

Module Title: Network Service Management & Virtualization

Assignment Type: Practical (submitted as report)

Project Title: Assessment 2 DNS, DHCP & Group Policy

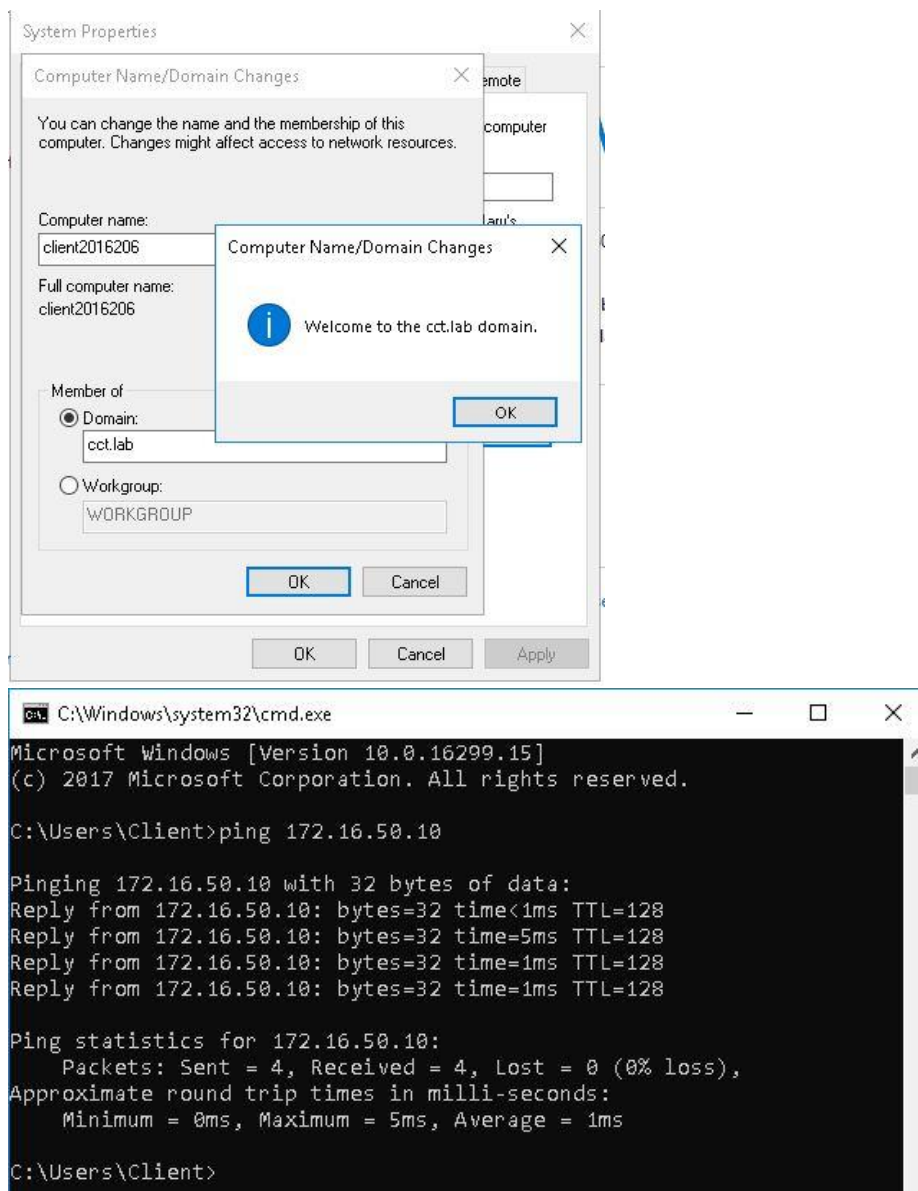
Assignment Compiler: Greg South

College of computer training

(CCT)

Specific Requirements

- 1) 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.
- 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).
- 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).
- 4) Assign the server a static IPv4 address using the following configuration.
- 5) Assign the client (initially) a static IPv4 address using the following configuration.
- 6) Convert the server into a Domain Controller.



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

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

Add Scope

A scope is a range of possible IP addresses for a network. The DHCP server cannot distribute IP addresses to clients until a scope is created.

Scope Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

Default Gateway (optional):

Subnet Type:

☒ Activate this scope

OK Cancel

Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[32], ser2016206.cct.lab., ...	4/19/2018 6:00:00 PM
(same as parent folder)	Name Server (NS)	ser2016206.cct.lab.	5/2/2018 1:00:00 PM
(same as parent folder)	Host (A)	172.16.50.10	4/19/2018 6:00:00 PM
client2016206	Host (A)	172.16.50.100	4/19/2018 6:00:00 PM
ftp	Host (A)	172.16.50.104	static
mx	Host (A)	172.16.50.103	static
ser2016206	Host (A)	172.16.50.10	5/2/2018 1:00:00 PM
test	Host (A)	172.16.50.102	static
www	Host (A)	172.16.50.101	static
2016206	Alias (CNAME)	www.cct.lab	

Address Pool		
Start IP Address	End IP Address	Description
172.16.50.1	172.16.50.254	Address range for distribution
172.16.50.1	172.16.50.1	IP Addresses excluded from distribution
172.16.50.10	172.16.50.10	IP Addresses excluded from distribution
172.16.50.100	172.16.50.120	IP Addresses excluded from distribution

Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(same as parent folder)	Start of Authority (SOA)	[32], ser2016206.cct.lab., ...
(same as parent folder)	Name Server (NS)	ser2016206.cct.lab.
(same as parent folder)	Host (A)	172.16.50.10
client2016206	Host (A)	172.16.50.100
ftp	Host (A)	172.16.50.104
ser2016206	Host (A)	172.16.50.10
test	Host (A)	172.16.50.102
www	Host (A)	172.16.50.101
2016206	Alias (CNAME)	www.cct.lab
mx	Mail Exchanger (MX)	[10] 172.16.50.103

[

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.

- DHCP

No.	Time	Source	Destination	Protocol	Length	Info
30	19.175782	172.16.50.2	172.16.50.10	DHCP	361	DHCP Request - Transaction ID 0xf6d526d4
31	19.177331	172.16.50.10	172.16.50.2	DHCP	342	DHCP ACK - Transaction ID 0xf6d526d4
74	28.258631	172.16.50.2	172.16.50.10	DHCP	342	DHCP Release - Transaction ID 0xb0b6b6b6
103	34.863216	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb5523e4f
104	34.865824	172.16.50.10	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xb5523e4f
107	34.872176	0.0.0.0	255.255.255.255	DHCP	373	DHCP Request - Transaction ID 0xb5523e4f
108	34.873799	172.16.50.10	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xb5523e4f
183	37.388002	192.168.43.1	255.255.255.255	DHCP	351	DHCP Offer - Transaction ID 0xb5523e4f
186	37.390751	192.168.43.1	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xb5523e4f

> Frame 30: 361 bytes on wire (2888 bits), 361 bytes captured (2888 bits) on interface 0
> Ethernet II, Src: PcsCompu_6e:dc:af (08:00:27:6e:dc:af), Dst: PcsCompu_5c:c1:b3 (08:00:27:5c:c1:b3)
> Internet Protocol Version 4, Src: 172.16.50.2, Dst: 172.16.50.10
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Request)

- DNS

The image shows a Wireshark packet capture of DNS traffic. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
257	1051.183691	192.168.192.49	8.8.8.8	DNS	130	Standard query 0x0860 SRV _ldap._tcp.ca5b877b-c7f5-4634-85f9-ccc8f39b21e8.domains._msd
258	1051.197489	8.8.8.8	192.168.192.49	DNS	205	Standard query response 0x0860 No such name SRV _ldap._tcp.ca5b877b-c7f5-4634-85f9-ccc
259	1111.228819	192.168.192.49	8.8.8.8	DNS	119	Standard query 0xda26 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.cct.lab
260	1111.239396	8.8.8.8	192.168.192.49	DNS	194	Standard query response 0xda26 No such name SRV _ldap._tcp.Default-First-Site-Name._si
261	1111.241313	192.168.192.49	8.8.8.8	DNS	88	Standard query 0xa40f SRV _ldap._tcp.dc._msdcs.cct.lab
262	1111.256546	8.8.8.8	192.168.192.49	DNS	163	Standard query response 0xa40f No such name SRV _ldap._tcp.dc._msdcs.cct.lab SOA a.roo
263	1111.257998	192.168.192.49	8.8.8.8	DNS	130	Standard query 0xcdd1 SRV _ldap._tcp.ca5b877b-c7f5-4634-85f9-ccc8f39b21e8.domains._msd
264	1111.271537	8.8.8.8	192.168.192.49	DNS	205	Standard query response 0xcdd1 No such name SRV _ldap._tcp.ca5b877b-c7f5-4634-85f9-ccc

The packet details pane shows the selected packet (No. 257) details:

- Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
- Ethernet II, Src: PcsCompu_6e:dc:af (08:00:27:6e:dc:af), Dst: SamsungE_9c:27:88 (20:00:00:00:00:00)
- Internet Protocol Version 4, Src: 192.168.192.49, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 59699, Dst Port: 53
- Domain Name System (query)

The packet bytes pane shows the raw data in hexadecimal and ASCII.

Overlaid on the Wireshark window is a Windows Command Prompt window showing the output of the 'ipconfig' command:

```

Administrator: Command Prompt

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : net
    Link-local IPv6 Address . . . . . : fe80::2dc7:3e7e:775d:ca7b%4
    IPv4 Address. . . . . : 192.168.192.49
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.192.1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:0:9d38:6abd:1c54:11f:3f57:3fce
    Link-local IPv6 Address . . . . . : fe80::1c54:11f:3f57:3fce%10
    Default Gateway . . . . . : ::

C:\Users\administrator>
  
```

Brief description:

First, IPCONFIG /RELEASE is executed to force the client to immediately give up its lease by sending the server a DHCP RELEASE notification which updates the server's status information and marks the old clients IP ADDRESS as "available". Then, the command IPCONFIG /RENEW is executed to request a new IP ADDRESS.

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

The image shows a Wireshark packet capture of DNS traffic. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
325	1294.855892	192.168.192.49	8.8.8.8	DNS	130	Standard query 0xb%4
326	1294.866846	8.8.8.8	192.168.192.49	DNS	205	Standard query response 0xb%4
327	1310.935375	192.168.192.49	8.8.8.8	DNS	119	Standard query 0xda26 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.cct.lab
328	1310.948935	8.8.8.8	192.168.192.49	DNS	194	Standard query response 0xda26 No such name SRV _ldap._tcp.Default-First-Site-Name._si
329	1325.979260	192.168.192.49	8.8.8.8	DNS	88	Standard query 0xa40f SRV _ldap._tcp.dc._msdcs.cct.lab
330	1326.018713	8.8.8.8	192.168.192.49	DNS	163	Standard query response 0xa40f No such name SRV _ldap._tcp.dc._msdcs.cct.lab SOA a.roo
331	1332.382552	192.168.192.49	8.8.8.8	DNS	130	Standard query 0xcdd1 SRV _ldap._tcp.ca5b877b-c7f5-4634-85f9-ccc8f39b21e8.domains._msd
332	1332.425565	8.8.8.8	192.168.192.49	DNS	205	Standard query response 0xcdd1 No such name SRV _ldap._tcp.ca5b877b-c7f5-4634-85f9-ccc

The packet details pane shows the selected packet (No. 325) details:

- Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
- Ethernet II, Src: PcsCompu_6e:dc:af (08:00:27:6e:dc:af), Dst: SamsungE_9c:27:88 (20:00:00:00:00:00)
- Internet Protocol Version 4, Src: 192.168.192.49, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 59699, Dst Port: 53
- Domain Name System (query)

The packet bytes pane shows the raw data in hexadecimal and ASCII.

Overlaid on the Wireshark window is a Windows Command Prompt window showing the output of the 'nslookup' command:

```

Administrator: Command Prompt - nslookup

IPv4 Address. . . . . : 192.168.192.49
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.192.1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

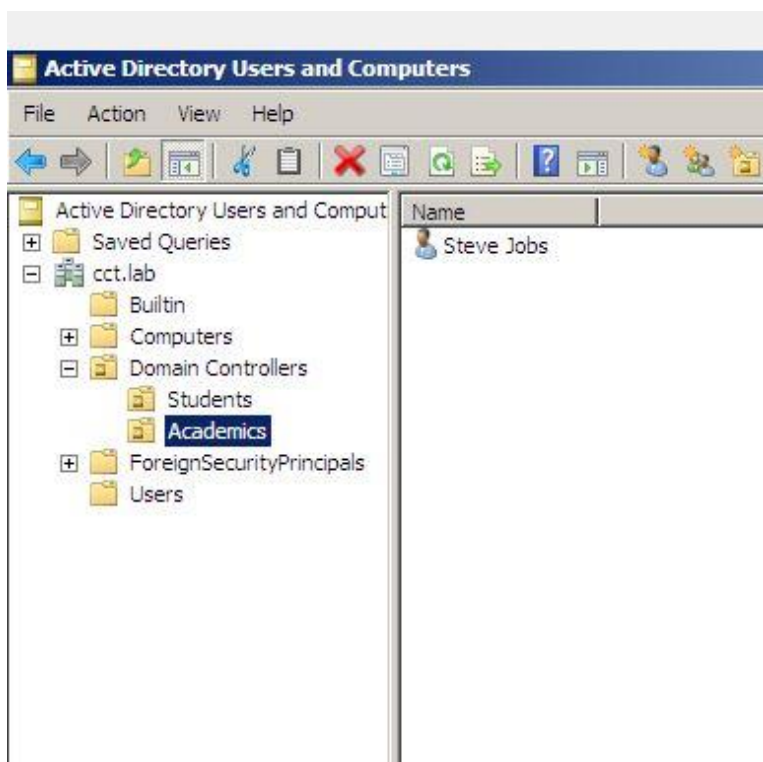
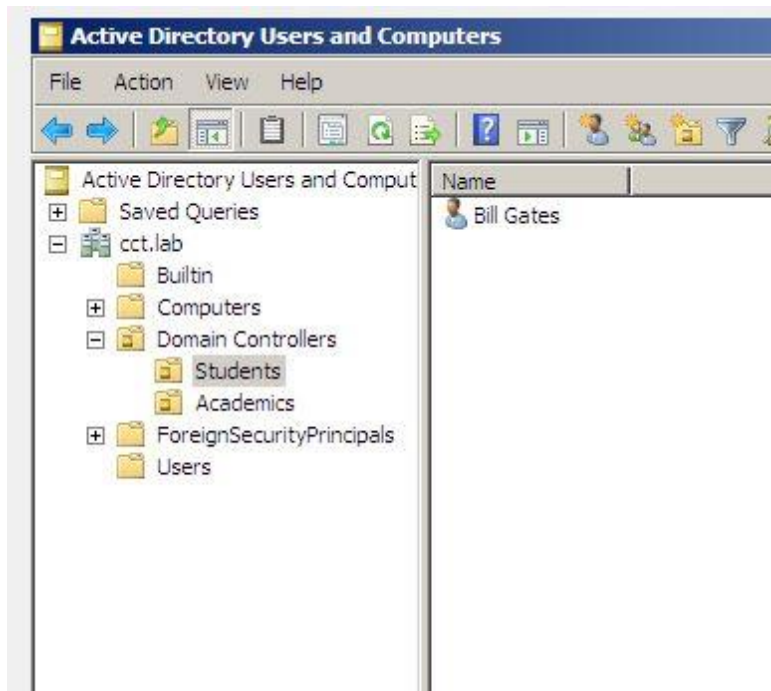
    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:0:9d38:6abd:1007:16df:3f57:3fce
    Link-local IPv6 Address . . . . . : fe80::1007:16df:3f57:3fce%10
    Default Gateway . . . . . : ::

C:\Users\administrator>nslookup
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8

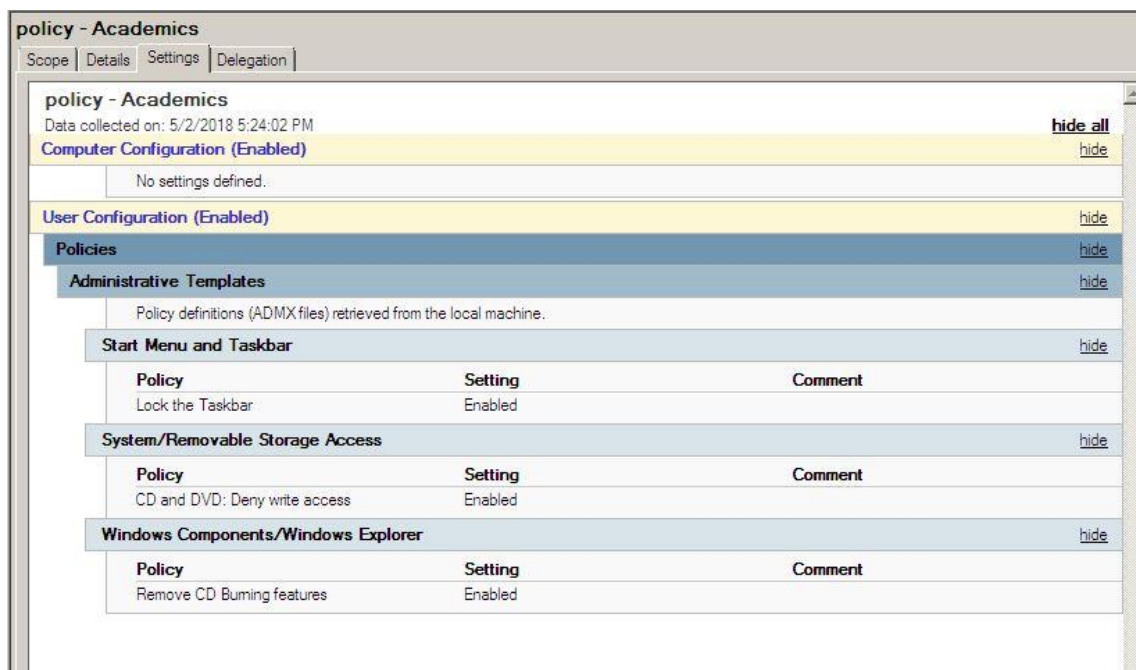
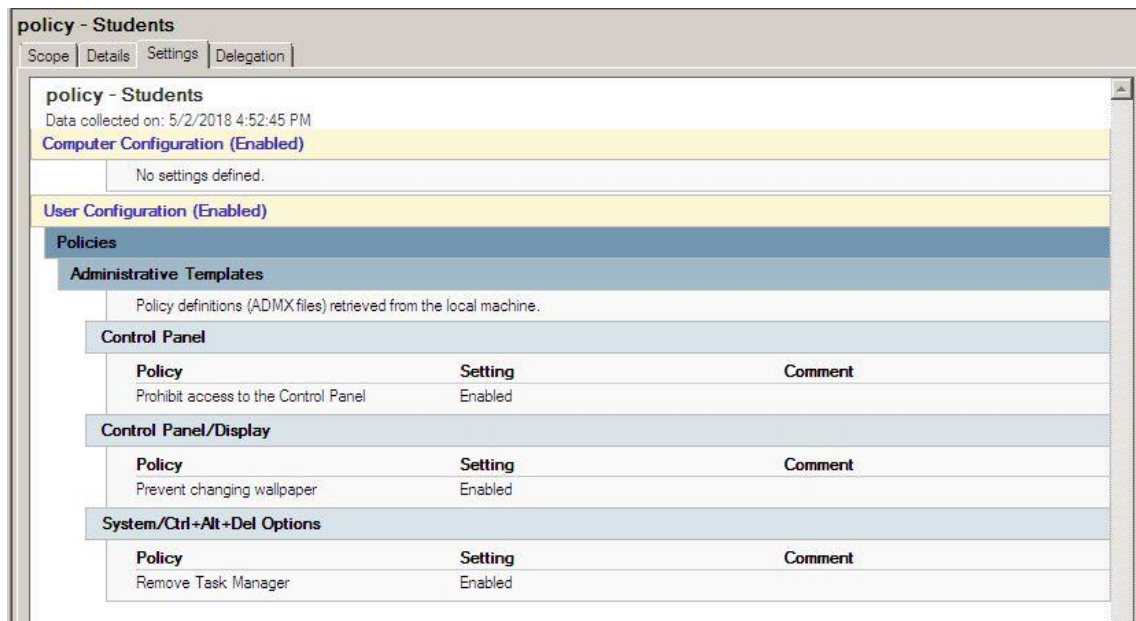
>
  
```

NSLOOKUP is the name of a program that lets an Internet server administrator or any computer user enter a host name (for example, "what.is.com") and find out the corresponding IP address. It will also do reverse name lookup and find the host name for an IP address you specify.

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).



12) Use the group policy editor to create 6 separate policies (3 x Students and 3 x Academics)
Ensure to print screen these policies and briefly describe why you choose each one. (Use research and referencing here.)



I went to approach the policies for student and academics I did small research on it and I tried to be reasonable about it because the windows provide a huge amount of policies for any type o security. Before to approach the policies it will depends of the field that you are like college field. In this case was a bit simple we could just give more freedom for academics and less for students. But both has limits in terms or security.

Prohibit access to the panel control

The reason why we might want to disable access to control panel on a Windows computer or server is to minimize the risk of exposing the computer settings to anyone. As we all know, in control panel we can find almost every configuration and settings on our computer; such as User Accounts, System and Security, Programs and Features, etc. These are all settings that we don't want somebody else to mess with. For that purpose, Windows gives a way to restrict control panel access. On a managed domain, administrators usually disable control panel access using Group Policy on Windows.

Prevent changing wallpaper

The Prevent changing wallpaper Group Policy prevents users from changing the desktop wallpaper by using Display Properties. However, there are ways of changing the wallpaper setting, such as through Image Preview, which does not involve Display Properties. By these other methods, users do not experience the limitations that apply to Display Properties. You must specify Active Desktop Wallpaper in Group Policy to prevent users from changing the desktop wallpaper without using Display Properties.

Remove task manager

Windows Task Manager is used to view details about processes running on your computer. Since it can be used to terminate programs that are misbehaving or are viruses disguised in the form of harmless programs, most spyware and viruses disable it to prevent themselves from being closed through it. Some administrators also disable Task Manager to prevent users from closing important security programs like antiviruses and anti-malwares.

Lock the task bar

Windows includes a special application desktop toolbar called the taskbar that shows on the bottom of a display screen by default. The taskbar allows you to find, see, open, and switch between your apps. You can also see the date and time, system icons, and items running in the background on the notification area. You can make the taskbar look how you want, manage your calendar, pin your favourite apps to it, change the size, change location on screen, and specify how taskbar buttons group together when you have more than one window open.

You must be signed in as an administrator to enable or disable "Lock the taskbar".

CD and DVD: Deny write access

This policy setting denies write access to the CD and DVD removable storage class. If you enable this policy setting write access is denied to this removable storage class. If you disable or do not configure this policy setting write access is allowed to this removable storage class.

Remove CD burning features

Let's say you are the IT admin of a school and you don't want the kids to bring in CDs or DVDs to copy the game setups from school's computer systems. You definitely would be pleased if you could just disable the CD/DVD burning feature in Windows.

Report /snapshots

Introduction

The purpose of this assignment was to create a virtual experiment, designed to test two virtual machines. This allowed us in a (realistic) way to learn how to work as a Network Administrator. We had to install features that are in Windows to get our devices and network up and running.

Working and doing tests helped to develop the knowledge that security is very important. For example, one tool, the firewall, is essential to prevent malicious access to any network. Also, when you are going to give access to the user, you shouldn't give too much permission to them in a company or college.

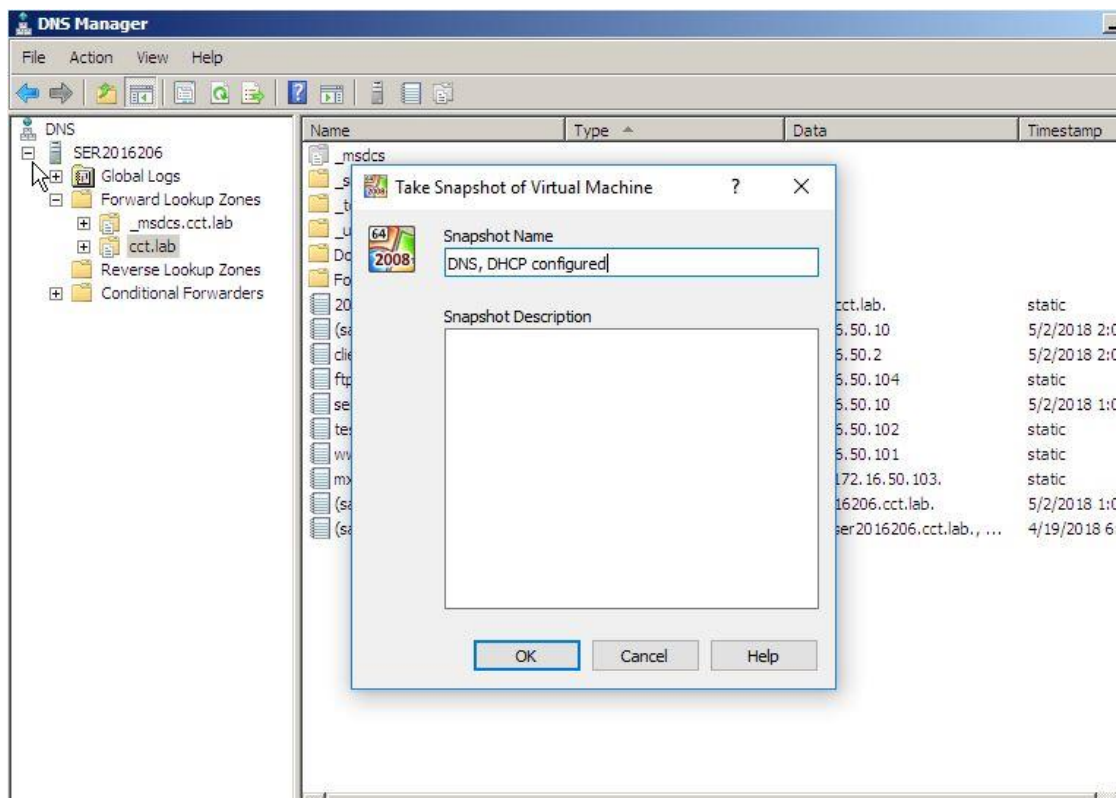
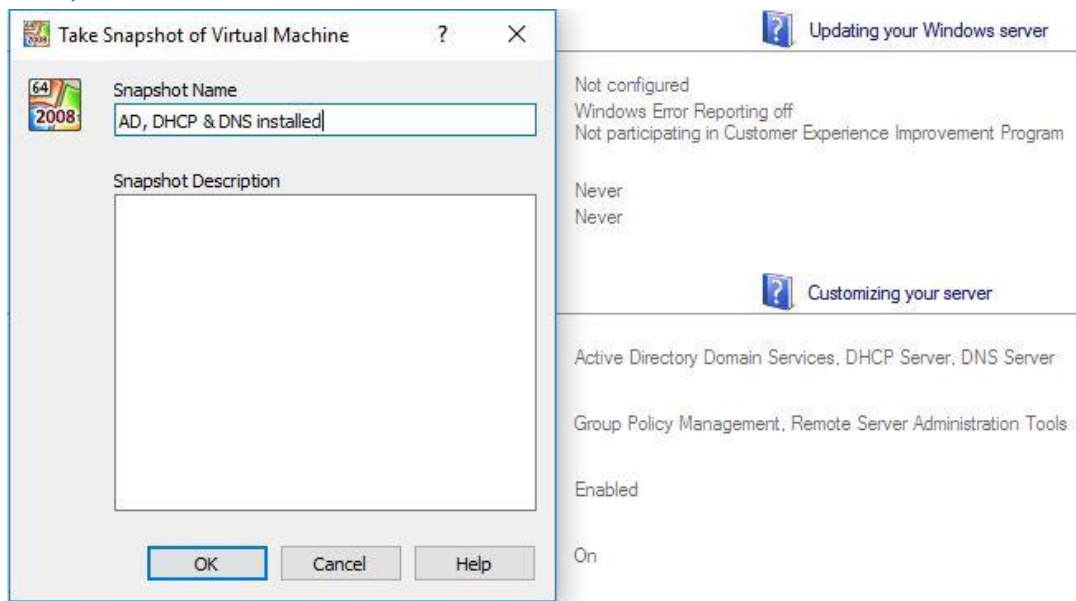
Methods

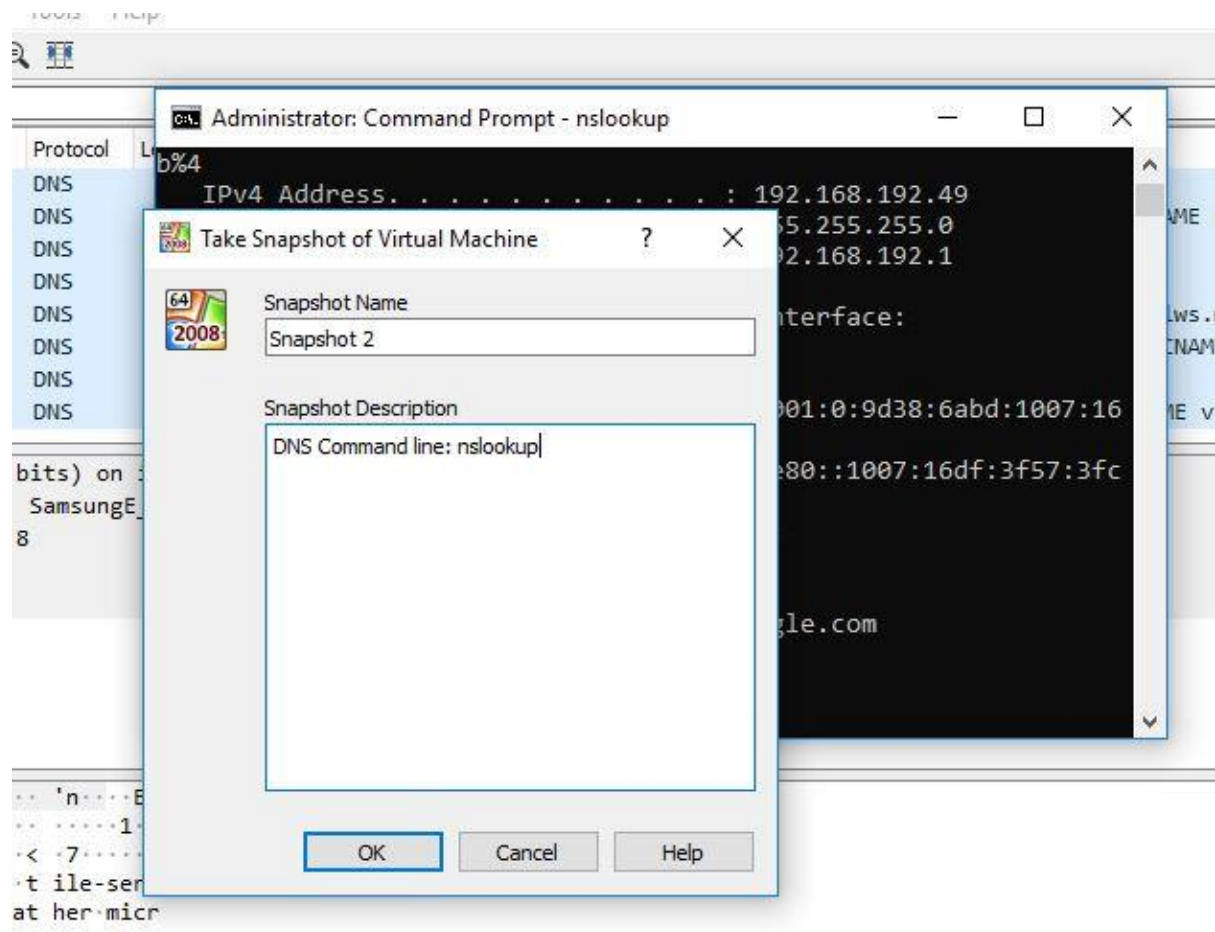
1. I created two virtual machines.
2. I had to create Organizational Units to connect the Academic department and the user student.
3. I set up security policies for the students and academics and take the snapshots
1. DNS resolves names to numbers and resolves domain names to I.P addresses. DNS also works like a phone book. When you want to find a number, you don't look up at the number first. You look up the name first, then it will give you the number.
2. DHCP provides an easier way to assign a computer. This is called Dynamic I.P. That is where a computer gets an I.P address from a DHCP server.
3. DHCP servers automatically assign a computer and I.P address and also assign a subnet mask, default gateway and DNS server.
4. Reservation ensures that a specific computer or device identified by using a MAC address always be given the same I.P address when that computer or device requests an I.P address from a DHCP server.

Conclusions

What was learned from doing this experiment was to have a better awareness of DNS, DHCP and the MAC address layer 2, which gives a permanent address. This task was achieved by using the Domain controller for the network to set up the groups as academic department and a user student, also by implementing the policy for the entire domain.

Snapshots





Research

<http://www.mustbegeek.com/disable-control-panel-access-using-group-policy-on-windows/>

<https://support.microsoft.com/en-ie/help/327998/you-can-change-the-desktop-wallpaper-setting-after-administrator-selec>

<https://www.tenforums.com/tutorials/104265-enable-disable-lock-taskbar-windows-10-a.html>

<https://merabheja.com/enable-disable-cddvd-burning-feature-windows-10/>

<https://searchnetworking.techtarget.com/definition/nslookup>