SUBHASH B
727722EUAI063

Ex.No : 1

Date :

Configuring and accessing a Switch in Packet Tracer

AIM:

To configure and access a Cisco switch using command-line interface (CLI) in Packet Tracer.

DESCRIPTION:

Switch:

A switch is a networking device used to connect multiple computers, printers, and servers within a Local Area Network (LAN)**.** It operates mainly at Layer 2 (Data Link Layer) of the OSI model, though some advanced switches can also operate at Layer 3 (Network Layer)**.** The switch receives data packets and forwards them only to the specific device (port) that the data is intended for, rather than broadcasting it to all devices like a hub. This makes data transmission faster, more secure, and efficient**.**

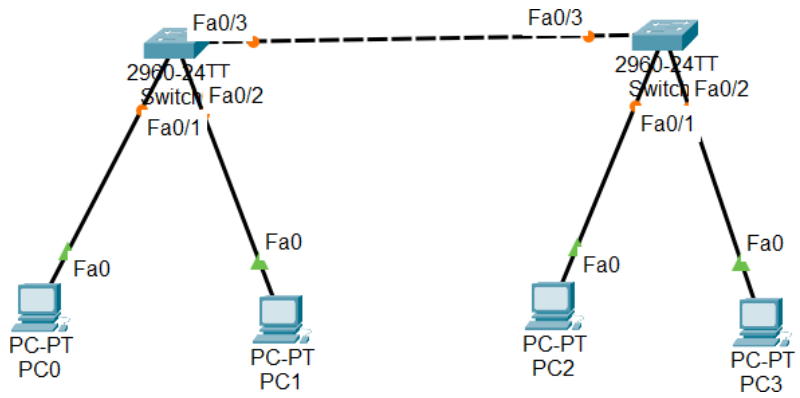
Switches use MAC addresses to identify connected devices and maintain a MAC address table to make intelligent forwarding decisions. They support various functions such as VLAN configuration, port security, spanning tree protocol (STP), and link aggregation**,** which enhance network performance and reliability.

Steps:

- Open Packet Tracer and place a 2960 switch on the workspace.
- Connect a PC to the switch using a Console cable (PC → RS232 → Switch Console port).
- Open the CLI from the PC or directly from the switch.

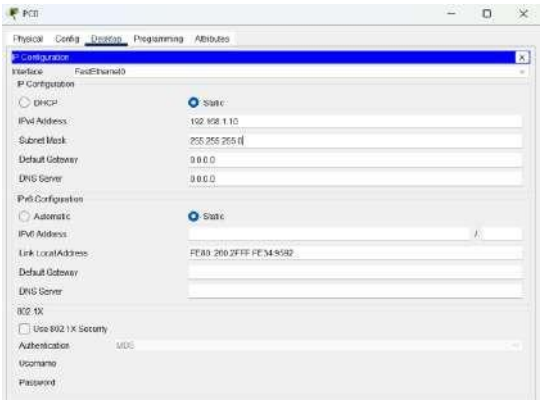
NETWORK DIAGRAM:

SUBHASH B
727722EUAI063

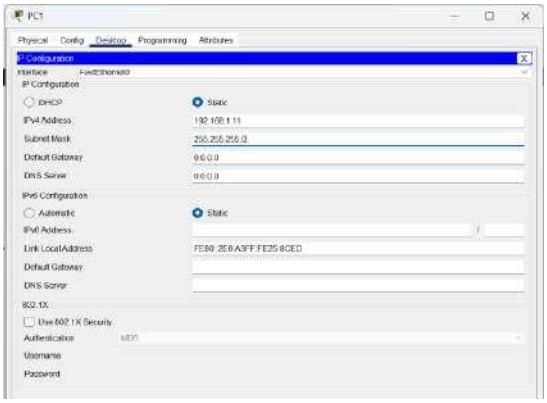


CONFIGURATION:

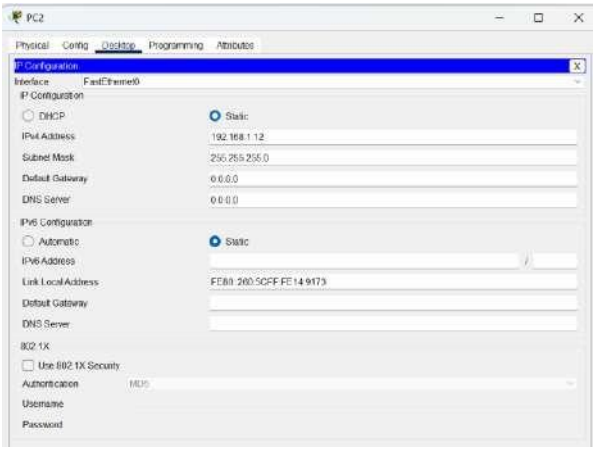
PC0 IP Configuration



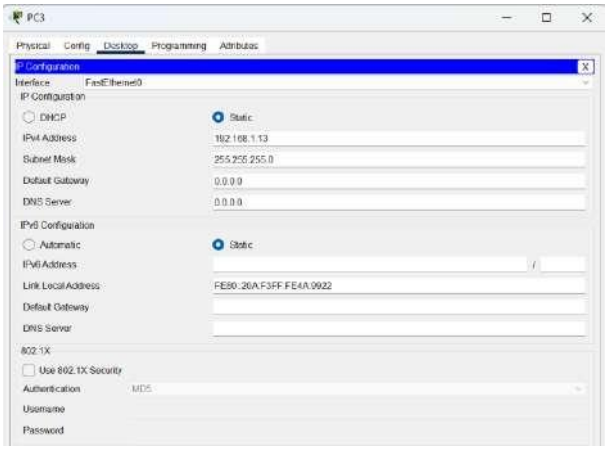
PC1 IP Configuration



PC2 IP Configuration



PC3 IP Configuration



Switch0 Configuration

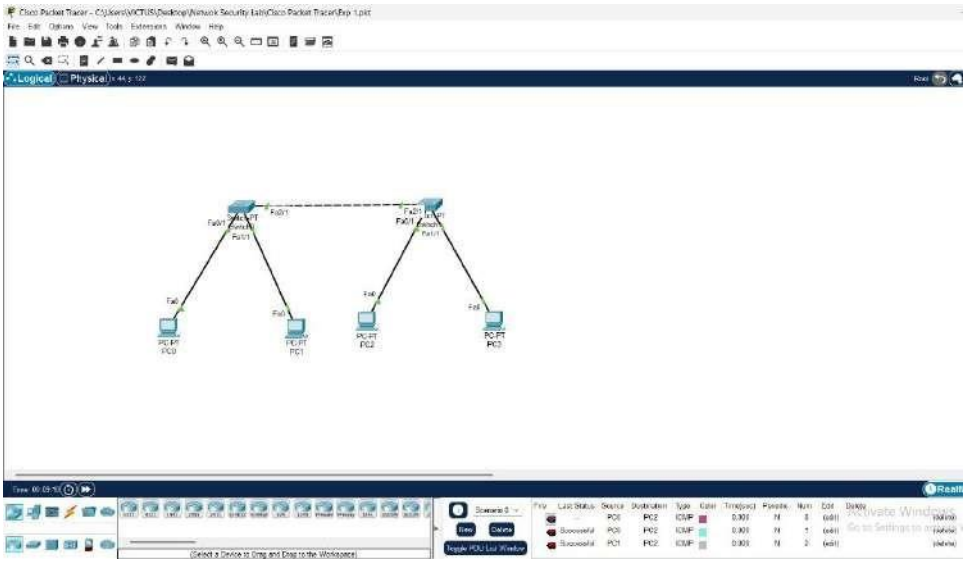
Switch>en

```
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#int vlan1
S1(config-if)#ip address 10.0.0.1 255.0.0.0
S1(config-if)#no shut
```

Switch1 Configuration

```
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#int vlan1
S2(config-if)#ip address 10.0.0.2 255.0.0.0
S2(config-if)#no shut Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#spanning-tree vlan 1 priority 8192
Switch(config)#int fa0/1
Switch(config-if)#spanning-tree vlan 1 cost 10
```

OUTPUT:



RESULT:

Thus the switch was successfully configured and accessed.

SUBHASH B
727722EUAI063

Ex.No : 2 a

Date :

Configure and analyze IPv4 addressing schemes and subnetting

AIM:

To simulate and configure DHCP Relay in a network so that clients in a different network can obtain IP addresses from a centralized DHCP server.

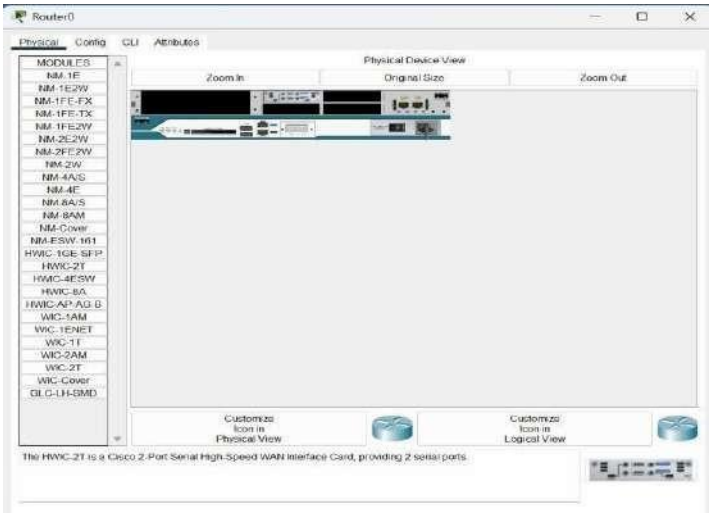
DESCRIPTION:

The IPv4 addressing scheme provides unique logical addresses for devices on a network, enabling communication across LANs and WANs. Subnetting is the process of dividing a large IP network into smaller, manageable subnetworks (subnets) to improve network performance, enhance security, and optimize address usage.

Steps:

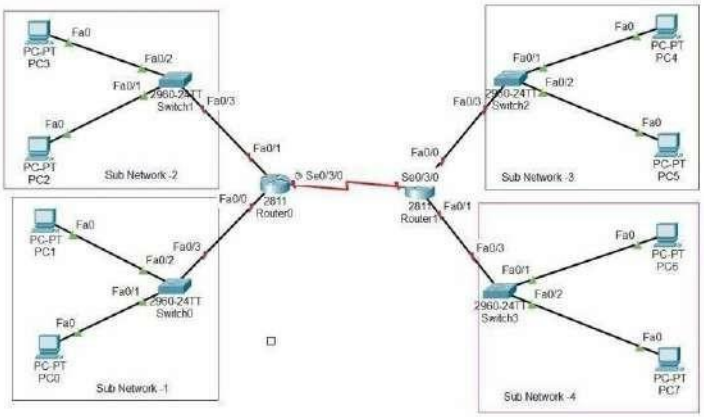
1. Select an IPv4 network (e.g., 192.168.10.0/24).
2. Calculate subnet ranges using subnetting (e.g., divide /24 into four /26 networks).
3. Assign IP addresses to hosts and routers accordingly.
4. Configure interfaces with static IPs.
5. Test connectivity using the ping command.

NETWORK DIAGRAM:



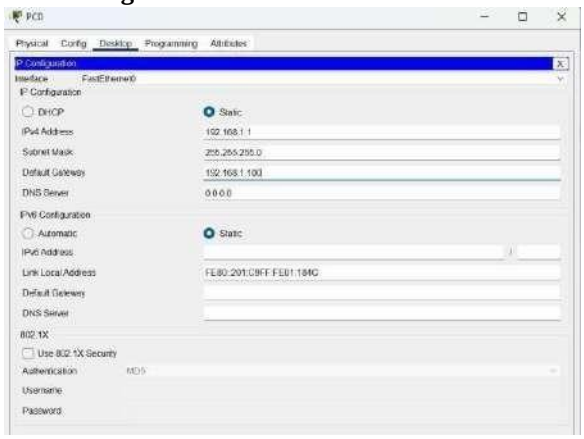
Add Serial Port (WIC-1T) to the Router

SUBHASH B
727722EUAI063

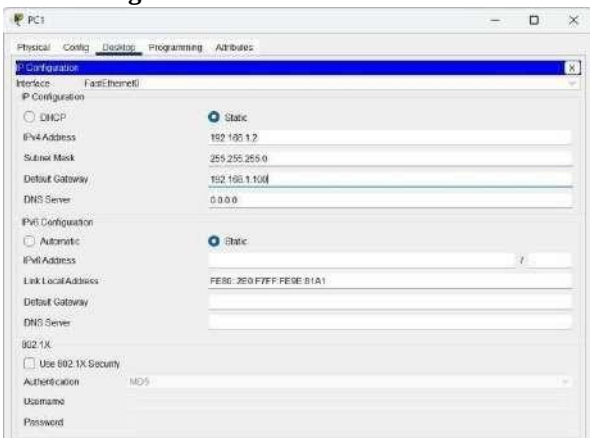


CONFIGURATION:

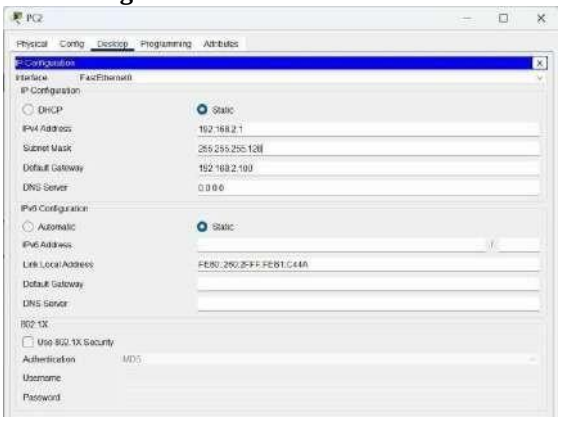
PC0 IP Configuration



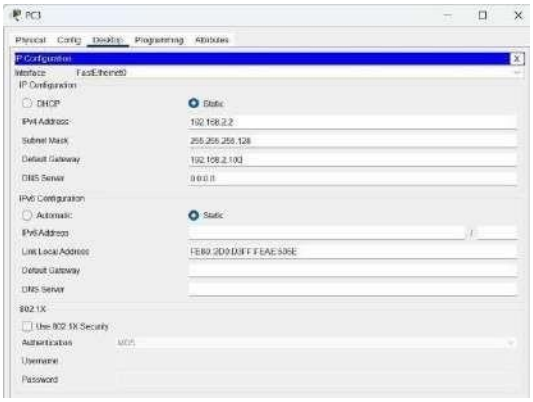
PC1 IP Configuration



PC2 IP Configuration



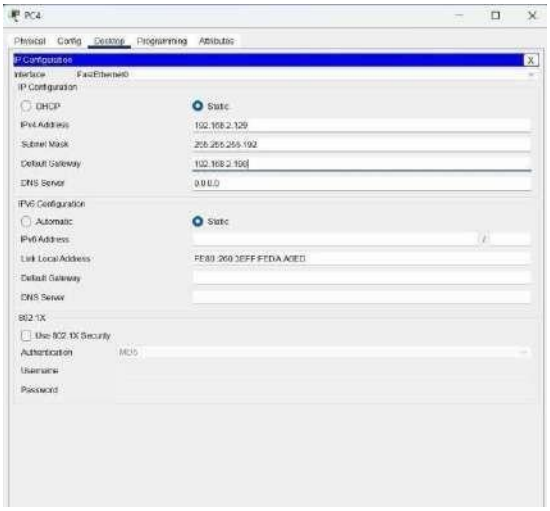
PC3 IP Configuration

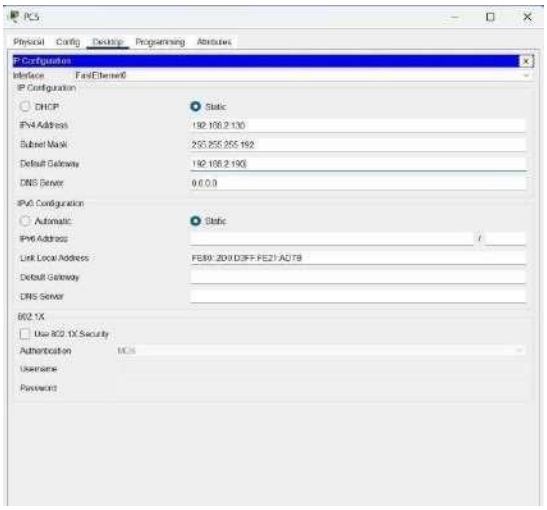


PC4 IP Configuration

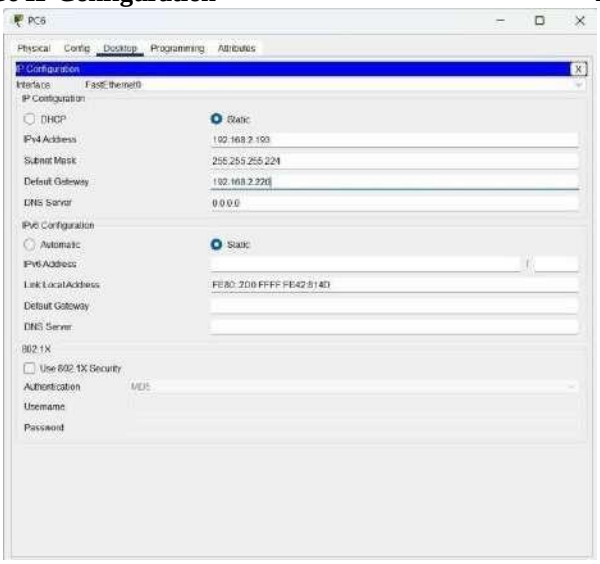
PC5 IP Configuration

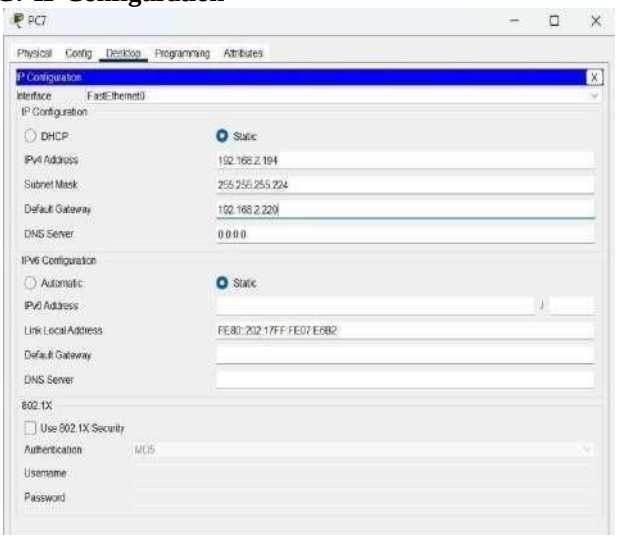
SUBHASH B
727722EUAI063



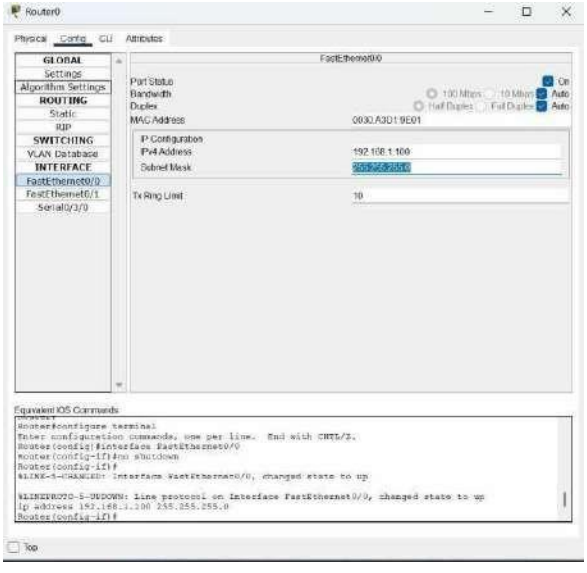


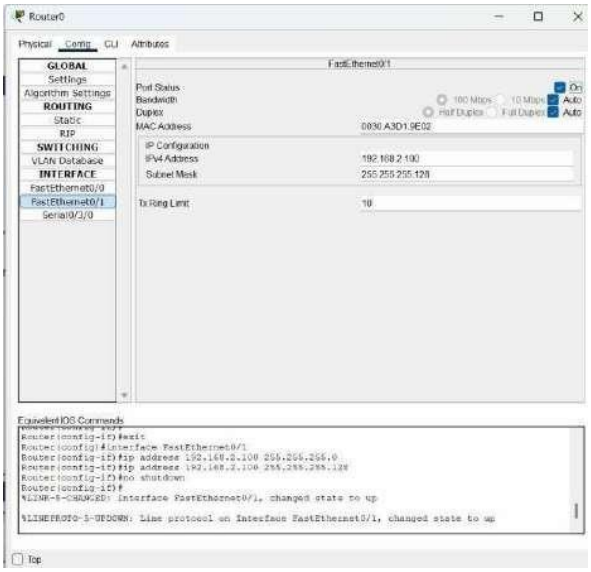
PC6 IP Configuration **PC7 IP Configuration**





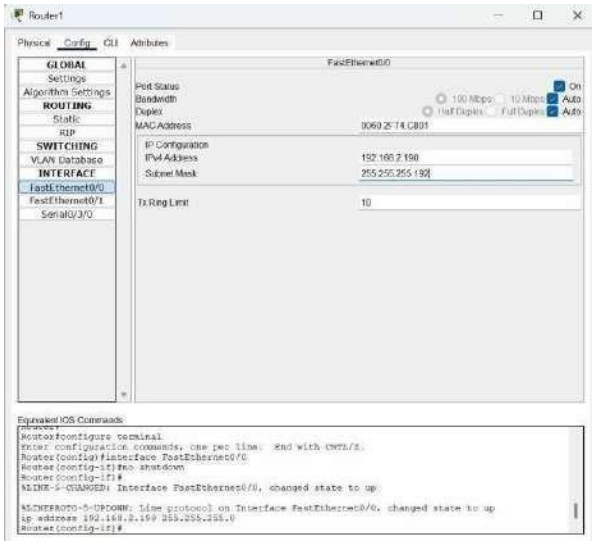
Router0 fa0/0 **Router0 fa0/1**



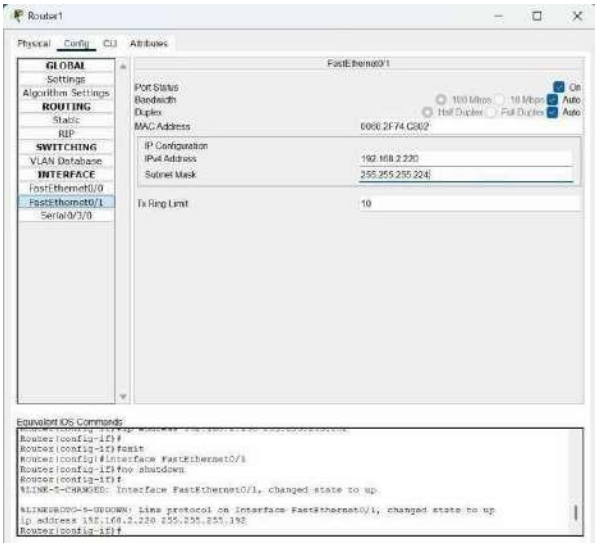


SUBHASH B
727722EUAI063

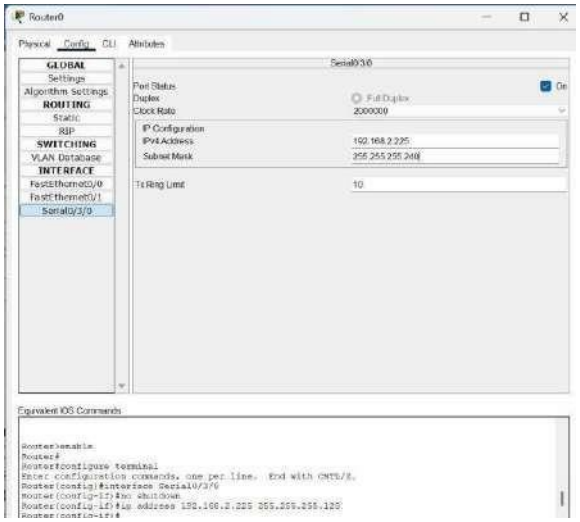
Router1 fa0/0



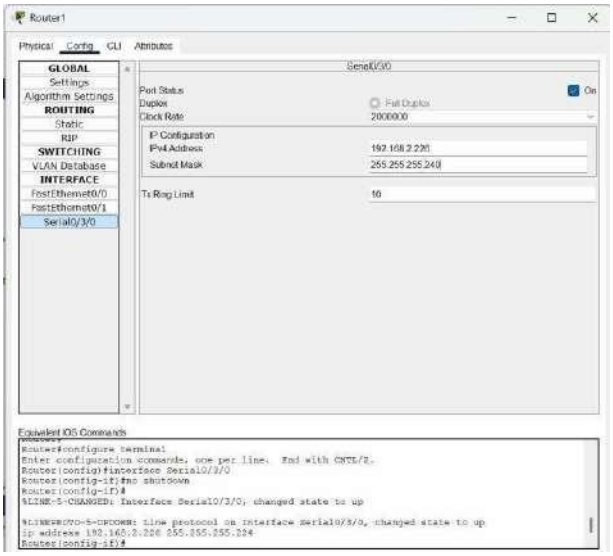
Router1 fa0/1



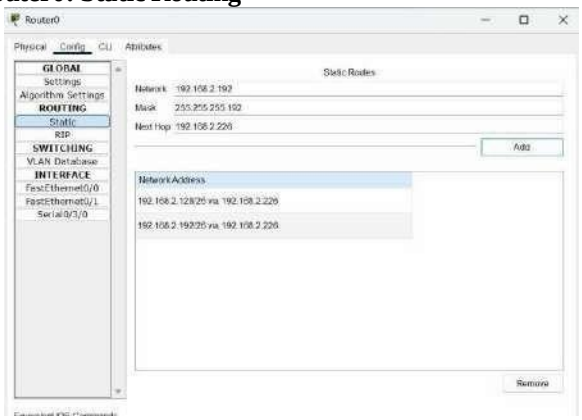
Router0 Serial0/3/0



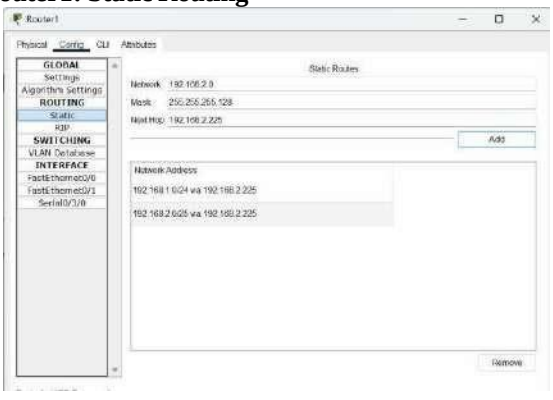
Router1 Serial0/3/0



Router0: Static Routing

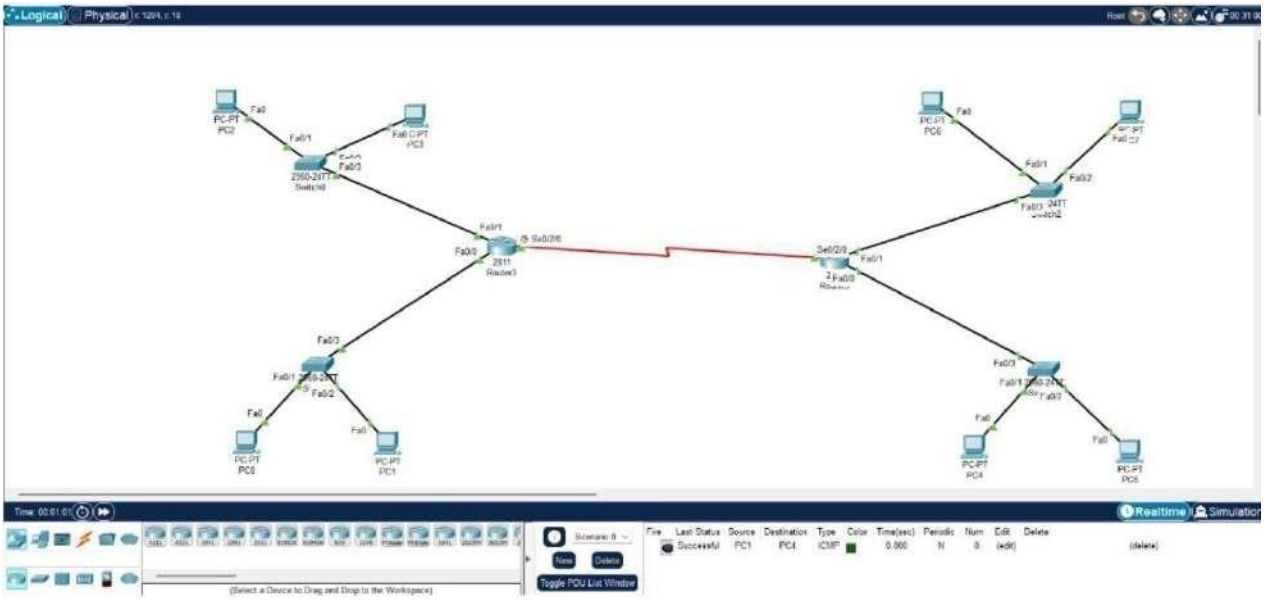


Router1: Static Routing



SUBHASH B
727722EUAI063

OUTPUT:



RESULT:

Thus the IPv4 addressing scheme and subnetting were successfully configured and tested.

SUBHASH B
727722EUAI063

Ex.No : 2 b

Date :

Configure and analyze IPv6 addressing schemes

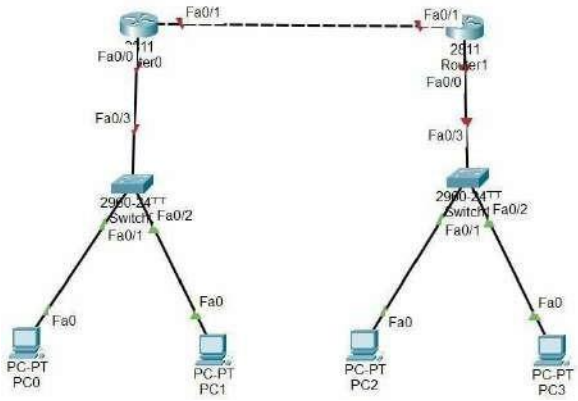
AIM:

To understand, configure, and analyze an IPv6 addressing scheme for devices in a network to enable communication using next-generation Internet Protocol (IPv6).

DESCRIPTION:

IPv6 (Internet Protocol version 6) is the successor to IPv4 and was developed to overcome IPv4 address exhaustion. It uses a 128-bit address, allowing for a vastly larger number of unique IP addresses. IPv6 simplifies network configuration, enhances security, and improves routing efficiency.

NETWORK DIAGRAM:



CONFIGURATION:

Router0 Configuration:

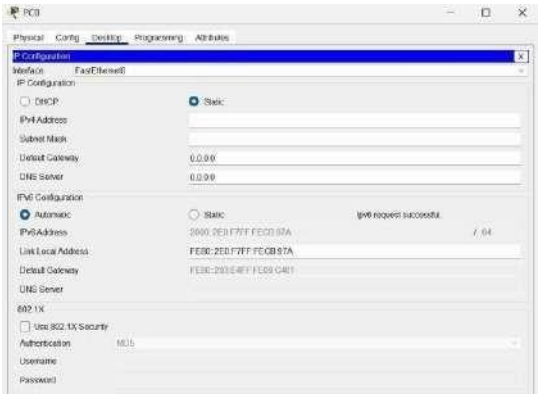
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#int fa0/0
Router(config-if)#ipv6 address 2000::1/64
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

```
Router(config-if)#exit
Router(config)#int fa0/1
Router(config-if)#ipv6 address 2001::1/64
Router(config-if)#no shut
Router(config-if)#exit

Router(config)#ipv6 route 2002::/64 2001::2
```

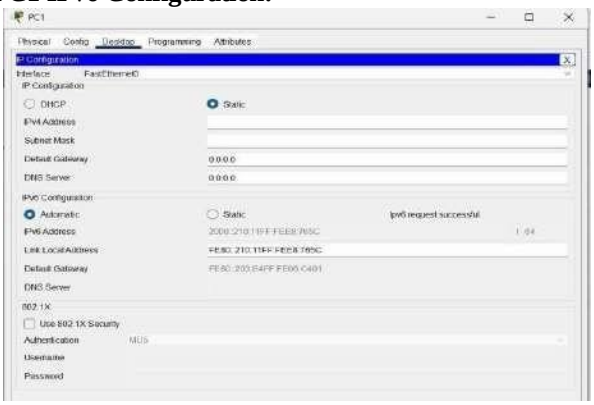
Router1 Configuration

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#int fa0/0
Router(config-if)#ipv6 address 2002::1/64
Router(config-if)#no shut
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)#exit
Router(config)#int fa0/1
Router(config-if)#ipv6 address 2001::2/64
Router(config-if)#no shut       Router(configif)#exit

Router(config)#ipv6 route 2000::/64 2001::1
```

PC0 IPv6 Configuration:



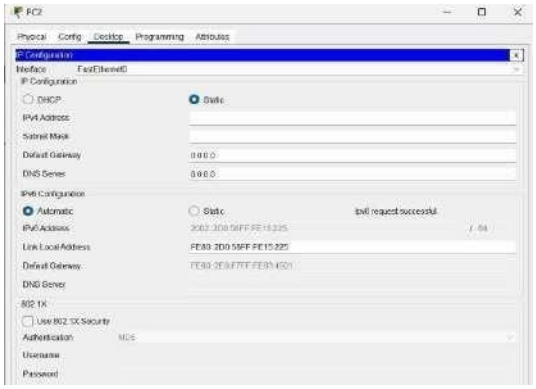
PC1 IPv6 Configuration:

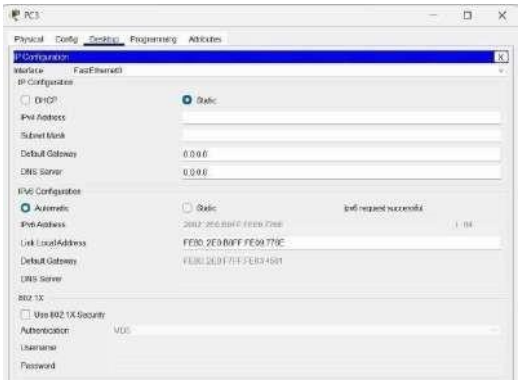


PC2 IPv6 Configuration:

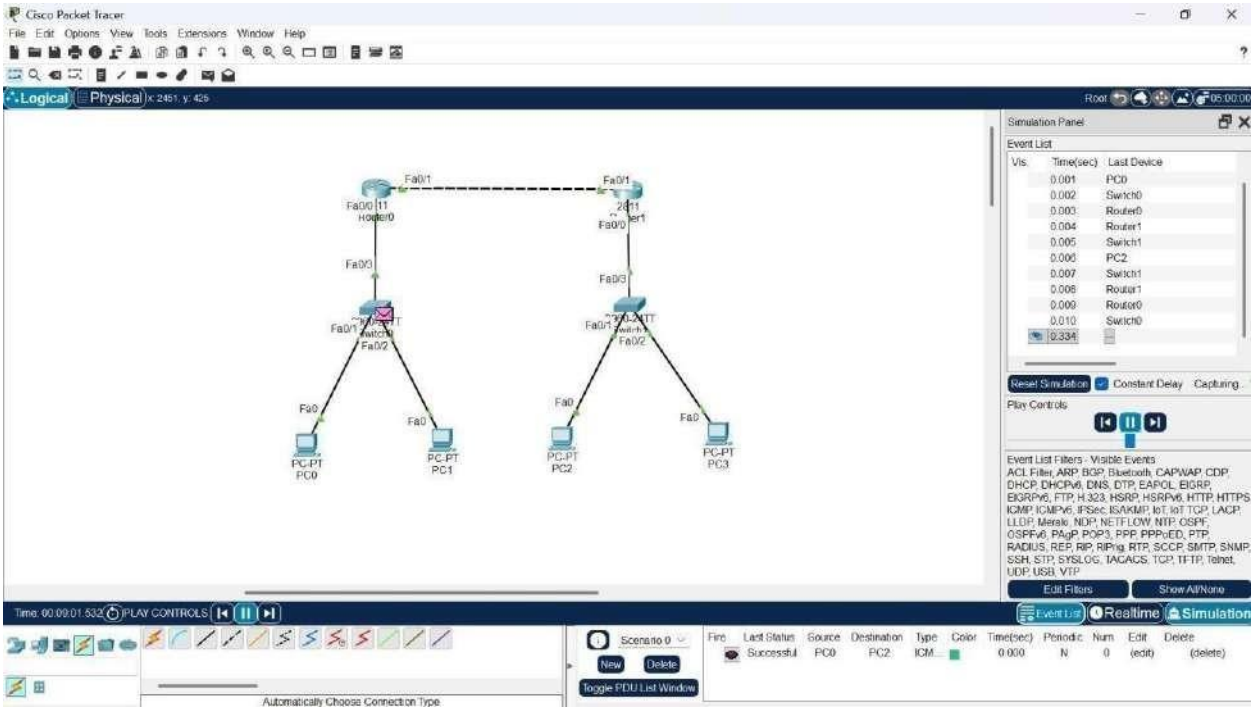
PC3 IPv6 Configuration:

SUBHASH B
727722EUAI063





OUTPUT:



RESULT:

Thus the IPv6 addressing scheme was successfully configured.

SUBHASH B
727722EUAI063

Ex.No : 3

Date :

Design and simulate VLAN configuration with inter-VLAN routing and static IP routing

AIM:

To design and simulate a network using VLANs, configure inter-VLAN routing, and establish static IP routing between multiple networks.

DESCRIPTION:

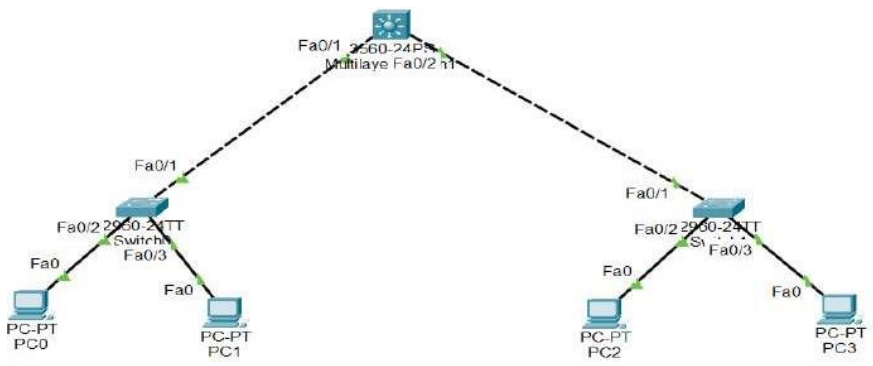
VLAN:

Virtual Local Area Networks (VLANs) are used to logically segment a LAN into multiple broadcast domains, improving network performance and security. The multiple VLANs are created on a Layer-2 switch, and devices are assigned to different VLANs. Since devices in different VLANs cannot communicate directly, inter-VLAN routing is configured using a Layer-3 device (Router-on-a-Stick or Layer-3 Switch).Additionally, static routing is implemented to enable communication between different networks or routers in the topology.

Steps:

- Create VLANs on the switch (e.g., VLAN 10, VLAN 20).
- Assign switch ports to the corresponding VLANs.
- Configure trunking between the switch and router (or Layer-3 switch).
- Set up sub-interfaces on the router for each VLAN with IP addresses (Router-on-a-Stick).
- Configure static routes between networks if multiple routers are used.
- Verify communication using the ping command between hosts in different VLANs.

NETWORK DIAGRAM:



SUBHASH B
727722EUAI063

CONFIGURATION:

Switch0 Configuration

```
s1>en
s1#config t
Enter configuration commands, one per line. End with CNTL/Z.
s1(config)#hostname S1
S1(config)#vlan 10
S1(config-vlan)#vlan 20
S1(config)#int fa0/1
S1(config-if)#no shut
S1(config-if)#switchport mode trunk
S1(config-if)#int fa0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#no shut
S1(config-if)#int fa0/3
S1(config-if)#no shut
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
```

Switch1 Configuration

```
s2>en
s2#config t
Enter configuration commands, one per line. End with CNTL/Z.
s2(config)#hostname S2
S2(config)#vlan 20
S2(config-vlan)#vlan 10
S2(config-vlan)#int fa0/1
S2(config-if)#no shut
S2(config-if)#switchport mode trunk
S2(config-if)#int fa0/2
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#int fa0/3
S2(config-if)#no shut
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
```

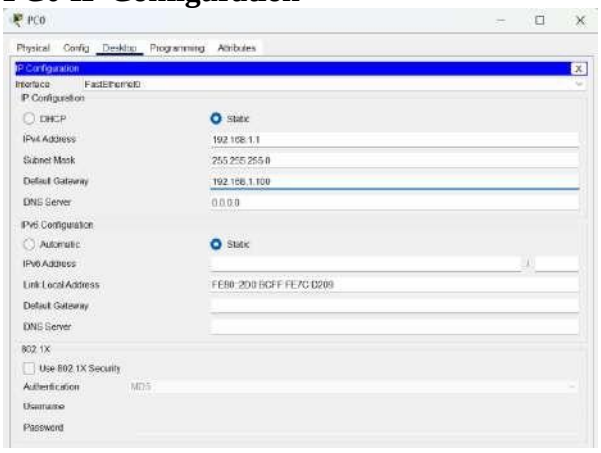
Multilayer Switch Configuration

```
L3_switch>en
L3_switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
L3_switch(config)#hostname L3_switch
L3_switch(config)#ip routing
```

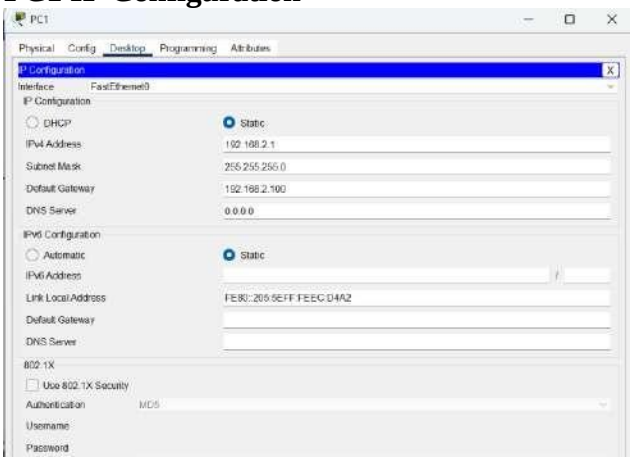
SUBHASH B
727722EUAI063

```
L3_switch(config)#vlan 10
L3_switch(config-vlan)#vlan 20
L3_switch(config-vlan)#int vlan 10
L3_switch(config-if)#ip address 10.1.1.1 255.255.255.0
L3_switch(config-if)#no shut
L3_switch(config-if)#int vlan 20
L3_switch(config-if)#ip address 20.1.1.1 255.255.255.0
L3_switch(config-if)#no shut
```

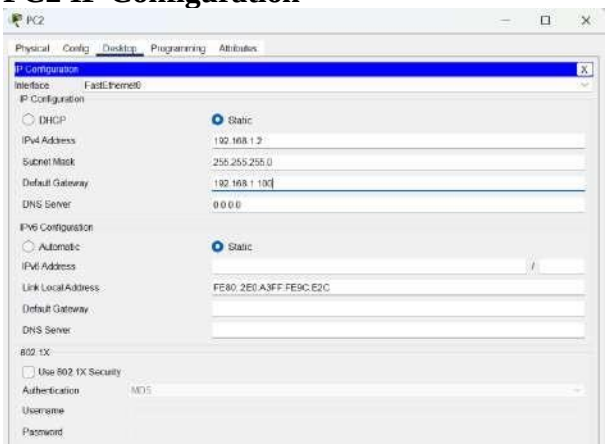
PC0 IP Configuration



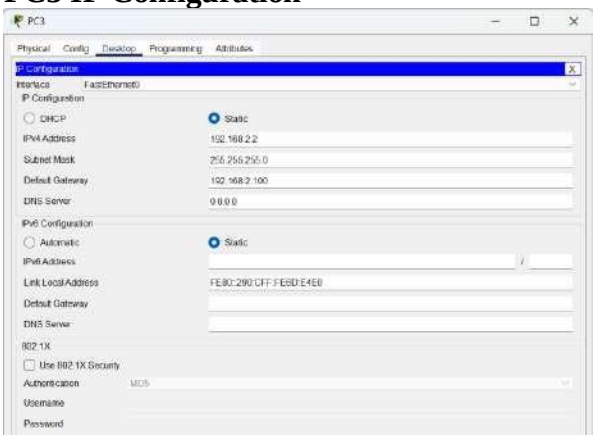
PC1 IP Configuration



PC2 IP Configuration

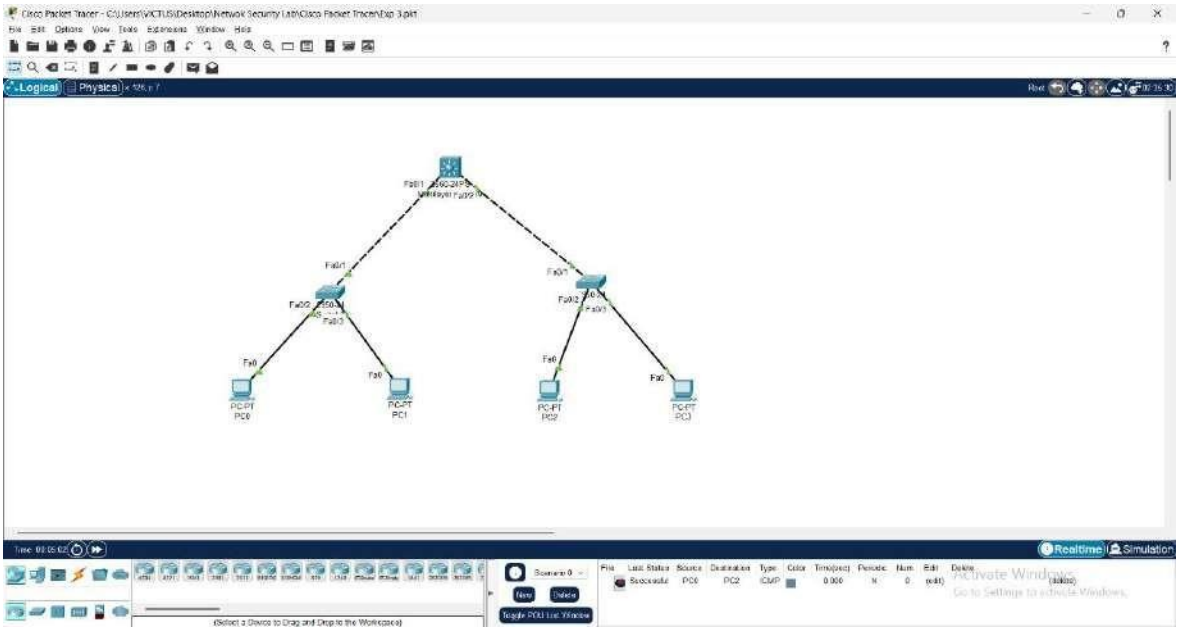


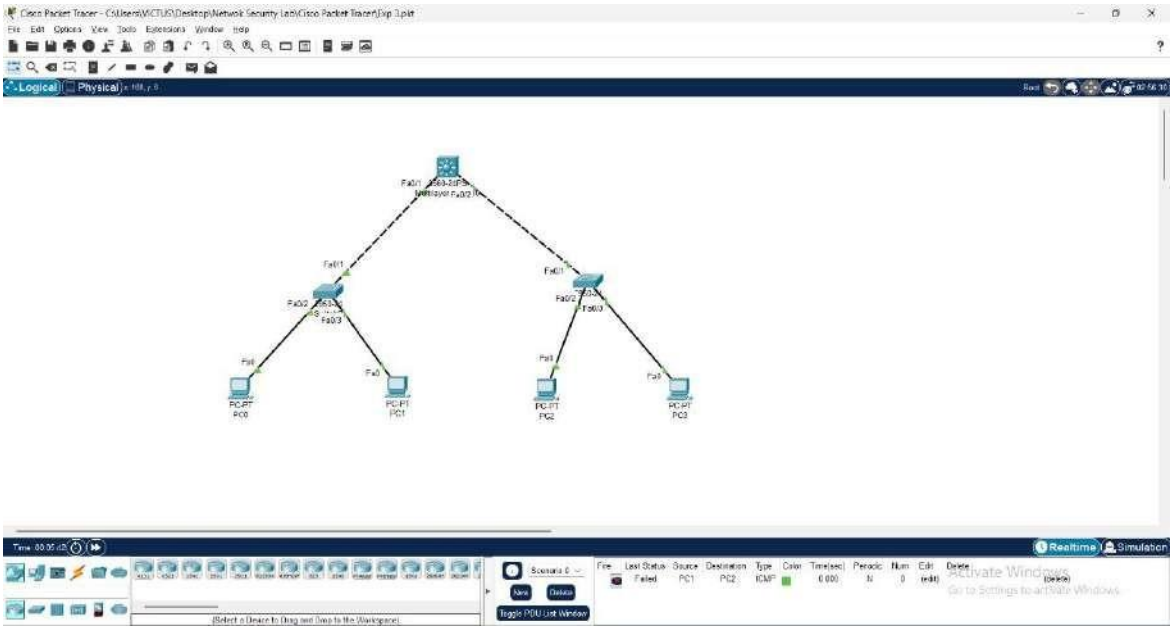
PC3 IP Configuration



SUBHASH B
727722EUAI063

OUTPUT:





RESULT:

Thus the VLANs were successfully created, and inter-VLAN communication was achieved through the configured router (or Layer-3 switch).

SUBHASH B
727722EUAI063

Ex.No : 4 a

Date :

Simulate DHCP relay using Cisco Packet Tracer

AIM:

To simulate and configure DHCP Relay in a network so that clients in a different network can obtain IP addresses from a centralized DHCP server.

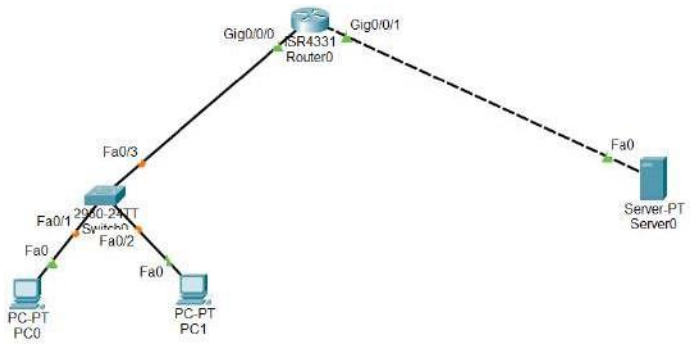
DESCRIPTION:

The Dynamic Host Configuration Protocol (DHCP) automates the assignment of IP addresses and other network parameters to hosts. However, by default, DHCP operates only within the local broadcast domain. When a client and DHCP server are on different networks, the DHCP broadcast cannot cross routers. To overcome this limitation, a DHCP Relay Agent is configured on the router interface connected to the client network. This relay agent forwards DHCP requests from clients to the remote DHCP server and relays the server's responses back to the clients.

Steps:

1. Configure IP addresses on all router interfaces.
2. Set up a DHCP server on one network with a defined IP pool.
3. Enable the **ip helper-address** command on the router interface of the client network to relay DHCP requests.
4. Connect a DHCP client (e.g., PC) in another network and verify it receives an IP address automatically.

NETWORK DIAGRAM:



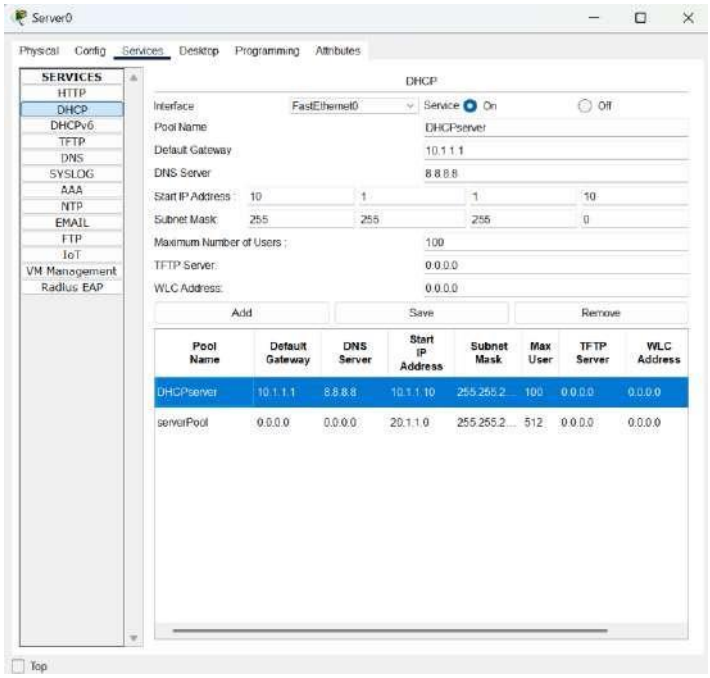
SUBHASH B
727722EUAI063

CONFIGURATION:

Router Configuration:

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int gig0/0/0
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#int gig0/0/1
Router(config-if)#ip address 20.1.1.1 255.255.255.0
Router(config-if)#ip helper-address 20.1.1.2
```

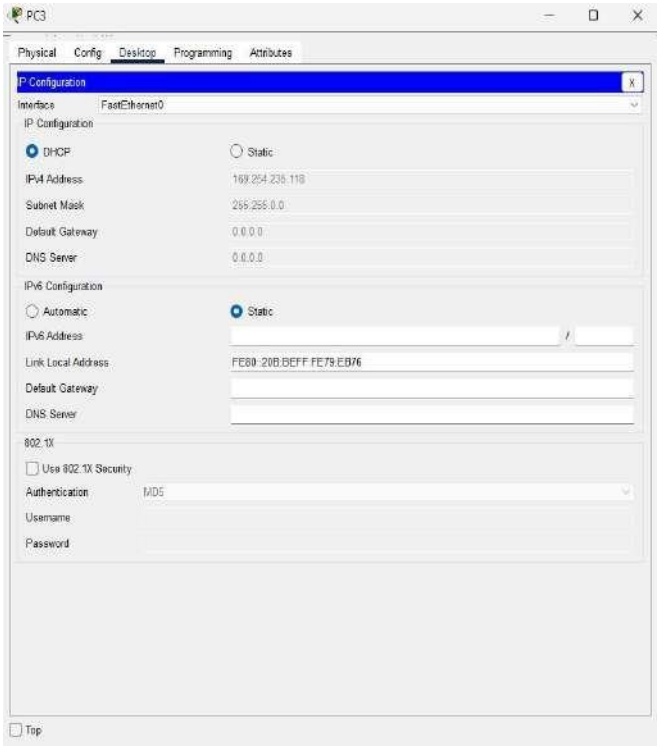
DHCP Server

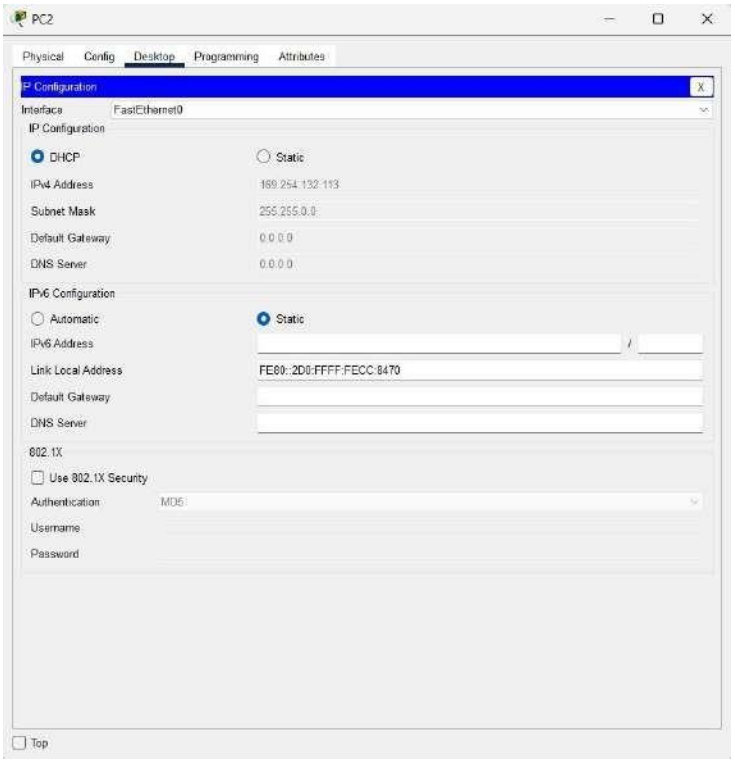


Click Server -> Services
Service -> Turn ON
PoolName -> DHCPServer
Default Gateway -> 10.1.1.1
DNS Server -> 8.8.8.8
Start IP Address -> 10.1.1.10
Subnet Mask -> 255.255.255.0
Maximum Number of Users -> 100
Click Save

SUBHASH B
727722EUAI063

OUTPUT:





RESULT:

Thus the DHCP Relay Agent was successfully configured.

SUBHASH B
727722EUAI063

Ex.No : 4 b

Date :

Basic VoIP Setup

AIM:

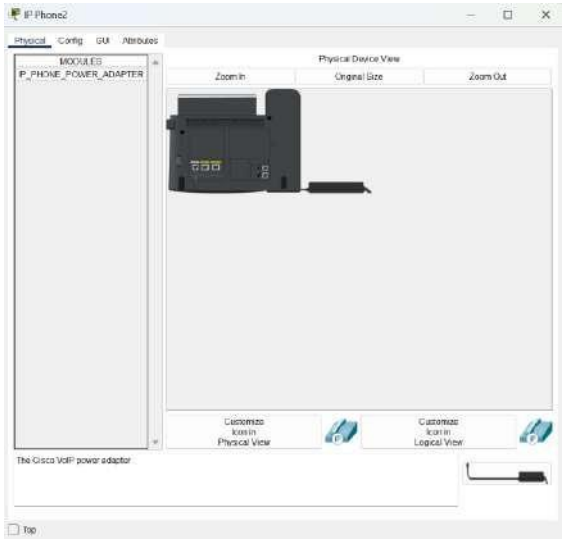
To configure a basic Voice over Internet Protocol (VoIP) network to enable voice communication between IP phones.

DESCRIPTION:

VoIP (Voice over Internet Protocol) allows voice communication to be transmitted over an IP network instead of traditional telephone lines. A basic VoIP setup is created using network devices such as routers and switches configured with telephony services. Each IP phone (or softphone) is assigned an extension number and registered with the VoIP server. Once configured, users can make calls between IP phones using these extensions.

Steps:

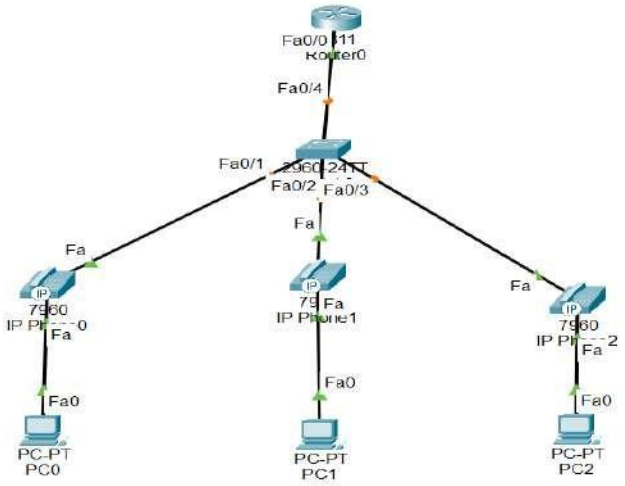
1. Configure IP addressing on routers and switches.
2. Enable telephony service on the router (if using Cisco Packet Tracer).
3. Assign extension numbers to each IP phone.
4. Connect IP phones to the switch and ensure they obtain IP addresses.
5. Test calling between IP phones using the assigned extensions.



Power ON IP Phone using Power Cord cable.

SUBHASH B
727722EUAI063

NETWORK DIAGRAM:



CONFIGURATION:

Router Configuration:

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ip dhcp pool voice
Router(dhcp-config)#network 192.168.10.1 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#option 150 ip 192.168.10.1
Router(dhcp-config)#telephony-service
Router(config-telephony)#max-dn 5
Router(config-telephony)#max-ephones 5
Router(config-telephony)#ip source-address 192.168.10.1 port 2000
Router(config-telephony)#auto assign 1 to 5
Router(config-telephony)#ephone-dn 1
Router(config-ephone-dn)#number 1001
Router(config-ephone-dn)#ephone-dn 2
Router(config-ephone-dn)#number 1002
Router(config-ephone-dn)#ephone-dn 3
Router(config-ephone-dn)#number 1003
```

Switch Configuration

```
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
```

SUBHASH B
727722EUAI063

```
Switch(config)#int range fa0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 1
```

OUTPUT:

RESULT:

Thus the basic VoIP network was successfully configured.

SUBHASH B
727722EUAI063

Ex.No : 5

Date :

Configure STP (Spanning Tree Protocol) and analyze redundancy in network switches

AIM:

To configure the Spanning Tree Protocol (STP) on network switches and analyze the redundancy and loop prevention mechanism in a switched network.

DESCRIPTION:

STP:

In a switched network, redundant paths are often created to ensure network fault tolerance and high availability. However, these redundant links can cause switching loops, leading to broadcast storms and MAC table instability.

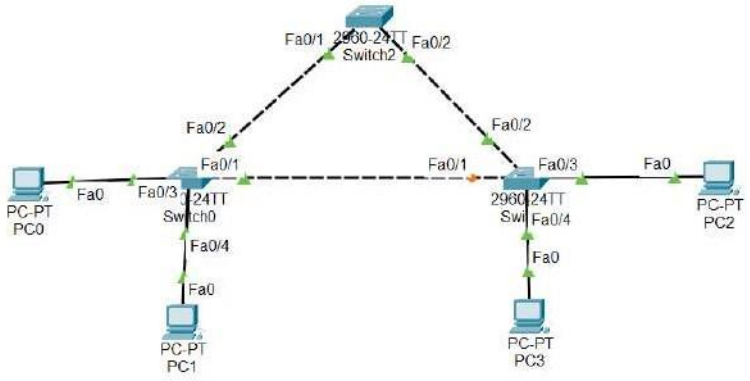
To prevent such issues, Spanning Tree Protocol (STP) is implemented. STP identifies the most efficient path between switches and blocks redundant links until they are needed (in case of a link failure).

Key STP Concepts:

- **Root Bridge:** The central switch chosen based on the lowest Bridge ID (priority + MAC address).
- **Root Port (RP):** The port on a non-root switch with the least cost path to the root bridge.
- **Designated Port (DP):** The forwarding port on a network segment with the lowest cost to the root.
- **Blocked Port:** A port that is not used for forwarding to prevent loops.

NETWORK DIAGRAM:

SUBHASH B
727722EUAI063



CONFIGURATION:

Switch0 Configuration

Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S0
S0(config)#spanning-tree mode rapid-pvst
S0(config)#spanning-tree vlan 1 root primary

S0(config)#int range fa0/1-2
S0(config-if-range)#spanning-tree portfast

Switch1 Configuration

Switch>
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#spanning-tree vlan 1 priority 8192
Switch(config)#int fa0/1
Switch(config-if)#spanning-tree vlan 1 cost 10

Switch1 Configuration

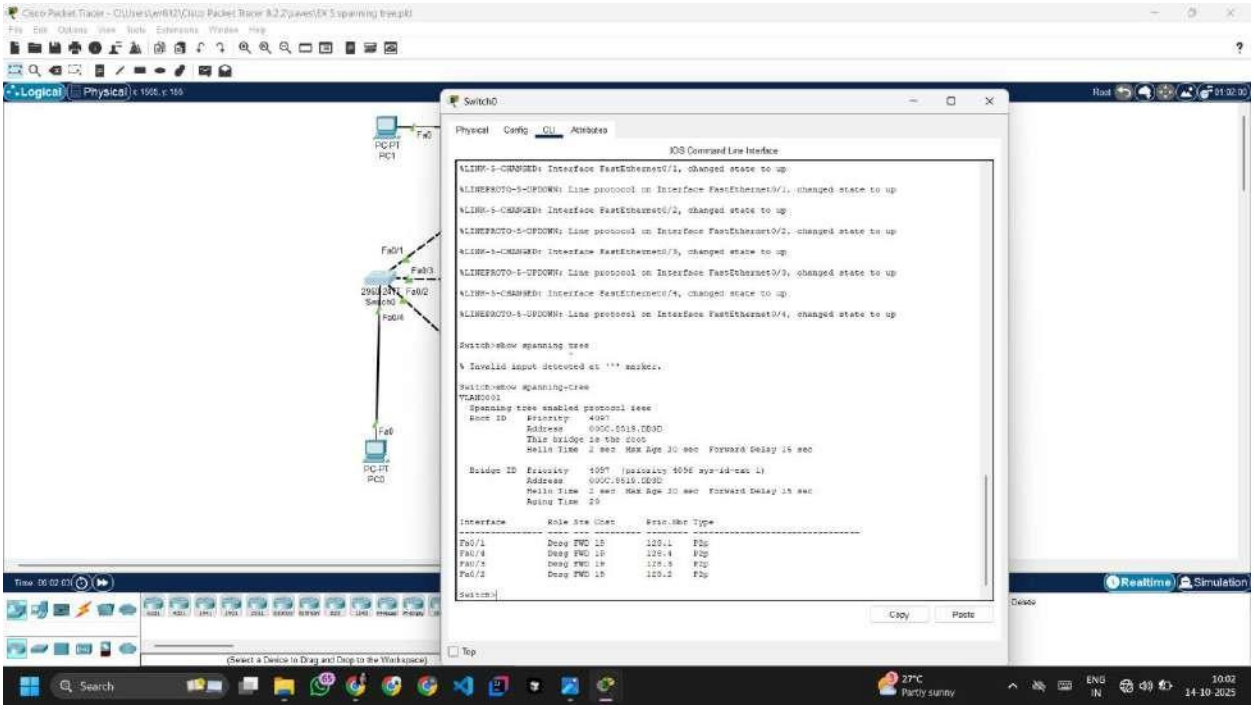
Switch>
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#spanning-tree vlan 1 priority 32768
Switch(config)#int fa0/1

SUBHASH B
727722EUAI063

Switch(config-if)#spanning-tree vlan 1 cost 10

OUTPUT:

Show Spanning-tree



RESULT:

Thus the Spanning Tree Protocol was successfully configured on the switches. The network automatically elected a Root Bridge, identified redundant paths, and blocked one port to prevent loops.

SUBHASH B
727722EUAI063

Ex.No : 6

Date :

Setup and test VRRP using GNS3

AIM:

To configure and verify VRRP (Virtual Router Redundancy Protocol) in GNS3 to provide default gateway redundancy and ensure network availability during a router failure.

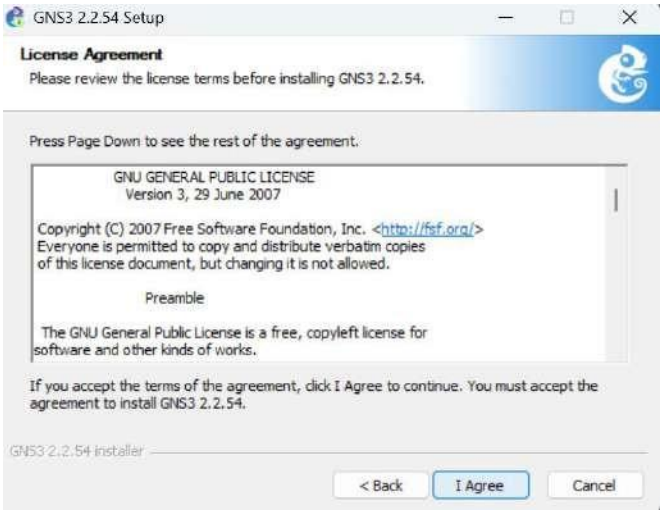
DESCRIPTION:

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol that allows multiple routers to share a virtual IP address acting as a default gateway for end devices. One router is elected as the Master, while the others act as Backups. If the Master router fails, a Backup takes over the virtual IP, providing uninterrupted network connectivity.

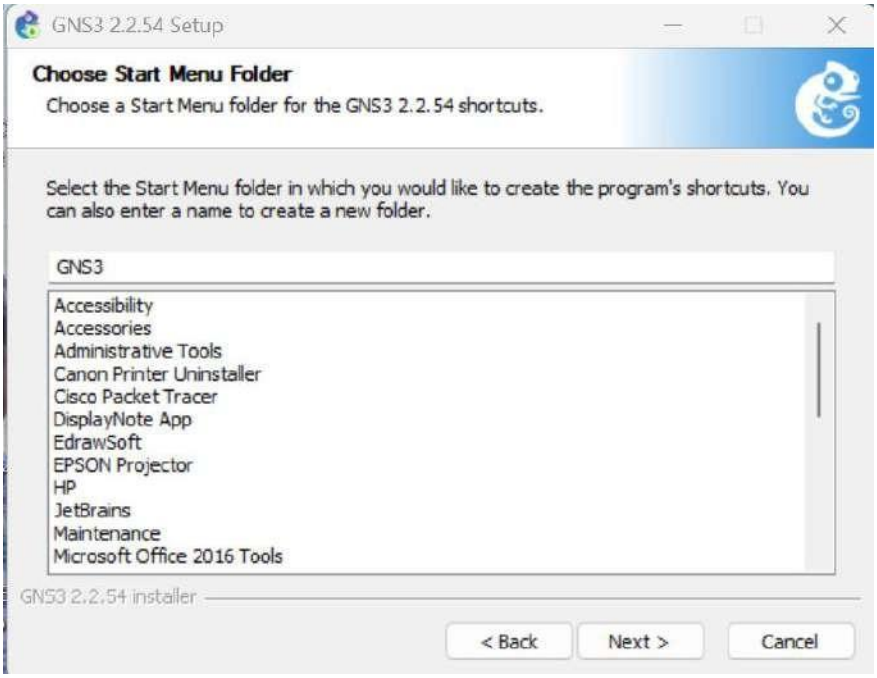
INSTALLATION PROCEDURE:

Link to download: https://gns3.com/software/download

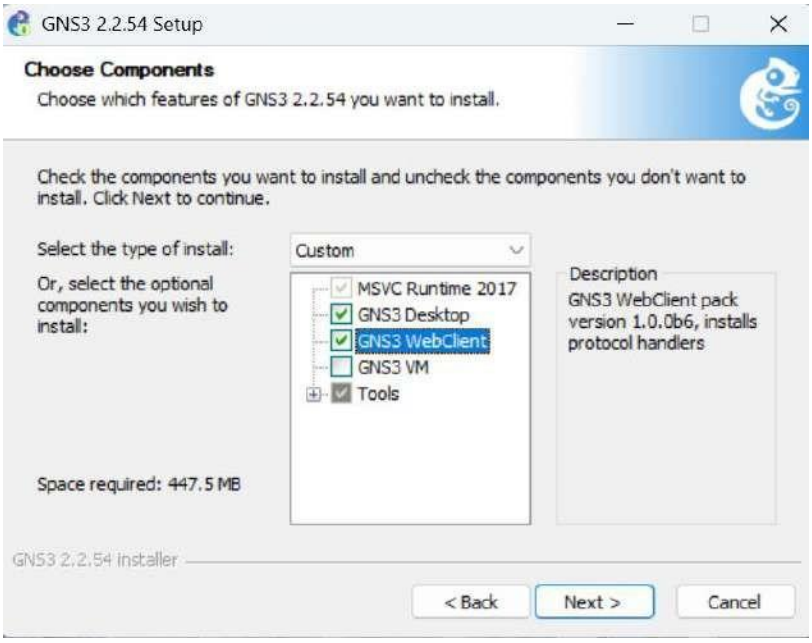
Click Next



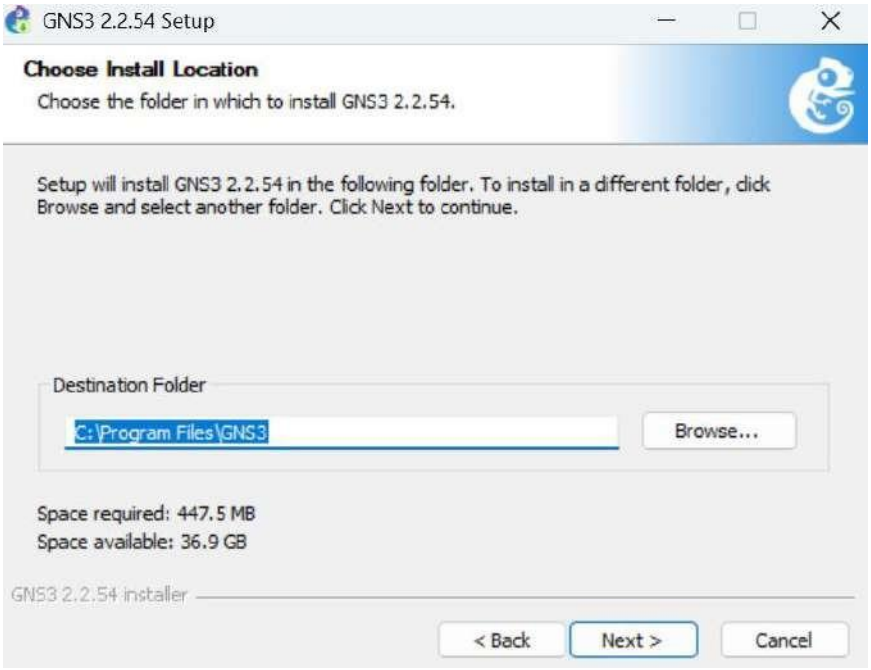
Click I Agree



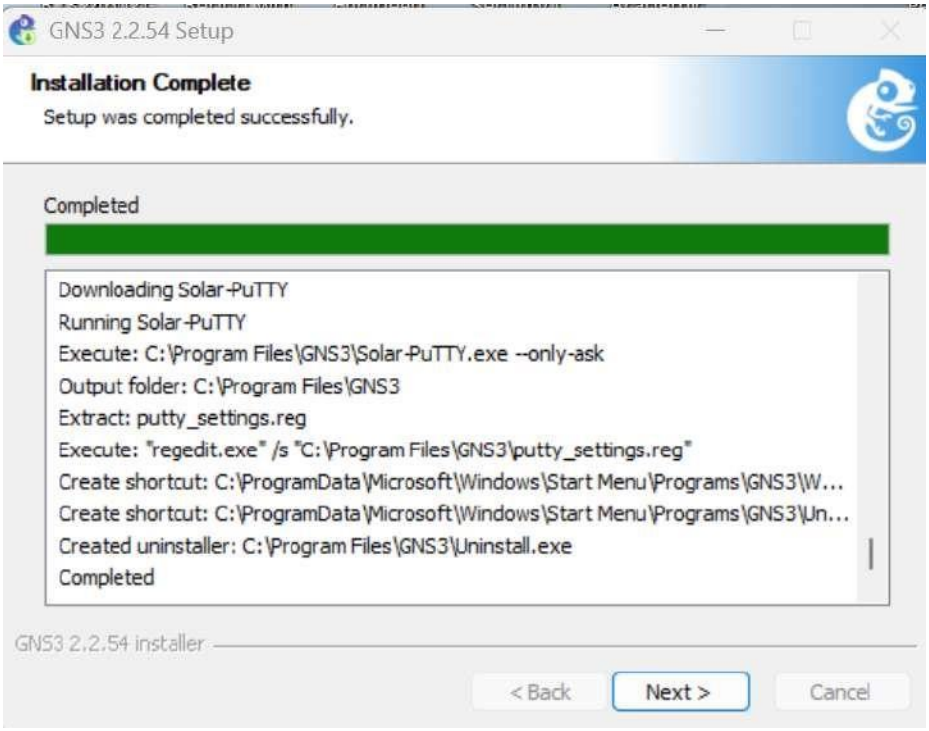
Click Next



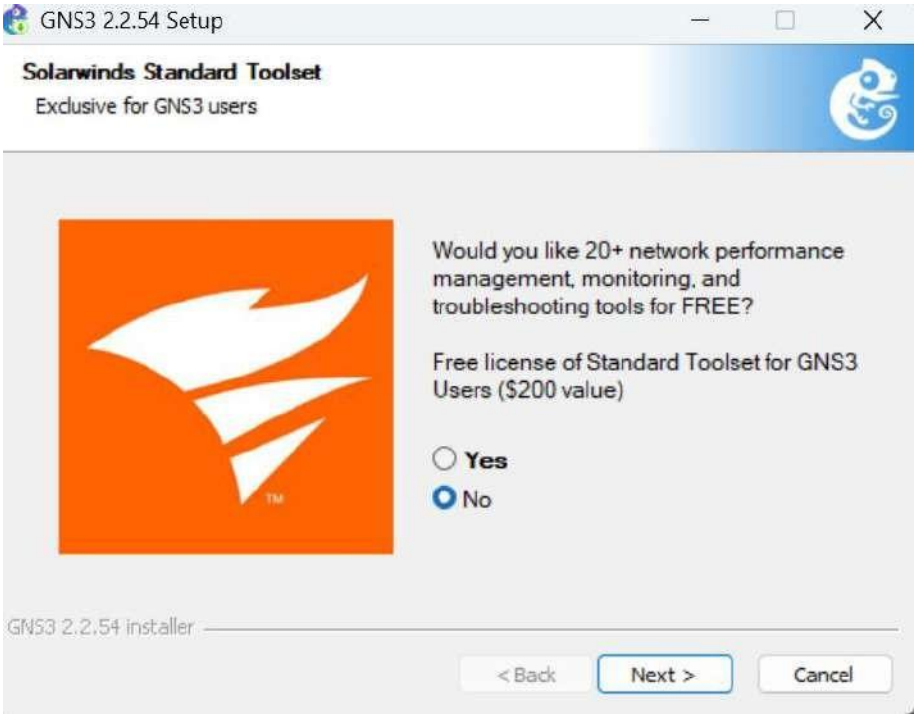
Select GNS3 Desktop and GNS3 WebClient then Click Next



Select Destination Folder and Click Next

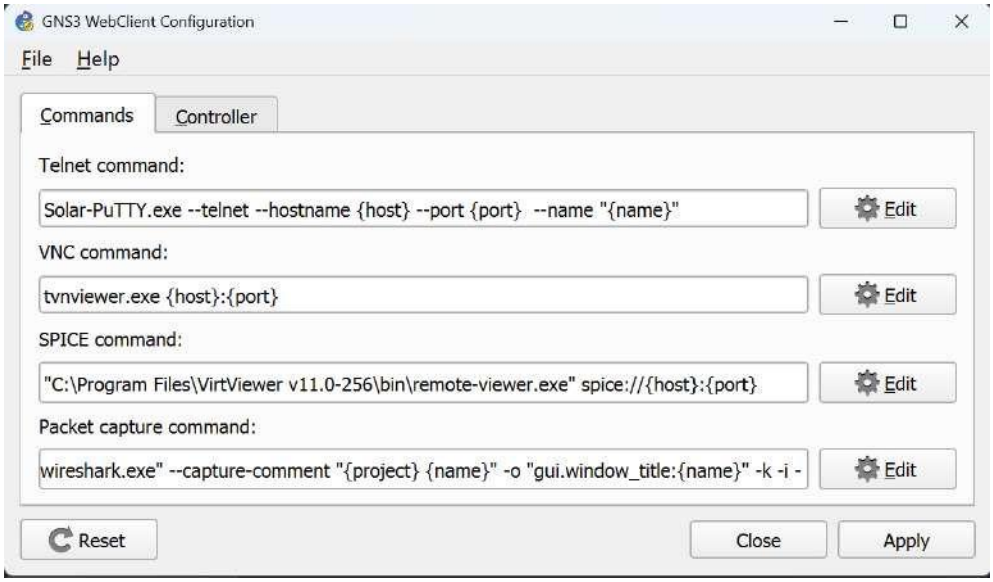


Click Next

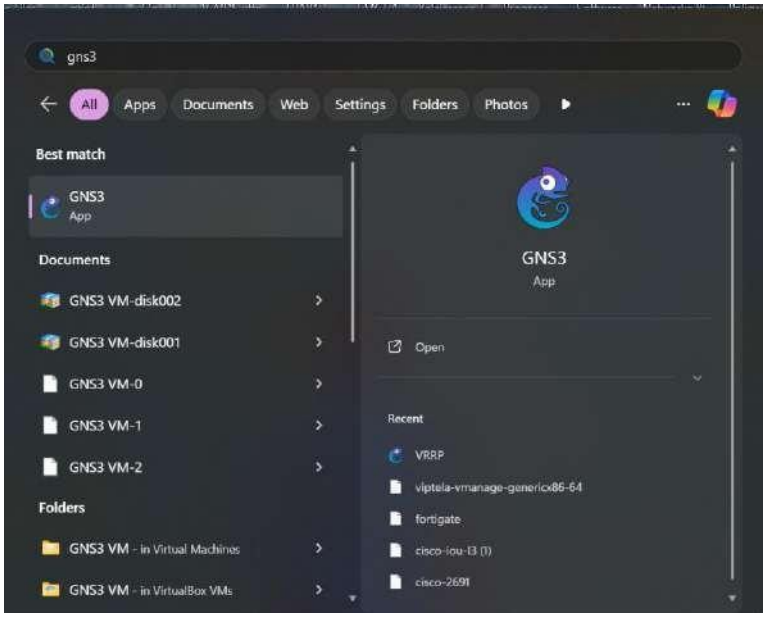


Choose No and Click Next

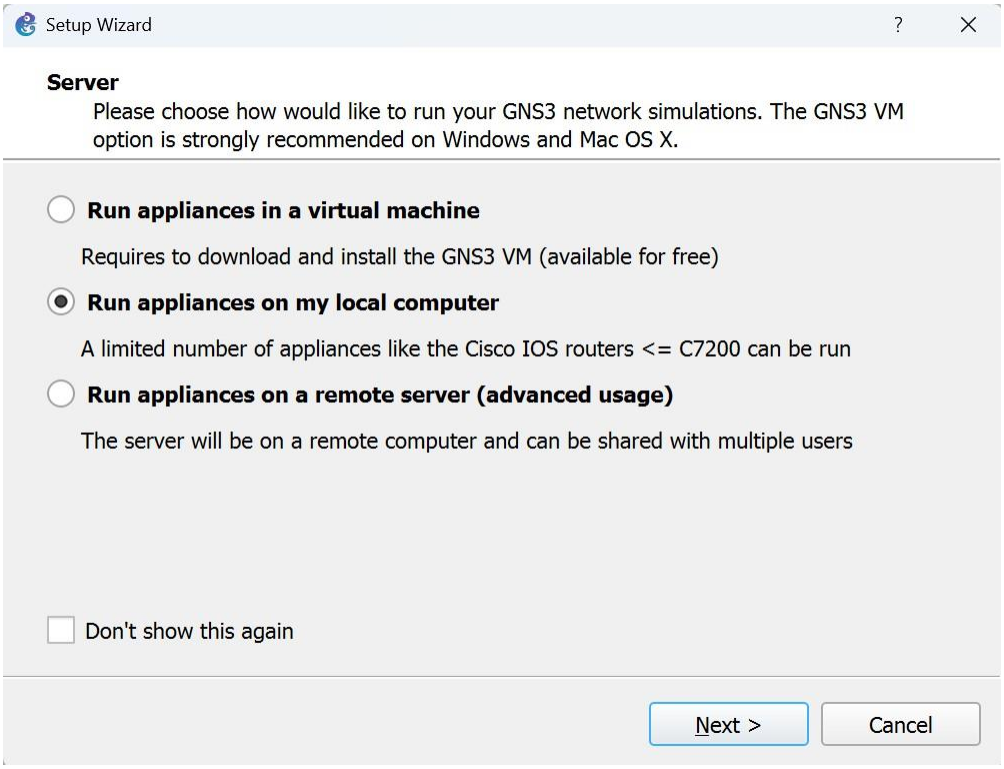
Click Finish



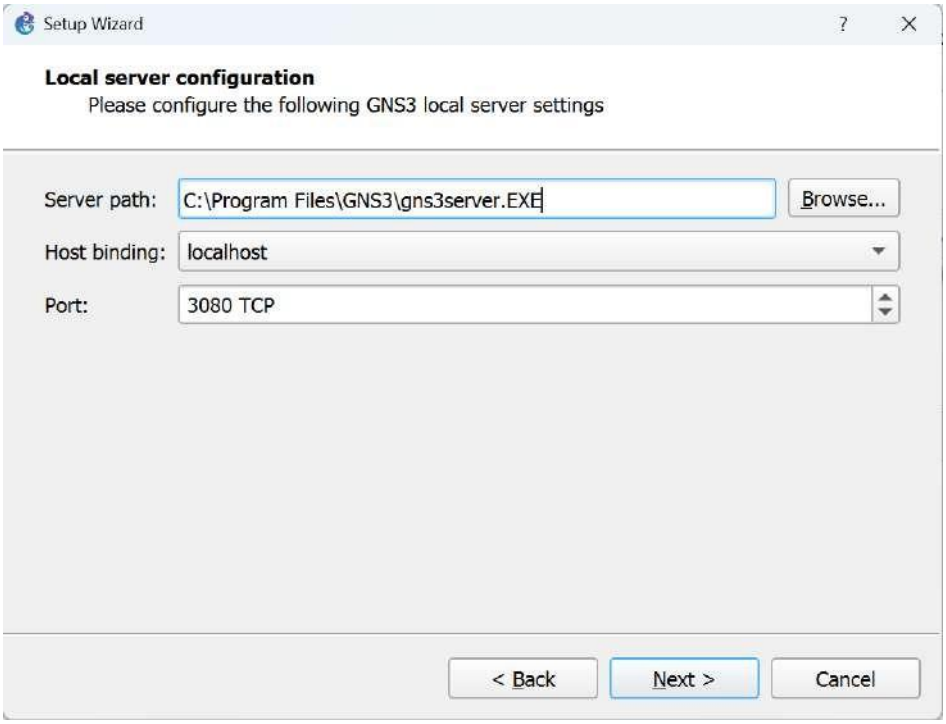
Click Close



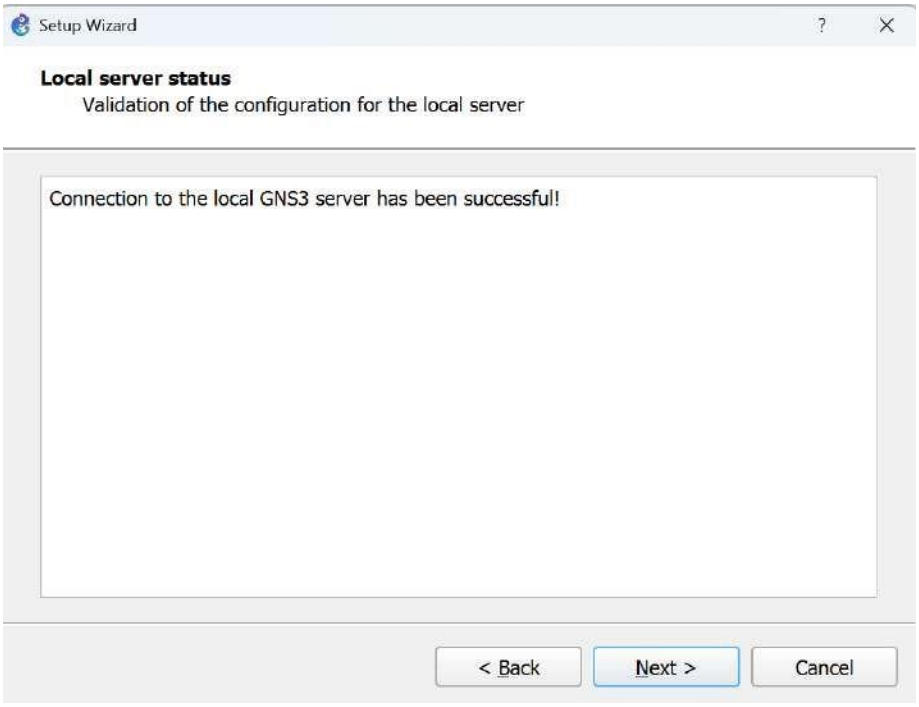
Open GNS3



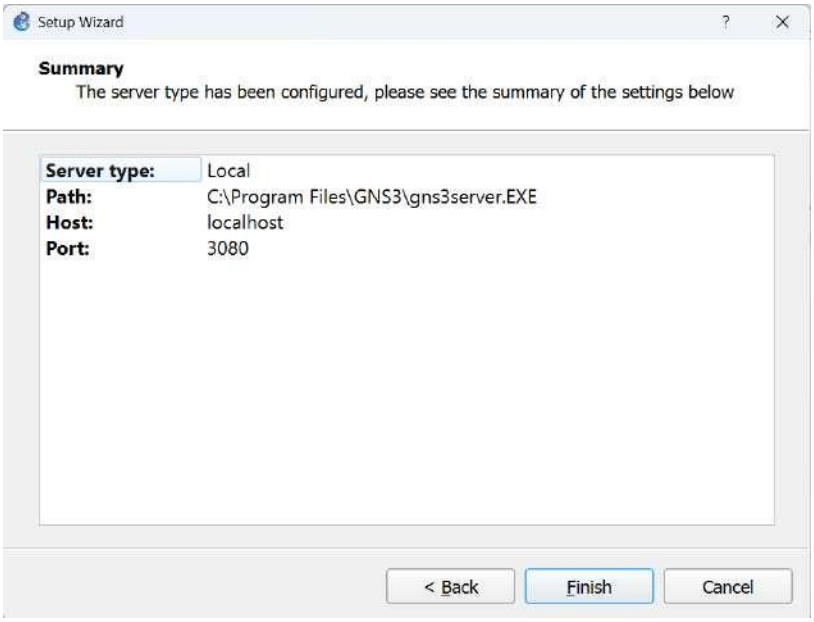
Select Run appliances on my local computer then Click Next



Browser server path and Click Next



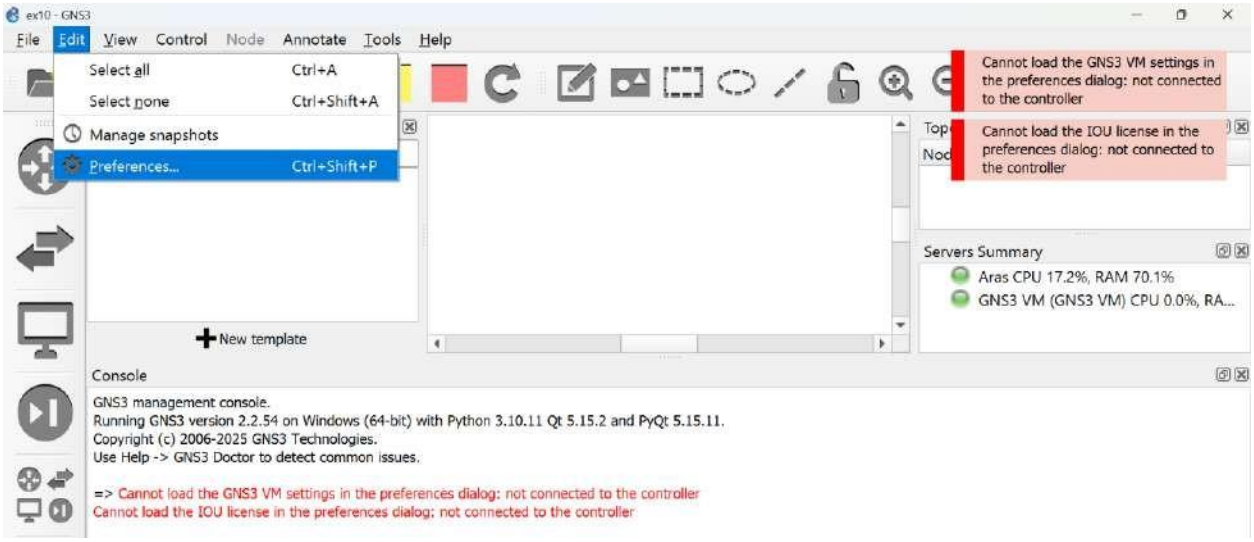
Click Next



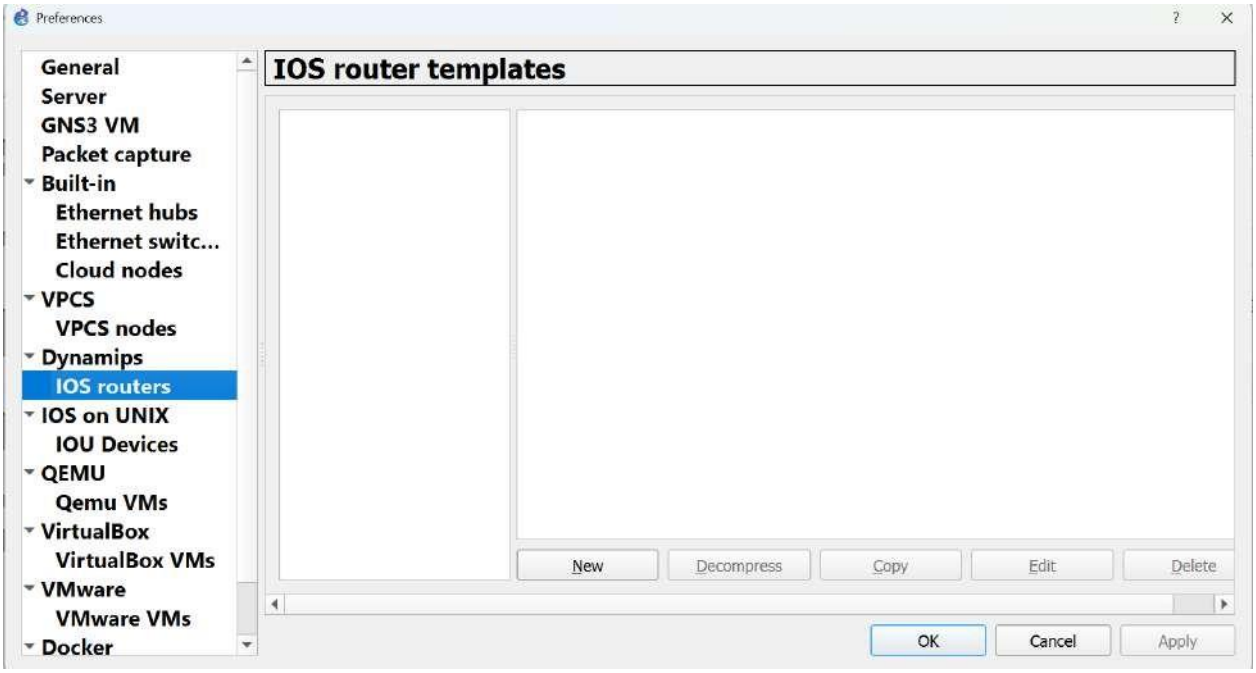
Click Finish

Adding router to gns3

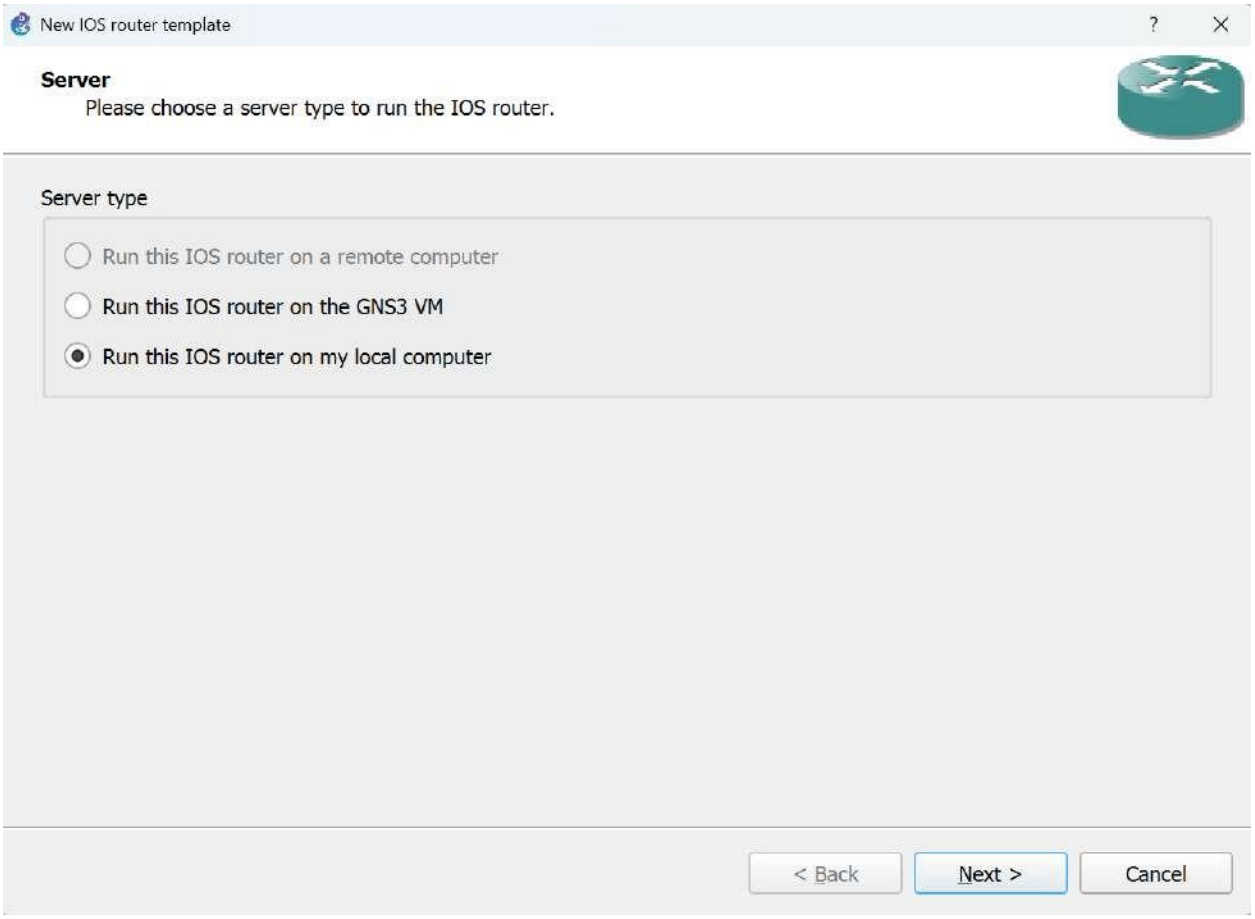
Download link : https://www.sysnettechsolutions.com/en/cisco-ios-download-for-gns3/



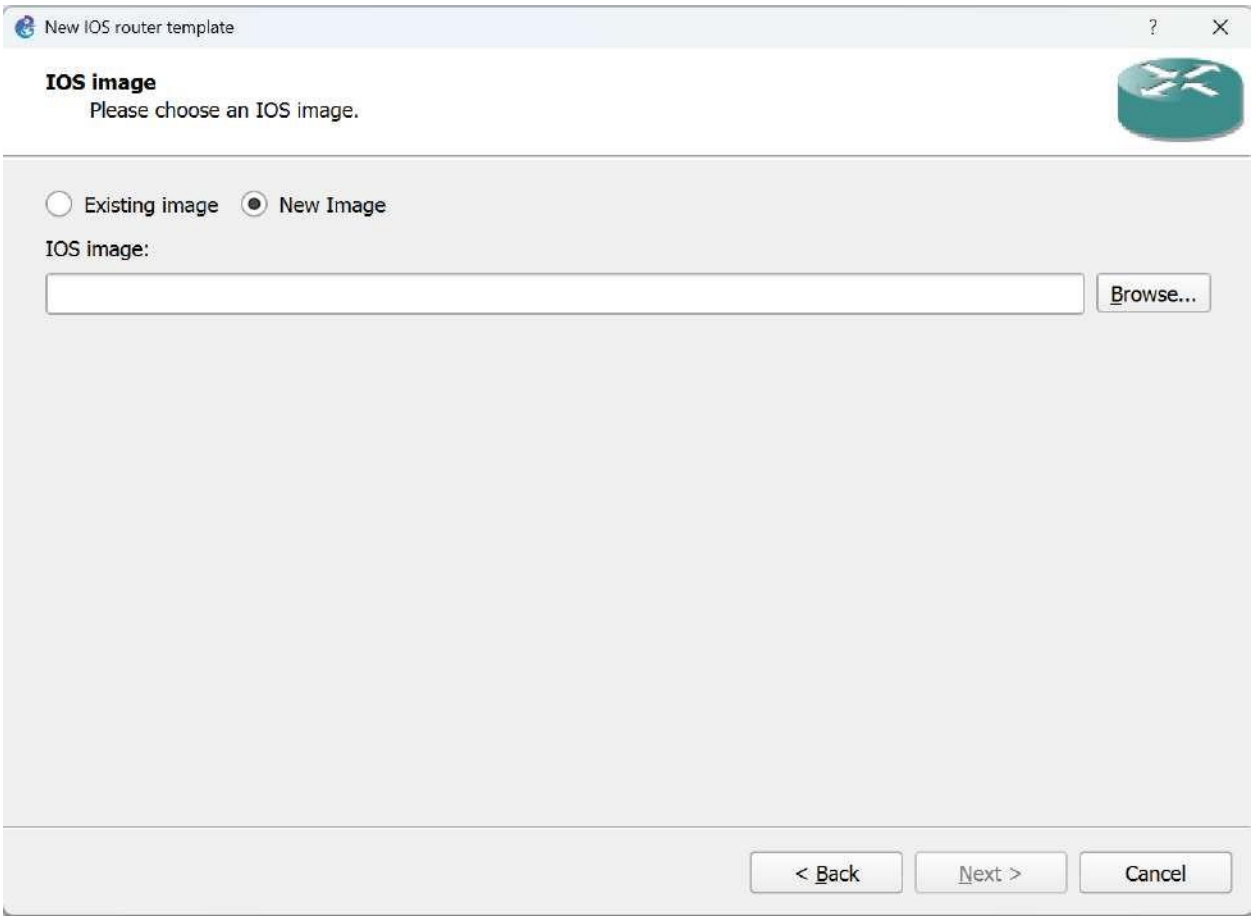
Click Edit and select Preferences



Select IOS routers and click New

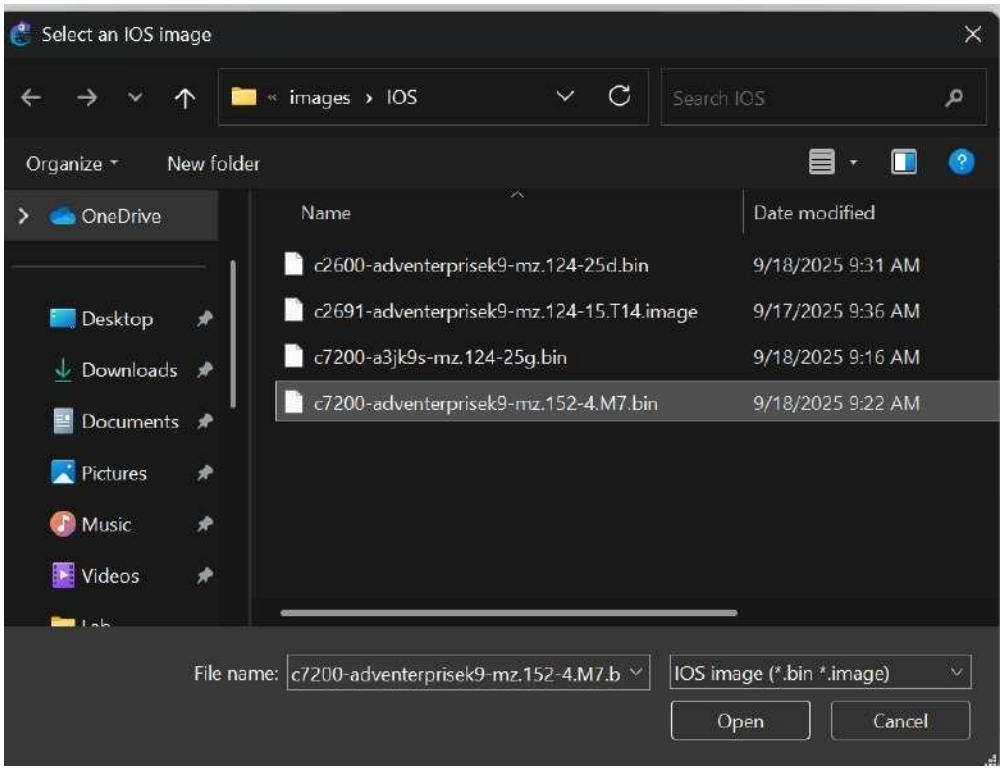


Choose Run this IOS router on my local computer and click Next

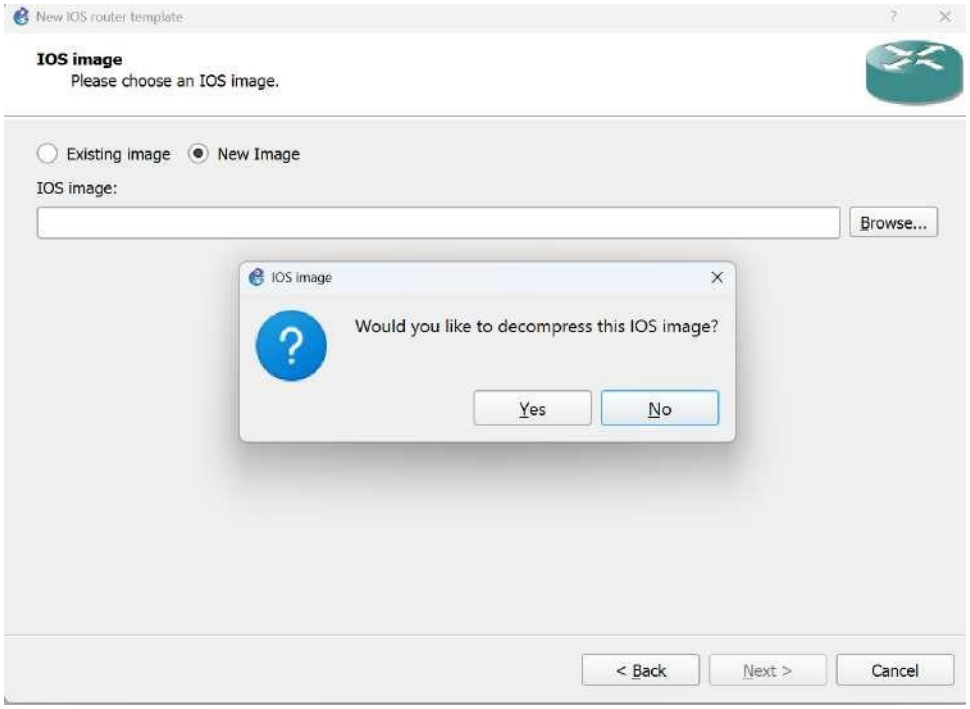


Browse IOS image

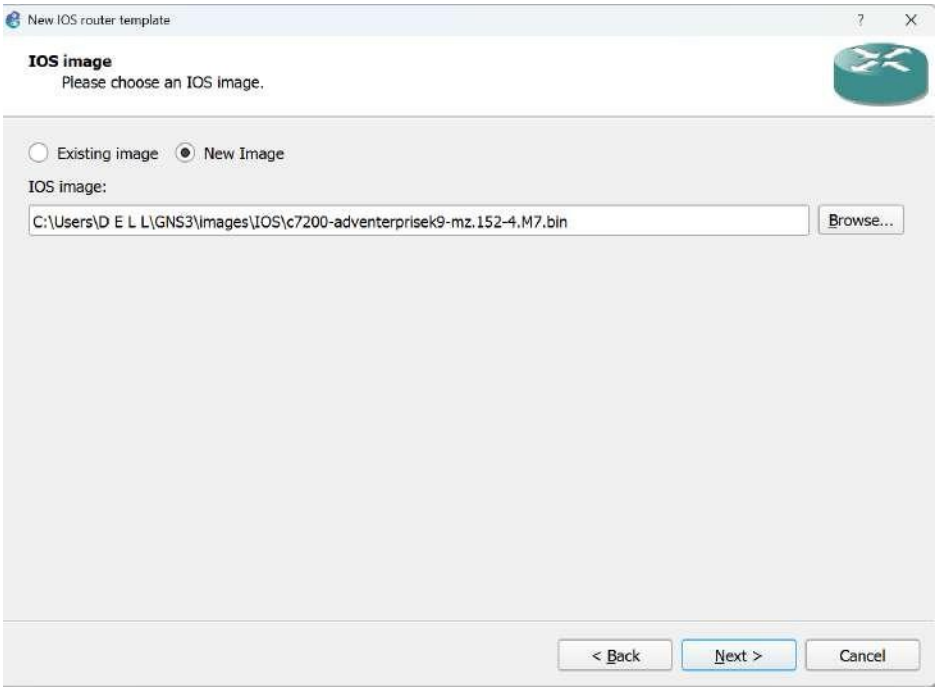
SUBHASH B
727722EUAI063



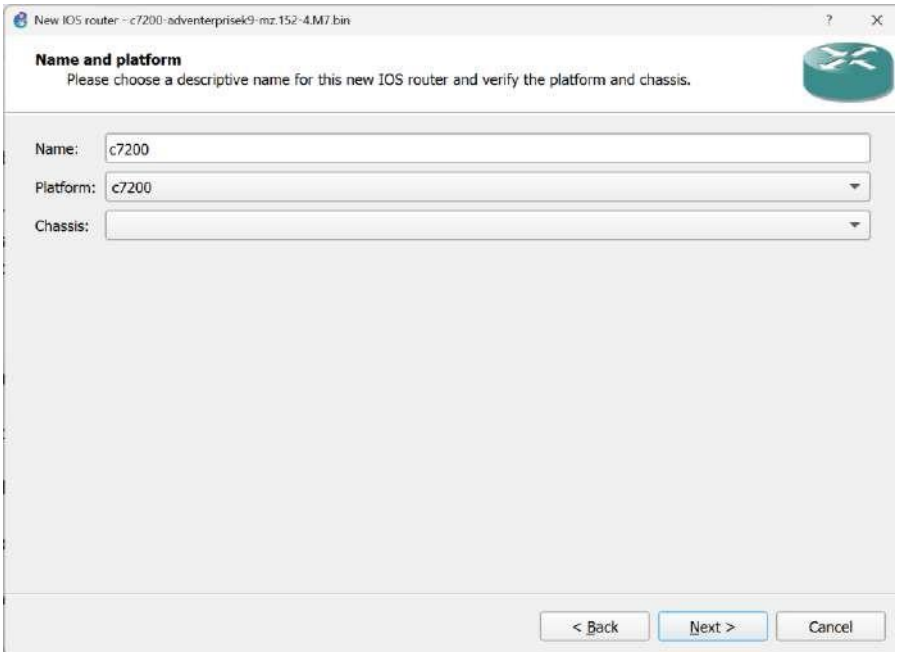
Select IOS file



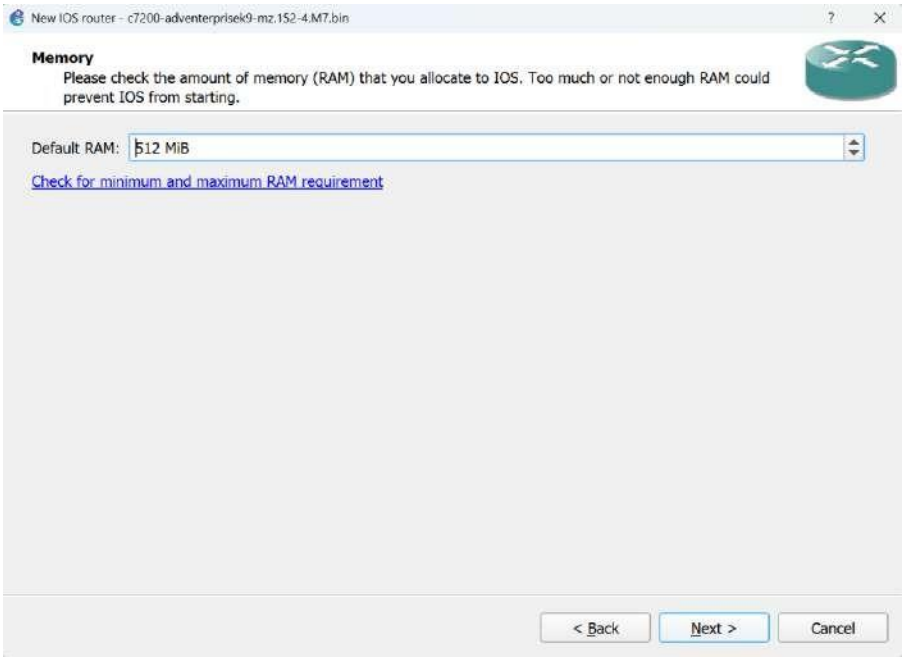
Select No



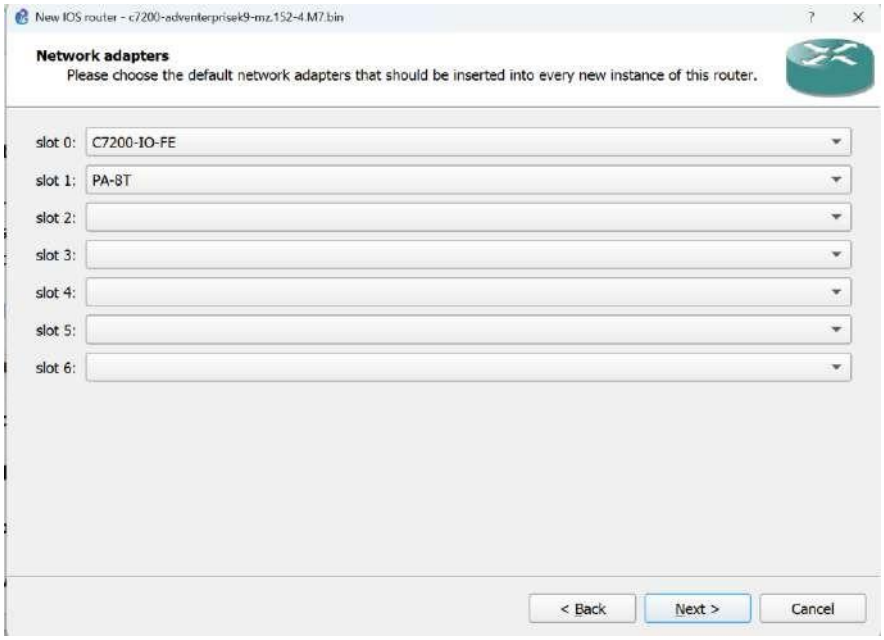
Click Next



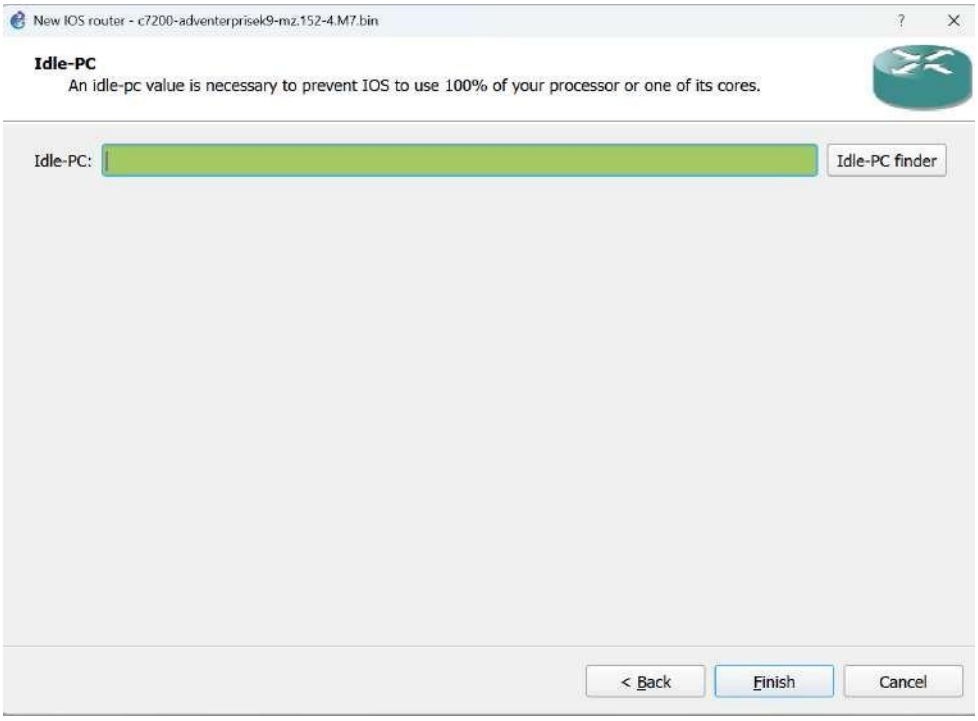
Click Next



Click Next

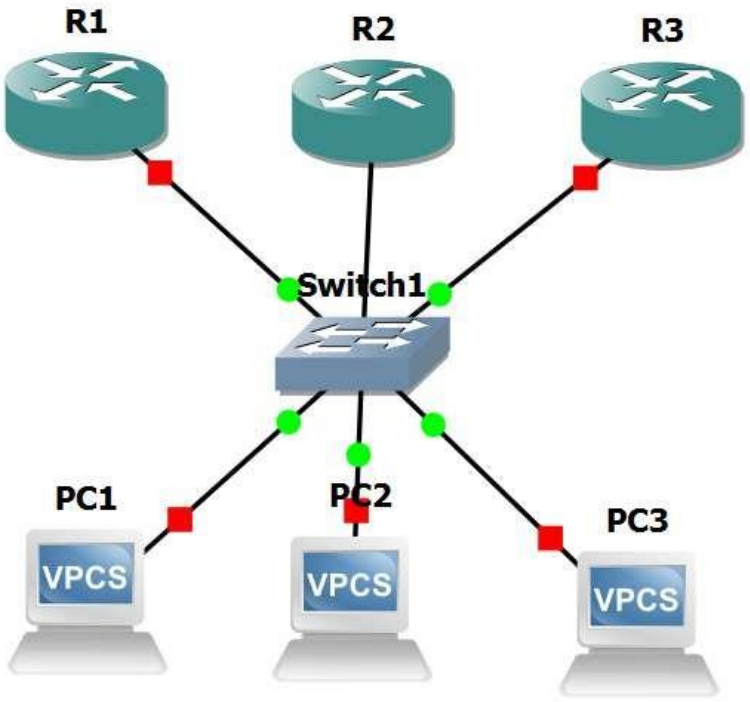


Click Next



Click Idle-PC finder and click Finish

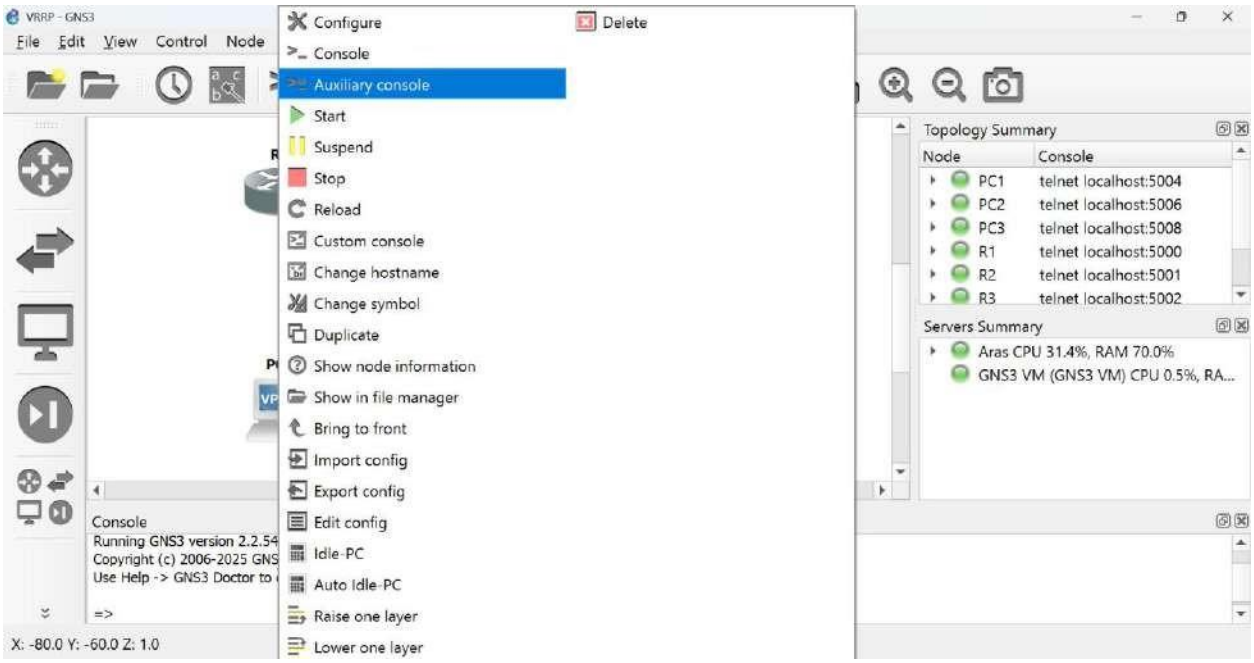
NETWORK DIAGRAM



SUBHASH B
727722EUAI063

CONFIGURATION

Start all devices by selecting Play button



Right click on R1 and Click Console

R1#en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int fa0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#vrrp 10 ip 192.168.10.10
*Sep 28 17:08:33.059: %VRRP-6-STATECHANGE: Fa0/0 Grp 10 state Init -> Backup
*Sep 28 17:08:33.079: %VRRP-6-STATECHANGE: Fa0/0 Grp 10 state Init -> Backup
*Sep 28 17:08:36.691: %VRRP-6-STATECHANGE: Fa0/0 Grp 10 state Backup -> Master
R1(config-if)#vrrp 10 priority 120
R1(config-if)#vrrp 10 preempt

Right click on R2 and Click Console

R2#en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int fa0/0
R2(config-if)#no shut
*Sep 28 17:09:05.023: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

*Sep 28 17:09:06.023: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config-if)#ip address 192.168.10.2 255.255.255.0
R2(config-if)#vrrp 10 ip 192.168.10.10
*Sep 28 17:09:42.651: %VRRP-6-STATECHANGE: Fa0/0 Grp 10 state Init -> Backup
*Sep 28 17:09:42.671: %VRRP-6-STATECHANGE: Fa0/0 Grp 10 state Init -> Backup
R2(config-if)#vrrp 10 priority 100
R2(config-if)#vrrp 10 preempt

Right click on R3 and Click Console

R3#en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int fa0/0
R3(config-if)#ip address 192.168.10.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#
*Sep 28 17:11:52.323: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Sep 28 17:11:53.323: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R3(config-if)#vrrp 10 ip 192.168.10.10
R3(config-if)#vrrp
*Sep 28 17:12:12.851: %VRRP-6-STATECHANGE: Fa0/0 Grp 10 state Init -> Backup
*Sep 28 17:12:12.871: %VRRP-6-STATECHANGE: Fa0/0 Grp 10 state Init -> Backup
R3(config-if)#vrrp 10 priority 80
R3(config-if)#vrrp 10 preempt

Right Click on PC1 and Select Console

PC1> ip 192.168.10.20 255.255.255.0 192.168.10.10
Checking for duplicate address...
PC1 : 192.168.10.20 255.255.255.0 gateway 192.168.10.10

Right Click on PC2 and Select Console

PC2> ip 192.168.10.21 255.255.255.0 192.168.10.10
Checking for duplicate address...
PC1 : 192.168.10.21 255.255.255.0 gateway 192.168.10.10

Right Click on PC3 and Select Console

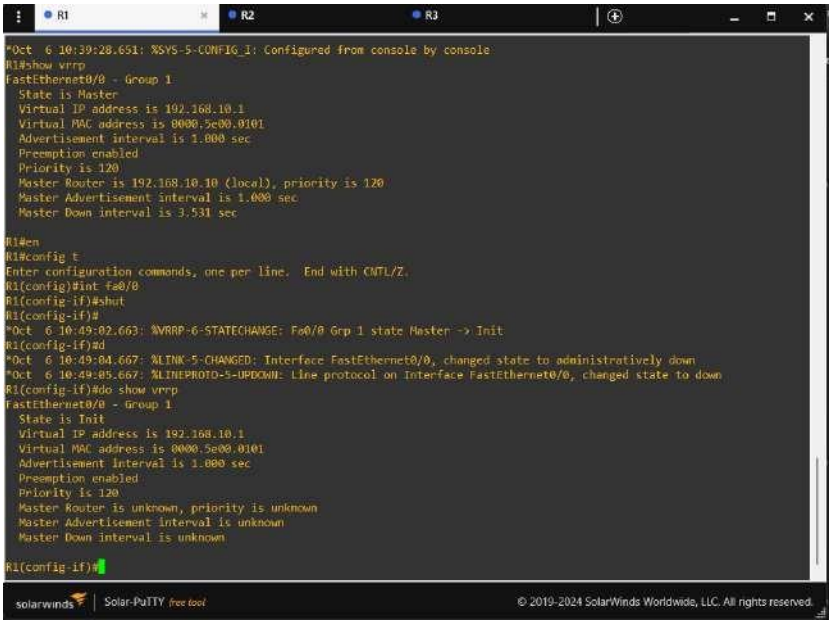
PC3> ip 192.168.10.22 255.255.255.0 192.168.10.10
Checking for duplicate address...
PC1 : 192.168.10.22 255.255.255.0 gateway 192.168.10.10

SUBHASH B
727722EUAI063

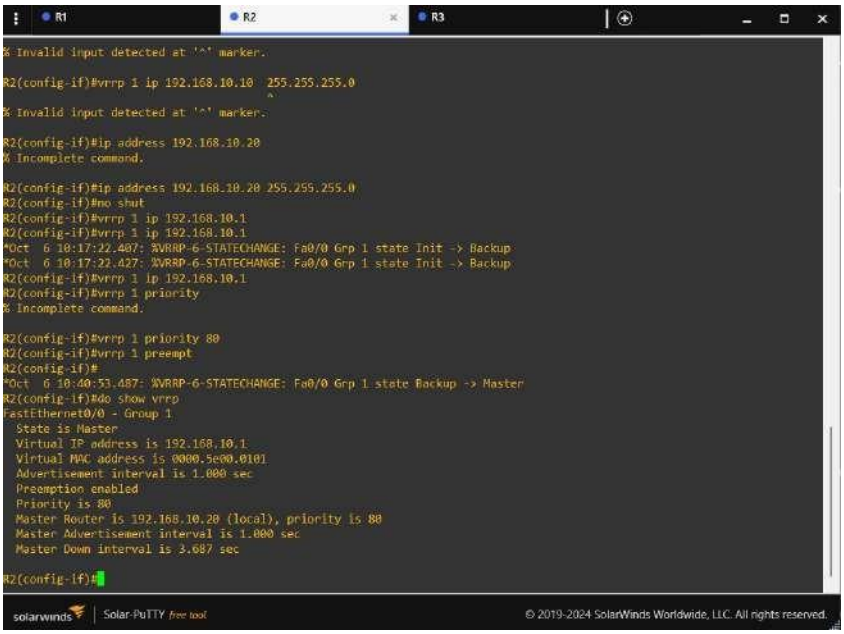
OUTPUT:

Master is Shifting based on priority:

Router 1:



Router 2:



SUBHASH B
727722EUAI063

PC's are in the network:

PC1 to PC3

PC2 to PC1

PC3 to PC2

RESULT:

Thus the VRRP configuration successfully provided gateway redundancy.

SUBHASH B
727722EUAI063

Ex.No : 7

Date :

Implement secure WLAN setup using 802.1X authentication with RADIUS

AIM:

To configure and implement a secure Wireless LAN (WLAN) using 802.1X authentication with a RADIUS server to ensure that only authenticated users can access the wireless network.

DESCRIPTION:

WIRELESS LAN (WLAN):

A Wireless Local Area Network (WLAN) is a network that allows devices to connect and communicate wirelessly within a local area (such as a home, office, or campus) using Wi-Fi technology**.**
Instead of using cables, WLANs rely on radio frequency (RF) signals to transmit data between wireless devices and a central access point.

802.1 X AUTHENTICATION:

802.1 X is an IEEE standard for port-based network access control. It provides a secure method for authenticating devices before granting them access to the network.

Working Principle

1. The client tries to connect to the WLAN.
2. The AP (authenticator) blocks all traffic except 802.1X authentication messages**.**
3. The client sends its credentials (username/password or certificate) using EAP (Extensible Authentication Protocol)**.**
4. The authenticator forwards these credentials to the RADIUS server**.**
5. If the RADIUS server validates the credentials, the AP changes the port state to "authorized," granting network access.

RADIUS Server

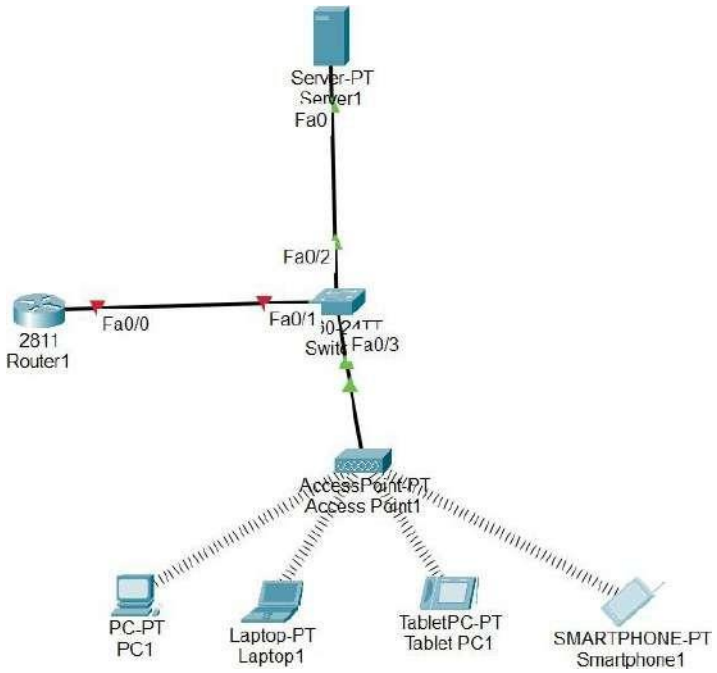
A RADIUS (Remote Authentication Dial-In User Service) server is a centralized server used to authenticate users, authorize access, and keep accounting records.

Functions of RADIUS

- **Authentication:** Verifies user identity using credentials stored in a database (e.g., Active Directory, LDAP).
- **Authorization:** Determines what network resources the user can access (e.g., VLAN assignment).
- **Accounting:** Keeps logs of user activities, such as connection time and data usage.

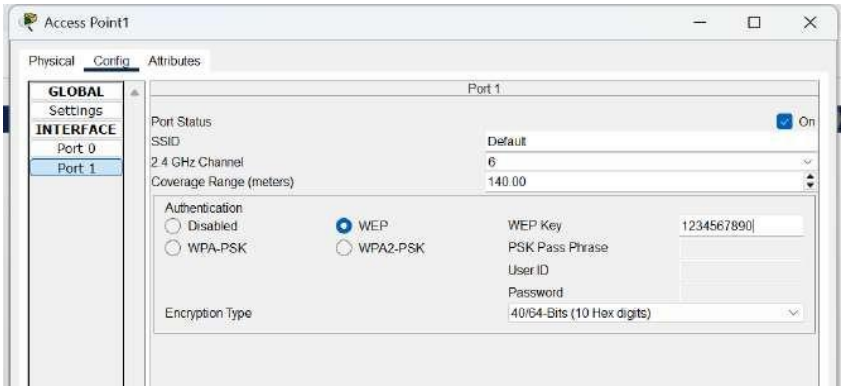
SUBHASH B
727722EUAI063

NETWORK DIAGRAM:



CONFIGURATION:

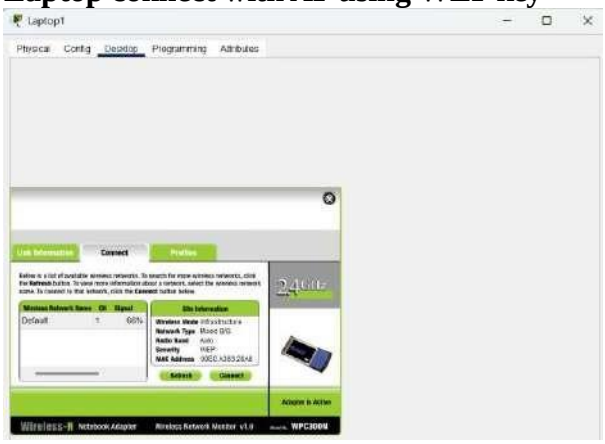
Config Access Point with WEP key



PC1 connect with AP using WEP Key

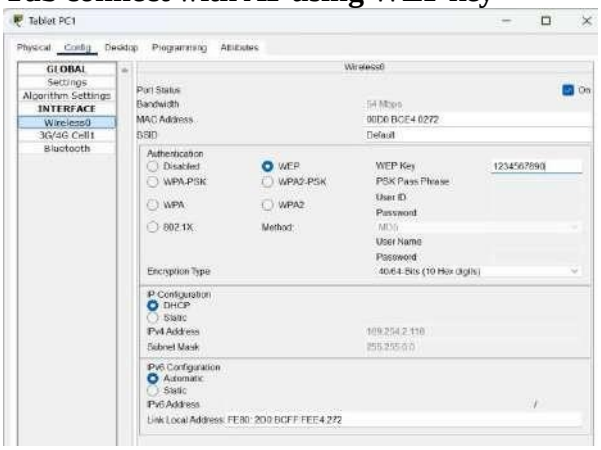
Choose Desktop -> PC wireless-> connect-> enter WEP key

Laptop connect with AP using WEP key



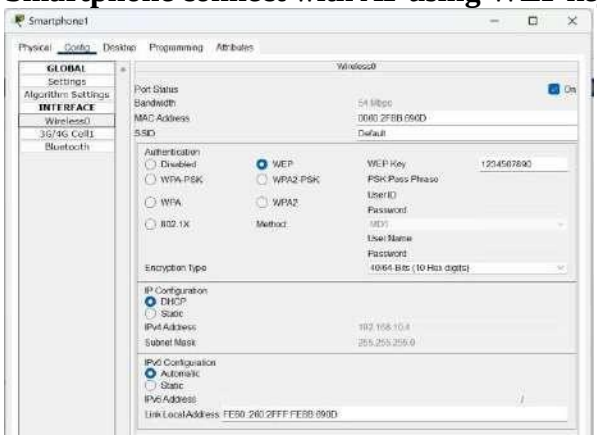
Choose Desktop -> PC wireless-> connect-> enter WEP key

Tab connect with AP using WEP key



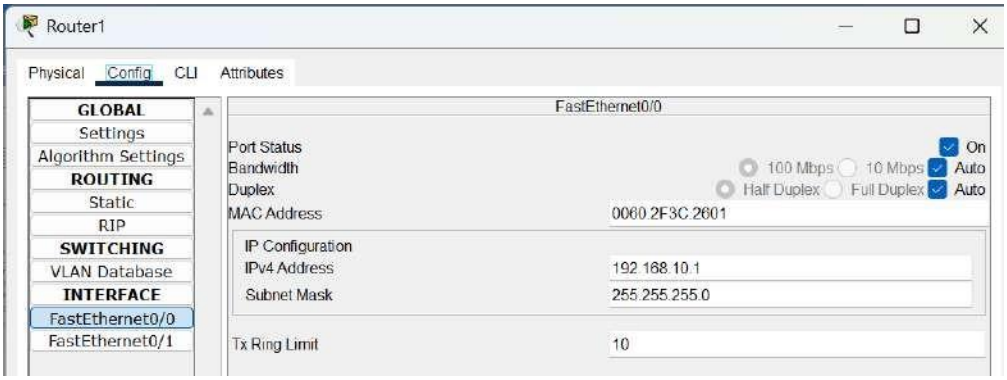
Choose Config -> Wireless0-> WEP-> enter WEP key

Smartphone connect with AP using WEP key



Choose Config -> Wireless0-> WEP-> enter WEP key

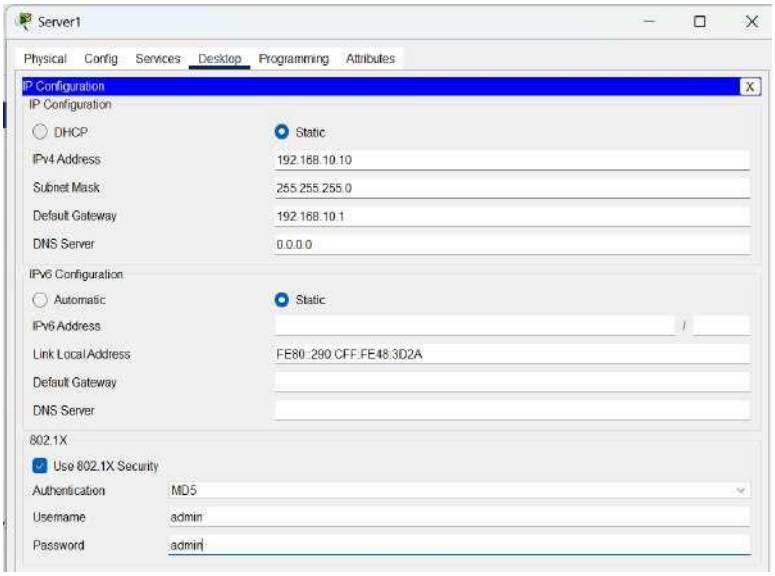
Router R1:



Enter IP configuration: 192.168.10.1 Subnet Mask : 255.255.255.0

SUBHASH B
727722EUAI063

Server 1:

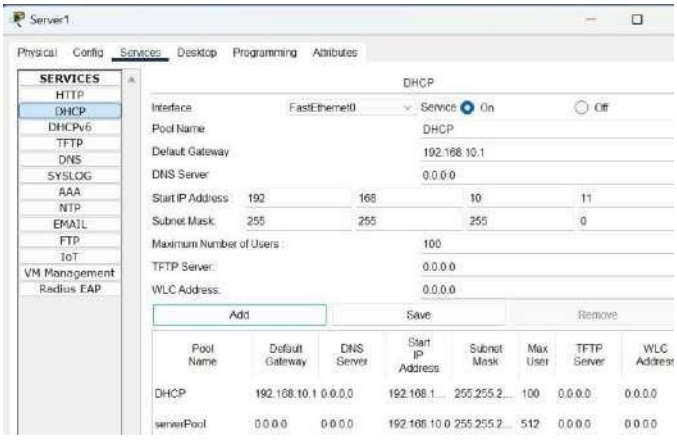


Enter IPv4 address :
192.168.10.10

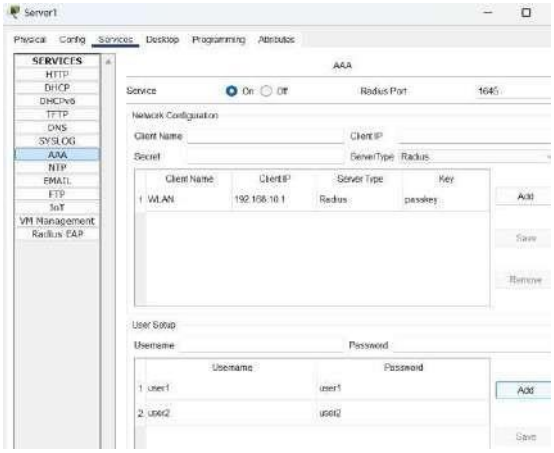
Subnet Mask:
255.255.255.0

Default Gateway:
192.168.10.1
{Router IP Address}

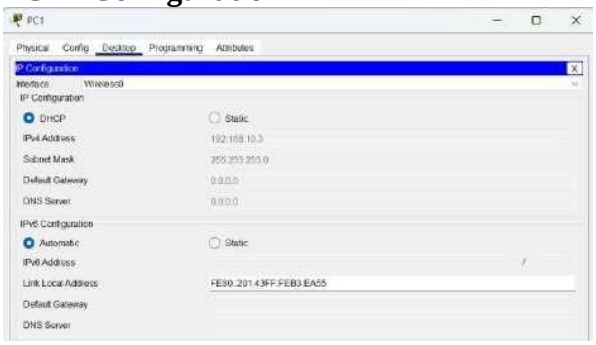
DHCP Service



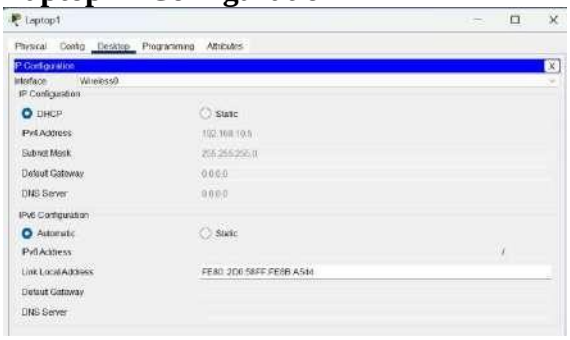
RADIUS Service



PC IP Configuration

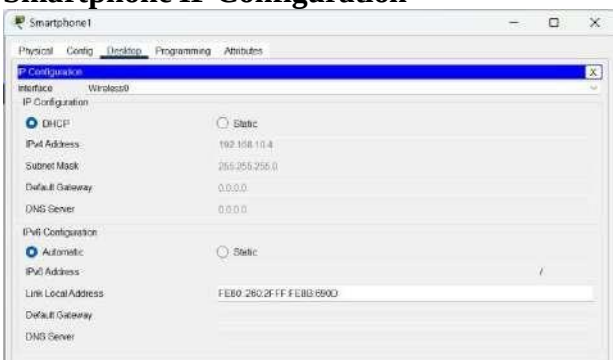


Laptop IP Configuration



Tablet IP Configuration

Smartphone IP Configuration

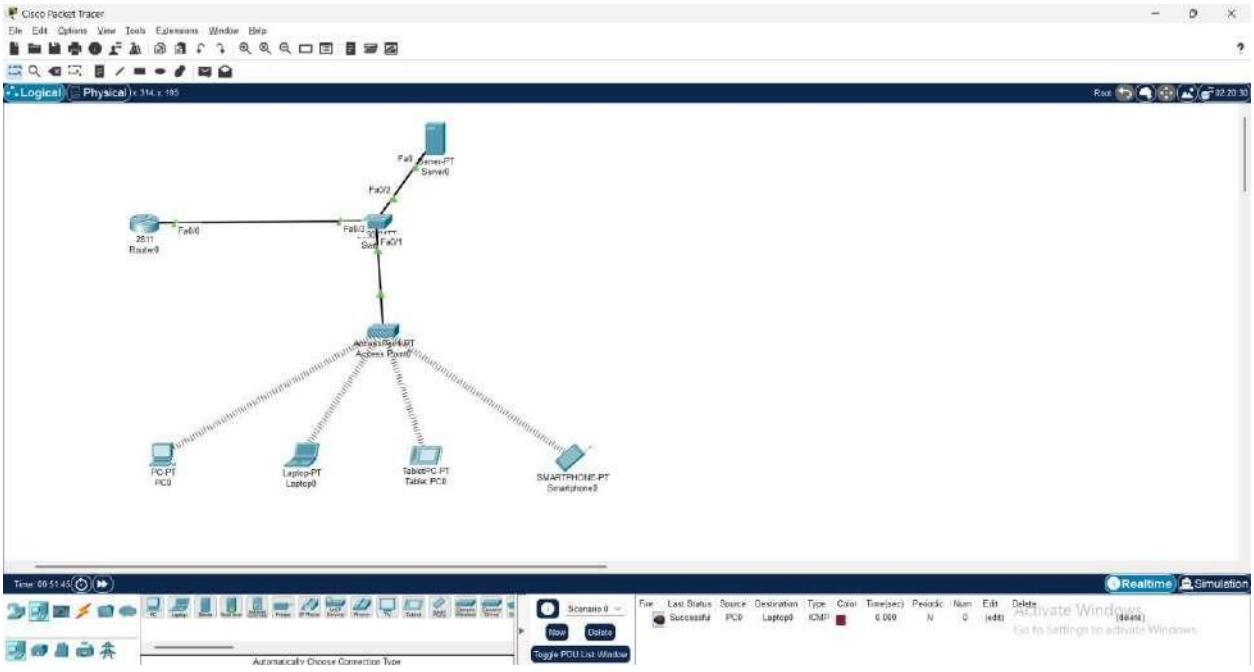


Router configuration:

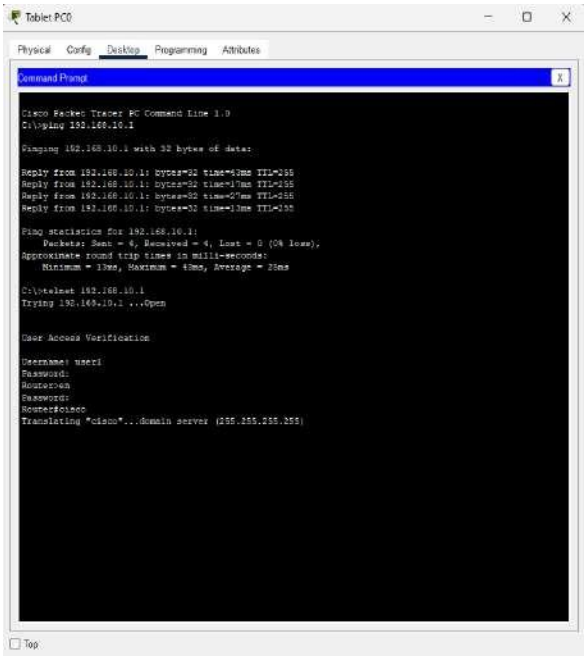
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# enable secret cisco123
Router(config)#aaa authentication login default group radius
Router(config)#line vty 0 4
Router(config-line)#login authentication default
Router(config-line)#transport input telnet

OUTPUT:

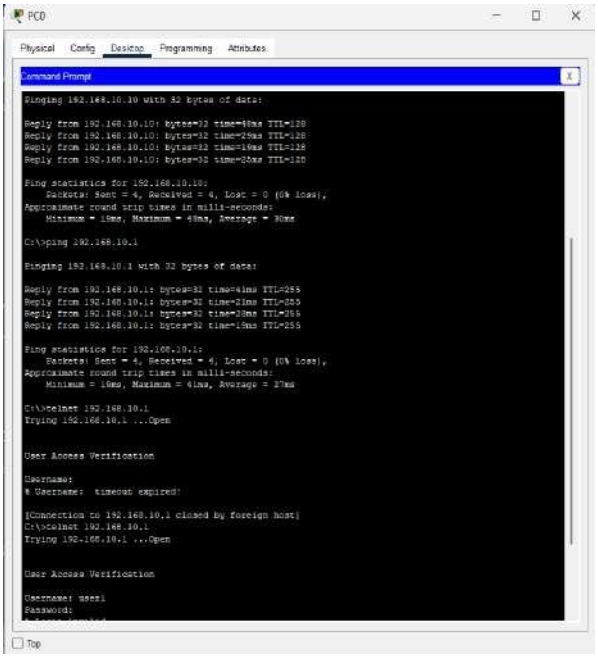
File Transfer



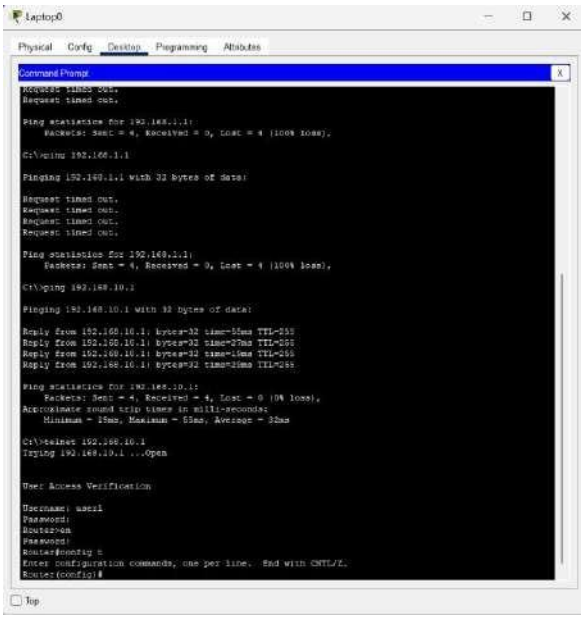
Tablet



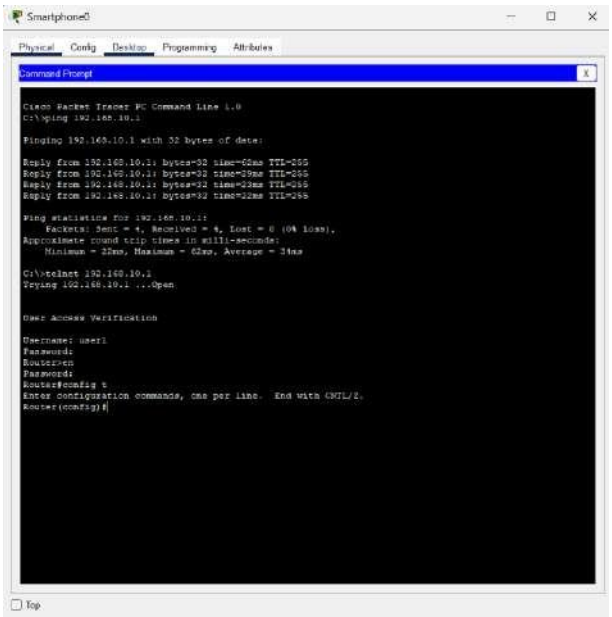
PC



Laptop



Smartphone



RESULT:

Thus the secure WLAN was successfully configured and tested using 802.1X authentication with a RADIUS server**.**

SUBHASH B
727722EUAI063

Ex.No : 8
Date :

Create and analyze WLANs with guest access via captive portals

AIM:

To configure and analyze a Wireless LAN (WLAN) with guest access using a captive portal and verify that unauthenticated clients are redirected to a login page before gaining network access.

DESCRIPTION:

WLAN:

A Wireless Local Area Network (WLAN) is a type of local area network that uses radio waves instead of physical cables to connect devices such as laptops, smartphones, and PCs within a limited geographical area (like a building, campus, or office).

CAPTIVE PORTAL:

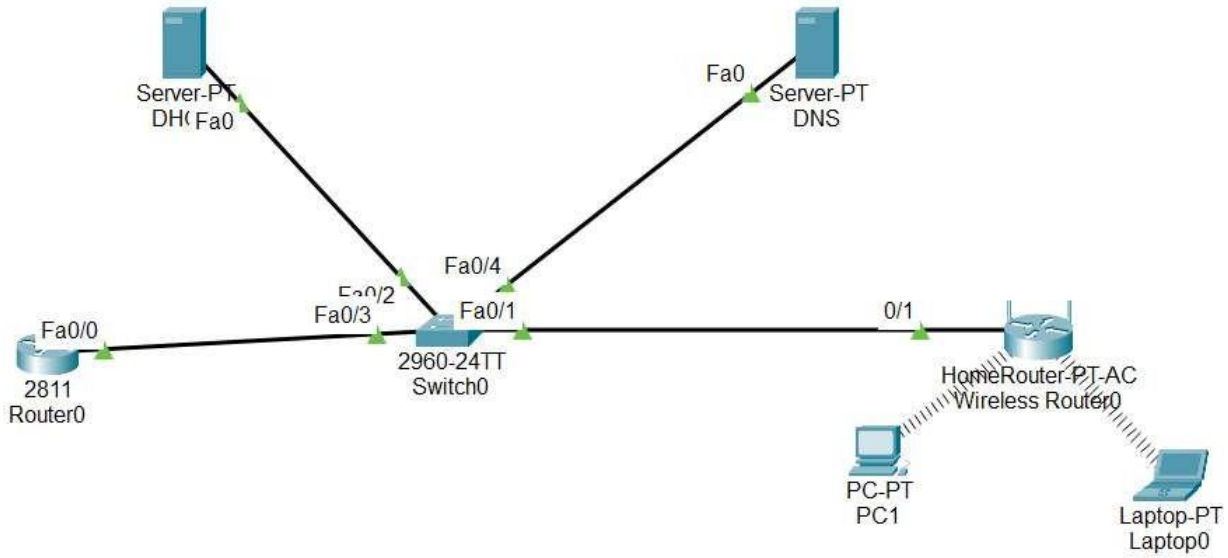
A Captive Portal is a web-based authentication mechanism used in public or enterprise WLANs to control user access.

How it works:

1. A guest device connects to the WLAN and gets an IP address via DHCP.
2. When the user opens a browser and tries to access any website, the request is intercepted.
3. The user is redirected to a login page (portal) hosted on the router or a server.
4. The user enters credentials (username/password).
5. If authentication is successful (locally or via RADIUS server), the user is allowed to access the internet or network resources.

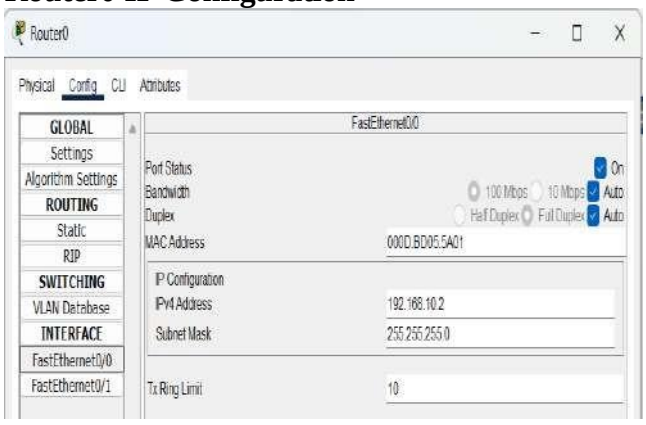
SUBHASH B
727722EUAI063

NETWORK DIAGRAM:

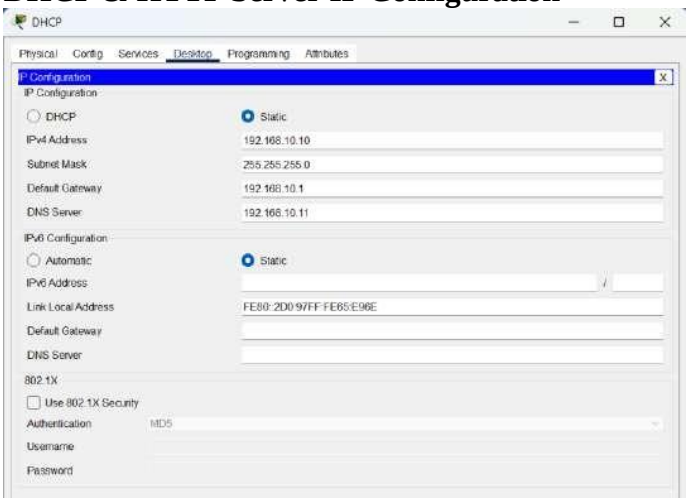


CONFIGURATION:

Router0 IP Configuration

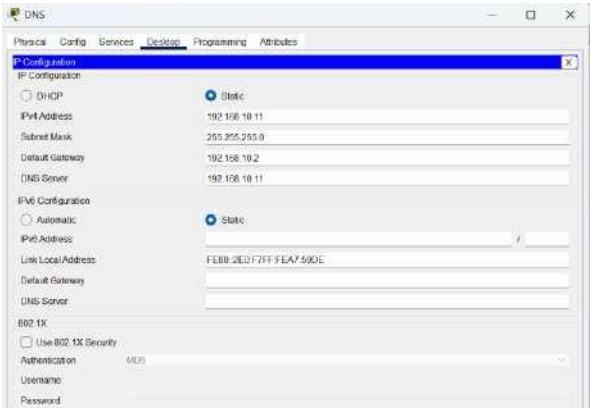


DHCP & HTTP Server IP Configuration

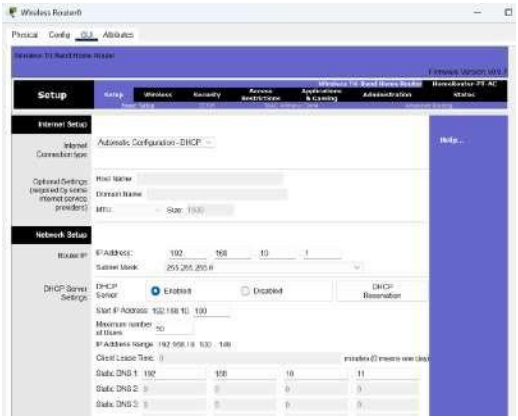


SUBHASH B
727722EUAI063

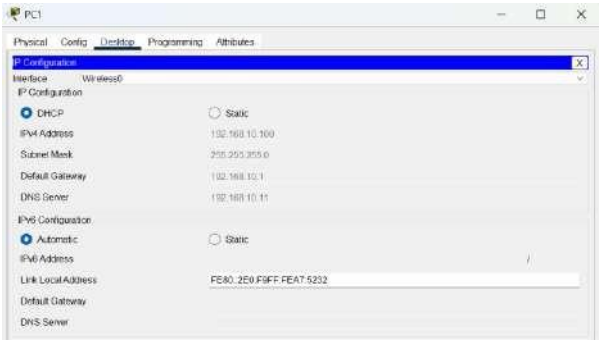
DNS Server IP Configuration



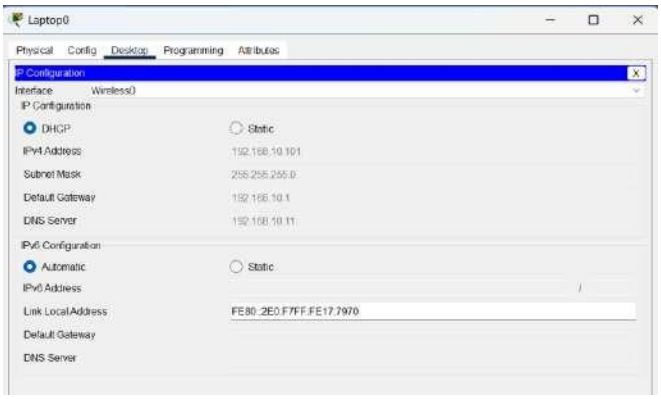
Home Router IP Configuration



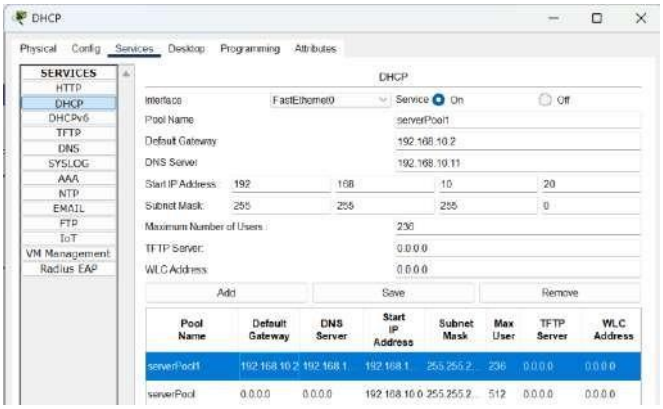
PC1 dynamic IP



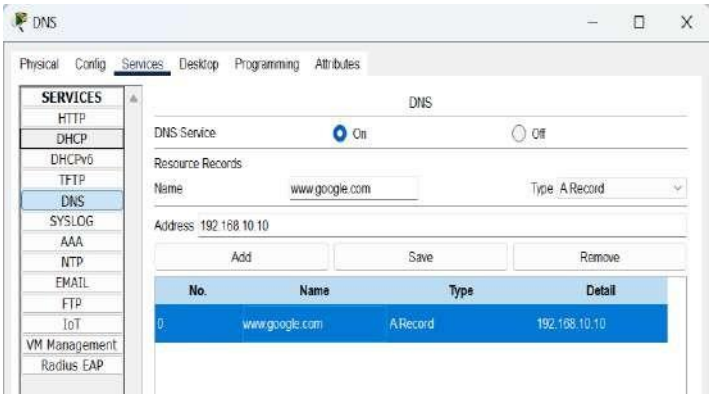
Laptop dynamic IP



DHCP Service

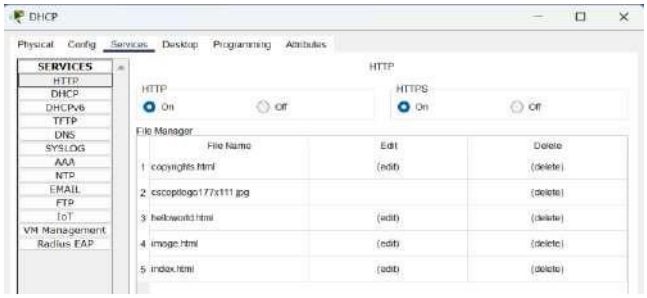


DNS Service



SUBHASH B
727722EUAI063

HTTP Service



HTTP Service (index.html)

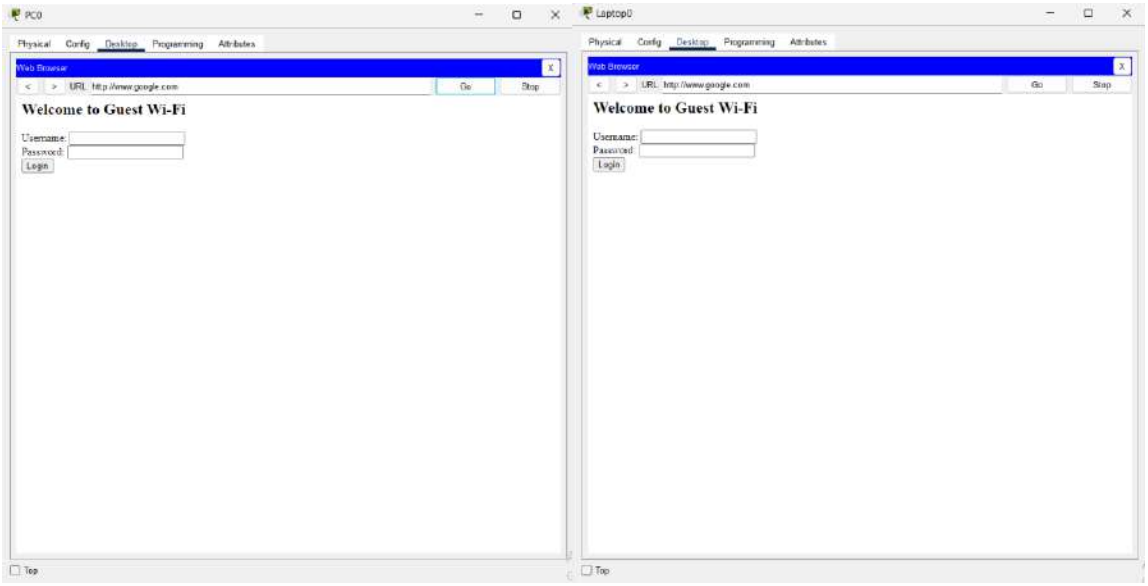
Captive Portal:

```
<html>
<head>
<title>Guest Login</title>
<style>
#message {
font-weight: bold;
color: green;
margin-top: 20px;
}
#error {
color: red;
}
</style>
<script>
function showLoginMessage() {
var username = document.getElementById("username").value;
var password = document.getElementById("password").value;
var messageDiv = document.getElementById("message");

if(username === "guest1" && password === "guest123") {
messageDiv.innerHTML = "Login Successful!";
messageDiv.style.color = "green";
} else {
messageDiv.innerHTML = "Login Failed! Incorrect username or password.";
messageDiv.style.color = "red";
}
}
</script>
</head>
<body>
<h2>Guest Login</h2>
<form onsubmit="showLoginMessage(); return false;">
Username: <input type="text" id="username" required><br><br>
Password: <input type="password" id="password" required><br><br>
<input type="submit" value="Login">
</form>
<!-- Message will appear here -->
<div id="message"></div>
</body>
</html>
```

SUBHASH B
727722EUAI063

OUTPUT:

PC: **LAPTOP:**



RESULT:

Thus the WLAN with guest access was successfully created and configured. PCs connected to the WLAN were redirected to the captive portal page when trying to access any website.

SUBHASH B
727722EUAI063

Ex.No : 9

Date :

Analyze OSPF routing protocol performance through simulation

AIM:

To analyze the performance of the OSPF (Open Shortest Path First) routing protocol through network simulation.

DESCRIPTION:

OSPF:

Open Shortest Path First (OSPF) is a dynamic, link-state routing protocol that efficiently distributes routing information within a single autonomous system (AS). As an Interior Gateway Protocol (IGP), it enables routers to discover the best (shortest and most efficient) path for data transfer. OSPF is an open standard protocol.

Areas:

OSPF uses a hierarchical design by dividing a large network into smaller areas to enhance scalability and reduce the size of routing tables.

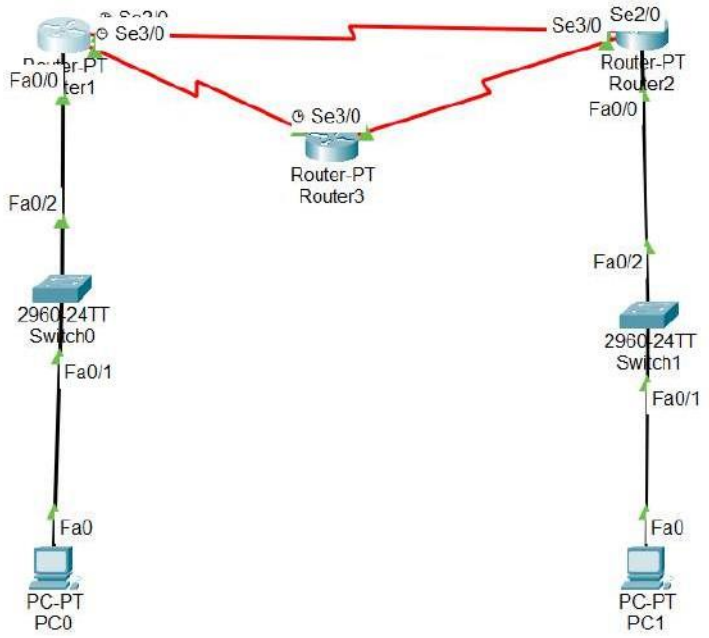
- Backbone area (Area 0): This is the central, mandatory area to which all other areas must connect. It is the primary transport for inter-area traffic.
- Area Border Routers (ABRs): Routers with interfaces in more than one area, including the backbone. They connect the backbone to other areas and summarize routing information.

Open Shortest Path First (OSPF) States:

Down State: No Hello packets have been received from the neighbor.
Init State: Hello packet received from neighbor, but own router ID is not listed in the neighbor field of the Hello packet.
Two-way State: Bi-directional communication established (our Router ID appears in neighbor's Hello packet).
ExStart State: Routers begin to exchange Database Description (DBD) packets.
Exchange State: Routers exchange DBD packets describing their LSDB (Link-State Database).
Loading State: Routers send LSR (Link State Requests) for missing LSAs and receive LSU (Link State Updates)**.**
Full State: Neighbors are fully adjacent, LSDBs are synchronized.

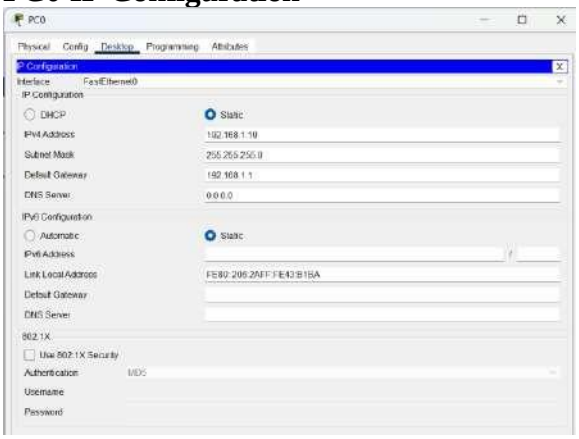
NETWORK DIAGRAM:

SUBHASH B
727722EUAI063

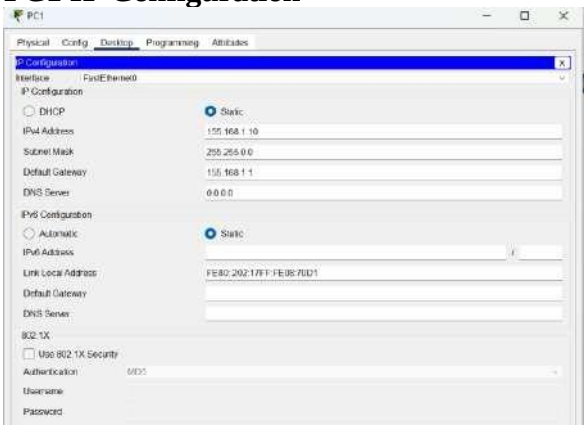


CONFIGURATION:

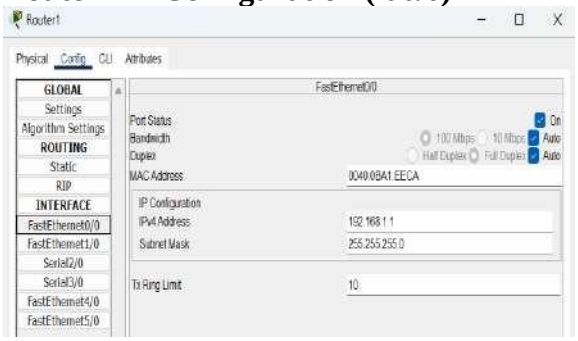
PC0 IP Configuration



PC1 IP Configuration



Router1 IP Configuration (fa0/0)

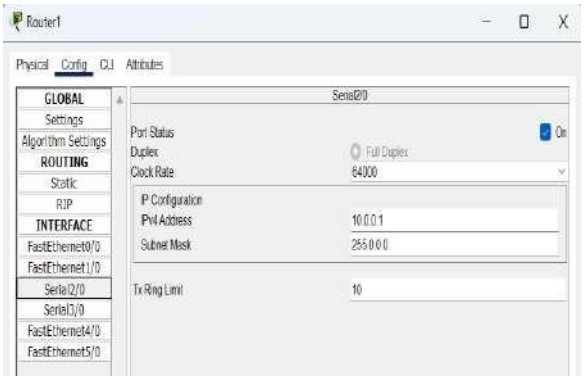


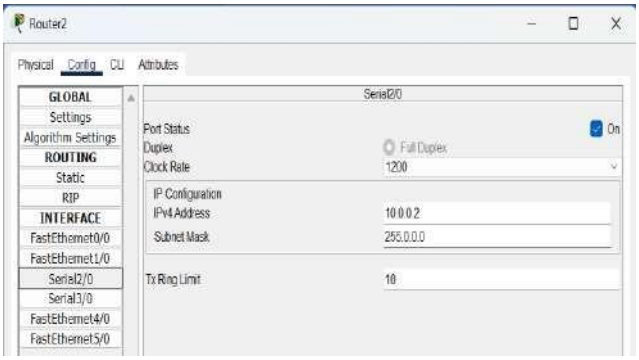
Router2 IP Configuration (fa0/0)

Router1 IP Configuration (Se2/0)

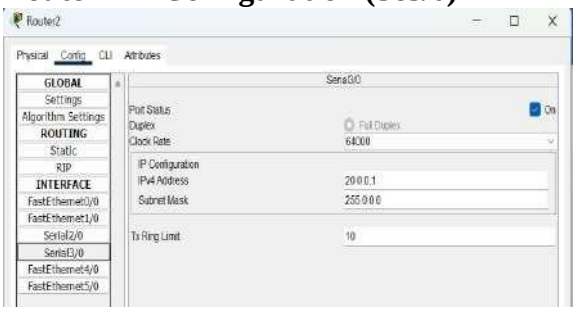
Router2 IP Configuration (Se2/0)

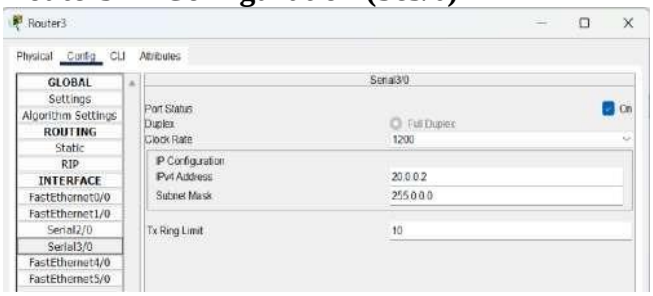
SUBHASH B
727722EUAI063



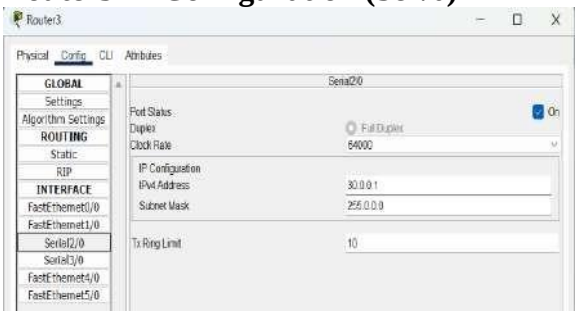


Router2 IP Configuration (Se3/0) **Router3 IP Configuration (Se3/0)**





Router3 IP Configuration (Se2/0) **Router1 IP Configuration (Se3/0)**



Router1 configuration:

Router(config-if)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 10.0.0.0 0.255.255.255 area 0
Router(config-router)#network 30.0.0.0 0.255.255.255 area 0

Router2 configuration:

Router(config-if)#router ospf 1
Router(config-router)#network 155.168.1.0 0.0.255.255 area 0
Router(config-router)#network 10.0.0.0 0.255.255.255 area 0
Router(config-router)#network 20.0.0.0 0.255.255.255 area 0

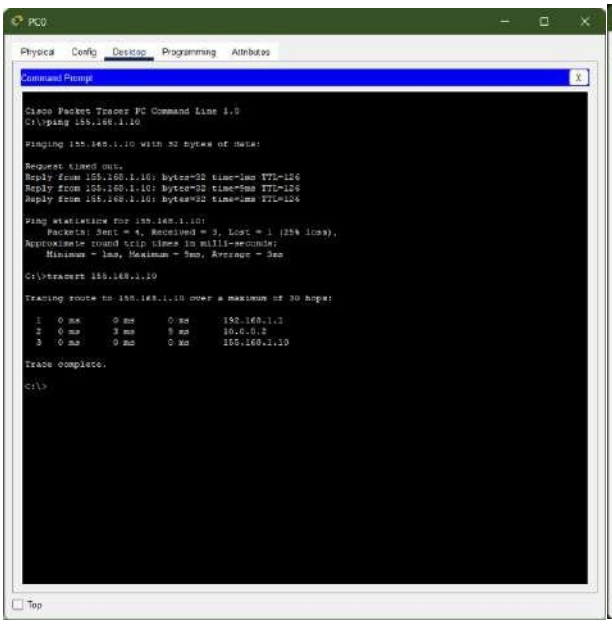
Router3 configuration:

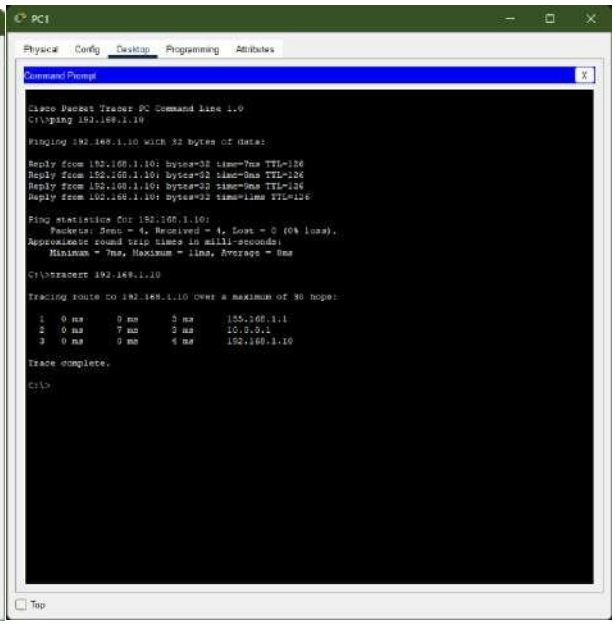
Router(config-if)#router ospf 1
Router(config-router)#network 20.0.0.0 0.255.255.255 area 0

Router(config-router)#network 30.0.0.0 0.255.255.255 area 0

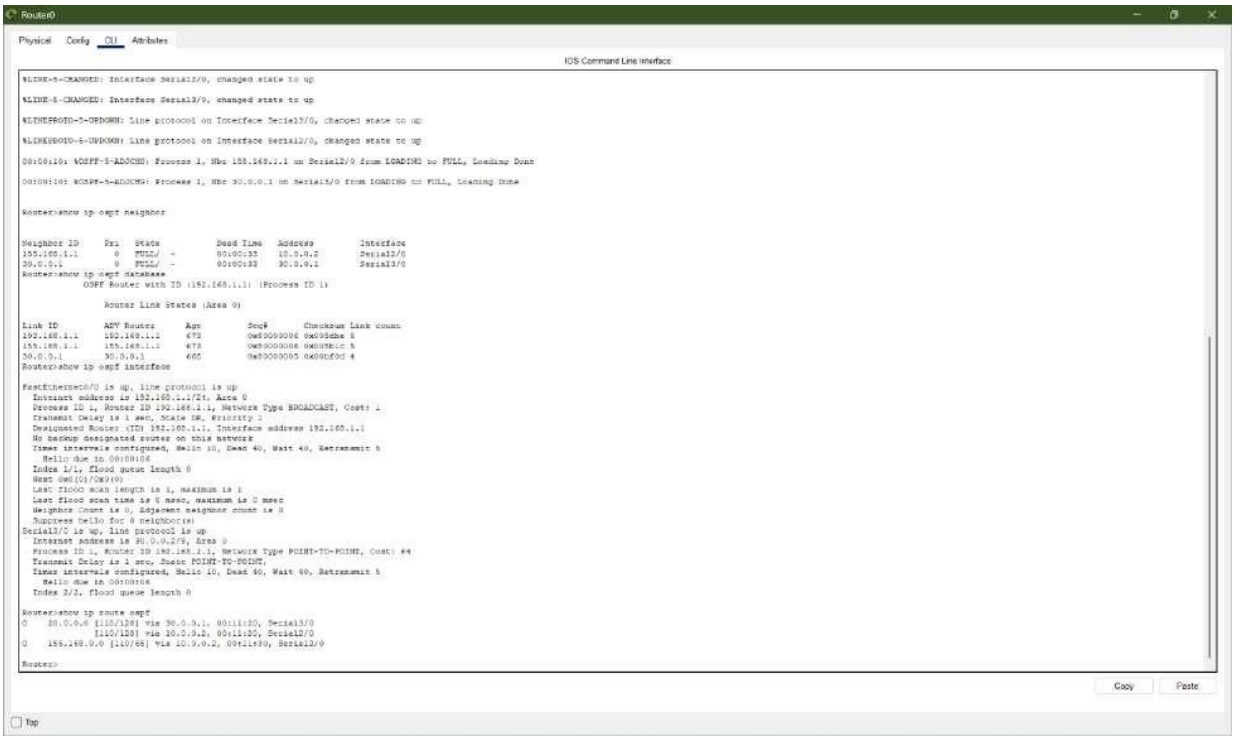
OUTPUT:

PC0: **PC1:**



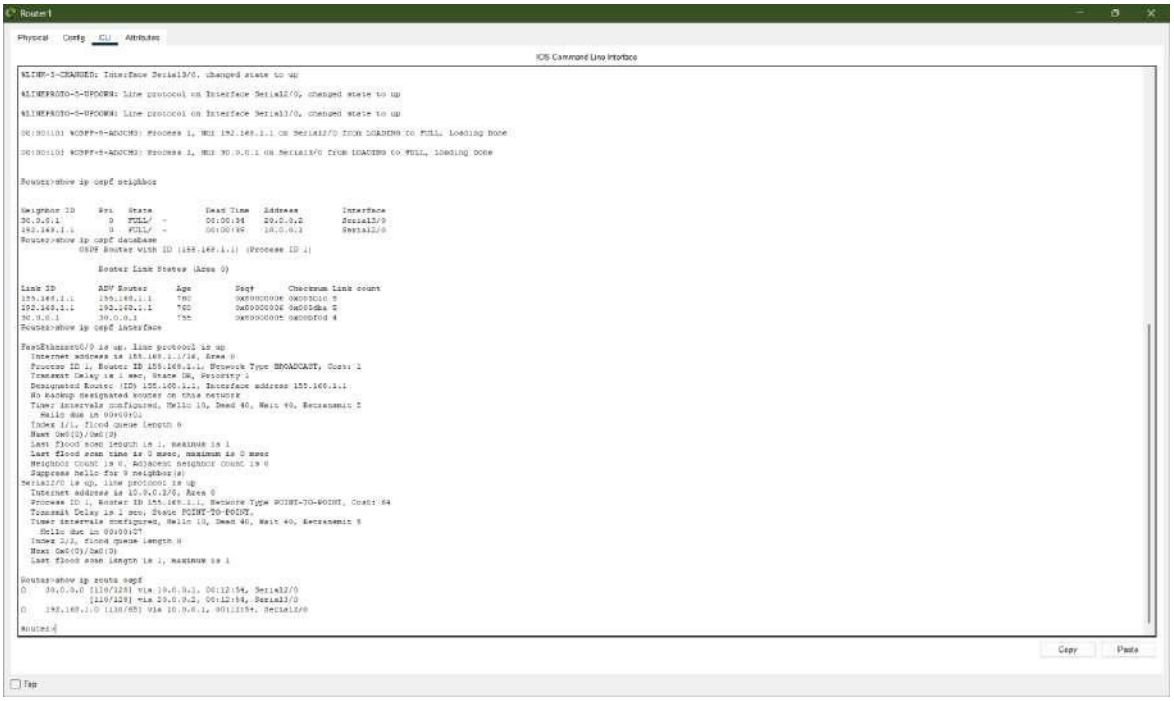


ROUTER0:

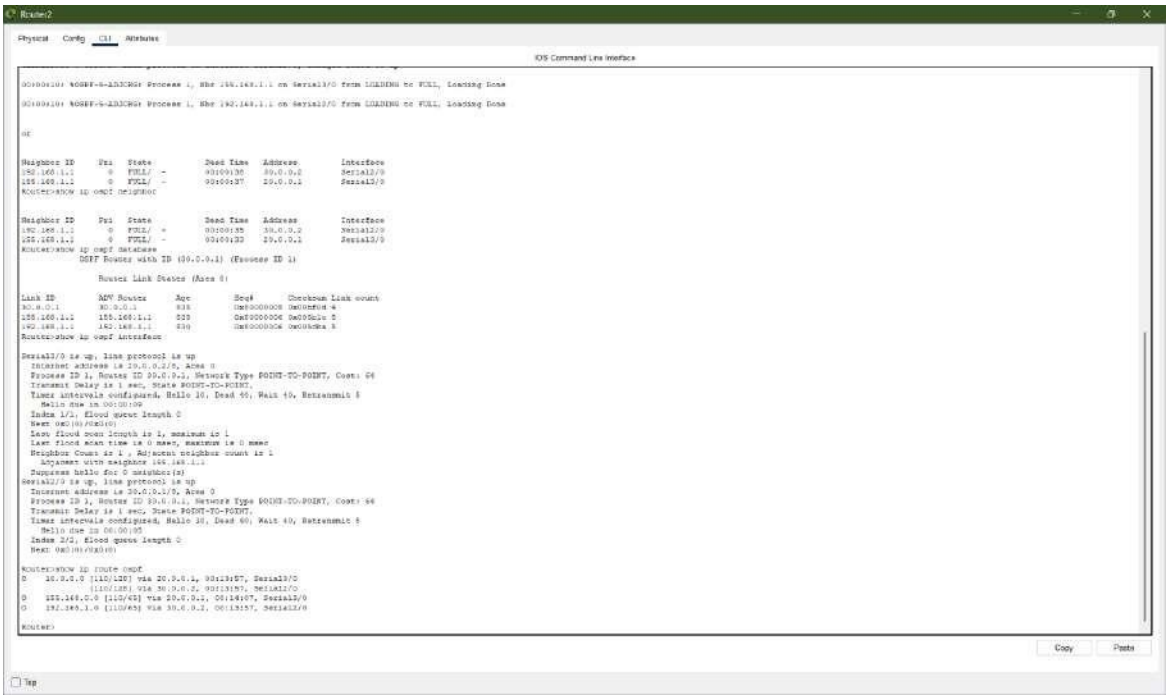


SUBHASH B
727722EUAI063

ROUTRE 1:



ROUTER 2:



RESULT:

Thus the OSPF routing protocol was successfully simulated and analyzed.

SUBHASH B
727722EUAI063

Ex.No : 10

Date :

Emulate SD-WAN-like behavior using static routes and redundancy simulation

AIM:

To simulate SD-WAN-like traffic steering and redundancy in an EVE-NG lab.

DESCRIPTION:

SD-WAN:

SD-WAN is a technology that simplifies the management and operation of a wide area network (WAN) by decoupling the networking hardware from the control mechanism, enabling more agile, cost-effective, and efficient network management. It uses software-based controllers to provide centralized control, dynamic traffic management, and flexible use of multiple connection types (e.g., MPLS, broadband, LTE) across a distributed network.

Components:

1. **SD-WAN Edge Devices**:
    - These devices are located at branch offices or remote sites and form the primary interaction point with the SD-WAN.
    - They are responsible for routing and forwarding traffic across different types of WAN connections (MPLS, internet broadband, LTE, etc.).
2. **SD-WAN Controller**:
    - The controller is a centralized software platform responsible for managing the SD-WAN deployment, policy configuration, and network monitoring.
    - It dynamically distributes routing policies and configuration updates to the edge devices.
3. **Overlay Network**:
    - SD-WAN creates a virtualized overlay network that abstracts the underlying physical network. This helps in maintaining the network's flexibility and redundancy.
4. **Orchestration**:
    - The orchestration layer provides centralized configuration and management of the network.
    - It automates tasks like applying security policies, configuring routes, and monitoring the network's health.

5. **Transport Network**:
    - SD-WAN allows for multiple types of transport networks to be used simultaneously, including MPLS, broadband Internet, 4G/5G LTE, and more.

INSTALLATION PROCEDURE:

EVE – NG
Download link: https://customers.eve-ng.net/eve-pro-prod-bm-6.4.0-10-full.iso

VMware
Download link: https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion

WinSCP
Download link: https://winscp.net/eng/download.php

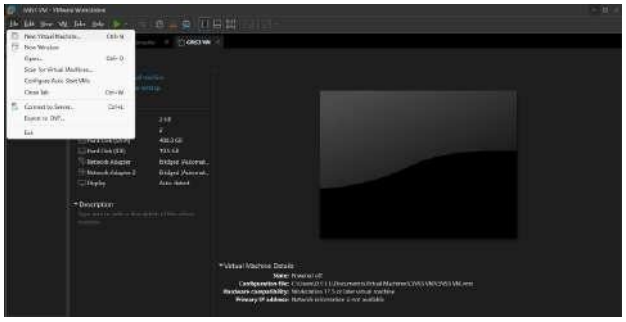
Image files
Download link: https://networkrare.com/free-download-cisco-viptela-images-vmanage-vsmart-vbond-vedge-cedge-for-eve-ng/
https://www.sysnettechsolutions.com/en/cisco-ios-download-for-gns3/

SecureCRT
https://www.vandyke.com/cgi-bin/releases.php?product=securecrt

Important Settings:
- Turn Windows features on or off -> Uncheck Hyper-V, Virtual Machine Platform, Windows Hypervisor Platform
- Device Security -> Core isolation -> Core isolation details -> Turn OFF memory integrity
- Windows Settings ->Apps->Default Apps->SecureCRT->TELNET->set default

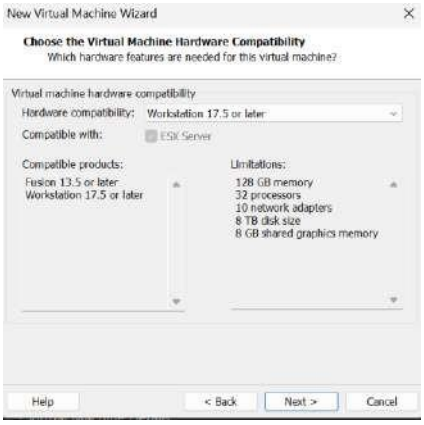
Open VMWare Workstation

SUBHASH B
727722EUAI063

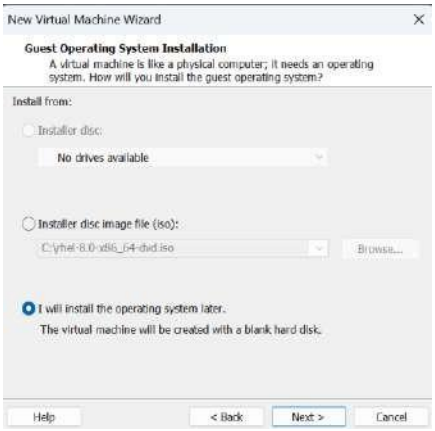


Click File then New Virtual Machine

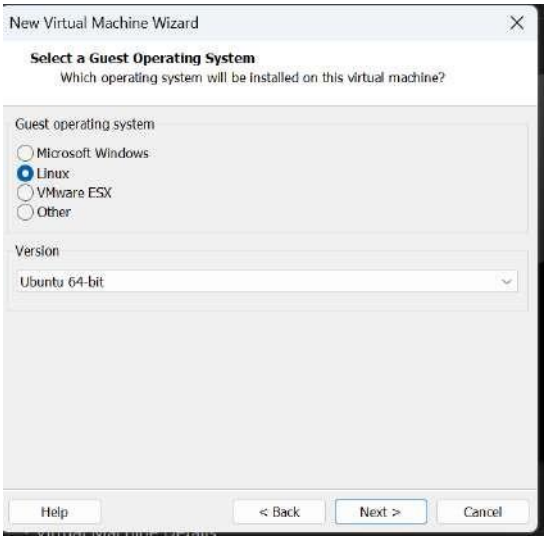
Select Custom then Click Next



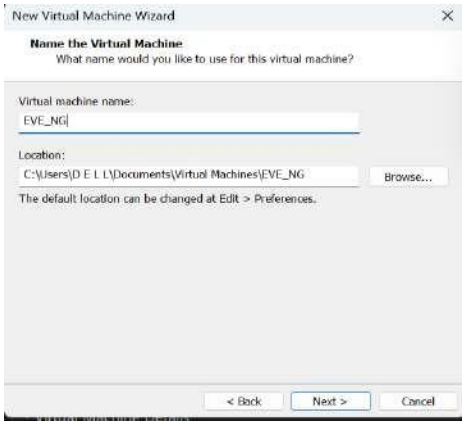
Click Next



Choose I will Install OS later then Click Next

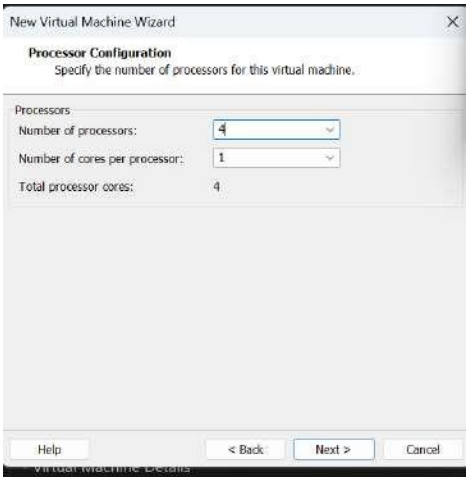


Choose Guest OS - Linux and Version Ubuntu 64-bit then click Next

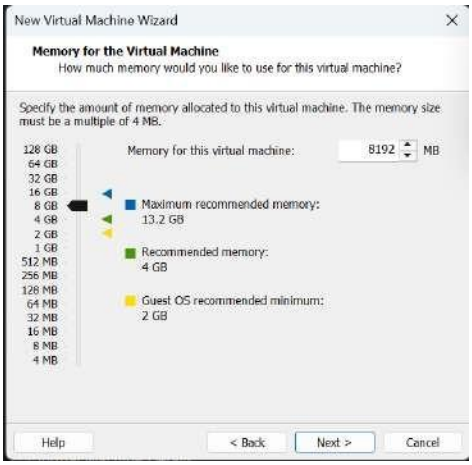


VM Name: EVE_NG and Click Next

SUBHASH B
727722EUAI063



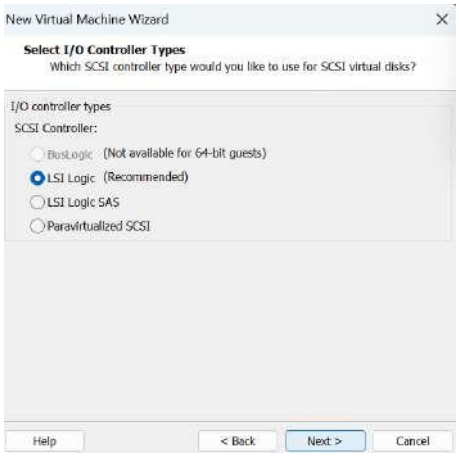
Number of Processors: 4 and Click Next



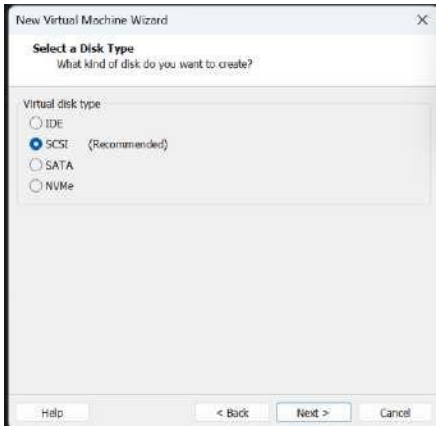
Click Next

Select NAT and Click Next

SUBHASH B
727722EUAI063



Click Next

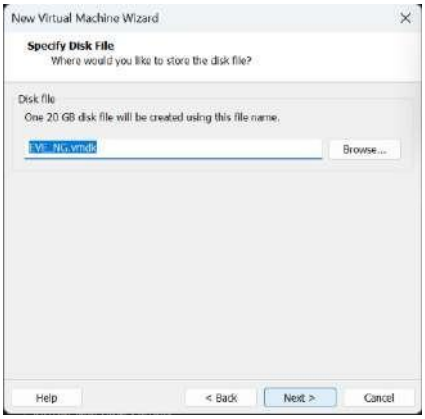


Click Next

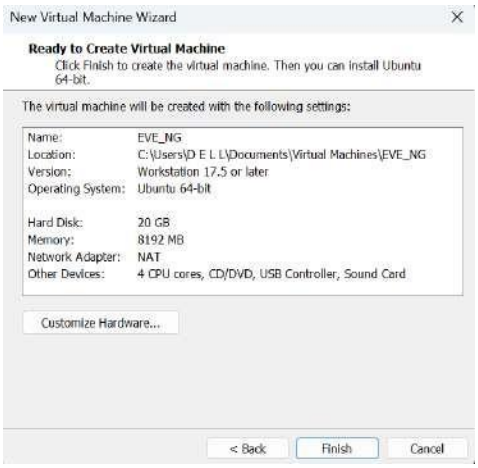
Choose New Virtual disk and Click Next

SUBHASH B
727722EUAI063

Choose Store virtual disk as a single file and Click Next

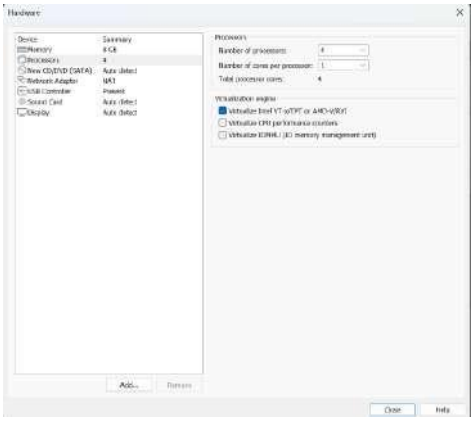


Click Next

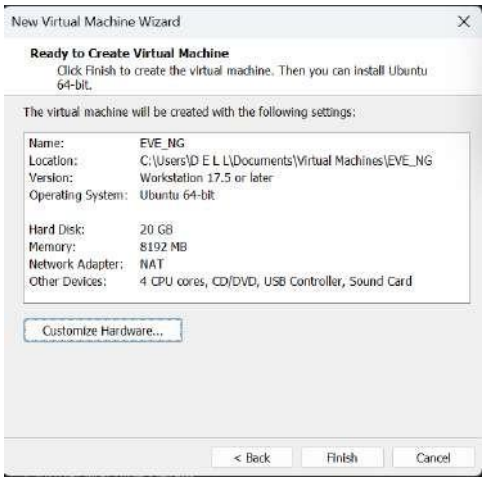


Click Customize Hardware

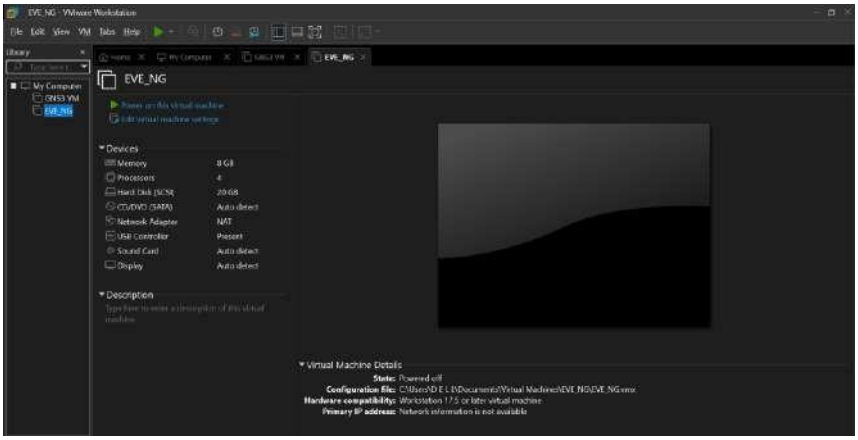
SUBHASH B
727722EUAI063



Choose Processors and Enable Virtualize Intel VT-x/EPT or AMD-V/RVI

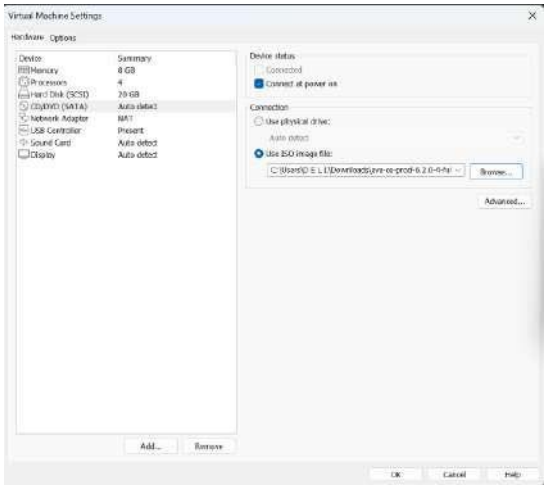


Click Finish

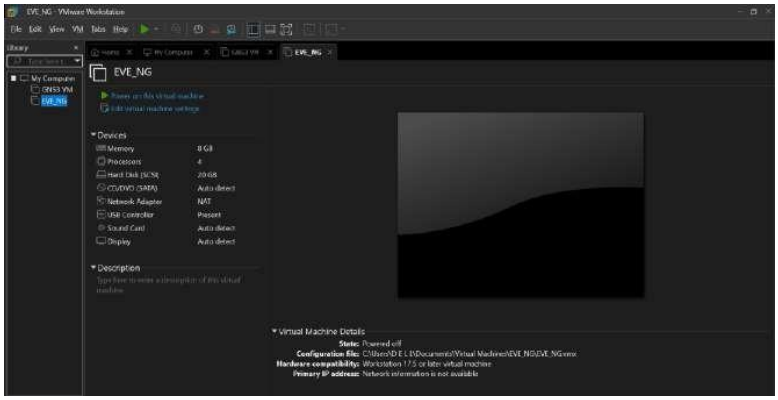


Choose EVE_NG and Edit virtual machine settings

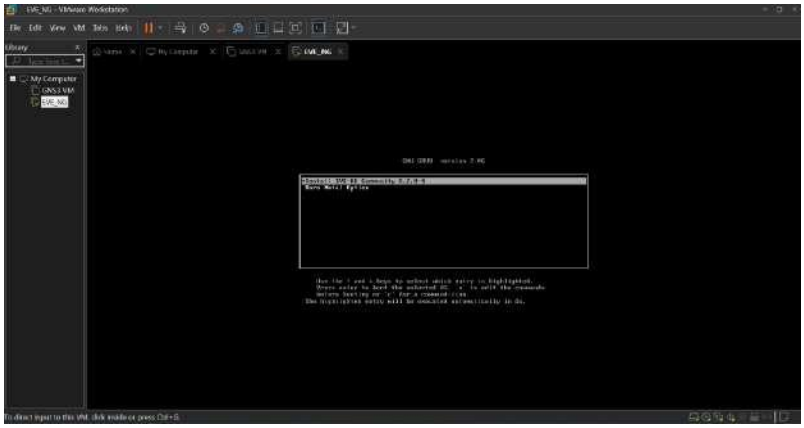
SUBHASH B
727722EUAI063



Select CD/DVD then Browse EVE-NG ISO file and Click OK

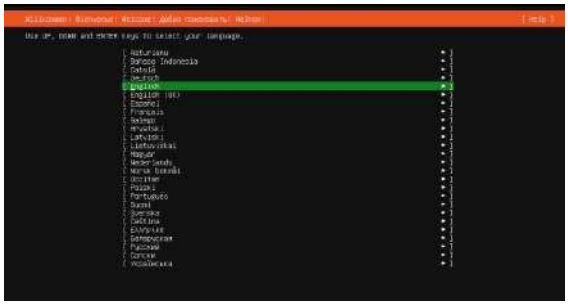


Click Power on this virtual machine

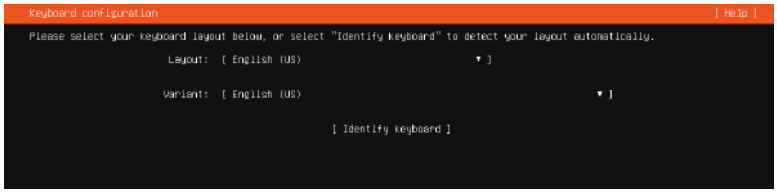


Choose Install EVE-NG

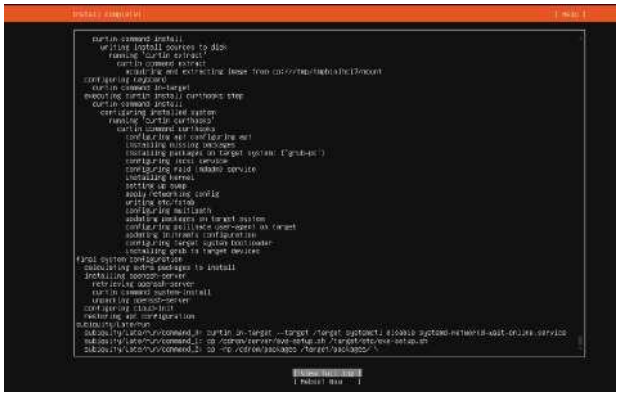
SUBHASH B
727722EUAI063



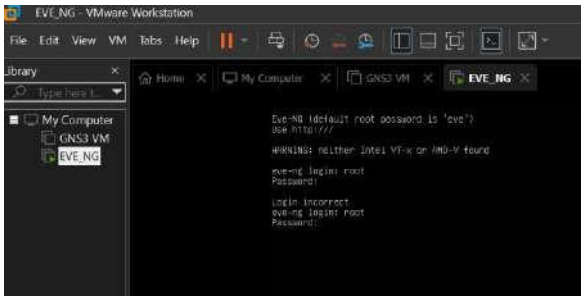
Choose English



Click Done

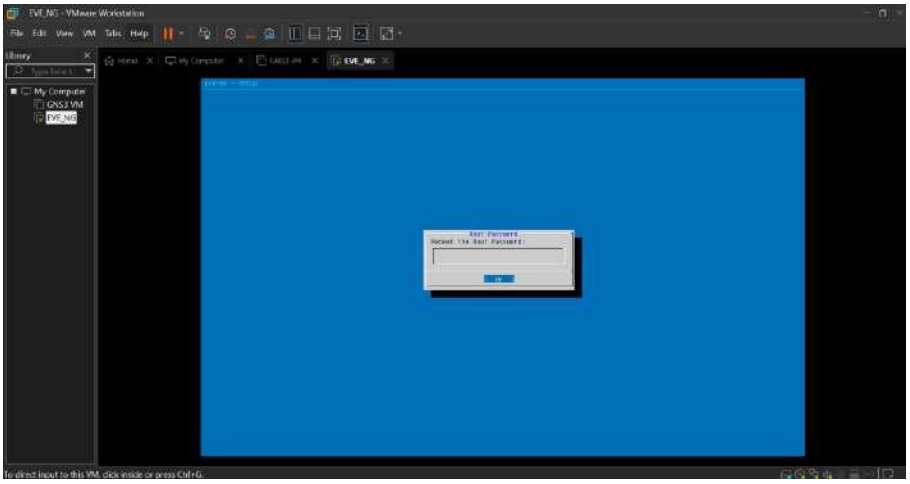


Click Reboot Now

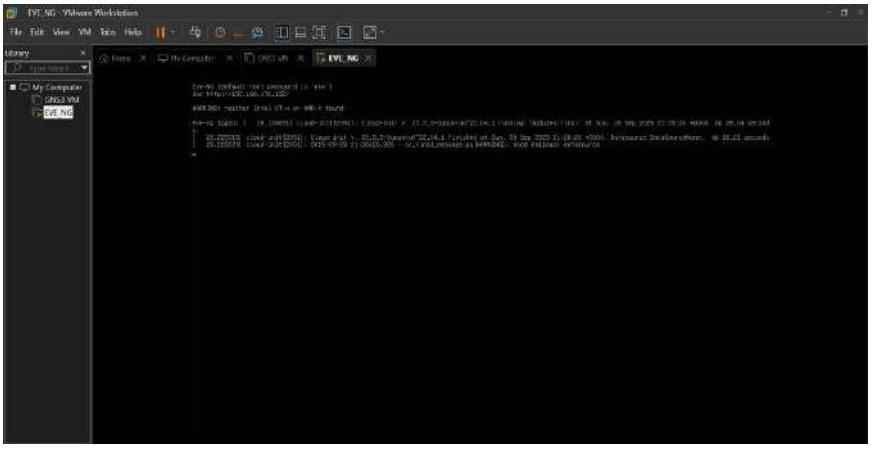


Login : root
Password : eve

SUBHASH B
727722EUAI063



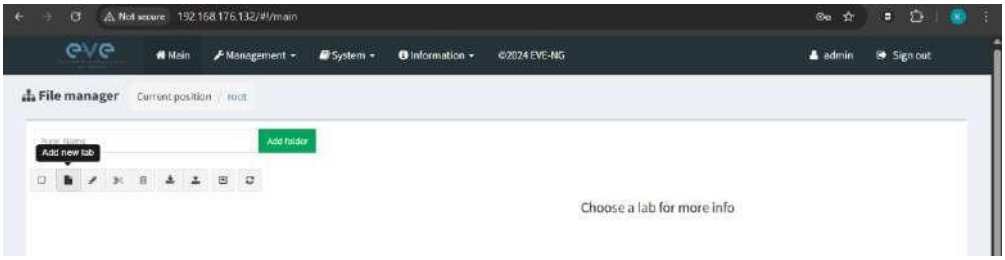
Set root password

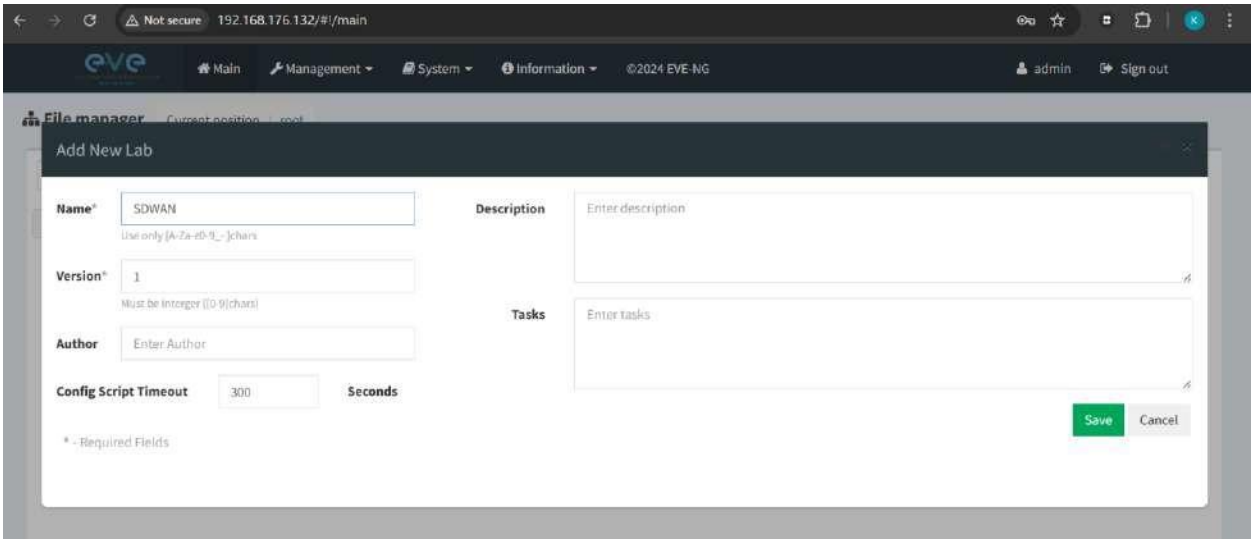


http://192.168.176.132

Username : admin password : eve

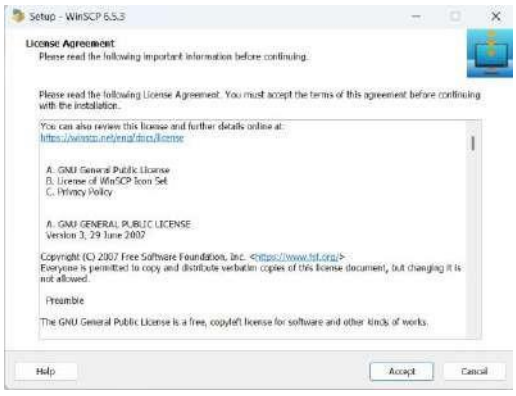
SUBHASH B
727722EUAI063



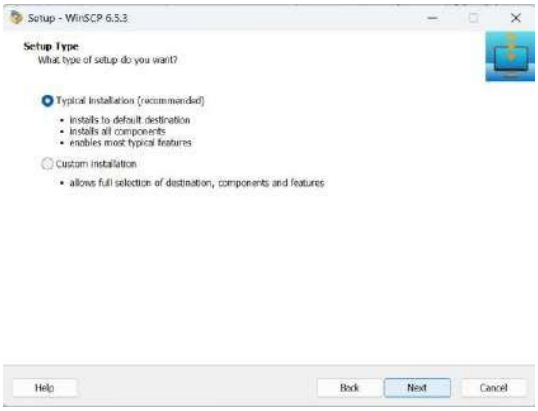


Enter Name: SDWAN

Instal WinSCP

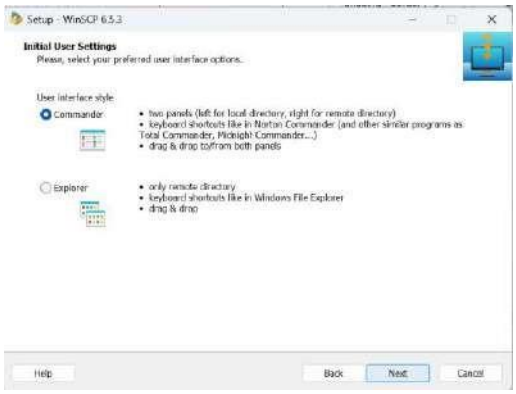


Click Accept

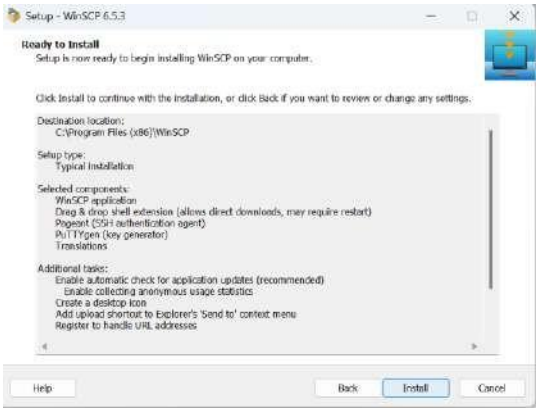


Select Typical and click Next

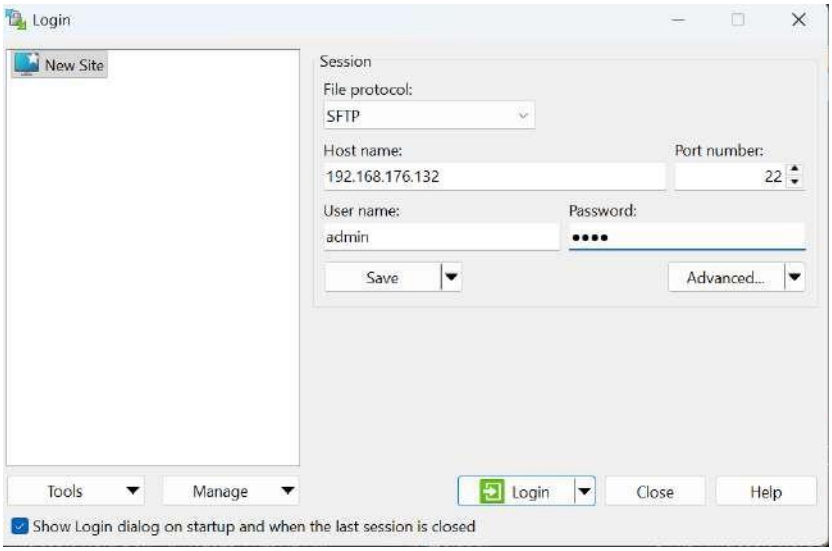
SUBHASH B
727722EUAI063



Select Commander and click next



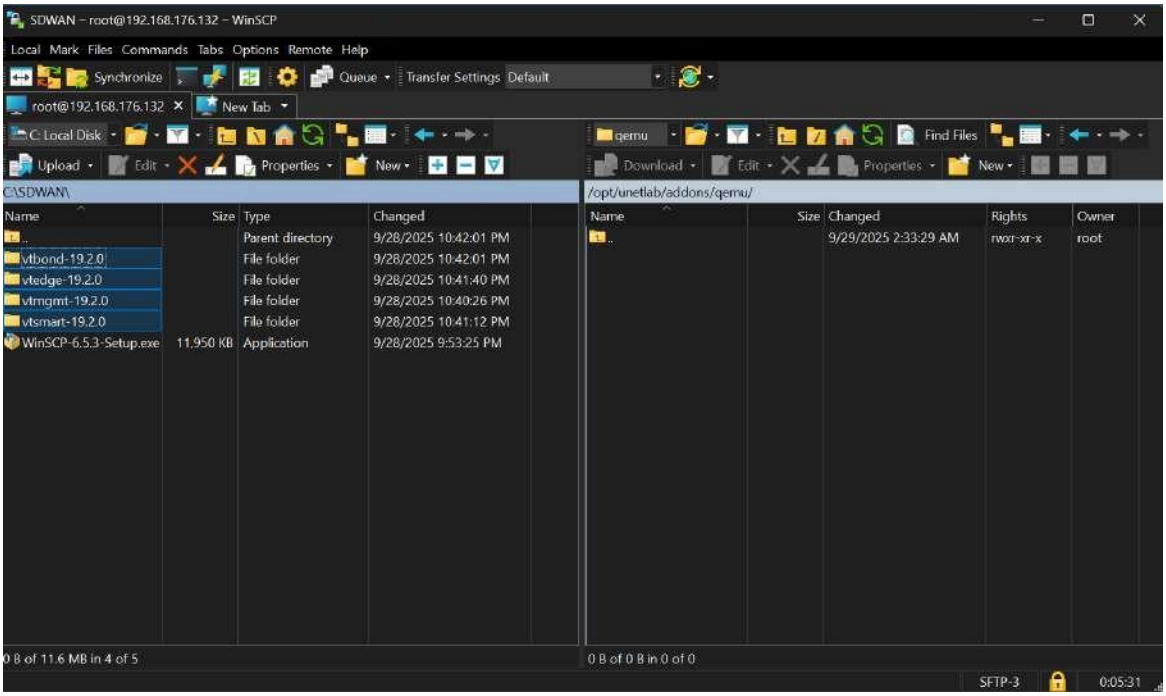
Click Install



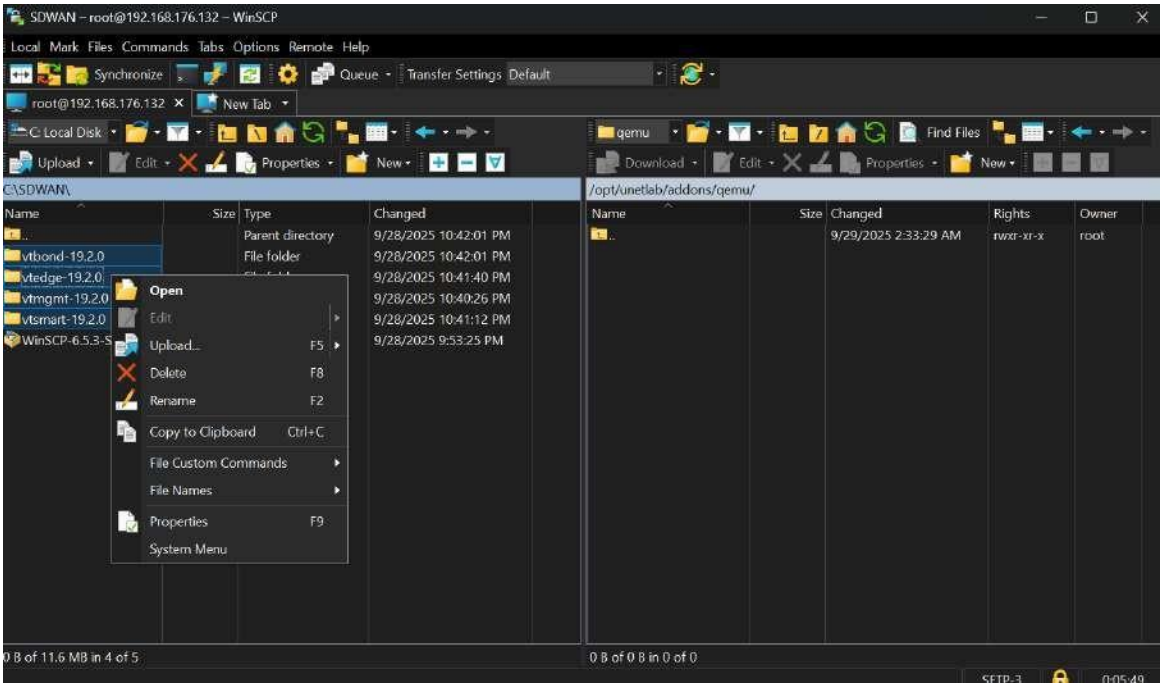
Host name : 192.168.172.132 Port number : 22

path: /opt/unetlab/addons/qemu

SUBHASH B
727722EUAI063

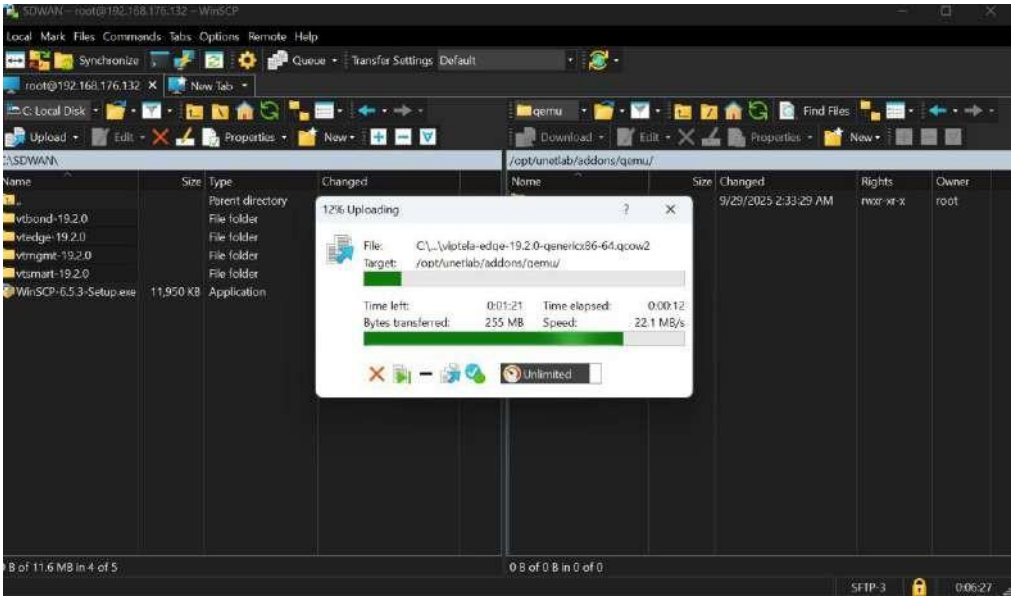


Change path to upload image

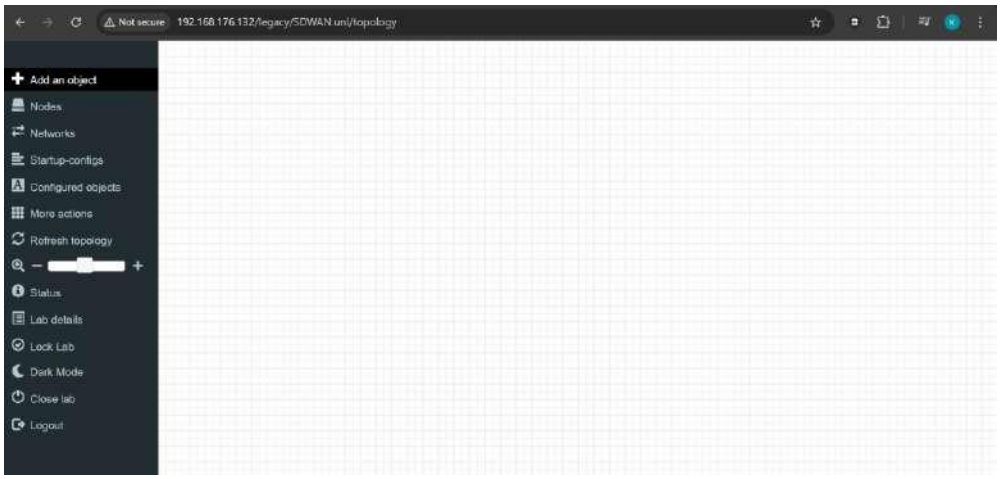


Right Click on images and Select Upload

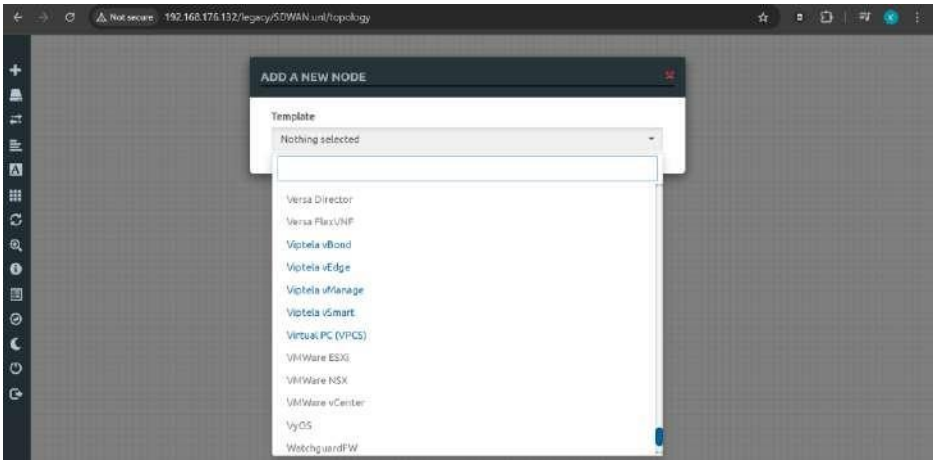
SUBHASH B
727722EUAI063



Install SecureCRT
After Installation Goto Windows Settings ->Apps->Default Apps->SecureCRT->TELNET->set default

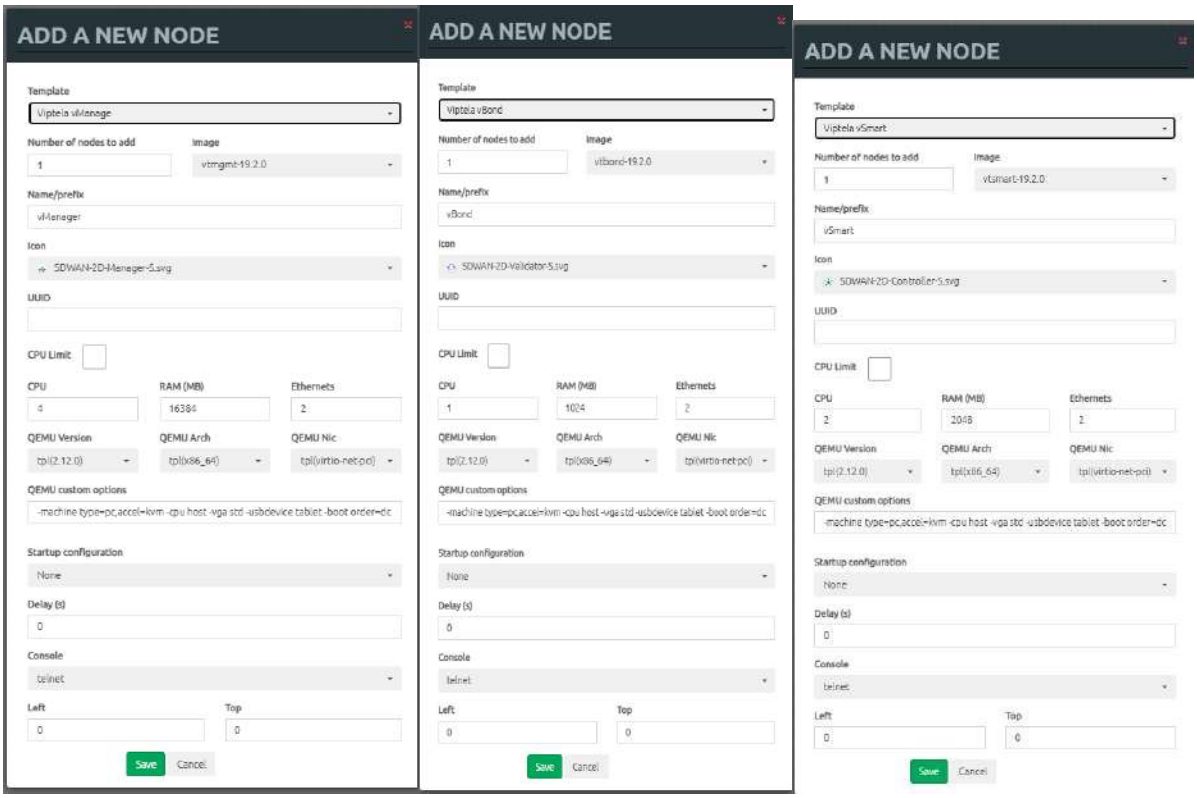


Click add an object and Click on Node



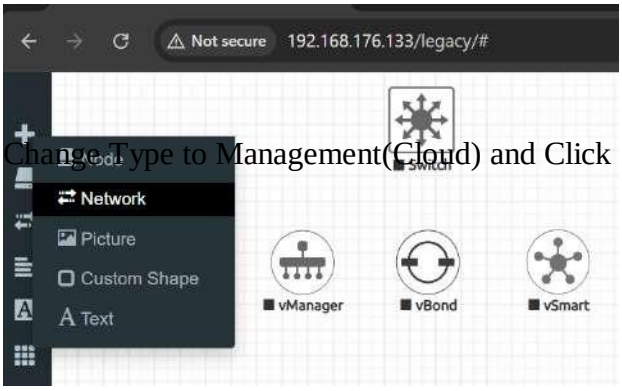
SUBHASH B
727722EUAI063

Add Nodes like vManage,vBond,vSmart,vEdge,CiscovIOS switch

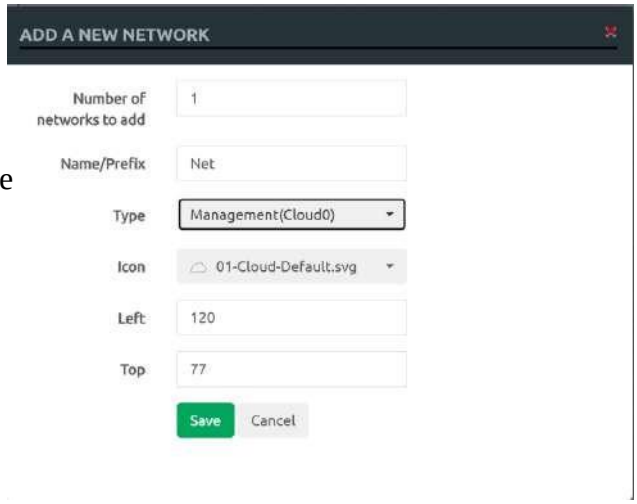


Click Add an object and Select Network

Add Nodes and Click Save

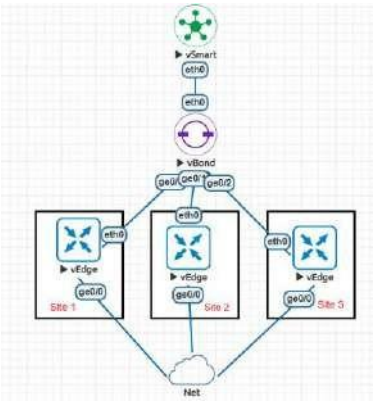


Change Type to Management(Cloud) and Click Save



SUBHASH B
727722EUAI063

NETWORK DIAGRAM:



CONFIGURATION:

VBond:

Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vedge
vedge# config t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# host-name vBond
vedge(config-system)# site-id 100
vedge(config-system)# system-ip 1.1.1.1
vedge(config-system)# organization-name SKCET
vedge(config-system)# vbond 10.0.0.1
vedge(config-system)# exit
vedge(config)# vpn 512
vedge(config-vpn-512)# int eth0
vedge(config-interface-eth0)# ip address 192.168.0.10/24
vedge(config-interface-eth0)# no shut
vedge(config-interface-eth0)# exit
vedge(config-vpn-512)# exit
vedge(config)# vpn 0
vedge(config-vpn-0)# int ge0/0
vedge(config-interface-ge0/0)# ip address 10.0.0.1/24
vedge(config-interface-ge0/0)# no shut
vedge(config-interface-ge0/0)# tunnel-interface

```
vedge(config-tunnel-interface)# encapsulation ipsec
vedge(config-tunnel-interface)# color default
vedge(config-tunnel-interface)# allow-service all
vedge(config-tunnel-interface)# exit
vedge(config-interface-ge0/0)# exit
vedge(config-vpn-0)# int ge0/1
vedge(config-interface-ge0/1)# ip address 10.0.1.1/24
vedge(config-interface-ge0/1)# no shut
vedge(config-interface-ge0/1)# tunnel-interface
vedge(config-tunnel-interface)# encapsulation ipsec
vedge(config-tunnel-interface)# color biz-internet
vedge(config-tunnel-interface)# allow-service all
vedge(config-tunnel-interface)# exit
vedge(config-interface-ge0/1)# int ge0/2
vedge(config-interface-ge0/2)# ip address 10.0.2.1/24
vedge(config-interface-ge0/2)# no shut
vedge(config-interface-ge0/2)# tunnel-interface
vedge(config-tunnel-interface)# encapsulation ipsec
vedge(config-tunnel-interface)# color mpls
vedge(config-tunnel-interface)# allow-service all
vedge(config-tunnel-interface)# exit
vedge(config-interface-ge0/2)# commit
Commit complete.
```

vSmart:

```
viptela 19.2.097
vsmart login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vsmart
You must set an initial admin password.
Password:
Re-enter password:
vsmart# config t
Entering configuration mode terminal
vsmart(config)# system
vsmart(config-system)# system-ip 1.1.1.2
vsmart(config-system)#host-name vSmart
```

```
vsmart(config-system)# site-id 200
vsmart(config-system)# organization-name SKCET
vsmart(config-system)# vbond 10.0.0.1
vsmart(config-system)# vpn 0
vsmart(config-vpn-0)# int eth0
vsmart(config-interface-eth0)# ip address 192.168.0.11/24
vsmart(config-interface-eth0)# no shut
vsmart(config-interface-eth0)# tunnel-interface
vsmart(config-tunnel-interface)# allow-service all
vsmart(config-tunnel-interface)# exit
vsmart(config-interface-eth0)# exit
vsmat(config-interface)# omp
vsmart(config-omp)# no shut
vsmart(config-omp)# graceful-restart
vsmart(config-omp)# commit
Commit complete.
```

vEdge1:

```
viptela 19.2.0

vedge login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vedge
You must set an initial admin password.
Password:
Re-enter password:
vedge# config t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# host-name vEdge1
vedge(config-system)# site-id 300
vedge(config-system)# system-ip 1.1.1.3
vedge(config-system)# organization-name SKCET
vedge(config-system)# vbond 10.0.0.1
vedge(config-system)# vpn 0
vedge(config-vpn-0)# int ge0/0
vedge(config-interface-ge0/0)# ip address 10.0.0.3/24
```

```
vedge(config-interface-ge0/0)# no shut
vedge(config-interface-ge0/0)# tunnel-interface
vedge(config-tunnel-interface)# encapsulation ipsec
vedge(config-tunnel-interface)# allow-service all
vedge(config-tunnel-interface)# exit
vedge(config-interface-ge0/0)# exit
vedge(config-vpn-0)# omp
vedge(config-omp)# advertise connected
vedge(config-omp)# advertise static
vedge(config-omp)# no shut
vedge(config-omp)# commit
Commit complete.
```

vEdge2:

```
viptela 19.2.0

vedge login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vedge
You must set an initial admin password.
Password:
Re-enter password:
vedge# config t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# host-name vEdge2
vedge(config-system)# system-ip 1.1.1.4
vedge(config-system)# site-id 400
vedge(config-system)# organization-name SKCET
vedge(config-system)# vbond 10.0.0.1
vedge(config-system)# vpn 0
vedge(config-vpn-0)# int ge0/1
vedge(config-interface-ge0/1)# ip address 10.0.0.4/24
vedge(config-interface-ge0/1)# no shut
vedge(config-interface-ge0/1)# tunnel-interface
vedge(config-tunnel-interface)# encapsulation ipsec
vedge(config-tunnel-interface)# color biz-internet
vedge(config-tunnel-interface)# allow-service all
```

```
vedge(config-tunnel-interface)# exit
vedge(config-interface-ge0/1)#  exit
vedge(config-vpn-0)# omp
vedge(config-omp)# advertise connected
vedge(config-omp)# advertise static
vedge(config-omp)# no shut
vedge(config-omp)# commit
Commit complete.
```

VEdge3:

```
vedge login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vedge
You must set an initial admin password.
Password:
Re-enter password:
vedge# config t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# host-name vEdge3
vedge(config-system)# system-ip 1.1.1.5
vedge(config-system)# site-id 500
vedge(config-system)# organization-name SKCET
vedge(config-system)# vbond 10.0.0.1
vedge(config-system)# vpn 0
vedge(config-vpn-0)# int ge0/2
vedge(config-interface-ge0/2)# ip address 10.0.0.5/24
vedge(config-interface-ge0/2)# no shut
vedge(config-interface-ge0/2)# tunnel-interface
vedge(config-tunnel-interface)# encapsulation ipsec
vedge(config-tunnel-interface)# color mpls
vedge(config-tunnel-interface)# allow-service all
vedge(config-tunnel-interface)# exit
vedge(config-interface-ge0/2)# exit
vedge(config-vpn-0)# omp
vedge(config-omp)# advertise connected
vedge(config-omp)# advertise static
vedge(config-omp)# no shut
```

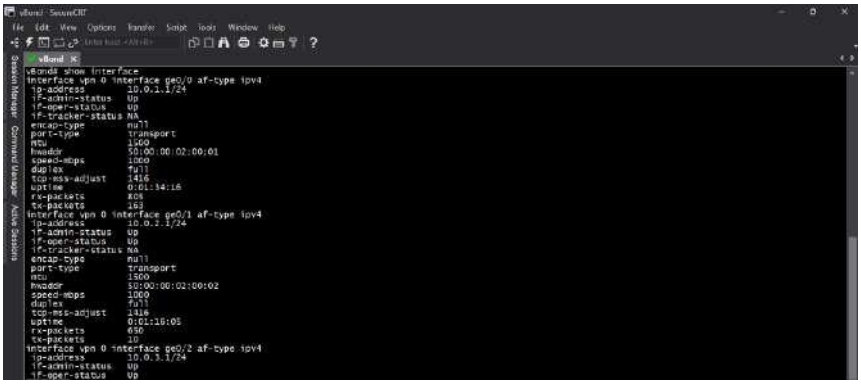
vedge(config-omp)# commit

Commit complete.

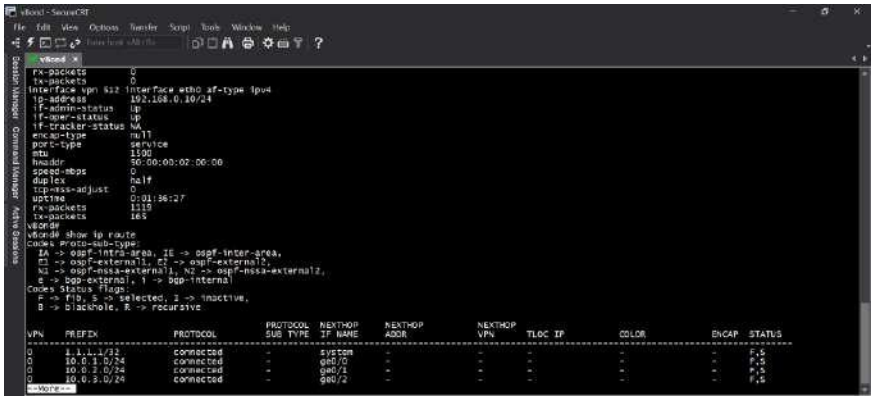
OUTPUT:

vBond:

Show interface



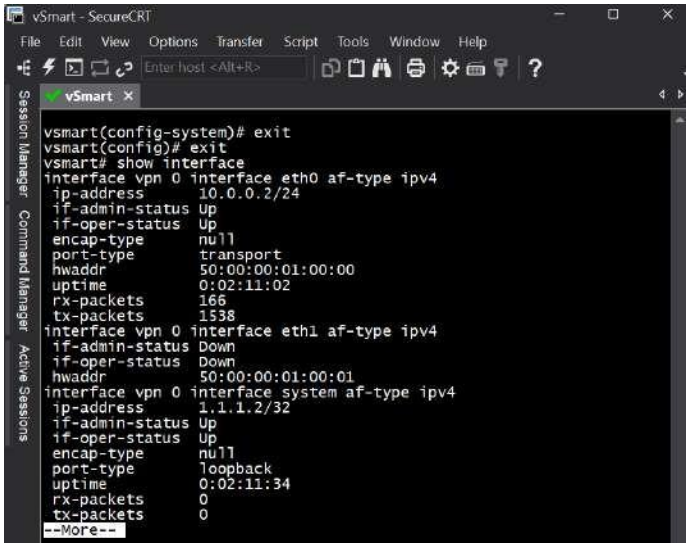
Show ip route



vSmart:

Show interface

SUBHASH B
727722EUAI063

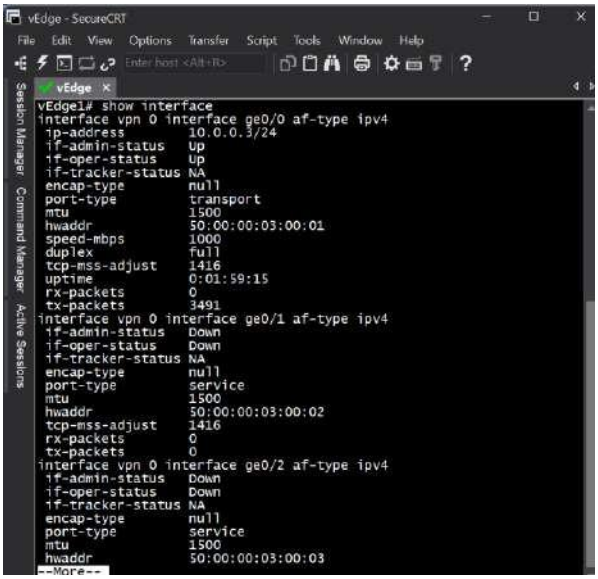


Show ip route

vEdge1:

Show interface

SUBHASH B
727722EUAI063



Show ip route

RESULT:

Thus the traffic shifts to the backup route when the main link fails, showing basic SD-WAN-like failover using static routes was simulated successfully.