UNIVERSITY OF MUMBAI

DEPARTMENT OF COMPUTER SCIENCE

M.Sc. Computer Science – Semester III

Track C: Computer Networking

Elective I: Server and Data Centric Networking

JOURNAL

2022-2023

Seat No. _____

मुंबई विद्यापीठ
University of Mumbai
Re-accredited with A++ Grade
(CGPA 3.65) by NAAC (3rd Cycle 2021)

UNIVERSITY OF MUMBAI

DEPARTMENT OF COMPUTER SCIENCE

CERTIFICATE

This is to certify that the work entered in this journal was done in the University Department of Computer Science laboratory by Mr./Ms. _____ Seat No. _____ for the course of M.Sc. Computer Science - Semester III (CBCS) (Revised) during the academic year 2022- 2023 in a satisfactory manner.

_____ _____

Subject In-charge **Head of Department**

_____

External Examiner

Index

Practical-1A

Aim: Installation of VMware Esxi, Citrix Xen, Microsoft Hyper-V

Esxi Server:

VMware ESXi, also called VMware ESXi Server, is a bare-metal hypervisor developed by VMware for vSphere. ESXi is one of the primary components in the VMware infrastructure software suite. ESXi is a Type 1 hypervisor, meaning it runs directly on system hardware without the need for an OS.

Implement VMware on ESXI Server

Step 1:

Open VMware Workstation. Click on New VM.

Step 2:

Select Typical(recommended) & click on Next.

Step 3:

Click on Installer Disc image file > Select VMware ESXi Server.iso file > Next.

Step 4:

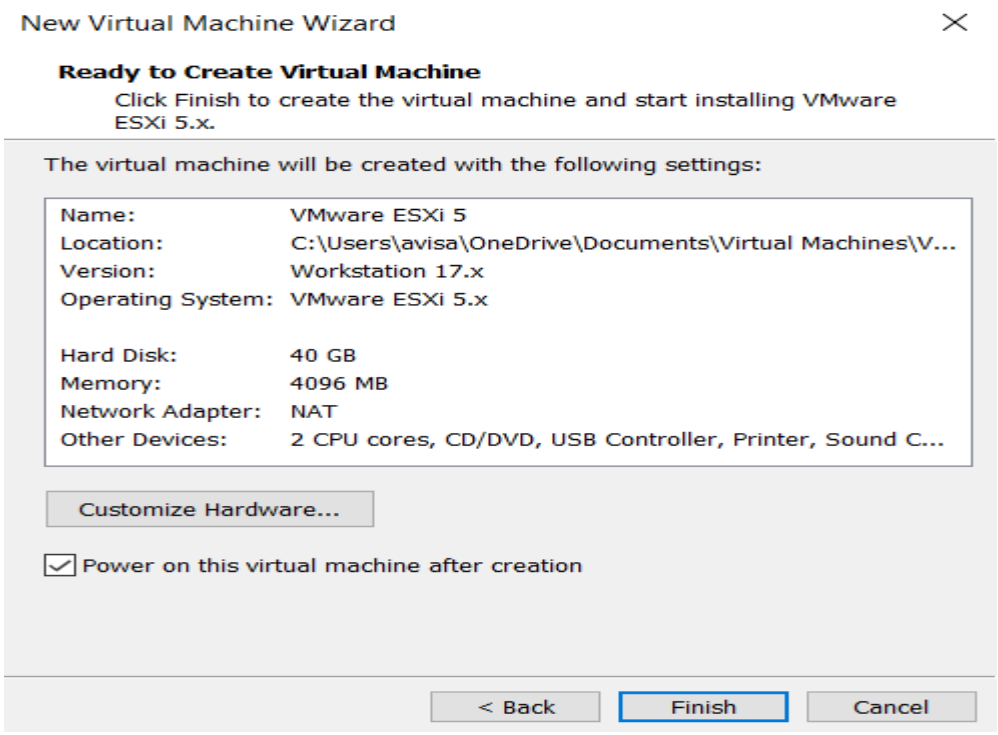
Give name: - VMware ESXi 5

Step 5:

Select Store virtual disk as a single file & Give size as 40.0 Gb.

Step 6:

Click on Finish.



Step 7:

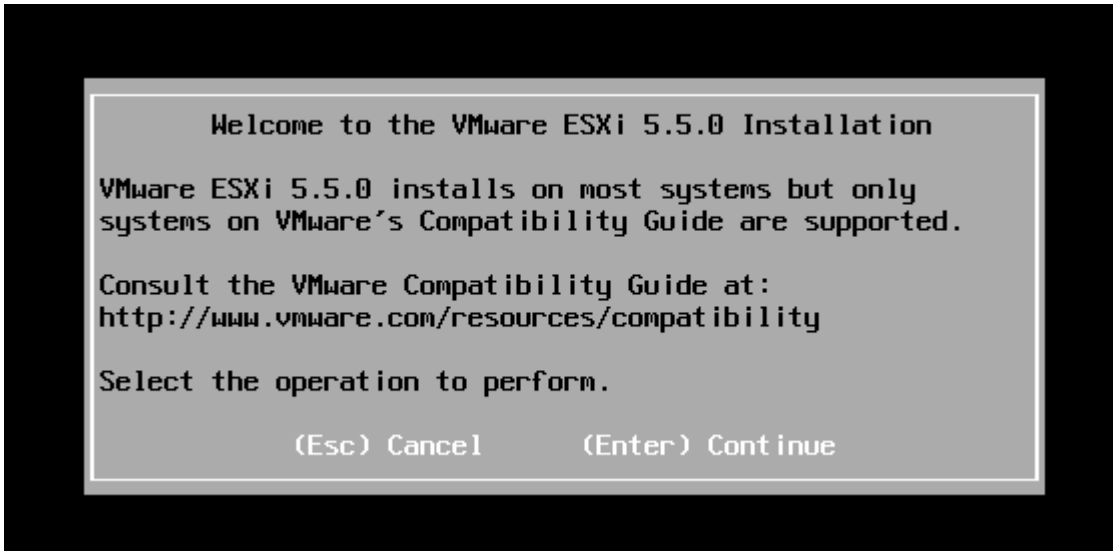
Click on Start > Select 1st option.

Step 8:

Wait until all packages are installed.

Step 9:

Press Enter.



Step 10:

Press Enter.

Step 11:

Select US Default > Enter.

Step 12:

Give password: - admin123.

Step 13:

Press F11 Button.

Step 14:

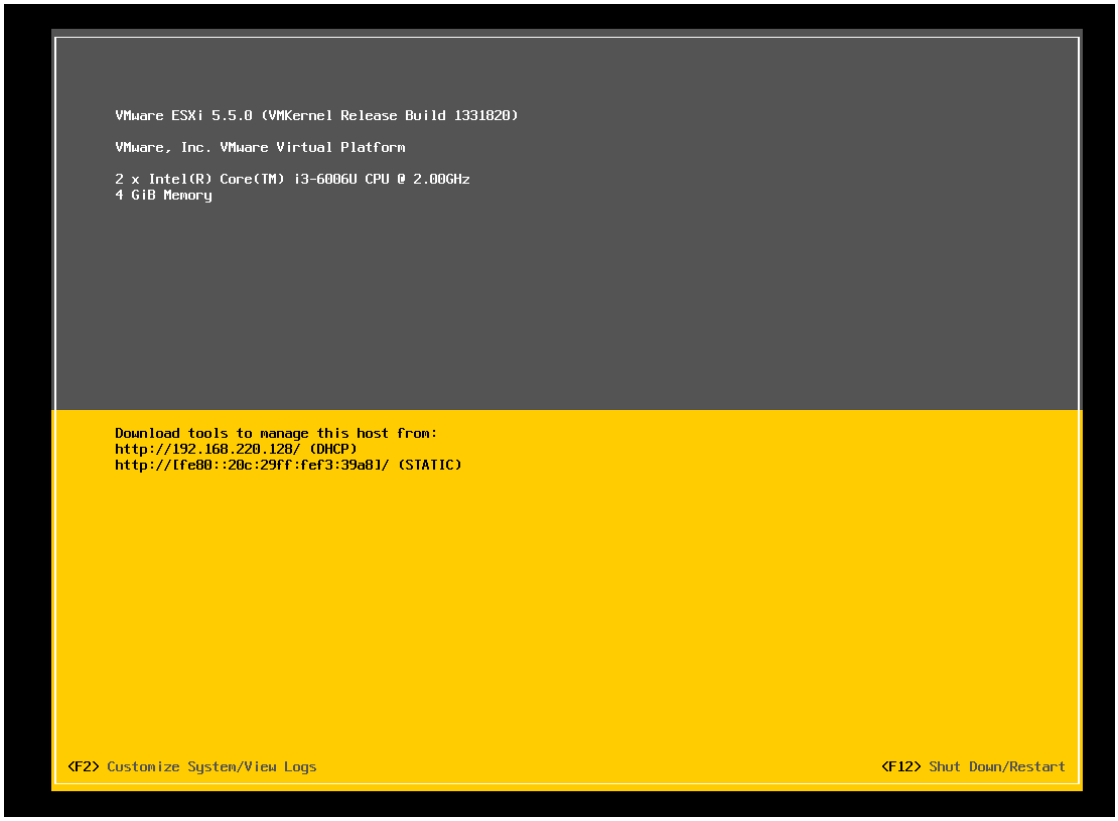
VMware ESXi is being installed.

Step 15:

Press Enter to Reboot.

Step 16:

After Reboot you can see the ip address: - 192.168.159.129.



Step 17:

Select VMware-viclient-all-5.1.0.exe installer and install it.

Step 18:

Click on Ok.

Step 19:

Click on Next > Click on Install.

Step 20:

Click on Finish.

Step 21:

Select VMware vSphere Client shortcut on Desktop.

Step 22:

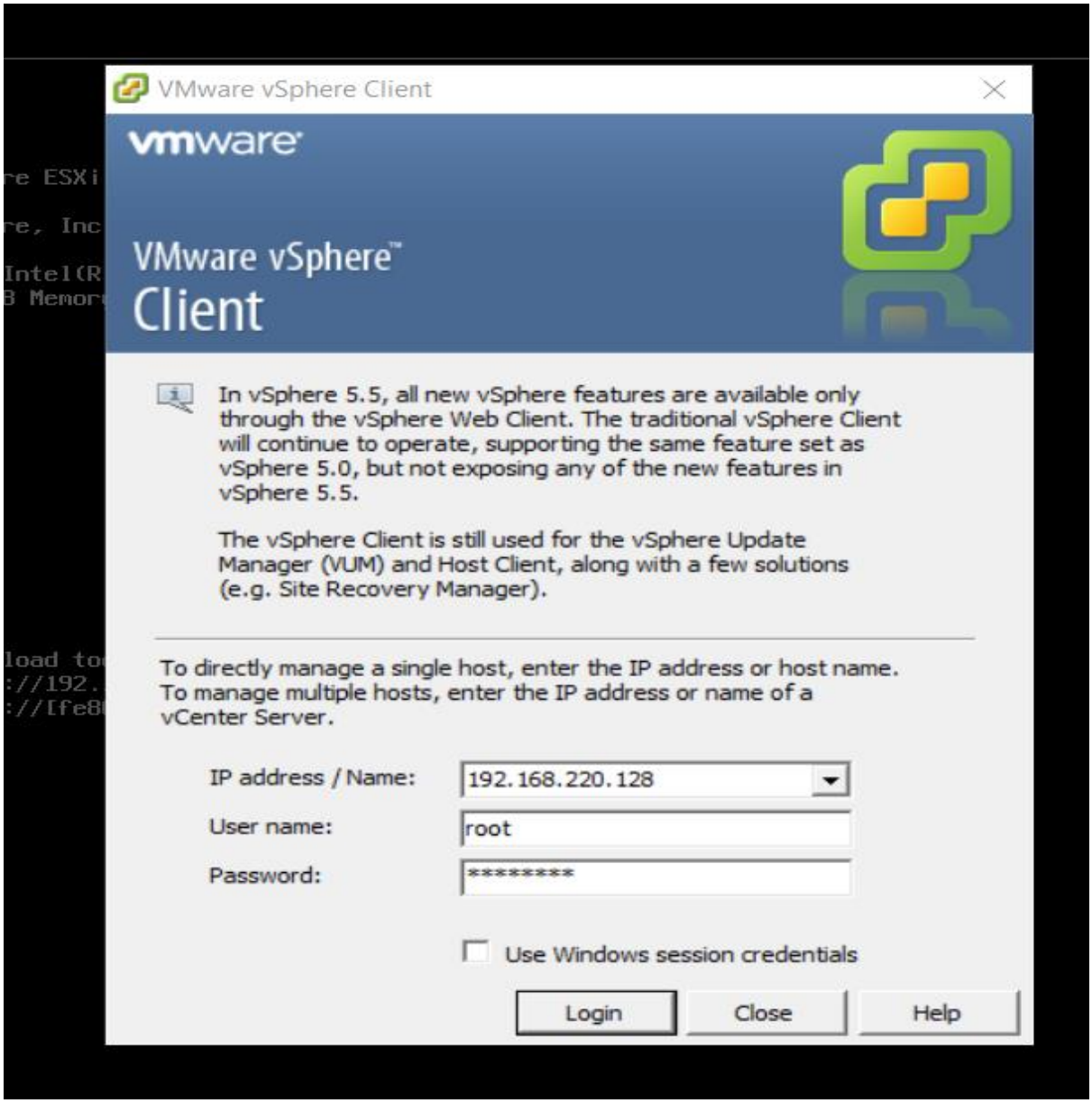
Give Ip address: - 192.168.228.128

User name: - root

Password: - admin123

Step 23:

Click on Login.


VMware vSphere Client
vmware
VMware vSphere™
Client
In vSphere 5.5, all new vSphere features are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0, but not exposing any of the new features in vSphere 5.5.
The vSphere Client is still used for the vSphere Update Manager (VUM) and Host Client, along with a few solutions (e.g. Site Recovery Manager).
To directly manage a single host, enter the IP address or host name.
To manage multiple hosts, enter the IP address or name of a vCenter Server.
IP address / Name:
192.168.220.128
User name:
root
Password:
****
Use Windows session credentials
Login
Close
Help

Practical-1B

Citrix Xen:

Citrix XenServer is an open-source server virtualization platform based on the Xen hypervisor. Citrix also offers a supported version that you can purchase, with two options: Standard and Enterprise.

This platform is used by virtualization administrators to deploy, host and manage VMs. It's also used to distribute hardware resources -- CPU, memory, networking, storage -- to VMs.

Prerequisites:

Step 1:

Create a folder > Give any name (cloud in our case),

Copy Windows 7 Iso File in it,

Right Click on the folder, click on properties and go to Sharing Tab.

Step 2:

Select > Everyone and Give > Read/Write (Permission Level)

Step 3:

Go to Start Menu > Control Panel > Network and Sharing Centre > Change advanced sharing settings.

Step 4:

Turn Off Password Protection Sharing > Save Changes.

Implement VM on XEN Server

Step 1:

Open VMware & Click on Add New Virtual Machine.

Step 2:

Select Hardware Compatibility as Workstation 11.x

Step 3:

Click on Installer disk image & Select Xen Server.iso file

Step 4:

Select VMware ESX as O.S & Version VMware ESXi 5

Step 5:

Give virtual machine name :- XEN SERVER AVINASH 2022

Step 6:

Select 2 Processors and Select 1 Core.

Step 7:

Select Ram as 4096 MB

Step 8:

Network Type :- Use host-only networking

Step 9:

Disk :- Create a new virtual disk

Step 10:

Storage Capacity :- 40Gb & Select Store virtual disk as a single file.

Step 11:

Your configuration is ready

Step 12:

Your new virtual machine XEN SERVER is created.

Step 13:

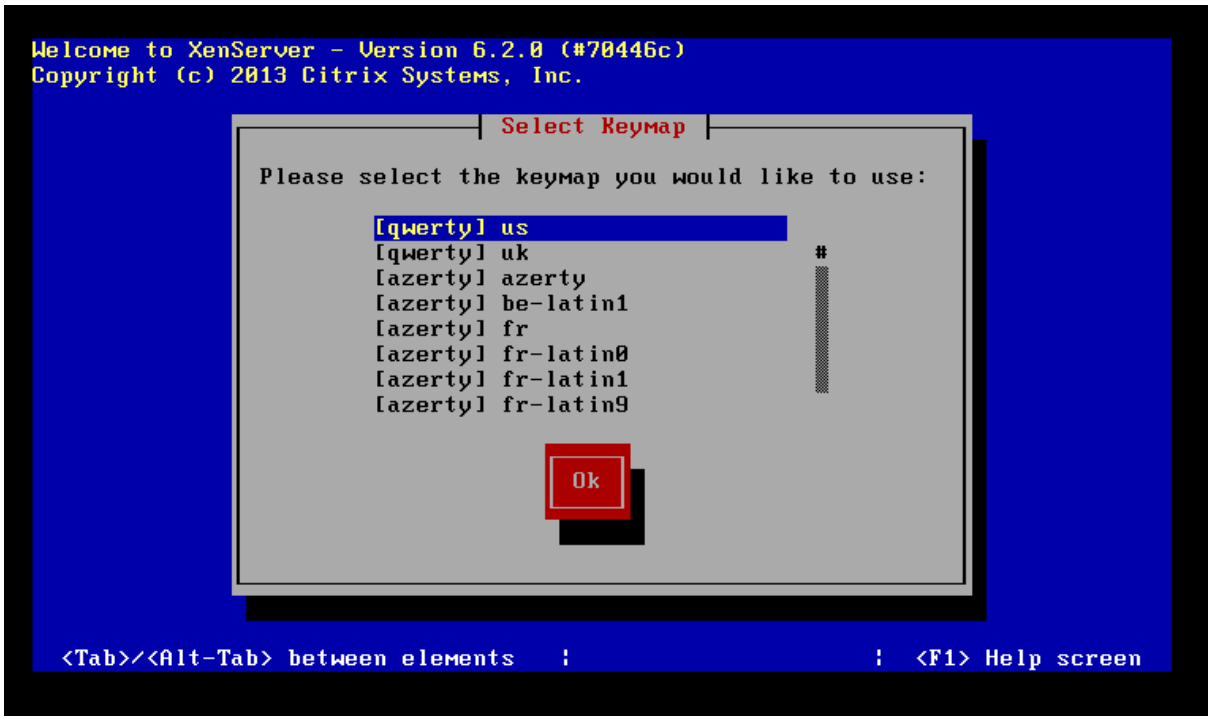
Click on Edit Virtual Machine > Processors > Select Virtualize Intel.

Step 14:

Start your virtual machine.

Step 15:

Select “[qwerty] us” and click on ok.



Step 16:

Click on Ok.

Step 17:

Click on “Accept EULA”.

Step 18:

Click on Ok.

Step 19:

Select “Local Media” and click on Ok.

Step 20:

Click on No.

Step 21:

Select “Skip verification” and click on Ok.

Step 22:

Username :- root (default) & Password :- admin123456. Click on Ok.

Step 23:

Click on Ok.

Step 24:

Enter the name for Hostname configuration and click on Ok.

Step 25:

Select “Asia” and click on Ok.

Step 26:

Select “Calcutta” and click on Ok.

Step 27:

Select “Using NTP” and click on Ok.

Step 28:

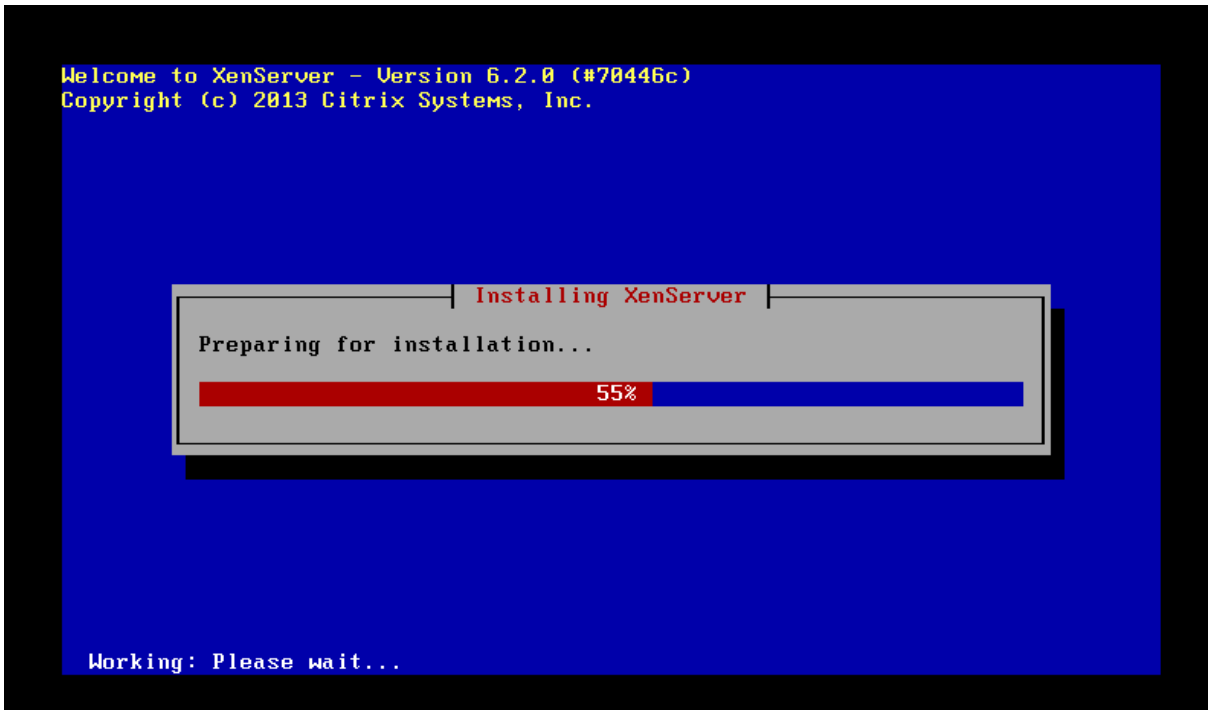
Click on Ok.

Step 29:

Click on “Install XenServer”.

Step 30:

Installing XenServer.



Step 31:

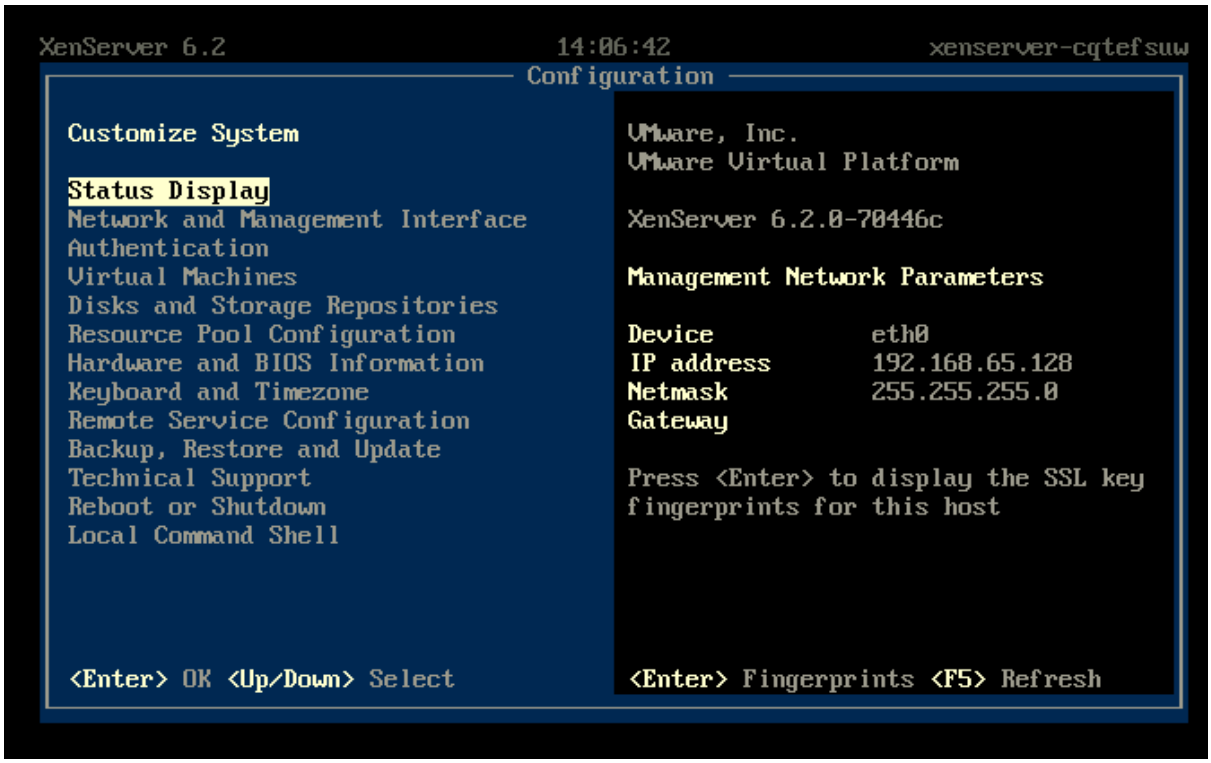
Click on Ok to reboot.

Step 32:

Machine is Rebooted.

Step 33:

Make note of Ip Address provided :- 192.168.65.128



Step 34:

Go to Authentication Tab

Step 35:

Write the Password :- admin123456

Practical-1C

Microsoft Hyper-V:

Hyper-V is Microsoft's hardware virtualization product. It lets you create and run a software version of a computer, called a virtual machine. Each virtual machine acts like a complete computer, running an operating system and programs.

Implement Hypervisor

Step 1:

Start the Virtual Machine, Select File -> Click on New Virtual Machine.

Step 2:

In Virtual Machine wizard. Select Custom (advanced) button and then Click on Next.

Step 3:

Click on Next.

Step 4:

Browser the Windows Server (Hypervisor) image file and then Click on Next.

Step 5:

Give the Windows product key.

Step 6:

Give the Virtual Machine Name as Avinash_Hypervisor. Click on Next.

Step 7:

Click on Next.

Step 8:

Give the total processor as 2. Click on Next.

Step 9:

Give the memory allocation as 2 GB. Click on Next.

Step 10:

Use the NAT. Click on Next.

Step 11:

Select the LSI logic and Click on Next.

Step 12:

Select the SCSI Virtual Disk Type. Click on Next.

Step 13:

Select, Create a new virtual disk. Click on Next.

Step 14:

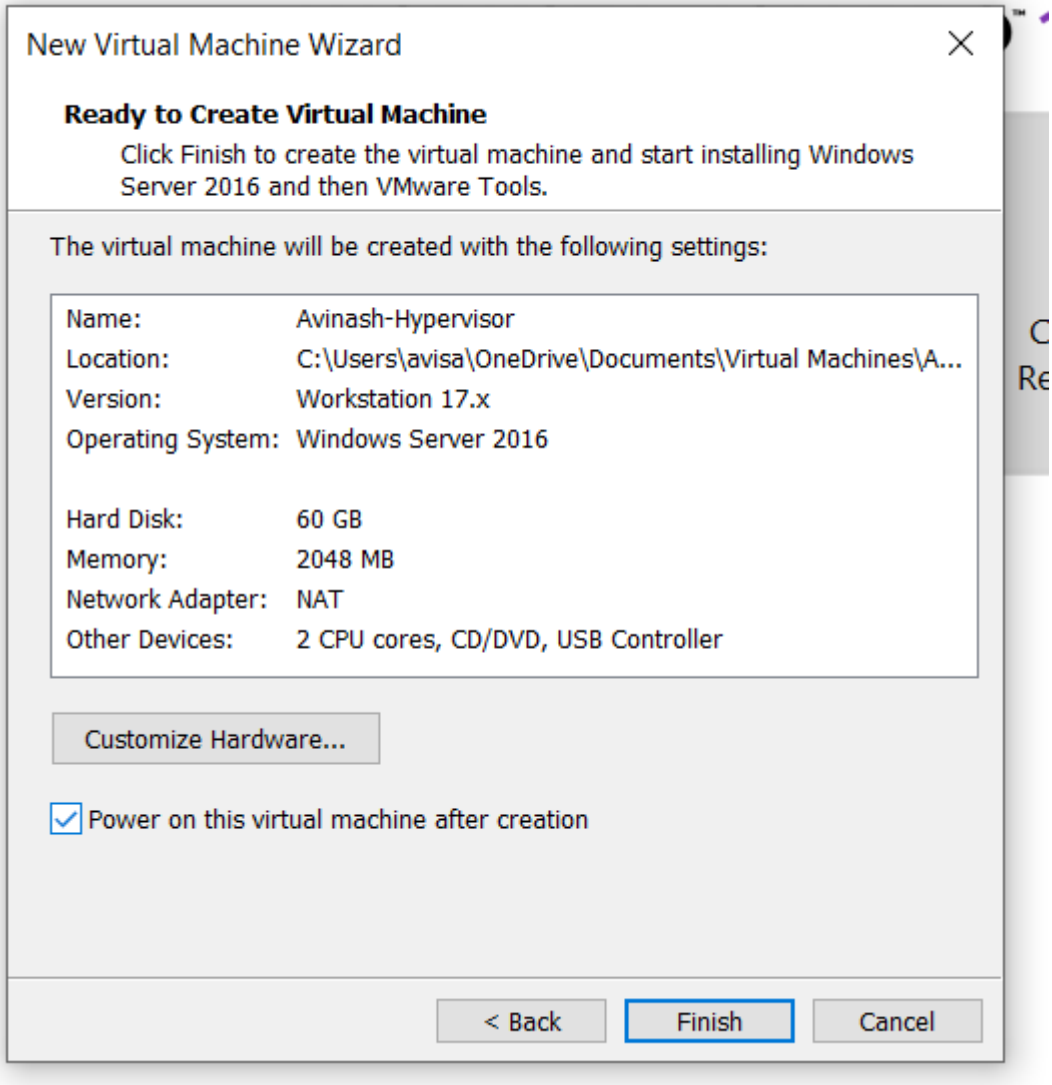
Store Virtual Disk into multiple disks. Click on Next.

Step 15:

Check the name of the virtual machine and then Click on Next.

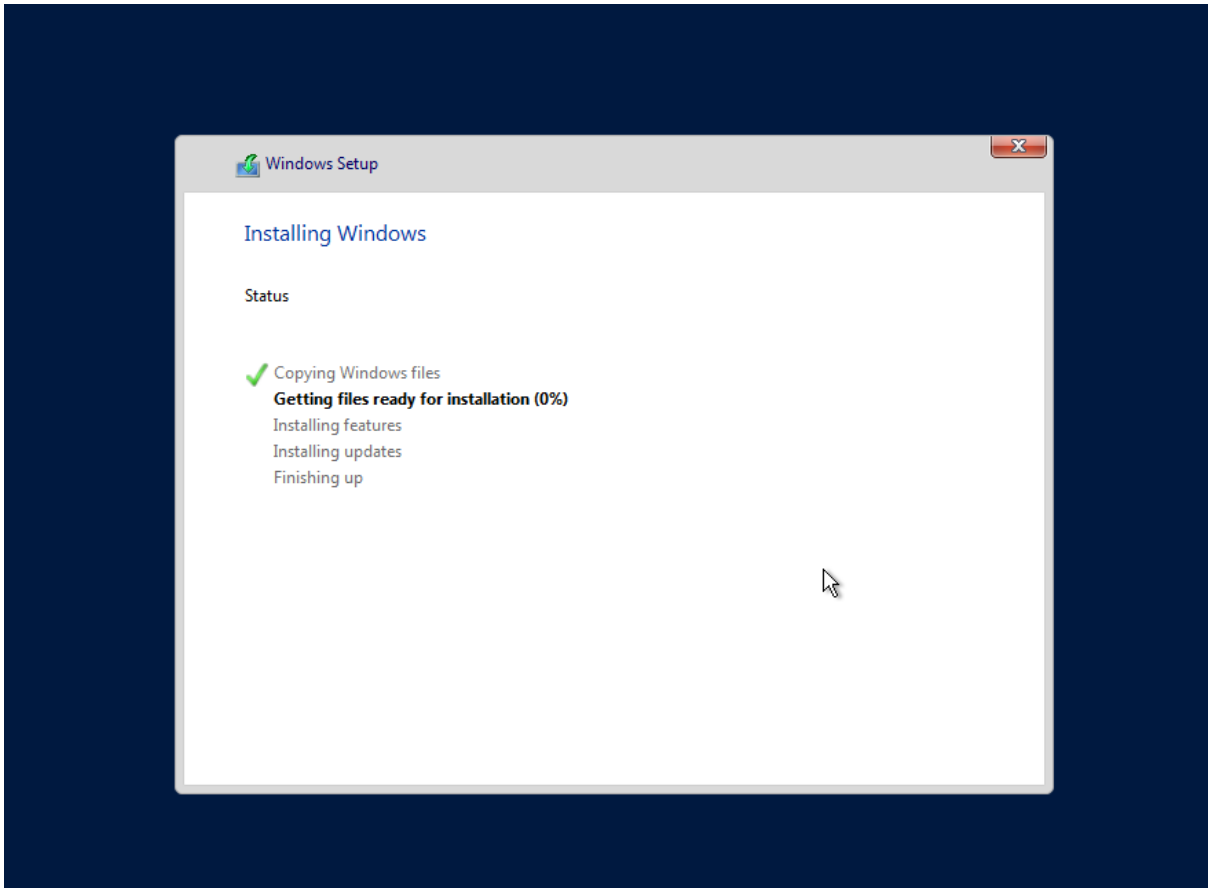
Step 16:

Click on finish.



Step 17:

Avinash_Hypervisor begins to installed.


Windows Setup
Installing Windows
Status
Copying Windows files
Getting files ready for installation (0%)
Installing features
Installing updates
Finishing up

Practical-2A

Aim: Create and manage the inter connectivity of Virtual Machine on VMware Esxi, Citrix Xen, Microsoft Hyper-V

inter connectivity of Virtual Machine on VMware

Step 1:

Select VMware vSphere Client shortcut on Desktop.

Step 2:

Give Ip address :- 192.168.220.128

User name :- root

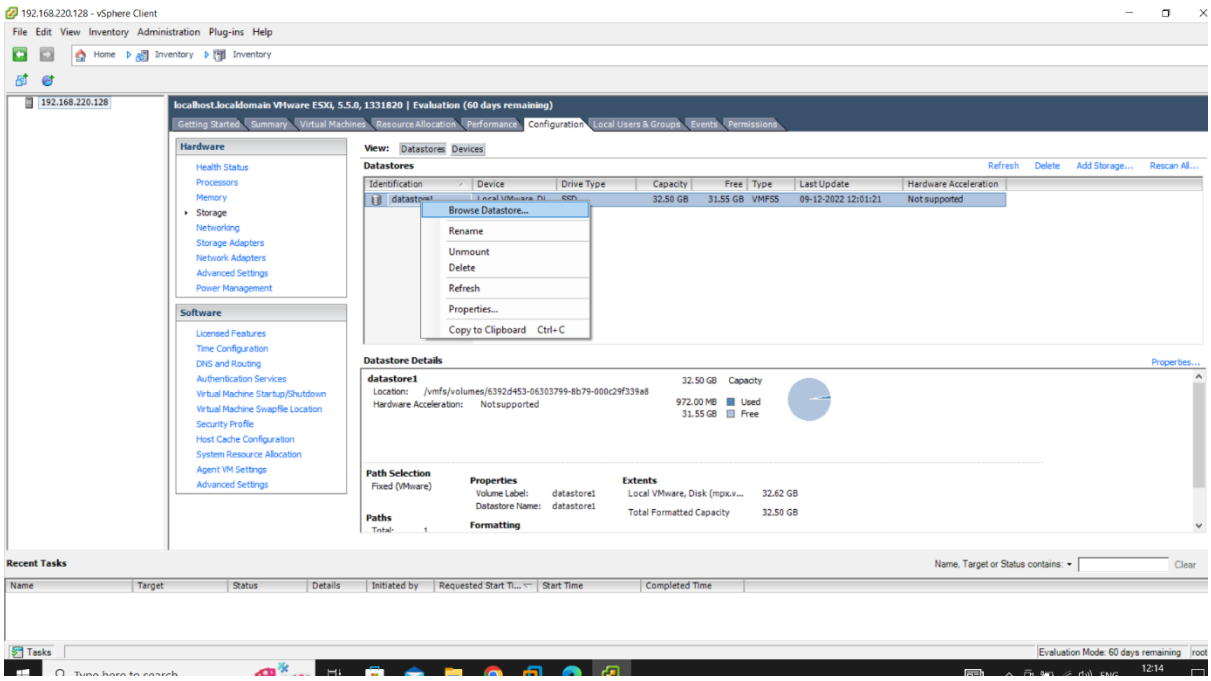
Password :- admin123

Step 3:

Click on Login.

Step 4:

Click on Configuration Tab > Storage > (Right-Click) on datastore1 and Select Browse Datastore.



Step 5:

Click on Upload Icon and Select Upload File

Step 6:

Select Windows 7 x86 Iso and Click on Upload.

Step 7:

You can see the Windows 7 x86 iso in datastore1.

Step 8:

(Right-click) on Server IP > Select New Virtual Machine.

Step 9:

Select Typical

Step 10:

Give name :- Windows 7 Pro Avinash 2022>Next.

Step 11:

Select the datastore1>Next

Step 12:

Select Windows as Guest O.S and select Windows 7 (32-bit).

Step 13:

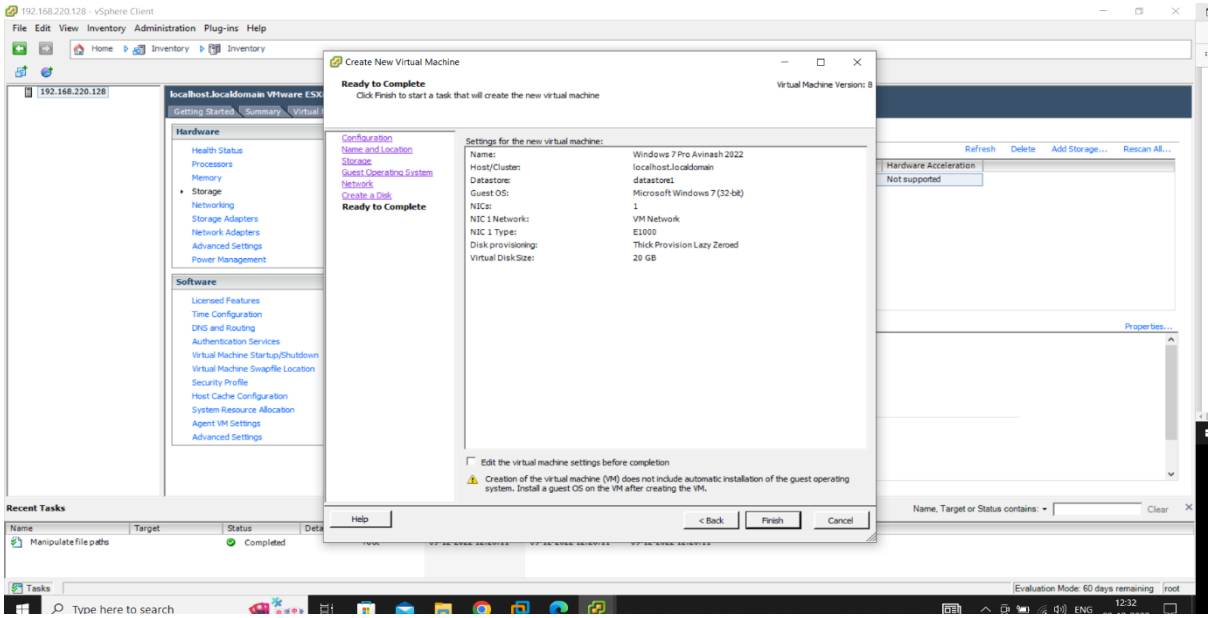
Leave as default.

Step 14:

Give Virtual disk size as 20Gb > Next.

Step 15:

Click on Finish.



Step 16:

Right-Click on Windows 7 Pro under Server Ip and Select Edit Settings.

Step 17:

Go to CD/DVD drive 1 and select Datastore ISO file and Select your Windows 7 iso file

Also check the Connect at power on option > Click on Ok.

Step 18:

Right-Click on Windows 7 Pro under Server Name and Select Open Console

Step 19:

Click on Power On > Windows will start for first time.

Step 20:

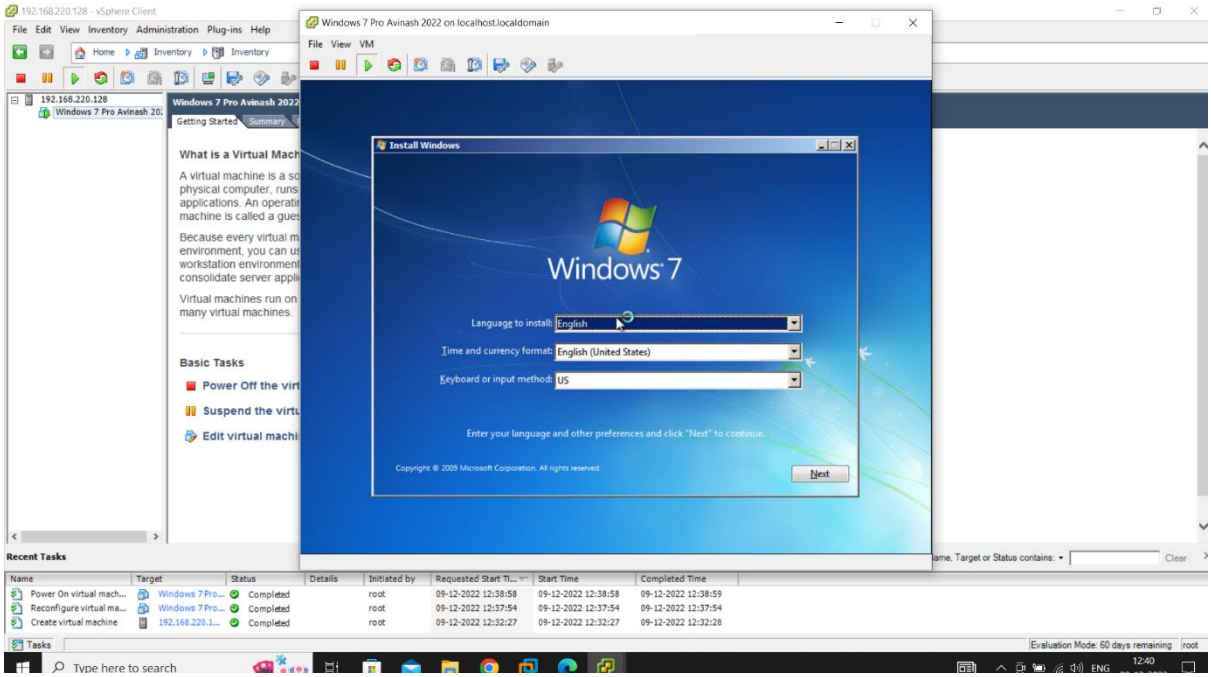
Click on Next Until this screen > Windows in installing.

Step 21:

After install it will Reboot.

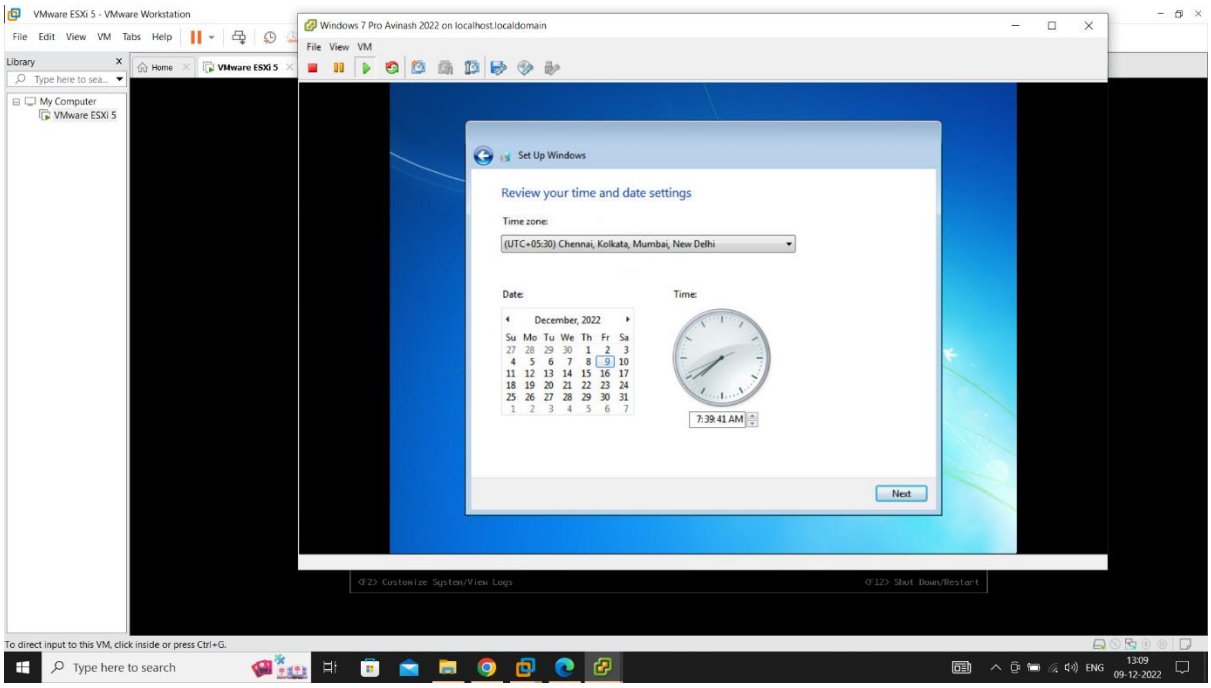
Step 22:

Give name to Machine :-



Step 23:

Select Clock as (UTC +5:30)



Practical-2B

inter connectivity of Virtual Machine on Citrix Xen

Step 1:

Open Citrix Xen Server Management Program

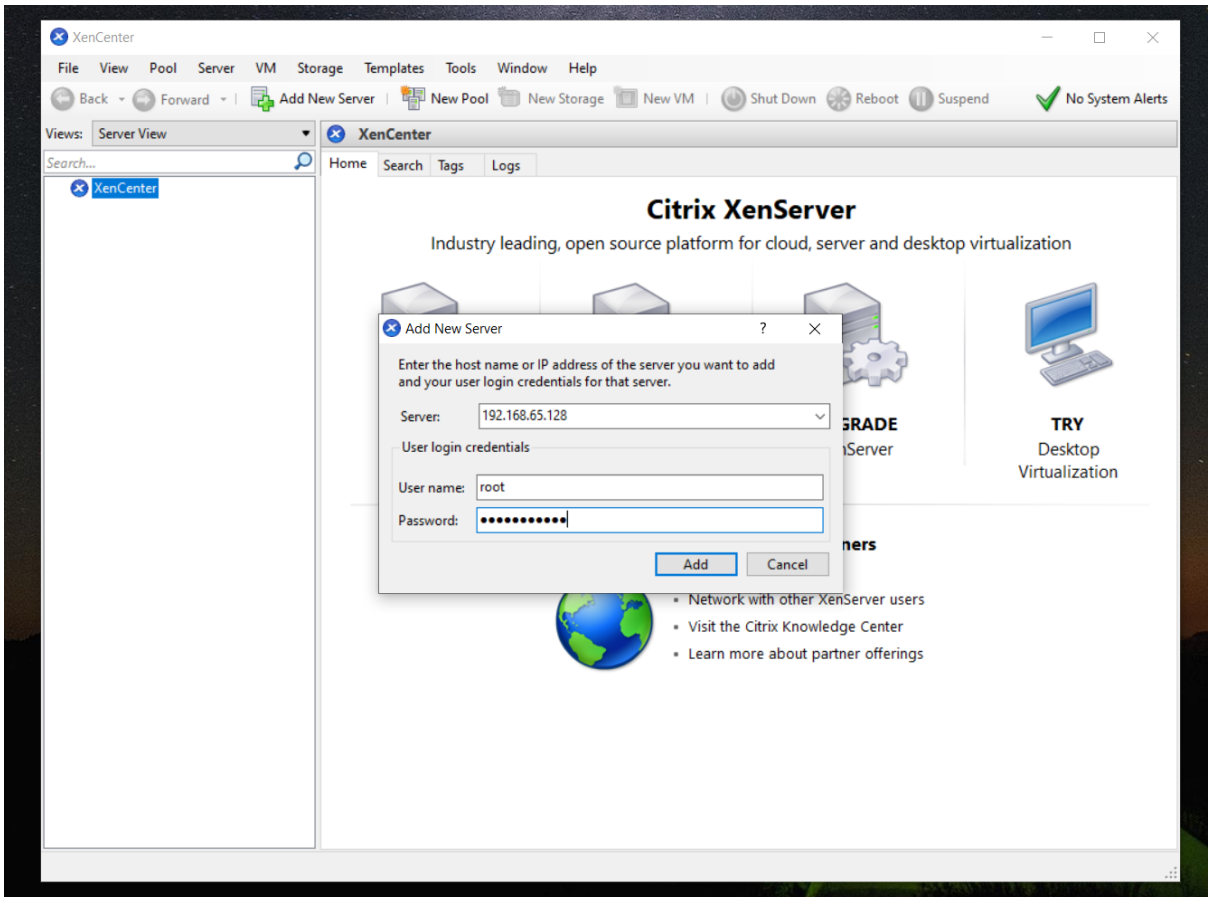
Step 2:

Click on “New Server” and enter the following details:

✓ Server : 192.168.65.128

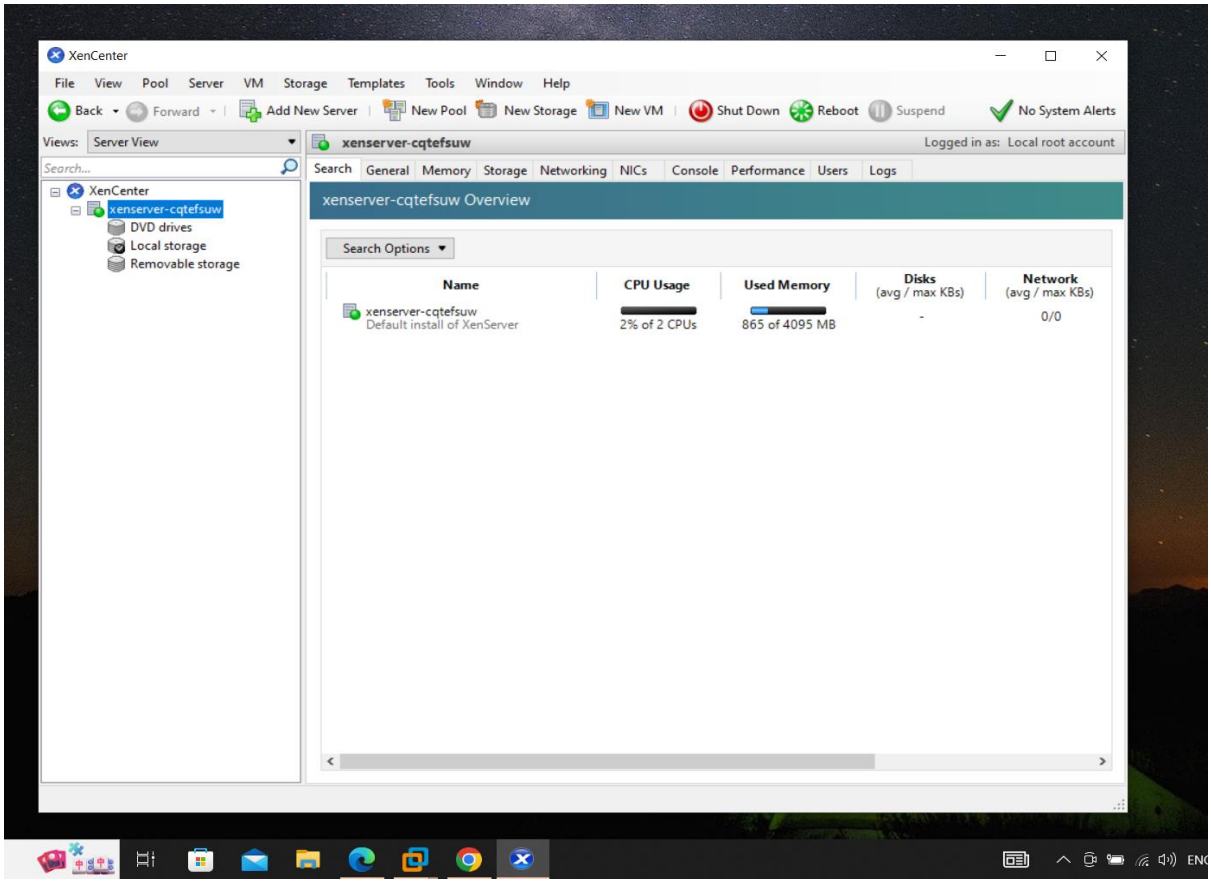
✓ Username :- root

✓ Password :- admin123456



Step 3:

Your Xen Server Machine is Added.



Step 4:

Click on New Storage Button and Select Windows File Sharing (SMB/CIFS).

Step 5:

Leave as default and click on Next.

Step 6:

Share name :- \\192.168.61.1\cloud and click on Finish

Step 7:

Right-Click on Added Server and Select New VM

Step 8:

Select Windows 7 (32-Bit) and click on Next.

Step 9:

Windows 7 (32-Bit) and click on Next

Step 10:

Windows 7 Iso from your shared folder and click on Next.

Step 11:

Click on Next.

Step 12:

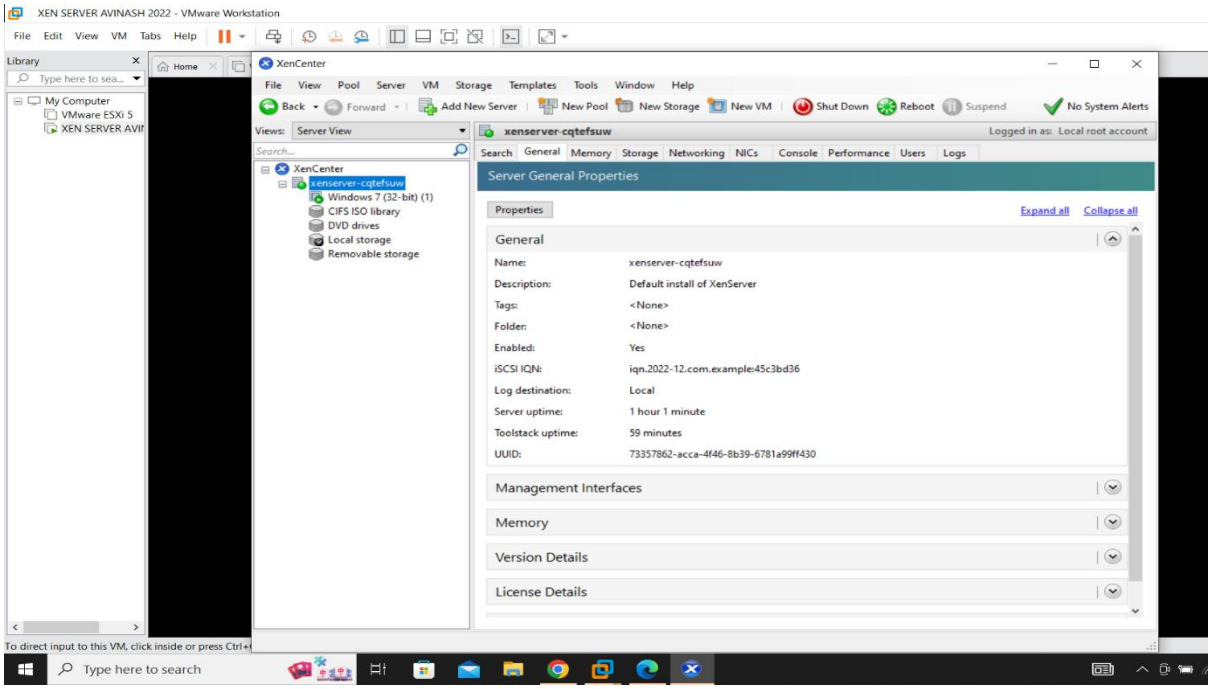
Click on Next.

Step 13:

Click on Next.

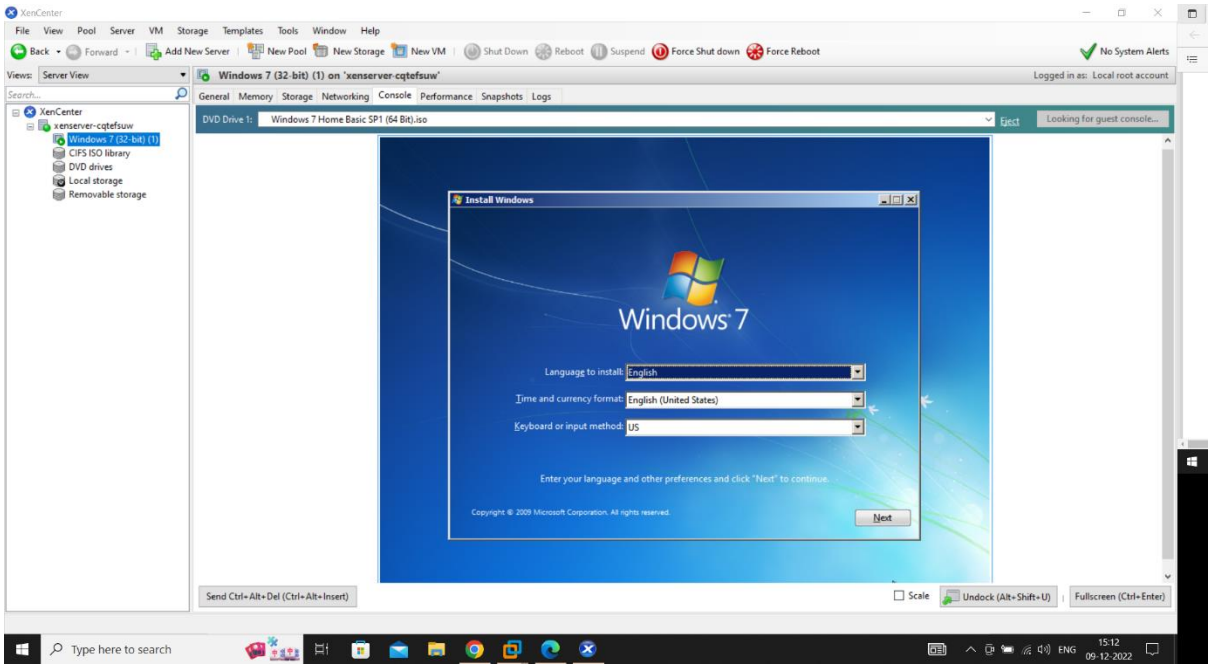
Step 14:

Your VM Configuration. Click on “Create Now”.



Step 15:

Select the Console Tab. Your new VM Is Ready. Complete the installation.



Practical-2C

inter connectivity of Virtual Machine on Microsoft Hyper-V

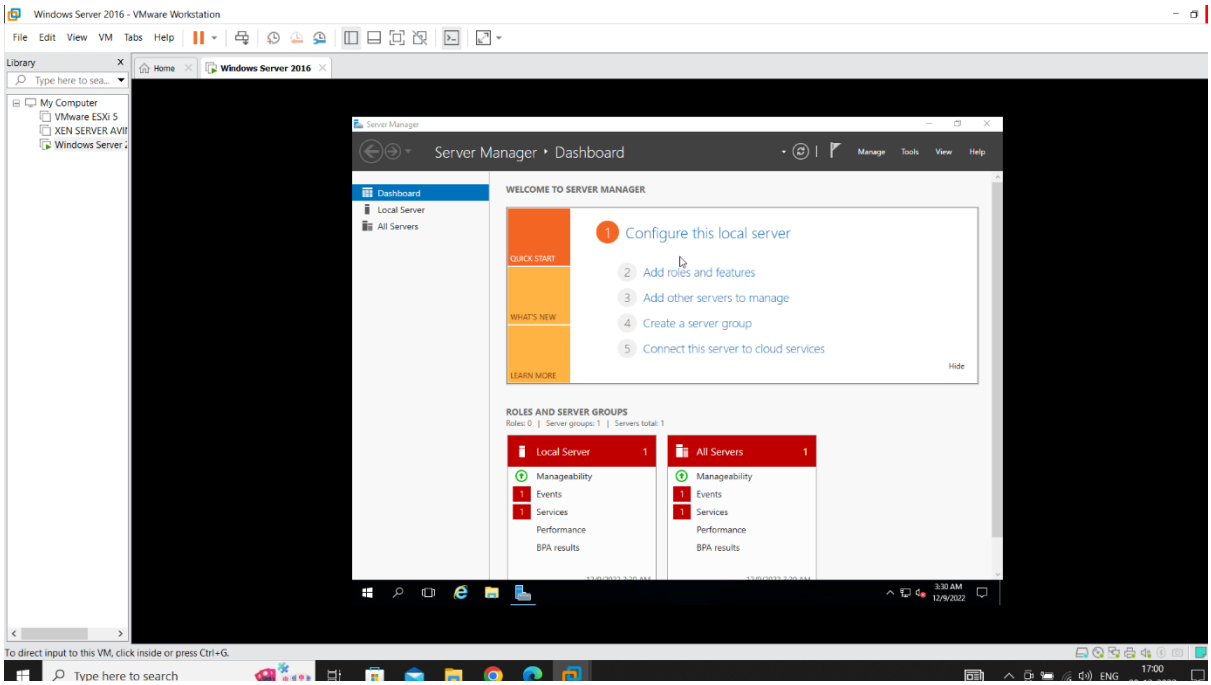
Step 1:

Click on Server Manager.

Step 2:

On Windows Server 2012, install Hyper-V manager features. Open Server Manager and

Click on Add roles and features.



Step 3:

Click on Next

Step 4:

Select Role-based or feature-based installation. Click on Next

Step 5:

Select a server from the server pool.

Step 6:

Click on Hyper-V

Step 7:

Check on Failure Clustering and Group Policy Management. Click on Next.

Step 8:

Click on Next.

Step 9:

Check on Ethernet0 Checkbox. Click on Next.

Step 10:

Check the Checkbox. Click on Next.

Step 11:

Click on Next

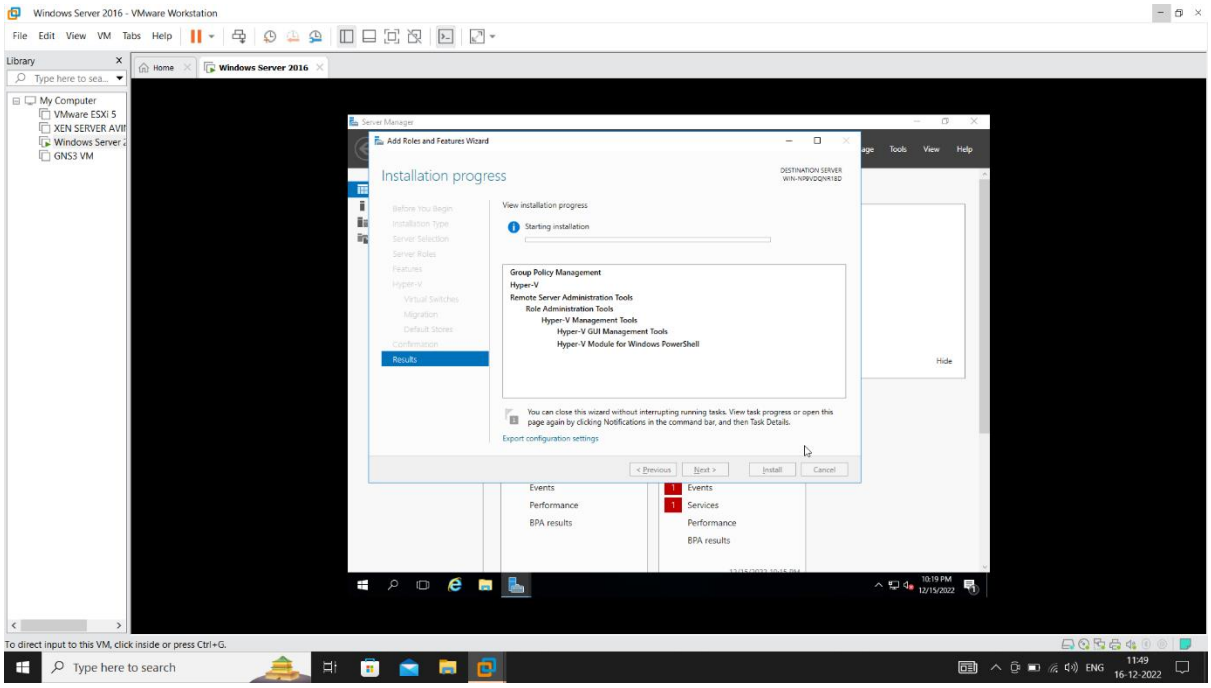
Step 12:

Click on Install.

Step 13:

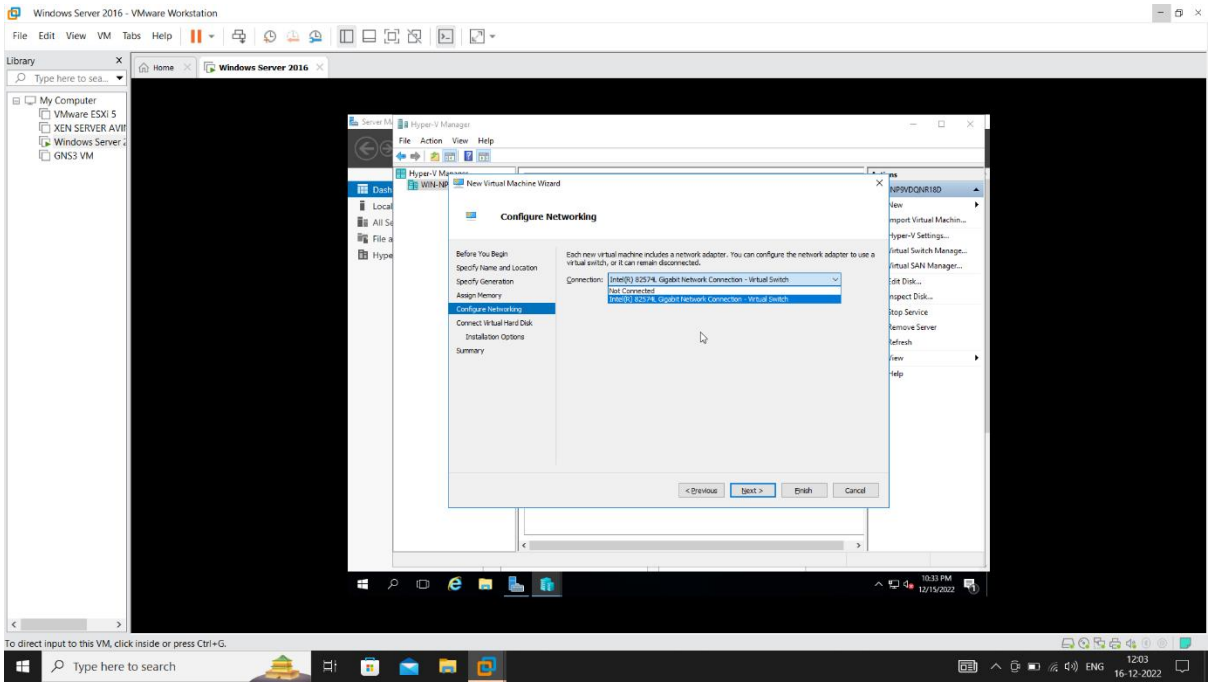
It will show the feature Installation. That show that restarted is pending…

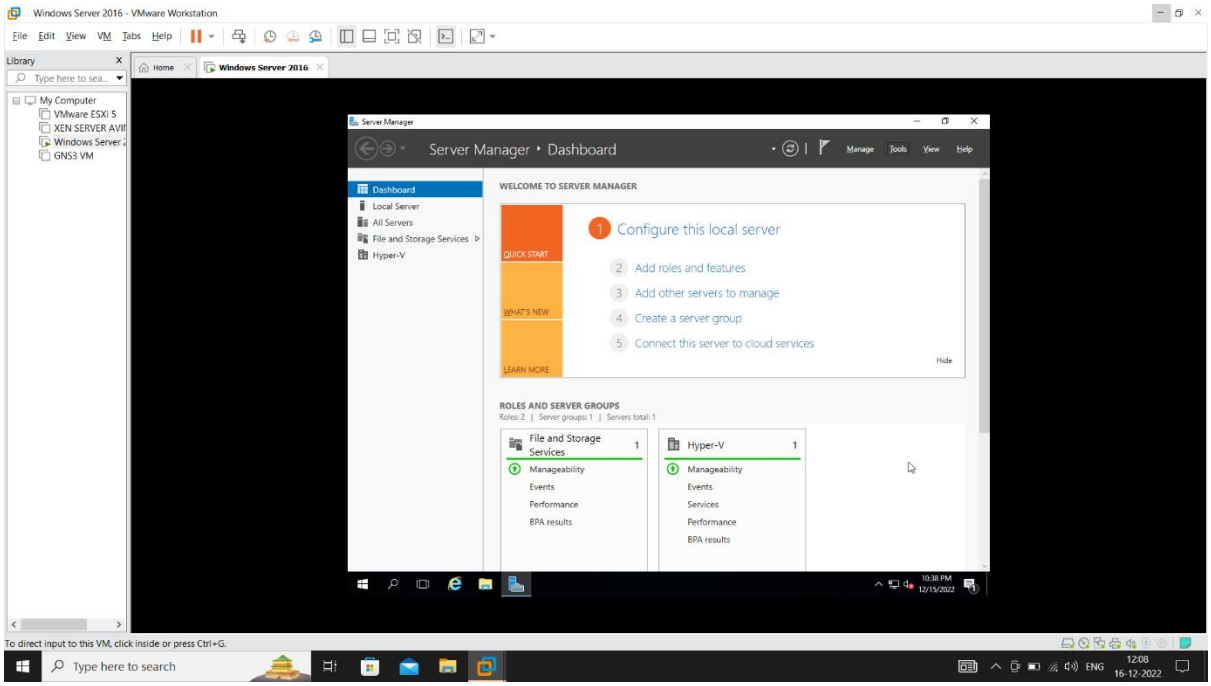
Now restart on VM ware machine and open Server Manager, go to Tools Menu and Click on Hyper-V Manager.



Step 14:

Right Click on Your Machine. i.e WIN-XXXXXXXXXX. And Click on New and Virtual Machine.


Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
VMware ESXi 5
XEN SERVER AVM
Windows Server 2
GNS3 VM
Home
Windows Server 2016
Hyper-V Manager
File Action View Help
New Virtual Machine Wizard
Configure Networking
Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary
Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.
Connection:
Intel(R) 82574L Gigabit Network Connection - Virtual Switch
Not Connected
Intel(R) 82574L Gigabit Network Connection - Virtual Switch
< Previous
Next >
Finish
Cancel
10:33 PM
12/15/2022
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
ENG
12:03
16-12-2022


Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
VMware ESXi 5
XEN SERVER AVM
Windows Server 2
GNS3 VM
Home
Windows Server 2016
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
File and Storage Services
Hyper-V
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
Hyper-V 1
Manageability
Events
Services
Performance
BPA results
10:38 PM
12/15/2022
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
ENG
12:08
16-12-2022

Practical-3

Aim: Configuring EtherChannel's

EtherChannel:

EtherChannel is a port link aggregation technology in which multiple physical port links are grouped into one logical link. It is used to provide high-speed links and redundancy. A maximum of 8 links can be aggregated to form a single logical link.

EtherChannel protocols – To form an EtherChannel, there are 2 protocols, port aggregation Protocol (PAgP) and link aggregation control protocol (LACP).

1. Port Aggregation Protocol (PAgP) –

The Cisco proprietary protocol Port Aggregation Protocol (PAgP) is an EtherChannel technology. It's a type of data/traffic load balancing that involves the logical aggregation of Cisco Ethernet switch ports. A PAgP EtherChannel can merge up to eight physical links into one virtual link. LACP, or Link Aggregation Control Protocol, is an IEEE open standard. These are namely:

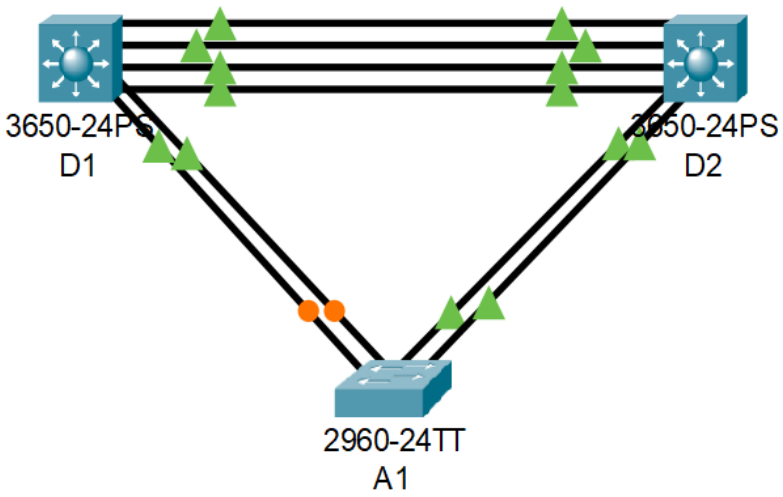
- ON: In this mode, the interface will be a part of EtherChannel but no negotiation takes place.
- Desirable: In this mode, the interface will continuously attempt to convert the other side interface into an EtherChannel.
- Auto: In this mode, the interface will become a part of EtherChannel if and only if it is requested by the opposite interface.
- Off: No EtherChannel configured on the interface.

2. Link Aggregation Control Protocol (LACP) –

Link Aggregation Control Protocol is an IEEE protocol, originally defined in 802.3ad, used to form an EtherChannel. This protocol is almost similar to Cisco PAgP. There are different modes in which you can configure your interface. These are namely:

- ON: In this mode, the interface will be a part of EtherChannel but no negotiation takes place
- Active: In this mode, the interface will continuously attempt to convert the other side interface into an EtherChannel.
- Passive: In this mode, the interface will become a part of EtherChannel if and only if it is requested by the opposite interface.
- Off: No EtherChannel configured on the interface.

Step 1: Design the Topology.



Objectives

Part 1: Build the Network and Explore Dynamic Trunking Protocol

Part 2: Configure Basic Device Settings

Part 3: Configure Static EtherChannel

Part 4: Implement EtherChannel Using PAgP

Part 5: Implement EtherChannel Using LACP

Part 1: Build the Network and Explore Dynamic Trunking Protocol

Step 1: Examine the default port status and manipulate DTP.

For this step, we will focus on the connections between D1 and A1.

If the switches are in their default configuration, this connection between the two switches defaults to be an access port in VLAN 1, which can be seen in the output of show interfaces g1/0/5 switchport and show interfaces f0/1 switchport

Switch D1

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname D1
D1(config)# end
D1#
D1# show interfaces g1/0/5 switchport
Name: Gi1/0/5
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

```
Administrative Native VLAN tagging: disabled
Voice VLAN: none
<output omitted>
```

Switch A1

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname A1
A1(config)# end
A1#
A1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<output omitted>
```

Change the administrative mode of interface f0/1 on A1 to Dynamic Desirable with the interface configuration command switchport mode dynamic desirable. After a few moments, check the interface switchport status and you will see that it is in trunk mode. The output of show interfaces trunk will show the protocol as desirable. The output of show interfaces trunk on D1 will show auto

```
A1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)# interface f0/1
A1(config-if)# switchport mode dynamic desirable
A1(config-if)# end
Jan  7 14:39:33.138: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
A1#
Jan  7 14:39:34.581: %SYS-5-CONFIG_I: Configured from console by
console
Jan  7 14:39:36.158: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
A1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       desirable        802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
```

```
D1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/5     auto             802.1q         trunking      1
<output omitted>
```

DTP datagrams continue to be sent if the port is set statically to trunk mode. However, if the port is set statically to the access mode, both sending and processing DTP datagrams on that port are deactivated. To see this, configure D1 interface g1/0/6 with the switchport mode trunk command. After a few moments, you should once again see that A1 has automatically negotiated a trunk, this time between f0/2 and D1 g1/0/6.

```
D1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)# interface g1/0/6
D1(config-if)# switchport mode trunk
D1(config-if)# end

A1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       desirable        802.1q         trunking      1
Fa0/2       auto             802.1q         trunking      1
```

On A1, shutdown interfaces f0/1 and f0/2 if necessary. Then go to D1 and configure interfaces g1/0/5 and g1/0/6 as trunks with the additional command switchport nonegotiate. A few moments after you re-enable the interfaces at A1, you will see that they do not form trunks with D1

```
D1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)# interface range g1/0/5-6
D1(config-if-range)# switchport mode trunk
D1(config-if-range)# switchport nonegotiate
D1(config-if-range)# end

A1(config-if-range)# no shutdown
A1(config-if-range)# end

A1# show interfaces trunk

A1# show interfaces f0/1 switchport | i Mode
Administrative Mode: dynamic desirable
Operational Mode: static access
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Capture Mode Disabled
```

Part 2: Configure Basic Device Settings

Switch D1

```
hostname D1
banner motd # D1, Implement EtherChannel #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface range g1/0/1-24, g1/1/1-4, g0/0
shutdown
exit
interface range g1/0/1-6
switchport mode trunk
no shutdown
exit
```

Switch D2

```
hostname D2
banner motd # D2, Implement EtherChannel #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface range g1/0/1-24, g1/1/1-4, g0/0
shutdown
exit
interface range g1/0/1-6
switchport mode trunk
no shutdown
exit
```

Switch A1

```
hostname A1
banner motd # A1, Implement EtherChannel#
line con 0
exec-timeout 0 0
logging synchronous
exit
interface range f0/1-24, g0/1-2
shutdown
exit
interface range f0/1-4
switchport mode trunk
no shutdown
exit
```

Part 3: Configure Static EtherChannel

.

Configure the ports interconnecting D2 and A1 as static trunk ports with the **switchport nonenegotiable**

```
D2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)# interface range g1/0/5-6
D2(config-if-range)# switchport nonegotiate
D2(config-if-range)# end
```

Verify the trunks have formed.

```
A1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      1
Fa0/2       on               802.1q         trunking      1
Fa0/3       on               802.1q         trunking      1
Fa0/4       on               802.1q         trunking      1
<output omitted>
```

Add the command **channel-group 1 mode on** to all the trunk interfaces between D2 and A1.

```
D2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)# interface range g1/0/5-6
D2(config-if-range)# channel-group 1 mode on
Creating a port-channel interface Port-channel 1

A1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)# interface range f0/3-4
A1(config-if-range)# channel-group 1 mode on
Creating a port-channel interface Port-channel 1
A1#
Jan   7 15:01:37.641: %SYS-5-CONFIG_I: Configured from console by
console
A1#
Jan  7 15:01:39.562: %LINK-3-UPDOWN: Interface Port-channel1, changed
state to up
A1#
Jan  7 15:01:40.568: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Port-channel1, changed state to up

A1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3      S - Layer2
U - in use      f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
```

```
w - waiting to be aggregated
d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
----
1      Po1(SU)           -        Fa0/3(P)    Fa0/4(P)

A1# show spanning-tree

VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
Address     d8b1.9028.af80
Cost        16
Port        64 (Port-channel1)
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
Address     f078.1647.4580
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
---
Fa0/1               Altn BLK 19        128.1    P2p
Fa0/2               Altn BLK 19        128.2    P2p
Po1                 Root FWD 12        128.64   P2p
```

Make a change to the EtherChannel

With very few exceptions, changes to the EtherChannel configuration (whether a negotiation protocol is used or not) must be made at the port-channel level. Changes you make directly to the member interfaces of a port-channel may create synchronization issues that will cause the group to fail or underperform.

On D2 and A1, create VLAN 999 with the name NATIVE_VLAN.

On D2 and A1, modify interface port-channel 1 so that it uses VLAN 999 as the native VLAN.

```
A1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)# interface port-channel 1
A1(config-if)# switchport trunk native vlan 999
A1(config-if)# end
```

Verify the change has been applied by examining the output of **show interfaces trunk**.

```
A1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
```

```
Fa0/1       on              802.1q         trunking      1
Fa0/2       on              802.1q         trunking      1
Po1         on              802.1q         trunking      999
<output omitted>
```

Part 4: Implement EtherChannel Using PAgP

Step 1: Configure and verify an EtherChannel using PAgP between D1 and A1

Add the command **channel-group 2 mode desirable non-silent** to all the trunk interfaces between D1 and A1.

```
A1(config)# interface range f0/1-2
A1(config-if-range)# channel-group 2 mode desirable non-silent
Creating a port-channel interface Port-channel 2

A1(config-if-range)# end
A1#
Jan  7 15:10:12.483: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Port-channel2, changed state to up
Jan  7 15:10:14.253: %LINK-3-UPDOWN: Interface Port-channel2, changed
state to up
```

Verify the EtherChannel has formed by examining the output of the **show etherchannel summary** command.

```
A1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3      S - Layer2
U - in use      f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
----
1      Po1(SU)          -        Fa0/3(P)    Fa0/4(P)
2      Po2(SU)         PAgP      Fa0/1(P)    Fa0/2(P)
```

Make a change to the EtherChannel

On D1 and A1, modify interface port-channel 2 so that it uses VLAN 999 as the native VLAN.

```
D1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)# interface port-channel 2
D1(config-if)# switchport trunk native vlan 999
D1(config-if)# end
```

Verify the change has been applied by examining the output of **show interfaces trunk | i Port|Po2**.

```
D1# show interfaces trunk | i Port|Po2
Port        Mode             Encapsulation  Status        Native vlan
Po2         on               802.1q         trunking      999
<output omitted>
```

Part 5: Implement EtherChannel using LACP

Step 1: Configure and verify an EtherChannel using LACP between D1 and D2.

Add the command **channel-group 3 mode active** to all the trunk interfaces between D1 and D2.

```
D2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)# interface range g1/0/1-4
D2(config-if-range)# channel-group 3 mode active
Creating a port-channel interface Port-channel 3

D2# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3      S - Layer2
U - in use      f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

A - formed by Auto LAG


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
----
1      Po1(SU)          -          Gi1/0/5(P)    Gi1/0/6(P)
3      Po3(SU)          LACP       Gi1/0/1(P)    Gi1/0/2(P)    Gi1/0/3(P)
Gi1/0/4(P)
```

Make a change to the EtherChannel

On D1 and D2, modify interface port-channel 3 so that it uses VLAN 999 as the native VLAN.

```
D1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)# interface port-channel 3
D1(config-if)# switchport trunk native vlan 999
D1(config-if)# exit
D1(config)# end
```

Verify the change has been applied by examining the output of **show interfaces trunk | i Port|Po3**

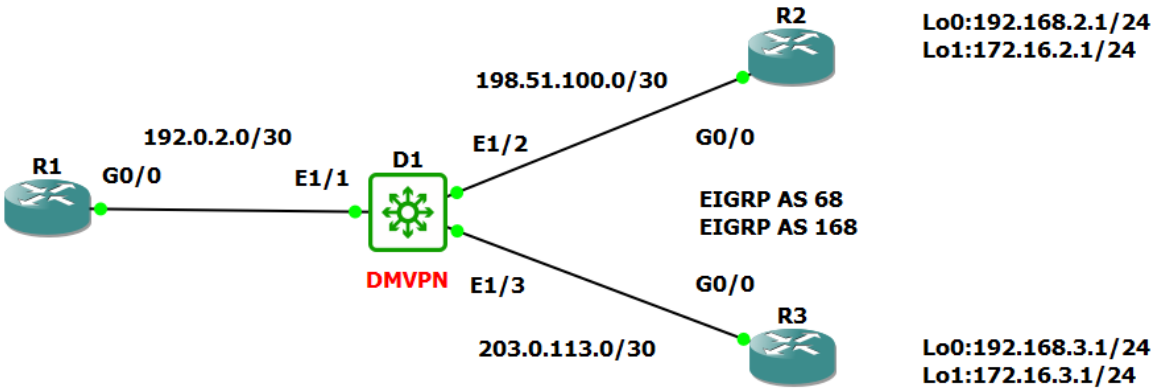
```
D1# show interfaces trunk | i Port|Po3
Port        Mode             Encapsulation  Status        Native vlan
Po3         on               802.1q         trunking      999
<output omitted>
```

Practical-4A

Aim: Implement a DMVPN Phase 1 Hub-to-Spoke Topology

Dynamic Multipoint Virtual Private Network (DMVPN) is a solution which enables the data to transfer from one site to another, without having the verification process of traffic. That use to be held at main VPN server of the concerned organization. This process helps the data to move from one end to another in the establishment of secured network. It is integrated with a unique software which construct IPsec and GRE VPNs in an unchallenged way.

Topology:



Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure and Verify DMVPN Phase 1

Part 3: Configure EIGRP Routing for the Tunnel Networks

Part 1: Build the Network and Configure Basic Device Settings

```
Hub Router R1
hostname R1
no ip domain lookup
banner motd # R1, Implement a DMVPN hub #
line con 0
exec-timeout 0 0
logging synchronous
exit
line vty 0 4
privilege level 15
password cisco123
exec-timeout 0 0
logging synchronous
login
exit
```

```
ip route 0.0.0.0 0.0.0.0 g0/0/1
interface g0/0/1
ip address 192.0.2.1 255.255.255.252
no shutdown
exit
end

Spoke Router R2
hostname R2
no ip domain lookup
banner motd # R2, Implement DMVPN Spoke 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
line vty 0 4
privilege level 15
password cisco123
exec-timeout 0 0
logging synchronous
login
exit
ip route 0.0.0.0 0.0.0.0 g0/0/1
interface g0/0/1
ip address 198.51.100.2 255.255.255.252
no shutdown
exit
interface loopback 0
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
interface loopback 1
ip address 172.16.2.1 255.255.255.0
no shutdown
exit
end

Spoke Router R3
hostname R3
no ip domain lookup
```

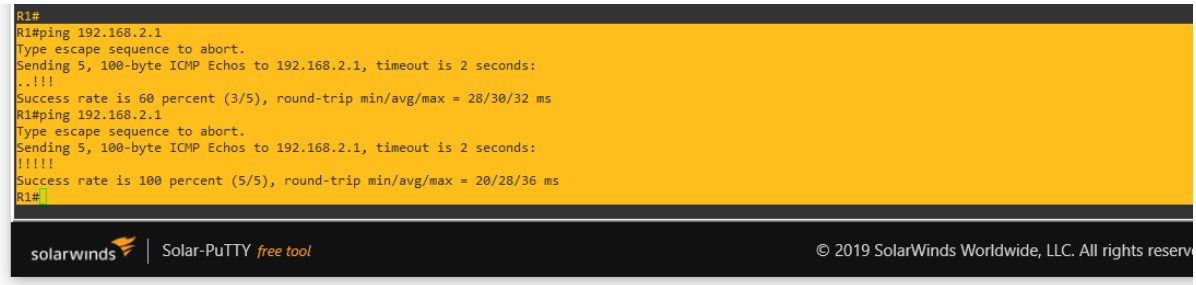
```
banner motd # R3, Implement DMVPN Spoke 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
line vty 0 4
privilege level 15
password cisco123
exec-timeout 0 0
logging synchronous
exit
ip route 0.0.0.0 0.0.0.0 g0/0/1
interface g0/0/1
ip address 203.0.113.2 255.255.255.252
no shutdown
exit
interface loopback 0
ip address 192.168.3.1 255.255.255.0
no shutdown
exit
interface loopback 1
ip address 172.16.3.1 255.255.255.0
no shutdown
exit
end
```

```
DMVPN Layer 3 Switch
hostname DMVPN
no ip domain lookup
ip routing
banner motd # DMVPN, DMVPN cloud switch #
line con 0
exec-timeout 0 0
logging synchronous
exit
line vty 0 4
privilege level 15
password cisco123
exec-timeout 0 0
logging synchronous
```

```
login
exit
interface g1/0/11
no switchport
ip address 192.0.2.2 255.255.255.252
no shutdown
exit
interface g1/0/12
no switchport
ip address 198.51.100.1 255.255.255.252
no shutdown
exit
interface g1/0/13
no switchport
ip address 203.0.113.1 255.255.255.252
no shutdown
exit
ip route 192.168.2.0 255.255.255.0 g1/0/12
ip route 172.16.2.0 255.255.255.0 g1/0/12
ip route 192.168.3.0 255.255.255.0 g1/0/13
ip route 172.16.3.0 255.255.255.0 g1/0/13
end
```

Part 2: Configure and Verify DMVPN Phase 1

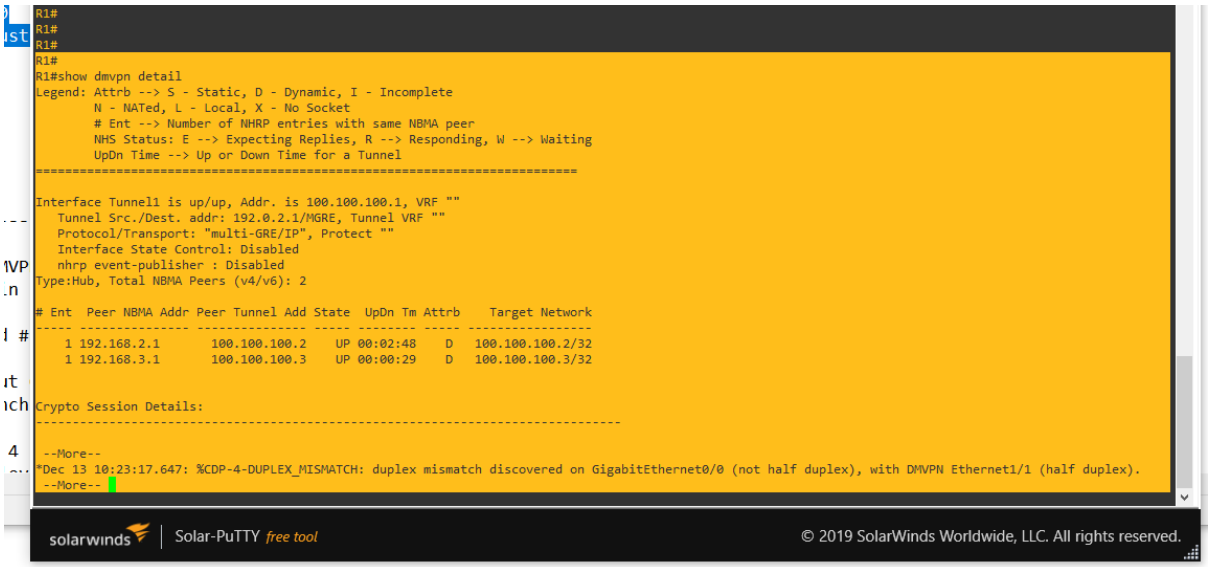
Step 1: Verify connectivity in the underlay network.



Step 2: Configure the tunnel interface on the hub router.

```
R1(config)# interface tunnel 1
R1(config-if)# tunnel mode gre multipoint
R1(config-if)# tunnel source GigabitEthernet0/0/1
R1(config-if)# tunnel key 999
R1(config-if)# ip address 100.100.100.1 255.255.255.248
R1(config-if)# ip nhrp network-id 1
R1(config-if)# ip nhrp authentication NHRPauth
R1(config-if)# ip nhrp map multicast dynamic
```

```
R1(config-if)# bandwidth 4000
R1(config-if)# ip mtu 1400
R1(config-if)# ip tcp adjust-mss 1360
R1(config-if)# end
```

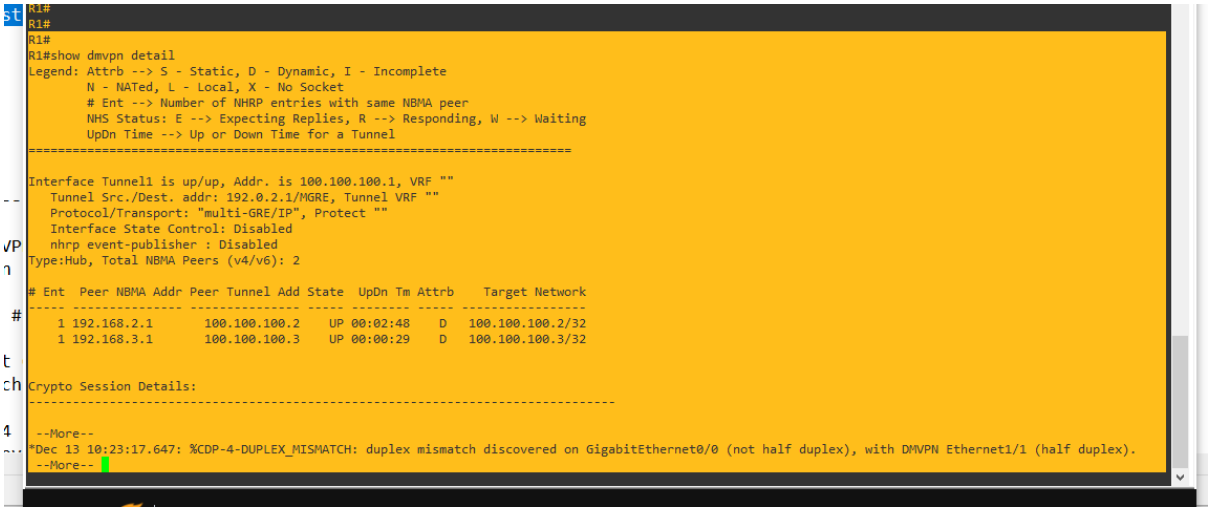


Step 3: Configure the R2 and R3 spoke router tunnel interfaces.

```
R2(config)# interface tunnel 1
R2(config-if)# tunnel mode gre ip
R2(config-if)# tunnel source loopback 0
R2(config-if)# tunnel destination 192.0.2.1
R2(config-if)# tunnel key 999
R2(config-if)# ip address 100.100.100.2 255.255.255.248
R2(config-if)# ip nhrp network-id 1
R2(config-if)# ip nhrp authentication NHRPauth
R2(config-if)# ip nhrp nhs 100.100.100.1
R2(config-if)# ip nhrp map multicast 192.0.2.1
R2(config-if)# ip nhrp map 100.100.100.1 192.0.2.1
R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp adjust-mss 1360
```

```
R3(config)# interface tunnel 1
R3(config-if)# tunnel mode gre ip
R3(config-if)# tunnel source loopback 0
R3(config-if)# tunnel destination 192.0.2.1
R3(config-if)# tunnel key 999
R3(config-if)# ip address 100.100.100.3 255.255.255.248
R3(config-if)# ip nhrp network-id 1
```

```
R3(config-if)# ip nhrp authentication NHRPauth
R3(config-if)# ip nhrp nhs 100.100.100.1
R3(config-if)# ip nhrp map multicast 192.0.2.1
R3(config-if)# ip nhrp map 100.100.100.1 192.0.2.1
R3(config-if)# ip mtu 1400
R3(config-if)# ip tcp adjust-mss 1360
```



Part 3: Configure EIGRP Routing for the Tunnel Networks

Step 1: Configure dynamic routing for the overlay network.

R1, R2, and R3

```
no ip route 0.0.0.0 0.0.0.0 g0/0/1
```

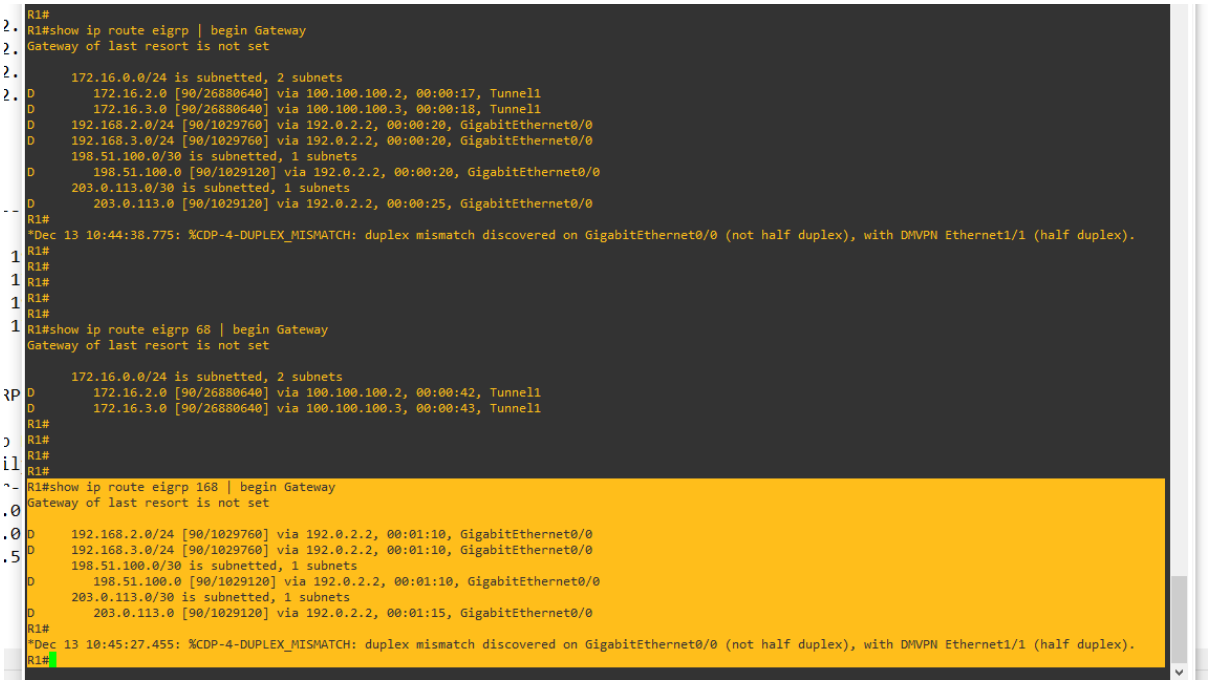
DMVPN switch

```
no ip route 192.168.2.0 255.255.255.0 g1/0/12
no ip route 172.16.2.0 255.255.255.0 g1/0/12
no ip route 192.168.3.0 255.255.255.0 g1/0/13
no ip route 172.16.3.0 255.255.255.0 g1/0/13

R1(config)# router eigrp DMVPN_TUNNEL_NET
R1(config-router)# address-family ipv4 unicast autonomous-system 68
R1(config-router-af)# eigrp router-id 1.1.1.1
R1(config-router-af)# network 100.100.100.0 255.255.255.248
R1(config-router-af)# af-interface tunnel 1
R1(config-router-af-interface)# no split-horizon

R2(config)# router eigrp DMVPN_TUNNEL_NET
R2(config-router)# address-family ipv4 unicast autonomous-system 68
R2(config-router-af)# eigrp router-id 2.2.2.2
```

```
R2(config-router-af)# network 100.100.100.0 255.255.255.248
R2(config-router-af)# network 172.16.2.0 255.255.255.0
R2(config-router-af)# eigrp stub connected

R3(config)# router eigrp DMVPN_TUNNEL_NET
R3(config-router)# address-family ipv4 unicast autonomous-system 68
R3(config-router-af)# eigrp router-id 3.3.3.3
R3(config-router-af)# network 100.100.100.0 255.255.255.248
R3(config-router-af)# network 172.16.3.0 255.255.255.0
R3(config-router-af)# eigrp stub connected
```

Step 2: Configure dynamic routing for the underlay network.

```
R1(config)# router eigrp DMVPN_TRANS_NET
R1(config-router)# address-family ipv4 unicast autonomous-system 168
R1(config-router-af)# eigrp router-id 10.1.1.1
R1(config-router-af)# network 192.0.2.0 255.255.255.252

R2(config)# router eigrp DMVPN_TRANS_NET
R2(config-router)# address-family ipv4 unicast autonomous-system 168
R2(config-router-af)# eigrp router-id 20.2.2.2
R2(config-router-af)# network 198.51.100.0 255.255.255.252
R1(config-router-af)# network 192.168.2.0 255.255.255.0
R2(config-router-af)# eigrp stub connected

R3(config)# router eigrp DMVPN_TRANS_NET
R3(config-router)# address-family ipv4 unicast autonomous-system 168
R3(config-router-af)# eigrp router-id 30.3.3.3
R3(config-router-af)# network 203.0.113.0 255.255.255.252
R3(config-router-af)# network 192.168.3.0 255.255.255.0
R3(config-router-af)# eigrp stub connected

DMVPN(config)# router eigrp DMVPN_TRANS_NET
DMVPN(config-router)# address-family ipv4 unicast autonomous-system 168
DMVPN(config-router-af)# eigrp router-id 40.4.4.4
DMVPN(config-router-af)# network 203.0.113.0 255.255.255.252
DMVPN(config-router-af)# network 192.0.2.0 255.255.255.252
DMVPN(config-router-af)# network 198.51.100.0 255.255.255.252
```

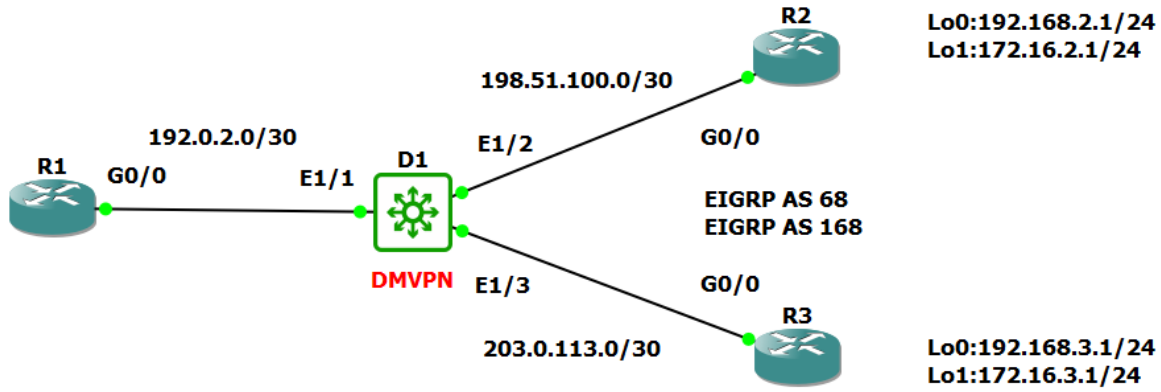


Step 3: Verify DMVPN Phase 1 operation.

Practical-4B

Aim: Implement a DMVPN Phase 3 Spoke-to-Spoke Topology

Topology:



Objectives:

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure DMVPN Phase 3

Part 3: Verify DMVPN Phase 3

R1 hub router

```
hostname R1
no ip domain lookup
banner motd # R1, Implement DMVPN Hub #
line con 0
exec-timeout 0 0
logging synchronous
exit
line vty 0 4
privilege level 15
password cisco123
exec-timeout 0 0
logging synchronous
login
exit
interface g0/0/1
ip address 192.0.2.1 255.255.255.252
no shutdown
exit
```

```
interface tunnel 1
tunnel mode gre multipoint
tunnel source g0/0/1
tunnel key 999
ip address 100.100.100.1 255.255.255.248
ip nhrp network-id 1
ip nhrp authentication NHRPauth
ip nhrp map multicast dynamic
bandwidth 4000
ip mtu 1400
ip tcp adjust-mss 1360
exit
router eigrp DMVPN_TUNNEL_NET
address-family ipv4 unicast autonomous-system 68
eigrp router-id 1.1.1.1
network 100.100.100.0 255.255.255.248
af-interface tunnel 1
no split-horizon
router eigrp DMVPN_TRANS_NET
address-family ipv4 unicast autonomous-system 168
eigrp router-id 10.1.1.1
network 192.0.2.0 255.255.255.252
end
R2 spoke router 1
hostname R2
no ip domain lookup
banner motd # R2, Implement DMVPN Spoke 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
line vty 0 4
privilege level 15
password cisco123
```

```
exec-timeout 0 0
logging synchronous
login
exit
interface g0/0/1
ip address 198.51.100.2 255.255.255.252
no shutdown
exit
interface loopback 0
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
interface loopback 1
ip address 172.16.2.1 255.255.255.0
no shutdown
exit
interface tunnel 1
tunnel mode gre ip
tunnel source loopback 0
tunnel destination 192.0.2.1
tunnel key 999
ip address 100.100.100.2 255.255.255.248
ip nhrp network-id 1
ip nhrp authentication NHRPauth
ip nhrp nhs 100.100.100.1
ip nhrp map multicast 192.0.2.1
ip nhrp map 100.100.100.1 192.0.2.1
ip mtu 1400
ip tcp adjust-mss 1360
router eigrp DMVPN_TUNNEL_NET
address-family ipv4 unicast autonomous-system 68
eigrp router-id 2.2.2.2
network 100.100.100.0 255.255.255.248
network 172.16.2.0 255.255.255.0
```

```
eigrp stub connected
router eigrp DMVPN_TRANS_NET
address-family ipv4 unicast autonomous-system 168
eigrp router-id 20.2.2.2
network 198.51.100.0 255.255.255.252
network 192.168.2.0 255.255.255.0
end
Router R3 spoke 2
hostname R3
no ip domain lookup
banner motd # R3, Implement DMVPN Spoke 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
line vty 0 4
privilege level 15
password cisco123
exec-timeout 0 0
logging synchronous
login
exit
interface g0/0/1
ip address 203.0.113.2 255.255.255.252
no shutdown
exit
interface loopback 0
ip address 192.168.3.1 255.255.255.0
no shutdown
exit
interface loopback 1
ip address 172.16.3.1 255.255.255.0
no shutdown
exit
```

```
interface tunnel 1
tunnel mode gre ip
tunnel source loopback 0
tunnel destination 192.0.2.1
tunnel key 999
ip address 100.100.100.3 255.255.255.248
ip nhrp network-id 1
ip nhrp authentication NHRPauth
ip nhrp nhs 100.100.100.1
ip nhrp map multicast 192.0.2.1
ip nhrp map 100.100.100.1 192.0.2.1
ip mtu 1400
ip tcp adjust-mss 1360
router eigrp DMVPN_TUNNEL_NET
address-family ipv4 unicast autonomous-system 68
eigrp router-id 3.3.3.3
network 100.100.100.0 255.255.255.248
network 172.16.3.0 255.255.255.0
eigrp stub connected
router eigrp DMVPN_TRANS_NET
address-family ipv4 unicast autonomous-system 168
eigrp router-id 30.3.3.3
network 203.0.113.0 255.255.255.252
network 192.168.3.0 255.255.255.0
eigrp stub connected
end
Layer 3 Switch DMVPN
hostname DMVPN
no ip domain lookup
ip routing
banner motd # DMVPN, DMVPN cloud switch #
line con 0
exec-timeout 0 0
logging synchronous
```

```
exit
line vty 0 4
privilege level 15
password cisco123
exec-timeout 0 0
logging synchronous
login
interface g1/0/11
no switchport
ip address 192.0.2.2 255.255.255.252
no shutdown
exit
interface g1/0/12
no switchport
ip address 198.51.100.1 255.255.255.252
no shutdown
exit
interface g1/0/13
no switchport
ip address 203.0.113.1 255.255.255.252
no shutdown
exit
router eigrp DMVPN_TRANS_NET
address-family ipv4 unicast autonomous-system 168
eigrp router-id 40.4.4.4
network 192.0.2.0 255.255.255.252
network 198.51.100.0 255.255.255.252
network 203.0.113.0 255.255.255.252
end
```

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure DMVPN Phase 3

```
R2(config)# interface tunnel 1

R2(config-if)# tunnel mode gre multipoint

R2(config-if)# no tunnel destination

R2(config-if)# tunnel mode gre multipoint

R2(config)# interface tunnel 1

R2(config-if)# ip nhrp shortcut

R3# show interface tunnel 1 | include Tunnel protocol


R3(config)# interface tunnel 1

R3(config-if)# ip nhrp shortcut

R1(config)# interface tunnel 1

R1(config-if)# ip nhrp redirect
```

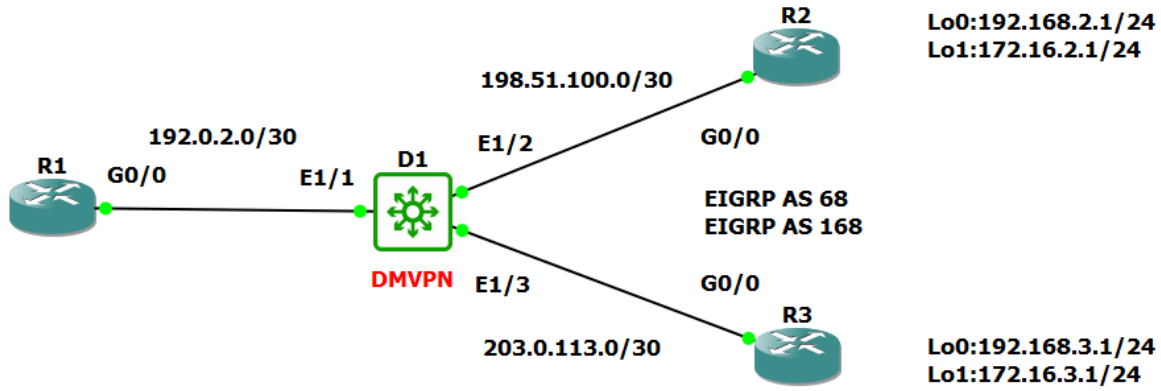
Part 3: Verify DMVPN Phase 3

Verify the DMVPN

Practical-4C

Aim: Configure Secure DMVPN Tunnels

Topology:



Objectives:

Part 1: Build the Network and Verify DMVPN Phase 3 Operation

Part 2: Secure DMVPN Phase 3 Tunnels

R1 hub router

```
hostname R1
no ip domain lookup
banner motd # R1, Implement DMVPN Hub #
line con 0
exec-timeout 0 0
logging synchronous
exit
line vty 0 4
privilege level 15
password cisco123
exec-timeout 0 0
logging synchronous
login
exit
interface g0/0/1
ip address 192.0.2.1 255.255.255.252
```

```
no shutdown
exit
interface tunnel 1
tunnel mode gre multipoint
tunnel source g0/0/1
tunnel key 999
ip address 100.100.100.1 255.255.255.248
ip nhrp network-id 1
ip nhrp authentication NHRPauth
ip nhrp map multicast dynamic
ip nhrp redirect
bandwidth 4000
ip mtu 1400
ip tcp adjust-mss 1360
exit
router eigrp DMVPN_TUNNEL_NET
address-family ipv4 unicast autonomous-system 68
eigrp router-id 1.1.1.1
network 100.100.100.0 255.255.255.248
af-interface tunnel 1
no split-horizon
router eigrp DMVPN_TRANS_NET
address-family ipv4 unicast autonomous-system 168
eigrp router-id 10.1.1.1
network 192.0.2.0 255.255.255.252
end
R2 spoke router 1
hostname R2
no ip domain lookup
banner motd # R2, Implement DMVPN Spoke 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

```
line vty 0 4
privilege level 15
password cisco123
exec-timeout 0 0
logging synchronous
login
exit
interface g0/0/1
ip address 198.51.100.2 255.255.255.252
no shutdown
exit
interface loopback 0
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
ip address 172.16.2.1 255.255.255.0
no shutdown
exit
interface tunnel 1
tunnel mode gre multipoint
tunnel source loopback 0
no tunnel destination
tunnel key 999
ip address 100.100.100.2 255.255.255.248
ip nhrp network-id 1
ip nhrp authentication NHRPauth
ip nhrp nhs 100.100.100.1
ip nhrp map multicast 192.0.2.1
ip nhrp map 100.100.100.1 192.0.2.1
ip nhrp shortcut
ip mtu 1400
ip tcp adjust-mss 1360
router eigrp DMVPN_TUNNEL_NET
address-family ipv4 unicast autonomous-system 68
```

```
eigrp router-id 2.2.2.2
network 100.100.100.0 255.255.255.248
network 172.16.2.0 255.255.255.0
eigrp stub connected
router eigrp DMVPN_TRANS_NET
address-family ipv4 unicast autonomous-system 168
eigrp router-id 20.2.2.2
network 198.51.100.0 255.255.255.252
network 192.168.2.0 255.255.255.0
end
Router R3 spoke 2
hostname R3
no ip domain lookup
banner motd # R3, Implement DMVPN Spoke 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
line vty 0 4
privilege level 15
password cisco123
exec-timeout 0 0
logging synchronous
login
exit
interface g0/0/1
interface loopback 1
ip address 203.0.113.2 255.255.255.252
no shutdown
exit
interface loopback 0
ip address 192.168.3.1 255.255.255.0
no shutdown
exit
```

```
interface loopback 1
ip address 172.16.3.1 255.255.255.0
no shutdown
exit
interface tunnel 1
tunnel mode gre multipoint
tunnel source loopback 0
no tunnel destination
tunnel key 999
ip address 100.100.100.3 255.255.255.248
ip nhrp network-id 1
ip nhrp authentication NHRPauth
ip nhrp nhs 100.100.100.1
ip nhrp map multicast 192.0.2.1
ip nhrp map 100.100.100.1 192.0.2.1
ip nhrp shortcut
ip mtu 1400
ip tcp adjust-mss 1360
router eigrp DMVPN_TUNNEL_NET
address-family ipv4 unicast autonomous-system 68
eigrp router-id 3.3.3.3
network 100.100.100.0 255.255.255.248
network 172.16.3.0 255.255.255.0
eigrp stub connected
router eigrp DMVPN_TRANS_NET
address-family ipv4 unicast autonomous-system 168
eigrp router-id 30.3.3.3
network 203.0.113.0 255.255.255.252
network 192.168.3.0 255.255.255.0
eigrp stub connected
end
Layer 3 Switch DMVPN
hostname DMVPN
no ip domain lookup
```

```
ip routing
banner motd # DMVPN, DMVPN cloud switch #
line con 0
exec-timeout 0 0
logging synchronous
exit
line vty 0 4
privilege level 15
password cisco123
exec-timeout 0 0
logging synchronous
login
interface g1/0/11
no switchport
ip address 192.0.2.2 255.255.255.252
no shutdown
exit
interface g1/0/12
no switchport
ip address 198.51.100.1 255.255.255.252
no shutdown
exit
interface g1/0/13
no switchport
ip address 203.0.113.1 255.255.255.252
no shutdown
exit
router eigrp DMVPN_TRANS_NET
address-family ipv4 unicast autonomous-system 168
eigrp router-id 40.4.4.4
network 192.0.2.0 255.255.255.252
network 198.51.100.0 255.255.255.252
network 203.0.113.0 255.255.255.252
end
```

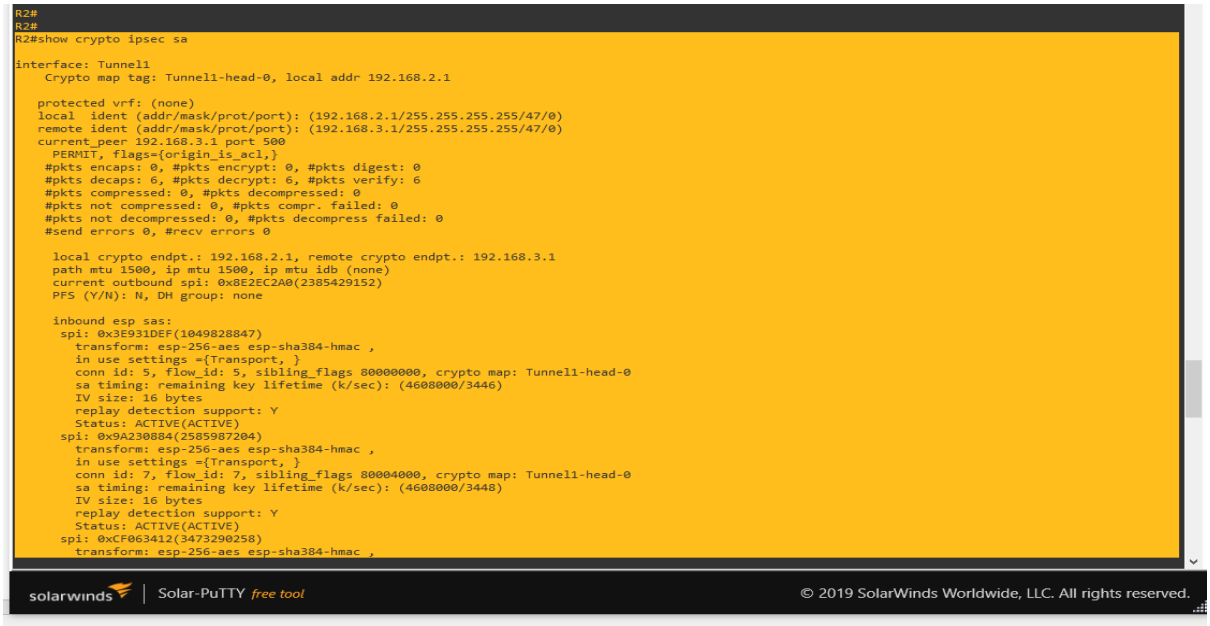
Part 1: Build the Network and Verify DMVPN Phase 3 Operation

Part 2: Secure DMVPN Phase 3 Tunnels

```
R1(config)# crypto isakmp policy 99
R1(config-isakmp)# hash sha384
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# group 14
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# exit
R1(config)# crypto isakmp key DMVPN@key# address 0.0.0.0
R1(config)# crypto ipsec transform-set DMVPN_TRANS esp-aes 256 esp-
sha384-hmac
R1(cfg-crypto-trans)# mode transport
R1(cfg-crypto-trans)# exit
R1(config)# crypto ipsec profile DMVPN_PROFILE
R1(ipsec-profile)# set transform-set DMVPN_TRANS
R1(ipsec-profile)# exit
R1(config)# interface tunnel 1
R1(config-if)# tunnel protection ipsec profile DMVPN_PROFILE
R1(config-if)# exit
```

```
R2(config)# crypto isakmp policy 99
R2(config-isakmp)# hash sha384
R2(config-isakmp)# encryption aes 256
R2(config-isakmp)# group 14
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# exit
R2(config)# crypto isakmp key DMVPN@key# address 0.0.0.0
R2(config)# crypto ipsec transform-set DMVPN_TRANS esp-aes 256 esp-
sha384-hmac
R2(cfg-crypto-trans)# mode transport
R2(cfg-crypto-trans)# exit
R2(config)# crypto ipsec profile DMVPN_PROFILE
```

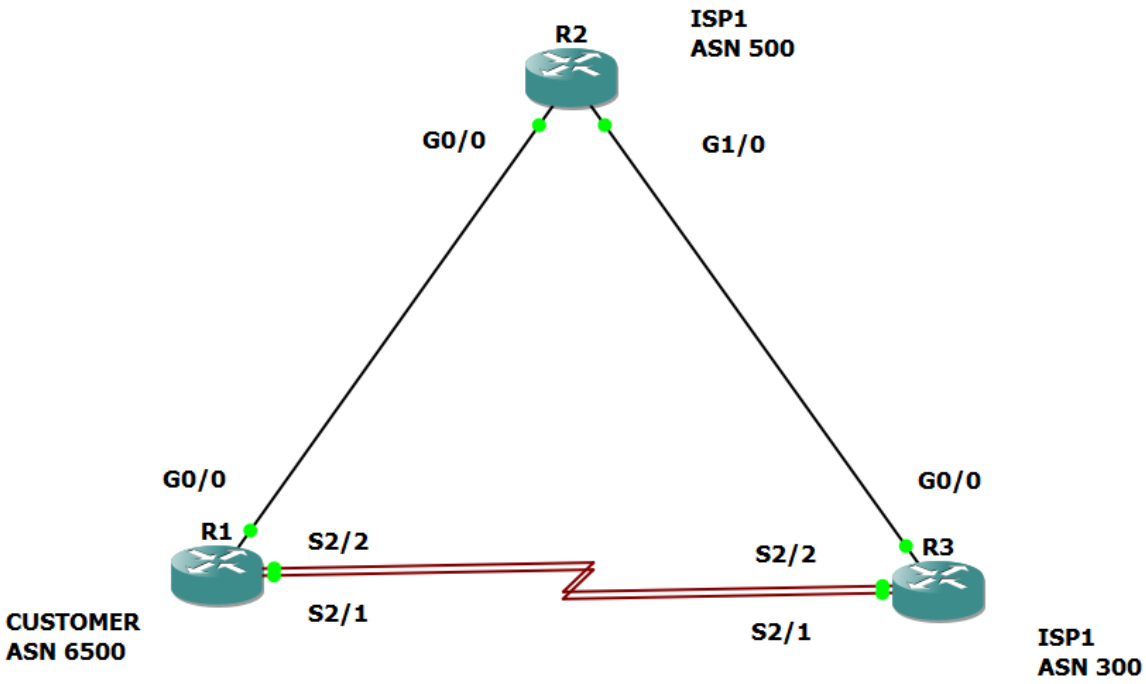
```
R2(ipsec-profile)# set transform-set DMVPN_TRANS
R2(ipsec-profile)# exit
R2(config)# interface tunnel 1
R2(config-if)# tunnel protection ipsec profile DMVPN_PROFILE
R2(config-if)# exit
R3(config)# crypto isakmp policy 99
R3(config-isakmp)# hash sha384
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# group 14
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# exit
R3(config)# crypto isakmp key DMVPN@key# address 0.0.0.0
R3(config)# crypto ipsec transform-set DMVPN_TRANS esp-aes 256 esp-sha384-hmac
R3(cfg-crypto-trans)# mode transport
R3(cfg-crypto-trans)# exit
R3(config)# crypto ipsec profile DMVPN_PROFILE
R3(ipsec-profile)# set transform-set DMVPN_TRANS
R3(ipsec-profile)# exit
R3(config)# interface tunnel 1
R3(config-if)# tunnel protection ipsec profile DMVPN_PROFILE
R3(config-if)# exit
```



Practical-5A

Aim: Implement BGP Path Manipulation

Topology:



Objectives

Part 1: Build the Network and Configure Basic Device Settings and Interface Addressing

Part 2: Configure and Verify Multi-Protocol BGP on all Routers

Part 3: Configure and Verify BGP Path Manipulation Settings on all Routers

Part 1: Build the Network and Configure Basic Device Settings and Interface Addressing

Router R1

```
no ip domain lookup
hostname R1
line con 0
exec-timeout 0 0
logging synchronous
banner motd # This is R1, BGP Path Manipulation Lab #
ipv6 unicast-routing
interface g0/0/0
ip address 10.1.2.1 255.255.255.0
```

```
ipv6 address fe80::1:1 link-local
ipv6 address 2001:db8:acad:1012::1/64
no shutdown
interface s0/1/0
ip address 10.1.3.1 255.255.255.128
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:acad:1013::1/64
no shutdown
interface s0/1/1
ip address 10.1.3.129 255.255.255.128
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:acad:1014::1/64
no shutdown
interface loopback 0
ip address 192.168.1.1 255.255.255.224
ipv6 address fe80::1:4 link-local
ipv6 address 2001:db8:acad:1000::1/64
no shutdown
interface loopback 1
ip address 192.168.1.65 255.255.255.192
ipv6 address fe80::1:5 link-local
ipv6 address 2001:db8:acad:1001::1/64
no shutdown
```

Router R2

```
no ip domain lookup
hostname R2
line con 0
exec-timeout 0 0
logging synchronous
banner motd # This is R2, BGP Path Manipulation Lab #
ipv6 unicast-routing
interface g0/0/0
ip address 10.1.2.2 255.255.255.0
```

```
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:acad:1012::2/64
no shutdown
interface g0/0/1
ip address 10.2.3.2 255.255.255.0
ipv6 address fe80::2:2 link-local
ipv6 address 2001:db8:acad:1023::2/64
no shutdown
interface loopback 0
ip address 192.168.2.1 255.255.255.224
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:acad:2000::1/64
no shutdown
interface loopback 1
ip address 192.168.2.65 255.255.255.192
ipv6 address fe80::2:4 link-local
ipv6 address 2001:db8:acad:2001::1/64
no shutdown
```

Router R3

```
no ip domain lookup
hostname R3
line con 0
exec-timeout 0 0
logging synchronous
banner motd # This is R3, BGP Path Manipulation Lab #
ipv6 unicast-routing
interface g0/0/0
ip address 10.2.3.3 255.255.255.0
ipv6 address fe80::3:1 link-local
ipv6 address 2001:db8:acad:1023::3/64
no shutdown
interface s0/1/0
ip address 10.1.3.3 255.255.255.128
```

```
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:acad:1013::3/64
no shutdown
interface s0/1/1
ip address 10.1.3.130 255.255.255.128
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:acad:1014::3/64
no shutdown
interface loopback 0
ip address 192.168.3.1 255.255.255.224
ipv6 address fe80::3:4 link-local
ipv6 address 2001:db8:acad:3000::1/64
no shutdown
interface loopback 1
ip address 192.168.3.65 255.255.255.192
ipv6 address fe80::3:5 link-local
ipv6 address 2001:db8:acad:3001::1/64
no shutdown
```

Part 2: Configure and Verify Multi-Protocol BGP on all Routers

```
R1(config)# router bgp 6500
R1(config-router)# bgp router-id 1.1.1.1
R1(config-router)# no bgp default ipv4-unicast
R1(config-router)# neighbor 10.1.2.2 remote-as 500
R1(config-router)# neighbor 10.1.3.3 remote-as 300
R1(config-router)# neighbor 10.1.3.130 remote-as 300
R1(config-router)# neighbor 2001:db8:acad:1012::2 remote-as 500
R1(config-router)# neighbor 2001:db8:acad:1013::3 remote-as 300
R1(config-router)# neighbor 2001:db8:acad:1014::3 remote-as 300
R1(config-router)# address-family ipv4 unicast
R1(config-router-af)# network 192.168.1.0 mask 255.255.255.224
R1(config-router-af)# network 192.168.1.64 mask 255.255.255.192
R1(config-router-af)# no neighbor 2001:db8:acad:1012::2 activate
R1(config-router-af)# no neighbor 2001:db8:acad:1013::3 activate
```

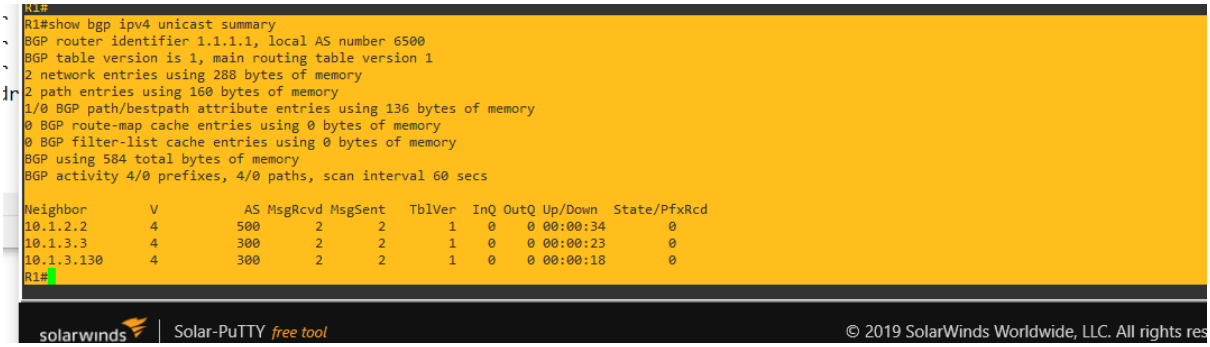
```
R1(config-router-af)# no neighbor 2001:db8:acad:1014::3 activate
R1(config-router-af)# neighbor 10.1.2.2 activate
R1(config-router-af)# neighbor 10.1.3.3 activate
R1(config-router-af)# neighbor 10.1.3.130 activate
R1(config-router)# address-family ipv6 unicast
R1(config-router-af)# network 2001:db8:acad:1000::/64
R1(config-router-af)# network 2001:db8:acad:1001::/64
R1(config-router-af)# neighbor 2001:db8:acad:1012::2 activate
R1(config-router-af)# neighbor 2001:db8:acad:1013::3 activate
R1(config-router-af)# neighbor 2001:db8:acad:1014::3 activate
```

Step 4: Configure MP-BGP on R2 and R3 as you did in the previous step.

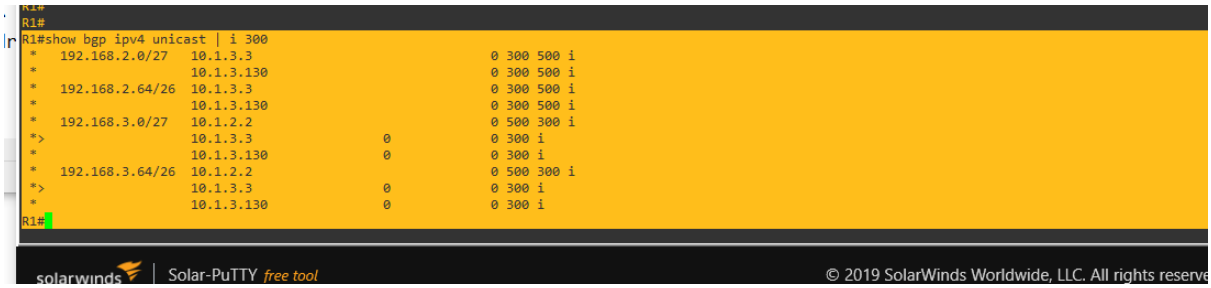
```
R2(config)# router bgp 500
R2(config-router)# bgp router-id 2.2.2.2
R2(config-router)# no bgp default ipv4-unicast
R2(config-router)# neighbor 10.1.2.1 remote-as 6500
R2(config-router)# neighbor 10.2.3.3 remote-as 300
R2(config-router)# neighbor 2001:db8:acad:1012::1 remote-as 6500
R2(config-router)# neighbor 2001:db8:acad:1023::3 remote-as 300
R2(config-router)# address-family ipv4
R2(config-router-af)# network 192.168.2.0 mask 255.255.255.224
R2(config-router-af)# network 192.168.2.64 mask 255.255.255.192
R2(config-router-af)# neighbor 10.1.2.1 activate
R2(config-router-af)# neighbor 10.2.3.3 activate
R2(config-router-af)# no neighbor 2001:db8:acad:1012::1 activate
R2(config-router-af)# no neighbor 2001:db8:acad:1023::3 activate
R2(config-router-af)# exit-address-family
R2(config-router)# address-family ipv6
R2(config-router-af)# network 2001:db8:acad:2000::/64
R2(config-router-af)# network 2001:db8:acad:2001::/64
R2(config-router-af)# neighbor 2001:db8:acad:1012::1 activate
R2(config-router-af)# neighbor 2001:db8:acad:1023::3 activate
R2(config-router-af)# exit-address-family
R3(config)# router bgp 300
```

```
R3(config-router)# bgp router-id 3.3.3.3
R3(config-router)# no bgp default ipv4-unicast
R3(config-router)# neighbor 10.1.3.1 remote-as 6500
R3(config-router)# neighbor 10.1.3.129 remote-as 6500
R3(config-router)# neighbor 10.2.3.2 remote-as 500
R3(config-router)# neighbor 2001:db8:acad:1013::1 remote-as 6500
R3(config-router)# neighbor 2001:db8:acad:1014::1 remote-as 6500
R3(config-router)# neighbor 2001:db8:acad:1023::2 remote-as 500
R3(config-router)# address-family ipv4
R3(config-router-af)# network 192.168.3.0 mask 255.255.255.224
R3(config-router-af)# network 192.168.3.64 mask 255.255.255.192
R3(config-router-af)# neighbor 10.1.3.1 activate
R3(config-router-af)# neighbor 10.1.3.129 activate
R3(config-router-af)# neighbor 10.2.3.2 activate
R3(config-router-af)# no neighbor 2001:db8:acad:1013::1 activate
R3(config-router-af)# no neighbor 2001:db8:acad:1014::1 activate
R3(config-router-af)# no neighbor 2001:db8:acad:1023::2 activate
R3(config-router-af)# exit-address-family
R3(config-router)# address-family ipv6
R3(config-router-af)# network 2001:db8:acad:3000::/64
R3(config-router-af)# network 2001:db8:acad:3001::/64
R3(config-router-af)# neighbor 2001:db8:acad:1013::1 activate
R3(config-router-af)# neighbor 2001:db8:acad:1014::1 activate
R3(config-router-af)# neighbor 2001:db8:acad:1023::2 activate
R3(config-router-af)# exit-address-family
```

Step 5: Verify that MP-BGP is operational.



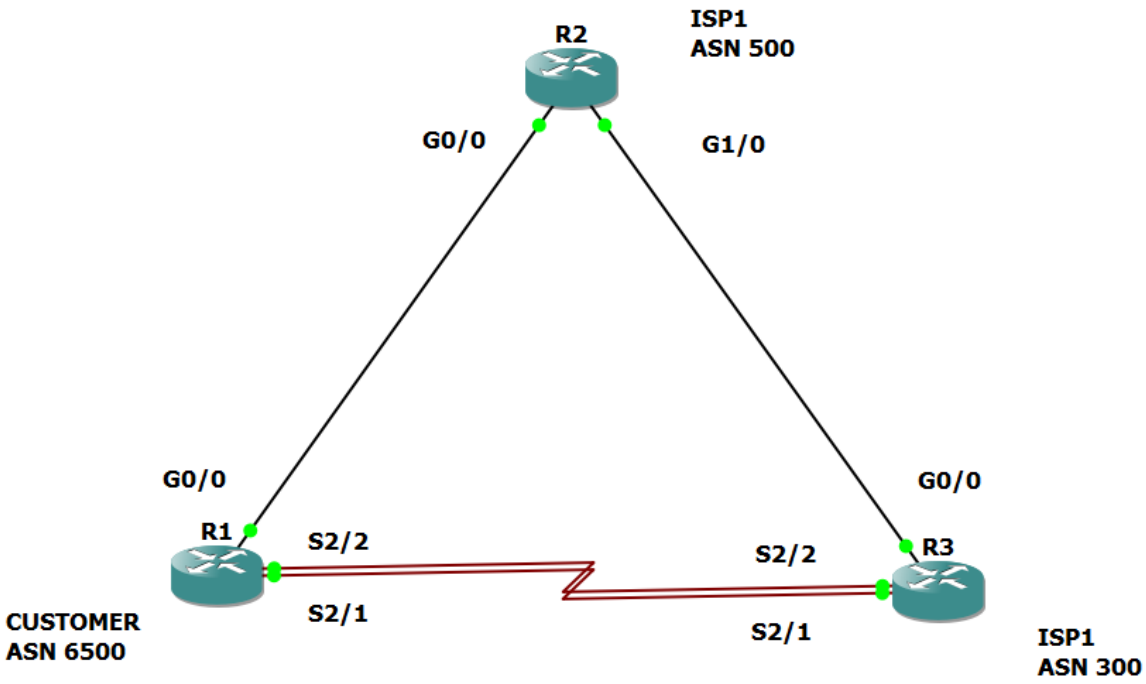
Part 3: Configure and Verify BGP Path Manipulation Settings on all Routers



Practical-5B

Aim: Implement BGP Communities

Topology:



Objectives:

Part 1: Build the Network and Configure Basic Device Settings and Interface Addressing

Part 2: Configure and Verify Multi-Protocol BGP on all Routers

Part 3: Configure and Verify BGP Communities on all Routers

Part 1: Build the Network and Configure Basic Device Settings and Interface Addressing

Router R1

```
no ip domain lookup
hostname R1
line con 0
exec-timeout 0 0
lo exit
banner motd # This is R1, BGP Path Manipulation Lab #
ipv6 unicast-routing
interface g0/0/0
ip address 10.1.2.1 255.255.255.0
```

```
ipv6 address fe80::1:1 link-local
ipv6 address 2001:db8:acad:1012::1/64
no shutdown
interface s0/1/0
ip address 10.1.3.1 255.255.255.128
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:acad:1013::1/80
no shutdown
interface s0/1/1
ip address 10.1.3.129 255.255.255.128
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:acad:1014::1/80
no shutdown
interface loopback 0
ip address 192.168.1.1 255.255.255.224
ipv6 address fe80::1:4 link-local
ipv6 address 2001:db8:acad:1000::1/64
no shutdown
interface loopback 1
ip address 192.168.1.65 255.255.255.192
ipv6 address fe80::1:5 link-local
ipv6 address 2001:db8:acad:1001::1/64
no shutdown
exit
```

Router R2

```
no ip domain lookup
hostname R2
line con 0
exec-timeout 0 0
logging synchronous
exit
banner motd # This is R2, BGP Path Manipulation Lab #
ipv6 unicast-routing
interface g0/0/0
```

```
ip address 10.1.2.2 255.255.255.0
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:acad:1012::2/64
no shutdown
interface g0/0/1
ip address 10.2.3.2 255.255.255.0
logging synchronous
ipv6 address fe80::2:2 link-local
ipv6 address 2001:db8:acad:1023::2/64
no shutdown
interface loopback 0
ip address 192.168.2.1 255.255.255.224
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:acad:2000::1/64
no shutdown
interface loopback 1
ip address 192.168.2.65 255.255.255.192
ipv6 address fe80::2:4 link-local
ipv6 address 2001:db8:acad:2001::1/64
no shutdown
```

Router R3

```
no ip domain lookup
hostname R3
line con 0
exec-timeout 0 0
logging synchronous
exit
banner motd # This is R3, BGP Path Manipulation Lab #
ipv6 unicast-routing
interface g0/0/0
ip address 10.2.3.3 255.255.255.0
ipv6 address fe80::3:1 link-local
ipv6 address 2001:db8:acad:1023::3/64
no shutdown
```

```
interface s0/1/0
ip address 10.1.3.3 255.255.255.128
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:acad:1013::3/80
no shutdown
interface s0/1/1
ip address 10.1.3.130 255.255.255.128
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:acad:1014::3/80
no shutdown
interface loopback 0
ip address 192.168.3.1 255.255.255.224
ipv6 address fe80::3:4 link-local
ipv6 address 2001:db8:acad:3000::1/64
no shutdown
interface loopback 1
ip address 192.168.3.65 255.255.255.192
ipv6 address 2001:db8:acad:3001::1/64
no shutdown
ipv6 address fe80::3:5 link-local
```

Part 2: Configure and Verify Multi-Protocol BGP on all Routers

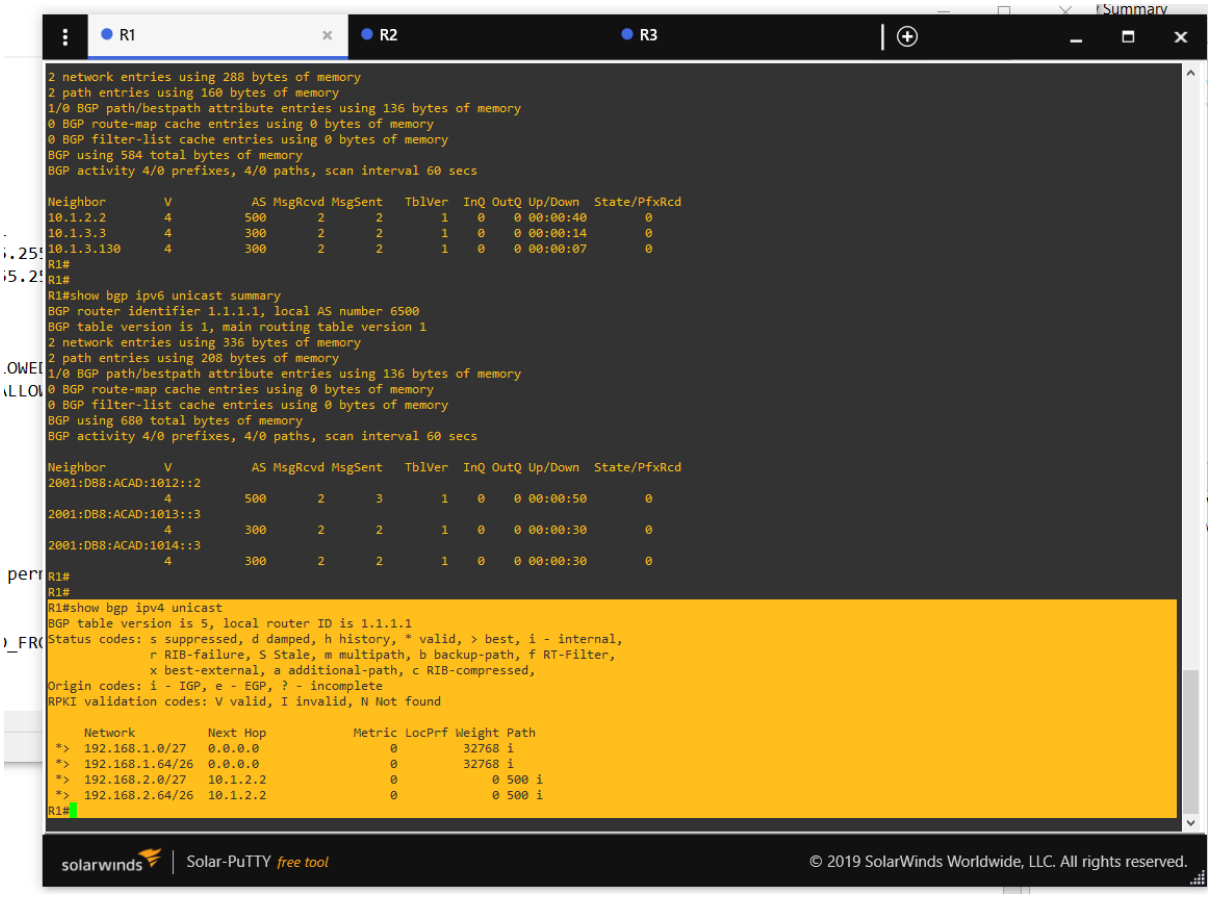
```
R1(config)# router bgp 6500
R1(config-router)# no bgp default ipv4-unicast
R1(config-router)# bgp router-id 1.1.1.1
R1(config-router)# neighbor 10.1.2.2 remote-as 500
R1(config-router)# neighbor 10.1.3.3 remote-as 300
R1(config-router)# neighbor 10.1.3.130 remote-as 300
R1(config-router)# neighbor 2001:db8:acad:1012::2 remote-as 500
R1(config-router)# neighbor 2001:db8:acad:1013::3 remote-as 300
R1(config-router)# neighbor 2001:db8:acad:1014::3 remote-as 300
R1(config-router)# address-family ipv4 unicast
R1(config-router-af)# network 192.168.1.0 mask 255.255.255.224
R1(config-router-af)# network 192.168.1.64 mask 255.255.255.192
R1(config-router-af)# no neighbor 2001:db8:acad:1012::2 activate
```

```
R1(config-router-af)# no neighbor 2001:db8:acad:1013::3 activate
R1(config-router-af)# no neighbor 2001:db8:acad:1014::3 activate
R1(config-router-af)# neighbor 10.1.2.2 activate
R1(config-router-af)# neighbor 10.1.3.3 activate
R1(config-router-af)# neighbor 10.1.3.130 activate
R1(config-router)# address-family ipv6 unicast
R1(config-router-af)# network 2001:db8:acad:1000::/64
R1(config-router-af)# network 2001:db8:acad:1001::/64
R1(config-router-af)# neighbor 2001:db8:acad:1012::2 activate
R1(config-router-af)# neighbor 2001:db8:acad:1013::3 activate
R1(config-router-af)# neighbor 2001:db8:acad:1014::3 activate
```

```
R2(config)# router bgp 500
R2(config-router)# bgp router-id 2.2.2.2
R2(config-router)# no bgp default ipv4-unicast
R2(config-router)# neighbor 10.1.2.1 remote-as 6500
R2(config-router)# neighbor 10.2.3.3 remote-as 300
R2(config-router)# neighbor 2001:db8:acad:1012::1 remote-as 6500
R2(config-router)# neighbor 2001:db8:acad:1023::3 remote-as 300
R2(config-router)# address-family ipv4
R2(config-router-af)# network 192.168.2.0 mask 255.255.255.224
R2(config-router-af)# network 192.168.2.64 mask 255.255.255.192
R2(config-router-af)# neighbor 10.1.2.1 activate
R2(config-router-af)# neighbor 10.2.3.3 activate
R2(config-router-af)# no neighbor 2001:db8:acad:1012::1 activate
R2(config-router-af)# no neighbor 2001:db8:acad:1023::3 activate
R2(config-router-af)# exit-address-family
R2(config-router)# address-family ipv6
R2(config-router-af)# network 2001:db8:acad:2000::/64
R2(config-router-af)# network 2001:db8:acad:2001::/64
R2(config-router-af)# neighbor 2001:db8:acad:1012::1 activate
R2(config-router-af)# neighbor 2001:db8:acad:1023::3 activate
R2(config-router-af)# exit-address-family
```

```
R3(config)# router bgp 300
R3(config-router)# bgp router-id 3.3.3.3
R3(config-router)# no bgp default ipv4-unicast
R3(config-router)# neighbor 10.1.3.1 remote-as 6500
R3(config-router)# neighbor 10.1.3.129 remote-as 6500
R3(config-router)# neighbor 10.2.3.2 remote-as 500
R3(config-router)# neighbor 2001:db8:acad:1013::1 remote-as 6500
R3(config-router)# neighbor 2001:db8:acad:1014::1 remote-as 6500
R3(config-router)# neighbor 2001:db8:acad:1023::2 remote-as 500
R3(config-router)# address-family ipv4
R3(config-router-af)# network 192.168.3.0 mask 255.255.255.224
R3(config-router-af)# network 192.168.3.64 mask 255.255.255.192
R3(config-router-af)# neighbor 10.1.3.1 activate
R3(config-router-af)# neighbor 10.1.3.129 activate
R3(config-router-af)# neighbor 10.2.3.2 activate
R3(config-router-af)# no neighbor 2001:db8:acad:1013::1 activate
R3(config-router-af)# no neighbor 2001:db8:acad:1014::1 activate
R3(config-router-af)# no neighbor 2001:db8:acad:1023::2 activate
R3(config-router-af)# exit-address-family
R3(config-router)# address-family ipv6
R3(config-router-af)# network 2001:db8:acad:3000::/64
R3(config-router-af)# network 2001:db8:acad:3001::/64
R3(config-router-af)# neighbor 2001:db8:acad:1013::1 activate
R3(config-router-af)# neighbor 2001:db8:acad:1014::1 activate
R3(config-router-af)# neighbor 2001:db8:acad:1023::2 activate
R3(config-router-af)# exit-address-family
```

Step 4: Verify that MP-BGP is operational.



Part 3: Configure and Verify BGP Communities on all Routers

```
R1(config)# ip bgp-community new-format
R1(config)# router bgp 6500
R1(config-router)# address-family ipv4 unicast
R1(config-router-af)# neighbor 10.1.2.2 send-community
R1(config-router-af)# neighbor 10.1.3.3 send-community
R1(config-router-af)# neighbor 10.1.3.130 send-community
R1(config-router-af)# address-family ipv6 unicast
R1(config-router-af)# neighbor 2001:db8:acad:1012::2 send-community
R1(config-router-af)# neighbor 2001:db8:acad:1013::3 send-community
R1(config-router-af)# neighbor 2001:db8:acad:1014::3 send-community
R1(config-router-af)# exit
R2(config)# ip bgp-community new-format
R2(config)# router bgp 500
R2(config-router)# address-family ipv4 unicast
R2(config-router-af)# neighbor 10.1.2.1 send-community
R2(config-router-af)# neighbor 10.2.3.3 send-community
```

```
R2(config-router-af)# address-family ipv6 unicast
R2(config-router-af)# neighbor 2001:db8:acad:1012::1 send-community
R2(config-router-af)# neighbor 2001:db8:acad:1023::3 send-community
R2(config-router-af)# exit
R3(config)# ip bgp-community new-format
R3(config)# router bgp 300
R3(config-router)# address-family ipv4 unicast
R3(config-router-af)# neighbor 10.1.3.1 send-community
R3(config-router-af)# neighbor 10.1.3.129 send-community
R3(config-router-af)# neighbor 10.2.3.2 send-community
R3(config-router-af)# address-family ipv6 unicast
R3(config-router-af)# neighbor 2001:db8:acad:1013::1 send-community
R3(config-router-af)# neighbor 2001:db8:acad:1014::1 send-community
R3(config-router-af)# neighbor 2001:db8:acad:1023::2 send-community
R3(config-router-af)# exit
```

Step 2: Configure and verify the effect of the no-export community.

```
R3(config)# ip prefix-list LOCAL_NETWORK_COMMSET seq 5 permit 192.168.3.0/24
le 27
R3(config)# ipv6 prefix-list LOCAL_6_NETWORK_COMMSET seq 5 permit
2001:db8:acad:3000::/64
R3(config)# ipv6 prefix-list LOCAL_6_NETWORK_COMMSET seq 10 permit
2001:db8:acad:3001::/64
R3(config)# route-map COMMSET permit 10
R3(config-route-map)# match ip address prefix-list LOCAL_NETWORK_COMMSET
R3(config-route-map)# set community no-export additive
R3(config-route-map)# exit
R3(config)# route-map COMMSET permit 20
R3(config-route-map)# set community internet additive
R3(config-route-map)# exit
R3(config)# route-map COMMSET_6 permit 10
R3(config-route-map)# match ipv6 address prefix-list LOCAL_6_NETWORK_COMMSET
R3(config-route-map)# set community no-export additive
R3(config-route-map)# exit
R3(config)# route-map COMMSET_6 permit 20
```

```
R3(config-route-map)# set community internet additive
R3(config)# router bgp 300
R3(config-router)# address-family ipv4 unicast
R3(config-router-af)# neighbor 10.1.3.1 route-map COMMSET out
R3(config-router-af)# neighbor 10.1.3.129 route-map COMMSET out
R3(config-router-af)# address-family ipv6 unicast
R3(config-router-af)# neighbor 2001:db8:acad:1013::1 route-map COMMSET_6 out
R3(config-router-af)# neighbor 2001:db8:acad:1014::1 route-map COMMSET_6 out
R3# clear bgp ipv4 unicast 6500 out
R3# clear bgp ipv6 unicast 6500 out
```

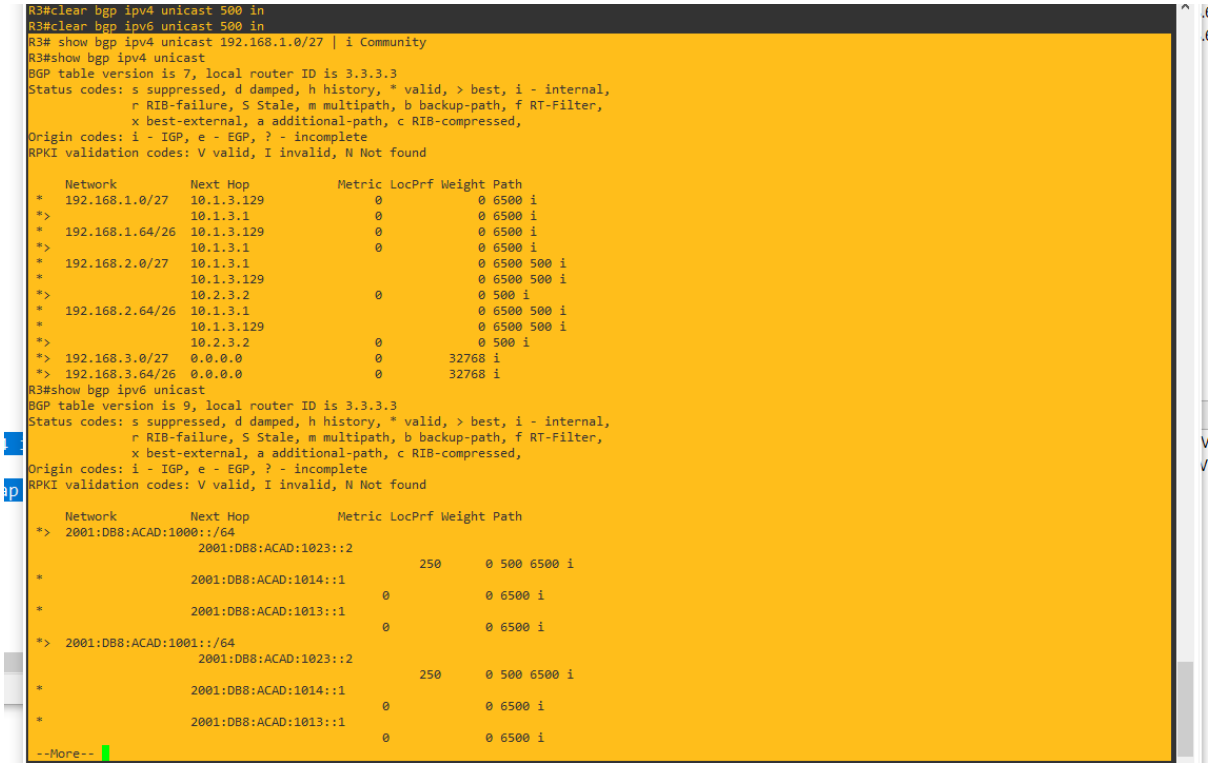
Step 3: Add private community information to routes advertised by R1.

```
R1(config)# route-map ADDCOMM permit 10
R1(config-route-map)# set community 650:400 additive
R1(config-route-map)# exit
R1(config)# route-map ADDCOMM_6 permit 10
R1(config-route-map)# set community 650:600 additive
R1(config-route-map)# exit
R1(config)# router bgp 6500
R1(config-router)# address-family ipv4 unicast
R1(config-router-af)# neighbor 10.1.2.2 route-map ADDCOMM out
R1(config-router-af)# address-family ipv6 unicast
R1(config-router-af)# neighbor 2001:db8:acad:1012::2 route-map ADDCOMM_6 out
R1(config-router-af)# end
R1# clear bgp ipv4 unicast 500 out
R1# clear bgp ipv6 unicast 500 out
```

Step 4: Configure community-based route filtering and manipulation.

```
R3(config)# ip community-list 100 permit 650:400
R3(config)# ip community-list 101 permit 650:600
R3(config)# route-map COMMCHECK_4 deny 10
R3(config-route-map)# match community 100
R3(config-route-map)# route-map COMMCHECK_4 permit 20
R3(config-route-map)# exit
R3(config)# route-map COMMCHECK_6 permit 10
R3(config-route-map)# match community 101
```

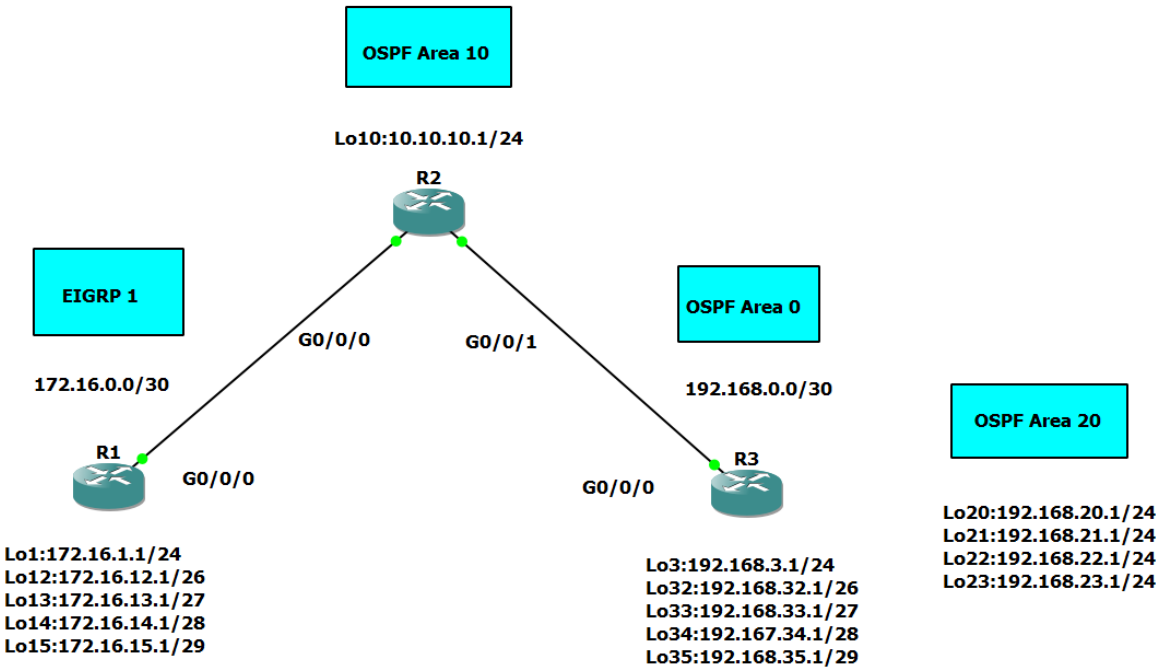
```
R3(config-route-map)# set local-preference 250
R3(config-route-map)# route-map COMMCHECK_6 permit 20
R3(config-route-map)# exit
R3(config)# router bgp 300
R3(config-router)# address-family ipv4 unicast
R3(config-router-af)# neighbor 10.2.3.2 route-map COMMCHECK_4 in
R3(config-router-af)# address-family ipv6 unicast
R3(config-router-af)# neighbor 2001:db8:acad:1023::2 route-map COMMCHECK_6 in
R3(config-router-af)# end
R3# clear bgp ipv4 unicast 500 in
R3# clear bgp ipv6 unicast 500 in
```



Practical-6A

Aim: Control Routing Updates

Topology:



Objectives:

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure Routing and Redistribution

Part 3: Filter Redistributed Routes using a Distribute List and ACL

Part 4: Filter Redistributed Routes using a Distribute List and Prefix List

Part 5: Filter Redistributed Routes using a Route Map

Part 1: Build the Network and Configure Basic Device Settings

Router R1

```
Open configuration window
hostname R1
no ip domain lookup
line con 0
logging sync
exec-time 0 0
exit
banner motd # This is R1, Controlling Routing Updates #
```

```
interface g0/0/0
description Connection to R2
ip add 172.16.0.2 255.255.255.252
no shut
exit
interface Lo1
ip address 172.16.1.1 255.255.255.0
exit
interface Lo12
ip address 172.16.12.1 255.255.255.192
exit
interface Lo13
ip address 172.16.13.1 255.255.255.224
exit
interface Lo14
ip address 172.16.14.1 255.255.255.240
exit
interface Lo15
ip address 172.16.15.1 255.255.255.248
end
```

Router R2

```
hostname R2
no ip domain lookup
line con 0
logging sync
exec-time 0 0
exit
banner motd # This is R2, Controlling Routing Updates #
interface g0/0/0
description Connection to R1
ip add 172.16.0.1 255.255.255.252
no shut
exit
interface GigabitEthernet0/0/1
```

```
description Connection to R3
ip address 192.168.0.1 255.255.255.252
no shut
exit
int lo10
ip add 10.10.10.1 255.255.255.0
ip ospf network point-to-point
end
```

Router R3

```
hostname R3
no ip domain lookup
line con 0
logging sync
exec-time 0 0
exit
banner motd # This is R3, Controlling Routing Updates #
interface g0/0/0
description Connection to R2
ip add 192.168.0.2 255.255.255.252
no shut
exit
interface Lo3
ip add 192.168.3.1 255.255.255.0
ip ospf network point-to-point
exit
interface Lo32
ip add 192.168.32.1 255.255.255.0
ip ospf network point-to-point
exit
interface Lo33
ip add 192.168.33.1 255.255.255.0
ip ospf network point-to-point
exit
interface Lo34
```

```
ip add 192.168.34.1 255.255.255.0
ip ospf network point-to-point
exit
interface Lo35
ip add 192.168.35.1 255.255.255.0
ip ospf network point-to-point
exit
interface Lo20
ip add 192.168.20.1 255.255.255.0
ip ospf network point-to-point
exit
interface Lo21
ip add 192.168.21.1 255.255.255.0
ip ospf network point-to-point
exit
interface Lo22
ip add 192.168.22.1 255.255.255.0
ip ospf network point-to-point
exit
interface Lo23
ip add 192.168.23.1 255.255.255.0
ip ospf network point-to-point
end
```

Part 2: Configure Routing and Redistribution

```
R1(config)# router eigrp 1
R1(config-router)# eigrp router-id 1.1.1.1
R1(config-router)# network 172.16.0.0 0.0.0.3
R1(config-router)# network 172.16.1.0 0.0.0.255
R1(config-router)# network 172.16.12.0 0.0.0.63
R1(config-router)# network 172.16.13.0 0.0.0.31
R1(config-router)# network 172.16.14.0 0.0.0.15
R1(config-router)# network 172.16.15.0 0.0.0.7
R1(config-router)# end
```

```
R3(config)# router ospf 123
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 192.168.0.0 0.0.0.3 area 0
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
R3(config-router)# network 192.168.32.0 0.0.0.63 area 0
R3(config-router)# network 192.168.33.0 0.0.0.31 area 0
R3(config-router)# network 192.168.34.0 0.0.0.15 area 0
R3(config-router)# network 192.168.35.0 0.0.0.7 area 0
R3(config-router)# network 192.168.20.0 0.0.3.255 area 20
R3(config-router)# end

R2(config)# router eigrp 1
R2(config-router)# eigrp router-id 2.2.2.2
R2(config-router)# network 172.16.0.0 0.0.0.3
R2(config-router)# exit
R2(config)# router ospf 123
R2(config-router)# router-id 2.2.2.2
R2(config-router)# network 192.168.0.0 0.0.0.3 area 0
R2(config-router)# network 10.10.10.0 0.0.0.255 area 10
R2(config-router)# end
R2(config)# router eigrp 1
R2(config-router)# redistribute ospf 123 metric 10000 100 255 1 1500
R2(config-router)# exit
R2(config)# router ospf 123
R2(config-router)# redistribute eigrp 1 subnets metric 100
R2(config-router)# end

foreach address {
192.168.0.1
192.168.20.1
192.168.21.1
192.168.22.1
192.168.23.1
192.168.3.1
```

```
192.168.32.1
192.168.33.1
192.168.34.1
192.168.35.1
10.10.10.1
172.16.0.1
172.16.0.2
172.16.1.1
172.16.12.1
172.16.13.1
172.16.14.1
172.16.15.1
} { ping $address }
```

Part 3: Filter Redistributed Routes using a Distribute List and ACL.

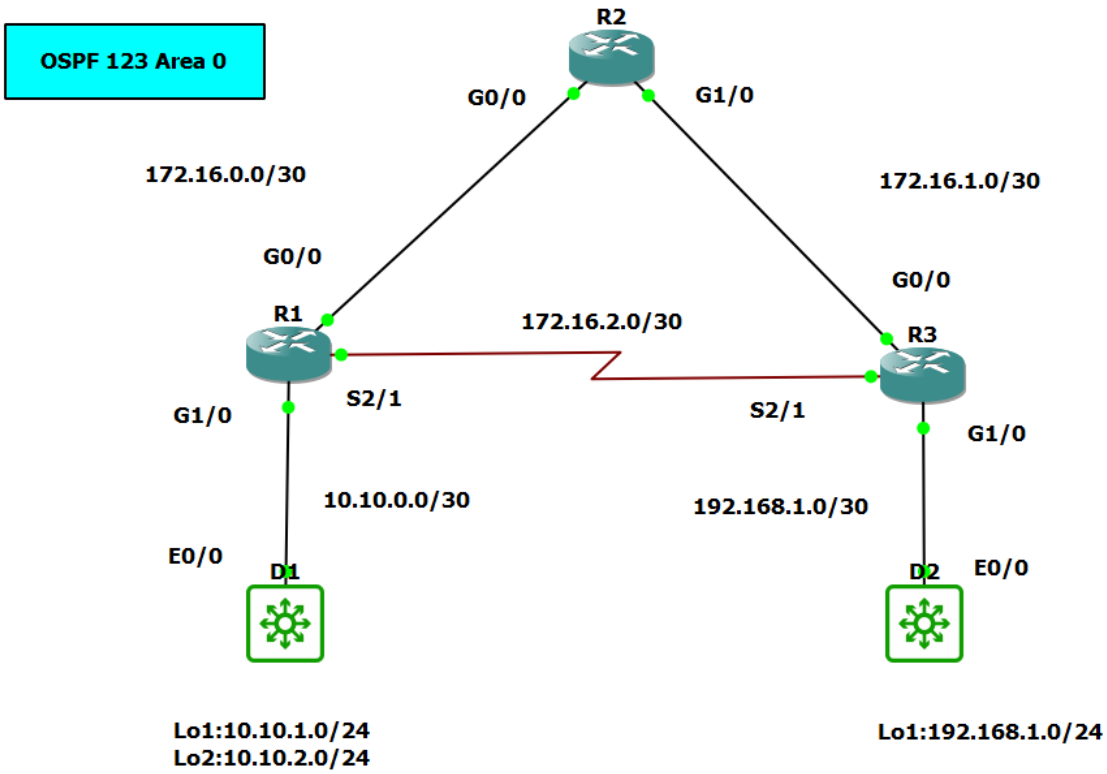
```
R2(config)# ip access-list standard OSPF20-FILTER
R2(config-std-nacl)# remark Used with DList to filter OSPF 20 routes
R2(config-std-nacl)# deny 192.168.20.0 0.0.3.255
R2(config-std-nacl)# permit any
R2(config-std-nacl)# exit
R2(config)# router eigrp 1
R2(config-router)# distribute-list OSPF20-FILTER out ospf 123
R2(config-router)# end

R2(config)# ip access-list standard R3-ACL
R2(config-std-nacl)# remark ACL used with the R3-FILTER route map
R2(config-std-nacl)# permit 192.168.34.0 0.0.0.15
R2(config-std-nacl)# permit 192.168.35.0 0.0.0.7
R2(config-std-nacl)# exit
R2(config)# route-map R3-FILTER deny 10
R2(config-route-map)# description RM filters R3 OSPF routes
R2(config-route-map)# match ip address R3-ACL
R2(config-route-map)# exit
R2(config)# route-map R3-FILTER permit 20
```

```
R2(config-route-map)# description RM permits all other R3 OSPF routes
R2(config-route-map)# exit
R2(config)# router eigrp 1
R2(config-router)# redistribute ospf 123 route-map R3-FILTER metric 1000000
100 255 1 1500
R2(config)# ip prefix-list R1-PL permit 172.16.13.0/27
R2(config)# route-map R1-FILTER permit 10
R2(config-route-map)# description RM filters 172.16.13.0/27
R2(config-route-map)# match ip address prefix-list R1-PL
R2(config-route-map)# set metric 25
R2(config-route-map)# set metric-type type-1
R2(config-route-map)# exit
R2(config)# route-map R1-FILTER permit 20
R2(config-route-map)# description RM permits all other R1 OSPF routes
R2(config-route-map)# exit
R2(config)# router ospf 123
R2(config-router)# redistribute eigrp 1 metric 100 subnets route-map R1-
FILTER
R2(config-router)# exit
```

Practical-6B

Aim: Path Control Using PBR

Topology:



Objectives:

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure and Verify Routing

Part 3: Configure PBR to Provide Path Control

Part 4: Configure Local PBR to Provide Path Control

Part 1: Build the Network and Configure Basic Device Settings

Router R1

```
hostname R1
no ip domain lookup
line con 0
logging sync
exec-time 0 0
exit
banner motd # This is R1, Path Control Using PBR #
```

```
interface G0/0/0
description Connection to R2
ip add 172.16.0.2 255.255.255.252
no shut
exit
interface S0/1/0
description Serial Connection to R3
ip add 172.16.2.1 255.255.255.252
no shut
exit
interface G0/0/1
description Connection to D1
ip add 10.10.0.1 255.255.255.252
no shut
exit
```

Router R2

```
hostname R2
no ip domain lookup
line con 0
logging sync
exec-time 0 0
exit
banner motd # This is R2, Path Control Using PBR #
interface G0/0/0
description Connection to R1
ip add 172.16.0.1 255.255.255.252
no shut
exit
interface GigabitEthernet0/0/1
description Connection to R3
ip address 172.16.1.1 255.255.255.252
no shut
exit
```

Router R3

```
hostname R3
no ip domain lookup
line con 0
logging sync
exec-time 0 0
exit
banner motd # This is R3, Path Control Using PBR #
interface G0/0/0
description Connection to R2
ip add 172.16.1.2 255.255.255.252
no shut
exit
interface S0/1/0
description Serial Connection to R1
ip add 172.16.2.2 255.255.255.252
no shut
exit
interface G0/0/1
description Connection to D2
ip add 192.168.0.1 255.255.255.252
no shut
exit
```

Switch D1

```
hostname D1
no ip domain lookup
line con 0
exec-timeout 0 0
logging synchronous
exit
banner motd # This is D1, Path Control Using PBR #
interface G1/0/11
no switchport
description Connects to R1
ip address 10.10.0.2 255.255.255.252
```

```
no shut
exit
interface Loopback 1
description Interface simulates network
ip ospf network point-to-point
ip address 10.10.1.1 255.255.255.0
exit
interface Loopback 2
description Interface simulates network
ip ospf network point-to-point
ip address 10.10.2.1 255.255.255.0
exit
```

Switch D2

```
hostname D2
no ip domain lookup
line con 0
logging sync
exec-time 0 0
exit
banner motd # This is D2, Path Control Using PBR #
interface G1/0/11
no switchport
description Connects to R3
ip address 192.168.0.2 255.255.255.252
no shut
exit
interface Loopback 1
description Interface simulates network
ip ospf network point-to-point
ip address 192.168.1.1 255.255.255.0
exit
```

Part 2: Configure and Verify Routing

```
D1(config)# ip routing
D1(config)# router ospf 123
```

```
D1(config-router)# router-id 1.1.1.2
D1(config-router)# auto-cost reference-bandwidth 1000
D1(config-router)# network 10.10.0.0 0.0.0.3 area 0
D1(config-router)# network 10.10.1.0 0.0.0.255 area 0
D1(config-router)# network 10.10.2.0 0.0.0.255 area 0
D1(config-router)# end
R1(config)# router ospf 123
R1(config-router)# router-id 1.1.1.1
R1(config-router)# auto-cost reference-bandwidth 1000
R1(config-router)# network 10.10.0.0 0.0.0.3 area 0
R1(config-router)# network 172.16.0.0 0.0.0.3 area 0
R1(config-router)# network 172.16.2.0 0.0.0.3 area 0
R1(config-router)# end

R2(config)# router ospf 123
R2(config-router)# router-id 2.2.2.1
R2(config-router)# auto-cost reference-bandwidth 1000
R2(config-router)# network 172.16.0.0 0.0.0.3 area 0
R2(config-router)# network 172.16.1.0 0.0.0.3 area 0
R2(config-router)# end

R3(config)# router ospf 123
R3(config-router)# router-id 3.3.3.1
R3(config-router)# auto-cost reference-bandwidth 1000
R3(config-router)# network 192.168.0.0 0.0.0.3 area 0
R3(config-router)# network 172.16.1.0 0.0.0.3 area 0
R3(config-router)# network 172.16.2.0 0.0.0.3 area 0
R3(config-router)# end

D2(config)# ip routing
D2(config)# router ospf 123
D2(config-router)# router-id 3.3.3.2
D2(config-router)# auto-cost reference-bandwidth 1000
D2(config-router)# network 192.168.0.0 0.0.0.3 area 0
```

```
D2(config-router)# network 192.168.1.0 0.0.0.255 area 0
D2(config-router)# end
```

Step 3: Verify end-to-end connectivity and path taken

```
tclsh
foreach address {
10.10.0.1
10.10.0.2
10.10.1.1
10.10.2.1
172.16.0.1
172.16.0.2
172.16.1.1
172.16.1.2
172.16.2.1
172.16.2.2
192.168.0.1
192.168.0.2
192.168.1.1
} { ping $address }
```

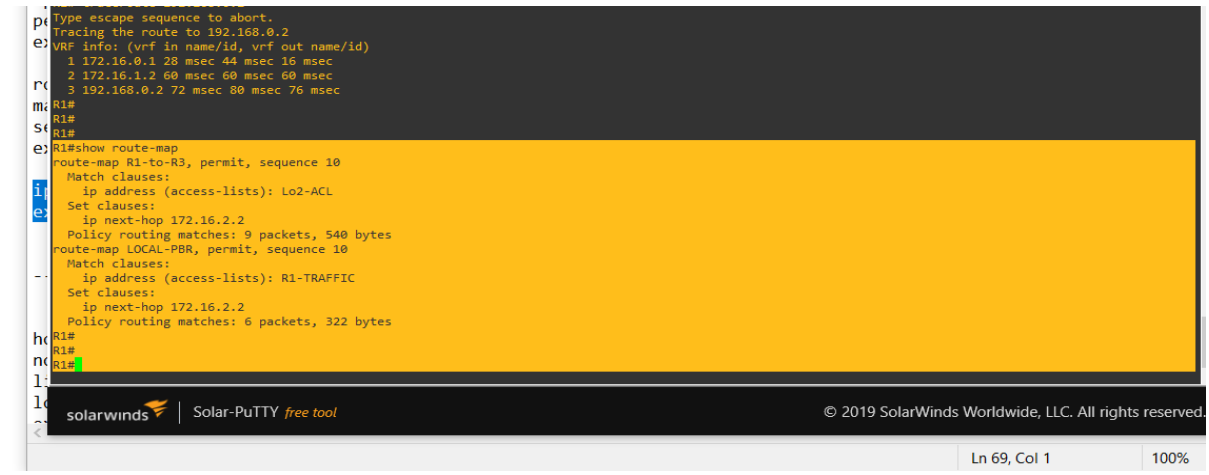
Part 3: Configure PBR to Provide Path Co3ntrol

```
R1(config)# ip access-list standard Lo2-ACL
R1(config-std-nacl)# remark ACL matches D1 Lo2 traffic
R1(config-std-nacl)# permit 10.10.2.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)# route-map R1-to-R3 permit
R1(config-route-map)# description RM to forward Lo2 traffic to R3
R1(config-route-map)# match ip address Lo2-ACL
R1(config-route-map)# set ip next-hop 172.16.2.2
R1(config-route-map)# exit
R1(config)# interface g0/0/1 (Change it according to your interace)
R1(config-if)# ip policy route-map R1-to-R3
R1(config-if)# end
```

Part 4: Configure Local PBR to Provide Path Control

```
R1(config)# ip access-list extended R1-TRAFFIC
```

```
R1(config-ext-nacl)# permit ip any 192.168.1.0 0.0.0.255
R1(config-ext-nacl)# exit
R1(config)# route-map LOCAL-PBR permit
R1(config-route-map)# match ip address R1-TRAFFIC
R1(config-route-map)# set ip next-hop 172.16.2.2
R1(config-route-map)# exit
R1(config)# ip local policy route-map LOCAL-PBR
R1(config)# exit
```

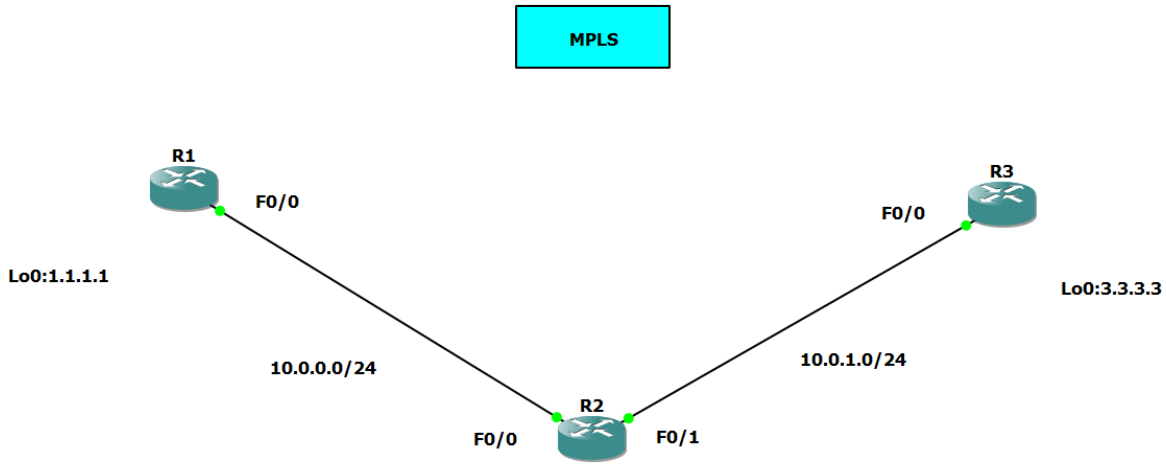


Practical-7

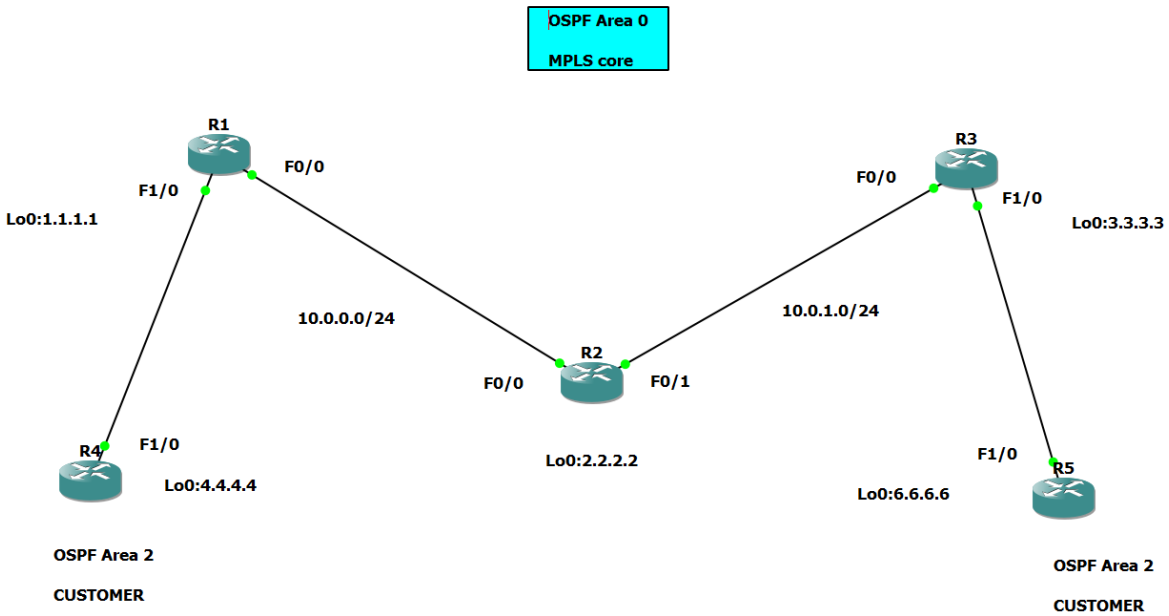
Aim: Lab Implementing MPLS

Topology:

A:



B:



```
------R1------

hostname R1
int lo0
ip add 1.1.1.1 255.255.255.255
ip ospf 1 area 0
int f0/0
ip add 10.0.0.1 255.255.255.0
no shut
ip ospf 1 area 0


router ospf 1
mpls ldp autoconfig


router bgp 1
neighbor 3.3.3.3 remote-as 1
neighbor 3.3.3.3 update-source Loopback0
no auto-summary!
address-family vpnv4
neighbor 3.3.3.3 activate


R1-----------

int f1/0
no shut
ip add 192.168.1.1 255.255.255.0

ip vrf RED
rd 4:4
route-target both 4:4

int f1/0
ip vrf forwarding RED

ip vrf f0
ip vrf forwarding RED


int f1/0
ip address 192.168.1.1 255.255.255.0



-----------R1----
sh run int f1/0

#Building configuration...
current configuration : 119 bytes!
interface FastEthernet1/0
ip vrf forwarding RED
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
```

```
end#----comments


int f1/0
ip ospf 2 area 2


------R2-------

hostname R2
int lo0
ip add 2.2.2.2 255.255.255.255
ip ospf 1 are 0
int f0/0
ip add 10.0.0.2 255.255.255.0
no shut
ip ospf 1 area 0
int f0/1
ip add 10.0.1.2 255.255.255.0
no shut
ip ospf 1 area 0


router ospf 1
mpls ldp autoconfig


----------R3-----


hostname R3
int lo0
ip add 3.3.3.3 255.255.255.255
ip ospf 1 are 0
int f0/0
ip add 10.0.1.3 255.255.255.0
no shut
ip ospf 1 area 0


router ospf 1
mpls ldp autoconfig


router bgp 1
neighbor 1.1.1.1 remote-as 1
neighbor 1.1.1.1 update-source Loopback0
no auto-summary!
address-family vpnv4
neighbor 1.1.1.1 activate


-----------r4------------

int lo0
ip add 4.4.4.4 255.255.255.255
ip ospf 2 area 2
```

```
int f1/0
ip add 192.168.1.4 255.255.255.0
ip ospf 2 area 2
no shut


--------------------------------------------------------------------------
--------------------------------

--------------r5--------

int lo0
ip add 6.6.6.6 255.255.255.255
ip ospf 2 area 2
int f1/0
ip add 192.168.2.6 255.255.255.0
ip ospf 2 area 2
no shut


---r3---

int f1/0
no shut
ip add 192.168.2.3 255.255.255.0

ip vrf RED
rd 4:4
route-target both 4:4

int f1/0
ip vrf forwarding RED

ip vrf forwarding RED

int f1/0
ip address 192.168.2.1 255.255.255.0

sh run int f1/0
--------------------------------

int f1/0
ip ospf 2 area 2


--------r1 and r3---------


router bgp 1
address-family ipv4 vrf RED
redistribute ospf 2


router bgp 1
address-family ipv4 vrf RED
redistribute ospf 2
```

```
------------r1 and r3-----------
router ospf 2
redistribute bgp 1 subnets

router ospf 2
redistribute bgp 1 subnets
```