Network Service Management & Virtualization

Project title: Assessment 2 DNS, DHCP & Group Policy.

STUDENT NAME: FLAVIA APARECIDA DA SILVA

STUDENT NUMBER: 2016265

Contents

Assignment Introduction

Scenario overview:

You have started a new role in an IT consultancy company. The company provides networking
consultancy services for companies located in Ireland. Your first proof of concept project is to create a
virtualized network infrastructure based on a new college's network.
The proof of concept is divided into a number of parts:
1) Use hosted type II (i.e VirtualBox) software to build a small client-server network.
2) Install DHCP, DNS services on the Server / install wireshark on the client.
3) Manually create DNS Records on the Server e.g. HOST record, New Alias (CNAME), New MX
record.
4) Create a Student OU and an Academics OU and test group policy for same– provide a brief
description of each policy (3 for each OU) and include research references in your work.
5) Use snapshots (with relevant names) as you progress through this project.
This assignment will help assess your understanding of group policy in Active Directory along with
virtualized network services such as DNS and DHCP. You are required to create group policies, for
Academics, and for Students. Each policy must contain three modifications appropriate for the user
type.

Specific Requirements

Using Type II software, install 2 VM's. Use Windows 2012 (full version, not core) for the server system and use Windows 10 for the client.

Both virtual machines were created in a VM VirtualBox from Oracle as screenshot below:
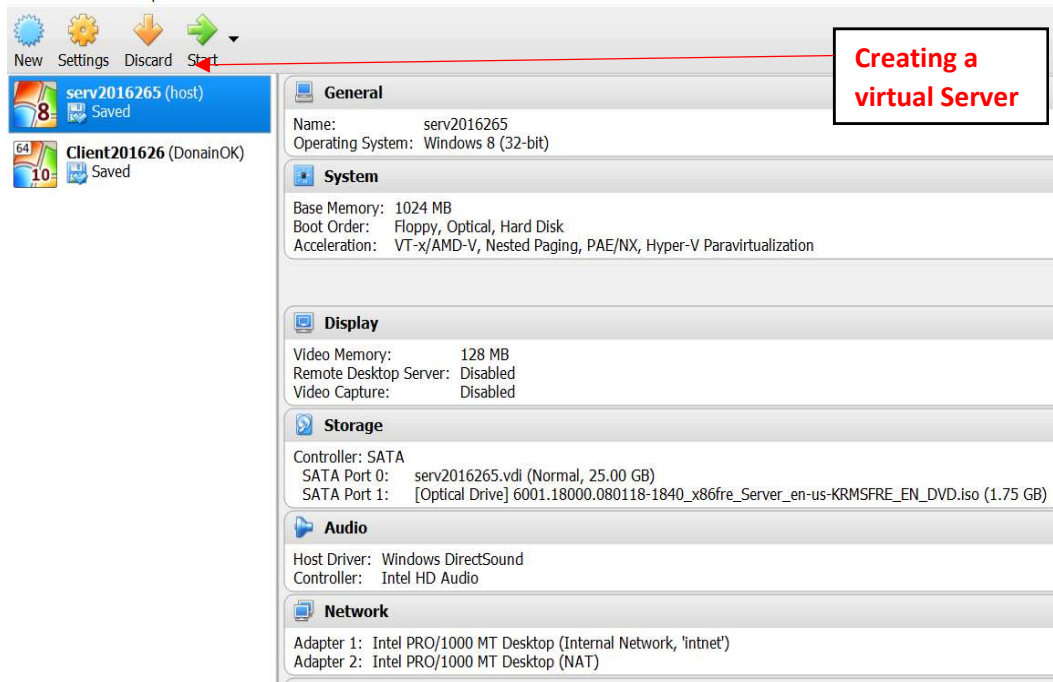

Figure 1

Client Windows 10:
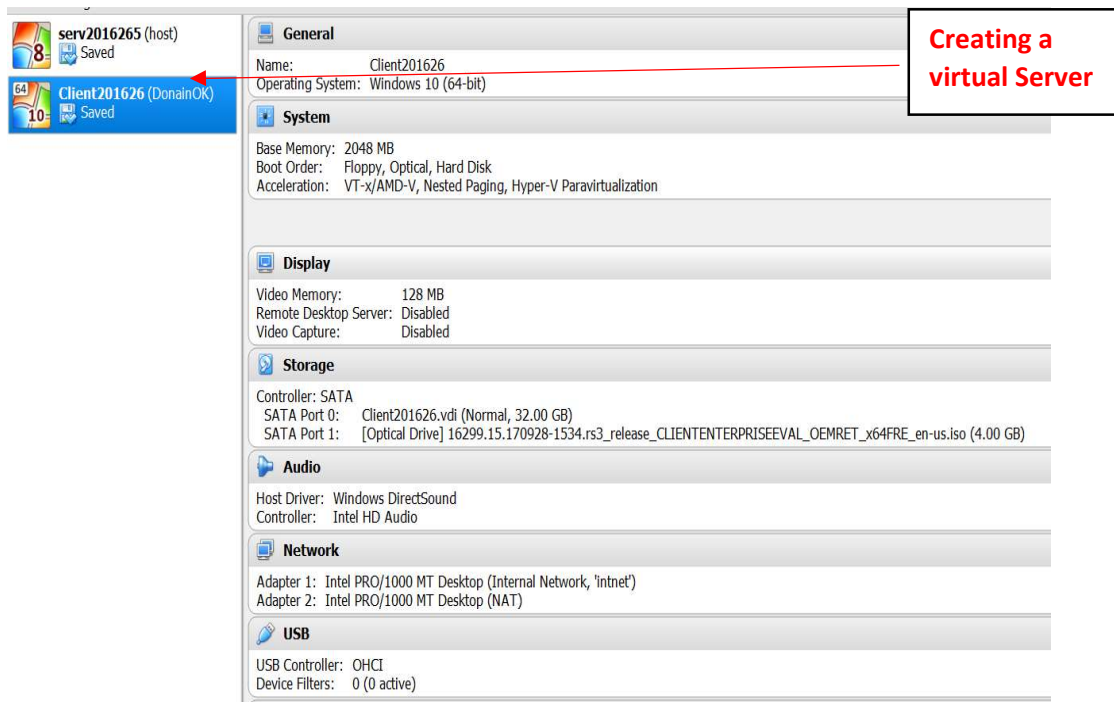
Figure 2

2) Using the snapshots feature ensure to take regular snapshots – take a print screen and include in final report (should include minimum of 3 snapshots with relevant names).
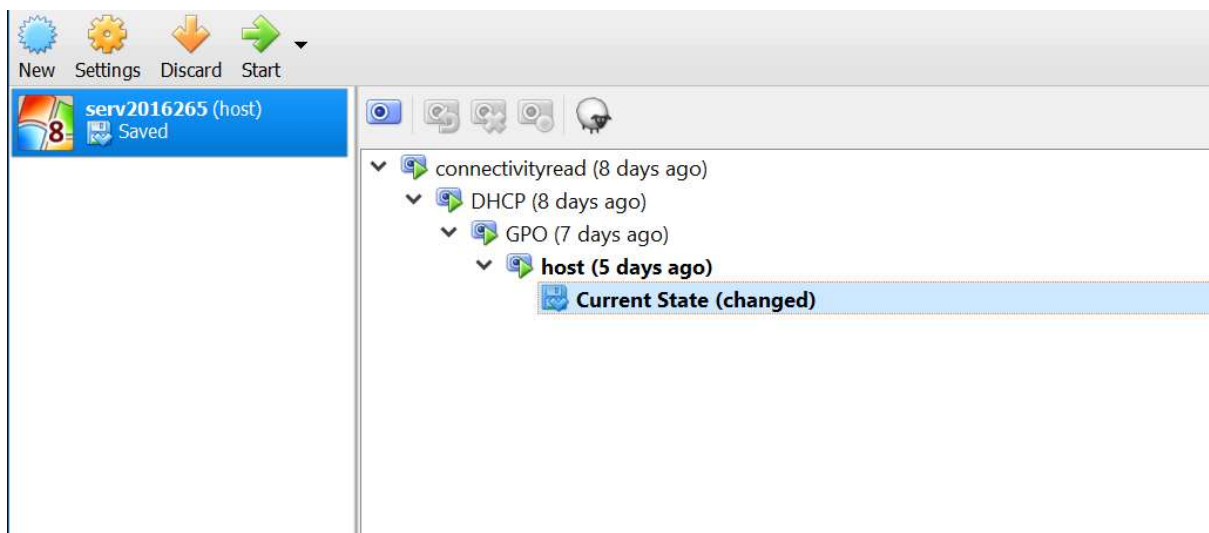
Figure 3

3) Rename the server with 'ser' followed by your student number e.g. ser2016111. Rename the client using the name client followed by your student number e.g. client2016111 (e.g. if my student number was 2016111).

In System Properties -> click Change -> next screen gives to us an option to name a computer as screen below:

Figure 4

4) Assign the server a static IPv4 address using the following configuration.

o Server IPv4 address: 172.16.50.10/24

o Default Gateway: 172.16.50.1

o DNS Server: 172.16.50.10

Figure 5

5) Assign the client (initially) a static IPv4 address using the following configuration.

o Client IPv4 address: 172.16.50.100/24
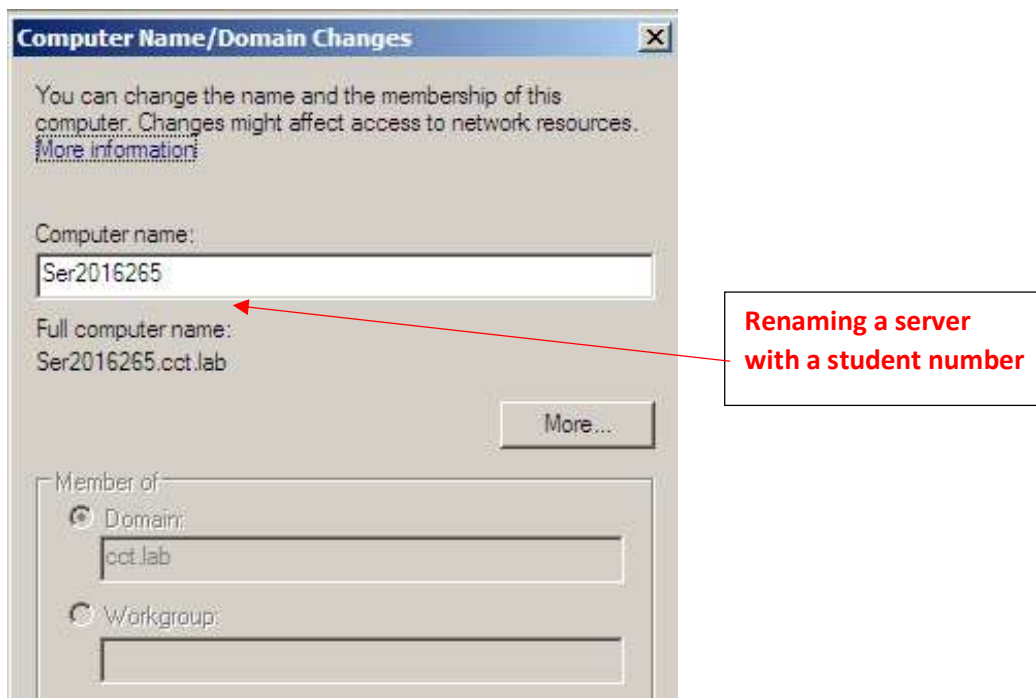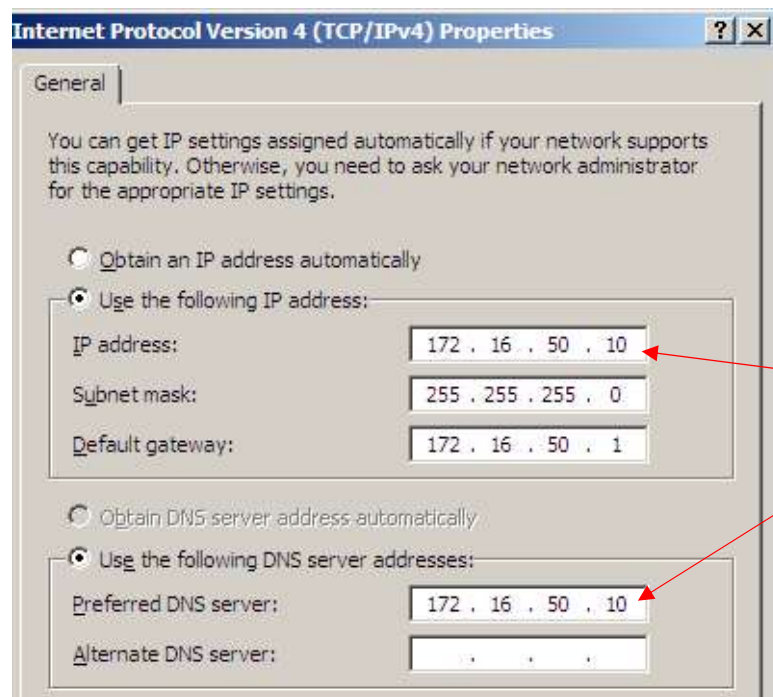
o Default Gateway: 172.16.50.1

o DNS Server: 172.16.50.10
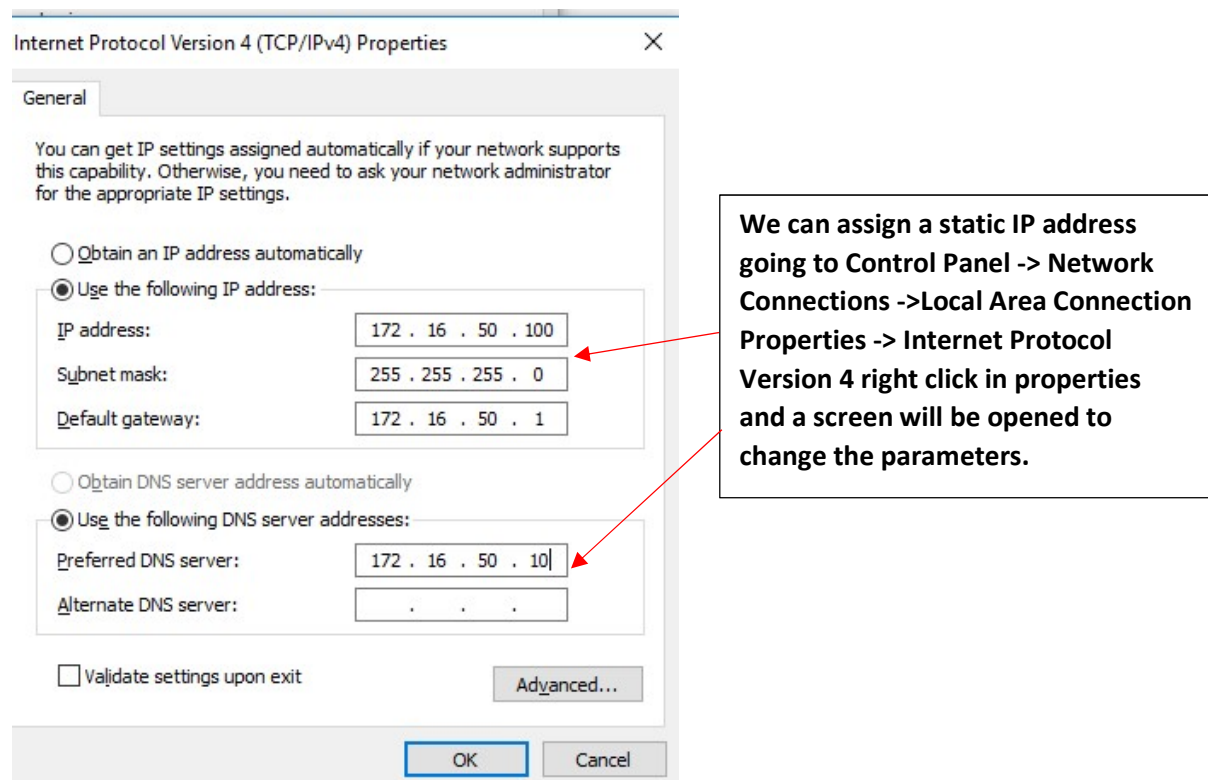
Figure 6

6) Convert the server into a Domain Controller.

o When creating the domain use the domain cct.lab (be sure to use this domain)
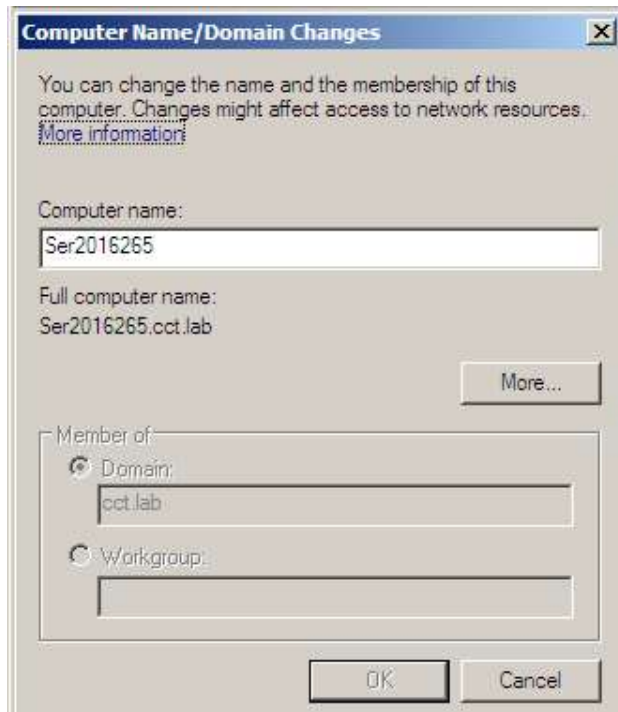
Figure 7

After the Domain Controller has been installed, join the client computer to the domain.

Joining the Client machine to a domain, we need to go to System Properties -> Computer Name/Domain Changes click in member of and pass the name of the server domain.

After type the domain, a windows security screen appears to confirm user name and password.
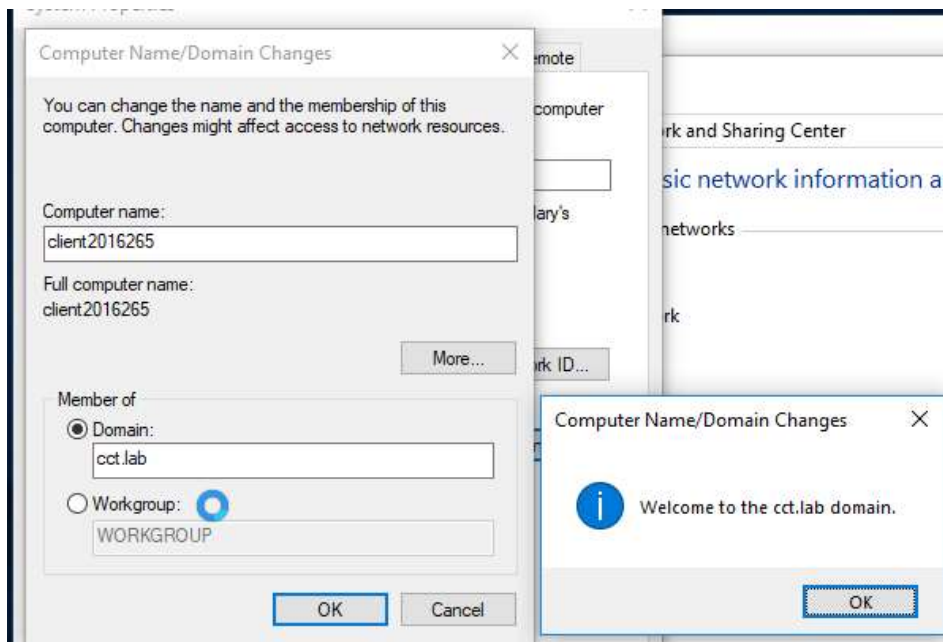
Figure 8

Figure 9

Ensure the client can ping the server from the command line.

Figure 10

7) Ensure to install the DNS service and DHCP service.

Figure 11

Adding a new role, we need to go to Server Manager -> Roles -> add roles
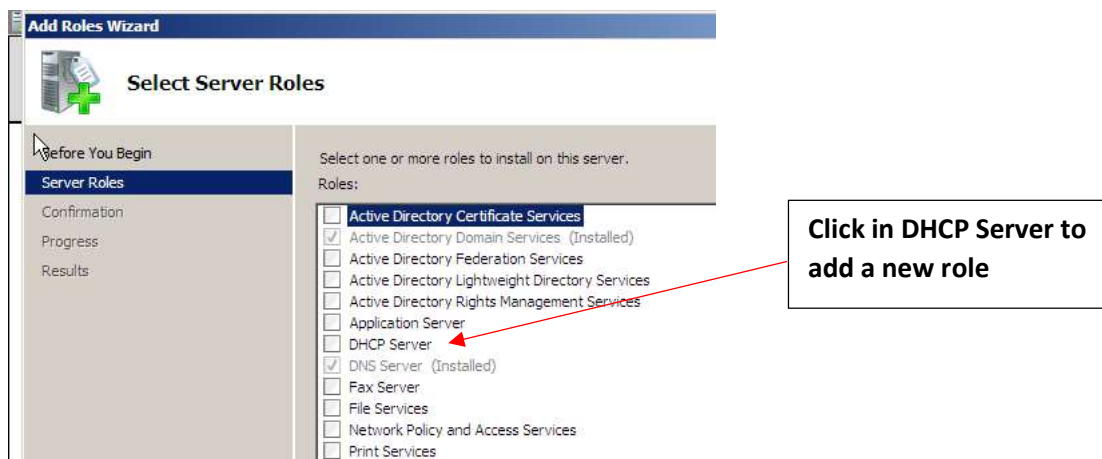
Figure 12

8) DHCP scope name should be the same as your domain. The scope should be set as follows:

o Starting IP address is 172.16.50.1/24 and ending address is 172.16.50.254

o The Subnet Mask is /24 and default gateway is 172.16.50.1

o Lease duration set for 8 hours.

Creating a new scope click and ADD to insert parameters as screenshot below:
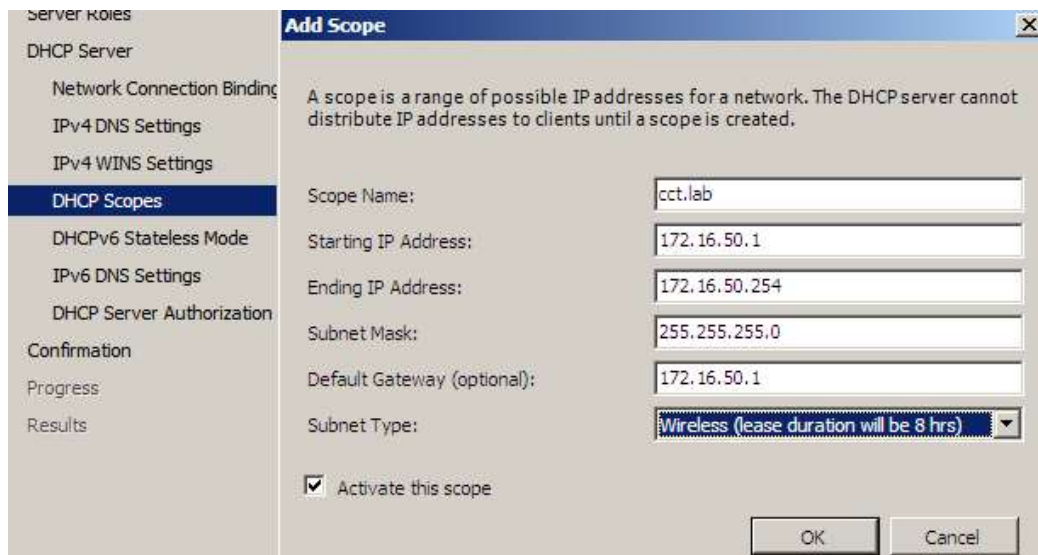
Figure 13

Create 2 individual DHCP exclusions:
§ DG: 172.16.50.1

DNS: 172.16.50.10
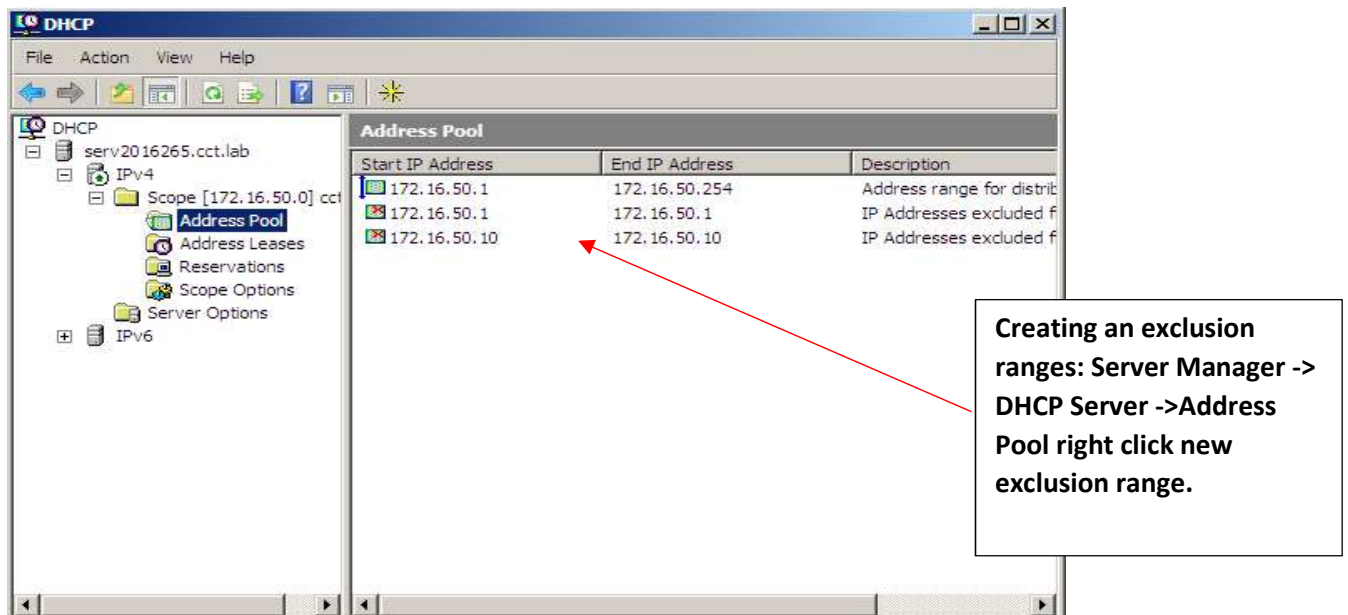
Figure 14

Create a pool of DHCP exclusions:
§ 172.16.50.100-172.16.50.120

Figure 15

Add a CNAME record pointing back as an alias to the www server (use your student number as the alias).
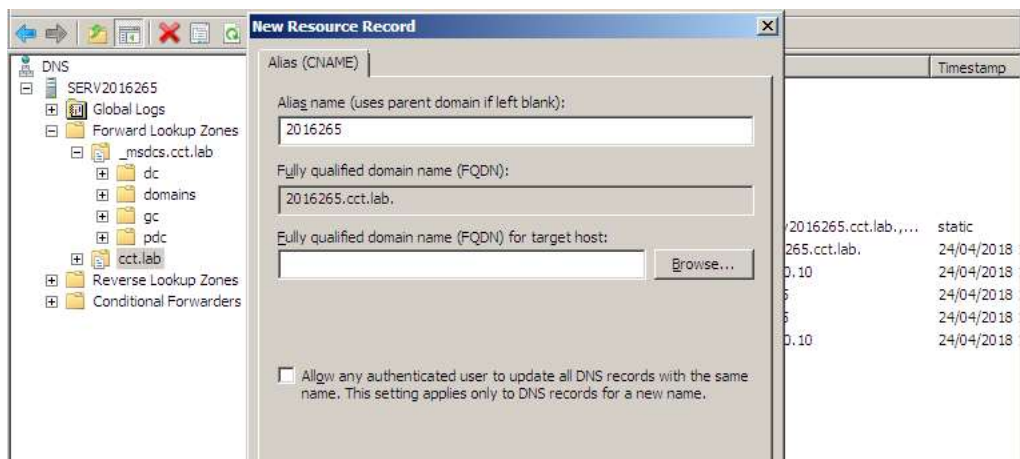
Figure 16
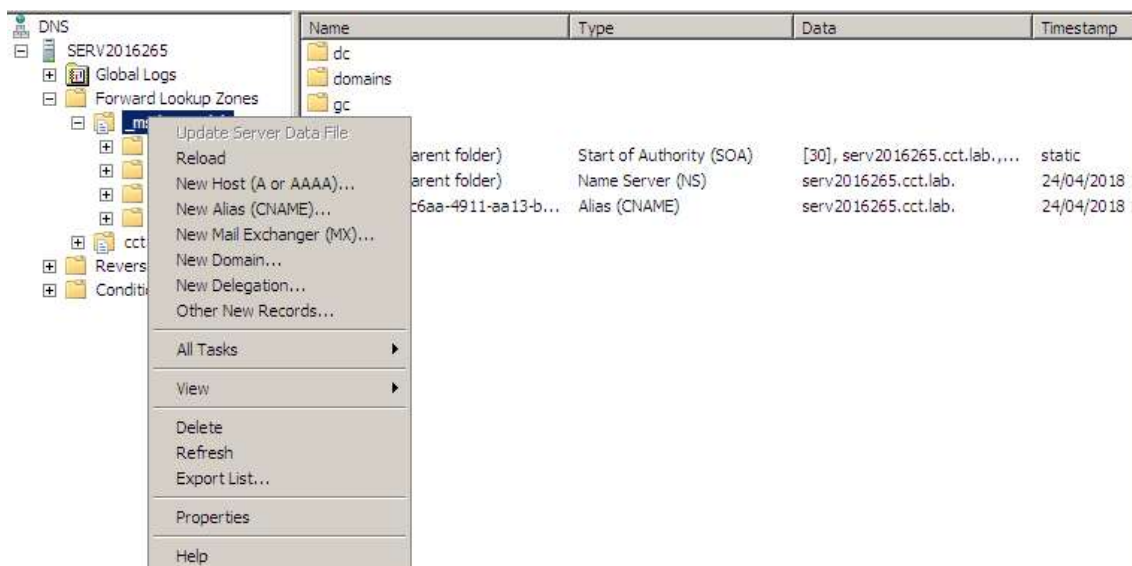
Figure 17

Web server (www): 172.16.50.101
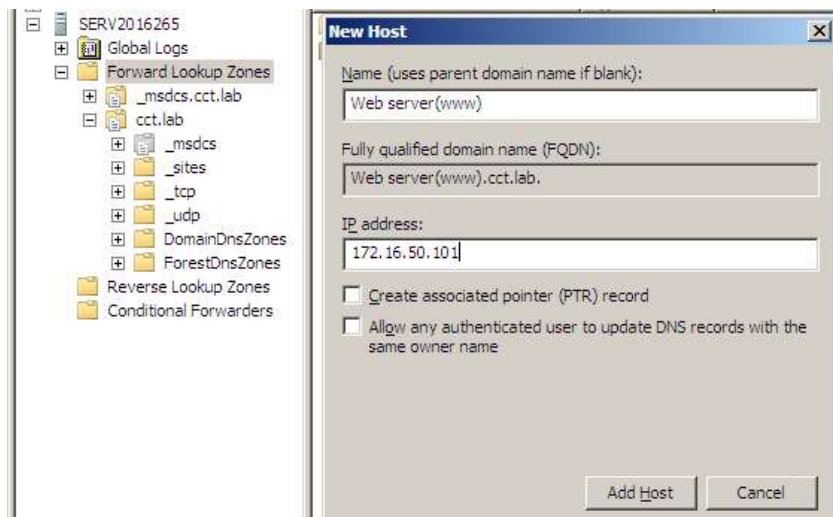
Figure 18

Email Server (MX): 172.16.50.103
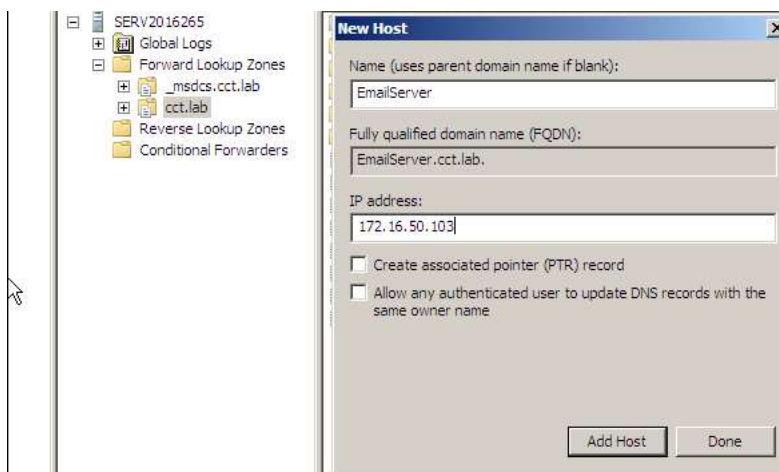
Figure 19

FTP Server (ftp): 172.16.50.104.

SERV2016265
  Global Logs
  Forward Lookup Zones
    _msdcs.cct.lab
    cct.lab
  Reverse Lookup Zones
  Conditional Forwarders

New Host

Name (uses parent domain name if blank):

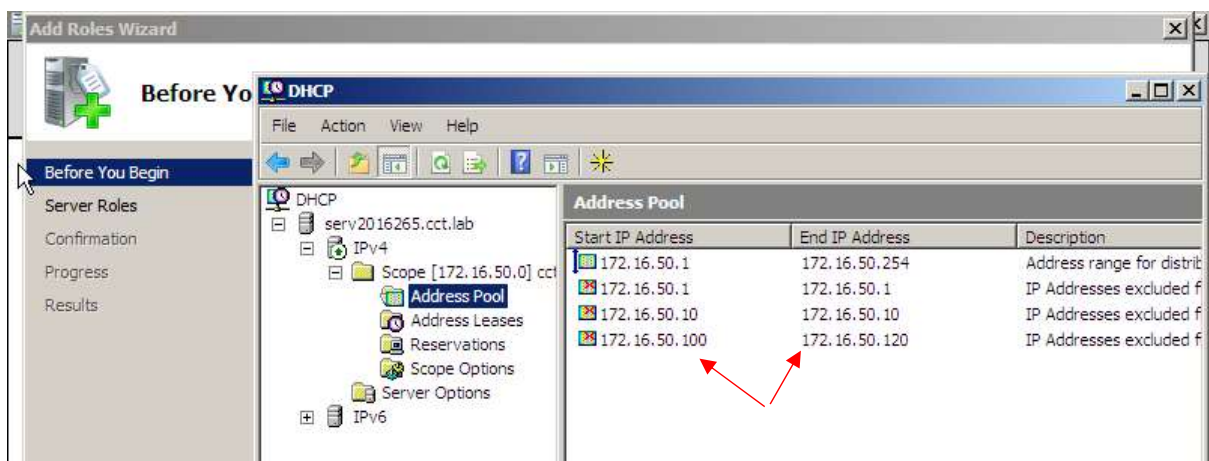FTPServer

Fully qualified domain name (FQDN):

FTPServer.cct.lab.

IP address:

172.16.50.104

☐ Create associated pointer (PTR) record

☐ Allow any authenticated user to update DNS records with the same owner name

[Add Host]   [Done]

Figure 20

Web server (test): 172.16.50.102

SERV2016265
  Global Logs
  Forward Lookup Zones
    _msdcs.cct.lab
    cct.lab
  Reverse Lookup Zones
  Conditional Forwarders

New Host

Name (uses parent domain name if blank):

Webservertest

Fully qualified domain name (FQDN):

Webservertest.cct.lab.

IP address:

172.16.50.102

☐ Create associated pointer (PTR) record

☐ Allow any authenticated user to update DNS records with the same owner name

[Add Host]   [Done]

Figure 21

All hosts add as screen shoot below:

Figure 22

Add a CNAME record pointing back as an alias to the www server (use your student number as the alias).

Choose DNS, click in cct.lab -> right click -> new host CNAME – type the name – click in browser -> double click in the server- double click forward zone – double click in the actual server – choose the host

Figure 23

Configure the client to dynamically receive the IP address from the pool of addresses

rather than using the original static IP address.

Figure 24

9) Use Wireshark on the client to demonstrate the dynamic IP address comes from server.

Ensure to print screen. (TIP: use ipconfig /release and ipconfig /renew). Add brief description.

Figure 25

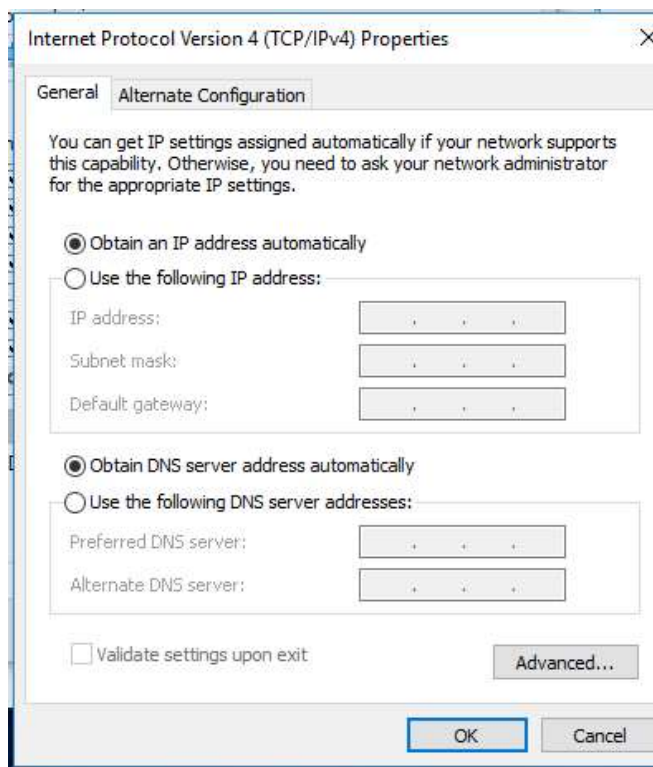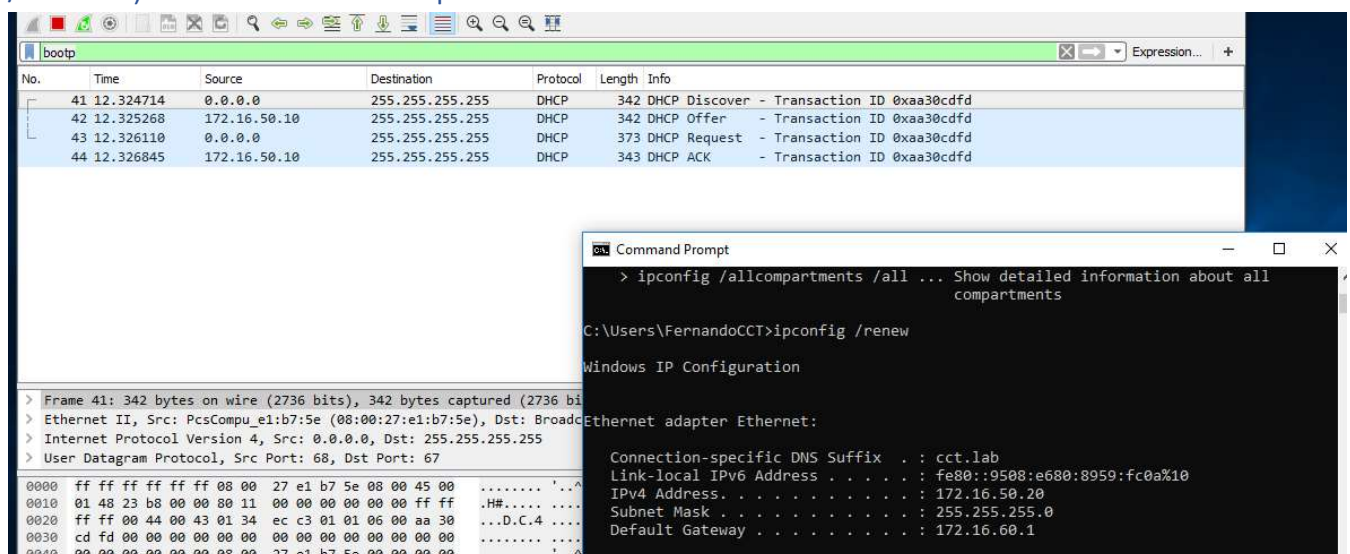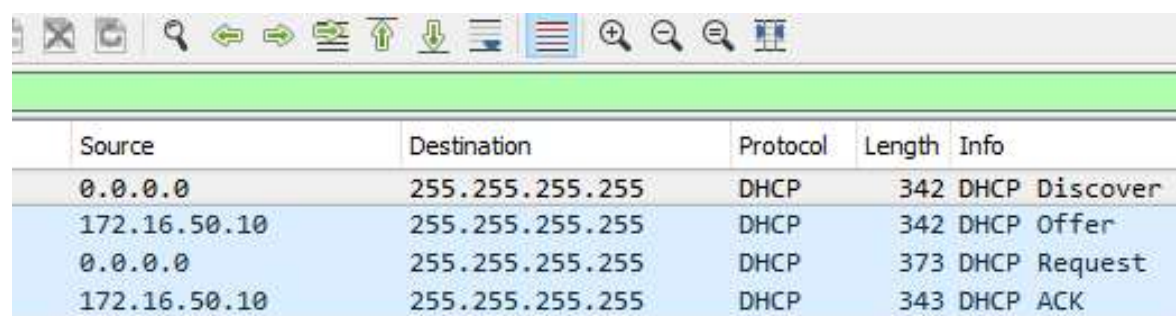Greg first I want to apologise about my print screen because I did my wireshark task in someone else computer's as we talked before my Client machine it does not work after I nearly finished all my assignment, as you allowed me to do it in another way, thank you for being understanding as well.

I will explain my analyse about the screenshot above:

Using a Wireshark we can analyse packets, network troubleshooting and communication protocols.

We can see the DORA process happening, flowing messages between client and servers.

DORA stands for discover, offer, request and Acknowledge.

Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover
172.16.50.10	255.255.255.255	DHCP	342	DHCP Offer
0.0.0.0	255.255.255.255	DHCP	373	DHCP Request
172.16.50.10	255.255.255.255	DHCP	343	DHCP ACK

Figure 26

Discovery sent by a client that is connected to a local subnet. While send discovery destination address is broadcast 255.255.255.255 and source address is 0.0.0.0.

Offer is a response to discovery message by DHCP client. It contains network configuration setting for the client like an IP address offer to client 172.16.50.10.

When exist a response to offer that means a client has accepted the network configuration.

After accepted the request message the IP by DHCP Server sent an ACK to the client, this means the client can start using the network.

Figure 27

10) Use Wireshark on client to demonstrate the lookup of a web server. Ensure to print screen.

(TIP: use nslookup). Add brief description.

Nslookup is used for querying the Domain Name System (DNS) to obtain domain name or IP address

DNS translates domain names to IP addresses so browsers can load internet resources.

1. A query travels into the Internet and is received by a DNS recursive resolver.
2. The resolver then queries a DNS root nameserver (query response).
3. The root server then responds to the resolver with the address of a Top-Level Domain (TLD) DNS server (www.cct.lab.cct.lab), which stores the information for its domains. When searching for cct.lab, our request is pointed toward the. lab TLD.
4.The resolver then makes a request to the. lab TLD.
5.The TLD server then responds with the IP address of the domain's nameserver, www.cct.lab.cct.lab.
6. Lastly, the recursive resolver sends a query to the domain's nameserver.
7.The IP address www.cct.lab is then returned to the resolver from the nameserver.
8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially.
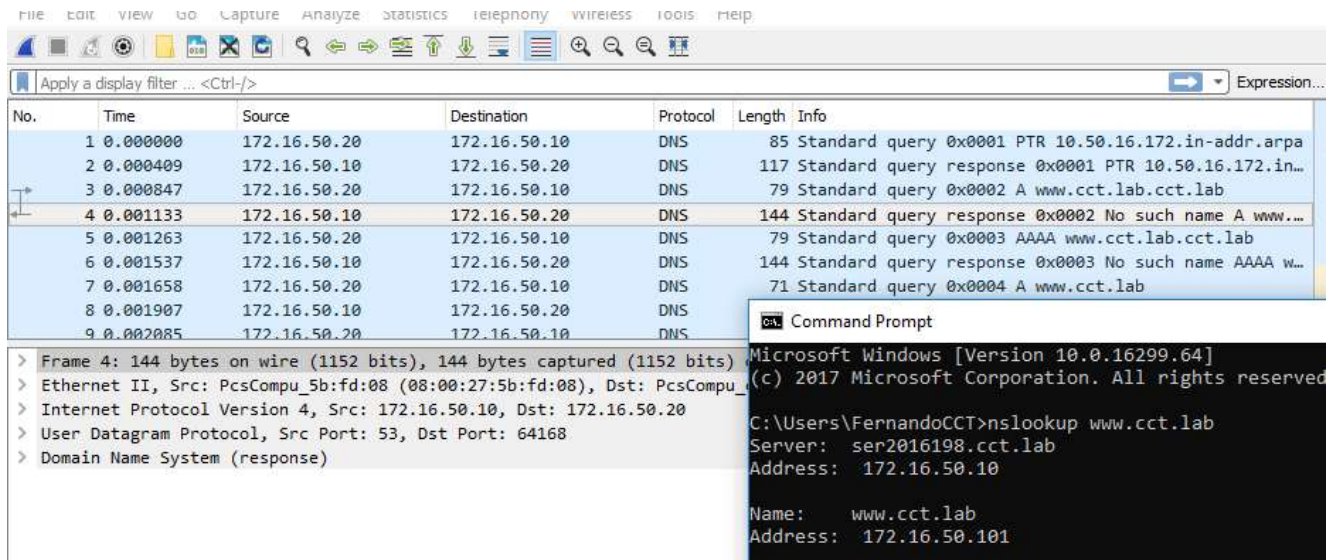
Figure 28

11) Create Organization Units - Students and Create OU Academics (and create one user

account to test each – you may create your own usernames for each)

Group Policy is used to allow administrator to define and set to the users what they can do on a group networking, it includes on access files, folders and applications.

Creating a OU -> Start -> Administrative Tools -> Active Directory Users and Computers -> cct.lab right click New – Organizational Unit
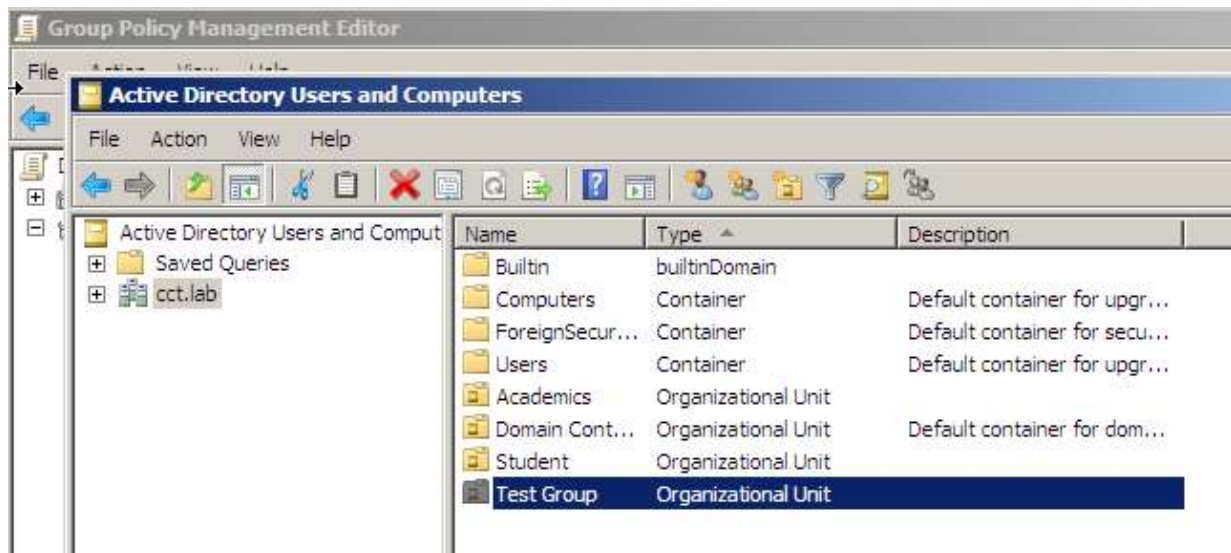
Figure 29

Creating User -> Start -> Administrative Tools -> Active Directory Users and Computers -> Domain2010265.cct right -> right click -> new Users.
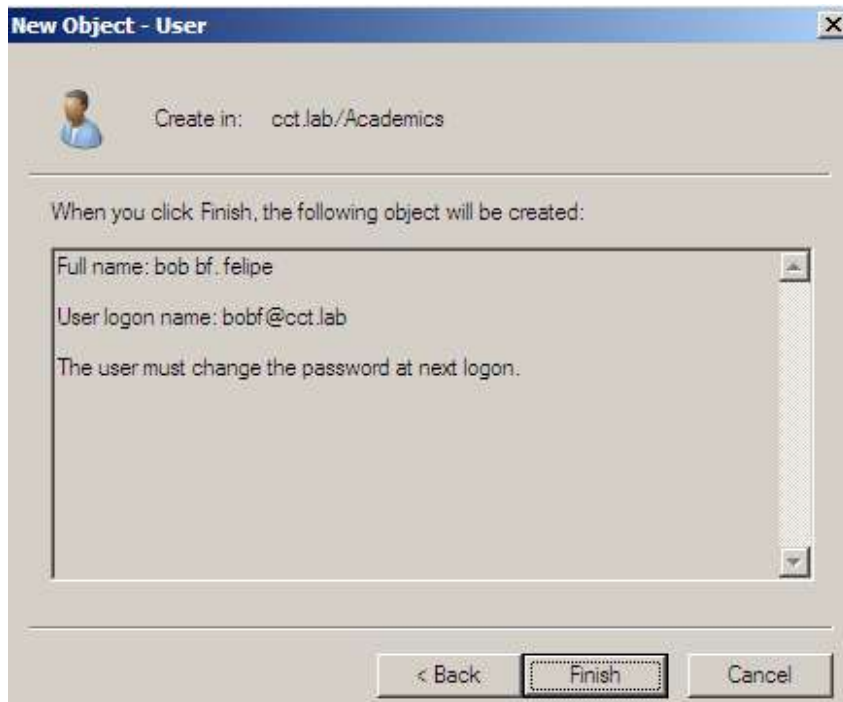
Creating a user for Academic:
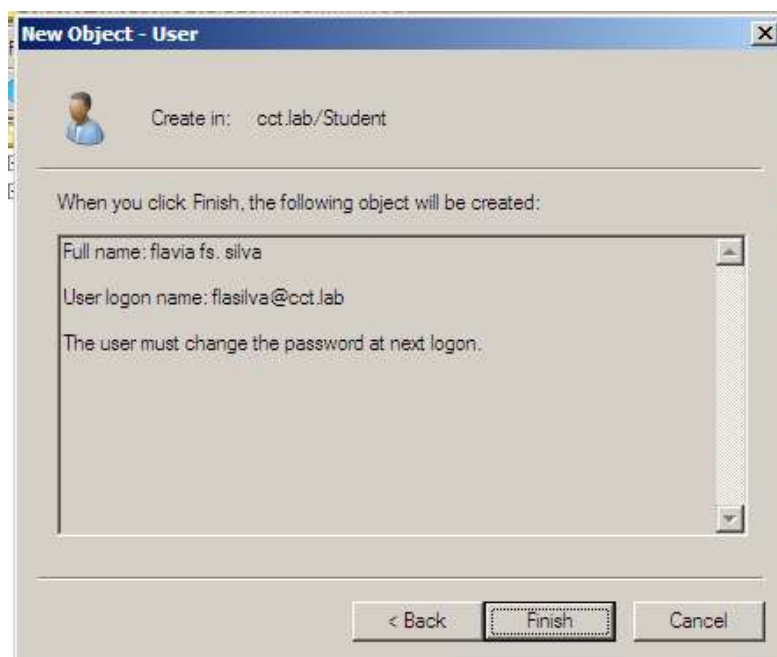
Figure 30

Creating a user for Students:

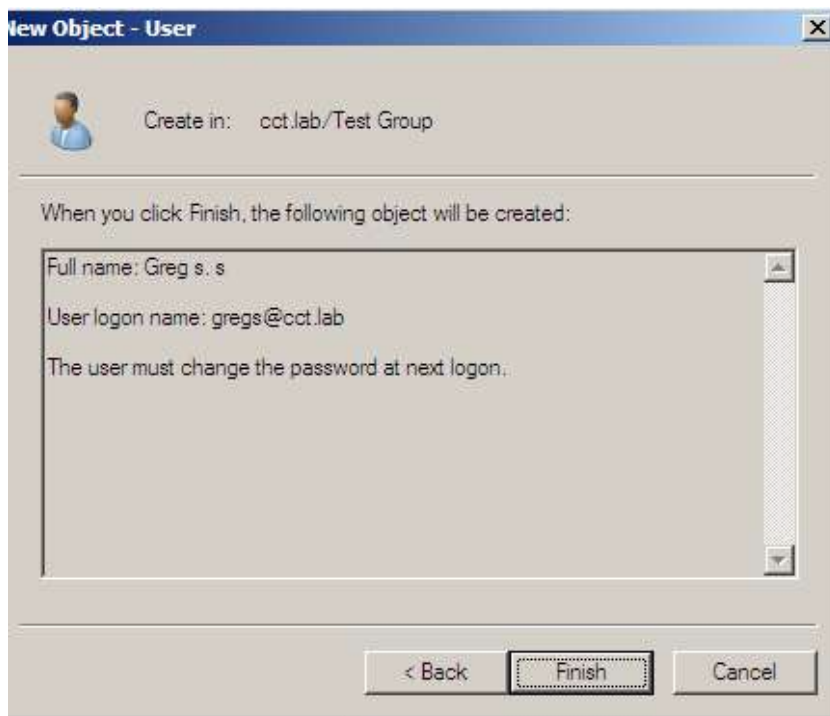

Figure 31

Creating test user:

Figure 32

12) Use the group policy editor to create 6 separate policies (3 x Students and 3 x Academics)

o Ensure to print screen these policies and briefly describe why you choose each

one

Students:

1.The first policy I have chosen for student is Prohibit Access to the control Panel Properties in my opinion I think is very important It prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items. It removes Control Panel from the Start screen and File Explorer, and removes PC Settings from the Start screen, Settings charm, Account picture and Search results. If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.
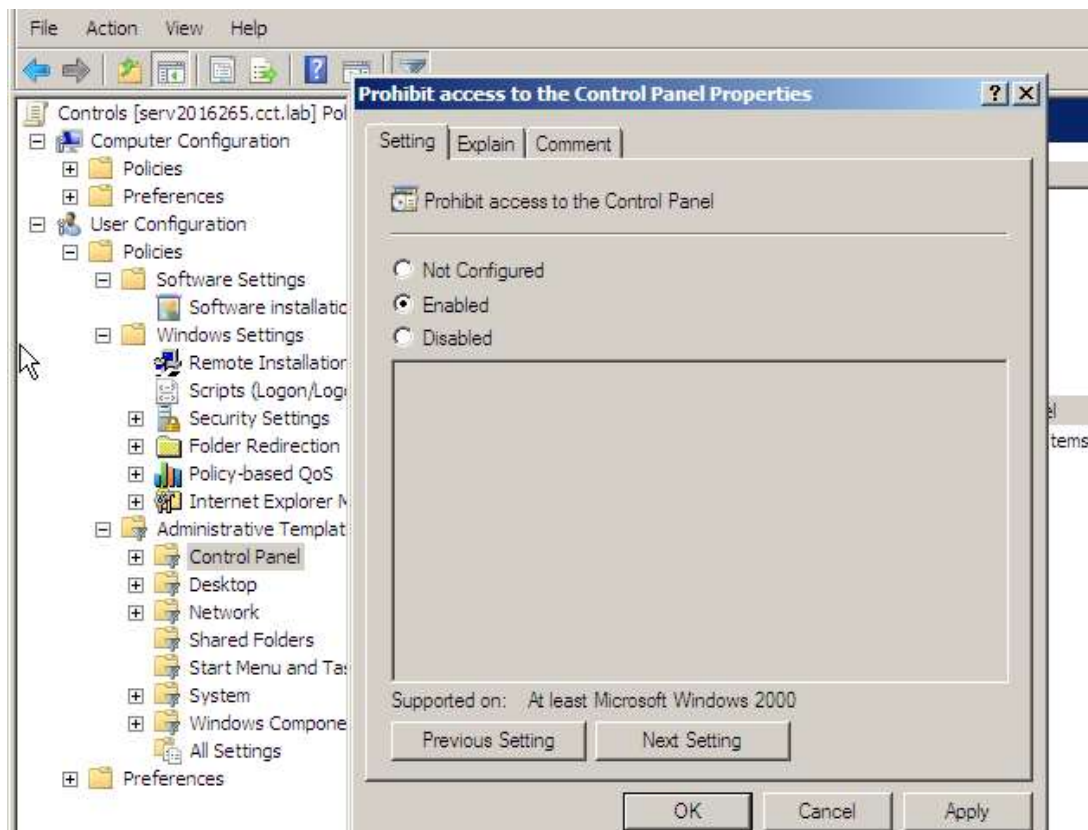
Figure 33

2.I choose to do not enable user to delete printers- that will prevent users from deleting local and network printers I think is important because a user sometimes wants a different printer such as pdf one instead the one previously installed they try to reinstall another one when they find available or mapped in another network.
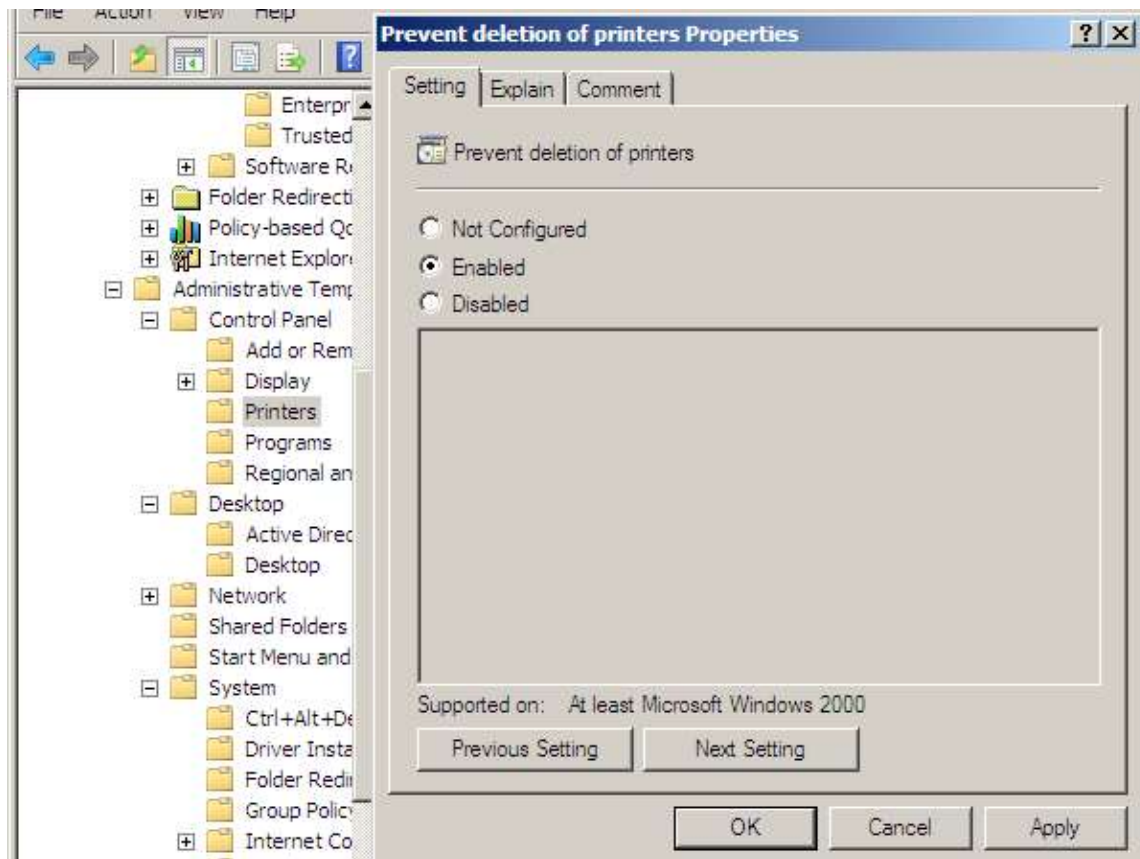
Figure 34

3.In my opinion another important one is do not allow that group of students to remove or install programs because if a student belogs to a student group they should be able to acess only specific tools for work in that moment, do not allow them to install unecessary programs and to not compromise the security of their workstation.
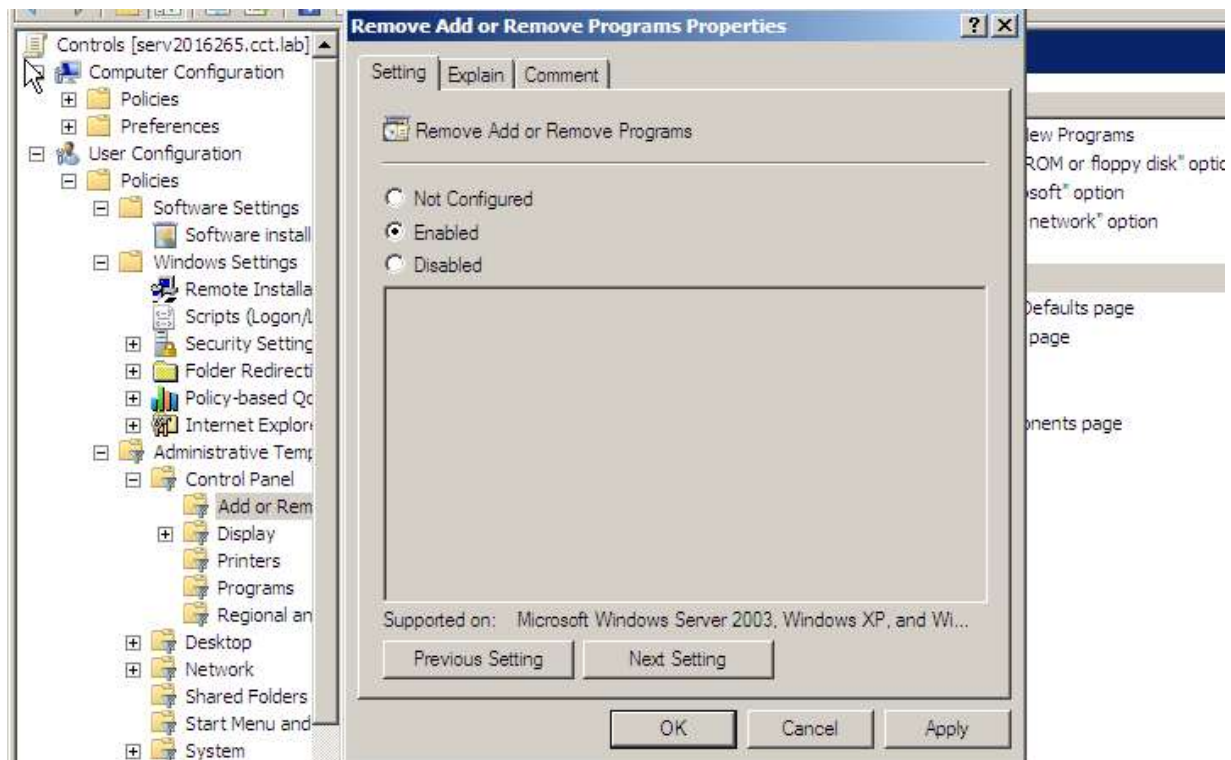
Figure 35

Academics:

1.For an academic group I think for secure reasons (important information) would be useful to have an account lockout after a few numbers of attempts, that means if a user cannot remember their password and try at least 6 times they will be locked at least for a certain period of time.
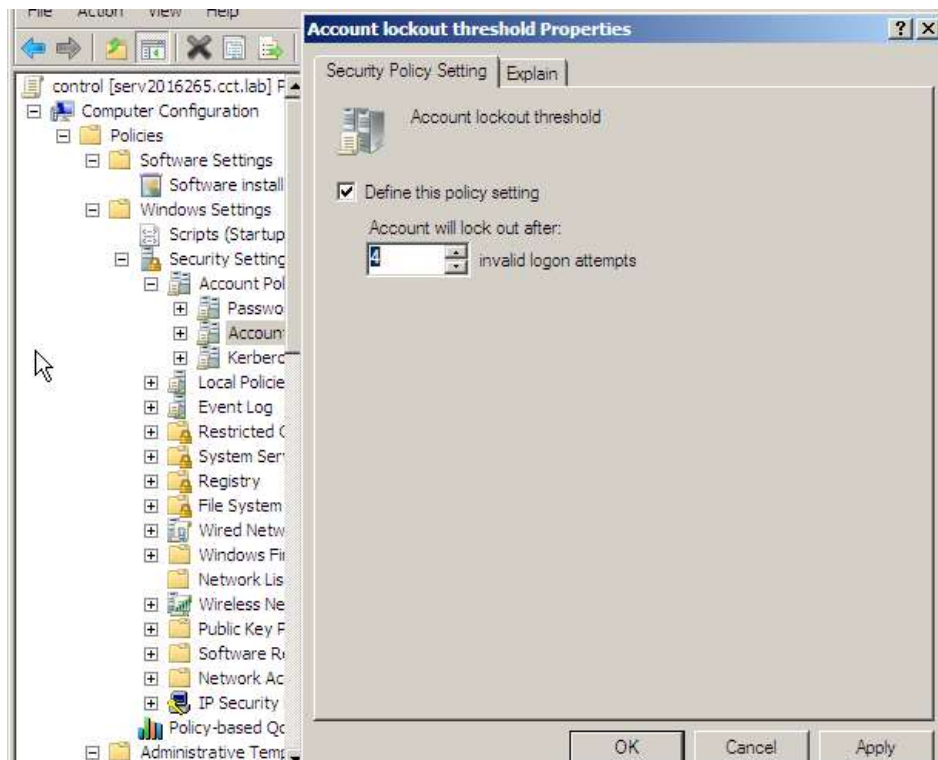
Figure 36

2. In my opinion another important policy is asking for a user change their password after a couple of days, using that policy users must change their will expire in 42 days, its one security tip for computer users is to constantly change your passwords to something new
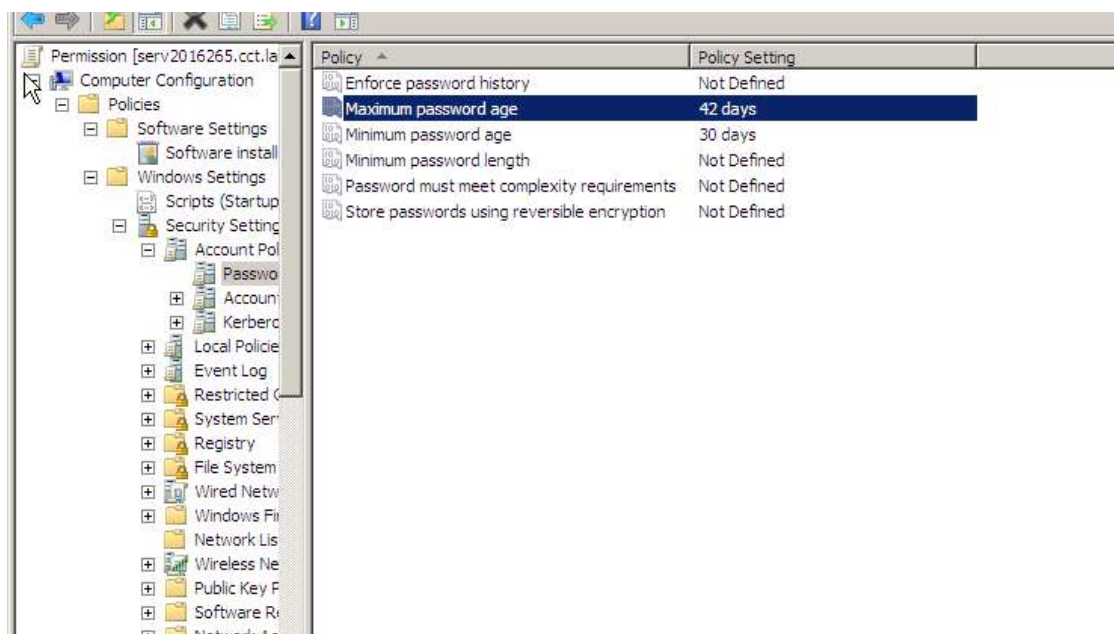

Figure 37

3.Device Installation Restrictions will prevent users to plug and play devices such as USB, Memory stick, new devices cannot be installed and existing devices cannot be updated
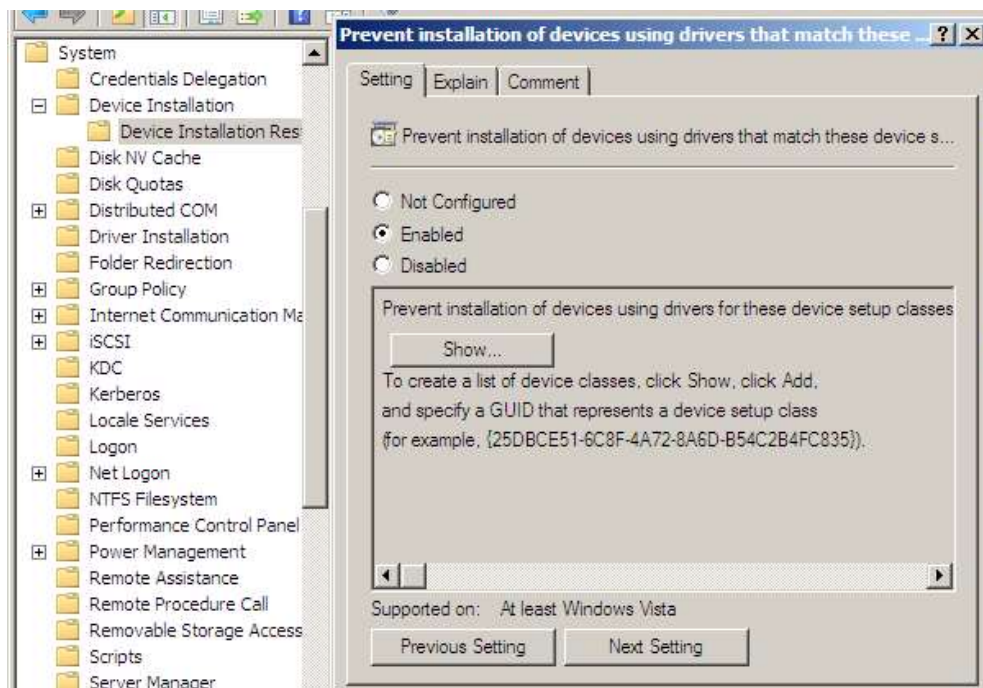

Figure 38