PRIME COLLEGE

LAB REPORT
ON
COMPUTER NETWORKING
(CACS 303)

Submitted By:

Saman Lama

BCA 5th Sem

TU Registration No. 6-2-410-305-2019

Submitted To:

Sharat Maharjan

Table of Content

Basic Windows Commands

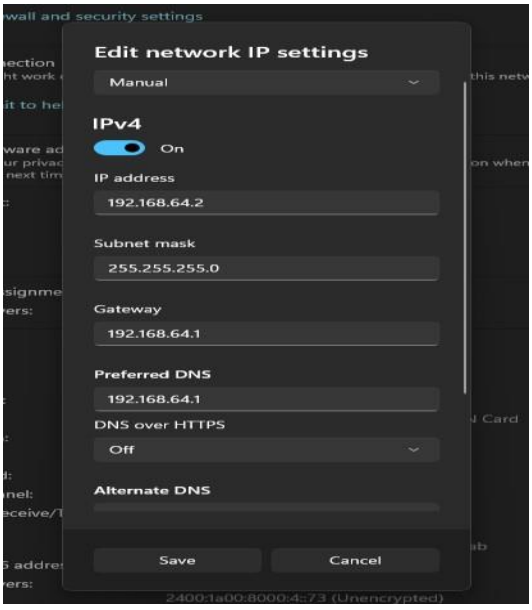
LAB 1 Configure the IP address of the computer

Background Theory:

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

Observation and Findings:

1. Select Start, then type settings. Select Settings > Network & internet.
2. Do one of the following:
    - For a Wi-Fi network, select Wi-Fi > Manage known networks. Choose the network for which you want to change the settings.
    - For an Ethernet network, select Ethernet, then select the Ethernet network you're connected to.
3. Next to IP assignment, select Edit.
4. Under Edit network IP settings or Edit IP settings, select Automatic (DHCP) or Manual.
    - Configure network



5. When you're done, select Save.

Output:

Conclusion:

The aim of this lab is to configure the network of a computer system.

LAB 2 Install Packet Tracer and identify the features of packet tracer.

Background Theory:

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag-and-drop user interface, allowing users to add and remove simulated network devices as they see fit.

Observation and Findings:

Follow the below steps to install Packet Tracer on Windows:

Step 1: Visit the official website of Netacad using any web browser.

Step 2: Press the login button and select the log-in option.

Step 3: Next screen will appear, click on the sign-up option.

Step 4: Next screen will appear and will ask for email and password and other simple details, fill them out and click on Register.

Step 5: Now the login screen appears again so fill in the Email id.

Step 6: On the next screen enter the password and press the Login button.

Step 7: Dashboard will initialize, now click on Resources and choose Download Packet Tracer Option.

Step 8: On the next web page choose the operating system to download the packet tracer.

Step 9: Check for the executable file in your system and run it.

Step 10: Next screen is of License Agreement so Click on **I accept** the license.

Step 11: Choose the installing location which has sufficient space.

Step 12: Select the start menu folder and click the **Next** button.

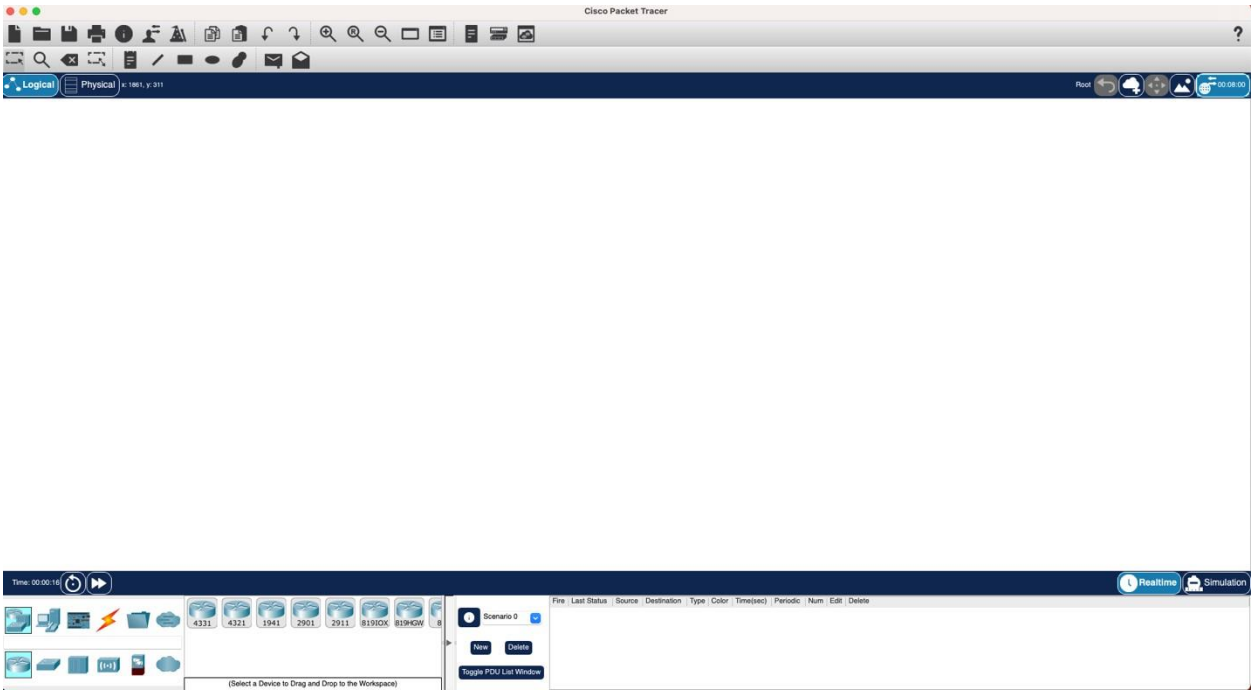
Step 13: Check the box for creating a desktop icon and click on the **Next** button.

Step 14: Now packet tracer is ready to install so click on the **Install** button.

Step 15: The installation process will start and will hardly take a minute.

Step 16: Click on the **Finish** button to complete the installation.

Output:



Conclusion:

The aim of this lab is to install and identify the features of Cisco Packet Tracer.

LAB 3 Perform Basic Networking Commands.

Background Theory:

Some of the basic networking commands are as follows:

1. Tracert

   This command is used to diagnose path-related problems.

2. Ping

   The ping command is used to test connectivity between two hosts.

3. Ipconfig

   This command displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. This command is mainly used to view the IP addresses on the computers that are configured to obtain their IP address automatically.

4. Arp

   To send IP packets, a computer needs two addresses. These addresses are the MAC address and the IP address. A MAC address is the physical or hardware address of the NIC. An IP address is the logical or software address of NIC. If a computer knows the IP address of the destination computer but it does not know the MAC address of the destination computer, it uses the ARP protocol to know the MAC address of the destination computer.

5. Netstat

   This command displays active connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, and IP statistics.

Observation and Findings:

Tracert:

```
C:\Users\legion>tracert www.google.com

Tracing route to www.google.com [2404:6800:4009:80f::2004]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  2400-1A00-B020.ip6.wlink.com.np [2400:1a00:b020:1120::1]
  2     6 ms     9 ms     7 ms  2400-1A00-B1A2.ip6.wlink.com.np [2400:1a00:b1a2:0:c84d:d2e0:9f1:c608]
  3     *        *       18 ms  2400:1a00:0:1::20
  4    20 ms     5 ms     3 ms  2400:1a00:0:1::155
  5    19 ms     7 ms     4 ms  2404:d180:1:212::201
  6     5 ms     5 ms     4 ms  2404:d180:1a:0:103:225:212:25
  7    51 ms    48 ms    48 ms  ix-ae-19-134.tcore1.mlv-mumbai.ipv6.as6453.net [2001:5a0:2300:200::81]
  8    70 ms    51 ms    50 ms  2001:5a0:2300:200::b5
  9    57 ms    57 ms    57 ms  2404:6800:80b1::1
 10    51 ms    51 ms    51 ms  2001:4860:0:1::11c0
 11    61 ms    43 ms    43 ms  2001:4860:0:1::17d1
 12    47 ms    48 ms    49 ms  bom12s05-in-x04.1e100.net [2404:6800:4009:80f::2004]

Trace complete.

C:\Users\legion>
```

Ping:

```
Pinging www.google.com [216.58.200.132] with 32 bytes of data:
Reply from 216.58.200.132: bytes=32 time=45ms TTL=55
Reply from 216.58.200.132: bytes=32 time=46ms TTL=55
Reply from 216.58.200.132: bytes=32 time=71ms TTL=55
Reply from 216.58.200.132: bytes=32 time=52ms TTL=55

Ping statistics for 216.58.200.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 71ms, Average = 53ms
```

Arp

```
C:\Users\legion>arp -a

Interface: 192.168.64.2 --- 0x5
  Internet Address      Physical Address      Type
  192.168.64.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.25.1 --- 0x6
  Internet Address      Physical Address      Type
  192.168.25.254        00-50-56-e8-bc-71     dynamic
  192.168.25.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.40.1 --- 0x7
  Internet Address      Physical Address      Type
  192.168.40.254        00-50-56-eb-40-91     dynamic
  192.168.40.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\legion>
```

Ipconfig


C:\WINDOWS\system32\cmd.
Microsoft Windows [Version 10.0.22621.1105]
(c) Microsoft Corporation. All rights reserved.
C:\Users\legion>ipconfig /all
Windows IP Configuration
Host Name . . . . . : DESKTOP-HQEOP5B
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : 84-A9-38-FE-A9-25
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Unknown adapter Local Area Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Kaspersky VPN
Physical Address. . . . . :
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Local Area Connection* 9:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 4E-D5-77-6A-D6-A7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Local Area Connection* 10:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 4E-D5-77-6A-D6-B7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Ethernet adapter VMware Network Adapter VMnet1:

Netstat:

```
C:\Users\legion>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49670        DESKTOP-HQEOP5B:49671  ESTABLISHED
  TCP    127.0.0.1:49671        DESKTOP-HQEOP5B:49670  ESTABLISHED
  TCP    127.0.0.1:49679        DESKTOP-HQEOP5B:49680  ESTABLISHED
  TCP    127.0.0.1:49680        DESKTOP-HQEOP5B:49679  ESTABLISHED
  TCP    127.0.0.1:50935        DESKTOP-HQEOP5B:65001  ESTABLISHED
  TCP    127.0.0.1:51012        DESKTOP-HQEOP5B:51028  ESTABLISHED
  TCP    127.0.0.1:51012        DESKTOP-HQEOP5B:53613  TIME_WAIT
  TCP    127.0.0.1:51012        DESKTOP-HQEOP5B:53614  TIME_WAIT
  TCP    127.0.0.1:51012        DESKTOP-HQEOP5B:53624  TIME_WAIT
  TCP    127.0.0.1:51012        DESKTOP-HQEOP5B:53625  TIME_WAIT
  TCP    127.0.0.1:51012        DESKTOP-HQEOP5B:53659  FIN_WAIT_2
  TCP    127.0.0.1:51012        DESKTOP-HQEOP5B:53660  TIME_WAIT
  TCP    127.0.0.1:51028        DESKTOP-HQEOP5B:51012  ESTABLISHED
  TCP    127.0.0.1:53464        DESKTOP-HQEOP5B:53465  ESTABLISHED
  TCP    127.0.0.1:53465        DESKTOP-HQEOP5B:53464  ESTABLISHED
  TCP    127.0.0.1:53466        DESKTOP-HQEOP5B:53467  ESTABLISHED
  TCP    127.0.0.1:53467        DESKTOP-HQEOP5B:53466  ESTABLISHED
  TCP    127.0.0.1:53659        DESKTOP-HQEOP5B:51012  CLOSE_WAIT
  TCP    127.0.0.1:65001        DESKTOP-HQEOP5B:50935  ESTABLISHED
  TCP    192.168.64.2:53683     149.13.68.146:https    SYN_SENT
^C
C:\Users\legion>
```

Conclusion:

The aim of this lab is to perform basic networking commands.

Cisco Packet Tracer

LAB 4 Implement peer-to-peer network using Packet Tracer.

Background Motivation:

Peer-to-peer computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the network. They are said to form a peer-to-peer network of nodes.

Observation and Findings:

Implement a peer-to-peer network between two PCs and testing connectivity between them.

Fig: Peer-to-Peer Network

Output:

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Conclusion:

The aim of this lab is to become familiar with the peer-to-peer network using two PCs.

LAB 5 Implement Local Area Network using Packet Tracer

Background Theory:

A local area network (LAN) consists of a series of computers linked together to form a network in a circumscribed location. The computers in a LAN connection to each other via TCP/IP ethernet or Wi-Fi.

Observation and Findings:

Implement a local area network and test the connectivity within the network.

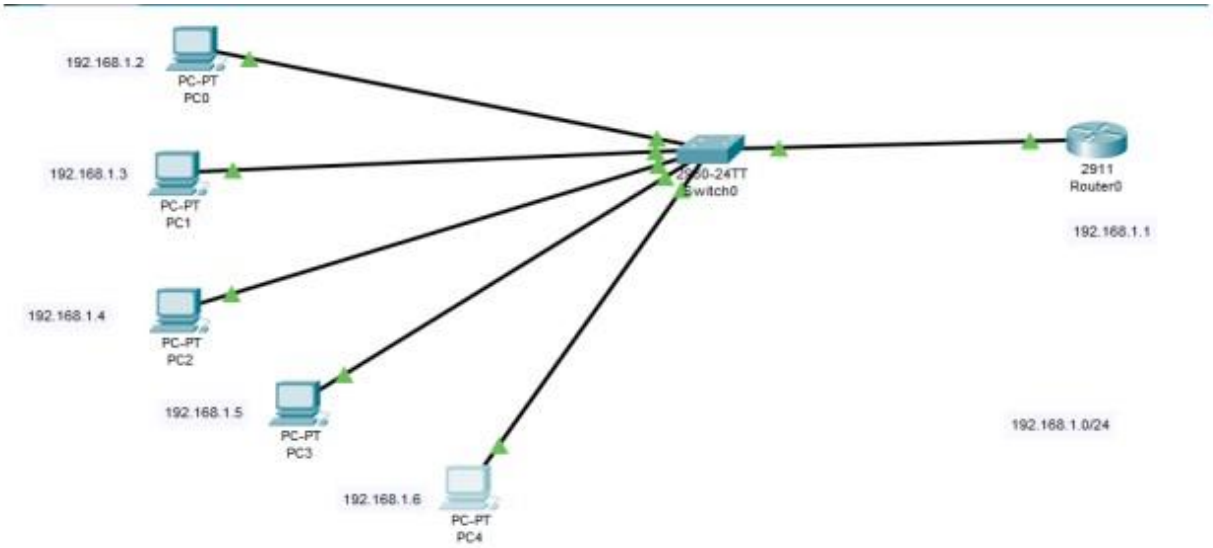


Fig: Local Area Network

Output:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Conclusion:

The aim of this lab is to become familiar with the Local Area Network (LAN).

LAB 6 Interconnect two different Local Area Networks using a Router using Packet Tracer.

Background Theory:

Local area network to local area network connections is often performed with a bridge. Local area network to wide area network connections is usually performed with a router. A third device, the switch, can be used to interconnect segments of a local area network.

Observation and Findings:

Interconnecting two different LANs and testing their interconnectivity.

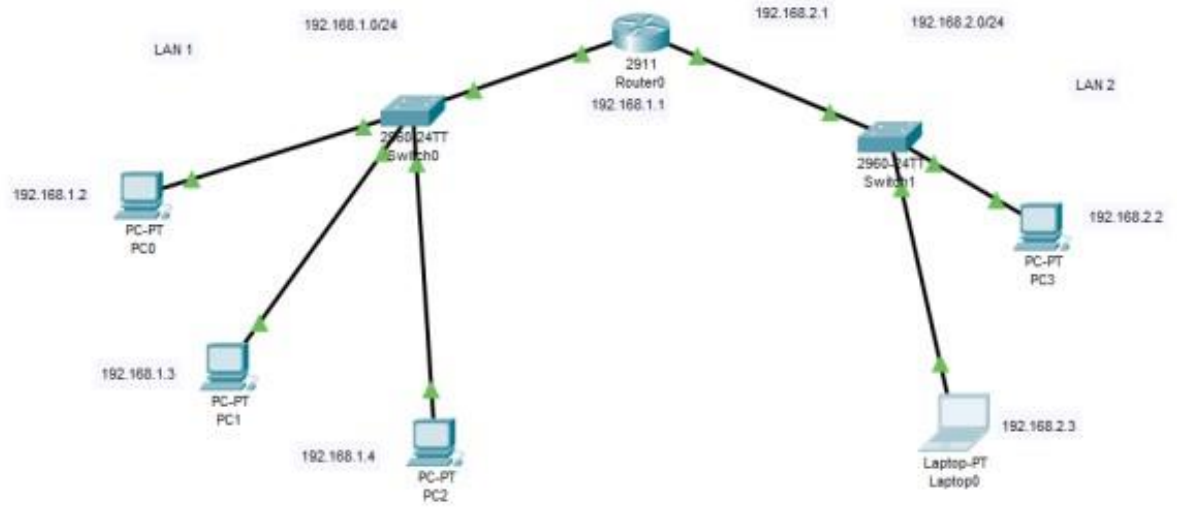
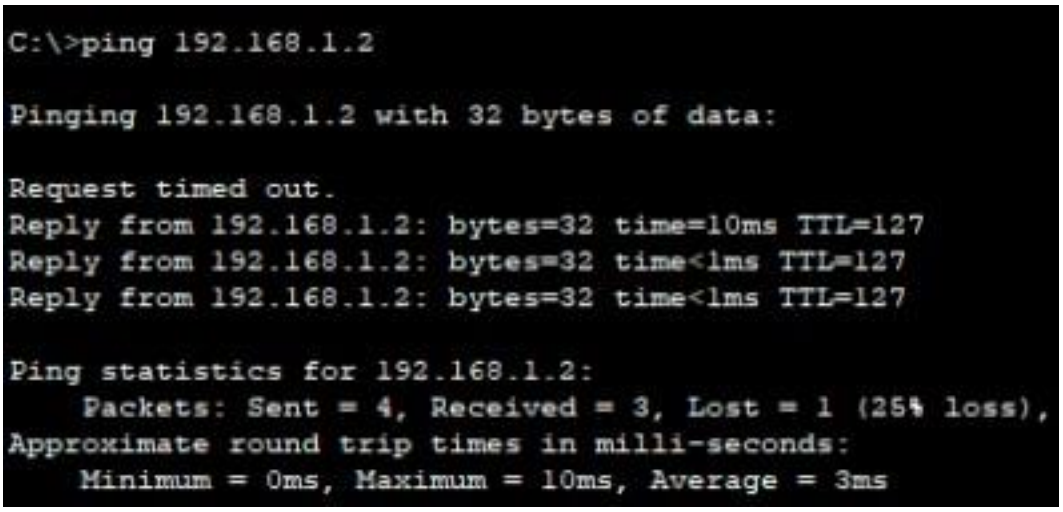


Fig: Connection between two LANs

Output:



Conclusion:

The aim of this lab is to be familiar with the interconnectivity between LANs.

LAB 7 Configure DHCP Server and assign IP address automatically using Packet Tracer.

Background Theory:

Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to configure network devices to communicate on an IP network. A DHCP client uses the DHCP protocol to acquire configuration information, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server.

Observation and Findings:

Step 1: Set one router with one server and set a desktop as required.

Step 2: enable the ports of routers and set an IP address for both the server and routers.

Step 3: Go to the services of a server and on the service and assign the IP address of the router in the server and set the start IP address.

Step 4: Enable the DHCP in the IP configuration section of a desktop.

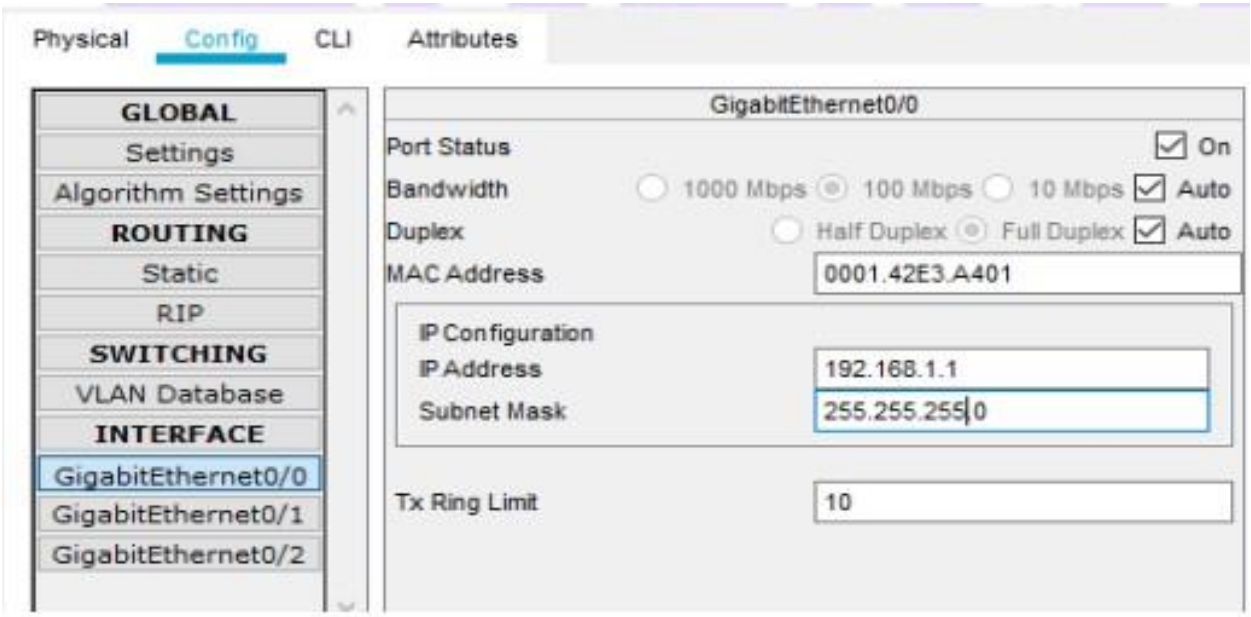
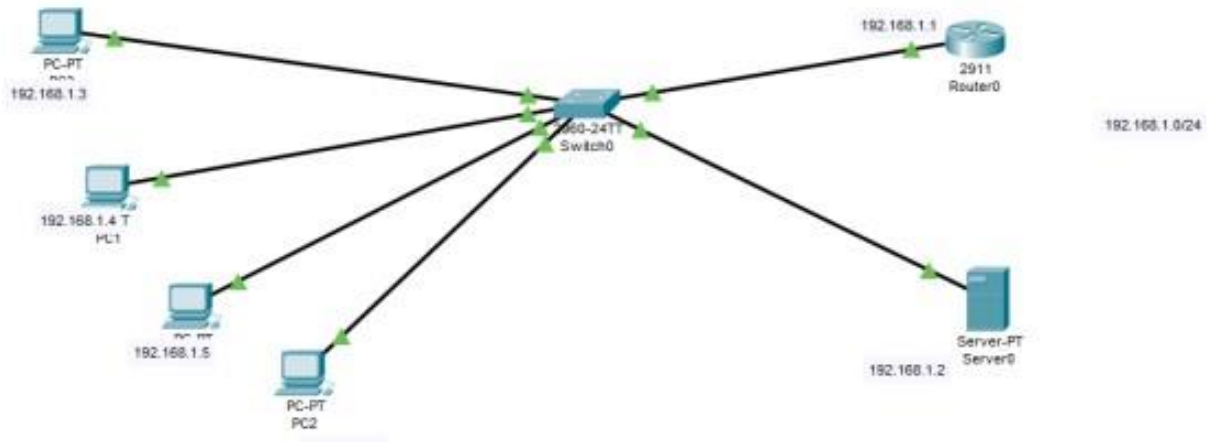


Fig: Router Configuration

Fig: Server Configuration

Fig: IP assignment Dynamically

Observation and Findings:



DHCP connection

Output:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Conclusion:

The aim of the lab is to learn about DHCP server configuration.

LAB 8 To configure and implement DNS Server using Packet Tracer.

Background Theory:

The Domain Name System is a hierarchical and distributed naming system for computers, services, and other resources on the Internet or other Internet Protocol networks. It associates various information with domain names assigned to each of the associated entities.

Observation and Findings:

Step 1: Set one switch with one server and set a desktop as required.

Step 2: Set the DNS IP address for a server and enable the DNS service.

Step 3: Go to the services of a server and set the domain name and address for a DNS server Step 4: Set an IP address for a desktop with a DNS IP address.

Fig: DNS Server Configuration

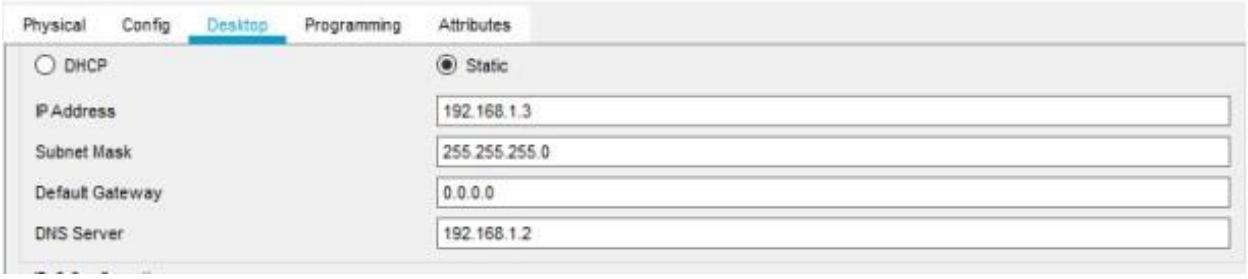


Fig: DNS PC Configuration

Observation and Findings:

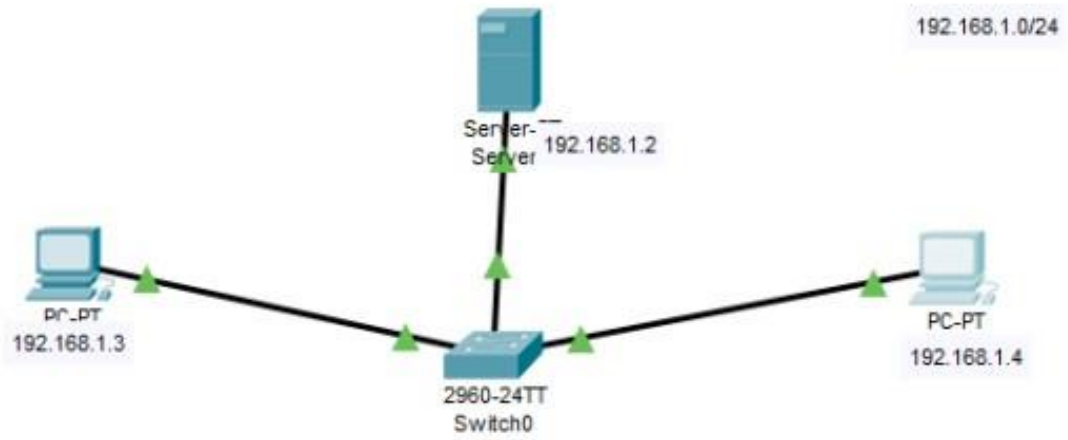


Fig: DNS Server

Output:

```
C:\>ping www.football.com

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Conclusion:

The aim of this lab is to learn about DNS servers.

LAB 9 To know about Router Configuration and Commands.

Background Theory:

A router receives and sends data on computer networks. Routers are sometimes confused with network hubs, modems, or network switches. However, routers can combine the functions of these components, and connect with these devices, to improve Internet access or help create business networks.

Observation and Findings:

Step 1: enable router using command enable or en.

Step 2: enter command configure terminal.

Step 3: enter command line console 0.

Step 4: set a password as you like

Step 5: exit

Step 6: enable router using password.

Step 7: go to the terminal using configure t command.

Step 8: set an IP address and subnet mask for Gigabit Ethernet of a Router.

Step 9: enable the ports of a router using no shutdown command.

Step 10: enable IP address of a computer.

```
Router>en
Router#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#enable password class
Router(config)#ecit
               ^
% Invalid input detected at '^' marker.

Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

```
Router>en
Password:
Password:
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#int gig0/1
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#exit
Router(config)#int gig0/2
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2,
changed state to up
```

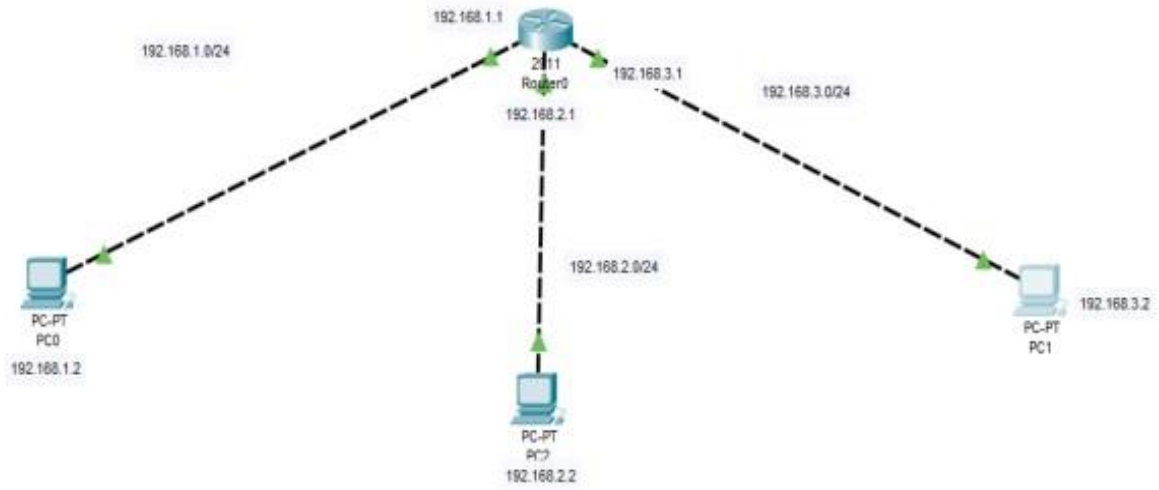
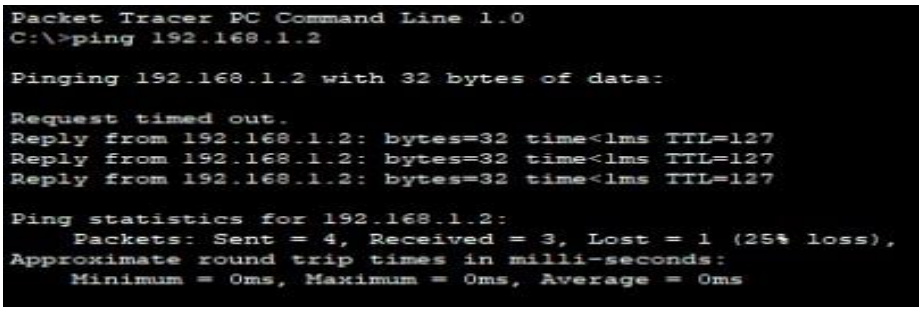


Fig: Router Configuration

Output:



Conclusion:

The aim of the lab is to become familiar with router configuration and its commands.

LAB 10 Demonstrate the use of VLAN in Packet Tracer

Background Theory:

A virtual LAN (VLAN) is a logical overlay network that groups together a subset of devices that share a physical LAN, isolating the traffic for each group. A LAN is a group of computers or other devices in the same place -- e.g., the same building or campus -- that share the same physical network.

Observation and Findings:

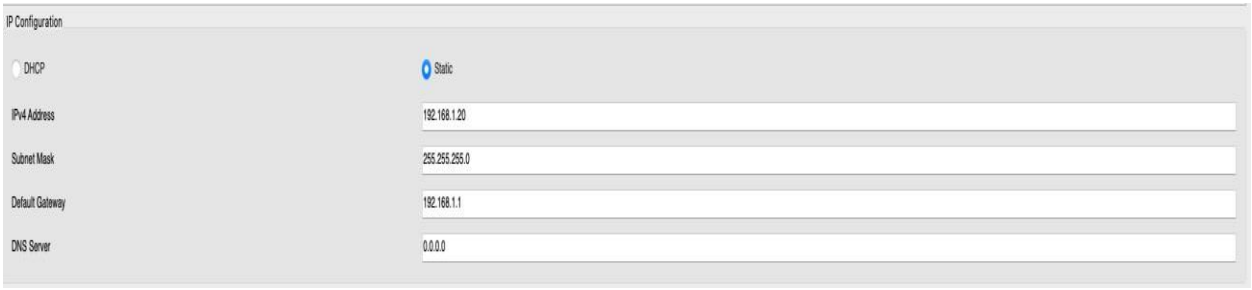


Fig: PC IP Configuration

```
Switch>enab
Switch#enable
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name HR
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name IT
Switch(config-vlan)#port
                    ^
% Invalid input detected at '^' marker.

Switch(config-vlan)#int fa 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switch access vlan 10
Switch(config-if)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switch access vlan 10
Switch(config-if)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switch access vlan 20
Switch(config-if)#int fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switch access vlan 20
Switch(config-if)#int fa0/5
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
```

Fig: Switch Configuration

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#fa0/0
               ^
% Invalid input detected at '^' marker.

Router(config)#int fa0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#int fa0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up

Router(config-subif)#encapsulation dot1q 10
                                        ^
% Invalid input detected at '^' marker.

Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip add 198.168.1.1 255.255.255.0
Router(config-subif)#int fa0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up

Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip add 198.168.2.2 255.255.255.0
Router(config-subif)#
```

Fig: Router Configuration

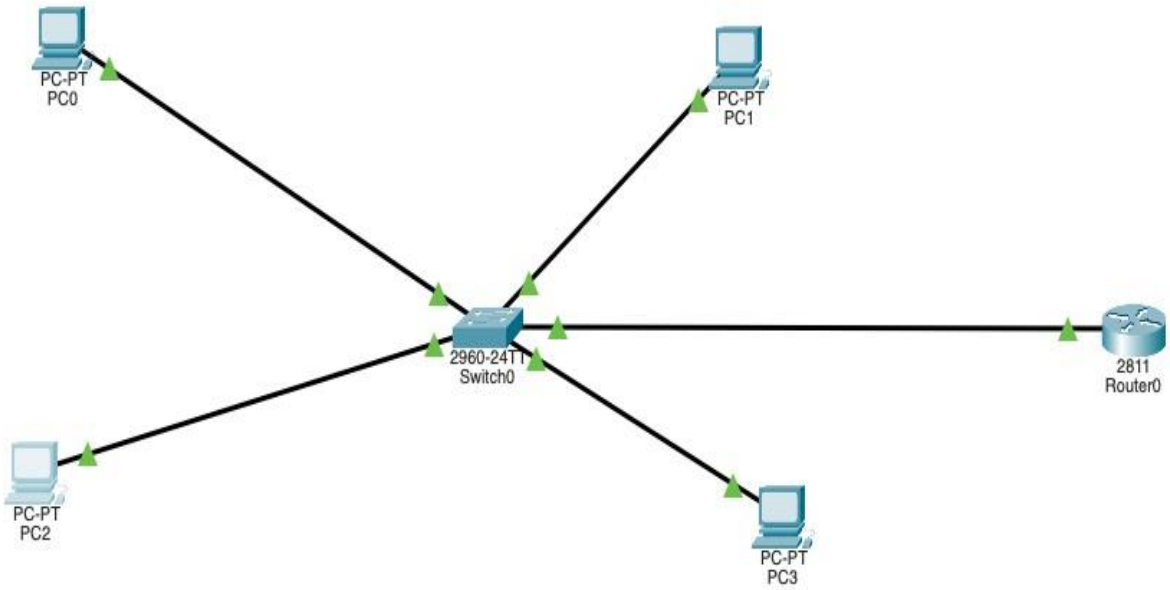
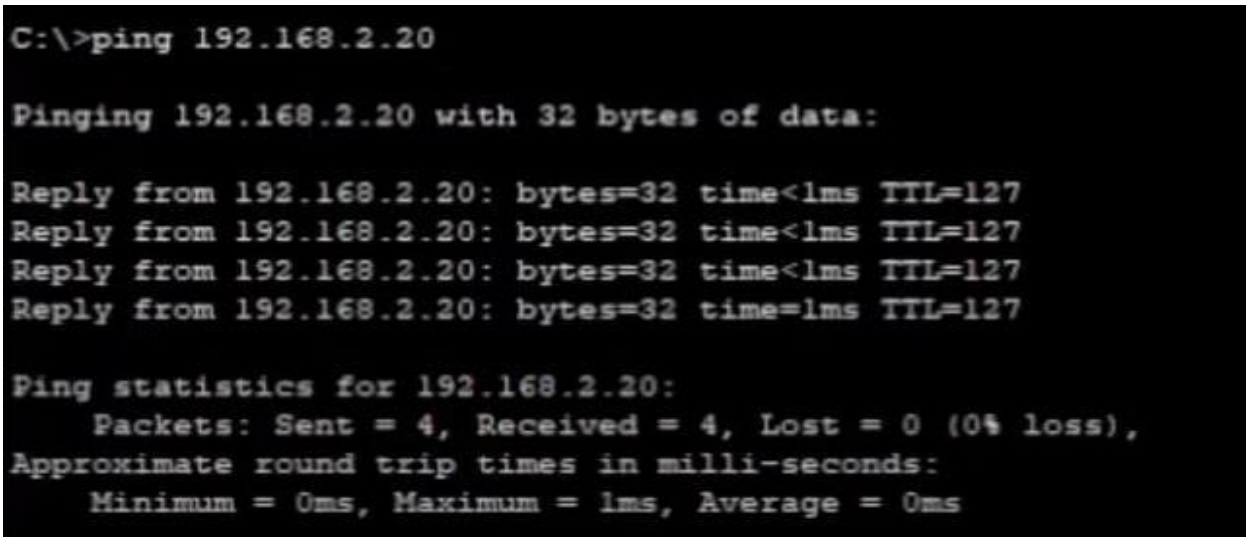


Fig: VLAN Configuration

Output:



Conclusion:

The aim of this lab is to learn about VLAN.

LAB 11 Implementation of Static Routing in Packet Tracer.

Background Theory:

Network administrators use static routing, or nonadaptive routing, to define a route when there is a single route or a preferred route for traffic to reach a destination. Static routing uses small routing tables with only one entry for each destination.

Observation and Findings:

Step 1: Set a router with IP address

Step 2: Setup switch and desktop for communication with IP address.

Step 3: Set another router with IP

address Step 4: enable ports of a

routers.

Step 5: Set a static route for Router one and two

Step 6: communicate from one network to another.

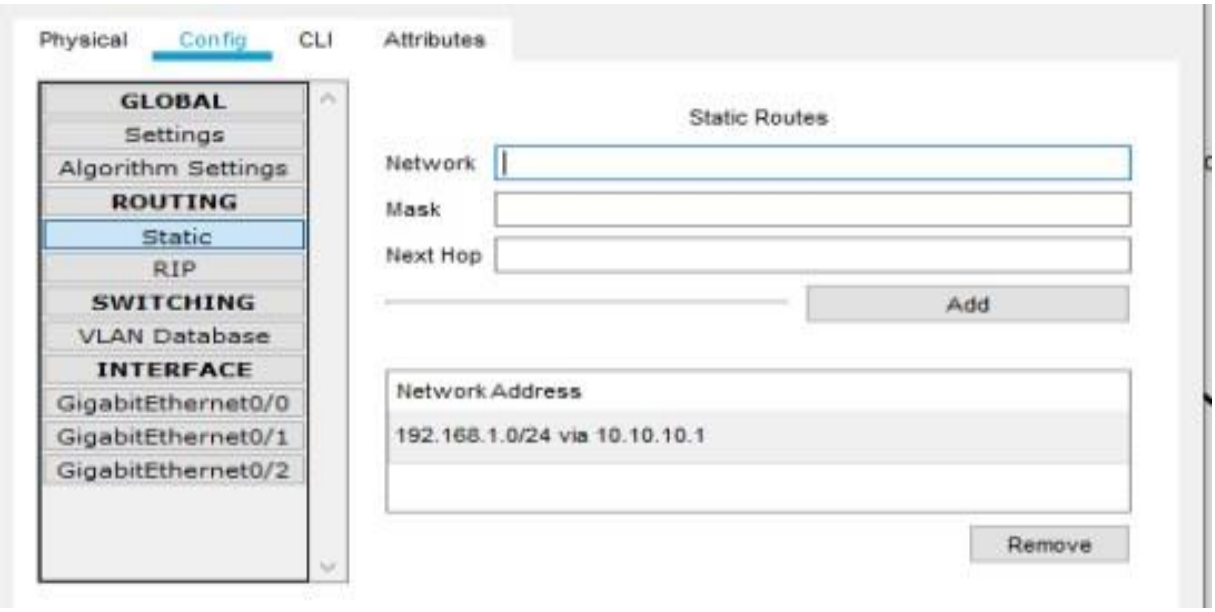


Fig: Static routers

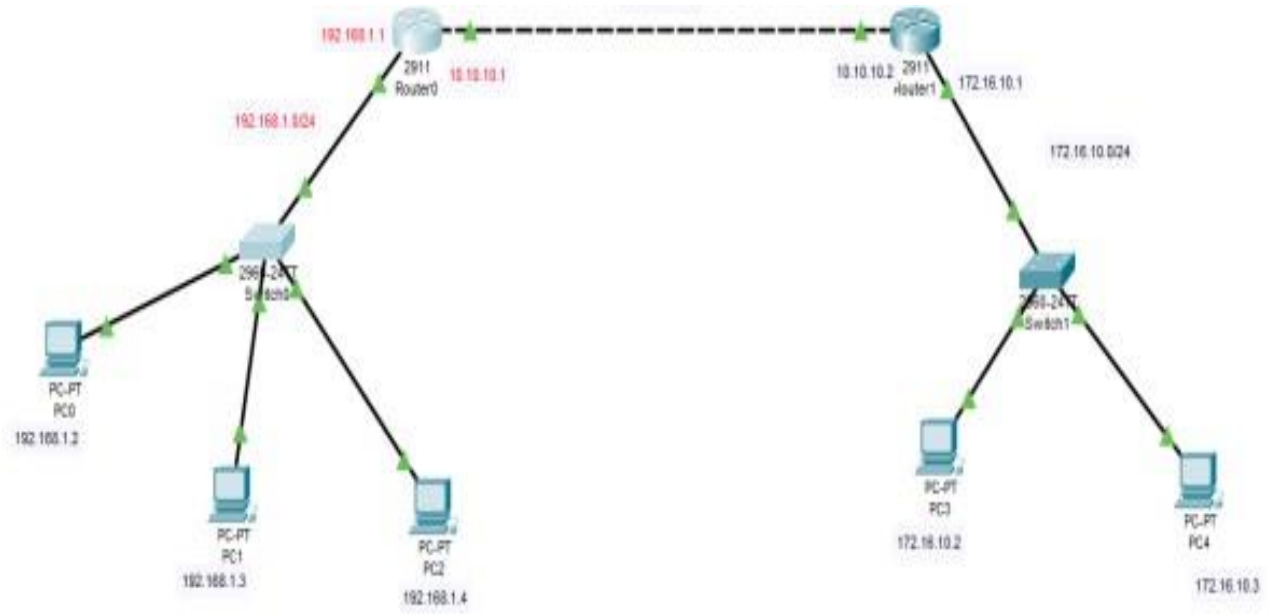


Fig: Static Routing

Output:

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=10ms TTL=126
Reply from 192.168.1.2: bytes=32 time=12ms TTL=126
Reply from 192.168.1.2: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 12ms, Average = 11ms
```

Conclusion:

The main aim of this lab to learn about static routing.

LAB 12 Create and test crossover and straight cables.

Crossover and Straight Through Cable:

Choose a Straight Through or Crossover Cable?

Usually, straight through cables are primarily used for connecting unlike devices. And crossover cables are use for connecting unlike devices alike devices.

Use straight through cable for the following cabling:

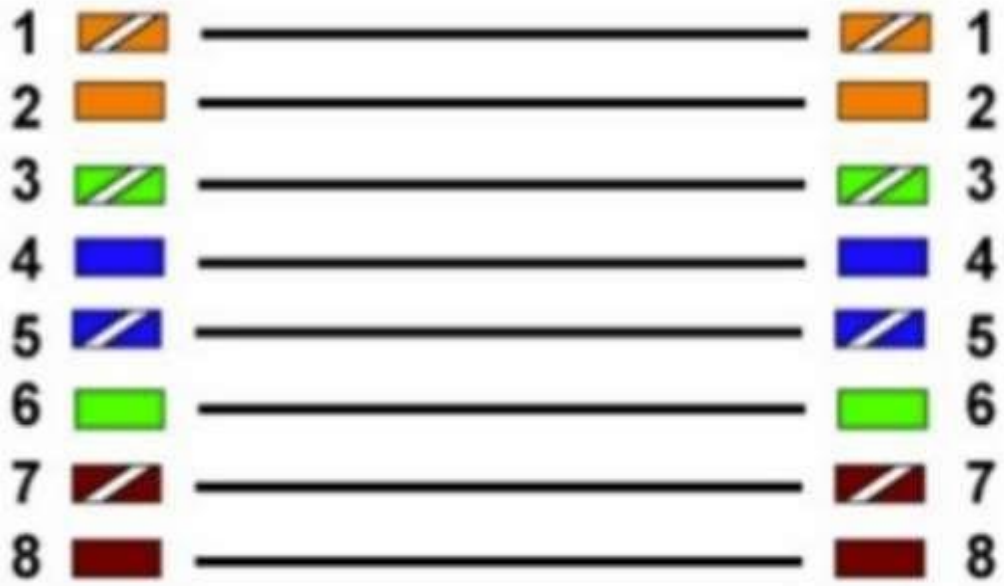
- Switch to router
- Switch to PC or server
- Hub to PC or server

Use crossover cables for the following cabling:

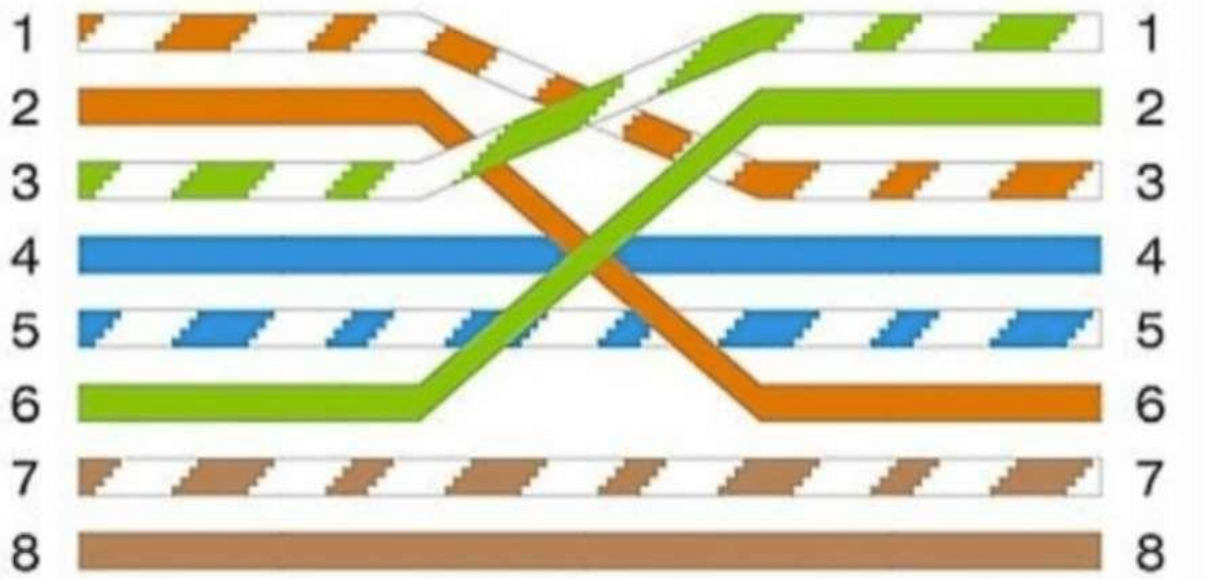
- Switch to switch
- Switch to hub
- Hub to hub
- Router to router
- Router Ethernet port to PC NIC
- PC to PC

The Main Differences-Straight Through and Crossover Cable

Straight through and crossover cables are wired differently from each other. One easy way to tell what you have is to look at the order of the colored wires inside the RJ45 connector. If the order of the wires is the same on both ends, then you have a straight through cable. If not, then it's most likely a crossover cable or was wired wrong.



Straight Through Cable



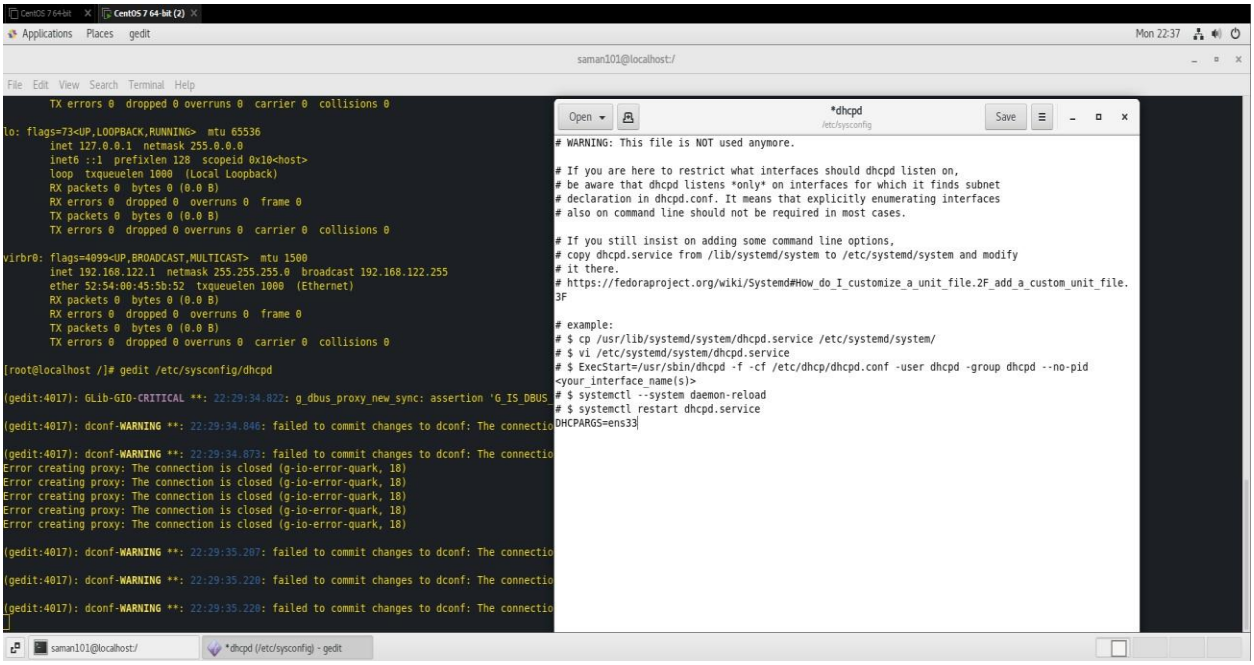
Crossover Cable

Linux Lab

Lab 13: DHCP Server Configuration in Linux Machine:

Step 1: Installing required packages:

Step 2: Setting specific interface for DHCP server (if multiple NIC is present)



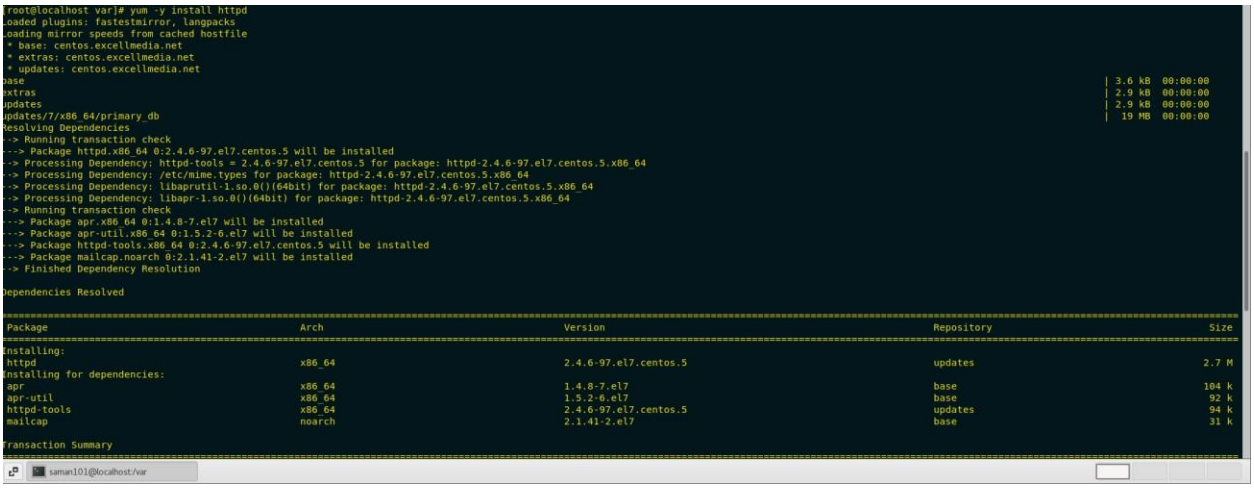
Step 3: Parameter Configuration

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
default-lease-time 3600;
max-lease-time 7200;

subnet 192.168.228.0 netmask 255.255.255.0 {
option routers 192.168.288.1;
range 192.168.228.254;
}
```

Lab 14: Apache Web Server Configuration in Linux Machine:

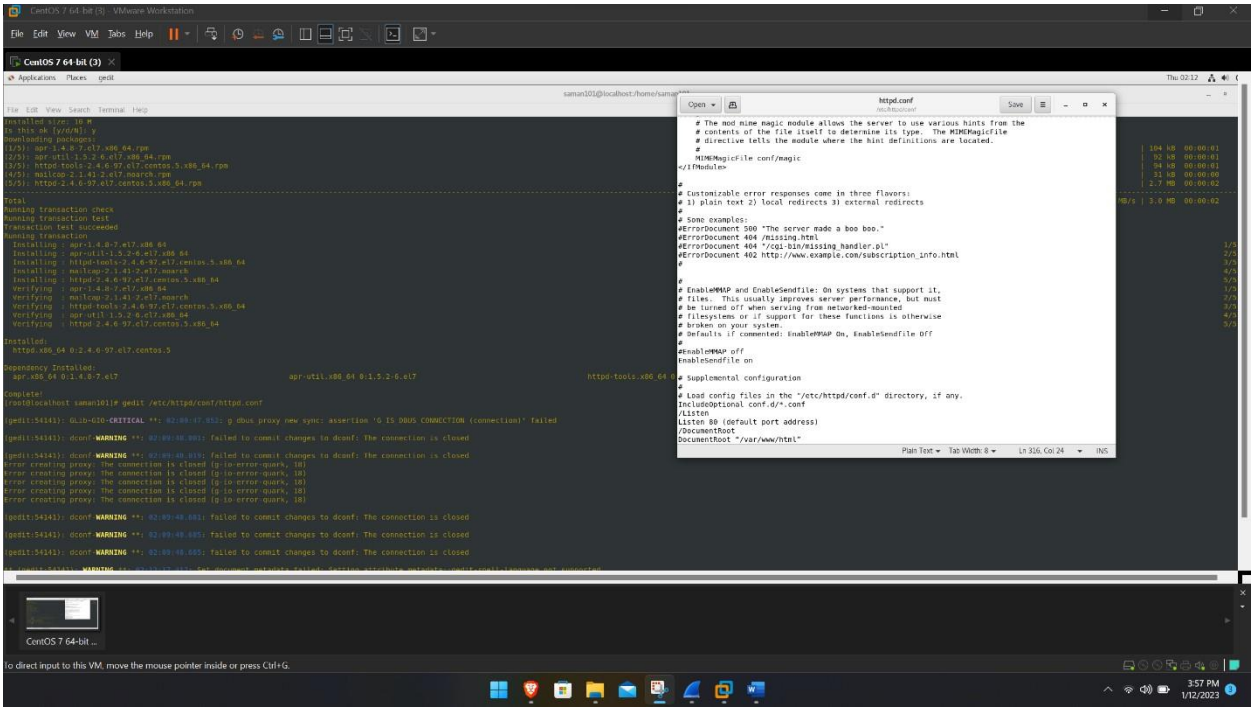
Step 1: Installing required packages



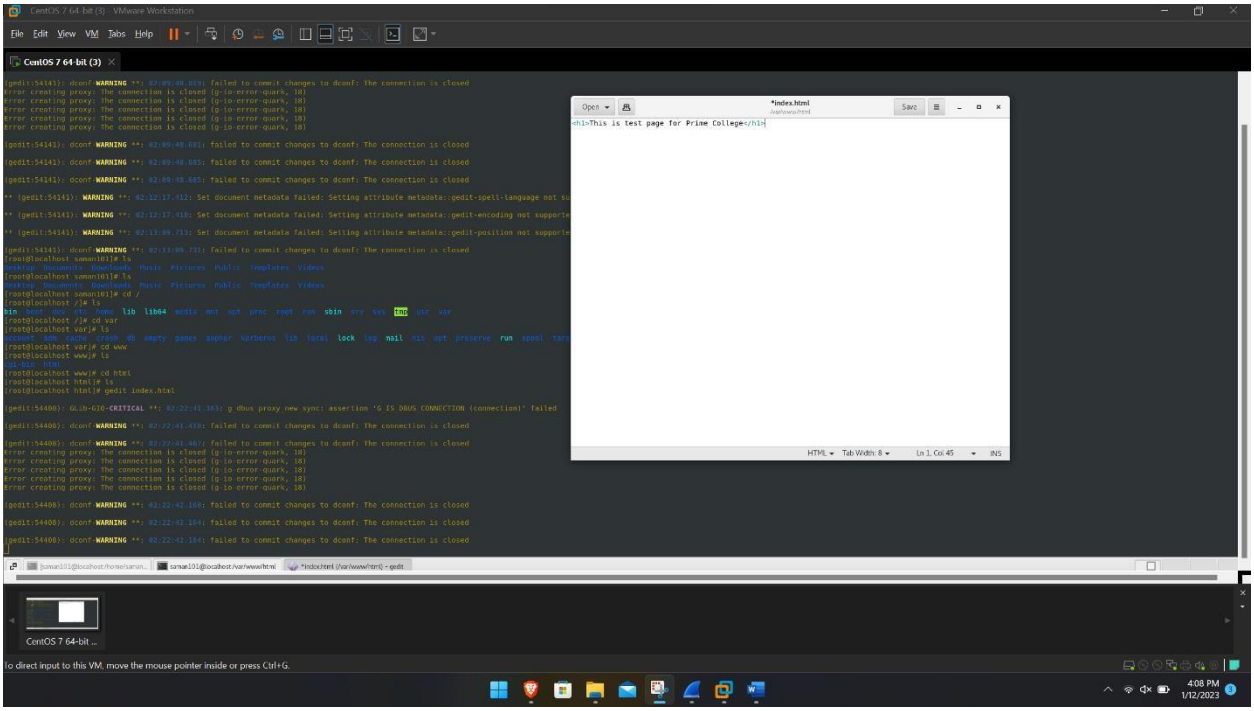
Step 2: Starting the web

```
[root@localhost var]# systemctl start httpd
[root@localhost var]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@localhost var]# gedit /etc/httpd/conf/httpd.conf
```

Step 3: Configuring web server

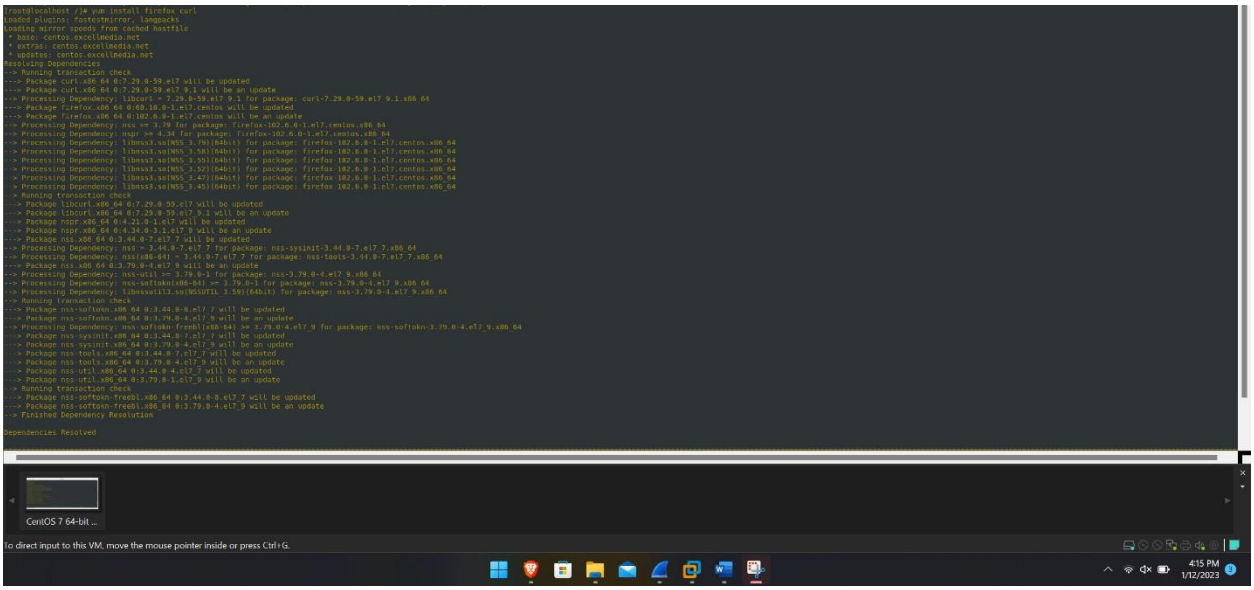


Step 4: Hosting a website

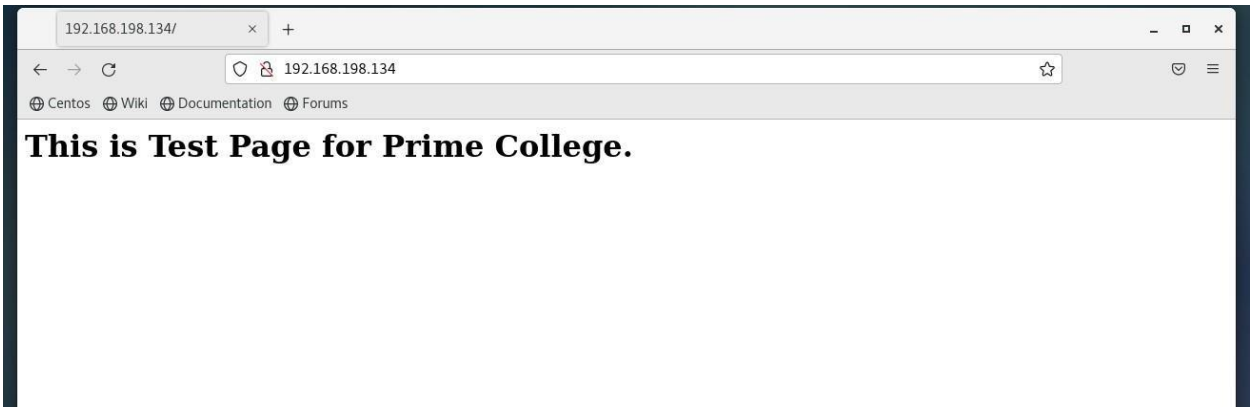


Lab 15 Client-Side

Step 1: Installing browser or curl tool to test the website

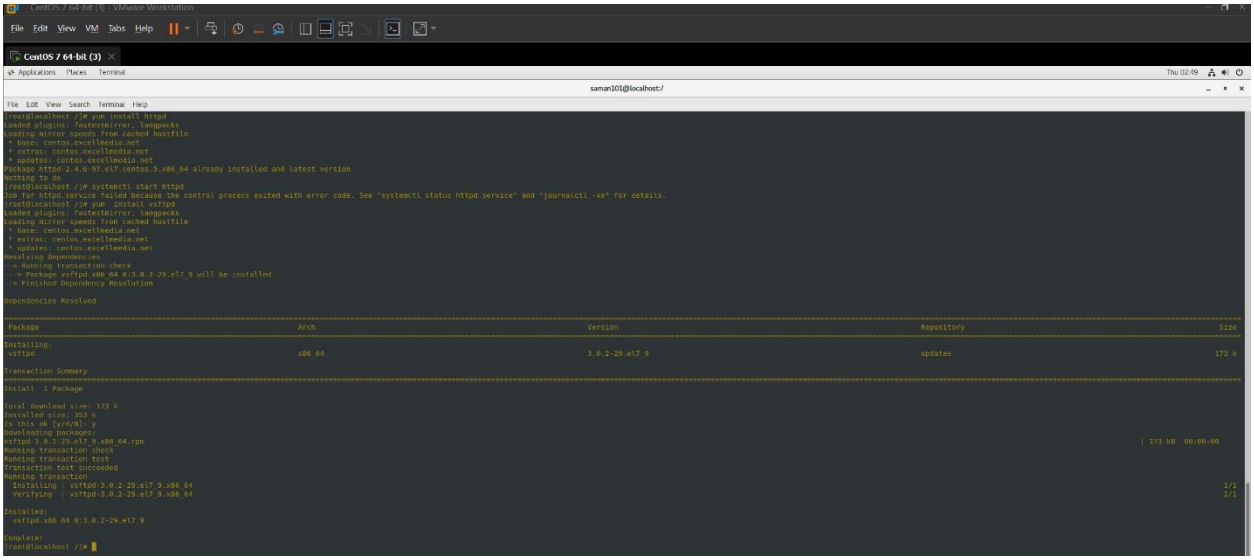


Step 2: Testing web page using curl



Lab 16: FTP Server Configuration in Linux Machine:

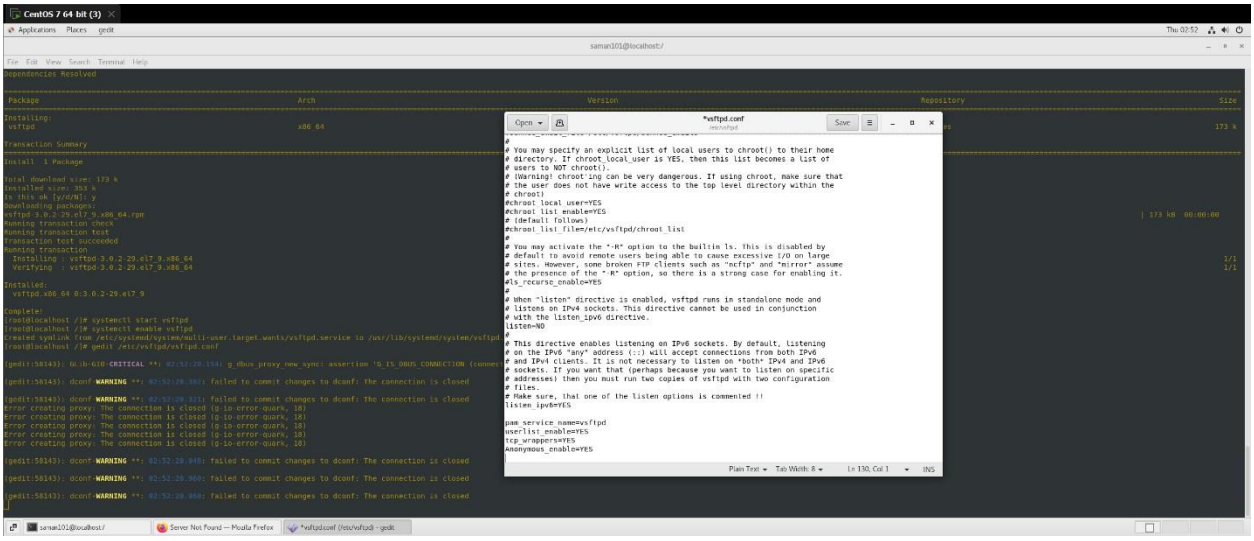
Step 1: Installing required packages



Step 2: Starting FTP service

```
[root@localhost /]# systemctl start vsftpd
[root@localhost /]# systemctl enable vsftpd
Created symlink from /etc/systemd/system/multi-user.target.wants/vsftpd.service to /usr/lib/systemd/system/vsftpd.service.
[root@localhost /]#
```

Step 3: Configuring FTP server



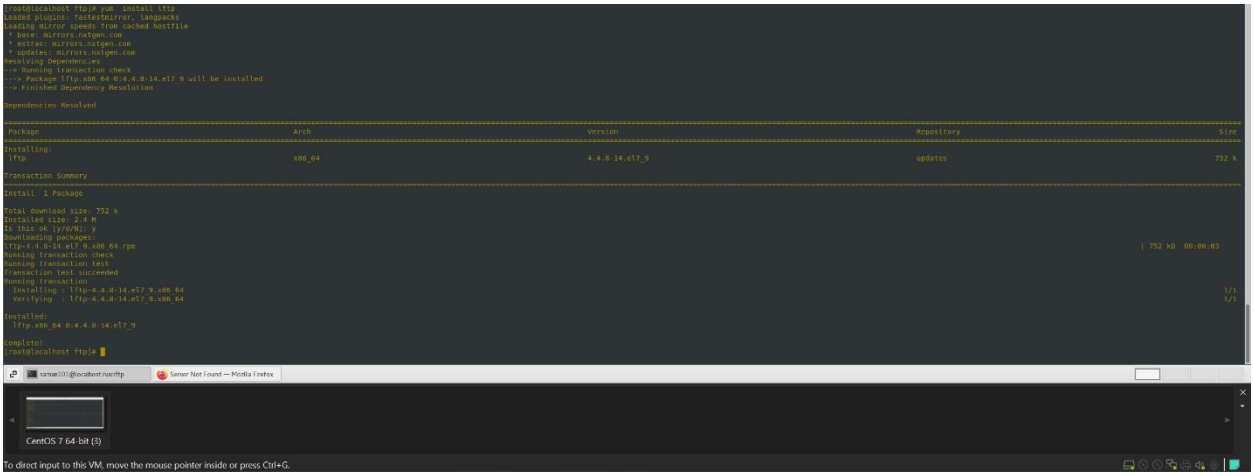
Step 4: Creating test files

```
[root@localhost /]# cd /var/ftp
[root@localhost ftp]# ls
pub
[root@localhost ftp]# touch saman.pdf
[root@localhost ftp]# ls
pub  saman.pdf
[root@localhost ftp]#
```

Step 5: Restarting ftp service

Client-side Configuration:

Client-side Configuration

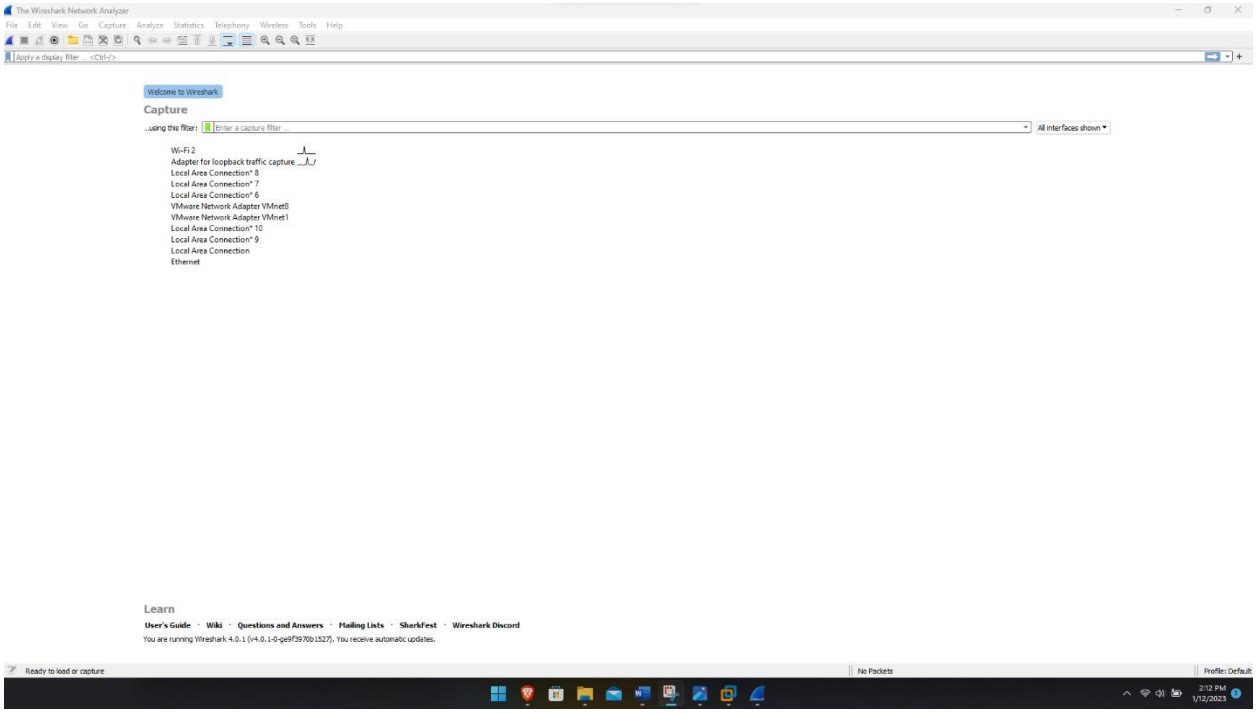


Connecting FTP server using browser Entering ip address in browser url

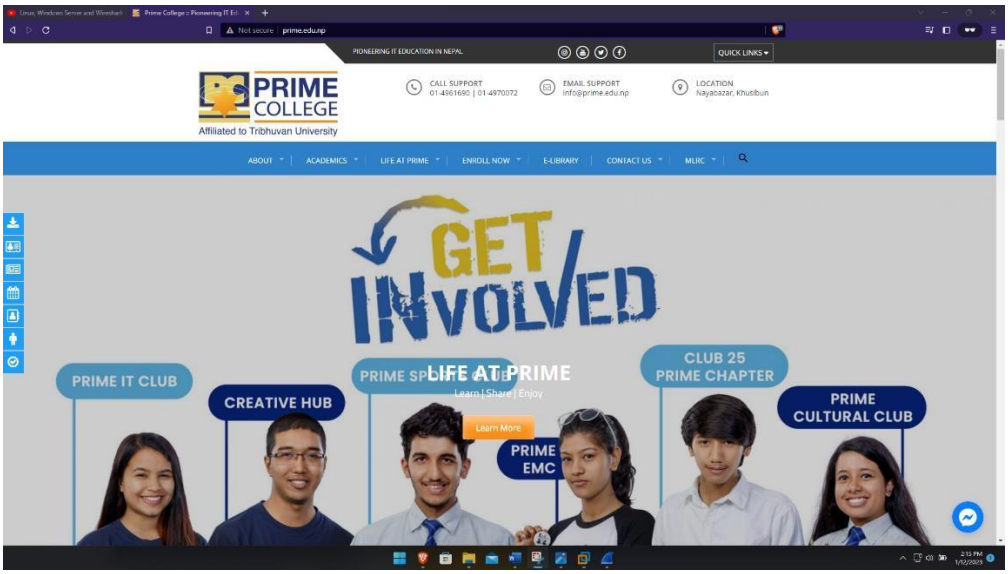
Lab 17:WireShark Lab

Test Run Do the following steps:

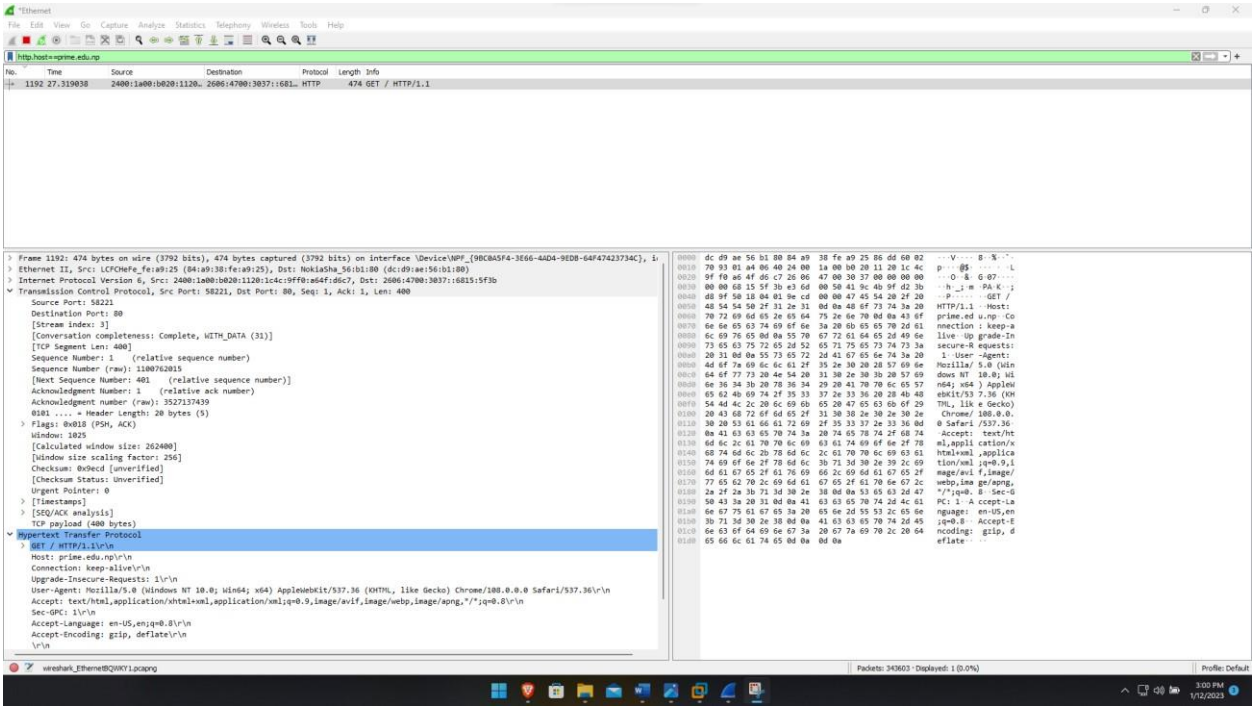
1. Start up the Wireshark program (select an interface and press start to capture packets).



2. Start up your favorite browser.
3. In your browser, go to Prime College homepage by typing www.primecollege.com.



4. After your browser has displayed the http://www.primecollege.com page, stop Wireshark packet capture by selecting stop in the Wireshark capture window.



5. Color Coding: You'll probably see packets highlighted in green, blue, and black. Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-oforder.

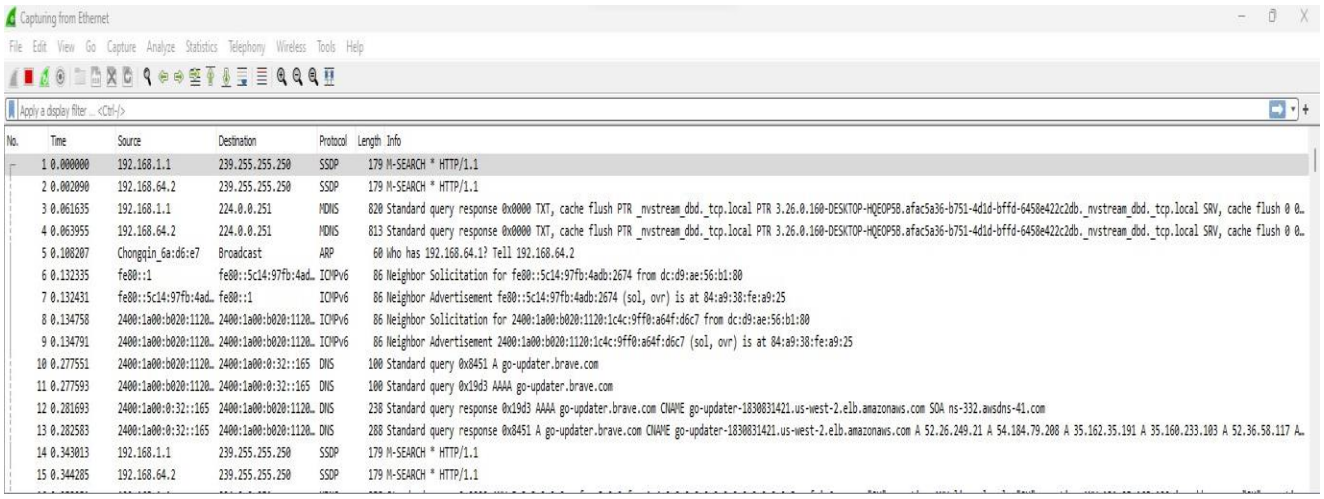
6. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! However, as you will notice the HTTP messages are not clearly shown because there are many other packets included in the packet capture. Even though the only action you took was to open your browser, there are many other programs in your computer that communicate via the network in the background. To filter the connections to the ones we want to focus on, we have to use the filtering functionality of Wireshark by typing "http" in the filtering field.

To View and Analyze Packet Contents:

The captured data interface contains three main sections:

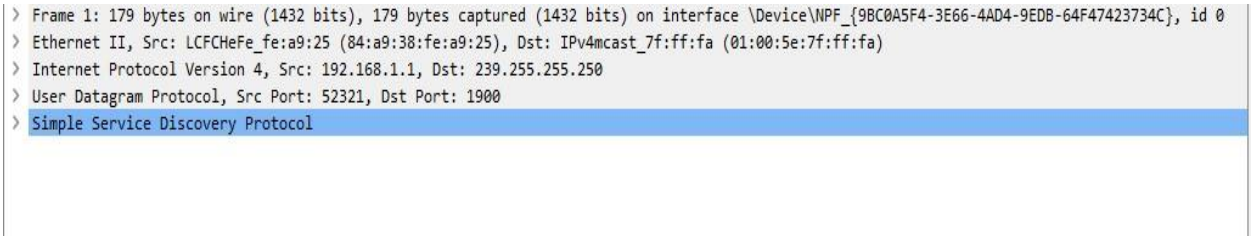
1. The packet list pane (the top section)
2. The packet details pane (the middle section)
3. The packet bytes pane (the bottom section)\

1. **Packet list**: It shows all packets found in the active capture file.
    - No: This field indicates which packets are part of the same conversation.
    - Time: The timestamp of when the packet was captured is displayed in this column.
    - Source: This column contains the address where the packet originated.
    - Destination: This column contains the address that the packet is being sent to.
    - Protocol: The packet's protocol name, such as TCP, can be found in this column.
    - Length: The packet length, in bytes, is displayed in this column.
    - Info: Additional details about the packet are presented here

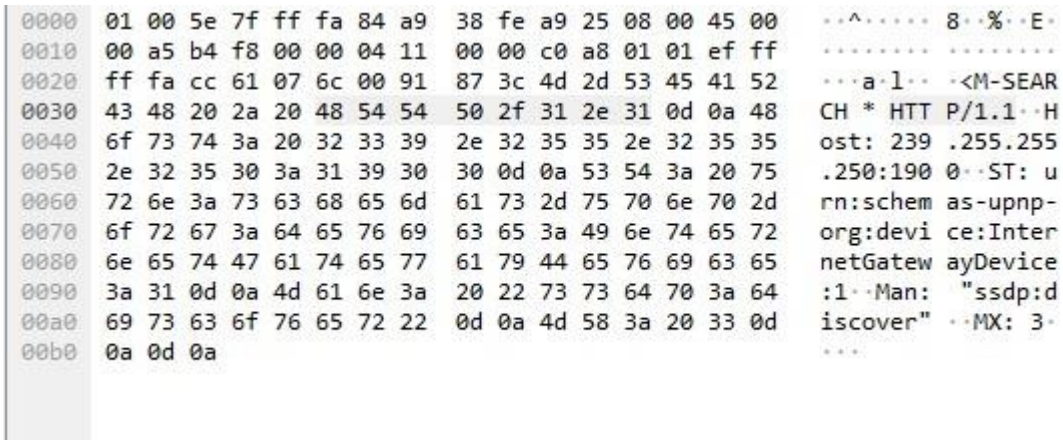


2. **Packet details:**

The details pane, found in the middle, presents the protocols andprotocol fields of the selected packet in a collapsible format. In additionto expanding each selection, you can apply individual Wireshark filtersbased on specific details and follow streams of data based on protocol type by right-clicking the desired item.



2. **Packet bytes:** At the bottom is the packet bytes pane, which displays the raw data of the selected packet in a hexadecimal view. This hex dump contains 16 hexadecimal bytes and 16 ASCII bytes alongside the data offset. Selecting a specific portion of this data automatically highlights its corresponding section in the packet details pane and vice versa. Any bytes that can't be printed are represented by a period. To display this data in bit format as opposed to hexadecimal, right-click anywhere within the pane and select as bits.

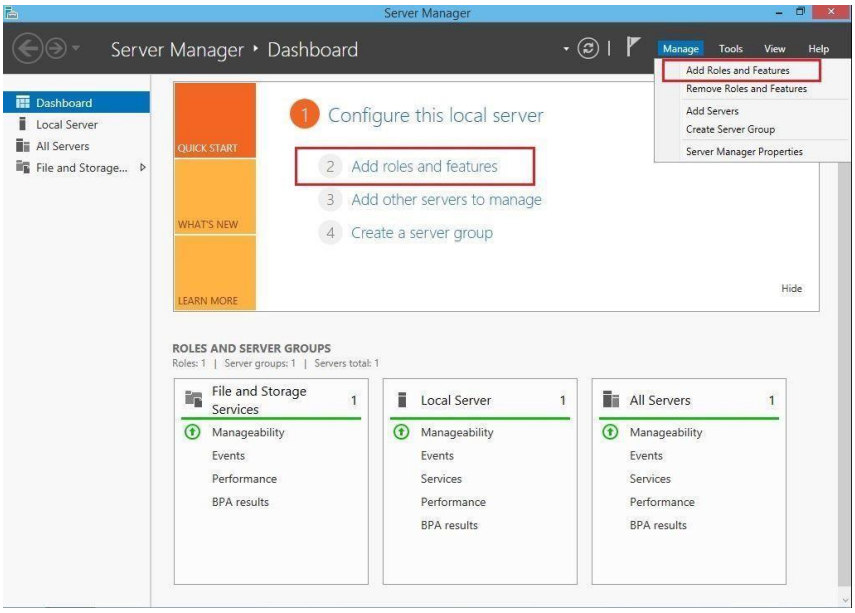


Windows Server 2012 R2 Lab

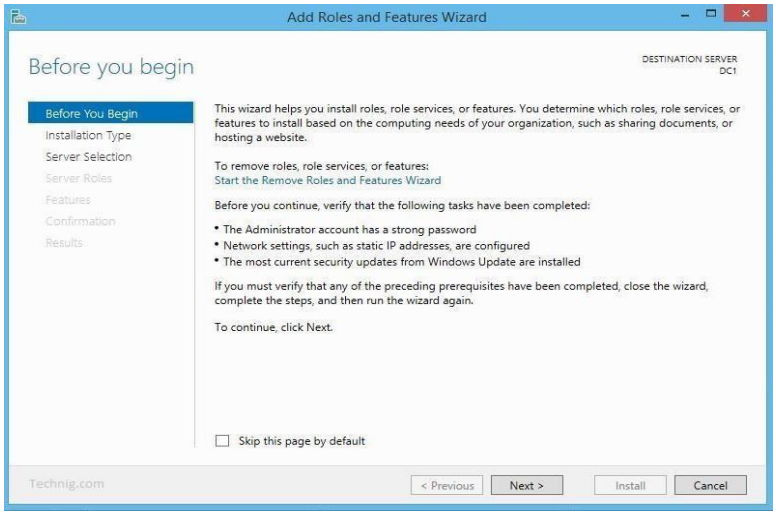
Lab 18: Configuring Active Directory Domain Service

1. Clicking on the **Server Manager** to open it.

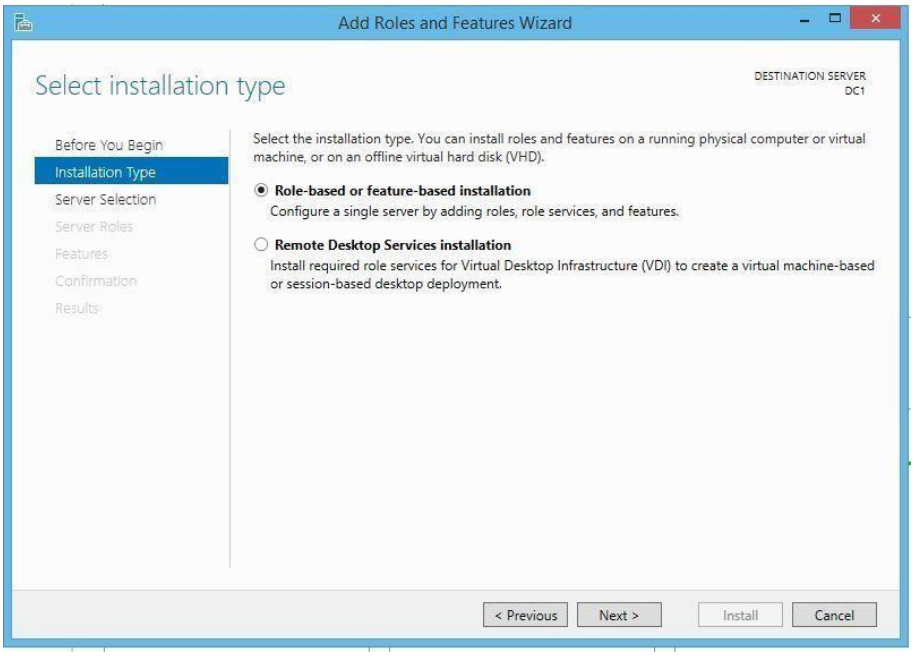
2. Here we see the Server Manager dashboard. Now going to **Manage** tab and clicking **Add Roles and Features**.



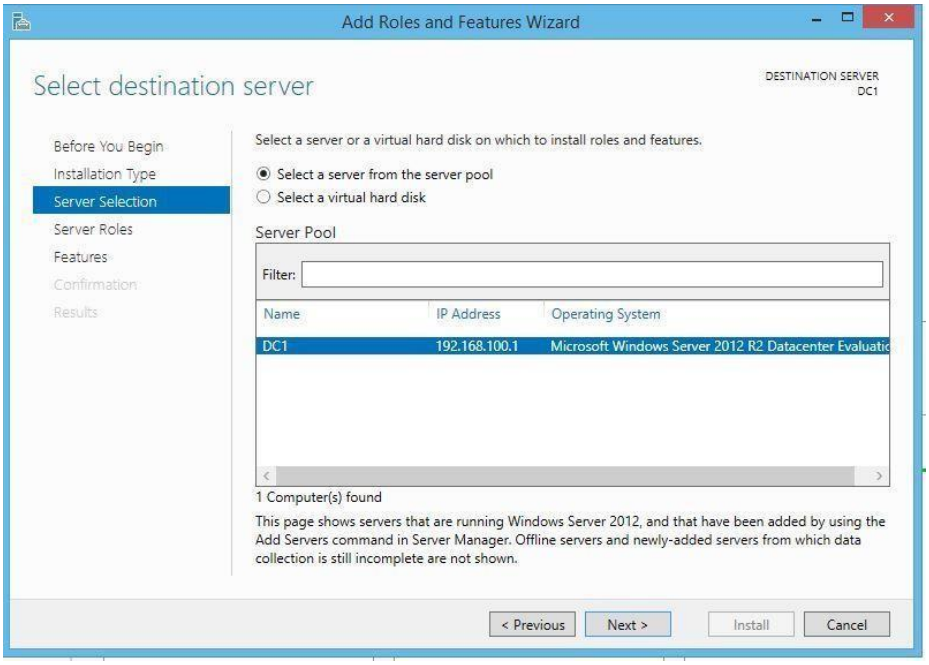
3. Clicking **Next** in **Add Roles and Features Wizard** page.



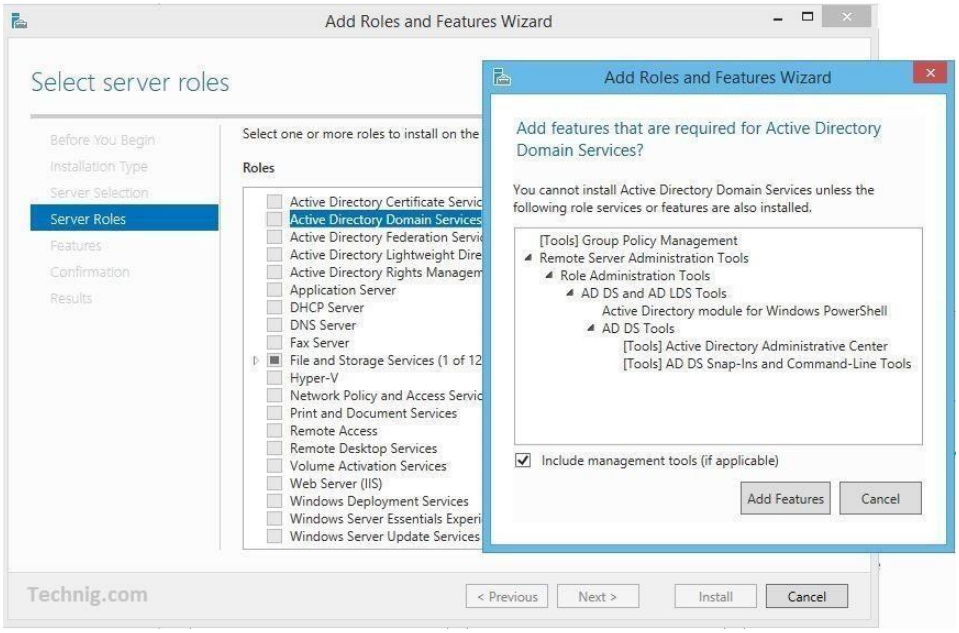
4. Letting the default **Role based or feature base installation** has selected and clicking **Next**.



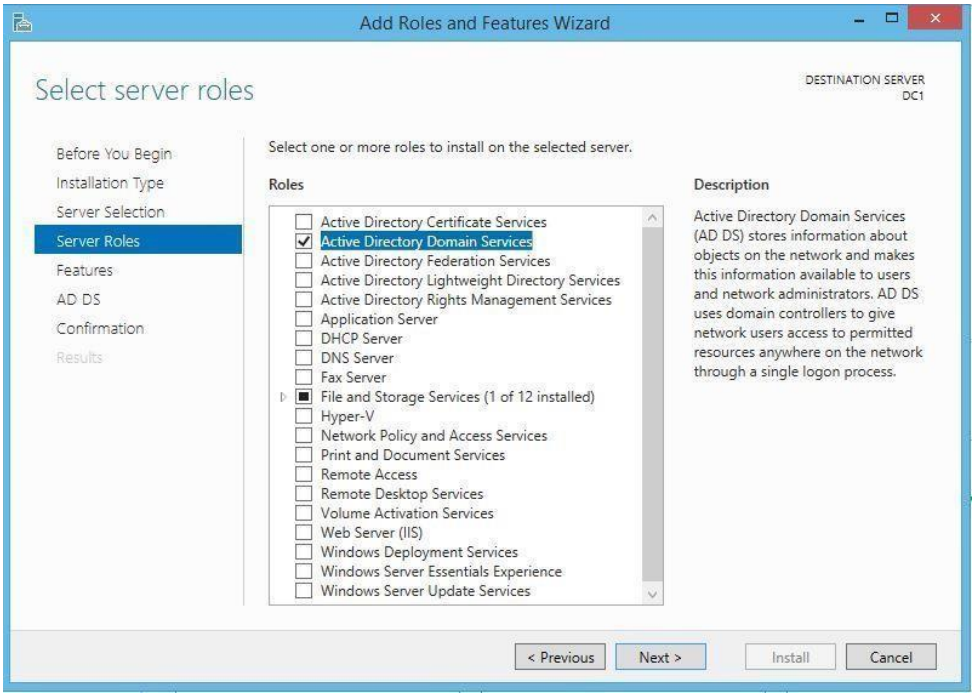
5. In the **Selecting destination server** page, selecting the server we want to install AD and clicking **Next**.



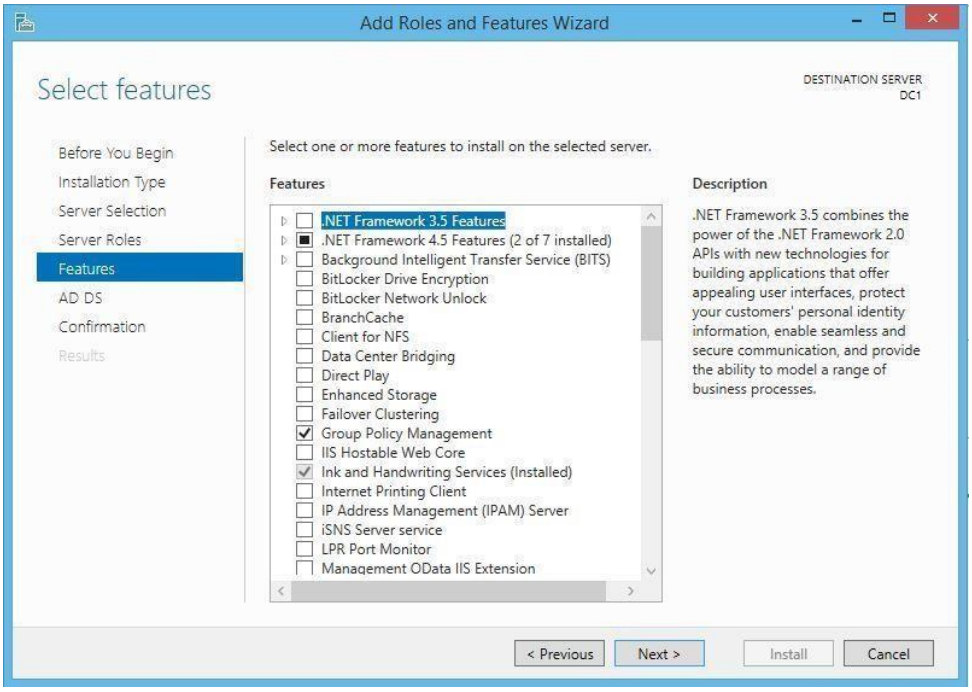
6. Now selecting the **Active Directory Domain Services** from Roles list in order to install it. When prompted to add the **required features for Active Directory Domain Services** within a new window, clicking **Add Features**.



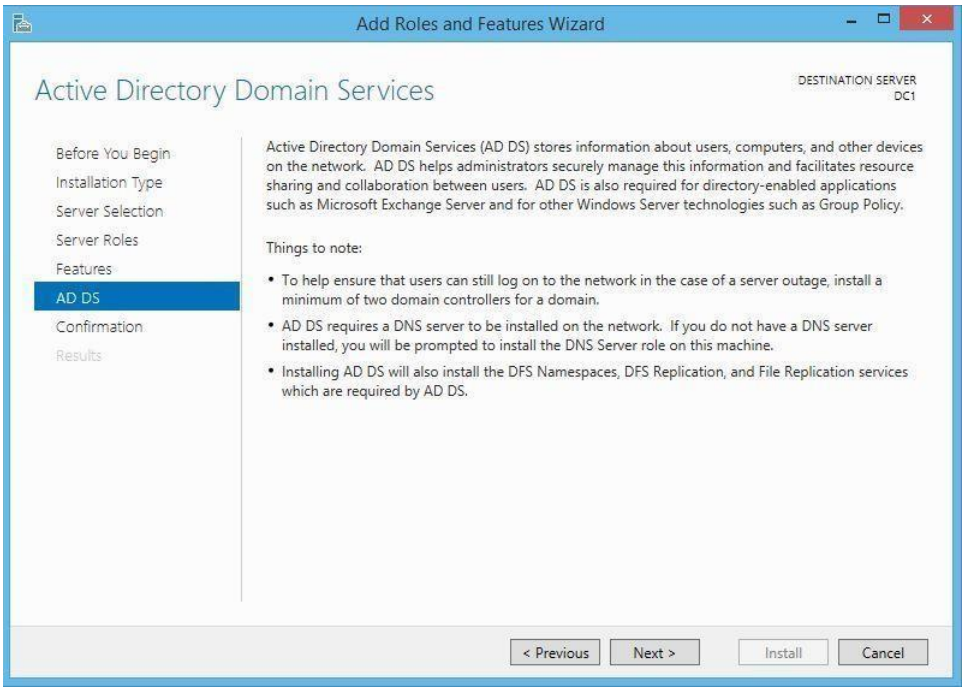
7. Now the **Active Directory Domain Services** has been selectinged and ready to install. Just clicking **Next**.



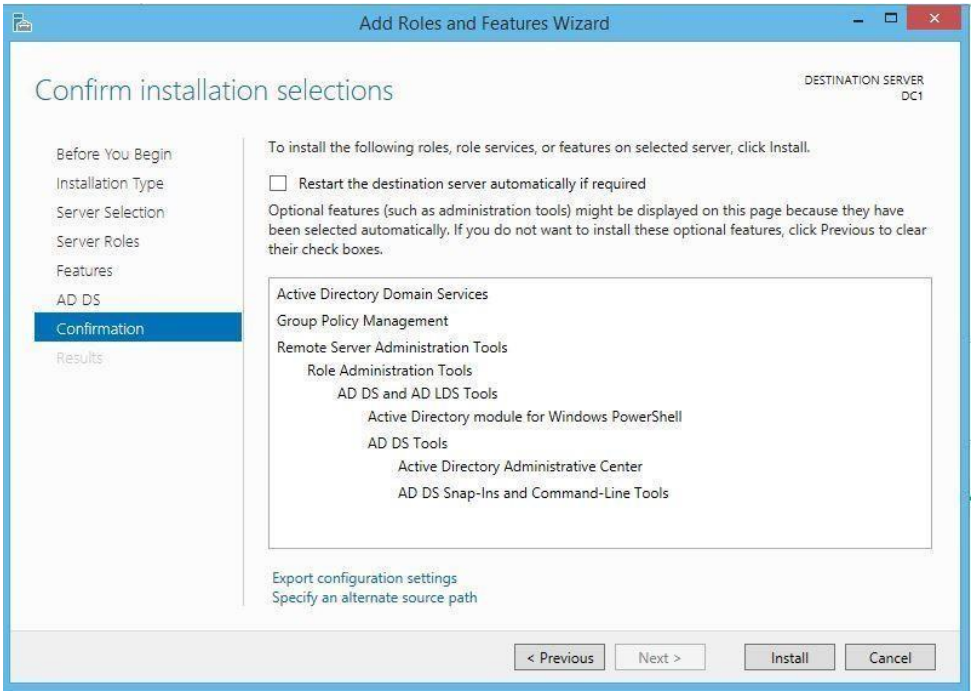
8. Leaving the **Windows Features** page by default and clicking **Next**.

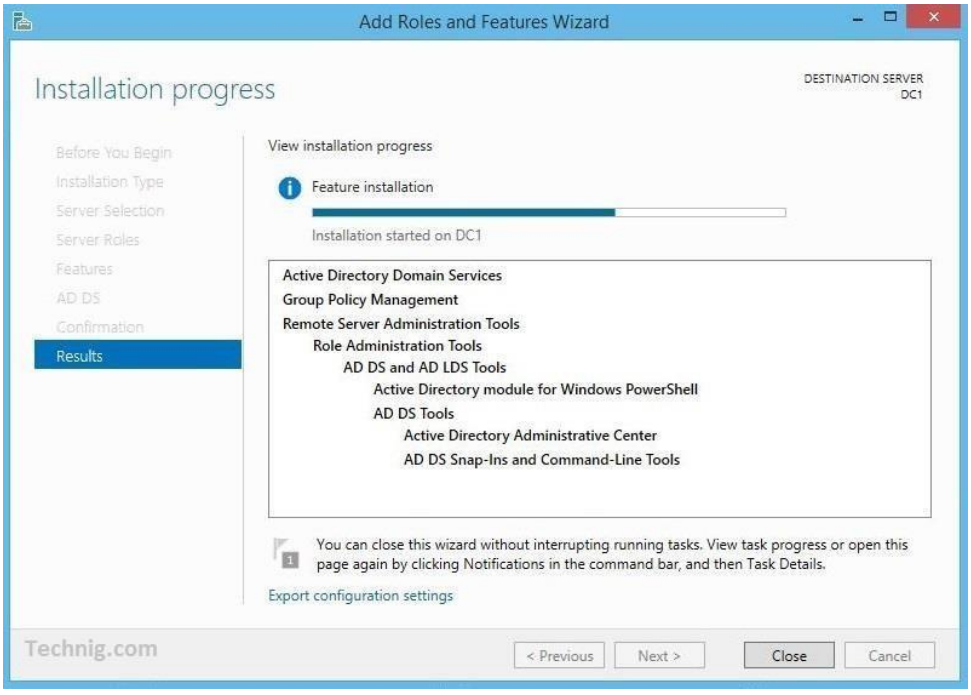


9. Now, we may need to read some information about **Active Directory Domain Service**. In this page reading once and clicking **Next**.

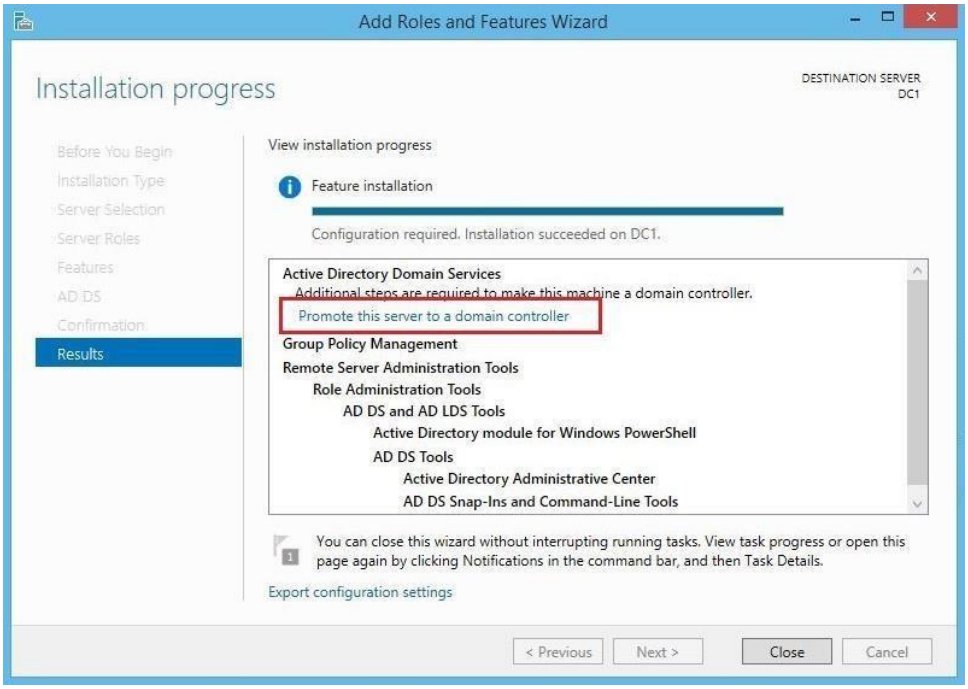


10. In the **Confirm Installation selectingions** page clicking **Install** to begin installation of AD DS.

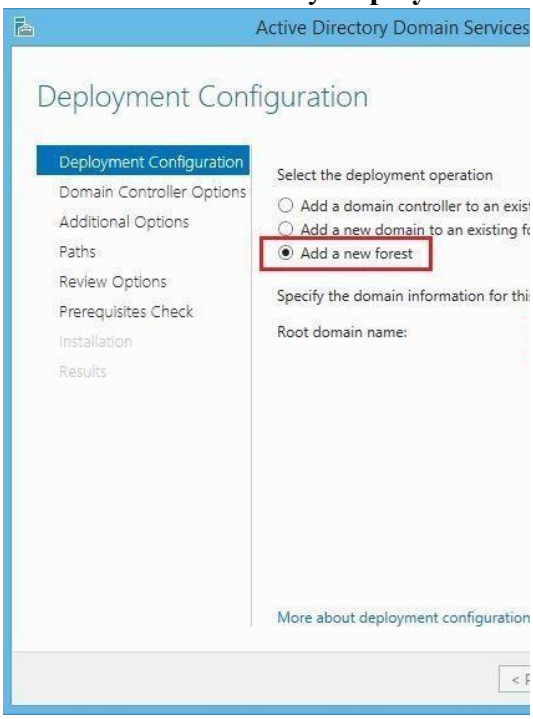




11. When the AD DS installation has completed. **clicking** the **Promote this server to a domain controller**.



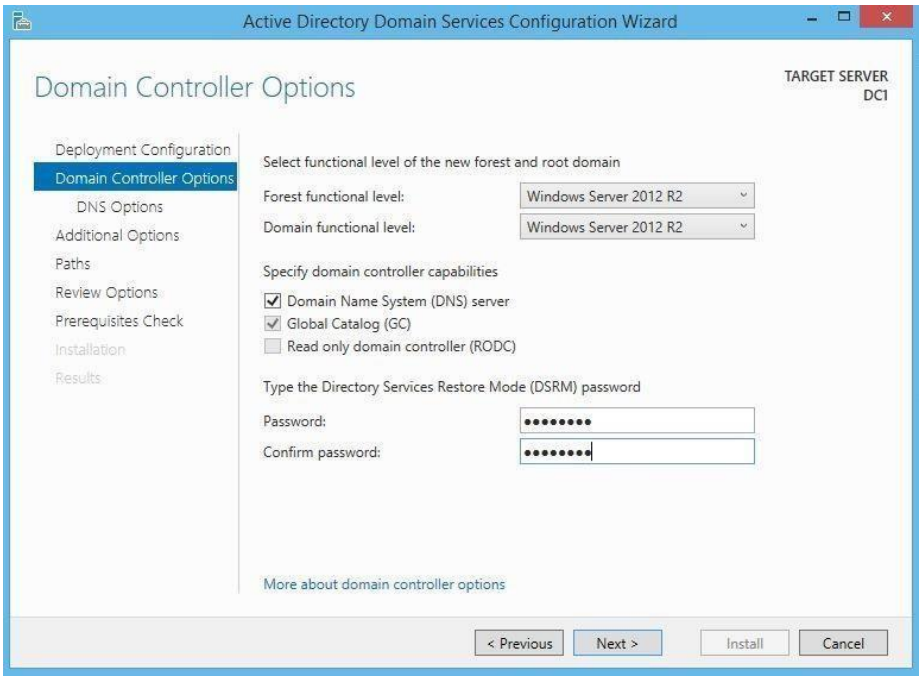
12. The Active directory **Deployment Configuration** page will open.



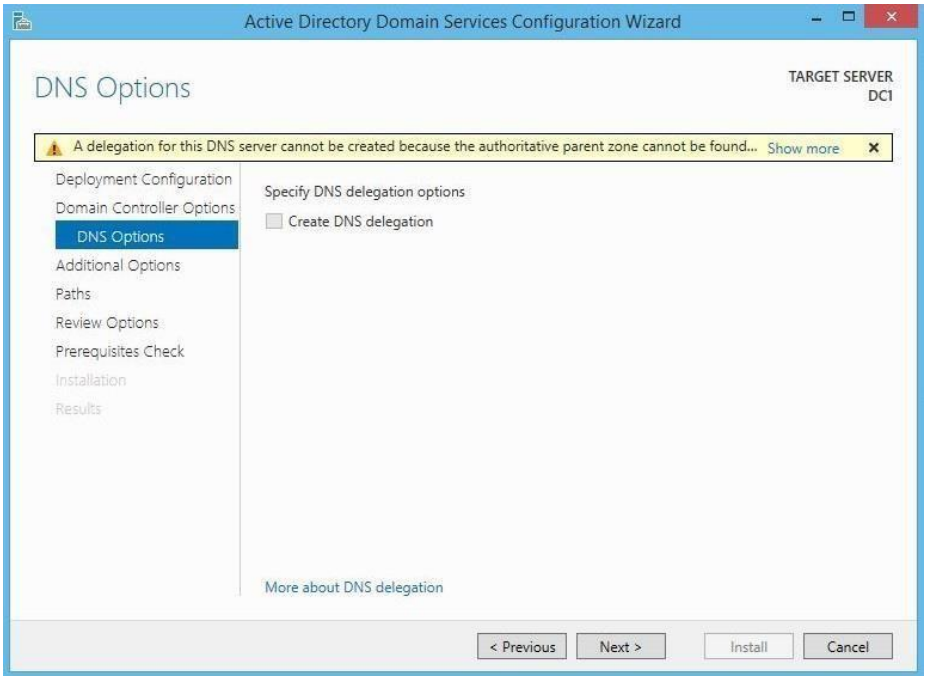
Primecollege.com

13. In this window selecting **add a new forest** and typing our domain name in the **Root domain name** field then clicking **Next**. I have chose the domain name **primecollege.com.**

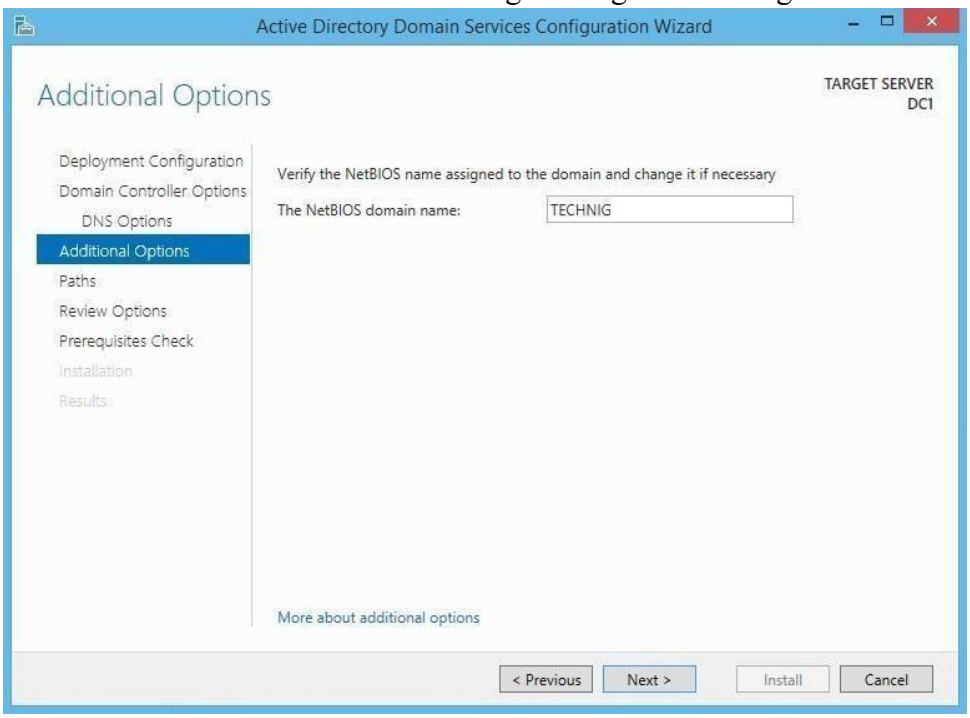
14. Leaving the **Domain Controller Options** by default, just typing password for **Directory Services Restore Mode (DSRM) password** and clicking **Next**.



15. Ignoring the delegation for DNS server warning and clicking **Next**.

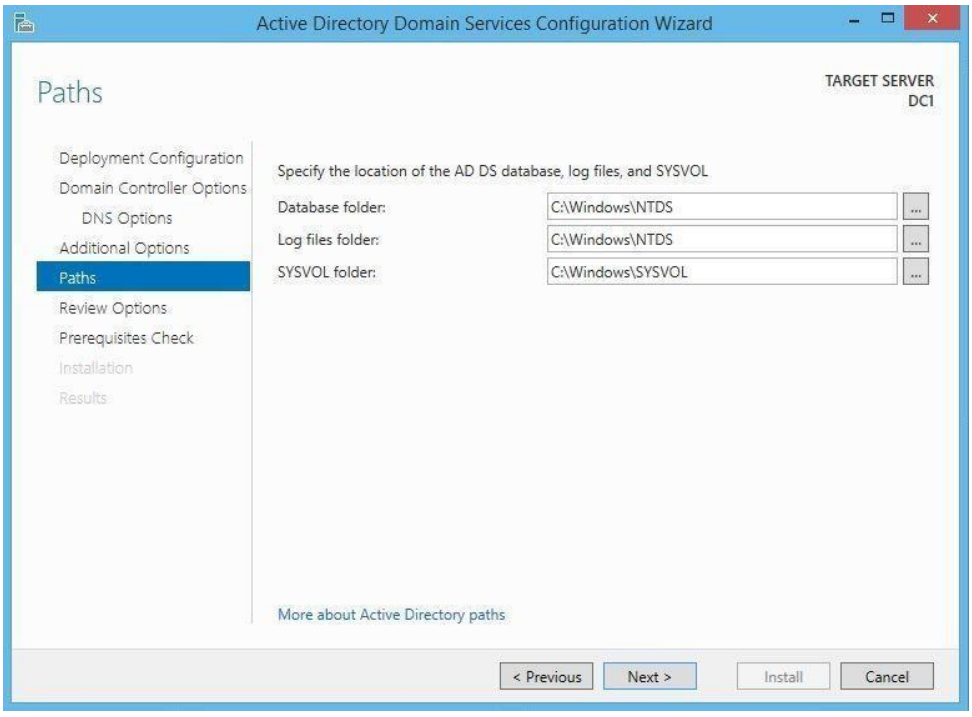


16. On the **Additional Options**, system will create a NetBIOS name according to our domain name. In this window doing nothing and clicking **Next**.

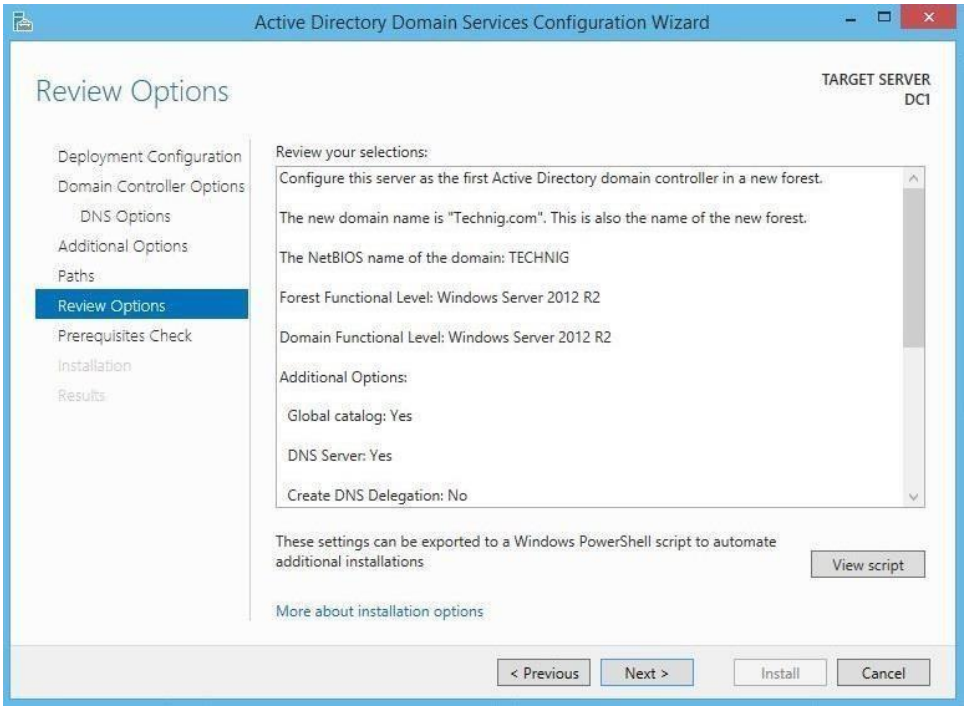


PRIMECOL

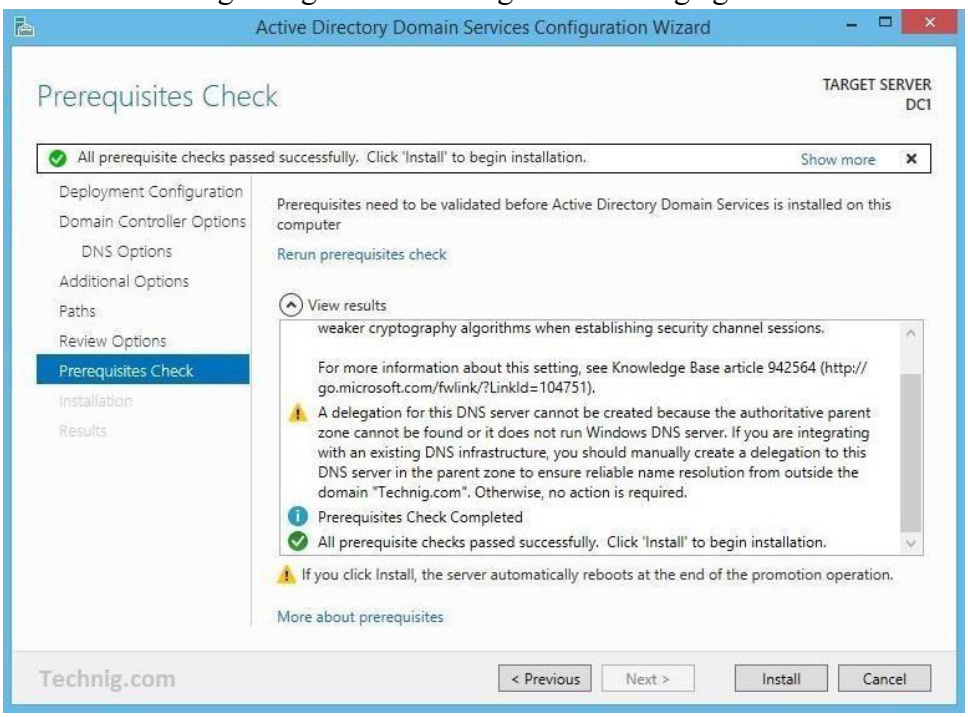
17. We can change the default directories for Database folder, Log files, and SYSVOL folder, and clicking **Next**.

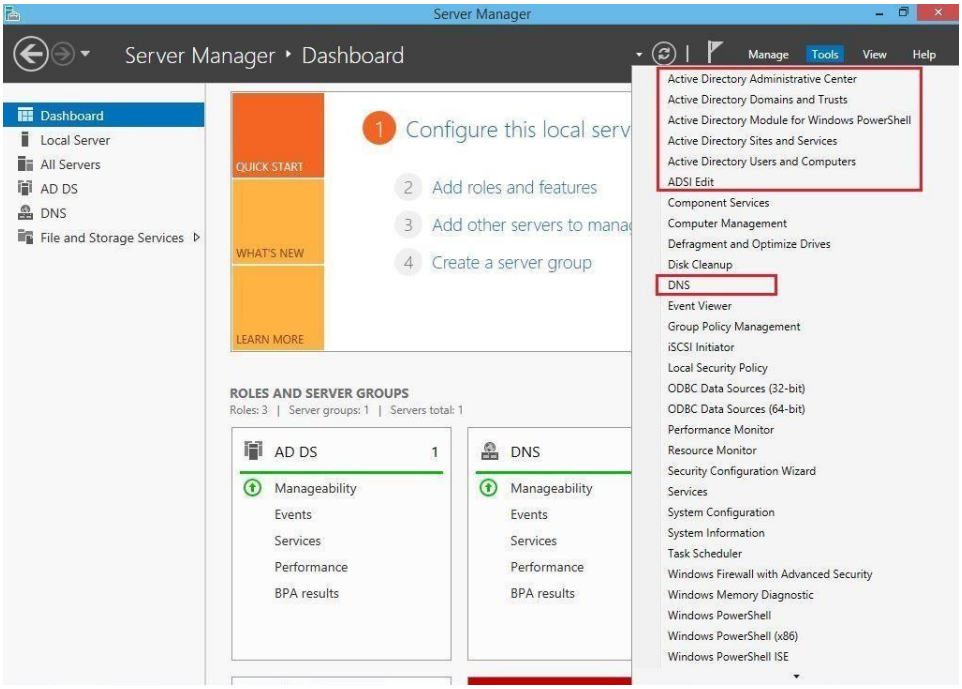


18. Finally on the **Review Options** page, checking and reviewing all option to insure and clicking **Next**.



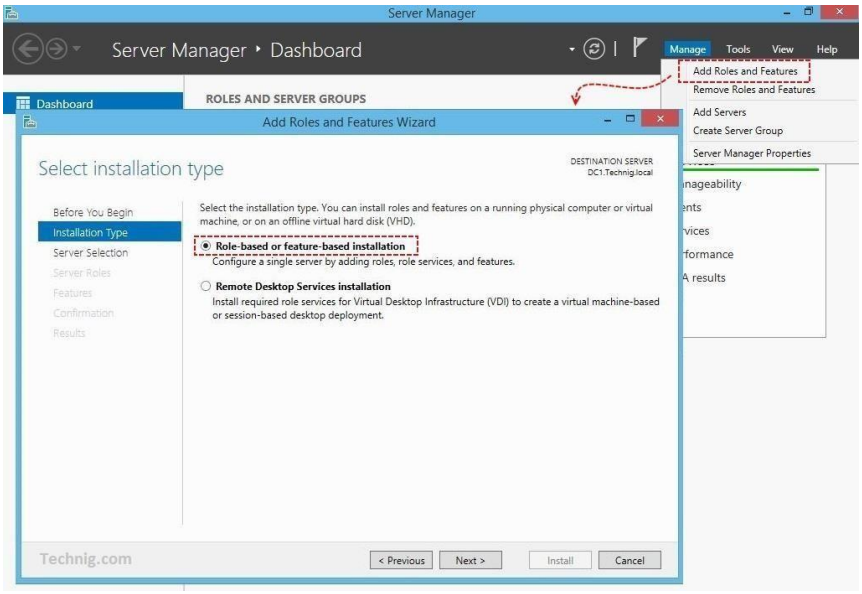
19. Once the system has checked prerequisites features for Active Directory, clicking **Install** and ignoring the DNS delegation warning again.





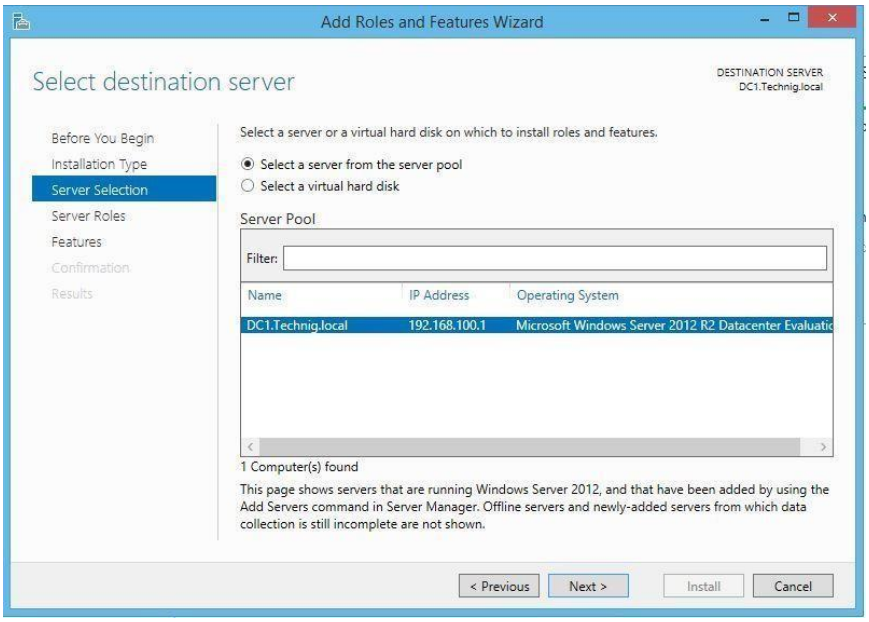
Lab 19: Configuring DHCP Service in Windows Server

1. Going to **Dashboard** on **Server Manager** and clicking **Manage** then clicking **Add Rules and Features**.

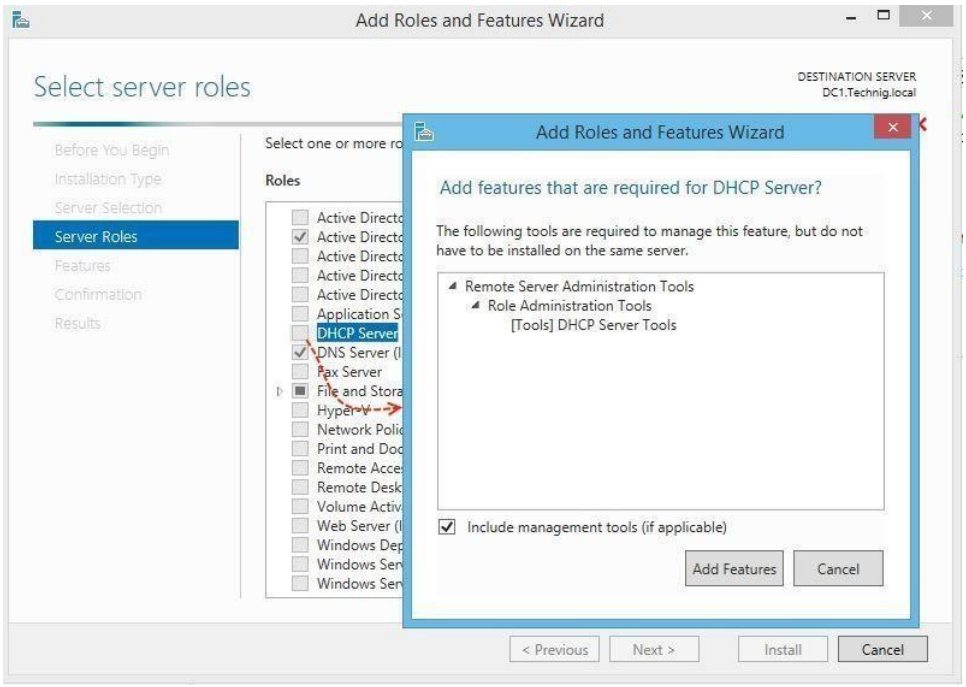


2. In the Role installation window selecting **Role-based or feature-based installation** the clicking **Next**.

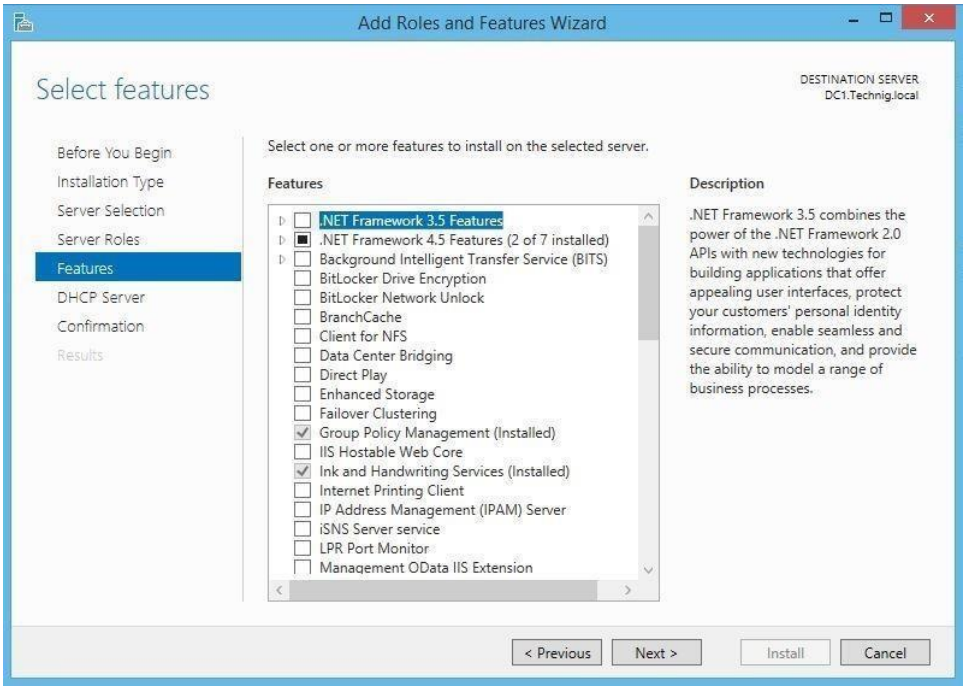
3. Choosing the server we want to install DHCP from the **Server pool**. Here we have one server and selecting by default.



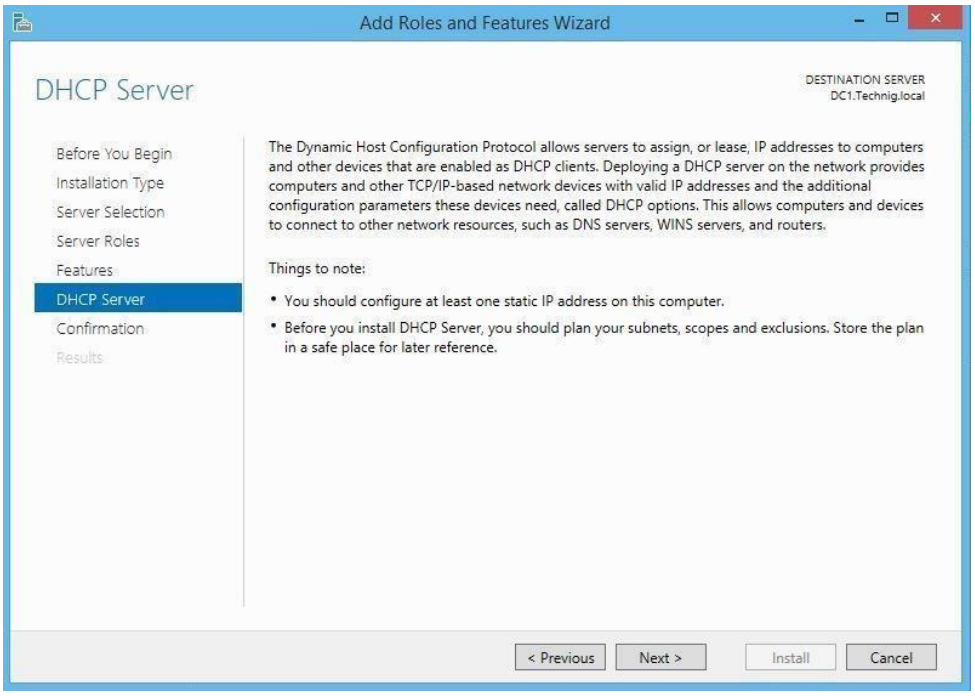
4. From the Roles list selecting DHCP Server. When the Add Roles and Features Wizard Page opened, clicking **Add Features** then clicking **Next**. That will install required features for DHCP Server.



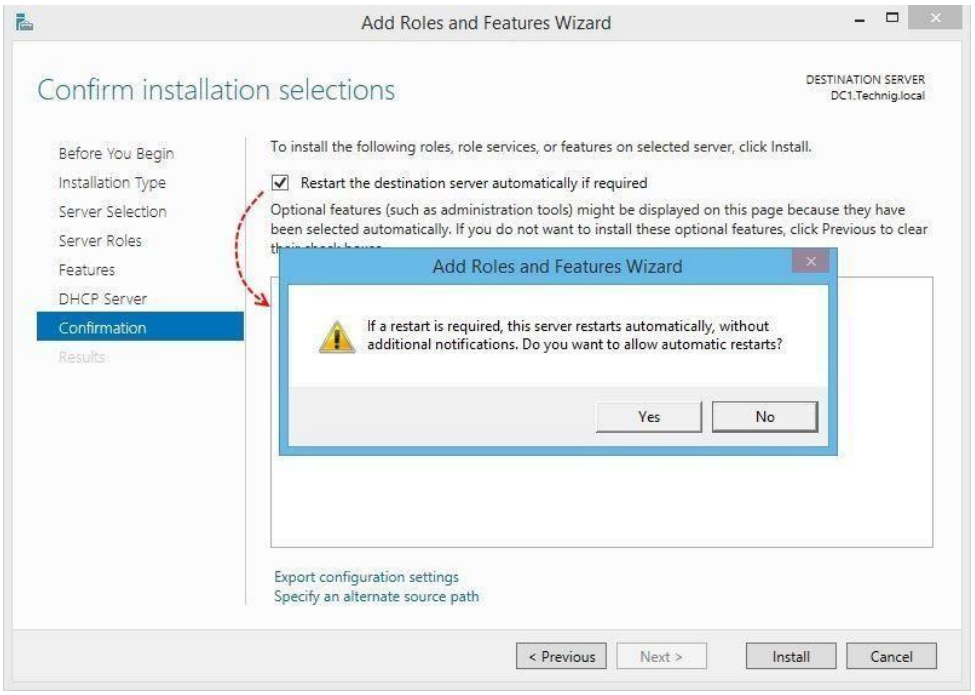
5. In the Features window, we do not change anything, just clicking **Next**.



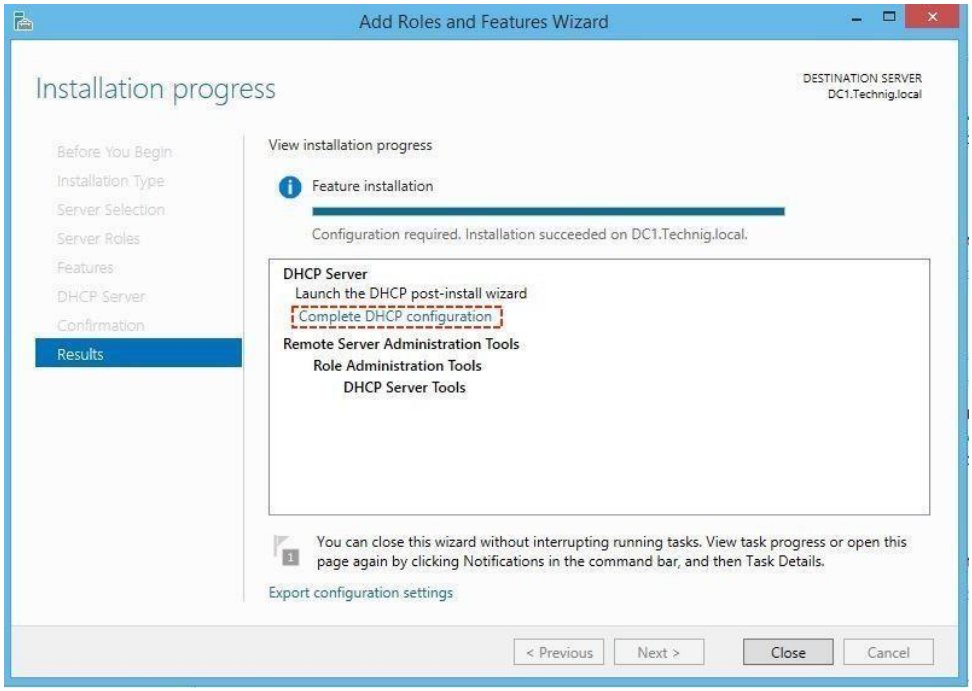
6. Once reading the information about DHCP Server and clicking **Next** button.



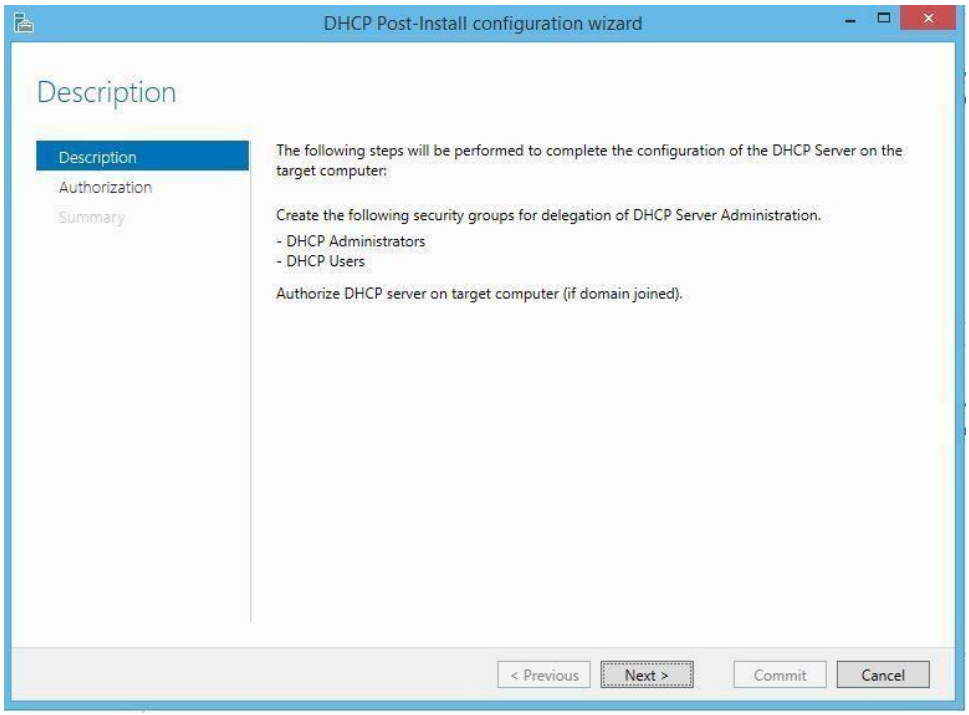
7. In the **Confirm Installation** page, selecting **Restart the destination server automatically if required**. Clicking **Yes** the warning window and clicking **Install**.



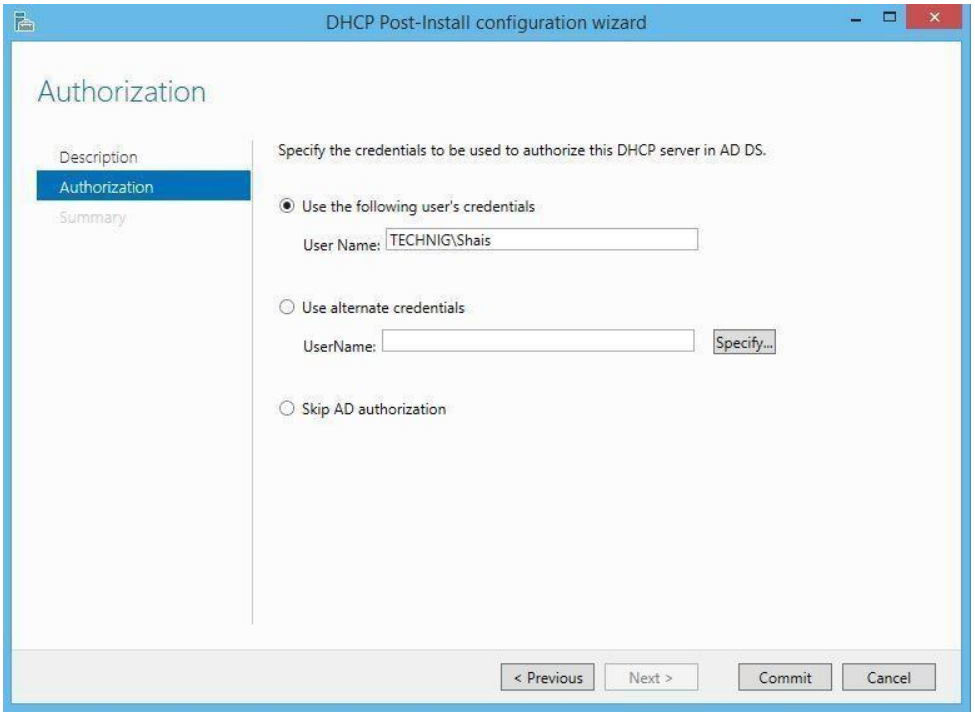
8. The installation will take a minute, when it has completed successfully clicking **Complete DHCP Configuration** link.



9. Reading **DHCP Post-Install configuration wizard description** and clicking **Next**.



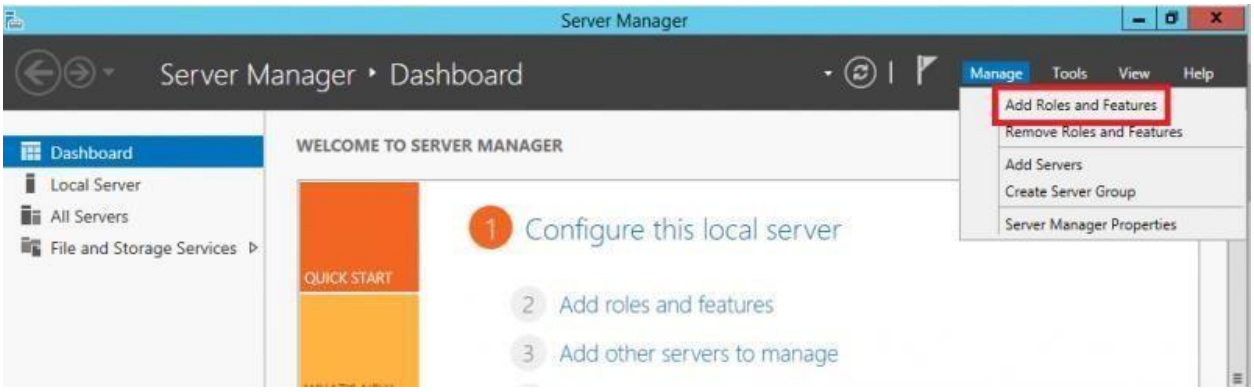
10. Setting the appropriate user for management of DHCP Server. Here we leave it by default.



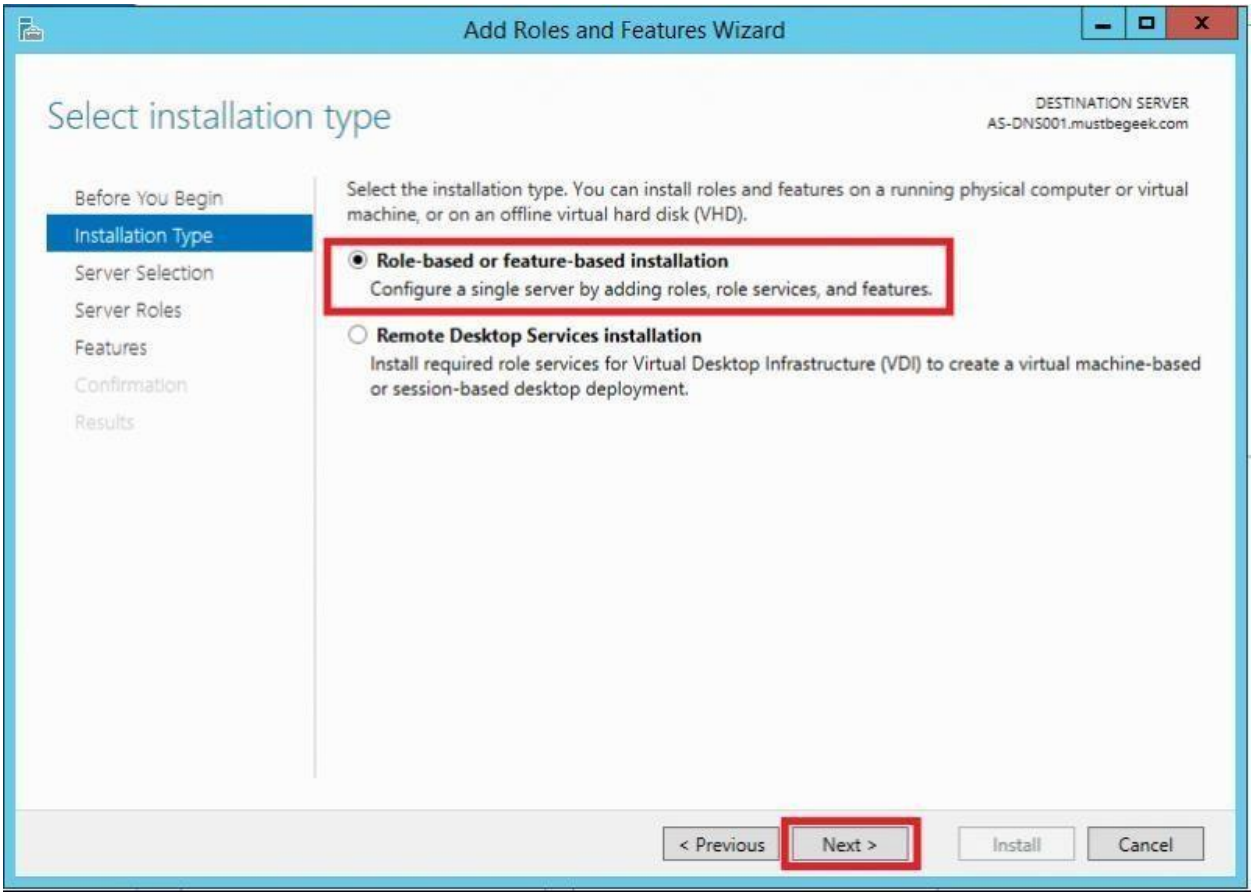
11. On the **DHCP summary** window clicking **Close** and closing the DHCP Installation page also.

Lab 20: Configuring DNS Service in Windows Server

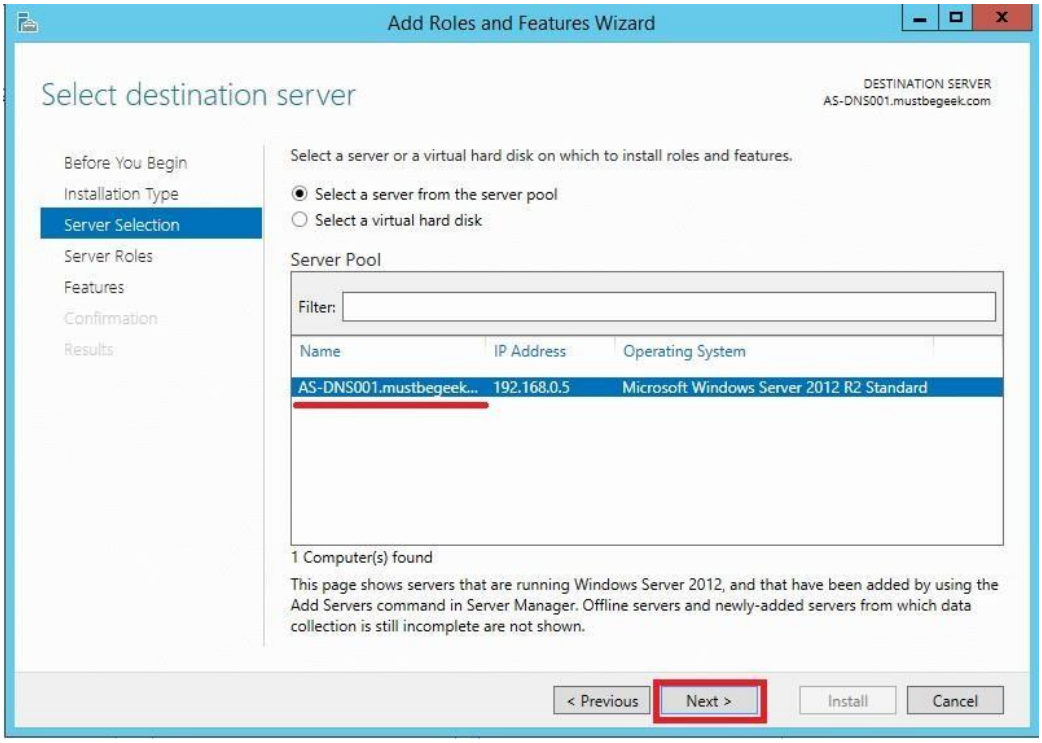
1. Opening **Server Manager** console and selecting **Manage > Add Roles and Features.**



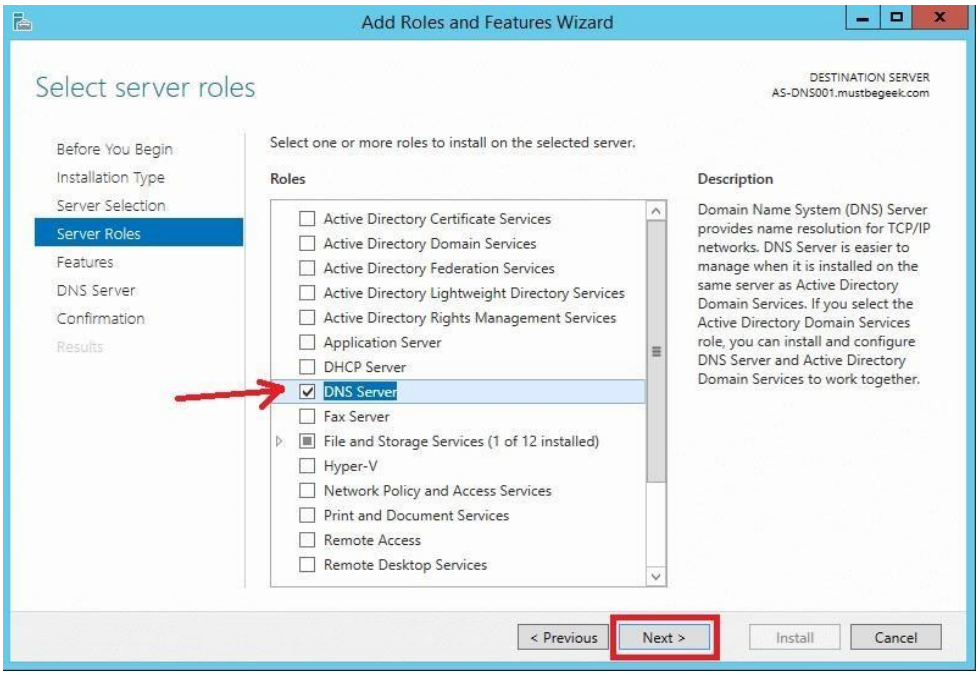
2. Selecting **Role-based or feature-based installation** and clicking the **Next** button.



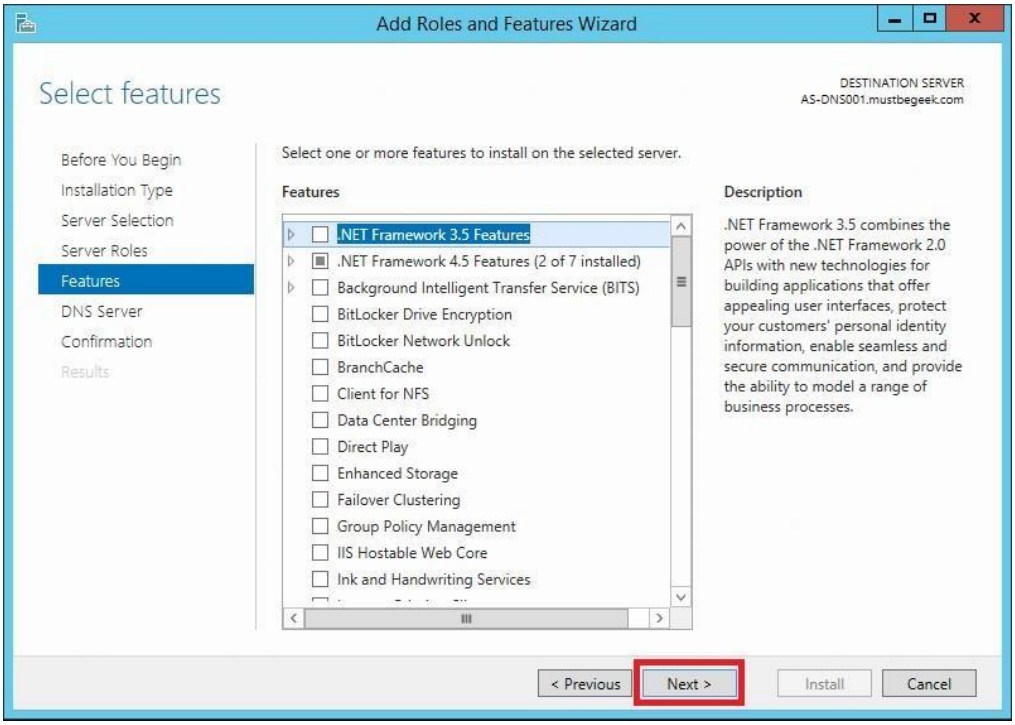
3. On the server pool selection, ensuring the local server is selected, then clicking **Next**.



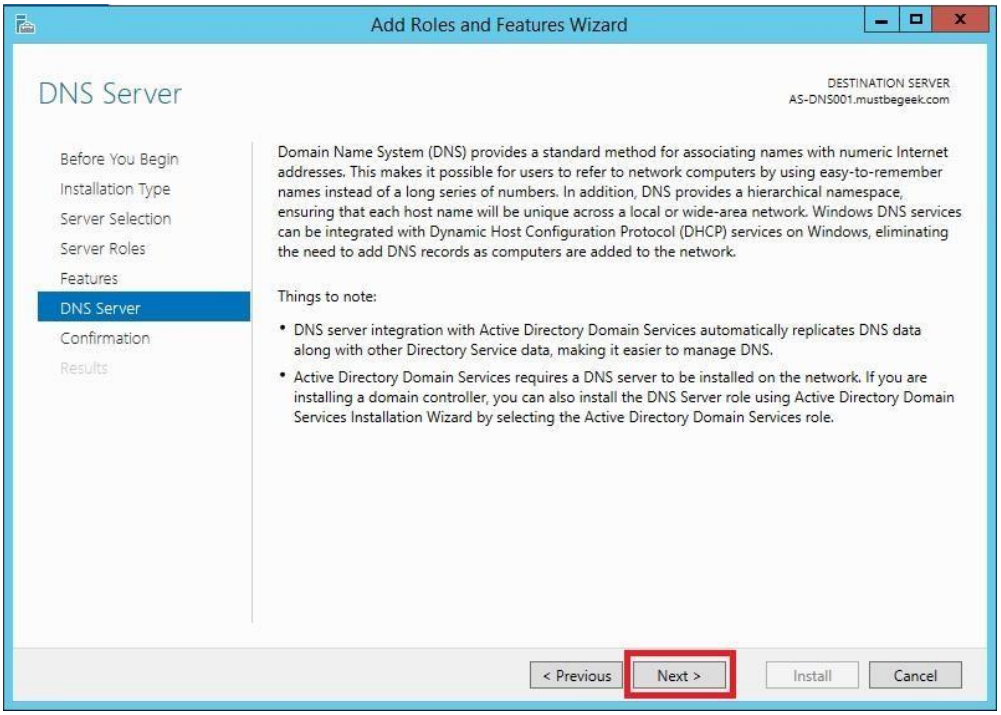
4. On the server roles selection, ticking the checkbox for **DNS Server** role.



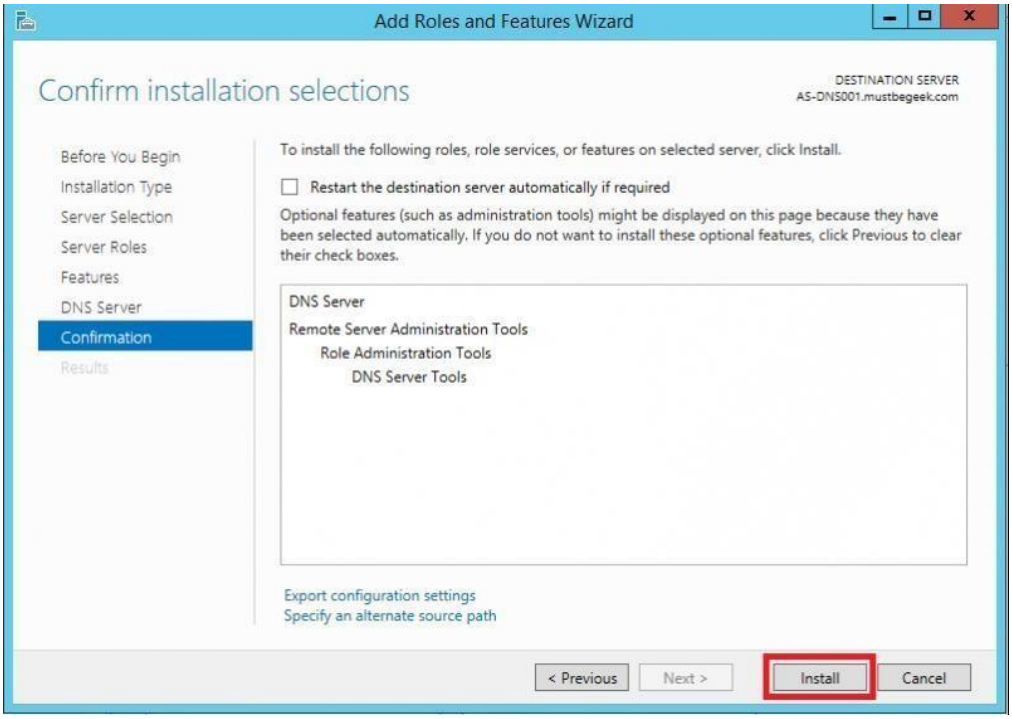
5. On the features selection, clicking **Next**.



6. Reading the summary about DNS Server then clicking **Next** to continue.



7. Confirming the installation summary then clicking **Install** button to proceed.



8. The progress bar showing the DNS Server role installation will start, clicking **Finish** when it is completed.