PROJECT REPORT FOR NETWORK DESIGN AND IMPLEMENTATION FOR A MEDIA COMPANY

Diploma Project Final Report DCN17.2F

Isuru chathuranga	CODCN172f-001
W.M.B.B. Malinda Bandara	CODCN172f-002
Sudeera Seneviratne	CODCN172f-021

2019

Final Project of Diploma in Computer Networks 17.2 (DCN17.2)

Supervisor: Mr. Milan Maduranga

NATIONAL INSTITUTE OF BUSINESS MANAGEMENT

M I S DIVISION

COLOMBO 07

"The Project is Submitted in Partial fulfillment of the requirement of the Diploma in Computer Networks of National Institute of Business Management"

OCTOBER 2019

Declaration

This is my original work and has not been submitted previously for a degree at this or any other university/institute.

To the best of my knowledge it does not contain any material published or written by another person, except as acknowledged in the text.

Students Names:

1. Isuru chathuranga Signature: …….

2. W.M.B.B. Malinda Bandara Signature: …….

3. Sudeera Seneviratne Signature: …….

Date:

This is to certify that this project is based on the work of …… under my supervision. The report has been prepared according to the format stipulated and is of acceptable standard.

Certified by:

Supervisor Name:

_____ _____

Signature: Date:

Acknowledgment

The success and final outcome of this required a lot of guidance and assistance from many people and we would like to express our special thanks to everyone who supported us through completion of this final project of our Diploma. We respect and thank Mr. Milan Maduranga for providing us an opportunity to do the project and giving us all support and guidance till the completion of our project work by providing all the necessary information for developing a good system which made us complete the project duly.

Thank You

Abstraction

This project is designed and implemented for a media company whose primary objective is to supply their clients' contracts with the ongoing demand for media. We designed a suitable network infrastructure for Mediamora company which has high availability with redundancy, quality, security, monitoring and backup. When it comes to media video and voice traffic are prominent than data. So various QoS strategies, mechanisms and special devices have been implemented throughout the project to give more value to the video traffic and voice traffic.

For this network we used a collapsed layer architecture and each layer be a well-defined, structured module with specific roles and functions in the network. This company will get two leased lines from SLT as primary and backup with sufficient bandwidths to provide the necessary connectivity and by doing this the network will always available for use when it is required. This is designed in a way that there will be no single points of failure and capable of achieving fast and predictable convergence times.

Infrastructure for the wireless user experience has been done through several stages of implementation with new wireless standards of IEEE 802.1ax and it was done by a professional well qualified IT service staff. This company creates proprietary media for their contracts, so we had to address the main problem of protecting those rights from external as well as internal attacks. We used some latest techniques and equipment to address the security issues including hardware firewalls as well as software firewalls, Intrusion detections systems and Intrusion prevention systems.

Overall we have addressed all the issues including both hardware and software. There were some issues with expanding the current network design if the company has any plans to open new branches in future. We have considered that matter and designed it easy for the company's future growth.

Contents

FIGURES & TABLES

Key Words

ISP – Internet Service Provider

DHCP – Dynamic Host Configuration Protocol

RADIUS – Remote Authentication Dial-in User Service

HD – High Definition

LAN – Local Area Network

HR – Human Resources

PC – Personal Computer

URL – Uniform Resource Locater

NAT – Network Address Translation

IP – Internet Protocol

Kbps – Kilobits per second

Mbps – Megabits per second

Gbps – Gigabits per second

AP – Access Point

VLAN – Virtual Local Area Network

ADDS – Active Directory Domain Services

ADCS - Active Directory Certificate Services

DNS – Domain Name System

HSRP – Hot Standby Router Protocol

IEEE – Institute of Electric & Electronics Engineers

STP – Spanning Tree Protocol

WDS – Windows Deployment Services

USB – Universal Serial Bus

1.0 Introduction

1.1 Organization Layout

Mediamora media company create Advertisements and Designs Graphics for various business organizations. This company also deals with supplying entertainment shows and Tv Shows to Television channels. This organization is responsible for the legal issues that occurs and resolve them accordingly. The requirements of this company was to create a network that is capable of handling 500 users with the option to expand their network and WIFI coverage to the entire building, network storage facilities and ADDS with high speed internet connection.

1.2 Identifying Organization Requirement & Solutions

- Access level for all users with authentication.

  We created the mediamora company's network with an ADDS (Active directory Domain Services) base on users to give the users their own logins to provide a high security. Personalized user experience. Because of ADDS all the users can't access everything and because of this we reduce network failure occurred by user interference.
- Access level for department wise.

  We created VLAN to identify each department easier. It's easier for the troubleshooting. And a reliable way to easily understand the network infrastructure. Also it will be easy to modify the network or fix small problems, even mediamora ICT staff will be able to make these modifications without the help of a network administrator.

- Up to 600 users.
  We supplied network connectivity with high performance with possibly of expanding the network. Currently 500 users work in mediamora company. If there is any additional work staff we provided the possibility of expanding the network easily to accommodate the new users.

- Network redundancy.

  We added redundancy for our network with best performance. We add redundant network paths and devices to ensure the network reliability. Because mediamora is a company that provides constant services to their customers they must be able to access the internet without any problems. We added a second internet service provider in case of an emergency. Also they are able to use the redundancy internet service provider for load balancing. With load balancing we can use the redundancy network paths so the resources will not be wasted.

- WIFI access (For company users and customers).
  Given WIFI access to user to use the internet. With a custom VLAN we implemented a WIFI coverage to mediamora company so people who work in their laptops are able to work with ease. Also the users are able to use the WIFI network in their mobile phones.

- Data Storage server management with security.

  We maintaining data center with high security (finger print scanner, cctv cameras) to protect and backup their data in proper way. The storage of the servers are shared to all the users in the mediamora company they can log into the shared storage using their credentials. With a backup storage we gave the option to mediamora company to backup their files and folders in case of a emergency.

2. Network Design

2.1 Department and users

Mediamora company has 3 floors, 7 departments and 600 users.

Department	Users
2nd Floor	
IT Department	Users - 50
Graphic Designing	Users – 150
Advertising Department	Users - 100
1st Floor	
HR	Users - 70
Legal	Users – 20
Finance & Management	Users - 80
Ground Floor	
Reception	Users - 8
Administration Department	Users - 70
Server Room	-

Table 2.1

2.2 IP Addressing

The following IP addressing scheme has been implemented for better connectivity throughout the organization.

Departments	Pool Range
2nd Floor	
IT Department	192.168.60.0/24
Graphics Designing	192.168.70.0/24
Advertising Department	192.168.80.0/24
1st Floor	
HR	192.168.30.0/24
Legal	192.168.40.0/24
Finance & Management	192.168.50.0/24
Ground Floor	
Reception	192.168.10.0/24
Administration Department	192.168.20.0/24
Data Center	192.168.200.0/24

Table 2.2

2.3 Assigning VLANs

Each Department has a unique VLAN to divide the departments/sub departments and to reduce traffic on each link on the network. For the easy reference we assigned the same VLAN ID to the DHCP pool of every department.

Department	VLAN ID
2nd Floor	
IT Department	60
Graphics Designing	70
Advertising Department	80
1st Floor	
HR	30
Legal	40
Finance & Management	50
Ground Floor	
Reception	10
Administration Department	20
Data Center	200

Table 2.3

2.4 Network topology

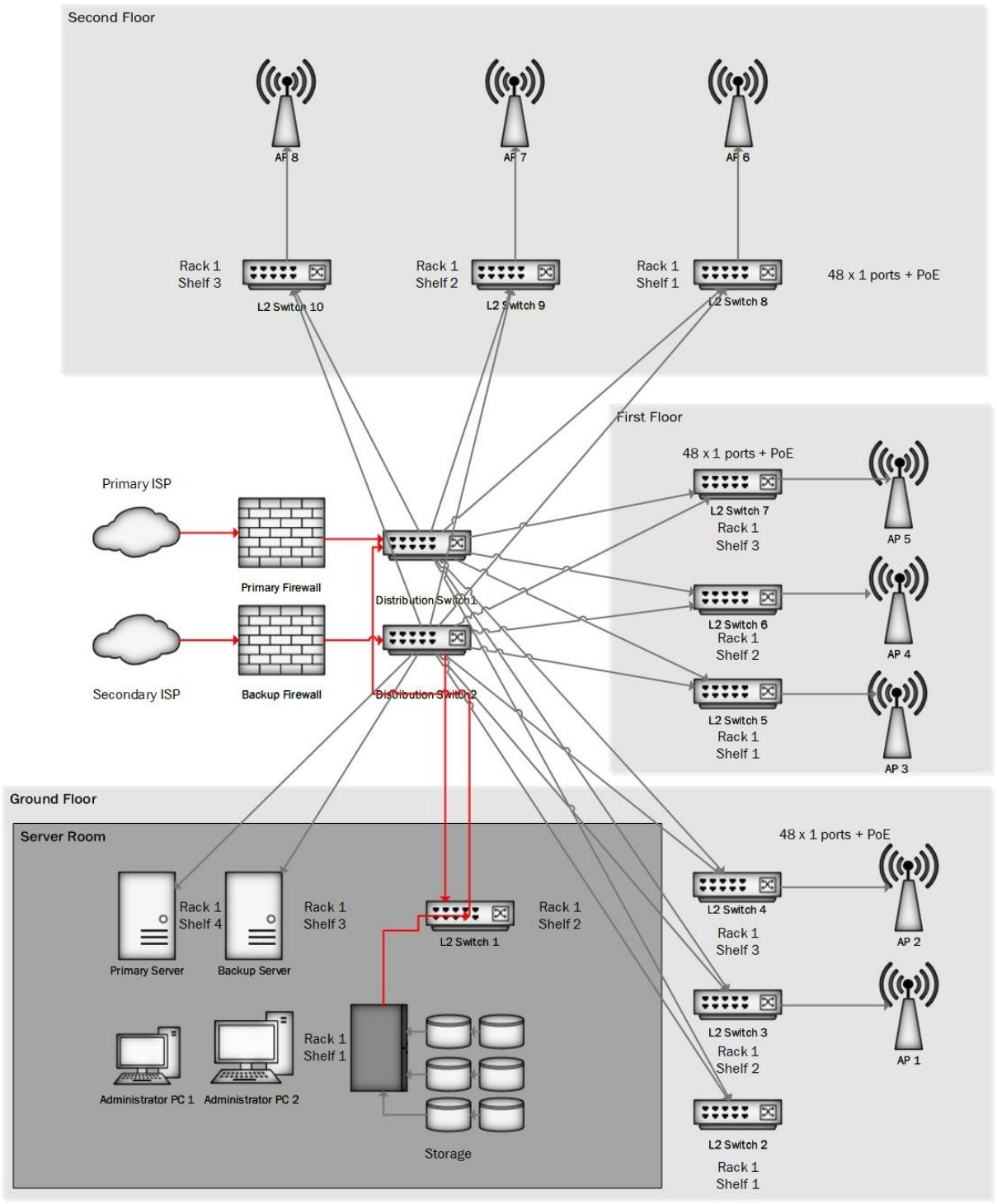


Figure 2.1

2.5 Network Architecture

The above topology has been implanted in the company with redundancy and high performance. Considering the company requirements, we selected collapsed layer architecture to design, deploy and maintain a scalable, trustworthy, cost effective hierarchical internetwork. Collapsed layer architecture would suit this organization because it's only having a main branch.

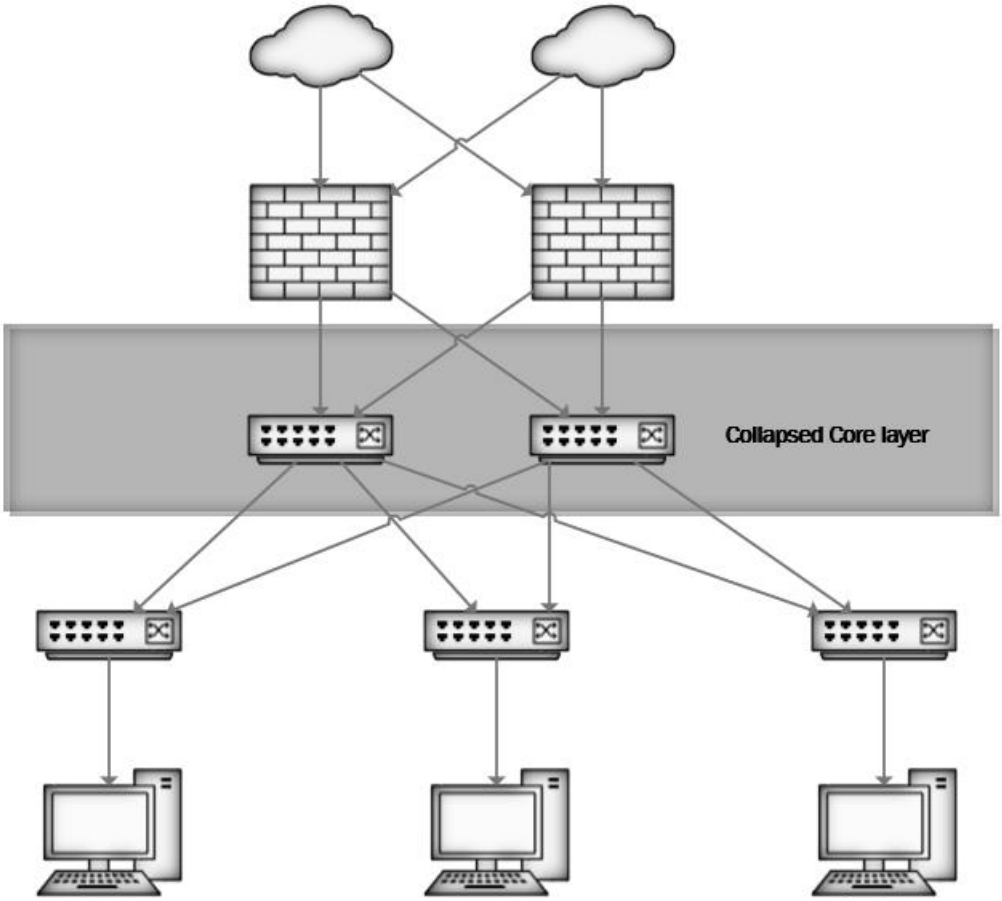


Figure 2.2

Internet access for end users are given from distribution switches to the access layer switches. We used fiber cabling to connect each distribution layer switches for redundancy. For each department we have used two or more access layer switches and redundant paths via cabling as well.

We have used two firewalls because of the security purpose and give the internet access through the firewalls and to block unauthorized access to the network from the outside networks.

We installed two main servers for redundancy purposes. For example, we are using DHCP server to issue the IP address for end users to access the network, maintaining domain users, maintaining storage with RAID. All the servers are placing on VM clusters which can be moved to the secondary server if the main server fails.

2.6 Logical Network Topology

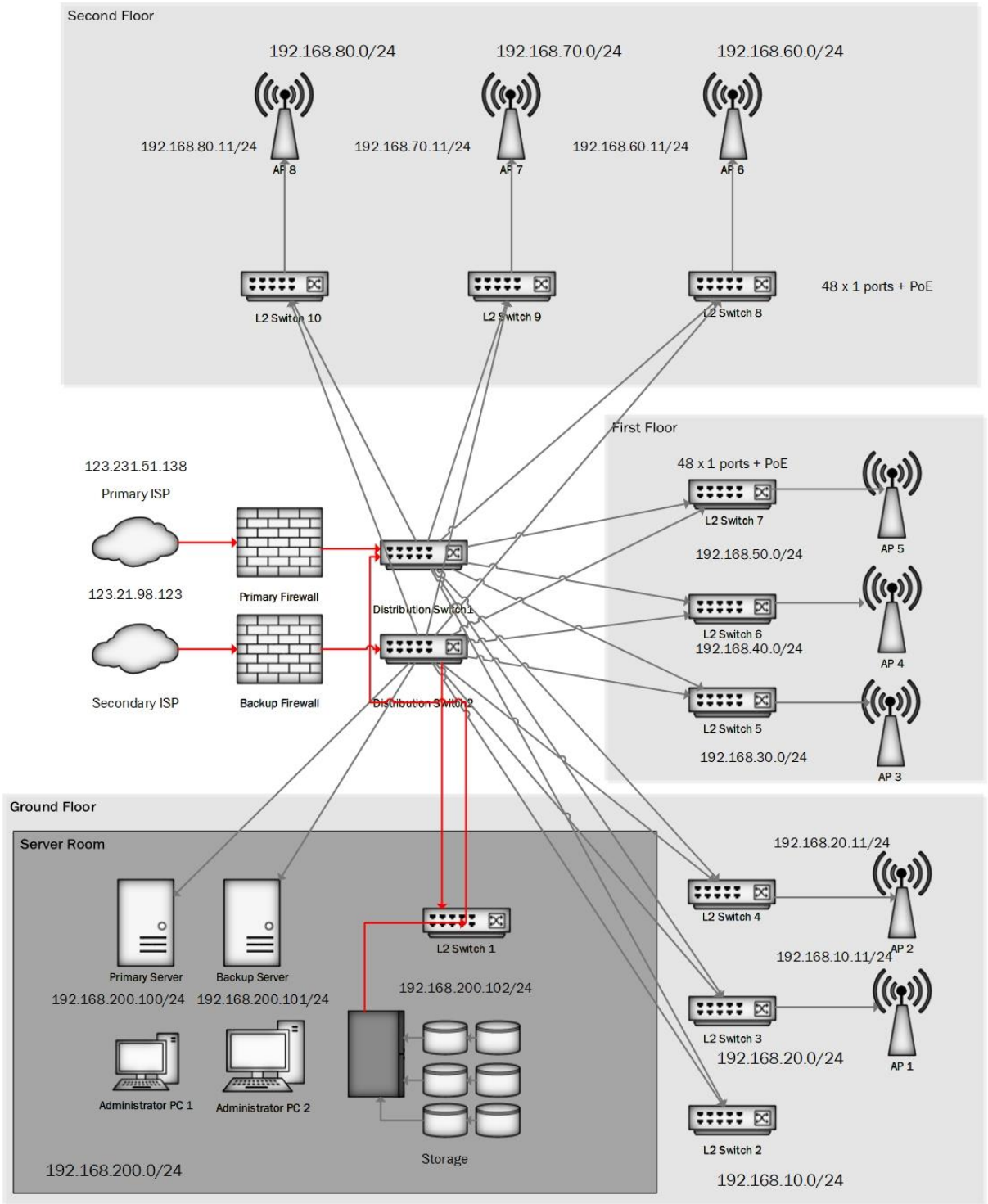


Figure 2.3

2.7 Port Map

Distribution switch 1

Device name	Port number	Description	Opposite end deice	Port number	Floor
Master	G1/0/1	Firewall	Primary firewall	G1/0	Ground
Master	G1/0/2	Firewall	Secondary firewall	G1/0	Ground
Master	G1/0/3	L2 link	L2 switch 1	Fa0/1	Ground
Master	G1/0/4	L2 link	L2 switch 1	Fa0/2	Ground
Master	G1/0/5	L2 link	L2 switch 2	Fa0/1	Ground
Master	G1/0/6	L2 link	L2 switch 2	Fa0/2	Ground
Master	G1/0/7	L2 link	L2 switch 3	Fa0/1	Ground
Master	G1/0/8	L2 link	L2 switch 3	Fa0/2	Ground
Master	G1/0/9	L2 link	L2 switch 5	Fa0/1	First
Master	G1/0/10	L2 link	L2 switch 5	Fa0/2	First
Master	G1/0/11	L2 link	L2 switch 6	Fa0/1	First
Master	G1/0/12	L2 link	L2 switch 6	Fa0/2	First
Master	G1/0/11	L2 link	L2 switch 7	Fa0/1	First
Master	G1/0/12	L2 link	L2 switch 7	Fa0/2	First
Master	G1/0/13	L2 link	L2 switch 8	Fa0/1	Second
Master	G1/0/14	L2 link	L2 switch 8	Fa0/2	Second
Master	G1/0/15	L2 link	L2 switch 9	Fa0/1	Second
Master	G1/0/16	L2 link	L2 switch 9	Fa0/2	Second
Master	G1/0/17	Distri 2	Distri 2	G1/0/17	NOC
Master	G1/0/21	Main server	Primary server	NIC	NOC
Master	G1/0/22	Backup server	Secondary server	NIC	NOC

Distribution switch 2

Device name	Port number	Description	Opposite end deice	Port number	Floor
Slave	G1/0/1	Firewall	Primary firewall	G1/1	Ground
Slave	G1/0/2	Firewall	Secondary firewall	G1/1	Ground
Slave	G1/0/3	L2 link	L2 switch 1	Fa0/3	Ground
Slave	G1/0/4	L2 link	L2 switch 1	Fa0/4	Ground
Slave	G1/0/5	L2 link	L2 switch 2	Fa0/3	Ground
Slave	G1/0/6	L2 link	L2 switch 2	Fa0/4	Ground
Slave	G1/0/7	L2 link	L2 switch 3	Fa0/3	Ground
Slave	G1/0/8	L2 link	L2 switch 3	Fa0/4	Ground
Slave	G1/0/9	L2 link	L2 switch 5	Fa0/3	First
Slave	G1/0/10	L2 link	L2 switch 5	Fa0/4	First
Slave	G1/0/11	L2 link	L2 switch 6	Fa0/3	First
Slave	G1/0/12	L2 link	L2 switch 6	Fa0/4	First
Slave	G1/0/11	L2 link	L2 switch 7	Fa0/3	First
Slave	G1/0/12	L2 link	L2 switch 7	Fa0/4	First
Slave	G1/0/13	L2 link	L2 switch 8	Fa0/3	Second
Slave	G1/0/14	L2 link	L2 switch 8	Fa0/4	Second
Slave	G1/0/15	L2 link	L2 switch 9	Fa0/3	Second
Slave	G1/0/16	L2 link	L2 switch 9	Fa0/4	Second
Slave	G1/0/17	Distri 1	Distri 1	G1/0/17	NOC
Slave	G1/0/21	Main server	Primary server	NIC	NOC
Slave	G1/0/22	Backup server	Secondary server	NIC	NOC

2.8 Floor Plans

This company has three floors within the same building. Below we have provided the floor plans for the entire building.

Ground Floor:

- Server room
- One department with 78 users

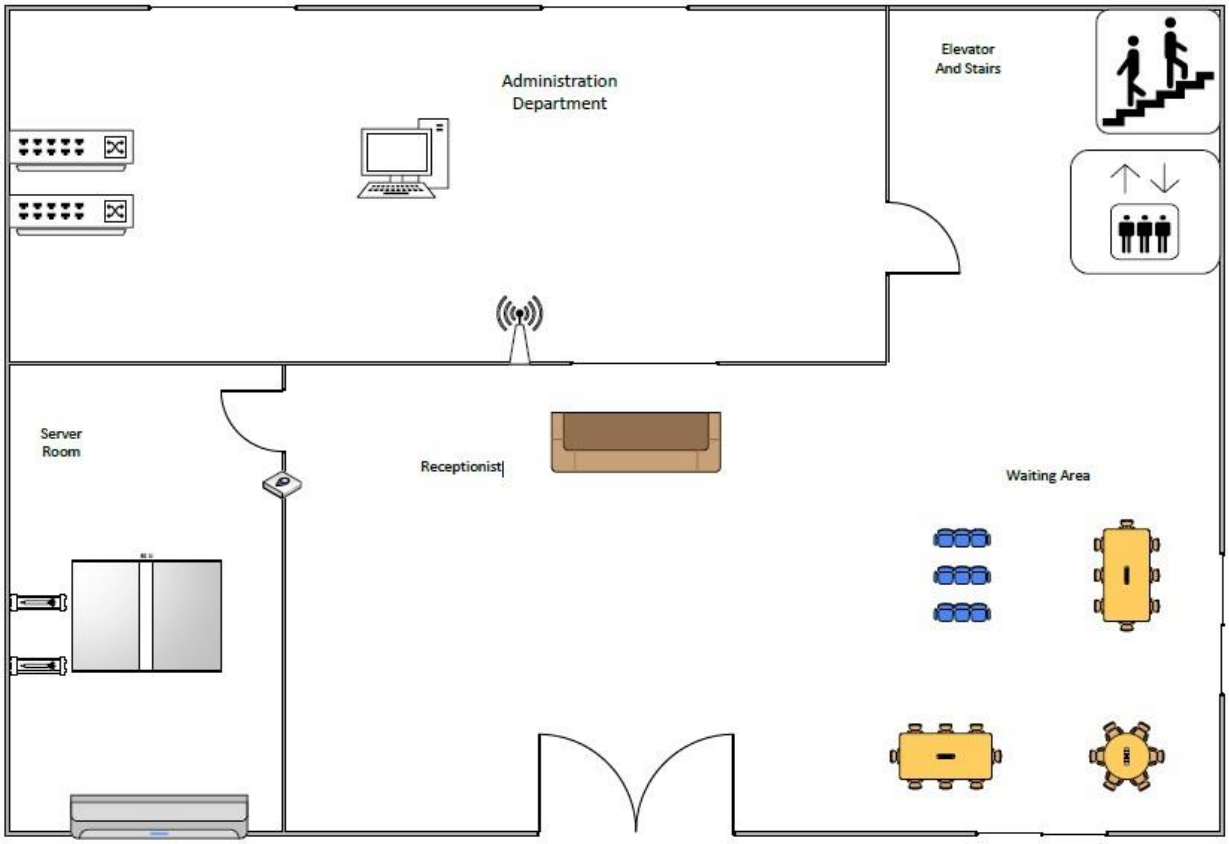


Figure 2.4

First Floor:

- Three departments with 170 users

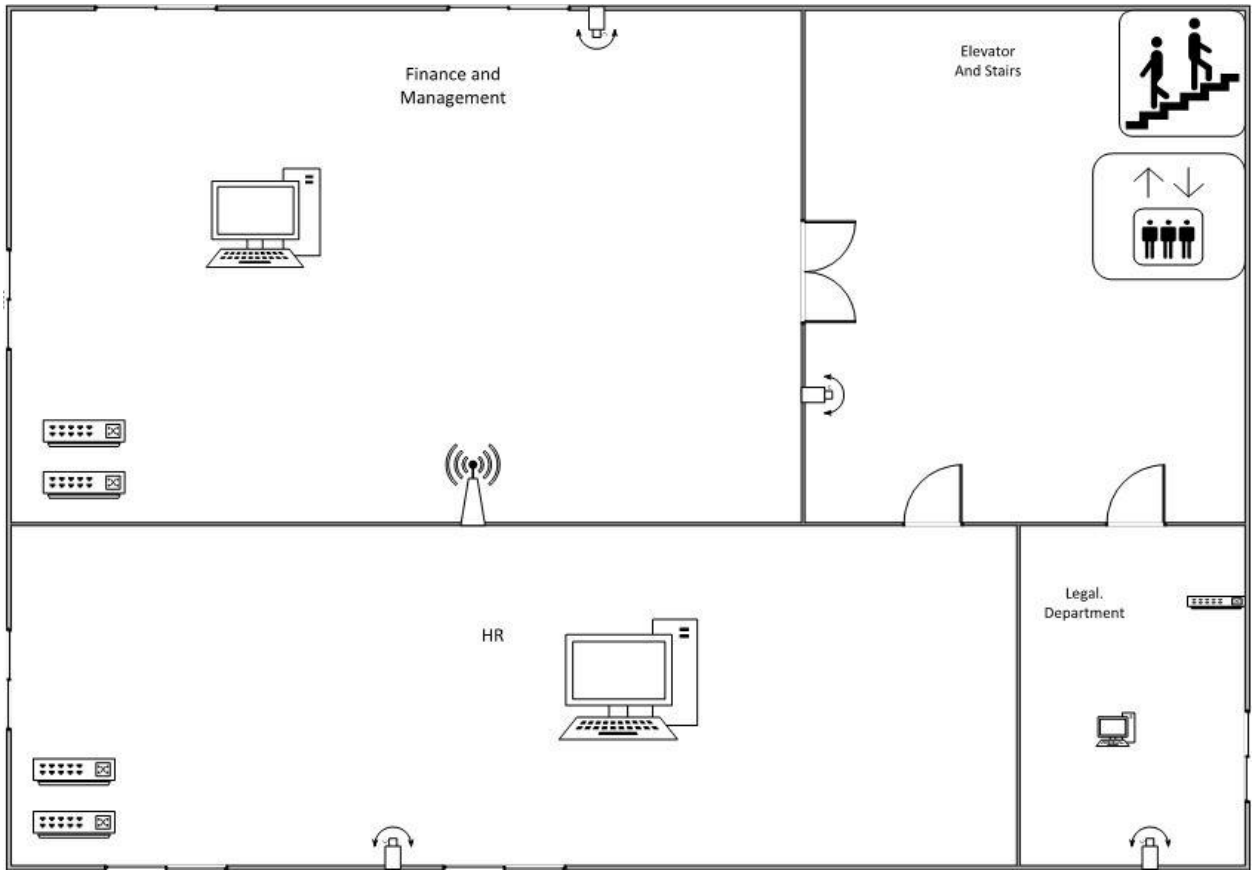


Figure 2.5

Second Floor:

- Three Departments with 300 users

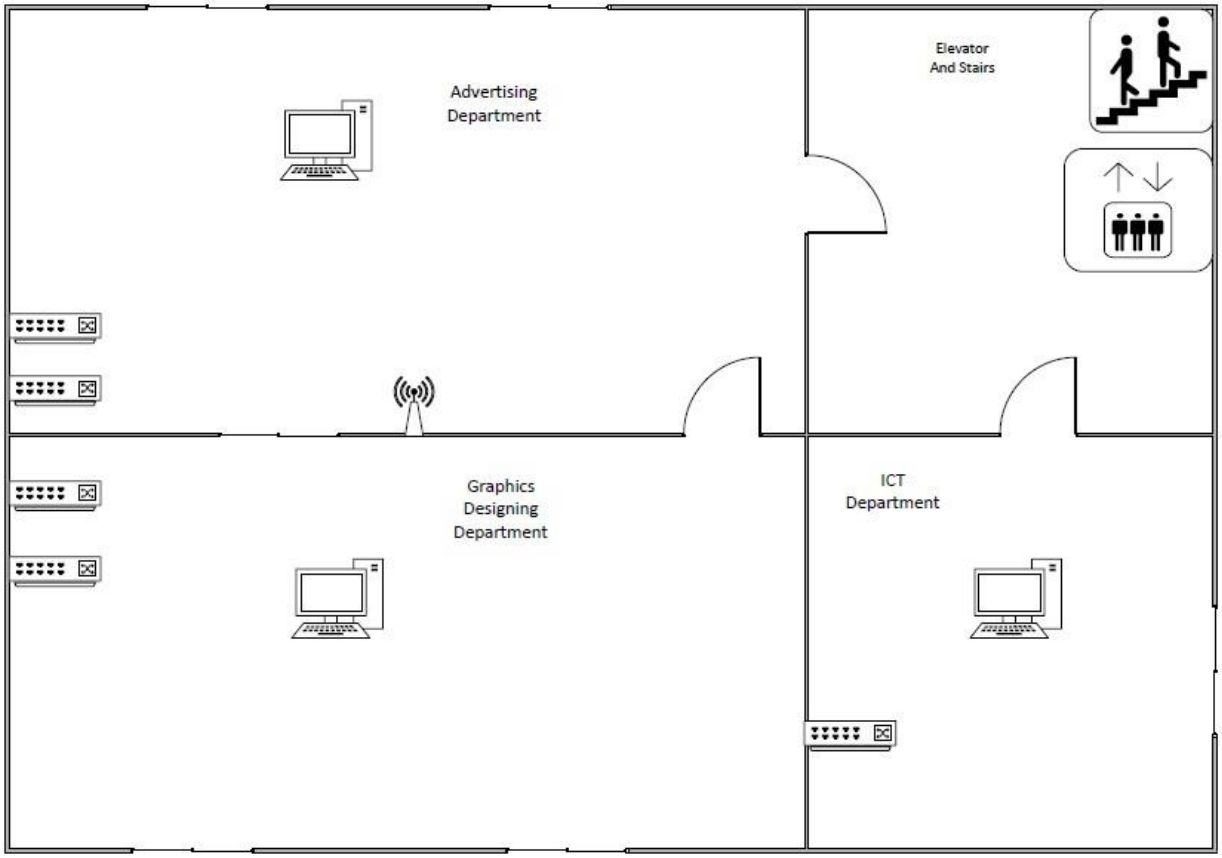


Figure 2.6

2.9 Network Caballing

- Each department connected with its computers and other wired devices by high speed 10Gbps CAT6 Ethernet cables because from the short distance between devices to each switch device in the departments.
- Additionally, each department has given the wireless network access through access points.
- Every access layer switch (Layer 2 switches) belongs to each department is connecting to the distribution multilayer switches through multimode fiber optic cables because of longer distance. Each ether-channel consists of 2 multimode fiber optic cables.
- Each access layer link connected to distribution layer is Ether-channeled for redundancy and to provide high capacity.
- Two leased lines have purchased from the same ISP with single mode fiber optic cables due to its ability to carry data far more distance without facing any problems.
- All multilayer switches connected with multimode fiber cable for link aggregation and redundancy. Each ether-channel consists with three cables providing high bandwidth between core layer and the access layer.
- Network is designed to give maximum redundancy so incase if the main leased line fails the secondary leased line will propagate network traffic through the backup route.

2.10 Leased line costing

There are two leased lines purchased from the same ISP to redundant the Internet and provide load balancing.

Types of users in the Department

- Light users - Email, Web browsing
- Moderate users - File Downloads, Streaming Music & Video, Uploading Music & Video, Cloud based resources.
- Heavy users - High Bandwidth Demand, Intense Internet-based Application Use, Multiple Devices per User, Interactive Web Conferencing.

We have implemented the following bandwidth limits for the users categorized in the above scenario

- Light users - 256 Kbps
- Moderate users - 512 Mbps
- Power User / Heavy users - 1 Mbps

Department	Users	Usage	Bandwidth
2nd Floor			
IT Department	50	1Mbps	50Mbps
Graphic Designing	150	2Mbps	300Mbps
Advertising Department	100	2Mbps	200Mbps
1st Floor			
HR	70	256Mbps	17.5Mbps
Legal	20	256Mbps	5Mbps
Finance & Management	80	1Mbps	80Mbps
Ground Floor			
Reception	8	256Kbps	2Mbps
Administration Department	70	1Mbps	70Mbps

Table 2.4

Total bandwidth for the company = 724.5 Mbps. We can assume that 1 Gbps primary connection is enough for this company considering the future growth. As for the secondary ISP connection we can have a connection of 0.450 Gbps.

Sri Lanka telecom is the internet provider to the Mediamora company. The most reliable option was to contact Sri Lanka Telecom and get a link that can fulfil the bandwidth up-to 1 Gbps. When you get those customized package solutions it's hard to mention a fixed monthly internet free. According to our research we have got in between 2.0 – 2.5 million rupees per month as internet fee with this solution.

2.11 Protocols and services

Main Routing Protocol

- For this topology we use Single-Area OSPF as the main routing protocol. This has several benefits because in vast network the routing table would be big and quite complex to observe.
- OSPF can simplify routing tables compared to other routing protocols.

Backup Routing Protocol

- We have chosen RIP as the back-up routing protocol in case if the main routing protocol fails.
- Mainly due to the simplicity of configuration

Ether Channel

Ether Channel technology was originally developed by Cisco as a LAN switch-to-switch technique of grouping several Fast Ethernet or Gigabit Ethernet ports into one logical channel. When an Ether Channel is configured, the resulting virtual interface is called a port channel. The physical interfaces are bundled together into a port channel interface. We have used three fiber optic cables in a single ether channel.

Ether Channel technology has many advantages:

- Most Configurations Performed on Ether channel interface, ensuring Consistency throughout link.
- Relies on existing switch ports- no need for upgrades.
- Load Balances Between link on the same Ether channel.
- Creates an aggregation viewed as one logical link by STP.

Provides redundancy because overall link is viewed as one logical connection. If one physical link within a channel goes down, this does not cause a change in the topology and does not require STP recalculation.

HSRP (Hot Standby Router Protocol)

HSRP is a cisco proprietary. It provides high network availability by providing first hop routing redundancy. HSRP is use in a group of routers for selecting an active device and a standby device.

RSTP (Rapid Spanning Tree Protocol)

RSTP speeds the recalculation of the spanning tree when the Layer 2 network topology changes. RSTP can achieve much faster convergence in a properly configured network, sometimes in as little as a few hundred milliseconds. RSTP redefines the type of ports and their state. If a port is configured to be an alternate port or a backup port, it can immediately change to a forwarding state without waiting for the network to converge.

PXE Server (Pre-boot Execution Environment)

A specific technique to solve the operating system issues because any operating system failure will affect the quality of service or it might delay the work process for each employee. In this case, the information technology department will have to resolve these problems as soon as possible to keep the work process safe. Also, most operating system problems could be solved by re-imaging the computers which are setting up new operating systems for these machines. If the IT technician need to install operating systems individually, it would be more difficult and plenty of time will be wasted.

In this situation, there should be a tool that can support more than one task at the same time. A PXE server is the appropriate service to support operating systems to the clients on any local networks. This service can be provided by installing a PXE server on the local network, and the clients can access and obtain the operating systems by only connecting to the same network by using network cards.

Proxy Server

The proxy server usually designs to hold the resources that come from the internet and save them until the users request them again. This tool allows prioritization based on user needs. Also, this server can hold the information that is requested from Internet by users and save them on it's his hard disk. This server is designed to serve many users inside the local network at the same time this server has been placed alongside the primary internet service providers (ISP) and the one of the main multilayer switch in the network. The reason for that is that all the packets that are going from the local network and coming from outside to inside the instructions are passing through this main connection.

DHCP Server

This server is responsible for assigning internet protocols (IP) automatically for all users on the internet. Situations without this service address, all the IPs need to be assigned manually, situation which does not scale well.

This server can provide clients IPs even when they lose the IP that has been assigned to their devices, and the server will provide different IP for each request from the same subnet (range of IPs in the same network). We implement DHCP on all desktops and laptops except router interfaces and servers.

DHCP Failover Server

DHCP Failover is responsible for assigning same pool of IP addresses to computers in the LAN when primary DHCP is failed to assign IP addresses to LAN. Act as a backup server, configured partner server (backup) to standby mode.

File & Storage server

File and storage server makes easier to share files inside the network with many users. It does not perform any computations or run programs for clients. Only store files/ documents/ records and used to share them inside the network and, we have given each department, each user a certain limit of storage.

Active Directory & Domain Control server

The domain controller server is a special kind of computer that has specific properties for special tasks. This server is a part of Microsoft Corporation suite which is designed for security and other services inside any network. On the networking sides this server is used to establish a login and other security permissions. This server is placed inside main server in a VM.

Many common computers which are in the local network can be controlled by the Windows Server specifically the active directory tool in the server. The active directory contains many services but, in this part, all the configurations focus on the domain controller utility depending on the project scope. The Active Directory Domain Services (ADDS) represent a specific service that is placed in the Windows server operating system as a part of the server's software.

Web Server

Websites are often the most prioritize part of any network because this system retains all information for the users and customers from inside and outside the organization. A web server can be attacked from outside; this happens when the webserver opens a port on the computer for public uses. In addition, all the information in the computer will be at risk. If there is a database server on the same machine which includes all the users' information, this could represent a very big problem for any network around the world.

In this part of the project, design and implementation of the network has been focused on the data which created by the company under the contracts of many organizations.

- Important aspect of saving the website information was locating the web server in a secure place.
- Configuring ACL to prevent accessing web server from other departments such as Terminal department.

Radius Server

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics. Created by Livingston (now owned by Lucent), RADIUS is a de facto industry standard used by a number of network product companies and is a proposed IETF standard.

2.12 Server room specification

A server room is used to store, power and operate computer servers and their associated components. This room is part of a data center, which typical houses several physical servers lined up together in different form factors, such as rack mounted, or in tower or blade enclosures.

Spatial Specifications

- Room should have no windows.
- Ensure space is large enough for future growth.
- Ceiling should be at least nine feet.
- Should have drop ceiling return to exhaust heat.

Equipment Specifications

- Computer racks should have a clearance of at least 42 inches.
- All racks should have proper grounding and seismic bracing.
- Computing equipment should have a maximum electrical intensity of 300 watts per square foot.
- Server room should contain fire, smoke, water and humidity monitors.

Cooling Specifications

- Racks should be arranged in a hot-aisle/ cold-aisle configuration.
- Use cooling equipment with variable speed fans.
- Plan for redundancy, do not rely on building cooling for back-up.
- Under floor cooling systems require a raised floor with a minimum height of 24 inches, with the ability to hold the weight of server racks and equipment

Electrical Systems Specifications

- Computer equipment and HVAC should have separate power panels.
- There should be no heat-generating support equipment.
- Electrical systems should have an isolated ground, grounding grid and dedicated neutral.
- Separate back-up power should be available for data center.
- The electrical system should have a shunt trip for purposes of emergency shutdown.

2.13 Devices and equipment and Pricing

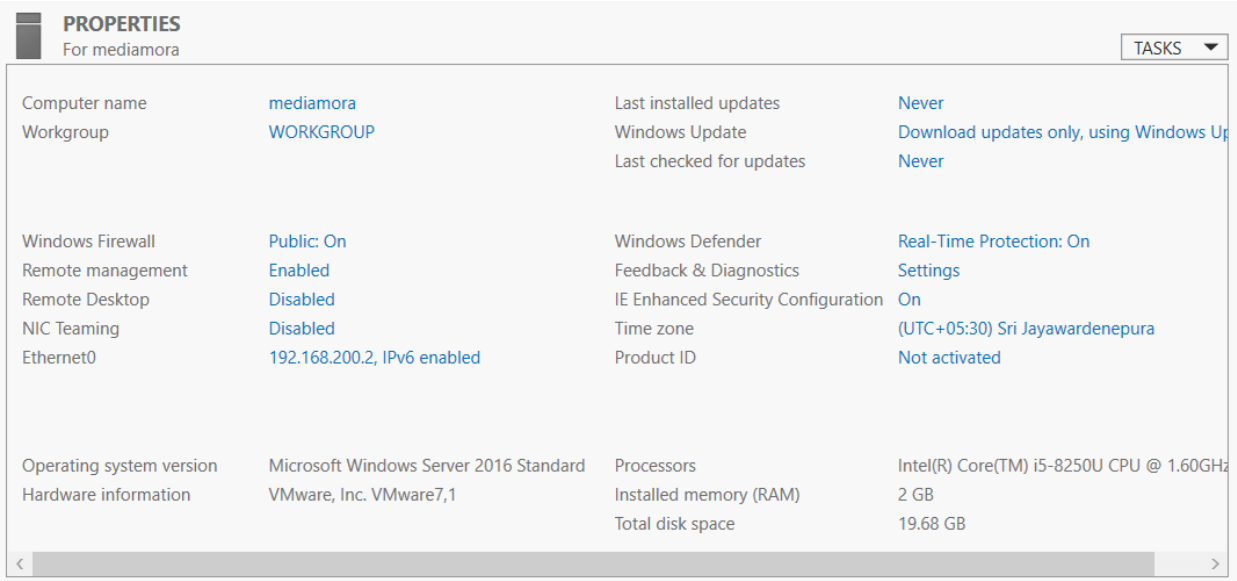
Floor	Area	Equipment
Ground floor	Reception	pc-5, one access point ,cisco 3560-C (1)
	waiting area	
	server room	layer 3 6800 series (2),
	Administrator department	pc-60, one access point, Cisco SGE2010(2)
1st floor	HR	pc-70, one access point, Cisco SGE2010(2)
	Legal	pc-20, one access point, Cisco 2960 x(1)
	Finance & management	pc-20, one access point, Cisco 2960 x(1)
		pc-20, one access point, Cisco 2960 x(1)
2nd floor	IT dept.	pc-60, one access point, Cisco SGE2010(2)
	Graphics	pc-80, one access point, Cisco SGE2010(2)
	Advertise	pc-60,one access point, Cisco SGE2010(2)

Table 2.5

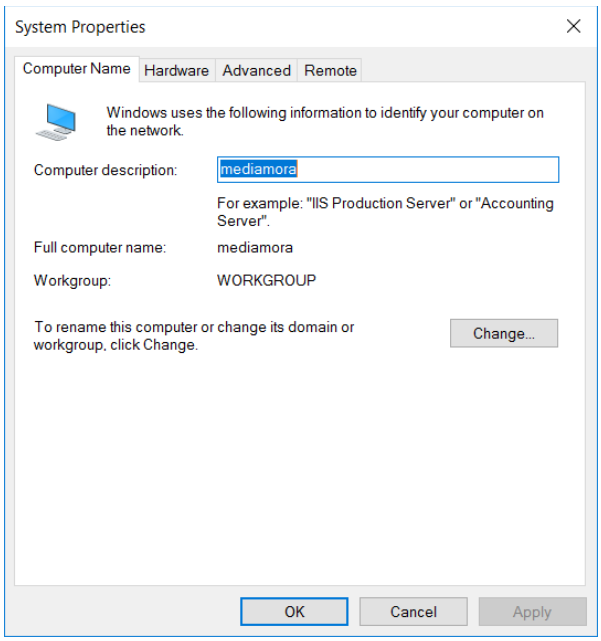
Equipment	Unit Price	Qts	Total
First floor Cisco Devices			Rs. 6,864,68.00
Second floor Cisco Devices			Rs. 2,528,18.00
Third floor Cisco Devices			Rs. 3,647,61.00
PowerEdge T130 Tower Server			Rs. 400,000.00
Patch Panel	Rs. 9,800.00	15	Rs. 147,000.00
Cable manager	Rs. 1,500.00	16	Rs. 24,000.00
CAT 6 305m cable box	Rs. 29,000.00	15	Rs. 435,000.00
Keystone	Rs. 210.00	600	Rs. 126,000.00
Rj45 connectors CAT6	Rs. 50.00	1300	Rs. 65,000.00
Patch Code 0.5m	Rs. 150.00	200	Rs. 30,000.00
12u wall mount rack	Rs. 19,000.00	3	Rs. 57,000.00
19u server rack	Rs. 25,000.00	1	Rs. 25,000.00
Sunbox	Rs. 50.00	300	Rs. 15,000.00
Faceplate	Rs. 325.00	300	Rs. 97,500.00
			Rs. 2,725,547.00

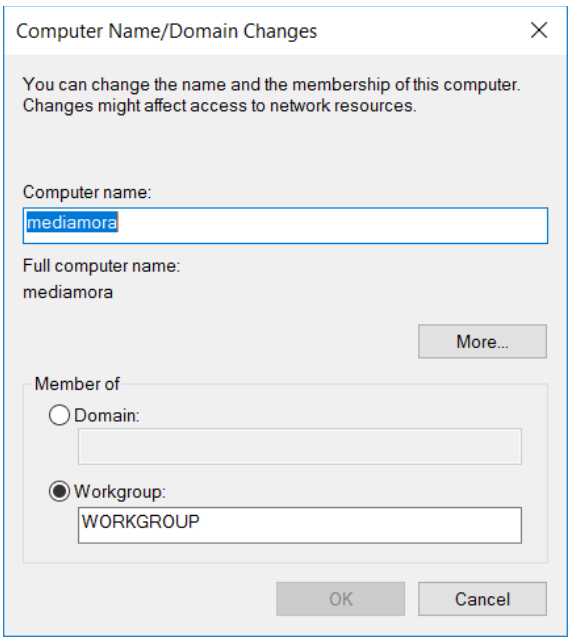
3.Implementaion

3.1 Configuring basic server configurations

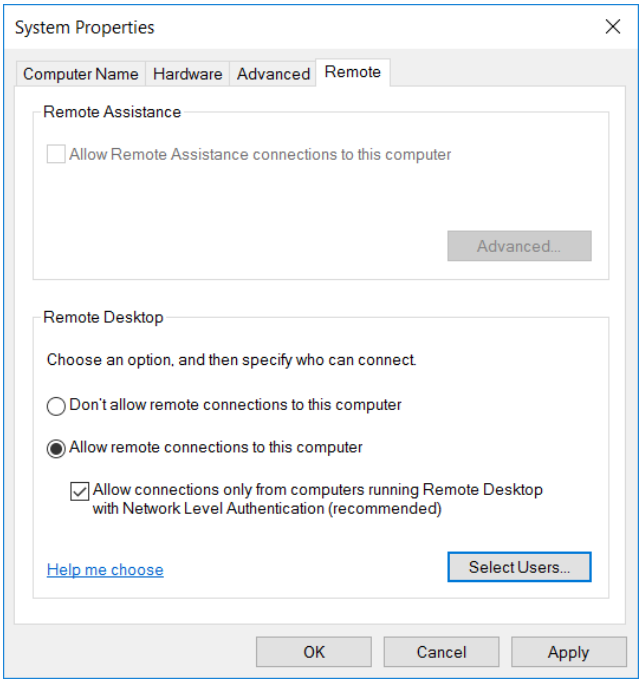


After installing the server assign a static IP address in a separated VLAN. Servers are hosts that contacted by the normal users frequently. In order to have connectivity between servers 24/7 servers are assigned static IP addresses.

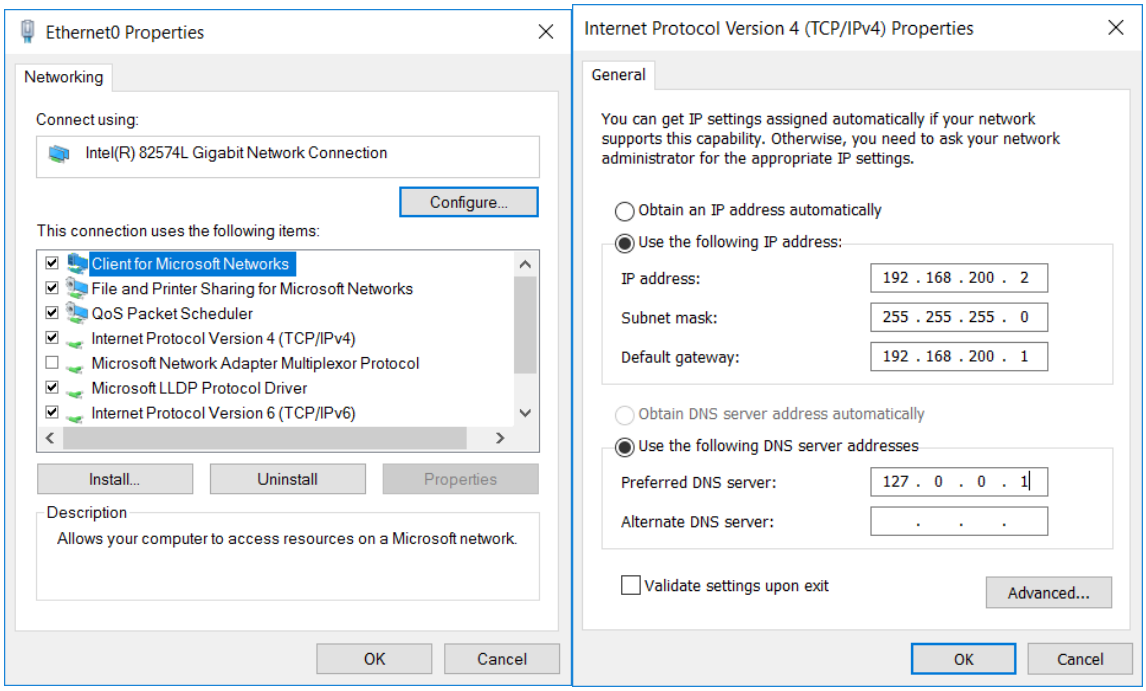




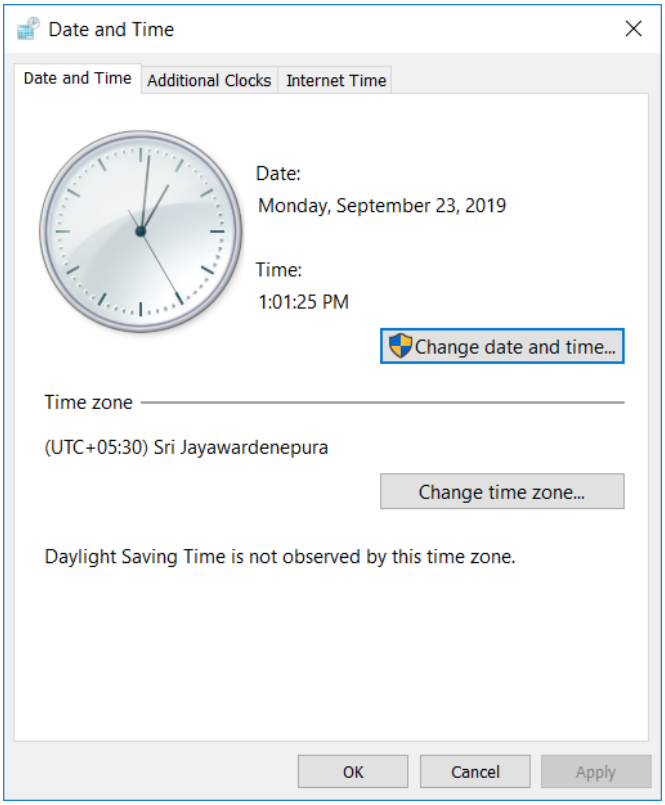
Step 1 – Change the computer name to easily recognize it in the domain



Step 2 – Enable the remote desktop connection to connect with server remotely

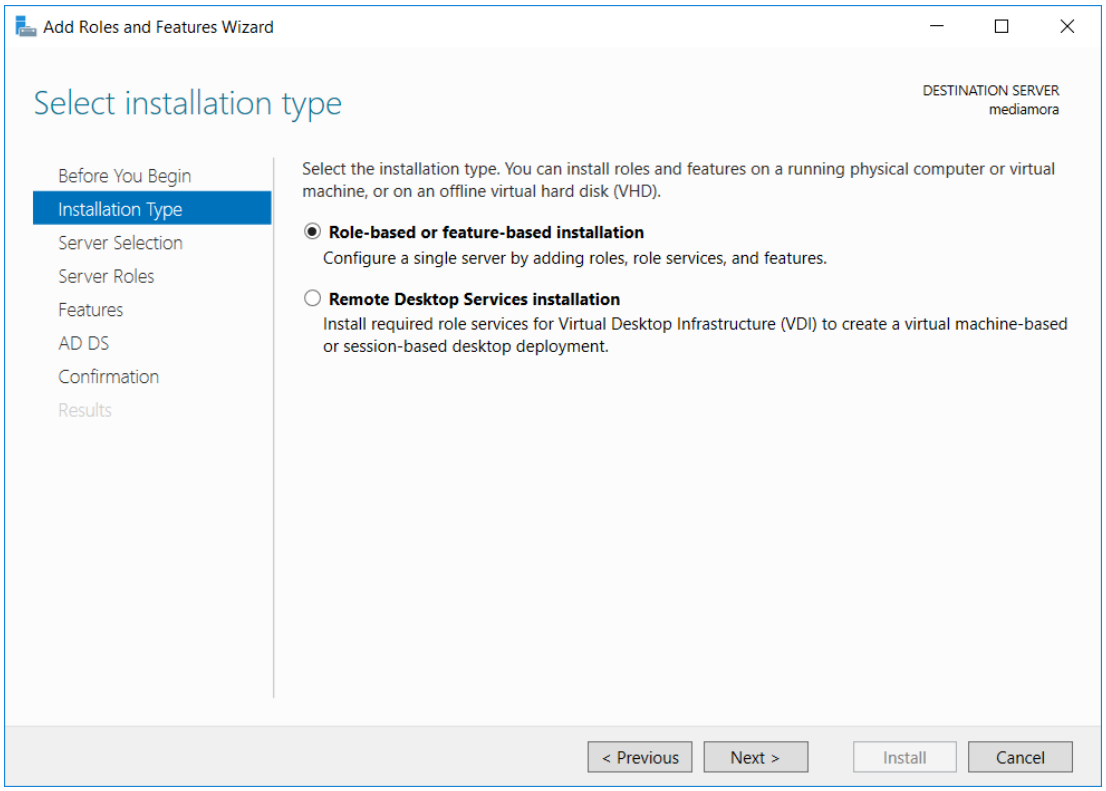


Step 4 – Configure a static IP address with proper subnet mask & a default gateway. Preferred DNS should be the same address as the IP address

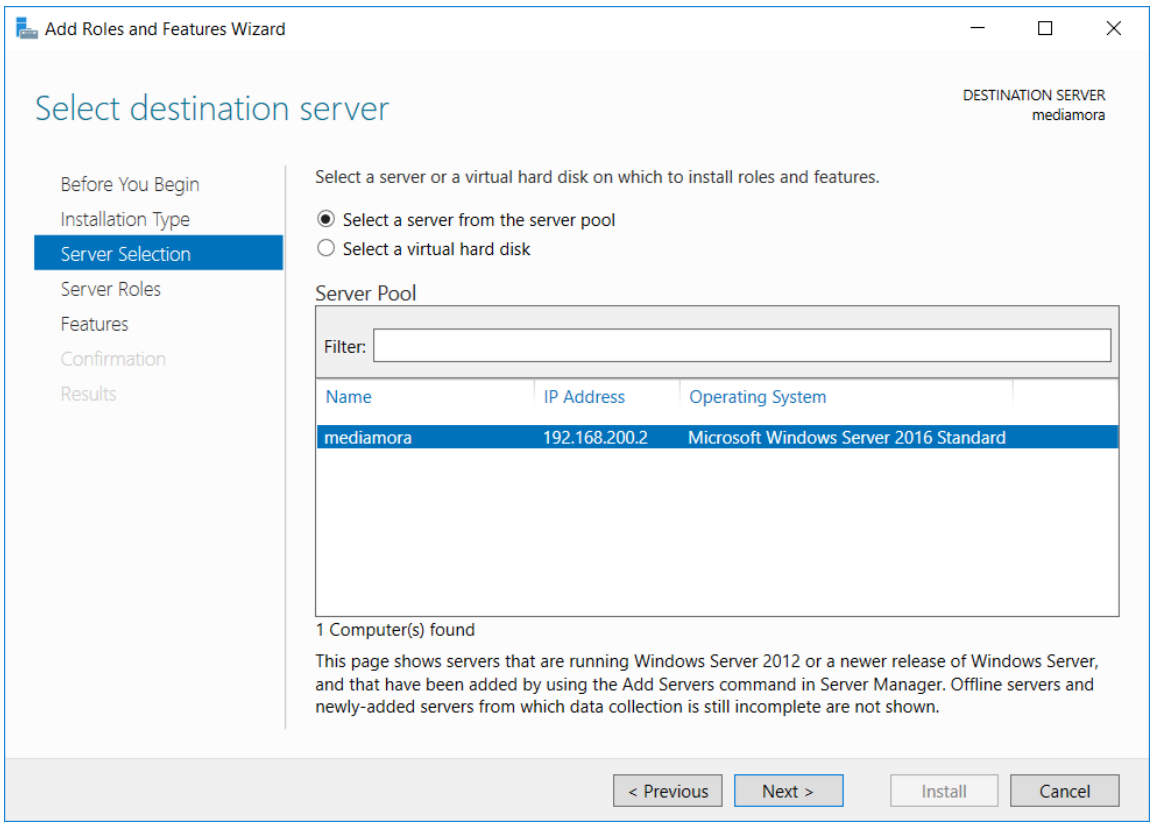


Step 5 – Change the proper time zone because wrong time zones may cause many issues

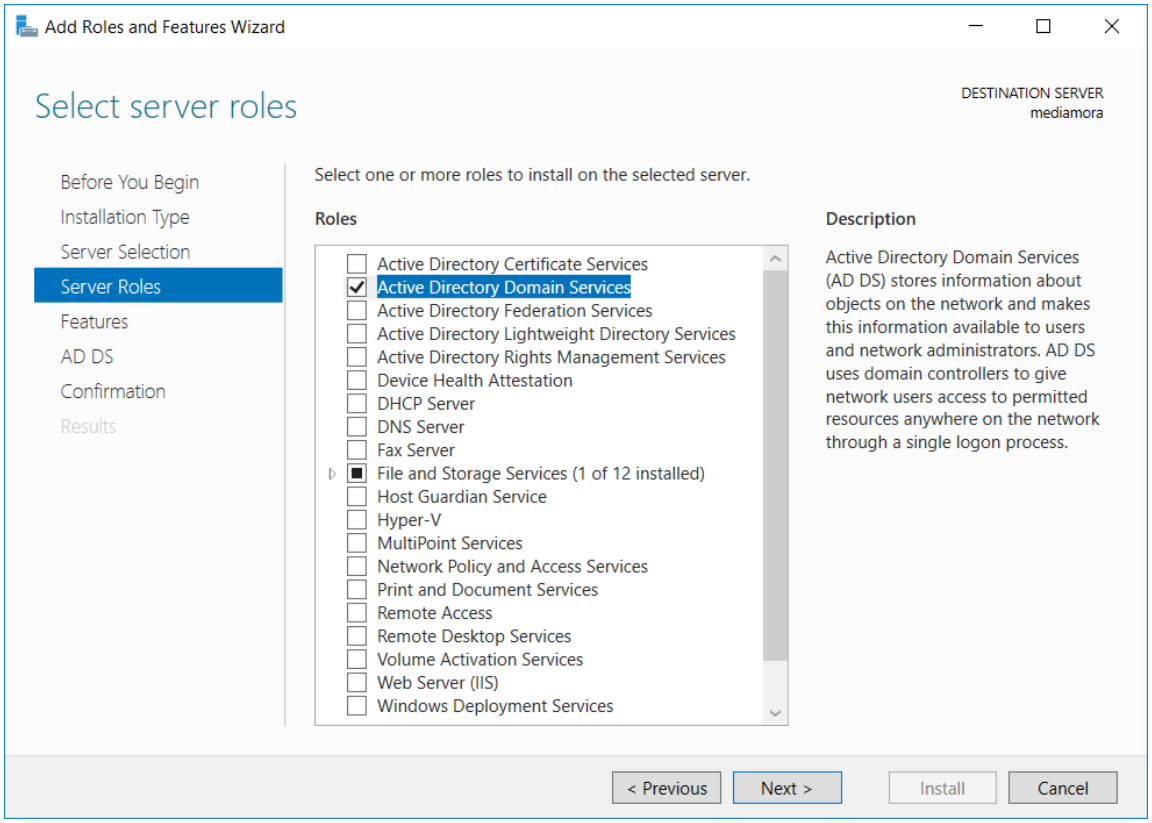
3.2 Implementing Active Directory Domain Controller



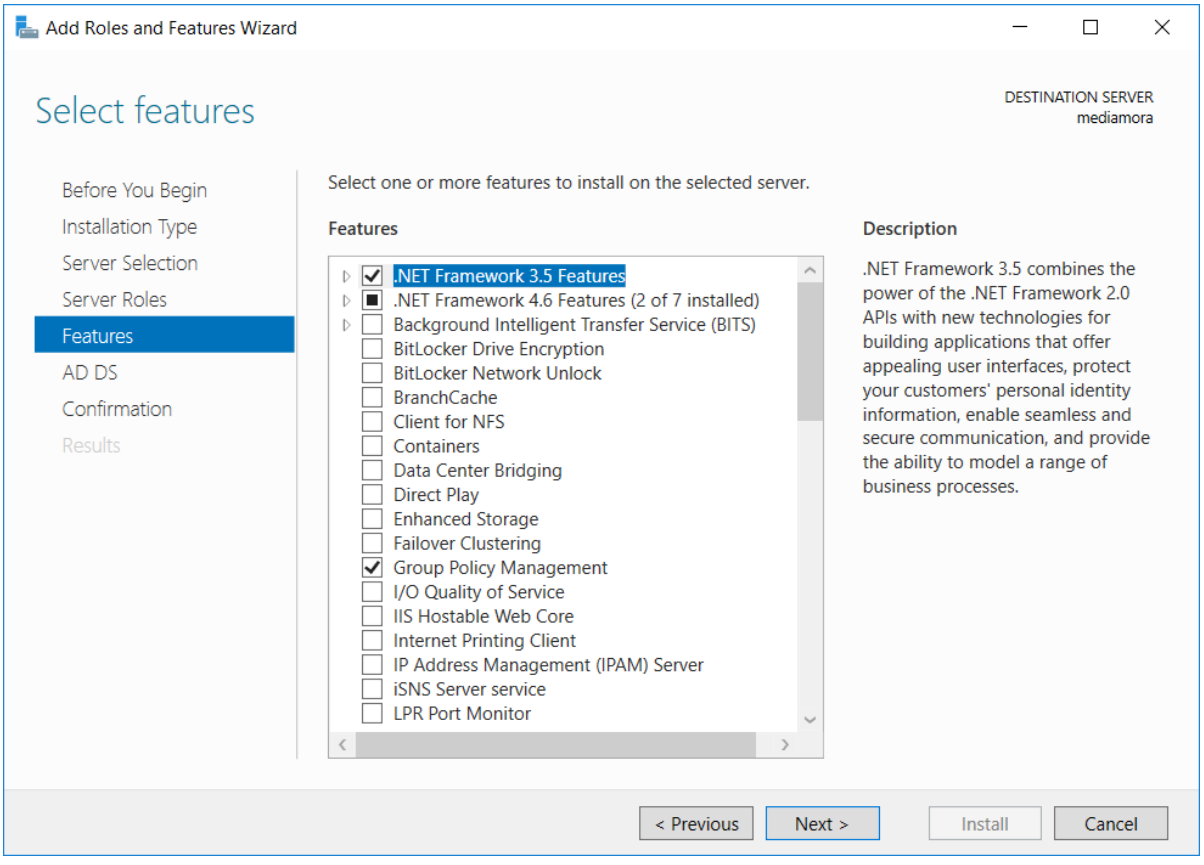
Step 1 – Select role-based or feature based installation option and click next



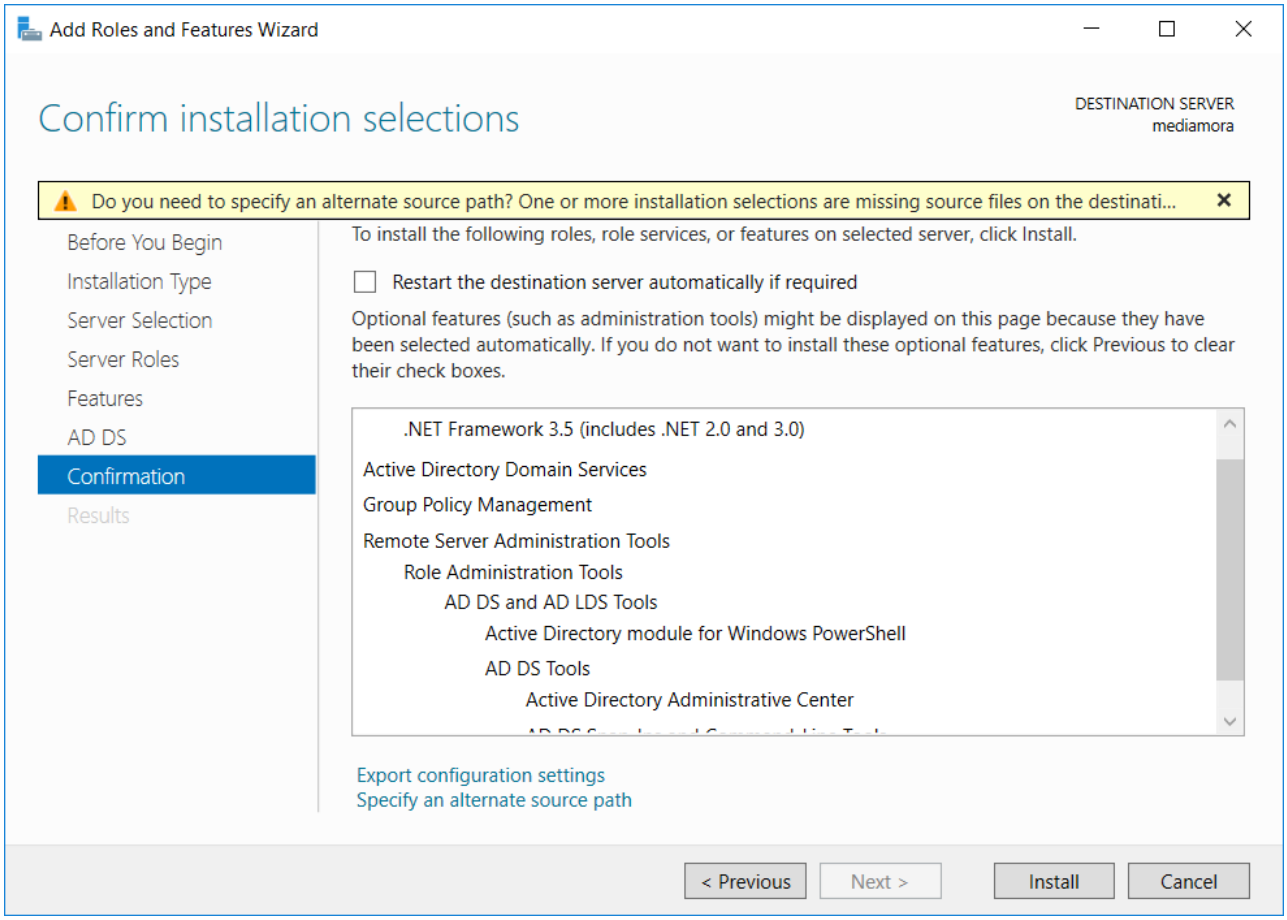
Step 2 – Select the server which the role should be installed and click next



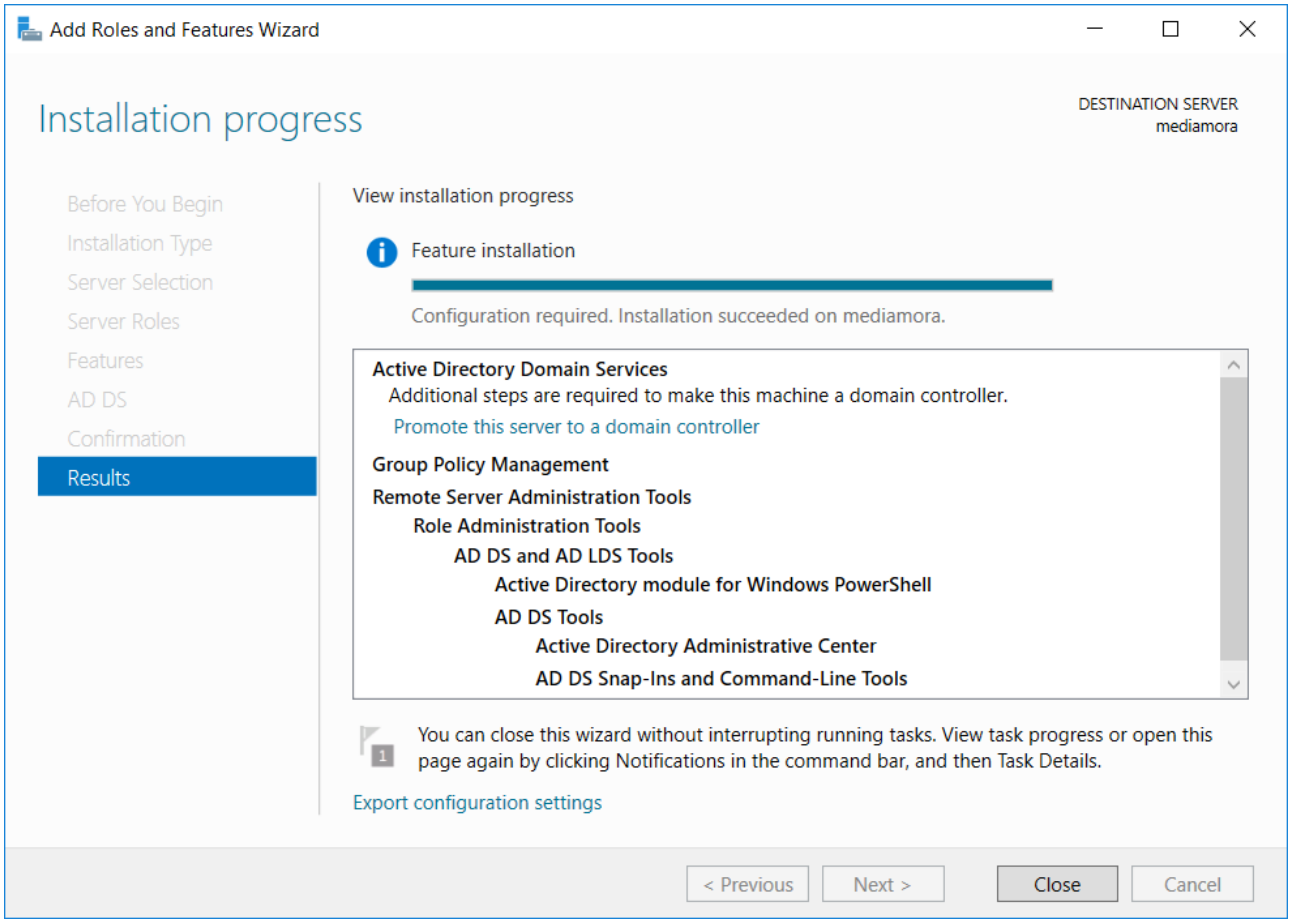
Step 3 – Select the role active directory domain services and click next



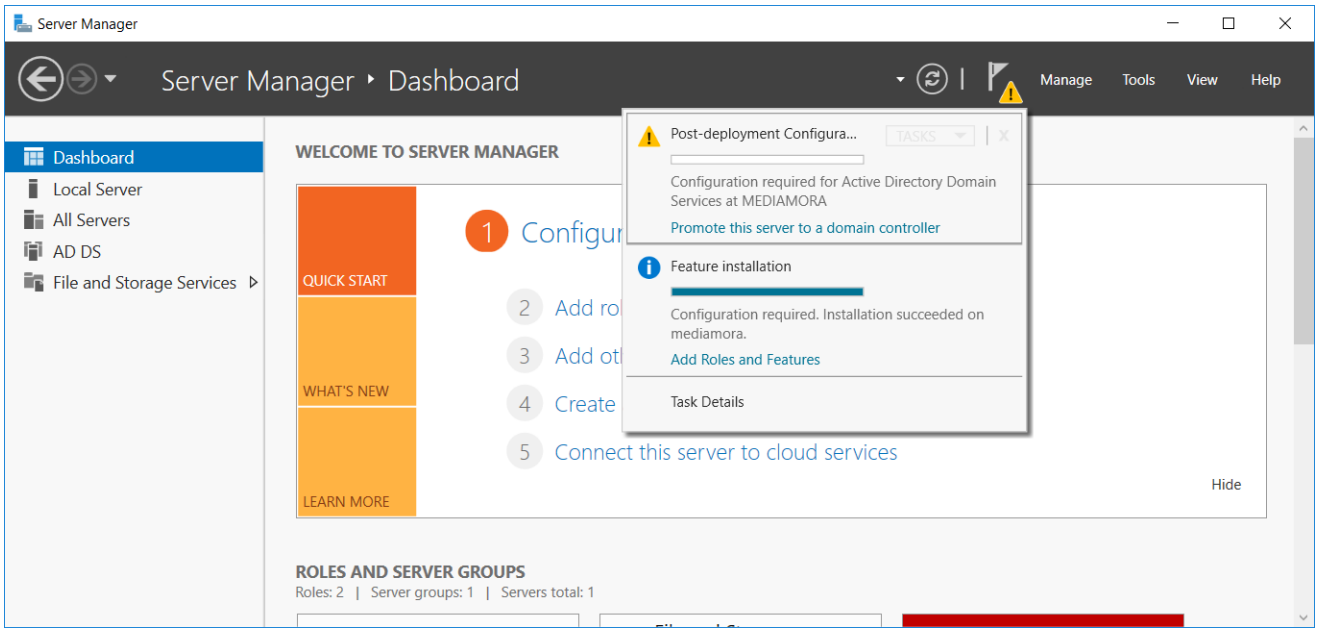
Step 4 – Select the required features and click next



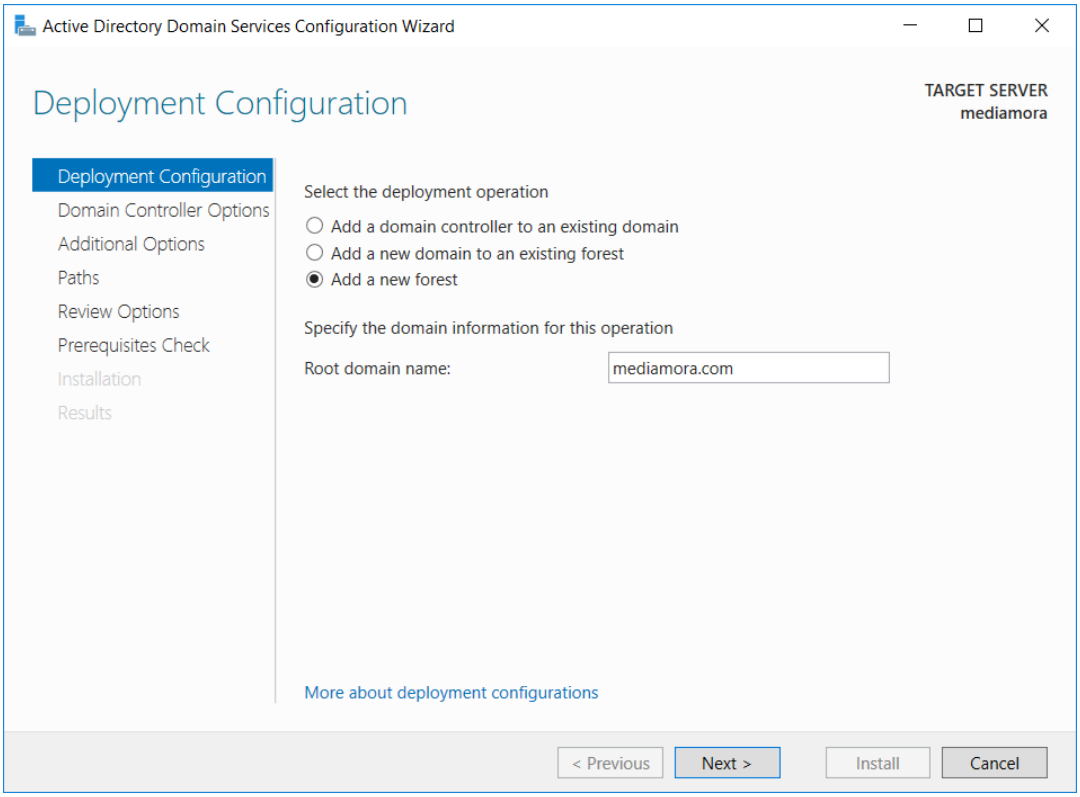
Step 5 – Click install to finalize the setup



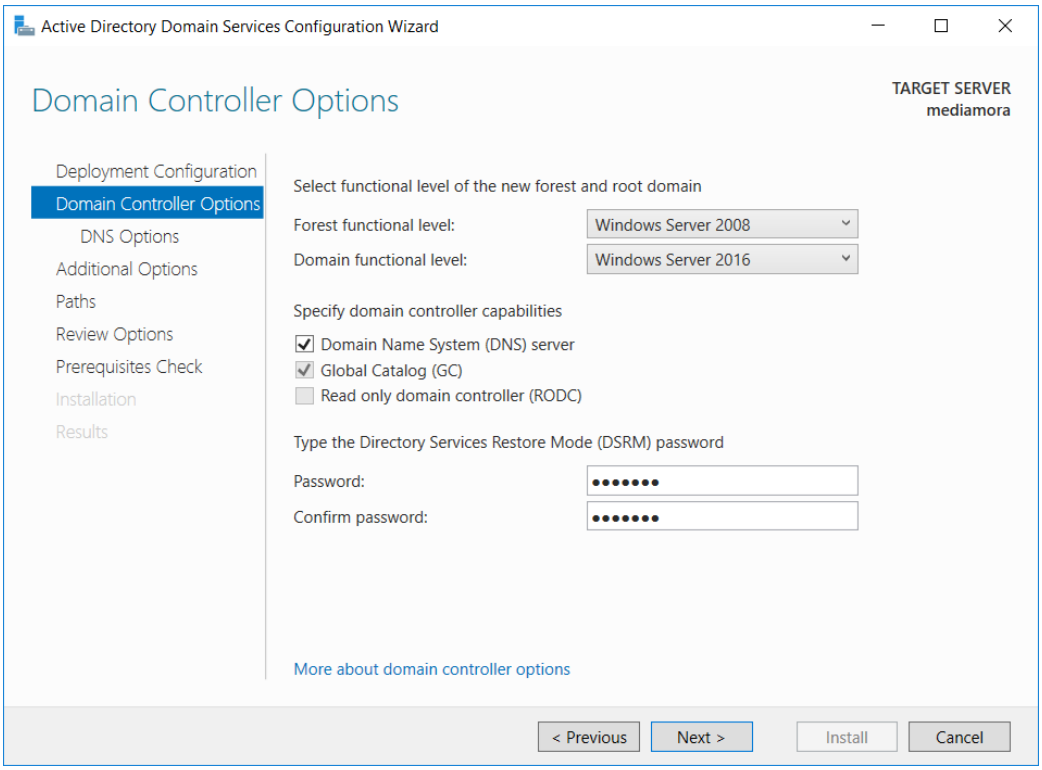
Step 6 – It will take some time to install the roles after that close it and proceed to the next step



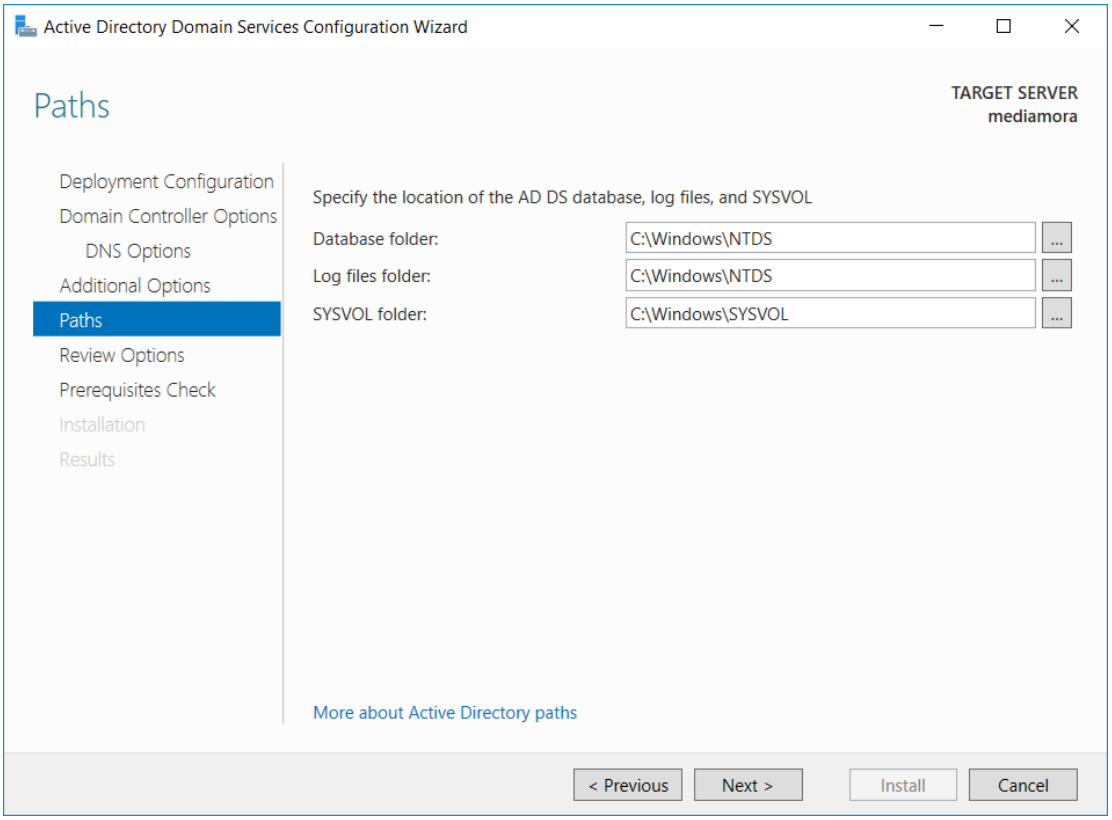
Step 7 – After closing the window it will prompt to promote the server to a domain controller



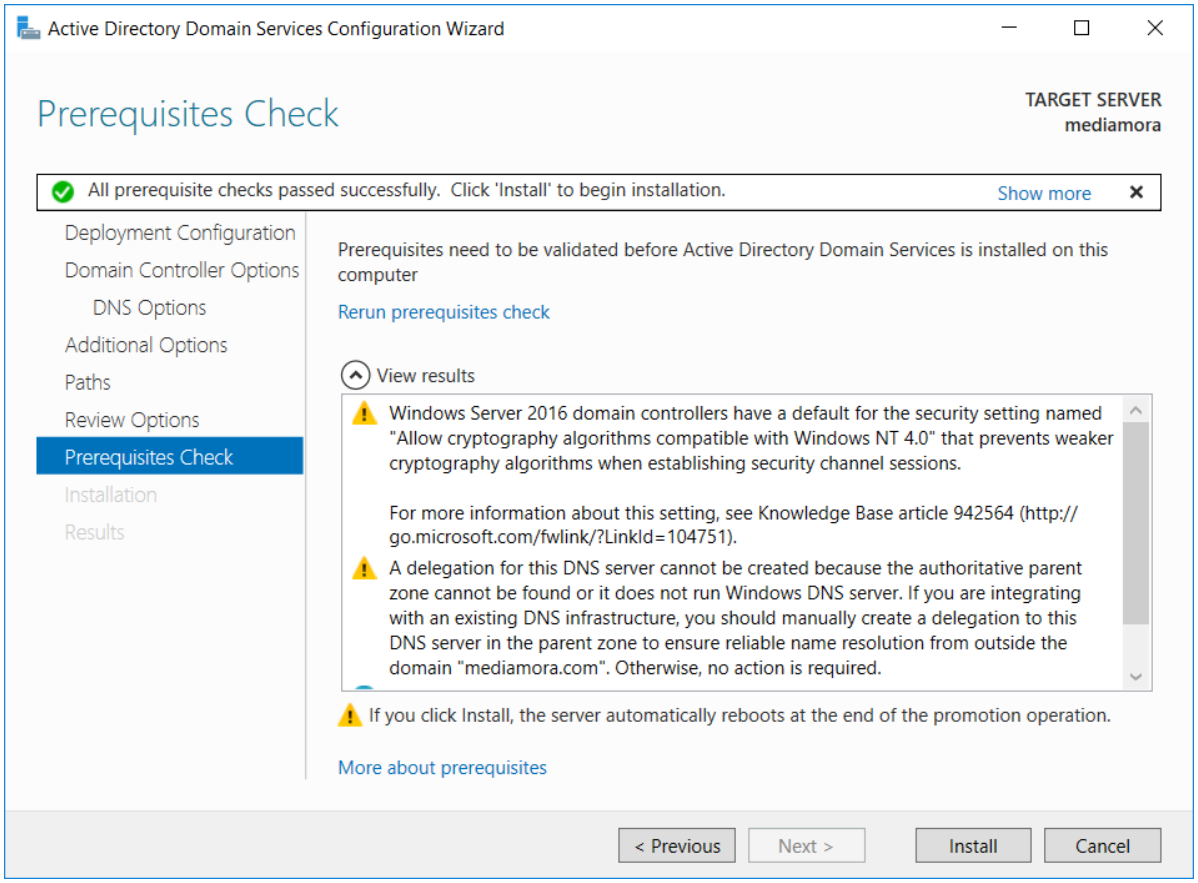
Step 8 – Add a new forest name for the domain and proceed to the next step



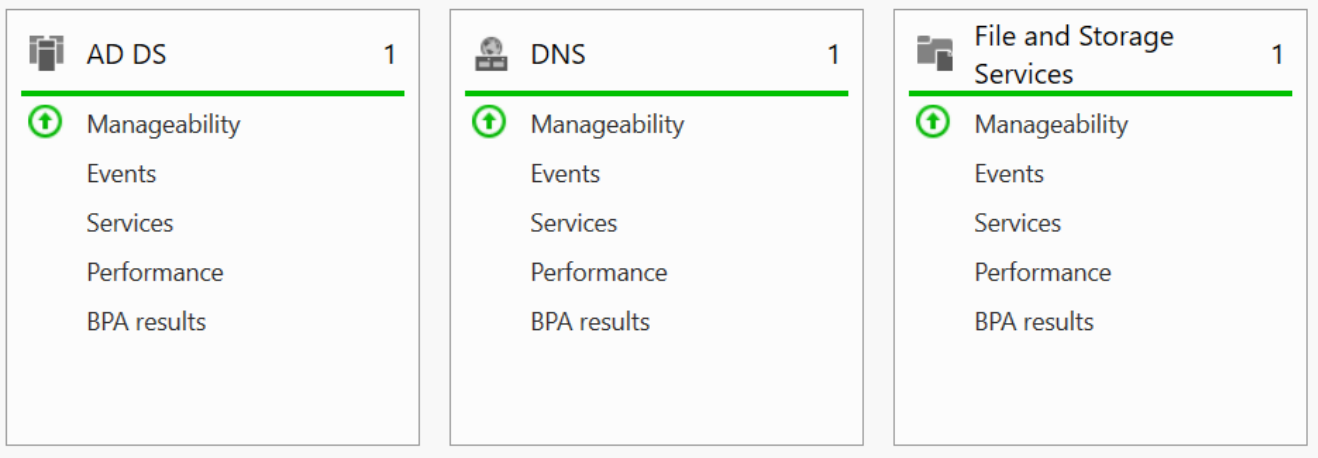
Step 9 – These options are available for early domain users. If you have a domain of early version of windows server images you should specify those in the forest function level. Proceed to the next step after entering a password



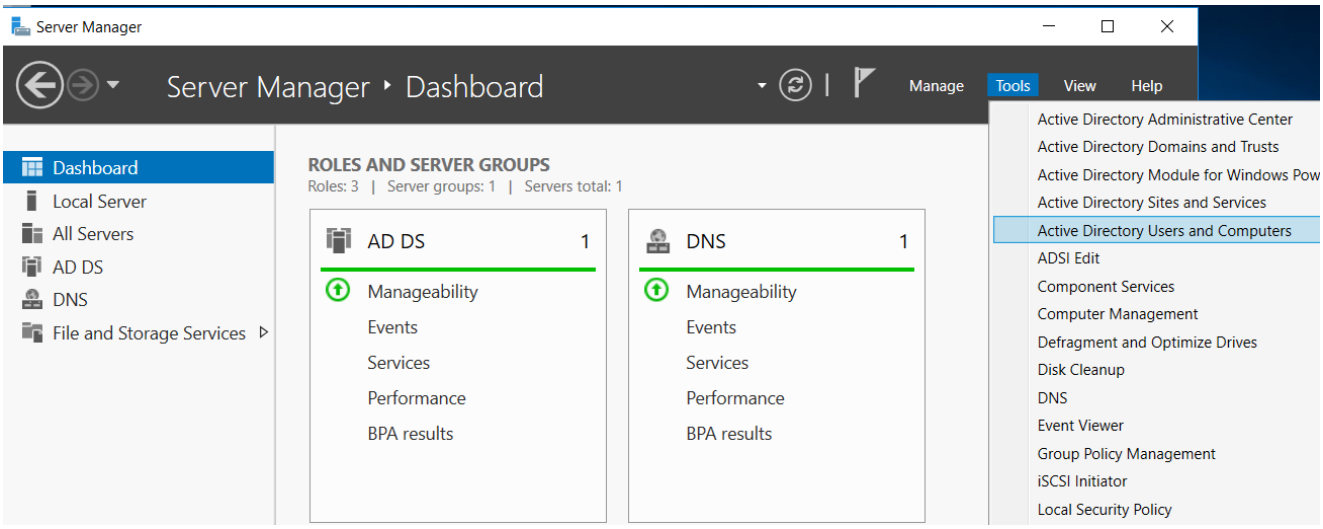
Step 10 – These are the paths which contains the database of the AD DS



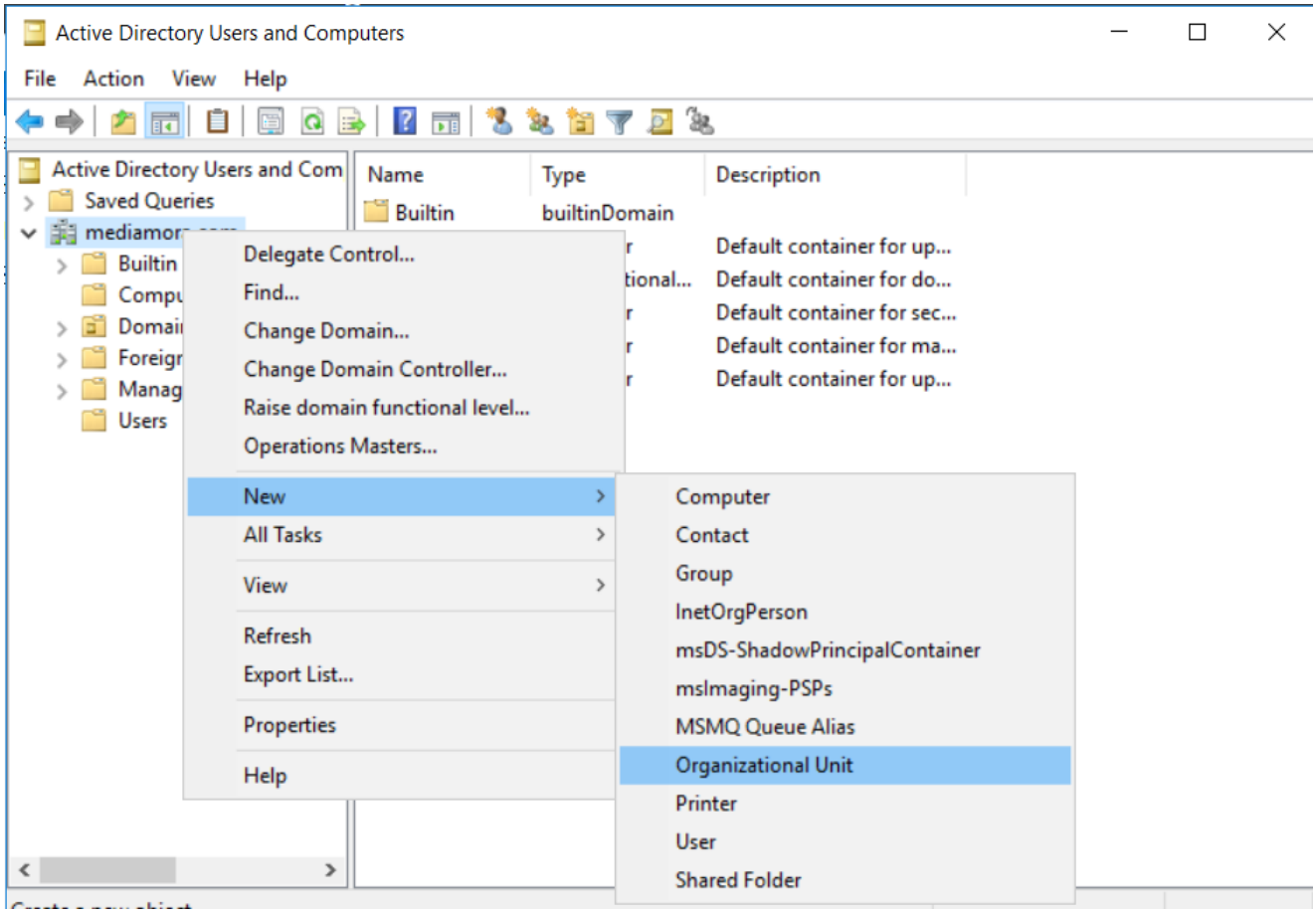
Step 11 – After doing the necessary selections click install to publish the new domain



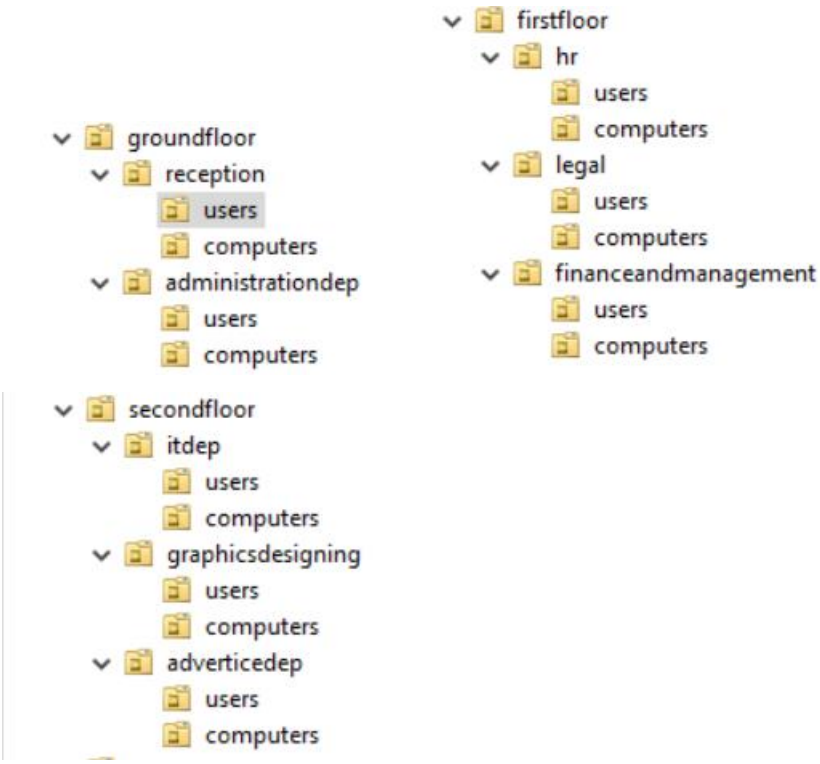
Step 12 – DNS server also will be automatically installed when installing AD DS



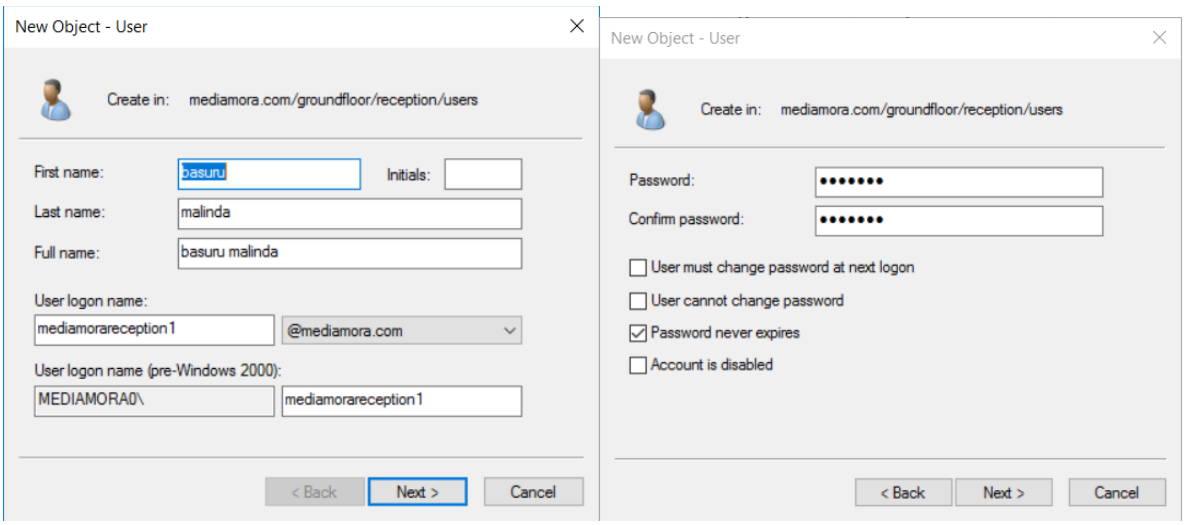
Step 13 – After the installation click users & computers in the tools menu to add users



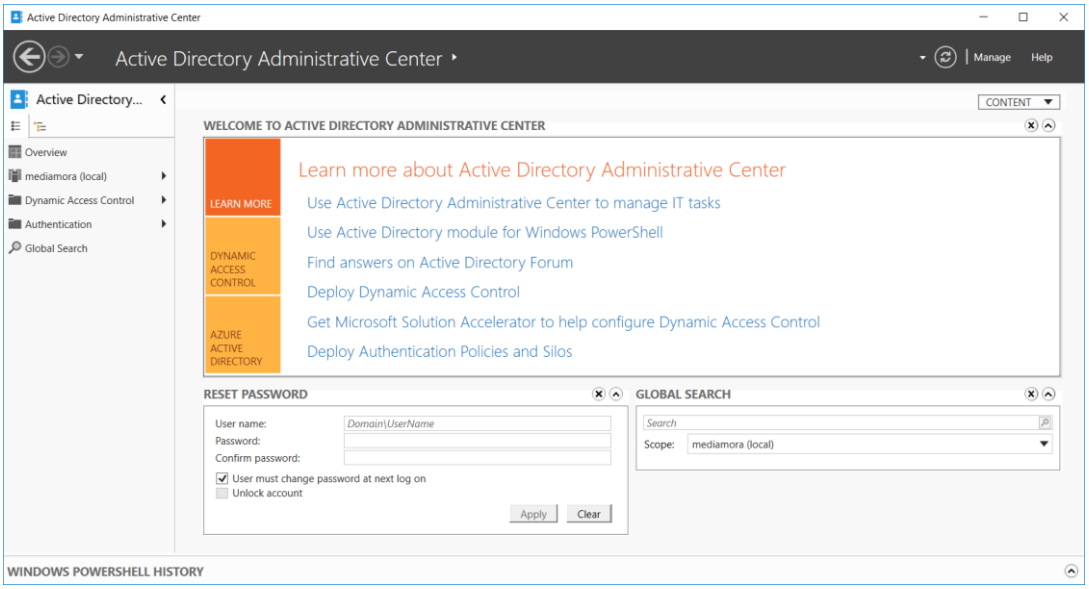
Step 14 – Right click the domain and add a new organizational unit

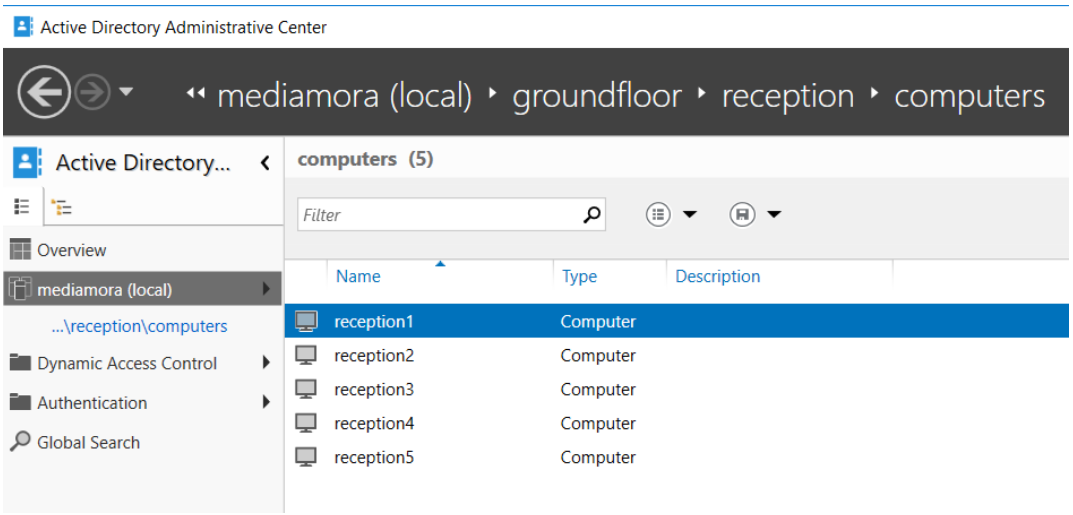


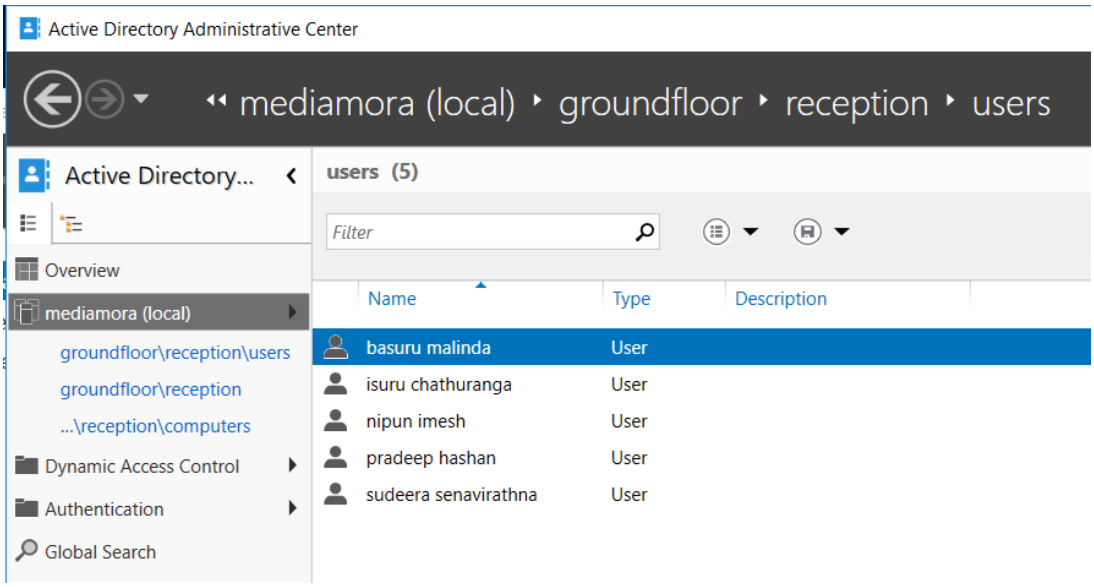
Step 15 – Create a OU for the central office and then create another OU within that for all users in the company



Step 16 – Add users by right clicking the users OU and enter the details and a strong password.

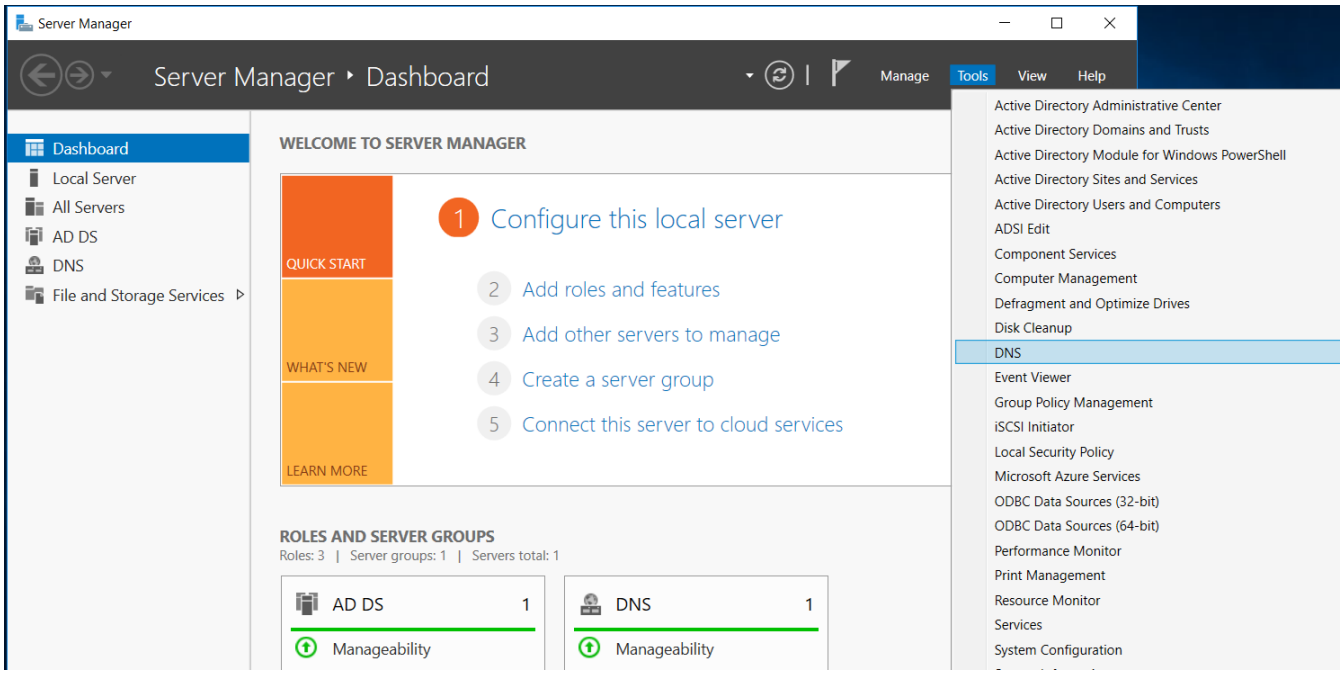




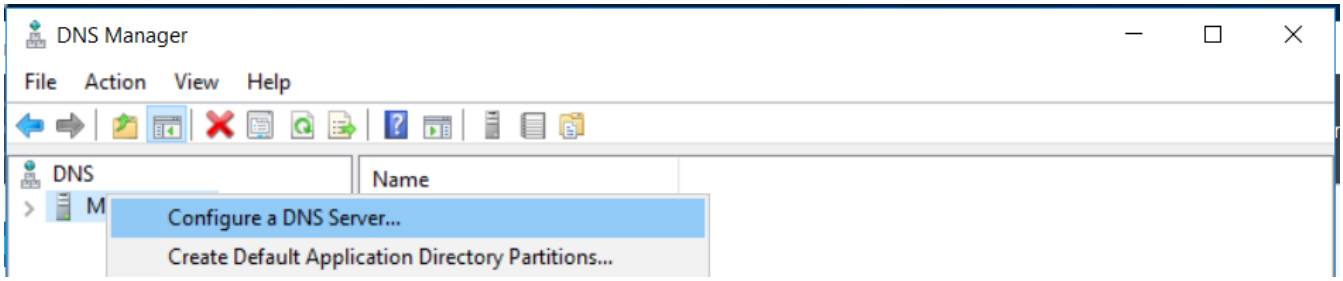


All the users, groups & computers can be managed through the active directory administrative center

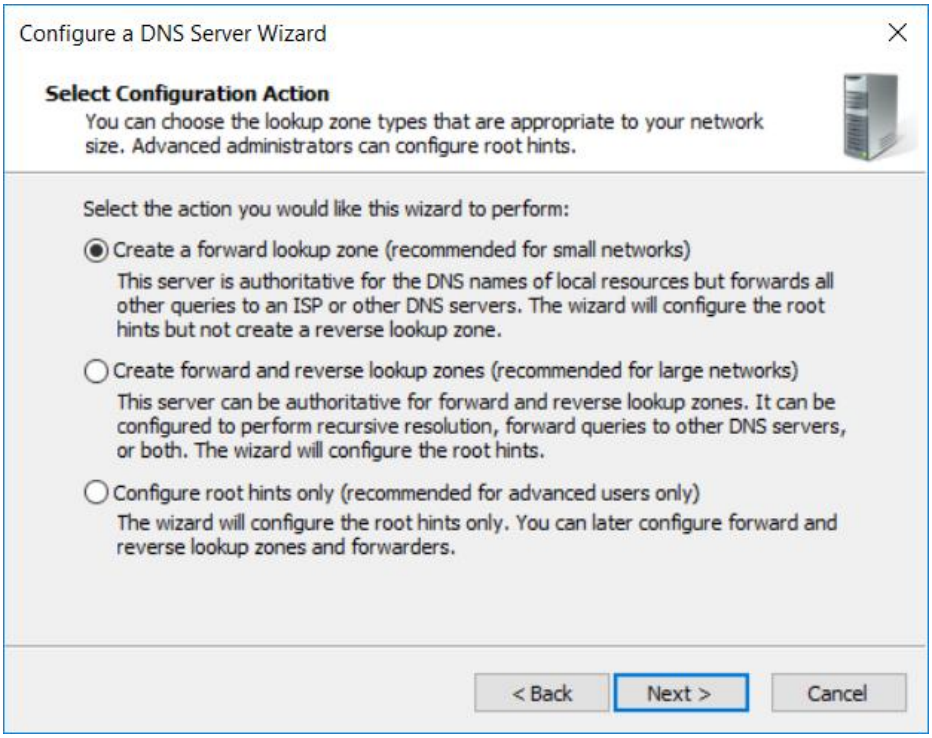
3.3 Implementing a DNS server



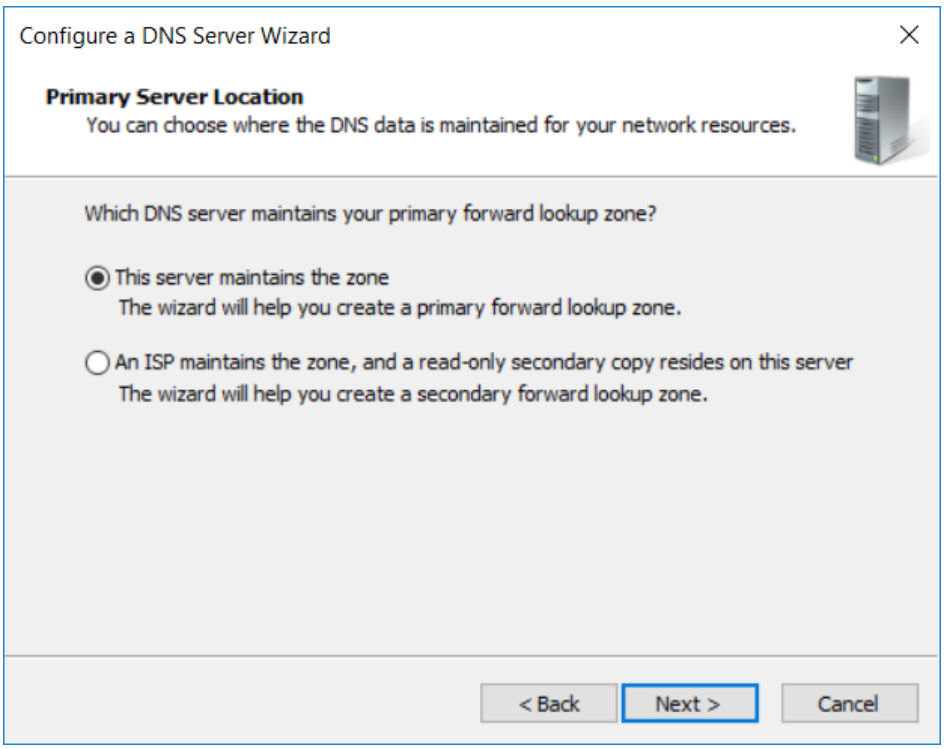
Step 1 – Click the DNS option in the tools menu



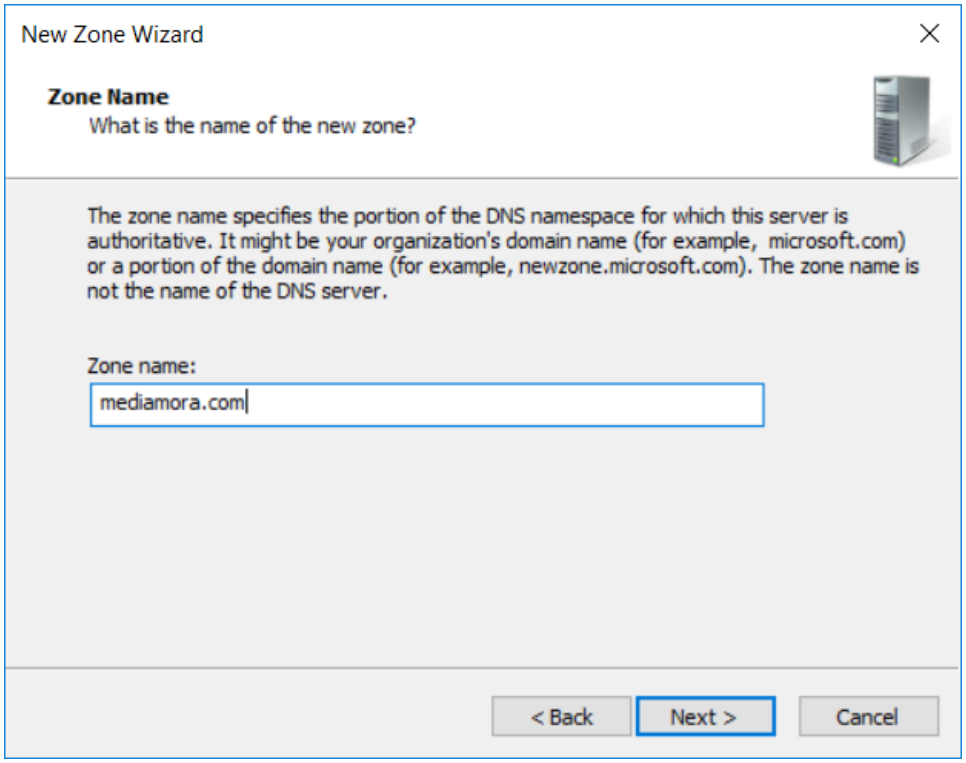
Step 2 – Right click the Server and click configure a DNS server



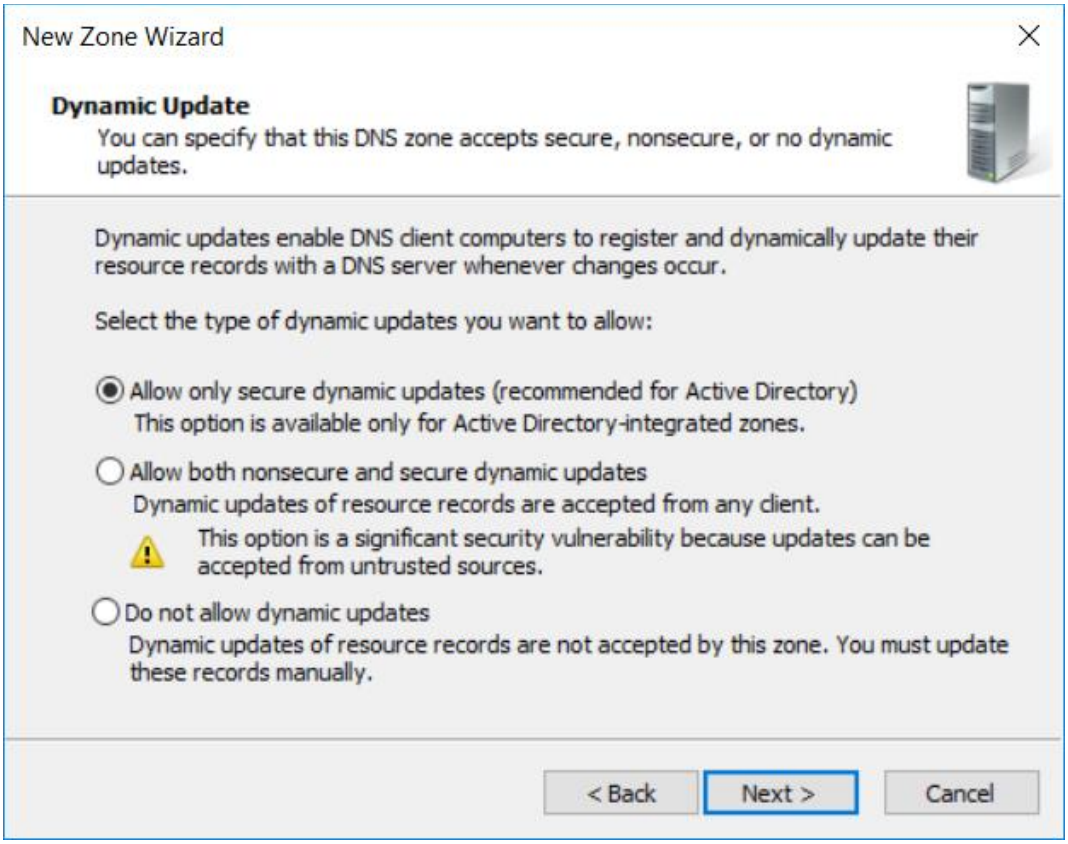
Step 3 – From the menu select primary zone because we only need to create a forward lookup zone for a small company



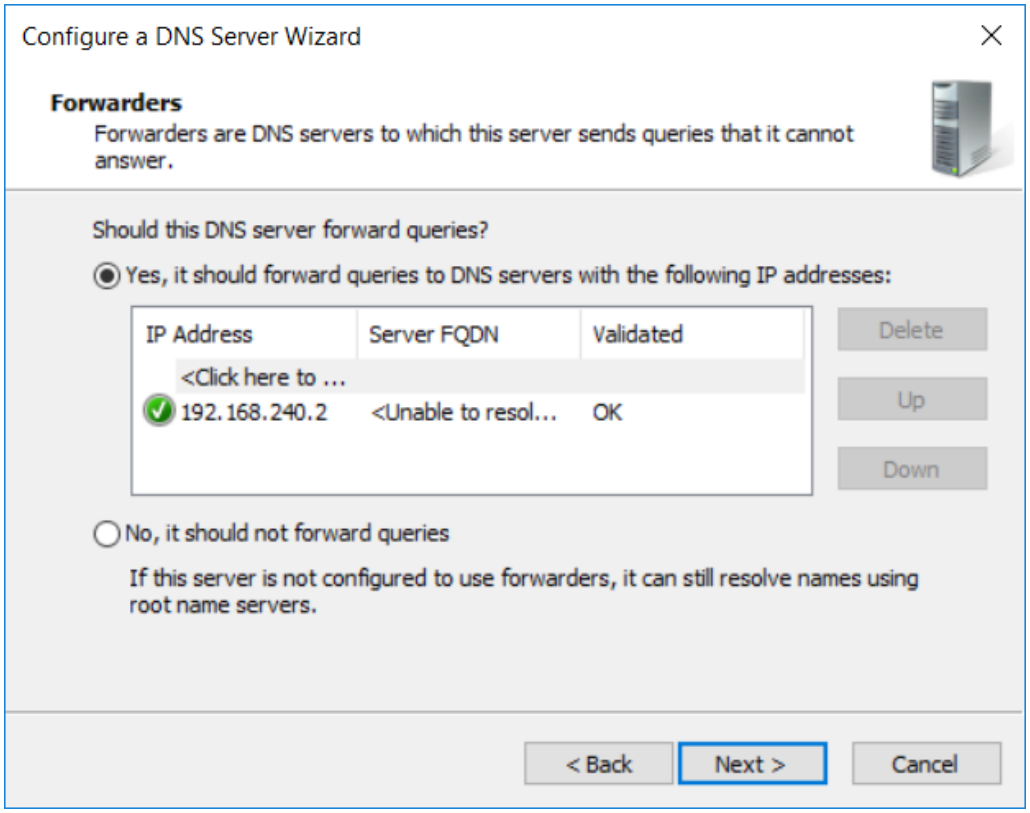
Step 4 – Click the first option and proceed to the next step



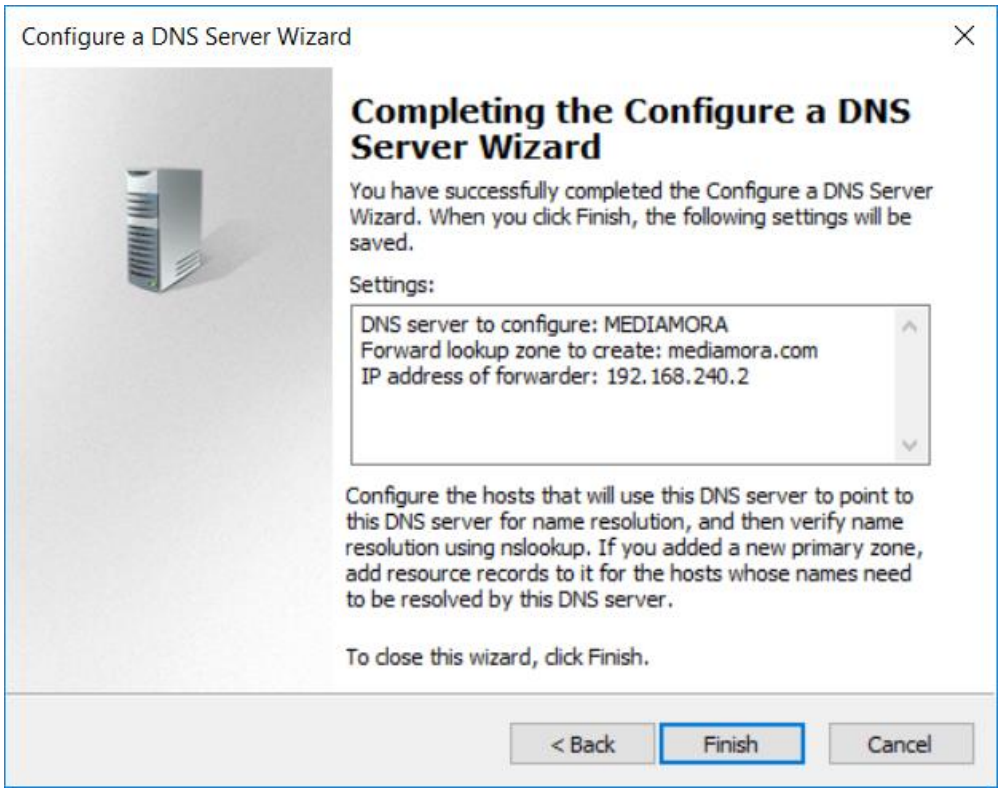
Step 5 – Enter the domain name or a new zone name and click next



Step 6 – Click allow secure updates only option and proceed next

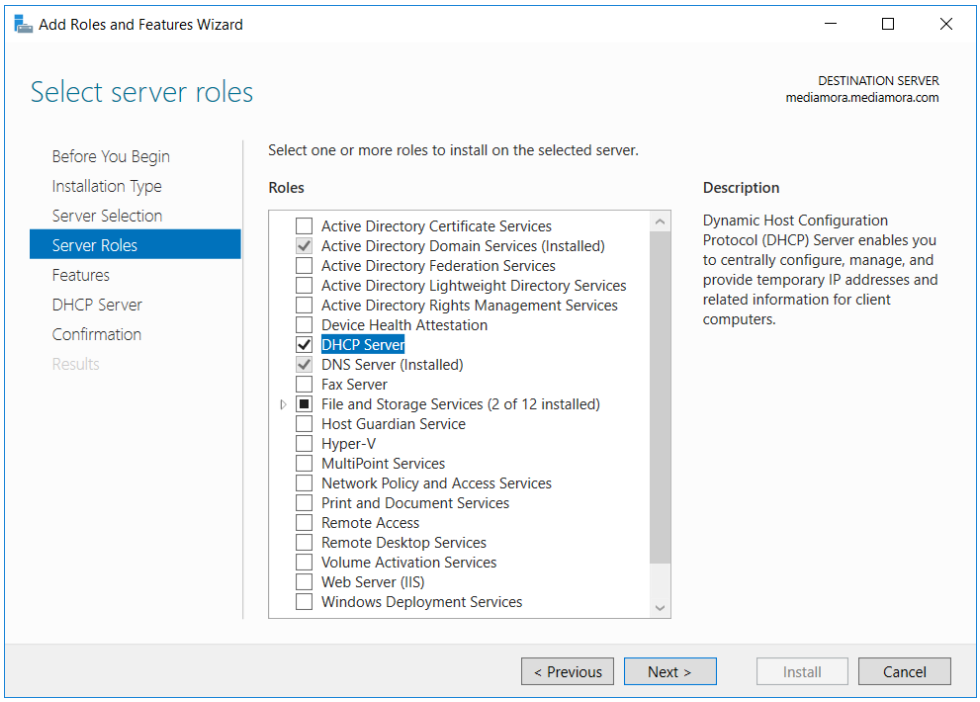


Step 7 – Enter the IP address of a DNS server provided by the ISP



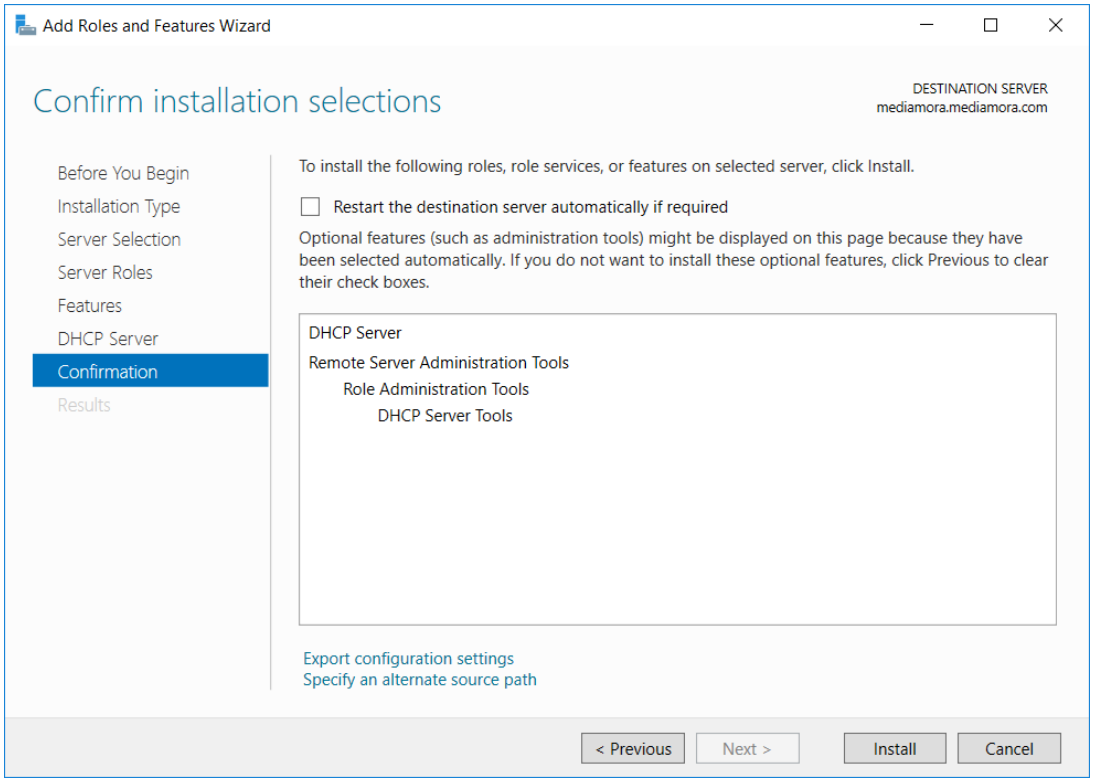
Step 8 – Click finish to end the setup

3.4 Implementing a DHCP server



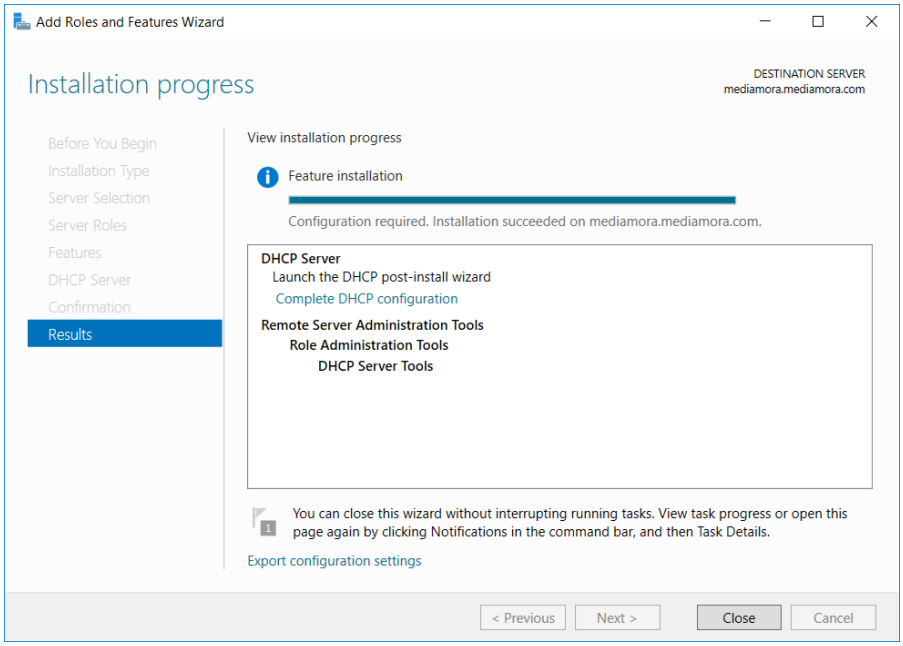
Step 1 – Click Add roles and features in Mange menu

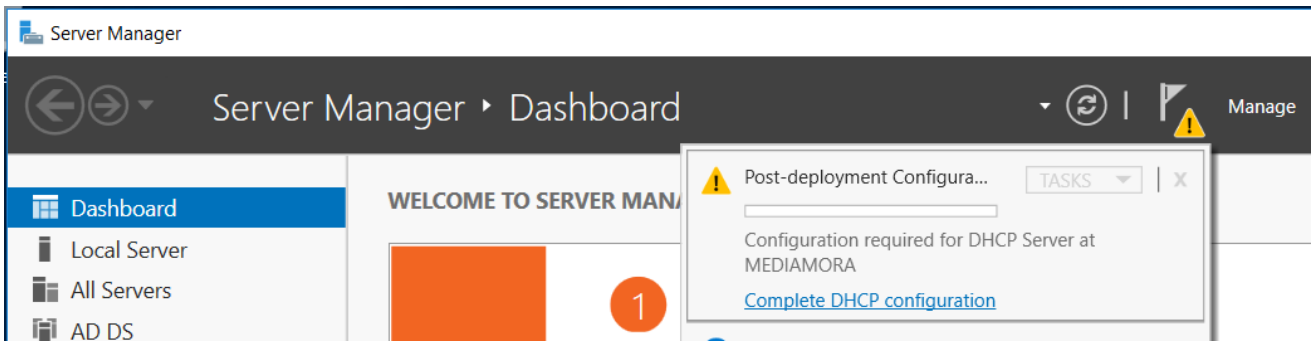
Step 2 – Select DHCP from the roles and click next



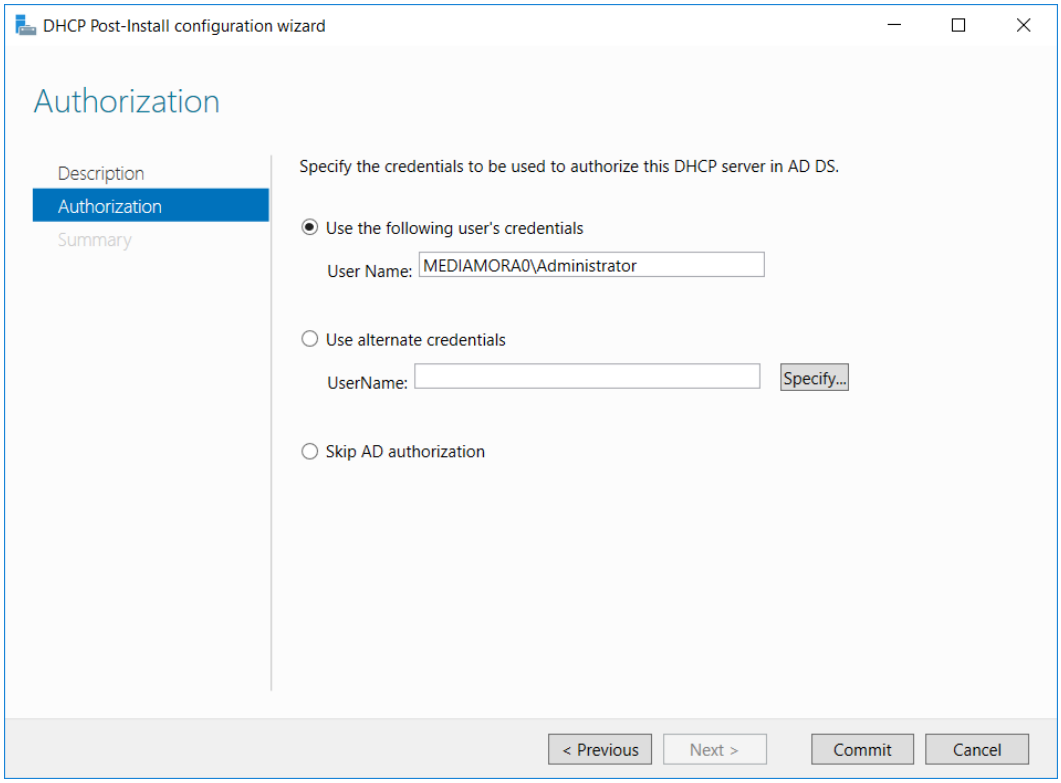
Step 3 – Leave the options as it is because we're installing this role for the 1st time. Proceed to the next step

Step 4 – Install the role by clicking install button

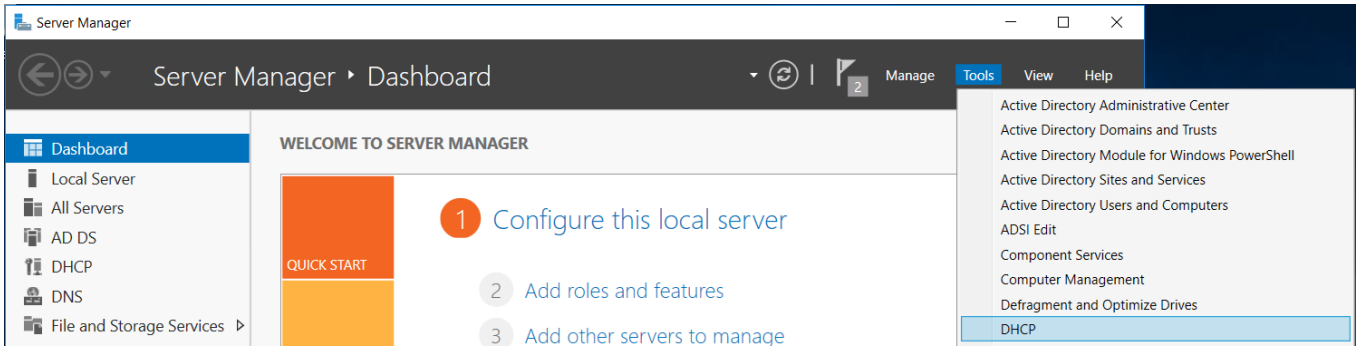




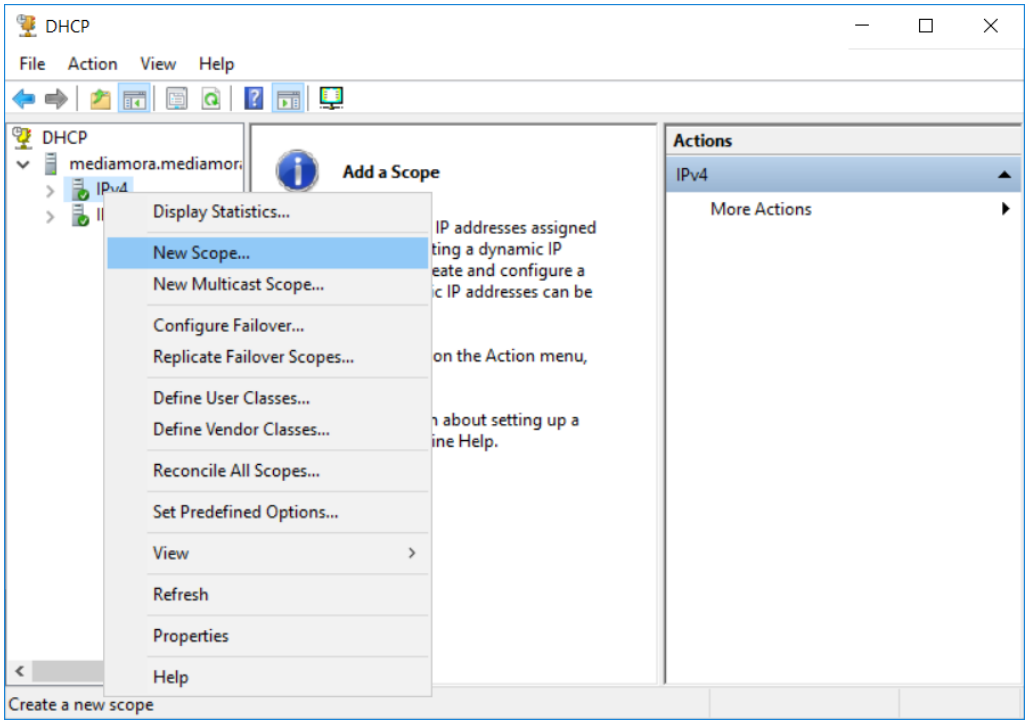
Step 5 – Complete the DHCP configuration in the post-deployment configuration menu



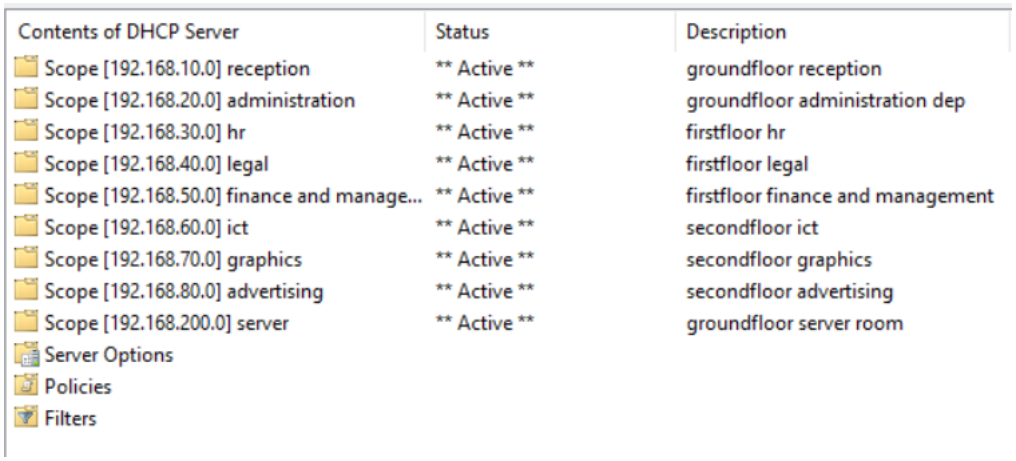
Step 6 – Provide the user's credentials and click commit



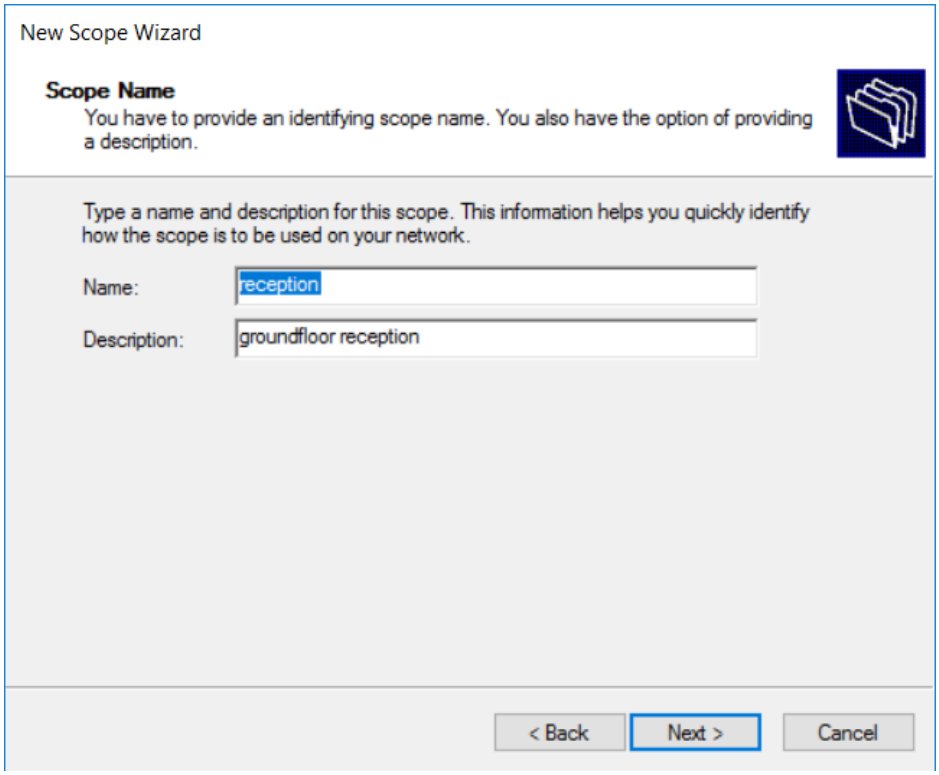
Step 7 – Click the DHCP option in the tools menu



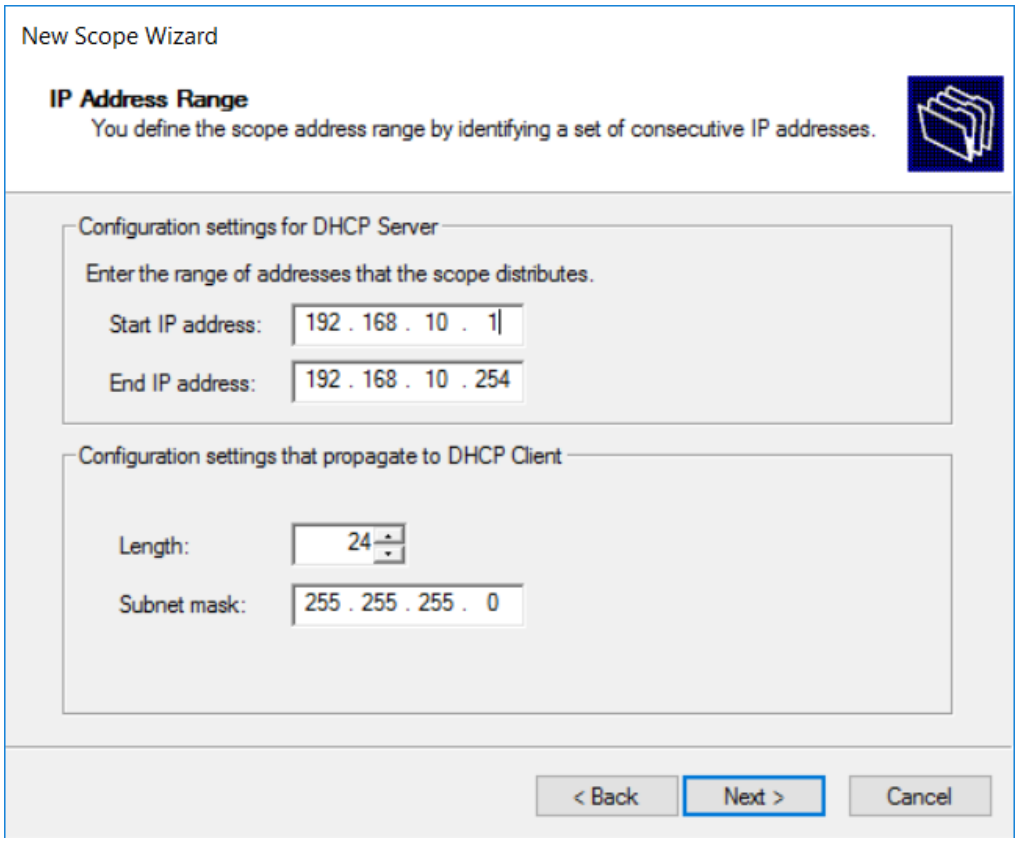
Step 8 – Right click the IPV4 section and click new scope



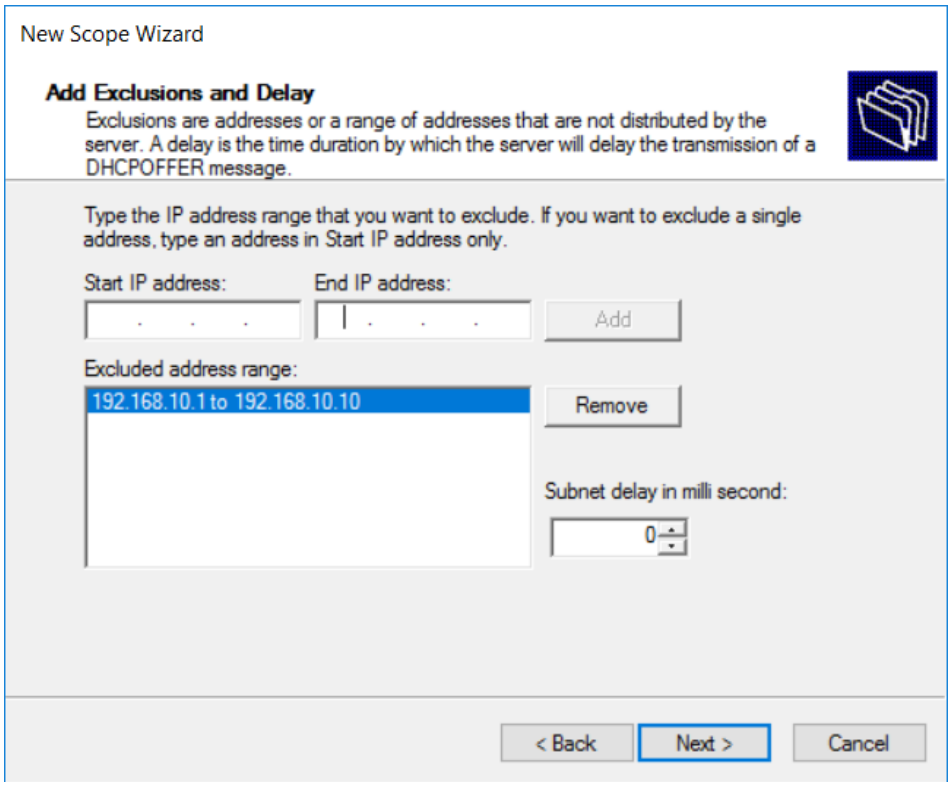
Contents of DHCP Server	Status	Description
Scope [192.168.10.0] reception	** Active **	groundfloor reception
Scope [192.168.20.0] administration	** Active **	groundfloor administration dep
Scope [192.168.30.0] hr	** Active **	firstfloor hr
Scope [192.168.40.0] legal	** Active **	firstfloor legal
Scope [192.168.50.0] finance and manage...	** Active **	firstfloor finance and management
Scope [192.168.60.0] ict	** Active **	secondfloor ict
Scope [192.168.70.0] graphics	** Active **	secondfloor graphics
Scope [192.168.80.0] advertising	** Active **	secondfloor advertising
Scope [192.168.200.0] server	** Active **	groundfloor server room
Server Options		
Policies		
Filters		



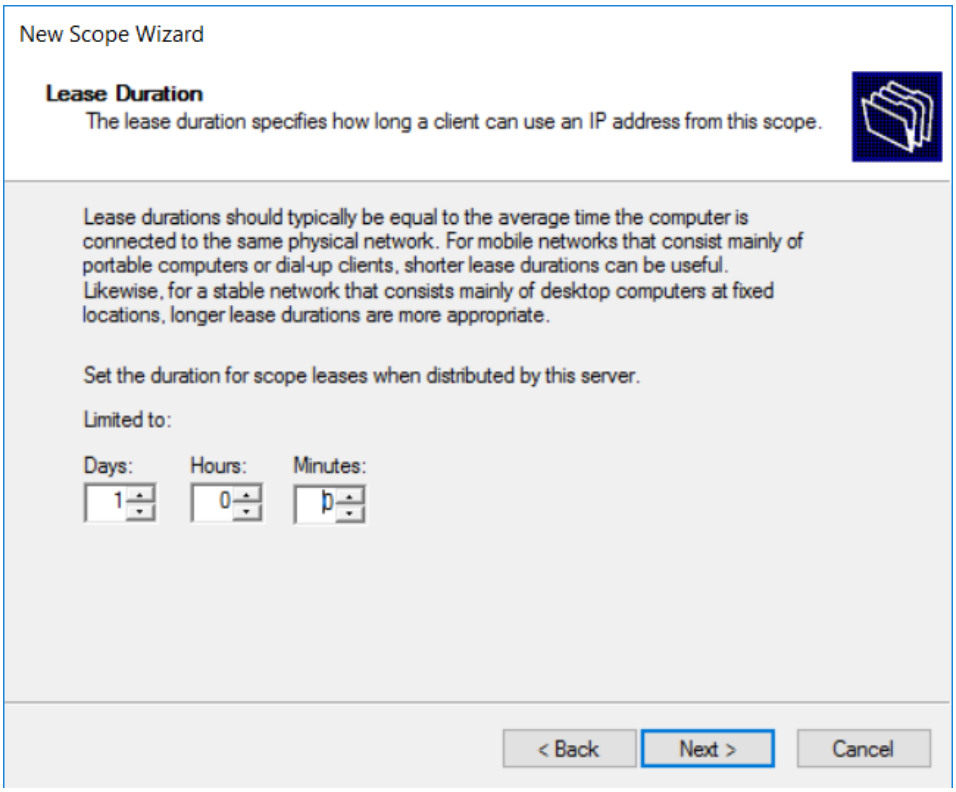
Step 9 – Provide a name and a description for a pool



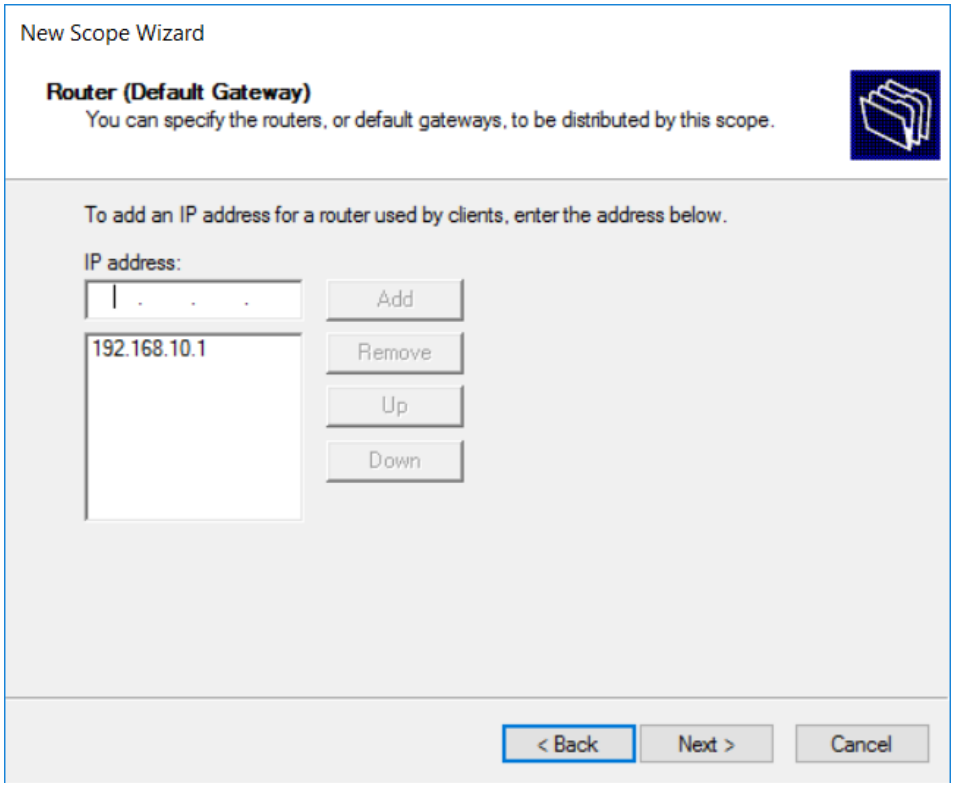
Step 10 – Enter the starting IP and the ending IP with a matching subnet mask



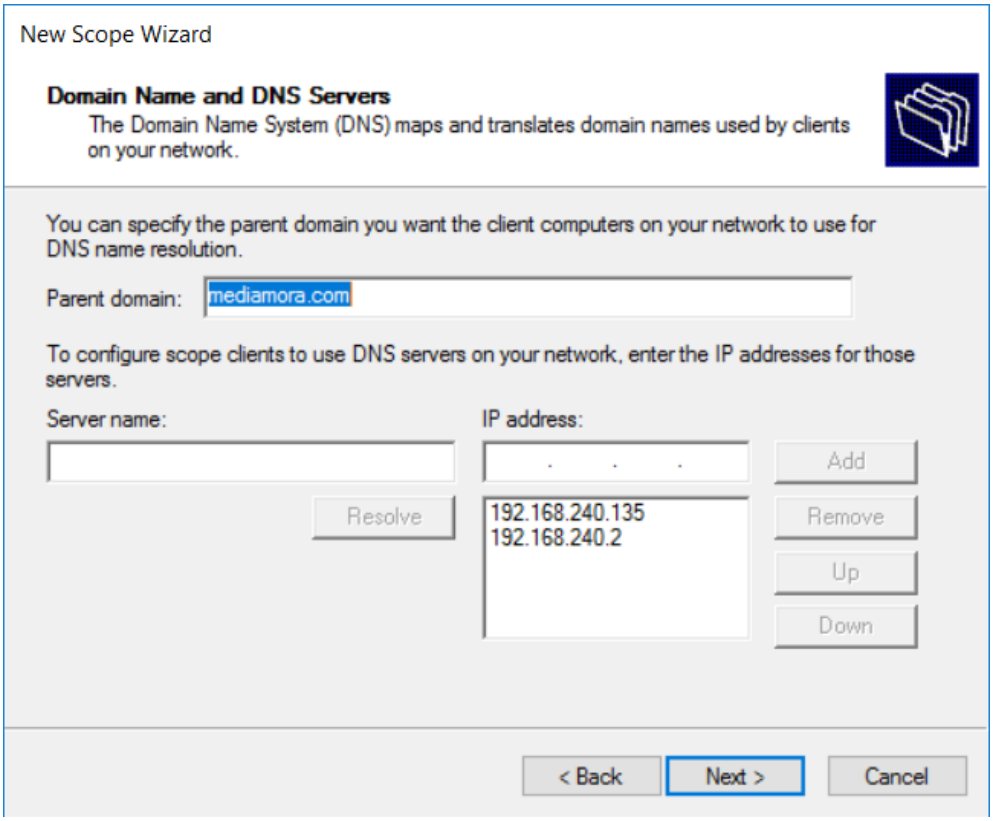
Step 11 – Add IP addresses which you want to exclude from the pool



Step 12 – In this step assign a proper lease time to avoid depletion of IP addresses. When assigning a pool for wireless users VLAN make sure the lease time is less than an hour. For computers and laptops 5 hours would be sufficient



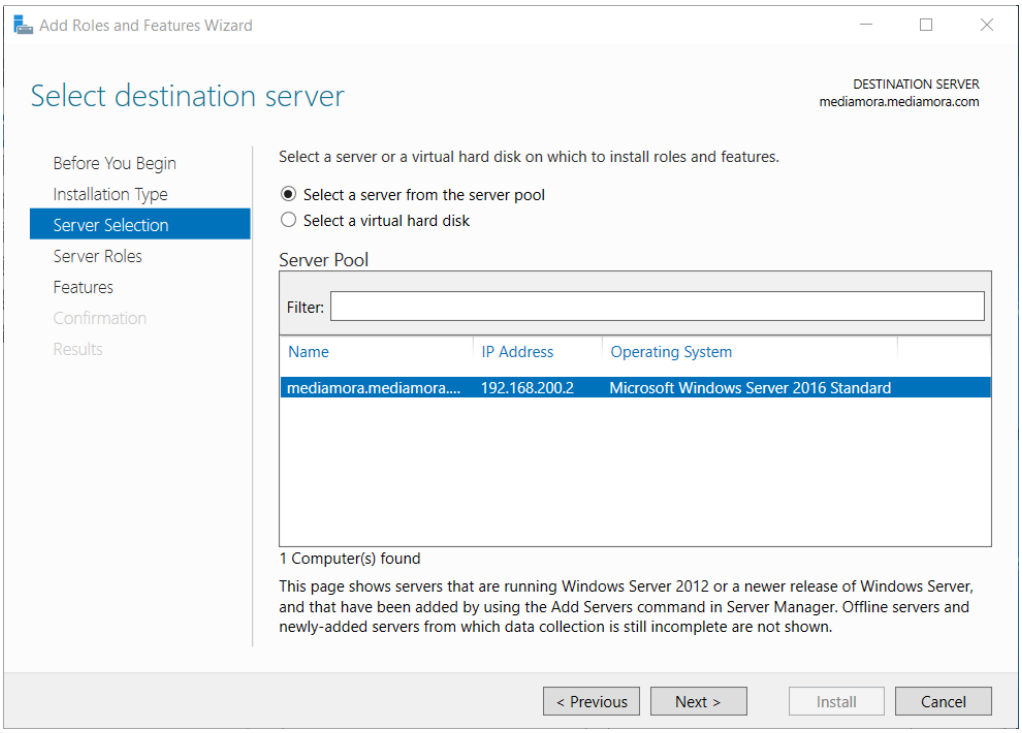
Step 11 – Add a default gateway for the pool



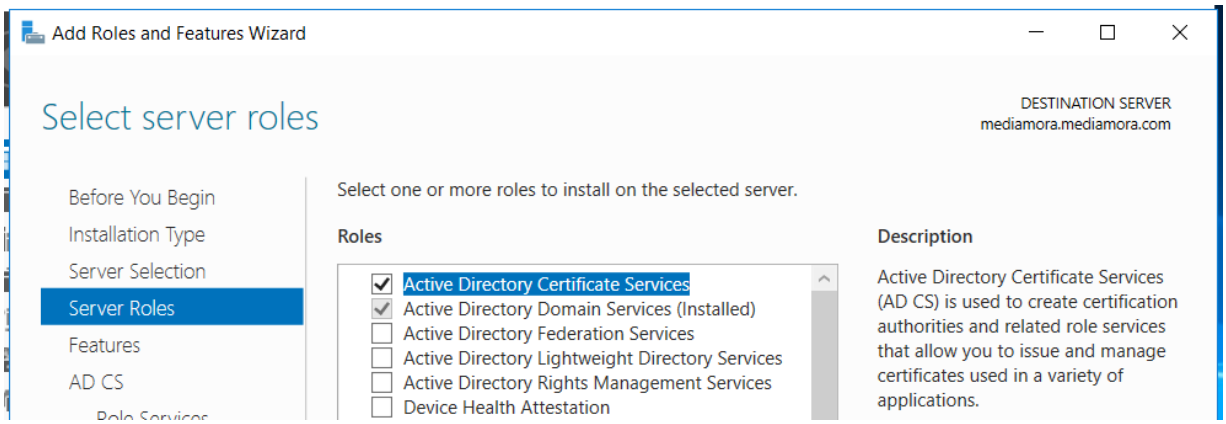
Step 12 – Click finish to end setup

3.5 Implementing an AD CS server

Step 1 – Select add roles & features from the drop down menu

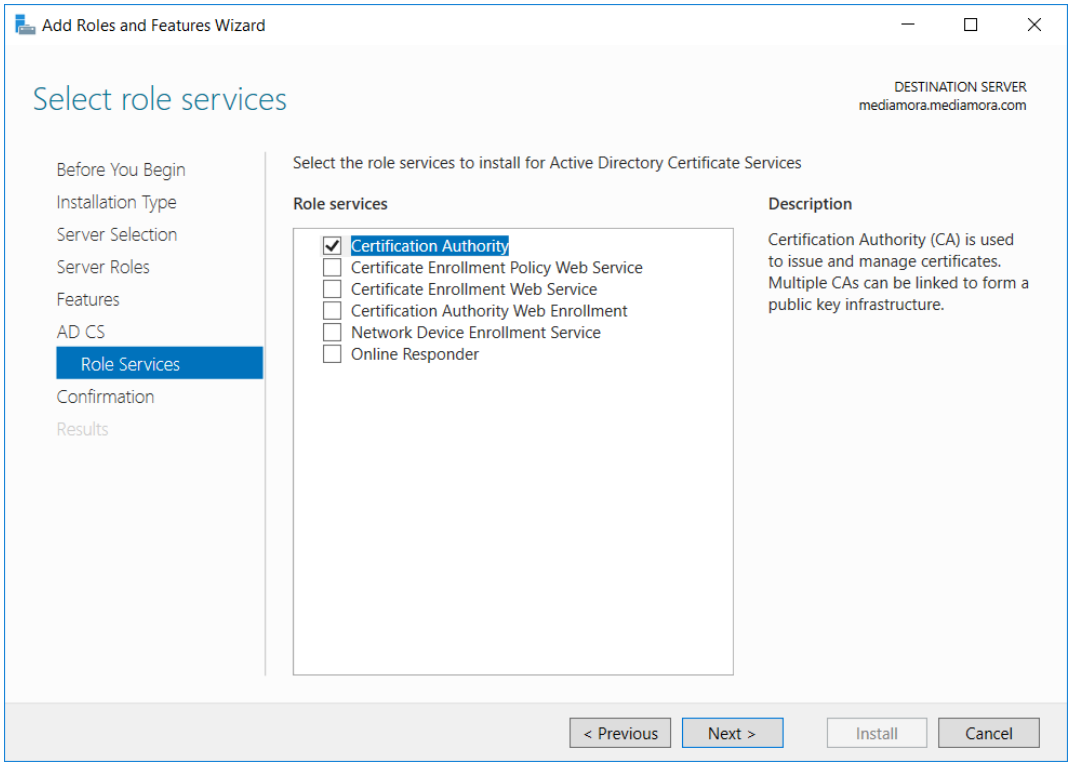


Step 2 – Select the server which you want to install and proceed next

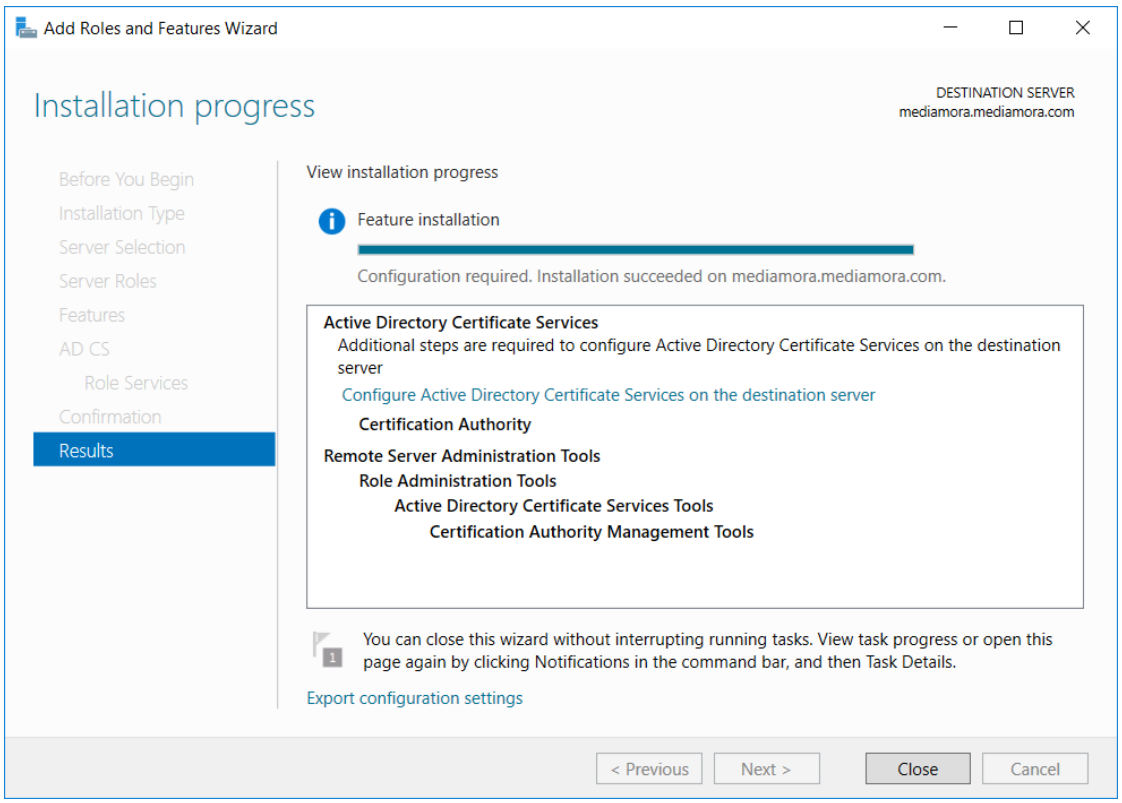


Step 3 – Select active directory certificate services and click next

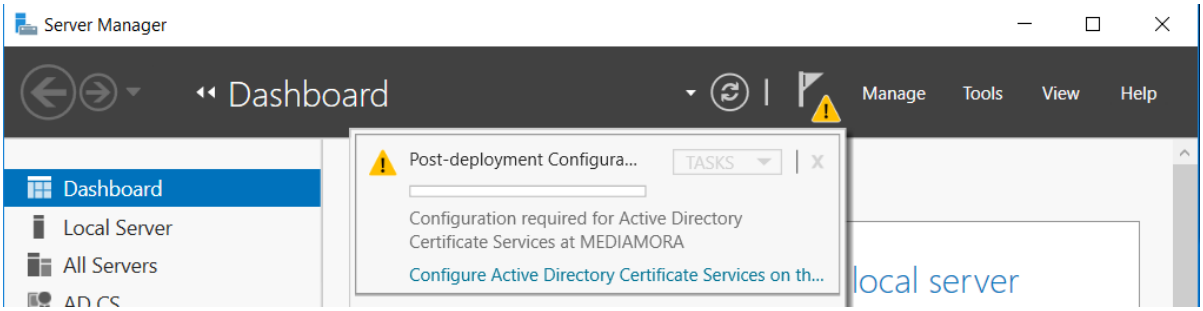
Step 4 – Proceed to the next step with the default settings



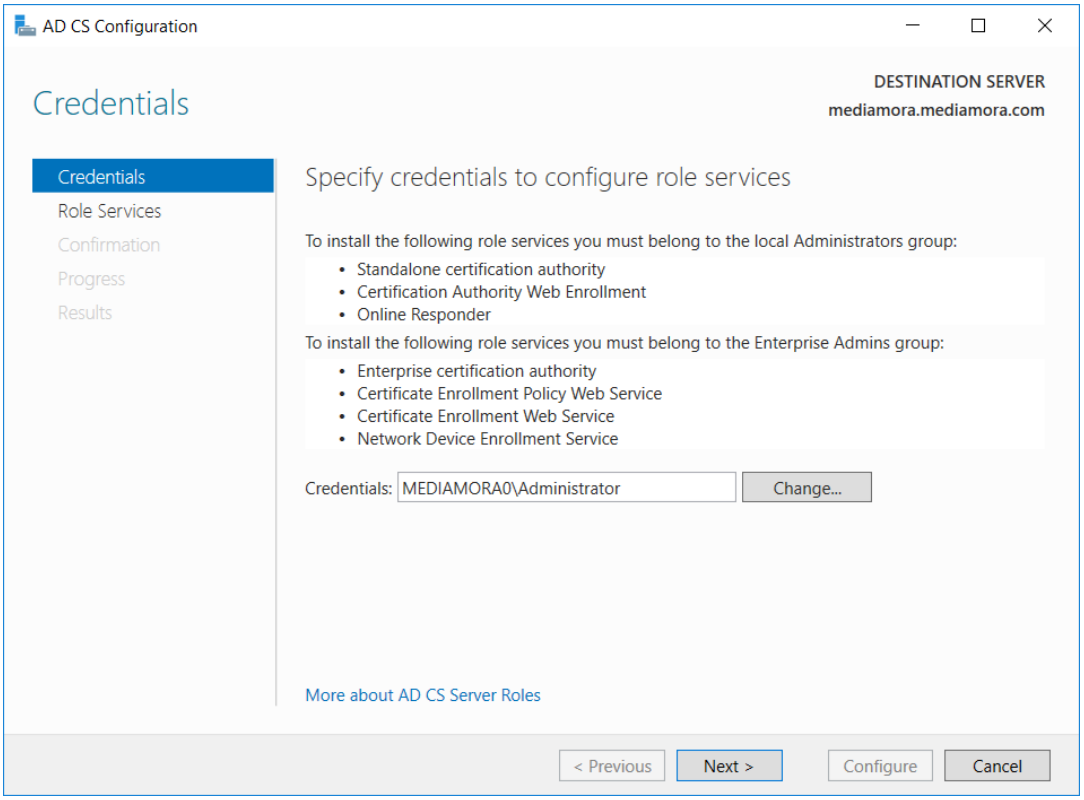
Step 5 – Select Certification authority and click next



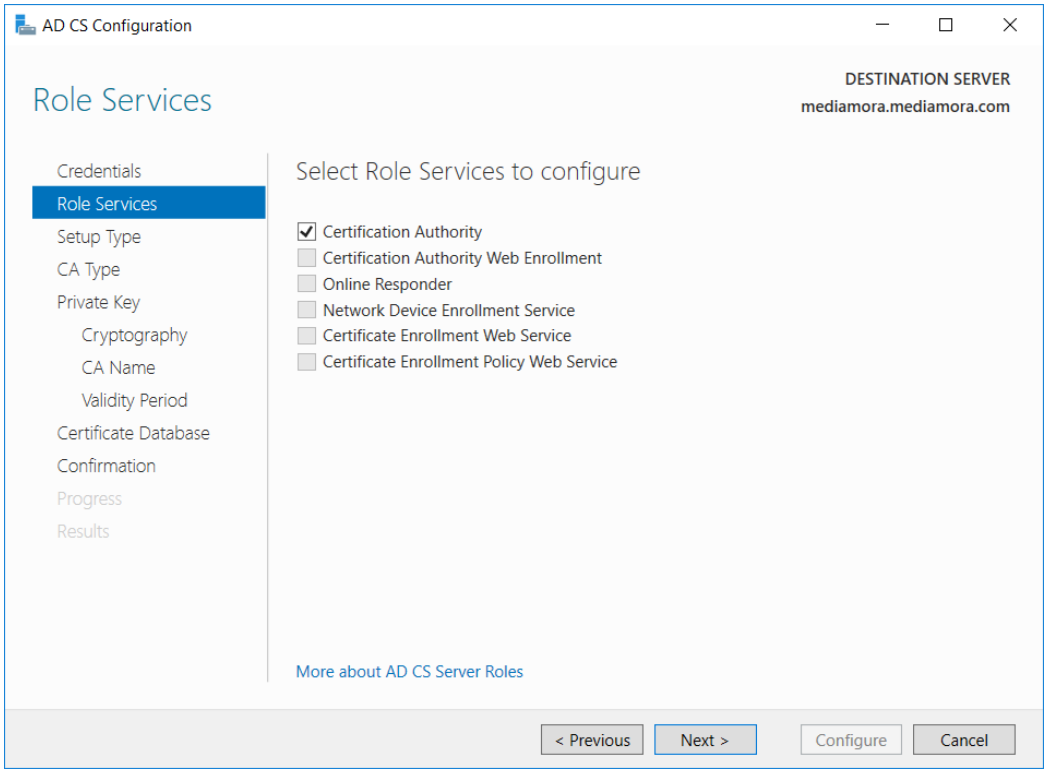
Step 6 – After installing the required roles close the setup



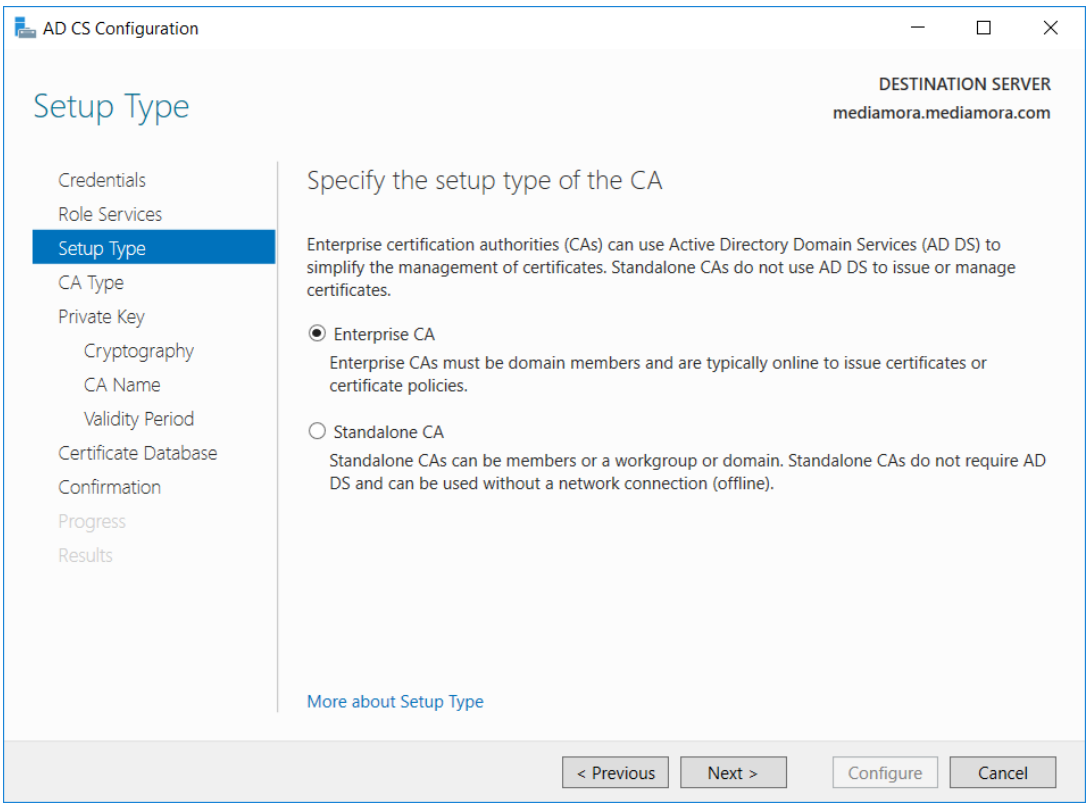
Step 7 – Configure the post-deployment configurations



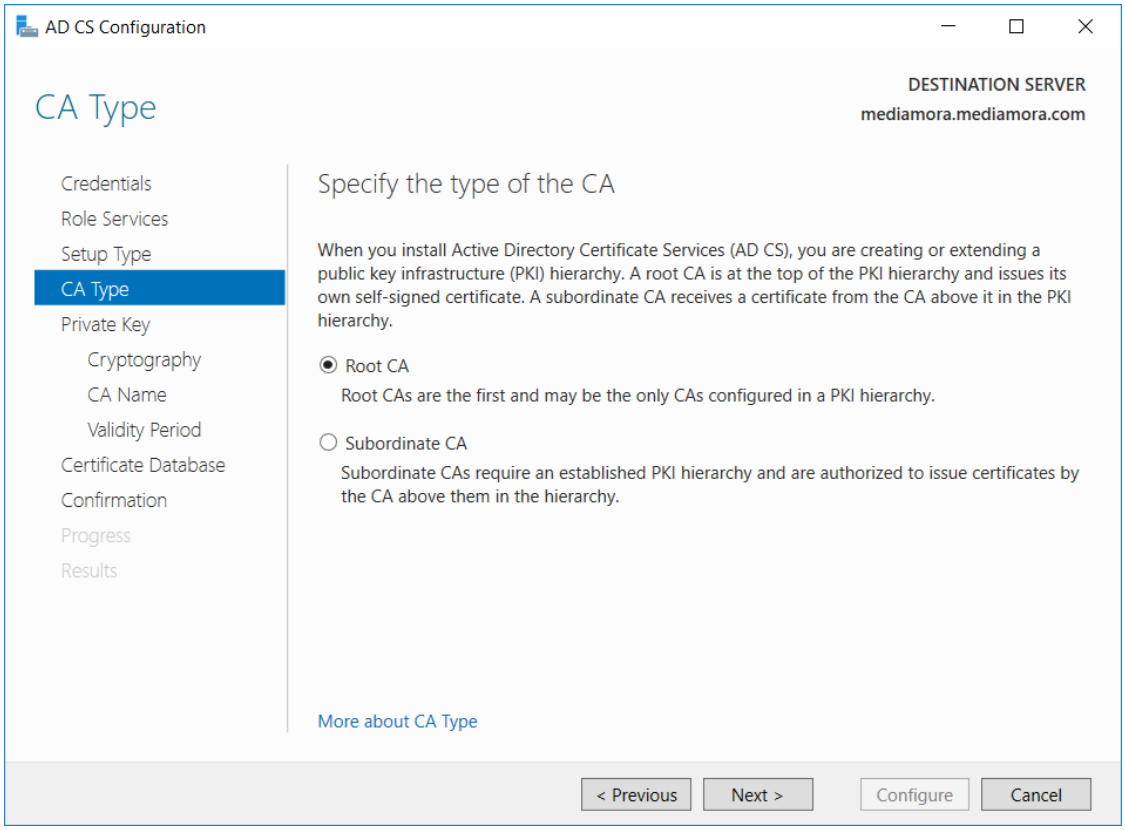
Step 8 – Provide the credentials and click next



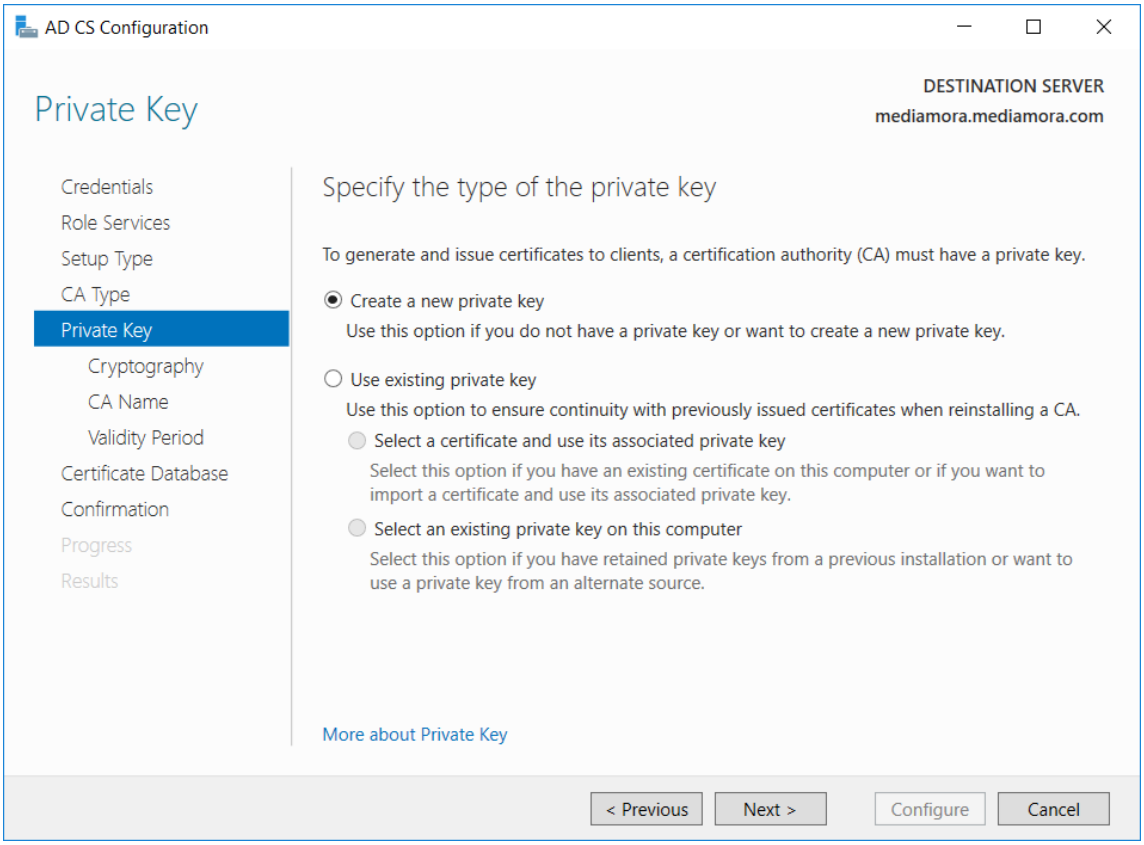
Step 9 – Select the certification authority option and click next



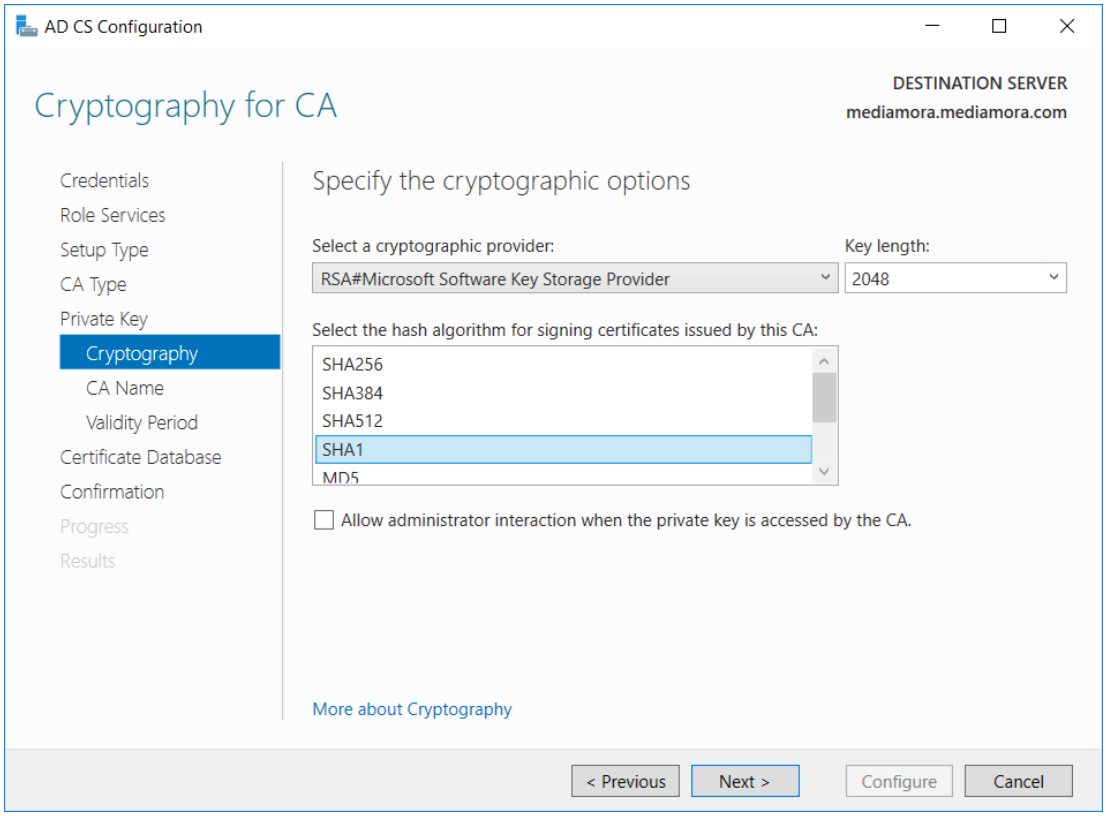
Step 10 – Select Enterprise CA option since we are using the active directory for the certification issues



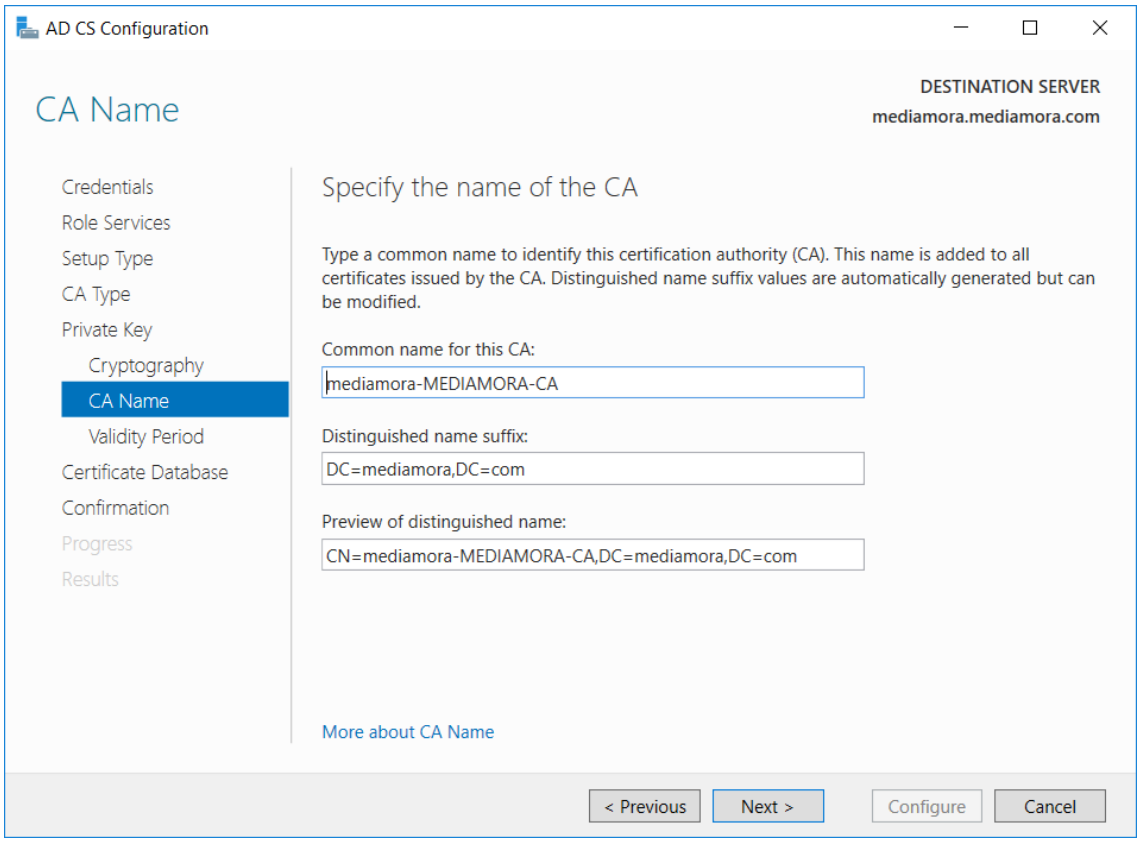
Step 11 – Select the Root CA option and proceed to the next step



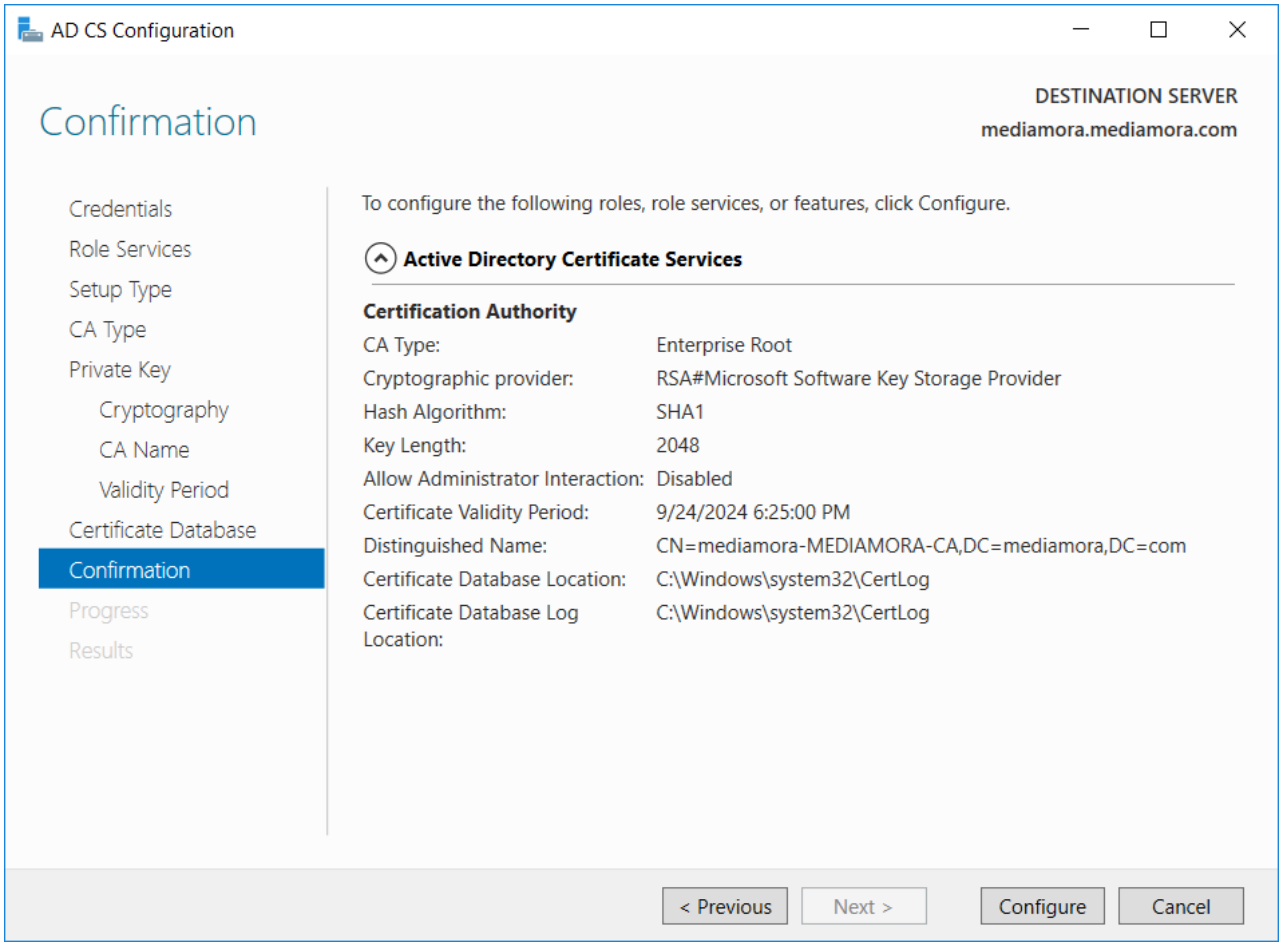
Step 12 – Select new private key option and proceed to the next step



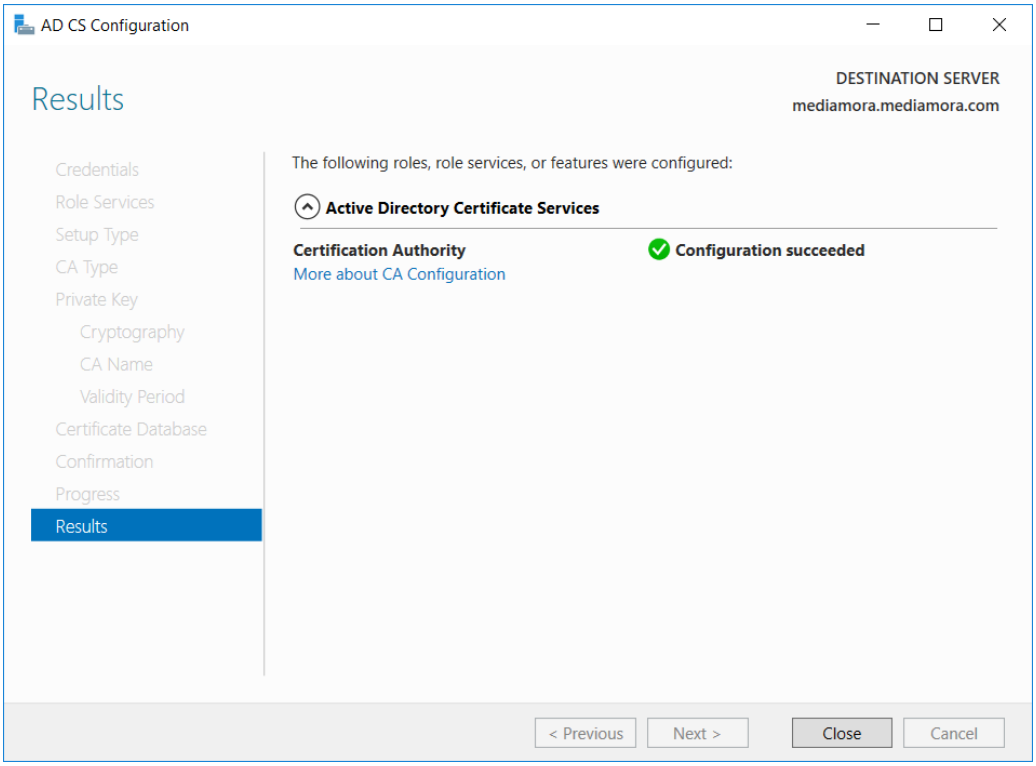
Step 13 – Provide the required cryptographic options for the private key and click next



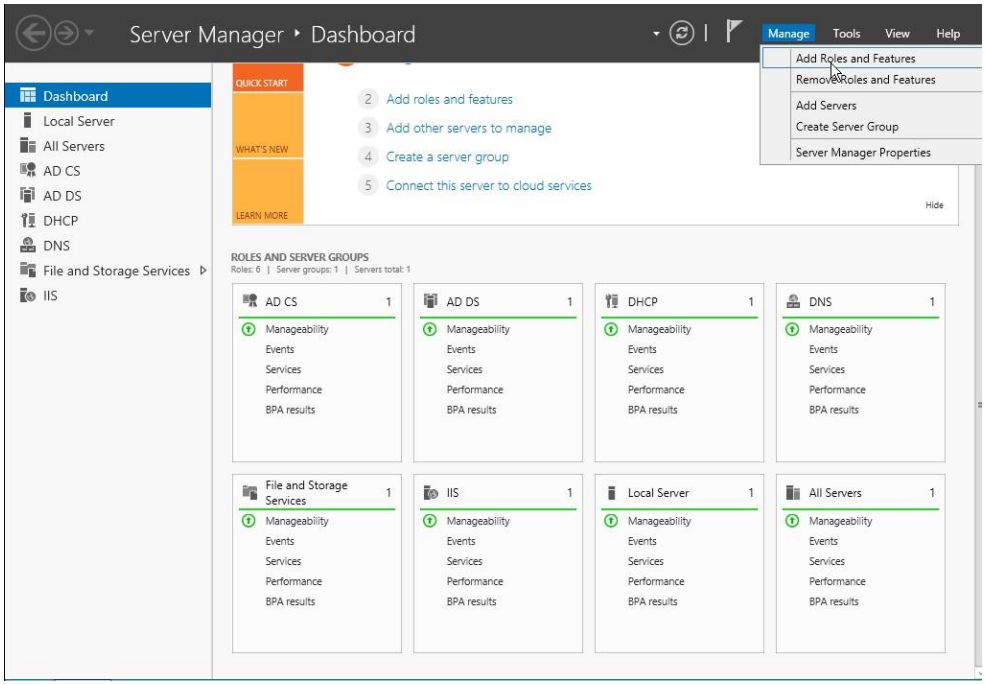
Step 14 – Here we can change the common name if we want but recommended names are not altered for the best use



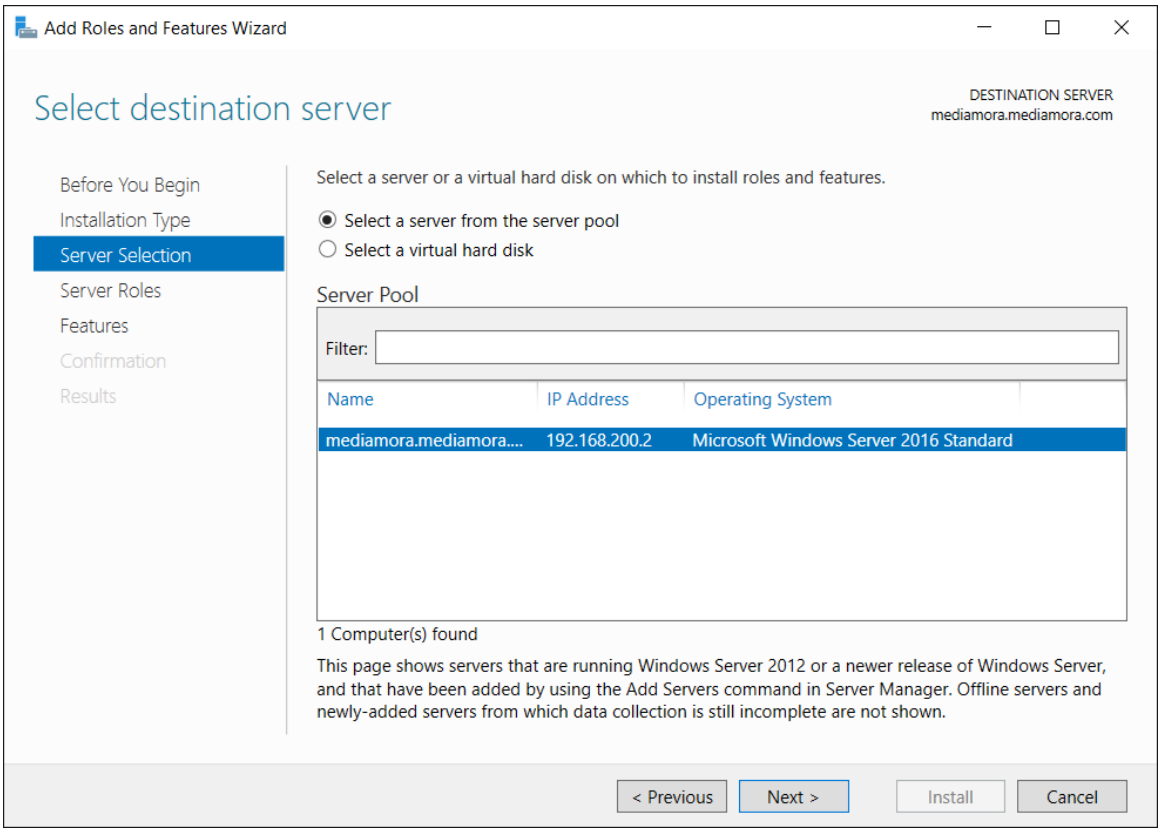
Step 15 – Click configure



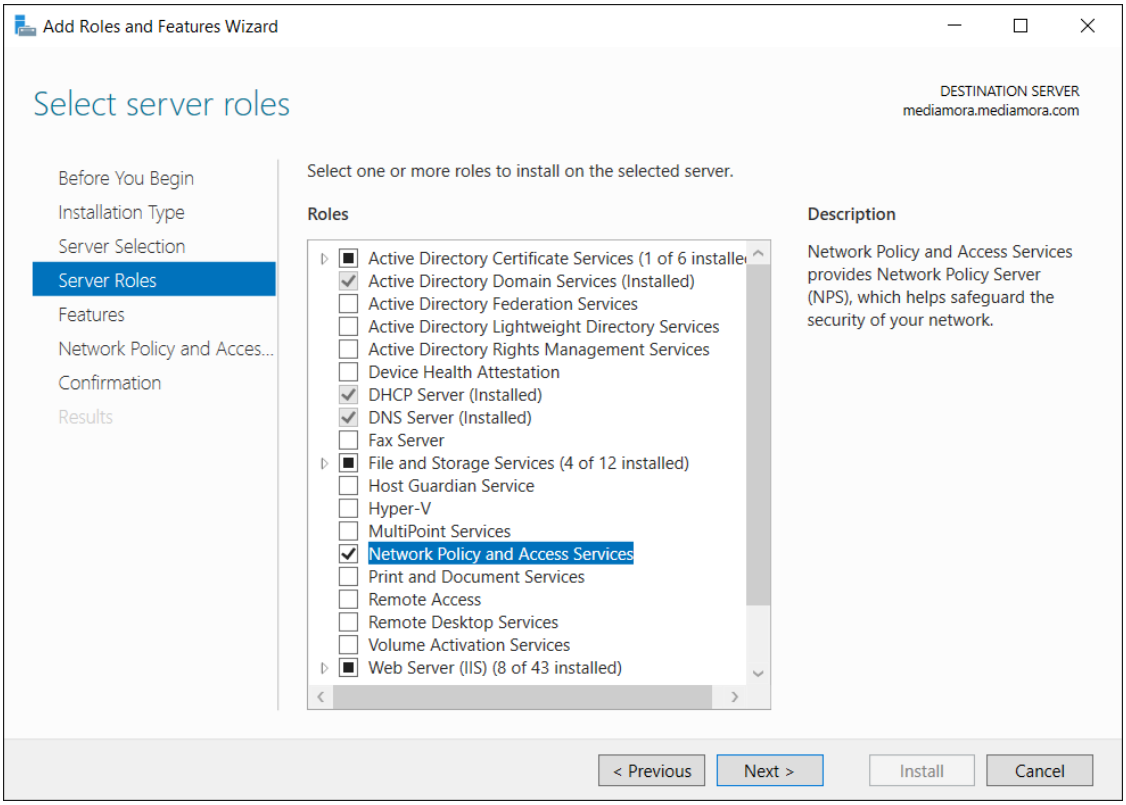
3.6 Implementing a NAP server



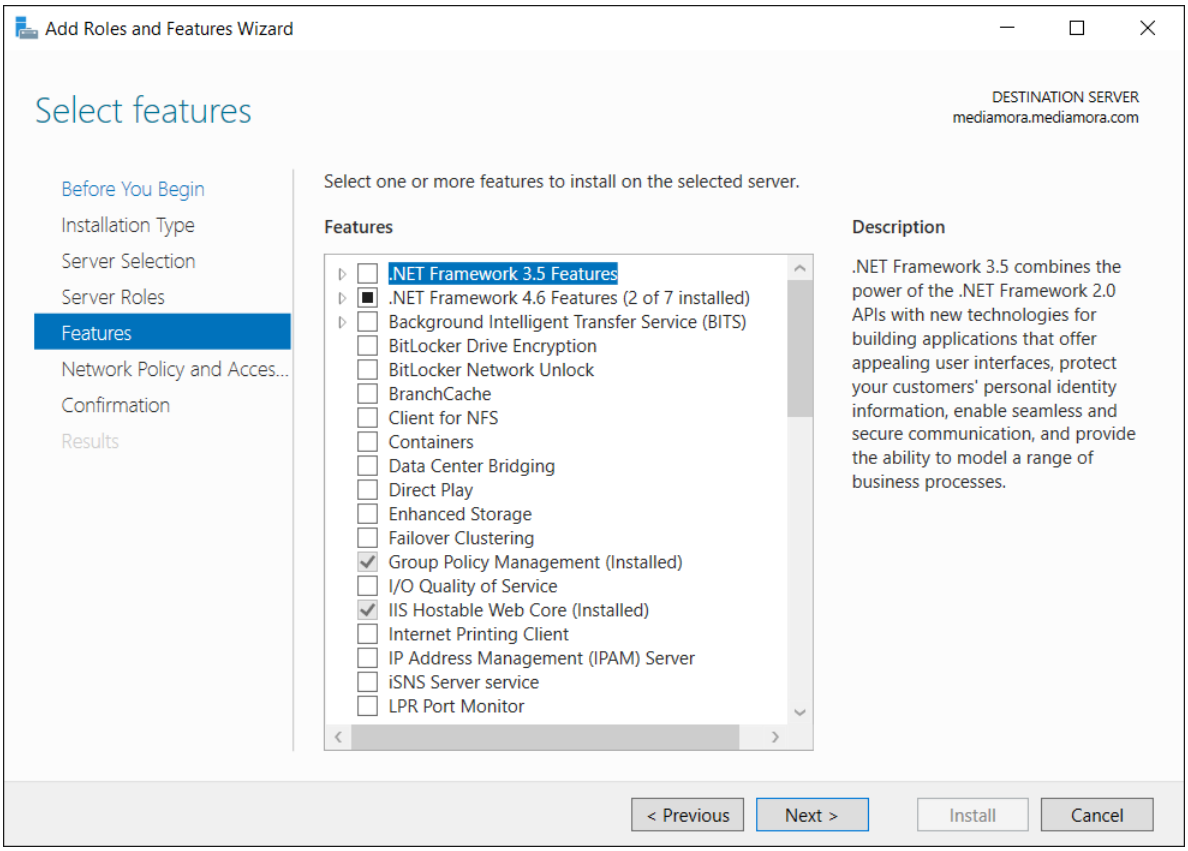
Step 1 – Click add roles and features



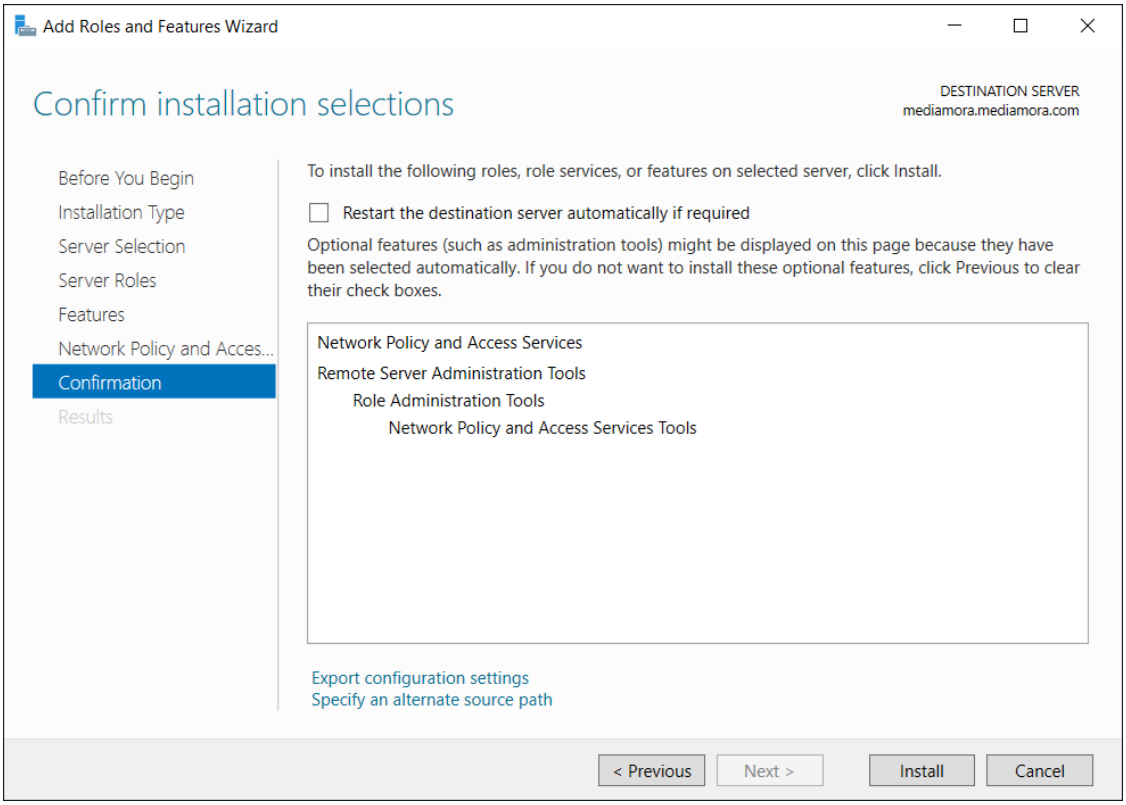
Step 2 – Select a server form the server pool and click next



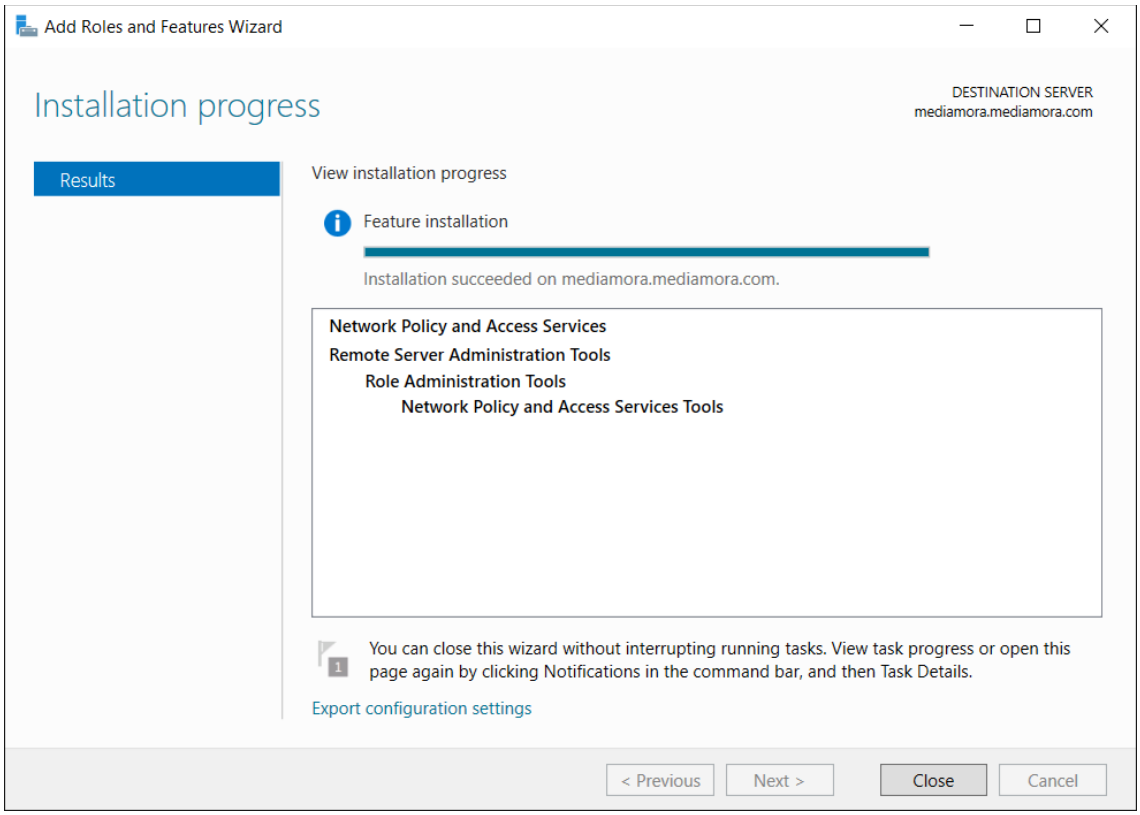
Step 3 – Select the network policy access services and click next



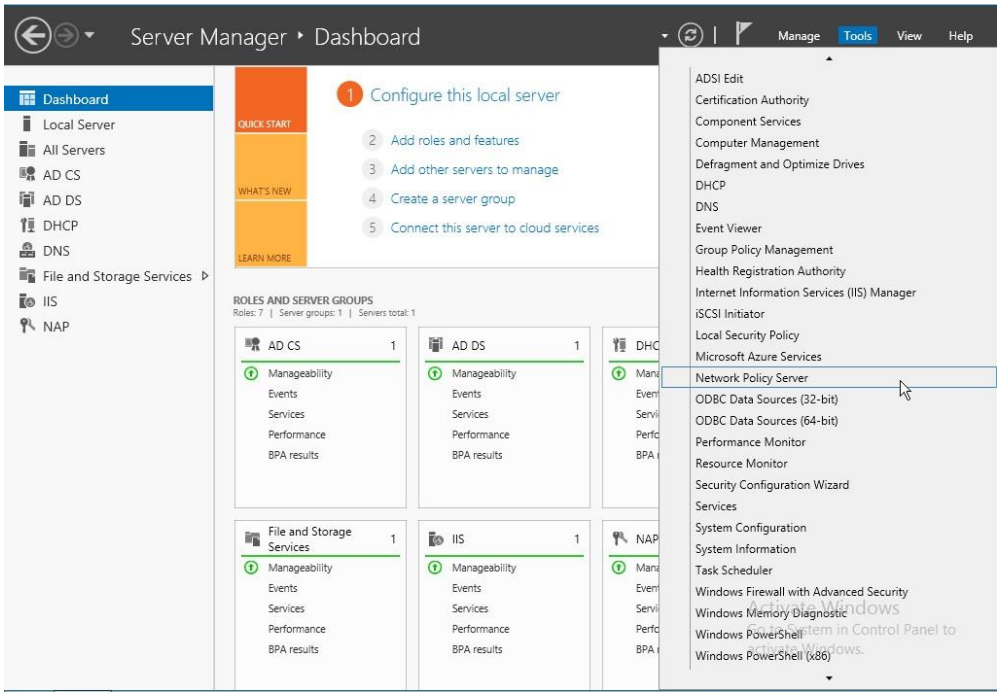
Step 4 – Proceed to the next setup without changing anything



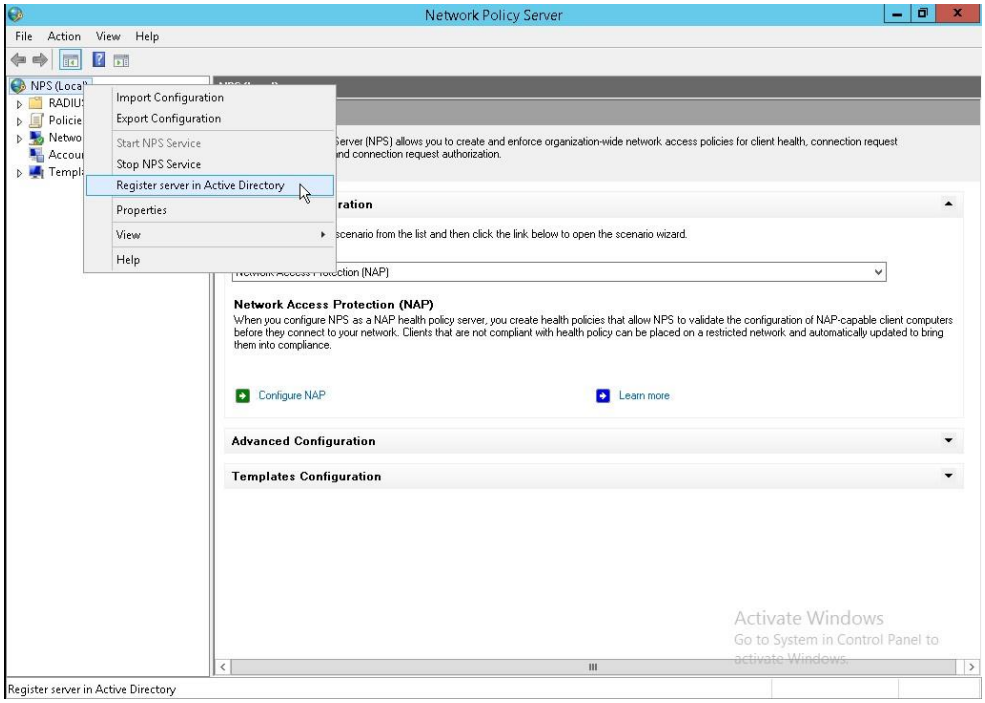
Step 5 – If network policy server is already installed it will not show here and click next



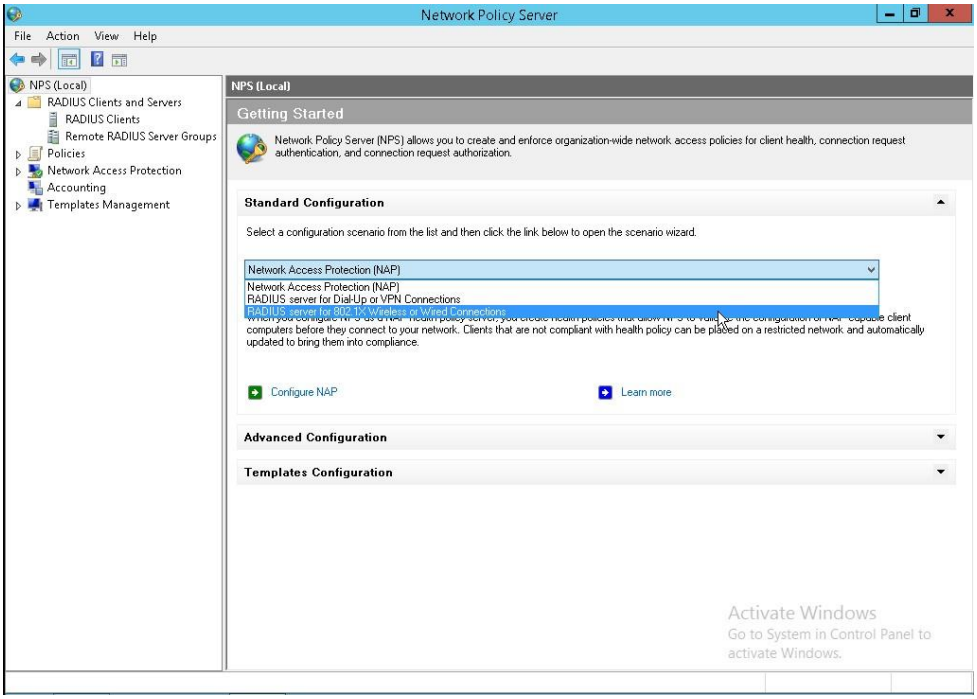
Step 6 – Close the setup after installing the roles



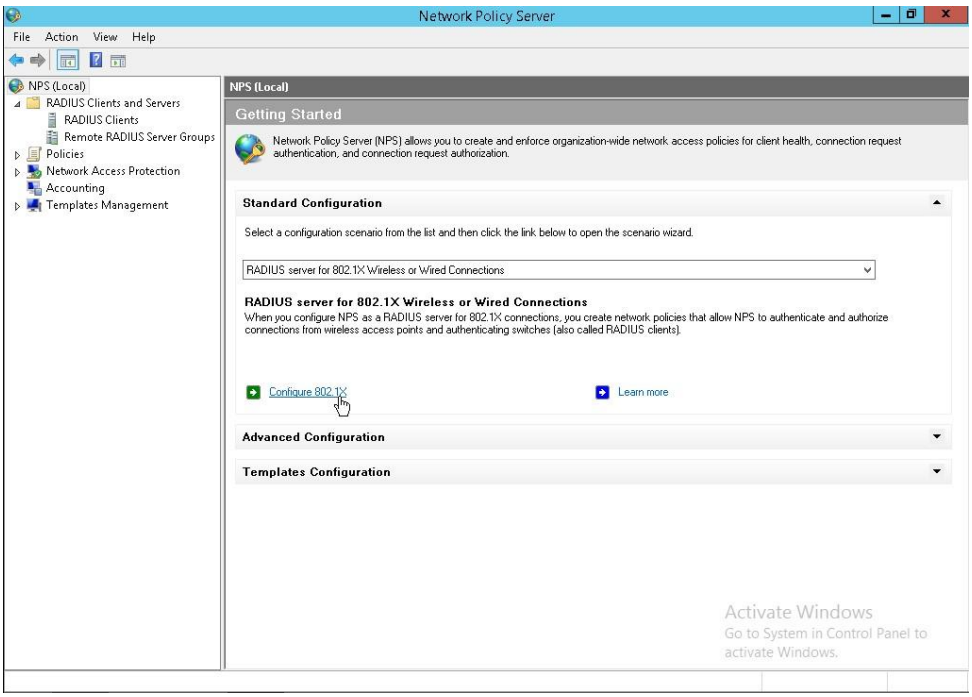
Step 7 – After installing the services go to tools and click network policy server



Step 8 – Right click the NPS local and click register server on active directory

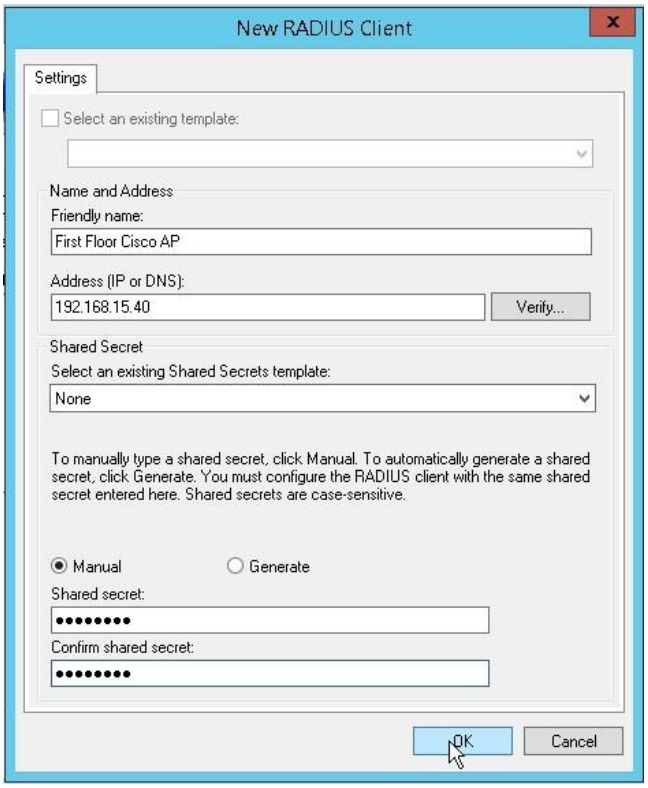


Step 9 – Click the NPS local and select radius server for 802.1x wireless or wired connections under the standard configuration

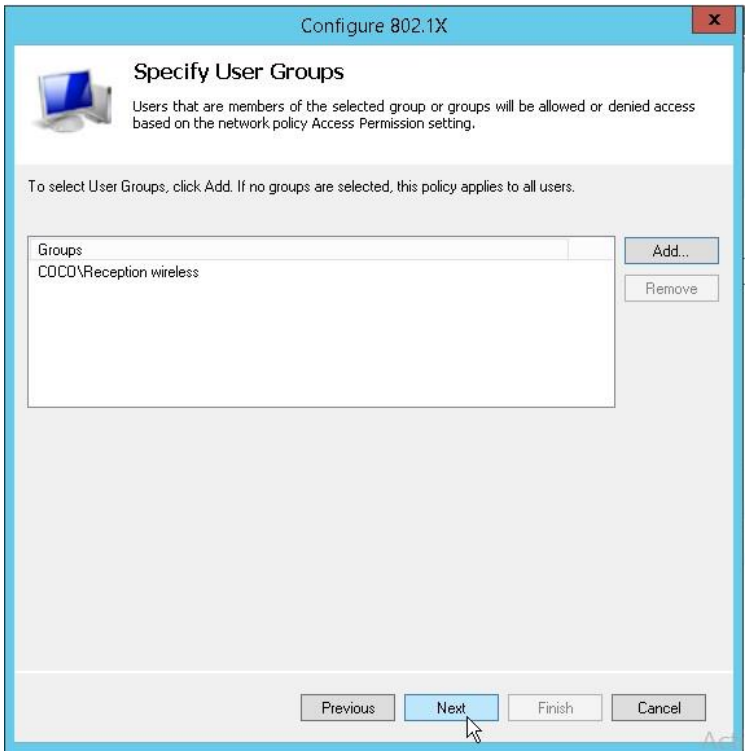


Step 10 – Then click configure 802.1x

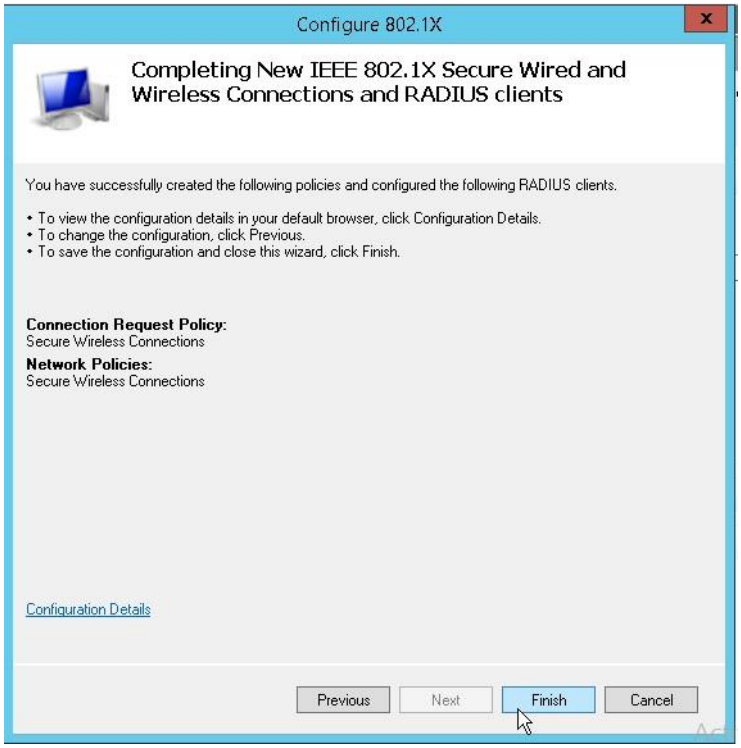
Step 11 – Select secure wireless connections since we are configuring radius for wireless



Step 12 – In the specify 802.1X switches windows click add to add wireless APs. Provide a Friendly name, IP address and the password for the AP.

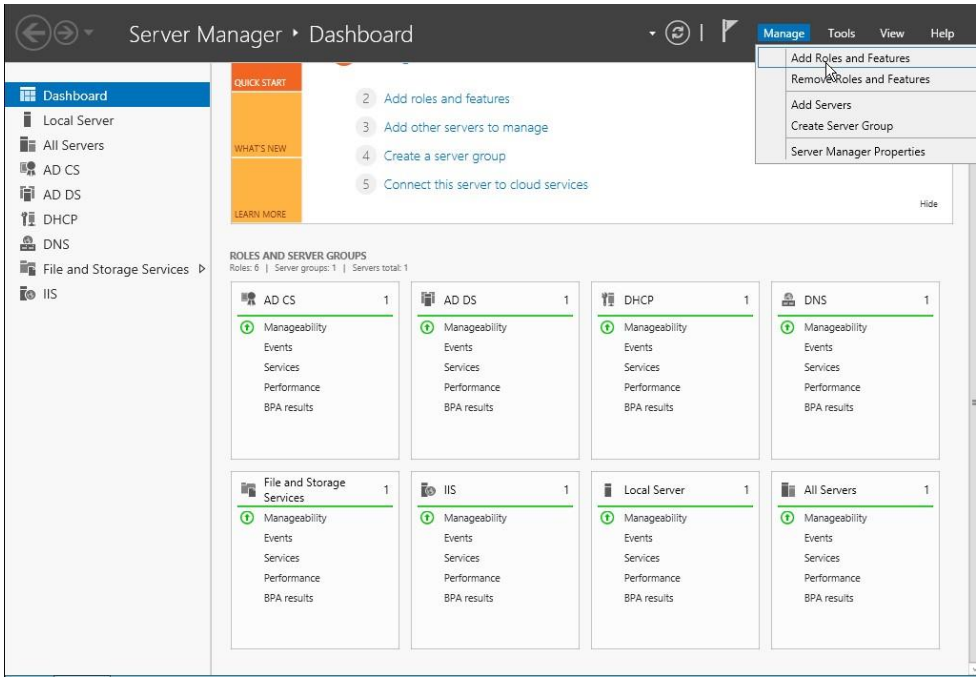


Step 13 – In the specify user groups window add the groups which were created in active directory

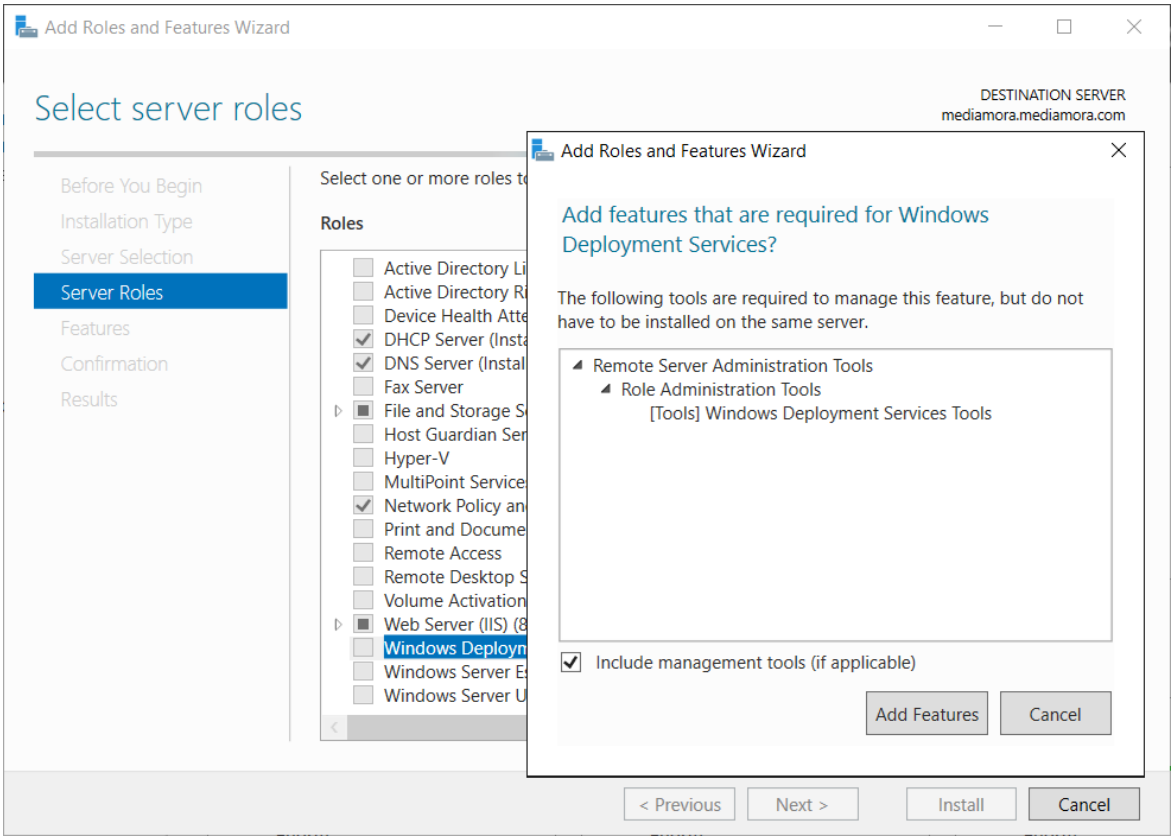


Step 14 – Finish the wizard

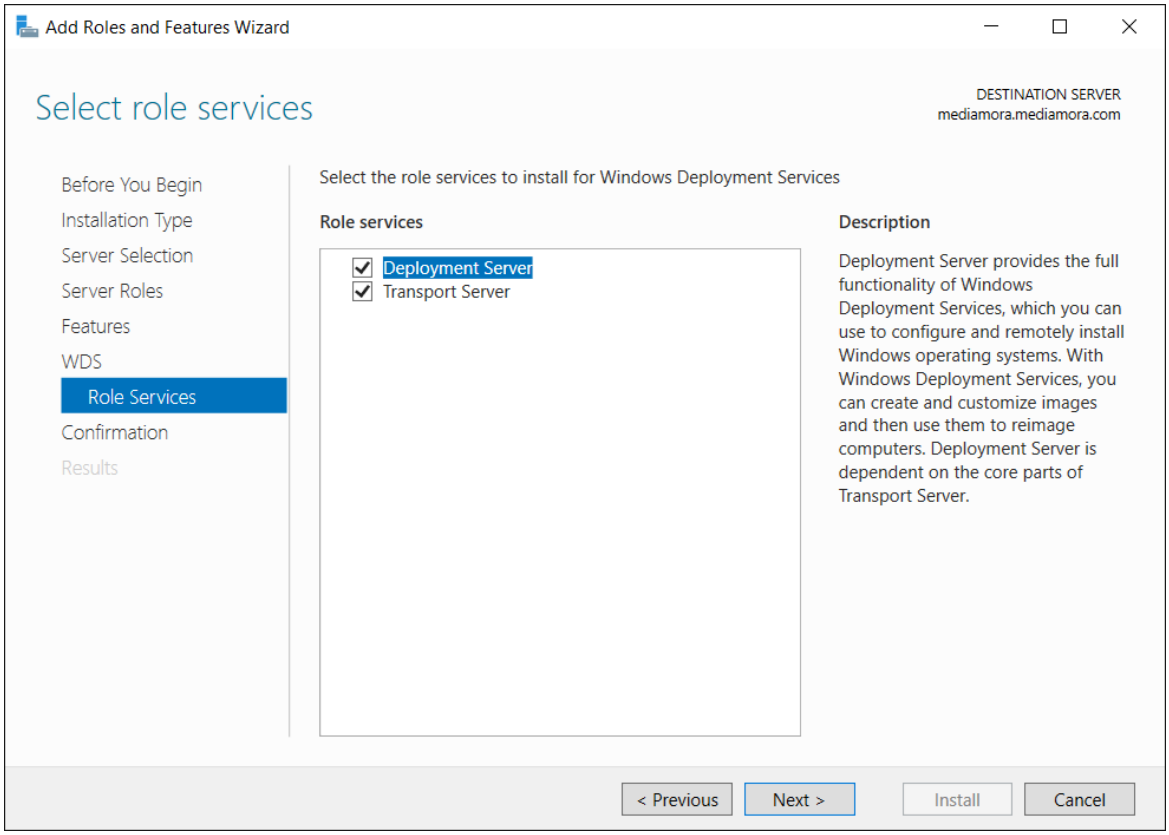
3.7 Implementing a WDS server



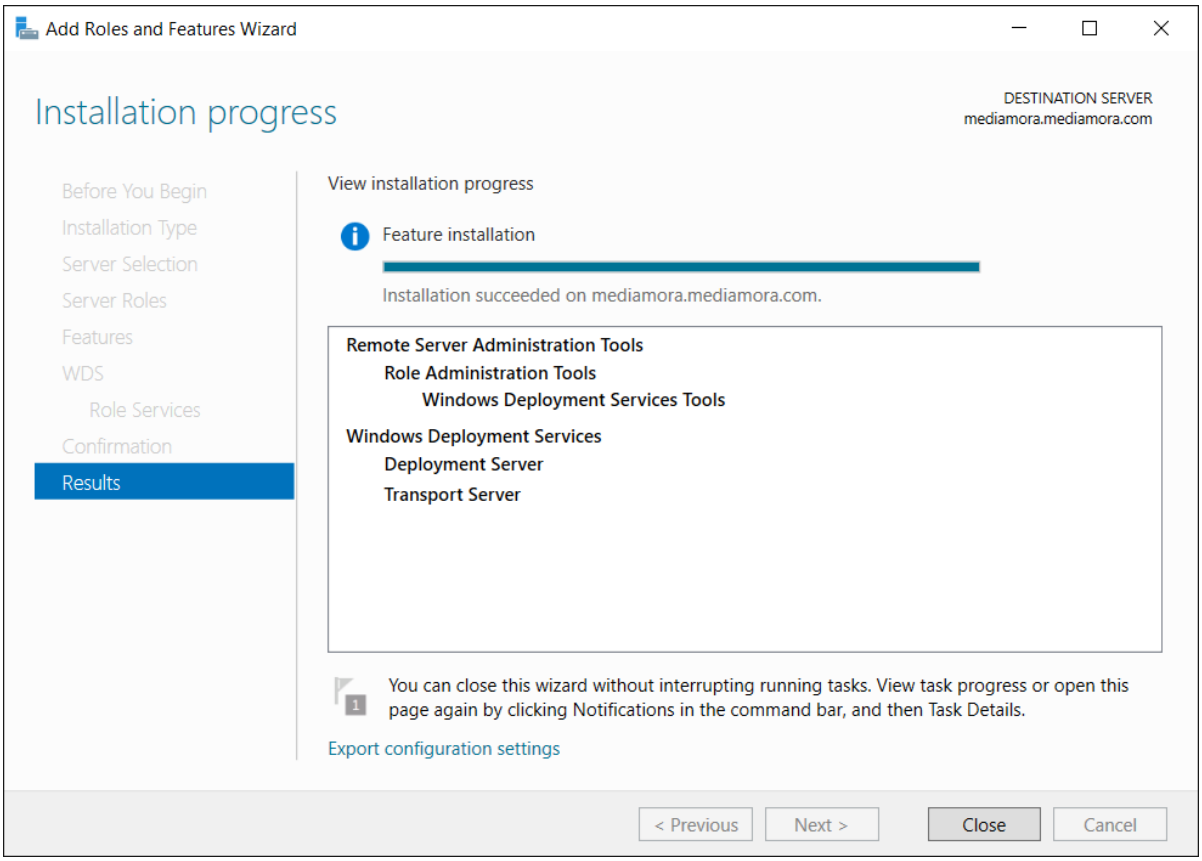
Step 1 – Click add roles and features in the manage



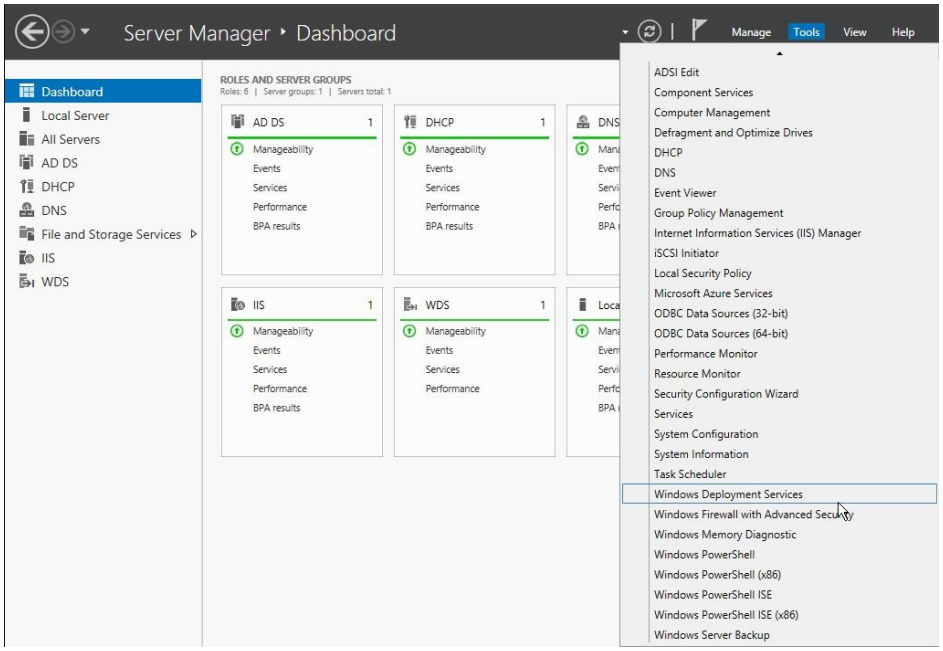
Step 2 – Select windows deployment services from the roles and click next



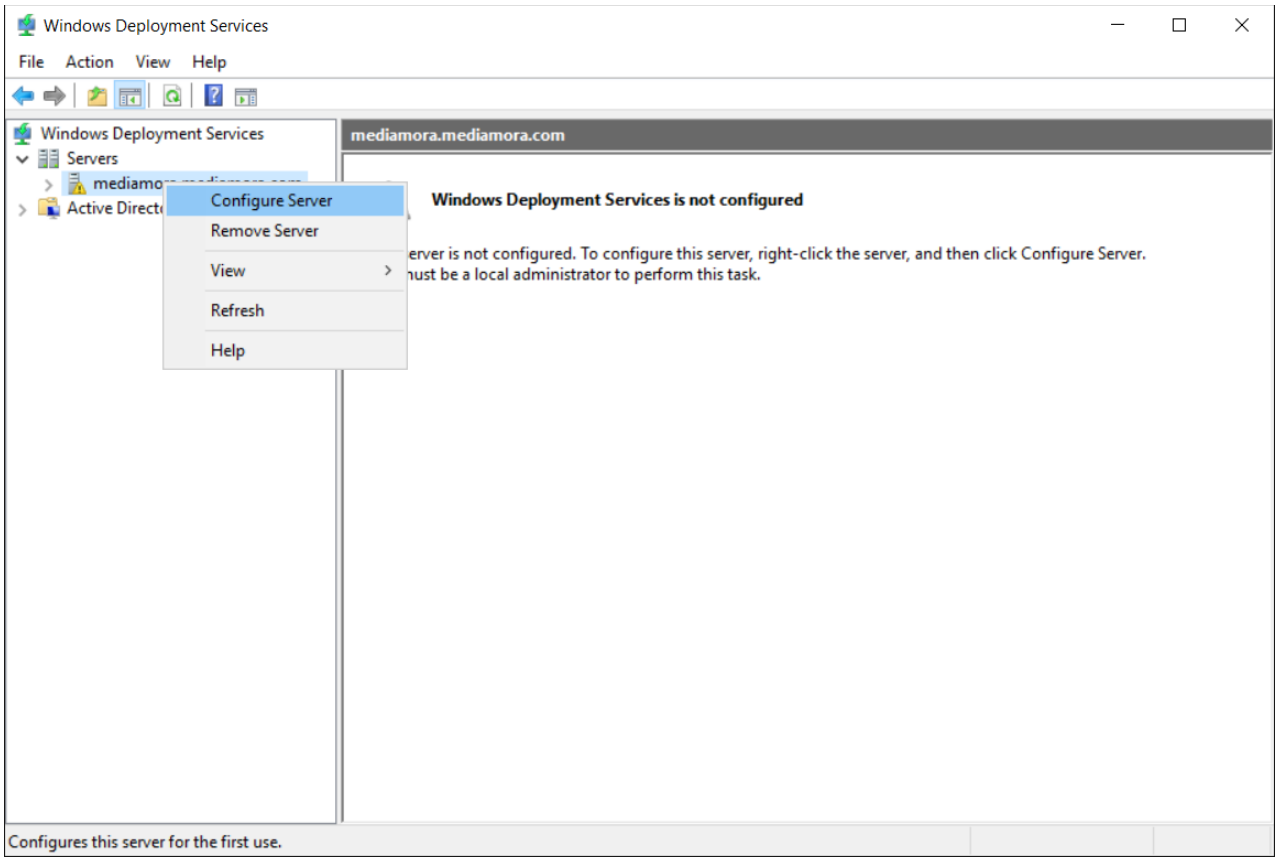
Step 3 – Leave the selections as it is and click next



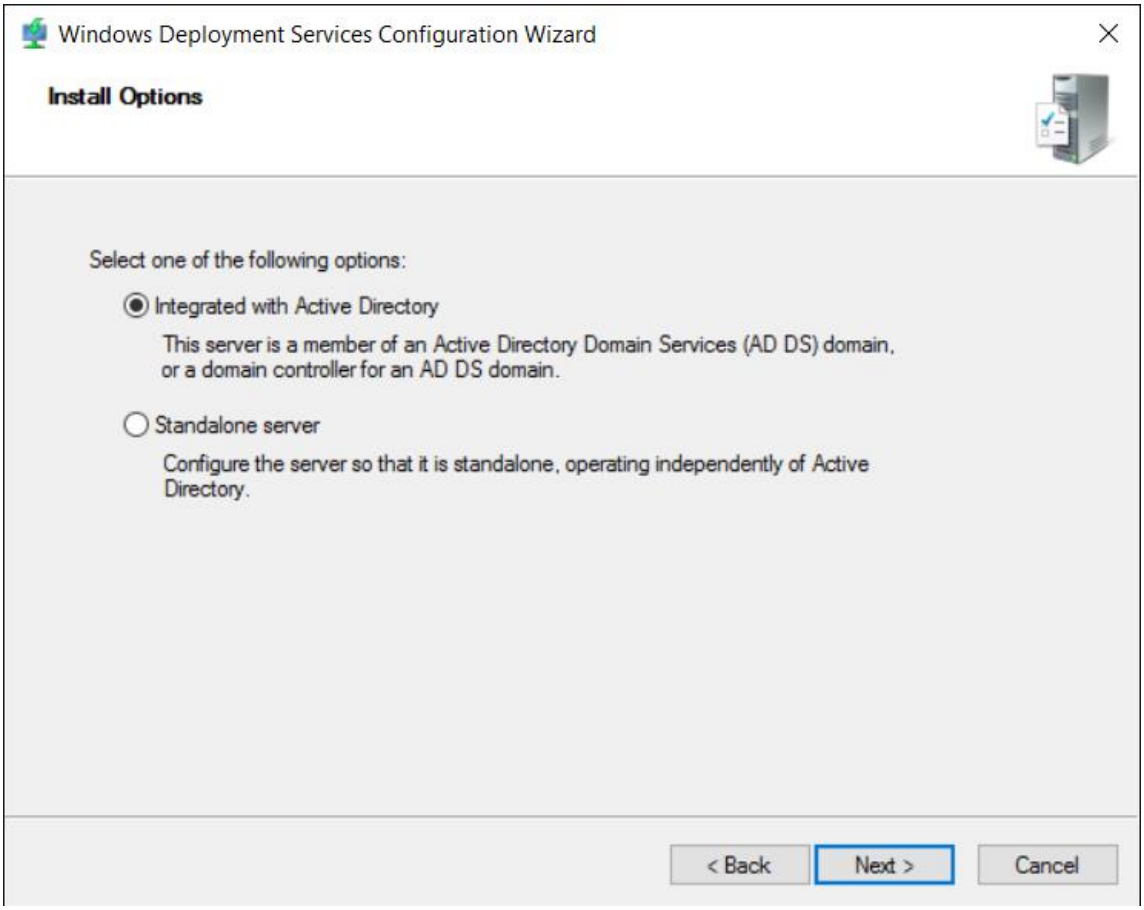
Step 4 – After finishing close the wizard



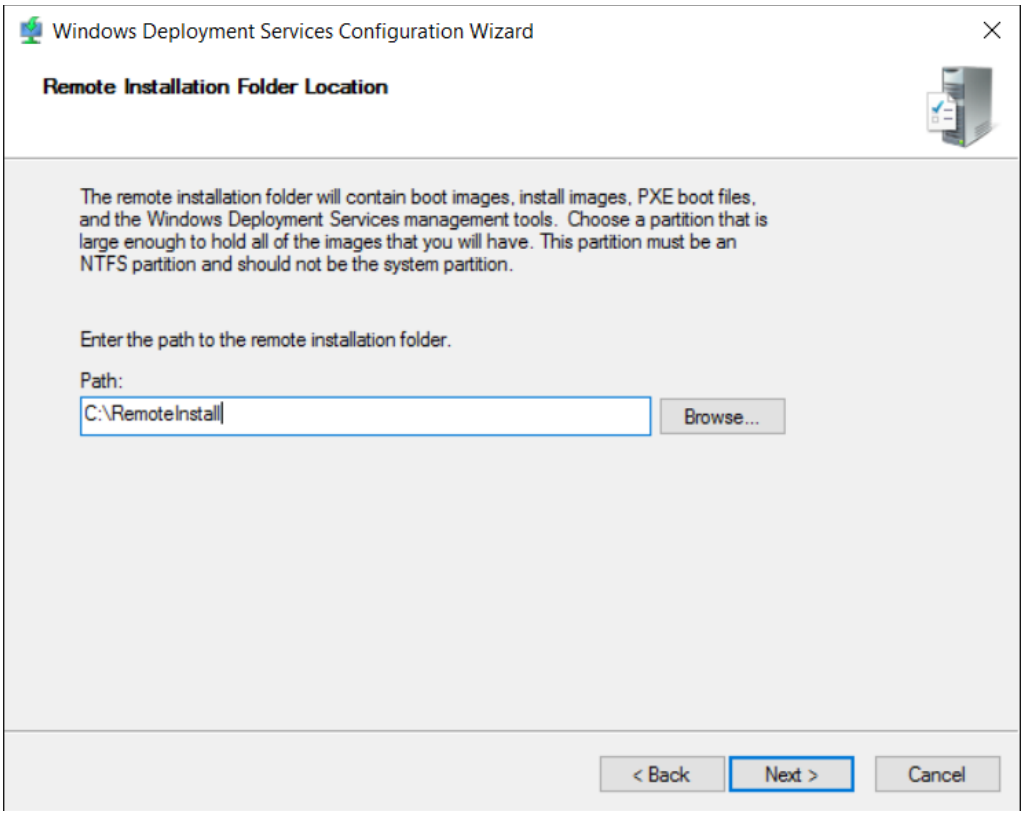
Step 5 – From the tools menu click windows deployment services



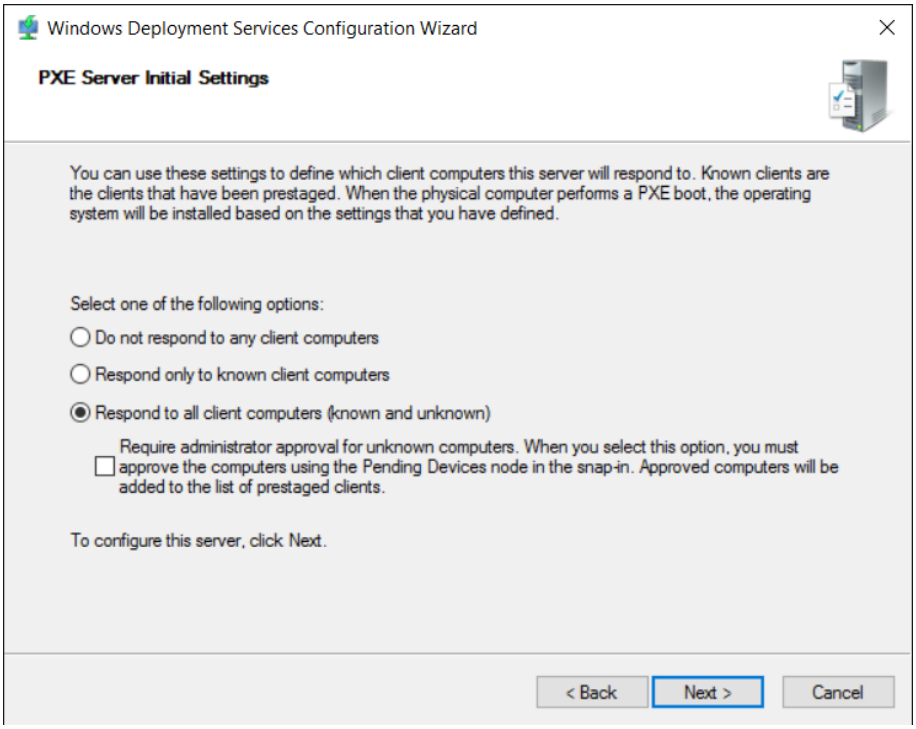
Step 6 – By default WDS is not configured so right click the domain under the servers and click configure server to create a WDS server



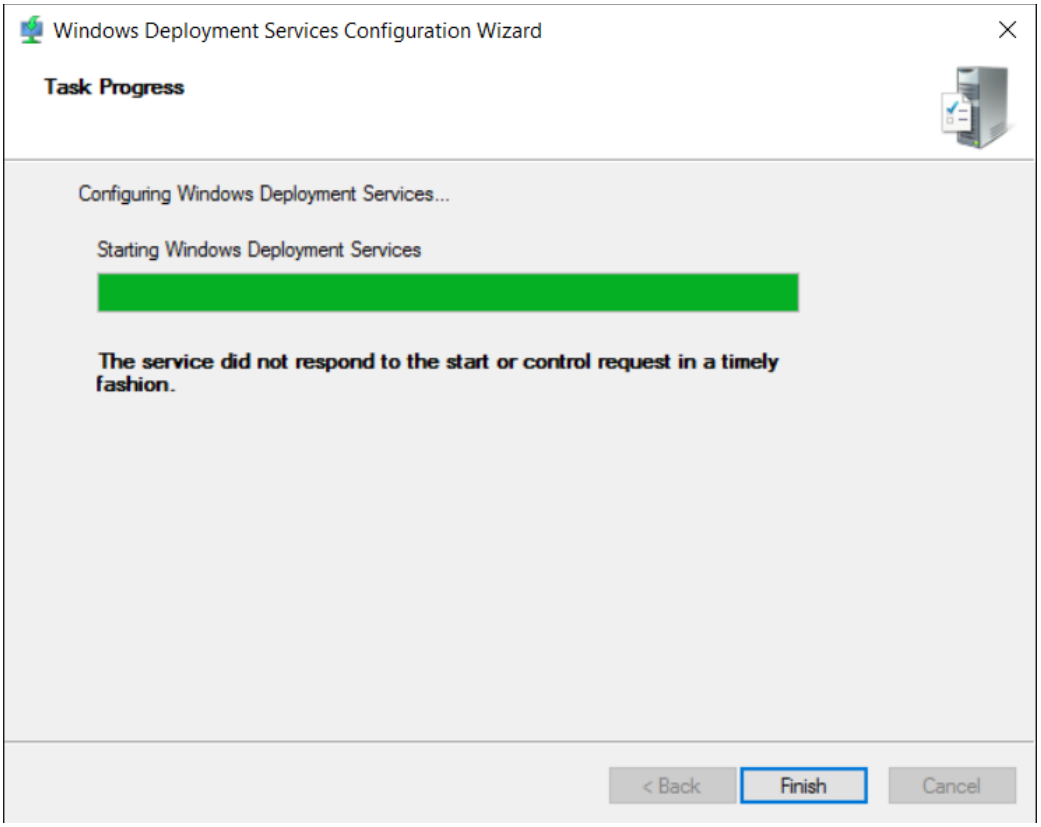
Step 7 – Select integrated with active directory and click next



Step 8 – Select a path to the folder which contains all the install.wim, boot.wim files

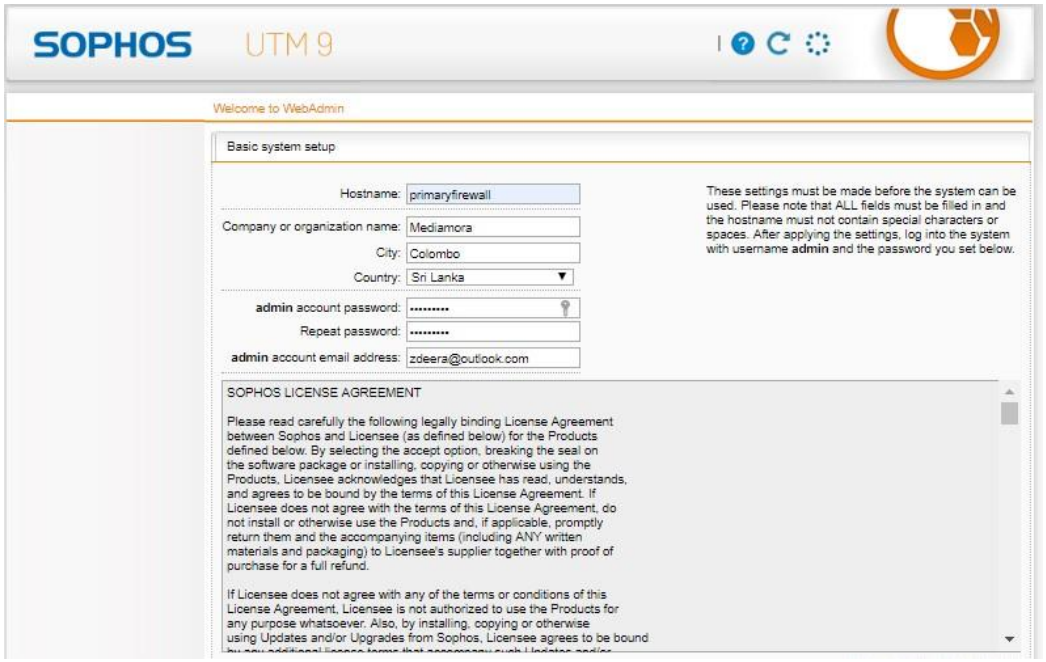


Step 9 – Select Respond to all clients and untick the check box below. Proceed to the next step

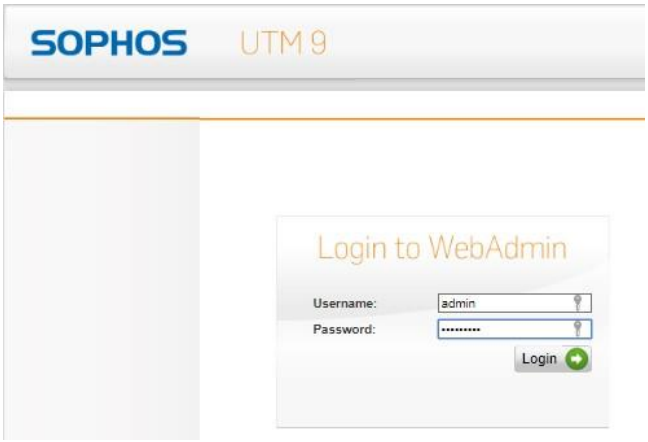


Step 10 – Click finish after installing the services

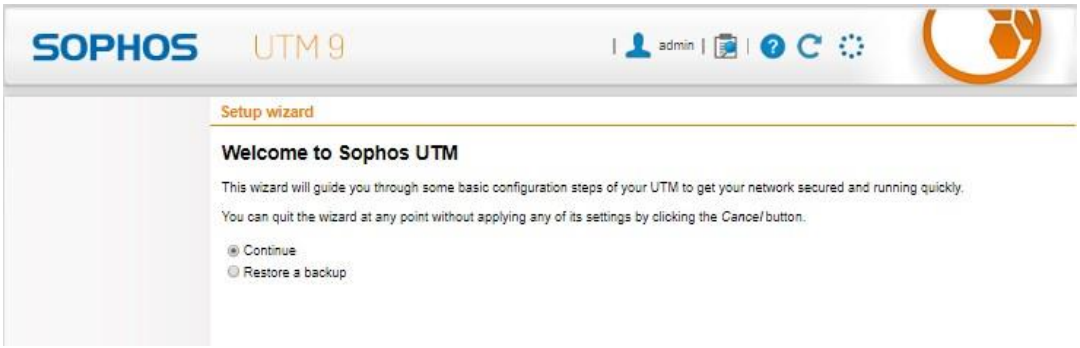
3.8 Implementing the firewall



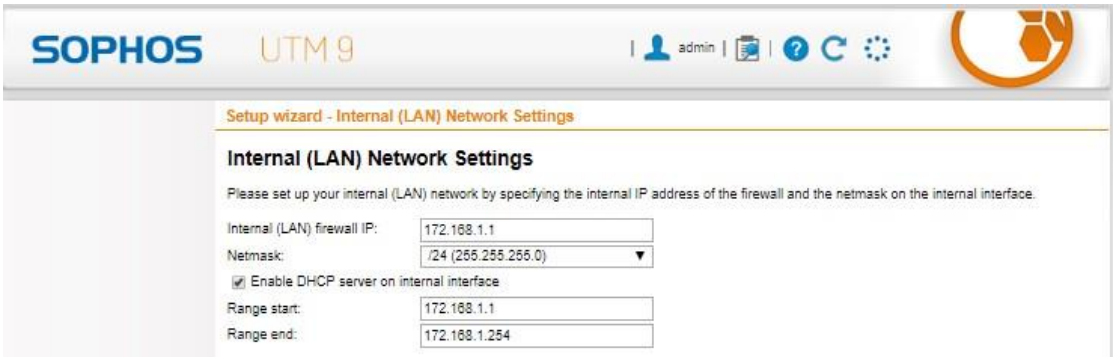
Step 1 – On the welcome screen enter the appropriate details and click perform basic system startup



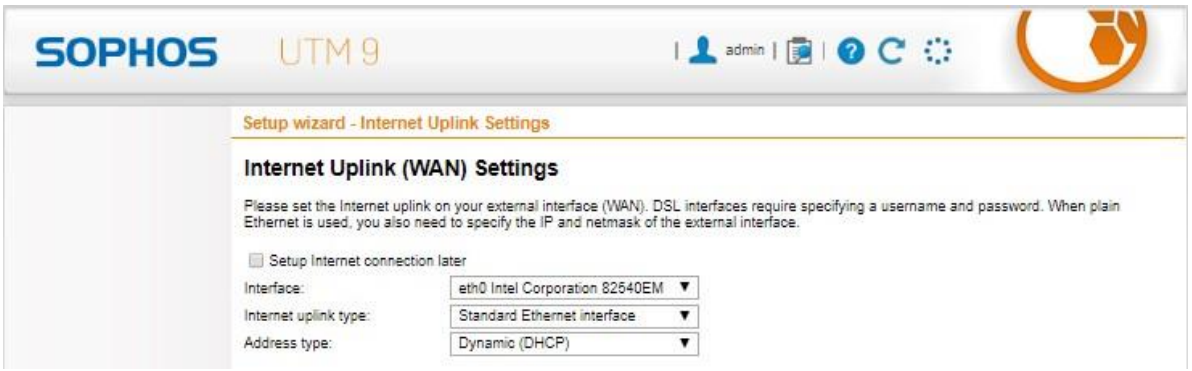
Step 2 – Enter the username and the password



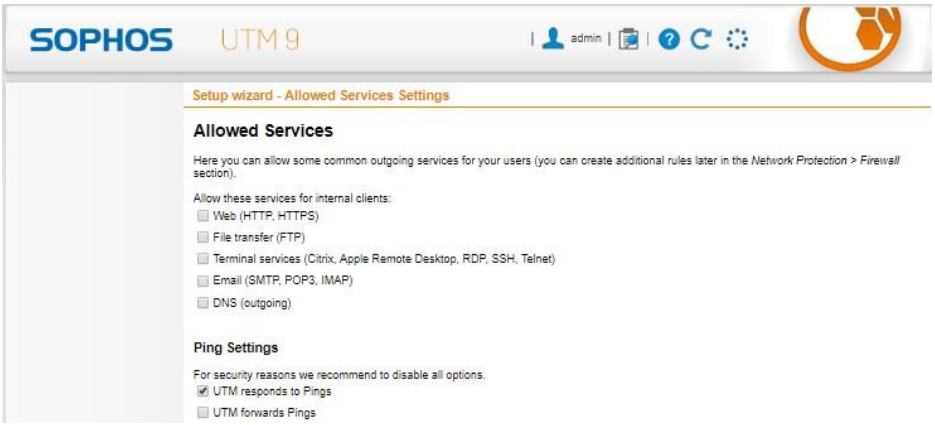
Step 3 – Click continue and proceed next



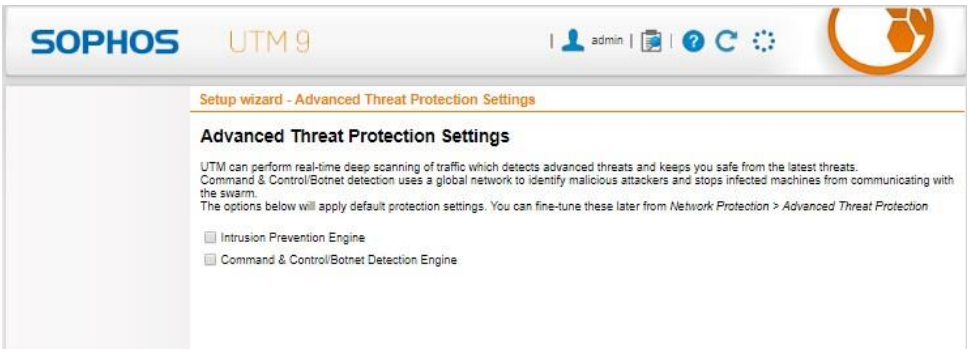
Step 4 - Enter the internal gateway for the firewall and the appropriate netmask and click next



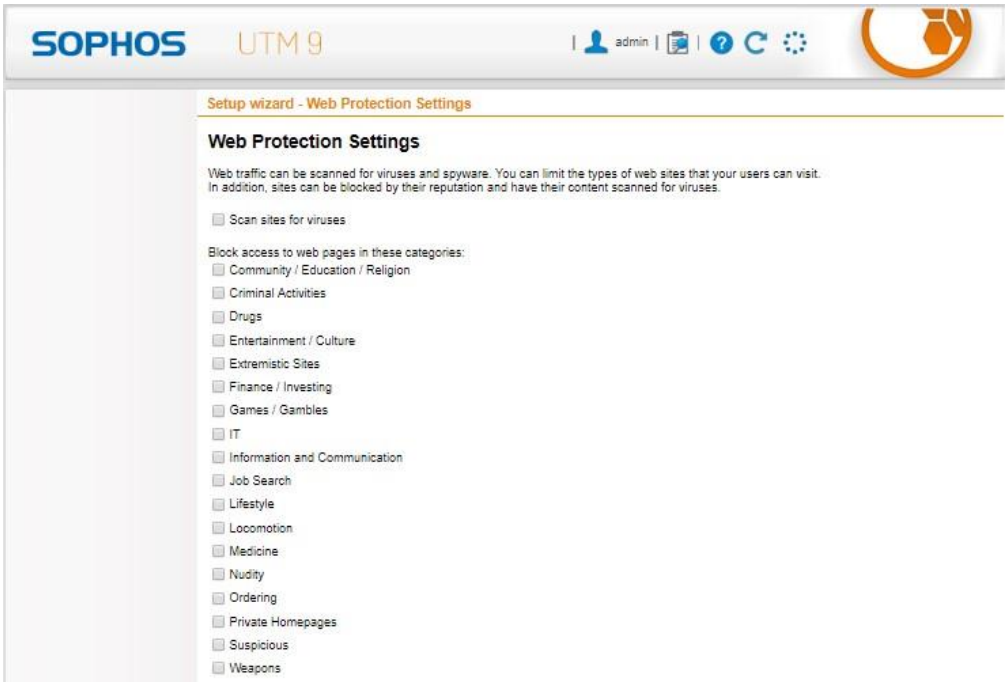
Step 5 – Select the appropriate WAN interface and click next



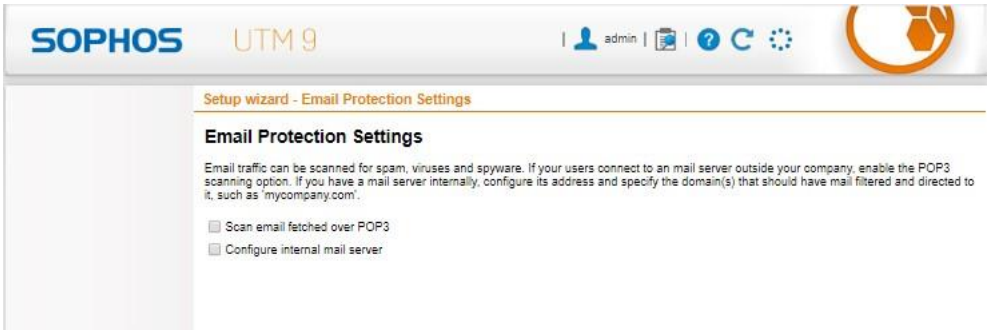
Step 6 – In the allowed list unselect everything because we will configure manually



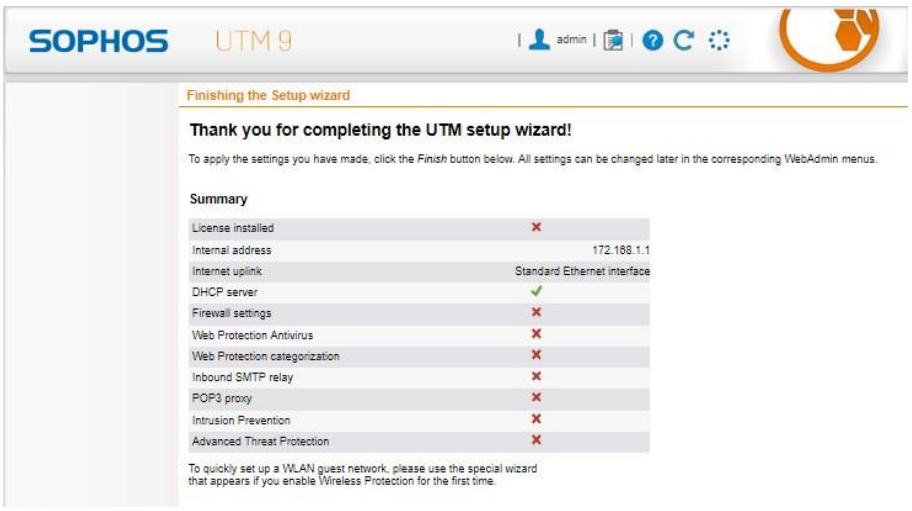
Step 7 – Proceed to the next step without making any changes



Step 8 – Select the areas you want to block but I recommend not to select anything because everything will be configured manually

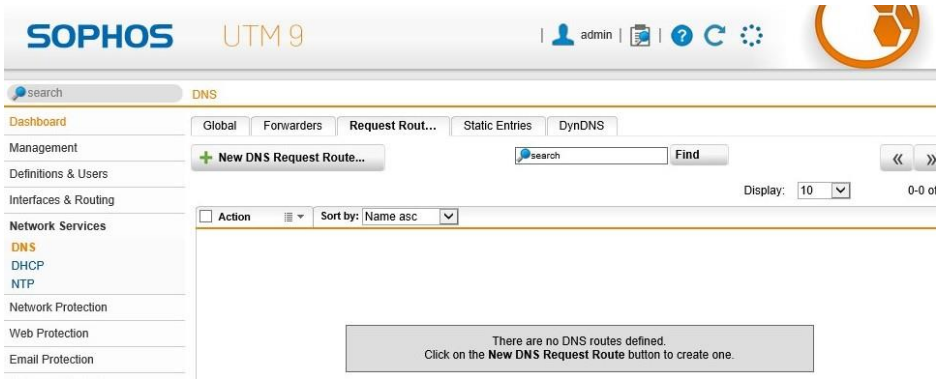


Step 9 – Proceed to the next step without making any changes

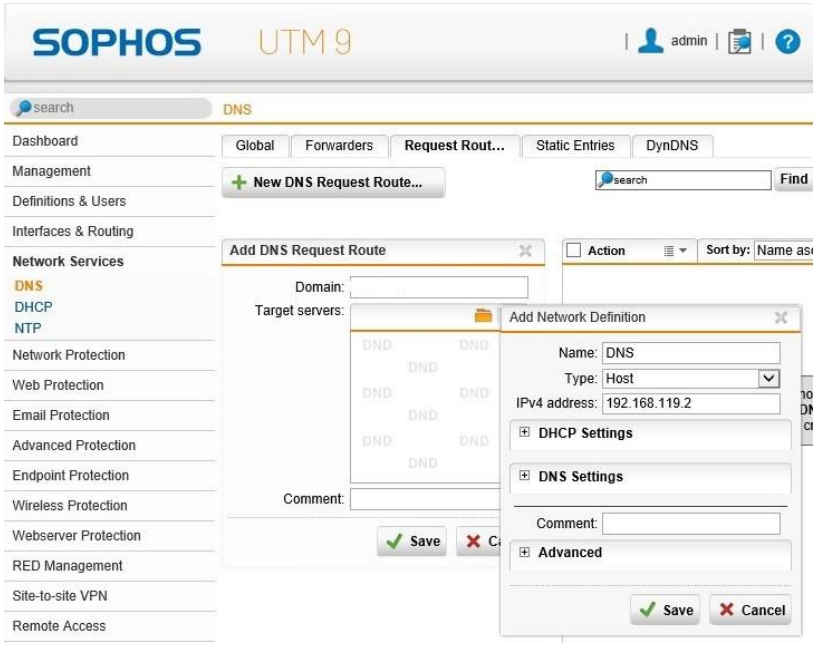


Step 10 – Finish the wizard

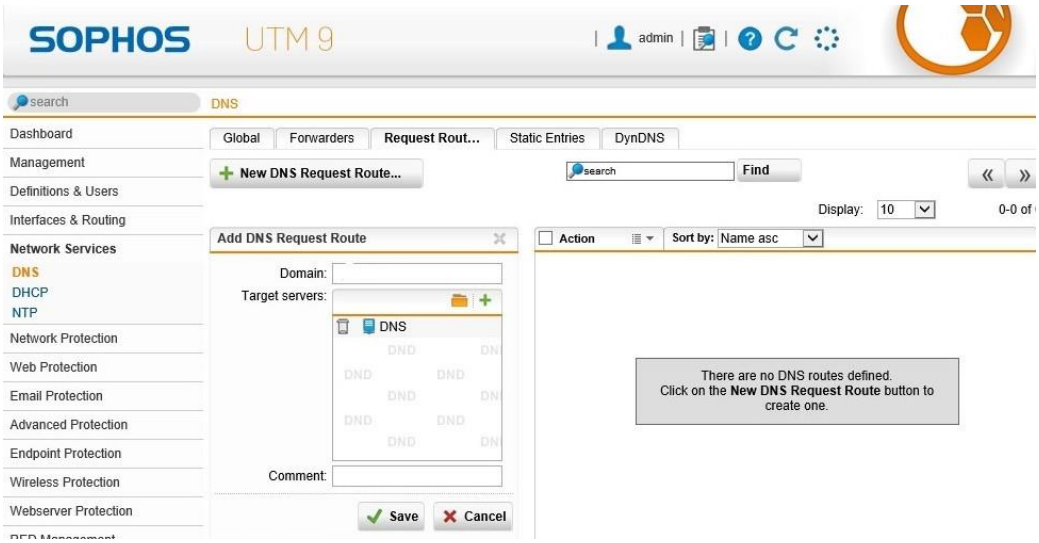
3.8.1 Adding domain users to the firewall and configuring DNS query service



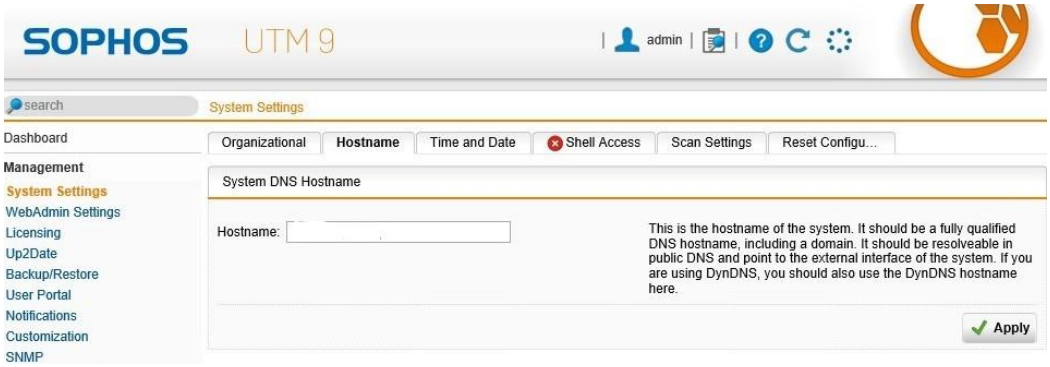
Step 1 – Go to network services and click DNS



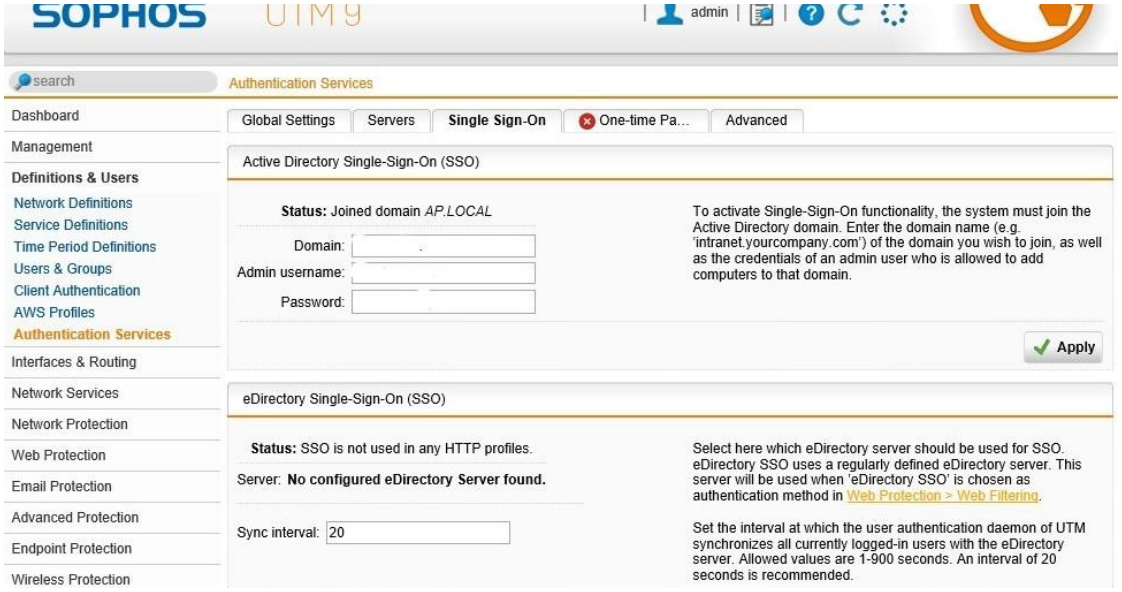
Step 2 – Enter the domain name and the IP address and click save



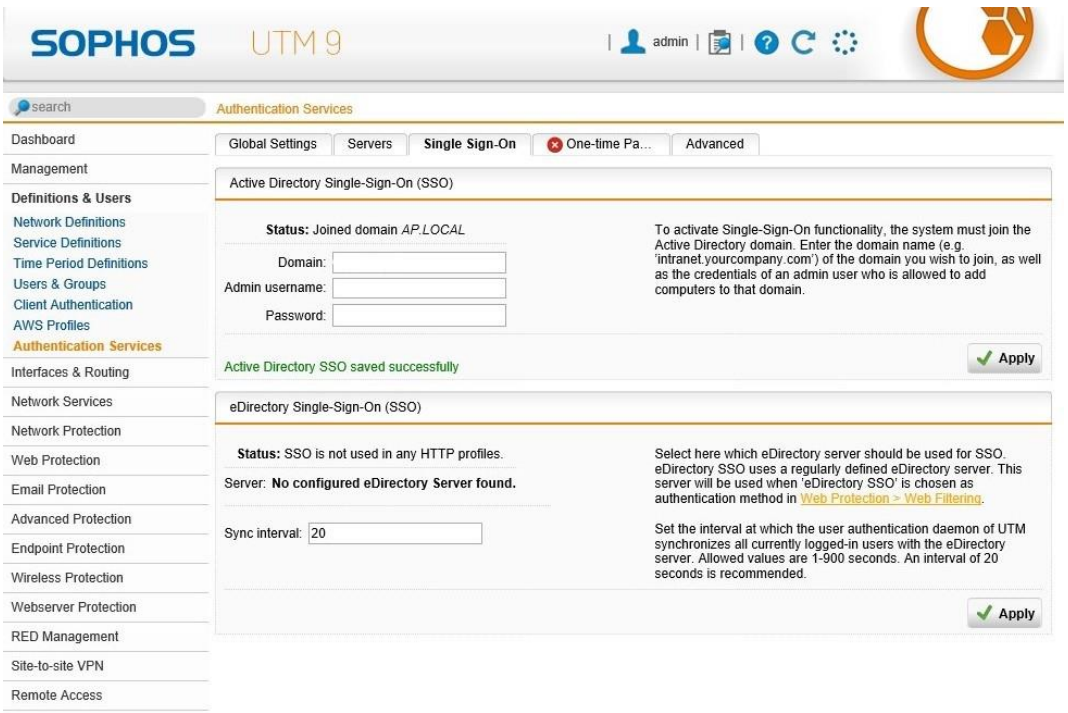
Step 3 – As you can see we have created the DHS request route successfully



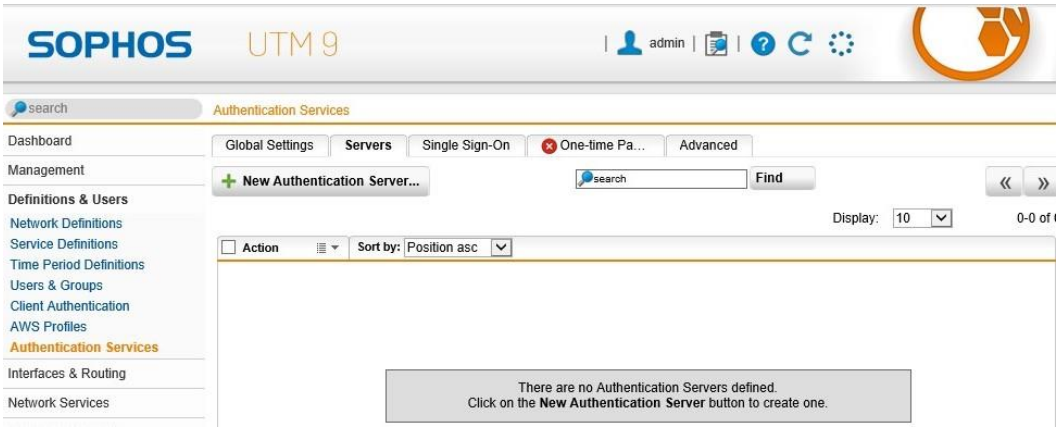
Step 4 – Go to the management section and enter a hostname



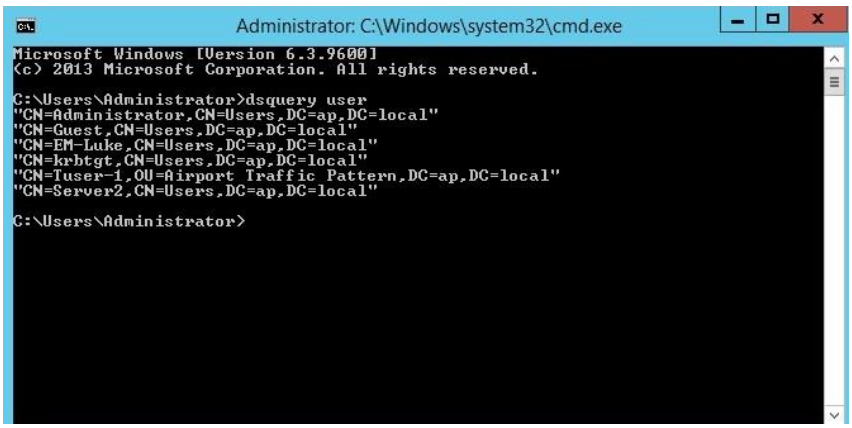
Step 5 – Enter the domain name, admin username and the password



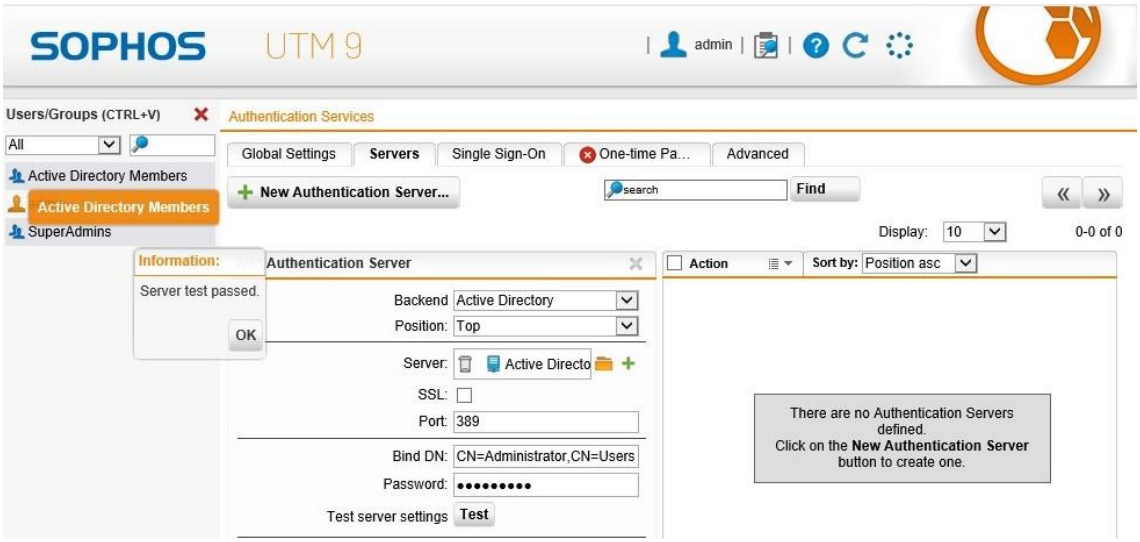
Step 6 – Active directory is successfully configured



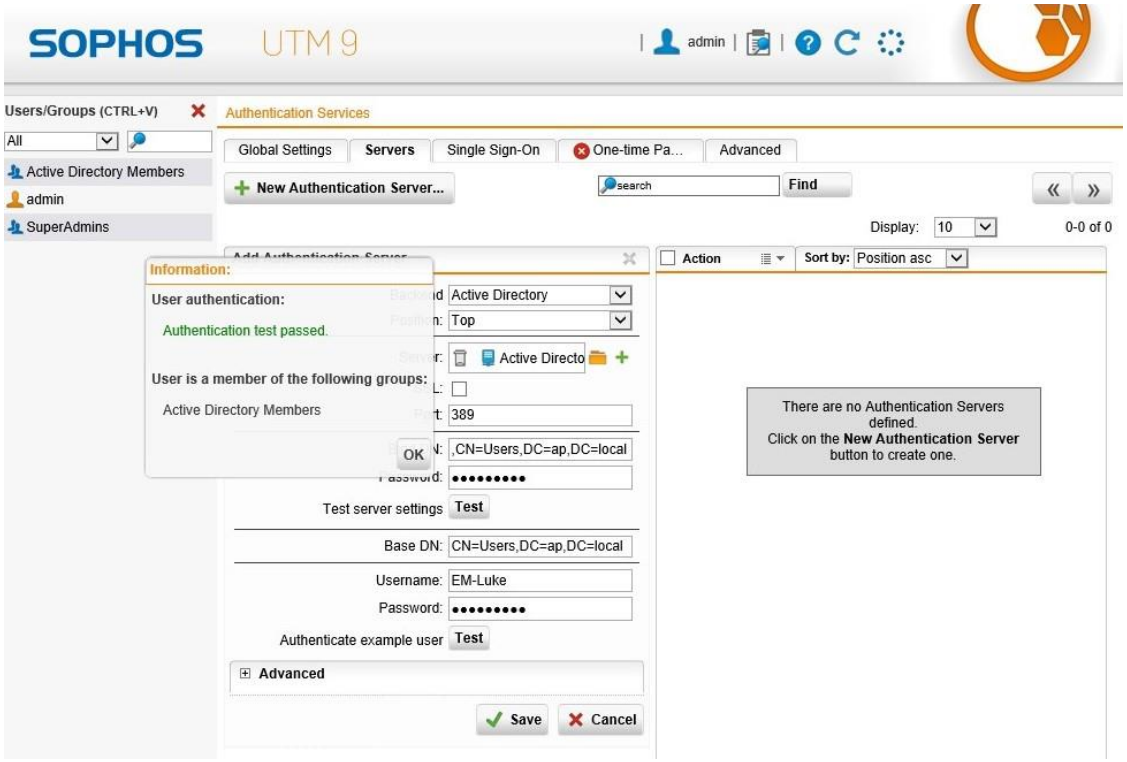
Step 7 – Go to the authentication services under the tab definitions and users to configure domain users to the firewall



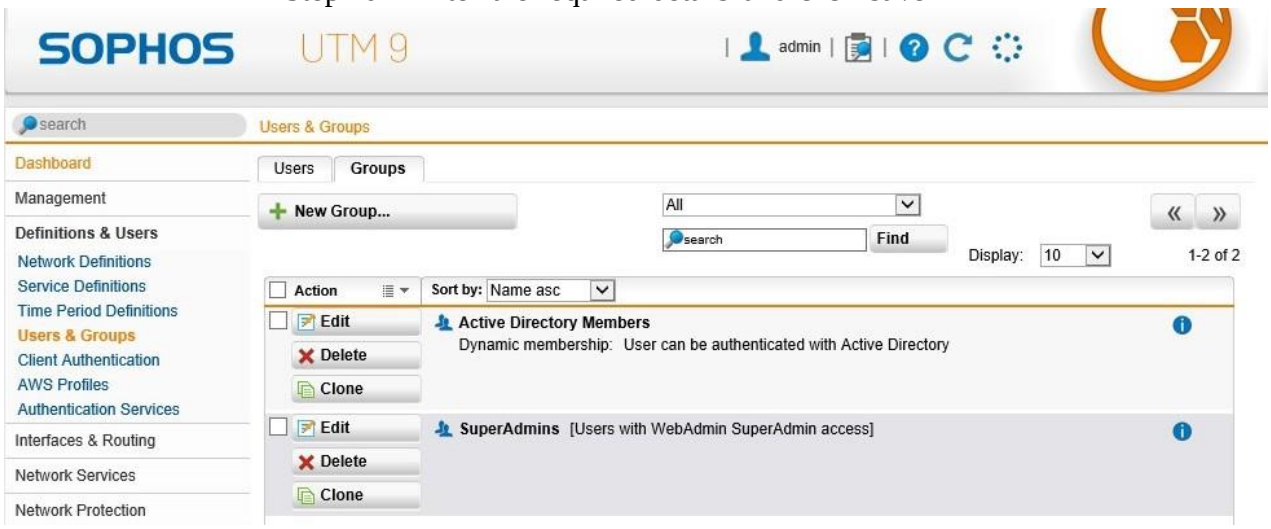
Step 8 – Open command prompt in the administrative mode and enter the dsquery user command



Step 9 – Under the authentication servers type the previous command in the bind DN blank

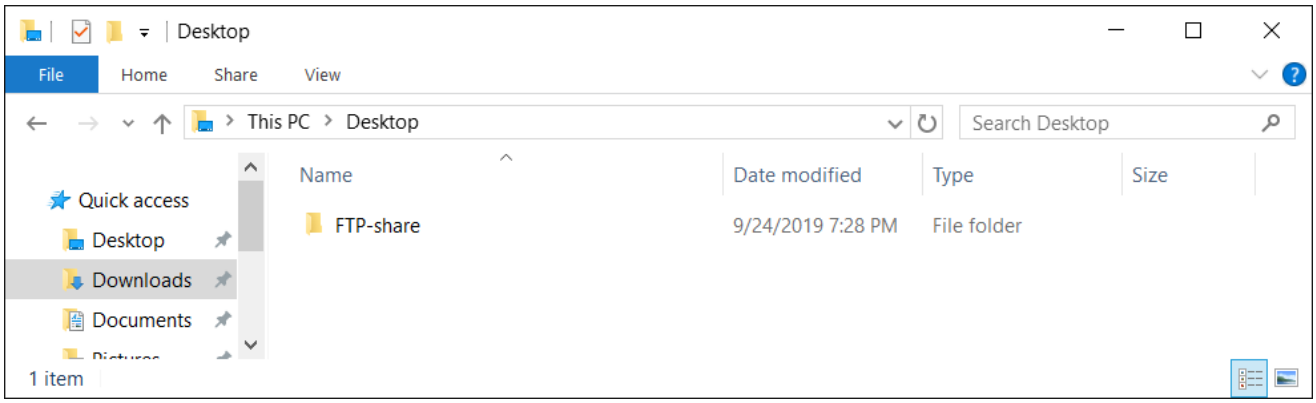


Step 10 – Enter the required details and click save

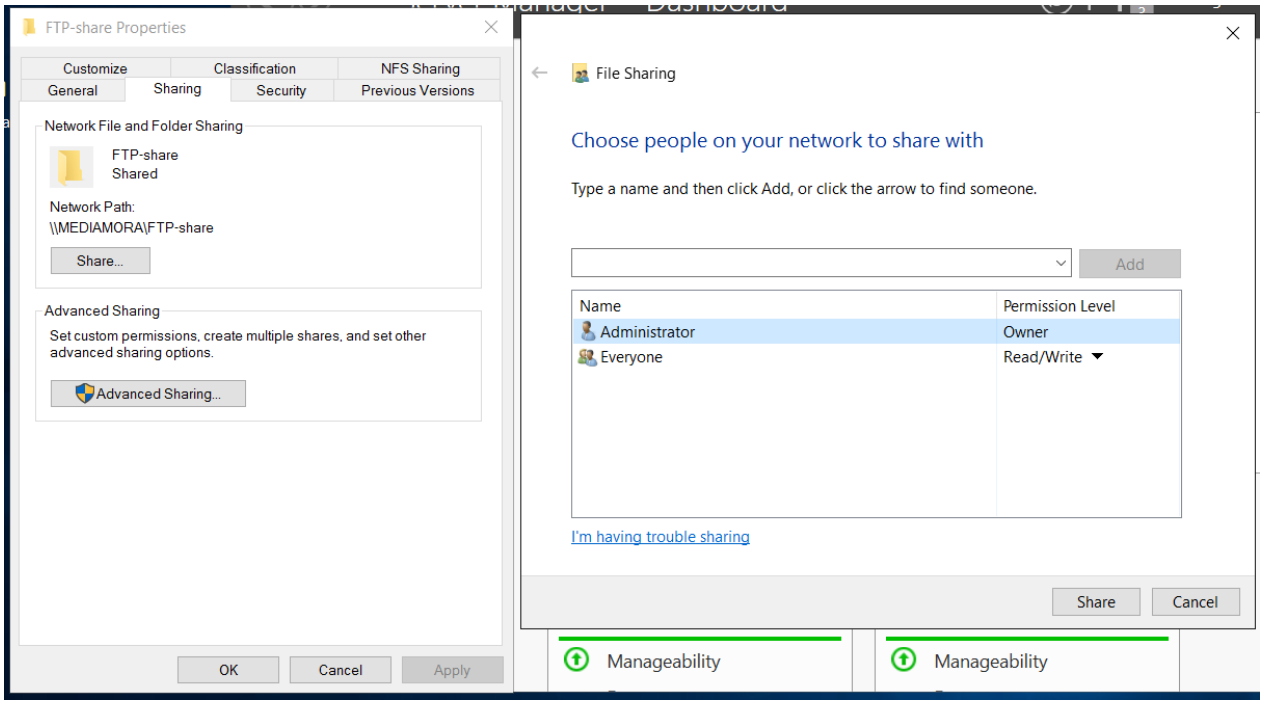


Step 11 – Under the firewall groups you can now see there are active directory users

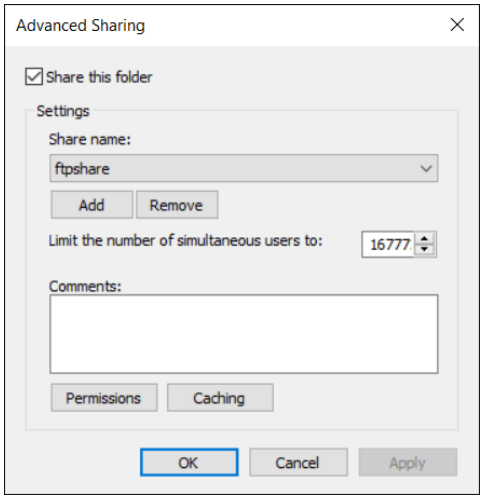
3.9 Implementing a SMB server



Step 1– Create a new folder and rename it as FTP-share



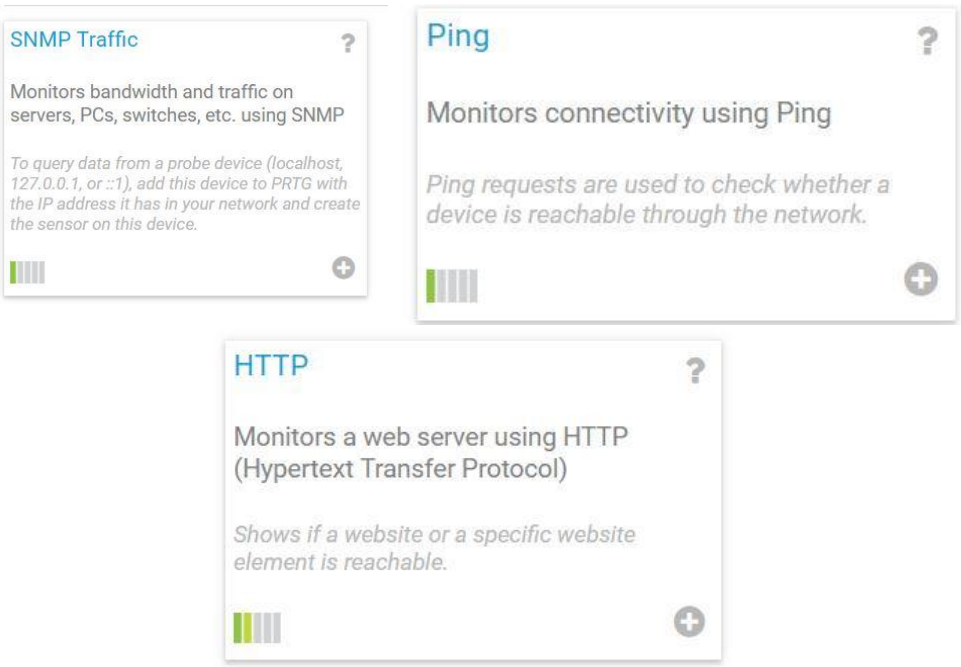
Step 2 – Share the folder and give access permission to everyone



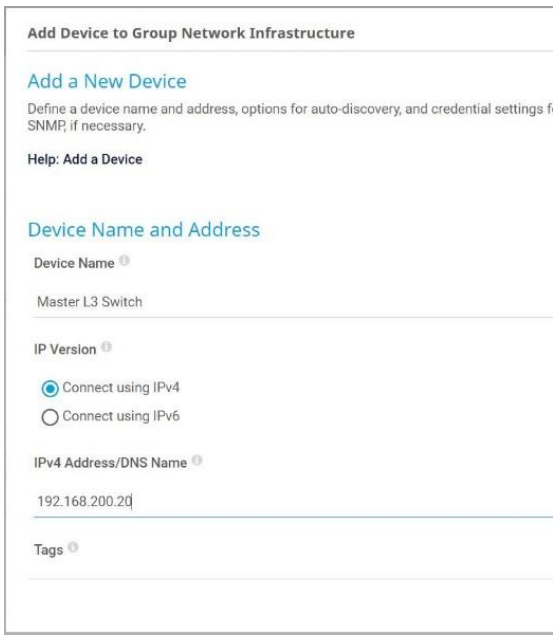
Step 3 – Give share name

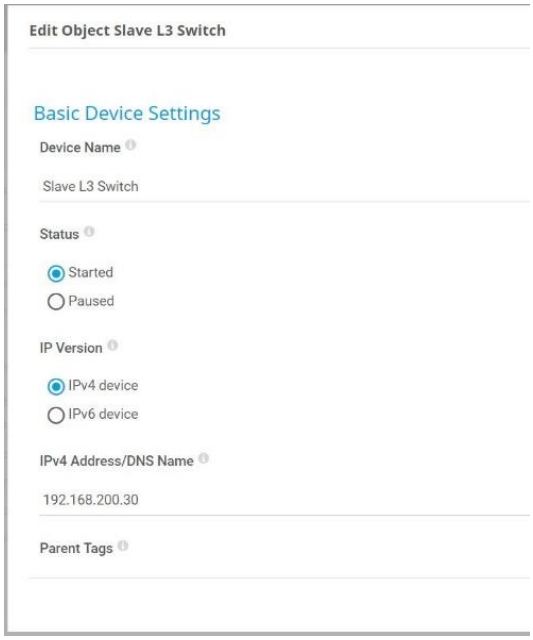
3.10 Implementing a network monitoring system

3.10.1 Monitoring methods to be implemented

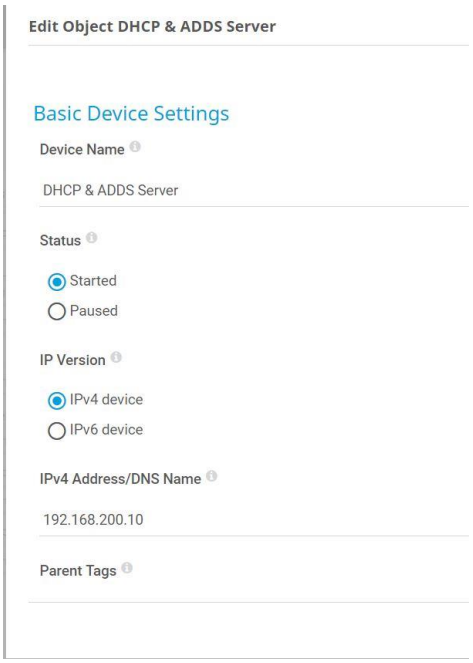


3.10.2 Master L3 Switch and Slave L3 Switch

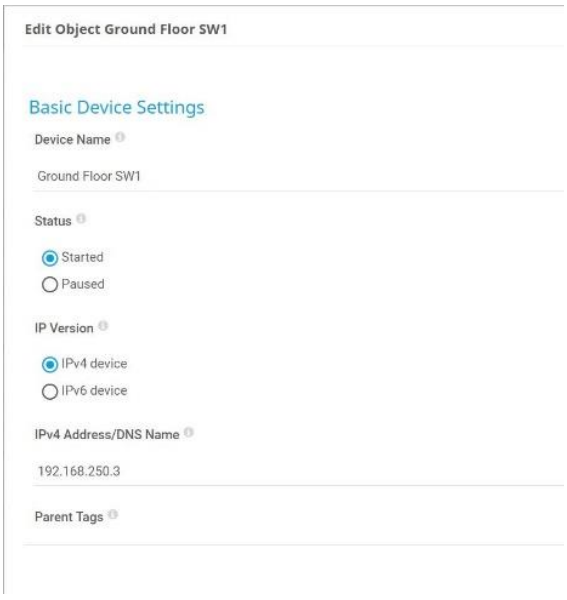


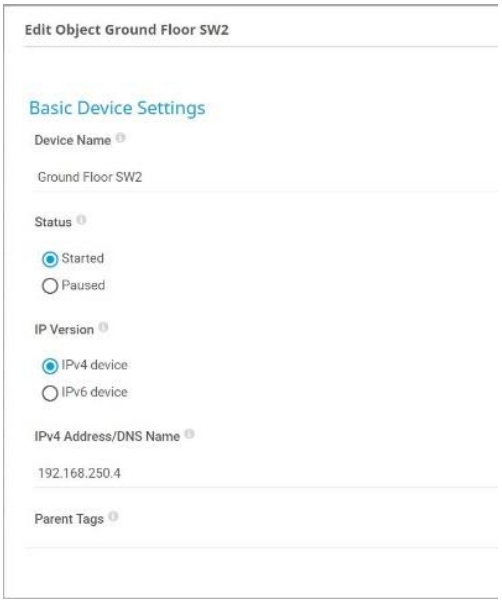


3.10.3 Adding Server for monitoring

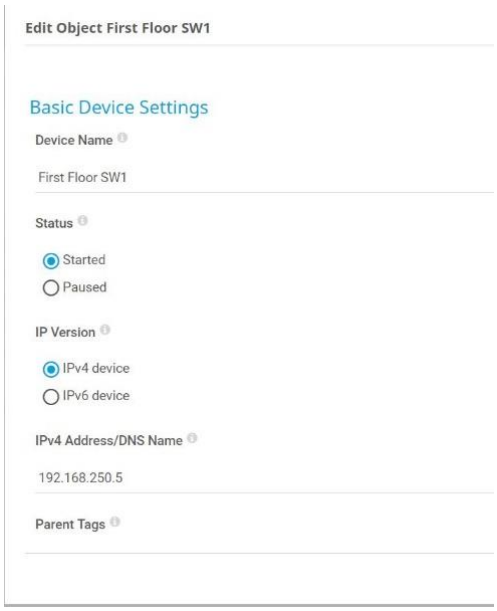


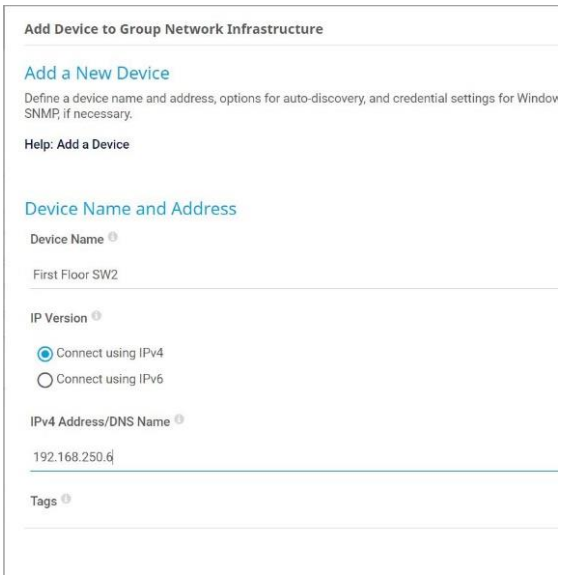
3.10.4. Ground Floor Switches

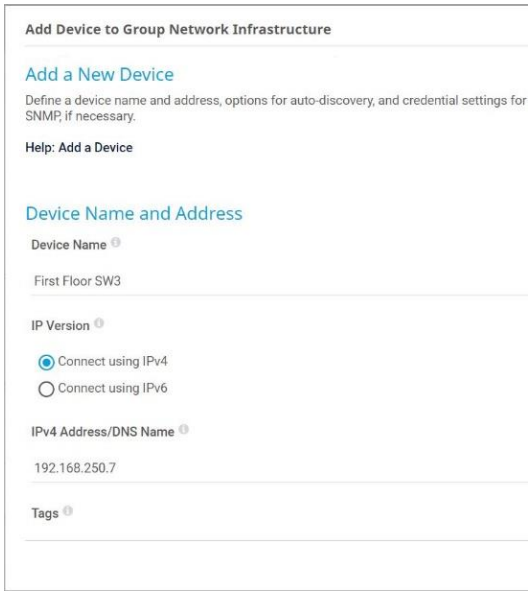


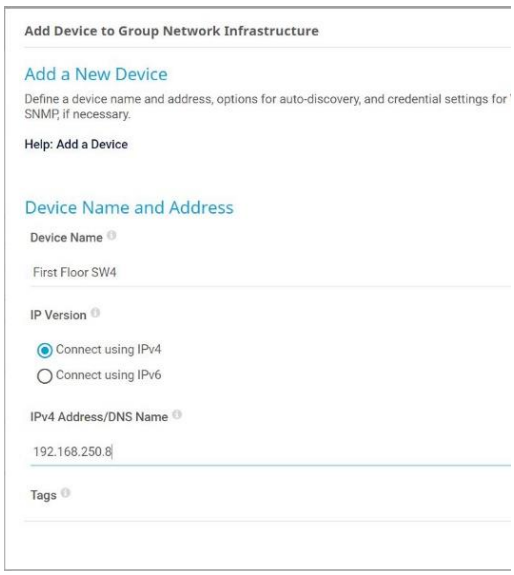


3.10.5 First Floor Switches

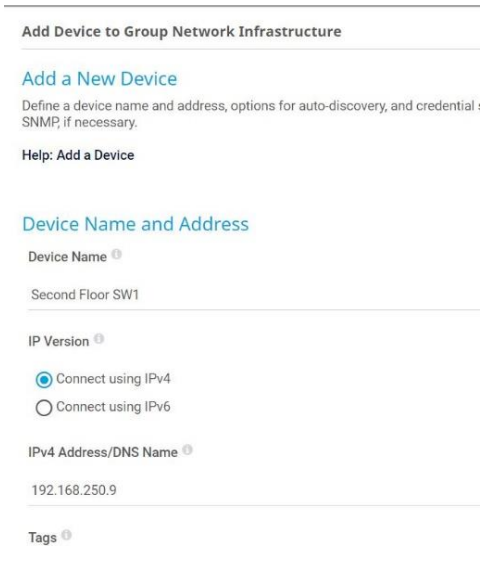


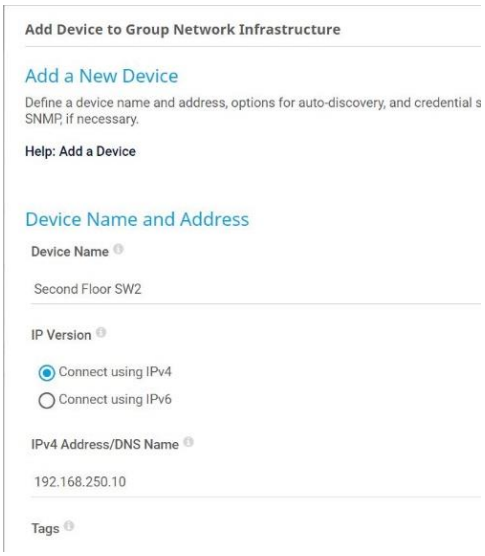


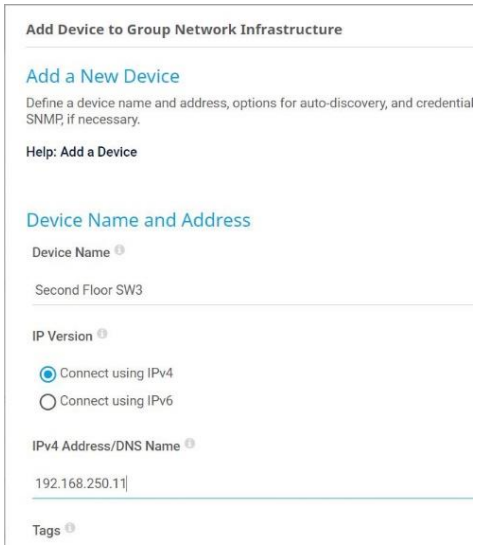


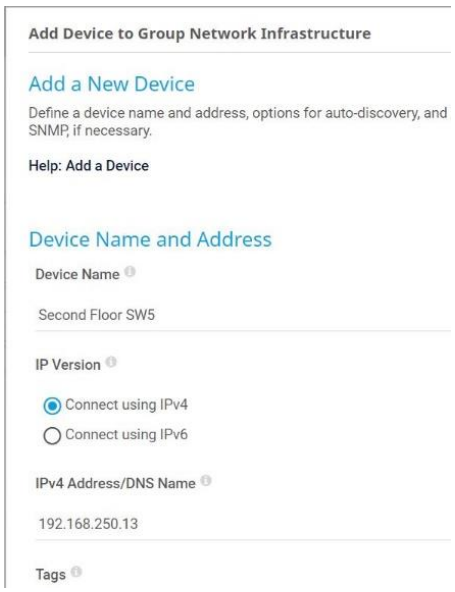


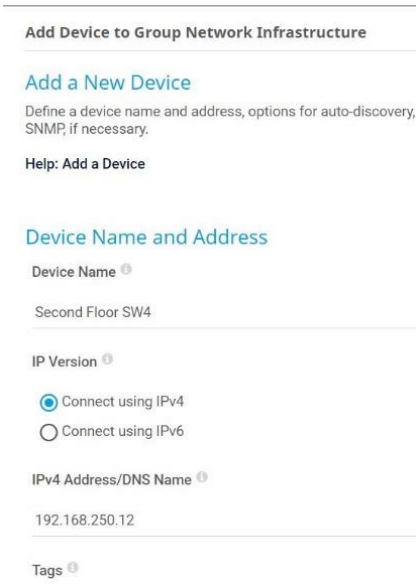
3.10.6 Second Floor Switches



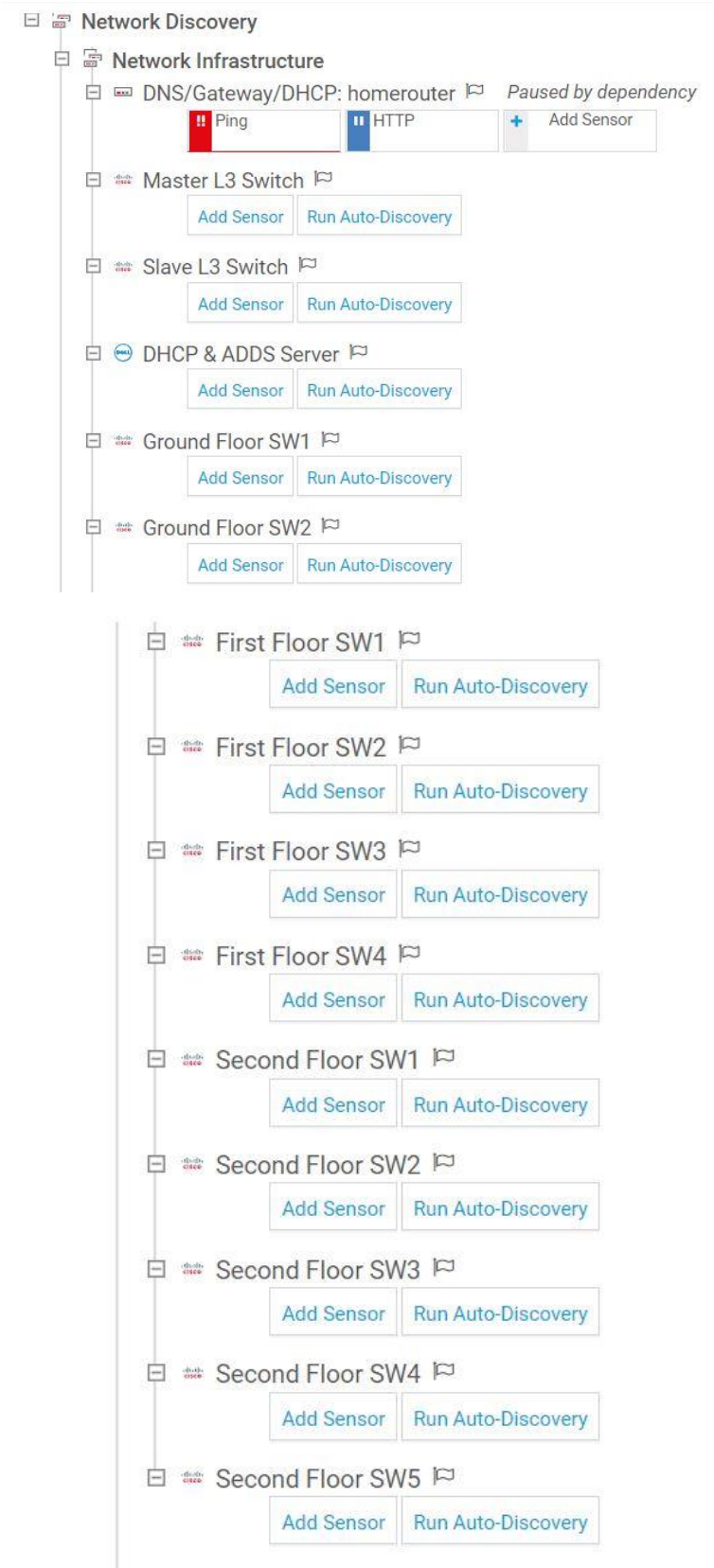




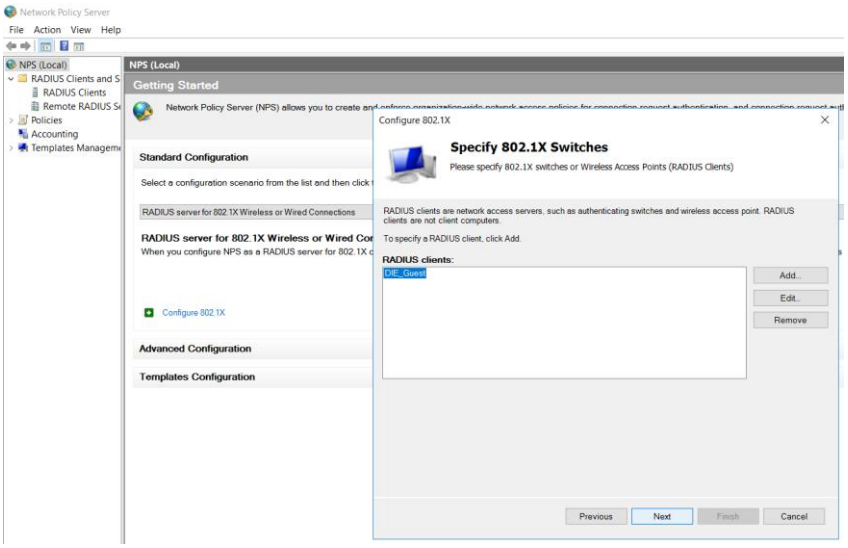


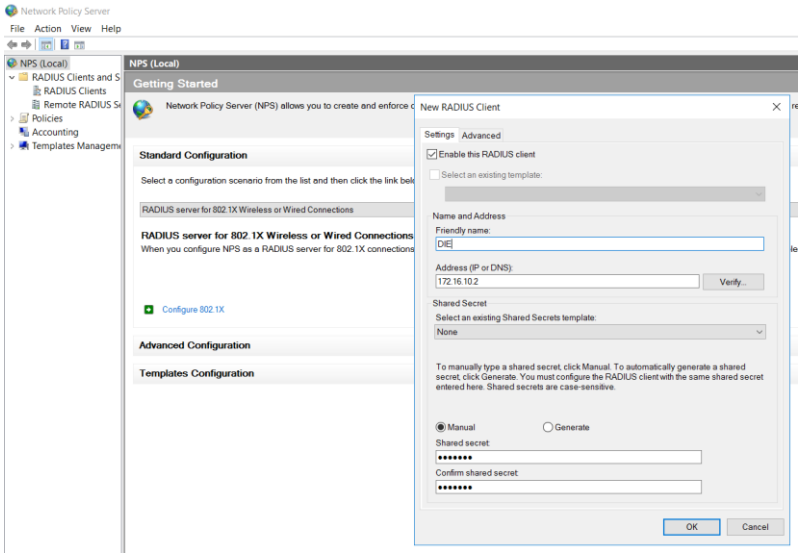


3.10.7 PRTG Devices Tab

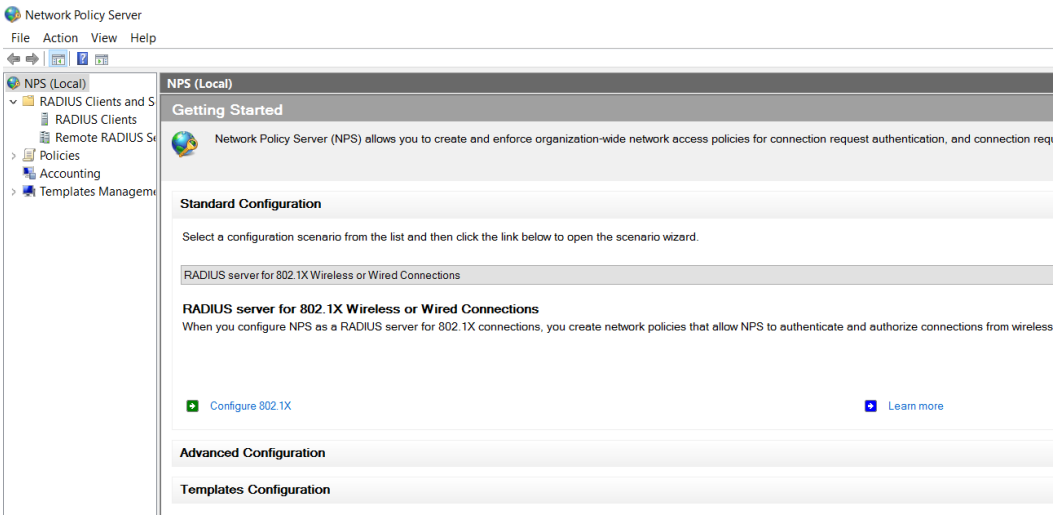


3.11 Implementing Radius

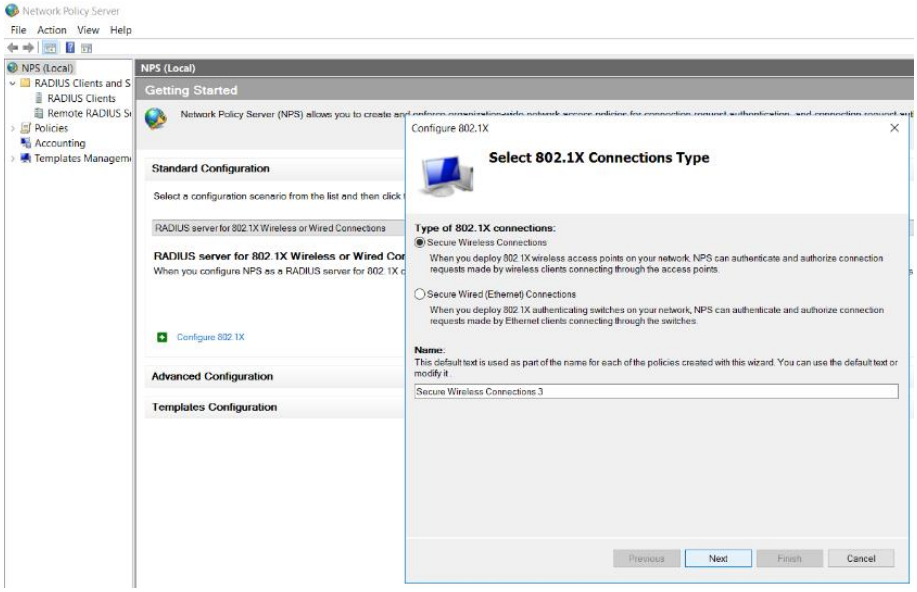




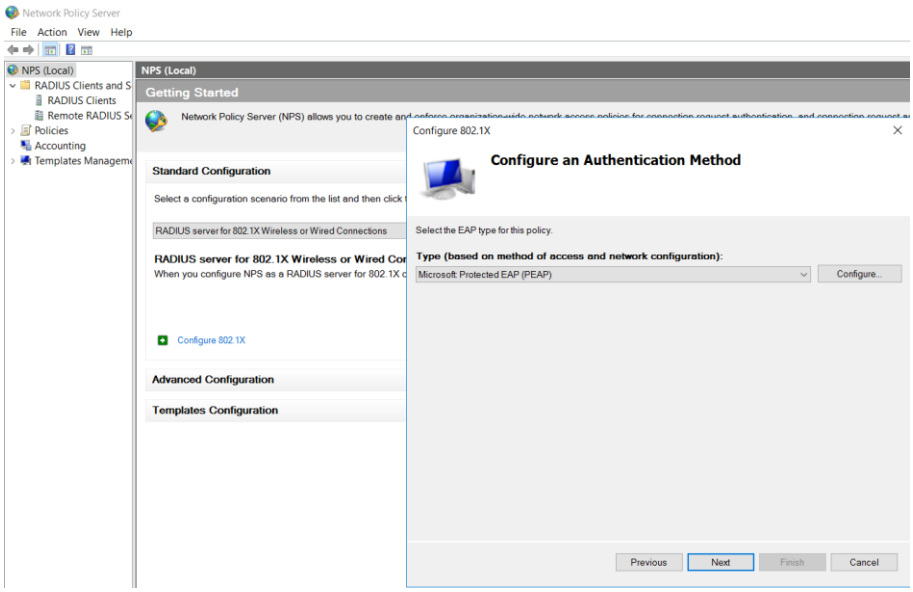
Step 1: Selecting radius client device



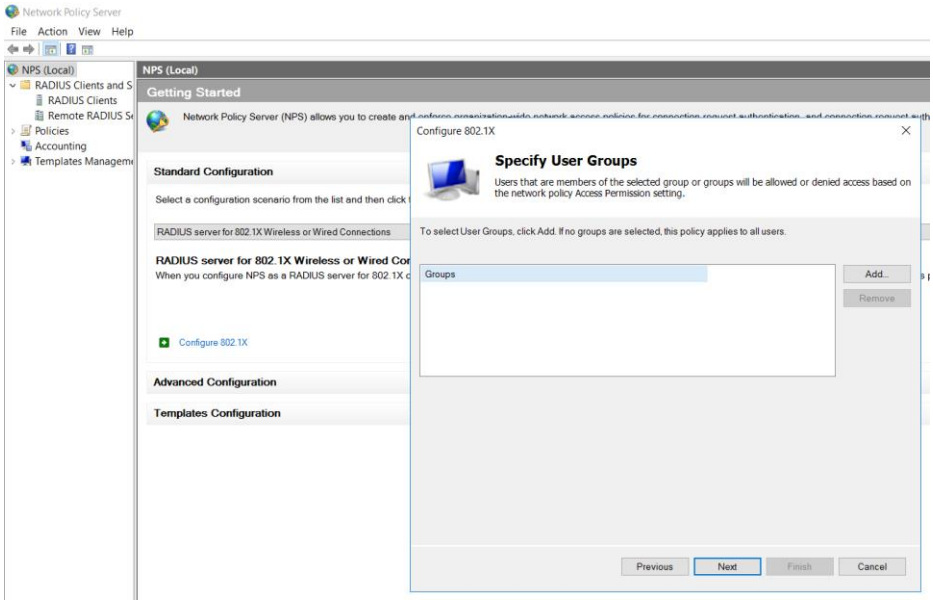
Step 2 : Select the network policy to be configured



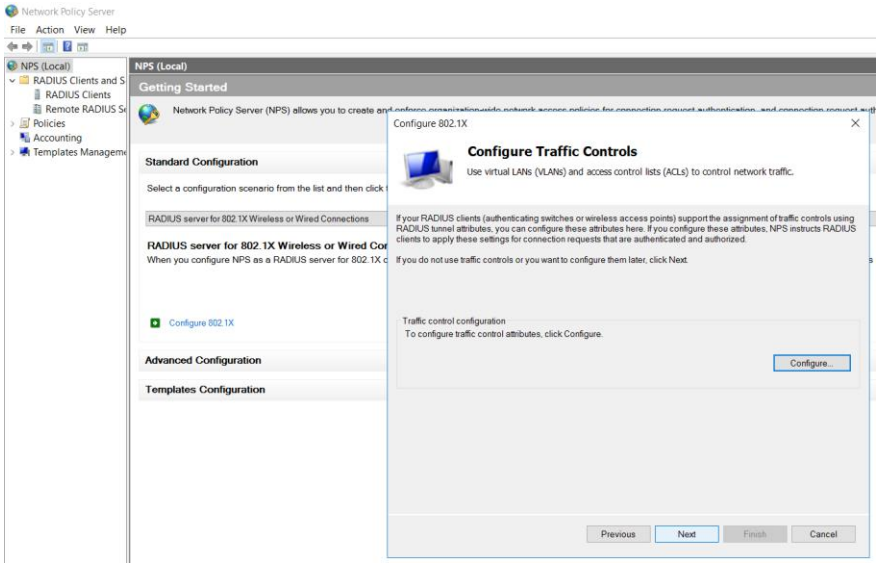
Step 3: Select the Wireless connection type



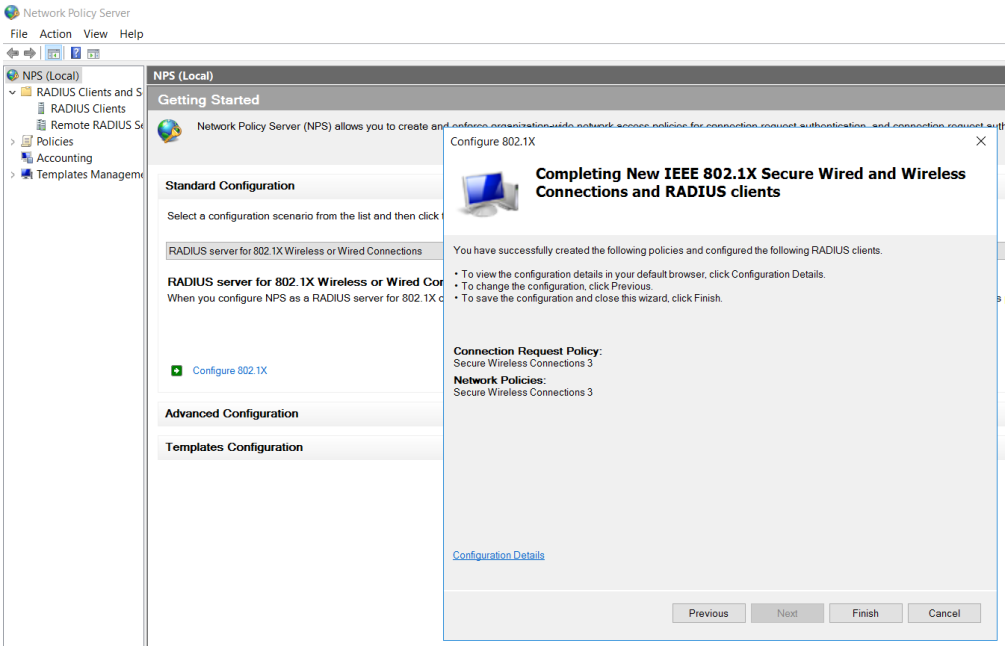
Step 4: Select the network authentication method

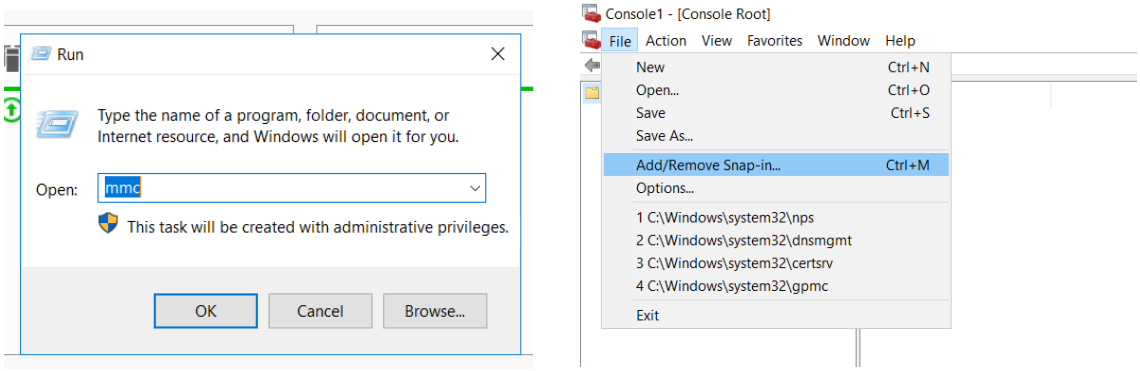


Step 5: Select and add the user group to authenticate

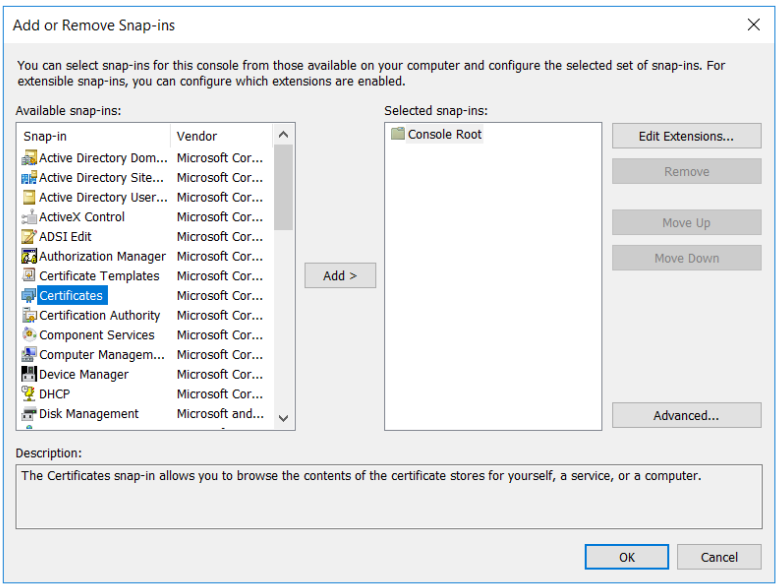


Step 6: Configure traffic controls for better security

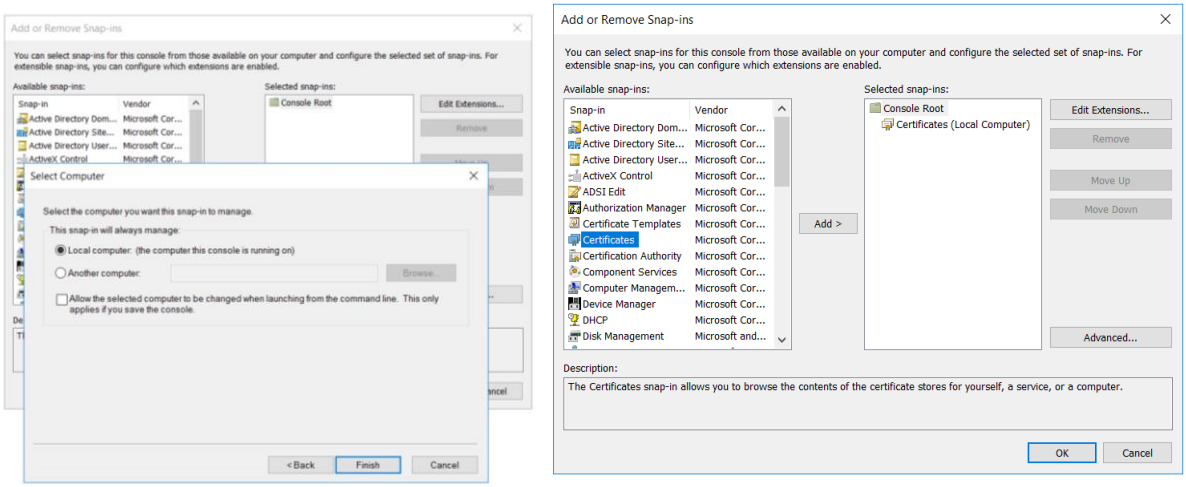




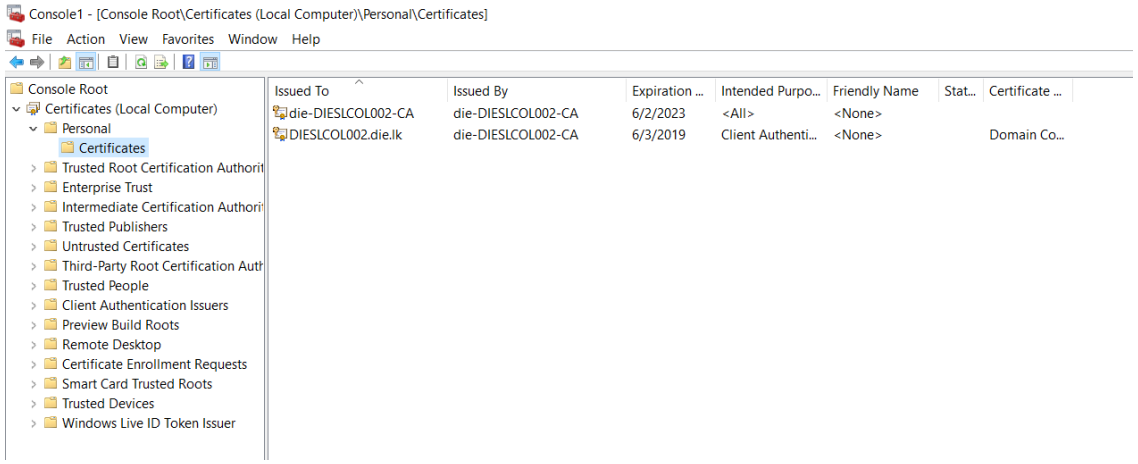
Step 7: Open Microsoft Management Console

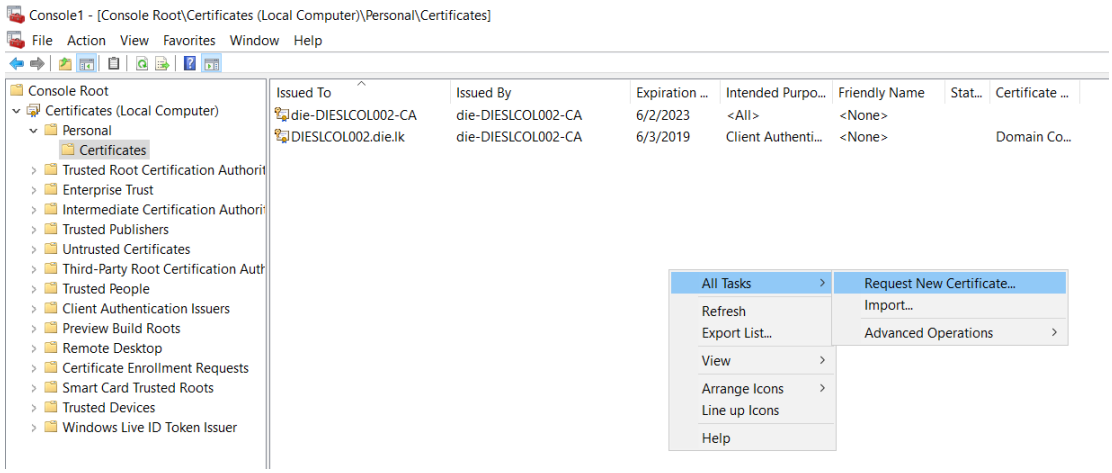


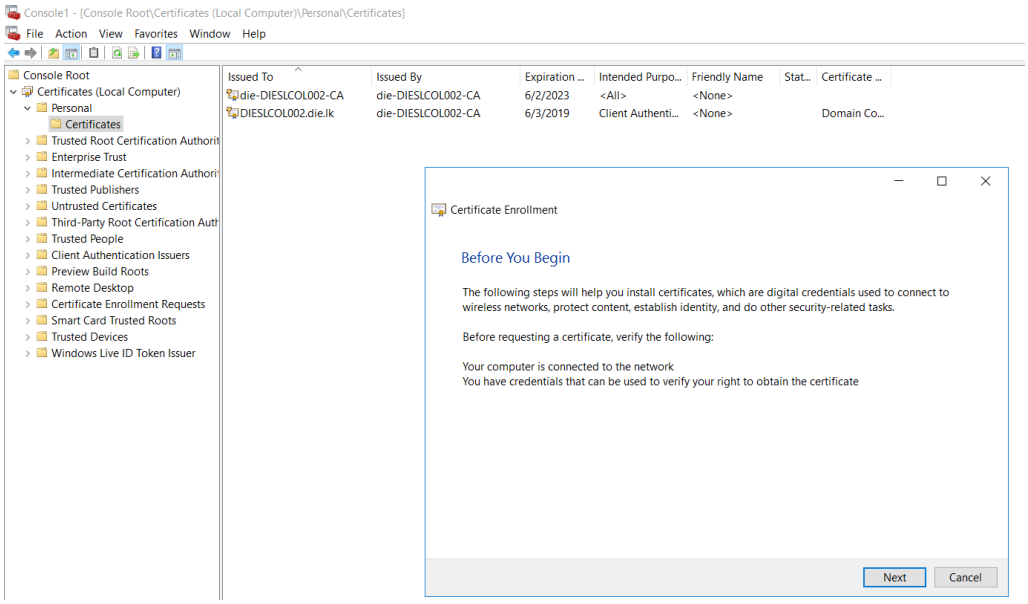
Step 8: Add certificate snap-in



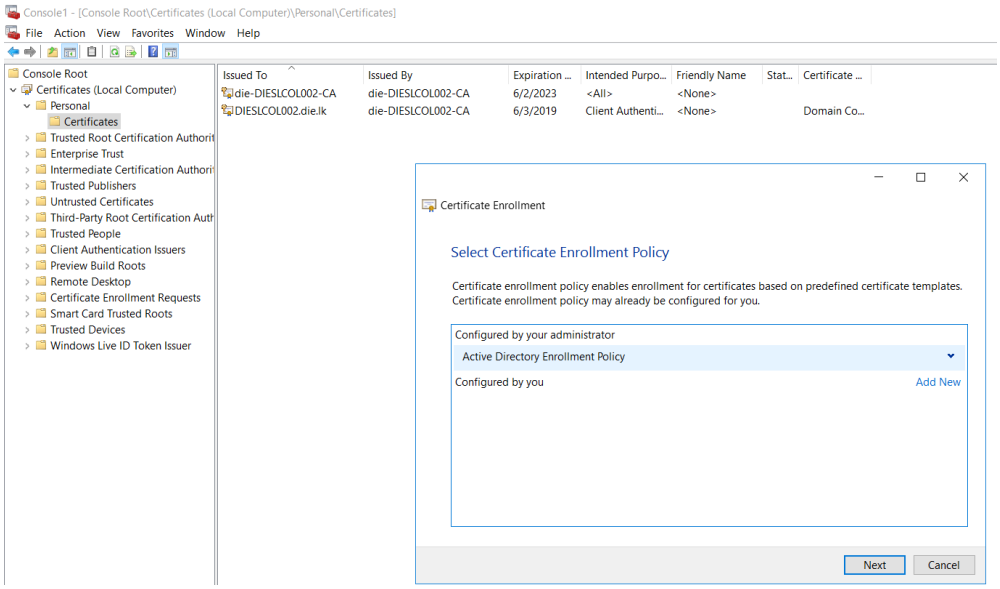
Step 9: Select the computer that manages the snap-in then click ok

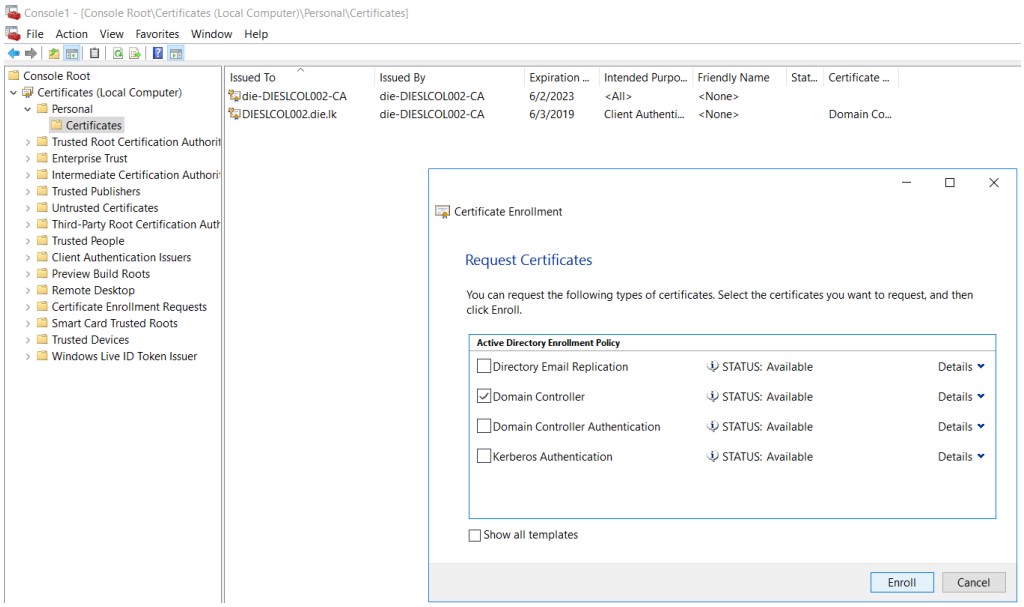




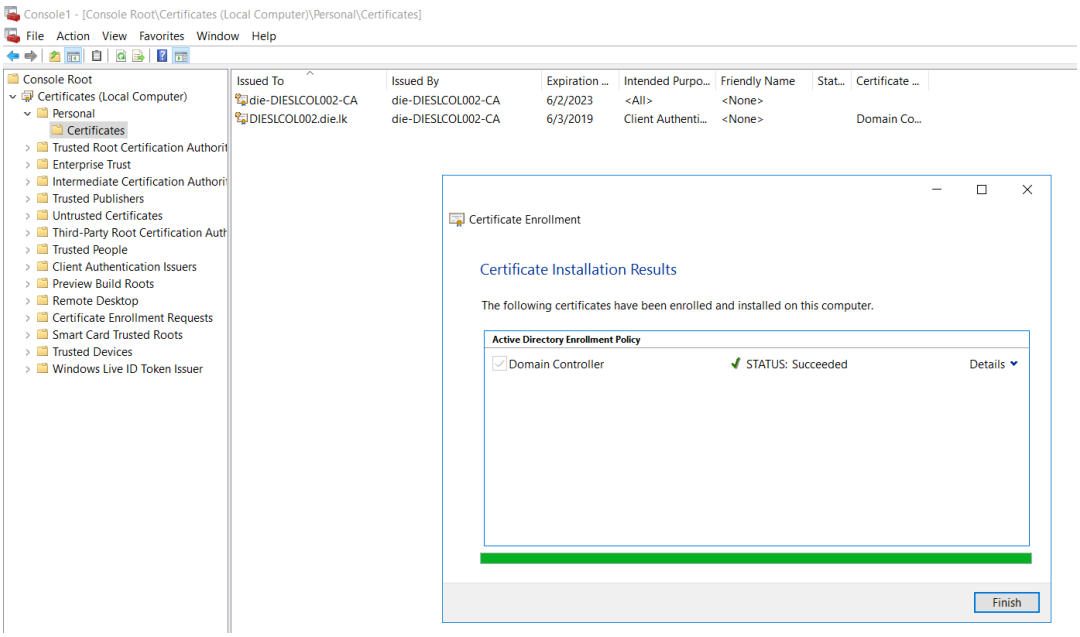


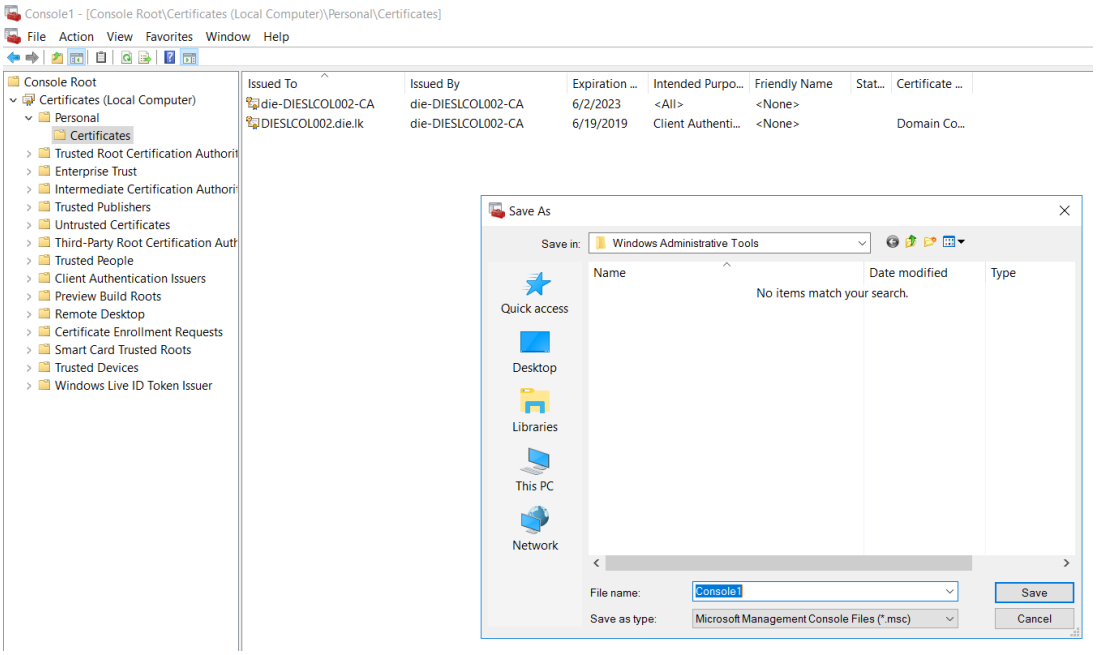
Step 10: Select Request new certificate to install





Step 11: Select Domain Controller from the certificate types





Step 12: After successful installation save the Microsoft Management Console file

3.12 Network Configuration

Master Switch Basic Configuration

COM4 - PuTTY

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname MASTER
MASTER(config)#$n #A U T H O R I Z E D  A D M I N I S T R A T O R S  O N L Y#
MASTER(config)#line console 0
MASTER(config-line)#password class
MASTER(config-line)#login
MASTER(config-line)#exit
MASTER(config)#line aux 0
MASTER(config-line)#password class
MASTER(config-line)#login
MASTER(config-line)#exit
MASTER(config)#line vty 0 15
MASTER(config-line)#password class
MASTER(config-line)#login
MASTER(config-line)#exit
MASTER(config)#enable secret class
MASTER(config)#service password-encryption
MASTER(config)#interface vlan 1
MASTER(config-if)#ip address 192.168.31.1 255.255.255.0
MASTER(config-if)#no shutdown
MASTER(config-if)#exit
MASTER(config)#service timestamps log datetime msec
MASTER(config)#interface gigabitEthernet 1/0/7
MASTER(config-if)#switchport
MASTER(config-if)#no shut
MASTER(config-if)#switchport mode access
MASTER(config-if)#switchport access vlan 150
% Access VLAN does not exist. Creating vlan 150
MASTER(config-if)#exit
MASTER(config)#interface gigabitEthernet 1/0/8
MASTER(config-if)#no switchport
MASTER(config-if)#no shut
MASTER(config-if)#ip address dhcp
MASTER(config-if)#exit
```

COM4 - PuTTY

```
MASTER(config)#spanning-tree mode rapid-pvst
MASTER(config)#spanning-tree vlan 60 root primary
MASTER(config)#spanning-tree vlan 70 root primary
MASTER(config)#spanning-tree vlan 80 root primary
MASTER(config)#spanning-tree vlan 90 root primary
MASTER(config)#spanning-tree vlan 150 root primary
MASTER(config)#spanning-tree vlan 10 root secondary
MASTER(config)#spanning-tree vlan 20 root secondary
MASTER(config)#spanning-tree vlan 30 root secondary
MASTER(config)#spanning-tree vlan 40 root secondary
MASTER(config)#spanning-tree vlan 50 root secondary
```

Slave Switch Basic Configuration

COM4 - PuTTY

```
*Dec 16 03:43:16.281: %AN-6-AN_ABORTED_BY_CONSOLE_INPUT: Autonomic disabled due t
ostname SLAVE
SLAVE(config)#$n #A U T H O R I Z E D  A D M I N I S T R A T O R S  O N L Y#
SLAVE(config)#line console 0
SLAVE(config-line)#password class
SLAVE(config-line)#login
SLAVE(config-line)#exit
SLAVE(config)#line aux 0
SLAVE(config-line)#password class
SLAVE(config-line)#login
SLAVE(config-line)#exit
SLAVE(config)#line vty 0 15
SLAVE(config-line)#password class
SLAVE(config-line)#login
SLAVE(config-line)#exit
SLAVE(config)#enable secret class
SLAVE(config)#service password-encryption
SLAVE(config)#interface vlan 1
SLAVE(config-if)#ip address 192.168.31.2 255.255.255.0
SLAVE(config-if)#no shutdown
SLAVE(config-if)#exit
SLAVE(config)#service timestamps log datetime msec
SLAVE(config)#interface gigabitEthernet 1/0/7
SLAVE(config-if)#switchport
SLAVE(config-if)#switchport mode access
SLAVE(config-if)#switchport access vlan 90
% Access VLAN does not exist. Creating vlan 90
SLAVE(config-if)#no shut
SLAVE(config-if)#exit
```

COM4 - PuTTY

```
SLAVE(config)#spanning-tree mode rapid-pvst
SLAVE(config)#spanning-tree vlan 10 root primary
SLAVE(config)#spanning-tree vlan 20 root primary
SLAVE(config)#spanning-tree vlan 30 root primary
SLAVE(config)#spanning-tree vlan 40 root primary
SLAVE(config)#spanning-tree vlan 50 root primary
SLAVE(config)#spanning-tree vlan 60 root secondary
SLAVE(config)#spanning-tree vlan 70 root secondary
SLAVE(config)#spanning-tree vlan 80 root secondary
SLAVE(config)#spanning-tree vlan 90 root secondary
SLAVE(config)#spanning-tree vlan 150 root secondary
SLAVE(config)#
*Dec 16 03:43:20.154: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
```

Master Switch Vlan Configuration

COM4 - PuTTY

```
Enter configuration commands, one per line.  End with CNTL/Z.
MASTER(config)#vtp mode server
Device mode already VTP Server for VLANS.
MASTER(config)#vtp domain mediamora
Changing VTP domain name from NULL to mediamora
MASTER(config)#vtp password class
Setting device VTP password to class
MASTER(config)#vlan 10
MASTER(config-vlan)#name Reception
MASTER(config-vlan)#vlan 20
MASTER(config-vlan)#name Administration
MASTER(config-vlan)#vlan 30
MASTER(config-vlan)#name HR
MASTER(config-vlan)#vlan 40
MASTER(config-vlan)#name Legal
MASTER(config-vlan)#vlan 50
MASTER(config-vlan)#name Finance&management
MASTER(config-vlan)#vlan 60
MASTER(config-vlan)#name IT
MASTER(config-vlan)#vlan 70
MASTER(config-vlan)#name Graphicdesigning
MASTER(config-vlan)#vlan 80
MASTER(config-vlan)#name Advertising
MASTER(config-vlan)#vlan 90
MASTER(config-vlan)#name WLAN
MASTER(config-vlan)#vlan 150
MASTER(config-vlan)#name Datacenter
MASTER(config-vlan)#exit
MASTER(config)#ip routing
MASTER(config)#interface vlan 10
MASTER(config-if)#description RECEPTION
MASTER(config-if)#ip address 192.168.1.2 255.255.255.0
MASTER(config-if)#standby 1 ip 192.168.1.1
MASTER(config-if)#standby 1 priority 150
MASTER(config-if)#standby 1 preempt
MASTER(config-if)#no shutdown
MASTER(config-if)#exit
```

COM4 - PuTTY

```
MASTER(config)#interface vlan 20
MASTER(config-if)#description ADMINISTRATION DEPARTMENT
MASTER(config-if)#ip address 192.168.2.2 255.255.255.0
MASTER(config-if)#standby 2 ip 192.168.2.1
MASTER(config-if)#standby 2 priority 150
MASTER(config-if)#standby 2 preempt
MASTER(config-if)#no shutdown
MASTER(config-if)#exit
MASTER(config)#interface vlan 30
MASTER(config-if)#description HUMAN RESOURCE MANAGMENT
MASTER(config-if)#ip address 192.168.3.2 255.255.255.0
MASTER(config-if)#standby 3 ip 192.168.3.1
MASTER(config-if)#standby 3 priority 150
MASTER(config-if)#standby 3 preempt
MASTER(config-if)#no shutdown
MASTER(config-if)#exit
MASTER(config)#interface vlan 40
MASTER(config-if)#description LEGAL DEPARTMENT
MASTER(config-if)#ip address 192.168.4.2 255.255.255.0
MASTER(config-if)#standby 4 ip 192.168.4.1
MASTER(config-if)#standby 4 priority 150
MASTER(config-if)#standby 4 preempt
MASTER(config-if)#no shutdown
MASTER(config-if)#exit
MASTER(config)#interface vlan 50
MASTER(config-if)#description FINANCE AND MANAGMENT DEPARTMENT
MASTER(config-if)#ip address 192.168.5.2 255.255.255.0
MASTER(config-if)#standby 5 ip 192.168.5.1
MASTER(config-if)#standby 5 priority 150
MASTER(config-if)#standby 5 preempt
MASTER(config-if)#no shutdown
MASTER(config-if)#exit
```

COM4 - PuTTY

```
MASTER(config)#interface vlan 60
MASTER(config-if)#description IT DEPARTMENT
MASTER(config-if)#ip address 192.168.6.2 255.255.255.0
MASTER(config-if)#standby 6 ip 192.168.6.1
MASTER(config-if)#standby 6 priority 150
MASTER(config-if)#standby 6 preempt
MASTER(config-if)#no shutdown
MASTER(config-if)#exit
MASTER(config)#interface vlan 70
MASTER(config-if)#description GRAPHIC DESIGNING DEPARTMENT
MASTER(config-if)#ip address 192.168.7.2 255.255.255.0
MASTER(config-if)#standby 7 ip 192.168.7.1
MASTER(config-if)#standby 7 priority 150
MASTER(config-if)#standby 7 preempt
MASTER(config-if)#no shutdown
MASTER(config-if)#exit
MASTER(config)#interface vlan 80
MASTER(config-if)#description ADVERTISING DEPARTMENT
MASTER(config-if)#ip address 192.168.8.2 255.255.255.0
MASTER(config-if)#standby 8 ip 192.168.8.1
MASTER(config-if)#standby 8 priority 150
MASTER(config-if)#standby 8 preempt
MASTER(config-if)#no shutdown
MASTER(config-if)#exit
MASTER(config)#interface vlan 90
MASTER(config-if)#description WIRELESS USERS
MASTER(config-if)#ip address 192.168.9.2 255.255.255.0
MASTER(config-if)#standby 9 ip 192.168.9.1
MASTER(config-if)#standby 9 priority 150
MASTER(config-if)#standby 9 preempt
MASTER(config-if)#no shutdown
MASTER(config-if)#exit
```

```
MASTER(config)#interface vlan 150
MASTER(config-if)#description DATA CENTER
MASTER(config-if)#ip address 192.168.15.2 255.255.255.0
MASTER(config-if)#standby 15 ip 192.168.15.1
MASTER(config-if)#standby 15 priority 150
MASTER(config-if)#standby 15 preempt
MASTER(config-if)#no shutdown
MASTER(config-if)#exit
*Dec 15 21:14:45.444: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to mediamora.
*Dec 15 21:14:47.329: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
*Dec 15 21:14:47.382: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to down
*Dec 15 21:14:47.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to down
*Dec 15 21:14:47.438: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to down
*Dec 15 21:14:47.745: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to down
*Dec 15 21:14:47.765: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan60, changed state to down
*Dec 15 21:14:48.283: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan70, changed state to down
*Dec 15 21:14:48.808: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan80, changed state to down
*Dec 15 21:14:48.830: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan90, changed state to down
*Dec 15 21:14:49.345: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan150, changed state to down
```

Slave Switch Vlan Configuration

COM4 - PuTTY

```
SLAVE(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SLAVE(config)#vtp domain mediamora
Changing VTP domain name from NULL to mediamora
SLAVE(config)#vtp password class
Setting device VTP password to class
SLAVE(config)#ip routing
SLAVE(config)#interface vlan 10
SLAVE(config-if)#description RECEPTION
SLAVE(config-if)#ip address 192.168.1.3 255.255.255.0
SLAVE(config-if)#standby 1 ip 192.168.1.1
SLAVE(config-if)#no shutdown
SLAVE(config-if)#exit
SLAVE(config)#interface vlan 20
SLAVE(config-if)#description ADMINISTRATION DEPARTMENT
SLAVE(config-if)#ip address 192.168.2.3 255.255.255.0
SLAVE(config-if)#standby 2 ip 192.168.2.1
SLAVE(config-if)#no shutdown
SLAVE(config-if)#exit
SLAVE(config)#interface vlan 30
SLAVE(config-if)#description HUMAN RESOURCE MANAGMENT
SLAVE(config-if)#ip address 192.168.3.3 255.255.255.0
SLAVE(config-if)#standby 3 ip 192.168.3.1
SLAVE(config-if)#no shutdown
SLAVE(config-if)#exit
SLAVE(config)#interface vlan 40
SLAVE(config-if)#description LEGAL DEPARTMENT
SLAVE(config-if)#ip address 192.168.4.3 255.255.255.0
SLAVE(config-if)#standby 4 ip 192.168.4.1
SLAVE(config-if)#no shutdown
SLAVE(config-if)#exit
SLAVE(config)#interface vlan 50
SLAVE(config-if)#description FINANCE AND MANAGMENT DEPARTMENT
SLAVE(config-if)#ip address 192.168.5.3 255.255.255.0
SLAVE(config-if)#standby 5 ip 192.168.5.1
SLAVE(config-if)#no shutdown
SLAVE(config-if)#exit
```

COM4 - PuTTY

```
SLAVE(config)#interface vlan 60
SLAVE(config-if)#description IT DEPARTMENT
SLAVE(config-if)#ip address 192.168.6.3 255.255.255.0
SLAVE(config-if)#standby 6 ip 192.168.6.1
SLAVE(config-if)#no shutdown
SLAVE(config-if)#exit
SLAVE(config)#interface vlan 70
SLAVE(config-if)#description GRAPHIC DESIGNING DEPARTMENT
SLAVE(config-if)#ip address 192.168.7.3 255.255.255.0
SLAVE(config-if)#standby 7 ip 192.168.7.1
SLAVE(config-if)#no shutdown
SLAVE(config-if)#exit
SLAVE(config)#interface vlan 80
SLAVE(config-if)#description ADVERTISING DEPARTMENT
SLAVE(config-if)#ip address 192.168.8.3 255.255.255.0
SLAVE(config-if)#standby 8 ip 192.168.8.1
SLAVE(config-if)#no shutdown
SLAVE(config-if)#exit
SLAVE(config)#interface vlan 90
SLAVE(config-if)#description WIRELESS USERS
SLAVE(config-if)#ip address 192.168.9.3 255.255.255.0
SLAVE(config-if)#standby 9 ip 192.168.9.1
SLAVE(config-if)#no shutdown
SLAVE(config-if)#exit
SLAVE(config)#interface vlan 150
SLAVE(config-if)#description DATA CENTER
SLAVE(config-if)#ip address 192.168.15.3 255.255.255.0
SLAVE(config-if)#standby 15 ip 192.168.15.1
SLAVE(config-if)#no shutdown
SLAVE(config-if)#exit
*Dec 16 03:48:13.299: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to mediamora.
*Dec 16 03:48:14.498: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
*Dec 16 03:48:14.527: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to down
*Dec 16 03:48:14.549: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to down
*Dec 16 03:48:14.596: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to down
*Dec 16 03:48:14.728: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to down
*Dec 16 03:48:14.928: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan60, changed state to down
```

Master Switch Port-Channel Configuration

COM4 - PuTTY

```
MASTER(config)#interface range gigabitEthernet 1/0/9-10
MASTER(config-if-range)#switchport mode trunk
MASTER(config-if-range)#switchport trunk allowed vlan add 10
MASTER(config-if-range)#switchport trunk allowed vlan add 20
MASTER(config-if-range)#switchport trunk allowed vlan add 30
MASTER(config-if-range)#switchport trunk allowed vlan add 40
MASTER(config-if-range)#switchport trunk allowed vlan add 50
MASTER(config-if-range)#channel-group 40 mode auto
Creating a port-channel interface Port-channel 40

MASTER(config-if-range)#no shutdown
MASTER(config-if-range)#exit
MASTER(config)#interface range gigabitEthernet 1/0/11-12
MASTER(config-if-range)#switchport mode trunk
MASTER(config-if-range)#switchport trunk allowed vlan add 60
MASTER(config-if-range)#switchport trunk allowed vlan add 70
MASTER(config-if-range)#switchport trunk allowed vlan add 80
MASTER(config-if-range)#switchport trunk allowed vlan add 150
MASTER(config-if-range)#channel-group 41 mode auto
Creating a port-channel interface Port-channel 41

MASTER(config-if-range)#no shutdown
MASTER(config-if-range)#exit
MASTER(config)#interface range gigabitEthernet 1/0/1-2
MASTER(config-if-range)#switchport mode trunk
MASTER(config-if-range)#switchport trunk allowed vlan add 10
MASTER(config-if-range)#switchport trunk allowed vlan add 20
MASTER(config-if-range)#channel-group 1 mode auto
Creating a port-channel interface Port-channel 1
```

COM4 - PuTTY

```
MASTER(config-if-range)#no shutdown
MASTER(config-if-range)#exit
MASTER(config)#interface range gigabitEthernet 1/0/3-4
MASTER(config-if-range)#switchport mode trunk
MASTER(config-if-range)#switchport trunk allowed vlan add 30
MASTER(config-if-range)#switchport trunk allowed vlan add 40
MASTER(config-if-range)#switchport trunk allowed vlan add 50
MASTER(config-if-range)#channel-group 2 mode auto
Creating a port-channel interface Port-channel 2

MASTER(config-if-range)#no shutdown
MASTER(config-if-range)#exit
MASTER(config)#interface range gigabitEthernet 1/0/5-6
MASTER(config-if-range)#switchport mode trunk
MASTER(config-if-range)#switchport trunk allowed vlan add 60
MASTER(config-if-range)#switchport trunk allowed vlan add 70
MASTER(config-if-range)#switchport trunk allowed vlan add 80
MASTER(config-if-range)#channel-group 3 mode auto
Creating a port-channel interface Port-channel 3

MASTER(config-if-range)#no shutdown
MASTER(config-if-range)#exit
```

Slave Switch Port-Channel Configuration

COM4 - PuTTY

```
SLAVE(config)#interface range gigabitEthernet 1/0/9-10
SLAVE(config-if-range)#switchport mode trunk
SLAVE(config-if-range)#switchport trunk allowed vlan add 10
SLAVE(config-if-range)#switchport trunk allowed vlan add 20
SLAVE(config-if-range)#switchport trunk allowed vlan add 30
SLAVE(config-if-range)#switchport trunk allowed vlan add 40
SLAVE(config-if-range)#switchport trunk allowed vlan add 50
SLAVE(config-if-range)#channel-group 40 mode desirable
Creating a port-channel interface Port-channel 40

SLAVE(config-if-range)#no shutdown
SLAVE(config-if-range)#exit
SLAVE(config)#interface range gigabitEthernet 1/0/11-12
SLAVE(config-if-range)#switchport mode trunk
SLAVE(config-if-range)#switchport trunk allowed vlan add 60
SLAVE(config-if-range)#switchport trunk allowed vlan add 70
SLAVE(config-if-range)#switchport trunk allowed vlan add 80
SLAVE(config-if-range)#switchport trunk allowed vlan add 150
SLAVE(config-if-range)#channel-group 41 mode desirable
Creating a port-channel interface Port-channel 41

SLAVE(config-if-range)#no shutdown
SLAVE(config-if-range)#exit
SLAVE(config)#interface range gigabitEthernet 1/0/1-2
SLAVE(config-if-range)#switchport mode trunk
SLAVE(config-if-range)#switchport trunk allowed vlan add 10
SLAVE(config-if-range)#switchport trunk allowed vlan add 20
SLAVE(config-if-range)#channel-group 4 mode auto
Creating a port-channel interface Port-channel 4

SLAVE(config-if-range)#no shutdown
SLAVE(config-if-range)#exit
```

COM4 - PuTTY

```
SLAVE(config)#interface range gigabitEthernet 1/0/3-4
SLAVE(config-if-range)#switchport mode trunk
SLAVE(config-if-range)#switchport trunk allowed vlan add 30
SLAVE(config-if-range)#switchport trunk allowed vlan add 40
SLAVE(config-if-range)#switchport trunk allowed vlan add 50
SLAVE(config-if-range)#channel-group 5 mode auto
Creating a port-channel interface Port-channel 5

SLAVE(config-if-range)#no shutdown
SLAVE(config-if-range)#exit
SLAVE(config)#interface range gigabitEthernet 1/0/5-6
SLAVE(config-if-range)#switchport mode trunk
SLAVE(config-if-range)#switchport trunk allowed vlan add 60
SLAVE(config-if-range)#switchport trunk allowed vlan add 70
SLAVE(config-if-range)#switchport trunk allowed vlan add 80
SLAVE(config-if-range)#channel-group 6 mode auto
Creating a port-channel interface Port-channel 6

SLAVE(config-if-range)#no shutdown
SLAVE(config-if-range)#exit
```

Master Switch Routing Configuration (OSPF)

COM4 - PuTTY

```
*Dec 15 21:24:29.820: %NGWC_USB_CONSOLE-6-USB_REMOVE: Switch
MASTER(config)#router ospf 10
MASTER(config-router)#router-id 1.1.1.1
MASTER(config-router)#network 192.168.1.0 0.0.0.255 area 0
MASTER(config-router)#network 192.168.2.0 0.0.0.255 area 0
MASTER(config-router)#network 192.168.3.0 0.0.0.255 area 0
MASTER(config-router)#network 192.168.4.0 0.0.0.255 area 0
MASTER(config-router)#network 192.168.5.0 0.0.0.255 area 0
MASTER(config-router)#network 192.168.6.0 0.0.0.255 area 0
MASTER(config-router)#network 192.168.7.0 0.0.0.255 area 0
MASTER(config-router)#network 192.168.8.0 0.0.0.255 area 0
MASTER(config-router)#network 192.168.9.0 0.0.0.255 area 0
MASTER(config-router)#network 192.168.15.0 0.0.0.255 area 0
MASTER(config-router)#network 192.168.19.0 0.0.0.255 area 0
MASTER(config-router)#exit
```

Slave Switch Routing Configuration (OSPF)

COM4 - PuTTY

```
SLAVE(config)#router ospf 10
SLAVE(config-router)#router-id 2.2.2.2
SLAVE(config-router)#network 192.168.1.0 0.0.0.255 area 0
SLAVE(config-router)#network 192.168.2.0 0.0.0.255 area 0
SLAVE(config-router)#network 192.168.3.0 0.0.0.255 area 0
SLAVE(config-router)#network 192.168.4.0 0.0.0.255 area 0
SLAVE(config-router)#network 192.168.5.0 0.0.0.255 area 0
SLAVE(config-router)#network 192.168.6.0 0.0.0.255 area 0
SLAVE(config-router)#network 192.168.7.0 0.0.0.255 area 0
SLAVE(config-router)#network 192.168.8.0 0.0.0.255 area 0
SLAVE(config-router)#network 192.168.9.0 0.0.0.255 area 0
SLAVE(config-router)#network 192.168.15.0 0.0.0.255 area 0
SLAVE(config-router)#network 192.168.19.0 0.0.0.255 area 0
SLAVE(config-router)#exit
```

Master Switch SNMP Configuration

```
MASTER(config)#ip access-list standard SNMP_PRIV
MASTER(config-std-nacl)#permit 192.168.200.0 0.0.0.255
MASTER(config-std-nacl)#exit
MASTER(config)#snmp-server view mediamora 1.3.6.1.4.1.9 included
MASTER(config)#$ group ADMINS v3 priv read 1.3.6.1.4.1.9 access SNMP_PRIV
```

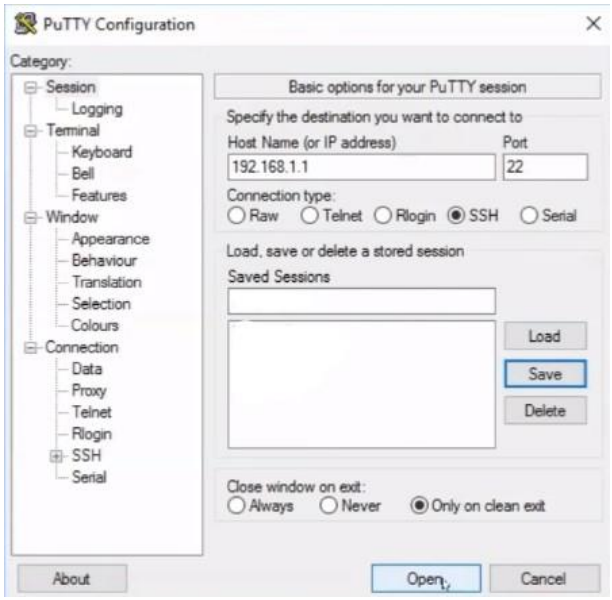
```
snmp-server group ADMINS v3 priv read 1.3.6.1.4.1.9 access SNMP_PRIV
snmp-server view mediamora cisco included
```

```
MASTER#show snmp chassis
FDO2104E0M8
MASTER#show snmp engineID
Local SNMP engineID: 8000000903002C5A0FE2E480
Remote Engine ID          IP-addr    Port
MASTER#show snmp group
groupname: ADMINS                           security model:v3 priv
contextname: <no context specified>         storage-type: nonvolatile
readview : 1.3.6.1.4.1.9                    writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active      access-list: SNMP_PRIV

MASTER#show snmp user

User name: sudeera
Engine ID: 8000000903002C5A0FE2E480
storage-type: nonvolatile        active access-list: SNMP_PRIV
Authentication Protocol: SHA
Privacy Protocol: 3DES
Group-name: ADMINS
```

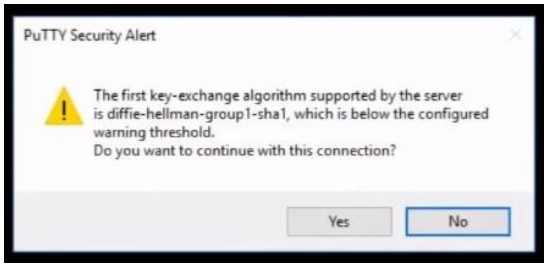
SNMP implemented Working Successfully

4. Evaluation

4.1 Testing SSH on a switch

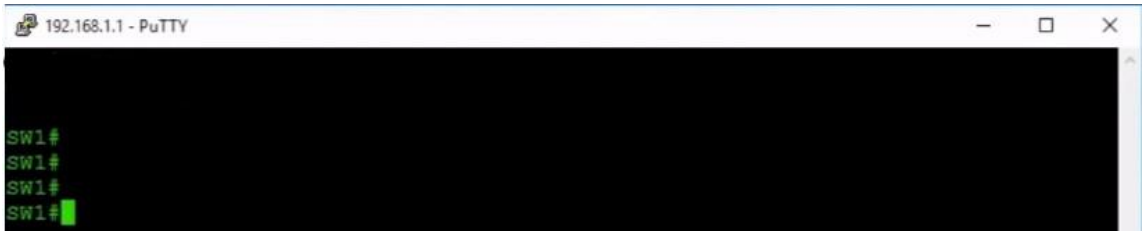


We are using PUTTY to check whether SSH is working or not. In the above scenario enter the SVI interface IP address change the port number to 22 and click open



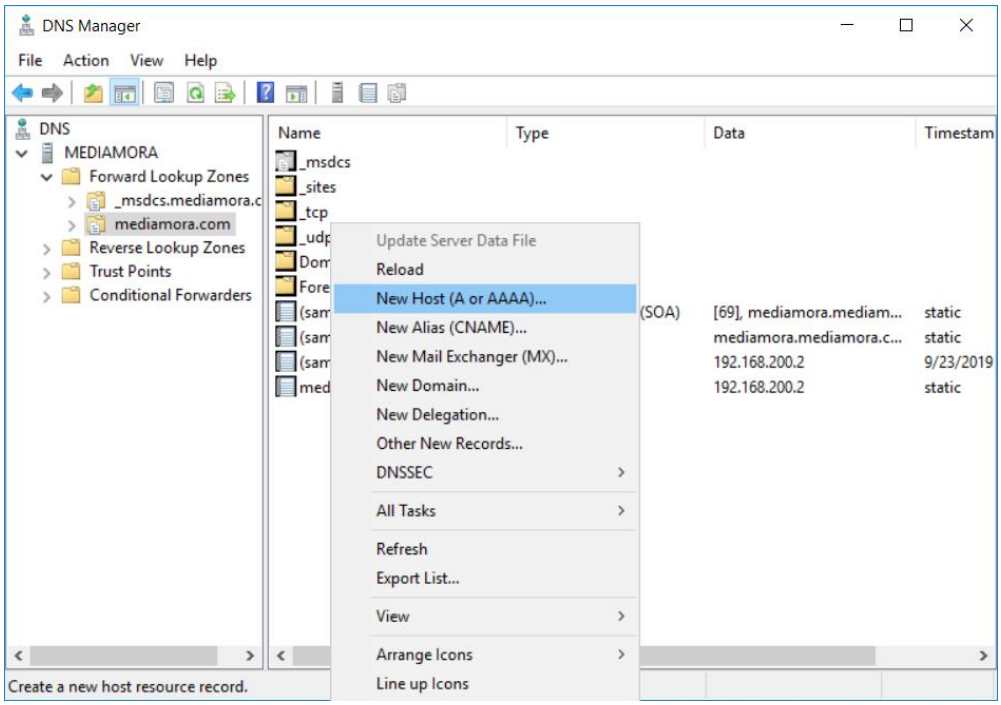
Above diagrams are about a warning of a key algorithm. Click yes in both instances.

Enter the username as we have configured on the switch

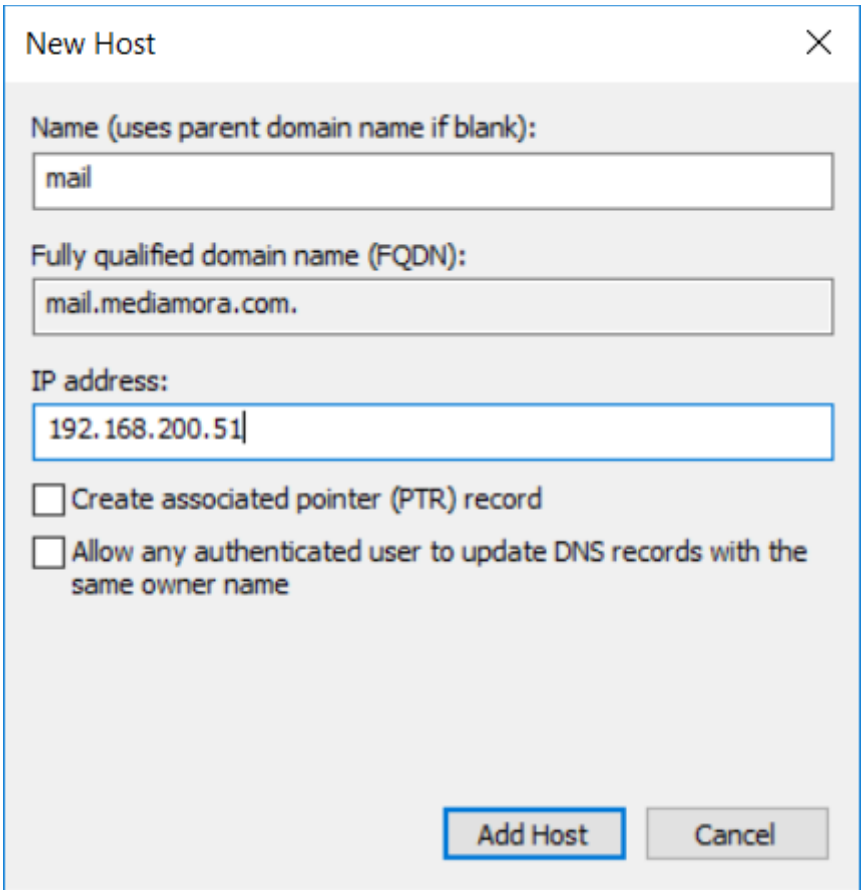


We have successfully logged in to the SW1

4.2 Testing local DNS resolver



Go to the DNS manager click forward lookup zones right click new host



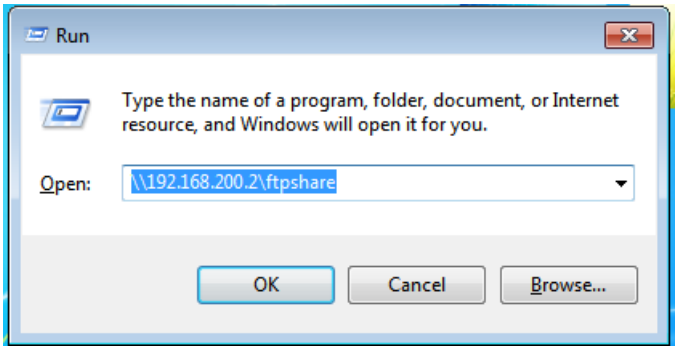
Enter the information above and click add host

```
C:\Users\Administrator>ping mail.mediamora.com

Pinging mail.mediamora.com [192.168.200.2] with 32 bytes of data:
Reply from 192.168.200.2: bytes=32 time<1ms TTL=128
Reply from 192.168.200.2: bytes=32 time<1ms TTL=128
Reply from 192.168.200.2: bytes=32 time<1ms TTL=128
Reply from 192.168.200.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.200.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

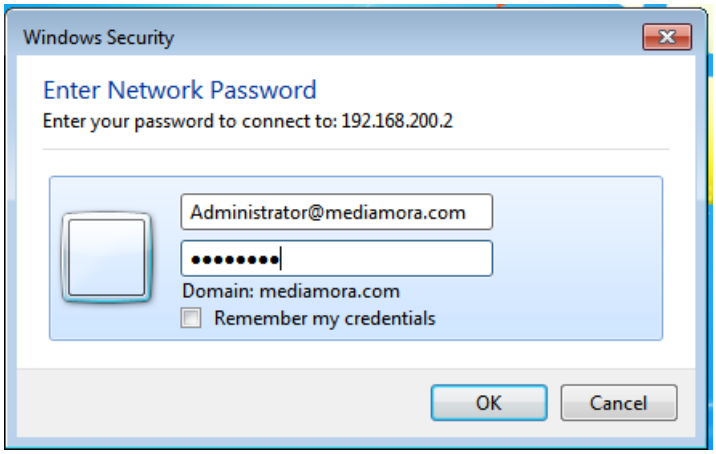
```
C:\Users\Administrator>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  ::1

> mail.mediamora.com
Server:  UnKnown
Address:  ::1

Name:    mail.mediamora.com
Address:  192.168.200.51
```

Go to the command prompt enter nslookp command. Then enter the FQDN you have entered in the previous step. As you can see the name is successfully translated to the IP address

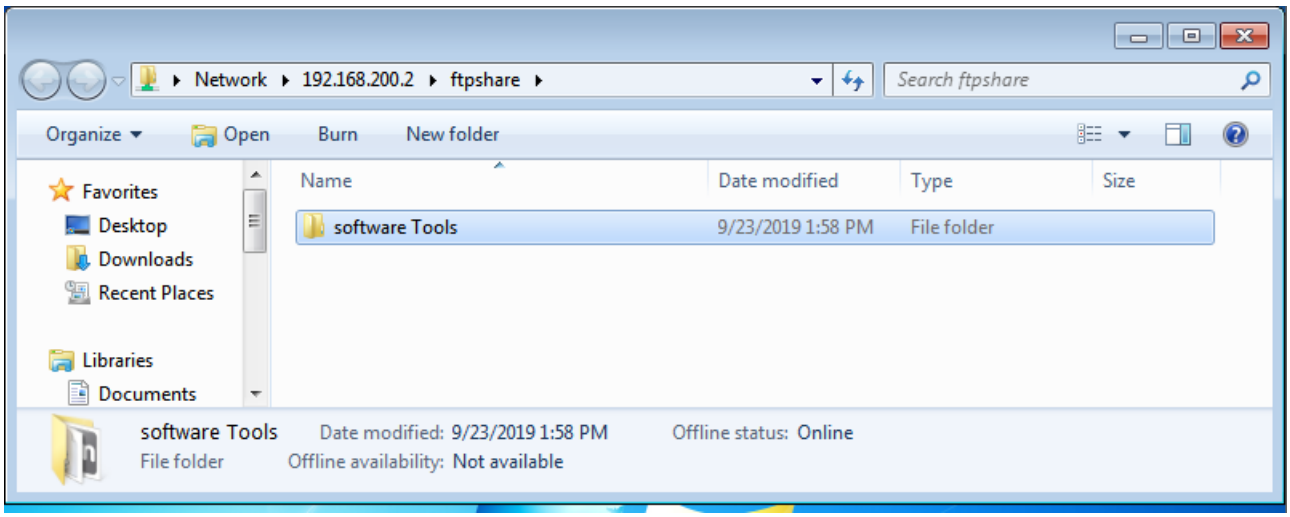
4.3 Testing SMB server access



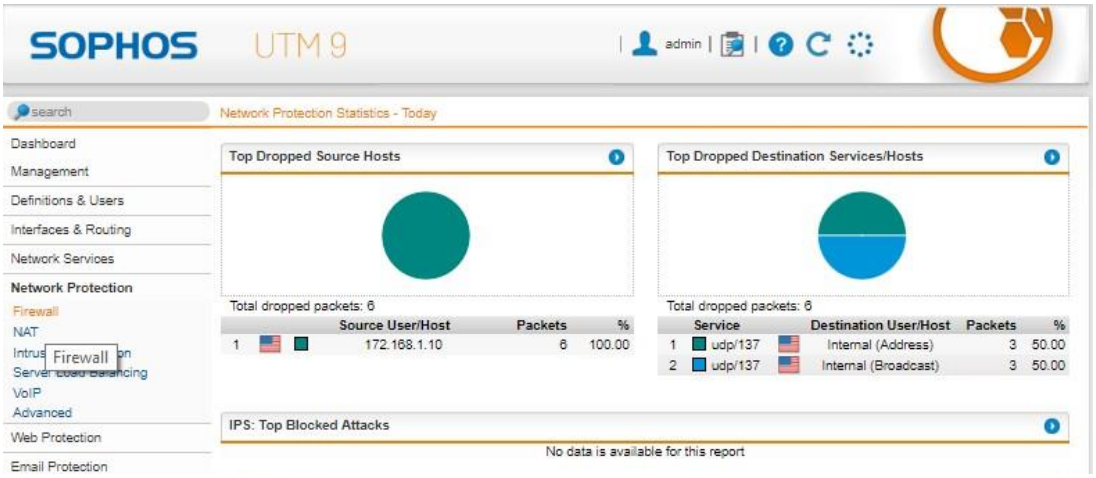
Go to the web browser and type SMB server IP address



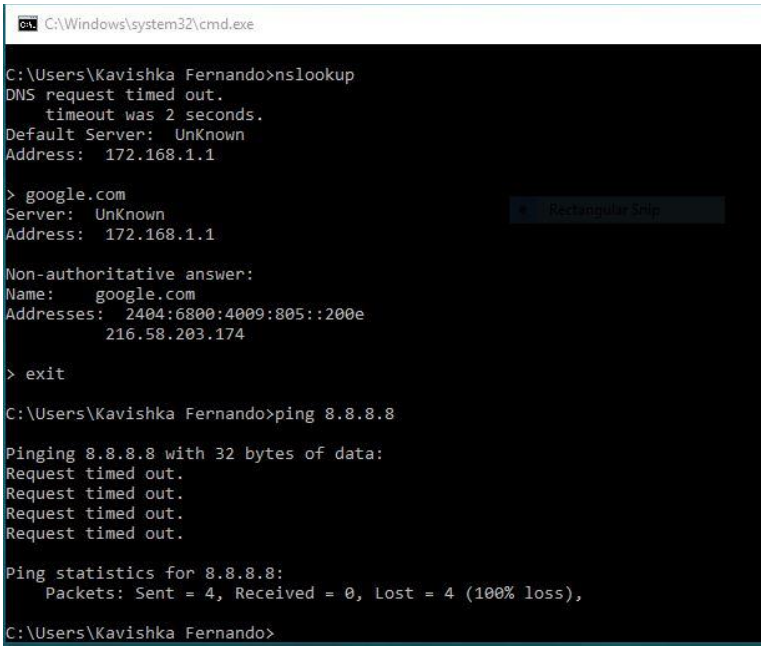
Enter the username and the password



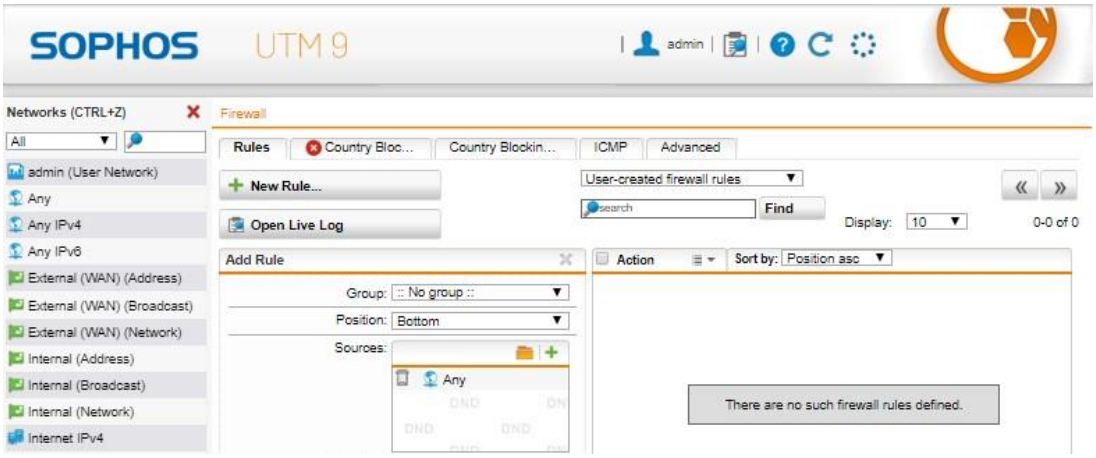
4.4 Testing the firewall and blocking web sites



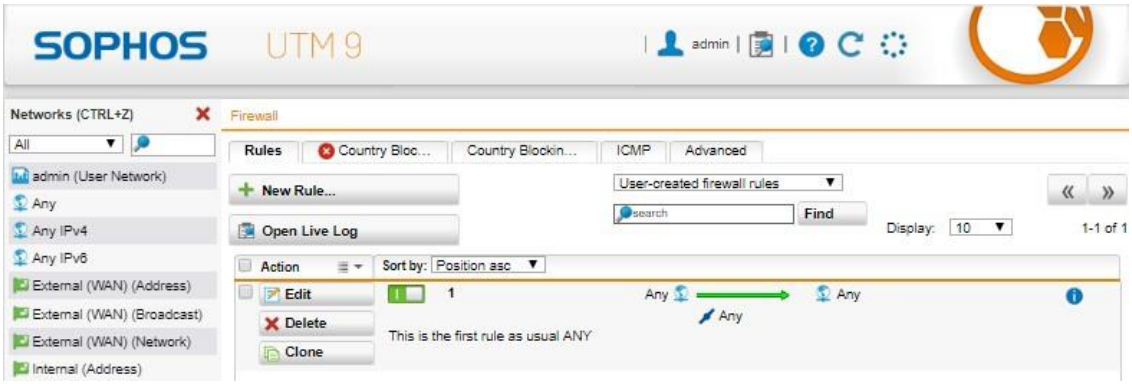
Go to firewall under the network protection. We haven't configured any rules yet



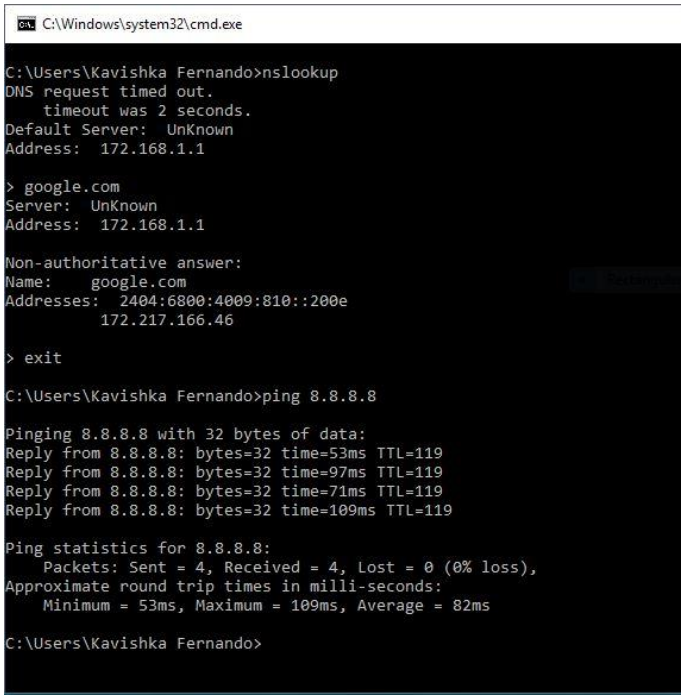
As you can see the ping to the public google DNS server is failing



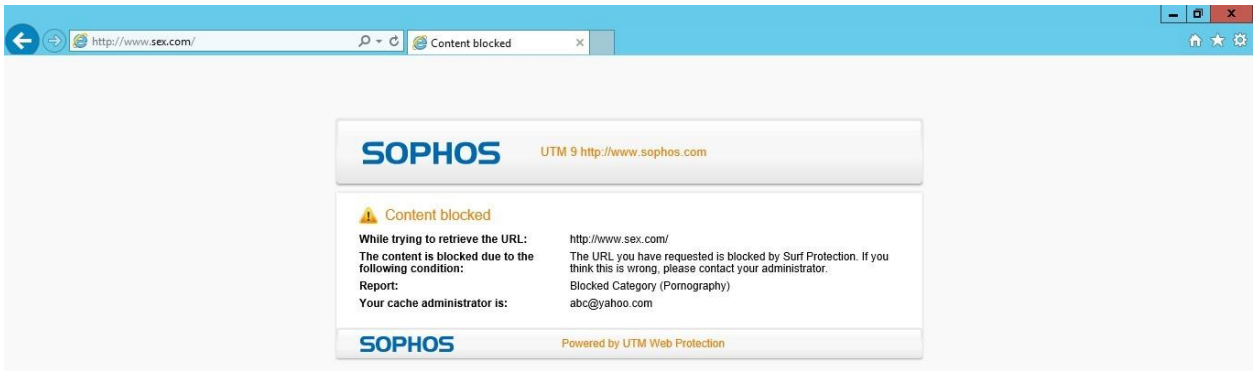
Click firewall and then click new rule to add rules



As you can see we have created any to any rule for internet access to the internal users



Now the ping is working because we have created the global rule



Here is a snapshot of a blocked web site

4.5 Network Configuration Check

Master Switch Spanning-Tree Summary

```
MASTER#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001, VLAN0060, VLAN0070, VLAN0080, VLAN0090, VLAN0150
EtherChannel misconfig guard is enabled
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN0001                    0         0        0          2          2
VLAN0010                    1         0        0          1          2
VLAN0020                    1         0        0          1          2
VLAN0030                    1         0        0          1          2
VLAN0040                    1         0        0          1          2
VLAN0050                    1         0        0          1          2
VLAN0060                    0         0        0          2          2
VLAN0070                    0         0        0          2          2

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN0080                    0         0        0          2          2
VLAN0090                    0         0        0          2          2
VLAN0150                    0         0        0          2          2
-------------------- -------- --------- -------- ---------- ----------
11 vlans                    5         0        0         17         22
```

Slave Switch Spanning-Tree Summary

```
SLAVE#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0010, VLAN0020, VLAN0030, VLAN0040, VLAN0050
EtherChannel misconfig guard is enabled
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN0001                    1         0        0          1          2
VLAN0010                    0         0        0          2          2
VLAN0020                    0         0        0          2          2
VLAN0030                    0         0        0          2          2
VLAN0040                    0         0        0          2          2
VLAN0050                    0         0        0          2          2
VLAN0060                    1         0        0          1          2
VLAN0070                    1         0        0          1          2

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN0080                    1         0        0          1          2
VLAN0090                    1         0        0          1          2
VLAN0150                    1         0        0          1          2
-------------------- -------- --------- -------- ---------- ----------
11 vlans                    6         0        0         16         22
```

Master Switch Etherchannel Summary

```
MASTER#show etherchannel 40 port-channel
               Port-channels in the group:
               ---------------------------

Port-channel: Po40
------------

Age of the Port-channel   = 0d:00h:39m:02s
Logical slot/port   = 12/40          Number of ports = 2
GC                  = 0x00280001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   PAgP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi1/0/9  Automatic-Sl       0
  0     00     Gi1/0/10 Automatic-Sl       0

Time since last port bundled:    0d:00h:24m:58s    Gi1/0/10
```

```
MASTER#show etherchannel 41 port-channel
               Port-channels in the group:
               ---------------------------

Port-channel: Po41
------------

Age of the Port-channel   = 0d:00h:39m:45s
Logical slot/port   = 12/41          Number of ports = 2
GC                  = 0x00290001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   PAgP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi1/0/11 Automatic-Sl       0
  0     00     Gi1/0/12 Automatic-Sl       0

Time since last port bundled:    0d:00h:20m:04s    Gi1/0/12
```

Slave Switch Etherchannel Summary

```
SLAVE#show etherchannel 40 port-channel
                Port-channels in the group:
                ---------------------------

Port-channel: Po40
------------

Age of the Port-channel   = 0d:00h:38m:10s
Logical slot/port   = 12/40          Number of ports = 2
GC                  = 0x00280001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   PAgP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi1/0/9  Desirable-Sl       0
  0     00     Gi1/0/10 Desirable-Sl       0

Time since last port bundled:    0d:00h:26m:41s    Gi1/0/10
```

```
SLAVE#show etherchannel 41 port-channel
                Port-channels in the group:
                ---------------------------

Port-channel: Po41
------------

Age of the Port-channel   = 0d:00h:38m:36s
Logical slot/port   = 12/41          Number of ports = 2
GC                  = 0x00290001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   PAgP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi1/0/11 Desirable-Sl       0
  0     00     Gi1/0/12 Desirable-Sl       0

Time since last port bundled:    0d:00h:21m:30s    Gi1/0/12
```

Master Switch and Slave Switch Vlan Summary

```
MASTER#show vlan summary
Number of existing VLANs              : 15
 Number of existing VTP VLANs         : 15
 Number of existing extended VLANS    : 0

MASTER#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                Gi1/0/19, Gi1/0/20, Gi1/0/21
                                                Gi1/0/22, Gi1/0/23, Gi1/0/24
                                                Gi1/1/1, Gi1/1/2, Gi1/1/3
                                                Gi1/1/4
10   Reception                        active
20   Administration                   active
30   HR                               active
40   Legal                            active
50   Finance&management               active
60   IT                               active
70   Graphicdesigning                 active
80   Advertising                      active
90   WLAN                             active
150  Datacenter                       active    Gi1/0/7
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

```
SLAVE#show vlan summary
Number of existing VLANs              : 15
 Number of existing VTP VLANs         : 15
 Number of existing extended VLANS    : 0

SLAVE#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/8, Gi1/0/13, Gi1/0/14
                                                Gi1/0/15, Gi1/0/16, Gi1/0/17
                                                Gi1/0/18, Gi1/0/19, Gi1/0/20
                                                Gi1/0/21, Gi1/0/22, Gi1/0/23
                                                Gi1/0/24, Gi1/1/1, Gi1/1/2
                                                Gi1/1/3, Gi1/1/4
10   Reception                        active
20   Administration                   active
30   HR                               active
40   Legal                            active
50   Finance&management               active
60   IT                               active
70   Graphicdesigning                 active
80   Advertising                      active
90   WLAN                             active    Gi1/0/7
150  Datacenter                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Master Switch and Slave Switch VTP Summary

```
MASTER#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : mediamora
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 2c5a.0fe2.e480
Configuration last modified by 0.0.0.0 at 12-15-19 21:14:46
Local updater ID is 192.168.31.1 on interface Vl1 (lowest numbered VLAN interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 15
Configuration Revision          : 11
MD5 digest                      : 0x6A 0x20 0xEF 0x15 0x7D 0x3C 0x35 0xBD
                                  0x0B 0x12 0x59 0x2D 0x4D 0xAF 0xBB 0x3E

MASTER#sh
MASTER#show vtp pas
MASTER#show vtp password
VTP Password: class
```

```
SLAVE#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : mediamora
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 2c5a.0ffb.2a80
Configuration last modified by 0.0.0.0 at 12-15-19 21:14:46

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 15
Configuration Revision          : 11
MD5 digest                      : 0x6A 0x20 0xEF 0x15 0x7D 0x3C 0x35 0xBD
                                  0x0B 0x12 0x59 0x2D 0x4D 0xAF 0xBB 0x3E

SLAVE#show vtp password
VTP Password: class
```

Master Switch and Slave Switch HSRP Summary

```
MASTER#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        1    150 P Active  local           192.168.1.3     192.168.1.1
Vl20        2    150 P Active  local           192.168.2.3     192.168.2.1
Vl30        3    150 P Active  local           192.168.3.3     192.168.3.1
Vl40        4    150 P Active  local           192.168.4.3     192.168.4.1
Vl50        5    150 P Active  local           192.168.5.3     192.168.5.1
Vl60        6    150 P Active  local           192.168.6.3     192.168.6.1
Vl70        7    150 P Active  local           192.168.7.3     192.168.7.1
Vl80        8    150 P Active  local           192.168.8.3     192.168.8.1
Vl90        9    150 P Active  local           192.168.9.3     192.168.9.1
Vl150       15   150 P Active  local           192.168.15.3    192.168.15.1
```

```
SLAVE#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        1    100   Standby 192.168.1.2     local           192.168.1.1
Vl20        2    100   Standby 192.168.2.2     local           192.168.2.1
Vl30        3    100   Standby 192.168.3.2     local           192.168.3.1
Vl40        4    100   Standby 192.168.4.2     local           192.168.4.1
Vl50        5    100   Standby 192.168.5.2     local           192.168.5.1
Vl60        6    100   Standby 192.168.6.2     local           192.168.6.1
Vl70        7    100   Standby 192.168.7.2     local           192.168.7.1
Vl80        8    100   Standby 192.168.8.2     local           192.168.8.1
Vl90        9    100   Standby 192.168.9.2     local           192.168.9.1
Vl150       15   100   Standby 192.168.15.2    local           192.168.15.1
```

Master Switch and Slave Switch OSPF Summary

```
MASTER#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.2.0 0.0.0.255 area 0
    192.168.3.0 0.0.0.255 area 0
    192.168.4.0 0.0.0.255 area 0
    192.168.5.0 0.0.0.255 area 0
    192.168.6.0 0.0.0.255 area 0
    192.168.7.0 0.0.0.255 area 0
    192.168.8.0 0.0.0.255 area 0
    192.168.9.0 0.0.0.255 area 0
    192.168.15.0 0.0.0.255 area 0
    192.168.19.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)
```

```
SLAVE#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.2.0 0.0.0.255 area 0
    192.168.3.0 0.0.0.255 area 0
    192.168.4.0 0.0.0.255 area 0
    192.168.5.0 0.0.0.255 area 0
    192.168.6.0 0.0.0.255 area 0
    192.168.7.0 0.0.0.255 area 0
    192.168.8.0 0.0.0.255 area 0
    192.168.9.0 0.0.0.255 area 0
    192.168.15.0 0.0.0.255 area 0
    192.168.19.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)
```

HSRP Summary

```
R1#show standby
FastEthernet0/1 - Group 0 (version 2)
  State is Standby
    3 state changes, last state change 00:00:24
  Virtual IP address is 192.168.10.1
  Active virtual MAC address is 0000.0c9f.f000
    Local virtual MAC address is 0000.0c9f.f000 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.736 secs
  Preemption enabled
  Active router is 192.168.10.3, priority 100 (expires in 11.184 sec)
    MAC address is ca02.3308.0006
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Fa0/1-0" (default)
```

```
R2#show standby
FastEthernet0/1 - Group 0 (version 2)
  State is Active
    2 state changes, last state change 00:01:22
  Virtual IP address is 192.168.10.1
  Active virtual MAC address is 0000.0c9f.f000
    Local virtual MAC address is 0000.0c9f.f000 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.064 secs
  Preemption disabled
  Active router is local
  Standby router is 192.168.10.2, priority 100 (expires in 9.664 sec)
  Priority 100 (default 100)
  Group name is "hsrp-Fa0/1-0" (default)
```

```
PC1> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   192.168.10.2   9.221 ms  8.389 ms  9.430 ms
 2   192.168.221.2   14.470 ms  6.662 ms  2.575 ms
 3   192.168.221.2   5.448 ms  2.640 ms  5.467 ms
 4     *  *  *
 5     *  *  *
 6     *  *  *
 7     *  *  *
 8     *  *  *

PC1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=127 time=96.744 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=127 time=78.016 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=127 time=89.089 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=127 time=72.900 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=127 time=71.005 ms
```

```
R1(config)#int fas 0/1
R1(config-if)#sh
R1(config-if)#
*Jan  6 19:40:13.815: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 0 state Active -> Init
R1(config-if)#
*Jan  6 19:40:15.811: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
*Jan  6 19:40:16.811: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
```

```
R2#
*Jan  6 19:38:56.047: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 0 state Speak -> Standby
R2#
*Jan  6 19:40:23.075: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 0 state Standby -> Active
```

```
PC1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=127 time=107.773 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=127 time=80.640 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=127 time=83.945 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=127 time=66.734 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=127 time=74.254 ms

PC1> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   192.168.10.3   2.269 ms  10.951 ms  10.321 ms
 2   192.168.221.2   20.009 ms  21.068 ms  20.625 ms
 3     *  *  *
 4     *  *  *
 5     *  *  *
 6     *  *  *
 7     *  *  *
 8     *  *  *
```

5.Conclusion

The excess demand for media in Srilanka is due to the limited number of businesses who have involved in this sector. Mediamora company has been established very recently to fulfill those needs for the government sector as well as for the private sector. As a media company predominant types of traffic will be video and voice than data in their networks. So we had to design the network using special equipment, techniques and by using different QoS methods.

The headquarters of the company has two floors including seven departments. Each floor has two 48 port PoE switches which connects to the distribution layer. Vlans are assigned to different departments for internal communication. For wireless user experience each floor has three access points which are connected directly to the PoE switches. Two layer 3 switches have been installed for the backbone of the network and all the servers, storage switches and layer 3 switches are in a server room which is in the ground floor.

This company get contracts from government institutes as well as private institutes. Until the end of the contract period they hold some proprietary information. The security section of the company has been provided with hardware and software firewalls, IDSs and IPSs and by using the VPNs to communicate through the internet. A domain server has been implemented to prevents unauthorized access to the company network and it is well secured with technologies like RADIUS and TACACS. The quality part of the network has been enhanced through numerous tools.

It is clear that these kind of businesses will have more chances to expand rapidly due to the high demand. We have addressed several issues with the expanding it to branch offices in future.

6.References

- Gustavo A. A. Santana. (2016 April). CCNA Cloud CLDFND 210-451 Official Cert Guide.
- Chris Jackson, Hank Preston, Steve Wasko. (2016 November). CCNA Cloud CLDFND 210-455 Official Cert Guide.
- Navaid Shamsee, David Klebanov, Hesham Fayed, Ahmed Afrose, Ozden Karakok. (2016 Novmeber). CCNA Data Center DCICT 200-155 Official Cert Guide.
- Chad Hintz, Cesar Obediente, Ozden Karakkok. (2017 January). CCNA Data Center DCICN 200-150 Official Cert Guide.
- David Hucaby. (2014 February). CCNA Wireless 640-722 Official Cert Guide.

Softwares used:

- Microsoft Word
- Microsoft Visio
- Cisco Packet Tracer
- VMware ESXi
- PRTG network monitor
- Windows server 2016
- Sophos UTM
- Dell EMC unity demo