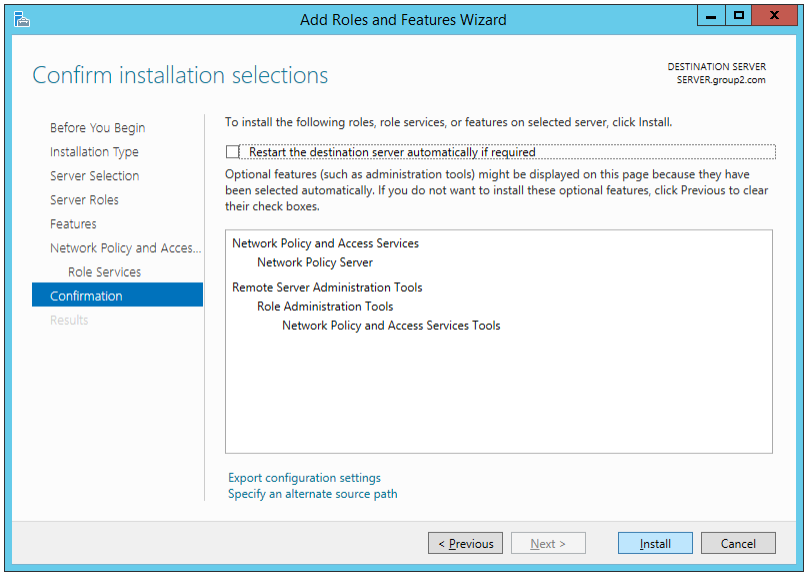


Figure 143 Result of Network Policy and Access Services Tools.

5.3.11.2 Create a new Active Directory Users and Computer

Step 5: Click Tools on top right on service manager page and Select Active Directory User and Computer. Then, click users file and it has users and group name.

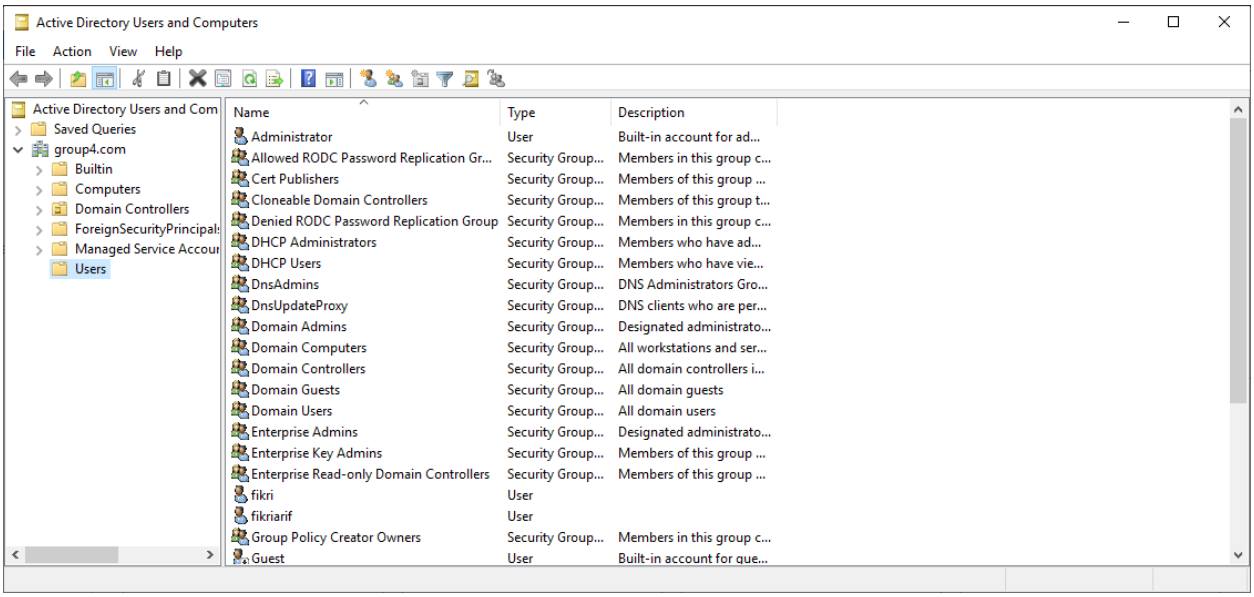


Figure 144 Active Directory Users and Computer

Step 6: Click button logo new Group or click right and select new group. Then create a group name and select global and security group. Then click button OK for done.

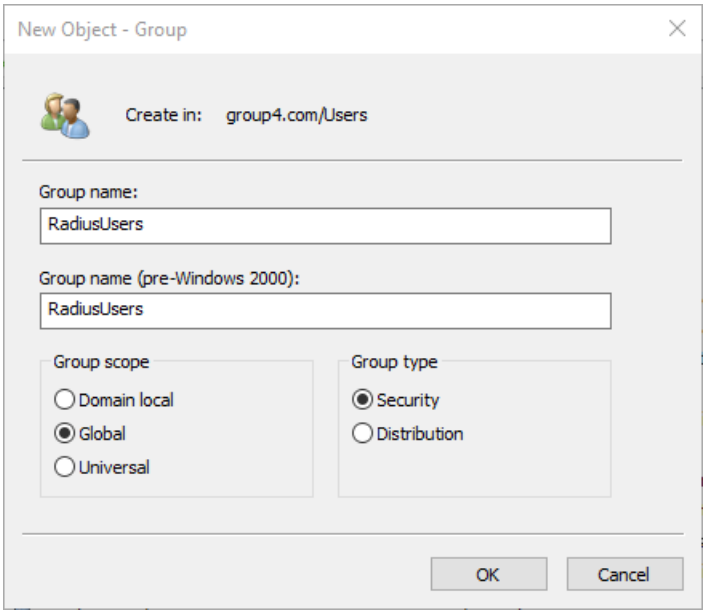


Figure 145 Create name group

Step 7: Click button logo new users or click right and select new users. Then create a user's first name, last name and logon name with mail DNS @group4.com. Then click button Next.

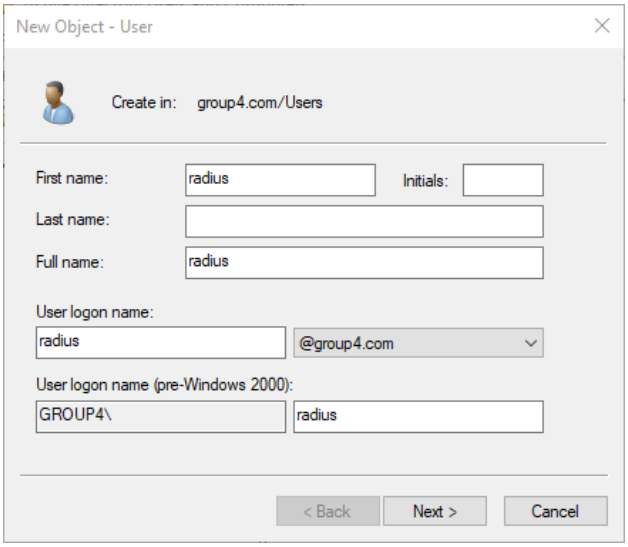


Figure 146 Create First name and Last name User

Step 8: Create new password and confirm password users then click button next. Then, output the result of user name "radius" and user logon name radius@group4.com. After finish everything, click button Finish.

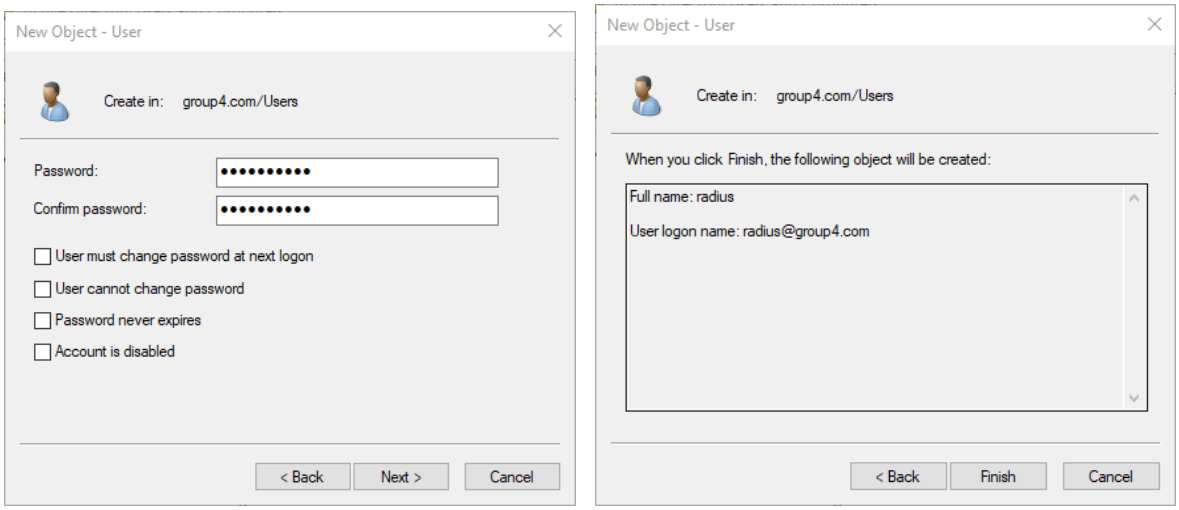


Figure 147 Create password and confirm password / Result of create new users.

Step 9: Click user name “radius” and click right then select add to group.

Figure 148 Select radius user

Step 10: After finish select add to group. Now select group is “RadiusUsers” and click Check Names to confirm the group will be selected. Then, click OK.

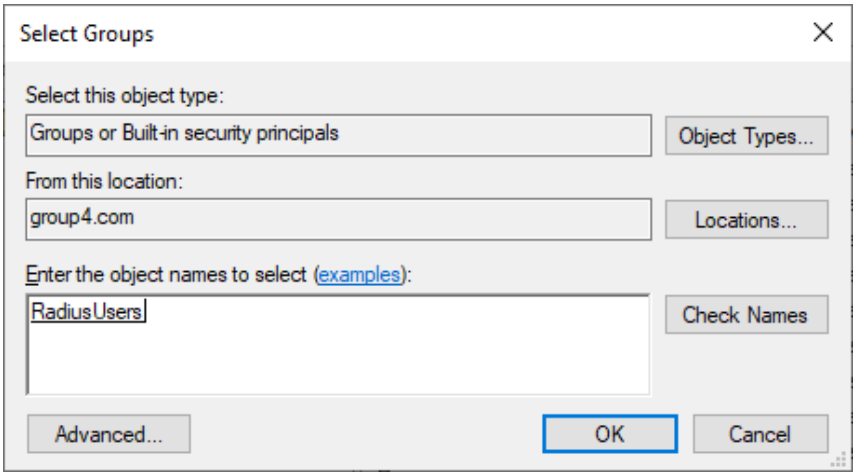


Figure 149 Select Group for user.

Step 11: Select a group name is RadiusUsers and click right. Select a properties to check have a user will done be group members.

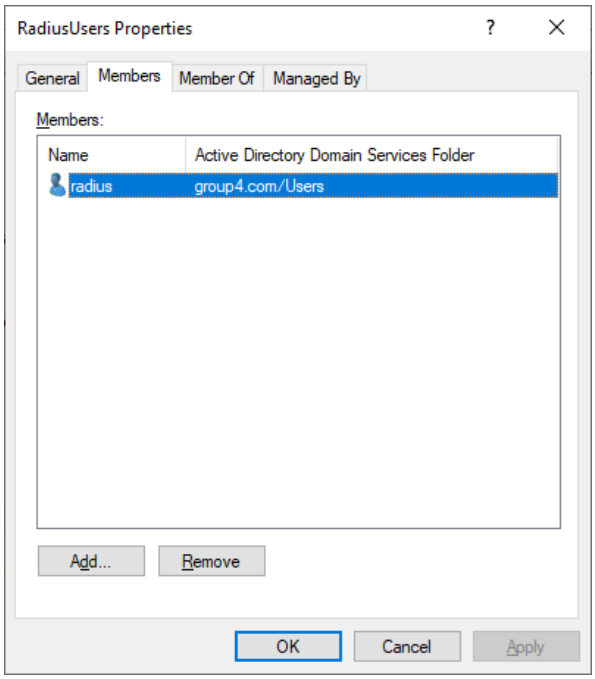


Figure 150 User Properties

Step 12: First go to tools at Service manager and select a DNS Manager. After that, click WINSVR_G4 > Click Forward Lookup Zones > Click group4.com. This DNS Manager is a monolithic DNS server that provides many types of DNS service, including caching, Dynamic DNS update, zone transfer, and DNS notification.

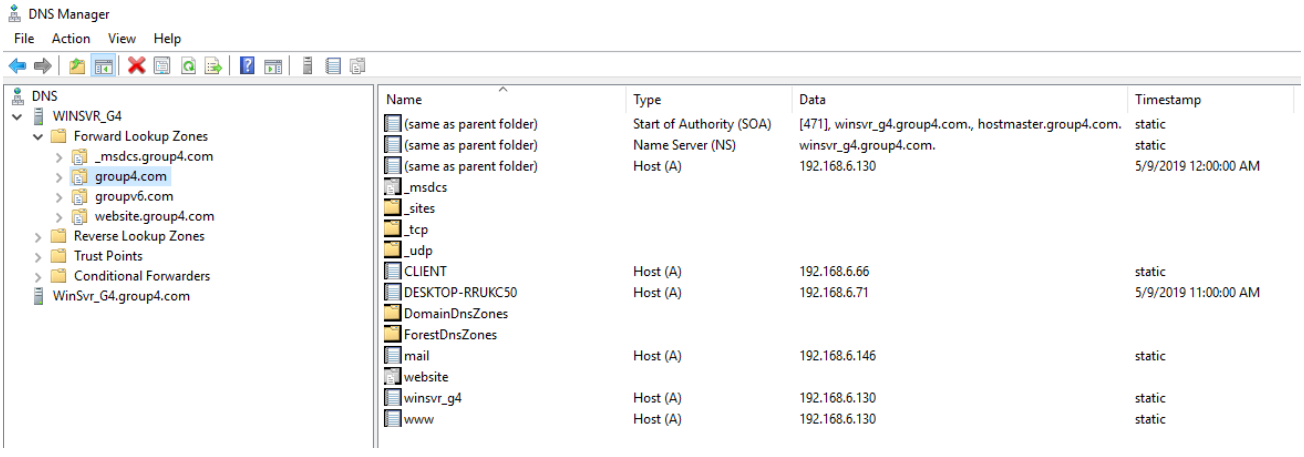


Figure 151 DNS Manager and group4.com

Step 13: Select a group4.com then click right and select New Host. Create new Name and set up IP address from router or IP address gateway. Then click Add Host. After click Add Host. The new host wil be record and was successfully created.

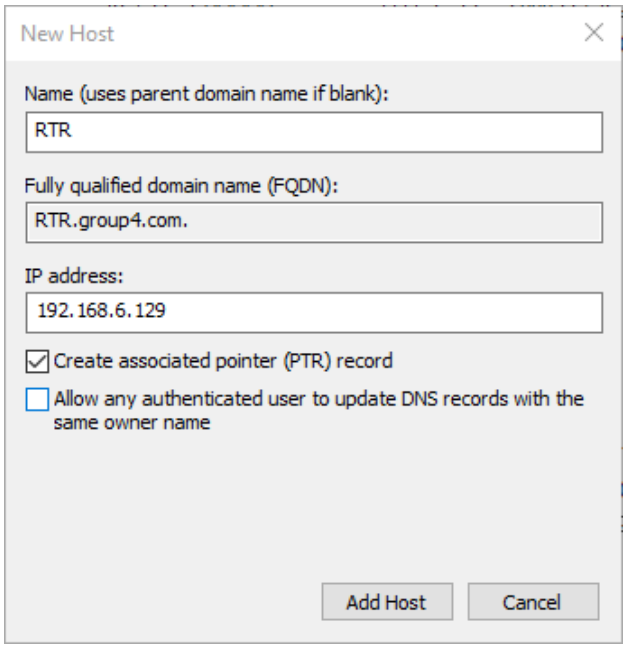


Figure 152 Create a new name and set up IP address

Step 15: First go to tools at Service manager and select a Network Policy Server. After that, click NPS (Local) > Click RADIUS Clients and Servers > Click RADIUS Clients. This DNS Manager is a monolithic DNS server that provides many types of DNS service, including caching, Dynamic DNS update, zone transfer, and DNS notification.

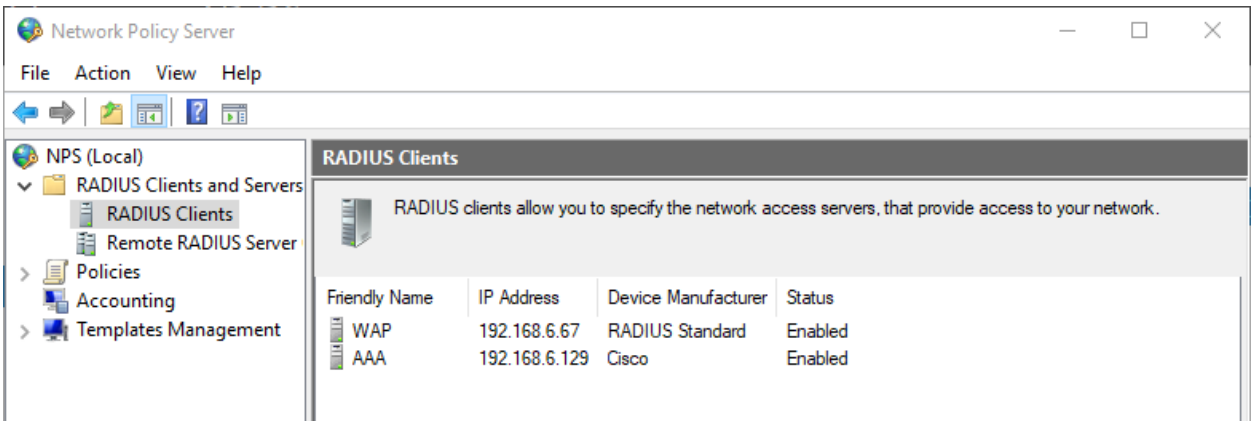


Figure 153 Radius Client

Step 16: Select a RADIUS Client then click right and select New RADIUS Client. Create Friendly Name and IP address from DNS. It can write rtr.group4.com is name of DNS. Select Manual password and enter the user password. Click of top button is Advanced > Click a vendor name and select Cisco. After finish click a "Verify…" button at Address (IP or DNS).

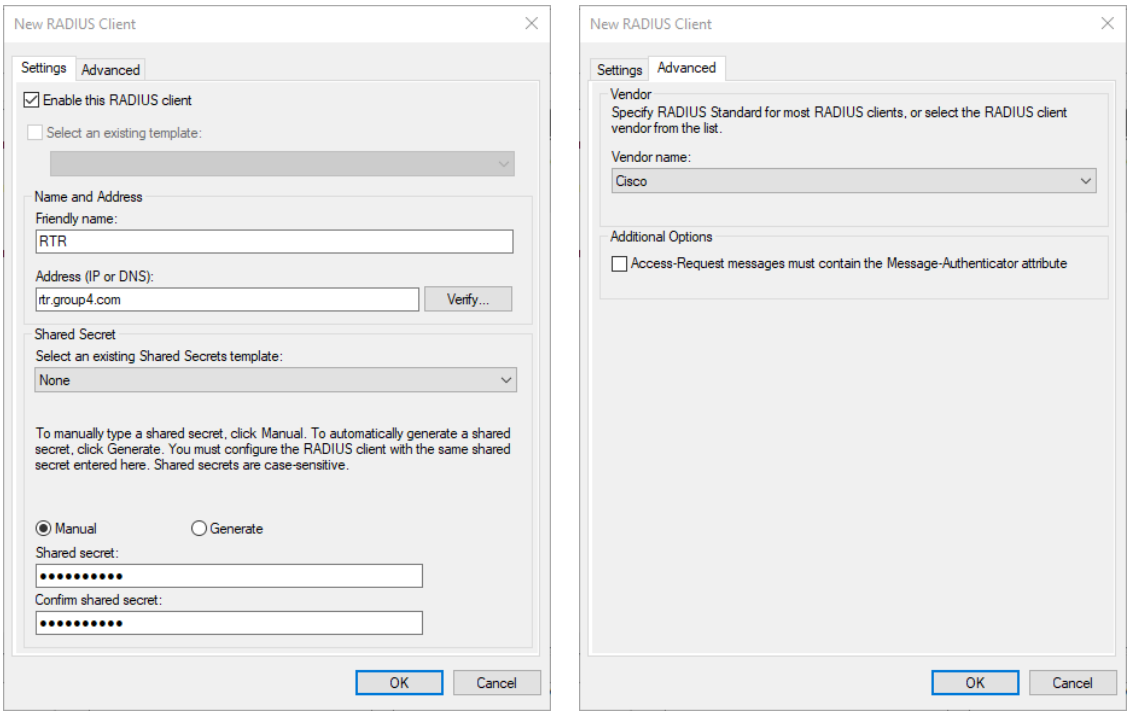


Figure 154 Create New Radius Client / Setting advanced

Step 17: After finish click button "Verify..." then go to page Verify Address and click button Resolve the IP address. After that, out of IP address from DNS Server.

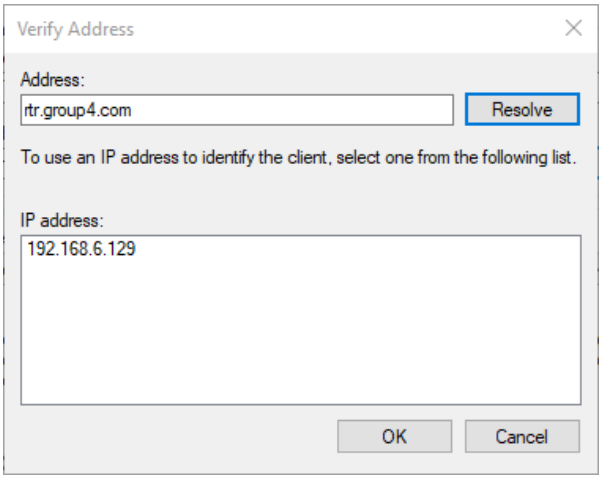


Figure 155 Verify Address from IP address DNS

Step 18: Firstly, Select a Policies. After that, click Connection Request. Connection (CRC). This CRC is to allow the designate whether connection request are processed locally or forwarded to remote RADIUS servers.

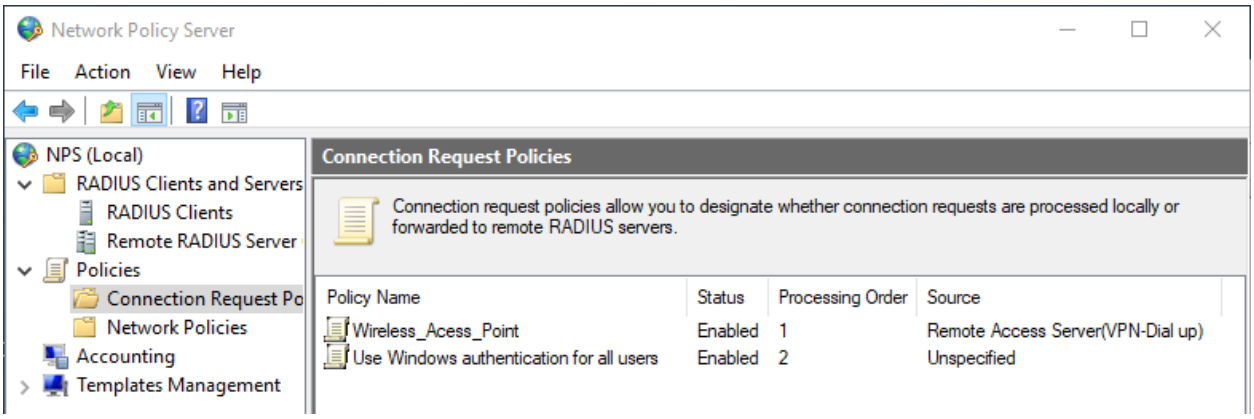


Figure 156 Connection Requites Policies

Step 19: Select a Connection Request Policy then click right and select New Connection Request. Connection. Create a new policy name. Then, click Next.

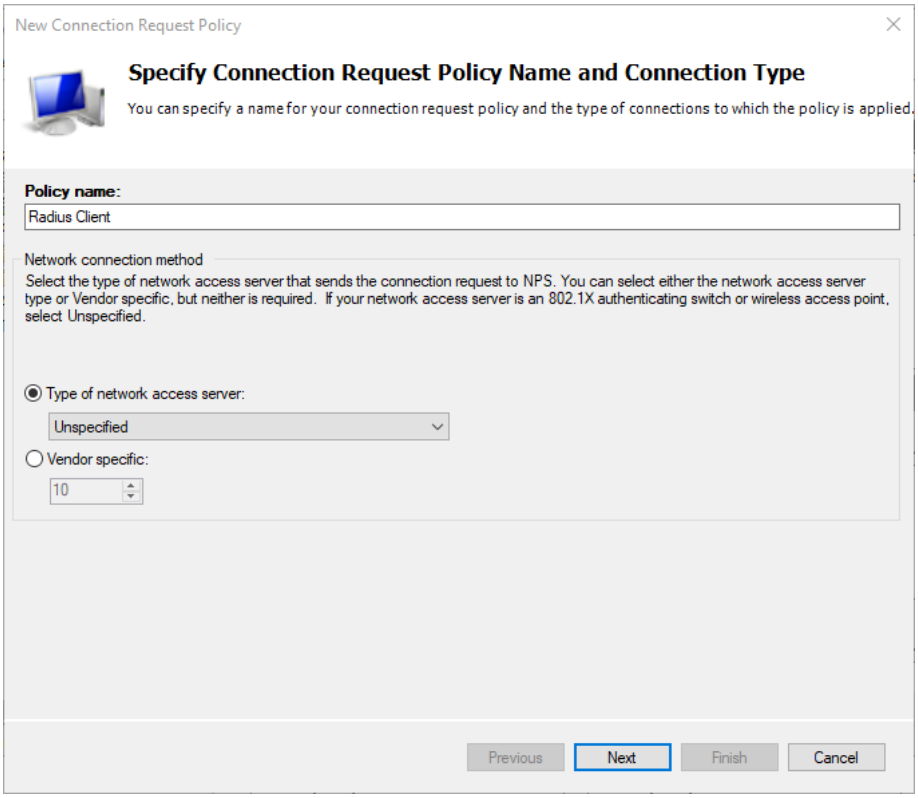


Figure 157 Create a new Policy Name

Step 20: Click button Select condition > Click Client Friendly Name then click button Add new Client Friendly Name.

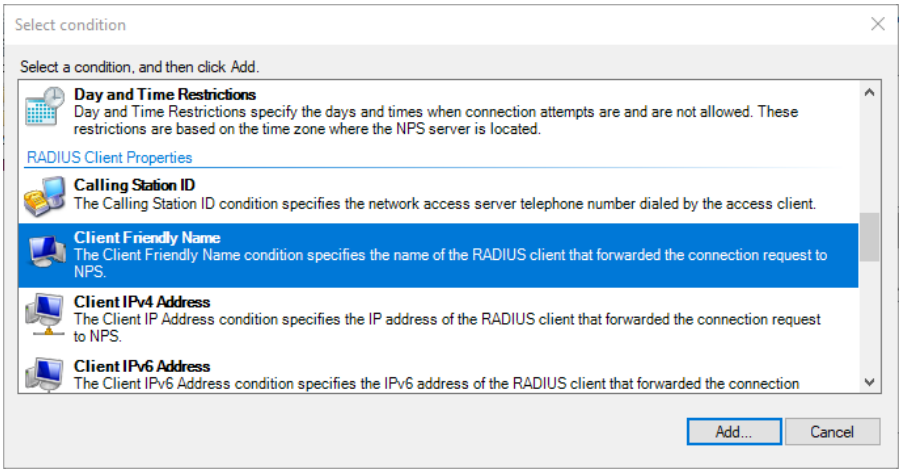


Figure 158 Select a Client Friendly Name

Step 21: Enter the value Client Friendly Name of the RADIUS client.

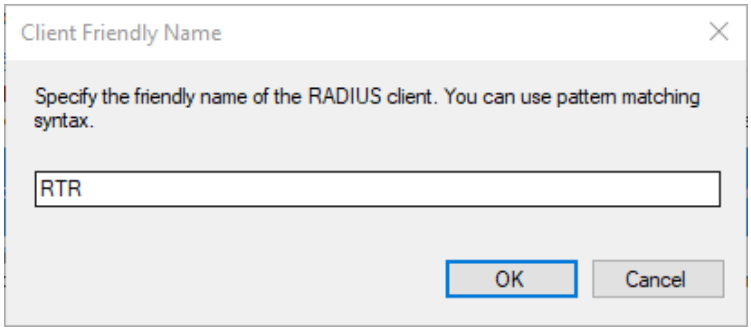


Figure 159 Create a name Friendly Name

Step 22: Result of Client Friendly Name with value is RTR. Then click button Next.

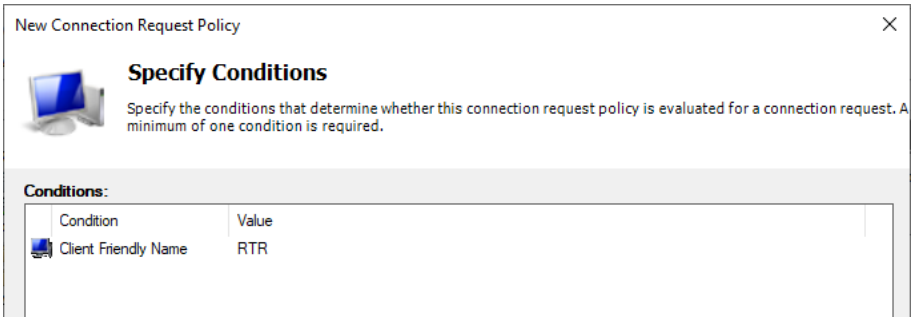


Figure 160 Check the result Friendly Name

Step 23: After finish set up the Client Friendly Name. Then, output of result Policy Conditions.

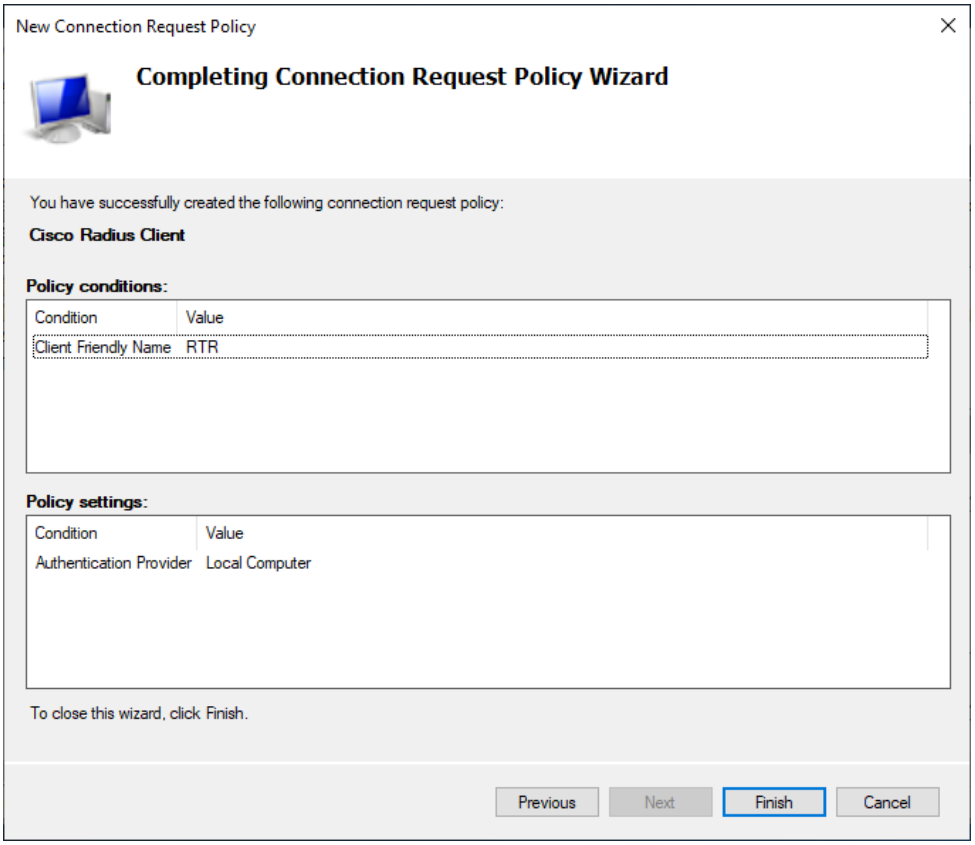


Figure 161 Result Client Friendly Name

Step 24: Secondly, Select a Policies. After that, click Network Policy. The Network Policy is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy. It is the successor of Internet Authentication Service (IAS).

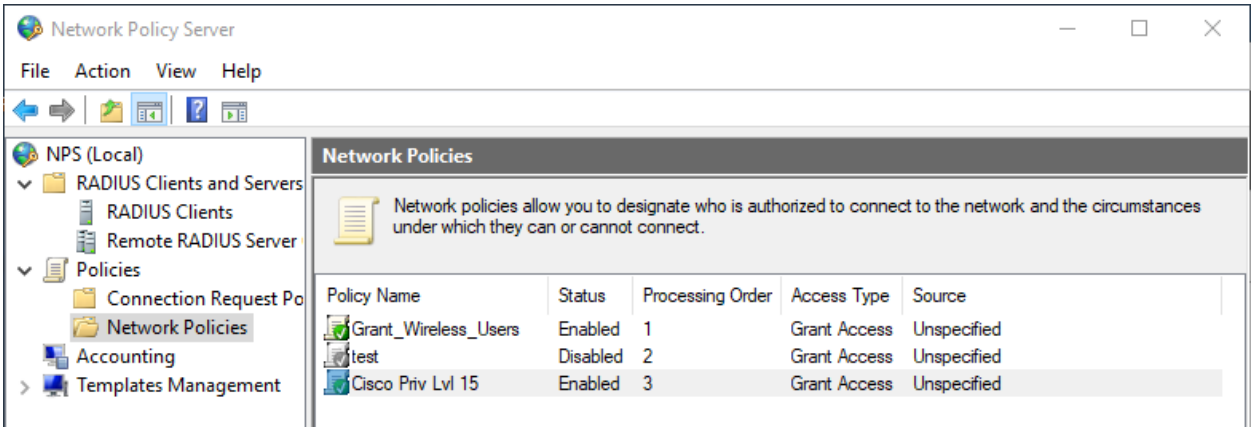


Figure 162 Network Policy

Step 25: Select a Network Policy then click right and select New Network Policy. Create a new policy name is “Cisco Priv Lvl 15”. Then, click Next.

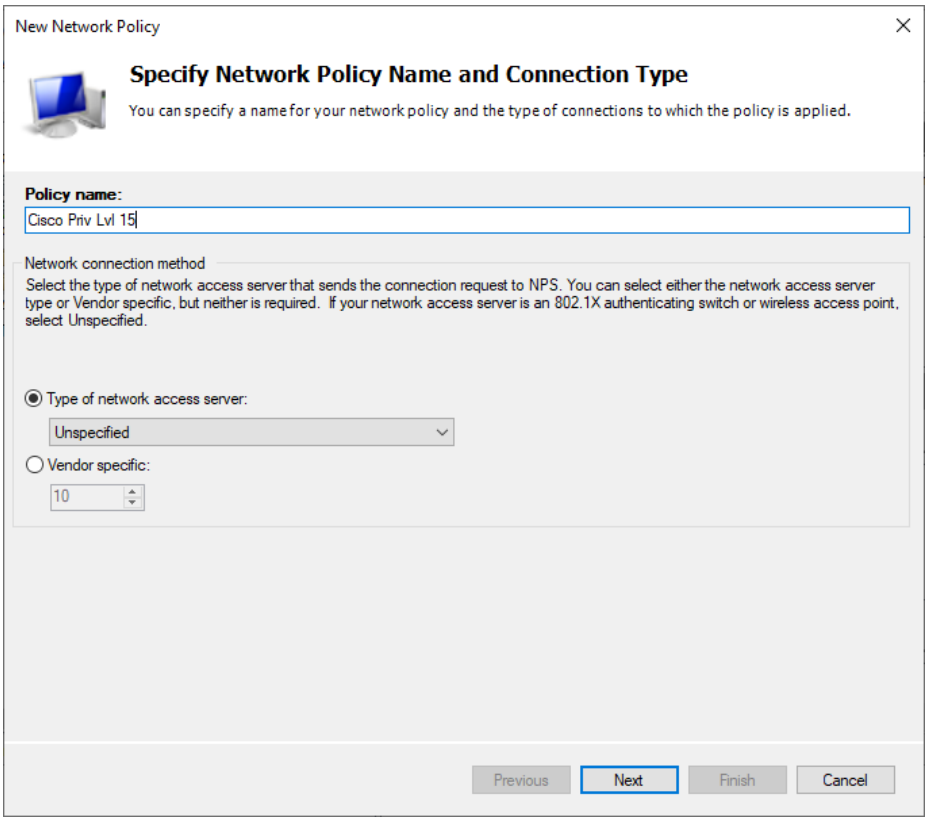


Figure 163 Create a New Network Policy

Step 26: After click Select condition go to Windows Groups and click button Add.

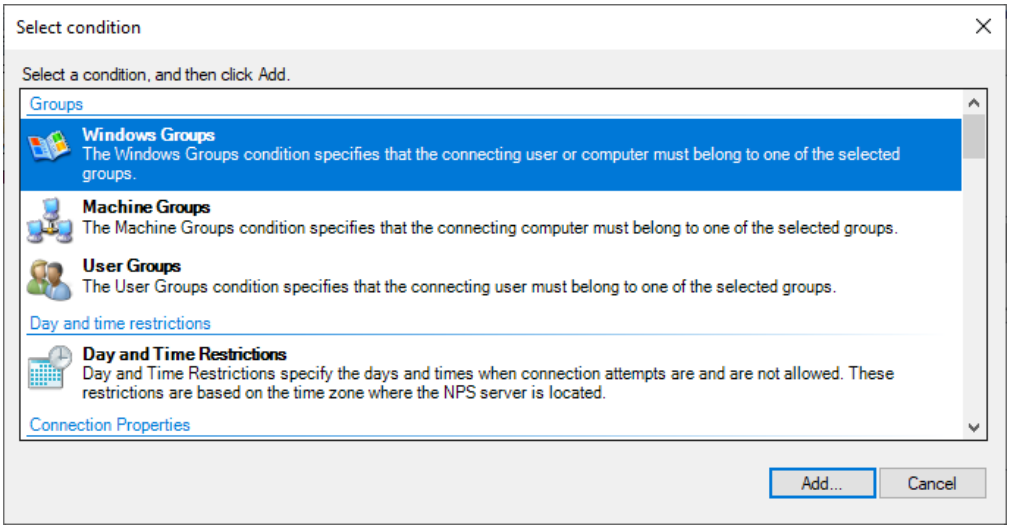


Figure 164 Select Condition Windows Groups

Step 27: After click Windows Groups go to page Select Group then write the group is "RadiusUsers" then click Check Names to confirm the group will be selected. Then, click OK.

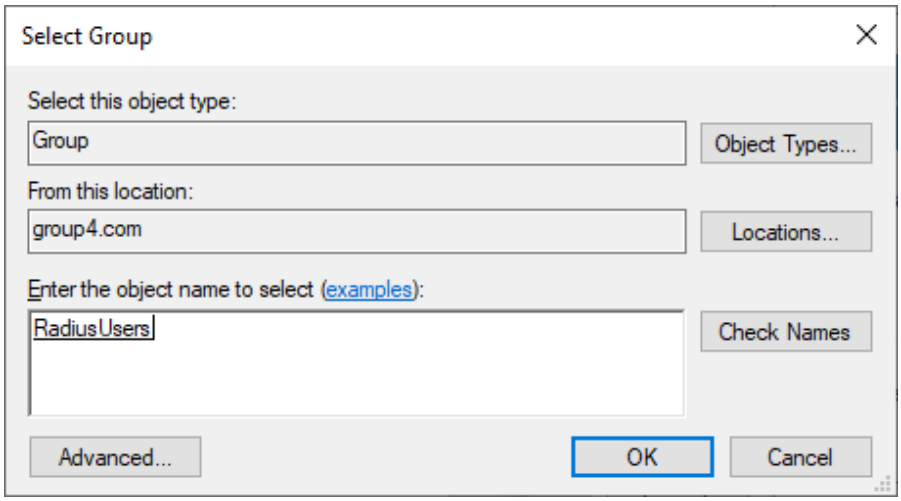


Figure 165 Check name group

Step 28: After finish set up the specify condition for Windows Groups. Then, go to page Configure Settings > Select a Standard at Radius Attributes > Click Framed Protocol (PPP) > Click button Remove. After that, done removed the Click Framed Protocol (PPP). After finish that, go to Vendor Specific.

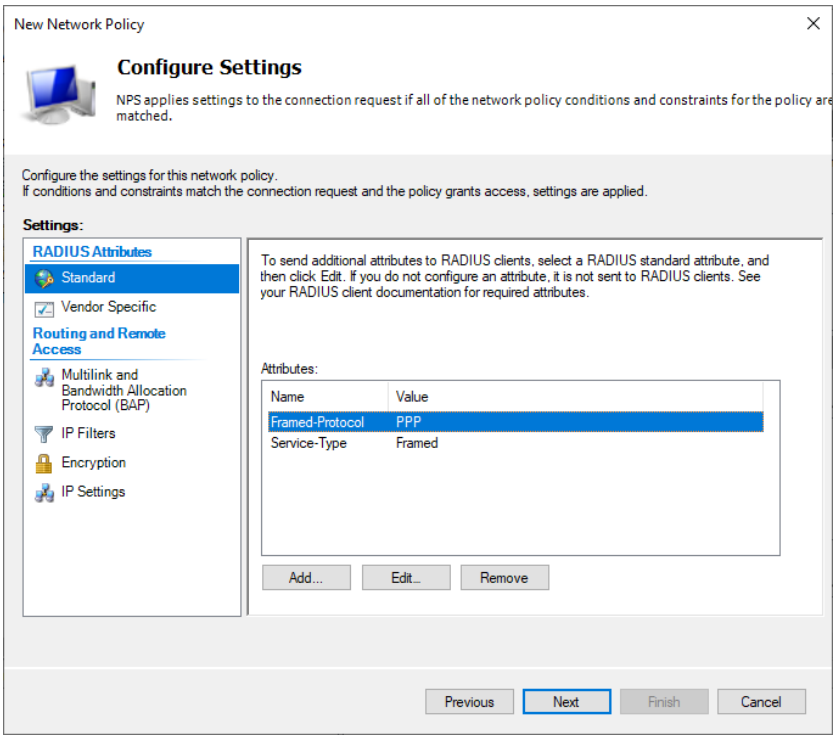


Figure 166 Configuration Setting Standard

Step 29: After click Vendor Specific, go to Add Vendor Specific Attribute and Select the Cisco-AV-Pair with Vendor is Cisco. Then click button Add.

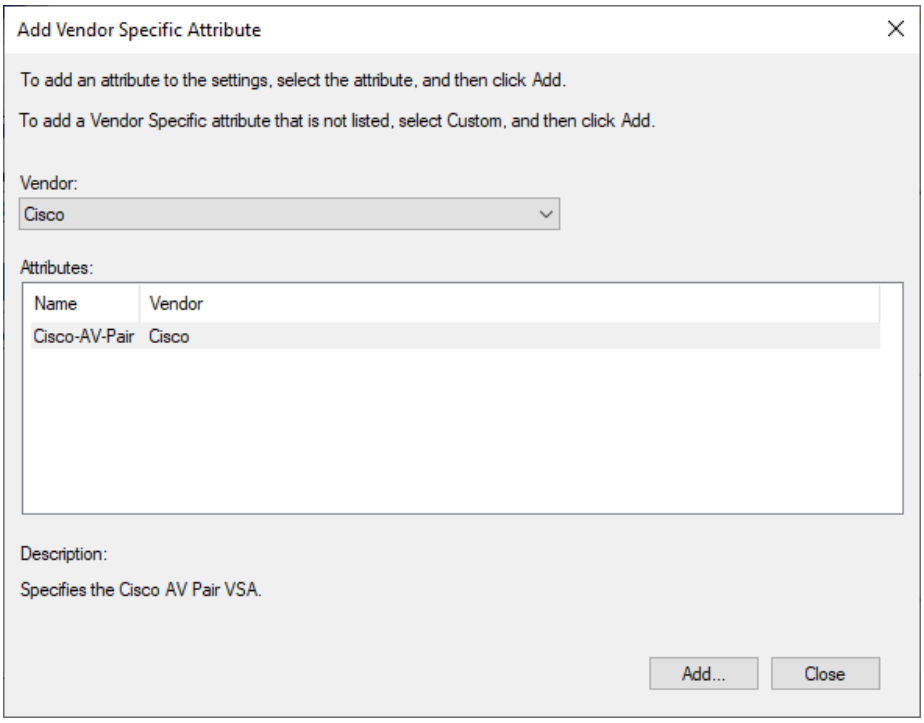


Figure 167 Add Vendor Specific Attribute

Step 30: After click button add for Cisco-AV-Pair with Vendor is Cisco. Enter the new attribute value is “shell-priv-lvl-15”. Then click the button OK.

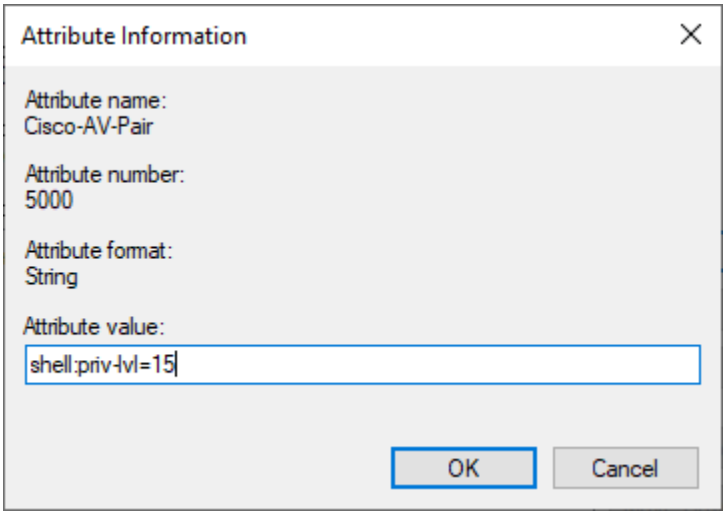


Figure 168 Attribute Information

Step 31: After finish set up the Cisco-AV-Pair with Vendor is Cisco and it has value “shell-priv-lvl-15”. Then, the output of result Vendor Specific.

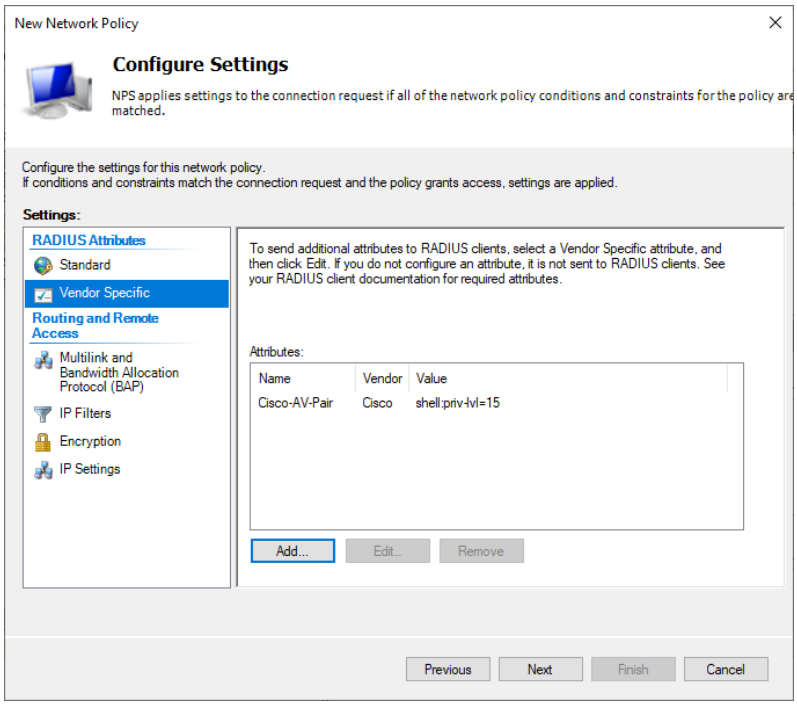


Figure 169 Configuration Settings

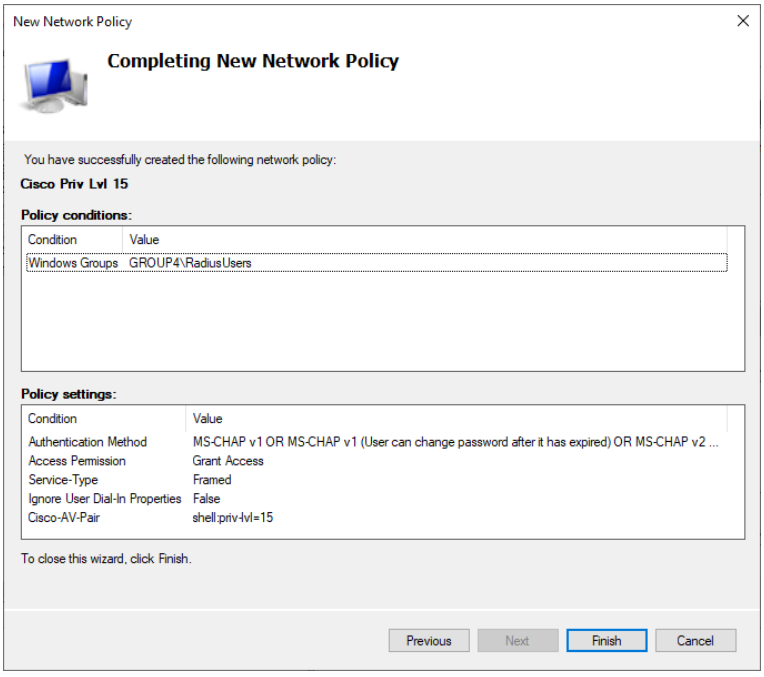


Figure 170 Completing New Network Policy

Step 32: After that, Select an Accounting. After that, click Change Log Properties. Accounting is atomically configure a local or remote SQL server with a database for NPS accounting.

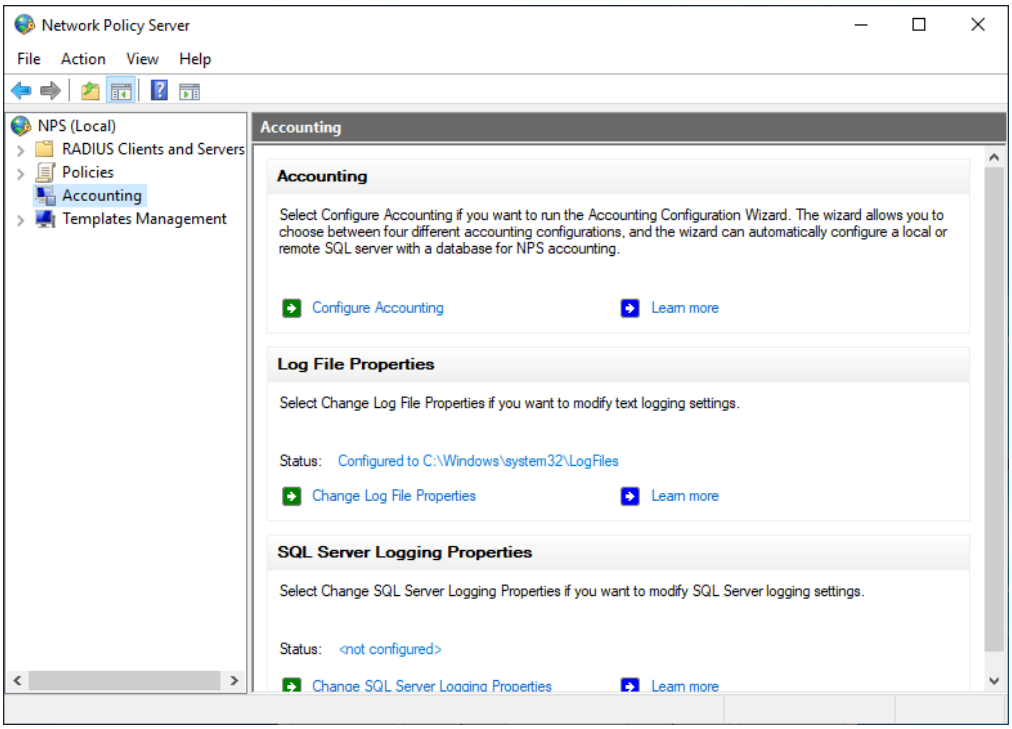


Figure 171 Accounting and Change Log File Properties

Step 32: Log File Properties, it can setting and

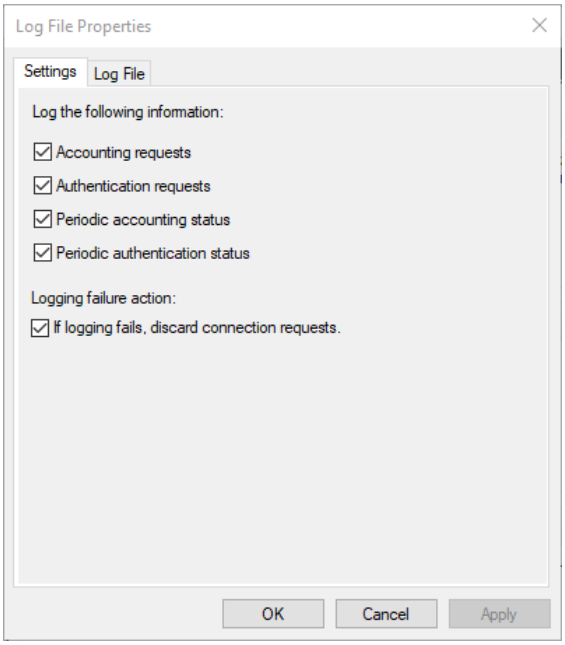


Figure 172 Log File Properties and Setting

Step 33: Log File Properties can create new log file likely Daily, Weekly, Monthly, Never and When log file reached that size. Then click OK.

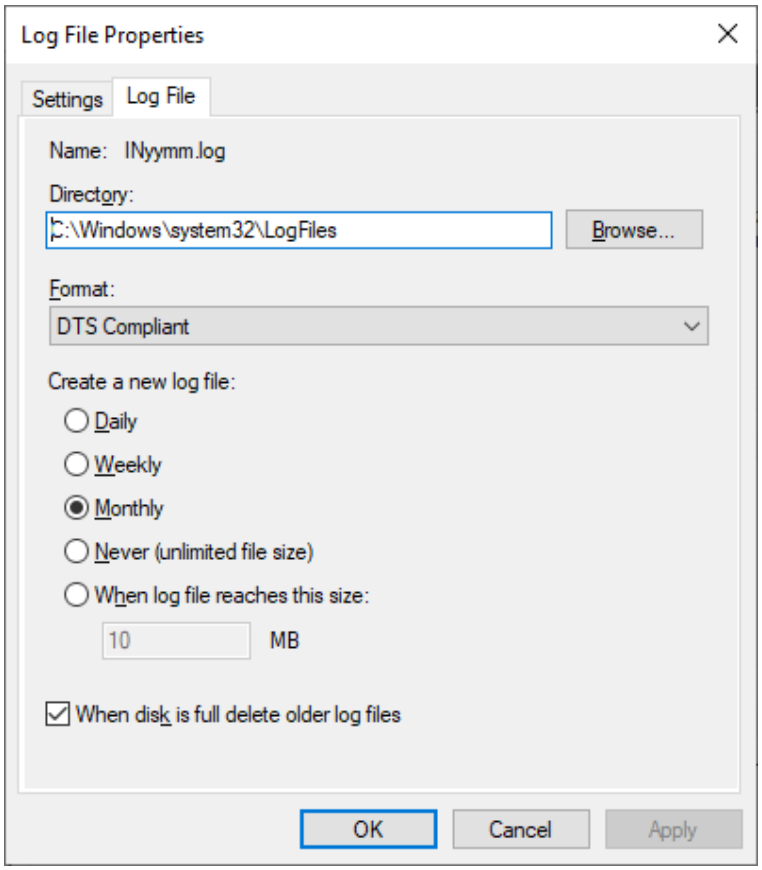


Figure 173 Log File Properties in Log File

5.3.11.3 Configuration of AAA

Step 1: Firstly, configuration and create the admin and secret password with privilege 15.

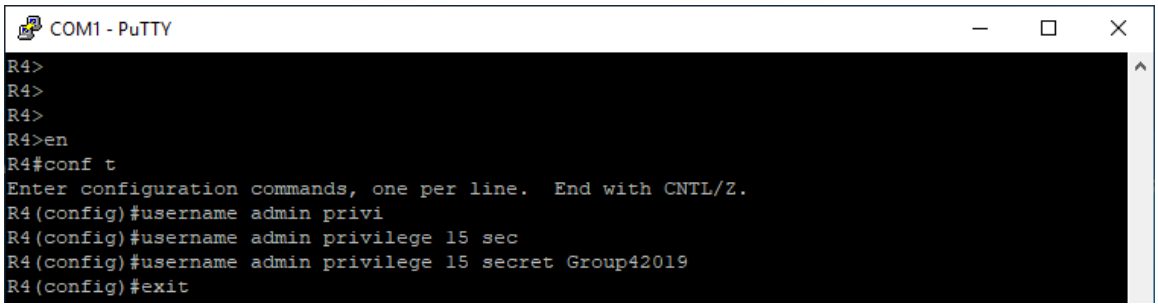


Figure 174 Configure and create the admin and password

Step 2: Enable ssh version 2. Then, call the ip domain-name is group4.com. Create the crypto key generate rsa and enter the value number of bits is 1024.

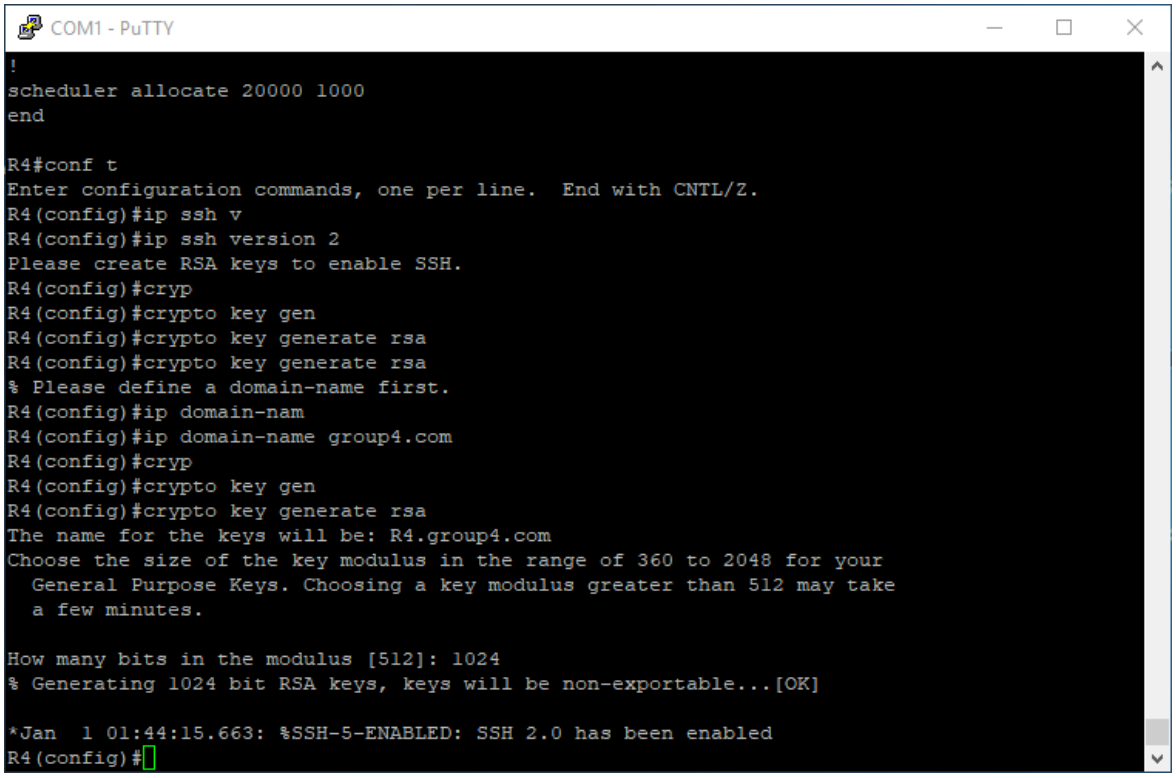


Figure 175 Crypto key generate rsa

Step 3: The line vty 0 4, line vty is Virtual Terminal lines of the router, used solely to control inbound Telnet connections. Line vty 0 4 is 0 4 for users how many user can access login at the router and the number of 0 4 has 5 users can access login at the router. After that, create and configure the aaa new-model have 3 modes are authentication, authorization and accounting.

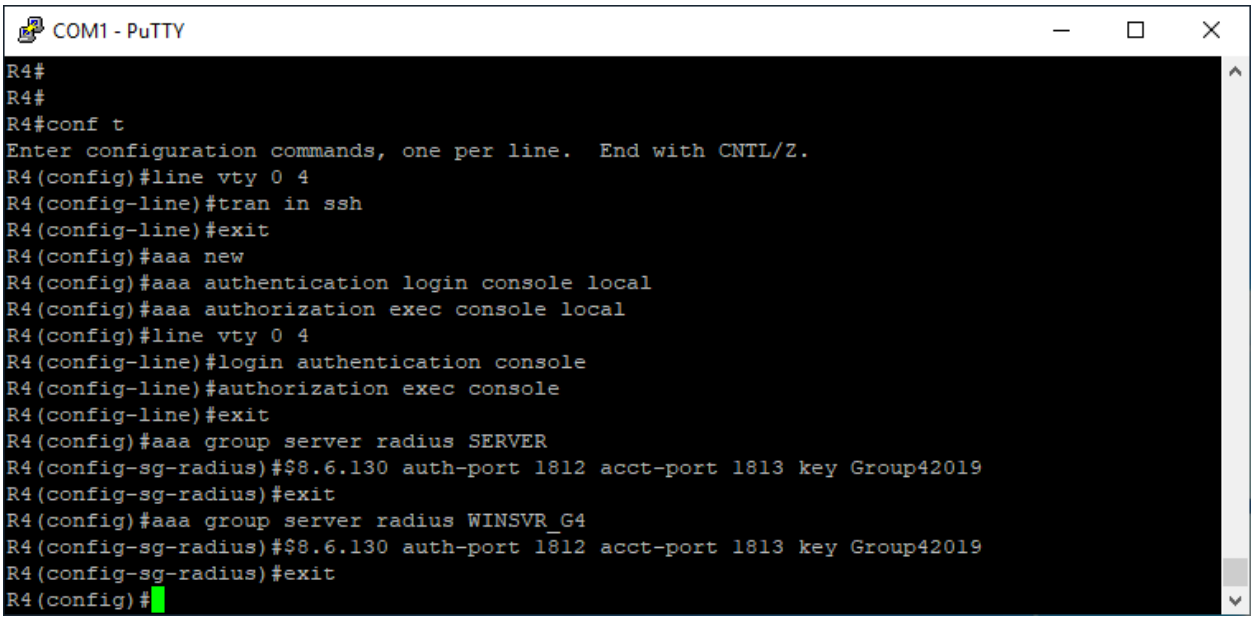


Figure 176 AAA new model authenticate and authorization

Step 4: Create aaa authentication login, create aaa group server radius WINSVR_G4. Then, create aaa authorization exec default group WINSVR_G4. Lastly, write debug radius.

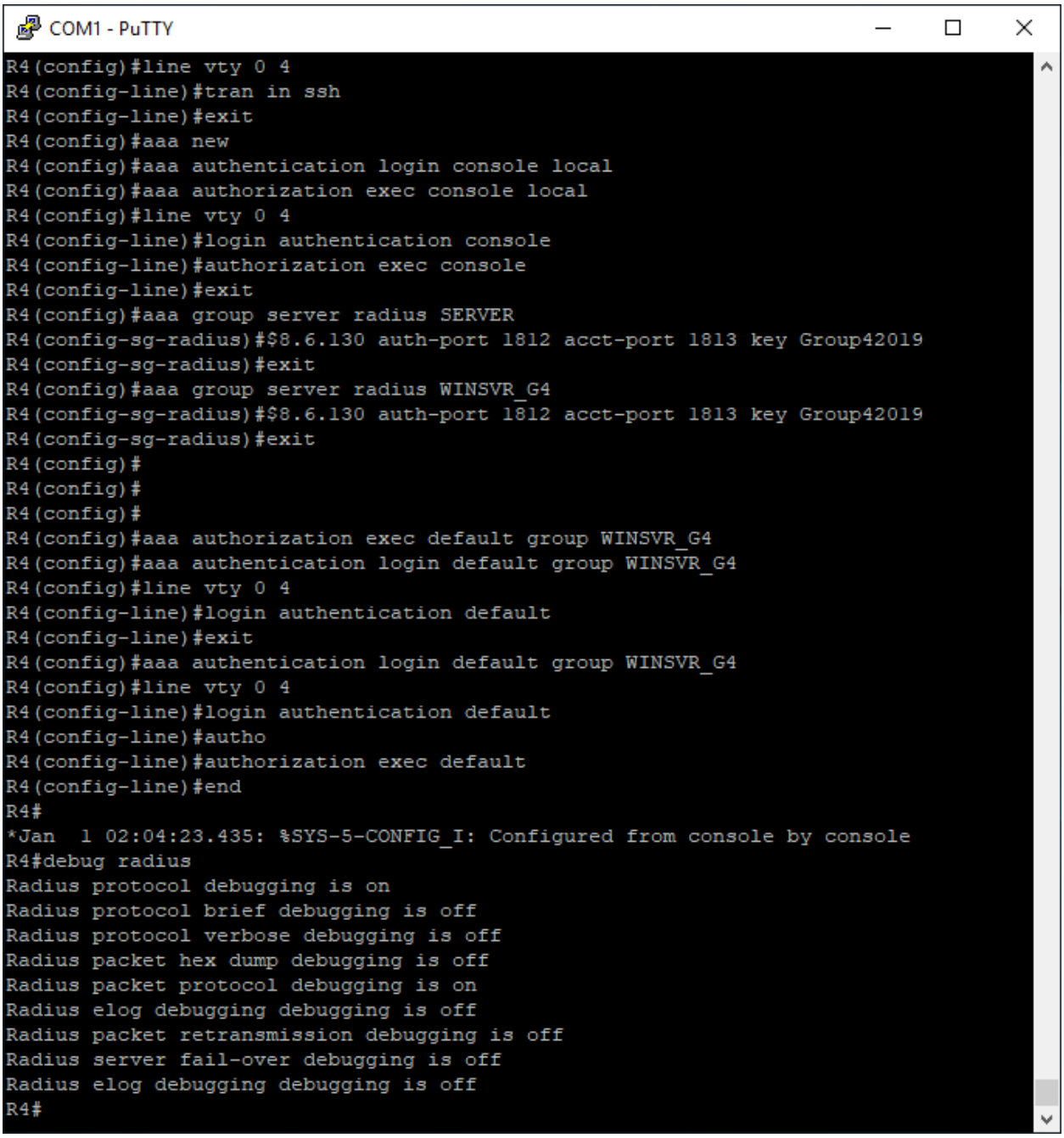


Figure 177 AAA new model with group server radius

Step 5: After finish all configuration authentication and authorization. Create line console 0 and login authentication console.

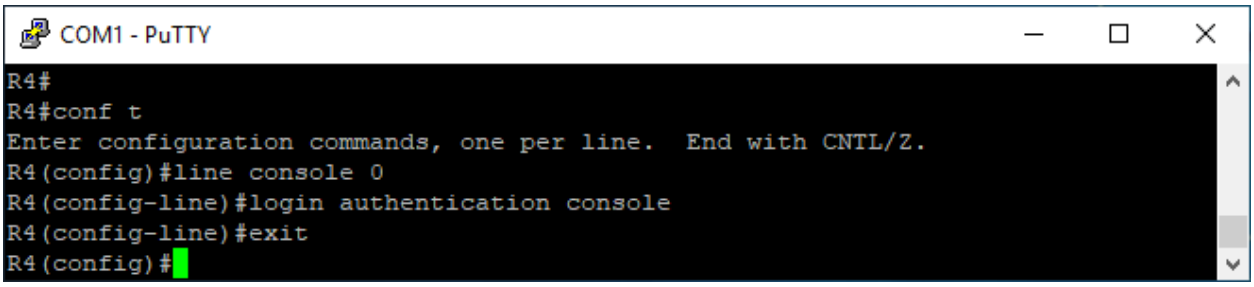


Figure 178 Login Authentication console

5.3.12 Secure FTP

5.3.12.1 Configuration of File Transfer Protocol (FTP)

Step 1: It is advisable to run this before installing any package and necessary to run it to install the latest updates version for Ubuntu 18.04 version.

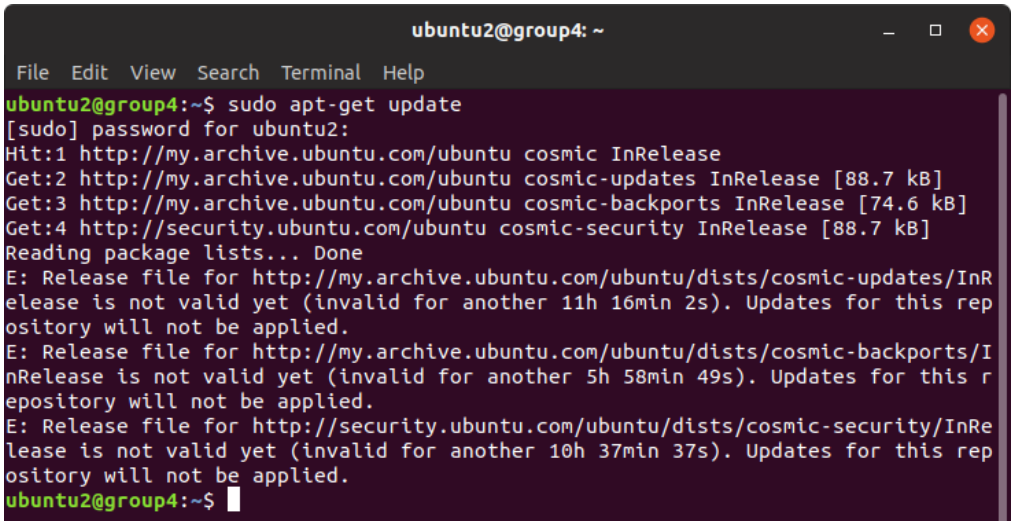


Figure 179 Update version for Ubuntu

Step 2: Installing vsftpd

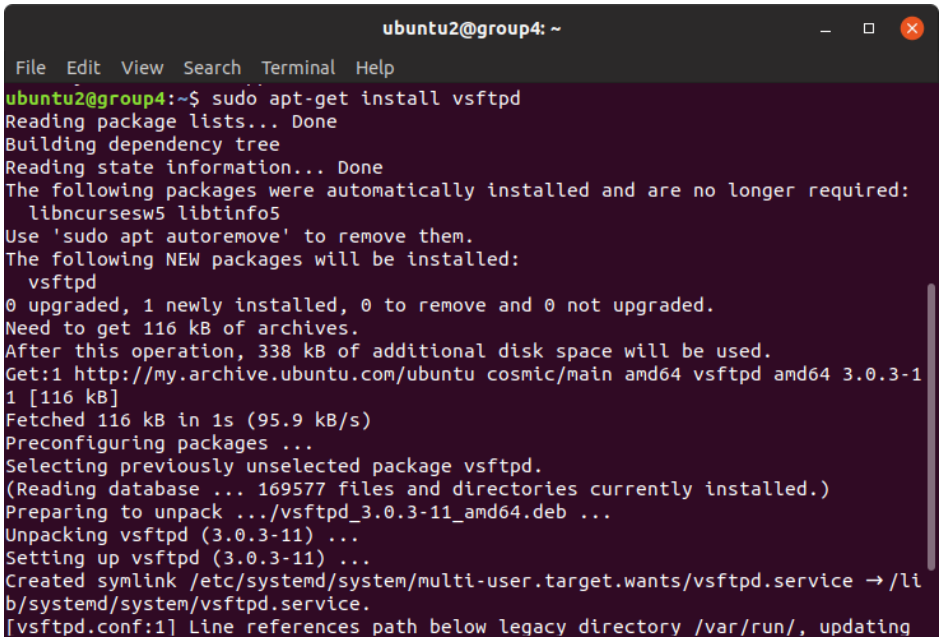


Figure 180 Install the vsftpd

Step 3: When the installation is complete, it copy the configuration file so it can start with a blank configuration, saving the original as a backup.

```
ubuntu2@group4:~$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig
```

Figure 181 Configuration file, save the original as a backup

Step 4: Opening the Firewall, It will check the firewall status to see if it's enabled. If so, it will ensure that FTP traffic is permitted so user won't run into firewall rules blocking user when it comes time to test.

```
ubuntu2@group4:~$ sudo apt-get install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-0ubuntu0.18.10.1).
ufw set to manually installed.
The following packages were automatically installed and are no longer required:
  libncursesw5 libtinfo5
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Figure 182 Install the firewall

```
ubuntu2@group4:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

Figure 183 Enable the firewall

Step 5: Opening and check the Firewall

```
ubuntu2@group4:~$ sudo ufw status
Status: active
```

Figure 184 Check status the firewall

Step 6: It may have other rules in place or no firewall rules at all. Since only ssh traffic is permitted in this case and it need to add rules for FTP traffic.

```
ubuntu2@group4:~$ sudo ufw enable
Firewall is active and enabled on system startup
ubuntu2@group4:~$ sudo ufw status
Status: active
ubuntu2@group4:~$ sudo ufw allow 20/tcp
Rule added
Rule added (v6)
ubuntu2@group4:~$ sudo ufw allow 21/tcp
Rule added
Rule added (v6)
ubuntu2@group4:~$ sudo ufw allow 990/tcp
Rule added
Rule added (v6)
ubuntu2@group4:~$ sudo ufw allow 40000:50000/tcp
Rule added
Rule added (v6)
```

Figure 185 Configuration protocol to allow

Step 7: Show output the firewall rules below figure like this.

```
ubuntu2@group4:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
20/tcp                     ALLOW       Anywhere
21/tcp                     ALLOW       Anywhere
990/tcp                    ALLOW       Anywhere
40000:50000/tcp            ALLOW       Anywhere
20/tcp (v6)                ALLOW       Anywhere (v6)
21/tcp (v6)                ALLOW       Anywhere (v6)
990/tcp (v6)               ALLOW       Anywhere (v6)
40000:50000/tcp (v6)       ALLOW       Anywhere (v6)
```

Figure 186 Check the status enable protocol

Step 8: Preparing the User Directory

Firstly, add a test user" arif".

```
ubuntu2@group4:~$ sudo adduser arif
Adding user `arif' ...
Adding new group `arif' (1002) ...
Adding new user `arif' (1002) with group `arif' ...
Creating home directory `/home/arif' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for arif
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
```

Figure 187 Create new user directory

Step 9: Create the ftp folder, set its ownership, and be sure to remove write permissions with the following commands.

```
ubuntu2@group4:~$ sudo mkdir /home/arif/ftp
ubuntu2@group4:~$ sudo chown nobody:nogroup /home/arif/ftp
ubuntu2@group4:~$ sudo chmod a-w /home/arif/ftp
```

Figure 188 Create ftp folder and set folder 3 permissions

Step 10: Let's verify the permissions.

```
ubuntu2@group4:~$ sudo ls -la /home/arif/ftp
total 8
dr-xr-xr-x 2 nobody nogroup 4096 Apr   9 10:13 .
drwxr-xr-x 3 arif   arif    4096 Apr   9 10:13 ..
```

Figure 189 Show and check the permissions user folder

Step 11: Next, create the directory where files can be uploaded and assign ownership to the user.

```
ubuntu2@group4:~$ sudo mkdir /home/arif/ftp/files
ubuntu2@group4:~$ sudo chown arif:arif /home/arif/ftp/files
```

Figure 190 Create the directory files can be upload and assign ownership

Step 12: A permissions check on the files directory should return the following.

```
ubuntu2@group4:~$ sudo ls -la /home/arif/ftp
total 12
dr-xr-xr-x 3 nobody nogroup 4096 Apr   9 10:16 .
drwxr-xr-x 3 arif   arif    4096 Apr   9 10:13 ..
drwxr-xr-x 2 arif   arif    4096 Apr   9 10:16 files
```

Figure 191 Show and check the permissions user folder

Step 13: Finally, add a test.txt file to use when it test later on.

```
ubuntu2@group4:~$ echo "vsftpd test file" | sudo tee /home/arif/ftp/files/test.txt
vsftpd test file
```

Figure 192 Add a test.txt file at in user folder directory

Step 14: Configuring FTP Access. The two key settings for this are already set in vsftpd.conf. Start by opening the config file to verify that the settings in this configuration match those below.

```
ubuntu2@group4:~$ sudo nano /etc/vsftpd.conf
```

Figure 193 Configuration the vsftpd.conf

Result output of text vsftpd.conf

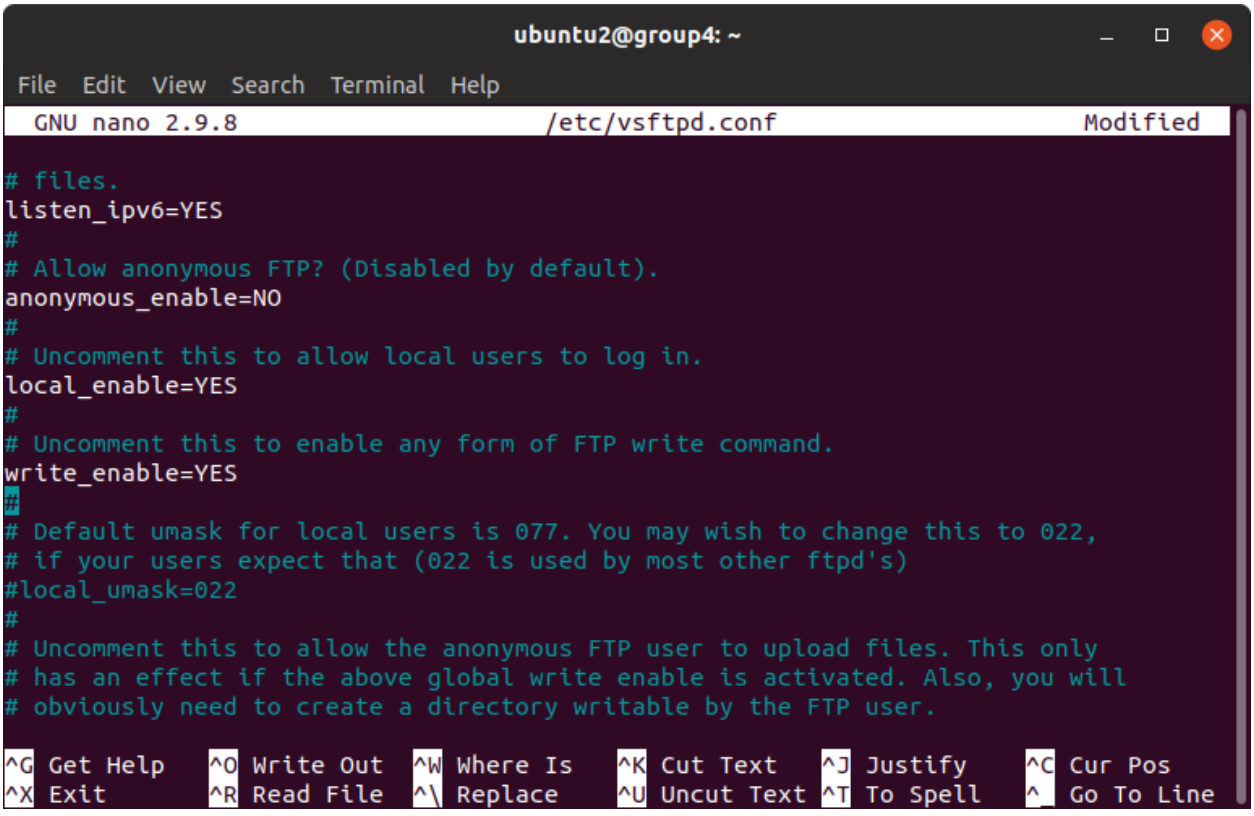


Figure 194 Open the file vsftpd.conf

Step 15: Next it need to change some values in the fil e. In order to allow the user to upload files and it uncomment the write enable setting this file conf.

```
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
```

Figure 195 Uncomment the write_enable=YES

Step 16: It also uncomment the chroot to prevent the FTP-connected user from accessing any files or commands outside the directory tree.

```
# chroot_list_enable below.
chroot_local_user=YES
#
```

Figure 196 Uncomment the chroot_local_user=YES

Step 17: To add a user_sub_token in order to insert the username in our local_root directory path so our configuration are work for this user and any future users that might be added.

```
user_sub_token=$USER
local_root=/home/$USER/ftp
```

Figure 197 Add the user_sub_token and local_root = directory path folder

Step 18: It is limit the range of ports that can be used for passive FTP to make sure enough connections are available.

```
pasv_min_port=40000
pasv_max_port=50000
```

Figure 198 Add the pasv_min_port and pasv_max_port

Step 19: Since the user are only planning to allow FTP access on a case-by-case basis, it will to set up the configuration so that access is given to a user only when users are explicitly added to a list rather than by default.

userlist_deny toggles the logic. When it is set to "YES", users on the list are denied FTP access. When it is set to "NO", only users on the list are allowed access. When it is done making the change, save and exit the file.

```
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
```

Figure 199 Add the userlist_enable, userlist_file and userlist_deny

Step 20: Finally, to create and add our user to the file. It is using the -a flag to append to file.

```
ubuntu2@group4:~$ echo "arif" | sudo tee -a /etc/vsftpd.userlist
arif
```

Figure 200 Create and add our user to the file

Step 21: Double-check that it was added as it expected.

```
ubuntu2@group4:~$ cat /etc/vsftpd.userlist
arif
```

Figure 201 Double check vsftpd.userlist

Step 22: Testing FTP Access.

Anonymous users should fail to connect: It disabled anonymous access. Here it will test that by trying to connect anonymously. If it have done it properly, anonymous users should be denied permission.

```
ubuntu2@group4:~$ ftp -p localhost
```

Figure 202 Test the FTP with localhost

It have configured the server to allow only the user “arif” to connect via FTP. Let's make sure that's the case.

```
ubuntu2@group4:~$ ftp -p localhost
Connected to localhost.
220 Welcome to group4 FTP service.
Name (localhost:ubuntu2): arif
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Figure 203 Enter the name and password in FTP

Close the connection.

```
ftp> bye
221 Goodbye.
```

Figure 204 Close the connection

5.3.12.2 Configuration of Secure FTP (SFTP)

Step 1: Update again and run it to install the latest updates version for Ubuntu 18.04 version.

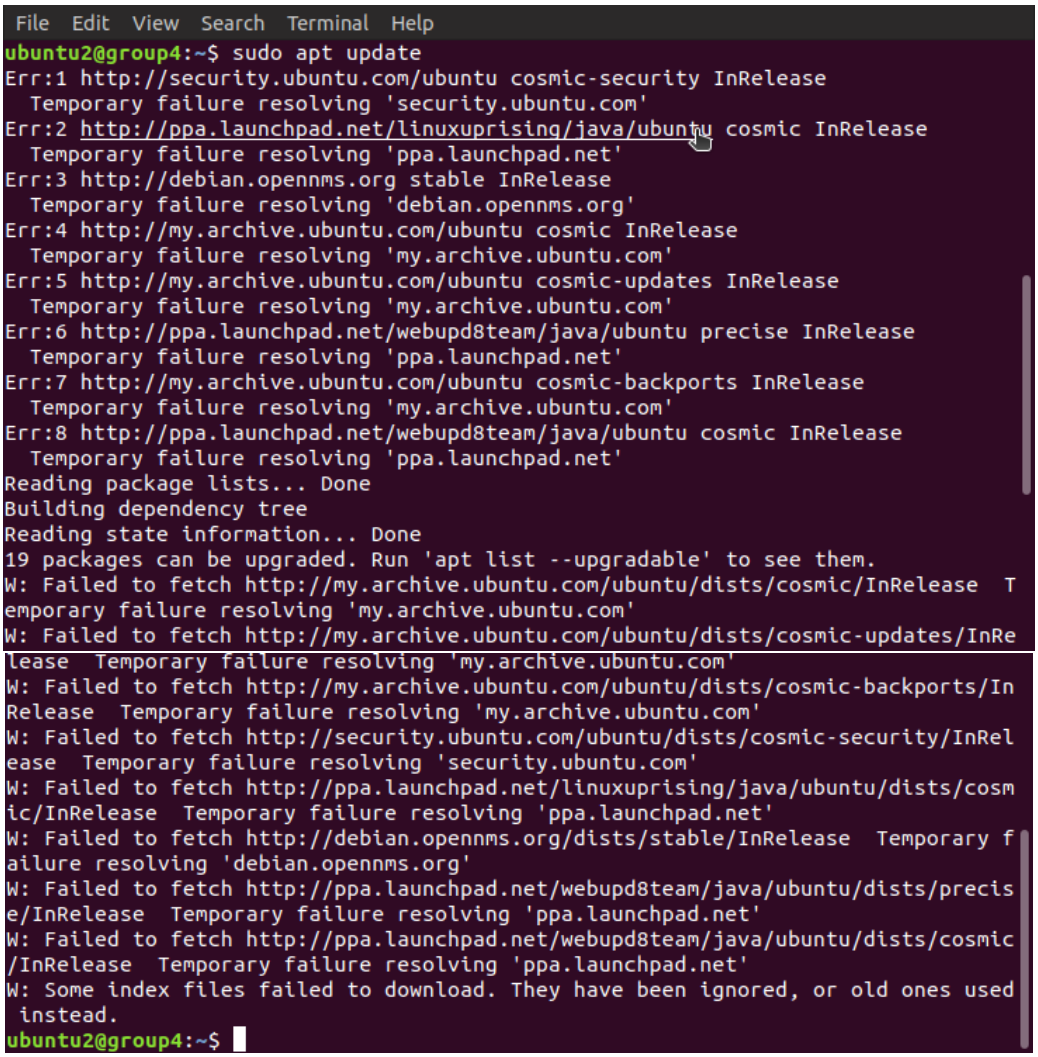


Figure 205 Update the version for Ubuntu

Step 2: Install Open SSH Server

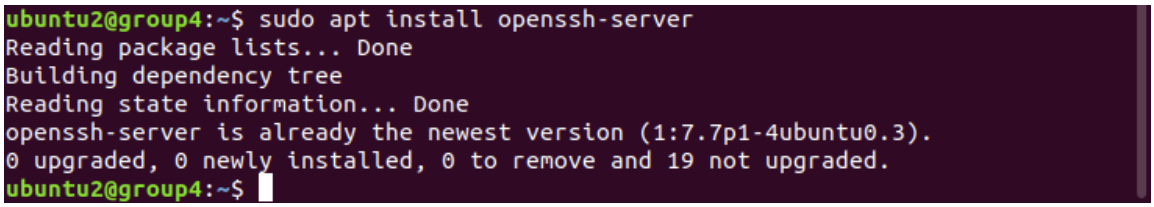


Figure 206 Install the openssh-server

Step 3: After installing, the commands below can be used to stop, start and enable the service to always start up when the server boots.

```
ubuntu2@group4:~$ sudo systemctl stop ssh.service
ubuntu2@group4:~$ sudo systemctl start ssh.service
ubuntu2@group4:~$ sudo systemctl enable ssh.service
Synchronizing state of ssh.service with SysV service script with /lib/systemd/sy
stemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
```

Figure 207 Configure the systemctl stop, start and enable the ssh.service

Step 4: Show status ssh service, ssh is Active and running process.

```
File  Edit  View  Search  Terminal  Help
ubuntu2@group4:~$ service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Tue 2019-05-28 15:39:20 +08; 6min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 12032 (sshd)
    Tasks: 1 (limit: 4915)
   Memory: 2.4M
   CGroup: /system.slice/ssh.service
           └─12032 /usr/sbin/sshd -D

Mei 28 15:39:20 group4 systemd[1]: Starting OpenBSD Secure Shell server...
Mei 28 15:39:20 group4 sshd[12032]: Server listening on 0.0.0.0 port 22.
Mei 28 15:39:20 group4 sshd[12032]: Server listening on :: port 22.
Mei 28 15:39:20 group4 systemd[1]: Started OpenBSD Secure Shell server.
Mei 28 15:40:50 group4 sshd[12237]: Connection closed by 192.168.6.138 port 4734
Mei 28 15:45:50 group4 sshd[12639]: Connection closed by 192.168.6.138 port 4740
lines 1-17/17 (END)
```

Figure 208 Show status ssh service active

Step 5: Configure SFTP

Now that OpenSSH Server is installed, open its default configuration file by running the commands below.

```
ubuntu2@group4:~$ sudo nano /etc/ssh/sshd_config
```

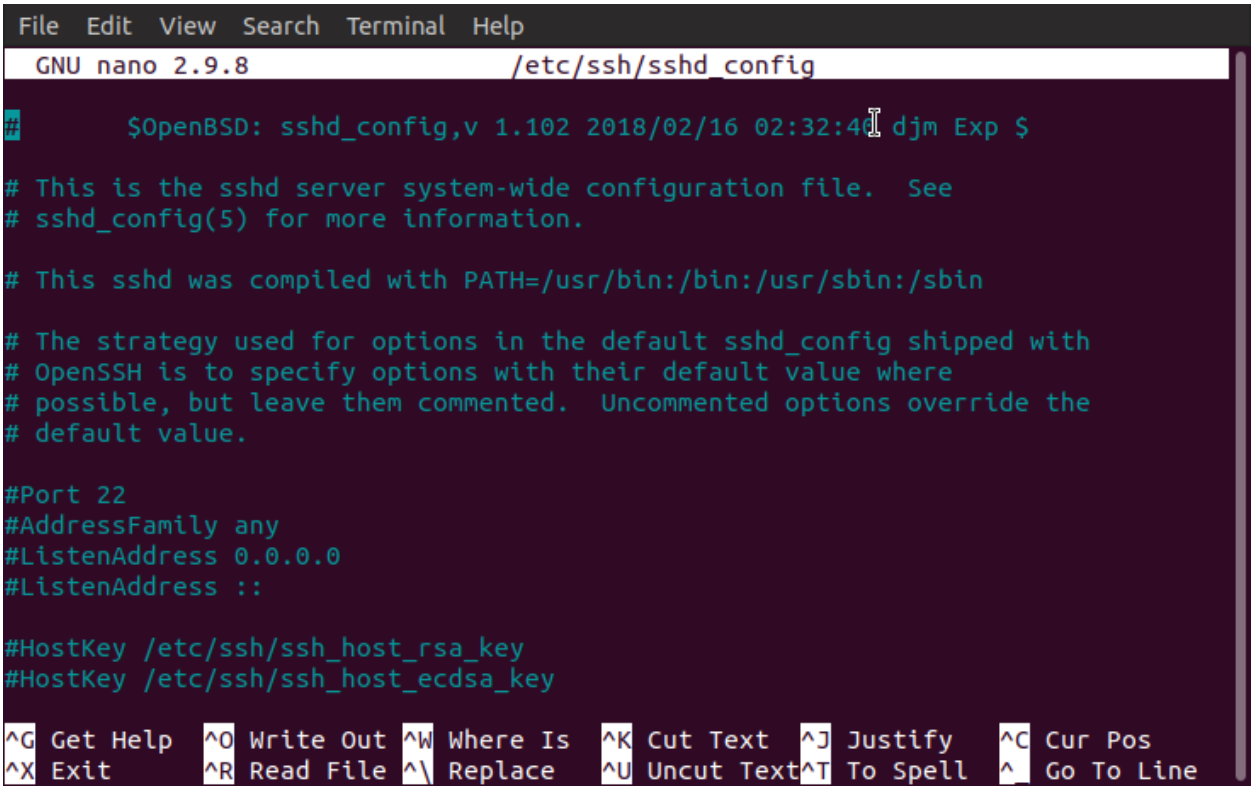


Figure 209 Open the sshd_config file

Step 6: Then edit the file and change highlighted line below… add the # before the first line, then add the highlighted line just below it to enable SFTP…. This will change the subsystem to internal-sftp only.

```
# override default of no subsystems
#Subsystem      sftp    /usr/lib/openssh/sftp-server
Subsystem sftp internal-sftp

#
```

Figure 210 Uncomment the Subsystem sftp internal-sftp

Step 7: Next, add the lines below at the end of the file or just below the highlighted line above

```
#
# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
Match Group sftp_users
X11Forwarding no
AllowTcpForwarding no
ChrootDirectory /home
ForceCommand internal-sftp
```

Figure 211 Add the information about ssh in sshd_config

Step 8: Create SFTP Group

```
ubuntu2@group4:~$ sudo groupadd sftp_users
groupadd: group 'sftp_users' already exists
```

Figure 212 Create sftp group

Step 9: Now add any user to the group by running the commands.

```
ubuntu2@group4:~$ sudo usermod -aG sftp_users fikri
```

Figure 213 Add the group by running with user directory

5.3.13 Linux Mail Server

5.3.13.1 Installing and configuring Postfix

On Windows Server run the following commands

1. Open on domain name system manager on Windows Server, then head to group4.com option under forward lookup zone

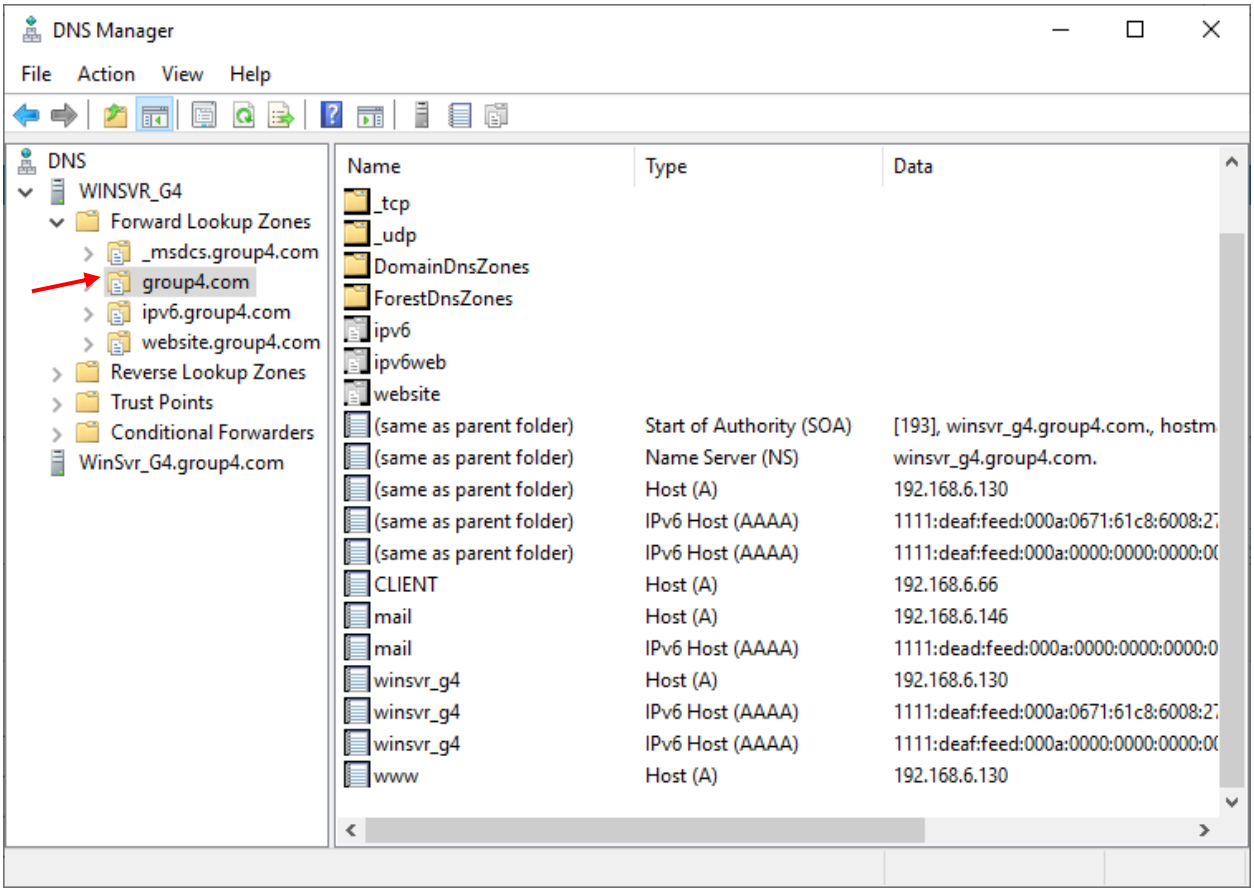


Figure 214 Domain Manager

2. Right click on group4.com option and choose new host then configure as picture below.

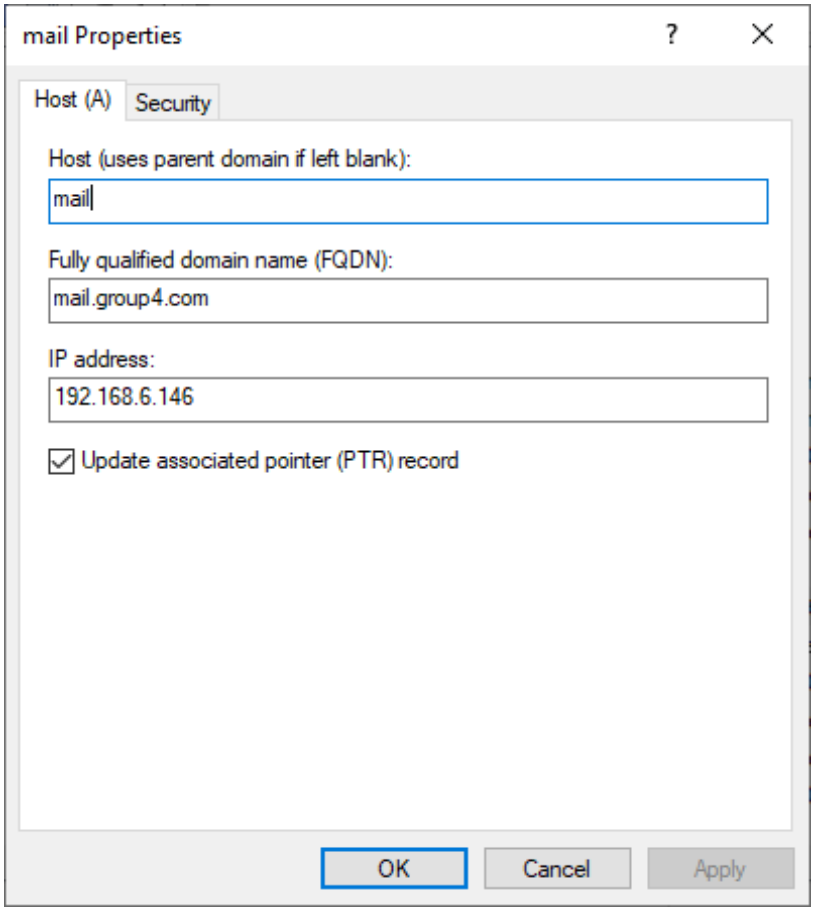


Figure 215 Set Host

3. Now go to Debian, open terminal and enter the following command to get into root and perform an update for system

```
su -
Group42019
apt update
```

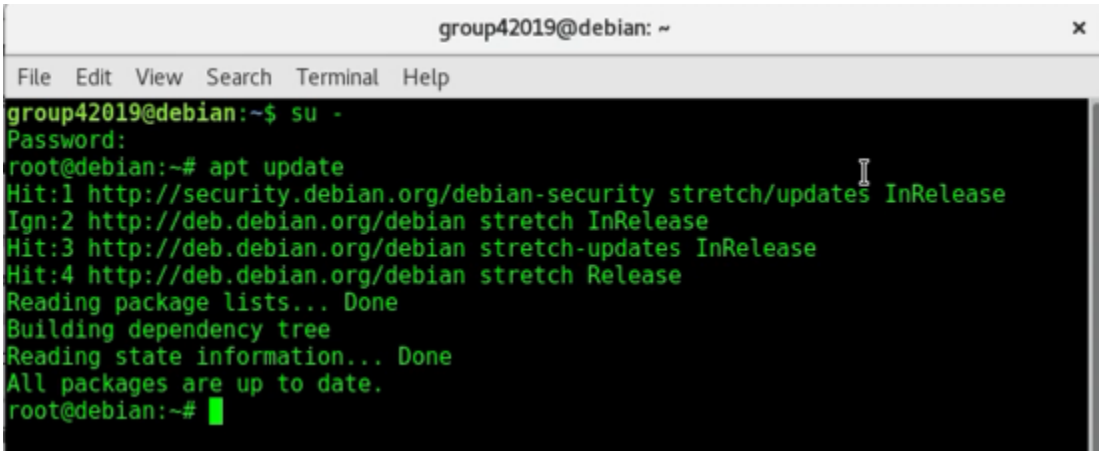


Figure 216 System update

4. Install **Postfix**

```
apt-get install postfix courier-imap
y
```

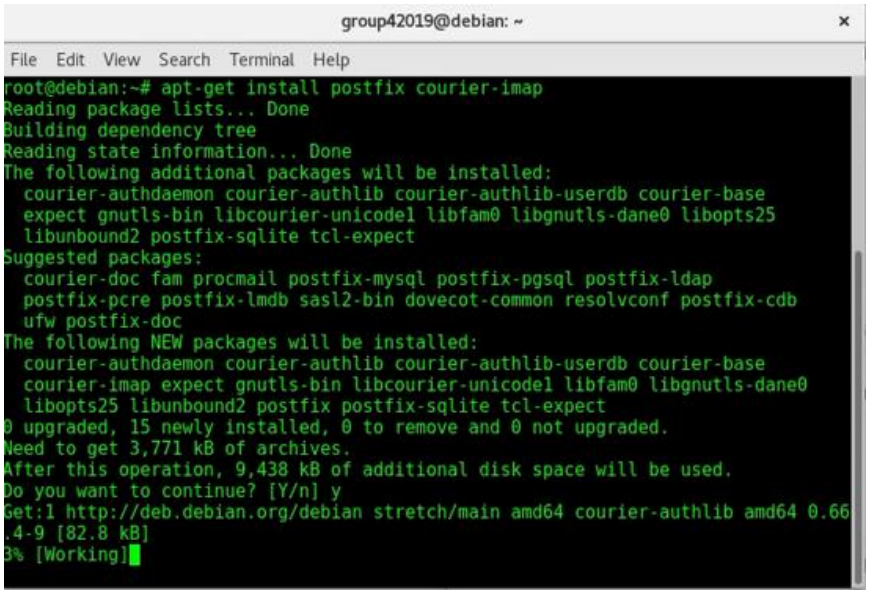


Figure 217 Installing Postfix

5. Configuring courier base as below

Step 1 : Click yes

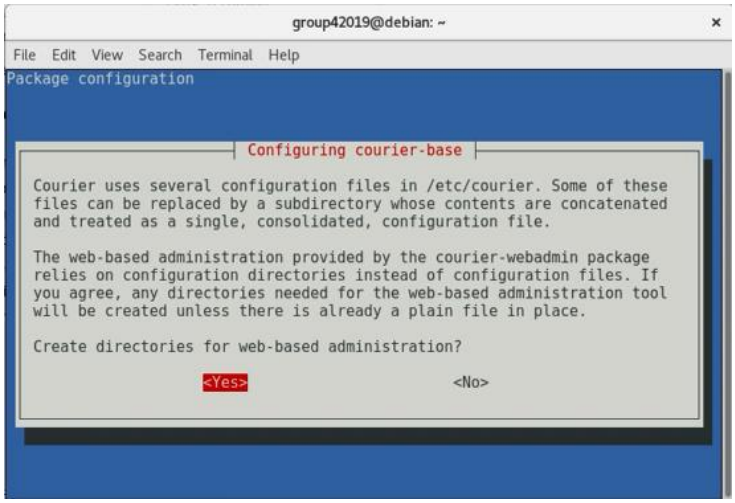


Figure 218 Directories Web Based

Step 2 : Click ok

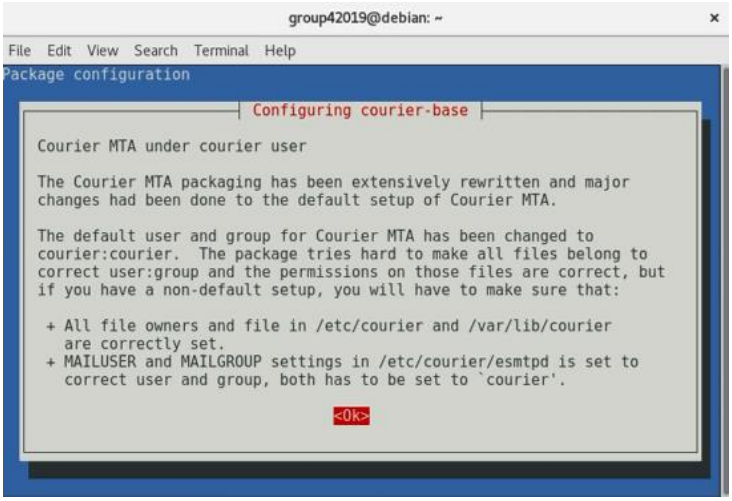


Figure 219 Directories Web Based II

Step 3: Click ok

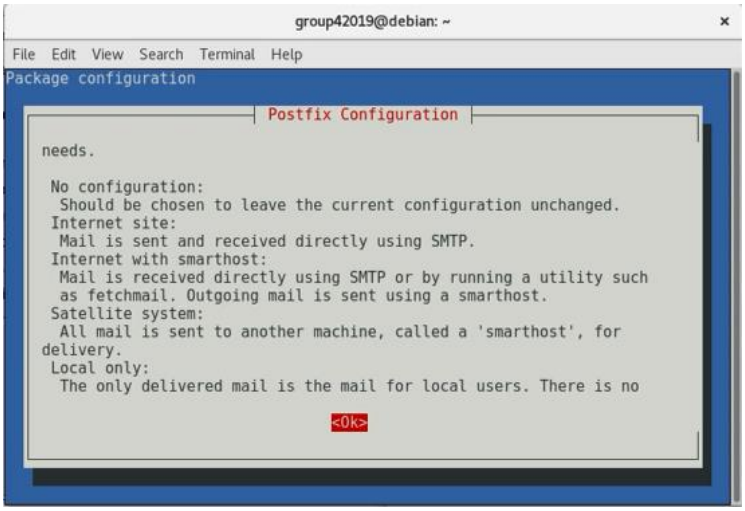


Figure 220 Directories Web Based III

Step 4 : During installation, you will be asked to **choose** the type **of mail configuration**, choose **"Internet Site".**

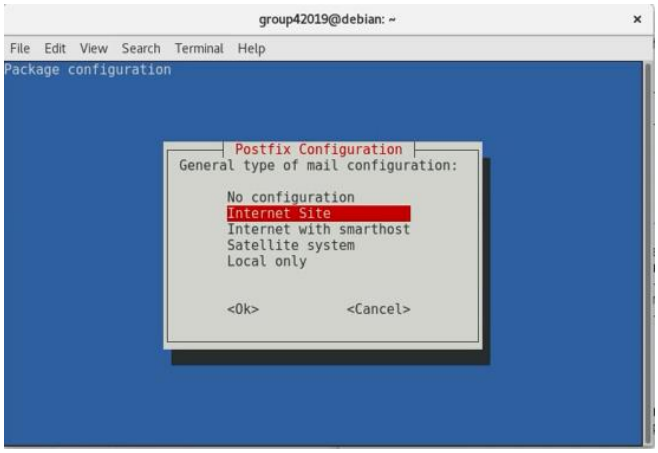


Figure 221 Directories Web Based IV

Step 5 : Enter system mail name then click ok

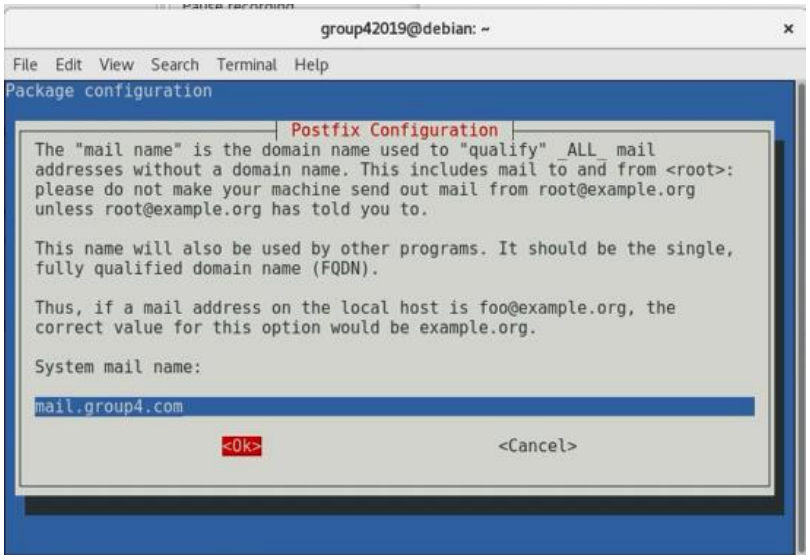


Figure 222 System mail name

6. Install **apache2** and **php**

```
apt install apache2 php7.0 libapache2-mod-php7.0
```

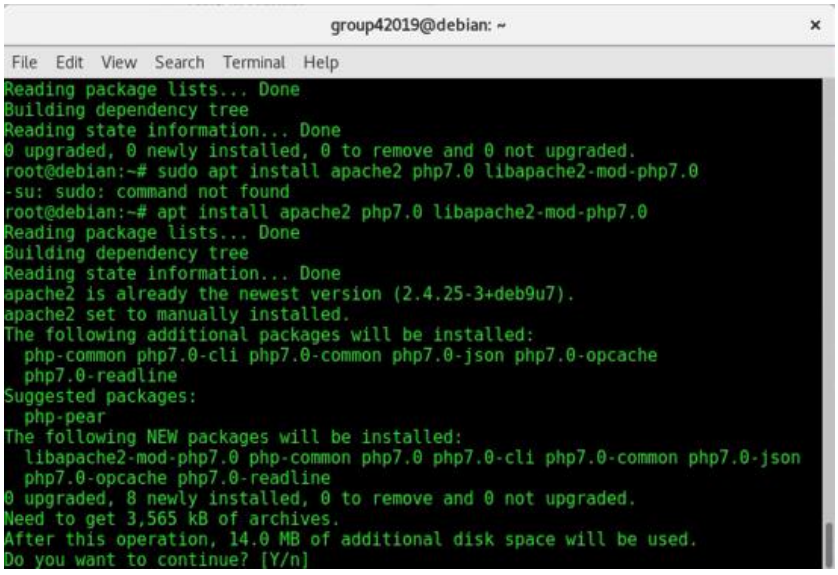


Figure 223 Installation apache2 and php

7. Checking **apache2** and **php** version

```
apache2 -v
php -v
```

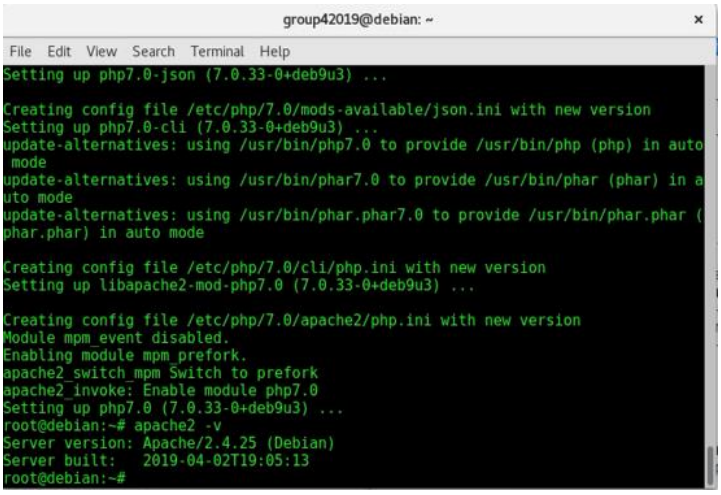


Figure 224 Checking version apache2 and php

8. Now, create the security part in between communication Postfix (SMTP) and Dovecot (IMAP) where use the Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) (TLS, formerly called SSL) provides certificate-based authentication and encrypted sessions. An encrypted session protects the information that is transmitted with SMTP mail or with SASL authentication and for IMAP security. This is the installation:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/group4.key -out /etc/ssl/certs/group4.pem
```

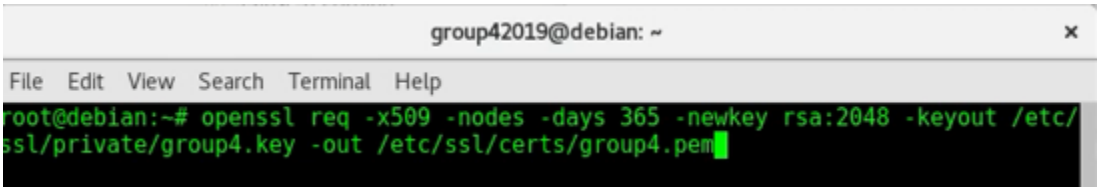


Figure 225 Command to create SSL certificate

9. It will request, to enter the following information.

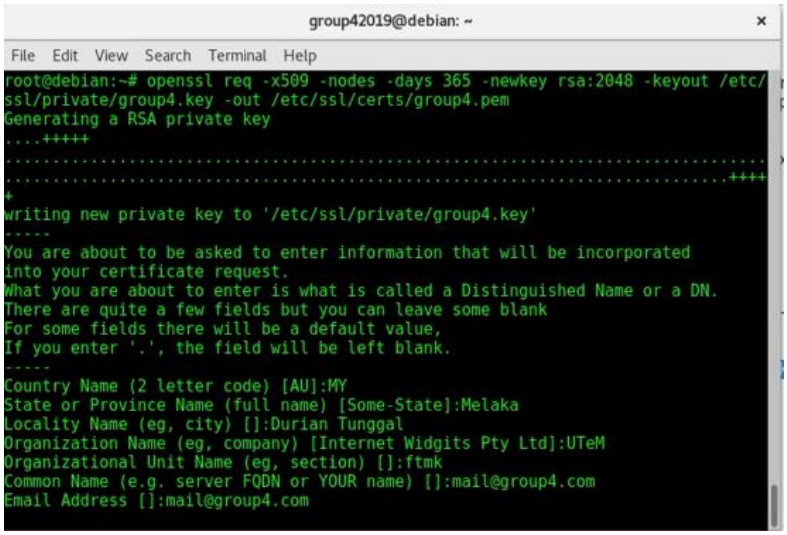


Figure 226 Set Information

10. To send emails from a desktop email client, enable the submission service of Postfix so that the email client can submit emails to Postfix SMTP server. Edit the master.cf file.

```
nano /etc/postfix/master.cf
```

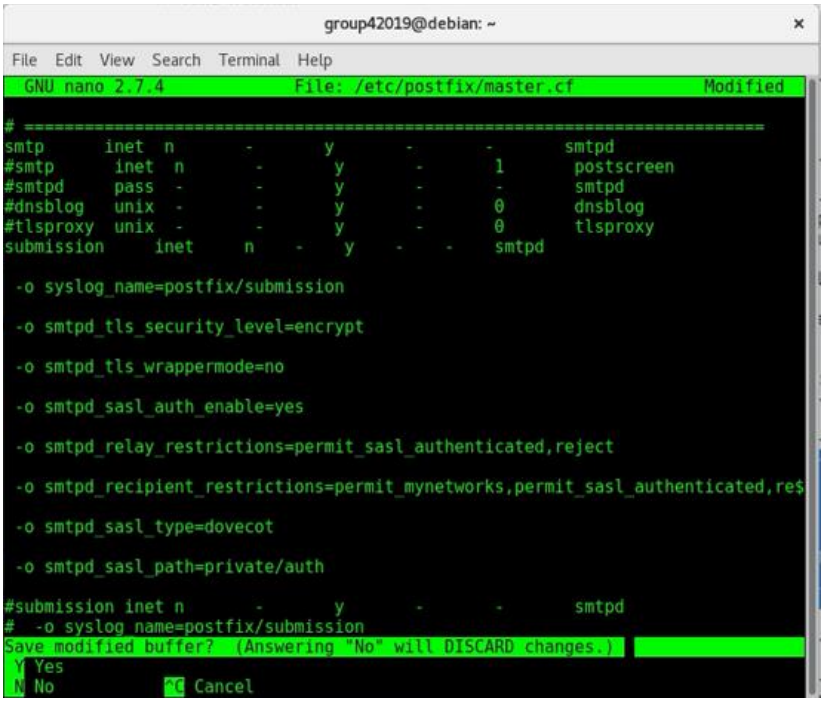


Figure 227 Edit master.cf

11. Save and close the file. Next, let Postfix know where TLS certificate and private key are. Edit main.cf file.

```
nano /etc/postfix/main.cf
```

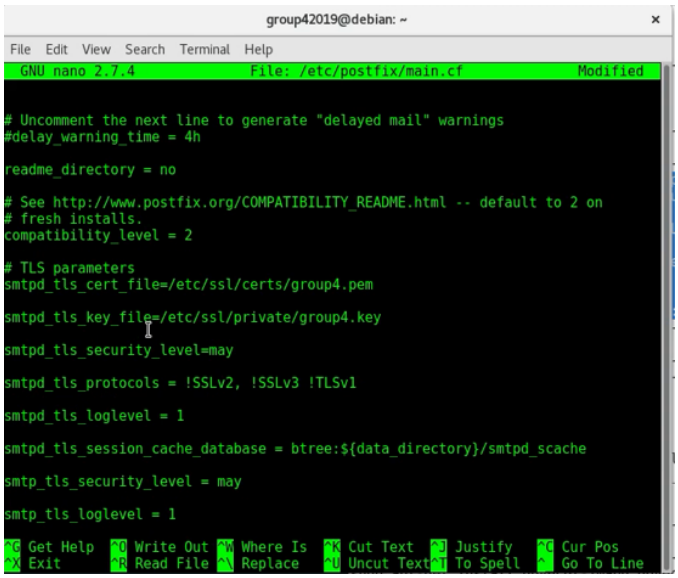


Figure 228 Edit main.cf

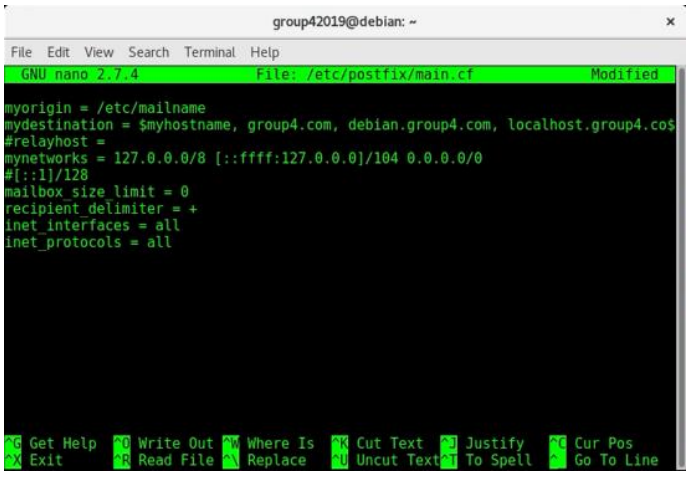


Figure 229 Edit main.cf

11. Restart postfix.

```
/etc/init.d/postfix restart
```

5.3.13.2 Installing and configuring Dovecot IMAP Server

- **Installing Dovecot**

Enter the following command to install Dovecot core package and the IMAP package on Ubuntu server.

1. Install the Dovecot service.

```
apt-get install dovecot-core dovecot-imapd
```

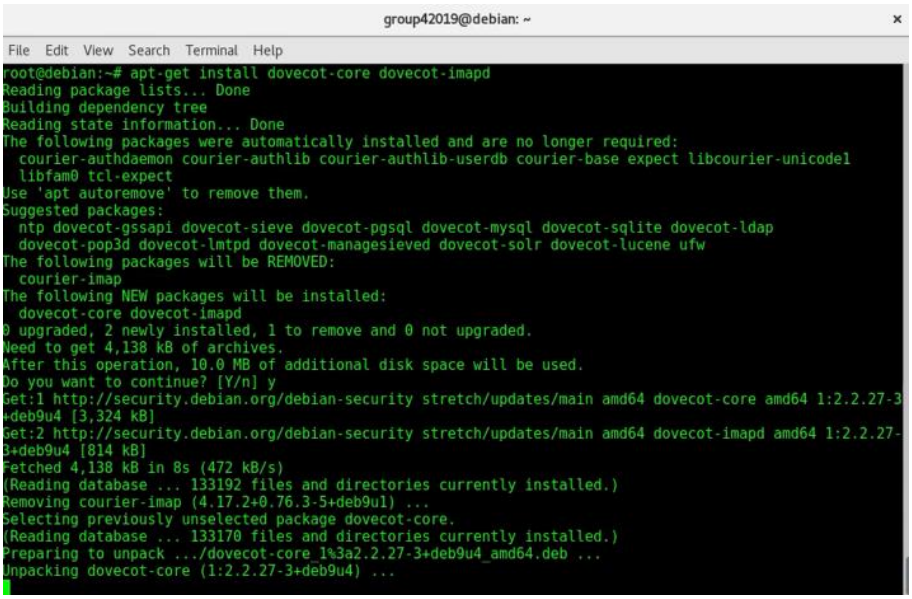


Figure 230 Installing Devecot

- **Configuring Dovecot**

2. First, edit main configuration file.

```
nano /etc/dovecot/dovecot.conf
```

3. Add the following line to enable IMAP protocol.

```
protocols = imap
```

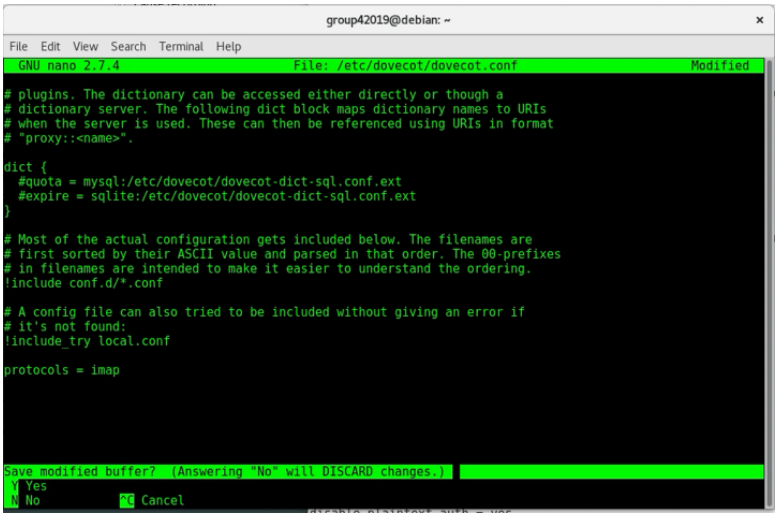


Figure 231 Edit dovecot.conf

- **Configuring Mailbox Location**

4. By default, Postfix uses mbox format to store emails. Each user's emails is stored in a single file /var/mail/username. Run the following command to find the mail spool directory.

postconf mail_spool_directory

Sample output:

mail_spool_directory = /var/mail

5. The config file for mailbox location is /etc/dovecot/conf.d/10-mail.conf.

```
nano  /etc/dovecot/conf.d/10-mail.conf
```

The default configuration is as follows, which is fine for a small email server.

mail_location = mbox:~/mail:INBOX=/var/mail/%u

6. Add the following line in the file.

mail_privileged_group = mail

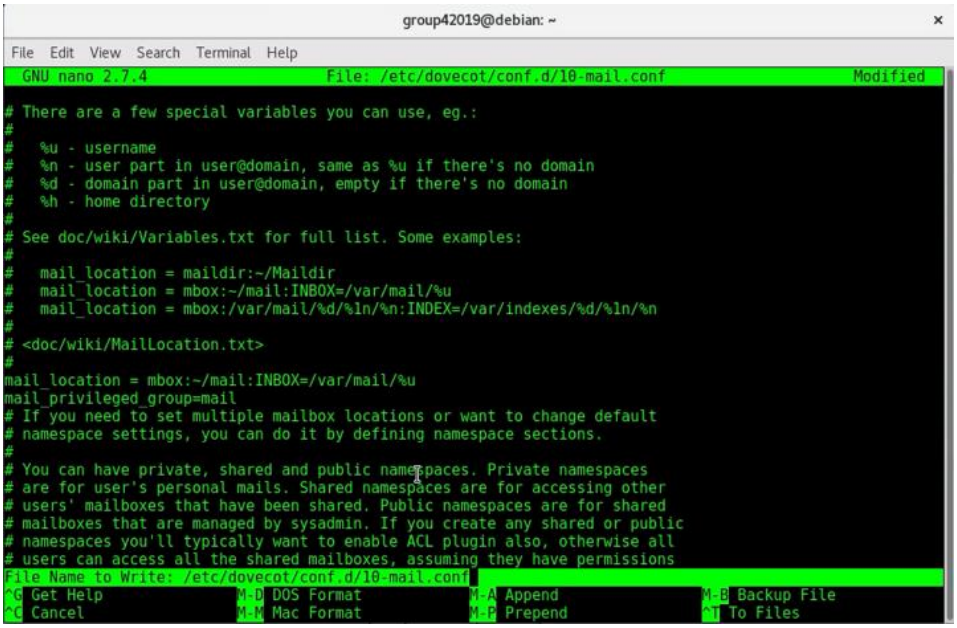


Figure 232 Edit 10-mail.conf

- **Configuring Authentication Mechanism**

8. Edit the authentication configuration file.

```
nano /etc/dovecot/conf.d/10-auth.conf
```

9. Uncomment the following line.

disable_plaintext_auth = yes

10. It will disable plaintext authentication when there is no SSL/TLS encryption. If want to use full email address (username@domain.com) to login, add the following line in the file.

auth_username_format = %n

11. Set the two line to enable plain and login authentication mechanism.

auth_mechanisms = plain

auth_mechanisms = plain login

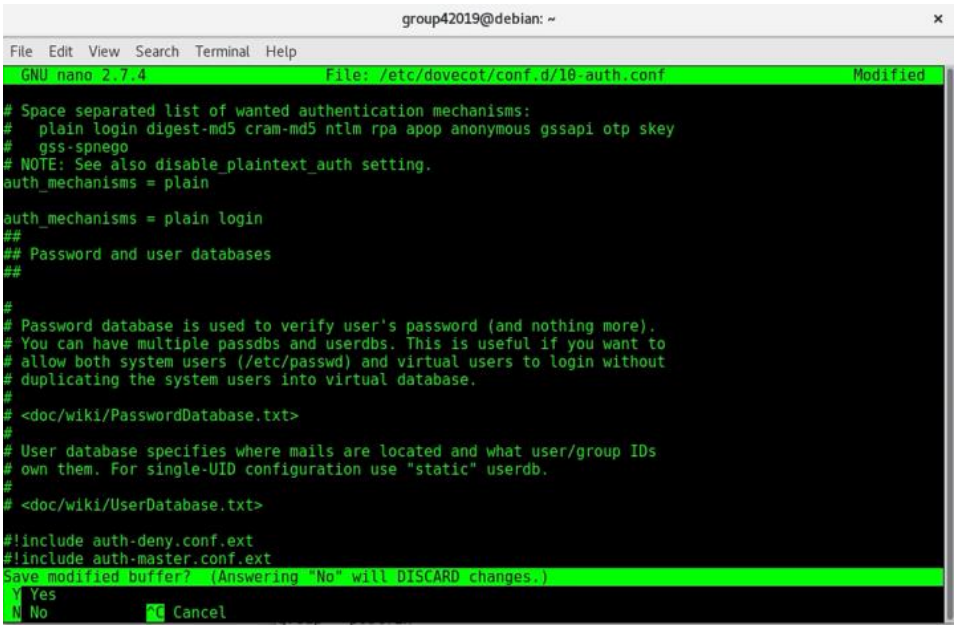


Figure 233 Edit 10-auth.conf

- **Configuring SSL/TLS Encryption**

12. Next, edit SSL/TLS configuration file. This configuration to make the communication betweensender (Postfix) and receiver (Dovecot) more secure with encrypted data transfer.

```
nano /etc/dovecot/conf.d/10-ssl.conf
```

13. Change ssl = no to ssl = required.

ssl = required

14. Then specify the location of ,r SSL/TLS cert and private key. Don’t leave out < character. It’s necessary.

ssl_cert = </etc/ssl/certs/group4.pem

ssl_key = </etc/ssl/private/group4.key

Then, save the file and exit

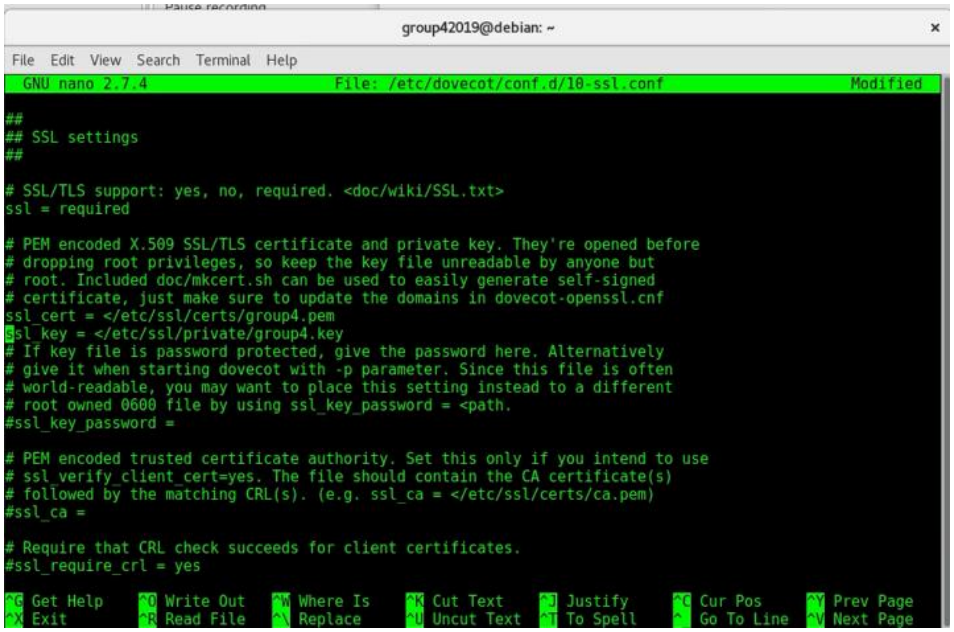


Figure 234 Edit 10-ssl.conf

SASL Authentication betweenPostfix and Dovecot

15. Edit the following file.

```
nano /etc/dovecot/conf.d/10-master.conf
```

Change service auth section to the following so that Postfix can find the Dovecot authentication server.

service auth {

unix_listener /var/spool/postfix/private/auth {

  mode = 8668

  user = postfix

  group = postfix

}

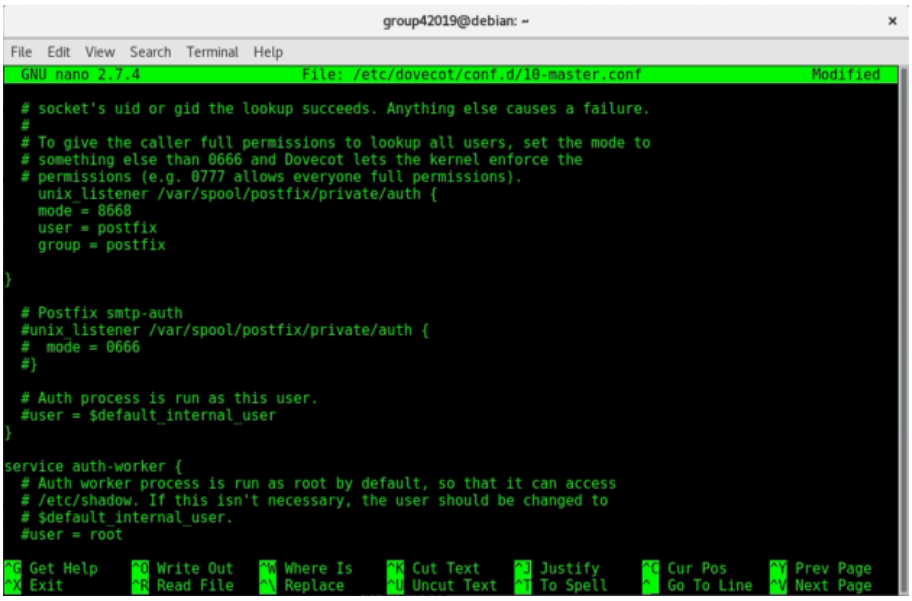


Figure 235 Edit 10-master.conf

16. Next, create includes: Drafts, Junk, Trash and Sent. These folders will be created at the user's home directory. Save and close all above configuration files, restart Dovecot.

sudo systemctl restart dovecot

Dovecot will be listening on port 143 (IMAP) and 993 (IMAPS). If there is a configuration error, dovecot will fail to restart. Restart Postfix to allow the login authentication mechanism.

sudo systemctl restart postfix

- **Installing Rainloop mail:**

Step 1: Download and Install RainLoop webmail

First, make a directory for rainloop in the current working directory.

```
mkdir rainloop
cd rainloop
```

Figure 236 Directory Rainloop

Step 2: Install Curl

```
apt-get install curl
```

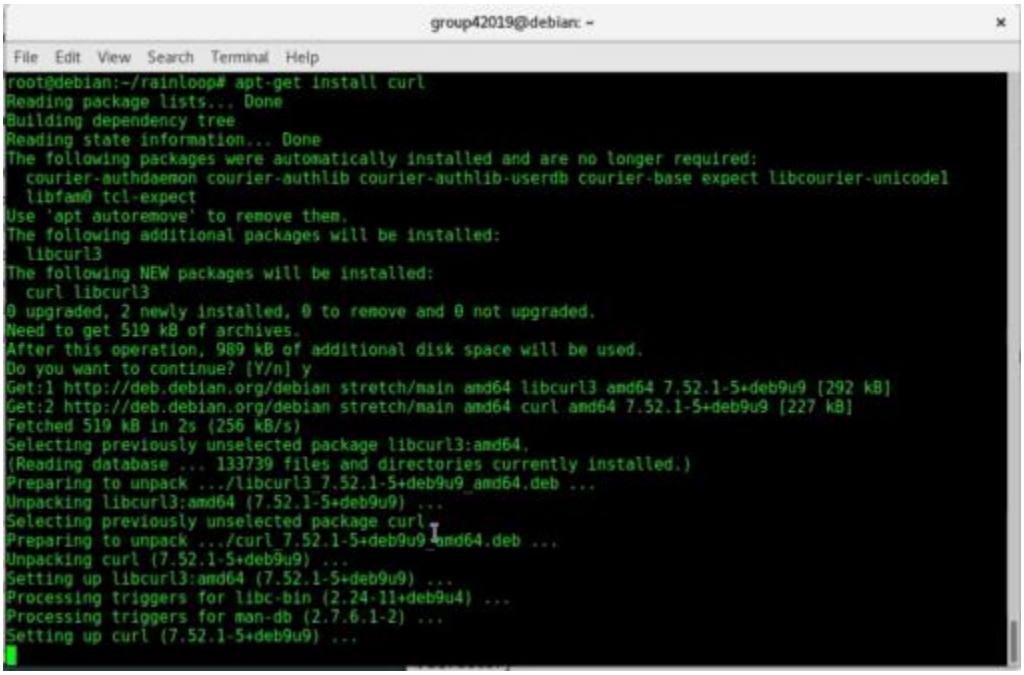


Figure 237 Install Curl

Step 3: Install Php-Curl

```
apt-get install php-curl
```

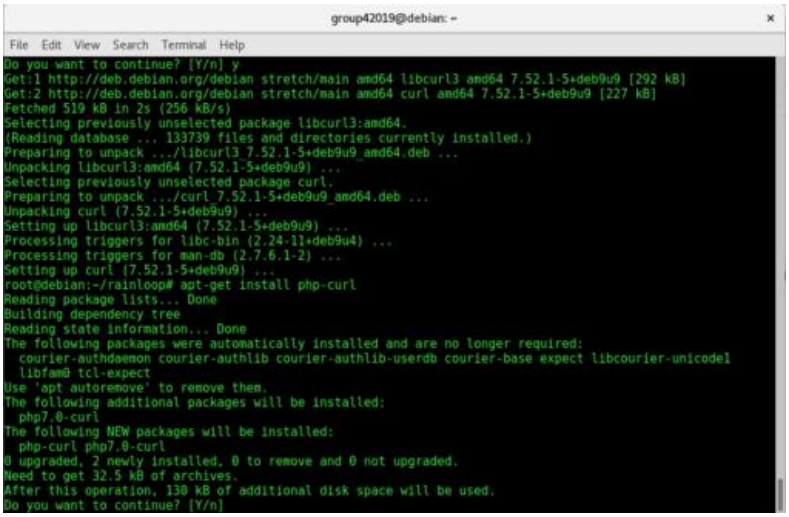


Figure 238 Install Php-Curl

Step 4: Install Php-Xml

```
apt-get install php-xml
```

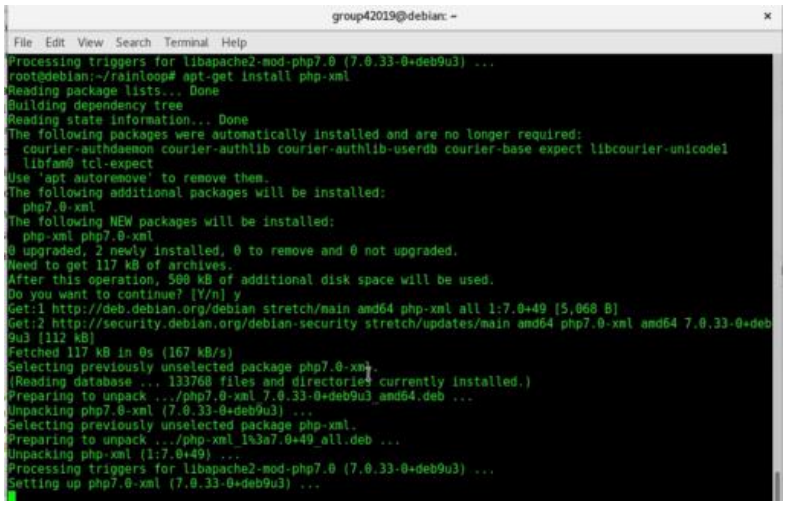


Figure 239 Install Php-Xml

Step 5: Download the latest RainLoop community edition with the following commands:

```
curl -s http://repository.rainloop.net/installer.php | php
```

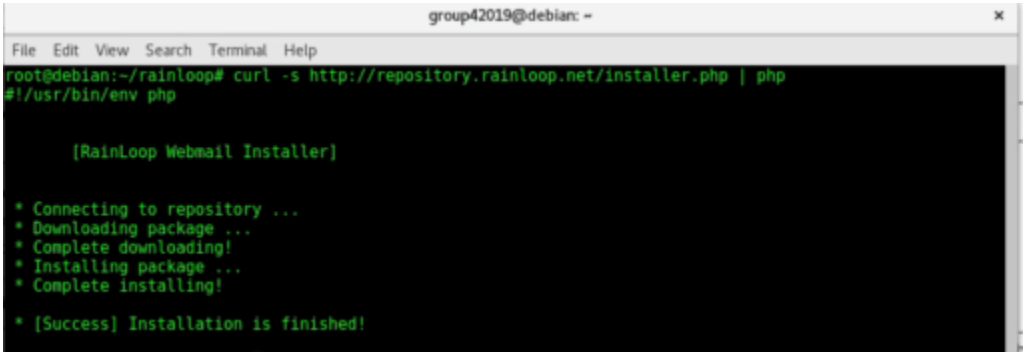


Figure 240 Download Rainloop

Step 6: Next, move this directory to /var/www/ and set web server user (www-data) as the owner.

```
mv rainloop /var/www/
chown www-data:www-data /var/www/rainloop/ -R
```

Figure 241 Move Directory

- **Configure a Virtual Host for RainLoop using Apache.**

Step 7: Create the virtual host file with the following command:

```
sudo nano /etc/apache2/sites-available/rainloop.conf
```

Put the following text into the file. Replace red text with ,r actual info

```
<VirtualHost *:80>
  ServerName mail.group4.com
  DocumentRoot "/var/www/rainloop/"
  ServerAdmin mailadmin@group4.com

  ErrorLog "/var/log/apache2/rainloop_error_log"
  TransferLog "/var/log/apache2/rainloop_access_log"

  <Directory />
    Options +Indexes +FollowSymLinks +ExecCGI
    AllowOverride All
    Order deny,allow
    Allow from all
    Require all granted
</Directory>

</VirtualHost>
```

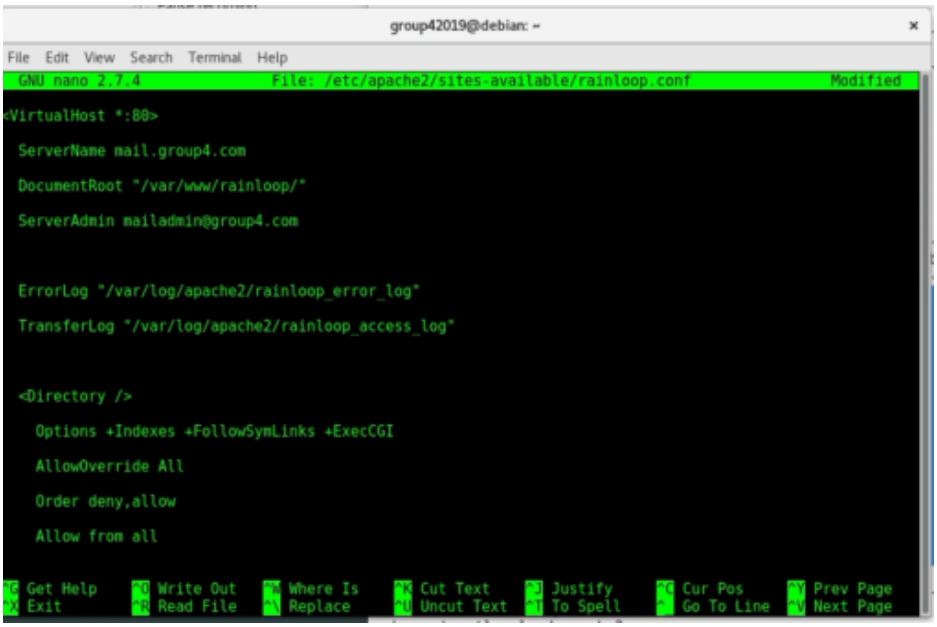


Figure 242 Virtual Host

Step 8. In order to start using it, you'll have to **create a new user** and **password** to do so, run.

```
Useradd megat
Passwd megat
Group42019
Group42019

Useradd haikal
Passwd haikal
Group42019
Group42019
```

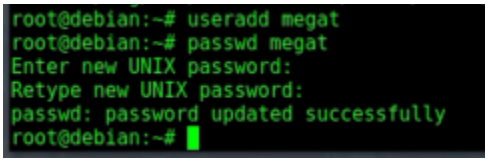


Figure 243 Create User Megat

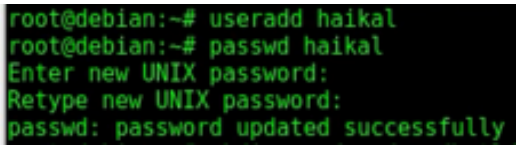


Figure 244 Create User haikal

Step 9 : **Create a home folder** for the **megat** in **/var/www/html/ megat** and make it **default** home directory.

```
mkdir -p /var/www/hmtl/megat
usermod -m -d /var/www/hmtl/megat

mkdir -p /var/www/hmtl/haikal
usermod -m -d /var/www/hmtl/haikal
```

Step 10: Give the "megat and haikal" the complete permissions on its home holder

```
chown -R megat:megat /var/www/hmtl/megat

chown -R haikal:haikal /var/www/hmtl/haikal
```

Step 11: Save and close the file. Then enable this virtual host. Then reload Apache

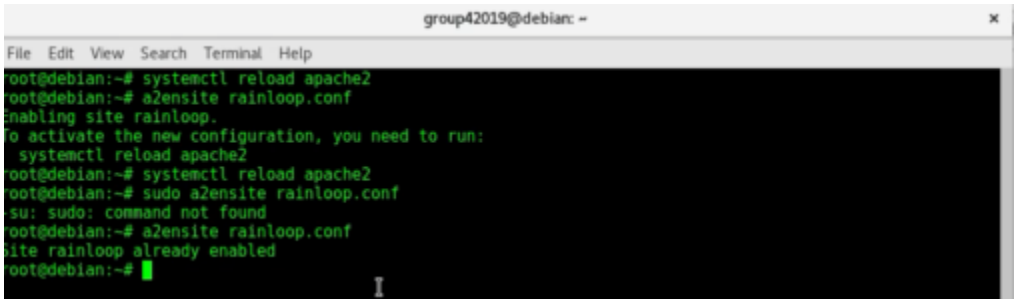


Figure 245 Enable Virtual Host

Step 12: The Rainloop mail now can access on browser, than go to browser enter mail.group4.com/?admin that has been set in /etc/apache2/sites-available/rainloop.conf. This login for admin configuration to make the Rainloop use the port for communication. On the domain set the following configuration on the figure below than click test. On the left menu, choose a domain menu and click on add domain.name **"group4.com"** .Use port 993 for IMAP and port 587 for SMTP. Click on test button and see if the IMAP and SMTP worked successfully by turning into green.

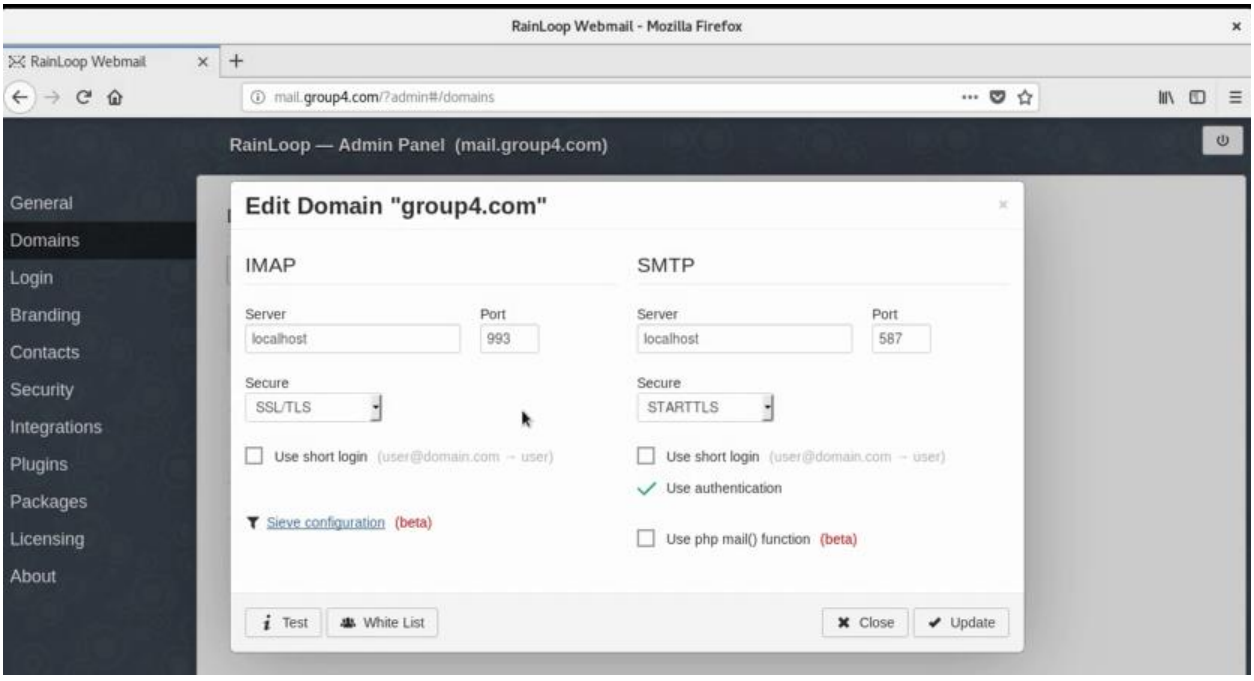


Figure 246 Go to browser enter mail.group4.com for admin

Step 13: Set Static IP for Debian

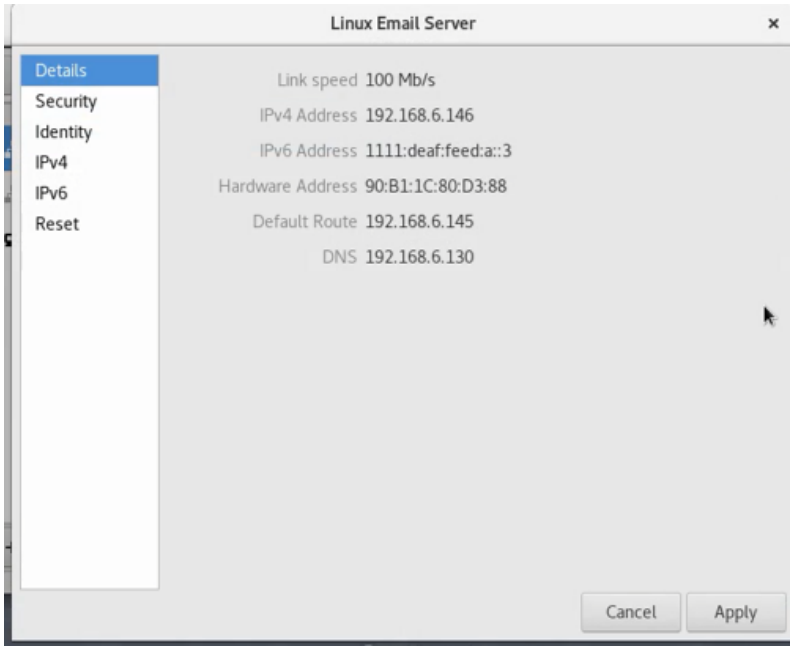


Figure 247 Static IP

Conclusion

Installation and configuration are important procedure to be done before testing the services. Installation of a program is the act of putting the program onto a computer system so that it can be executed. Because the requisite process varies for each program and each computer, many programs come with a general-purpose or dedicated installer (a specialized program which automates most of the work required for their installation). This stage must be done carefully to make sure the service can be run efficiently during the testing part. The installation guide will help get up and running in no time.

5.3.14 Network Management System

A set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network Management framework. A network Management System components assist with Network device discovery, identifying what devices are present on a network. Network device monitoring, monitoring at the device level to determine the health of network components and the extent to which their performance matches capacity plans and intra-enterprise service-level agreements (SLAs). Network performance analysis, tracking performance indicators such a bandwidth utilization, packet loss, latency, availability and uptime of routers, switches and other Simple Network Management Protocol (SNMP) –enabled devices. Intelligent notifications, configurable alerts that will respond to specific network scenarios by paging, emailing, calling or texting a network administrator.

5.3.14.1 Installation NMS

Step 1: Install postgresql by entering the following command

sudo apt-get install postgresql postgresql-contrib

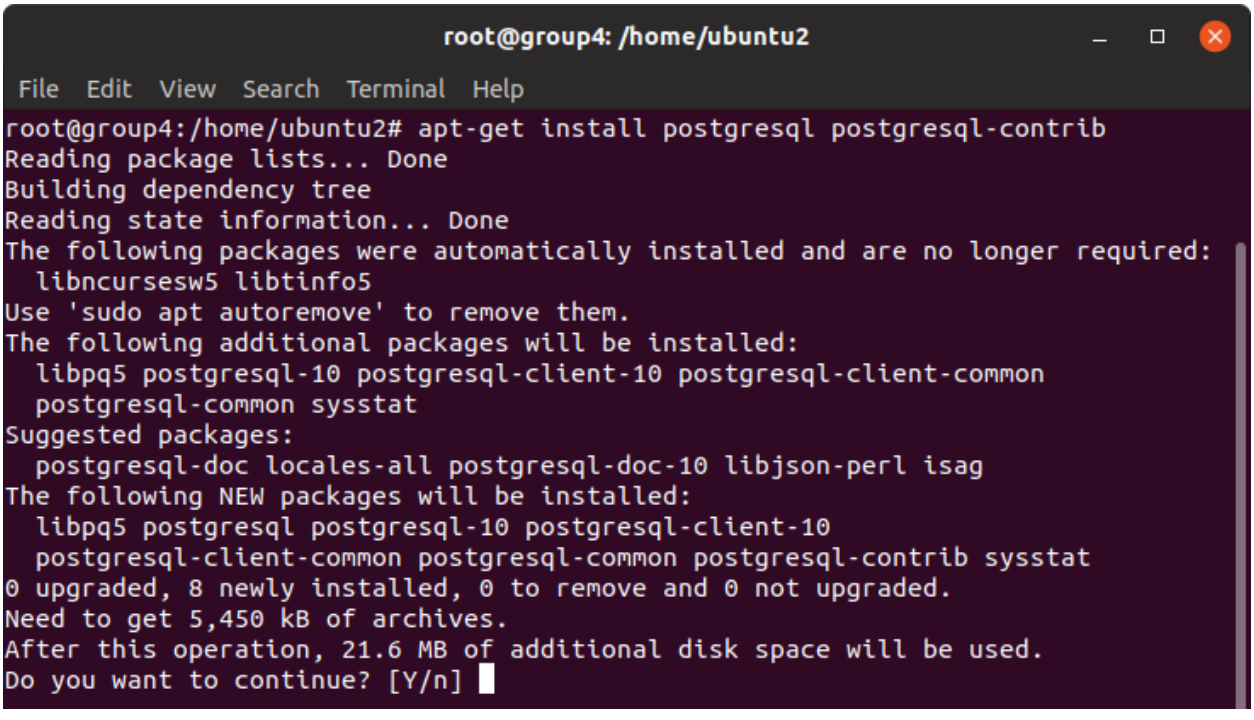


Figure 248 Install PostgreSQL

Step 2: The default database name and password is "**postgres**". Therefore, to perform any postgresql related operation, first switch to the postgres user through **sudo –u postgres psql postgres** and set the postgres password. Then, install the PostgreSQL Adminpack through the **CREATE EXTENSION** command.

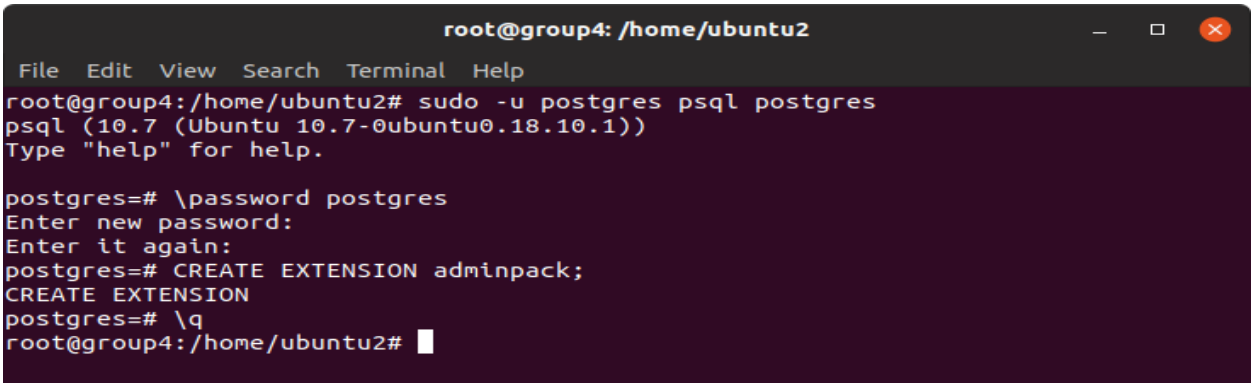


Figure 249 PostgreSQL commands

Step 3: Configure PostgreSQL for MD5 authentication which requires the client supply an MD5-encrypted password for authentication. For that, **/etc/postgresql/9.3/main/pg_hba.conf** file have to be edited.

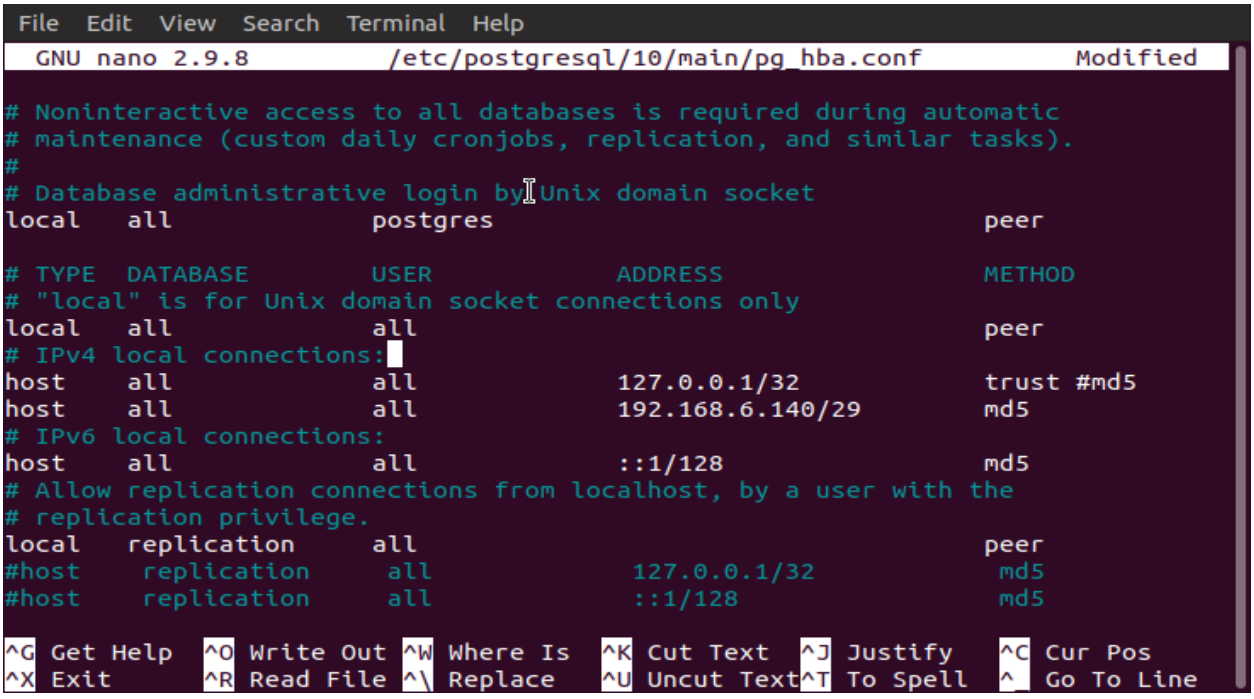


Figure 250 Configure PostgreSQL

Step 4 : Install phpPgAdmin which is a web-based administration utility to manage PostgreSQL.

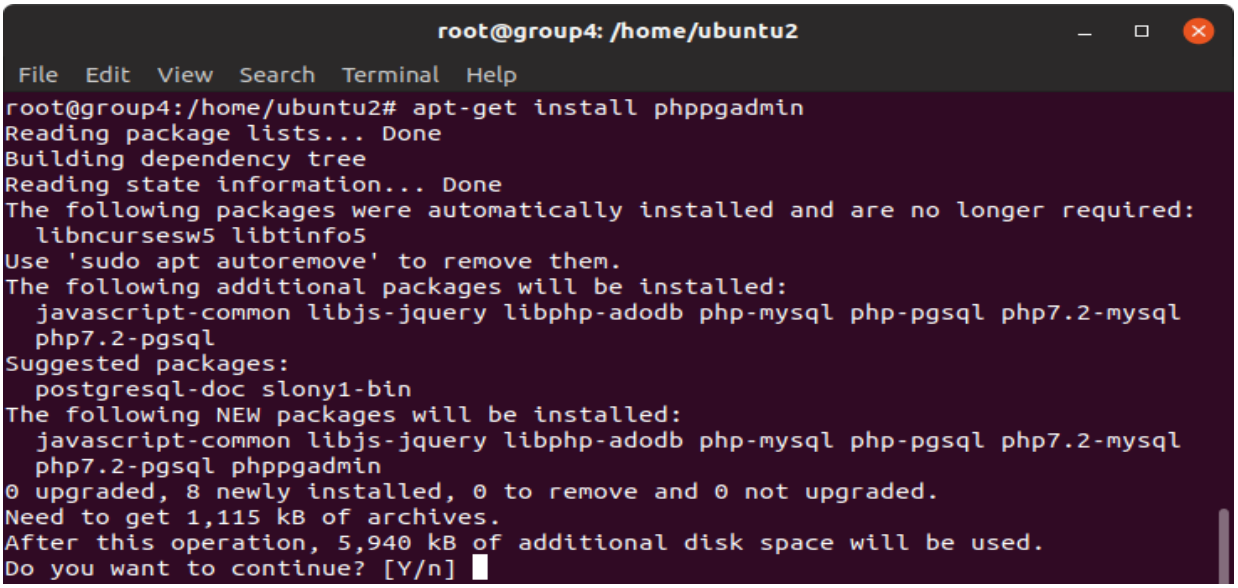


Figure 251 Install phpPgAdmin

Step 5: Edit the file **/etc/apache2/conf.d/phppgadmin** to make phppgadmin from all systems. Uncomment "**allow from all**" and comment "**allow from**" line.

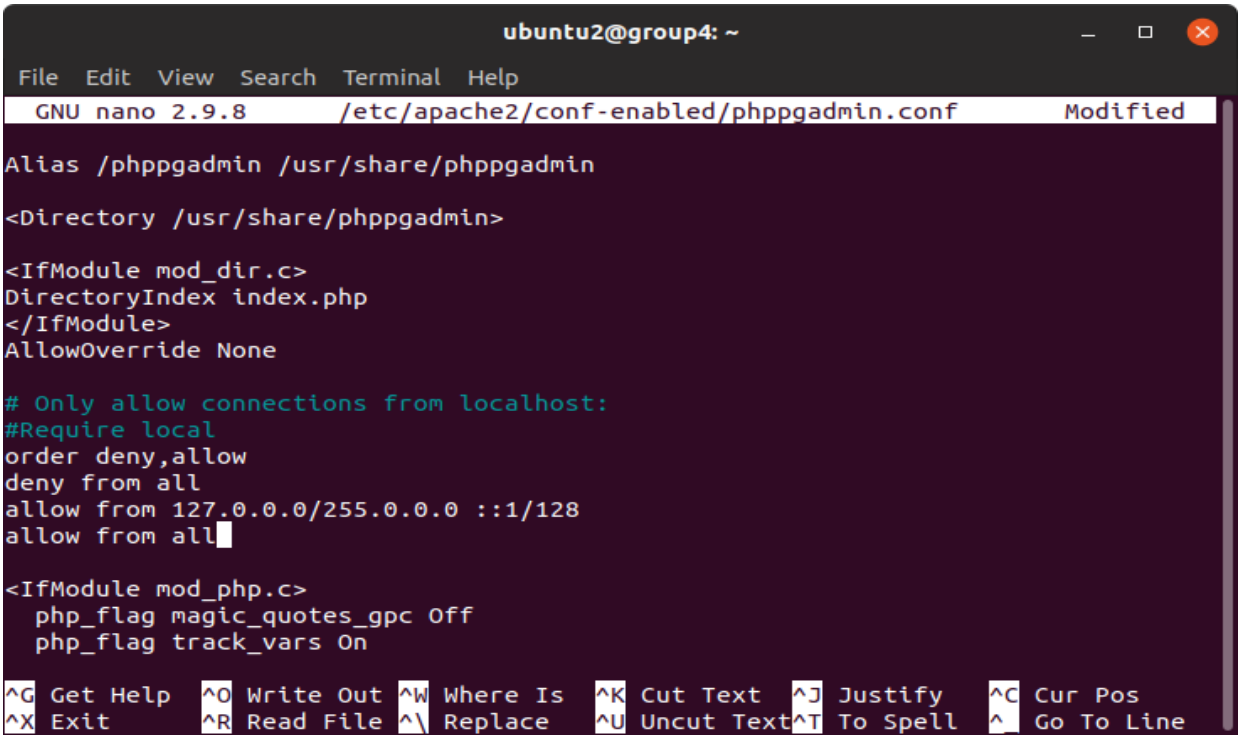


Figure 252 Edit /etc/apache2/conf.d/phpgadmin

Step 6: Then, restart the apache service through **sudo service apache2 restart**

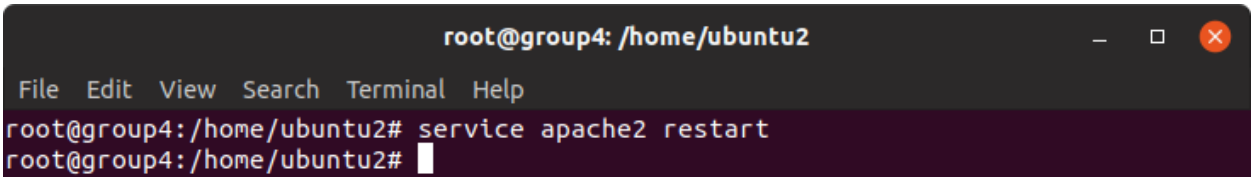


Figure 253 Restart services

Step 7 : To configure phpPgAdmin, edit the **/etc/phppgadmin/config.inc.php** file.

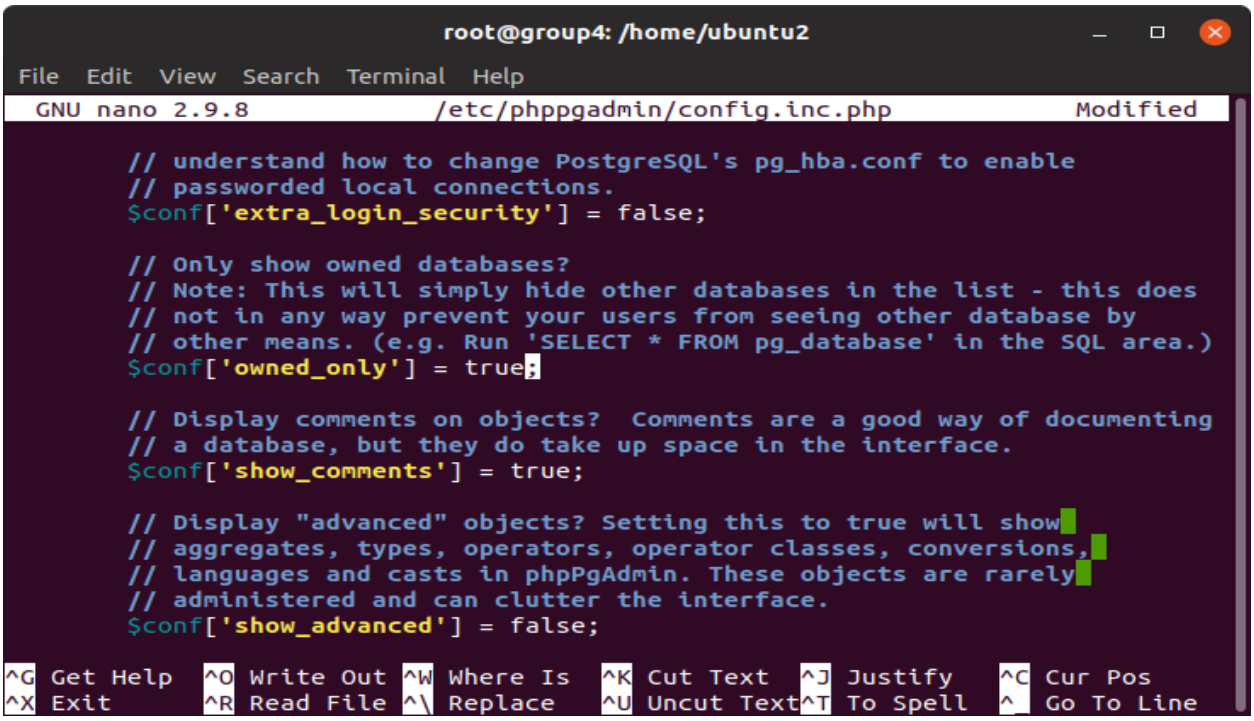


Figure 254 Edit /etc/phppgadmin/config.inc.php

Step 8: Restart the postgresql service through the command

sudo service postgresql restart

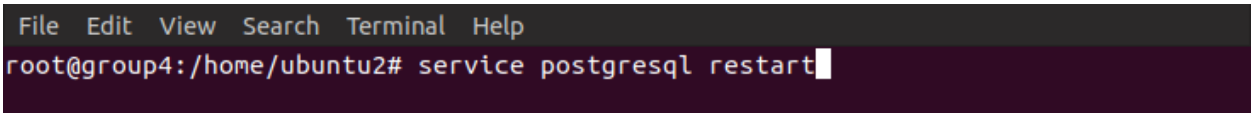


Figure 255 Restart services

Step 9: Create a new user and database to be used in our desired network. The new user is called **Group4** with password **Group42019** and a database called **mydb**.

```
File  Edit  View  Search  Terminal  Help
root@group4:/home/ubuntu2# sudo -u postgres createuser -D -A -P Group4
Enter password for new role:
Enter it again:
root@group4:/home/ubuntu2# sudo -u postgres createdb -O Group4 mydb
root@group4:/home/ubuntu2#
```

Figure 256 Create new user

Step 10: Open the browser and navigate to http://127.0.1.1/phppgadmin to see the phpPgAdmin website.

Step 11: Login using the user that has been created before which is **Group4**.

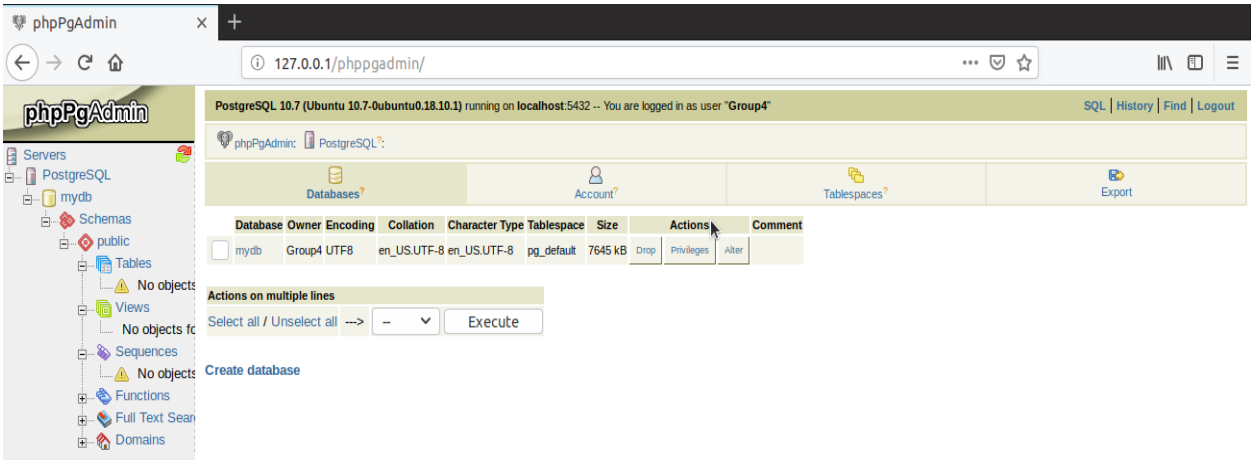


Figure 257 Login done

5.3.14.2 Install JDK

Step 1 : Install JDK by following these steps.

add-apt-repository ppa:linuxuprising /java

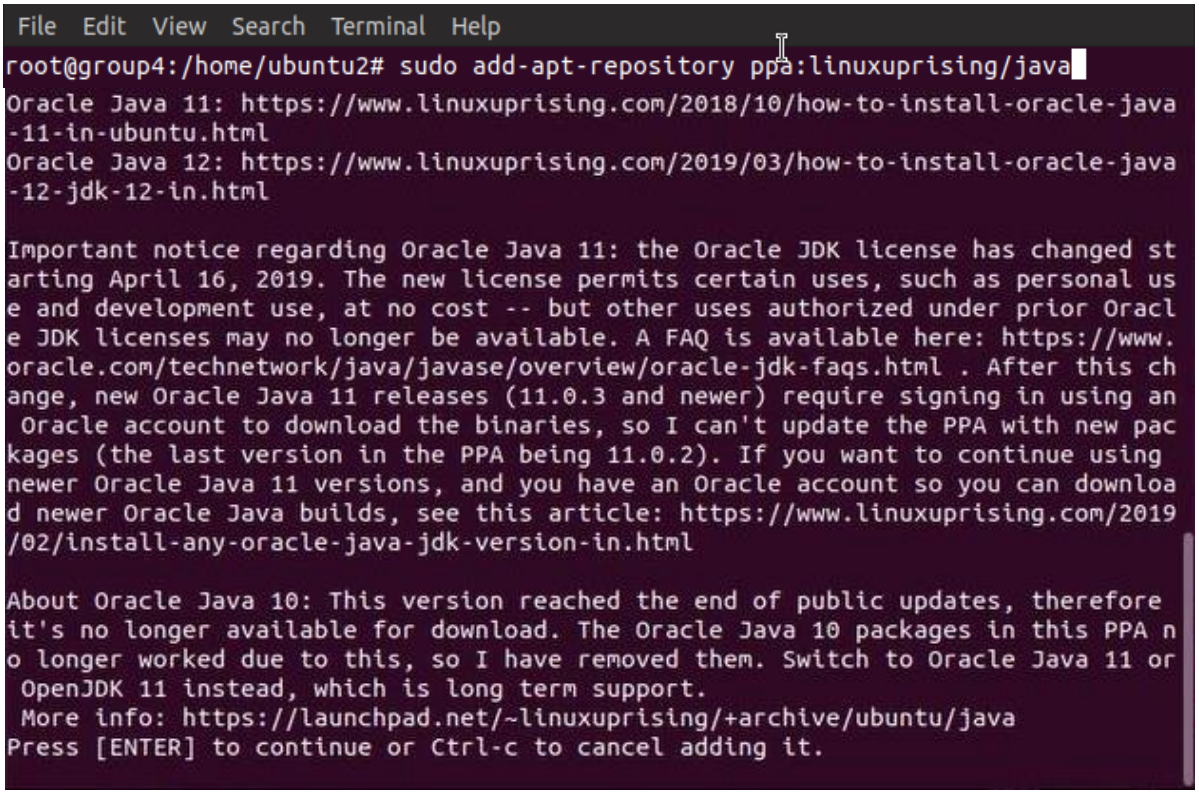


Figure 258 Step to install JDK

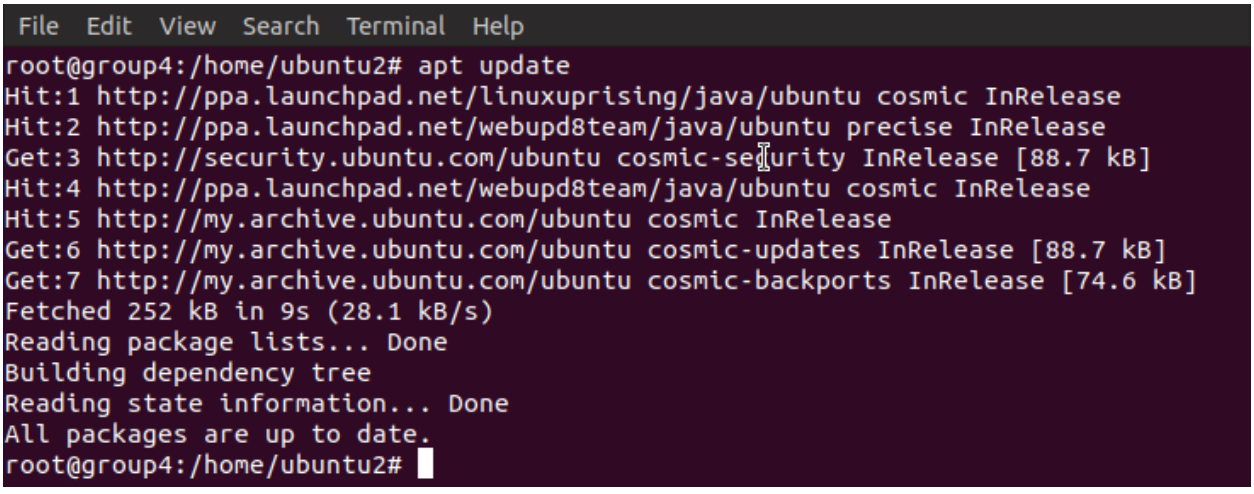


Figure 259 Update

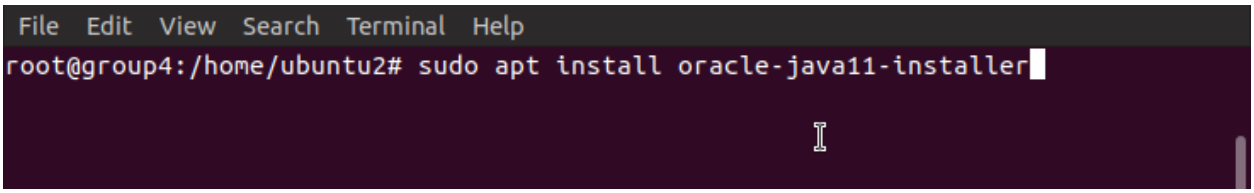


Figure 260 Install Java 11

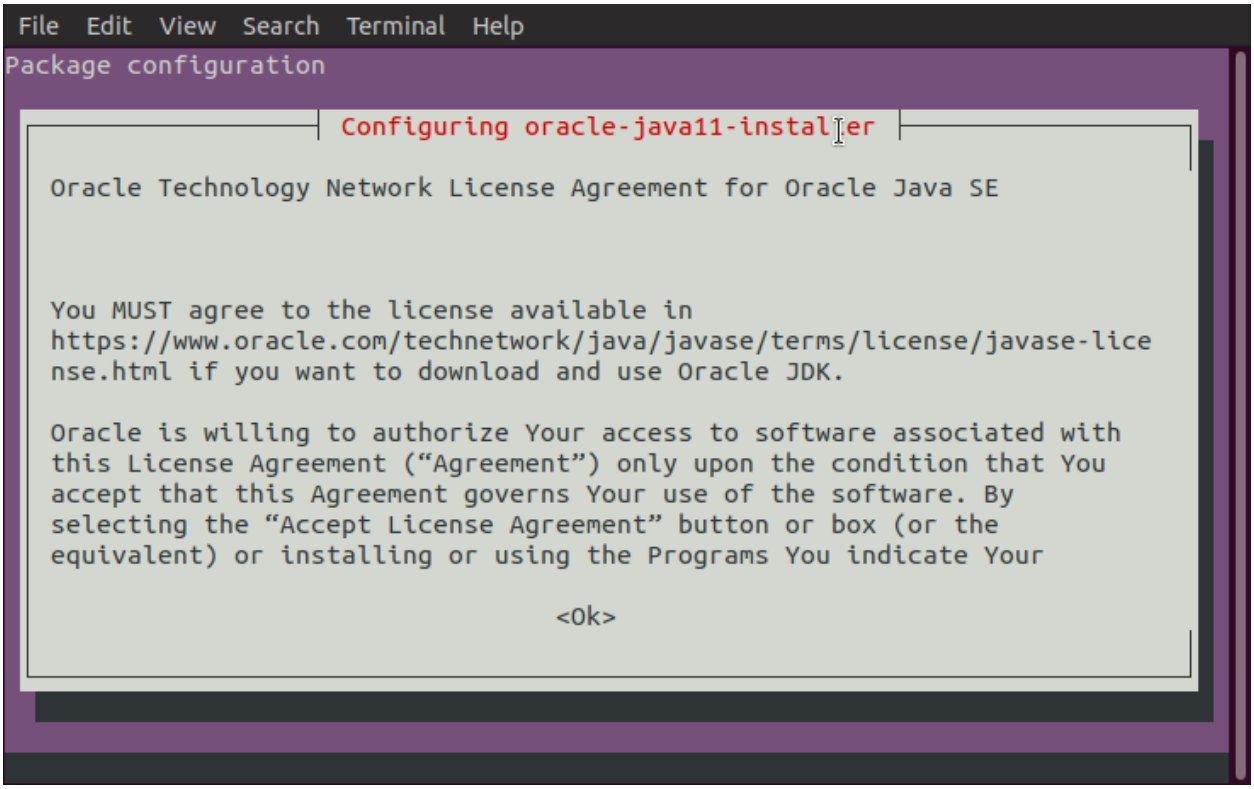


Figure 261 Click OK

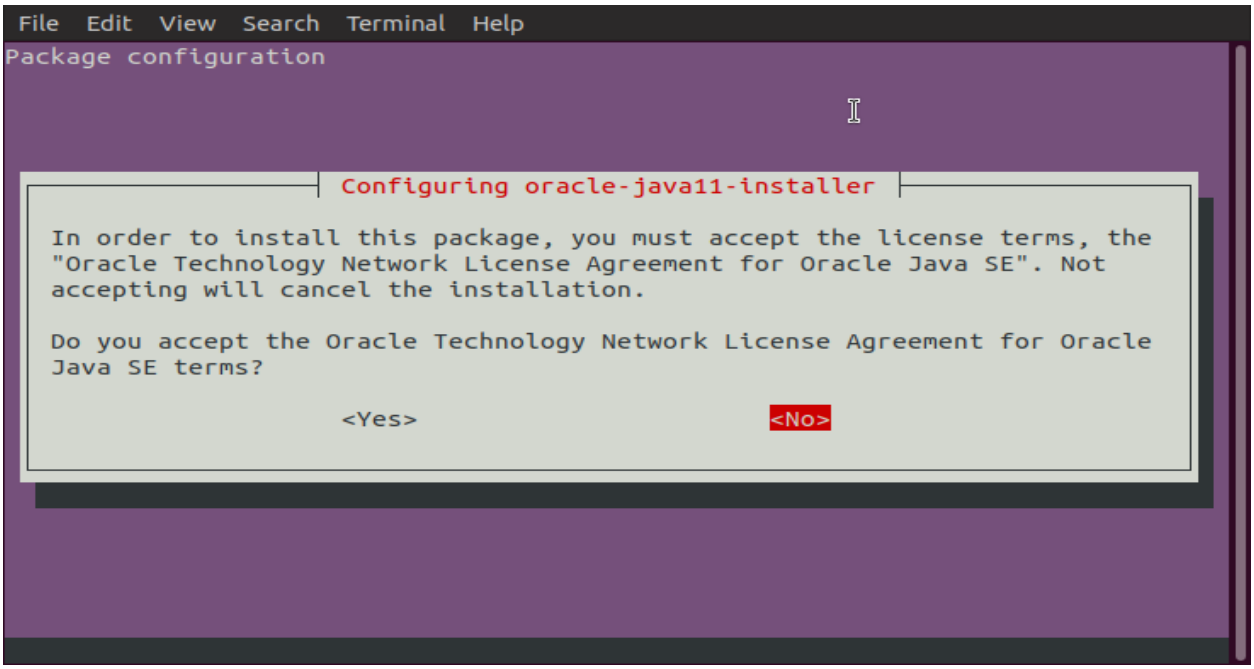


Figure 262 Click YES

5.3.14.3 Install OpenNMS Repository

Step 1: Create a file called **"opennms.list"** in **/etc/apt/sources.list.d** directory.

Add the OpenNMS APT repository

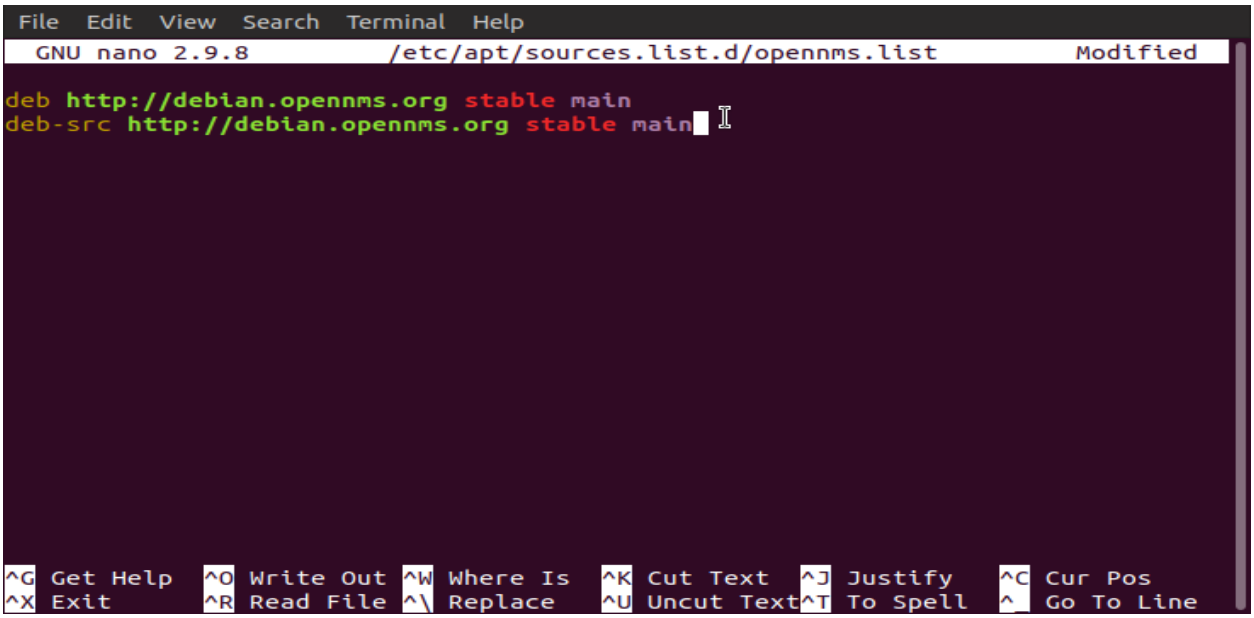


Figure 263 Create a file

Step 2: Add the OpenNMS key.

```
File  Edit  View  Search  Terminal  Help
root@group4:/home/ubuntu2# wget -O - http://debian.opennms.org/OPENNMS-GPG-KEY |
sudo apt-key add -
--2019-04-30 15:06:51--  http://debian.opennms.org/OPENNMS-GPG-KEY
Resolving debian.opennms.org (debian.opennms.org)... 104.236.160.233, 2604:a880:
1:20::d6:7001
Connecting to debian.opennms.org (debian.opennms.org)|104.236.160.233|:80... con
nected.
HTTP request sent, awaiting response... 200 OK
Length: 1725 (1.7K)
Saving to: ‘STDOUT’

-                   100%[===================>]   1.68K  --.-KB/s    in 0s

2019-04-30 15:06:51 (78.2 MB/s) - written to stdout [1725/1725]

OK
root@group4:/home/ubuntu2#
```

Figure 264 Add OpenNMS key

Step 3: Install OpenNMS.

```
File  Edit  View  Search  Terminal  Help
root@group4:/home/ubuntu2# sudo apt-get install opennms
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  guile-2.0-libs iplike-pgsql10 jicmp jicmp6 libdbd-pg-perl
  libgetopt-mixed-perl libgsasl7 libkyotocabinet16v5 libmailutils5
  libmysqlclient20 libnet-snmp-perl libntlm0 libopennms-java
  libopennmsdeps-java libxml2-utils mailutils mailutils-common mysql-common
  opennms-common opennms-db opennms-server opennms-source opennms-webapp-jetty
Suggested packages:
  libcrypt-des-perl libio-socket-inet6-perl mailutils-mh mailutils-doc
  opennms-doc jrrd2 rrdtool
The following NEW packages will be installed:
  guile-2.0-libs iplike-pgsql10 jicmp jicmp6 libdbd-pg-perl
  libgetopt-mixed-perl libgsasl7 libkyotocabinet16v5 libmailutils5
  libmysqlclient20 libnet-snmp-perl libntlm0 libopennms-java
  libopennmsdeps-java libxml2-utils mailutils mailutils-common mysql-common
  opennms opennms-common opennms-db opennms-server opennms-source
  opennms-webapp-jetty
0 upgraded, 24 newly installed, 0 to remove and 0 not upgraded.
Need to get 823 MB of archives.
After this operation, 1,112 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Figure 265 Install OpenNMS

Step 4: After a few minutes, the installer will be asked to run manually. Click **Ok** throughout.

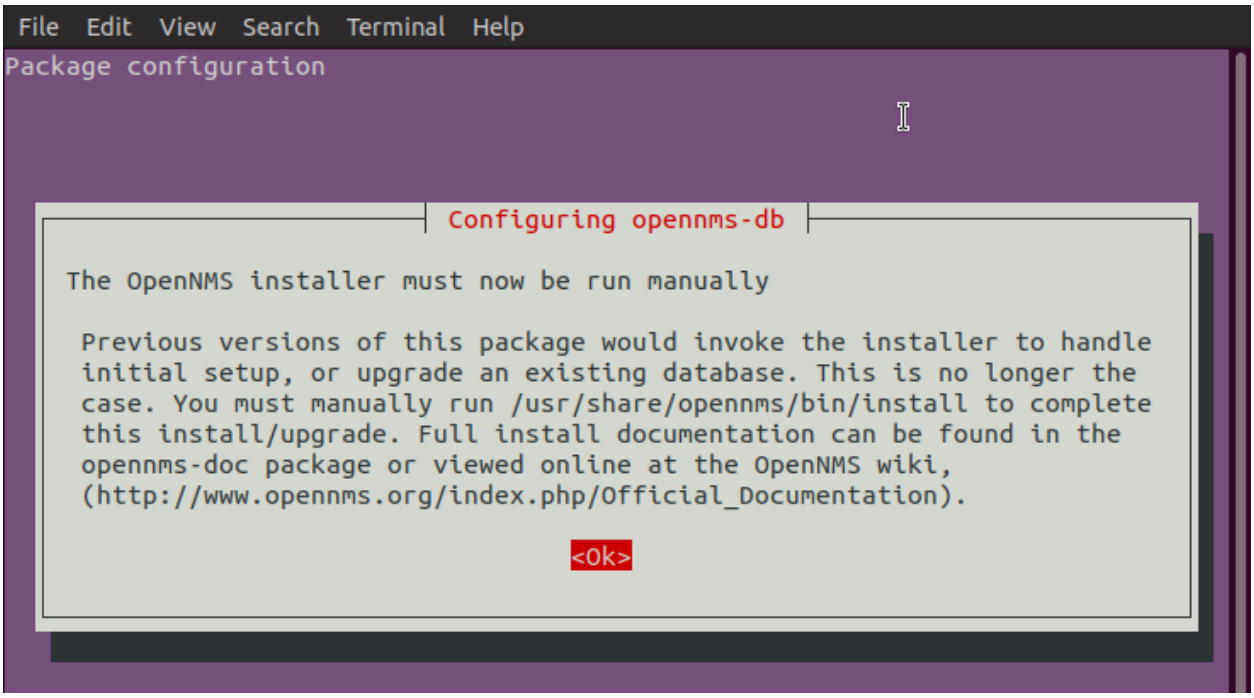


Figure 266 Installer and run manually then Click OK

Step 5: IPLIKE can be installed manually through the command

sudo /usr/sbin/install_iplike.sh

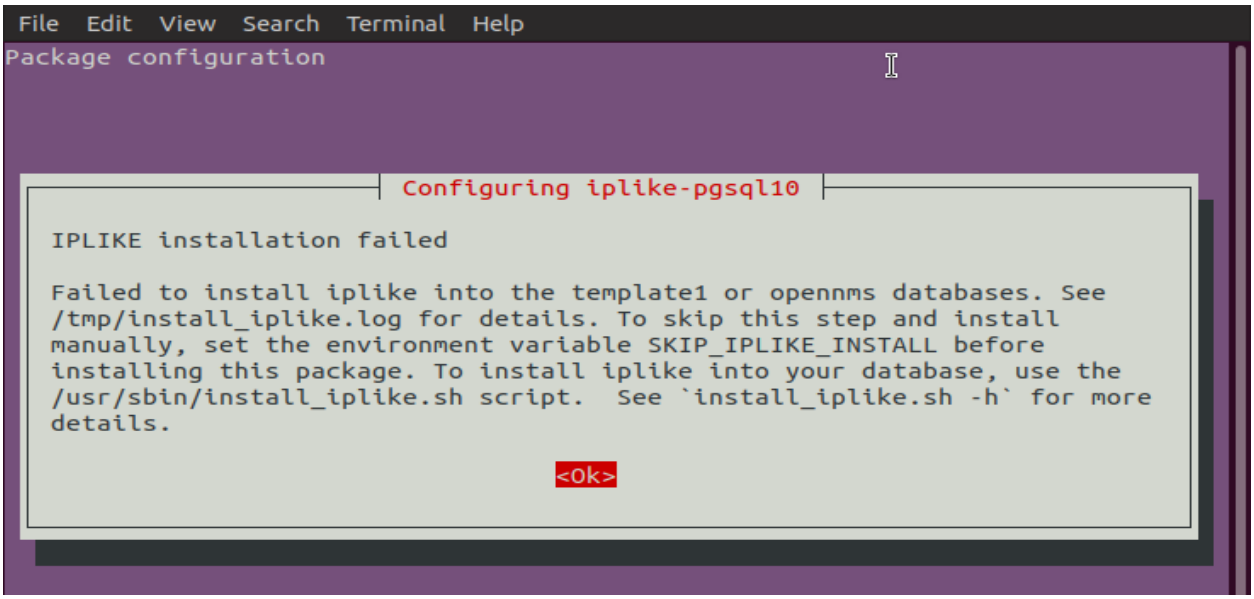


Figure 267 Installation failed then Click OK

5.3.14.4 Post Installation

Step 1: After that, inform OpenNMS on what version of Java are we using.

```
File  Edit  View  Search  Terminal  Help
root@group4:/home/ubuntu2# sudo /usr/share/opennms/bin/runjava -s
runjava: Looking for an appropriate JVM...
runjava: Checking for an appropriate JVM in JAVA_HOME...
runjava: Skipping... JAVA_HOME not set.
runjava: Checking JVM in the PATH: "/etc/alternatives/java"...
runjava: Did not find an appropriate JVM in the PATH: "/etc/alternatives/java"
runjava: Searching for a good JVM...
runjava: Found a good JVM in "/usr/lib/jvm/java-11-oracle/bin/java".
runjava: Value of "/usr/lib/jvm/java-11-oracle/bin/java" stored in configuration
 file.
root@group4:/home/ubuntu2#
```

Figure 268 Inform OpenNMS on what version of Java are we using

Step 2: Create a database for OpenNMS

```
File  Edit  View  Search  Terminal  Help

root@group4:/home/ubuntu2# sudo /usr/share/opennms/bin/install -dis
=============================================================================
OpenNMS Installer
=============================================================================

Configures PostgreSQL tables, users, and other miscellaneous settings.

DEBUG: Platform is IPv6 ready: true
- searching for libjicmp.so:
  - trying to load /libjicmp.so: NO
  - trying to load /usr/share/opennms/lib/libjicmp.so: NO
  - trying to load /usr/share/opennms/lib/linux64/libjicmp.so: NO
  - trying to load /usr/java/packages/lib/libjicmp.so: NO
  - trying to load /usr/lib64/libjicmp.so: NO
  - trying to load /lib64/libjicmp.so: NO
  - trying to load /lib/libjicmp.so: NO
  - trying to load /usr/lib/libjicmp.so: NO
  - trying to load /usr/lib/jni/libjicmp.so: OK
- searching for libjicmp6.so:
  - trying to load /libjicmp6.so: NO
  - trying to load /usr/share/opennms/lib/libjicmp6.so: NO
  - trying to load /usr/share/opennms/lib/linux64/libjicmp6.so: NO
  - trying to load /usr/java/packages/lib/libjicmp6.so: NO
```

Figure 269 Create a database for OpenNMS

Step 3: Open the browser and navigate it to http://192.168.6.138:8980/opennms. The login screen would appear and enter the default username and password which is ***admin*** and ***admin*** respectively.

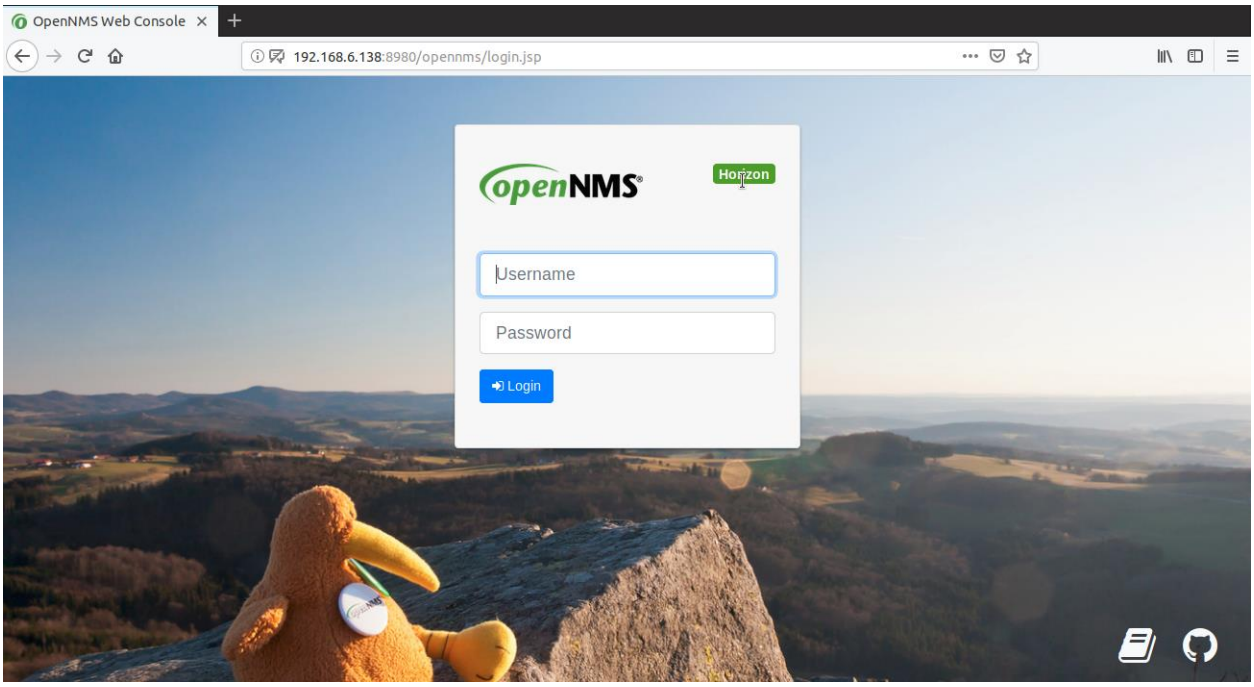


Figure 270 Open Browser and login

5.3.15 Proxy Server

A proxy server is computer that functions as an intermediary between a web browser and the Internet. Proxy servers help improve web performance by storing a copy of frequently used webpages. Whenever the client connects to a web proxy server and makes a request for the resources that reside on a remote server, the proxy server forwards this requests to the target server on behalf of the client, so as to fetch the requested resource and deliver it back to the client. An example of client can be a user operated computer that is connected to the Internet.

Step 1: Install the squid package

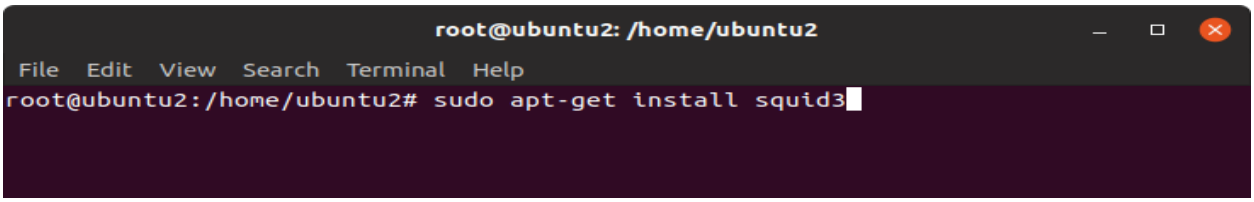


Figure 271 Install packages

Step 2: Check status the squid package

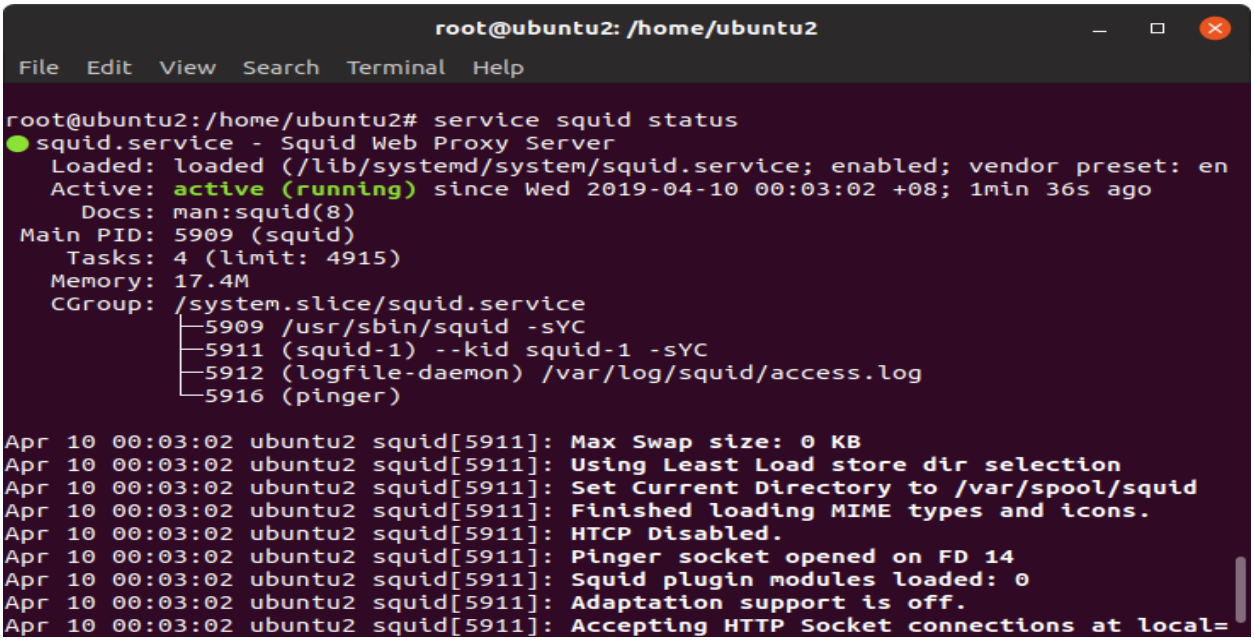


Figure 272 Status the squid package

Step 3: Edit the configuration file of squid

#sudo -H gedit /etc/squid/squid.conf &>/dev/null

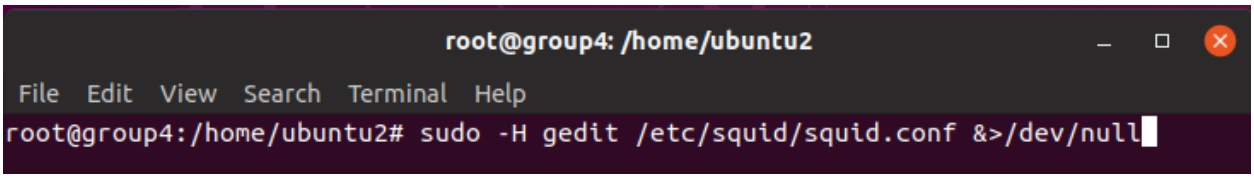


Figure 273 Edit ACL command on configuration file

Step 4: list all the website that will be block

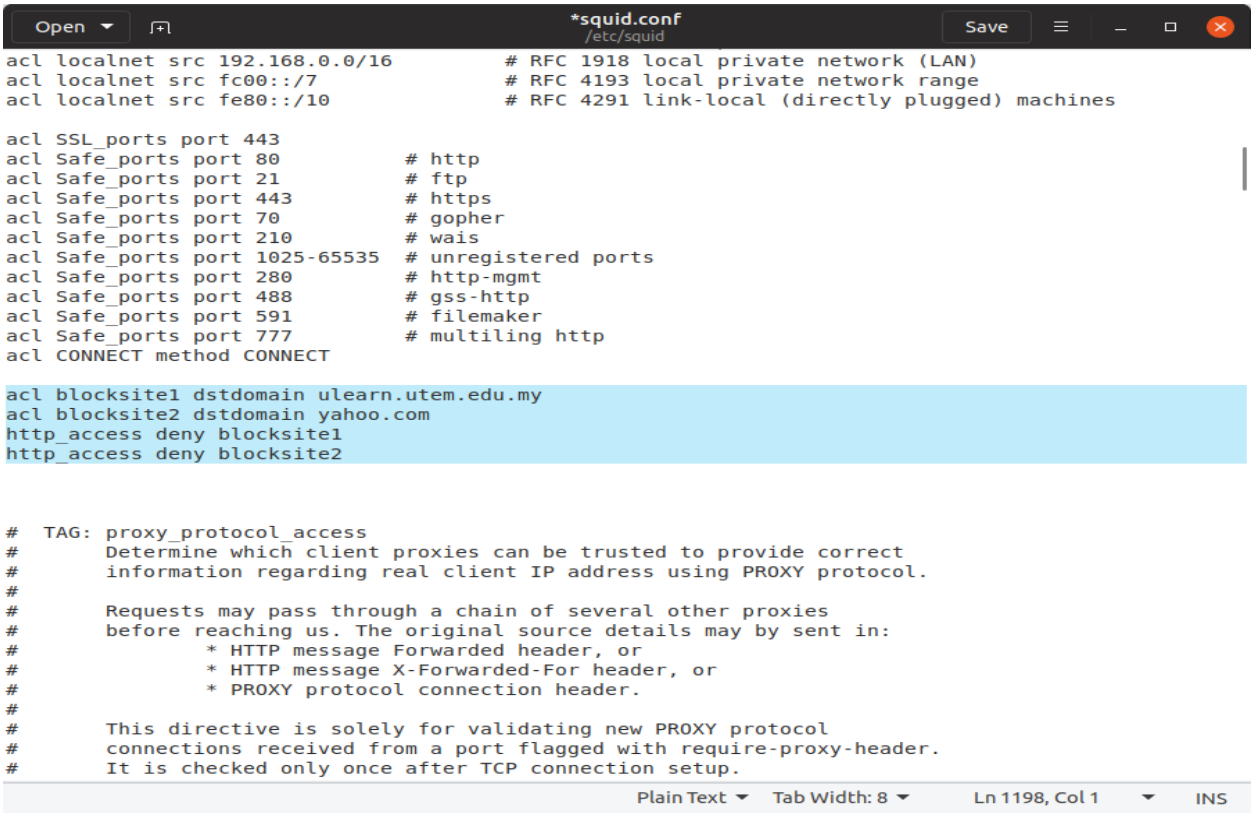


Figure 274 The list of blocking website

Step 5: Change ‘deny’ all to ‘allow’ all.

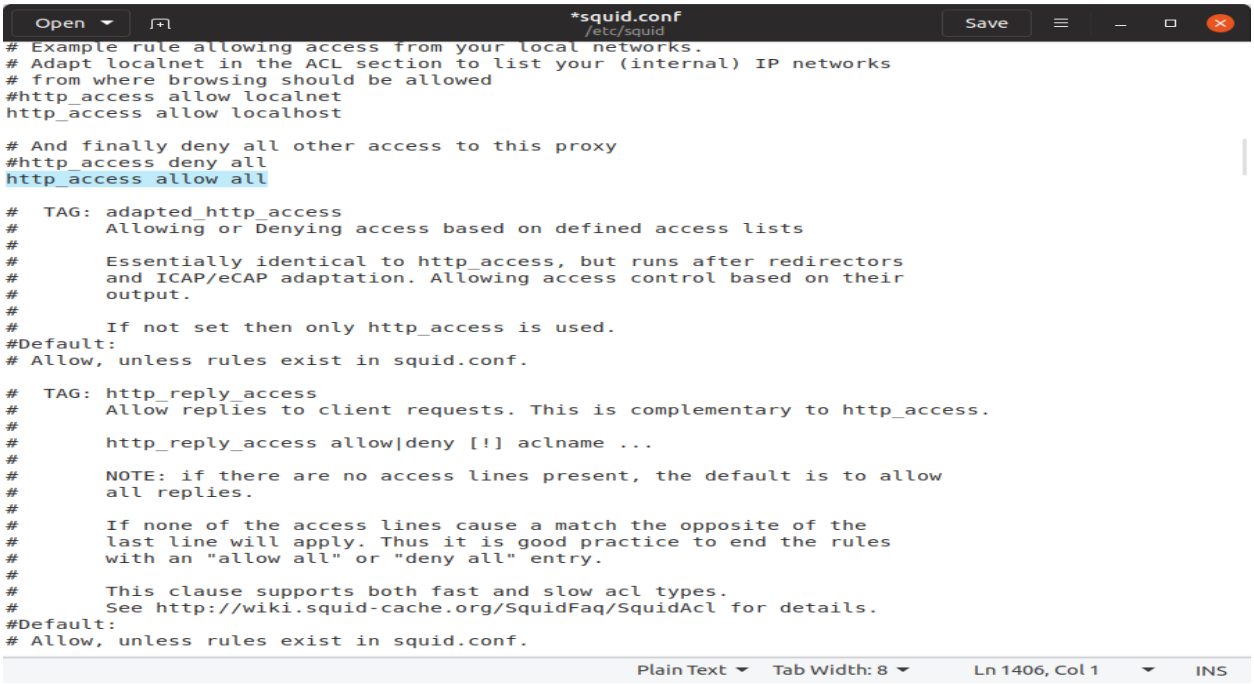


Figure 275 Change http access

Step 6: restart the squid proxy ***#sudo service squid restart.***

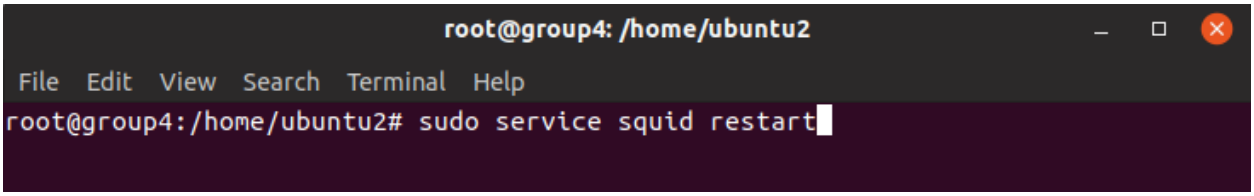


Figure 276 Restart service squid

Step 7: Open Your Browser

Step 8: At the top right bar, click and select “Preferences” option

Step 9: Select “Advance” option, “Network” and “Setting” button

Step 10: Select “Manual proxy configuration” and fill in as below

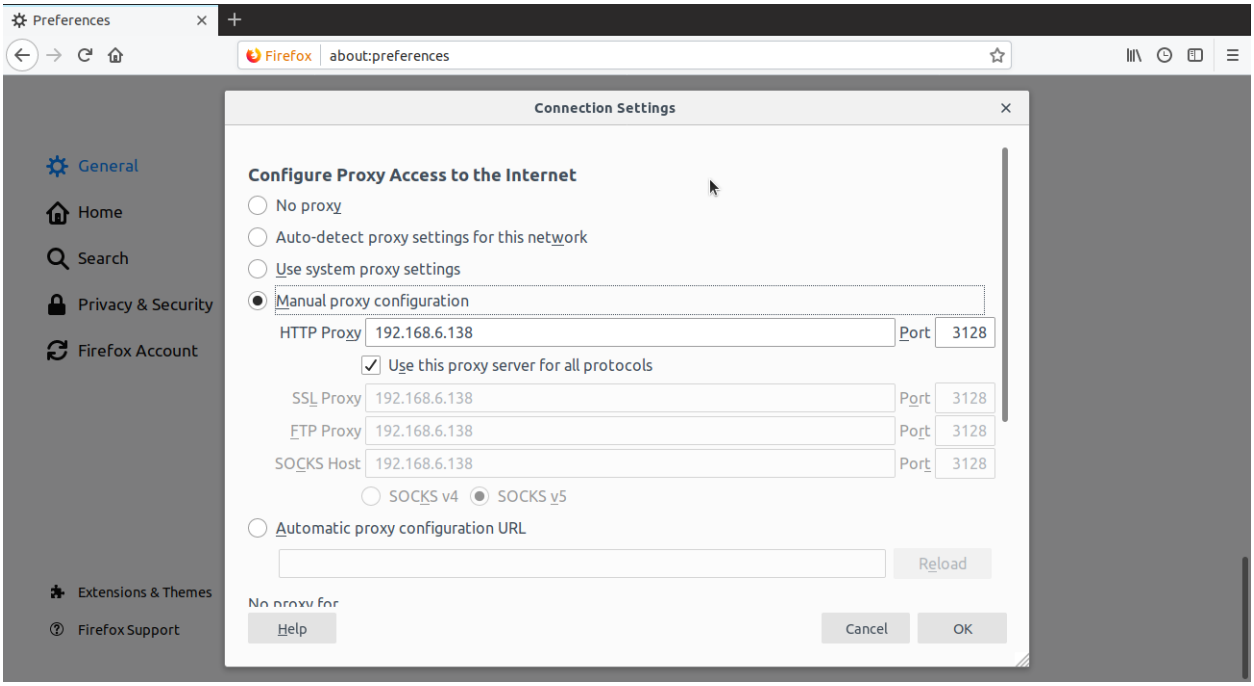


Figure 277 Setting IP proxy server at browser

5.3.16 Wireless User Authentication using Radius Server

WPA2-Enterprise with 802.1X authentication can be used to authenticate users or computers in a domain. The supplicant (wireless client) authenticates against the RADIUS server (authentication server) using an EAP method configured on the RADIUS server. The gateway APs (authenticator) role is to send authentication messages between the supplicant and authentication server. This means the RADIUS server is responsible for authenticating users.

Step 1 : Select the Server that you want to install the Network Policy Server (NPS)

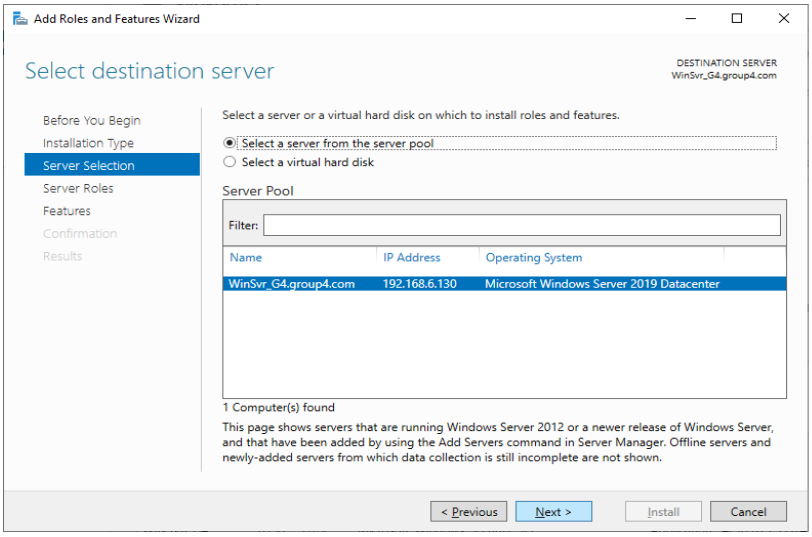


Figure 278 Select server

Step 2 : Select the Network Policy and Access Services to be installed on the server

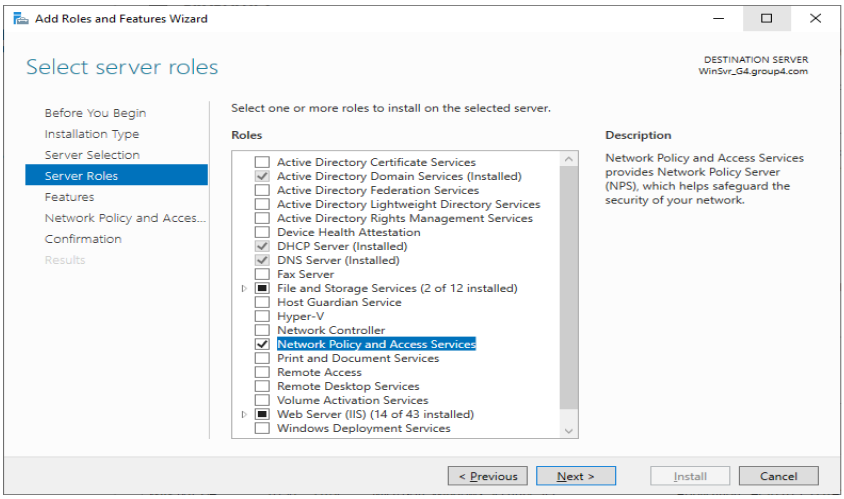


Figure 279 Select Network Policy and Access Services roles

Step 3 : After the installation services, there will be a pop up for the NPS to be authenticate in the Active Directory and click “OK”

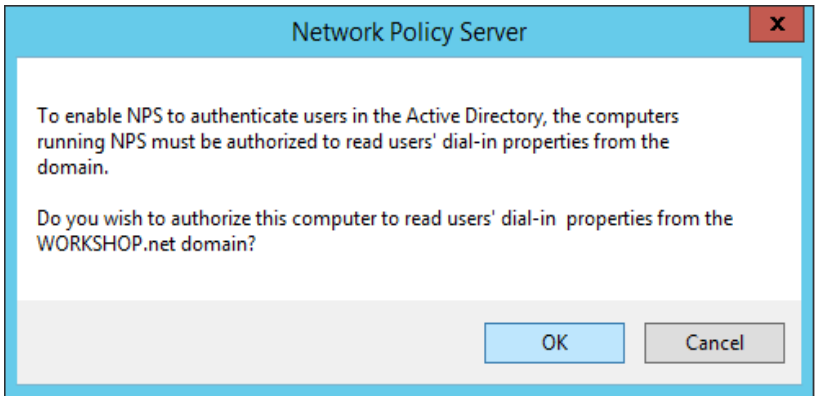


Figure 280 Authenticate NPS in Active Directory

Step 4: Open the Network Policy Server and create a new RADIUS Client

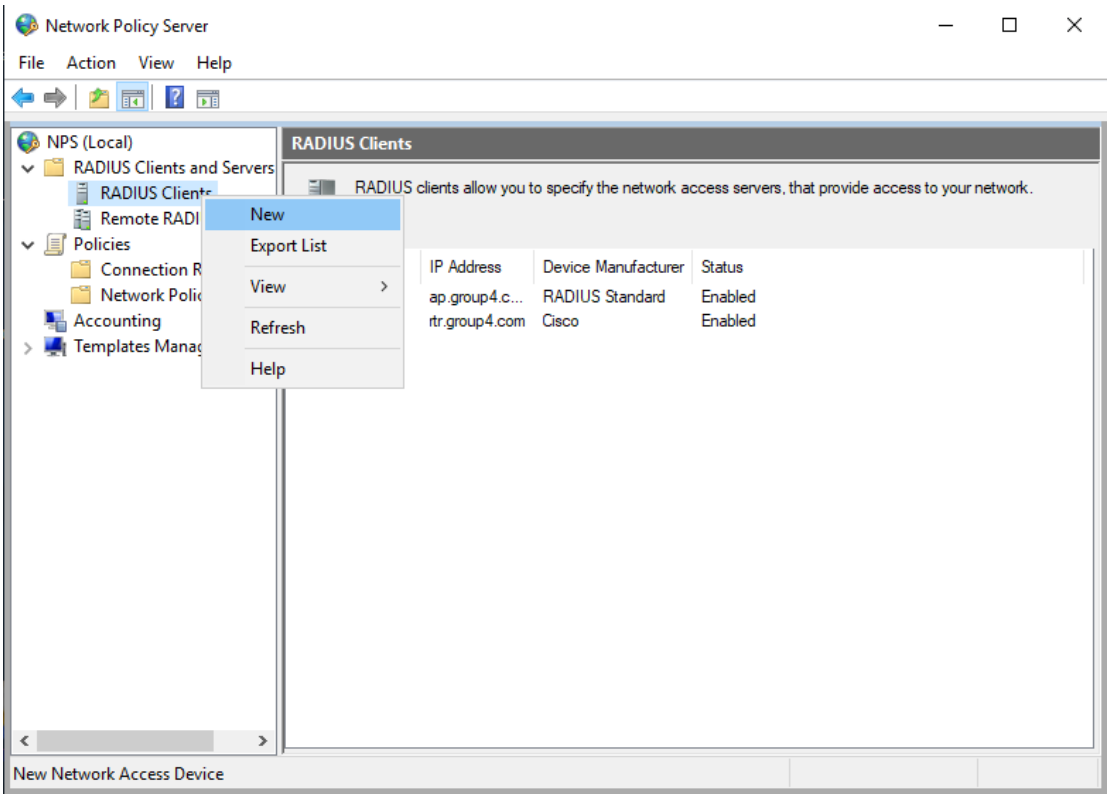


Figure 281 Create RADIUS Client

Step 5 : Crate new RADIUS Client by entering the access point IP address and the shared secret

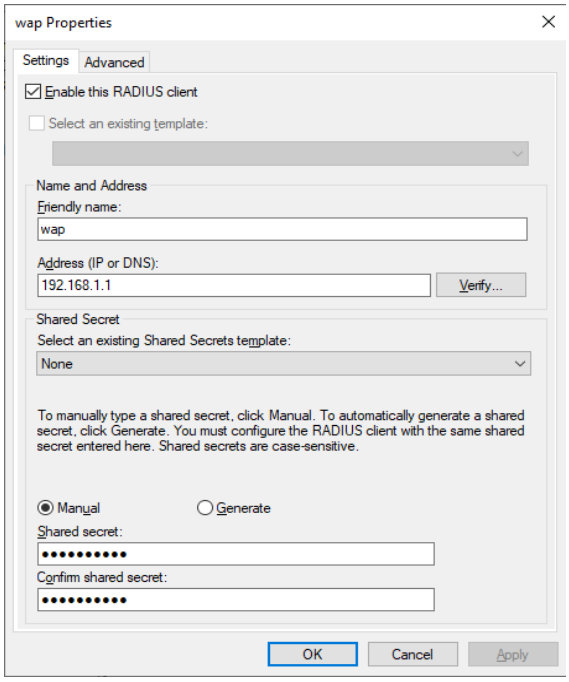


Figure 282 Configure RADIUS Client

Step 6 : Create a new Connection Request Policy under the Policies tab menu

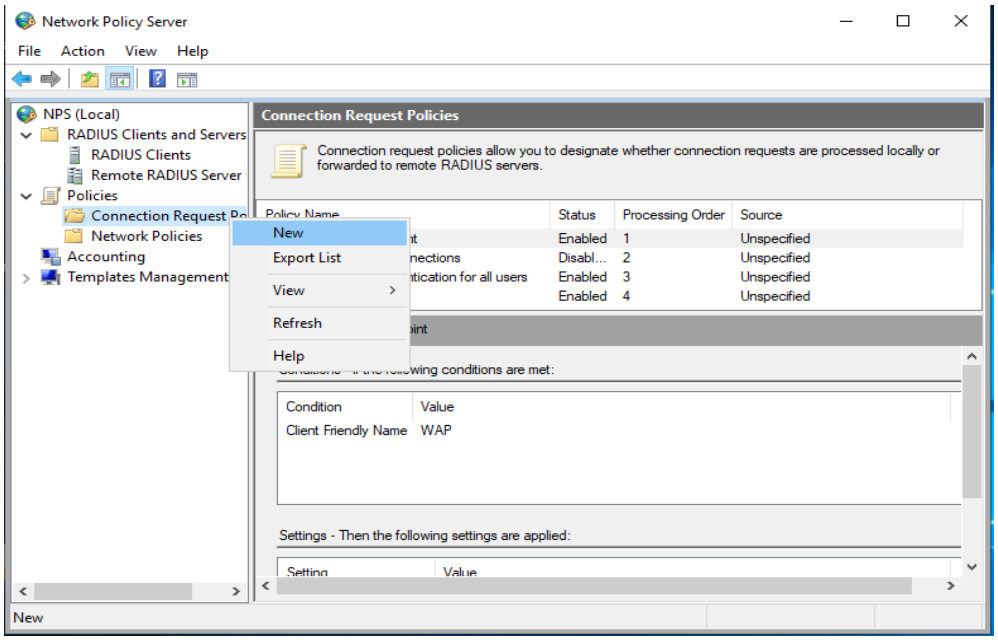


Figure 283 Create new Connection Request Policies

Step 7 : Enter the policy name for the new Connection Request Policy

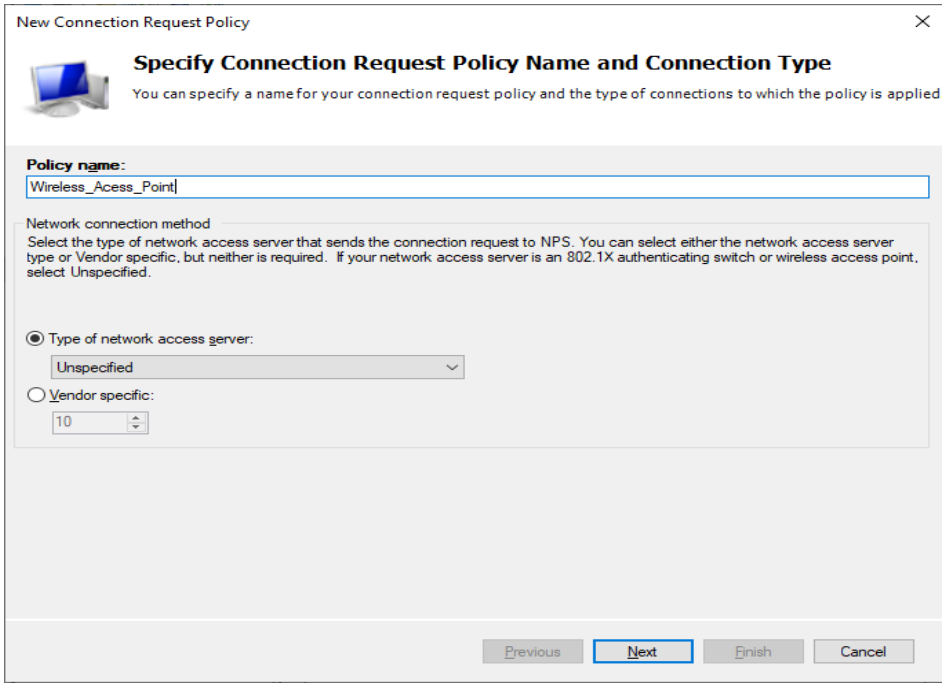


Figure 284 Enter the Policy Name

Step 8 : Select the condition and choose Client Friendly Name and enter the name of the RADIUS CLIENT

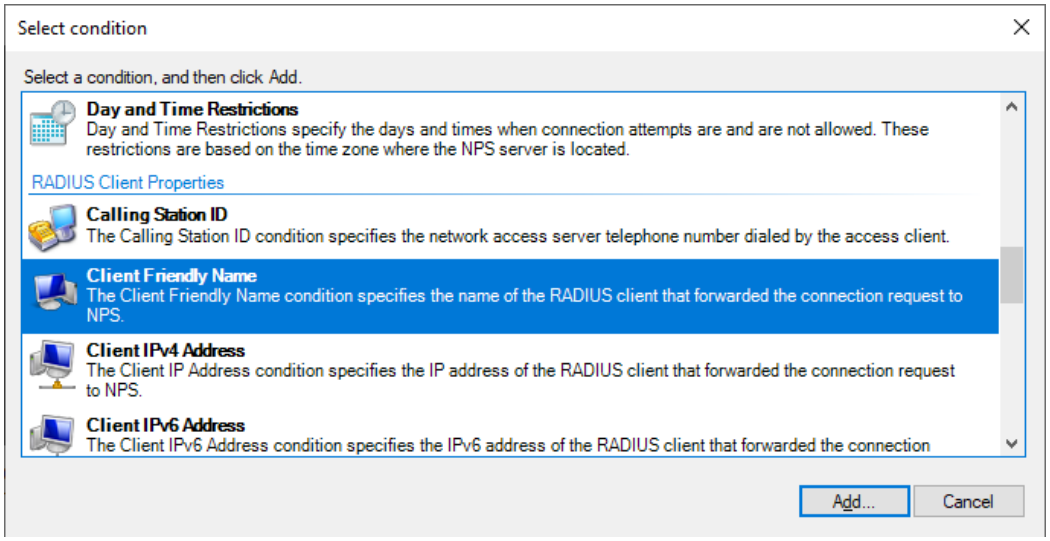


Figure 285 Choose Condition

Step 9 : Create a new user in the Active Directory User and Computer

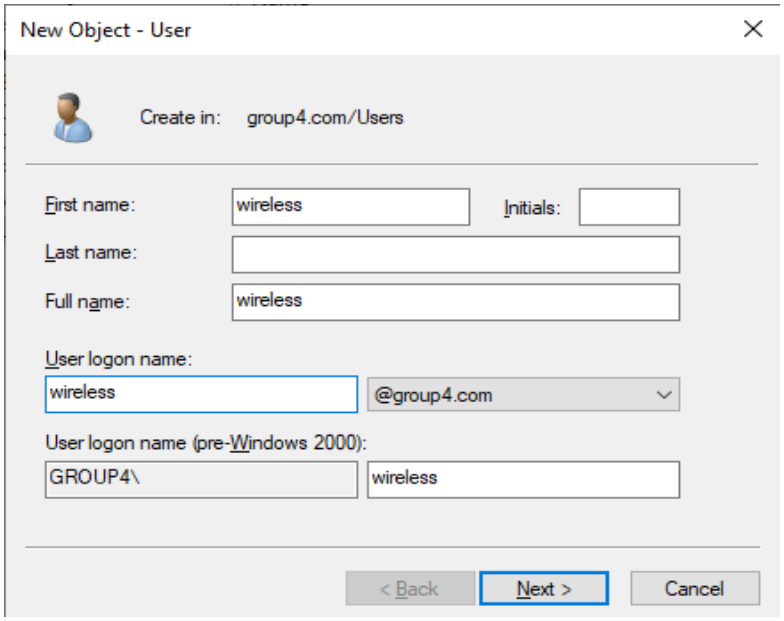


Figure 286 Create a new user

Step 10 : Create a new group for the wireless user

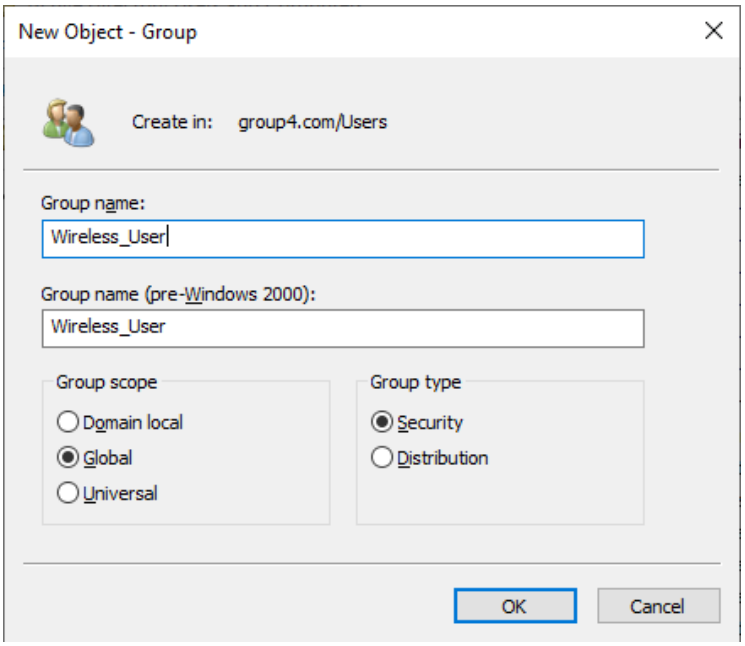


Figure 287 Create a new group

Step 11 : Add the wireless user in the wireless group

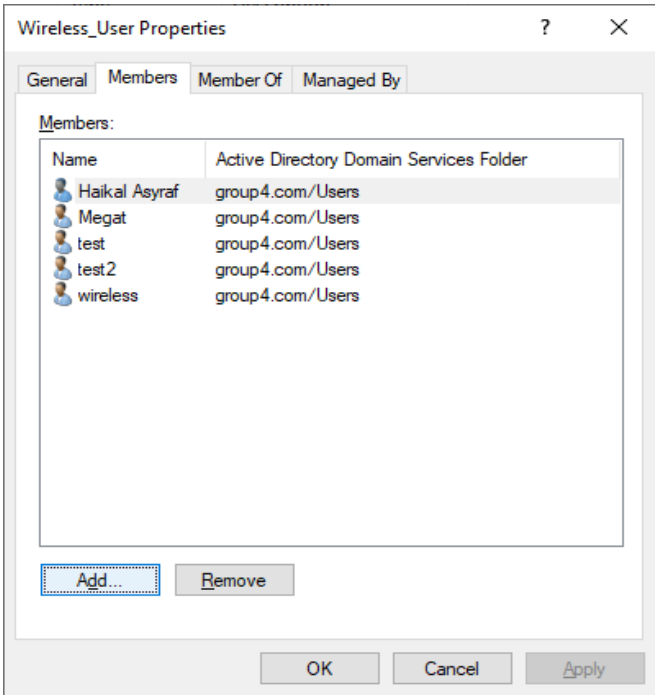


Figure 288 Add user in the wireless group

Step 12: Create a new Network Policies

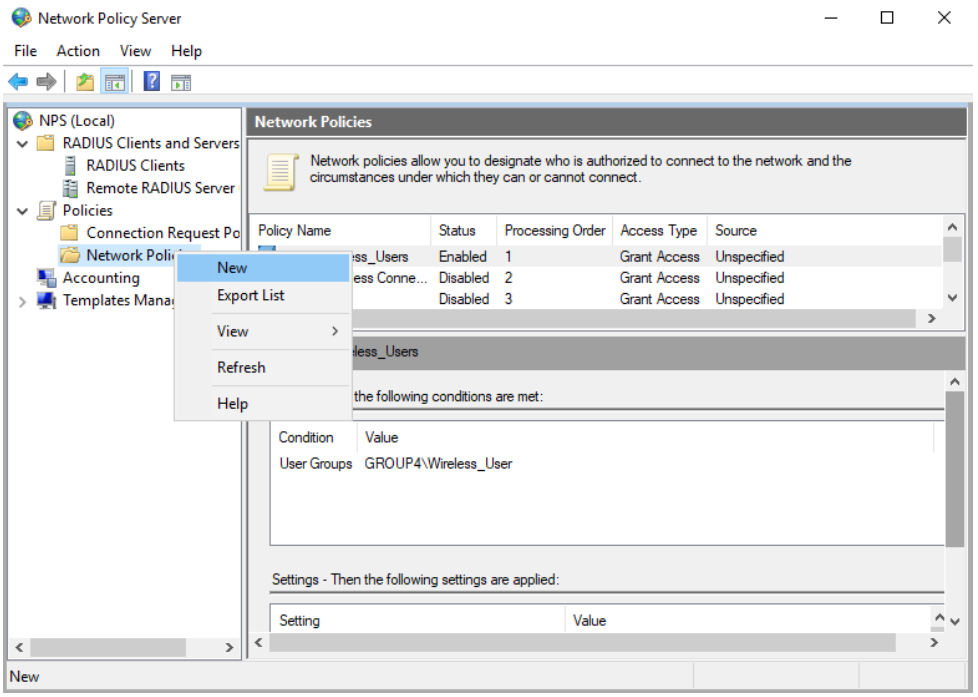


Figure 289 Create Network Policies

Step 13: Enter the policy name for the new Network Policy

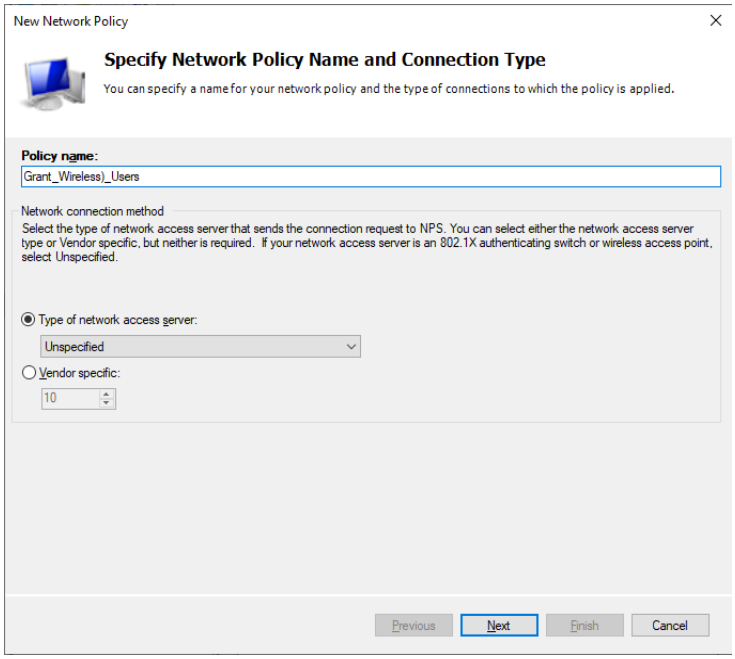


Figure 290 Enter Policy Name

Step 14 : At the select condition option, select the user groups option

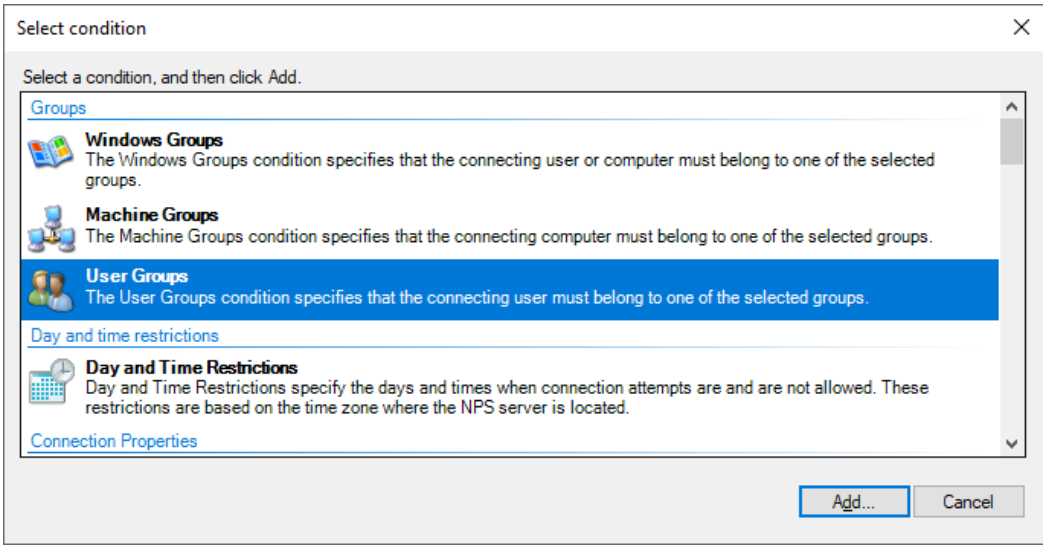


Figure 291 Select User Groups

Step 15 : Enter the group name that been created earlier in the Active Directory

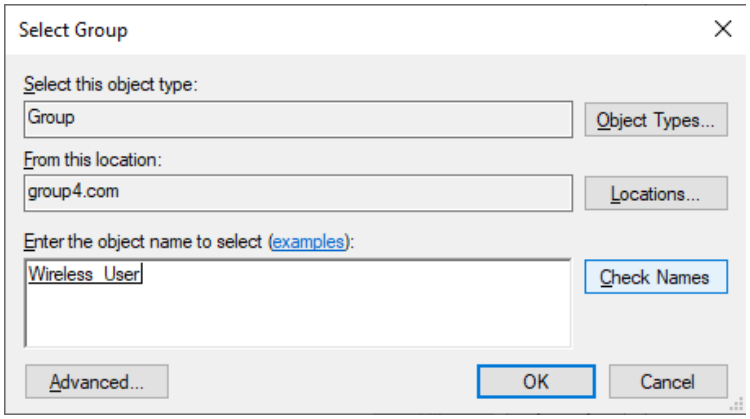


Figure 292 Select wireless group

Step 16 : Add the Microsoft : Secured password (EAP-MSCHAP v2) authentication method and make sure it placed above the (PEAP)

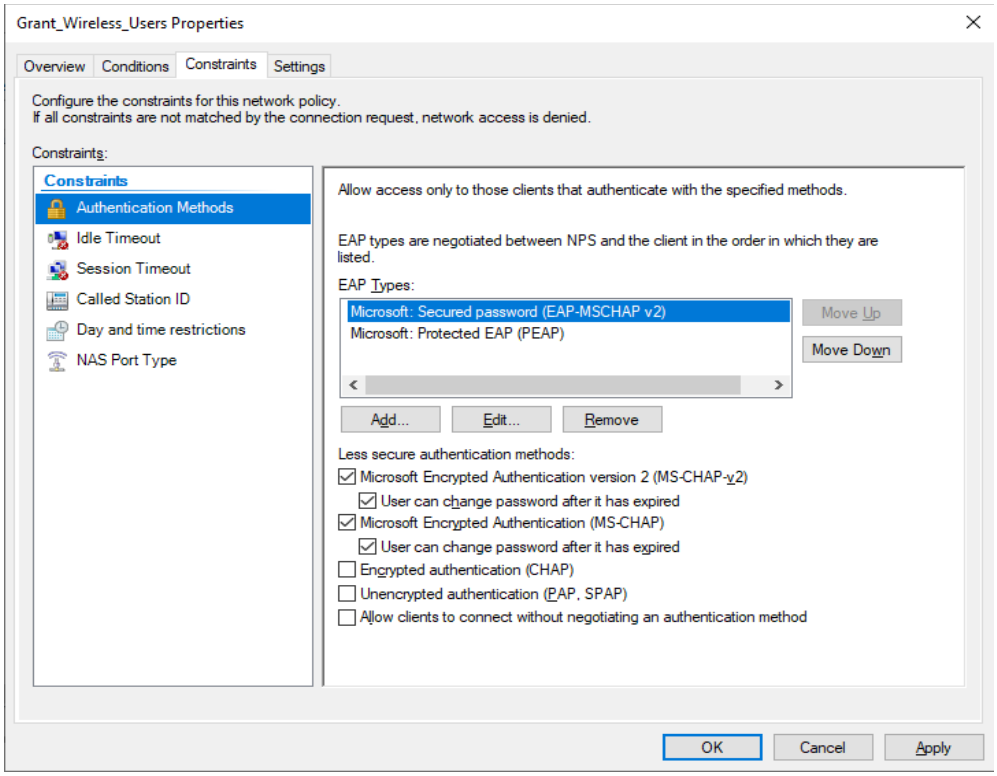


Figure 293 Add Authentication Method

5.3.17 Access Control List (ACL)

5.3.17.1 Configuration of ACL

Step 1: Access CLI prompt of R4 and enter the configuration terminal in global mode and type the command below, this extended access-list used to block specific protocol port from the outside client accessing to our network. Access-list from 100 until 199 is the extended access list and from 1 until 99 is standard access-list. However, deny is blocking what it wants to block the protocol and permit also is what it wants to allow the protocol.

access-list 123 deny tcp 192.168.5.0 0.0.0.63 any eq 80

access-list 123 permit ip any any

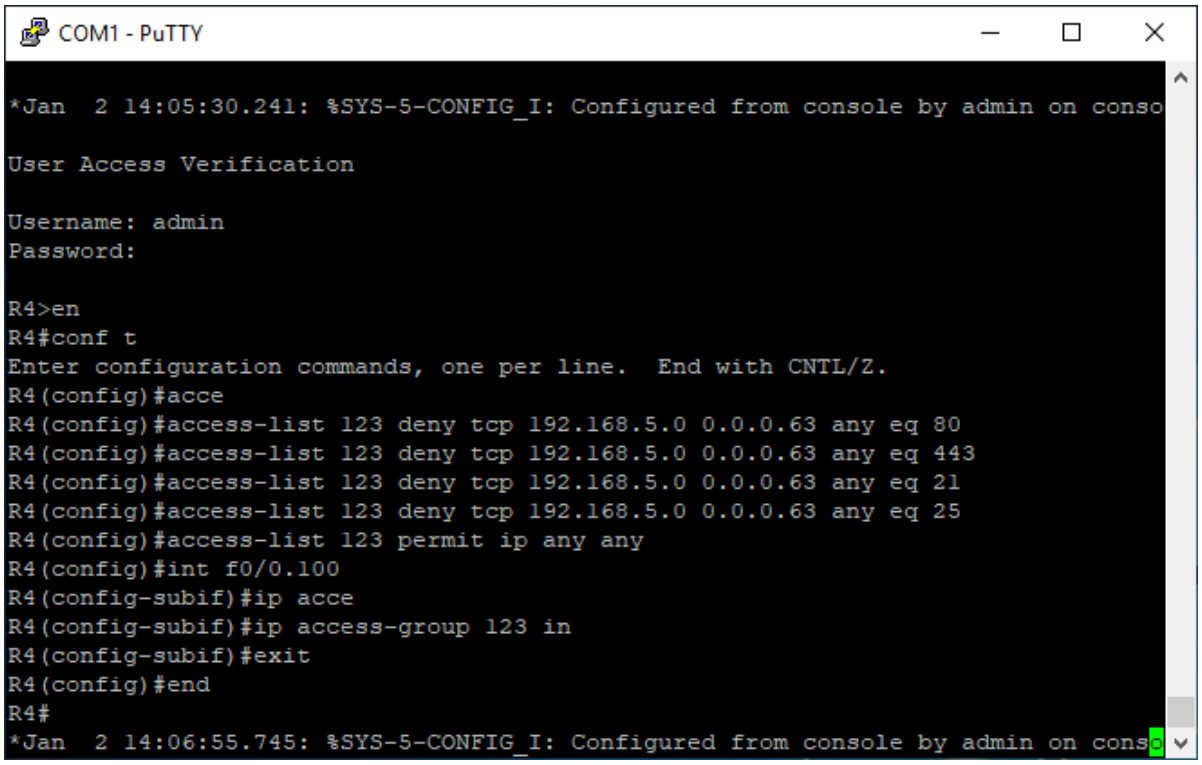


Figure 294 Configuration Access list can deny and permit each of protocol

Step 2: Create a new client and vlan is Client ACL and vlan 100. Firstly, it is make and add from a DHCP for vlan 100 and new client. Client ACL have a mode “ip access-group 123 in”. It has been successful the access-list mode.

```
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 192.168.5.1 255.255.255.192
 ip access-group 123 in
 ip helper-address 192.168.6.130
 ip nat inside
 ip virtual-reassembly
 ipv6 dhcp relay destination 1111:DEAF:FEED:D::3 FastEthernet0/0.20
```

Figure 295 Show IP Address Client ACL and new vlan 100

Step 3: Verify the rules created. Check ACL type the “show run" and to check back whether the rules created is like what it plans to configure the command access-list. It has been done to block protocol is www is web protocol, https is secure web transfer protocol, FTP is file transfer protocol and SMTP is simple email transfer protocol. Then, command of “permit ip any any” is what it has been success block the protocol and it will be a success to ping from client to host server.

show run > find acl command deny and permit

```
access-list 123 deny   tcp 192.168.5.0 0.0.0.63 any eq www
access-list 123 deny   tcp 192.168.5.0 0.0.0.63 any eq 443
access-list 123 deny   tcp 192.168.5.0 0.0.0.63 any eq ftp
access-list 123 deny   tcp 192.168.5.0 0.0.0.63 any eq smtp
access-list 123 permit ip any any
```

Figure 296 Show Access-list deny and permit

Problem

The client is connected to the internet. With the constantly evolving nature of the Internet, it is vital that it continuously protect the network and their information. The Client need to be restricted from freely connecting to anything using certain services. To increase the effectiveness of the security in the network. A certain measure must be taken to filter the incoming and outgoing packets that going through our network.

Solution

Apply ACL rules on router that will either permit or deny the incoming and outgoing packet through network with while permit or deny specific services.

5.3.18 Routing & NAT

Routing is a key feature of Internet because it enables messages to pass from one computer to the target machine. It is a process of moving a packet of data from source to destination. Routing usually performed by a device called router.

NAT (Network Address Translation) is the virtualization of IP (Internet Protocol) addresses. NAT helps improve security and decrease the number of IP addresses an organization needs. It also allows a router to modify packets to allow for multiple devices to share a single public IP address.

5.3.18.1 Routing

Step 1: Define an IP address in the se0/2/0. Then create the default routing to route two network.

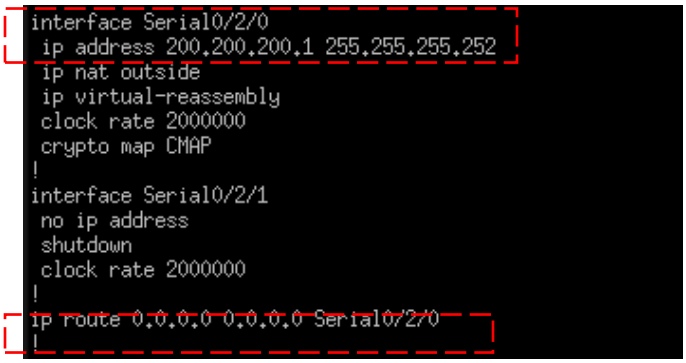


Figure 297 Default Route

5.3.18.2 Network Address Translation (NAT)

Step 1: Setup s0/2/0 as NAT outside**.**

```
R4(config-subif)#int s0/2/0
R4(config-if)#ip nat outside
R4(config-if)#
```

Figure 298 Set up NAT

Step 2: Used command below to configure static NAT for the three server.

```
R4(config)#
R4(config)#ip nat inside source static 192.168.6.130 200.200.200.11
R4(config)#ip nat inside source static 192.168.6.138 200.200.200.12
R4(config)#ip nat inside source static 192.168.6.146 200.200.200.13
```

Figure 299 Set up static NAT

Step 3: Setup f0/0 as NAT inside and all-sub interface as ***NAT inside***

```
R4(config)#int fa0/0.20
R4(config-subif)#ip nat inside
R4(config-subif)#int fa0/0.30
R4(config-subif)#ip nat inside
R4(config-subif)#int fa0/0.40
R4(config-subif)#ip nat inside
```

Figure 300 To identify the inside and outside interfaces

Step 4: Used command below to configure dynamic NAT to the client.

access-list 1 permit 192.168.6.64 0.0.0.63
ip nat pool group4 200.200.200.9 200.200.200.10 netmask 255.255.255.248
ip nat inside source list 1 pool group4

```
R4(config)#access-list 1 permit 192.168.6.64 0.0.0.63
```

Figure 301 Standard Access-List

```
R4(config)#$ group4 200.200.200.9 200.200.200.10 netmask 255.255.255.248
R4(config)#ip nat inside source list 1 pool group4
```

Figure 302 To configure dynamic NAT

CHAPTER 6: TESTING

6.1 Introduction

All the services that had been done have different methods and ways of testing. This section will show how to test all the services that have been configured and setup. The testing also is to ensure the functioning of the service are successfully up and running. Testing is important to isolate each part of the program and show that the individual parts are correct. Testing is the practice of making objective judgments regarding the extent to which the system (device) meets, exceeds or fails to meet stated objectives. Moreover, testing is about managing risk. A good testing program is when it can be finding errors so it is important to find out errors and try to modify for the best performance.

6.2 Services Testing

6.2.1 DNS Testing

Step 1: Click start and then open Windows PowerShell

Step 2: Type nslookup, and then press enter. There will be shown list of servers with their own DNS.

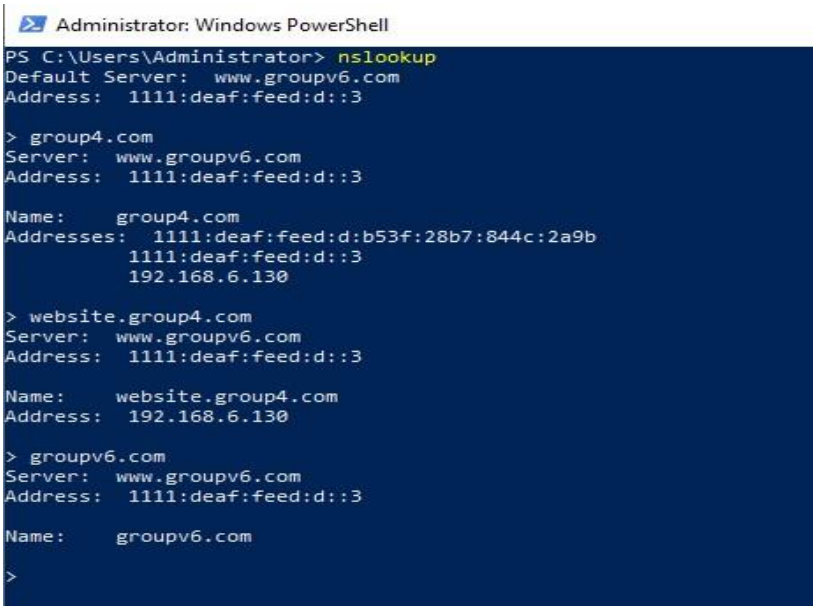


Figure 303 nslookup for group4.com

6.2.2 DHCP IPv4 and IPv6 Testing

Testing requirement.

• Hardware: Windows Server Workstation and Client Workstation

• Software: Windows Server 2019 and Windows 10

6.2.2.1 IPv4 Testing

1. Firstly, check if the Client PC get the IP address by opening the command prompt in Client PC and type ipconfig /all. This command will show all the available network interface with their corresponding IP address.

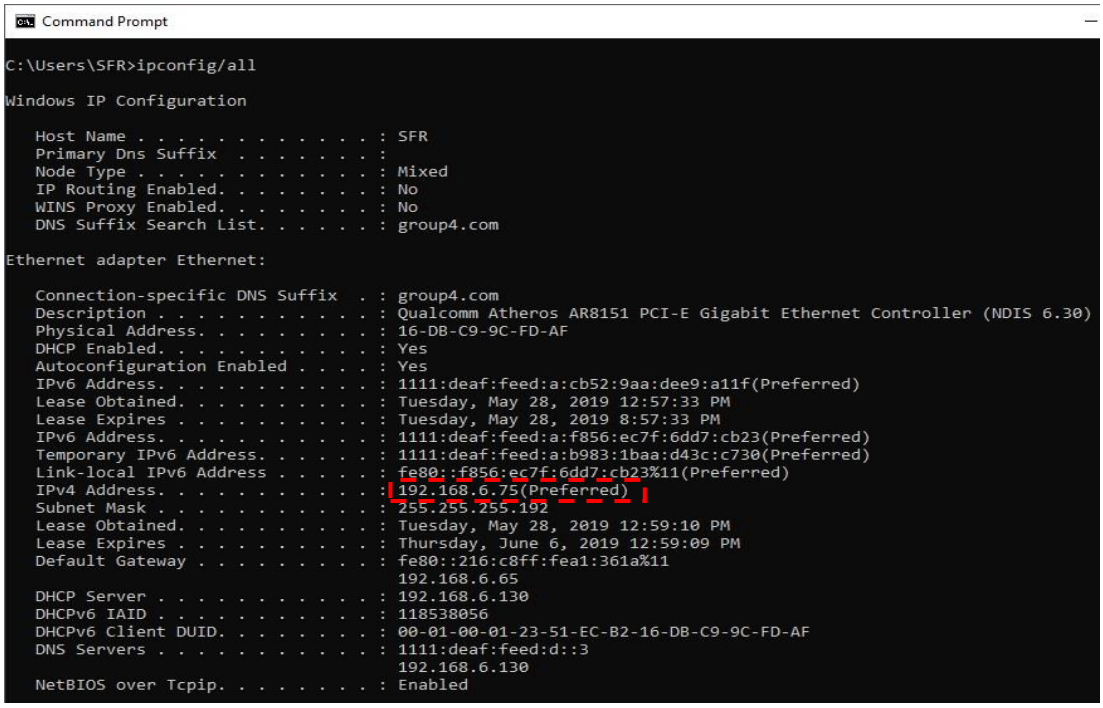


Figure 304 ipconfig IPv4

2. Open the Windows Server and open the DHCP services. Find IPv4>Scope>Scope Lease. Check if the IP address that lease in Windows Server is same with the Client PC.

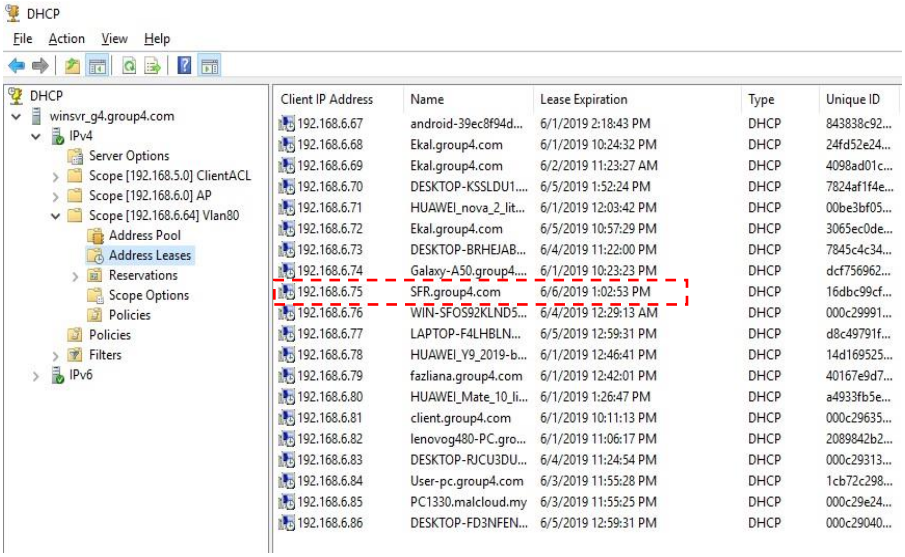


Figure 305 Address Lease IPv4

6.2.2.2 IPv6 Testing

1. Firstly, check if the Client PC get the IP address by opening the command prompt in Client PC and type ipconfig/all. This command will show all the available network interface with their corresponding IP address.

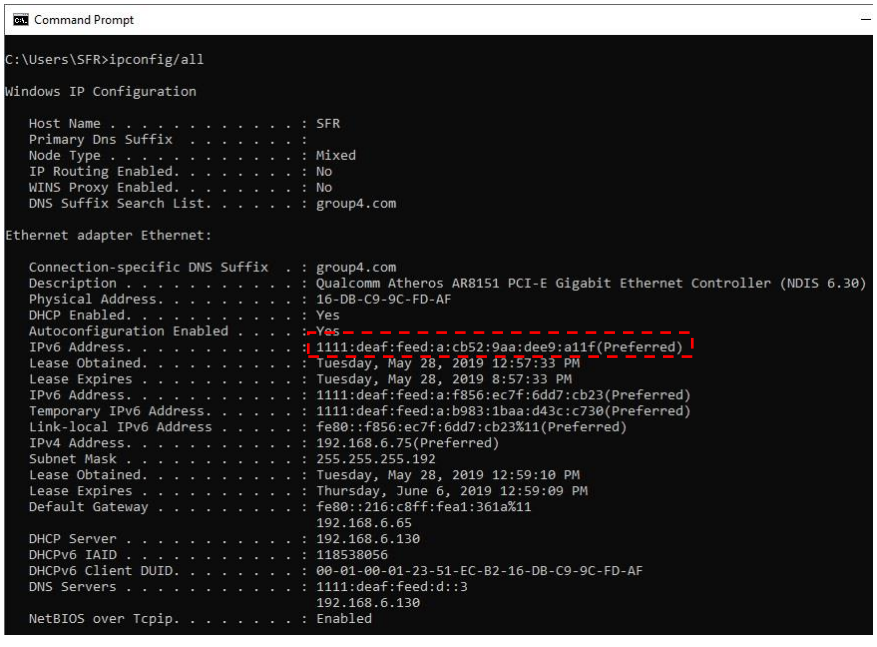


Figure 306 ipconfig IPv6

2. Open the Windows Server and open the DHCP services. Find IPv6 > Scope > Scope Lease. Check if the IP address that lease in Windows Server is same with the Client PC.

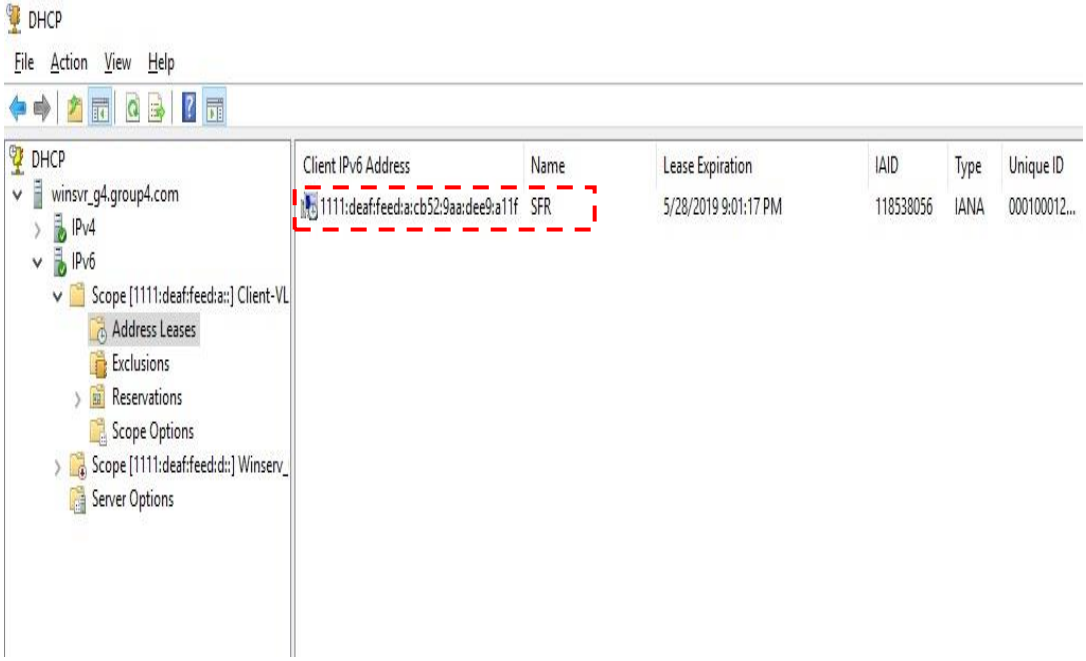


Figure 307 Address Lease IPv6

6.2.3 IPv6 Web and IPv6 Tunneling Testing

Step1: Browse http://www.groupv6.com

Figure 308 ipv6 web

6.2.3.1 Testing on neighbor

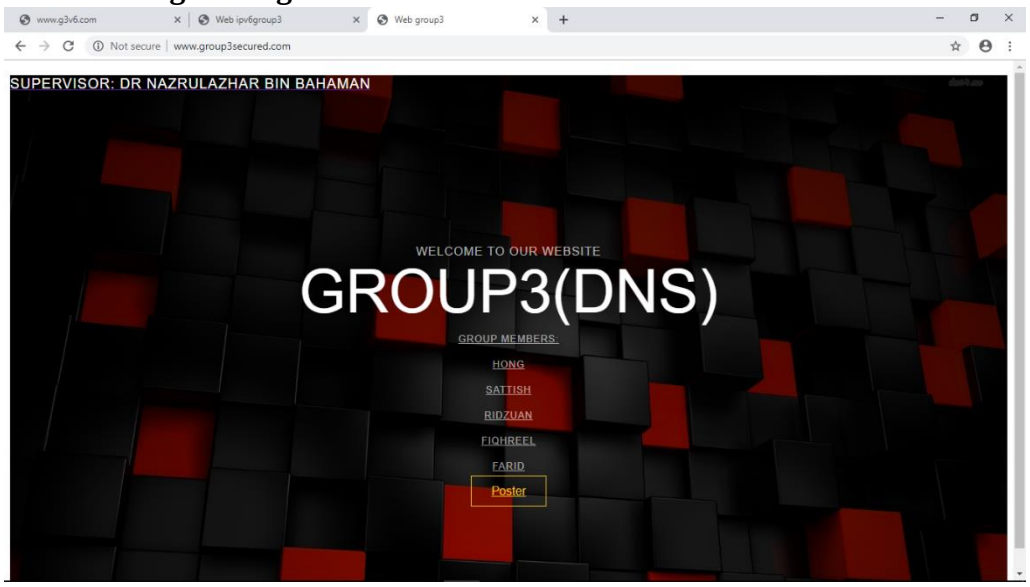


Figure 309 neighbour ipv4 web

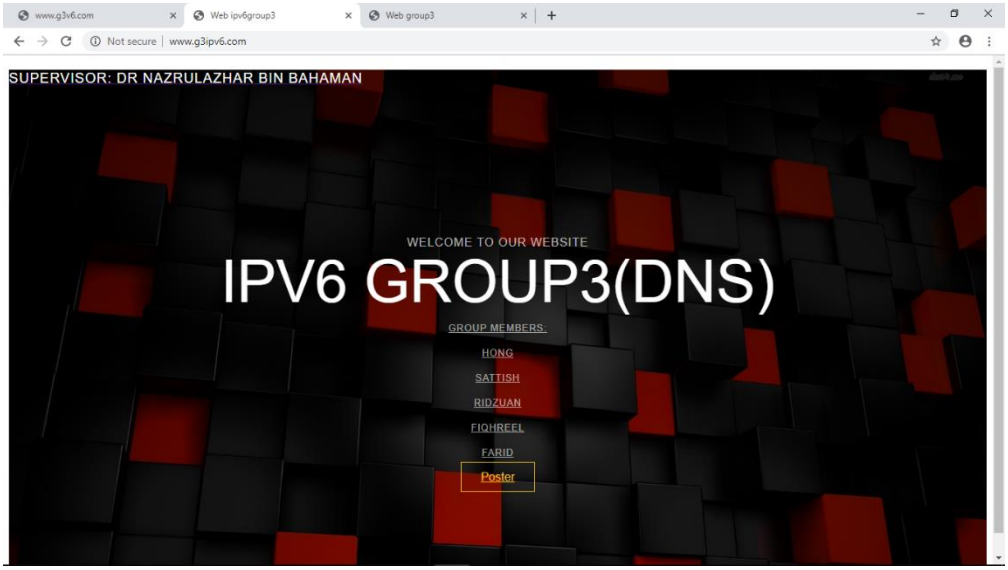


Figure 310 neighbour ipv6 web

6.2.4 Web, SSL and Virtual Hosting Testing

6.2.4.1 Web

Step1: Browse http://www.group4.com

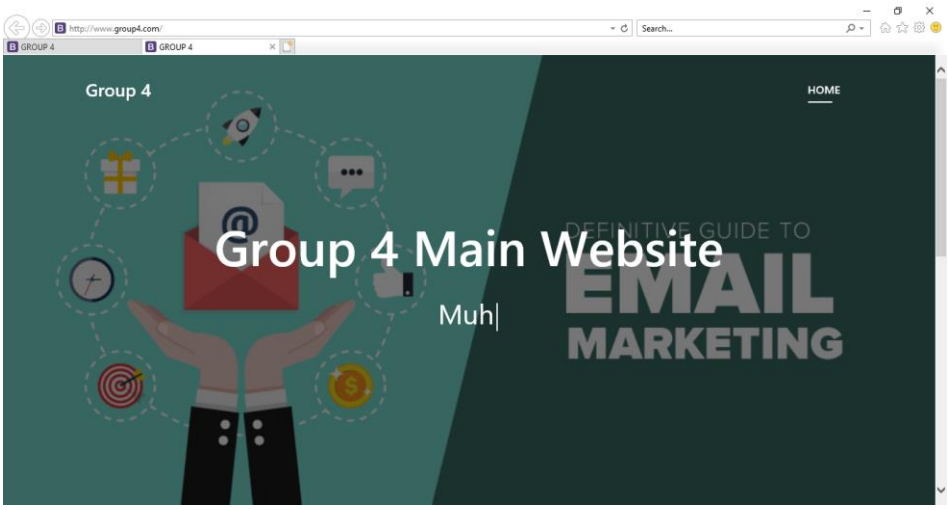


Figure 311 Main website (http://www.group4.com)

6.2.4.2 Secure Socket Layer (SSL)

Step2: Browse https://www.group4.com

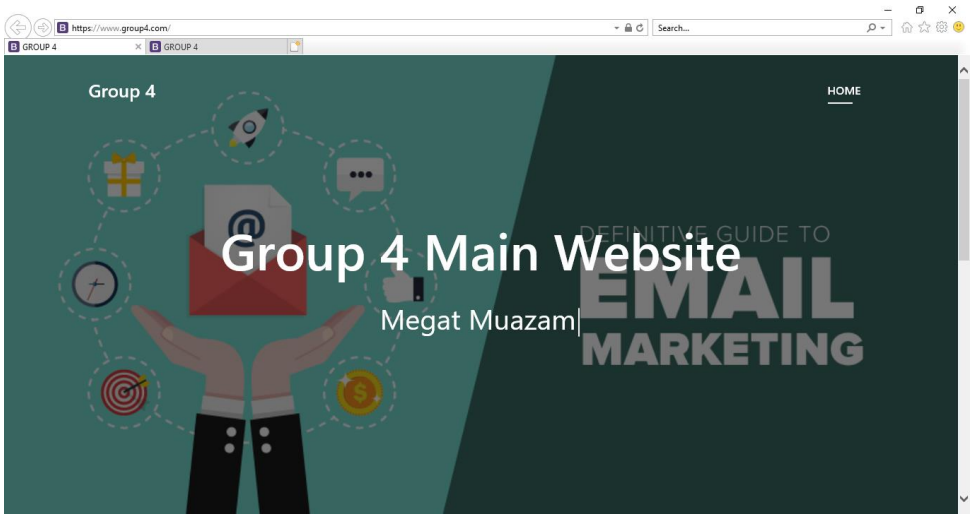


Figure 312 Main website (https://www.group4.com)

6.2.4.3 Virtual Hosting

Step3: Browse http://website.group4.com

Figure 313 Second webpage using virtual hosting (http://website.group4.com)

6.2.5 IPSec Site-To-Site Tunneling Testing

Step 1 : Test the connection by ping the private ip address of the neigbour using command “ping <neighbour ip_address> source <router ip_address>”

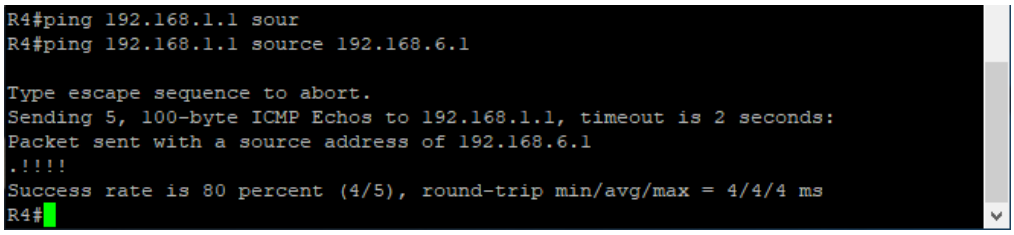


Figure 314 Ping ip address neighbor from router

Step 2 : Test the connection by ping the public ip address of the neigbour using command “ping <neighbour ip_address> source <router ip_address>”

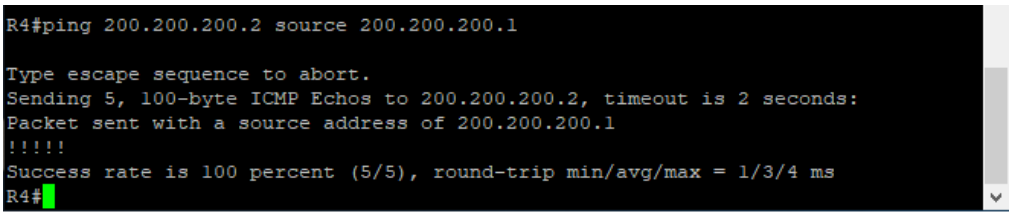


Figure 315 Ping neighbour public ip address

Step 3 : Show the ipsec mapping by using command "show crypto session” .

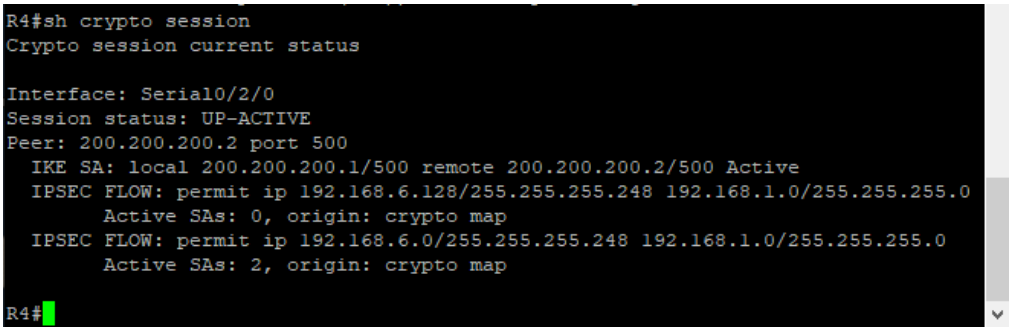


Figure 316 Ipsec mapping table

6.2.6 Active Directory (AD) Testing

Step 1 : Open the Vmware Workstation that been installed with client windows. Go to control panel > System and Security > System > Change Settings

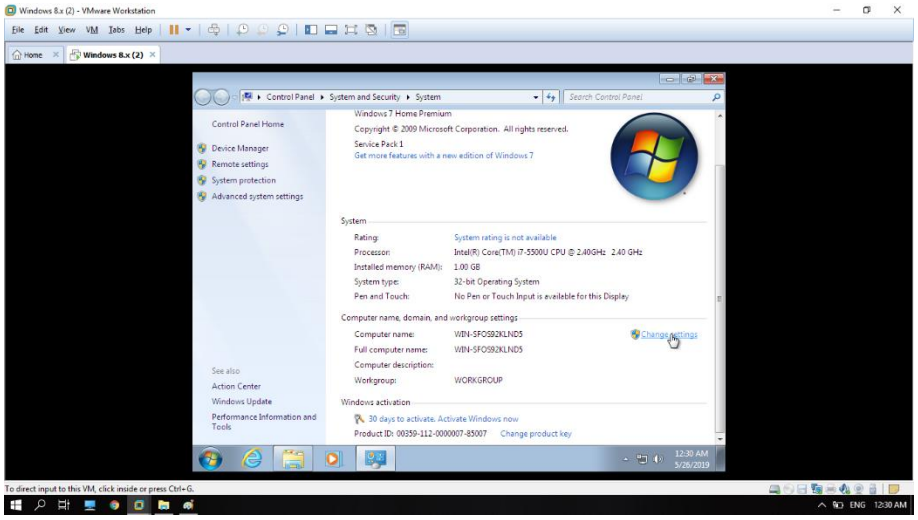


Figure 317 Change Setting Window

Step 2 : Next, on the system properties, click Change > Domain > Enter your domain name.

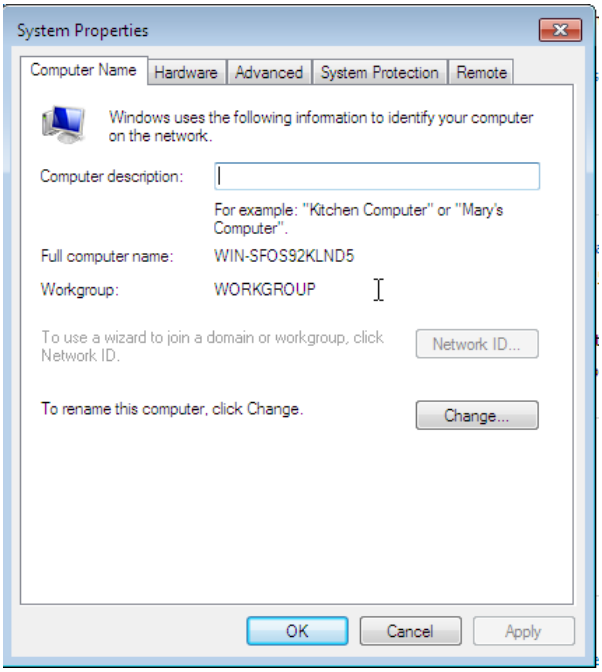


Figure 318 Change System Properties Panel

Step 3 : Login using the user account that have been created in the Active Directory Users and Computers.

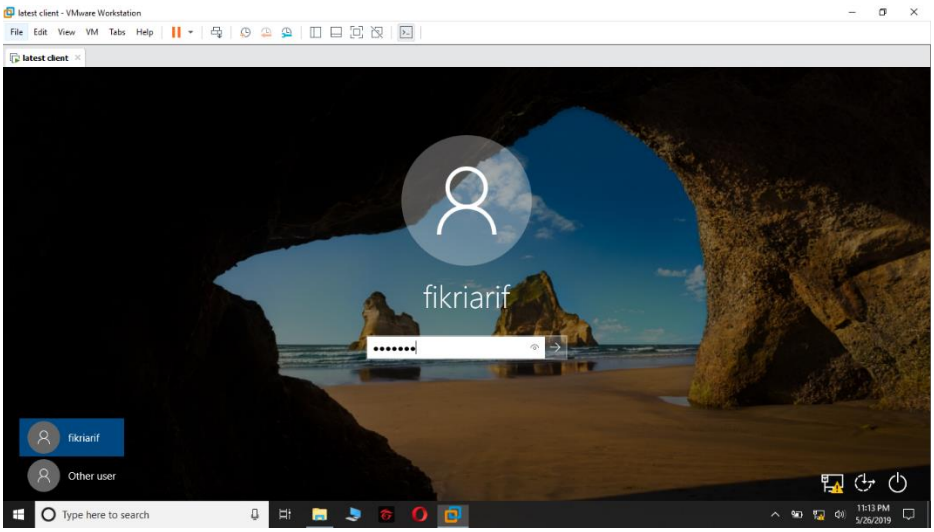


Figure 319 Login using user account

Step 4 : Client will receive the DHCP ip address in the client vlan ip address range.

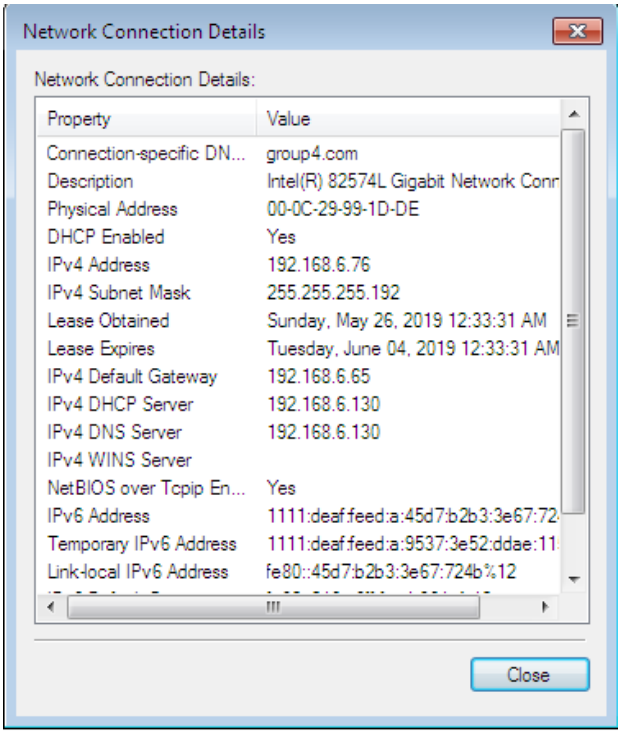


Figure 320 Client DHCP address

Step 5 : Client will able to open and access to the group Ipv4 and Ipv6 website.

Figure 321 Client have access to group website

Step 6 : Client also will able to open and have access to the neighbour website that we have configured tunelling.

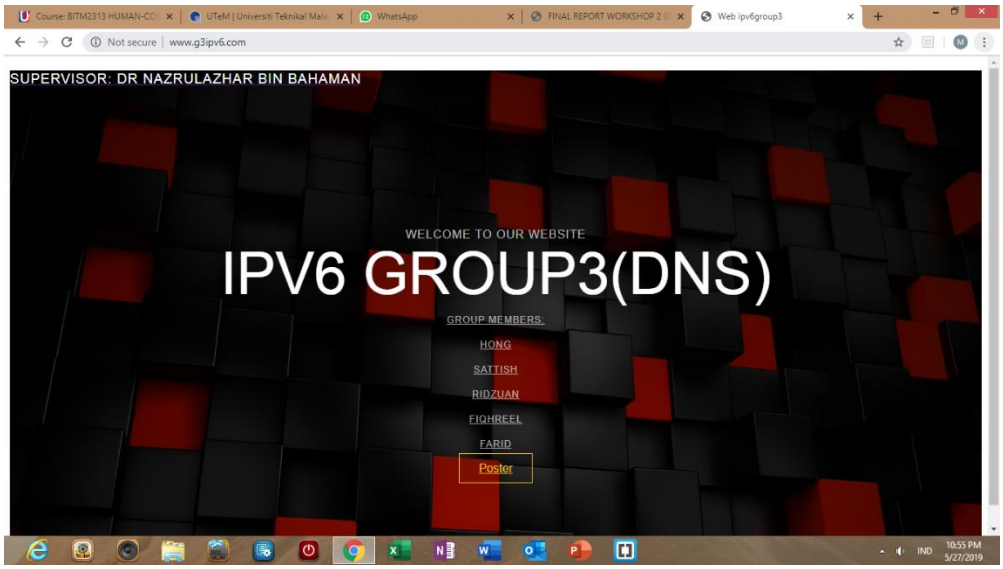


Figure 322 Neighbour website

6.2.7 Group Policy Management (GPO) Testing

Step 1 : Login as client using the user account that have been created in the Active Directory Users and Computer

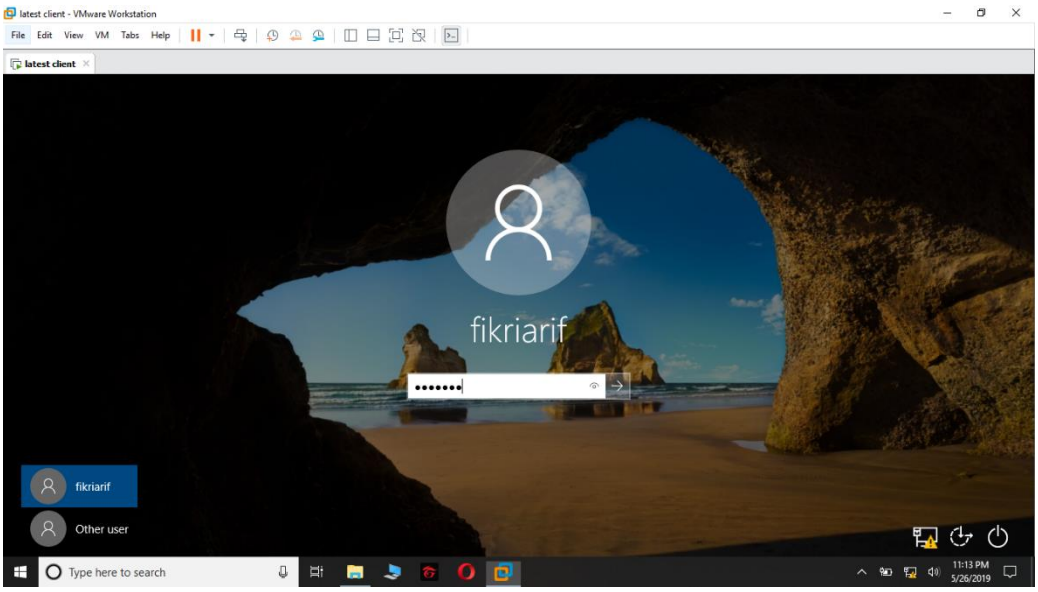


Figure 323 Login as client

Step 2 : After suceed login into the AD account, client will receive this message and this message is the first GPO policies that named as “banner”

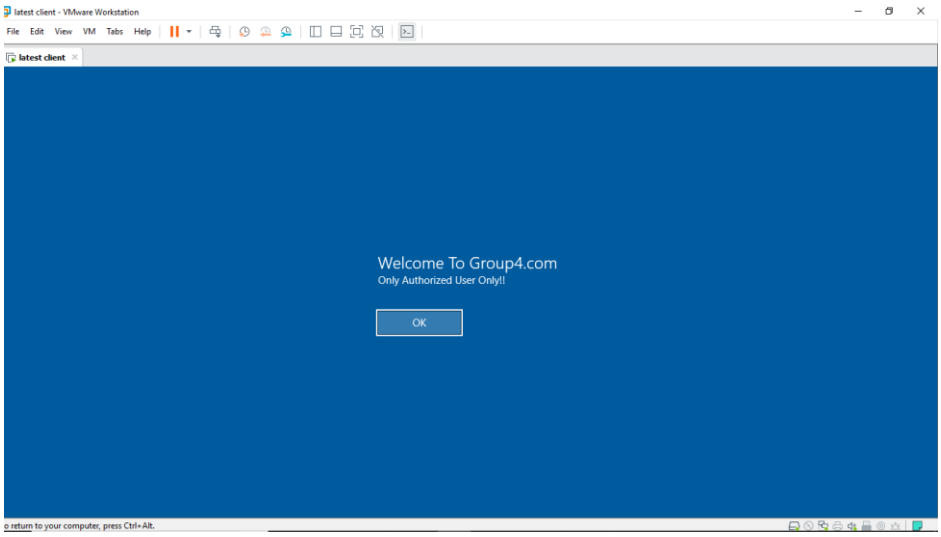


Figure 324 Client will receive message after login

Step 3 : Next, on the client “This PC” there will be a disk for the file sharing and this is defined by the second GPO policies that is “drive map”.

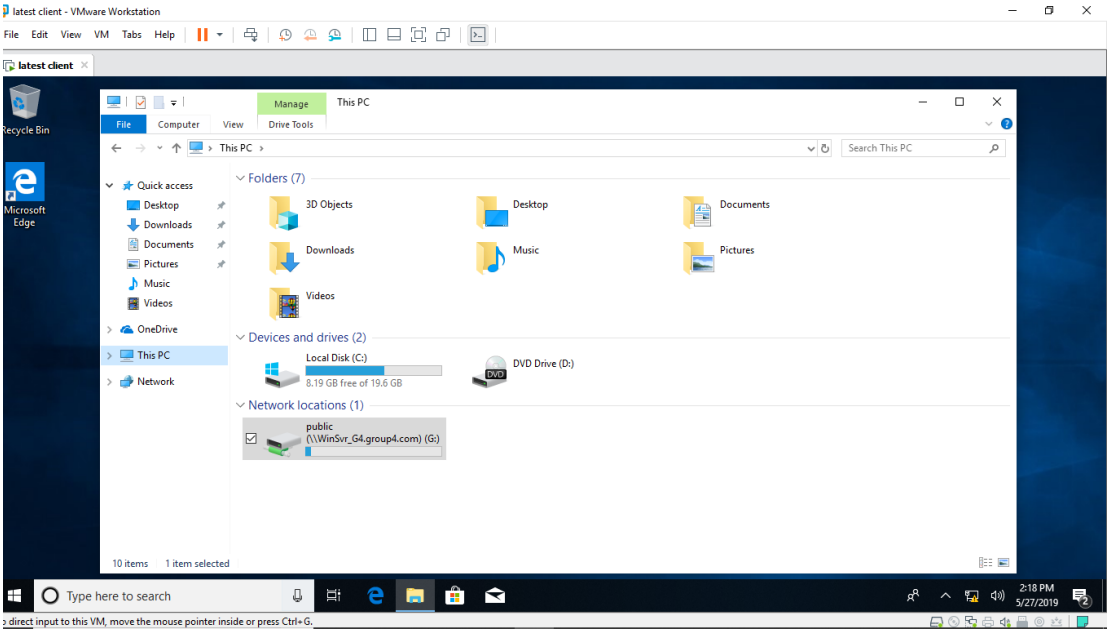


Figure 325 File sharing disk on the client “This PC”

Step 4 : Next, client will able to create a folder and view any folder in the file sharing disk.

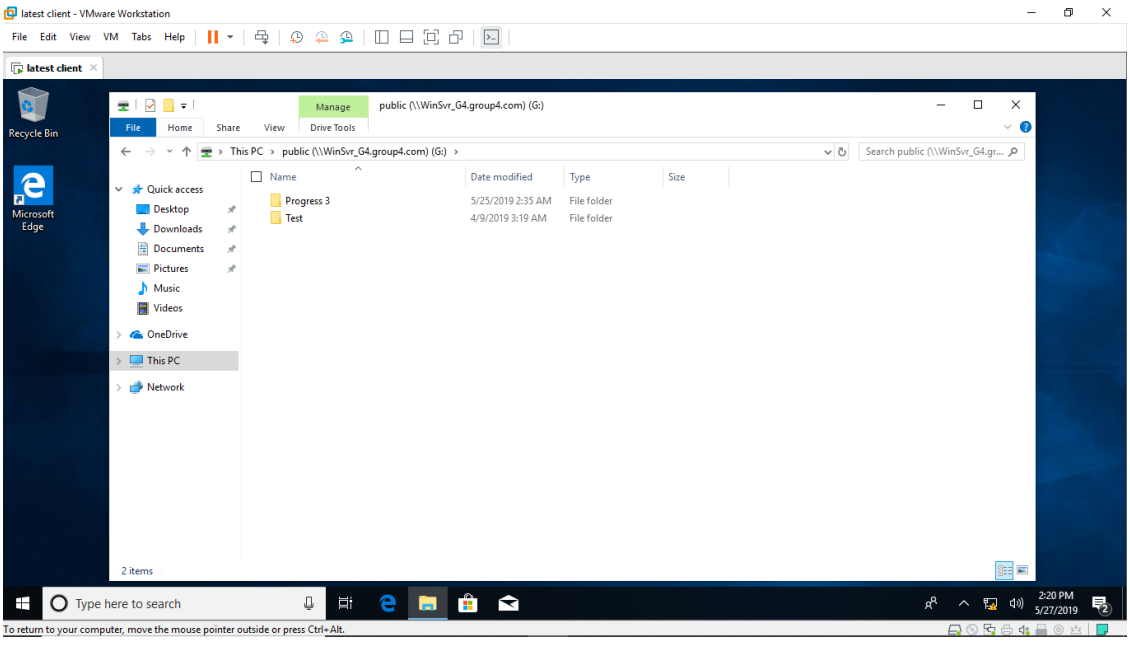


Figure 326 Client can view and crate folder in the file sharing

6.2.8 Server Virtualization Testing

Step1: User can access files from actual Windows Server to virtual machine

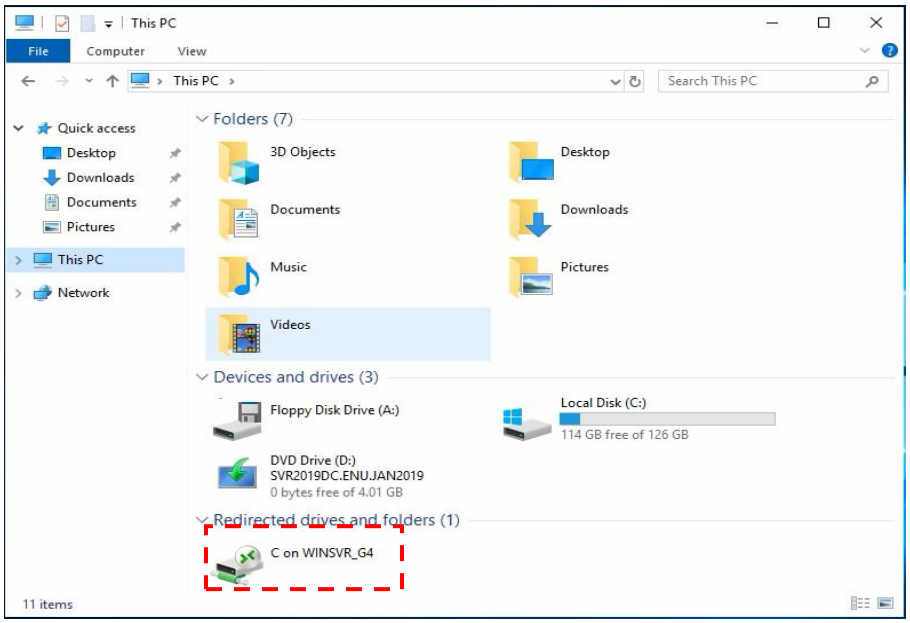


Figure 327 Files from Windows Server

6.2.9 AAA with Radius with Radius Testing

Step 1: Type a show run at router. To check the aaa configuration.

```
!
aaa new-model
!
!
aaa group server radius WinSvr_G4
 server-private 192.168.6.130 auth-port 1812 acct-port 1813 key abc@123
!
aaa authentication login default group WinSvr_G4
aaa authentication login console local
aaa authorization exec default group WinSvr_G4
aaa authorization exec console local
!
aaa session-id common
ip cef
!
```

Figure 328 Show run and check AAA configuration

Step 2: Open the putty. Then select Serial port and click button Open.

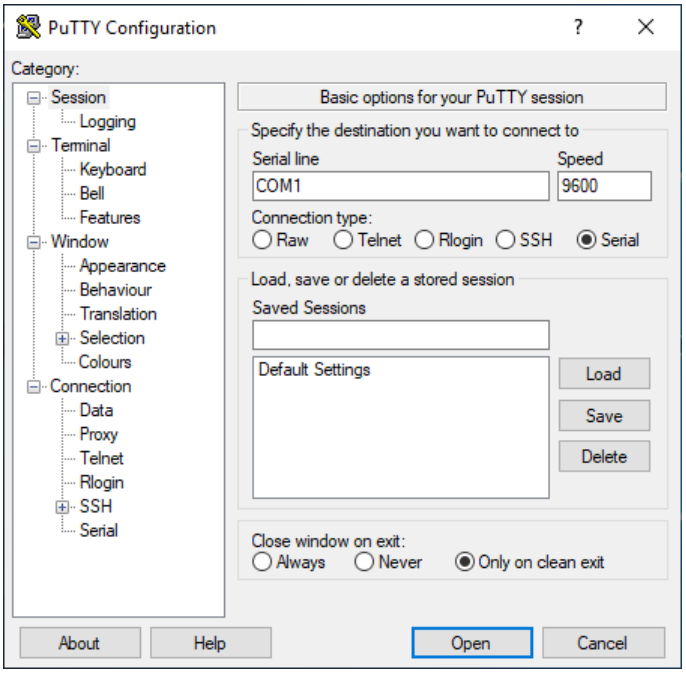


Figure 329 Open the putty and select the Serial port

After click button Open putty. Enter username and password admin. To success login the router.

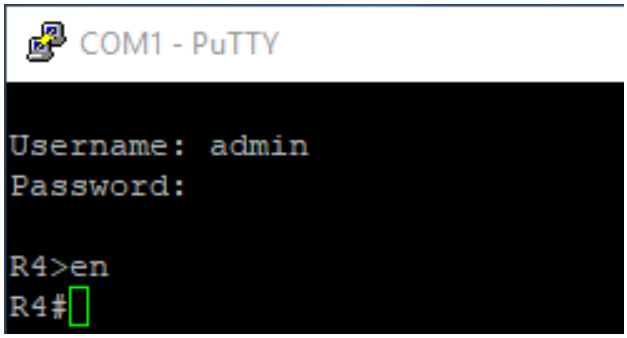


Figure 330 Enter the username admin and password for admin

Step 3: Open the putty. Then select SSH port and enter the IP address gateway. After finish Click button Open. .

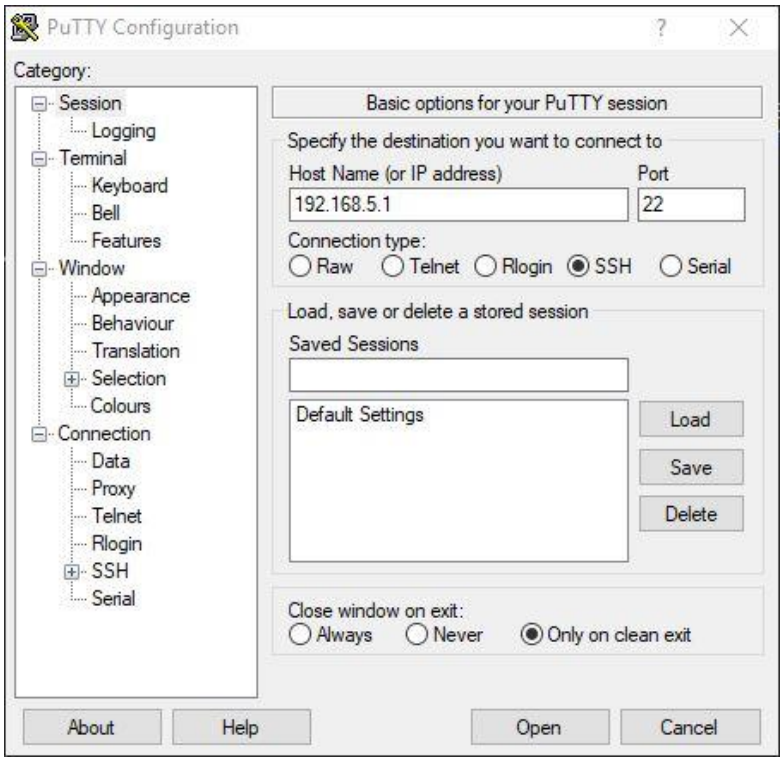


Figure 331 Open the putty and select the SSH port

Step 4: The AAA authentication can access each of user. This team have five members in per group and each user can access the username and password. To success login the router.

Figure 332 Enter the username admin and password for aqilah

Figure 333 Enter the username admin and password for fandi

Figure 334 Enter the username admin and password for fikriarif

Figure 335 Enter the username admin and password for haikal

Figure 336 Enter the username admin and password for megat95

Step 5: After that, open the Event View (Local) > Custom Views > Server Roles > Network Policy and Access Services. Then, look right hand site have many data log user and users login router using port ssh.

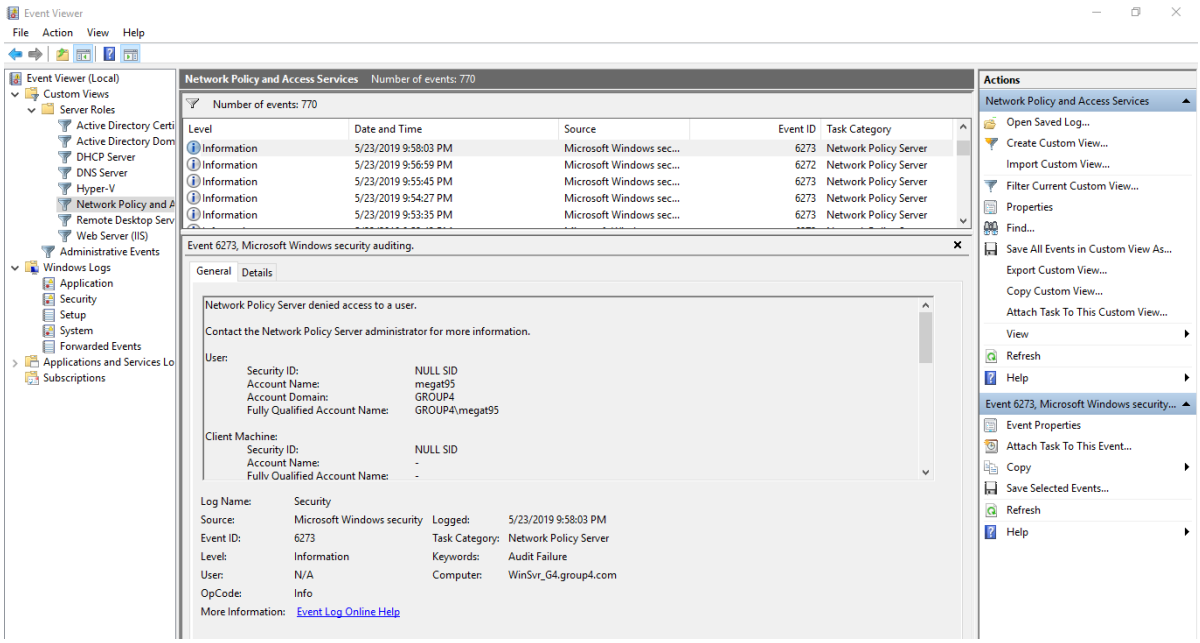


Figure 337 Open the Event View (Local)

Show data log the account name and account domain from user login router using ssh.

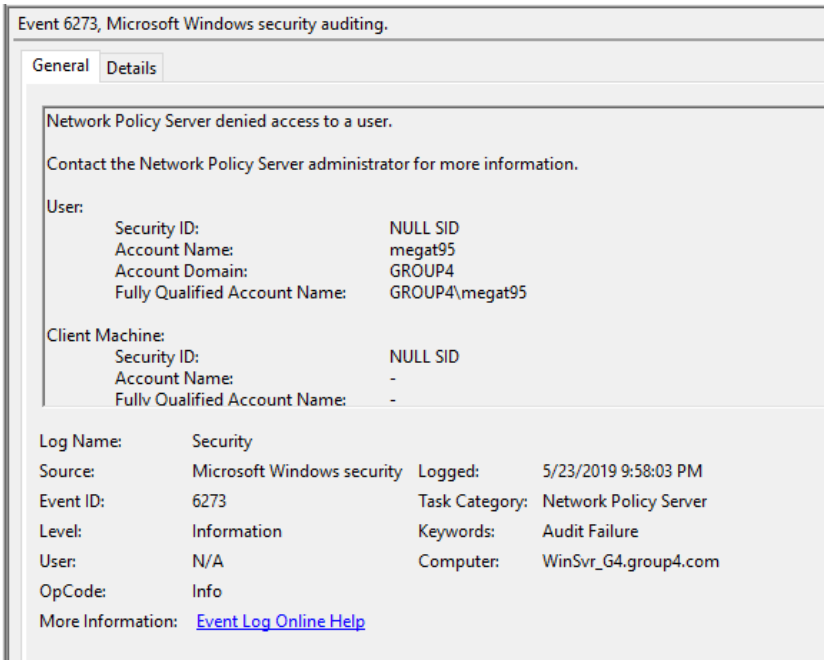


Figure 338 Show the data log from user login router

6.2.10 Secure FTP Testing

Step 1: Firstly, go to terminal Ubuntu. Type a ftp –p 192.168.6.138 (IP address local host). Users other than "fikri" should fail to connect: Next, we'll try connecting as our sudo user. They, too, should be denied access, and it should happen before they're allowed to enter their password.

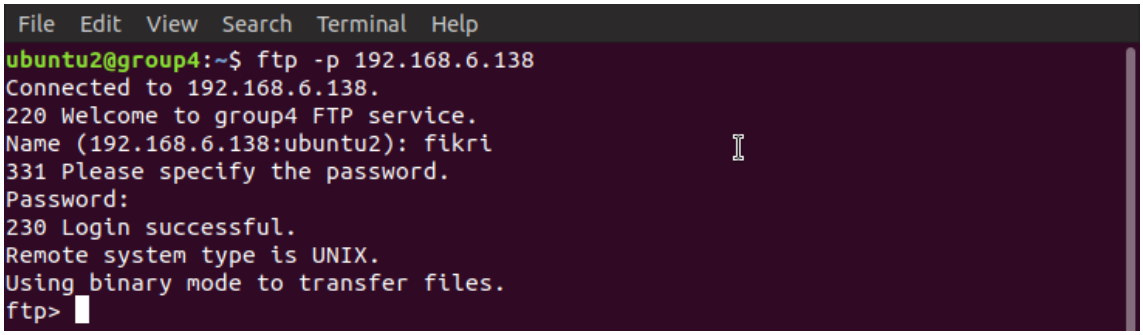


Figure 339 ftp local host user in Ubuntu

Step 2: Enter the IP address local host to connect file "fikri" user.

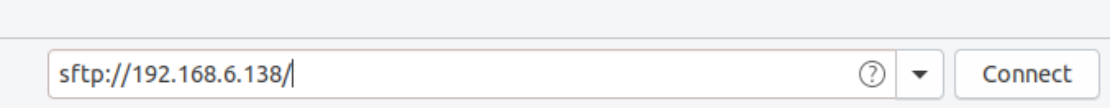


Figure 340 Enter the IP address local host sftp with IP local host

After enter the IP address local host. Enter the username and password user.

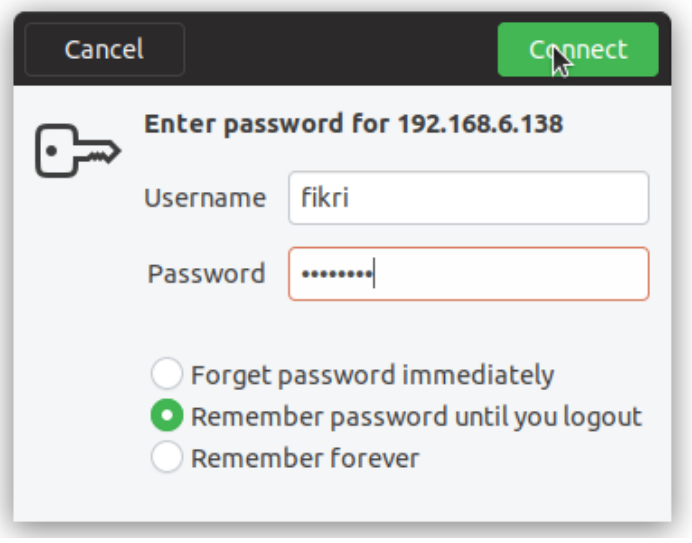


Figure 341 Enter the username and password

Step 3: After enter the username and password from user “fikri”. Connect and go to file location “fikri” user directory.

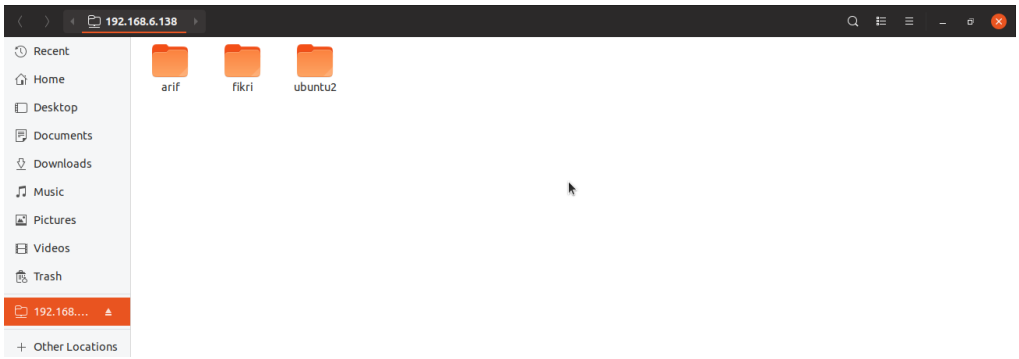


Figure 342 User local host directory file from 192.168.6.138

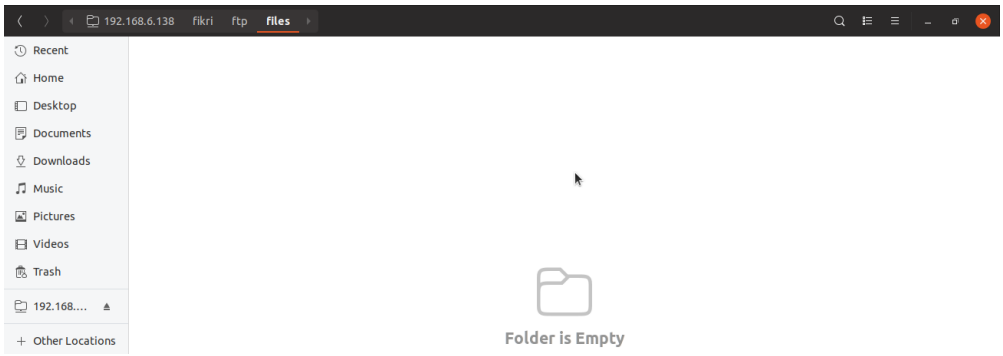


Figure 343 User local host directory file 192.168.6.138/fikri/ftp/files

Step 4: Open the third-party FileZilla to transfer the file from client to server host.

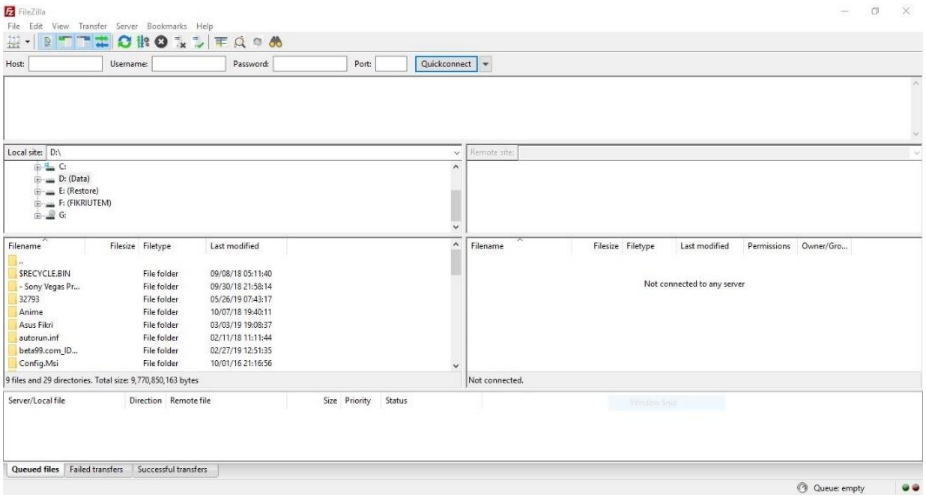


Figure 344 Open the FileZilla

Step 5: After enter the IP address local host, username and password user and port number 22. Click button Connect then continue going to right side have file location from host server.

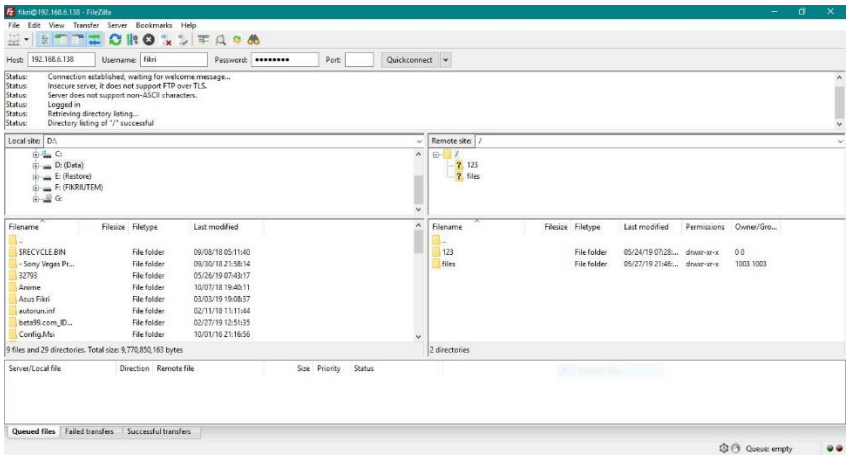


Figure 345 Enter the IP address, username and password

Step 6: Then, the file SFTP done.txt from the client to host server send the file is successful.

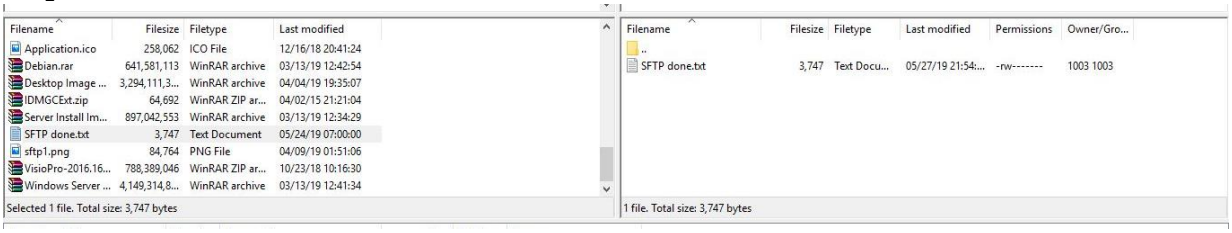


Figure 346 File SFTPdone.txt send to host server

Step 7: Show the file SFTP done.txt send to host serve done successful.

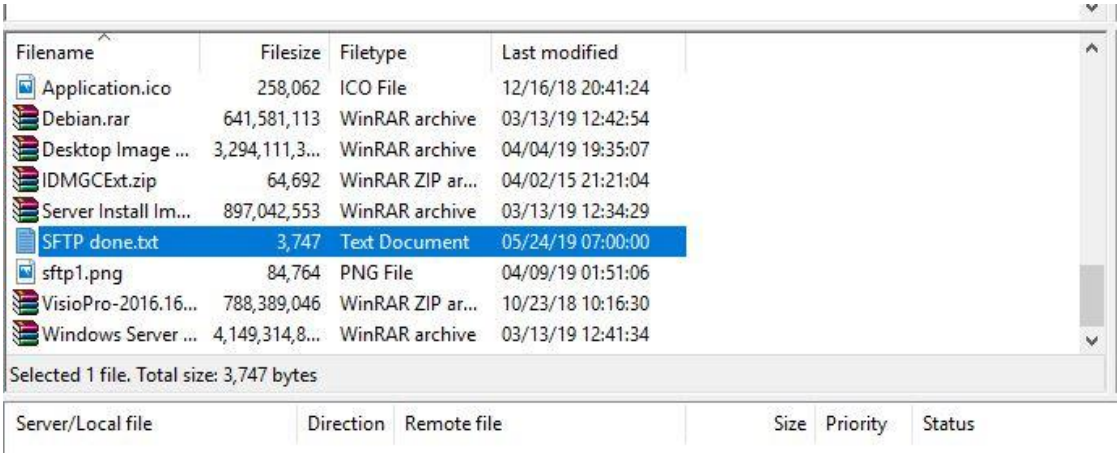


Figure 347 File SFTPdone.txt from Client

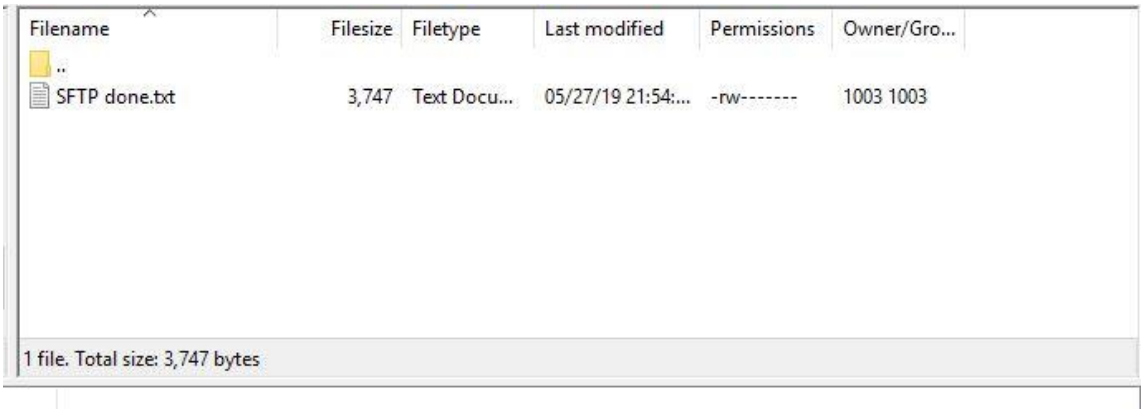


Figure 348 File SFTPdone.txt to host server

Step 8: Check file from host server SFTP file.txt and this file encryption because this file cannot delete and edit.

Figure 349 File SFTPdone.txt at host server Ubuntu.

Step 9: Open the Wireshark to check packet ftp and tcp. Wireshark also can check encryption file is username and password user.

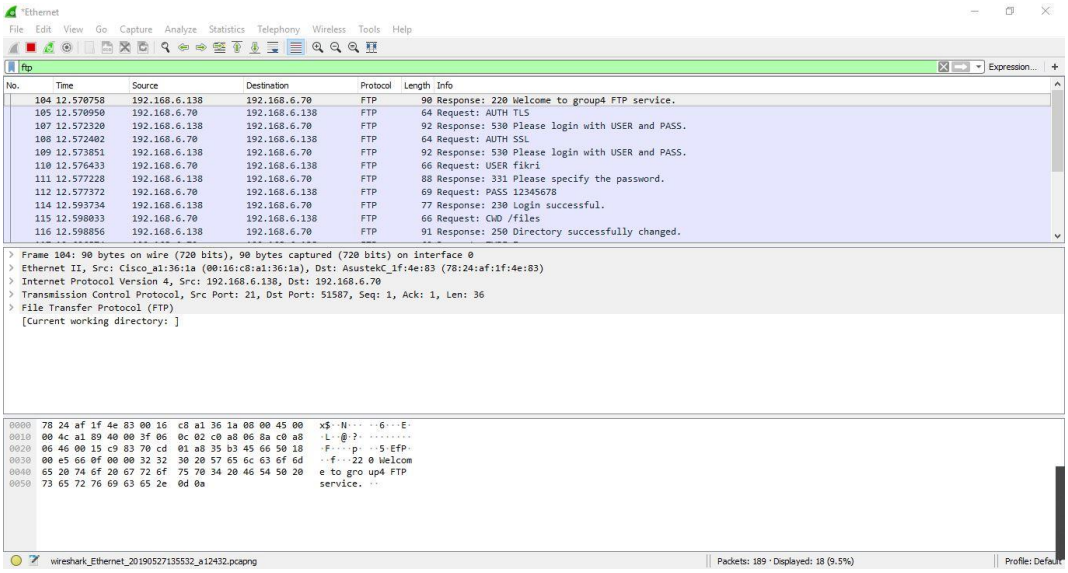


Figure 350 Open the Wireshark

6.2.11 Linux Mail Server Testing

6.2.11.1 Testing using Rainloop

Test the email function with send the message from user that create from Debian server account to another user in the server. From this project, the user that send the message is name haikal that on login account use haikal@group4.com and the receiver is name megat@group4.com. Use the same password as need been set to the two user in the Debian server.

1. Send message from megat account send some massage to haikal account.

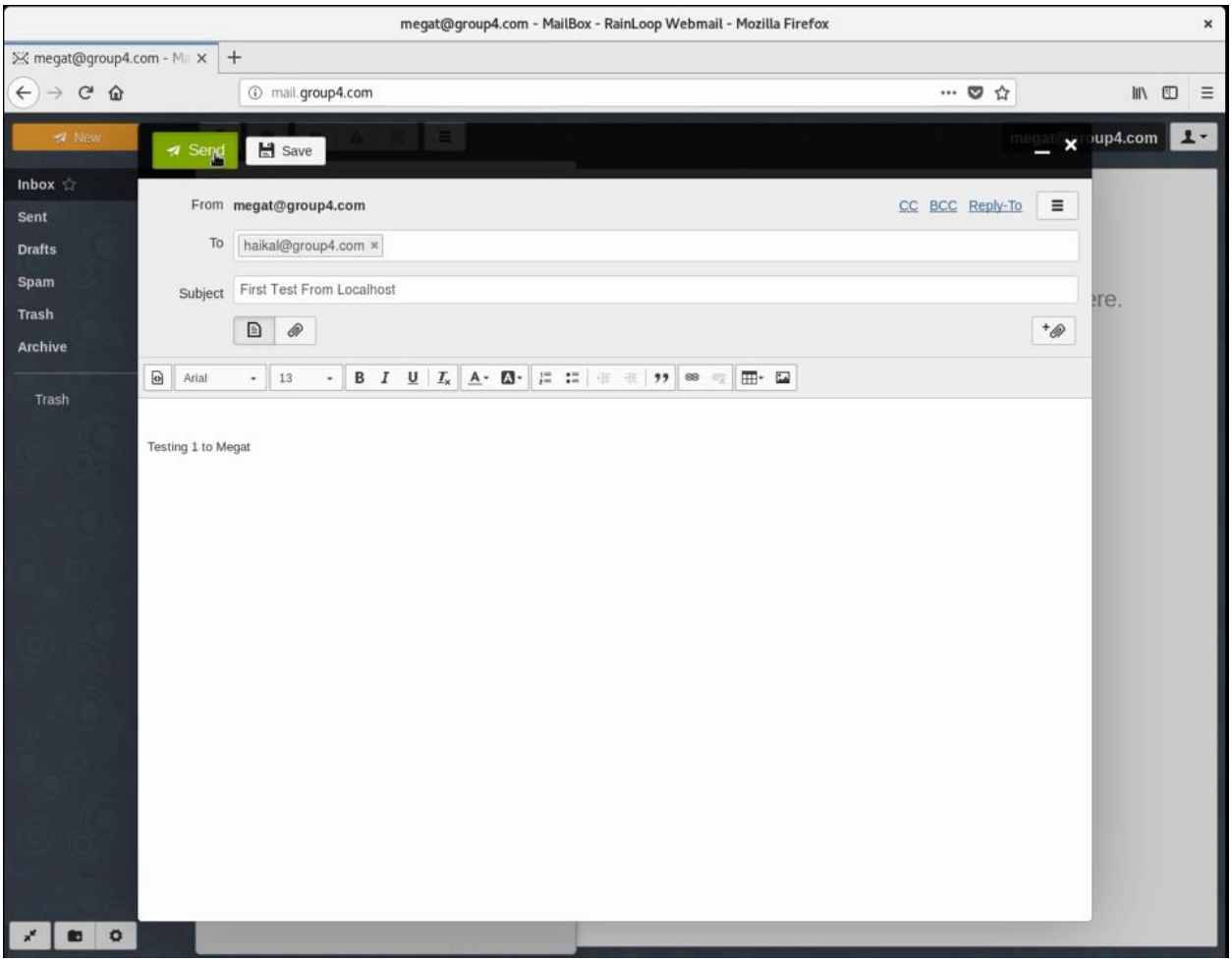


Figure 351 Sending Message

2. Check sent box from megat to confirm the text was send.

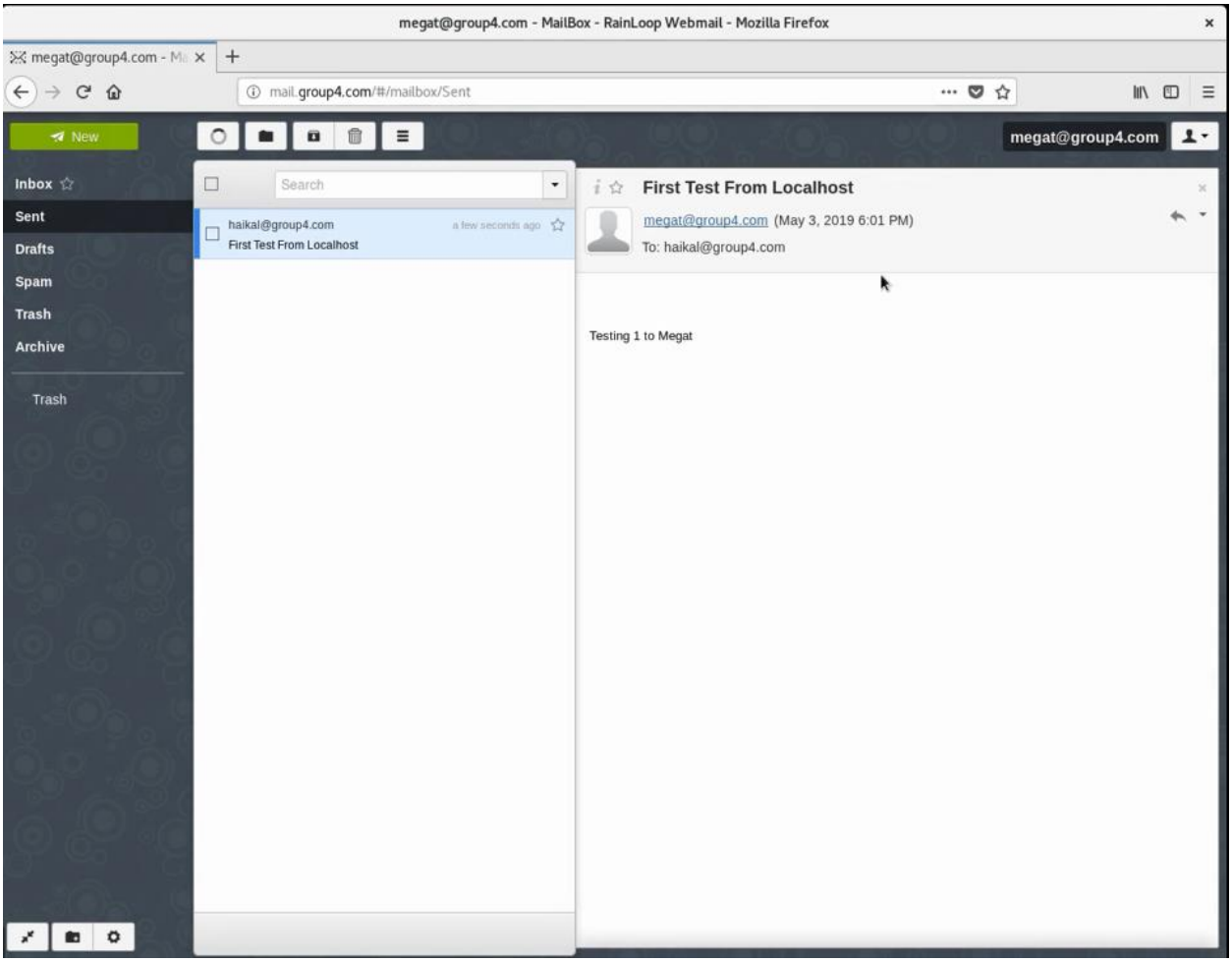


Figure 352 Sent Message

3. Check the email receive on haikal account on mailbox. If the email receives as send from megat account than the testing success.

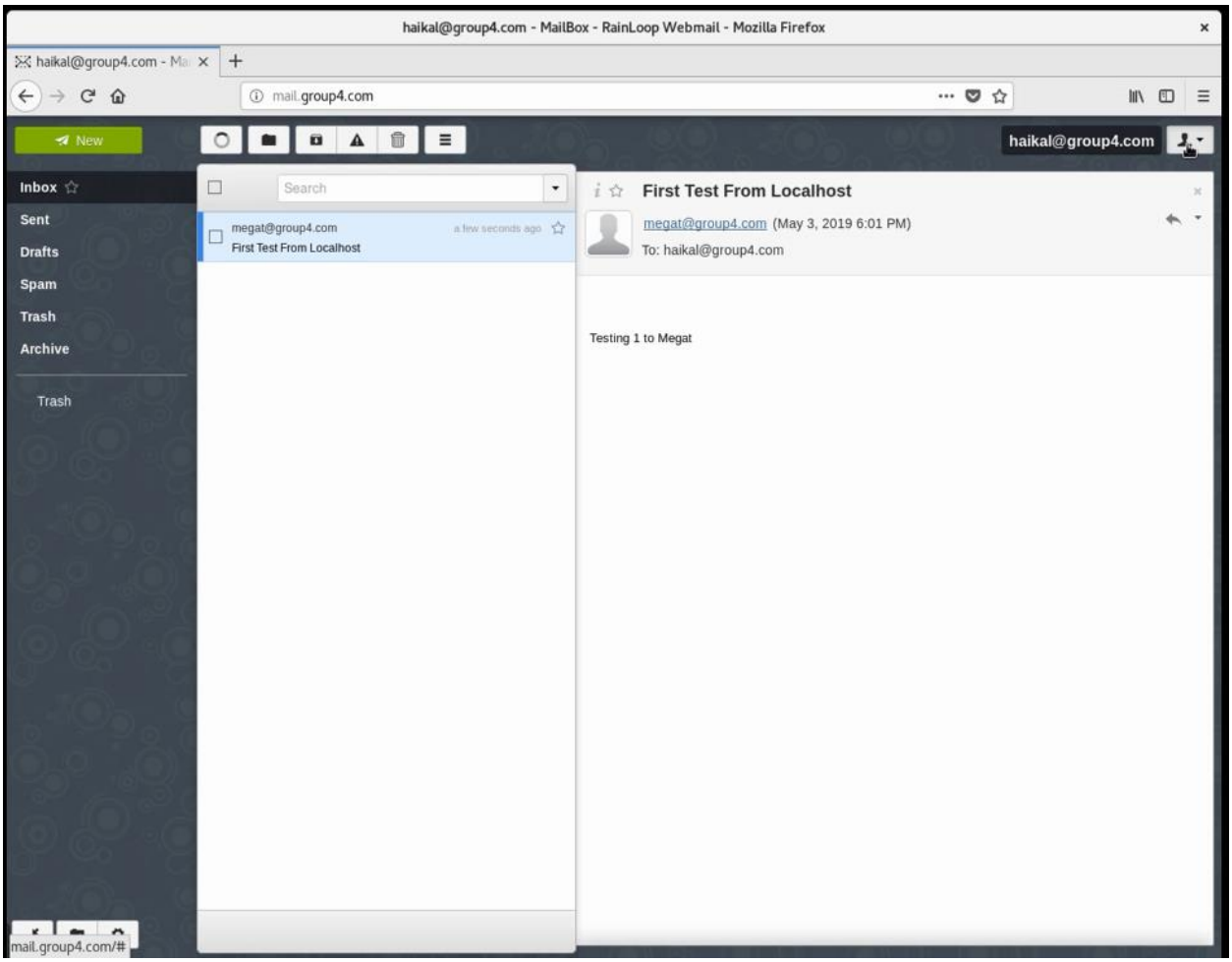


Figure 353 Haikal Inbox

6.2.11.2 Testing using Thunderbird

Test the email function with send the message from user that create from Debian server account to another user in the windows server. From this project, the user that send the message is name haikal that on login account use haikal@group4.com and the receiver is name megat@group4.com. Use the same password as need been set to the two user in the Debian server.

1. Login megat using thunderbird

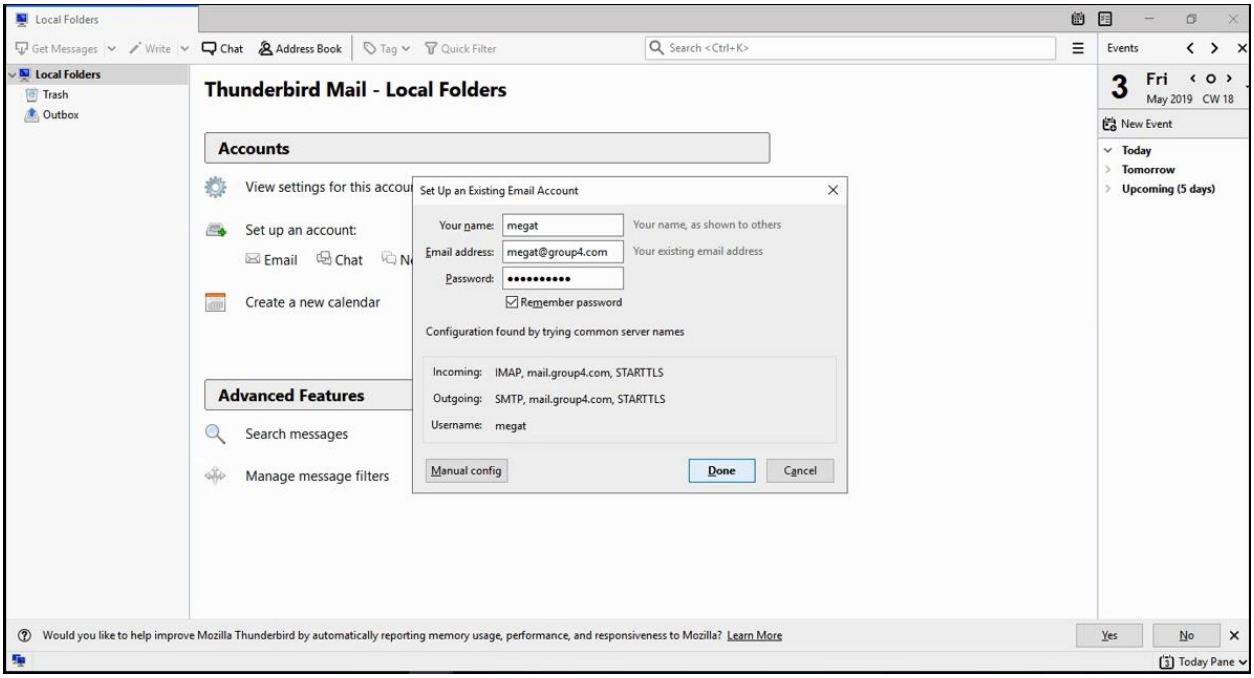


Figure 354 Thunderbird Megat Login

2. Send message from megat account send some massage to haikal account.

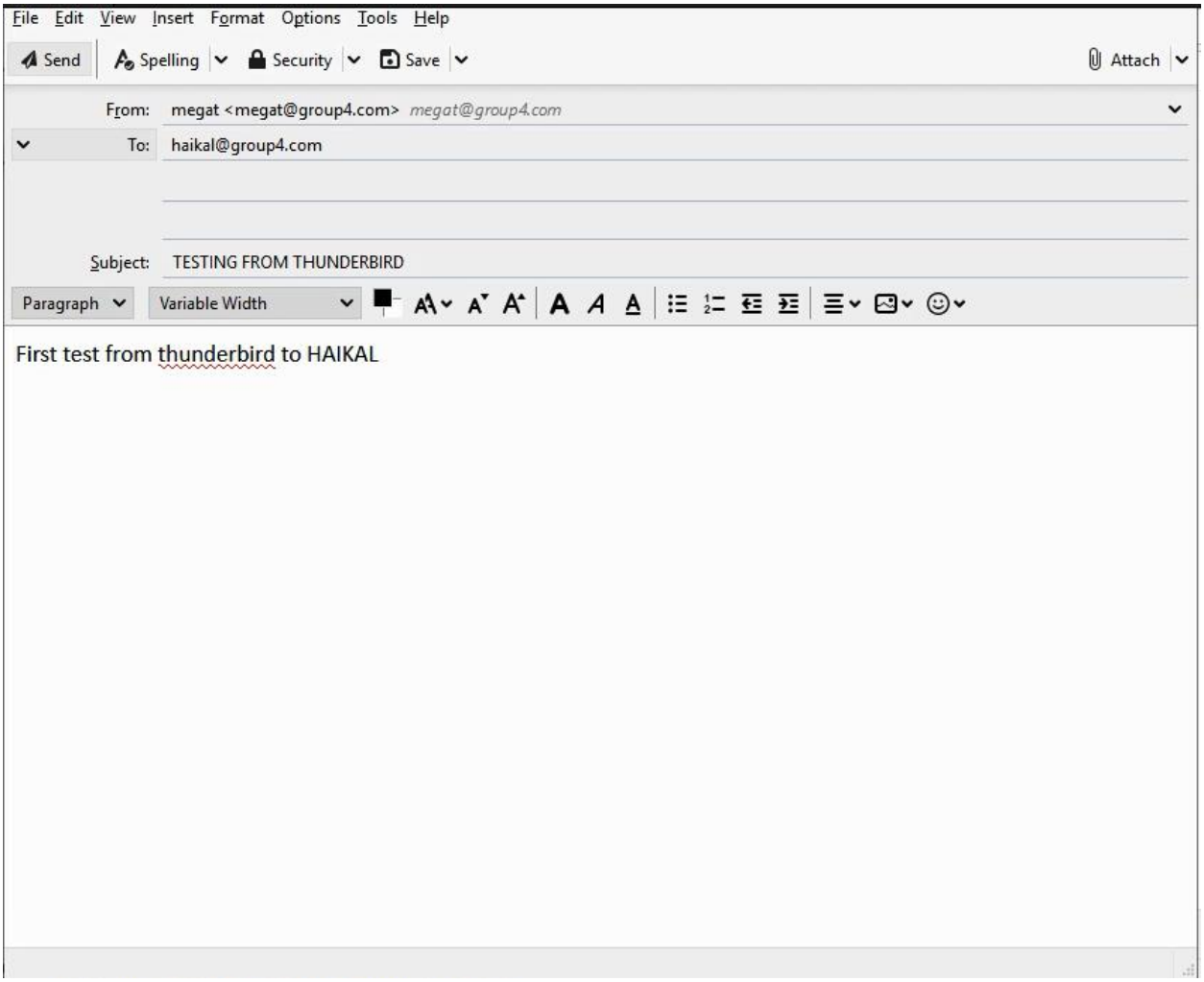


Figure 355 Thunderbird Send Message

3. Check sent box from megat to confirm the text was send.

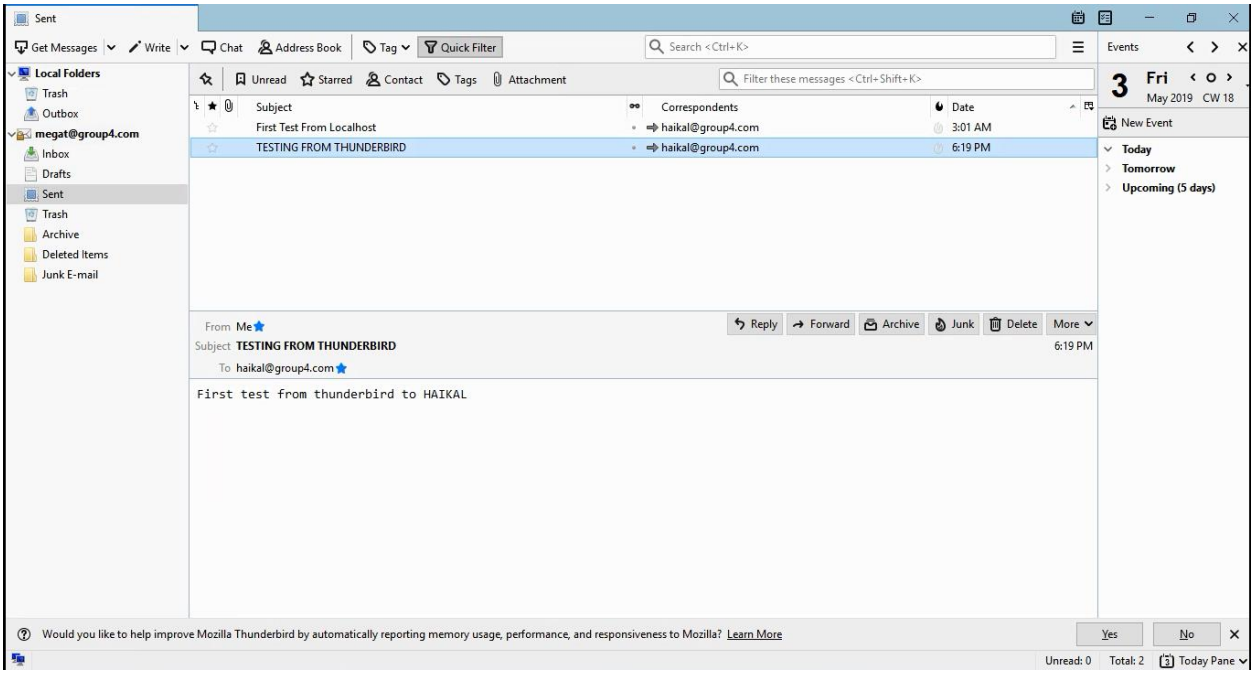


Figure 356 Thunderbird sent message

4. Haikal Login using Thunderbird

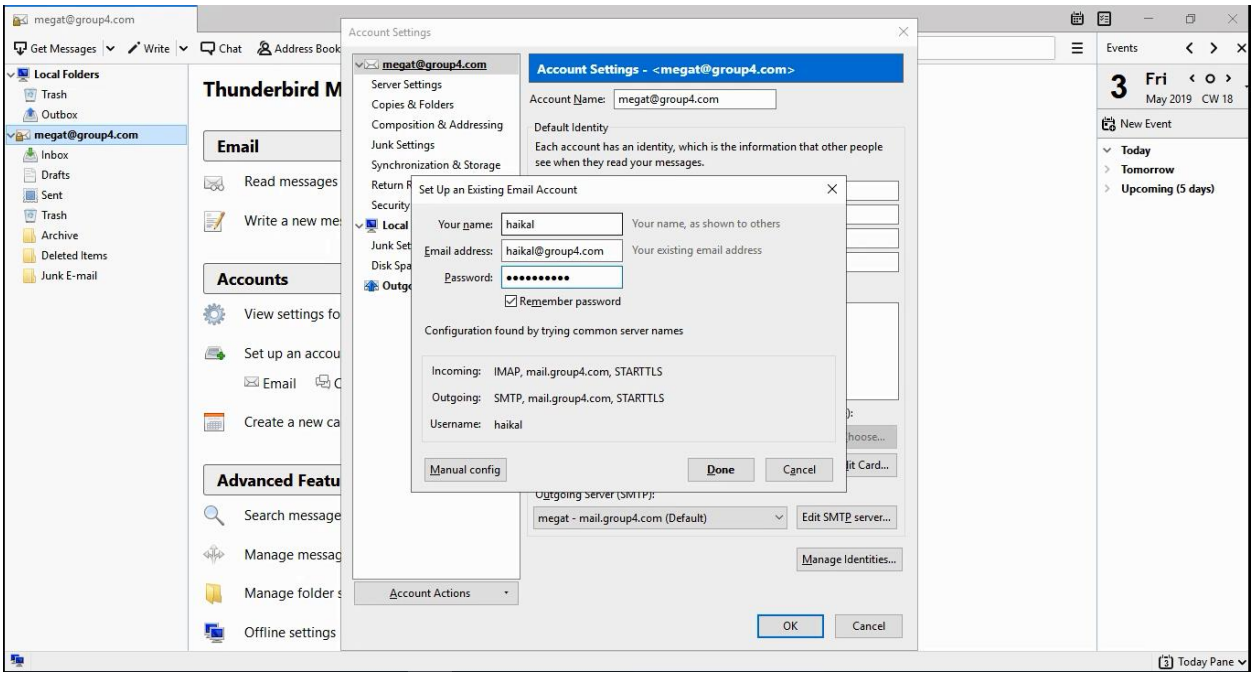


Figure 357 Thunderbird Haikal Login

5. Check the email receive on haikal account on mailbox. If the email receives as send from megat account than the testing using Thunderbird success.

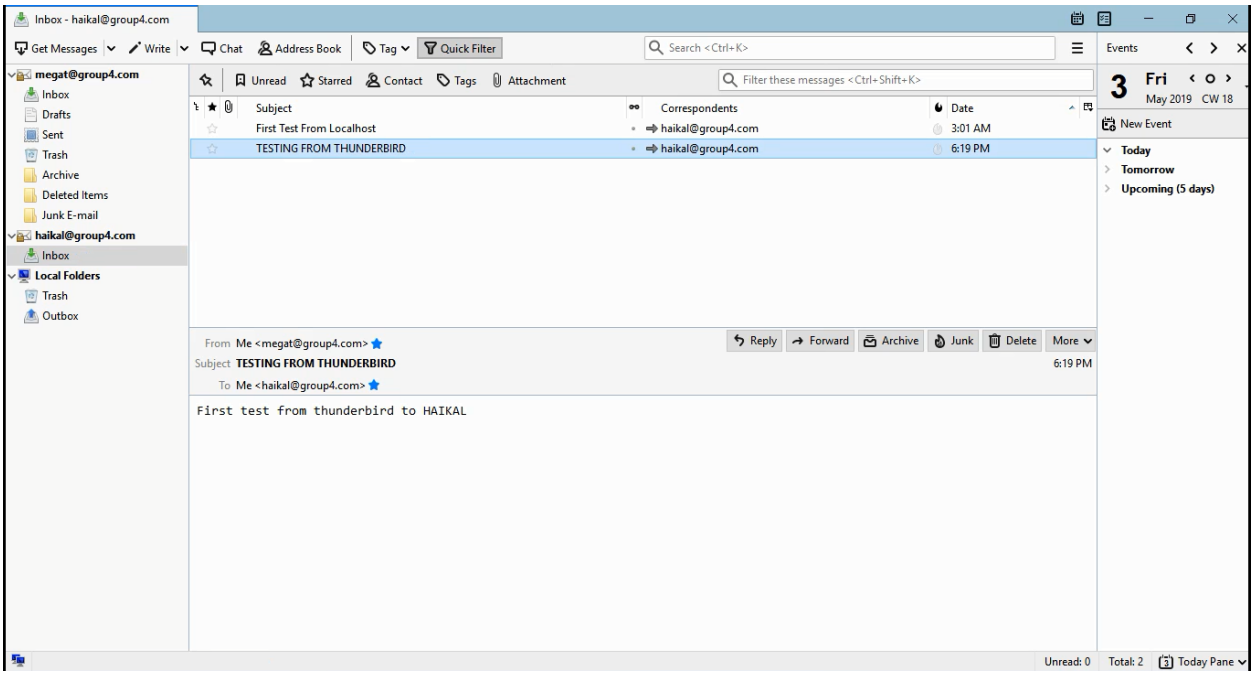


Figure 358 Thunderbird Haikal Inbox.

6.2.12 Network Management System Testing

Step 1: Click Configure Notifications to add email of a user to get notifications through email if any services in any nodes are down

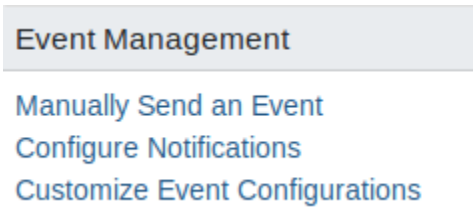


Figure 359 Configure Notifications

Step 2: Then, go to Destination Paths after that click edit.

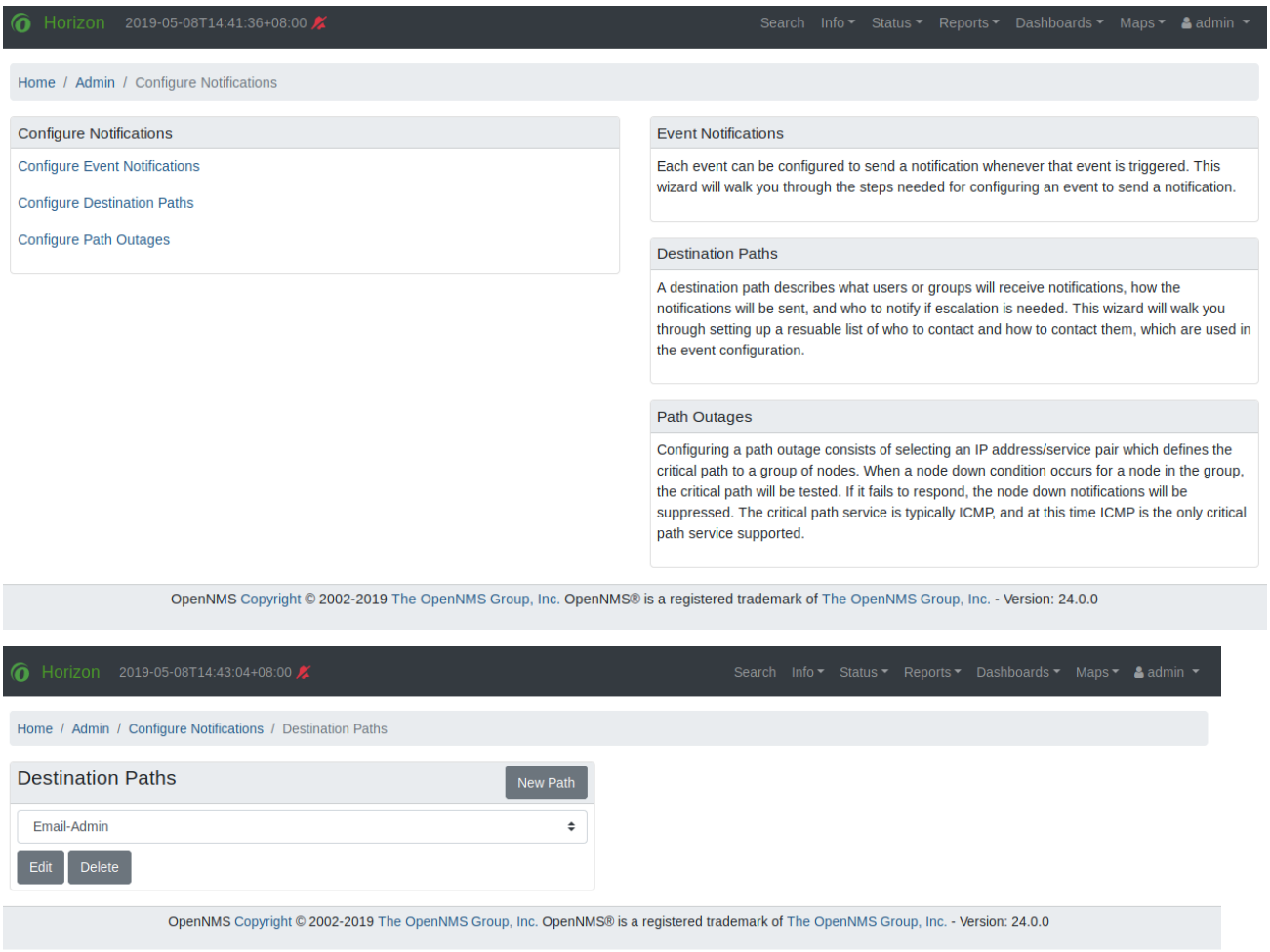


Figure 360 Destination Path

Step 3: Editing path by adding email of admin on initial target for example *megat@group4.com*

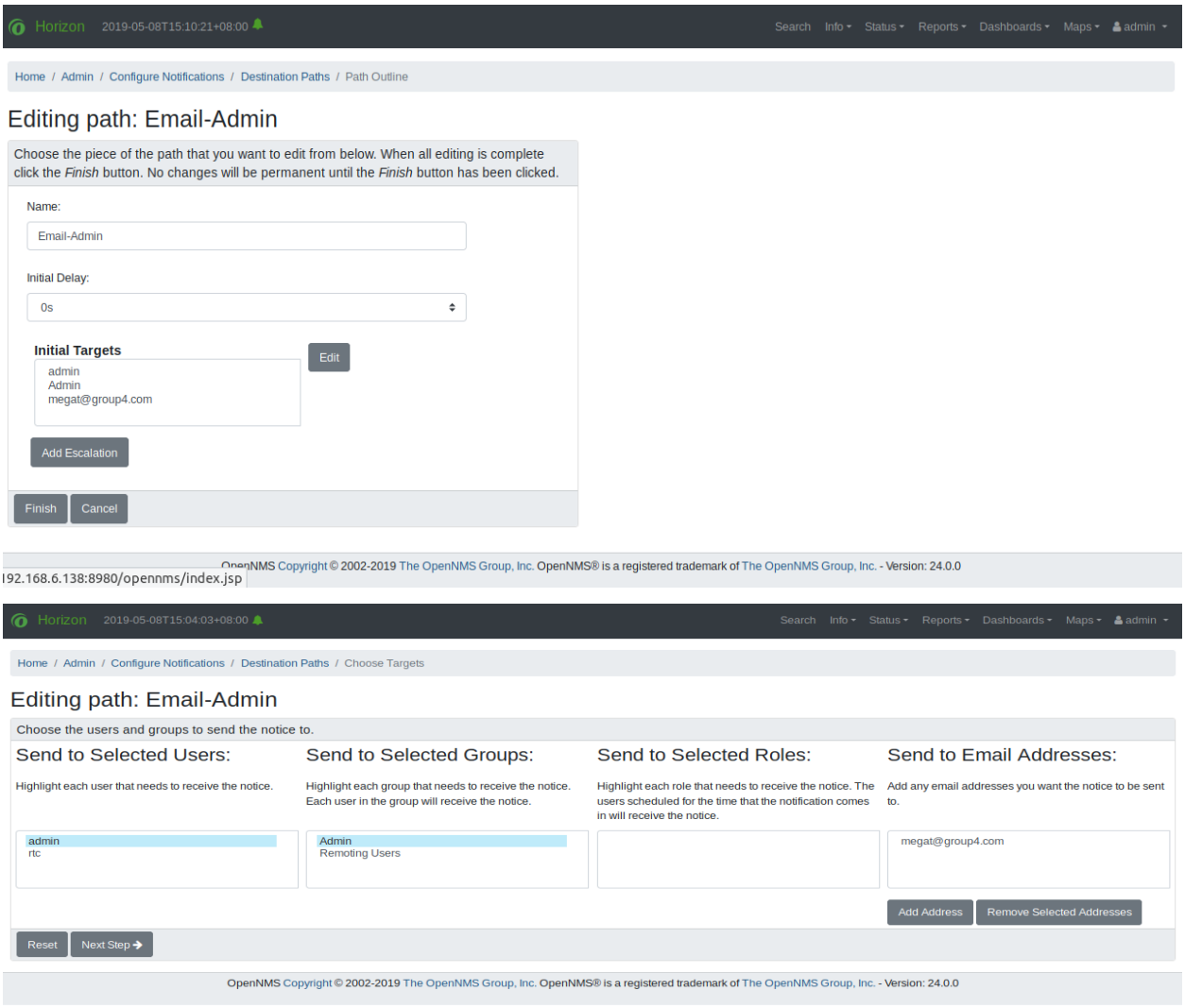


Figure 361 Editing Path

Step 4: Choose the users and groups to send the notice to by email addresses

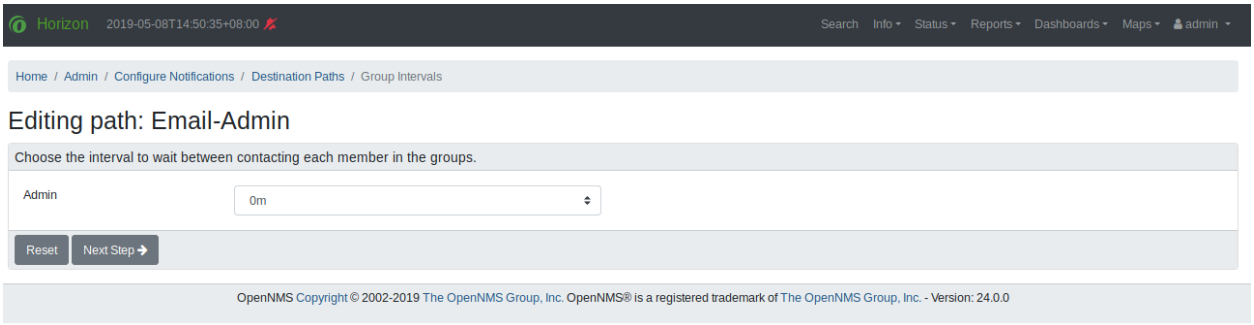


Figure 362 Choose users and groups

Step 5: Choose the commands java Email to use and click ‘on’ for the automatic notification on “UP” events

Step 6: After that, click Finish to save it.

Figure 363 Editing path: Email-Admin

Step 7: Select “On” and click “Update”

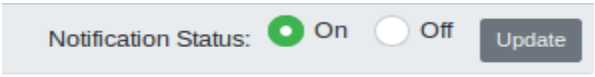


Figure 364 Update

6.2.12.1 Service

Step 1: Select representative node that contain service DNS.

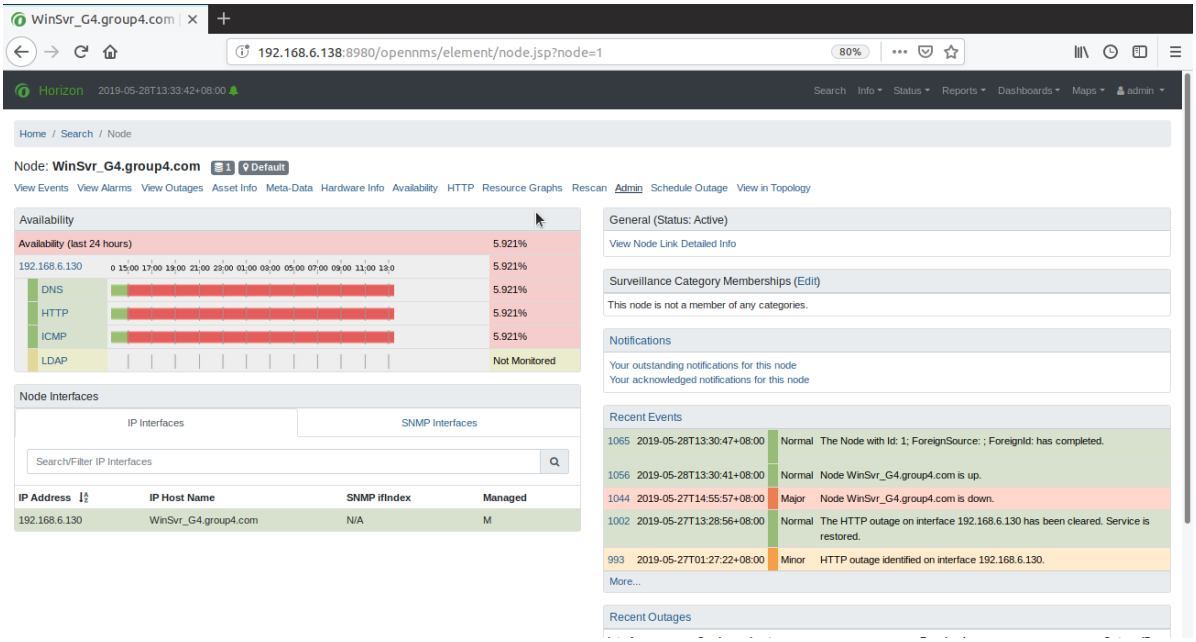


Figure 365 Select perspective node

Step 2: Turn off DNS service in Windows OS

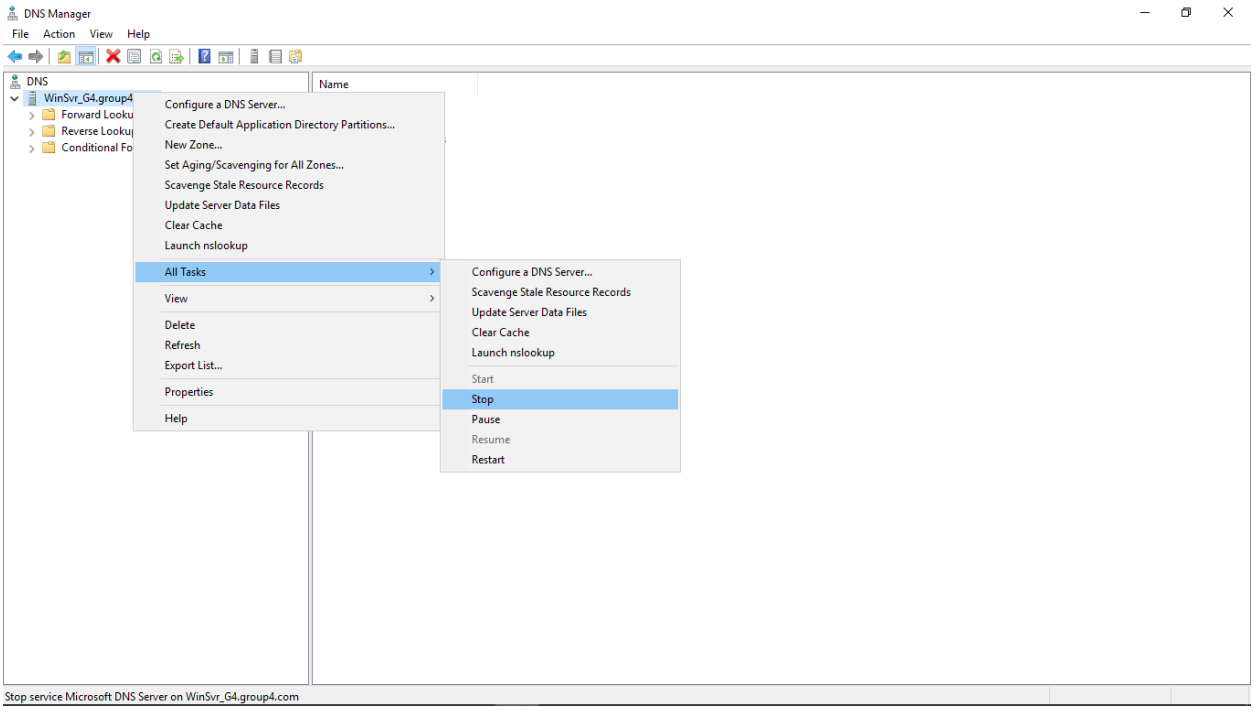


Figure 366 Turn OFF DNS service

Step 3: DNS service turn red colour when service down.

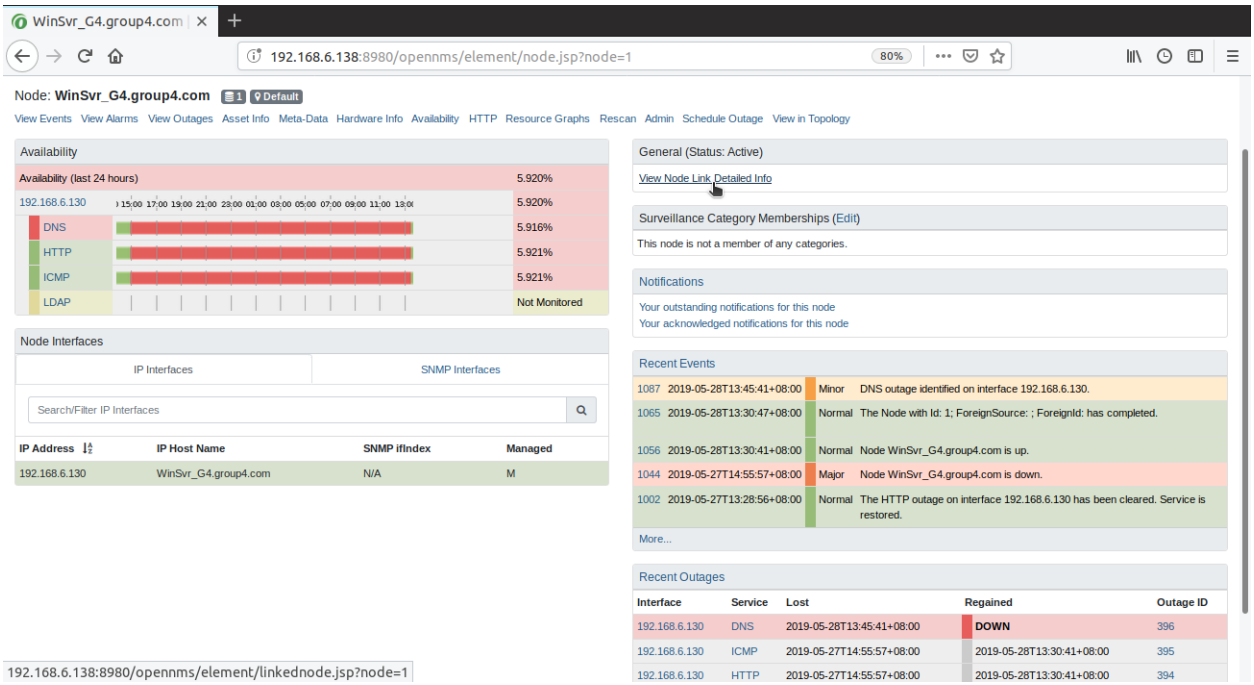


Figure 367 Turn ON DNS service

Step 4: Turn on DNS service in Windows OS

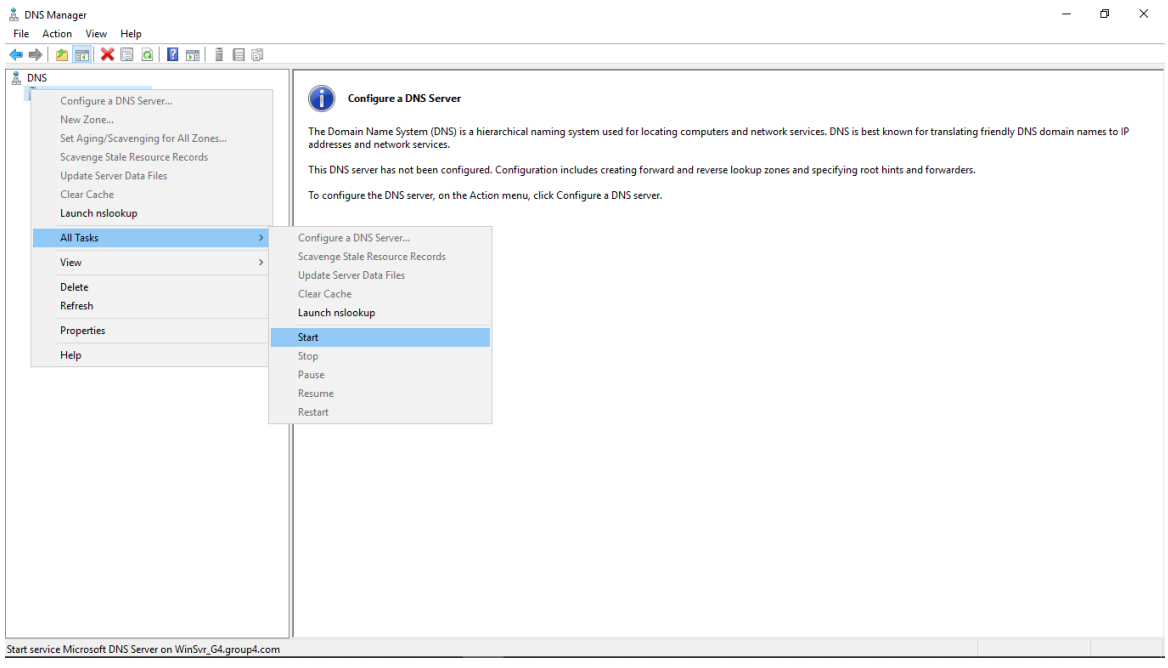


Figure 368 Turn ON DNS service

Step 5: DNS service turn green when service up.

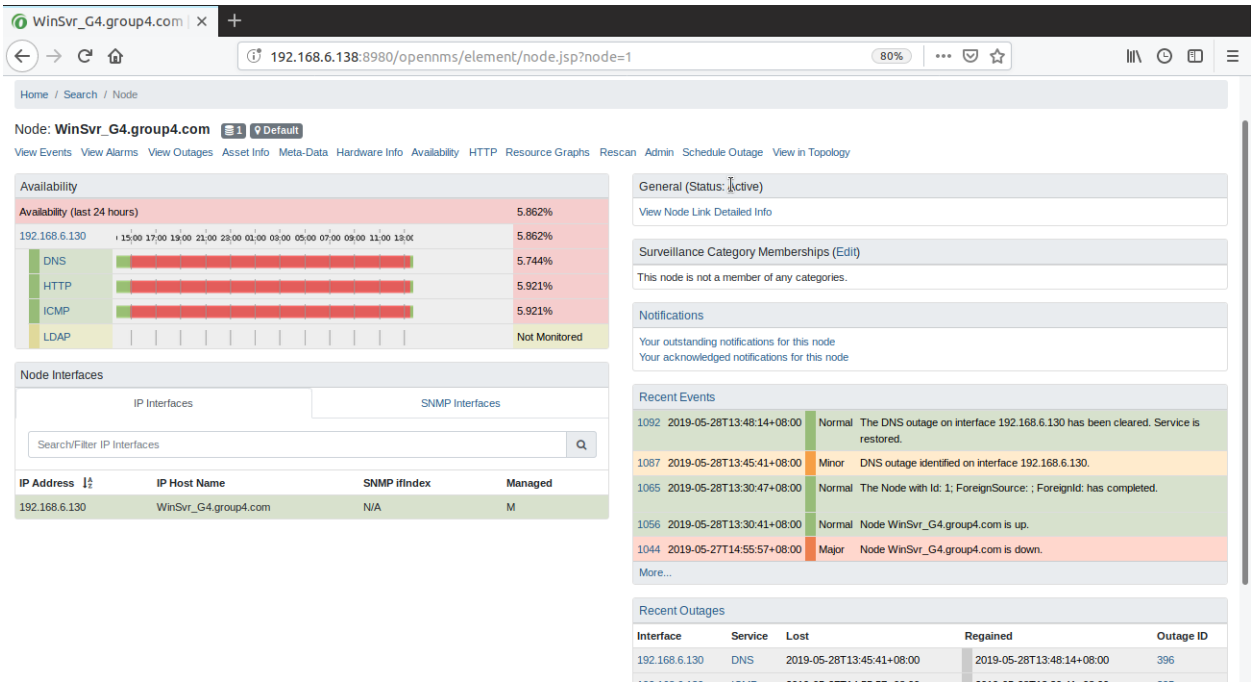
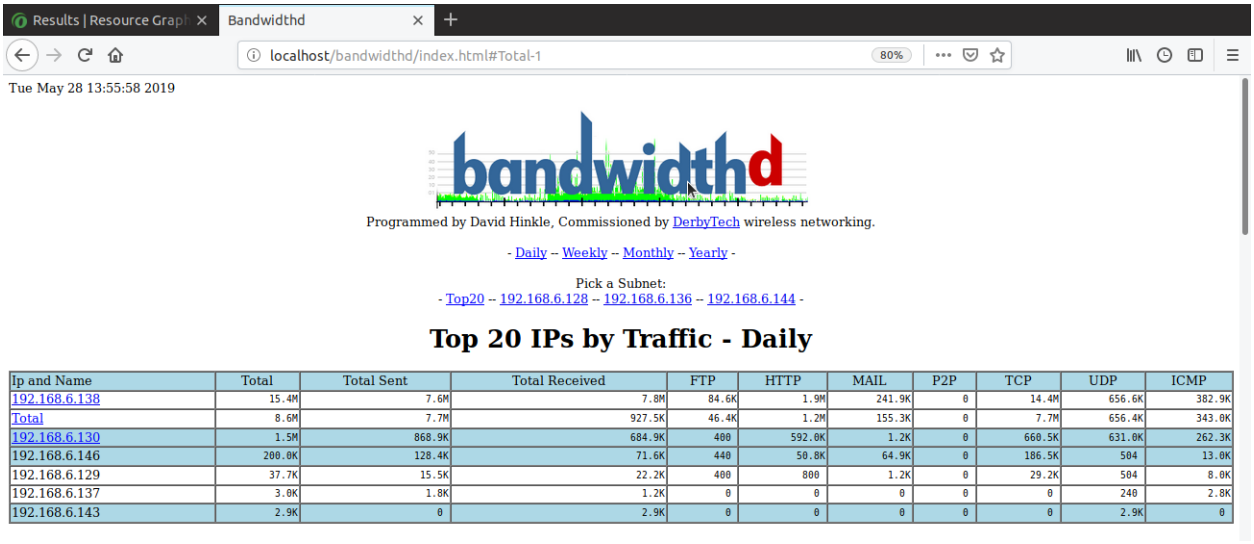


Figure 369 DNS service up

6.2.12.2 Bandwidth/Traffic



Ip and Name	Total	Total Sent	Total Received	FTP	HTTP	MAIL	P2P	TCP	UDP	ICMP
192.168.6.138	15.4M	7.6M	7.8M	84.6K	1.9M	241.9K	0	14.4M	656.6K	382.9K
Total	8.6M	7.7M	927.5K	46.4K	1.2M	155.3K	0	7.7M	656.4K	343.0K
192.168.6.130	1.5M	868.9K	684.9K	400	592.0K	1.2K	0	660.5K	631.0K	262.3K
192.168.6.146	200.0K	128.4K	71.6K	440	50.8K	64.9K	0	186.5K	504	13.0K
192.168.6.129	37.7K	15.5K	22.2K	400	800	1.2K	0	29.2K	504	8.0K
192.168.6.137	3.0K	1.8K	1.2K	0	0	0	0	0	240	2.8K
192.168.6.143	2.9K	0	2.9K	0	0	0	0	0	2.9K	0

Figure 370 Traffic by Daily

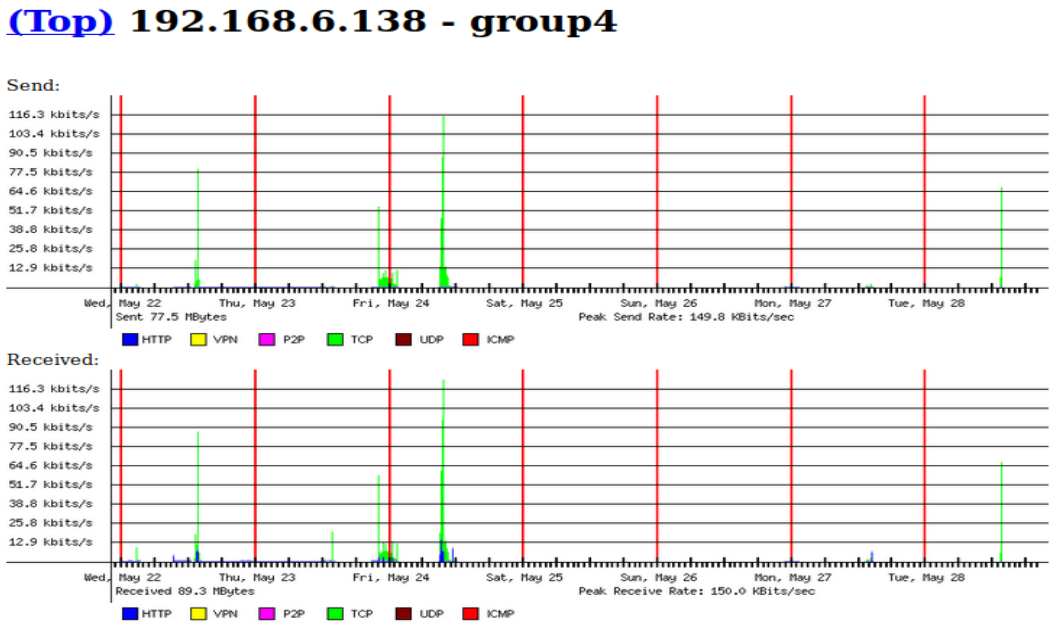


Figure 371 group4

(Top) 192.168.6.146 - debian.group4.com

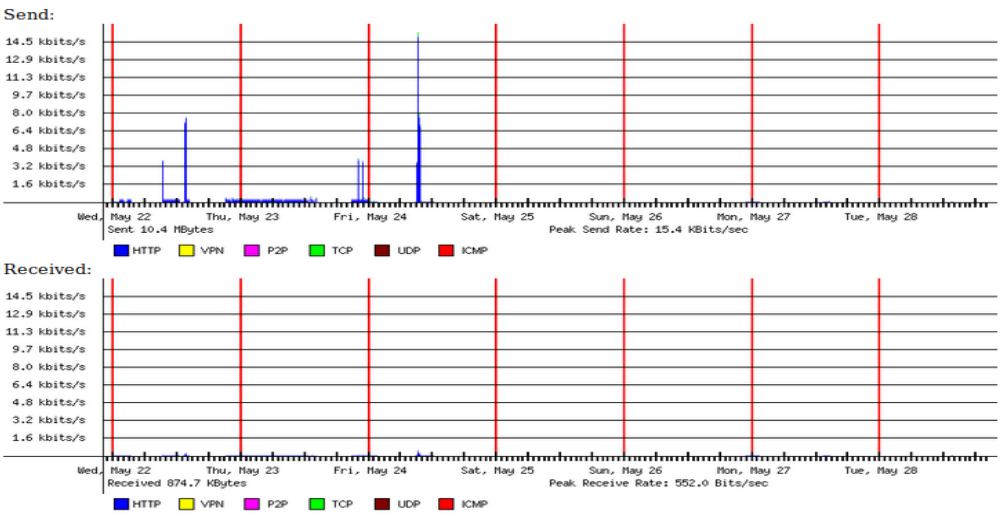


Figure 372 debian.group4.com

(Top) 192.168.6.130 - WinSvr_G4.group4.com

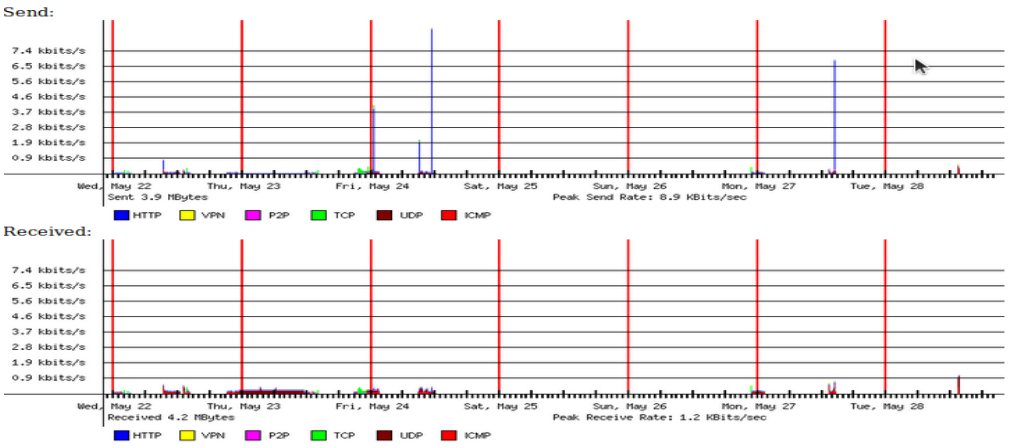


Figure 373 WinSvr_G4.group4.com

6.2.13 Proxy Server Testing

Step 1: Set IP address in Connection Settings

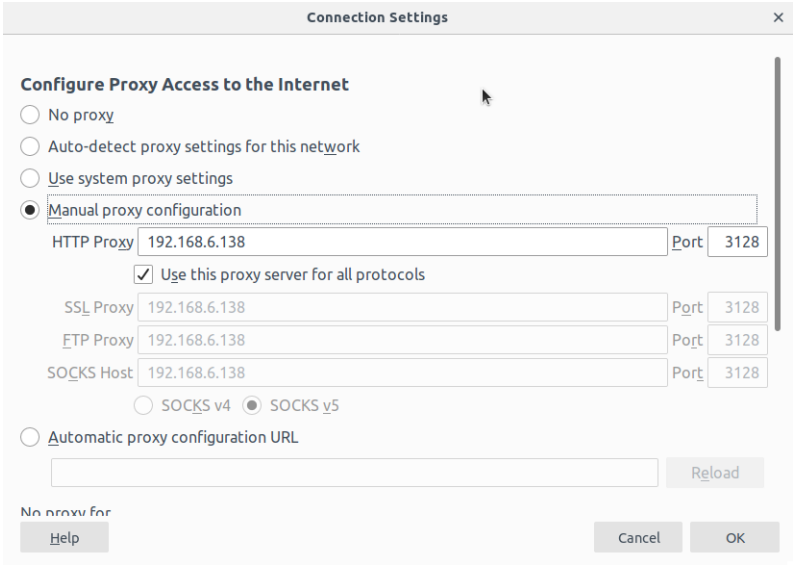


Figure 374 Test from client on Windows

6.2.13.1 Test from client on Ubuntu

ulearn.utem.edu.my

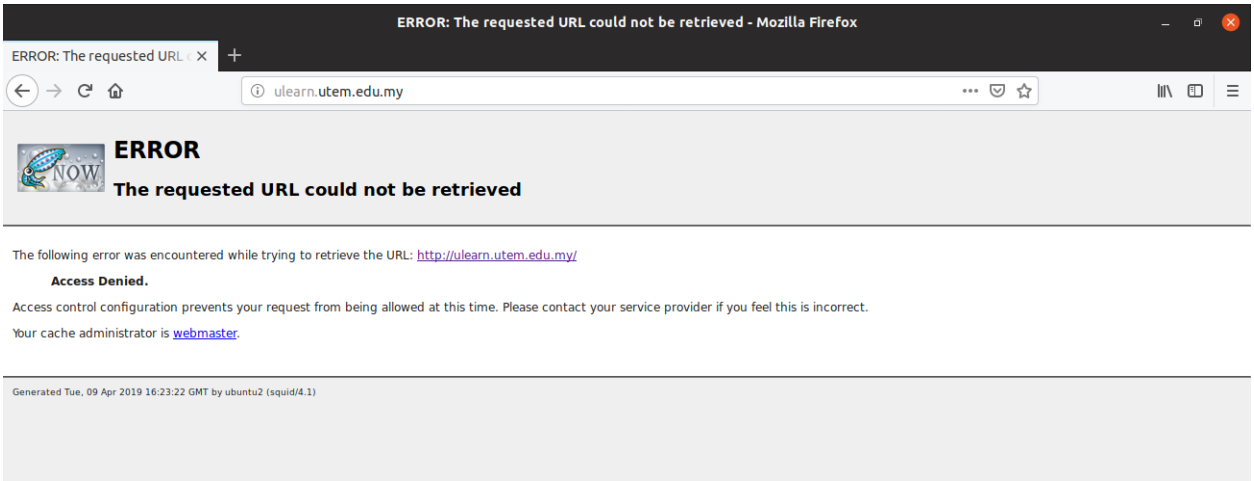


Figure 375 Error message when search "ulearn.utem.edu.my"

yahoo.com

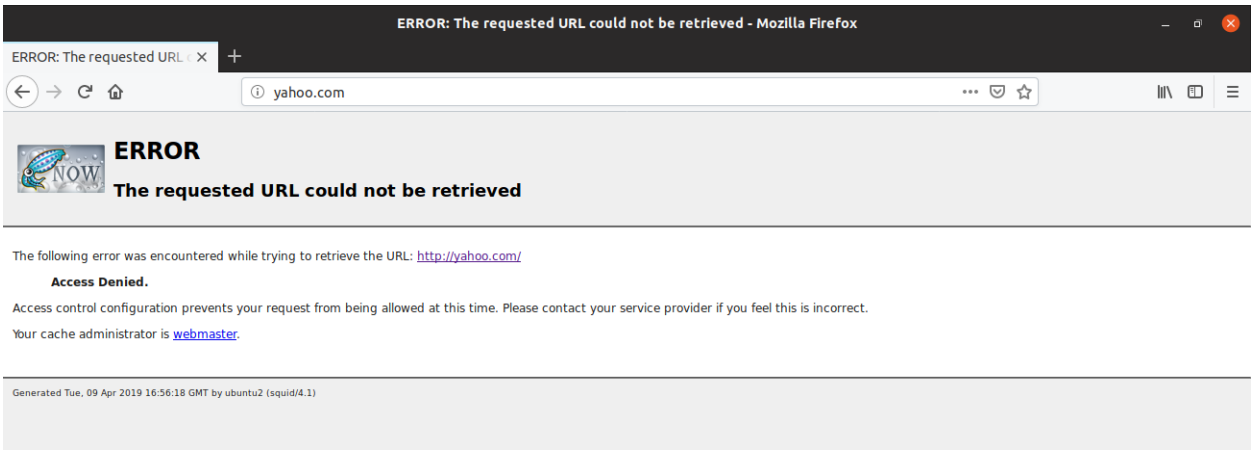


Figure 376 Error message when search "yahoo.com"

6.2.13.2 Test from client pc

ulearn.utem.edu.my

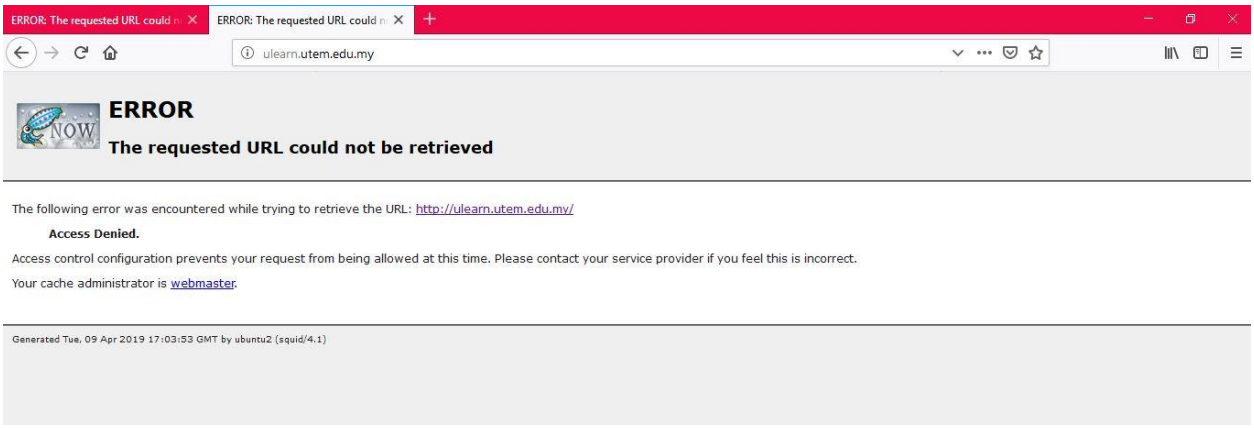


Figure 377 Error message when search "ulearn.utem.edu.my"

yahoo.com

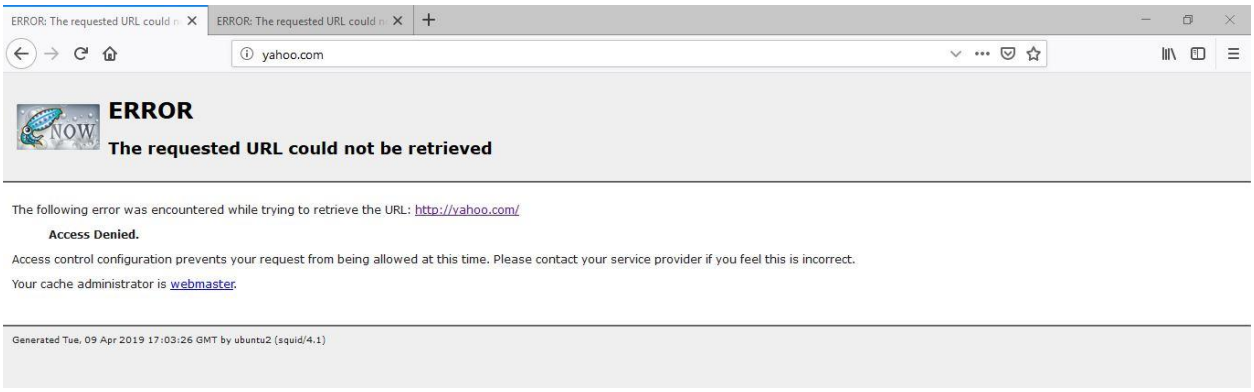


Figure 378 Error message when search "yahoo.com"

6.2.14 Wireless User Authentication using Radius Server Testing

Step 1: Find your group wifi ssid on your client workstation and click connect.

Figure 379 Connect to Radius Client wifi

Step 2: Enter the username and password. The username and password will be the user that been created on the Active Directory User and Computer.

Figure 380 Enter username and password

Step 3: Once the client has connected with the radius client, the user will received the DHCP ip configuration and the ip address will be in the client subnet.

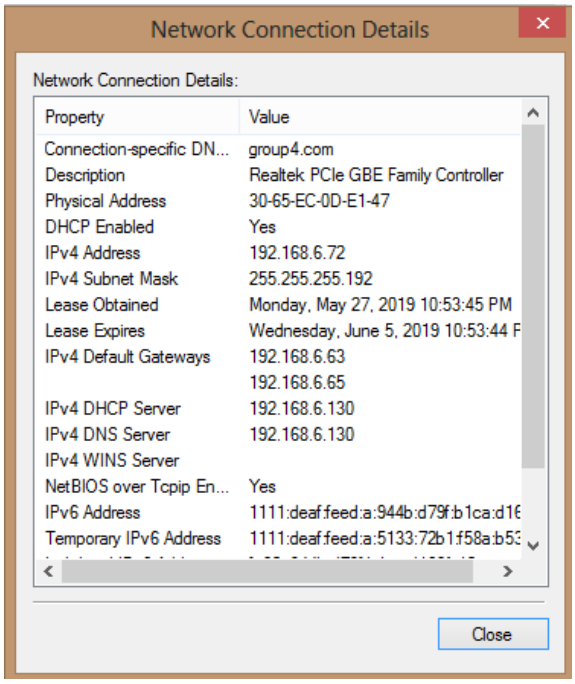


Figure 381 Client Get DHCP ip address

Step 4: Client also will have access to the group Ipv4 and Ipv6 website.

Figure 382 Client have access to group website

Step 5: Client also will have access to the neighbour website that we have configured tunelling.

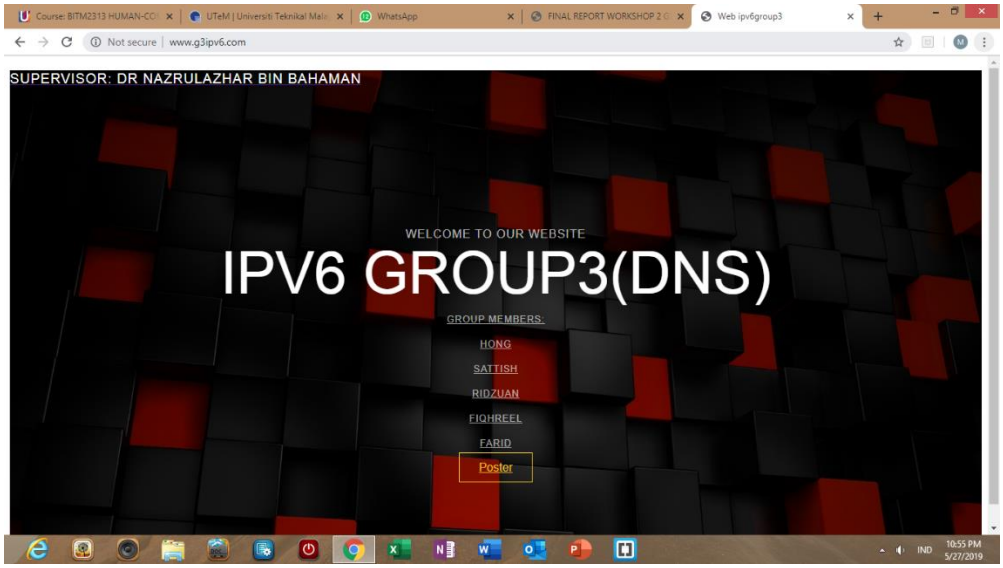


Figure 383 Neighbour website

6.2.15 ACL Testing

Step 1: Open the command prompt and check the new client. Write the ipconfig to check the IP address client.

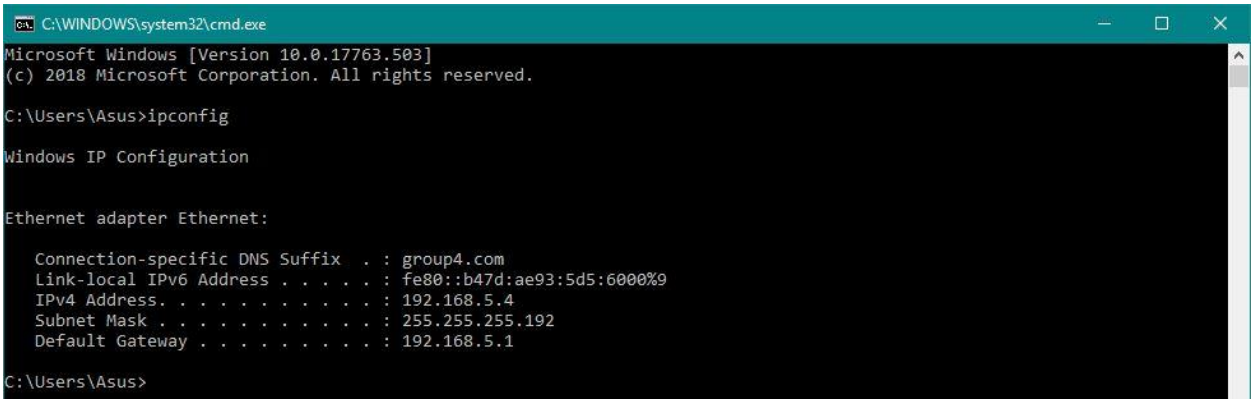


Figure 384 Open command prompt and check IP address

Step 2: The email hosting is blocked. mail.group4.com cannot open.

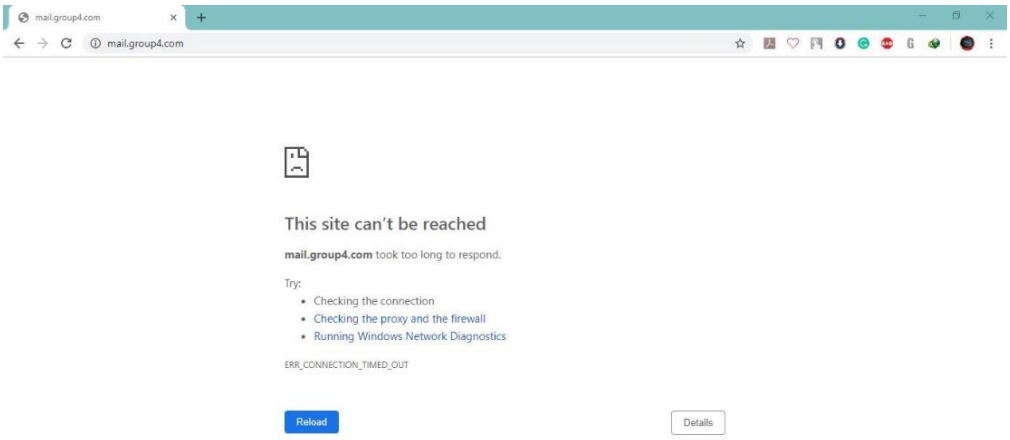


Figure 385 mail.group4.com is blocked

Open the command prompt. Check ping 192.168.6.146 host from Debian is successful ping.

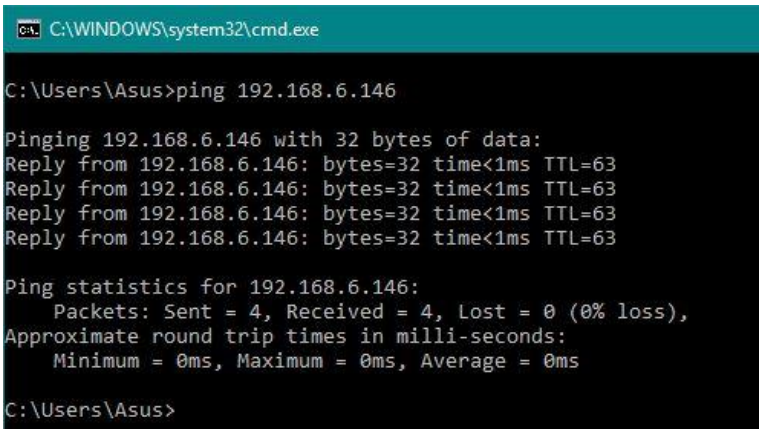


Figure 386 ping to host Debian is successful

Step 3: Open the command prompt. The ftp is blocked. ftp 192.168.6.138 is cannot open.

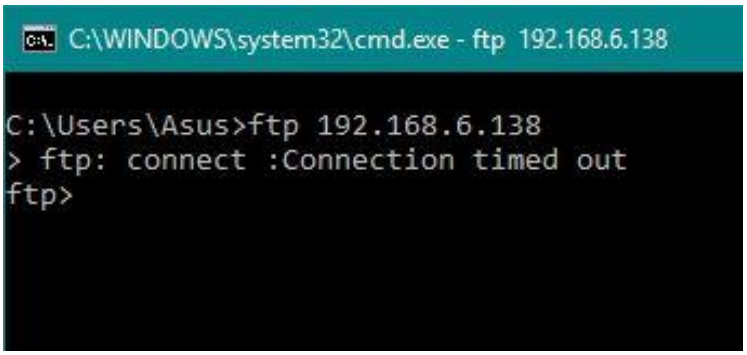


Figure 387 FTP IP address local host is blocked

Open the command prompt. Check ping 192.168.6.138 host from Ubuntu is successful ping.

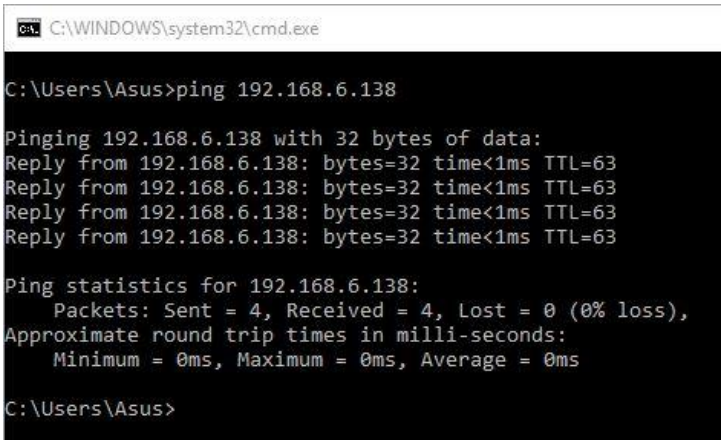


Figure 388 ping to host Ubuntu is successful

Step 4: The web hosting is blocked. http://www.group4.com cannot open.

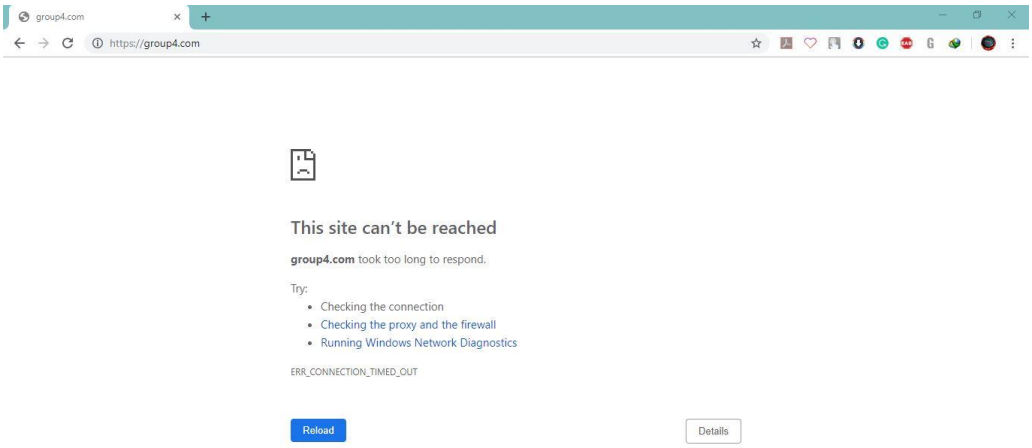


Figure 389 Web http://www.group4.com is blocked

Open the command prompt. Check ping 192.168.6.130 host from Windows Server 2019 is successful ping.

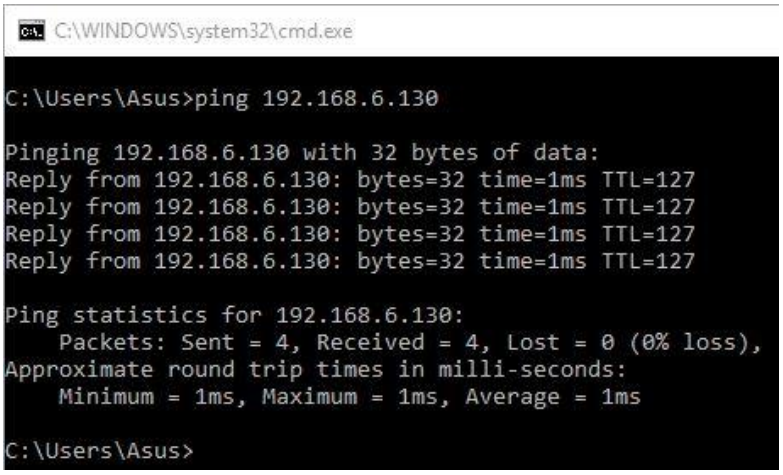


Figure 390 ping to host Windows Server is successful

Step 4: The https is blocked. https://www.group4.com cannot open.

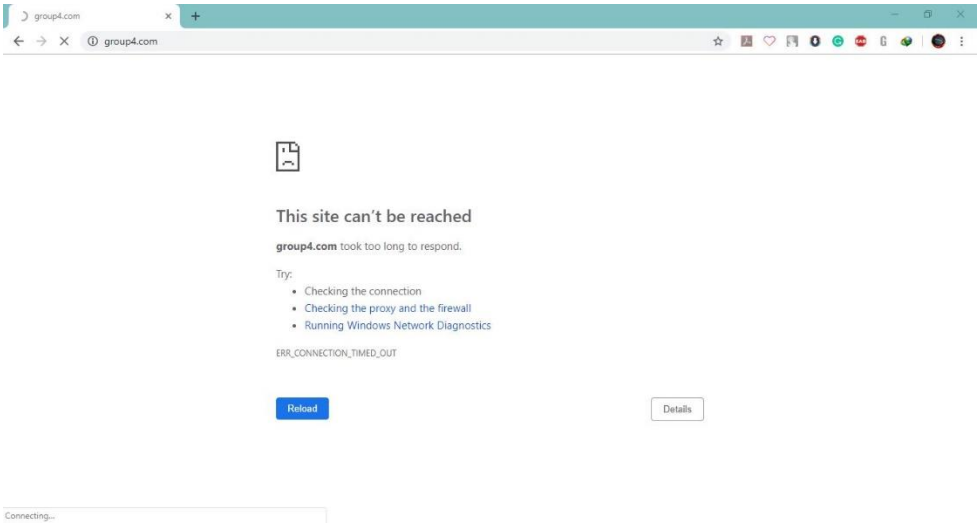


Figure 391 HTTPS https://www.group4.com is blocked

Open the command prompt. Check ping 192.168.6.130 host from Windows Server 2019 is successful ping.

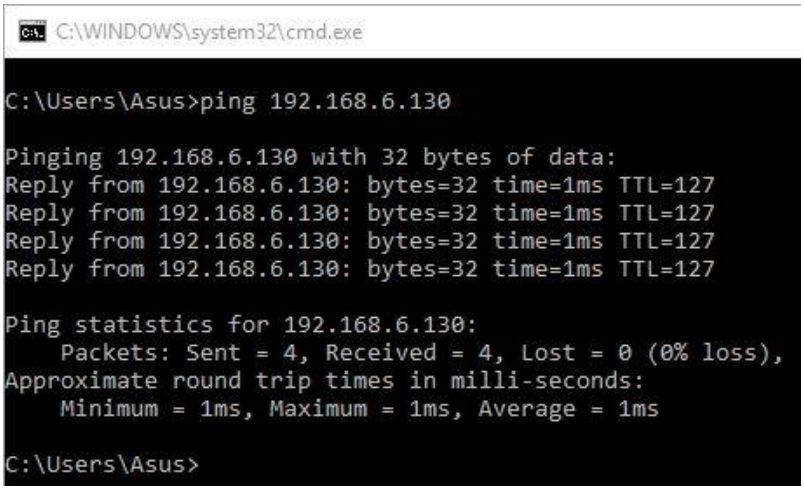


Figure 392 ping to host Windows Server is successful

6.2.16 Routing & NAT Testing

NAT is tested using the command show run where all the sub interface of NAT outside and NAT inside are configure. The show IP NAT translation command is used to check is the private address is translated to public and vice versa. Routing can be seen in show run when the protocol used in routing can be seen. The show IP route command is used to see the route of the IP of the router.

Network Address Translation (NAT)

Step 1: Used command "***show run***" to show the NAT inside and outside interface.

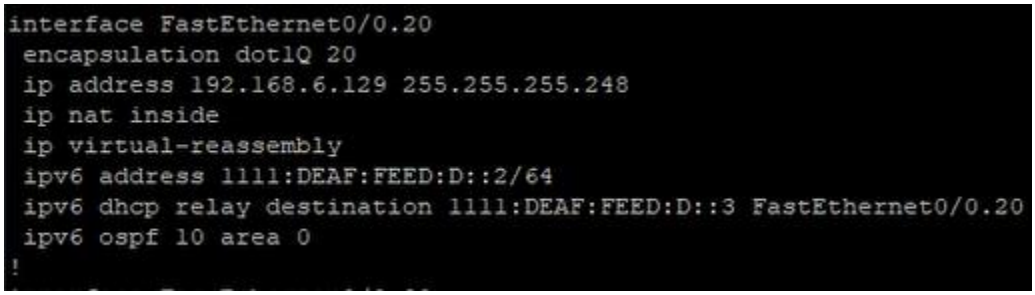


Figure 393 ip NAT inside (int f0/0.20)

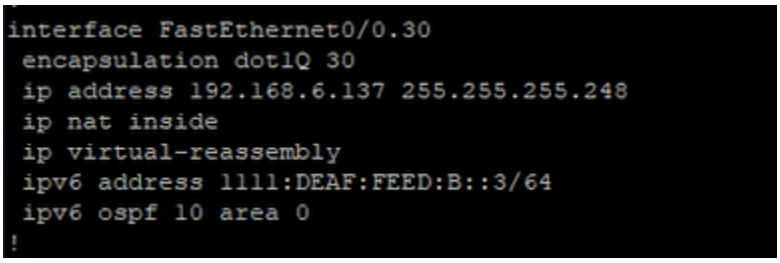


Figure 394 ip NAT inside (int f0/0.30)

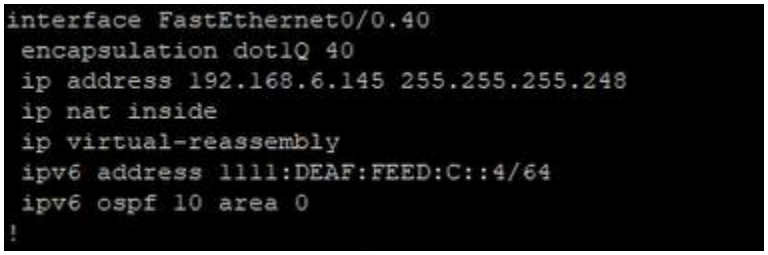


Figure 395 ip NAT inside (int f0/0.40)

```
interface Serial0/2/0
 ip address 200.200.200.1 255.255.255.248
 ip nat outside
 ip virtual-reassembly
 clock rate 2000000
 crypto map CMAP
!
```

Figure 396 ip NAT outside (int s0/2/0)

Step 2: Show configuration of static NAT and dynamic NAT.

```
no ip http server
no ip http secure-server
ip nat pool group4 200.200.200.9 200.200.200.10 netmask 255.255.255.248
ip nat inside source list 1 pool group4
ip nat inside source list 100 interface Serial0/2/0 overload
ip nat inside source static 192.168.6.130 200.200.200.11
ip nat inside source static 192.168.6.138 200.200.200.12
ip nat inside source static 192.168.6.146 200.200.200.13
!
ip access-list extended VPN-TRAFFIC
 permit ip 192.168.6.0 0.0.0.7 192.168.1.0 0.0.0.7
!
access-list 1 permit 192.168.6.64 0.0.0.63
```

Figure 397 Configuration of static NAT and dynamic NAT

Step 3: Ping from pc windows server (group 4) to pc group 3 using public IP.

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ping 200.200.200.21

Pinging 200.200.200.21 with 32 bytes of data:
Reply from 200.200.200.21: bytes=32 time=2ms TTL=126
Reply from 200.200.200.21: bytes=32 time=3ms TTL=126
Reply from 200.200.200.21: bytes=32 time=2ms TTL=126
Reply from 200.200.200.21: bytes=32 time=3ms TTL=126

Ping statistics for 200.200.200.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\Administrator>tracert 200.200.200.21

Tracing route to 200.200.200.21 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  RTR.group4.com [192.168.6.129]
  2     2 ms     2 ms     2 ms  200.200.200.2
  3     3 ms     3 ms     3 ms  www.group3try.com [200.200.200.21]

Trace complete.
```

Figure 398 Ping IP 200.200.200.21

Step 4: Show IP NAT translation

```
R4#sh ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 200.200.200.11:1  192.168.6.130:1    200.200.200.21:1   200.200.200.21:1
udp 200.200.200.11:53  192.168.6.130:53   200.200.200.21:52761 200.200.200.21:52761
```

Figure 399 Result IP NAT translation

Step 5: Ping from pc windows server (group 3) to pc group 4 using public IP.

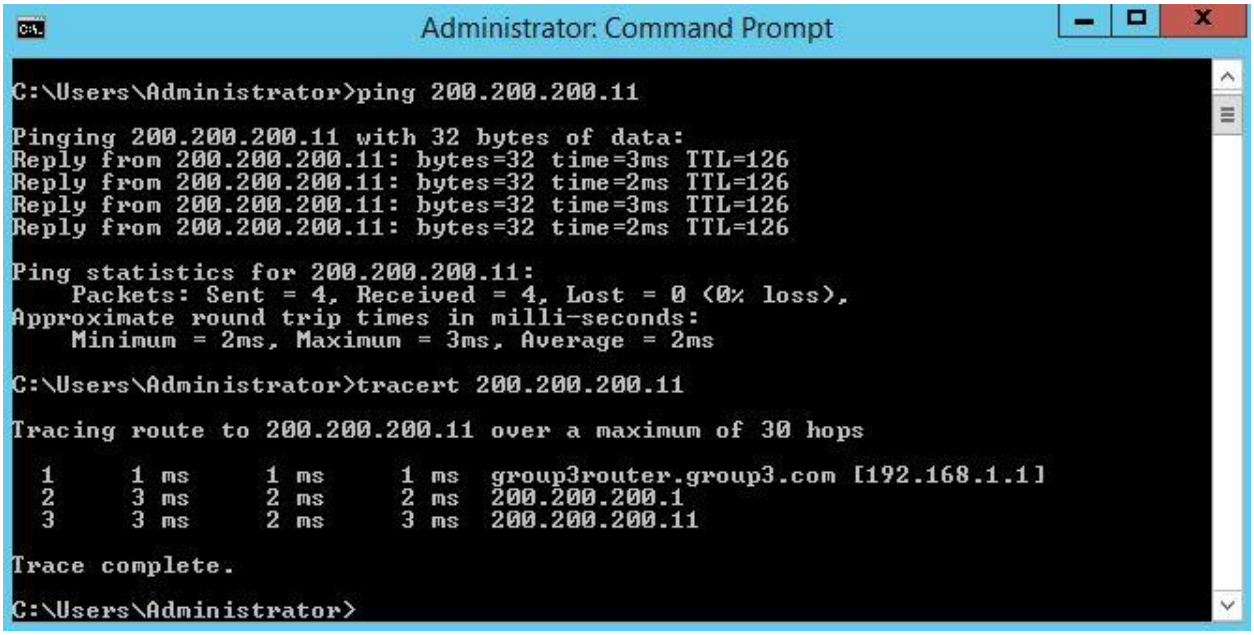


Figure 400 Ping IP 200.200.200.11

CHAPTER 7: CONCLUSION

7.1 Introduction

Workshop 2 is the prerequisite subject that preparing student before ongoing industrial training. In this workshop 2, student is more exposed the environment that working in a group with flexible schedule within a period time and all in real device instead of using simulation software such as Cisco packet tracer.

This workshop 2 is also a good platform that provide knowledge exchange and sharing between computer networking students. This course Bachelor Information Technology and Computer (BITC) student are able to expose to each other expertise field knowledge that will provide greater advantage in future of student career. Workshop 2 also provided the platform for student to explore the knowledge of configuration that can be done with different tools and software.

The network we setup in workshop 2 is suitable for small and medium enterprise business as it is easy to manage and implement. This network included all the basic service that are the minimum requirement to run a business.

7.2 Project Advantages

Through the workshop 2 project, we are able to gain the advantage as follows:

- To updated knowledge about the information of Computer technology such as operating system, hardware and others.
- To learned to work as a team and divide equally the task to be completed by each of the members.
- To implement designated network services.
- To integrate network services infrastructure to suit the network environment.
- To know what the vulnerability commonly appears on an operating system and solve it.
- To refresh our knowledge and explore further the knowledge of each service.
- To install and configure the service properly in a server.
- To share knowledge among the teammate and others group.
- To learn and adapt the real environment that preparing us for industrial training and also for career in future.

7.3 Project Disadvantages

However, this workshop 2 project also has disadvantages on achieving successful result. The disadvantages of the project are as following:

- To limited knowledge on these services.
- The hardware arrived late has caused delay in progression of configuration.
- The hardware which is older version has caused some configuration problem that complicated to solved and unable to perform.
- Some of the network equipment's are not in a good condition, it may not work as well as expected.
- The lab environment during the night time is very humid because the air condition is turned off and all of the servers are running causing the servers to heat up.

7.4 Project Limitation

There was some project limitation that was caused and we had to adapt and work harder to succeed in this project. These limitations were:

- The network was only implemented in wired environment.
- The network was not implemented in larger environment.
- The equipment that was provided to each group is not in good condition.
- The network for the projects only involved 3 servers.
- The wireless technology was not implemented in this project due to the problem in the wireless device.

7.5 Conclusion

In a nutshell, we are able to configure and set up our network using the basic network equipment through the workshop 2. We are also exposed with the operating system knowledge that will helped us in choosing operating system for our server in future. We are able to design our own network infrastructure and maintain it in a good condition at all time. We are also exposed with the knowledge of network vulnerability on the operating system and network and solve it using hardening in order to ensure the whole network that had been setup are network and ready to be use.

In this workshop 2, one of the main objective is to provide the environment for student to work in a team. Through this project, we learnt to planning among our team and giving fully cooperation among each other's along the project progression. This also enable us to prepare for facing the real environment of career and industrial training. We are also able to share our knowledge each other to ensure everyone able to gain new knowledge and experience that will be useful in future.

As a conclusion, this workshop has successful gives the real working environment exposure to us at the end of this workshop 2 project and we are managed to complete all the tasks given and setup the network as required.

BIBLIOGRAPHY

Active Directory, June 18 Retrieved from https://searchwindowsserver.techtarget.com/definition/Active-Directory

Authentication, Authorization, and Accounting, November 2010 Retrieved from https://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting and https://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting

How to Make Your Website Available Over IPv6, June 6, 2014 Retrieved from https://www.internetsociety.org/blog/2014/06/how-to-make-your-website-available-over-ipv6/

Network Management System Retrieved from https://www.techopedia.com/definition/11988/network-management-system-nms

RADIUS Server for Wireless Authentication Retrieved from https://www.watchguard.com/help/docs/fireware/12/en-US/Content/en-US/wireless/wireless_auth_radius_c.html

IPSec site to site tunnelling from https://computer.howstuffworks.com/vpn4.htm

How To Set Up vsftpd for a User's Directory on Ubuntu 16.04 from https://www.digitalocean.com/community/tutorials/how-to-set-up-vsftpd-for-a-user-s-directory-on-ubuntu-16-04

APPENDIX

Activity / Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Project Proposal Submission															
Setup of 5 Services Completed / Progress Report 1 Submission															
Setup of 10 Services Completed / Progress Report 2 Submission															
All Network & Services Setup Completed/ Progress Report 3 Submission															
Video & Poster															
Workshop II Exhibition															
Final Report & Log Book Submission															

Table 7 Appendix Mind Stone