National Institute of Business Management

Management Information System Division

Diploma in Computer Networks 17.1FT
Group – 3

Network for an Educational Institute

- **P.A.D Dulshan - DCN171FT008**
- **J.P.S.G Jayaweera - DCN171FT011**
- **D.S.B Kothalawala - DCN171FT013**
- **M.I.A Perera - DCN171FT018**

DECLARATION

We are hereby declaring the project report “Network for an Institute” that we submitted to the National Institute of Business Management as a partial fulfilment of diploma in Computer Network. We further declare that we did this project under the guidance and supervision of our lecturer Mr. Milan Maduranga. We also declare that the project we submitted is a genuine and this has not fully copied or partially copied from another project report. In addition, inclusion of this report only uses our knowledge regarding to the project and Netacad site.

Name	Signature
P. A. D. Dulshan	……
J. P. S. G. Jayaweera	……
D. S. B. Kothalawala	……
M. I. A. Perera	……

“I declare this project is proceeded under my guidance and acknowledgement. It does not contain any material or information from previously published projects or written by another person. I also hereby give consent for this project report that anyone can use this report to have knowledge about such as this project.”

…..……

Mr. Milan Maduranga (Supervisor)

Contents

Overview

Business Name: New Network Corporation

General Business Status New Network Corporation has been established as a new estate company in Sri Lanka. Our business model is based on the accomplishment of properties in the real estate markets in Sri Lanka. As beginners in industry we ready to make our way by making customers requirements. There is a great need for certified or official bank checks in the future to deal with some real estate transactions. In addition to real estate investments, the company has invested portions of its assets in the purchase and sale of securities such as stocks and bonds as well as Forex trading on global markets.

Company Strategy

- **Purpose:** To be the best network provider and a leader in the real estate industry by providing enhanced networks with suitable technology.
- **Vision**: To provide quality services that exceeds the expectations of our esteemed customers.
- **Mission statement:** To build long term relationships with our customers and clients and provide exceptional customer services by pursuing business through innovation and advanced technology.
- **Core values:** • We believe in treating our customers with respect and faith• We grow through creativity, invention and innovation. • We integrate honesty, integrity and business ethics into all aspects of our business functioning
- **Goals:** • Regional expansion in the field of networking and develop a strong base of customers. • Increase the market and investments of the company to support the development of services. • To build good reputation in the field of networking and become a key player in the industry.

Scope of Work

New Networks Corporation conducts real estate marketing as well as real estate network consulting. The company undertakes all maintenance duties for networks conducts all the security and surveillance for network.

Acknowledgement

We would like to thank our supervisor and lecturer Mr. Milan Maduranga for giving advises and share knowledge and guidance throughout our project. This project made path to improve our knowledge and our practical skills in computer networking.

Next, we would like to thank the friends who helped to complete this project in a short time by giving the knowledge that they knew.

Thank you again all those people who helped us through this project.

Project Abstract

The target of this project was to design a network to an institute which suitable for an educational environment. The project has focused on reliability, quality and reliability, which was the aim.

This project has provided with utilities to introduce a network with certain rules for the Institute. These utilities are firewalls, an IP access control list, Mac address port security, a domain server and redundant server. All of these utilities have configured to provide a secure to the network. Also, prevent unauthorized accesses to the network.

For the performance of the network are failover firewalls utility, a Pre-boot Execution Environment (PXE) server, a Dynamic Host Configuration Protocol (DHCP) server, a Domain Name System (DNS) server and a cabling system. These are the main tools can increase the performance of the better network with higher performance.

Redundant has kept by using Windows Servers backup (iSCSI initiators and iSCSI target) servers, which helps to keep the Institute's plans and financial information in a safe place. In addition, for Students personal information safety, the webserver has placed in the local network, which provides a secure environment.

Key Words

AD – Active Directory

AP – Access Point

BPDU – Bridge Protocol Data Unit

DCN – Diploma in Computer Networks

DHCP – Dynamic Host Configurations Protocol RADIUS - Remote Authentication Dial-In User Service

DNS – Domain Name System

Gbps – Gigabits per seconds

GUI – Graphical User Interface ADSSO - Active Directory Single Sign-On DN - Distinguished Name

HD – Higher Diploma

HR – Human Resources

HSRP – Hot Standby Router Protocol

IEEE – Institute of Electrical and Electronics Engineers

IT - Information Technology

IP – Internet Protocol

ISP – Internet Service Provider

Kbps – Kilobits per seconds

LACP – Link Aggregation Control Protocol

LAN – Local Area Network

Mbps – Megabits per second

MIS – Management Information Systems

MS Office – Microsoft Office

NAP – Network Access Protection

NIBM – National Institute of Business Management

NOC – Network Operations Center

NVR – Network Video Recorder

PC – Personal Computer

SMS – Short Message Service

STP – Spanning Tree Protocol

TFTP - Trivial File Transfer Protocol

UDP – User Datagram Protocol

URL – Uniform Resource Locator

USB – Universal Serial Bus

VPN – Virtual Private Network

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

WPA-2 – Wi-Fi Protected Access 2

Implementation Figures Tables

1. Introduction

1.1. Background

The purpose of this project was to design a network for an Institute. Network has included with wired, wireless and wide area network (WAN) applications. The WAN has designed to meet its specifications that would be able to operate in a complete receiver. This document provides the information about this project. Also, show and explains the tools that used for the network and how the implementation was proceed orderly.

2. Objectives

The objectives of this project we met were

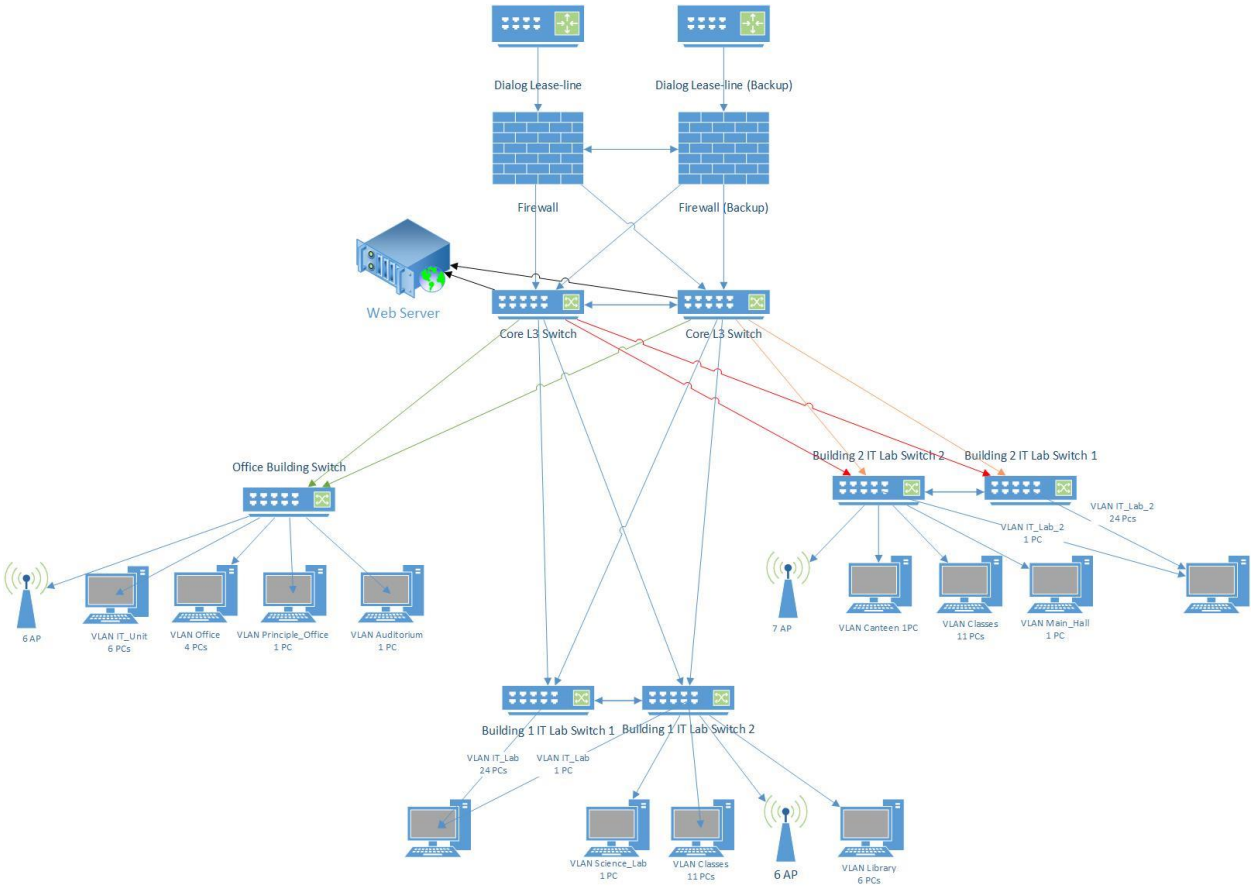
- Identify resources and risks.
- Design a redundancy in the network.
- Implement the designed network.
- Provide maximum security.
- Redundant internet service by use two ISPs.
- Provide high-speed network access inside anywhere in the area.

3. Specification

- **Firewall**
  - name: Sophos XG 85
  - Max throughput: 3000 mbps
- **Switche**s
  - name: cisco catalyst 2960XR-24TS-l
  - Max forwarding speed: 40Gps
- **l3 switches**
  - name: cisco Catalyst 3560-24TS
  - Max forwarding speed: 32Gps
- **Server**
  - name: PowerEdge T130 Tower Server
  - Maximum RAM: Up to 64GB
  - Operating System: Microsoft® Windows Server® 2016
  - Processor: Intel® Xeon® processor E3-1200 v6
- **AP**
  - name: cisco airnet 2700
  - Connection rate: Upto 1.3 Gbps

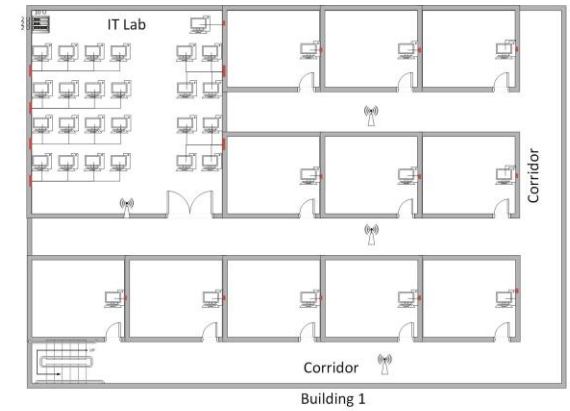
4. Design

4.1 Physical Network Diagram

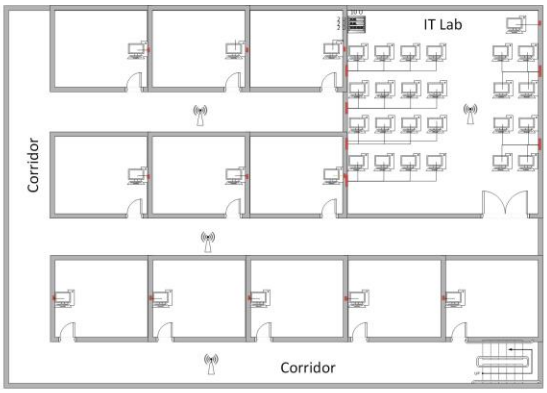


4.2 Floor Plans

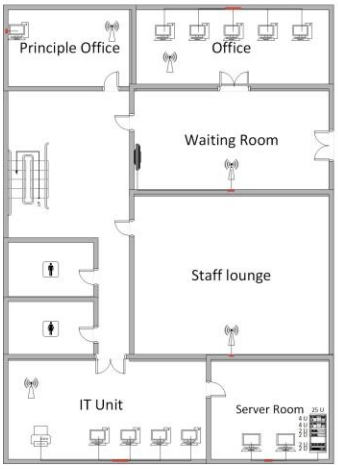
Ground Floor



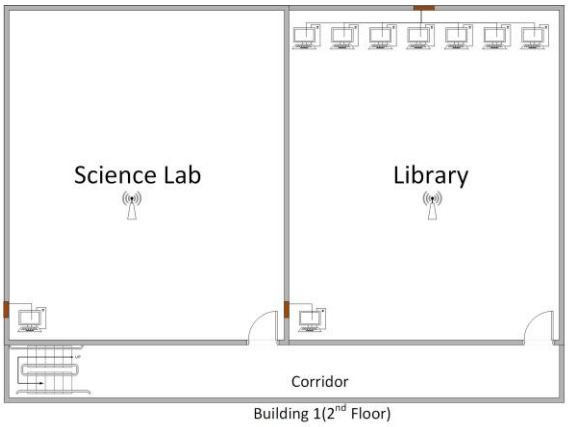
Building 1



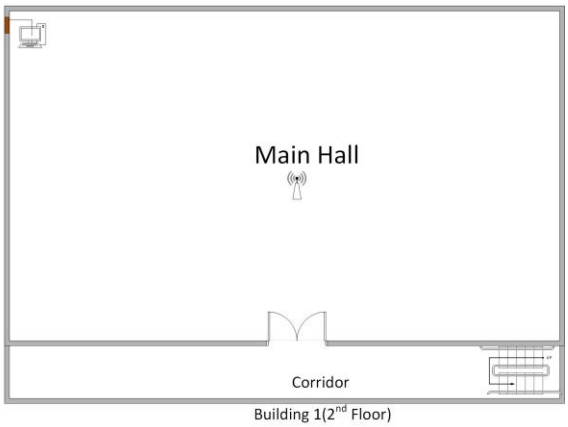
Building 2



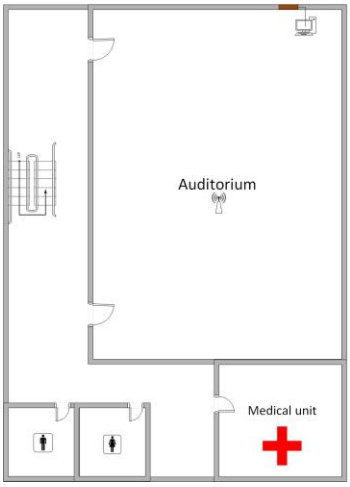
Second Floor



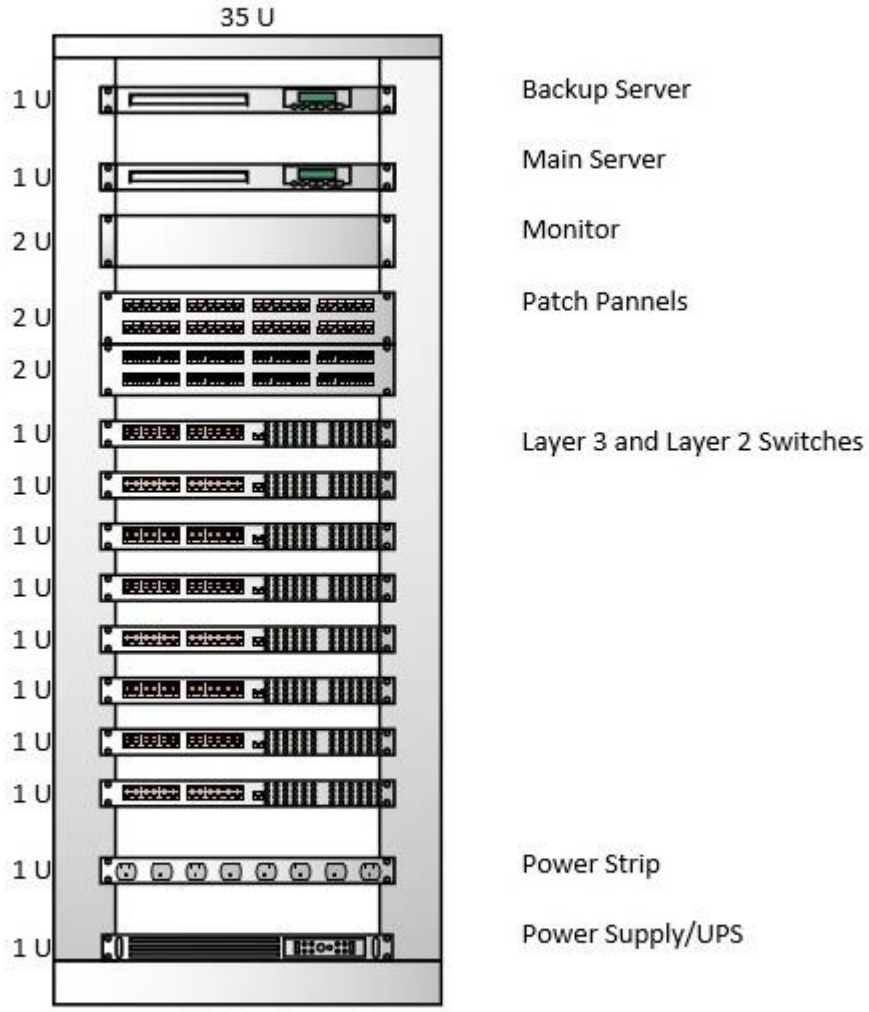
Building 1(2nd Floor)



Building 1(2nd Floor)



4.3 Rack Design



4.4 Bandwidth Calculation

- The Institute generally contains with main 13 Departments which has more sub departments.
- We estimated institute has 150 employees but concurrent employees 90.

Vlan Name	Estimated Concurrent Users	Usage	Allocated Bandwidth
WiFi	300	256 KB/s	76 MB/s
Classes	22	512 KB/s	12 MB/s
IT_Lab	26	800 KB/s	21 MB/s
IT_Lab 2	26	800 KB/s	21 MB/s
IT_Unit	6	2000 KB/s	12 MB/s
Office	6	800 KB/s	12 MB/s
Library	4	256 KB/s	1 MB/s
Science_Lab	4	256 KB/s	1 MB/s
Auditorium	1	512 KB/s	0.5 MB/s
Main_Hall	1	512 KB/s	0.5 MB/s
Principle_Office	1	2000 KB/s	2 MB/s
Canteen	1	256 KB/s	0.3 MB/s
Total			304,608 KB/s
			304 MB/s

4.5 IP Addressing

Vlan Name	Interface	IP Address	Subnet Mask	Default Gateway
WiFi	Vlan 1	192.168.0.0	255.255.252.0	192.168.0.1
Classes	Vlan 2	192.168.4.0	255.255.255.192	192.168.4.1
IT_Lab	Vlan 3	192.168.4.64	255.255.255.224	192.168.4.65
IT_Lab 2	Vlan 4	192.168.4.96	255.255.255.224	192.168.4.97
IT_Unit	Vlan 5	192.168.4.128	255.255.255.240	192.168.4.129
Office	Vlan 6	192.168.4.144	255.255.255.240	192.168.4.145
Library	Vlan 7	192.168.4.160	255.255.255.240	192.168.4.161
Science_Lab	Vlan 8	192.168.4.176	255.255.255.240	192.168.4.177
Auditorium	Vlan 9	192.168.4.192	255.255.255.248	192.168.4.193
Main_Hall	Vlan 10	192.168.4.200	255.255.255.248	192.168.4.201
Principle_Office	Vlan 11	192.168.4.208	255.255.255.248	192.168.4.209
Canteen	Vlan 12	192.168.4.216	255.255.255.248	192.168.4.217
Server Room	Vlan 13	192.168.4.224	255.255.255.248	192.168.4.225

4.6 Protocols

HSRP: Used to make redundancy in the core layer of the network. If the main Switch goes down the backup will take over the routing process.

SNMP: Protocol used for the monitoring of the hardware and stat of the devices. PRTG is the management software used.

IP Routing: Only VLANs are used, so this enables inter VLAN routing.

VTP: Sharing of VLAN database from the main switch(server) to all client switches in the same domain.

RSTP: Avoid any loop in the network which will affect device and network performance by assigning a root brigde.

SSH: Enables remote secure access to Devices after the initial configurations from concole.

ADDS: Active Directry Domain Service, Managing OU, Users and Computers.

DNS: Domain name server.

WDS: Windows deployment service, makes it easier to manage deployemnt, updating and backing of PCs with Windows OS in the network.

DHCP: Dynamically assigning of unique IP addresses based on the device VLAN and network automatically from a pool of available addresses for the specific vlan.

NPS: Wireless Authentication And Radius implementation

ADCS: Network Certificate authentication

SMTP: Mail server

4.7 Data Network Security

- Use the firewall to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.
- The wireless communication secured and protected with encryption algorithms such as WPA/ WPA2.
- Used to access control list filters for network traffic
- Port security use one-way to secure ports is by implementing.
- Administrative disable unused ports.
- Secure shell (SSH) is provides a secure management connection to a remote device.
- Encryption algorithm used to encrypt Password for user's data security.
- VTP mode, domain and password use manage and secure VLAN configurations between switches.

4.8 Physical Network Security

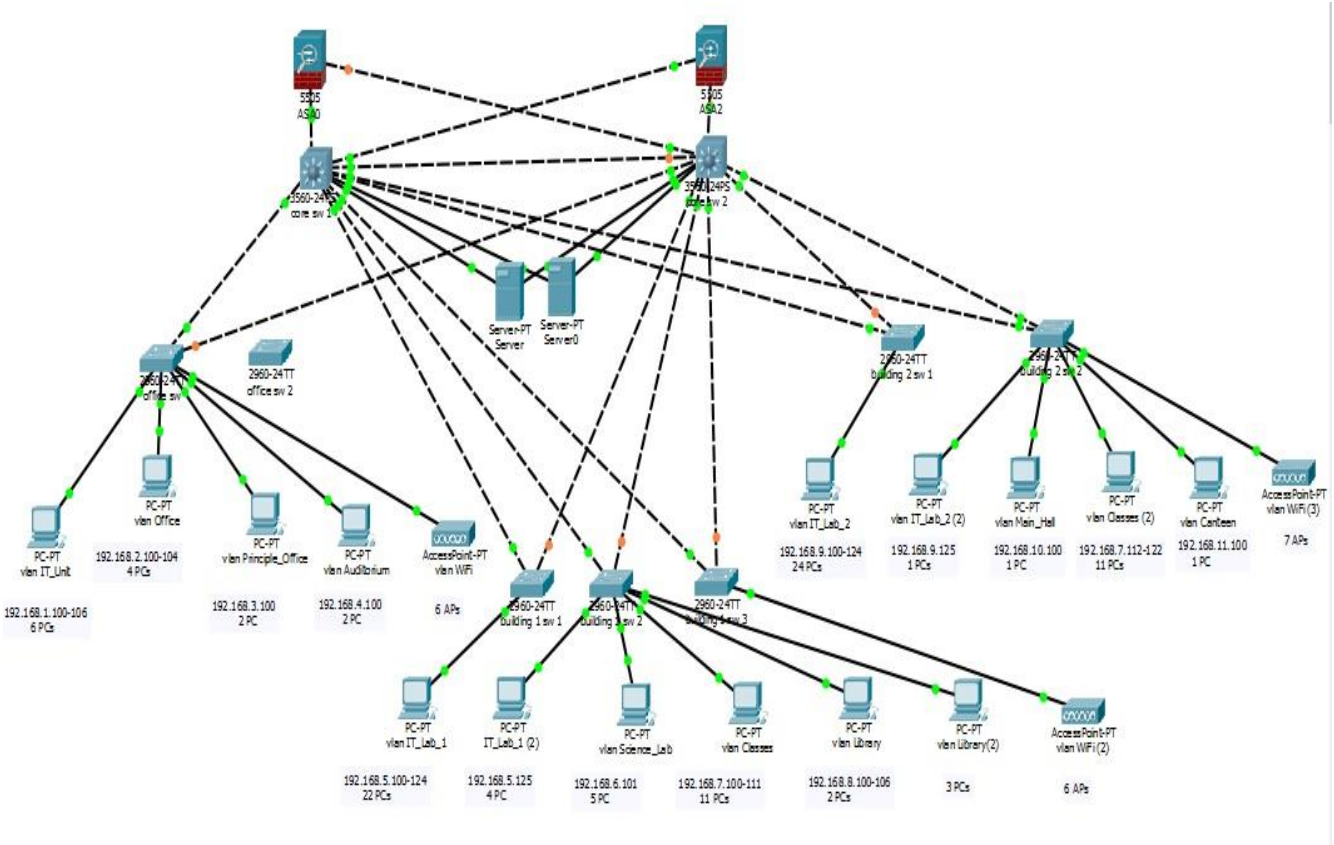
- Server room include with entrance permission by giving fingerprint. This security process provides through a fingerprint scanner. In addition, permission is only for authorized persons.
- Server room has a fire protection system with FM – 200 devices. Through this device provides server room a waterless fire suppression system.
- Unnecessary temperature has managed through air conditioner.
- Server rack has locked to prevent from unauthorized users due to a security breach.

4.9 Network Features

- All devices are redundancy in the network.
- Divided in 10 VLANs and native VLAN 99.
- Guest and staff can connect internet with Username and password.
- Hotel web page is host.
- We hope send the syslog to admin email.
- Guest chose SSID is Hotel Guest and staff chose Hotel Staff for connect WI-FI
- Centralized authentication, authorization and accounting management for users connect and use a network for use Remote Authentication Dial-In User Service (RADIUS) server.
- Gests' user names and passwords have time limit.
- Staffs' usernames and passwords not have time limit.
- Installed computer system connect ADDS.

5. Implementation

5.1 Network Configuration



Core_1

hostname Core_1

vtp mode server

vtp domain abc

ip domain-name ABCSc.lk

crypto key generate rsa

username abc secret abc

line vty 0 15

transport input ssh

login local

exit

```
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3

vlan 5
name WiFi
vlan 6
name Classes
vlan 7
name IT_Lab
vlan 8
name IT_Lab_2
vlan 9
name IT_Unit
vlan 10
name Office
vlan 11
name Library
vlan 12
name Science_Lab
vlan 13
name Auditorium
vlan 14
name Main_Hall
vlan 15
name Principle_Office
vlan 16
name Canteen
vlan 17
name Server_Room
vlan 100
```

```
name WAN

spanning-tree vlan 1-9 root primary
spanning-tree vlan 10-18 root secondary

ip access-list standard it_access
permit 192.168.4.128 255.255.255.240
deny any
exit

snmp-server community cisco
snmp-server enable trap

interface vlan 1
ip address 192.168.200.1 255.255.252.0
ip access-group it_access in
no shut

interface vlan 5
ip address 192.168.0.2 255.255.252.0
standby 5 ip 192.168.0.1
standby 5 priority 150
standby 5 pre
ip helper-address 192.168.16.108

interface vlan 6
ip address 192.168.4.2 255.255.255.192
standby 6 ip 192.168.4.1
standby 6 priority 150
standby 6 pre
ip helper-address 192.168.16.108
```

interface vlan 7
ip address 192.168.4.66 255.255.255.224
standby 7 ip 192.168.4.65
standby 7 priority 150
standby 7 pre
ip helper-address 192.168.16.108

interface vlan 8
ip address 192.168.4.98 255.255.255.224
standby 8 ip 192.168.4.97
standby 8 priority 150
standby 8 pre
ip helper-address 192.168.16.108

interface vlan 9
ip address 192.168.4.130 255.255.255.240
standby 9 ip 192.168.4.129
standby 9 priority 150
standby 9 pre
ip helper-address 192.168.16.108

interface vlan 10
ip address 192.168.4.146 255.255.255.240
standby 10 priority 150
standby 10 pre
ip helper-address 192.168.16.108
standby 10 ip 192.168.4.145
ip access-group it_access in

```
interface vlan 11
ip address 192.168.4.162 255.255.255.240
standby 11 ip 192.168.4.161
standby 11 priority 150
standby 11 pre
ip helper-address 192.168.16.108

interface vlan 12
ip address 192.168.4.178 255.255.255.240
standby 12 ip 192.168.4.177
standby 12 priority 150
standby 12 pre
ip helper-address 192.168.16.108

interface vlan 13
ip address 192.168.4.194 255.255.255.248
standby 13 ip 192.168.4.193
standby 13 priority 150
standby 13 pre
ip helper-address 192.168.16.108

interface vlan 14
ip address 192.168.4.202 255.255.255.248
standby 14 ip 192.168.4.201
standby 14 priority 150
standby 14 pre
ip helper-address 192.168.16.108

interface vlan 15
ip address 192.168.4.210 255.255.255.248
standby 15 ip 192.168.4.209
```

standby 15 priority 150
standby 15 pre
ip helper-address 192.168.16.108
ip access-group principle in

interface vlan 16
ip address 192.168.4.218 255.255.255.248
standby 16 ip 192.168.4.217
standby 16 priority 150
standby 16 pre
ip helper-address 192.168.16.108

interface vlan 17
ip address 192.168.16.2 255.255.255.0
standby 17 ip 192.168.16.254
standby 17 priority 150
standby 17 pre
ip access-group it_access in

Core_2

hostname Core_2
vtp mode client
vtp domain abc

spanning-tree vlan 1-9 root secondary
spanning-tree vlan 10-18 root primary

ip access-list standard it_access
permit 192.168.4.128 255.255.255.240
deny any

```
exit

ip domain-name ABCSc.lk
crypto key generate rsa
username abc secret abc
line vty 0 15
transport input ssh
login local
exit
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3

interface vlan 1
ip address 192.168.201.1 255.255.252.0
ip access-group it_access in
no shut

interface vlan 5
ip address 192.168.0.3 255.255.252.0
standby 5 ip 192.168.0.1
ip helper-address 192.168.16.108

interface vlan 6
ip address 192.168.4.3 255.255.255.192
standby 6 ip 192.168.4.1
ip helper-address 192.168.16.108

interface vlan 7
ip address 192.168.4.67 255.255.255.224
standby 7 ip 192.168.4.65
```

ip helper-address 192.168.16.108

interface vlan 8
ip address 192.168.4.99 255.255.255.224
standby 8 ip 192.168.4.97
ip helper-address 192.168.16.108

interface vlan 9
ip address 192.168.4.131 255.255.255.240
no shutdown
standby 9 ip 192.168.4.129
ip helper-address 192.168.16.108

interface vlan 10
ip address 192.168.4.147 255.255.255.240
no shutdown
standby 10 ip 192.168.4.145
ip helper-address 192.168.16.108
ip access-group it_access in

interface vlan 11
ip address 192.168.4.163 255.255.255.240
no shutdown
standby 11 ip 192.168.4.161
ip helper-address 192.168.16.108

interface vlan 12
ip address 192.168.4.179 255.255.255.240
no shutdown
standby 12 ip 192.168.4.177

```
ip helper-address 192.168.16.108

interface vlan 13
ip address 192.168.4.195 255.255.255.248
no shutdown
standby 13 ip 192.168.4.193
ip helper-address 192.168.16.108

interface vlan 14
ip address 192.168.4.203 255.255.255.248
no shutdown
standby 14 ip 192.168.4.201
ip helper-address 192.168.16.108

interface vlan 15
ip address 192.168.4.211 255.255.255.248
standby 15 ip 192.168.4.209
ip helper-address 192.168.16.108

interface vlan 16
ip address 192.168.4.219 255.255.255.248
standby 16 ip 192.168.4.217
ip helper-address 192.168.16.108

interface vlan 17
ip address 192.168.16.3 255.255.255.0
standby 17 ip 192.168.16.254
ip access-group it_access in
```

Office_Sw

```
hostname Office
vtp mode client
interface range fastEthernet 0/1-2
switchport mode trunk
exit
interface range fastEthernet 0/3-20
switchport mode access
no shutdown
```

Building 1 switch 1

```
hostname B1S1
vtp mode client
interface range fastEthernet 0/1-2
switchport mode trunk
no shutdown
interface range fastEthernet 0/3-24
switchport mode access
no shutdown
```

Building 1 switch 2

```
hostname B1S2
vtp mode client
interface range fastEthernet 0/1-2
switchport mode trunk
no shutdown
interface range fastEthernet 0/3-24
switchport mode access
no shutdown
```

Building 1 swicth 3

hostname B1S3
vtp mode client
interface range fastEthernet 0/1-2
switchport mode trunk
no shutdown
interface range fastEthernet 0/3-8
Bswitchport mode access
no shutdown
interface range fastEthernet 0/9-24
shutdown

Building 2 swicth 1

hostname B2S1
vtp mode client
interface range fastEthernet 0/1-2
switchport mode trunk
no shutdown
interface range fastEthernet 0/3-24
switchport mode access
no shutdown
exit

Building 2 switch 2

hostname B2S2
vtp mode client
interface range fastEthernet 0/1-2
switchport mode trunk

interface range fastEthernet 0/3-22

switchport mode access

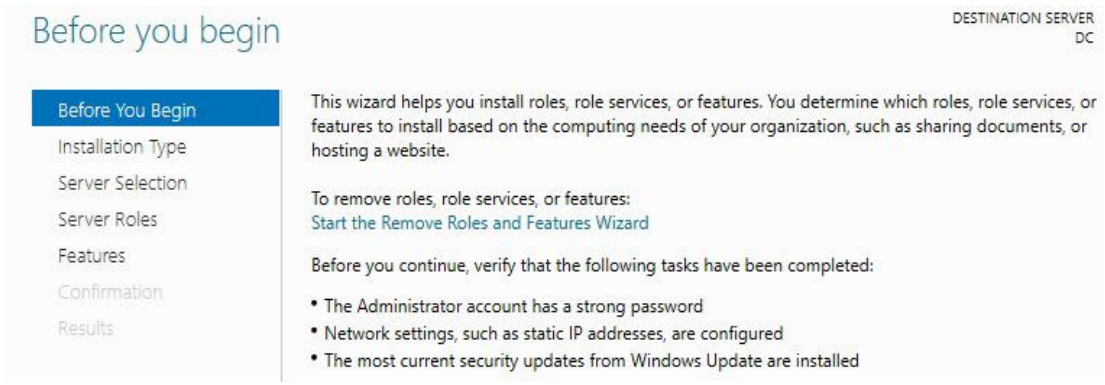
no shutdown

interface range fastEthernet 0/22-24

shutdown

5.2 Server Configuration

Implementing Adding Role



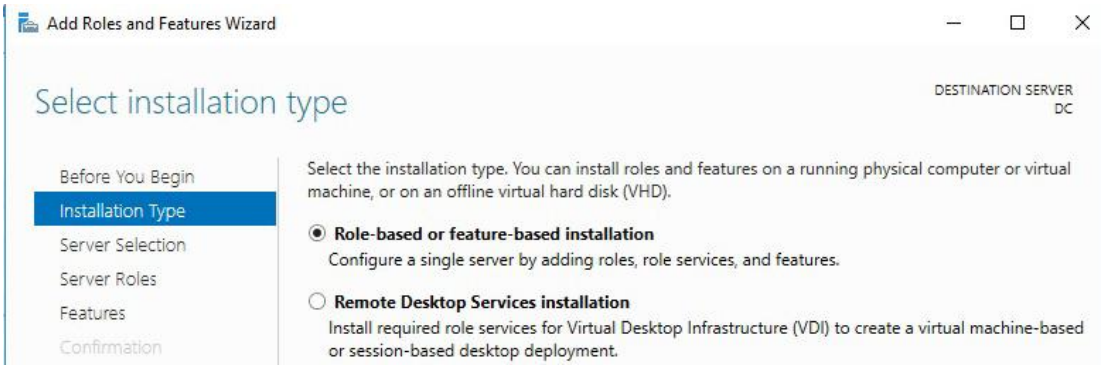


Figure 1 – 2

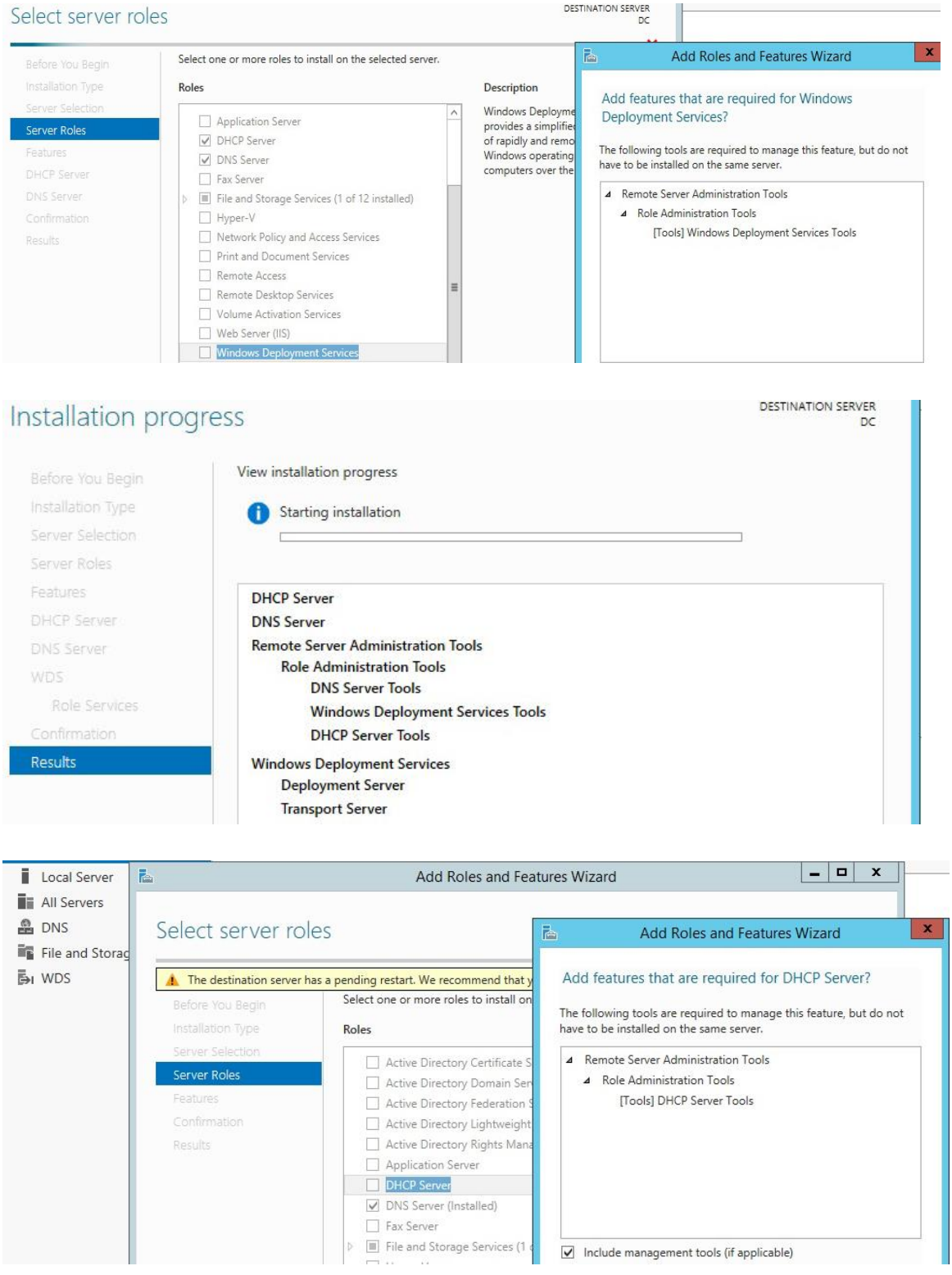
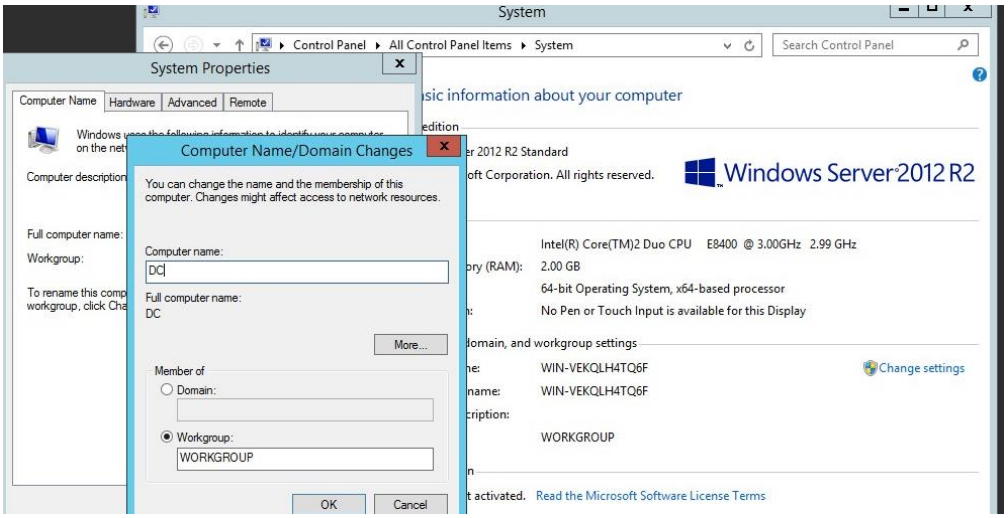

Select server roles
DESTINATION SERVER
DC
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Application Server
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Add Roles and Features Wizard
Add features that are required for Windows Deployment Services?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] Windows Deployment Services Tools
Installation progress
DESTINATION SERVER
DC
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
WDS
Role Services
Confirmation
Results
View installation progress
Starting installation
DHCP Server
DNS Server
Remote Server Administration Tools
Role Administration Tools
DNS Server Tools
Windows Deployment Services Tools
DHCP Server Tools
Windows Deployment Services
Deployment Server
Transport Server
Local Server
All Servers
DNS
File and Storag
WDS
Add Roles and Features Wizard
Select server roles
The destination server has a pending restart. We recommend that y
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on
Roles
Active Directory Certificate S
Active Directory Domain Ser
Active Directory Federation S
Active Directory Lightweight
Active Directory Rights Mana
Application Server
DHCP Server
DNS Server (Installed)
Fax Server
File and Storage Services (1
Add Roles and Features Wizard
Add features that are required for DHCP Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DHCP Server Tools
Include management tools (if applicable)

Figure 3 – 5

Implementing Changing Computer Name for DNS



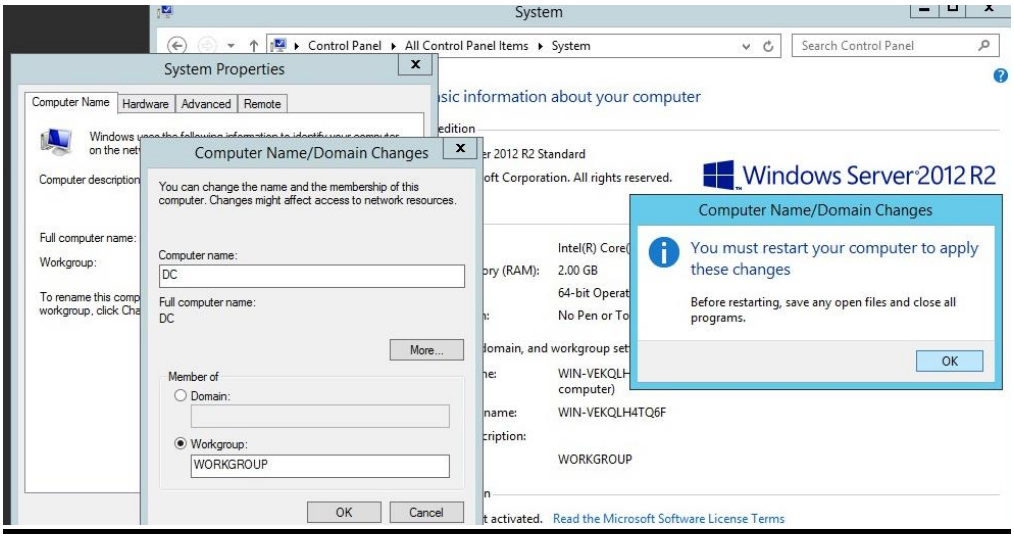


Figure 6 - 7

Implementing AD Configuration

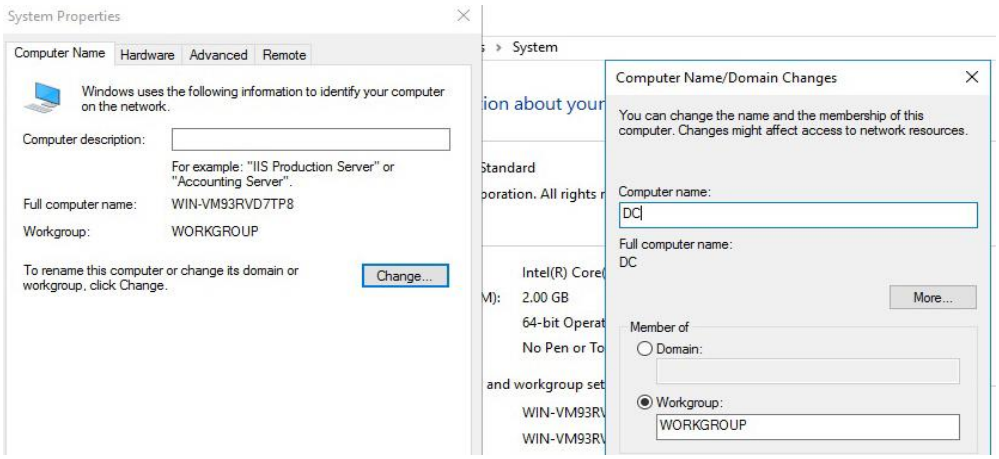
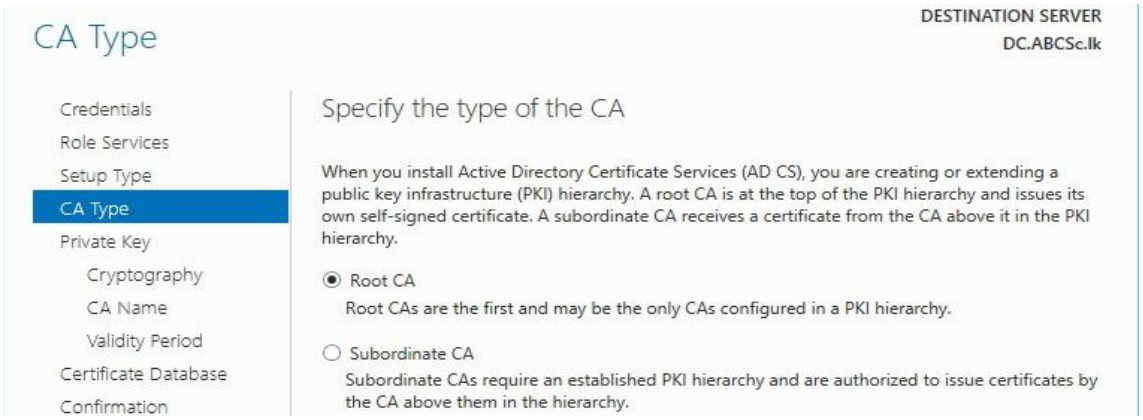
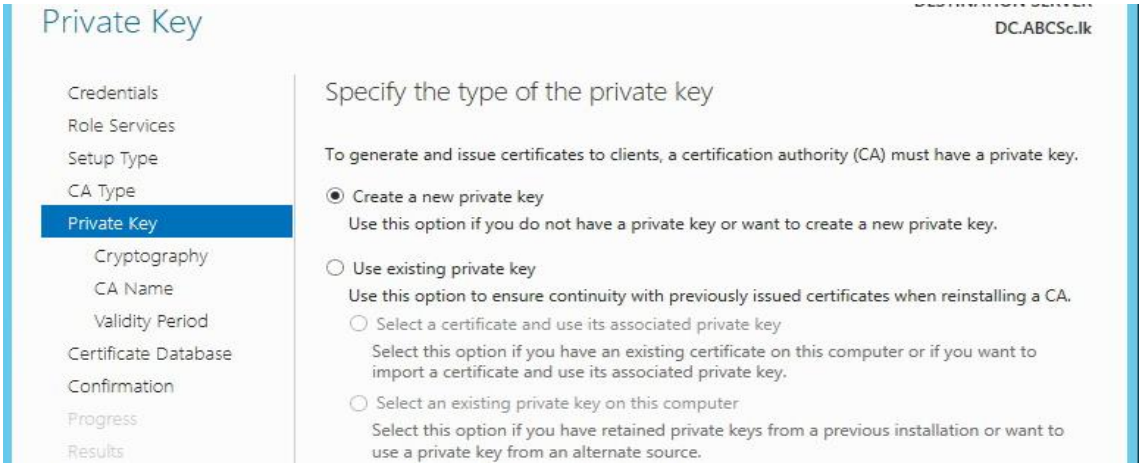


Figure 8 – 10


CA Type
DESTINATION SERVER
DC.ABCSc.lk
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Specify the type of the CA
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.
Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.


Private Key
DC.ABCSc.lk
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the type of the private key
To generate and issue certificates to clients, a certification authority (CA) must have a private key.
Create a new private key
Use this option if you do not have a private key or want to create a new private key.
Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.
Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.
Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.


Cryptography for CA
DC.ABCSc.lk
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Specify the cryptographic options
Select a cryptographic provider:
RSA#Microsoft Software Key Storage Provider
Key length:
2048
Select the hash algorithm for signing certificates issued by this CA:
SHA256
SHA384
SHA512
SHA1
MD5
Allow administrator interaction when the private key is accessed by the CA.

Figure 11 – 13


CA Name
DC.ABCSc.lk
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Specify the name of the CA
Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.
Common name for this CA:
ABCSc-DC-CA
Distinguished name suffix:
DC=ABCSc,DC=lk
Preview of distinguished name:
CN=ABCSc-DC-CA,DC=ABCSc,DC=lk


Validity Period
DC.ABCSc.lk
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Specify the validity period
Select the validity period for the certificate generated for this certification authority (CA):
5
Years
CA expiration Date: 4/28/2023 9:29:00 AM
The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

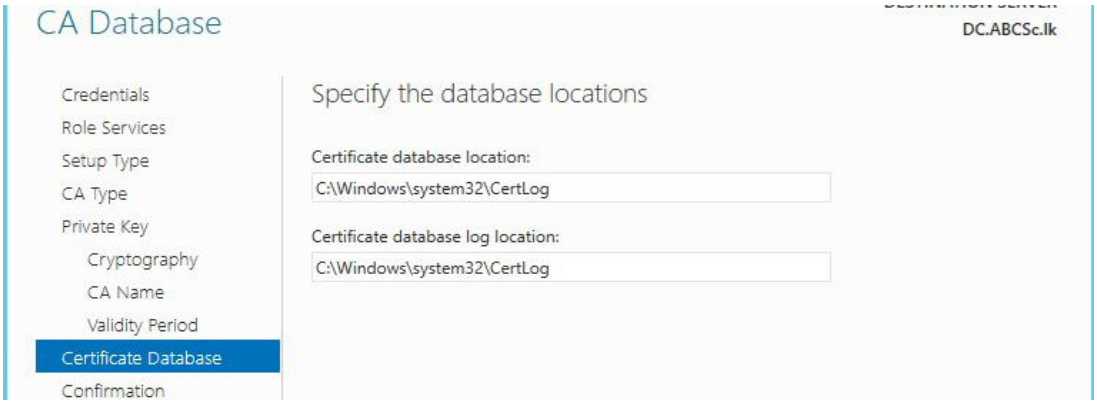
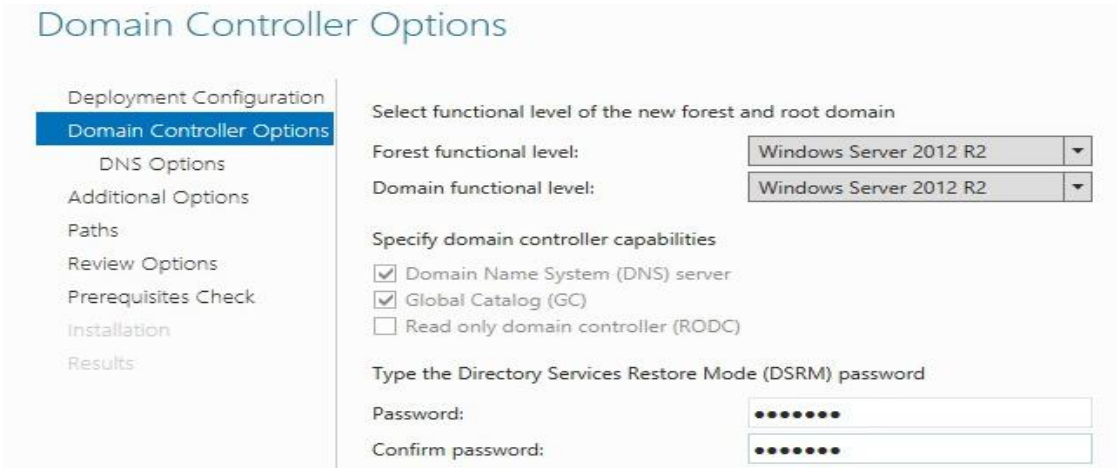
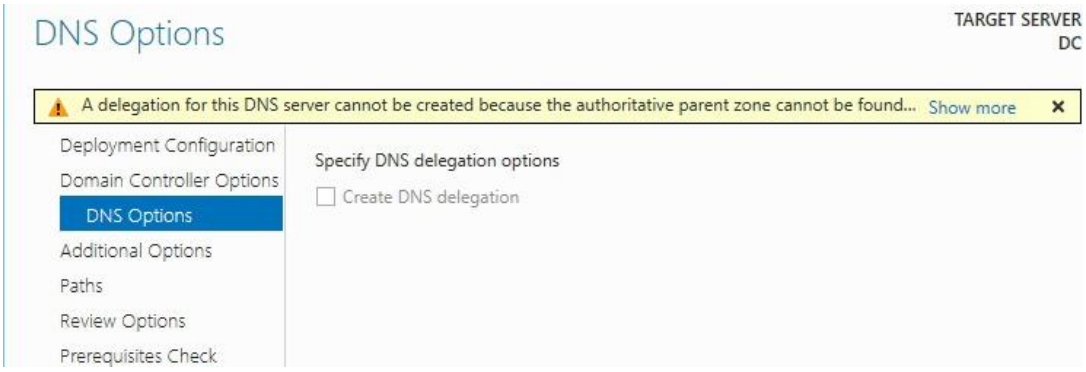

CA Database
DC.ABCSc.lk
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Specify the database locations
Certificate database location:
C:\Windows\system32\CertLog
Certificate database log location:
C:\Windows\system32\CertLog

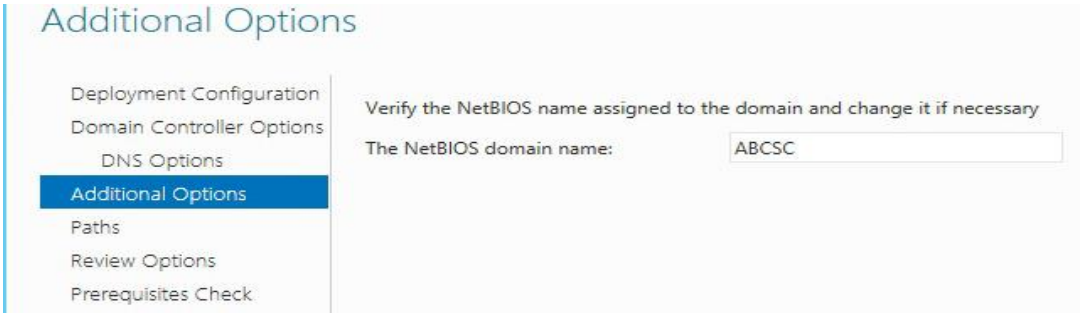
Figure 14 – 16

Implementing ADDS

Figure 17 – 19


Domain Controller Options
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server 2012 R2
Domain functional level:
Windows Server 2012 R2
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:


DNS Options
TARGET SERVER
DC
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Specify DNS delegation options
Create DNS delegation


Additional Options
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
ABCSC

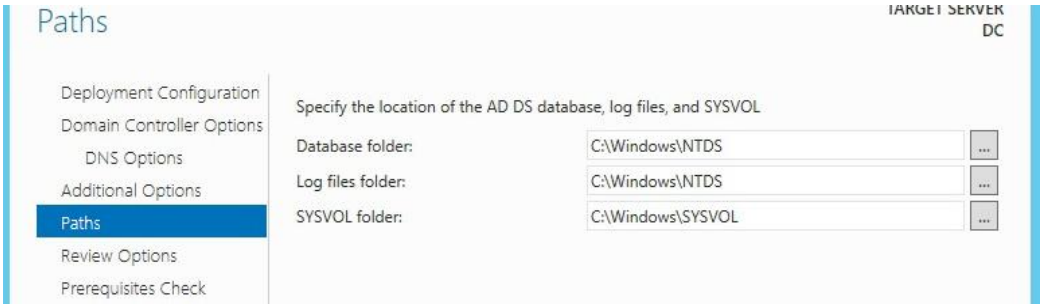
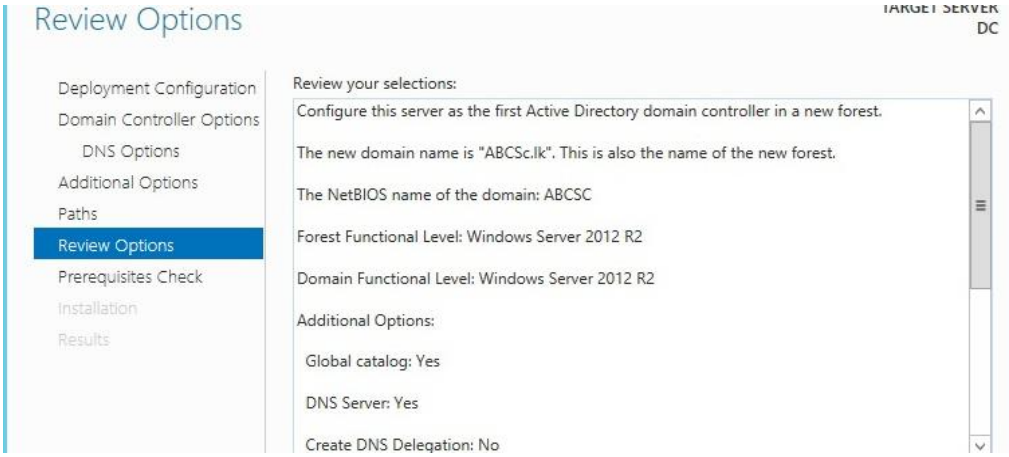

Paths
TARGET SERVER
DC
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL

Figure 20 – 23



Implementing DHCP

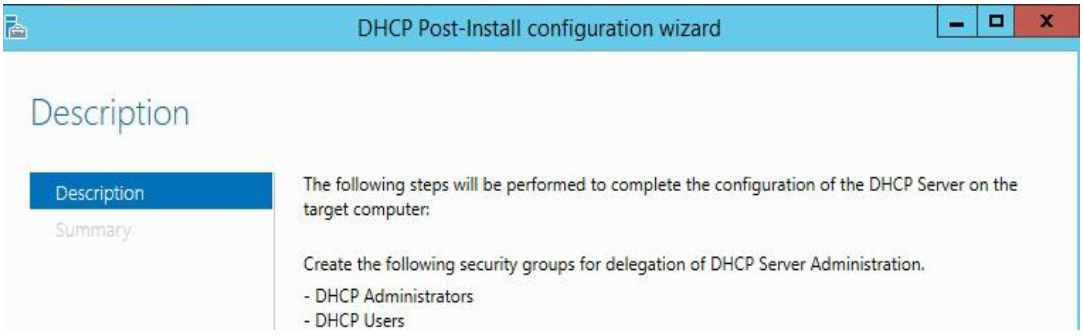
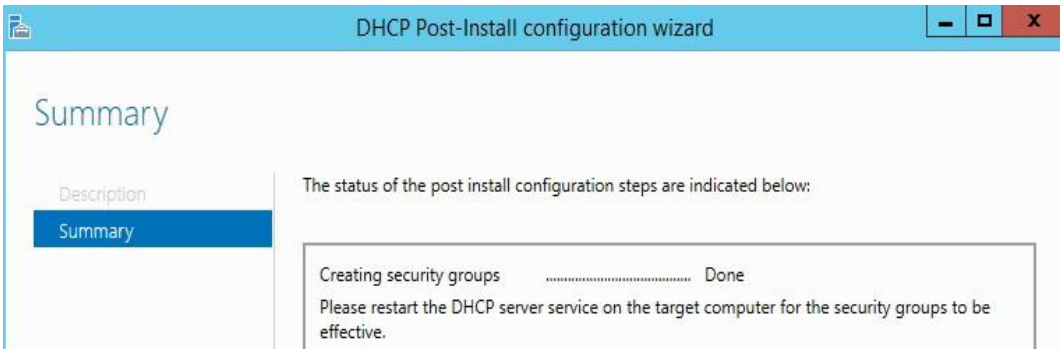
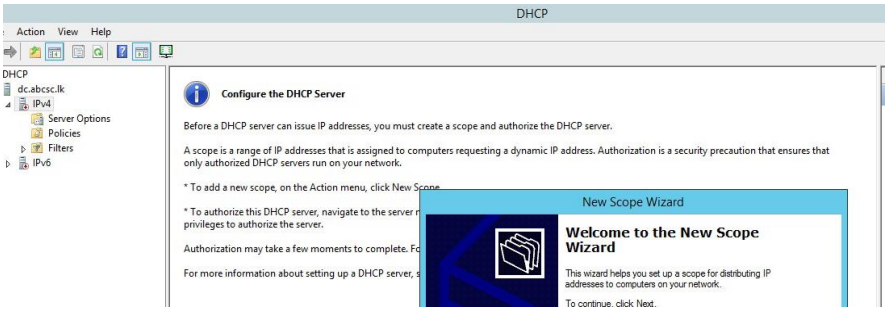
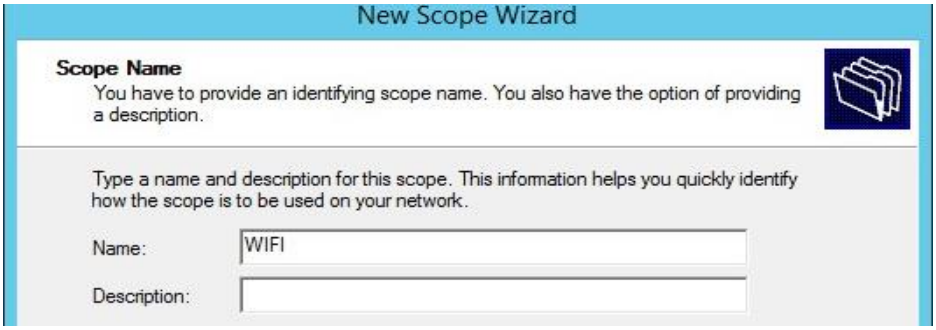


Figure 24 – 26


DHCP Post-Install configuration wizard
Summary
Description
Summary
The status of the post install configuration steps are indicated below:
Creating security groups ..... Done
Please restart the DHCP server service on the target computer for the security groups to be effective.


DHCP
Action View Help
DHCP
dc.abcsc.lk
IPv4
Server Options
Policies
Filters
IPv6
Configure the DHCP Server
Before a DHCP server can issue IP addresses, you must create a scope and authorize the DHCP server.
A scope is a range of IP addresses that is assigned to computers requesting a dynamic IP address. Authorization is a security precaution that ensures that only authorized DHCP servers run on your network.
New Scope Wizard
Welcome to the New Scope Wizard
This wizard helps you set up a scope for distributing IP addresses to computers on your network.
To continue, click Next.


New Scope Wizard
Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.
Name:
WIFI
Description:

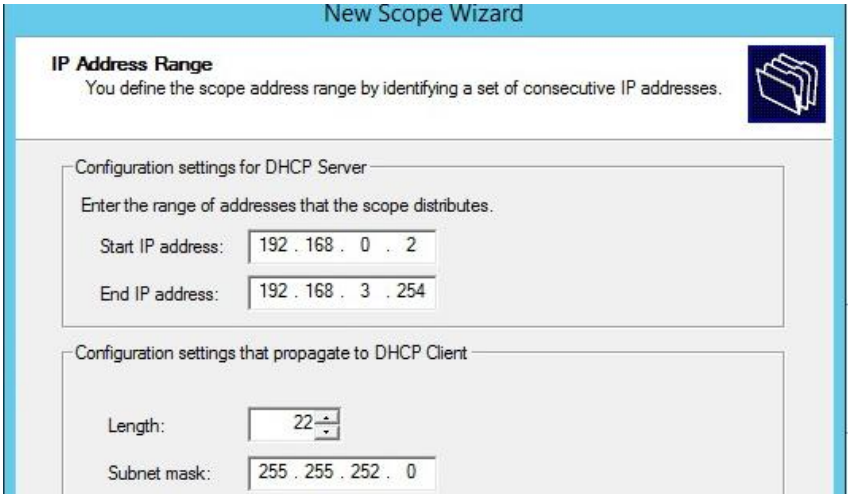
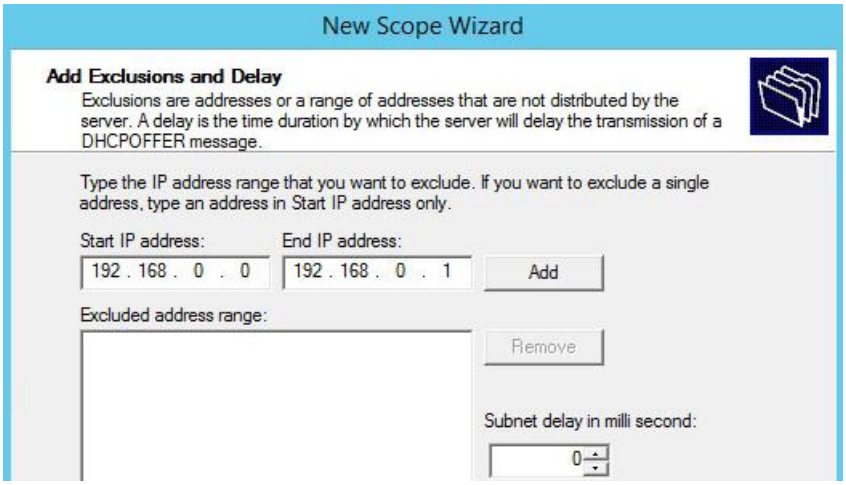
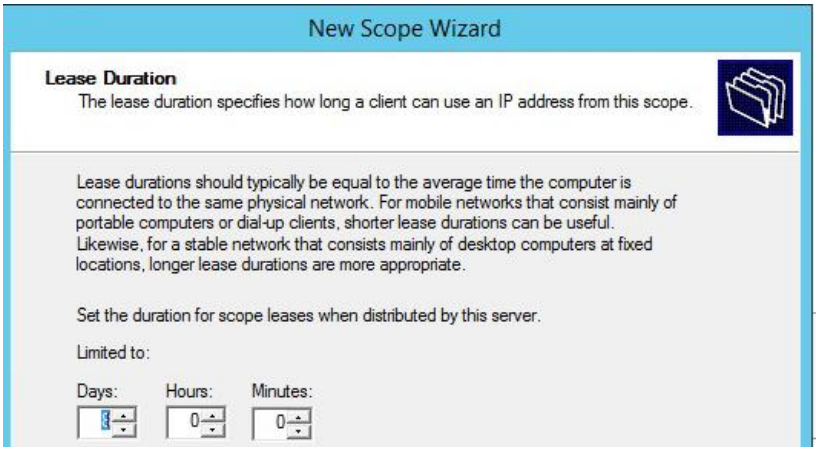

New Scope Wizard
IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.
Configuration settings for DHCP Server
Enter the range of addresses that the scope distributes.
Start IP address:
192 . 168 . 0 . 2
End IP address:
192 . 168 . 3 . 254
Configuration settings that propagate to DHCP Client
Length:
22
Subnet mask:
255 . 255 . 252 . 0

Figure 27 – 30

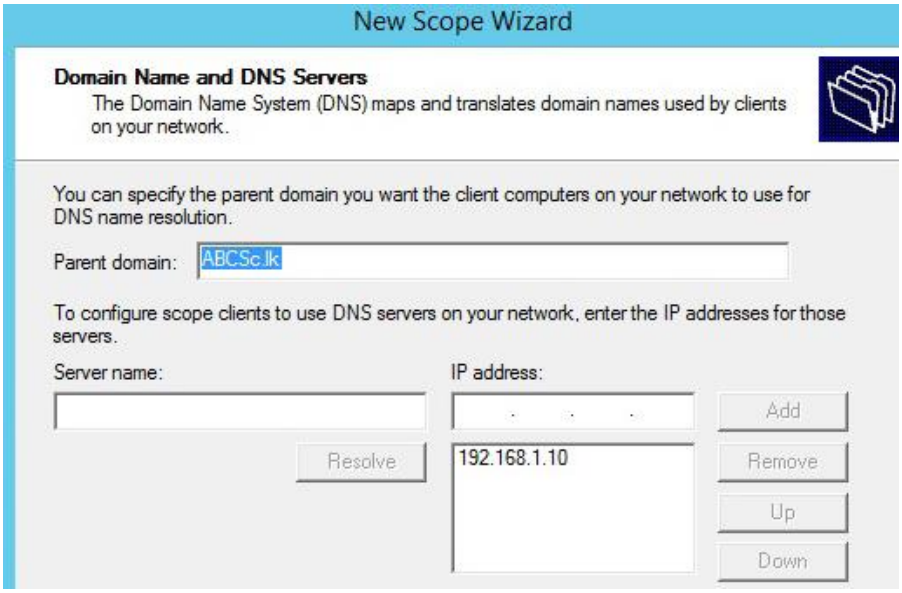

New Scope Wizard
Add Exclusions and Delay
Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCPOFFER message.
Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.
Start IP address:
End IP address:
192 . 168 . 0 . 0
192 . 168 . 0 . 1
Add
Excluded address range:
Remove
Subnet delay in milli second:
0


New Scope Wizard
Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.
Set the duration for scope leases when distributed by this server.
Limited to:
Days:
Hours:
Minutes:
8
0
0


New Scope Wizard
Configure DHCP Options
You have to configure the most common DHCP options before clients can use the scope.
When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.
Do you want to configure the DHCP options for this scope now?
Yes, I want to configure these options now
No, I will configure these options later

Figure 31 – 33


New Scope Wizard
Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.
To add an IP address for a router used by clients, enter the address below.
IP address:
192 . 168 . 0 . 1
Add
Remove
Up
Down


New Scope Wizard
Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.
You can specify the parent domain you want the client computers on your network to use for DNS name resolution.
Parent domain:
ABCSc.lk
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.
Server name:
IP address:
Add
Resolve
192.168.1.10
Remove
Up
Down

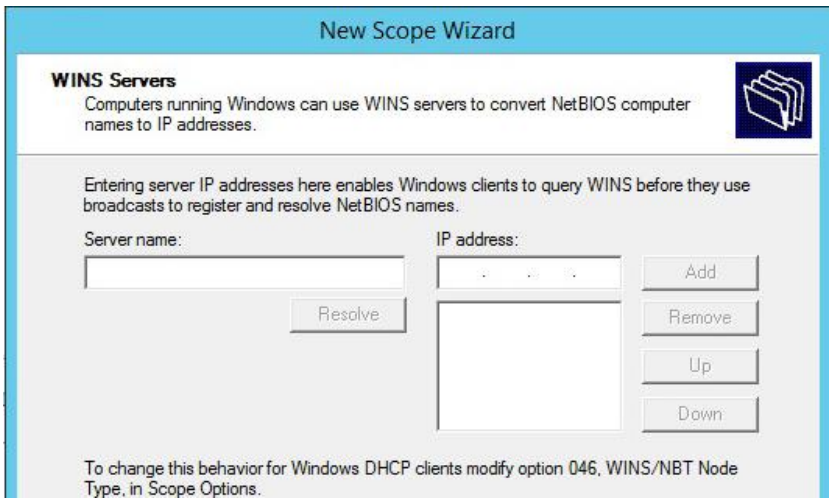
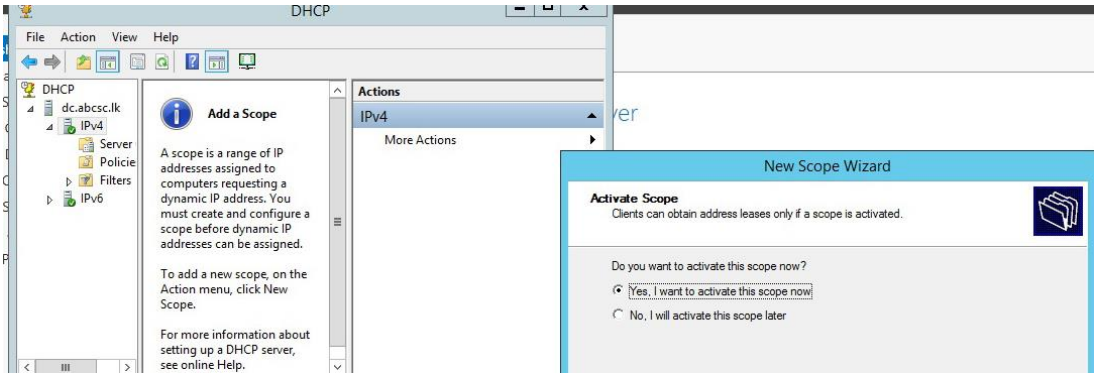
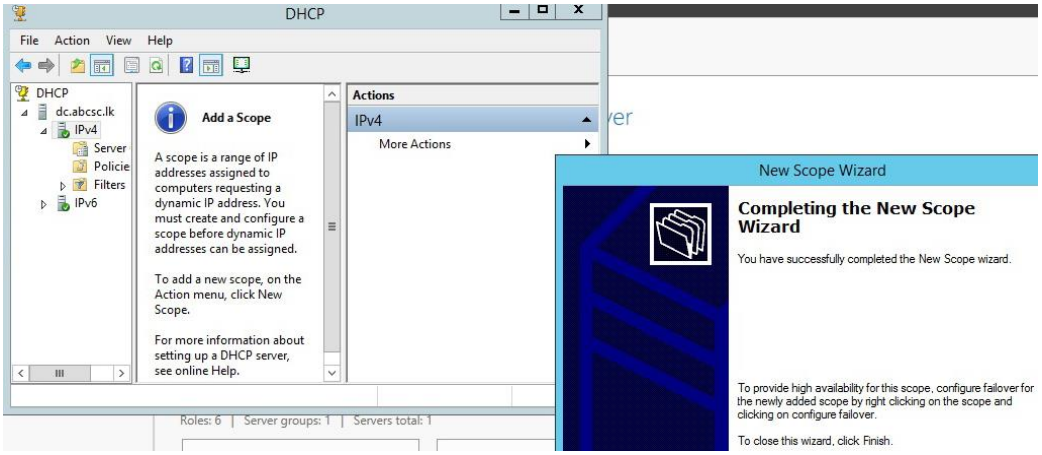

New Scope Wizard
WINS Servers
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.
Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.
Server name:
IP address:
Add
Resolve
Remove
Up
Down
To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

Figure 34 – 36


DHCP
File Action View Help
DHCP
dc.abcsc.lk
IPv4
Server
Policie
Filters
IPv6
Add a Scope
A scope is a range of IP addresses assigned to computers requesting a dynamic IP address. You must create and configure a scope before dynamic IP addresses can be assigned.
To add a new scope, on the Action menu, click New Scope.
For more information about setting up a DHCP server, see online Help.
Actions
IPv4
More Actions
New Scope Wizard
Activate Scope
Clients can obtain address leases only if a scope is activated.
Do you want to activate this scope now?
Yes, I want to activate this scope now
No, I will activate this scope later


DHCP
File Action View Help
DHCP
dc.abcsc.lk
IPv4
Server
Policie
Filters
IPv6
Add a Scope
A scope is a range of IP addresses assigned to computers requesting a dynamic IP address. You must create and configure a scope before dynamic IP addresses can be assigned.
To add a new scope, on the Action menu, click New Scope.
For more information about setting up a DHCP server, see online Help.
Actions
IPv4
More Actions
New Scope Wizard
Completing the New Scope Wizard
You have successfully completed the New Scope wizard.
To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.
To close this wizard, click Finish.

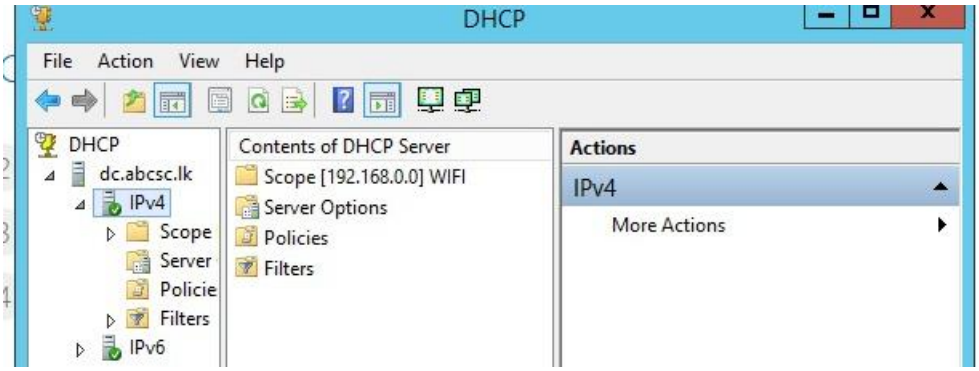
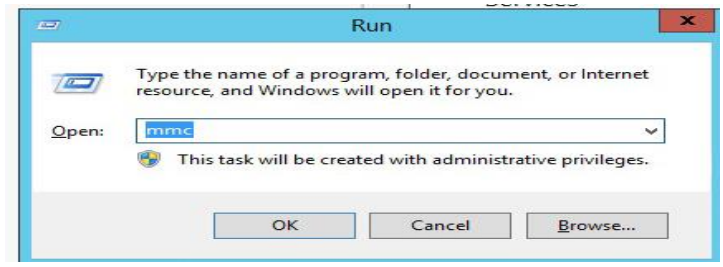
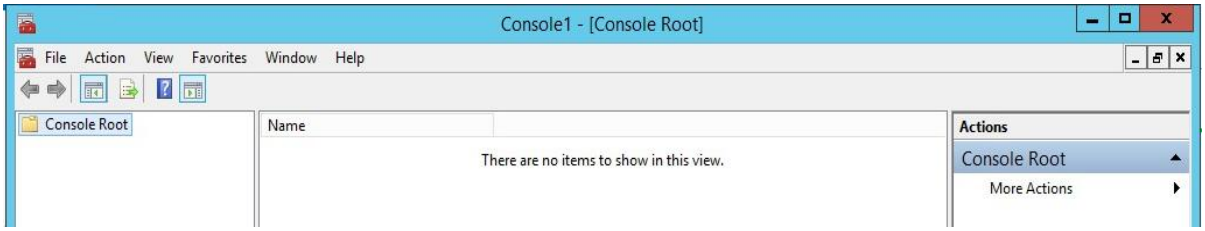
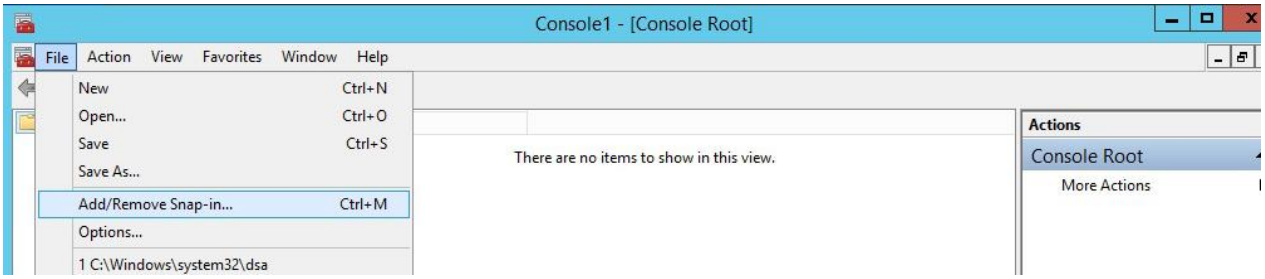

DHCP
File Action View Help
DHCP
dc.abcsc.lk
IPv4
Scope
Server
Policie
Filters
IPv6
Contents of DHCP Server
Scope [192.168.0.0] WIFI
Server Options
Policies
Filters
Actions
IPv4
More Actions

Figure 37 – 39

Implementing RADIUS Configuration







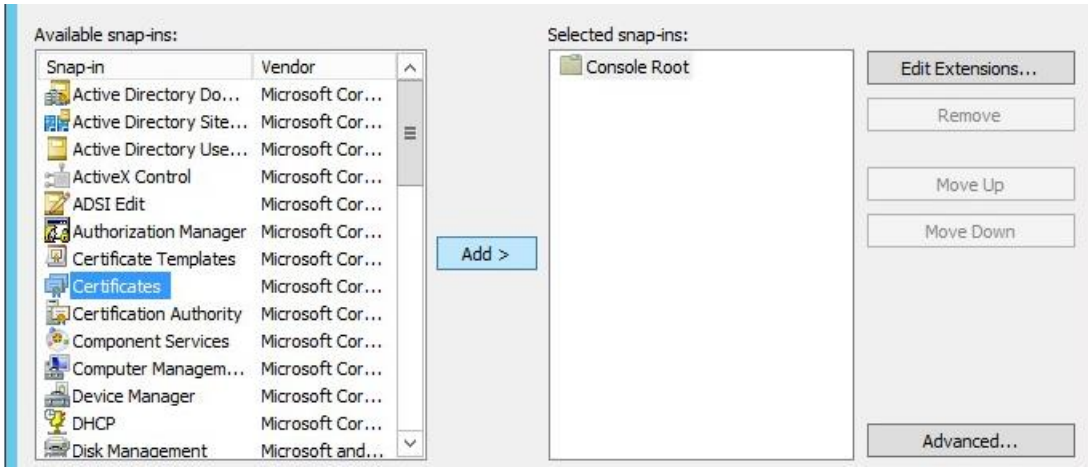
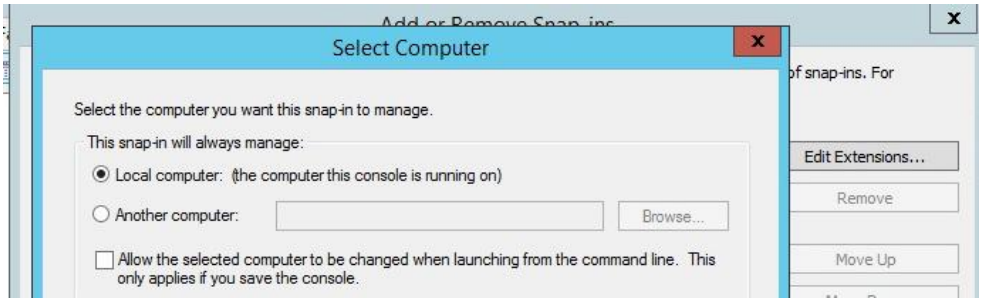


Figure 40 – 43


Certificates snap-in
This snap-in will always manage certificates for:
My user account
Service account
Computer account
Edit Extensions...
Remove
Move Up
Move Down


Select Computer
Select the computer you want this snap-in to manage.
This snap-in will always manage:
Local computer: (the computer this console is running on)
Another computer:
Browse...
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.
Edit Extensions...
Remove
Move Up

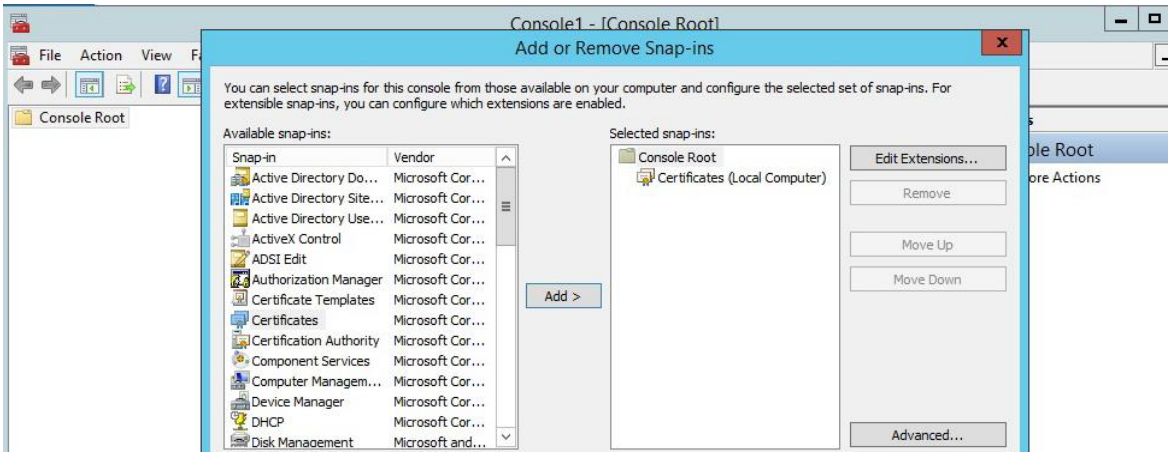

Console1 - [Console Root]
File Action View
Console Root
Add or Remove Snap-ins
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.
Available snap-ins:
Snap-in
Vendor
Active Directory Do...
Active Directory Site...
Active Directory Use...
ActiveX Control
ADSI Edit
Authorization Manager
Certificate Templates
Certificates
Certification Authority
Component Services
Computer Managem...
Device Manager
DHCP
Disk Management
Microsoft Cor...
Microsoft and...
Add >
Selected snap-ins:
Console Root
Certificates (Local Computer)
Edit Extensions...
Remove
Move Up
Move Down
Advanced...

Figure 44 – 46

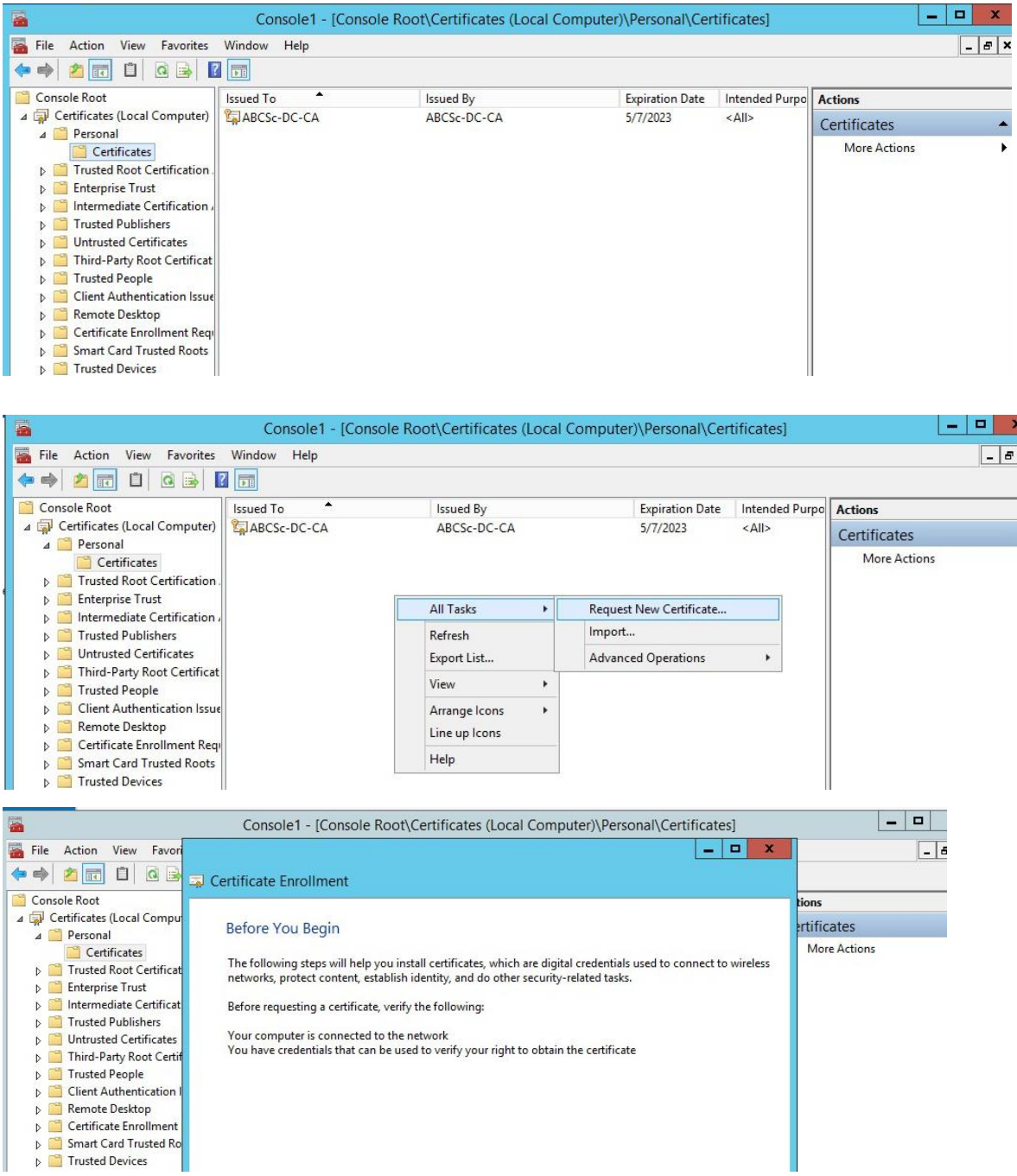
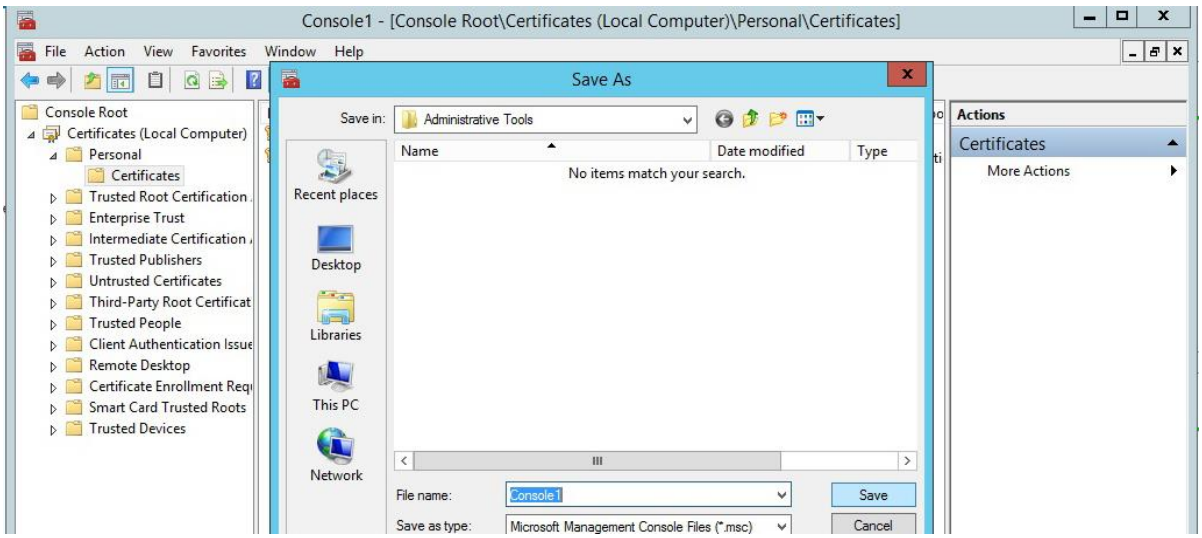

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issue
Remote Desktop
Certificate Enrollment Req
Smart Card Trusted Roots
Trusted Devices
Issued To
Issued By
Expiration Date
Intended Purpo
ABCSc-DC-CA
ABCSc-DC-CA
5/7/2023
<All>
Actions
Certificates
More Actions
All Tasks
Refresh
Export List...
View
Arrange Icons
Line up Icons
Help
Request New Certificate...
Import...
Advanced Operations
Certificate Enrollment
Before You Begin
The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.
Before requesting a certificate, verify the following:
Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate

Figure 47 – 49


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issue
Remote Desktop
Certificate Enrollment Req
Smart Card Trusted Roots
Trusted Devices
Save As
Save in: Administrative Tools
Recent places
Desktop
Libraries
This PC
Network
Name
Date modified
Type
No items match your search.
File name: Console1
Save as type: Microsoft Management Console Files (*.msc)
Save
Cancel
Actions
Certificates
More Actions


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
Certificate Enrollment
Select Certificate Enrollment Policy
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates.
Certificate enrollment policy may already be configured for you.
Configured by your administrator
Active Directory Enrollment Policy
Configured by you
Add New
Actions
More Actions

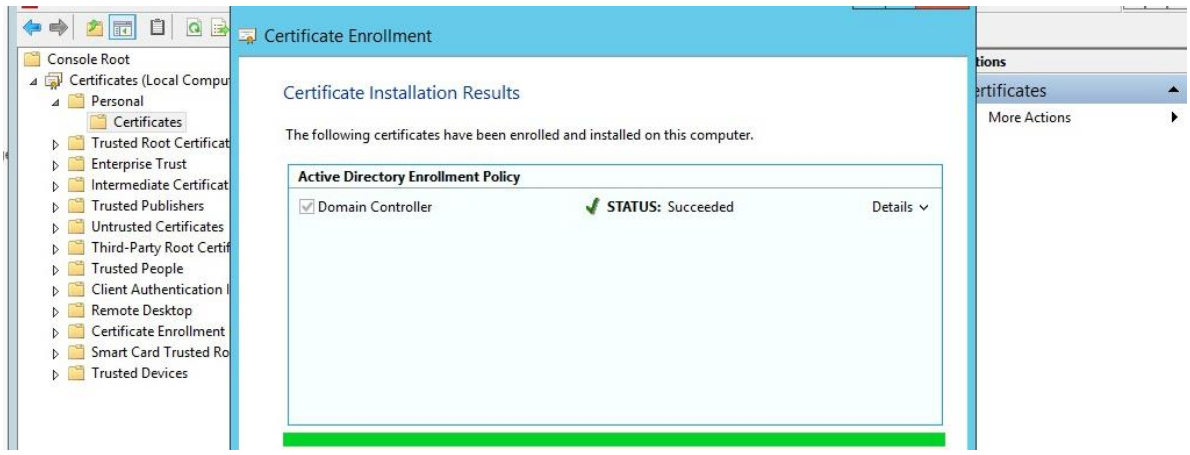
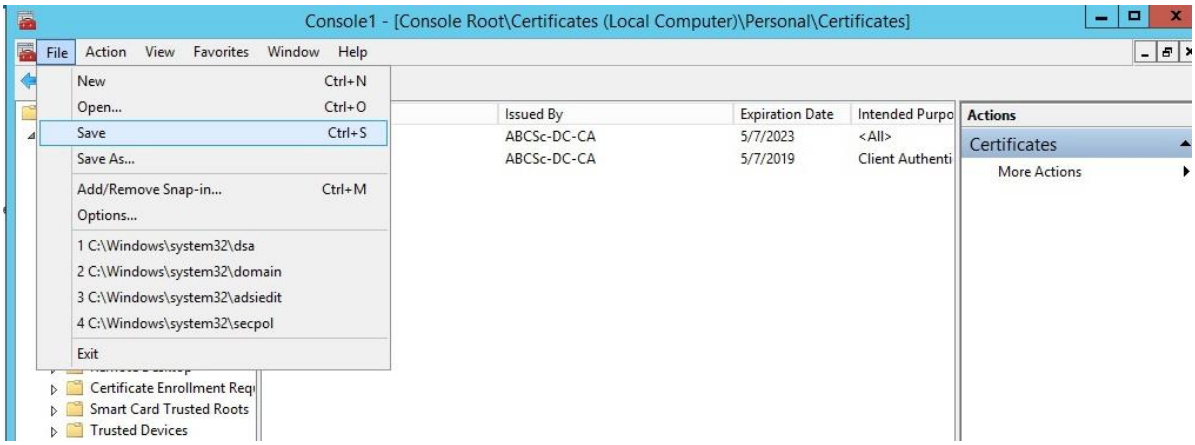
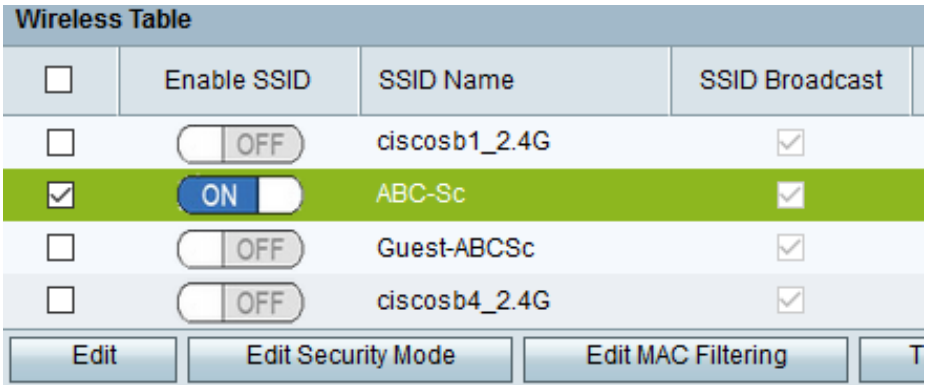

Certificate Enrollment
Certificate Installation Results
The following certificates have been enrolled and installed on this computer.
Active Directory Enrollment Policy
Domain Controller
STATUS: Succeeded
Details
More Actions

Figure 50 - 52


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\system32\dsa
2 C:\Windows\system32\domain
3 C:\Windows\system32\adsiedit
4 C:\Windows\system32\secpol
Exit
Issued By
Expiration Date
Intended Purpo
ABCSc-DC-CA
5/7/2023
<All>
ABCSc-DC-CA
5/7/2019
Client Authenti
Actions
Certificates
More Actions
Certificate Enrollment Req
Smart Card Trusted Roots
Trusted Devices


Wireless Table
Enable SSID
SSID Name
SSID Broadcast
OFF
ciscosb1_2.4G
ON
ABC-Sc
OFF
Guest-ABCSc
OFF
ciscosb4_2.4G
Edit
Edit Security Mode
Edit MAC Filtering

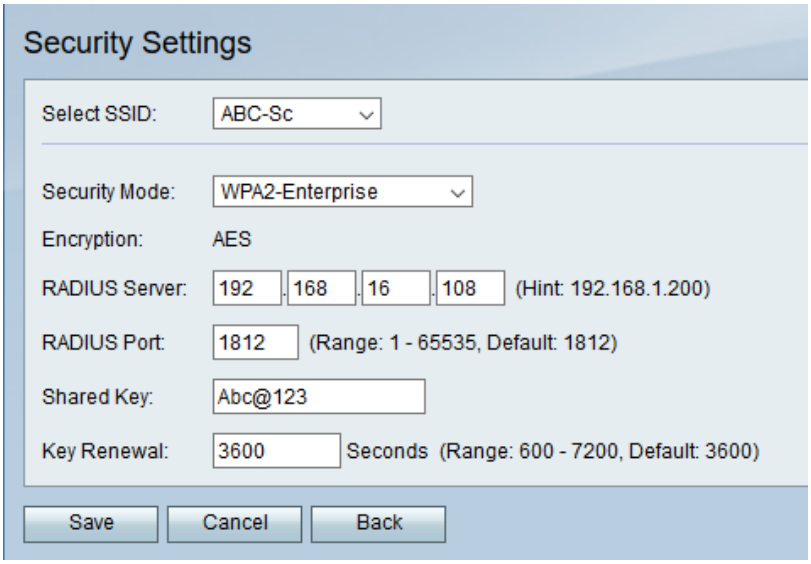

Security Settings
Select SSID:
ABC-Sc
Security Mode:
WPA2-Enterprise
Encryption:
AES
RADIUS Server:
192
168
16
108
(Hint: 192.168.1.200)
RADIUS Port:
1812
(Range: 1 - 65535, Default: 1812)
Shared Key:
Abc@123
Key Renewal:
3600
Seconds (Range: 600 - 7200, Default: 3600)
Save
Cancel
Back

Figure 53 – 55

Implementing WDS

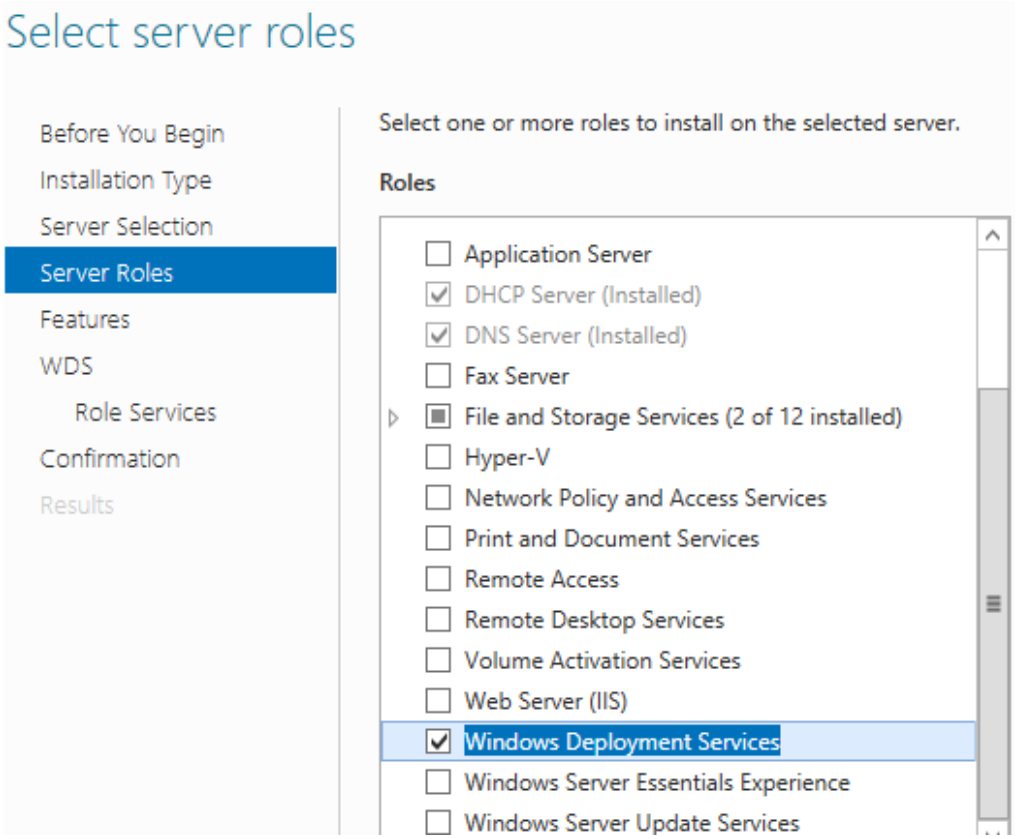
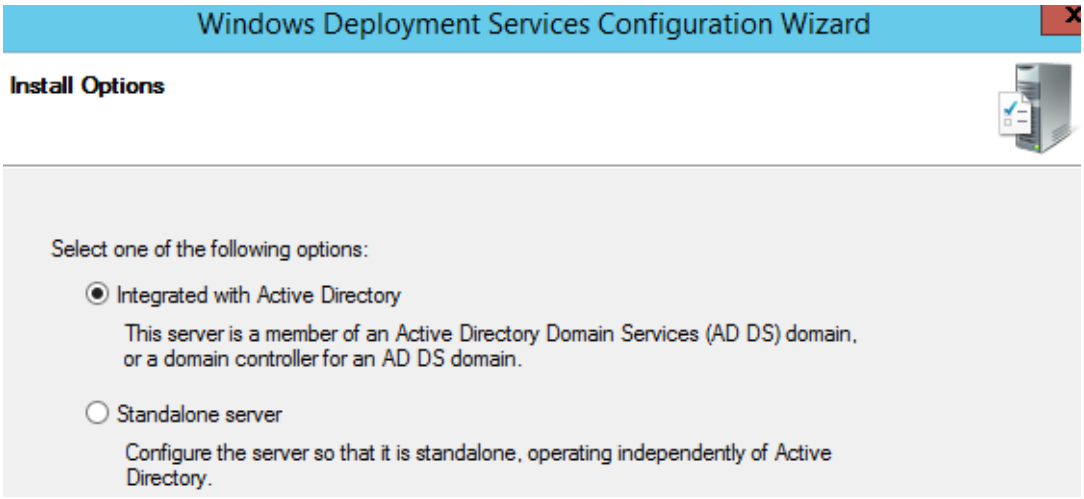
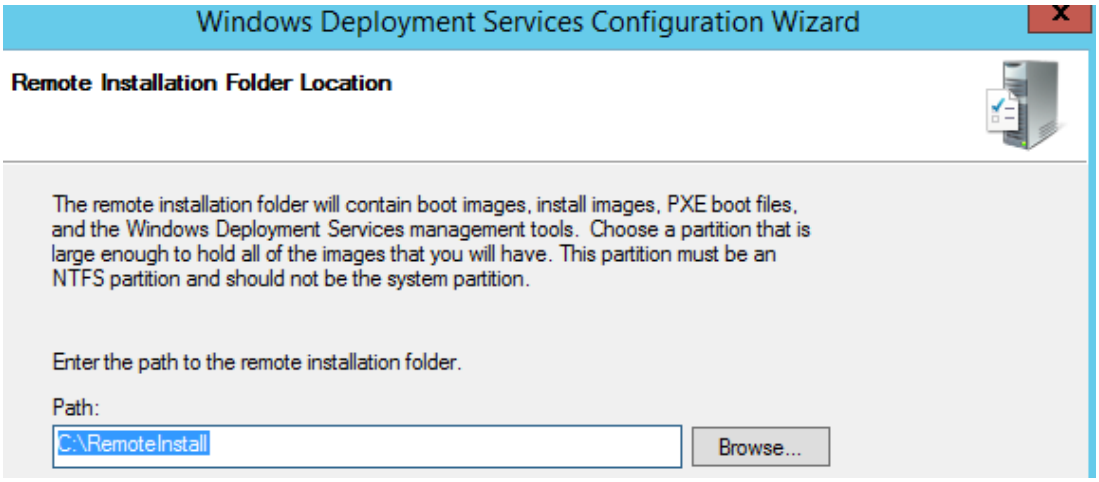


Figure 56 – 57


Windows Deployment Services Configuration Wizard
Install Options
Select one of the following options:
Integrated with Active Directory
This server is a member of an Active Directory Domain Services (AD DS) domain, or a domain controller for an AD DS domain.
Standalone server
Configure the server so that it is standalone, operating independently of Active Directory.


Windows Deployment Services Configuration Wizard
Remote Installation Folder Location
The remote installation folder will contain boot images, install images, PXE boot files, and the Windows Deployment Services management tools. Choose a partition that is large enough to hold all of the images that you will have. This partition must be an NTFS partition and should not be the system partition.
Enter the path to the remote installation folder.
Path:
C:\RemoteInstall
Browse...

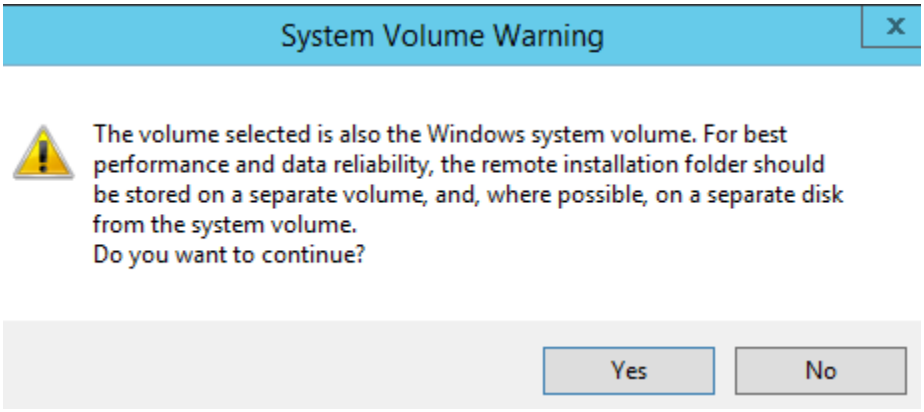
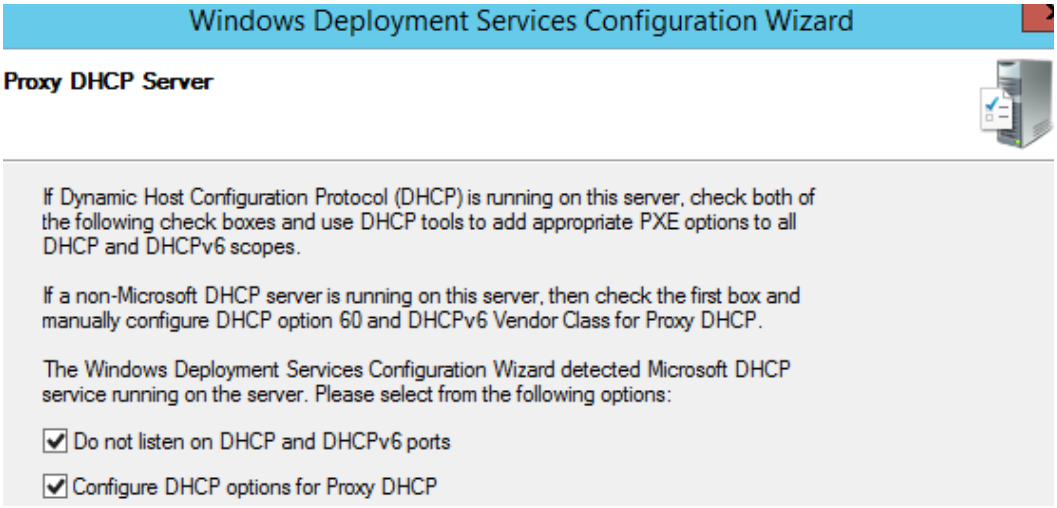
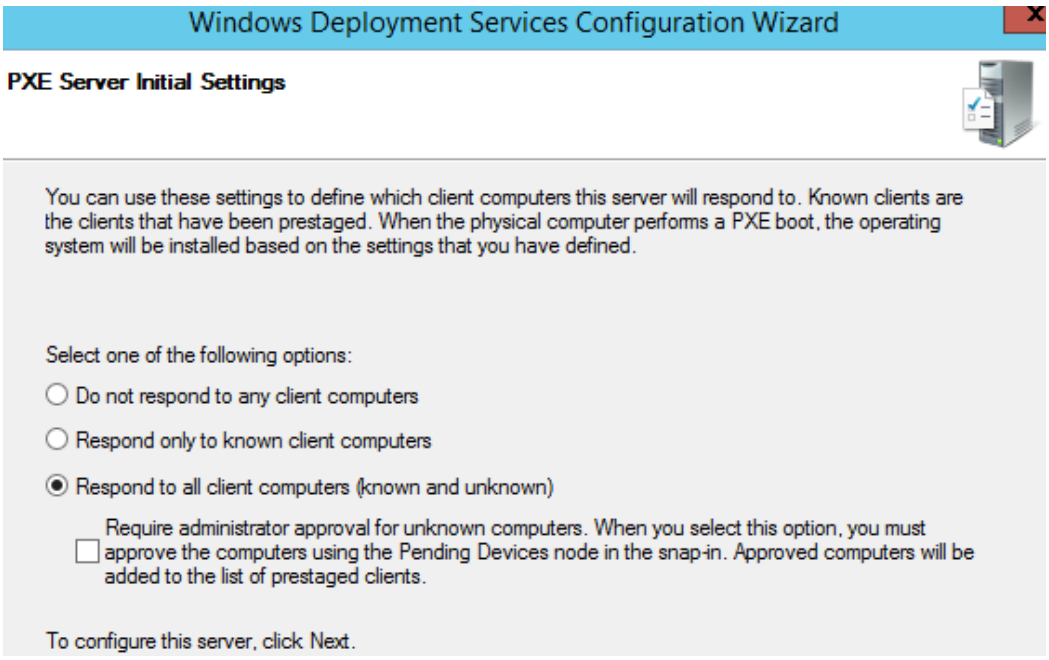

System Volume Warning
The volume selected is also the Windows system volume. For best performance and data reliability, the remote installation folder should be stored on a separate volume, and, where possible, on a separate disk from the system volume.
Do you want to continue?
Yes
No

Figure 58 - 60


Windows Deployment Services Configuration Wizard
Proxy DHCP Server
If Dynamic Host Configuration Protocol (DHCP) is running on this server, check both of the following check boxes and use DHCP tools to add appropriate PXE options to all DHCP and DHCPv6 scopes.
If a non-Microsoft DHCP server is running on this server, then check the first box and manually configure DHCP option 60 and DHCPv6 Vendor Class for Proxy DHCP.
The Windows Deployment Services Configuration Wizard detected Microsoft DHCP service running on the server. Please select from the following options:
Do not listen on DHCP and DHCPv6 ports
Configure DHCP options for Proxy DHCP


Windows Deployment Services Configuration Wizard
PXE Server Initial Settings
You can use these settings to define which client computers this server will respond to. Known clients are the clients that have been prestaged. When the physical computer performs a PXE boot, the operating system will be installed based on the settings that you have defined.
Select one of the following options:
Do not respond to any client computers
Respond only to known client computers
Respond to all client computers (known and unknown)
Require administrator approval for unknown computers. When you select this option, you must approve the computers using the Pending Devices node in the snap-in. Approved computers will be added to the list of prestaged clients.
To configure this server, click Next.

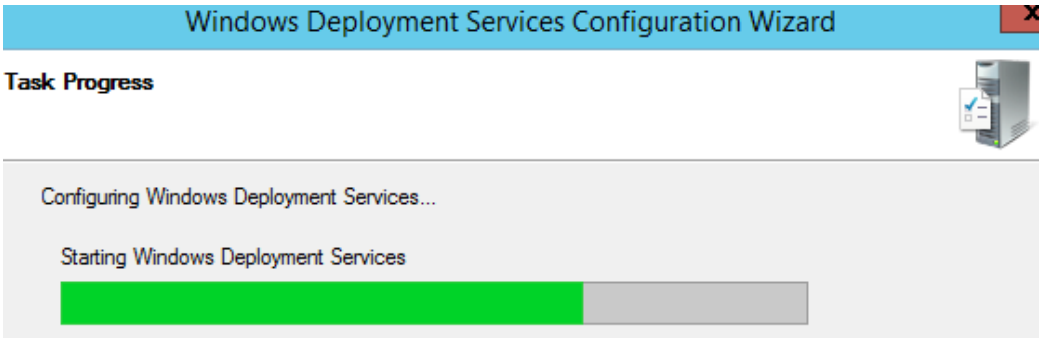
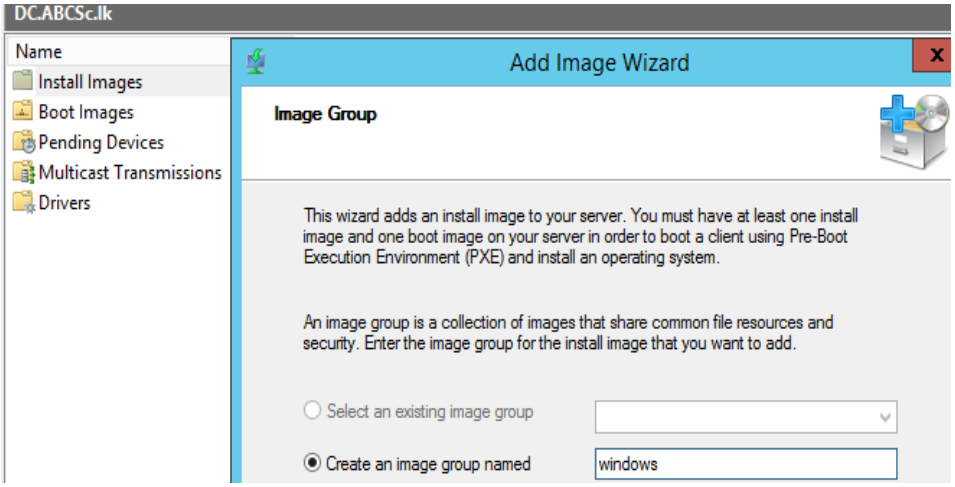

Windows Deployment Services Configuration Wizard
Task Progress
Configuring Windows Deployment Services...
Starting Windows Deployment Services

Figure 61 - 63


DC.ABCSc.lk
Name
Install Images
Boot Images
Pending Devices
Multicast Transmissions
Drivers
Add Image Wizard
Image Group
This wizard adds an install image to your server. You must have at least one install image and one boot image on your server in order to boot a client using Pre-Boot Execution Environment (PXE) and install an operating system.
An image group is a collection of images that share common file resources and security. Enter the image group for the install image that you want to add.
Select an existing image group
Create an image group named
windows


Add Image Wizard
Image File
Enter the location of the Windows image file that contains the images to add.
File location:
D:\sources\install.wim
Browse...
Note: The default boot and install images (Boot.wim and Install.wim) are located on the installation DVD in the \Sources folder.

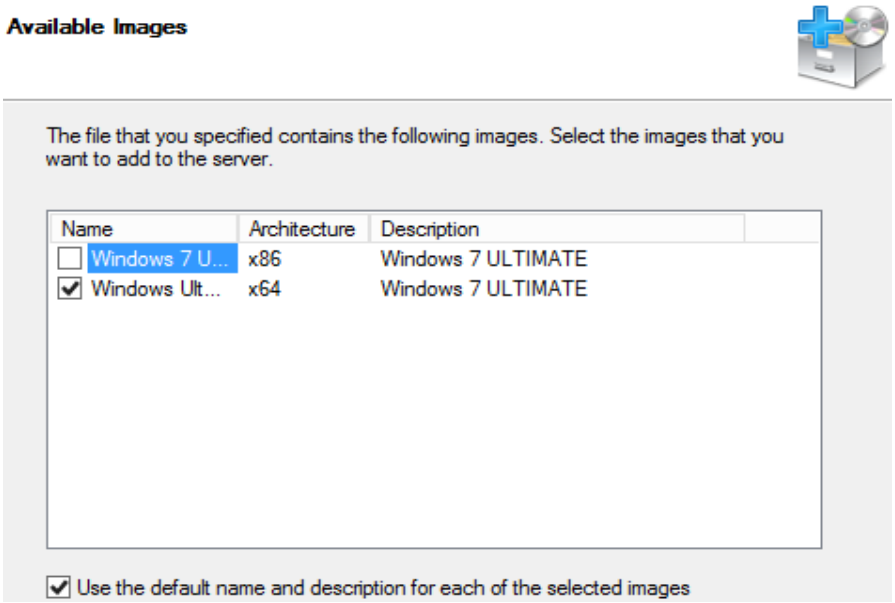

Available Images
The file that you specified contains the following images. Select the images that you want to add to the server.
Name
Architecture
Description
Windows 7 U...
x86
Windows 7 ULTIMATE
Windows Ult...
x64
Windows 7 ULTIMATE
Use the default name and description for each of the selected images

Figure 64 - 67

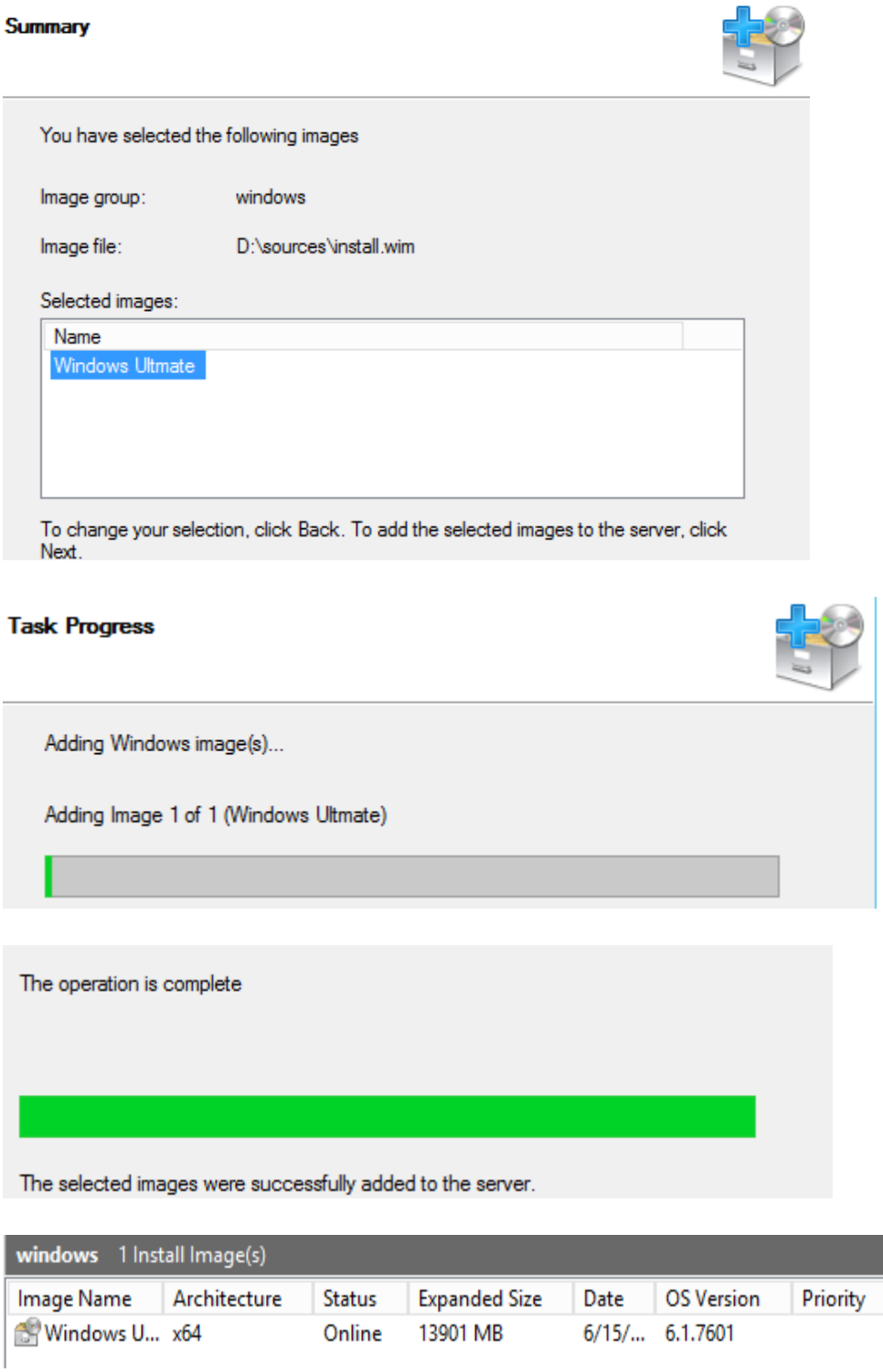

Summary
You have selected the following images
Image group: windows
Image file: D:\sources\install.wim
Selected images:
Name
Windows Ultmate
To change your selection, click Back. To add the selected images to the server, click Next.
Task Progress
Adding Windows image(s)...
Adding Image 1 of 1 (Windows Ultmate)
The operation is complete
The selected images were successfully added to the server.
windows 1 Install Image(s)
Image Name Architecture Status Expanded Size Date OS Version Priority
Windows U... x64 Online 13901 MB 6/15/... 6.1.7601

Figure 68 - 71

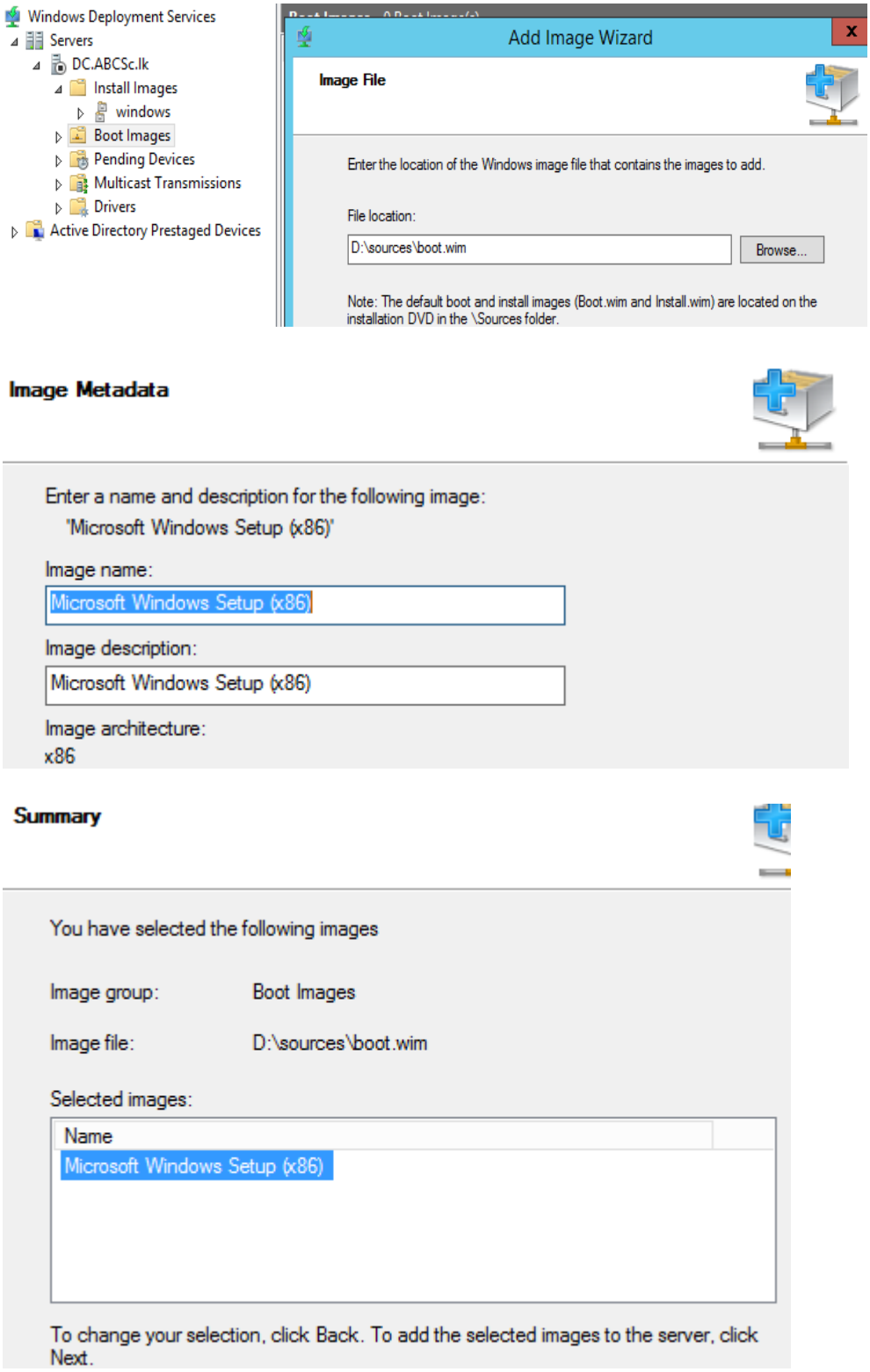
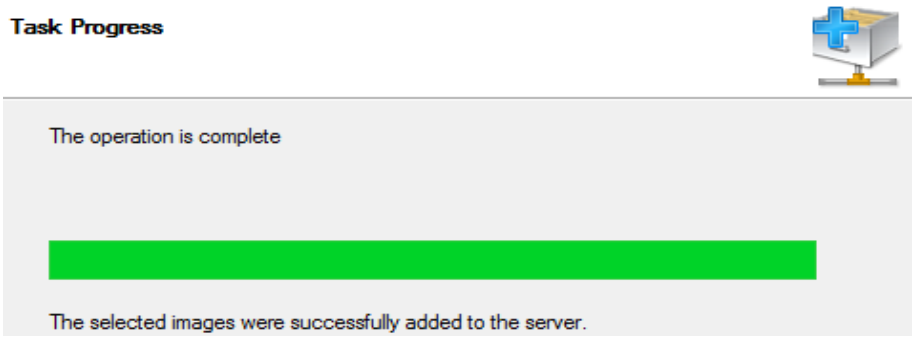
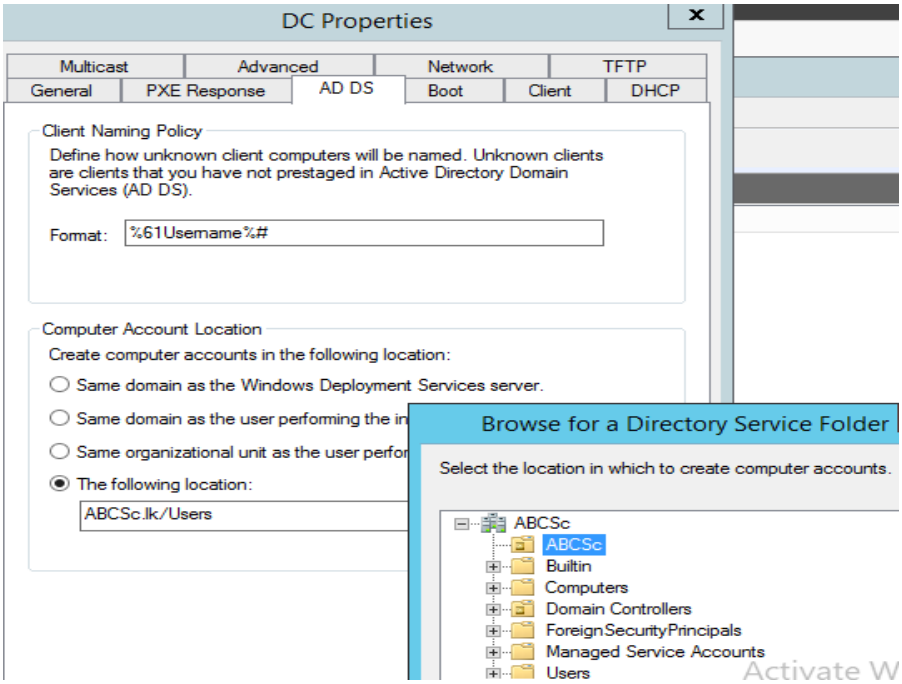

Windows Deployment Services
Servers
DC.ABCSc.lk
Install Images
windows
Boot Images
Pending Devices
Multicast Transmissions
Drivers
Active Directory Prestaged Devices
Add Image Wizard
Image File
Enter the location of the Windows image file that contains the images to add.
File location:
D:\sources\boot.wim
Browse...
Note: The default boot and install images (Boot.wim and Install.wim) are located on the installation DVD in the \Sources folder.
Image Metadata
Enter a name and description for the following image:
'Microsoft Windows Setup (x86)'
Image name:
Microsoft Windows Setup (x86)
Image description:
Microsoft Windows Setup (x86)
Image architecture:
x86
Summary
You have selected the following images
Image group:
Boot Images
Image file:
D:\sources\boot.wim
Selected images:
Name
Microsoft Windows Setup (x86)
To change your selection, click Back. To add the selected images to the server, click Next.

Figure 72 - 74


Task Progress
The operation is complete
The selected images were successfully added to the server.


DC Properties
Multicast
Advanced
Network
TFTP
General
PXE Response
AD DS
Boot
Client
DHCP
Client Naming Policy
Define how unknown client computers will be named. Unknown clients are clients that you have not prestaged in Active Directory Domain Services (AD DS).
Format:
%61Username%#
Computer Account Location
Create computer accounts in the following location:
Same domain as the Windows Deployment Services server.
Same domain as the user performing the in
Same organizational unit as the user perfor
The following location:
ABCSc.lk/Users
Browse for a Directory Service Folder
Select the location in which to create computer accounts.
ABCSc
ABCSc
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Activate W

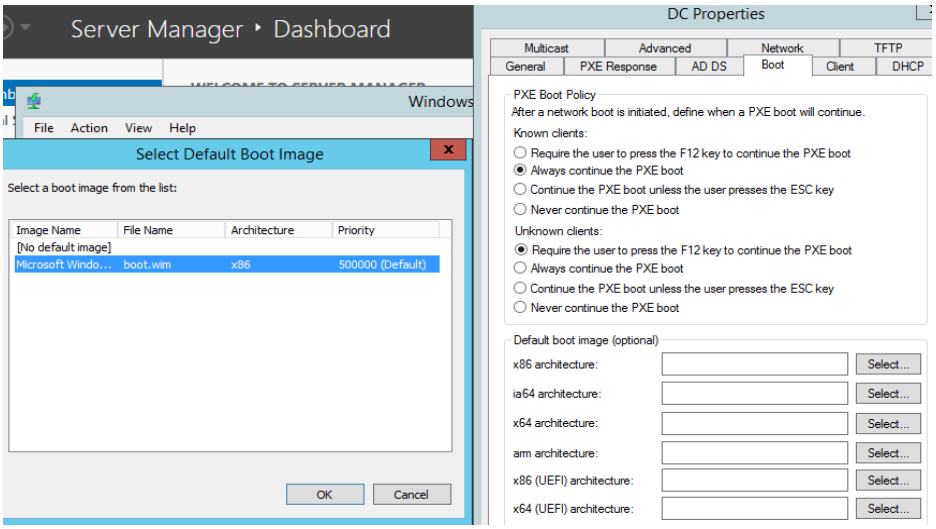
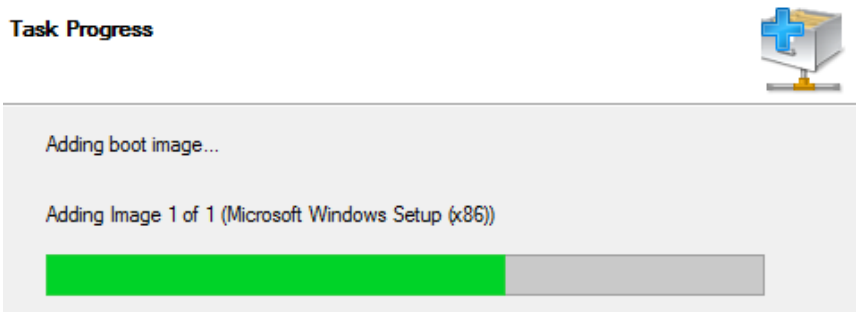
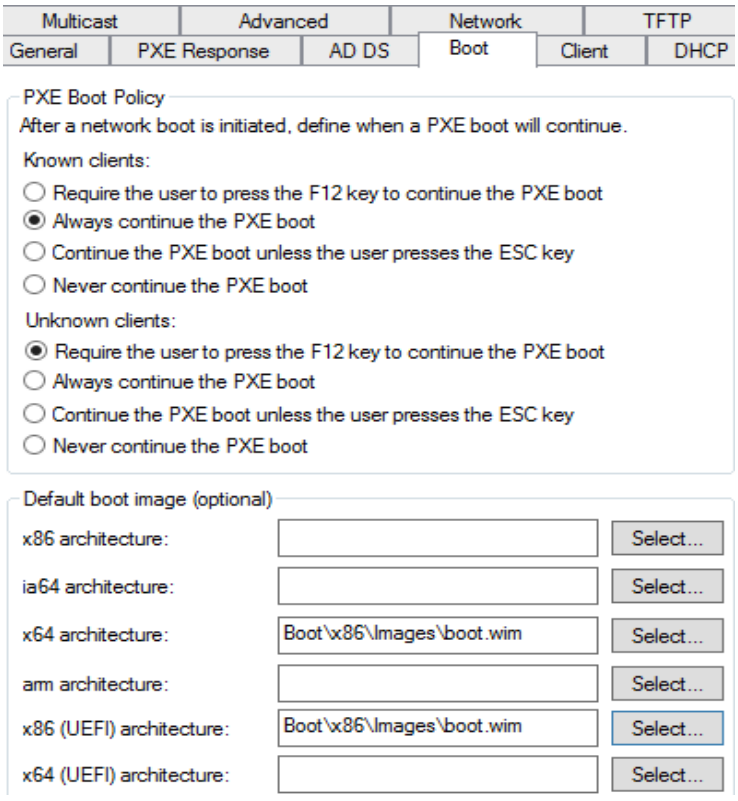

Server Manager ‣ Dashboard
Windows
File Action View Help
Select Default Boot Image
Select a boot image from the list:
Image Name
File Name
Architecture
Priority
[No default image]
Microsoft Windo...
boot.wim
x86
500000 (Default)
OK
Cancel
DC Properties
Multicast
Advanced
Network
TFTP
General
PXE Response
AD DS
Boot
Client
DHCP
PXE Boot Policy
After a network boot is initiated, define when a PXE boot will continue.
Known clients:
Require the user to press the F12 key to continue the PXE boot
Always continue the PXE boot
Continue the PXE boot unless the user presses the ESC key
Never continue the PXE boot
Unknown clients:
Require the user to press the F12 key to continue the PXE boot
Always continue the PXE boot
Continue the PXE boot unless the user presses the ESC key
Never continue the PXE boot
Default boot image (optional)
x86 architecture:
ia64 architecture:
x64 architecture:
arm architecture:
x86 (UEFI) architecture:
x64 (UEFI) architecture:
Select...

Figure 75 - 77


Task Progress
Adding boot image...
Adding Image 1 of 1 (Microsoft Windows Setup (x86))


Multicast
Advanced
Network
TFTP
General
PXE Response
AD DS
Boot
Client
DHCP
PXE Boot Policy
After a network boot is initiated, define when a PXE boot will continue.
Known clients:
Require the user to press the F12 key to continue the PXE boot
Always continue the PXE boot
Continue the PXE boot unless the user presses the ESC key
Never continue the PXE boot
Unknown clients:
Require the user to press the F12 key to continue the PXE boot
Always continue the PXE boot
Continue the PXE boot unless the user presses the ESC key
Never continue the PXE boot
Default boot image (optional)
x86 architecture:
Select...
ia64 architecture:
Select...
x64 architecture:
Boot\x86\Images\boot.wim
Select...
arm architecture:
Select...
x86 (UEFI) architecture:
Boot\x86\Images\boot.wim
Select...
x64 (UEFI) architecture:
Select...

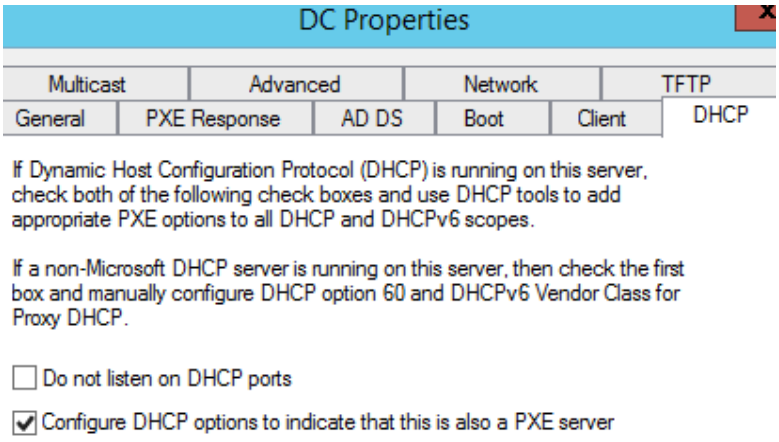
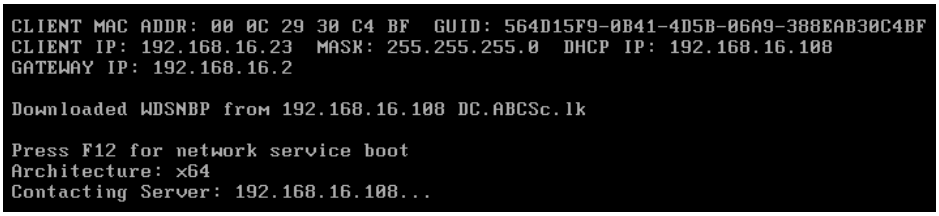
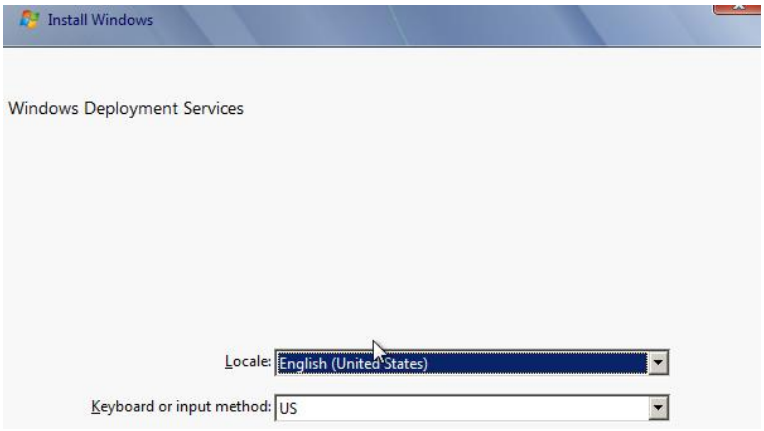

DC Properties
Multicast
Advanced
Network
TFTP
General
PXE Response
AD DS
Boot
Client
DHCP
If Dynamic Host Configuration Protocol (DHCP) is running on this server, check both of the following check boxes and use DHCP tools to add appropriate PXE options to all DHCP and DHCPv6 scopes.
If a non-Microsoft DHCP server is running on this server, then check the first box and manually configure DHCP option 60 and DHCPv6 Vendor Class for Proxy DHCP.
Do not listen on DHCP ports
Configure DHCP options to indicate that this is also a PXE server

Figure 78 – 80


Network boot from Intel E1000
Copyright (C) 2003-2014 VMware, Inc.
Copyright (C) 1997-2000 Intel Corporation
CLIENT MAC ADDR: 00 0C 29 30 C4 BF GUID: 564D15F9-0B41-4D5B-06A9-388EAB30C4BF
DHCP...


CLIENT MAC ADDR: 00 0C 29 30 C4 BF GUID: 564D15F9-0B41-4D5B-06A9-388EAB30C4BF
CLIENT IP: 192.168.16.23 MASK: 255.255.255.0 DHCP IP: 192.168.16.108
GATEWAY IP: 192.168.16.2
Downloaded WDSNBP from 192.168.16.108 DC.ABCSc.lk
Press F12 for network service boot
Architecture: x64
Contacting Server: 192.168.16.108...


Loading files...
IP: 192.168.16.108, File: \Boot\x86\Images\boot.wim


Install Windows
Windows Deployment Services
Locale: English (United States)
Keyboard or input method: US

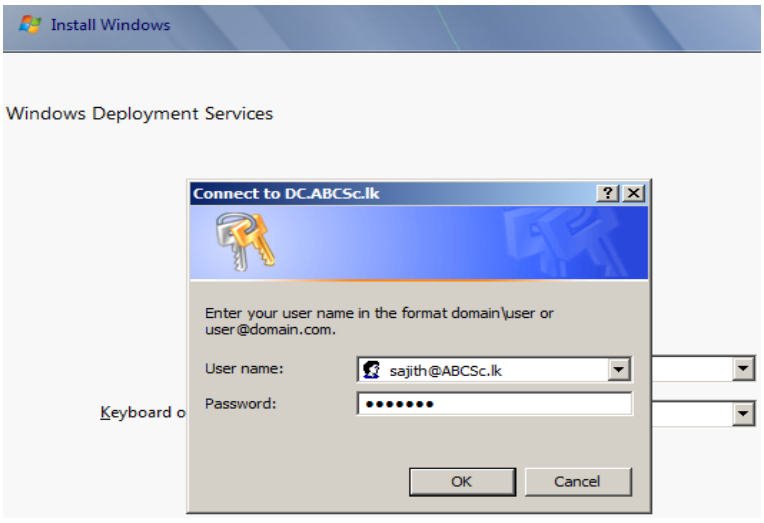
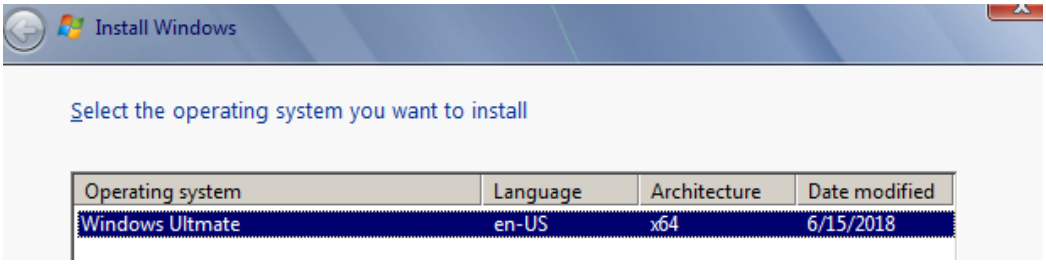
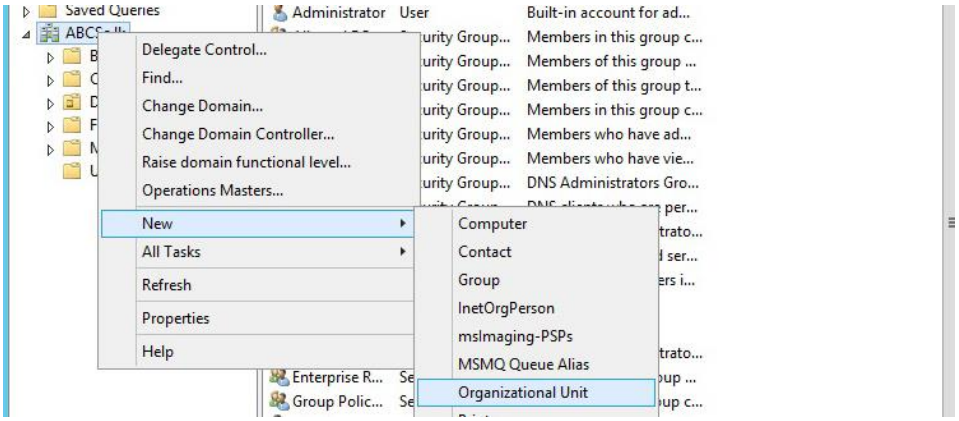

Install Windows
Windows Deployment Services
Connect to DC.ABCSc.lk
Enter your user name in the format domain\user or user@domain.com.
User name: sajith@ABCSc.lk
Password:
OK
Cancel
Keyboard o

Figure 81 - 85



Implementing Organization Unit



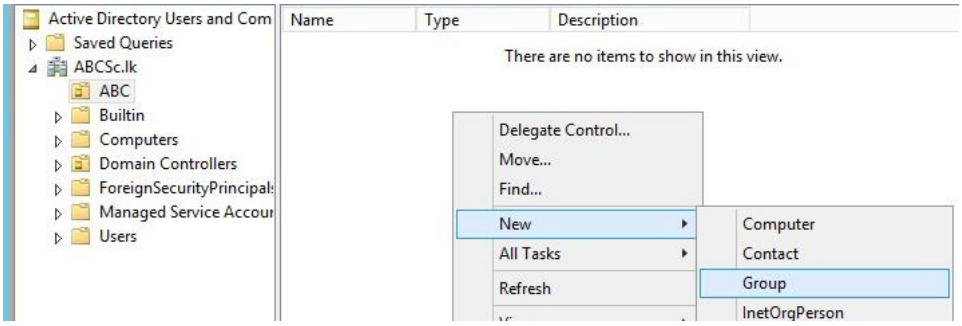
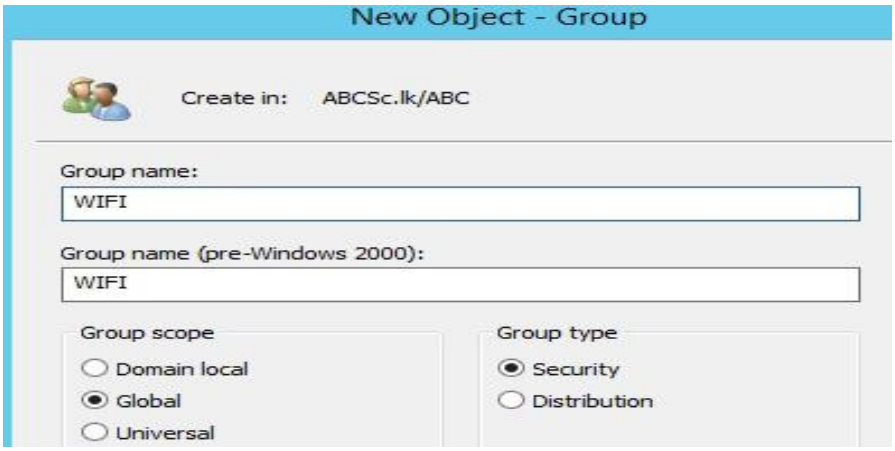
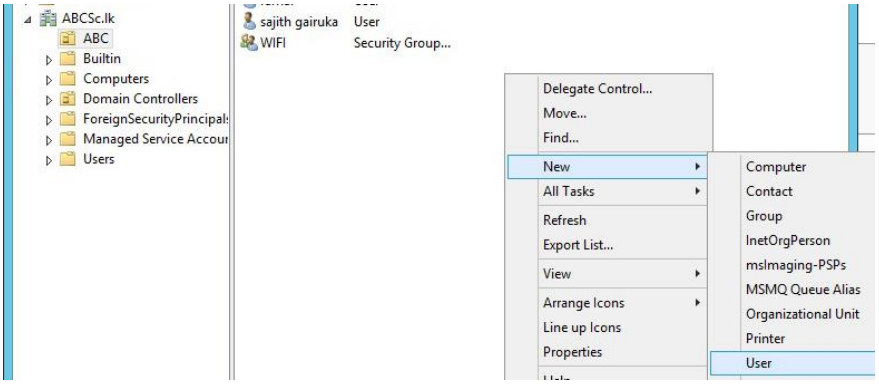


Figure 86 – 89


New Object - Group
Create in: ABCSc.lk/ABC
Group name:
WIFI
Group name (pre-Windows 2000):
WIFI
Group scope
Domain local
Global
Universal
Group type
Security
Distribution


ABCSc.lk
ABC
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
sajith gairuka User
WIFI Security Group...
Delegate Control...
Move...
Find...
New
All Tasks
Refresh
Export List...
View
Arrange Icons
Line up Icons
Properties
Computer
Contact
Group
InetOrgPerson
msImaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
User

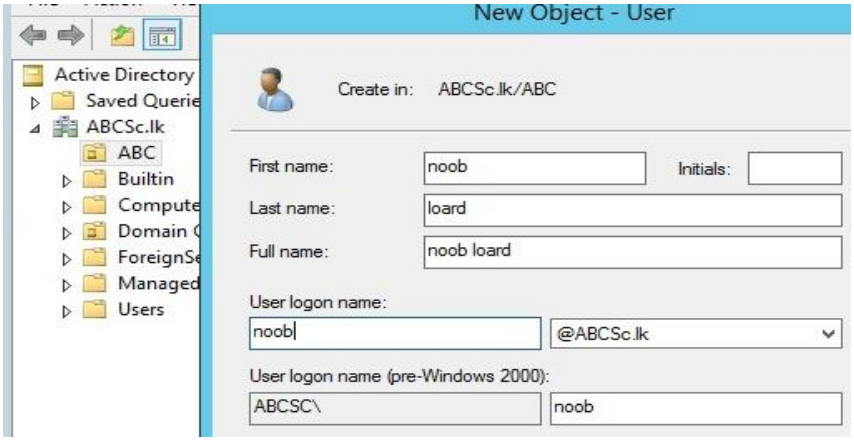

New Object - User
Active Directory
Saved Queries
ABCSc.lk
ABC
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Create in: ABCSc.lk/ABC
First name: noob
Initials:
Last name: loard
Full name: noob loard
User logon name:
noob
@ABCSc.lk
User logon name (pre-Windows 2000):
ABCSC\
noob

Figure 90 - 92

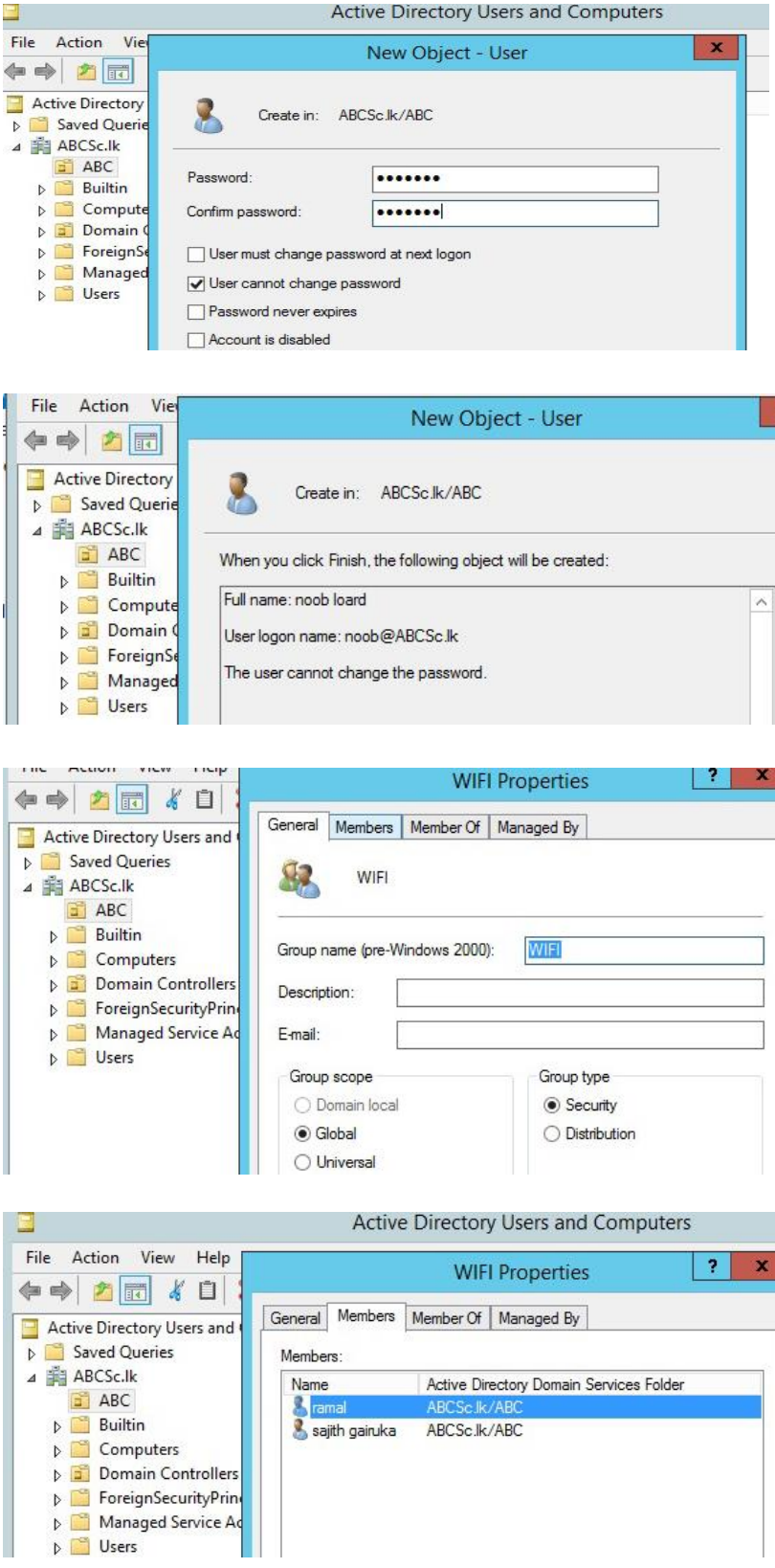

Active Directory Users and Computers
File Action Vie
New Object - User
Create in: ABCSc.lk/ABC
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
Active Directory
Saved Querie
ABCSc.lk
ABC
Builtin
Compute
Domain C
ForeignSe
Managed
Users
File Action Vie
New Object - User
Create in: ABCSc.lk/ABC
When you click Finish, the following object will be created:
Full name: noob loard
User logon name: noob@ABCSc.lk
The user cannot change the password.
Active Directory
Saved Querie
ABCSc.lk
ABC
Builtin
Compute
Domain C
ForeignSe
Managed
Users
WIFI Properties
General
Members
Member Of
Managed By
WIFI
Group name (pre-Windows 2000):
WIFI
Description:
E-mail:
Group scope
Domain local
Global
Universal
Group type
Security
Distribution
Active Directory Users and
Saved Queries
ABCSc.lk
ABC
Builtin
Computers
Domain Controllers
ForeignSecurityPrin
Managed Service Ac
Users
Active Directory Users and Computers
File Action View Help
WIFI Properties
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
ramal
ABCSc.lk/ABC
sajith gairuka
ABCSc.lk/ABC
Active Directory Users and
Saved Queries
ABCSc.lk
ABC
Builtin
Computers
Domain Controllers
ForeignSecurityPrin
Managed Service Ac
Users

Figure 93 - 96

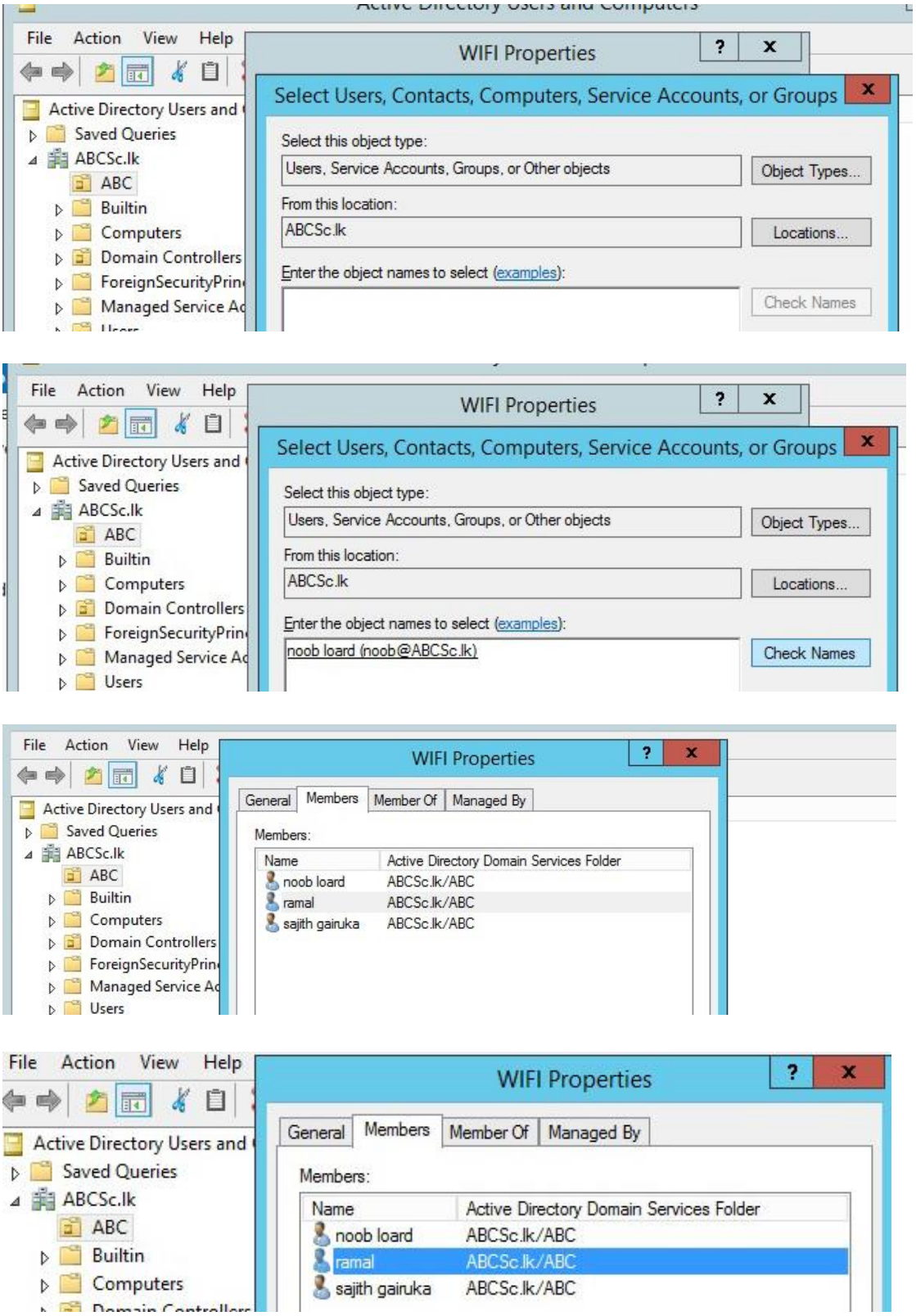
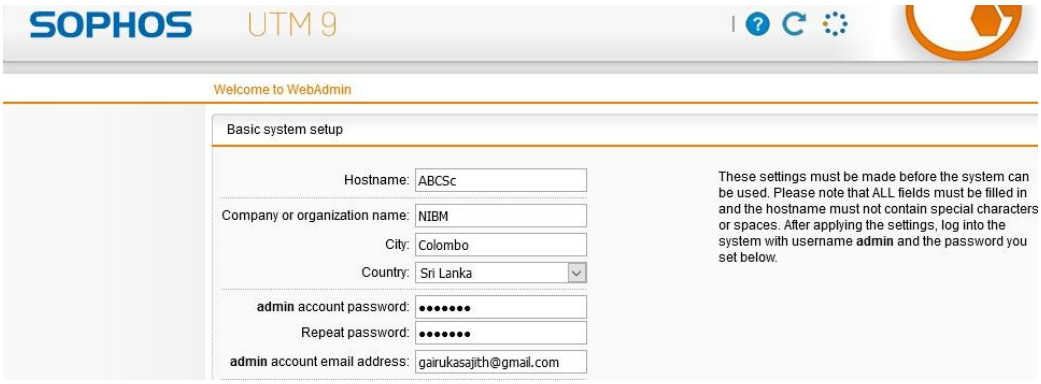
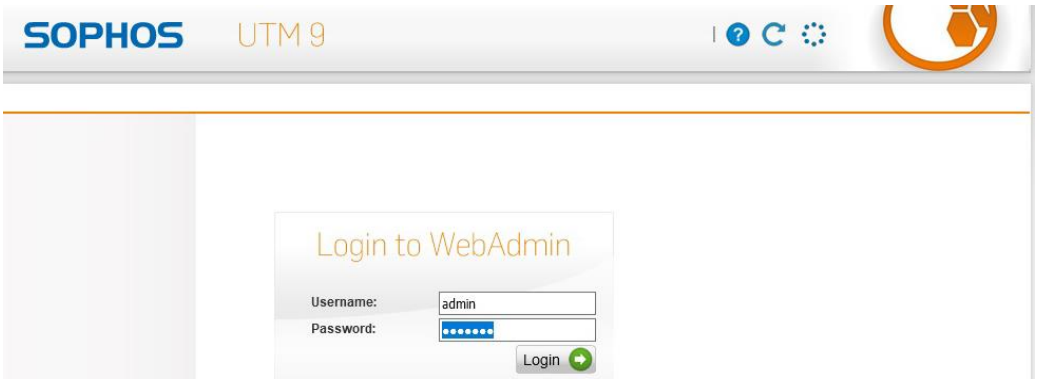
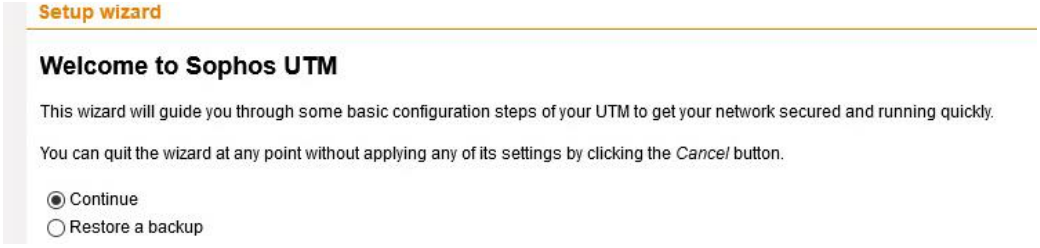


Figure 97 – 100

Implementing Firewall (SOPHOS)







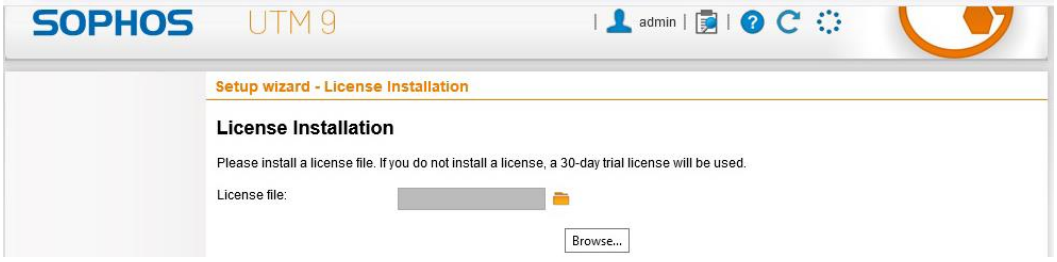


Figure 101 – 104

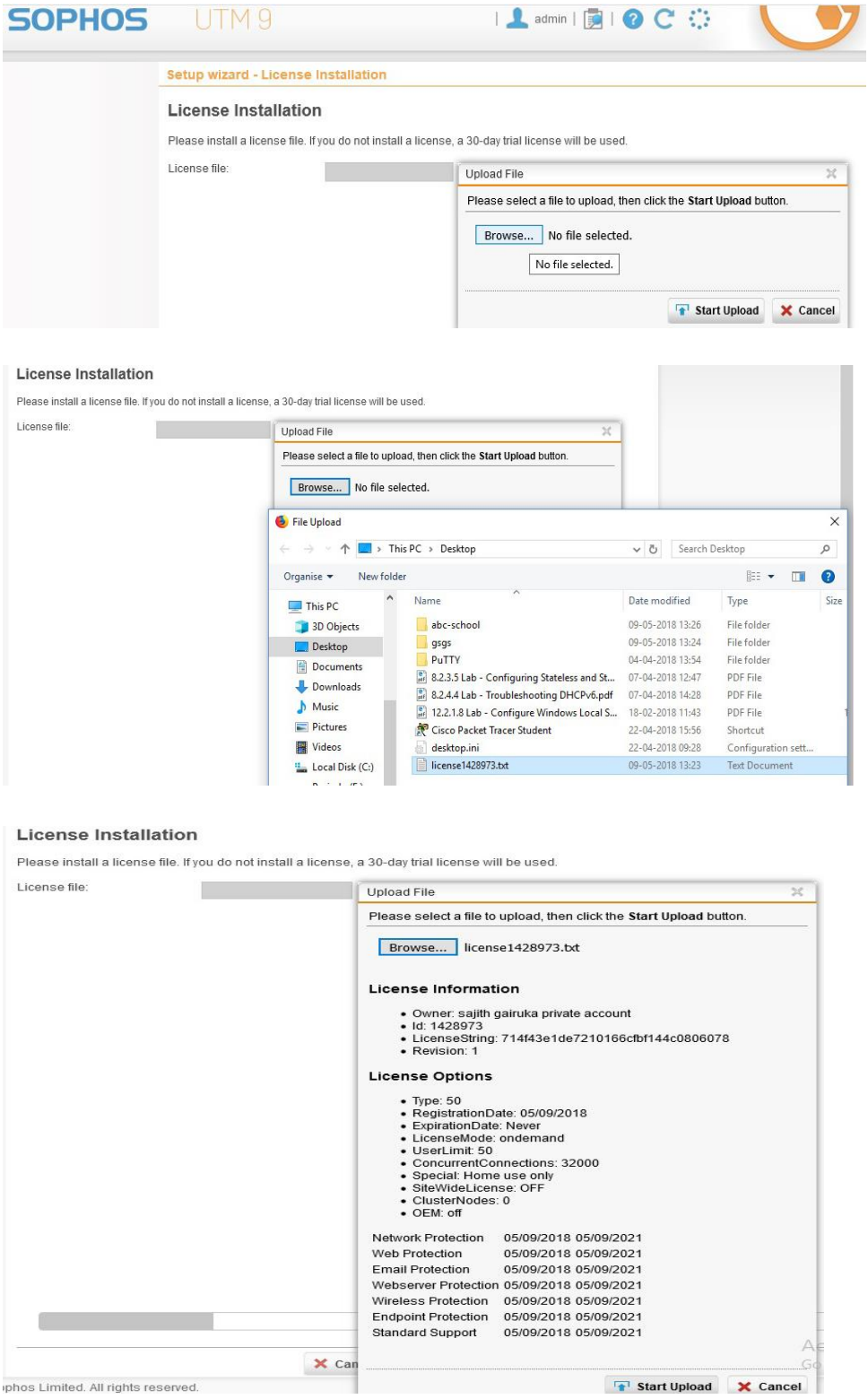
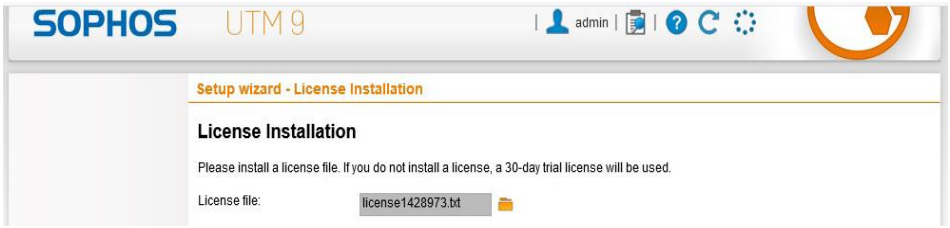
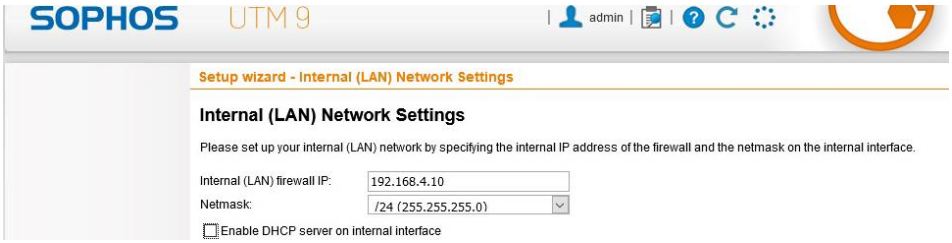
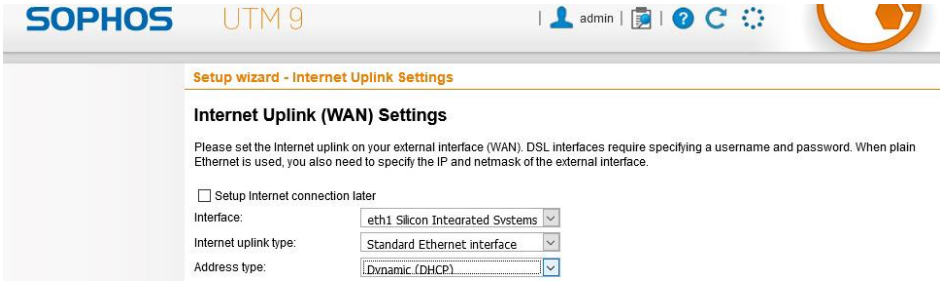
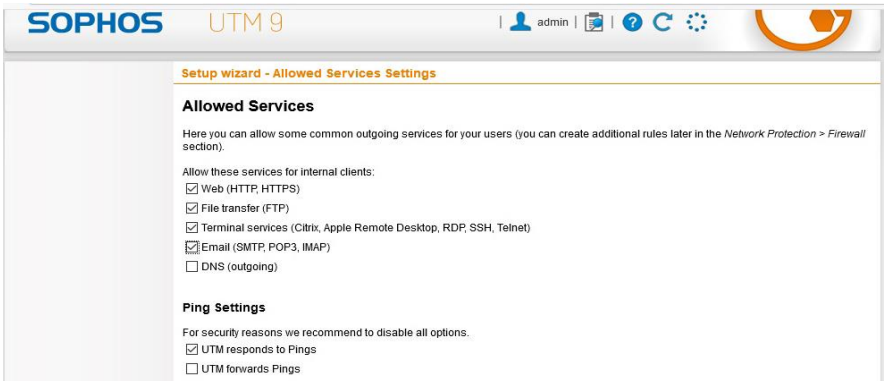


Figure 105 – 107









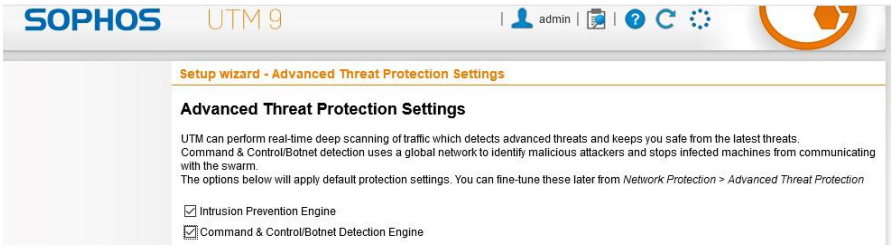
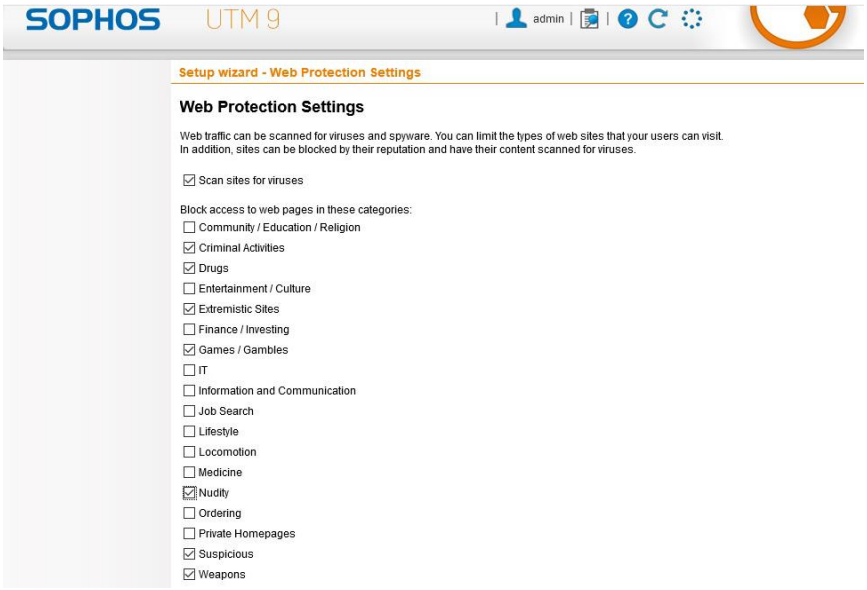
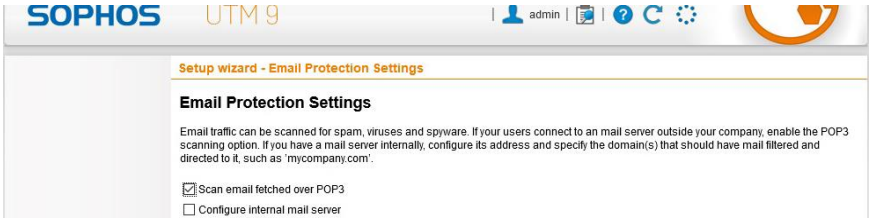
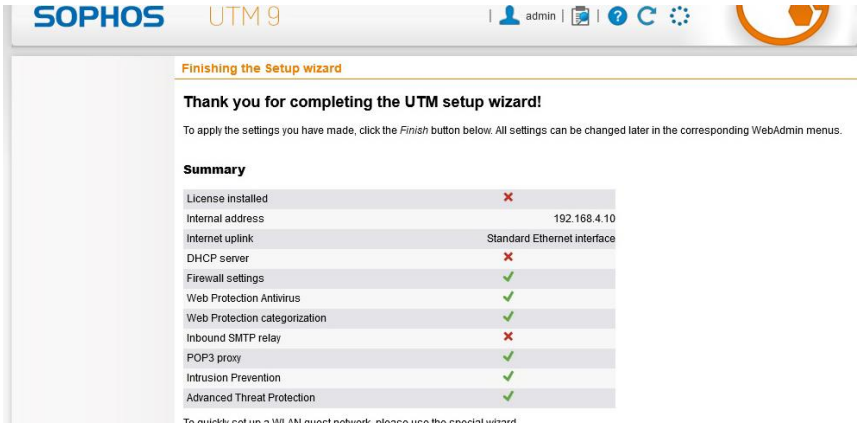


Figure 108 – 111







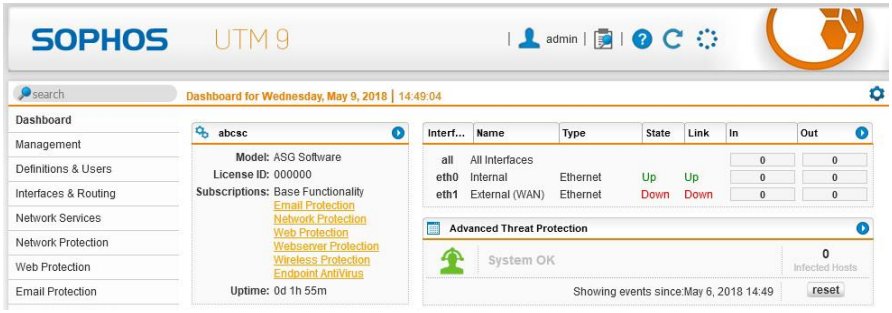
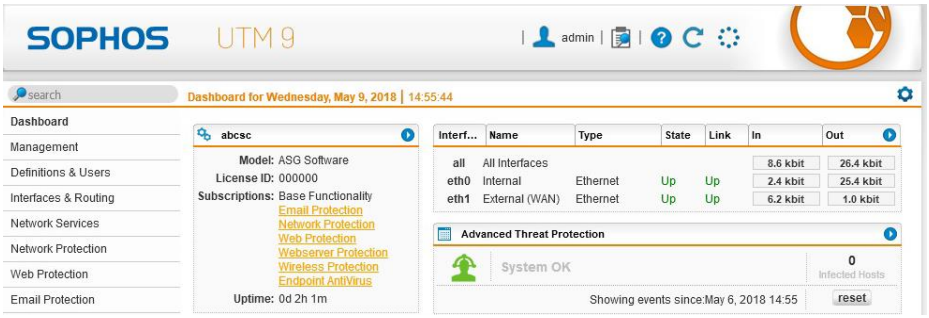
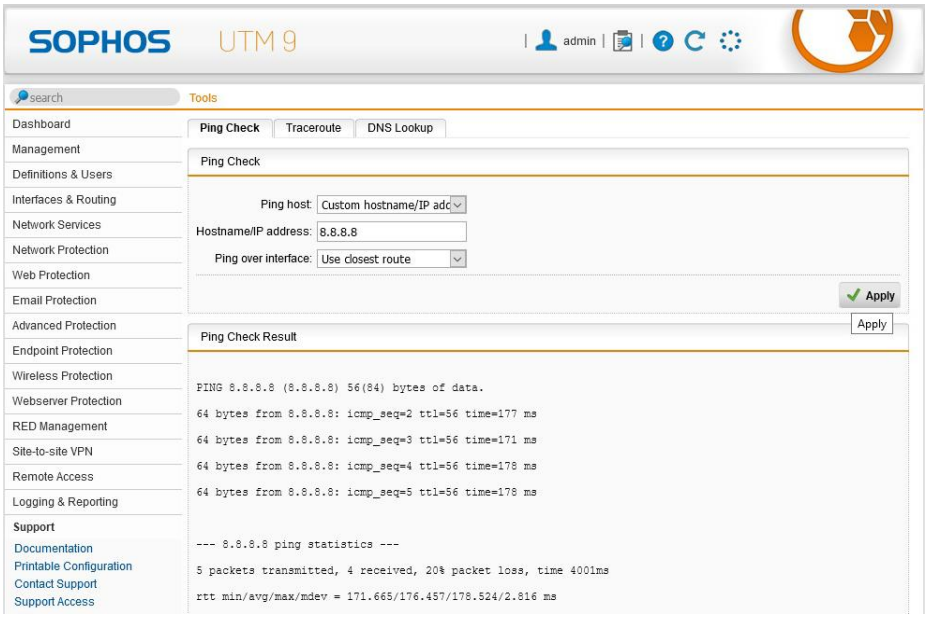


Figure 112 – 115





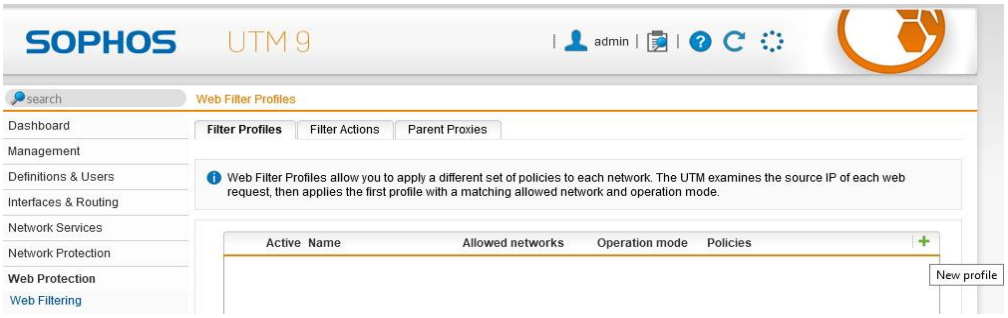
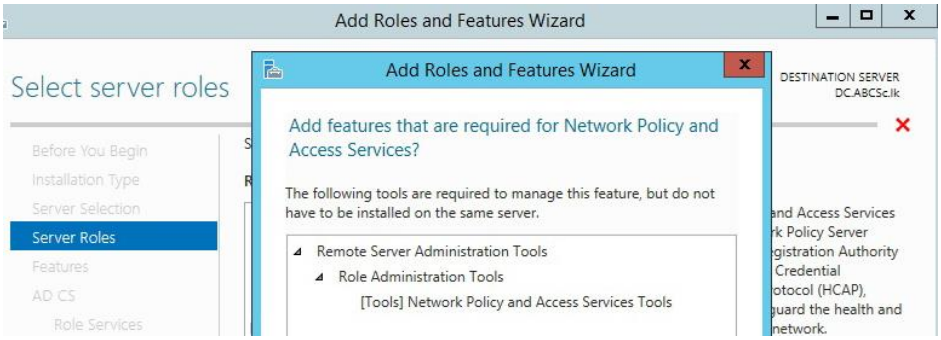


Figure 116 – 119

Implementing Network Access Policy



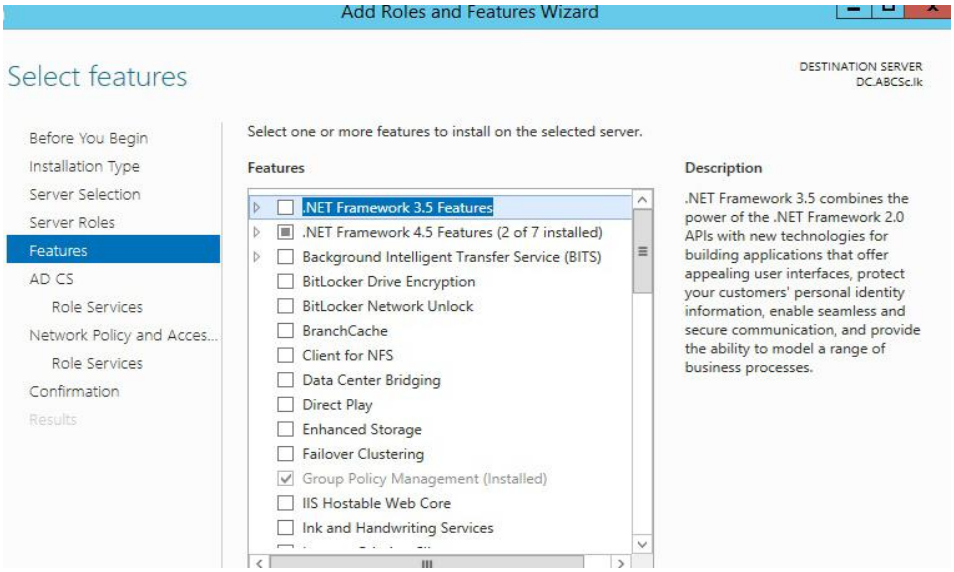
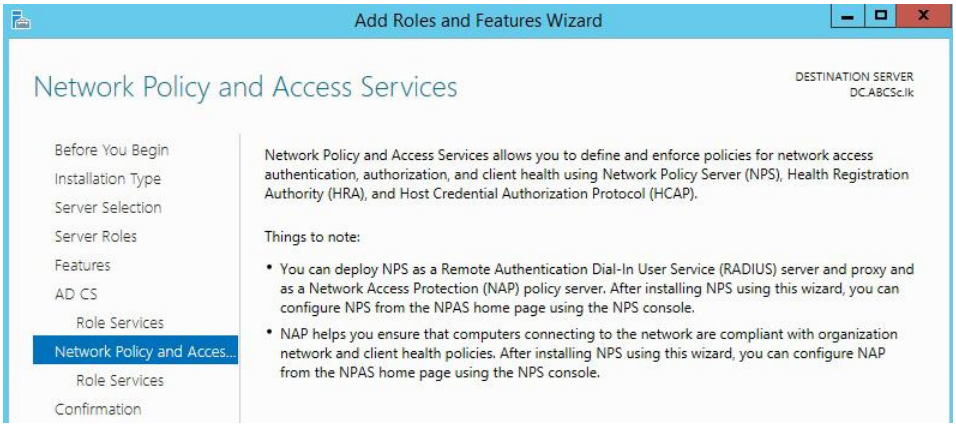
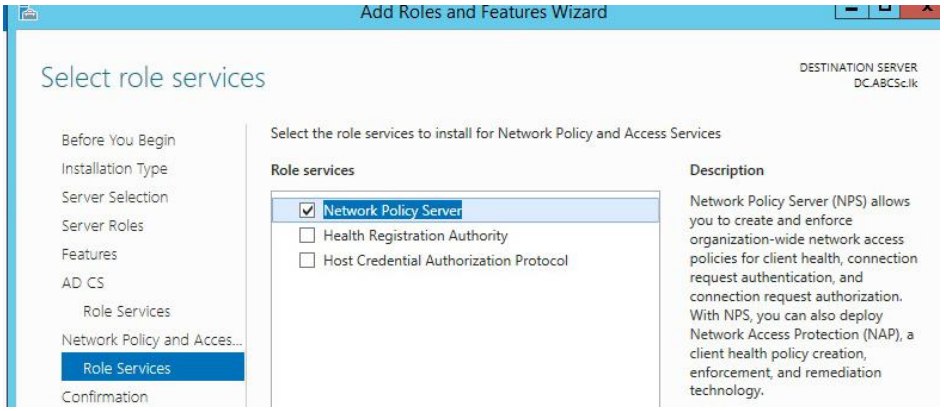


Figure 120 – 122





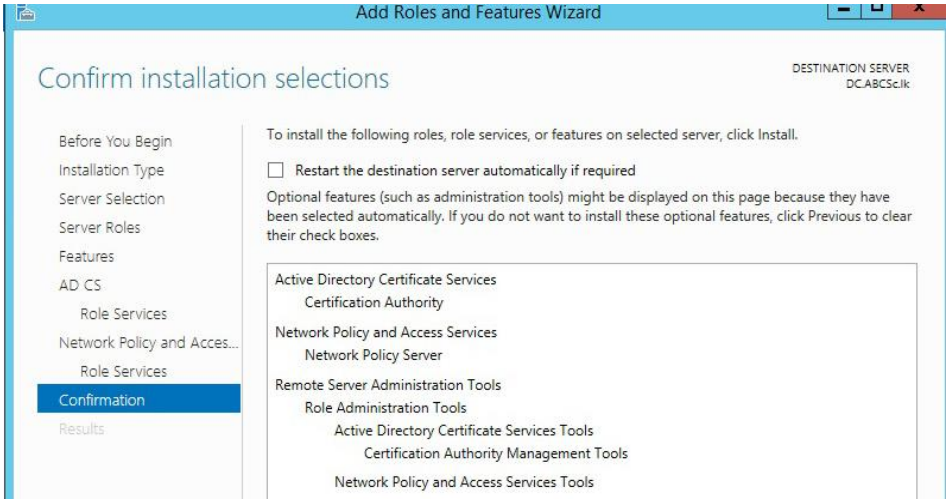
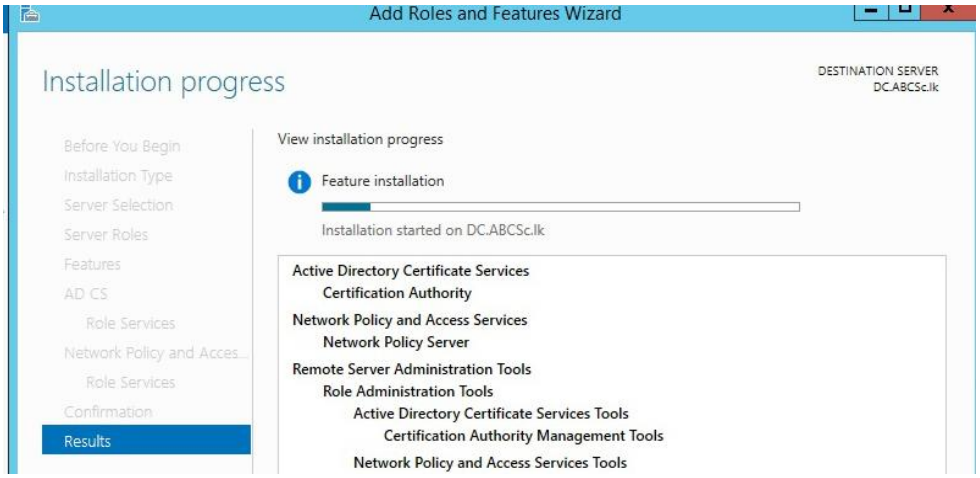
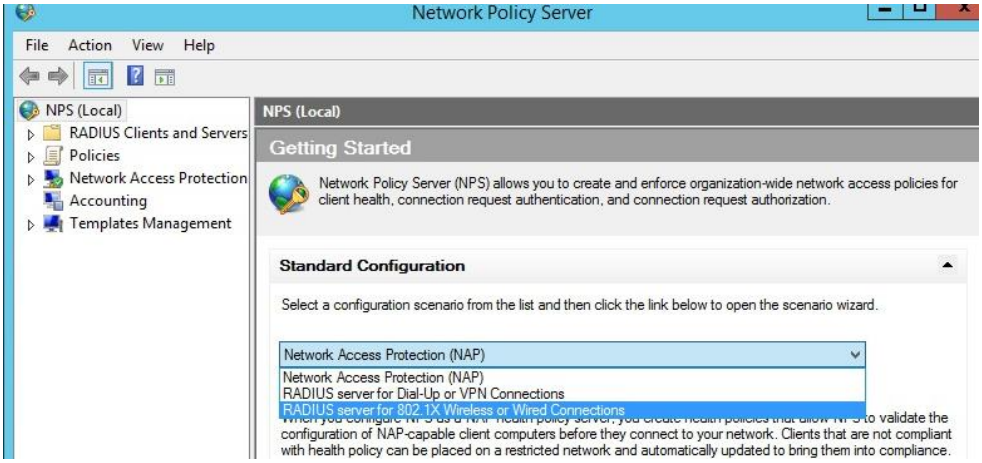


Figure 123 – 125





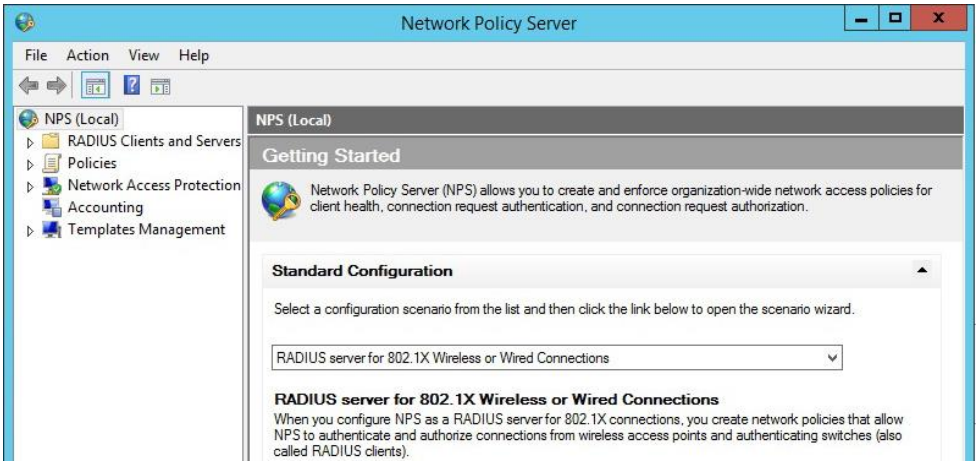
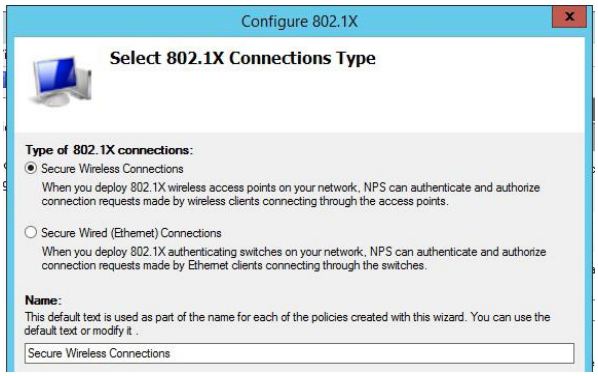
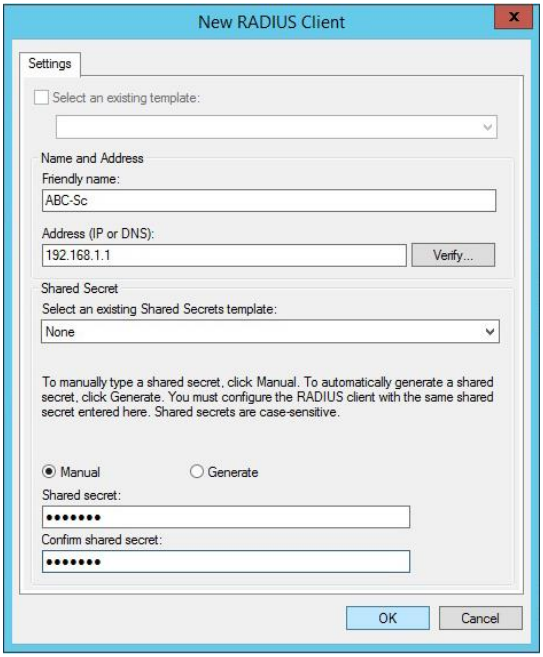


Figure 126 - 128





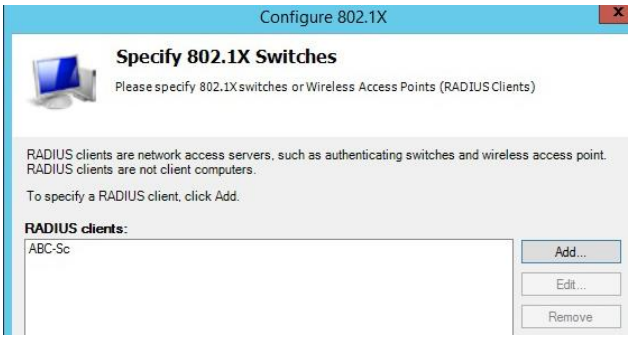
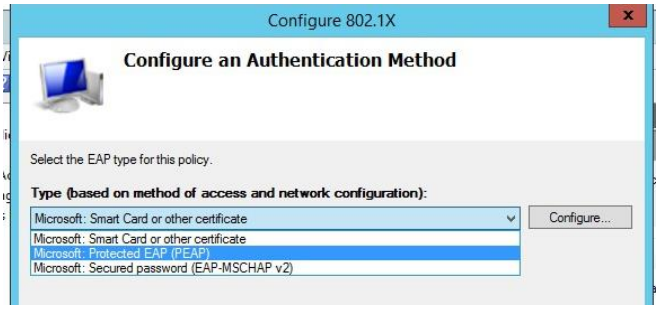
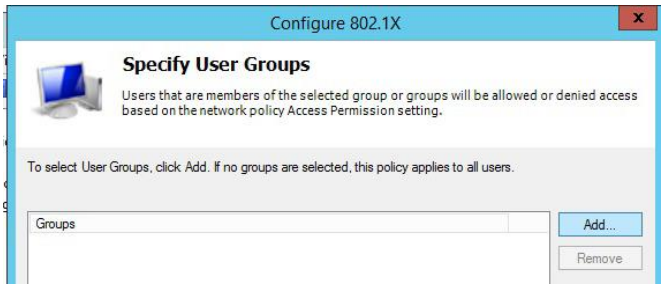
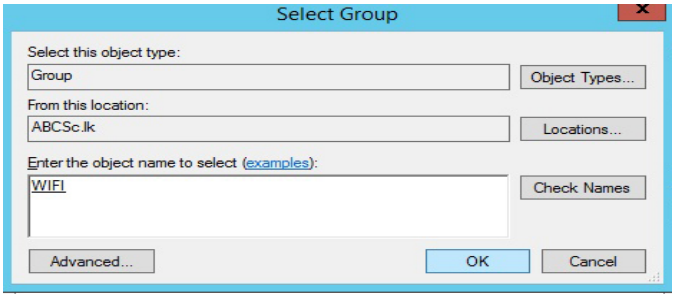


Figure 129 - 131







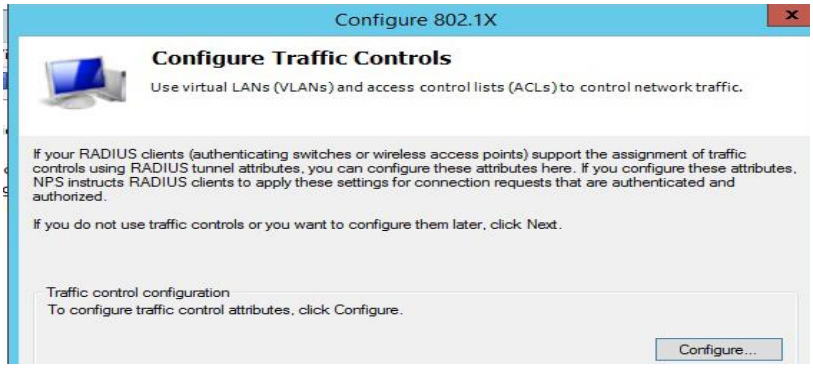
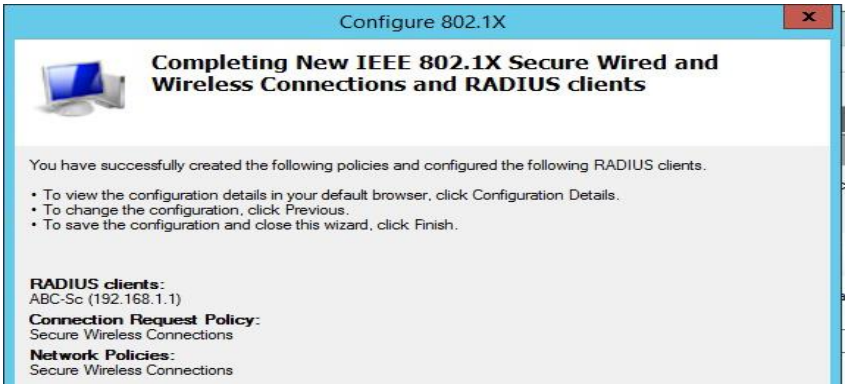
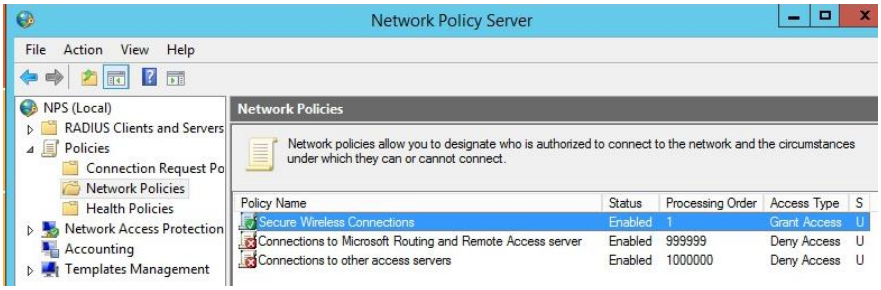


Figure 132 - 136





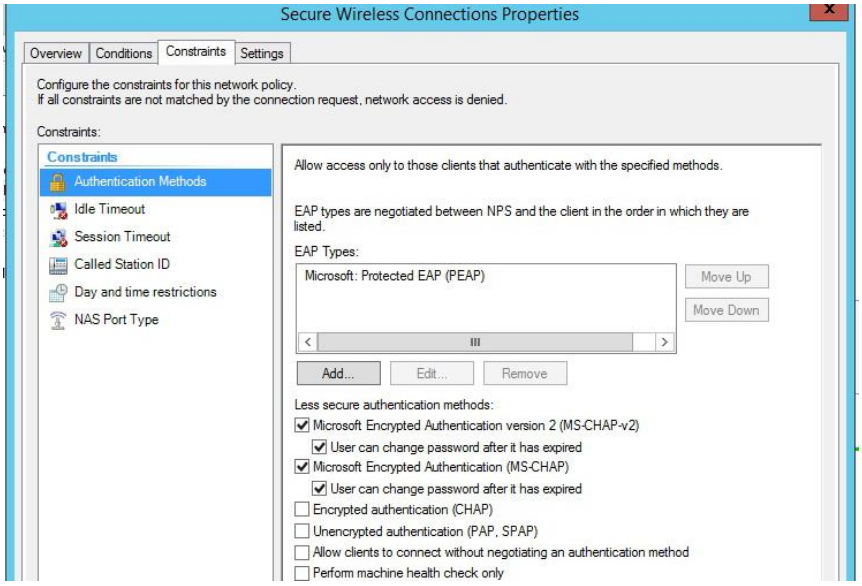


Figure 137 - 139

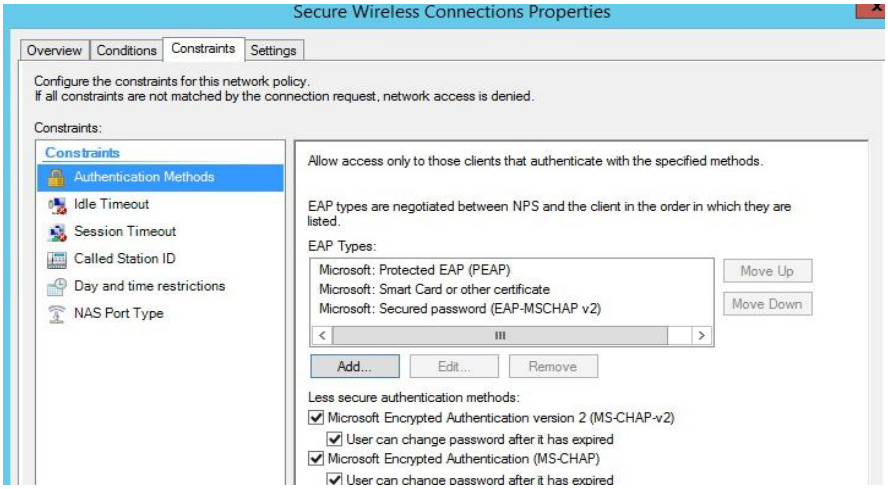
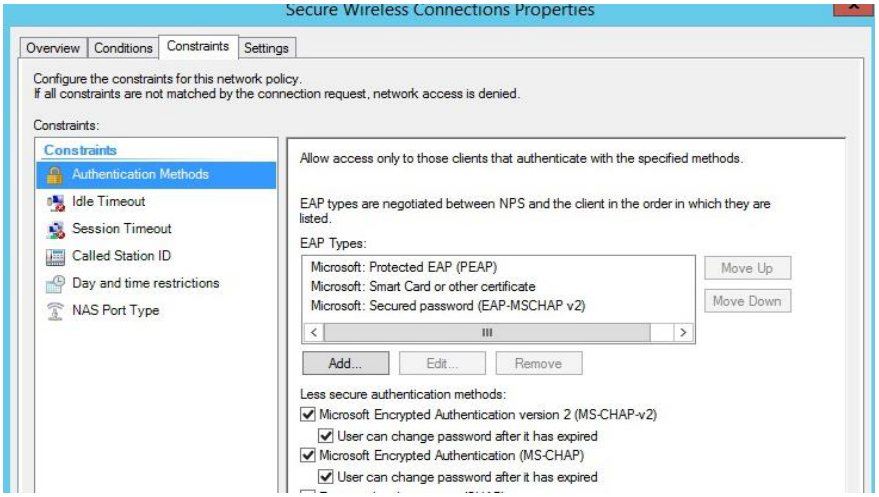
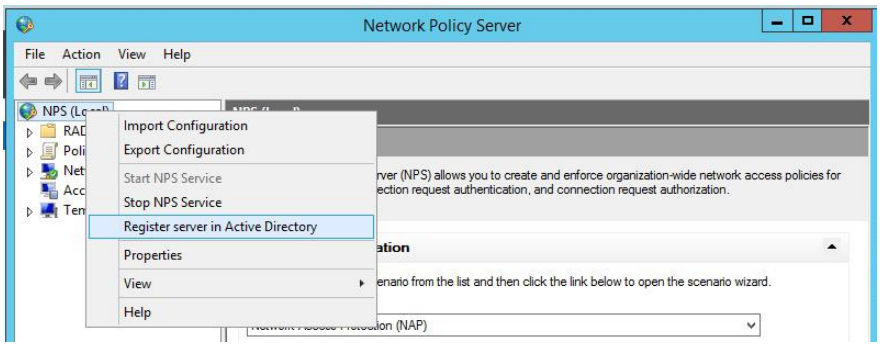


Figure 140 – 142





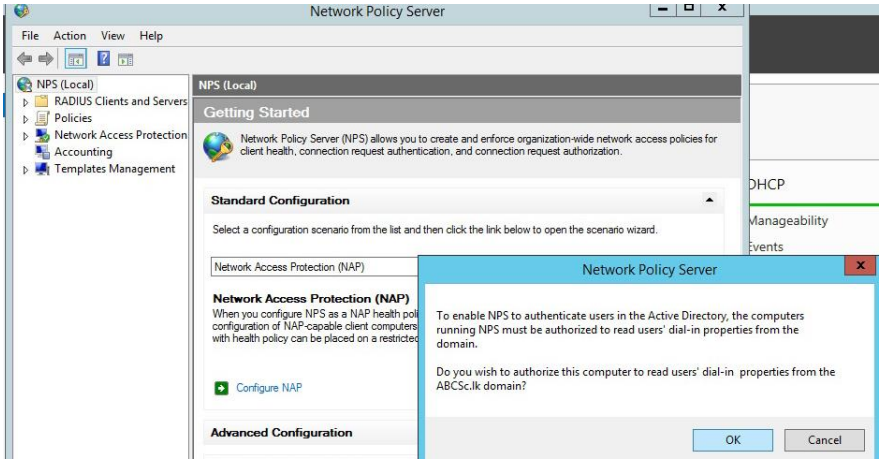
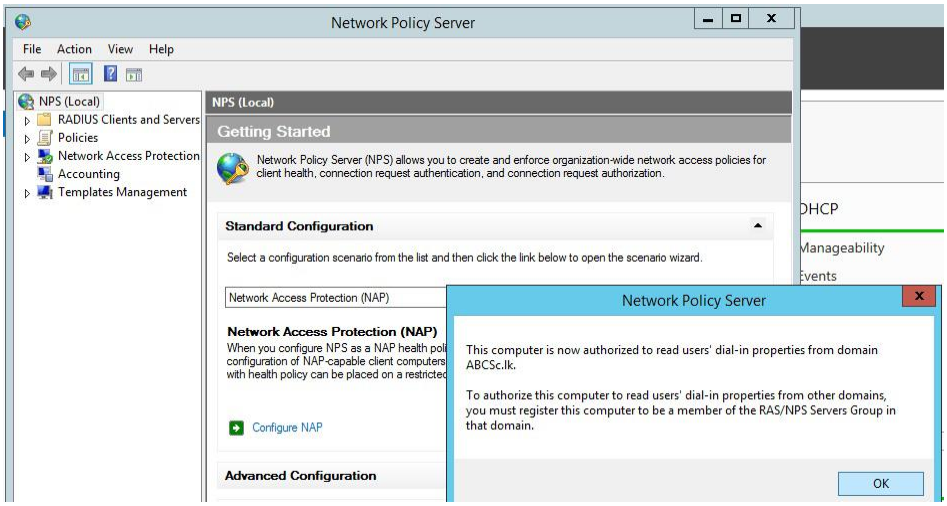


Figure 143 – 145



Implementing SNMP

```
Core_1(config)#snm
Core_1(config)#snmp-server com
Core_1(config)#snmp-server community abc
Core_1(config)#snmp-server enable trap
```

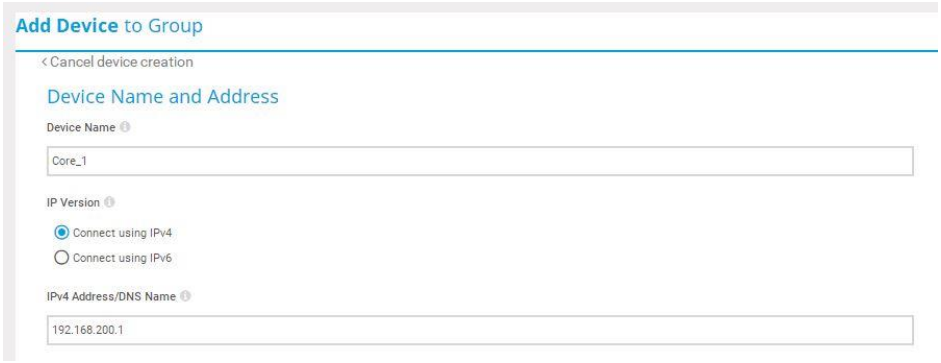
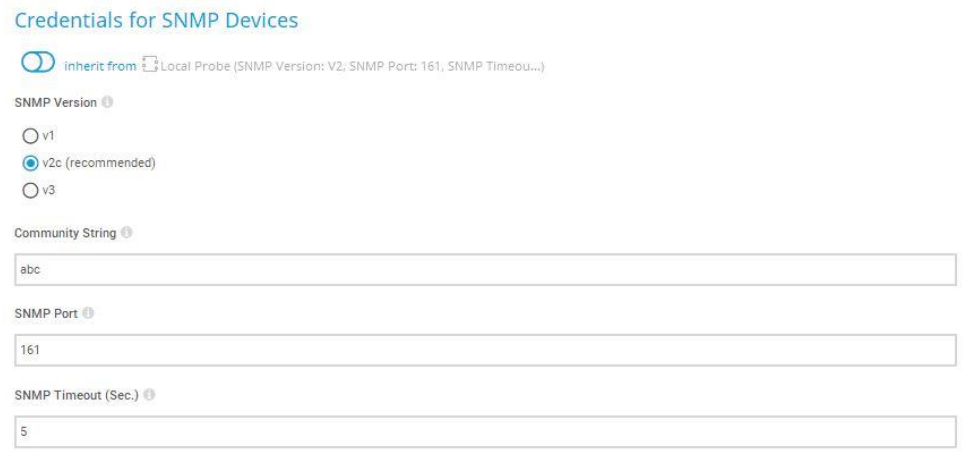


Figure 146 – 148



Implementing SMTP

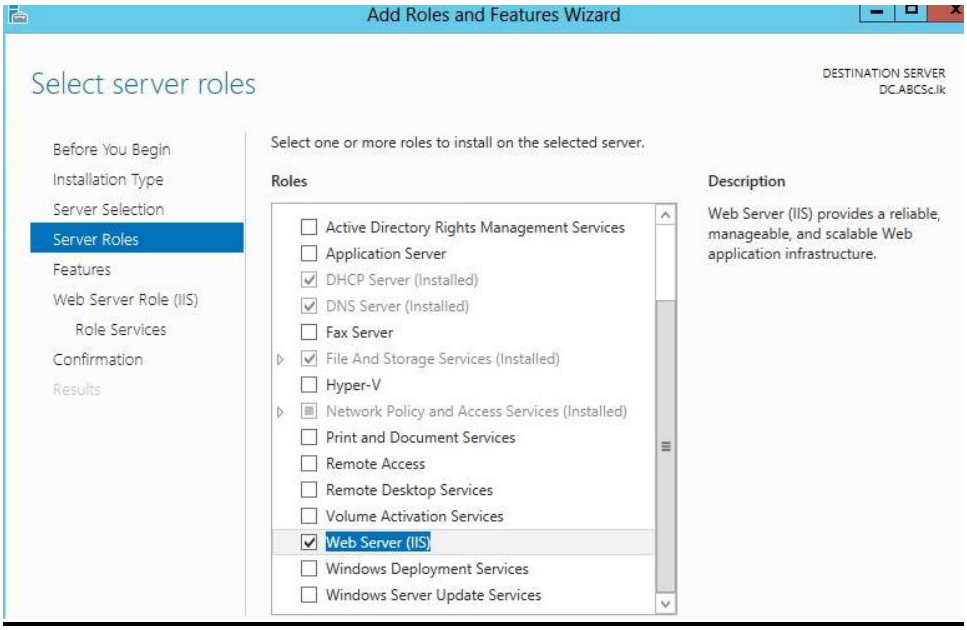


Figure 149 – 150

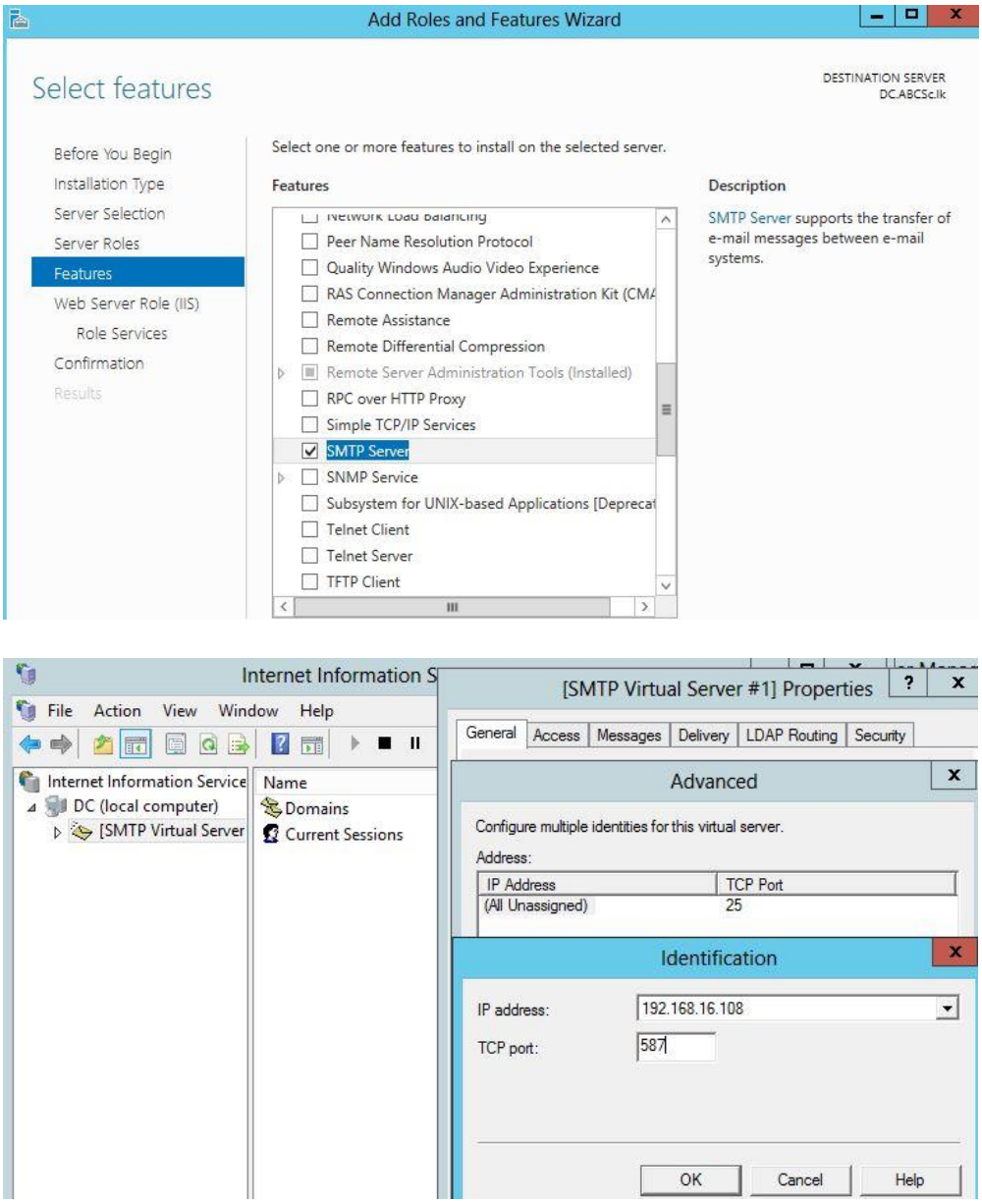
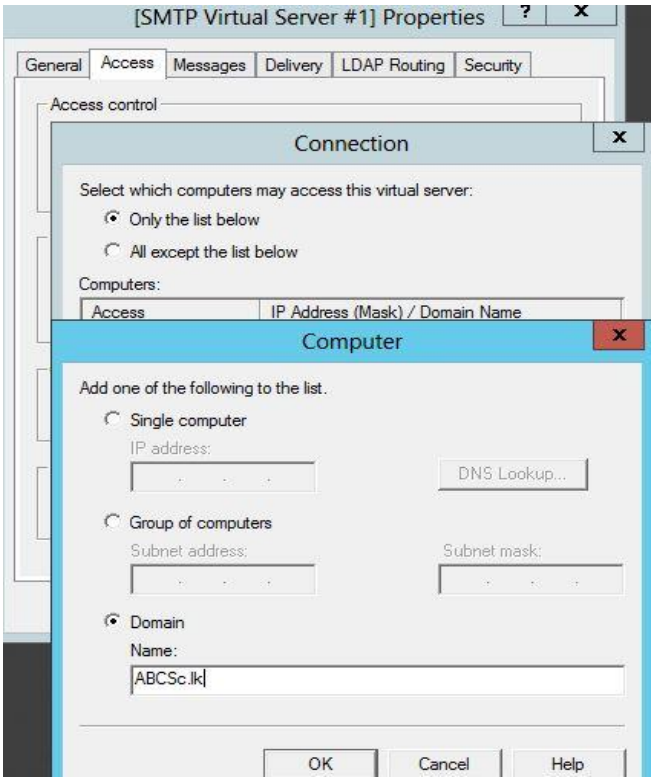


Figure 151 – 152



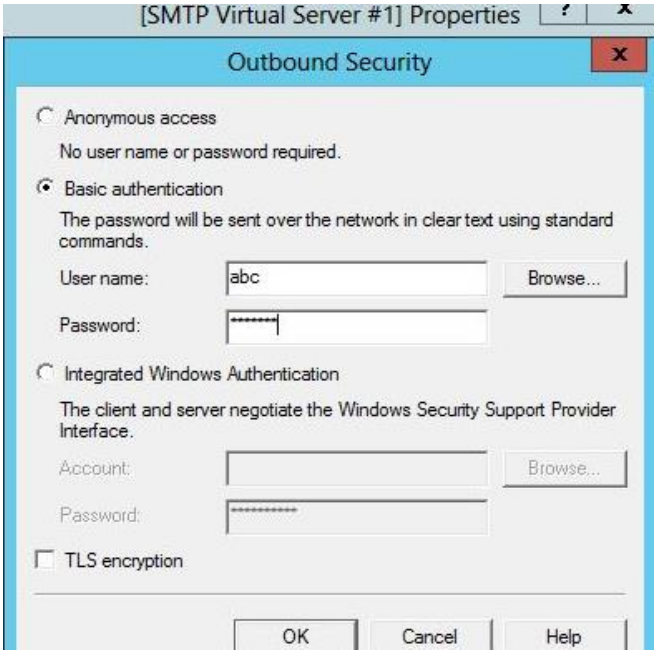


Figure 153 – 154

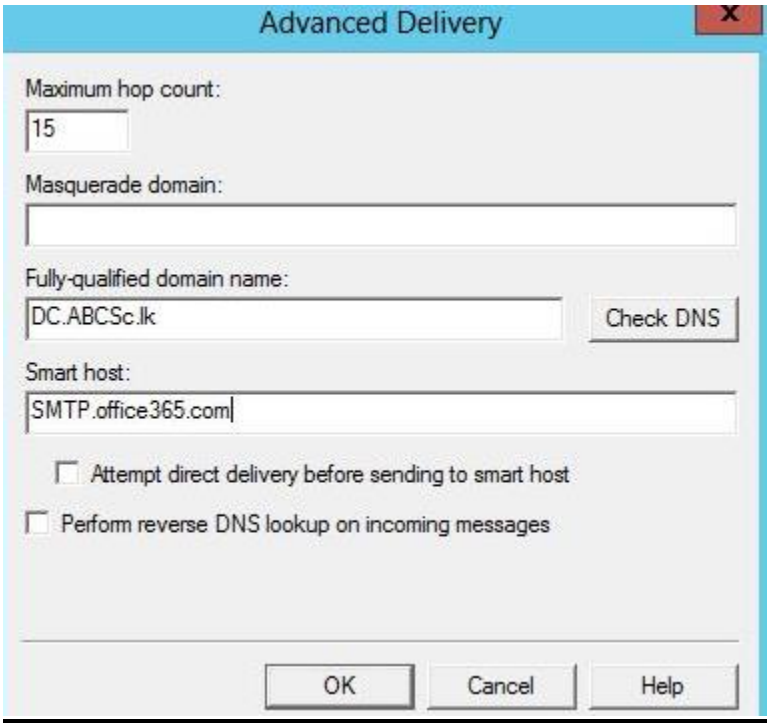
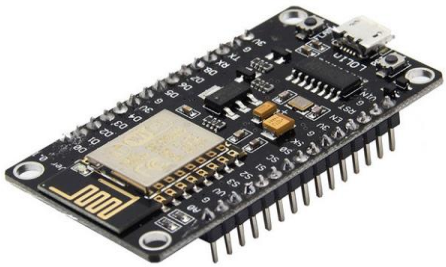

Advanced Delivery
Maximum hop count:
15
Masquerade domain:
Fully-qualified domain name:
DC.ABCSc.lk
Check DNS
Smart host:
SMTP.office365.com
Attempt direct delivery before sending to smart host
Perform reverse DNS lookup on incoming messages
OK
Cancel
Help

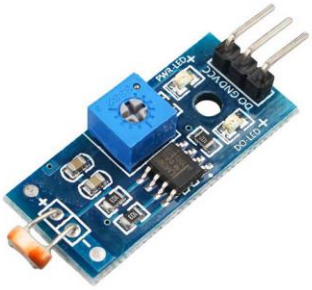
Figure 155

Implementing IOT devices



NodeMcu

NodeMcu Base v1.0



Light Sensitive Module

Laser Dot Diode Module

10K Thermistor NTC

Figure 156 – 160

6. Estimated Budget

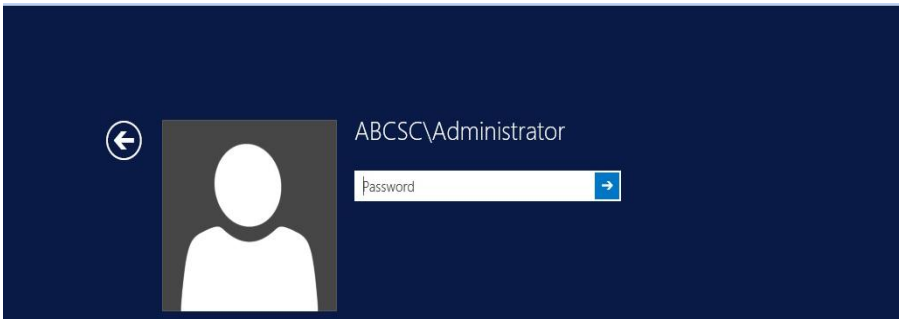
Cisco 2960 24TT switch	Rs.107,972	7	Rs.755,804.
Cisco CISCO1941-SEC/K9 1941 Router - Rs.146 854 *7 = Rs.1 027 978.	Rs.146,584	7	Rs.1,027,978
Cisco Aironet 1815i Wireless Access Point - Rs.40 227 *10 = Rs. 402 270.	Rs.40,227	10	Rs.402,270
Cisco ASA 5500-X Firewall - Rs.478 842 *1 = Rs.478 842.	Rs.478,842	1	Rs.478,842
Cat6 Ethernet cable roll (1000ft) - Rs.20 603.	Rs.20,603	1	Rs.20,603
Rack 36U - Rs.70 329.	Rs.70,329	1	Rs.70,329
12U Wall Mount Rack - Rs.51 275.	Rs.51,275	1	Rs.51,275
CAT 6 Faceplate socket - Rs.400	Rs.400	1	Rs.400
			Rs. 2,807,501

7. Evaluation

Tests and results

Result after AD Configuration

This is the logging account we had after AD configurations

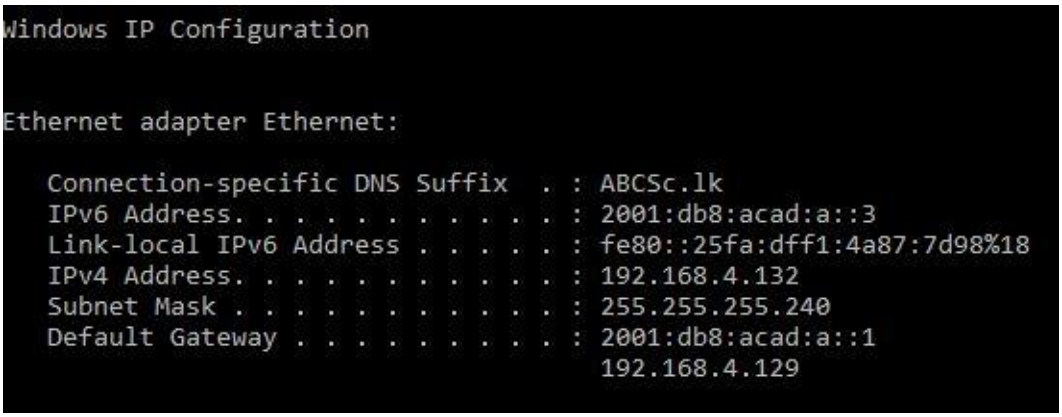


Results after the implementing Radius

Access point window from a mobile after the radius implementation

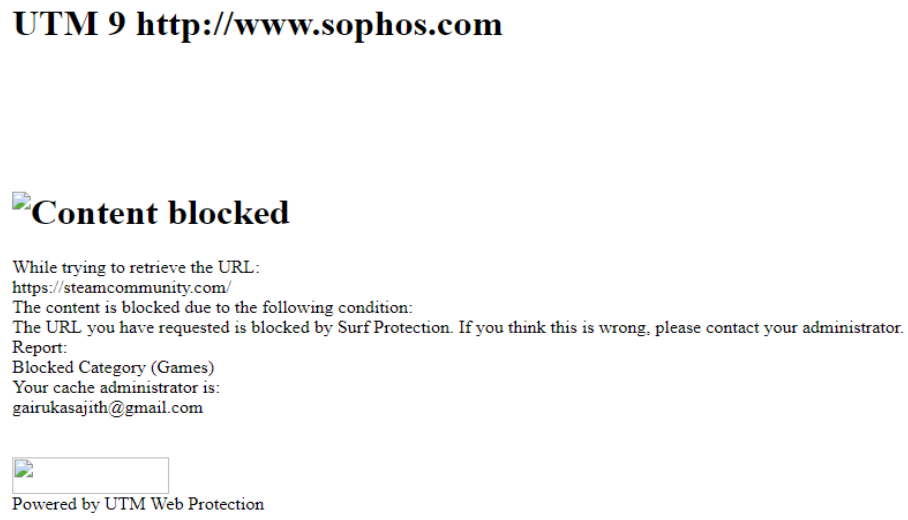
Results after the implementing DHCP and DNS

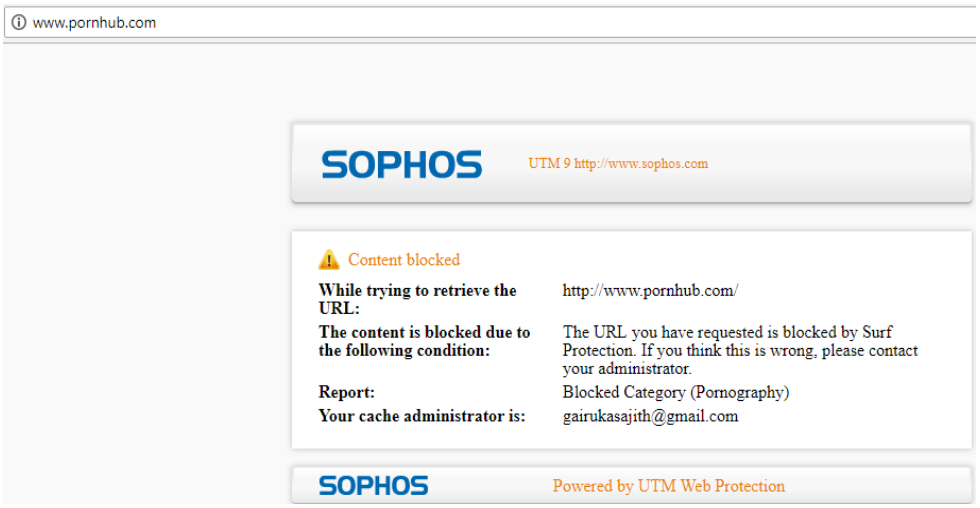
Results of the given ipconfig command in command prompt after DHCP and DNS implementation.



Results after the implementing Firewall

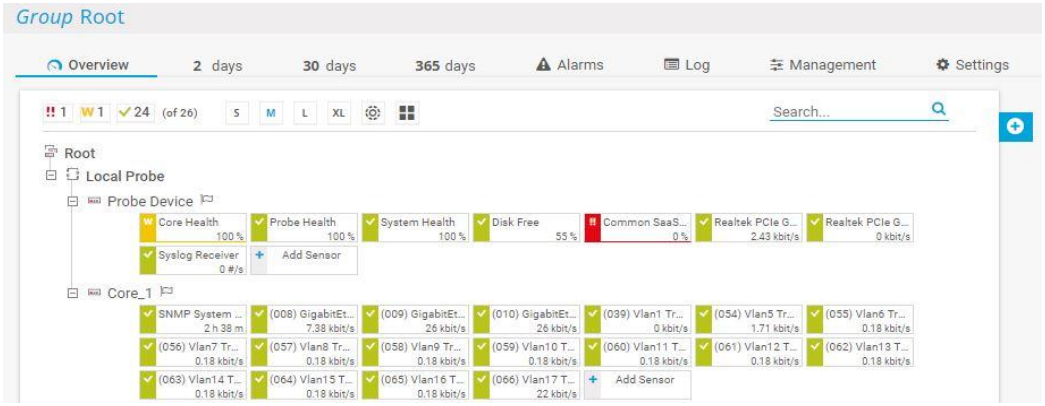
Results of accessing online gaming and adult content websites after implementing Firewall.

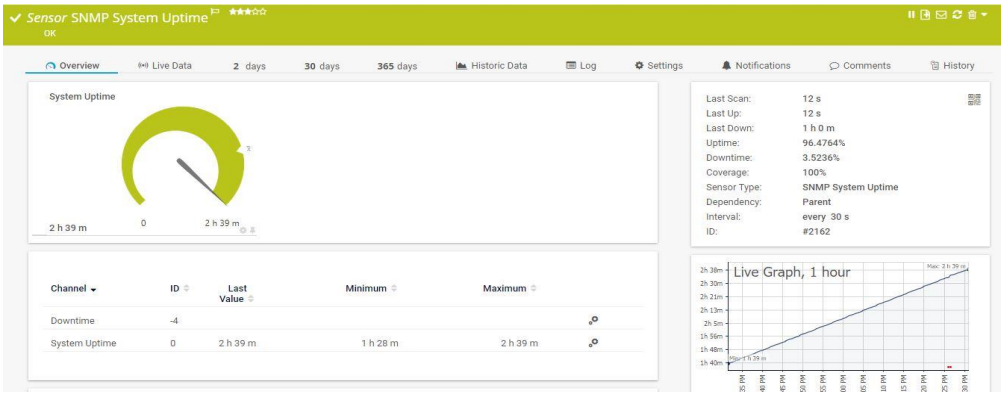


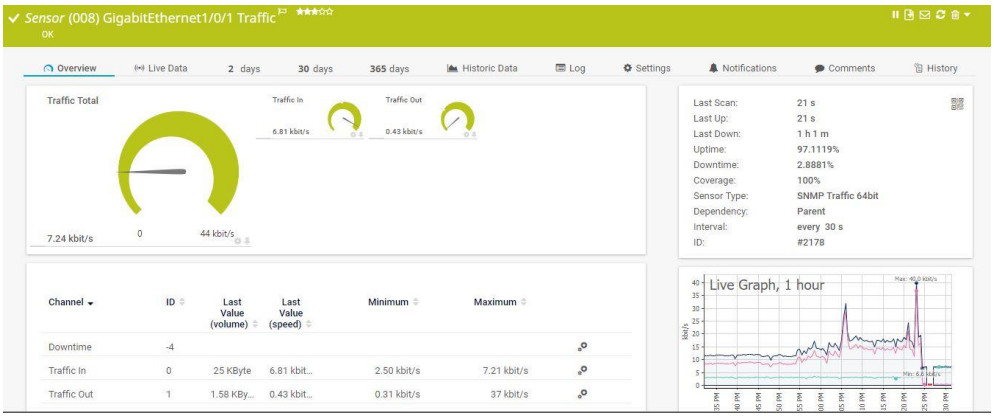


Results after the implementing SNMP

Ability to monitor and stats of the device resources, availability and Bandwidth usage of interfaces and devices.







HSRP Results

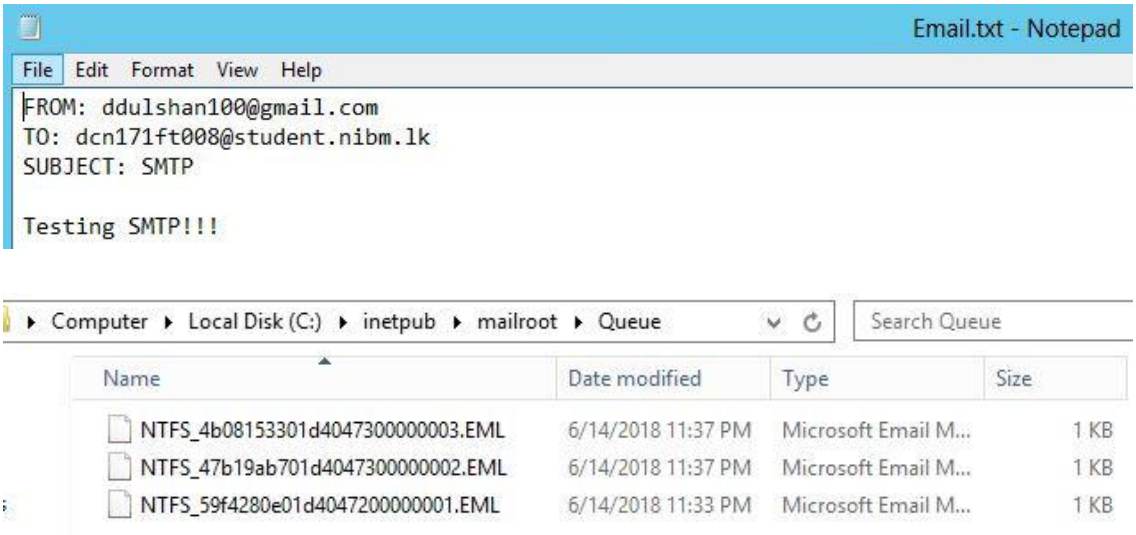
A continues ping while breaking the main link. The HSRP state of the backup switch changes to Active and take over the routing process.

```
C:\>ping -t 192.168.4.145

Pinging 192.168.4.145 with 32 bytes of data:

Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time=1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time=2ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time=1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time=1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.4.145:
    Packets: Sent = 27, Received = 22, Lost = 5 (19% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

```
%HSRP-6-STATECHANGE: Vlan13 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan17 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan10 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan11 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan17 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan14 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan11 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan10 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan14 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan16 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan16 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan6 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan7 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan7 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan6 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan8 Grp 0 state Speak -> Standby
```

SMTP Testing

Created a mail in notepad and copied the file to C:/inetpub/mailroot/pickup. Windows server picks up the file and moves to sending queue.



Issues and solutions

- We couldn’t implement radius in the beginning using access points to connect users via Wi-Fi Vlan.
- We had some issues with the firewall we used for Network protection. Because it’s license expire within a day. The reason was CMOS error. So, we had to replace the CMOS battery for prevent the error.
- We had problem pinging Windows server because the windows firewall had a rule blocking ICMP incoming and outgoing requests.

8. Conclusion

An institute is a place which has an educational environment. So, this project has been informed by many technical means that can provide a high level of security and quality of service while preserving safety for staff members and specially for students. The core layer of the network consists of two Layer 3 switches, the core layer switches switch consists of the VLAN database which is distributed to all access layer switches through servers. The Gateways of the VLANs are redundant with HSRP. Load balancing of the core layer is implemented by assigning STP with a half of the VLANs primary for one core switch and rest for the other switch. Secondary is also assigned if one switch goes down the other will act as the Root bridge for the VLANs.Each building has switches in the access layer, PCs are directly connected to Ethernet ports while APs are available for WiFi access. Radius authentication is used on PCs for virus and malware guard.

The security part of the institute's network has been provided with security tools such as SOPHOS firewall, an IP access control list, Mac address port security and a domain server to prevent unauthorized users from entering the institute's database system. ACL is implemented for Principle office, Office and server room blocking any access except for the IT Unit network. SNMP is implemented to monitor device states and resource usage to identify any Hardware malfunctions or failures. Port Mirroring is used to monitor all networks for suspicious or malicious activity.

These include DHCP server, DNS server and cabling design. The safety part was focused on saving the institute's information and users. The institute's information has been protected by backing up the Backup Systems' information to outside the local network with Windows server 2012 tools. As a result of using these techniques, institute's network is ready to provide a protected, user reliable and quality service and safety for the institute's system and users of the facility. In addition, we are planning to deploy security by using IOT devices with NodeMCU components that can connect through access point. These use for physical protection such as laser protecting service, also temperature detecting.

10. References

http://www.senith.lk/shop/item/1068/nodemcu-v3-wi-fi-development-board

http://www.senith.lk/shop/item/1135/nodemcu-base-v10

http://www.senith.lk/shop/item/35/light-sensitive-module

http://www.senith.lk/shop/item/9038/laser-dot-diode-module

https://www.arduino.lk/product/10k-thermistor-ntc-lug/

https://ifttt.com/

https://thingsboard.io/

https://www.sophos.com/en/products/free-tools/sophos-utm-home-edition.aspx

https://supportforums.cisco.com/t5/network-infrastructure-documents/hsrp-overview-and-basic-configuration/ta-p/3131590

https://glazenbakje.wordpress.com/2013/08/31/microsoft-windows-server-2012-radius-setup/

https://www.youtube.com/channel/UChPXqO3k8HiWp_6YhAkeRQg

https://www.youtube.com/user/elithecomputerguy

https://www.youtube.com/user/labminutes