

Table of Contents:

Objective	3
Introduction	3
DNS	3
DHCP	4
Lab procedure	4
Part I: Packet tracer	4
Part II: in the Lab	10
Questions	21
Conclusion	24

Objectives:

At the end of this experiment, the student will be able to:

- Build a common network infrastructure.
- Get familiar with Windows 2012 as an example for NOS.
- Install and Configure DNS service and DHCP service.

Introduction:

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6)

How Does DNS work?

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to allocate the example.com webpage

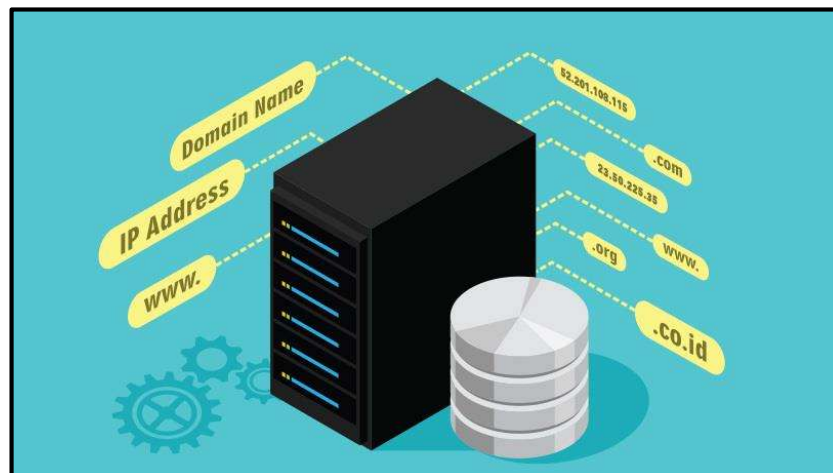


Figure 1: DNS service

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain required TCP/IP configuration information from a DHCP server.

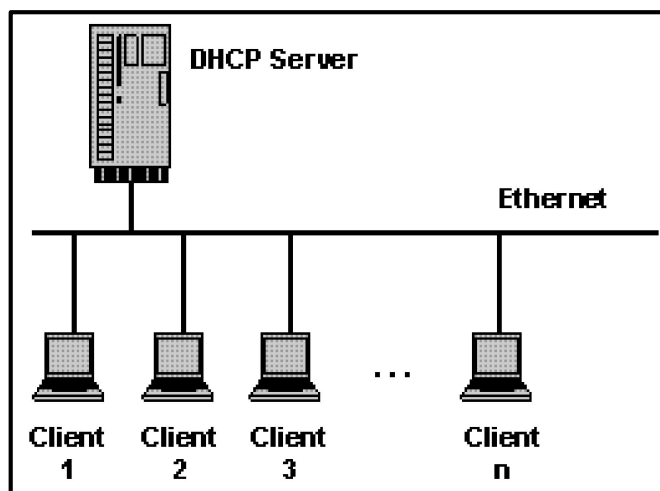


Figure 2: DHCP service

Lab Procedure:

Part I: Packet tracer

Example 1:

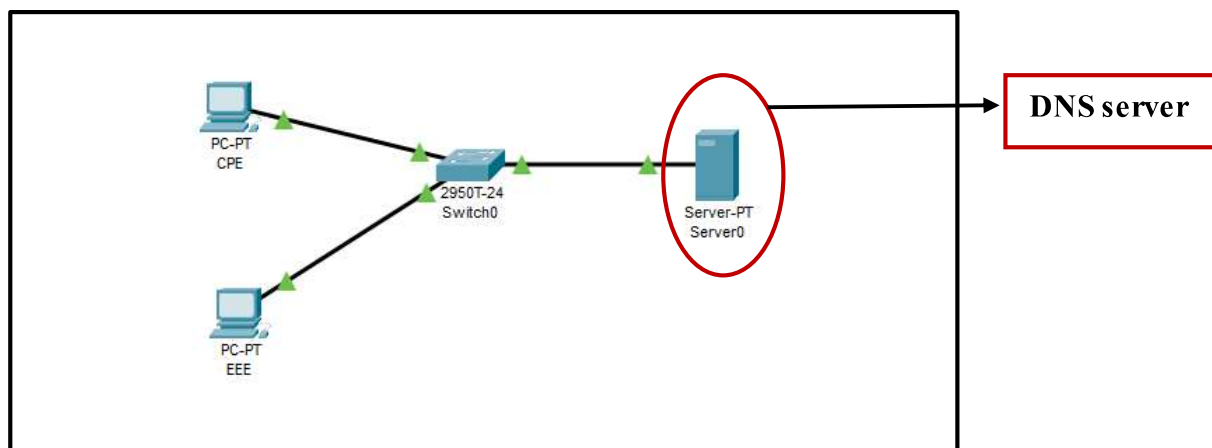


Figure 3: DNS server model

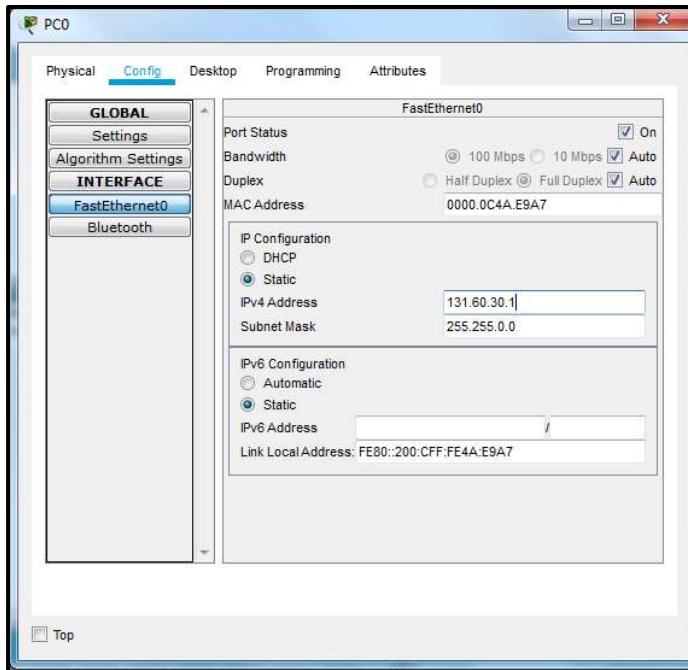


Figure 4: set IP address of PC0

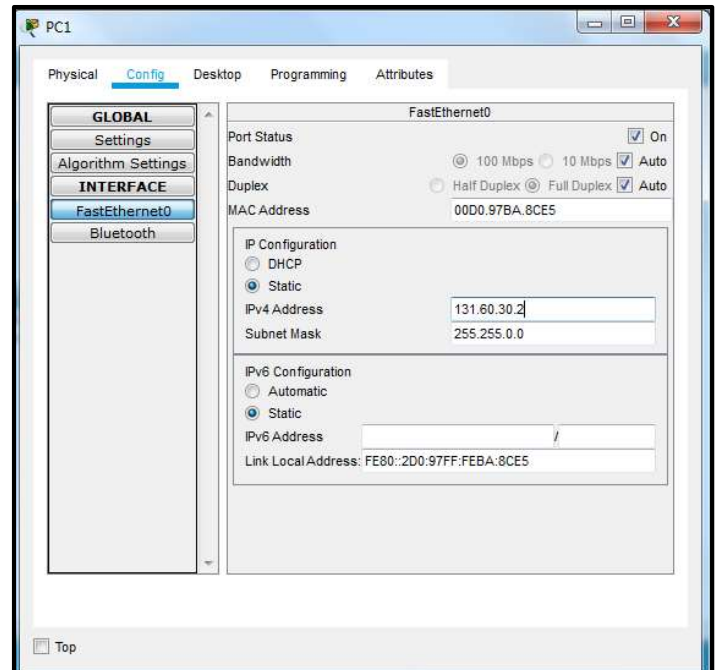


Figure 5: set IP address of PC1

As usual we give for each machine an IP address as shown in figure 4 and 5. And we change the name of PC0 to CPE and PC1 to EEE as in figure 3.

```
Packet Tracer PC Command Line 1.0
C:\>ping 131.60.30.2

Pinging 131.60.30.2 with 32 bytes of data:

Reply from 131.60.30.2: bytes=32 time=21ms TTL=128
Reply from 131.60.30.2: bytes=32 time<1ms TTL=128
Reply from 131.60.30.2: bytes=32 time<1ms TTL=128
Reply from 131.60.30.2: bytes=32 time<1ms TTL=128

Ping statistics for 131.60.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 21ms, Average = 5ms

C:\>ping EEE
Ping request could not find host EEE. Please check the name and try
again.
C:\>
```

Figure 6

When we tried to ping using an IP address we got replays

We didn't get reply when we pinged using machine name because we didn't configure the DNS server yet.

Server configuration:

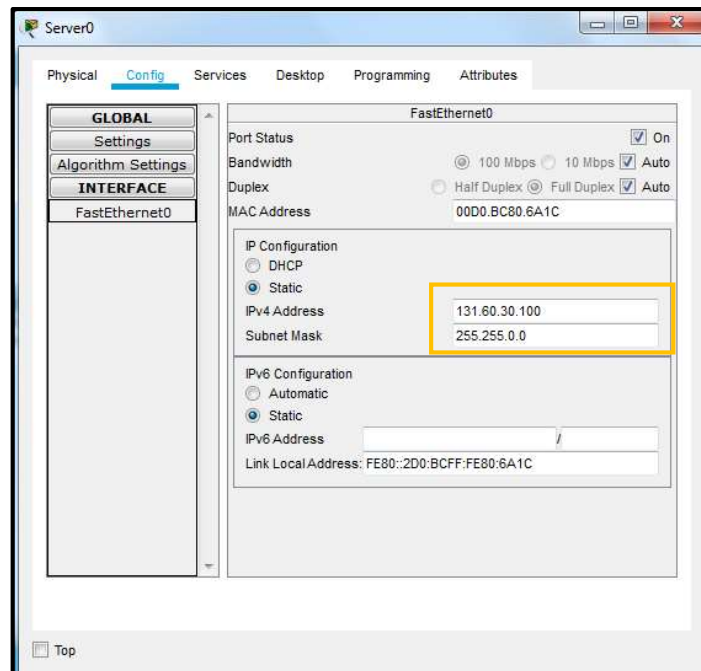


Figure 7

We set an IP address to the server by click on the config and write the IP address with same network IP but different host ID (131.31.20.100) as in figure 7.

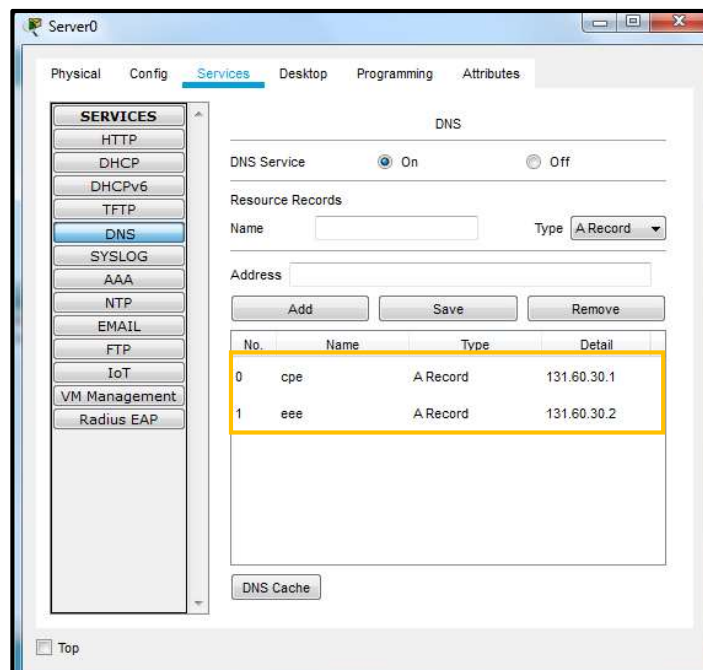


Figure 8

We click on the services bar and select DNS from the list and switch the server on and add the machines to the server with their IP address as in figure 8.

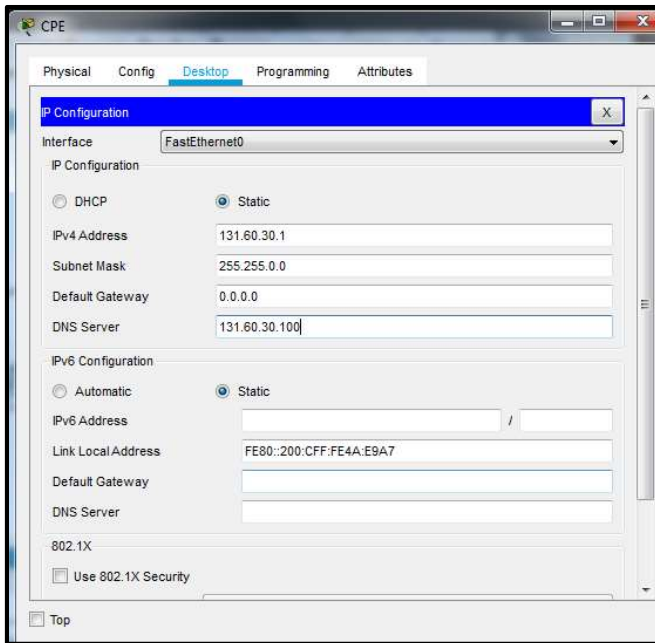


Figure 9

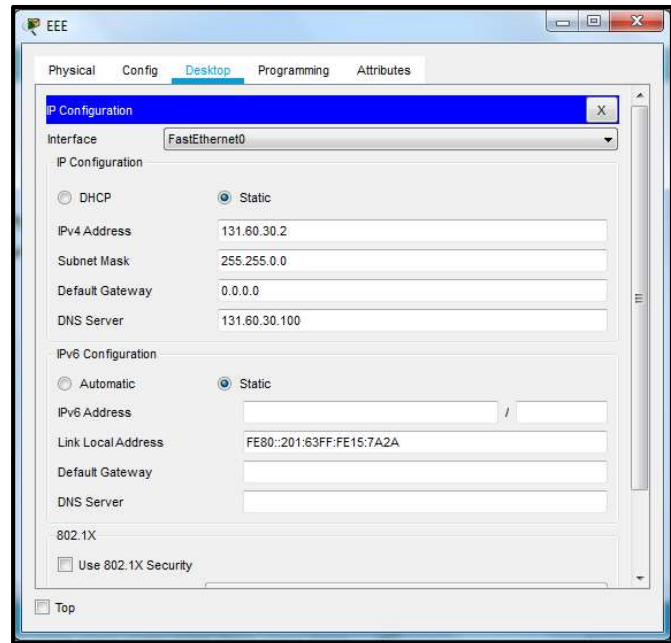


Figure 10

After setting the IP address to the server, we have to add the IP address of the DNS server to each PC as shown in above figures by click on the desktop bar then select IP config from the list

```
C:\>ping EEE

Pinging 131.60.30.2 with 32 bytes of data:

Reply from 131.60.30.2: bytes=32 time=69ms TTL=128
Reply from 131.60.30.2: bytes=32 time<1ms TTL=128
Reply from 131.60.30.2: bytes=32 time<1ms TTL=128
Reply from 131.60.30.2: bytes=32 time<1ms TTL=128

Ping statistics for 131.60.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 69ms, Average = 17ms
```

Figure 11

We try to ping the machines not by using machine name as in figure 11 to see if our configuration worked or not

```
C:\>nslookup

Server: [255.255.255.255]
Address: 255.255.255.255

>EEE
Server: [131.60.30.100]
Address: 131.60.30.100

Non-authoritative answer:
Name: eee
Address: 131.60.30.2

>CPE
Server: [131.60.30.100]
Address: 131.60.30.100

Non-authoritative answer:
Name: cpe
Address: 131.60.30.1
```

Using “nslookup” command on the server command window in order to see the mapping of each PC to its corresponding IP address

Figure 12

Example 2:

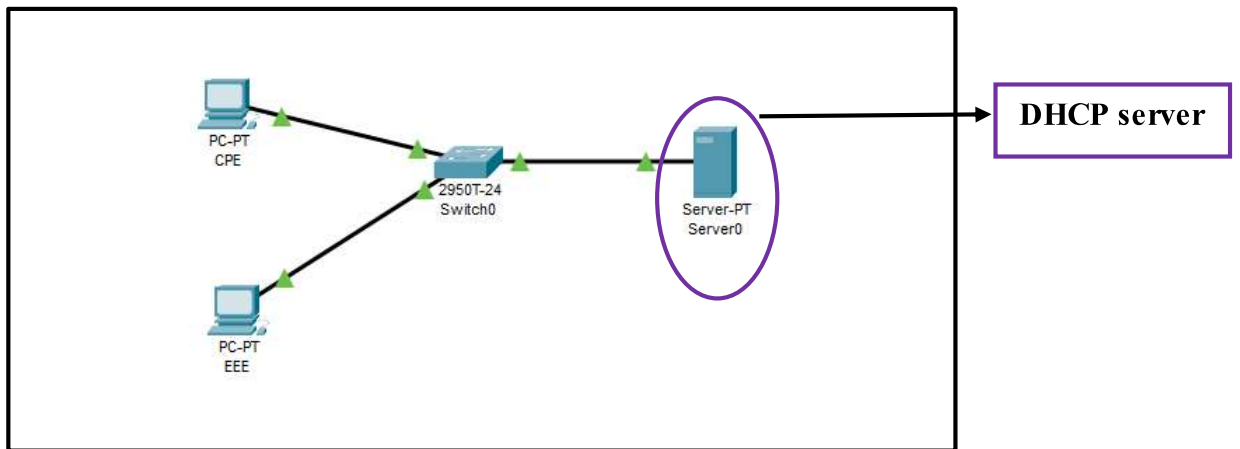


Figure 13: DHCP server model

In this part we set the IP address for each PC as well.

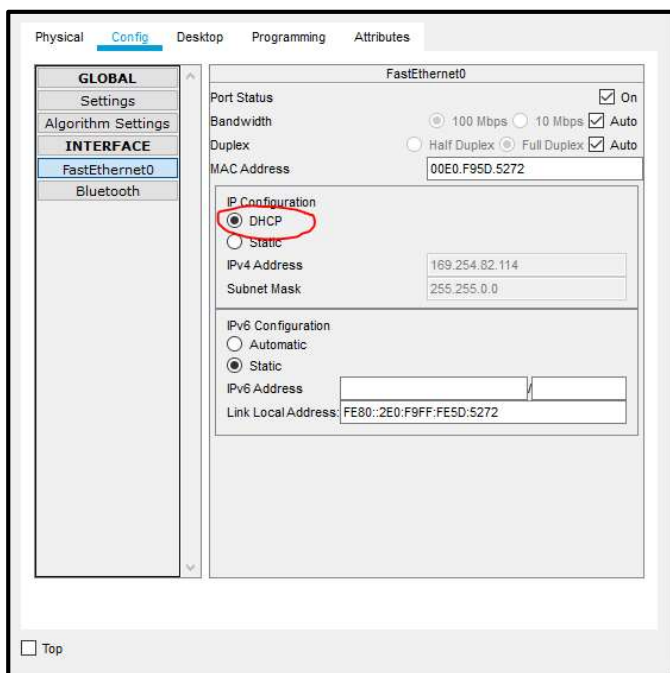


Figure 14: IP address of PC0

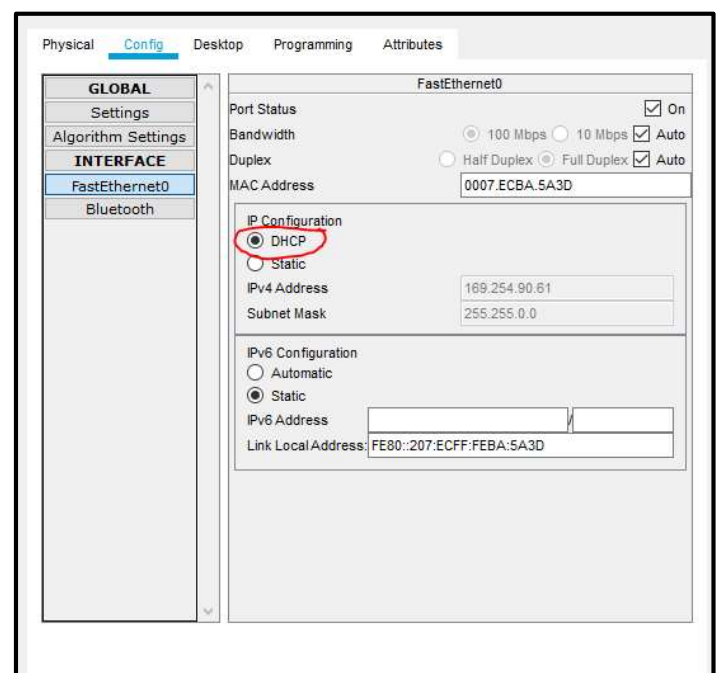


Figure 15: IP address of PC1

Then we give the server a static IP address before configuring it:

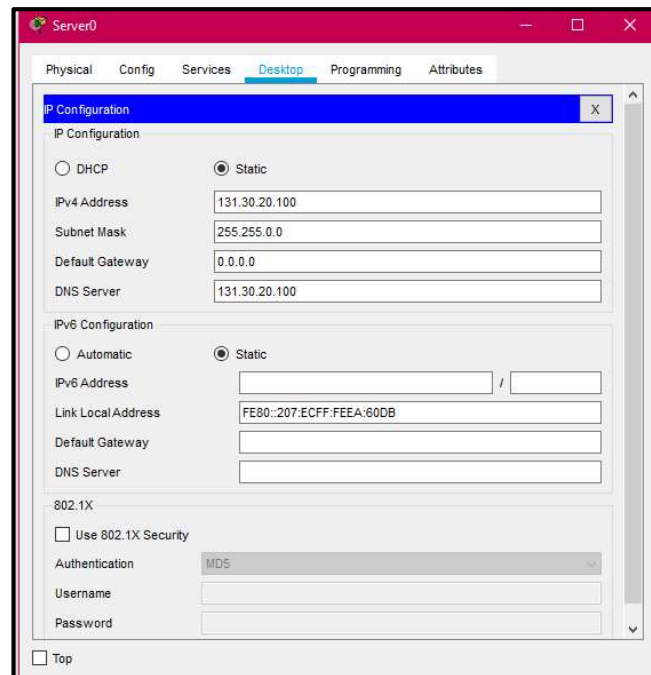


Figure 15

After, we configure the DHCP server and check the IP addresses of both clients on the server to see if they were given an IP address or not:

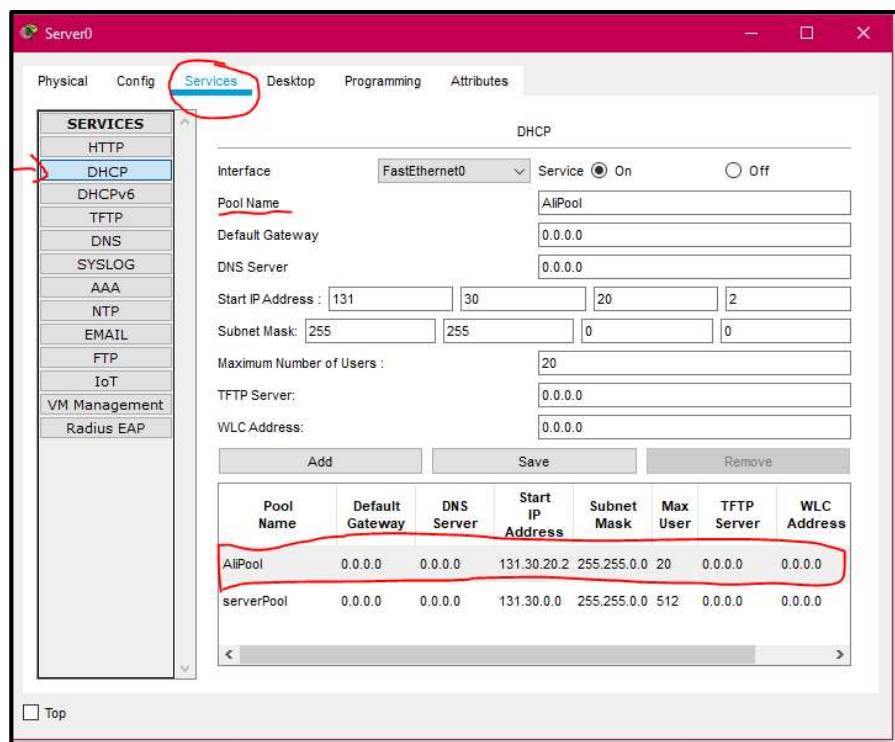


Figure 16


```

Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::207:ECFF:FEBA:5A3D
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 131.30.0.2
    Subnet Mask . . . . .: 255.255.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

C:\>

```

Figure 17

```

Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2E0:F9FF:FE5D:
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 131.30.0.1
    Subnet Mask . . . . .: 255.255.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

```

Figure 18

As we can clearly see both clients are connected and functional. Now we try to use the IP config release and renew command to see if it will regenerate the IP for the specific client we are working on:

```

    Default Gateway . . . . .: ::
                                0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

C:\>ipconfig /release

    IP Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: 0.0.0.0
    DNS Server . . . . .: 0.0.0.0

C:\>ipconfig /renew
Invalid Command.

C:\>ipconfig /renew

    IP Address . . . . .: 131.30.0.2
    Subnet Mask . . . . .: 255.255.0.0
    Default Gateway . . . . .: 0.0.0.0
    DNS Server . . . . .: 131.30.20.100

C:\>

```

Figure 19

Part II: in the Lab

DNS Role Installation Steps

Step 1: go to control panel, click on Network and Internet-> network and sharing center then click on change an adapter setting, assigned an IP address, preferably with a different host number as shown in figure 20

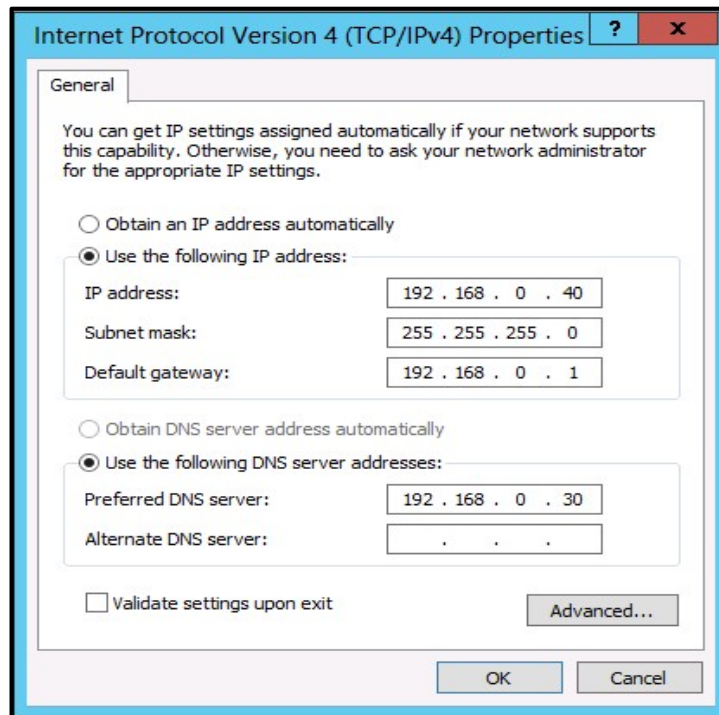


Figure 20

Step 2: go to insulation type and select as follows then press next

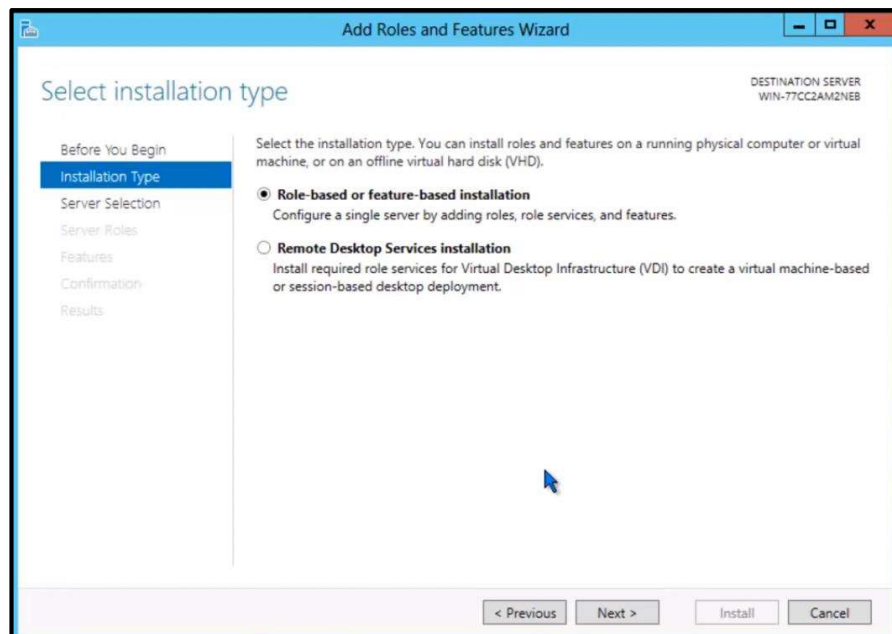


Figure 21

Step 3: a window will appear to you as in figure 22, since we are only deal with only one service, only one service is available.

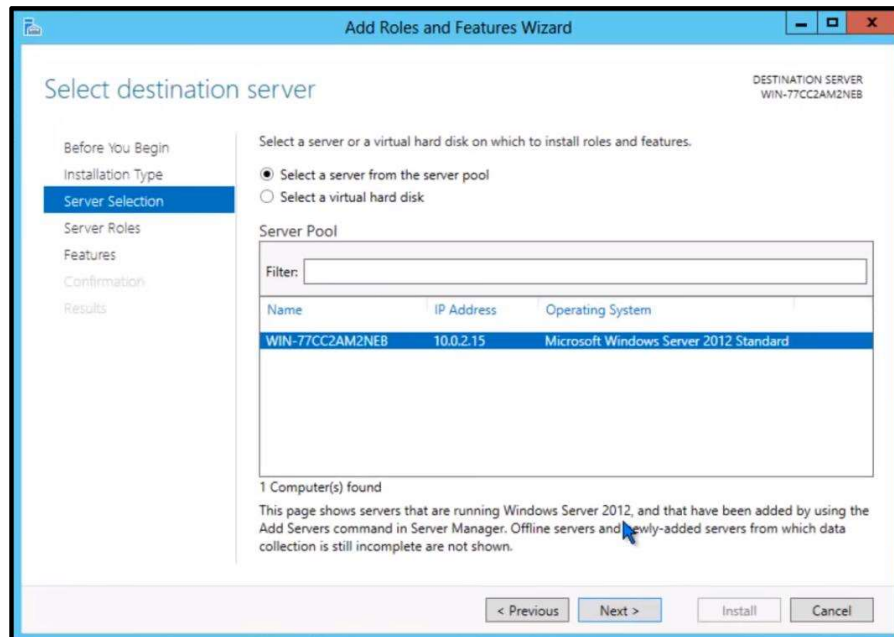


Figure 22

Step 4: select DNS server and click on Add feature as shown below

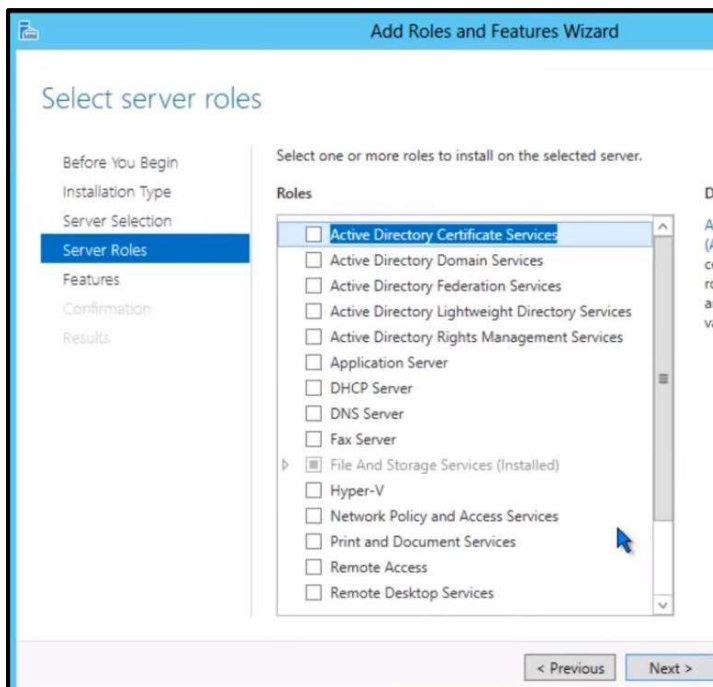


Figure 23

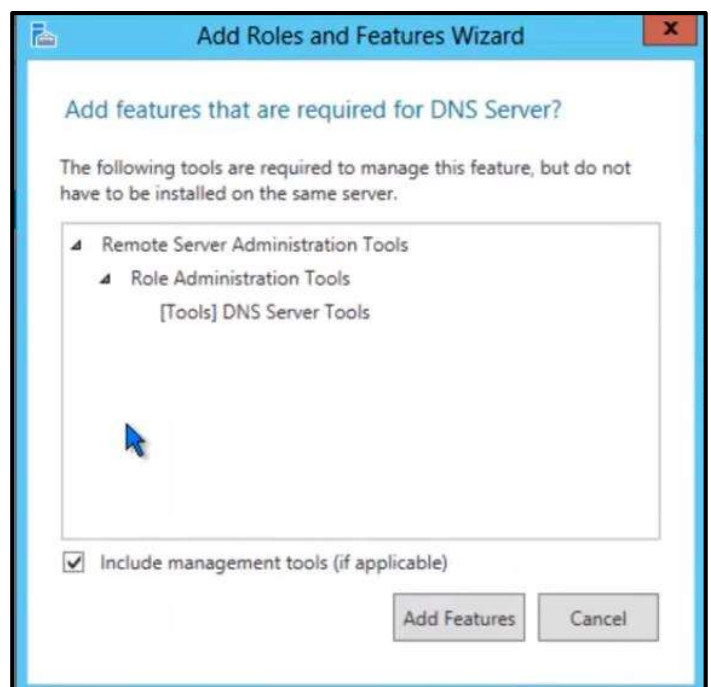


Figure 24

Step 5: click on insulation and once the insulation completed close the window.

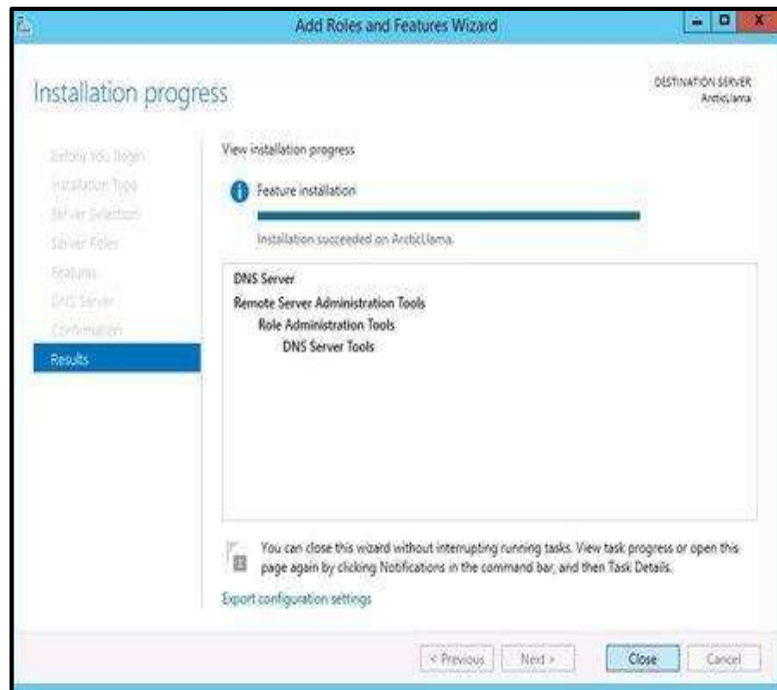


Figure 25

Step 6: go to start menu and click on DNS server that you install, then click on forward lookup and right click and select new Zone from the list as in figure 26. As in figure 27 click on next

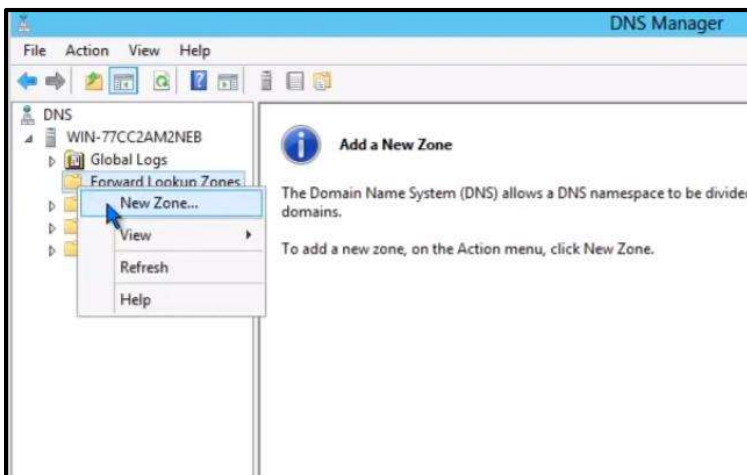


Figure 26



Figure 27

Step 7: do the following, and give the zone a name.

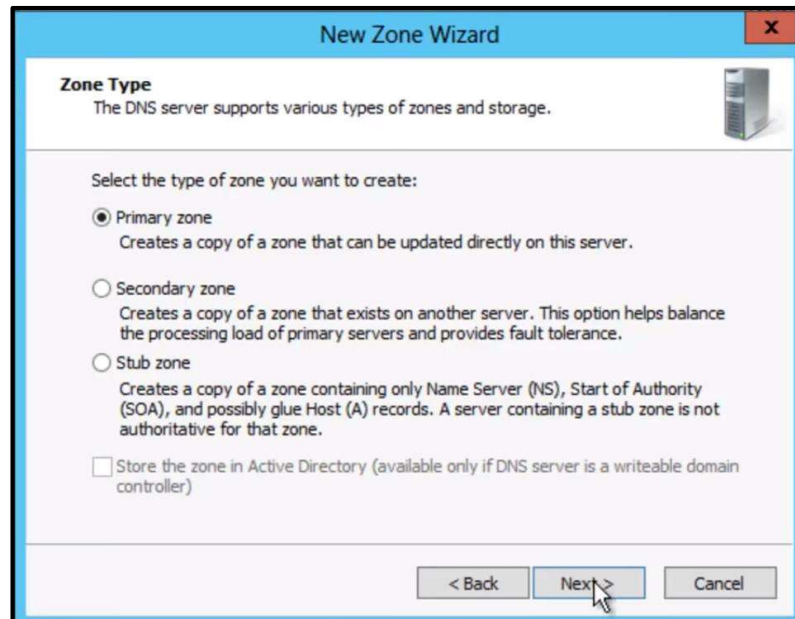
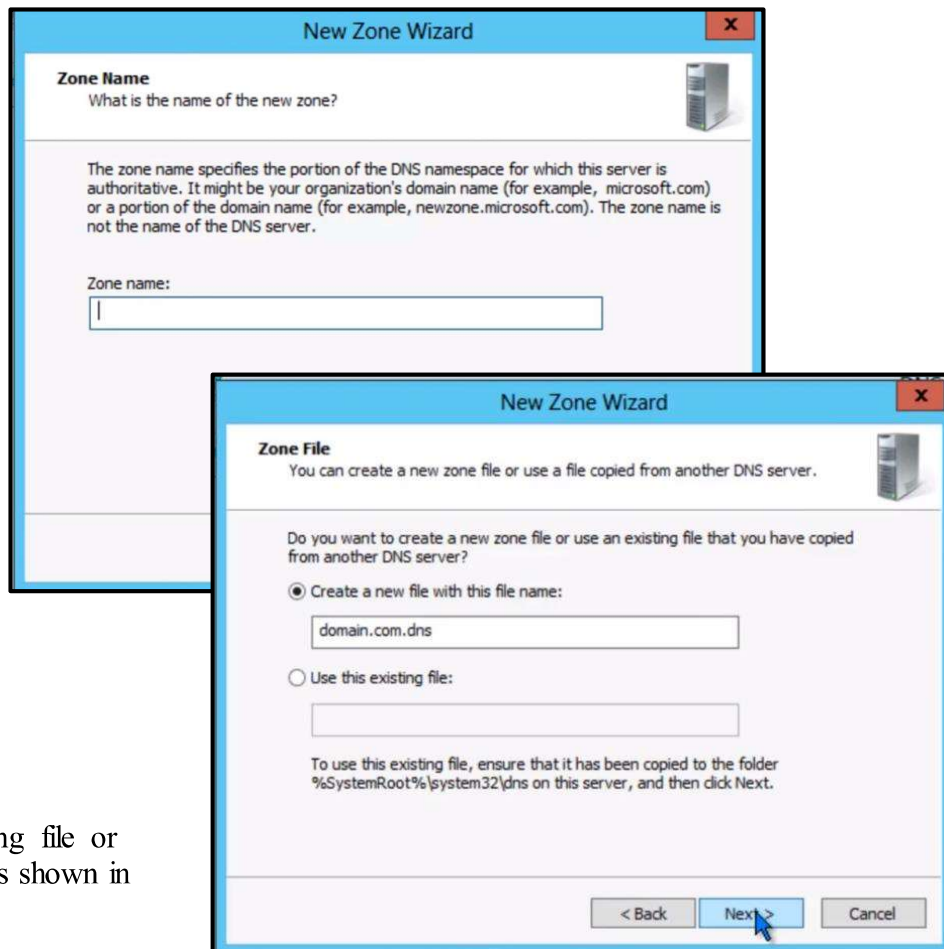


Figure 28



You can use existing file or create a new file as shown in figure 29

Figure 29

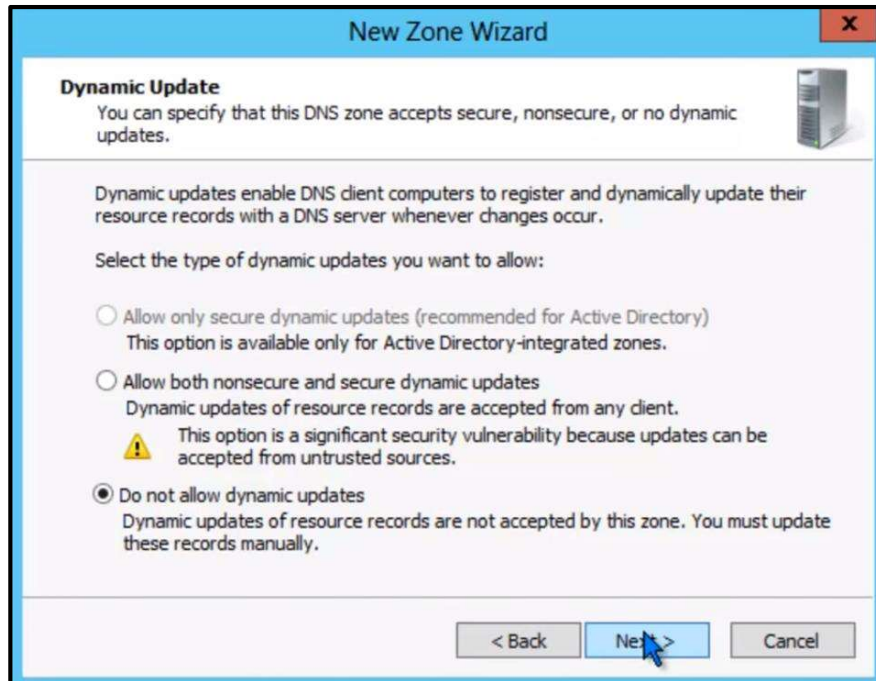


Figure 30

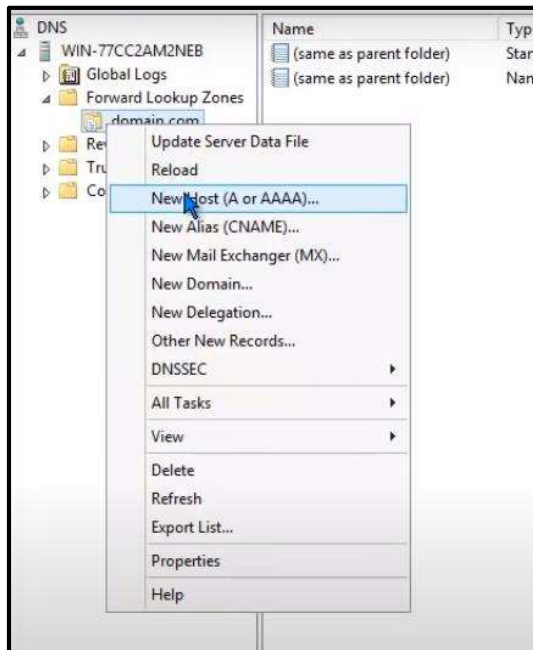


Figure 31

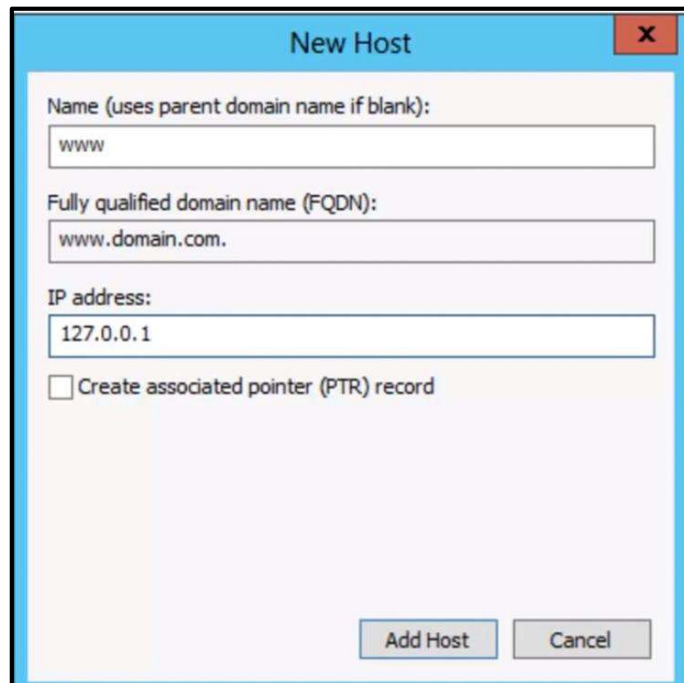


Figure 32

Click on Reverse lookup and right click and select new Zone from the list as in figure 33, then click next as in figure 34

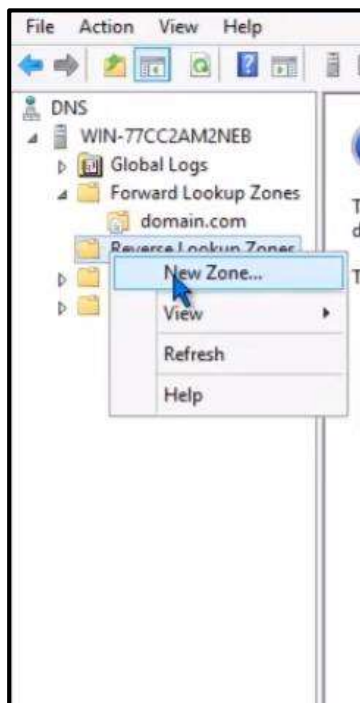


Figure 33



Figure 34

Set an IP address as in figure 35

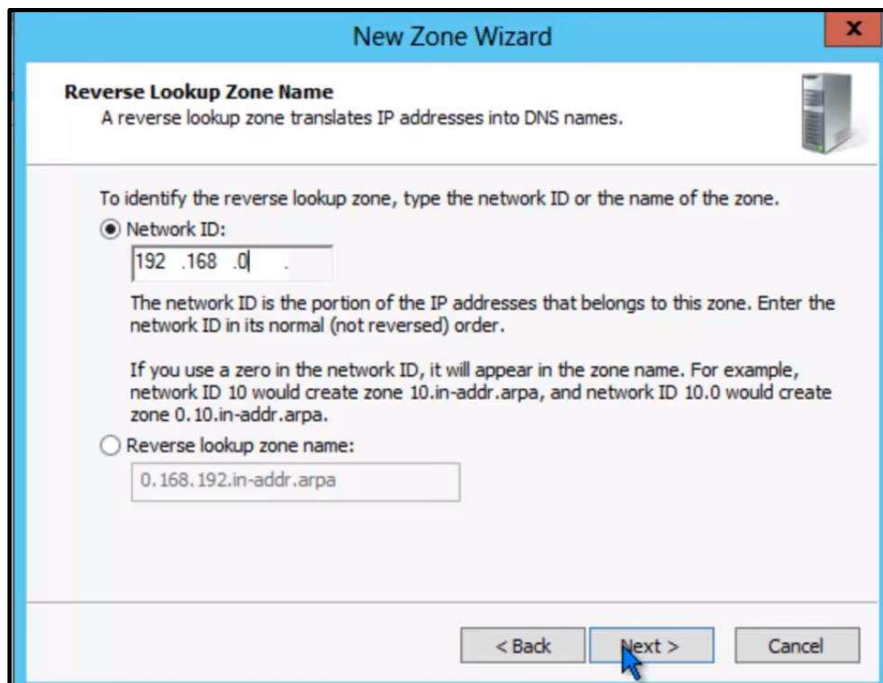


Figure 35

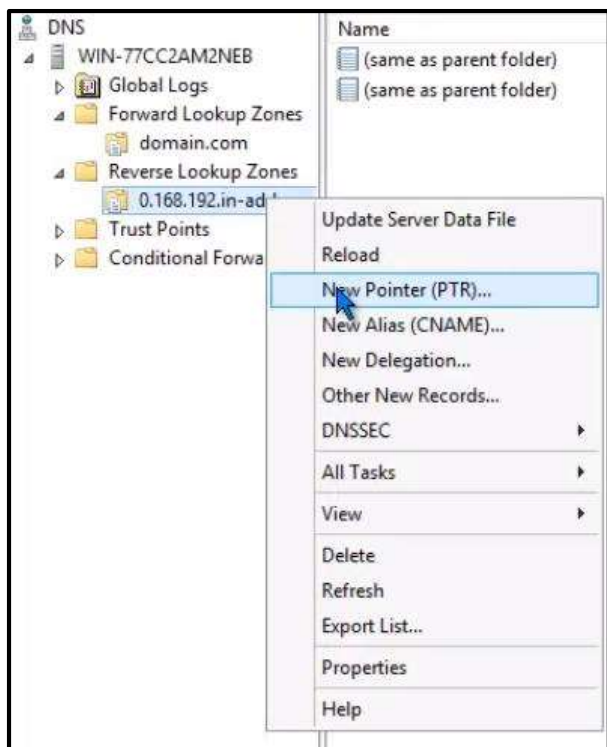


Figure 36

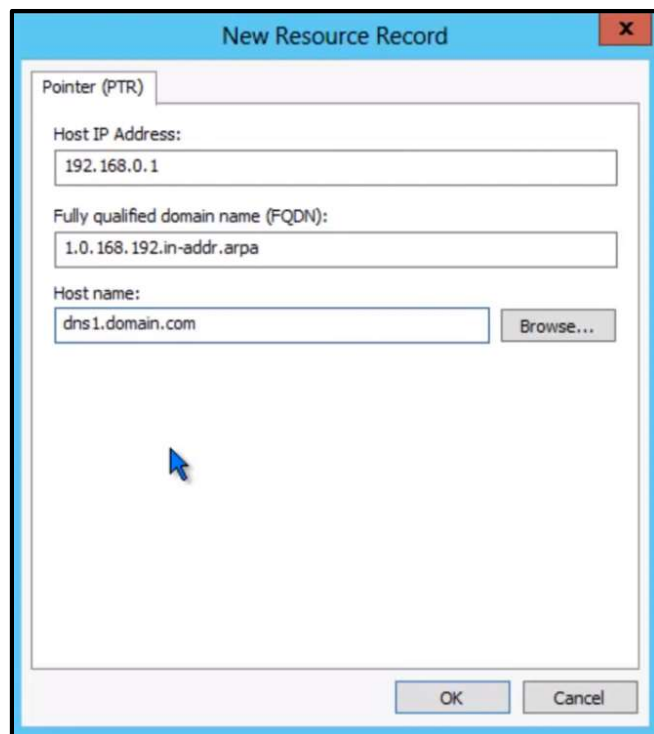


Figure 37

We test what we did by using “nslookup” utility in a command prompt as shown in figure 38

```
C:\Windows\system32>nslookup
Default Server: dns1.domain.com
Address: 192.168.0.1

> www.domain.com
Server: dns1.domain.com
Address: 192.168.0.1

Name: www.domain.com
Address: 127.0.0.1

> 192.168.0.1
Server: dns1.domain.com
Address: 192.168.0.1

Name: dns1.domain.com
Address: 192.168.0.1
```

Figure 38

DCHP Role Installation Steps

Step 1: after following the same steps we did to insulate DNS server, we choose the DHCP server from the list as in figure 39, then keep clicking next until you press install

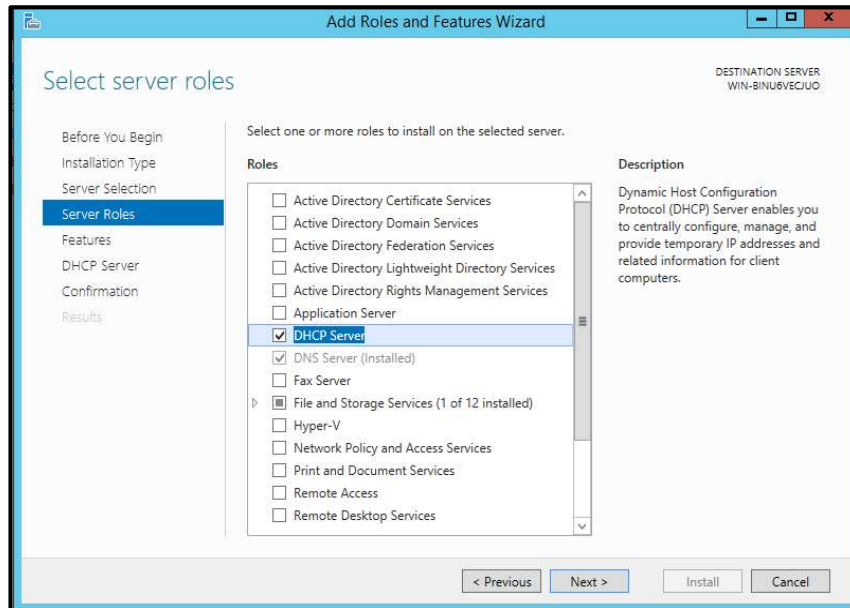


Figure 39

Step 2: once the insulation completed, right click on IPv4 and select new scope as figure 40 , a window will appear to you as figure 41 press next. Then we simply give it a name

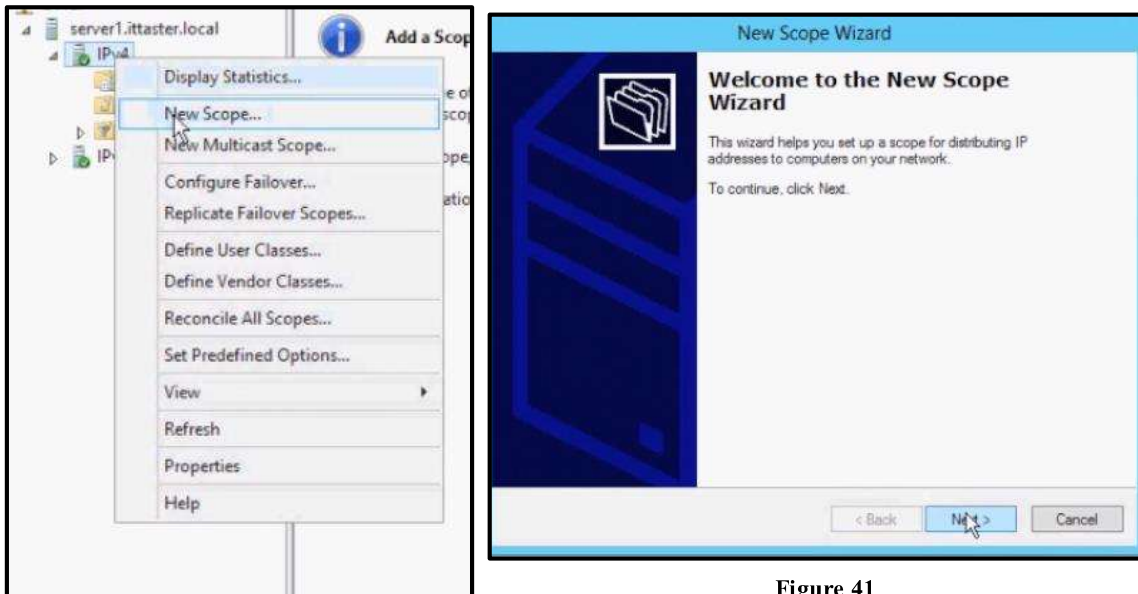


Figure 41

Figure 40



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.

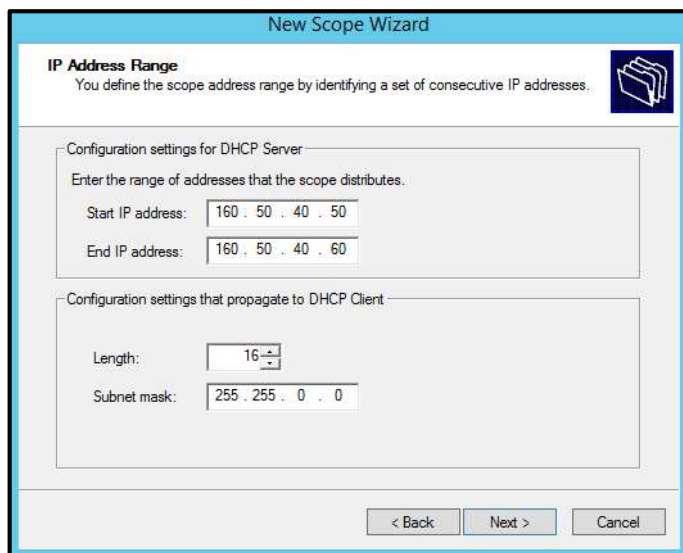
Name:

Description:

< Back Next > Cancel

Figure 42

Step 3: setup the range of IP Addresses that the scope distributes, In our example we used from 160.50.40.50 to 160.50.40.60 as in figure 43. We can add Exclusions and Delay IP Addresses in order to reserve them, In our example we added from 160.50.40.59 to 160.50.40.60 (they must be in the scope that you chose).



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:

End IP address:

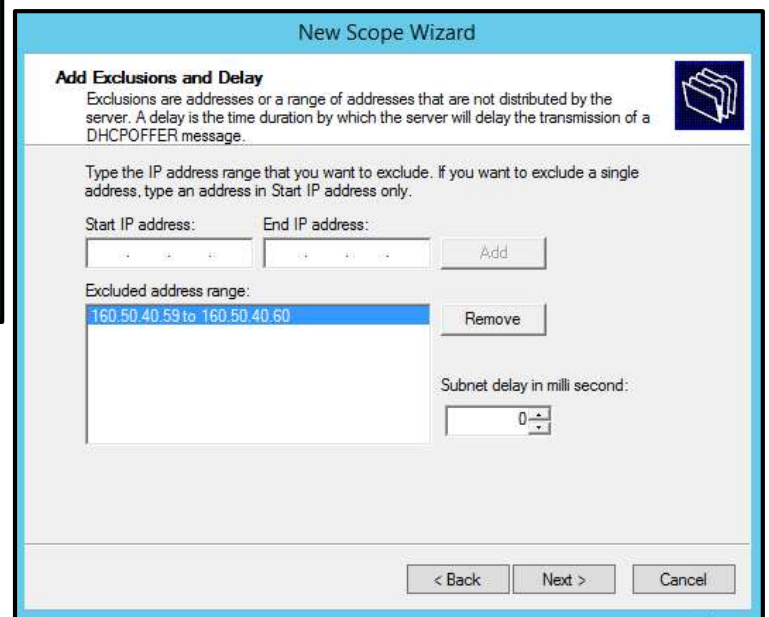
Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back Next > Cancel

Figure 43



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 DHCP OFFER 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:

Excluded address range:

Subnet delay in milli second:

< Back Next > Cancel

Figure 44

Step 4:

We have to choose 'Yes I want to activate the scope now' in order to test it.

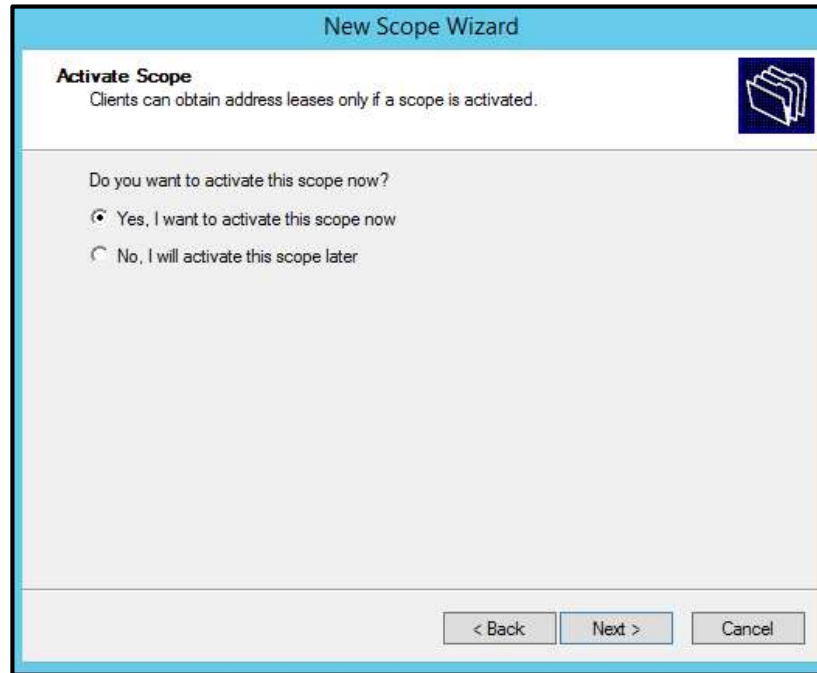


Figure 45

Step 5:

After we finished setting up our DHCP Server, We can check our scope IP Addresses and Excluded IP Addresses in 'Address Pool' .

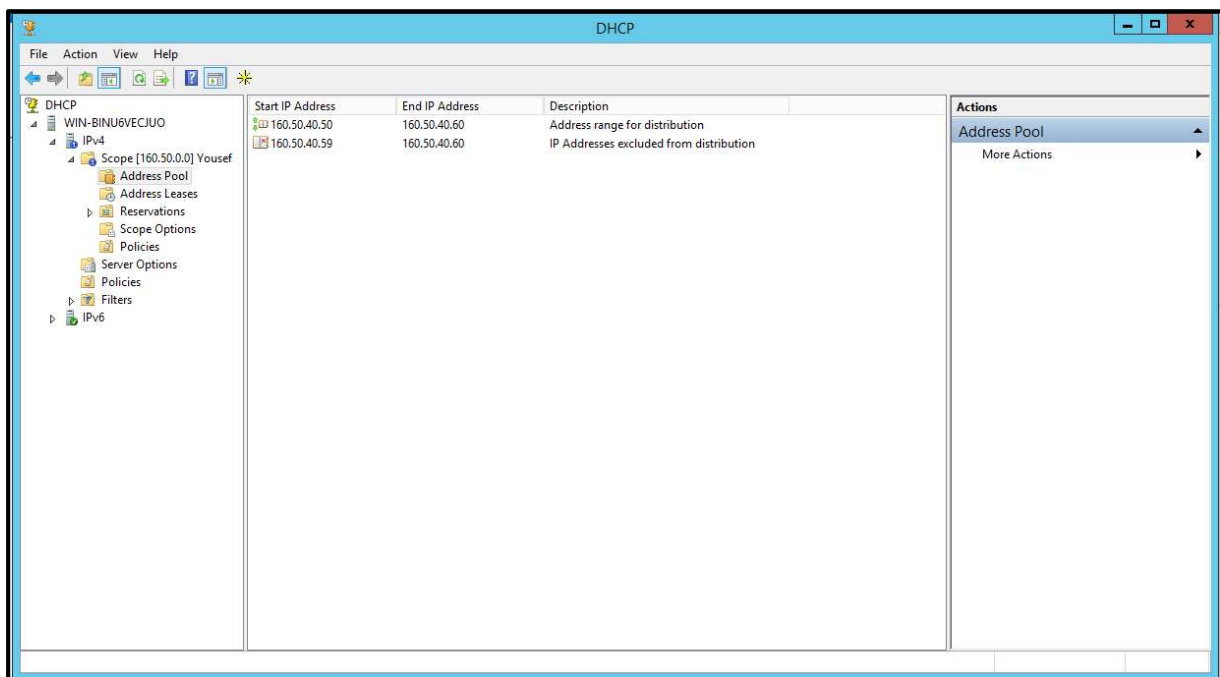


Figure 46

Step 6:

Also, we can check the Client IP Addresses that are currently connected to the DHCP Server, which is 160.50.40.50 that is shown in the picture.

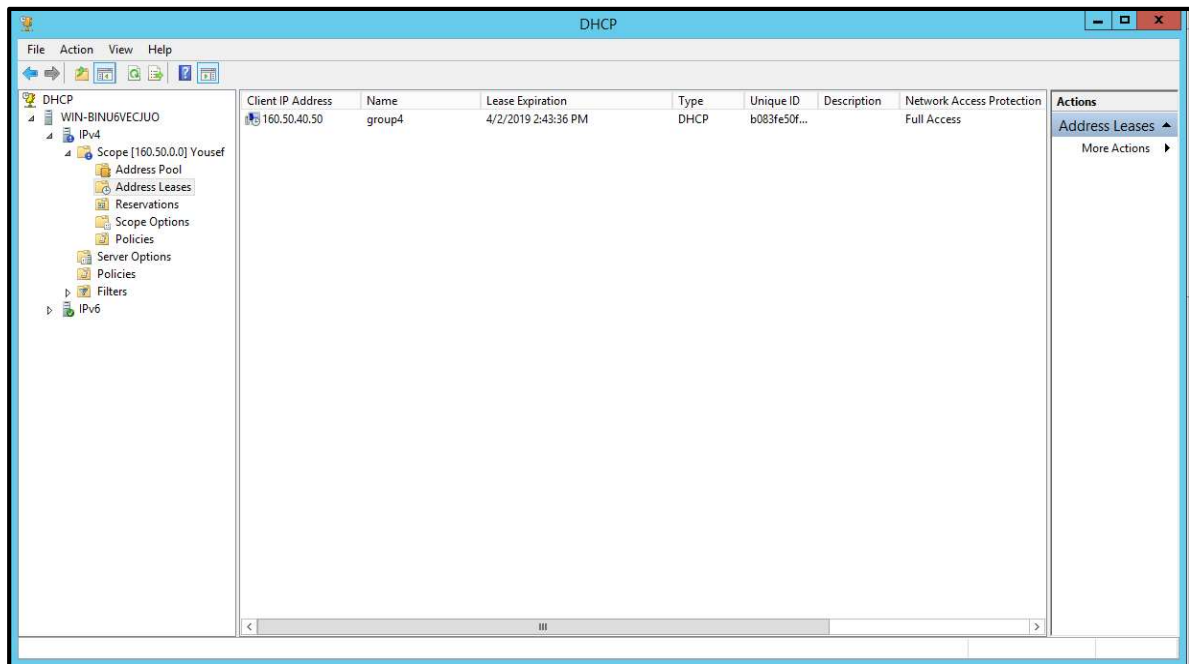


Figure 47

Questions:

1. What are the main uses for the NSLOOKUP utility?

NSLOOKUP is used to get and test the forward lookup zone and the backward lookup zone. It works like by providing IP address, it will return the hostname and domain name, and vice versa.

2. Imagine that the DNS server is down, Can the network still operate? Explain your answer.

Yes, it can operate. The reason of using DNS server is to translate a name to its IP address, so if the DNS server is down we need to use the real IP address to access any page we want.

3. What are the required zones while you are installing the DNS role? Explain each one.

1. Forward lookup zones are used to map a host name to an IP address.
2. Reverse lookup zones are used to map IP addresses to host names.

4. Summarize the basic steps of installing the DNS role?

1. Configure the IP address of the Ethernet (write the IP address, subnet mask, preferred DNS server)
2. Open service manager
3. Click on "roles and features" and click next
4. Choose Role-based or feature-based installation and click next
5. Install the necessary features, if not installed already
6. Choose the server and click next
7. Check the role you want to install and click next three times
8. Click install and close

5. Can DHCP support remote access?

When we enable the DHCP to assign an IP address, automatically it remotes access. This is known as doing DHCP by proxy

6. Can a DHCP client update its DNS entry through DHCP?

Yes, it can enable dynamic updates in the DNS server namespace for any one of its clients

7. How can I relay DHCP if my router does not support it?

By configuring dynamic routing using a switch

8. If a physical LAN has more than one logical subnet, how can different groups of clients be allocated addresses on different subnets?

If a physical LAN has one physical subnet, different groups of clients are allocated addresses on different subnets by existing in the scope or pool of the DHCP server.