COMPUTER NETWORKS-II LAB MASTER FILE

COURSE OUTCOME:

After completion of the Course, the trainee should be able to:

1. *Configure secure LAN and Wireless LAN.*
2. *Configure static and dynamic (OSPF) routing.*
3. *Implement access control list to secure the network.*
4. *Configure PAT interface implementation and NTP settings.*
5. *Implement NAT concept for IP address translation.*
6. *Configure TFTP server for backup.*

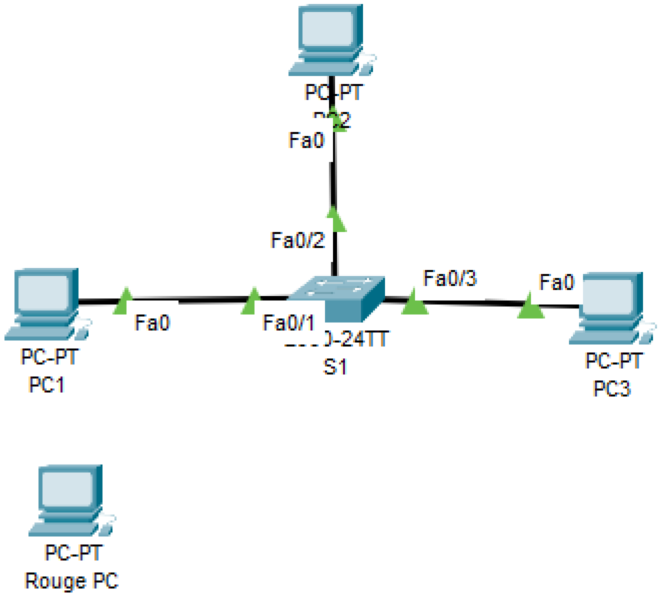
Compiled by : Anoop Jacob - CCNA Instructor

EXERCISE NO.1

Implement Port Security

- -Configure Port Security
- -Verify Port Security

TOPOLOGY



DEVICE MODLES

DEVICE NAME	MODEL
S1	2960

ADDRESSING TABLE

Device	Interface	IP Address	Subnet Mask	Description
PC1	NIC	192.168.10.10	255.255.255.0	Connected to S1 Fa0/1
PC2	NIC	192.168.10.11	255.255.255.0	Connected to S1 Fa0/2
PC3	NIC	192.168.10.12	255.255.255.0	Connected to S1 Fa0/3
Rouge PC	NIC	192.168.10.13	255.255.255.0	Need to Connect to S1 Fa0/1 to check Port-Security

S1 Configuration

```
Switch>enable
Switch#conf t
Switch(config)#hostname S1

S1(config)#interface fa0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security mac-address sticky

S1(config-if)#interface fa0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation restrict

S1(config-if)#interface fa0/3
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security mac-address 000C.CF35.D496 (MAC Address of PC3)
S1(config-if)#switchport port-security violation protect
S1(config-if)#do show port int fa0/3

S1(config-if)#interface range fa0/4-24,g0/1-2
S1(config-if-range)#shutdown

S1(config-if-range)#end
S1#copy run start
```

PC1 IP Configuration
IPv4 Address: 192.168.10.10
Subnet: 255.255.255.0

PC2 IP Configuration
IPv4 Address: 192.168.10.11
Subnet: 255.255.255.0

HR-PC1 IP Configuration
IPv4 Address: 192.168.10.12
Subnet: 255.255.255.0

HR-PC2 IP Configuration

IPv4 Address: 192.168.10.13
Subnet: 255.255.255.0

Verify Port Security

From PC1, ping PC2.

- Verify that port security is enabled and the MAC addresses of PC1 and PC2 were added to the running configuration.
  ```
  S1#show run | begin interface
  ```
- Attach Rogue PC to any unused switch port and notice that the link lights are red.
- Disconnect PC1 and connect Rogue PC to F0/1, which is the port to which PC1 was originally connected. Verify that Rogue Laptop is unable to ping PC2.
- Display the port-security violation for the port to which Rogue Laptop is connected.
  ```
  S1# show port-security interface f0/1
  ```
- Connect back to PC1 and activate the interface fa0/1
  ```
  S1(config)#interface fa0/1
  S1(config-if)#shutdown
  S1(config-if)#no shutdown
  ```

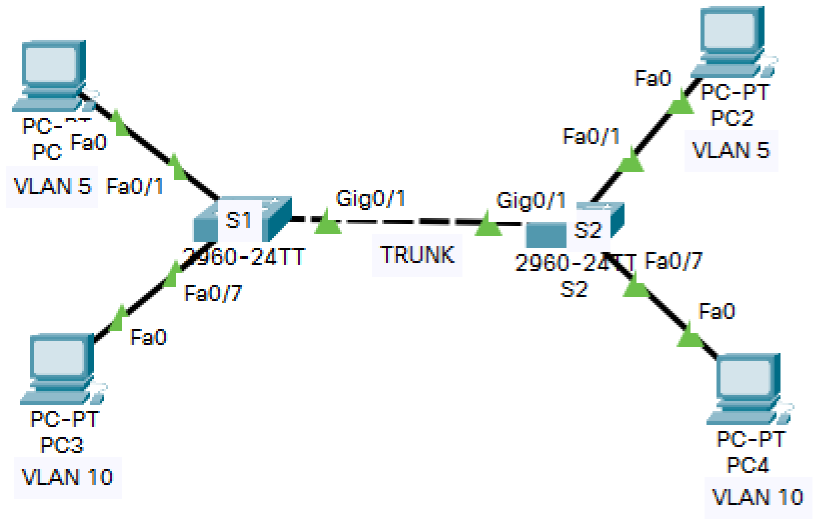
Result: *Configured and Verified Port-Security successfully.*

AEXERCISE NO.2

Switch Security Configuration

-Create a Secure Trunk
-Secure Unused Switch ports
-Implement Port Security
-Enable DHCP Snooping
-Configure Rapid PVST Port Fast and BPDU Guard

TOPOLOGY



DEVICE MODELS

DEVICE NAME	MODEL
S1	2960
S2	2960

ADDRESSING TABLE

Device	Interface	IP Address	Subnet Mask	Description
S1	VLAN 15	192.168.15.254	255.255.255.0	SVI for Management
S2	VLAN 15	192.168.15.253	255.255.255.0	SVI for Management
PC1	NIC	192.168.5.10	255.255.255.0	Connected to S1 Fa0/1
PC2	NIC	192.168.5.11	255.255.255.0	Connected to S2 Fa0/1
PC3	NIC	192.168.10.10	255.255.255.0	Connected to S1 Fa0/7
PC4	NIC	192.168.10.11	255.255.255.0	Connected to S2 Fa0/7

VLAN Table

VLAN ID	VLAN Name	Network Address	Subnet Mask	Ports to be assigned
5	HR	192.168.5.0	255.255.255.0	S1, S2: Fa0/1-6
10	Accounts	192.168.10.0	255.255.255.0	S1, S2: Fa0/7-12
15	Management	192.168.15.0	255.255.255.0	
25	Native	NOT APPLICABLE		S1, S2: G0/1
35	Unused	NOT APPLICABLE		S1, S2: Fa0/13-24,G0/2

S1 Configuration

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#vlan 5
S1(config-vlan)#name HR
S1(config-vlan)#vlan 10
S1(config-vlan)#name Accounts
S1(config-vlan)#vlan 15
S1(config-vlan)#name Management
S1(config-vlan)#vlan 25
S1(config-vlan)#name Native
S1(config-vlan)#vlan 35
S1(config-vlan)#name Unused

S1(config-vlan)#interface vlan 15
S1(config-if)#ip address 192.168.15.254 255.255.255.0

S1(config-vlan)#interface g0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 25
S1(config-if)#switchport trunk allowed vlan 5,10,15,25
S1(config-if)#switchport nonegotiate

S1(config-if)#interface range fa0/1-6
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#interface range fa0/7-12
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#interface range fa0/13-24,g0/2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 35
S1(config-if-range)#shutdown
```

```
S1(config-if-range)#interface range fa0/1-12
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security mac-address sticky
S1(config-if-range)#exit

S1(config)#spanning-tree mode rapid-pvst
S1(config-if-range)#interface range fa0/1-12
S1(config-if-range)#spanning-tree portfast
S1(config-if-range)#spanning-tree bpduguard enable

S1(config-if-range)#exit
S1(config)#ip dhcp snooping
S1(config)#ip dhcp snooping vlan 5,10,15,25

S1(config)#exit
S1#copy run start
```

S2 Configuration

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S2
S2(config)#vlan 5
S2(config-vlan)#name HR
S2(config-vlan)#vlan 10
S2(config-vlan)#name Accounts
S2(config-vlan)#vlan 15
S2(config-vlan)#name Management
S2(config-vlan)#vlan 25
S2(config-vlan)#name Native
S2(config-vlan)#vlan 35
S2(config-vlan)#name Unused

S2(config-vlan)#interface vlan 15
S2(config-if)#ip address 192.168.15.253 255.255.255.0

S2(config-vlan)#interface g0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 25
S2(config-if)#switchport trunk allowed vlan 5,10,15,25
S2(config-if)#switchport nonegotiate

S2(config-if)#interface range fa0/1-6
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#interface range fa0/7-12
S2(config-if-range)#switchport mode access
```

```
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#interface range fa0/13-24,g0/2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 35
S2(config-if-range)#shutdown
S2(config-if-range)#interface range fa0/1-12
S2(config-if-range)#switchport port-security
S2(config-if-range)#switchport port-security mac-address sticky
S2(config-if-range)#switchport port-security violation restrict
21(config-if-range)#exit

S2(config)#spanning-tree mode rapid-pvst
S2(config-if-range)#interface range fa0/1-12
S2(config-if-range)#spanning-tree portfast
S2(config-if-range)#spanning-tree bpduguard enable


S2(config-if-range)#exit
S2(config)#ip dhcp snooping
S2(config)#ip dhcp snooping    vlan 5,10,15,25

S2(config)#exit
S2#copy run start
```

PC1 IP Configuration
IPv4 Address: 192.168.5.10
Subnet: 255.255.255.0

PC2 IP Configuration
IPv4 Address: 192.168.5.11
Subnet: 255.255.255.0

PC3 IP Configuration
IPv4 Address: 192.168.10.10
Subnet: 255.255.255.0

PC4 IP Configuration
IPv4 Address: 192.168.10.11
Subnet: 255.255.255.0

Verification Commands Used:

```
S1#show vlan brief
S1#show interfaces trunk
S1#show running-config
```

End-to-End Connectivity Result

Ping From	Ping To	To IP Address	Successful Yes/No
PC1	PC2	192.168.5.11	Yes
PC3	PC4	192.168.10.11	Yes
S1	S2	192.168.15.253	Yes

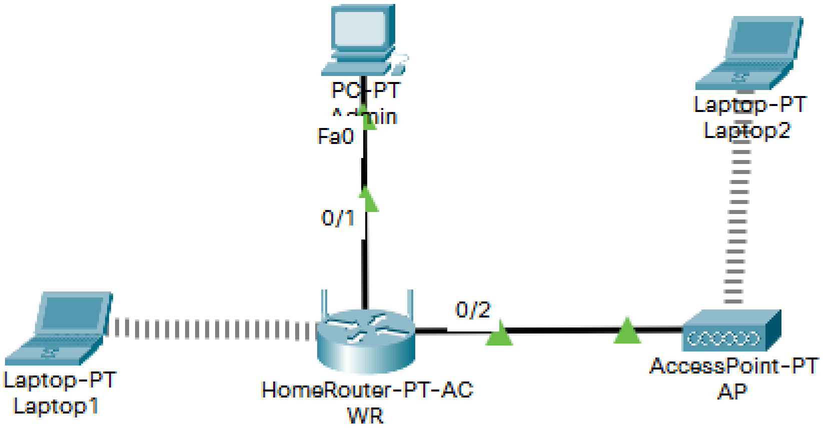
Result: *Configured and Verified Switch Security Configuration successfully.*

EXERCISE NO.3

Configure a Wireless Network

- -Connect to a wireless router
- -Configure the wireless router
- -Connect a wired device to the wireless router
- -Connect a wireless device to the wireless router
- -Add an AP to the network to extend wireless coverage
- -Update default router settings

TOPOLOGY



DEVICE MODELS

DEVICE NAME	MODEL
WR	HomeRouter-PT-AC
AP	AccessPoint-PT

Connect to a Wireless Router

Connect Admin to WR.

a. Connect **Admin** to **WR** using a straight-through Ethernet cable through the Ethernet ports. Select **Connections**, represented by a lightning bolt, from the bottom-left side of Packet Tracer. Click **Copper Straight-Through**, represented by a solid black line.

b. When the cursor changes to connection mode, click **Admin** and choose **FastEthernet0**. Click **WR** and choose an available Ethernet port to connect the other end of the cable.

WR will act as a switch to the devices connected to the LAN and as a router to the internet. **Admin** is now connected to the LAN (GigabitEthernet 1). When Packet Tracer displays green triangles on both sides of the connection between **Admin** and **WR**, continue to the next step.

Configure Admin to use DHCP.

To reach the **WR** management page, **Admin** must communicate on the network. A wireless router usually includes a DHCP server, and the DHCP server is usually enabled by default on the LAN. **Admin** will receive IP address information from the DHCP server on **WR**.

a. Click **Admin**, and select the **Desktop** tab.
b. Click **IP Configuration** and select **DHCP**

Connect to the WR Web Interface

a. In the Desktop tab on Admin, choose Web Browser.
b. Enter **192.168.0.1** in the URL field to open the web configuration page of the wireless router.
c. Use **admin** for both the username and password.
d. Under the Network Setup heading on the **Basic Setup** page, notice the IP address range for the DHCP server.

Configure the Wireless Settings

Configure the WR SSID.

a. Navigate to the **WR** GUI interface at **192.168.0.1** in a web browser on **Admin**.
b. Navigate to **Wireless** > **Basic Wireless Settings**.
c. Change **Network Name** (SSID) to **Annexe_WiFi1** for only **2.4 GHz**. Notice that SSIDs are case-sensitive.
d. Change the **Standard Channel** to **6 - 2.437GHz**.
e. For this activity, disable both 5 GHz frequencies. Leave the rest of the settings unchanged.
f. Scroll to the bottom of the window and click **Save Settings**.

Configure wireless security settings.

In this step, you configure the wireless security settings using WPA2 security mode with encryption and passphrase.
a. Navigate to **Wireless** > **Wireless Security**.
b. Under the 2.4 GHz heading, select **WPA2 Personal** for the **Security Mode**.
c. For the Encryption field, keep the default **AES** setting.
d. In the Passphrase field, enter **Cisco123** as the passphrase.
e. Click **Save Settings**.
f. Verify that the settings in the **Basic Wireless Settings** and **Wireless Security** pages are correct and saved.

Connect the Wireless Clients.

a. Open Laptop1. Select **Physical** tab, power off Laptop, remove Ethernet module, and add **Linksys-WPC300N** module.
b. Open Laptop1. Select **Desktop** tab, click **PC Wireless**.
c. Select the **Connect** tab. Click Refresh as necessary. Select the Wireless Network Name **Annexe_WiFi1**.
d. Enter the passphrase configured in the previous step. Enter **Cisco123** In the pre-shared key field and click Connect. Close the PC Wireless window.
e. Open **command prompt** and ping to **Admin** (192.168.0.1) and should succeed.

Connect Wireless Clients to an Access Point

An access point (AP) is a device that extends the wireless local area network. An access point is connected to a wired router using an Ethernet cable to project the signal to a desired location.

Configure the Access Point.

a. Connect **Port 0** of **AP** to an available Ethernet port of **WR** using a **straight-through** Ethernet cable.
b. Click **AP**. Select the Config tab.
c. Under the INTERFACE heading, select **Port 1**.
d. In the **SSID** field, enter **Annexe_WiFi2**.

e. Select **WPA2-PSK**. Enter the passphrase Cisco123 In the Pass Phrase field.
f. Keep **AES** as the default Encryption Type.

Connect the Wireless Clients.

a. Open **Laptop2**. Select **Physical** tab, power off Laptop, remove Ethernet module, and add **Linksys-WPC300N** module.
b. Open Laptop2. Select **Desktop** tab, click **PC Wireless**.
c. Select the **Connect** tab. Click Refresh as necessary. Select the Wireless Network Name **Annexe_WiFi2** and click **Connect**.
d. Open **command prompt** and ping to Admin (192.168.0.1) and should succeed.

Update default router settings

Change the WR Access Password.

a. On **Admin**, navigate to **WR** GUI interface at **192.168.0.1**.
b. Navigate to **Administration** > **Management** and change the current Router **Password** to **cisco**.
c. Scroll to the bottom of the window and click **Save Settings**.
d. Use the username **admin** and the new password **cisco** when prompted to log in to the wireless router. Click **OK** to continue.
e. Click **Continue** and move on to the next step.

Change the DHCP address range in WR.

In this step, you will change the internal network address from 192.168.0.0/24 to 192.168.50.0/24. When the LAN network address changes, the IP addresses on the devices in the LAN must be renewed to receive new IP addresses before the lease is timed out.
a. Navigate to **Setup** > **Basic Setup**.
b. Scroll down the page to **Network Setup**.
c. The IP address assigned to Router IP is **192.168.0.1**. Change it to **192.168.50.1**. Verify that IP address still start at .100, and there are 50 available IP addresses in the **DHCP** pool.
d. Scroll to the bottom of the window and **click Save Settings**.
e. Note that the **DHCP** range of addresses has been automatically updated to reflect the interface IP address change. The **Web Browser** will display a Request Timeout after a short time. Because the **Admin** IP address is no longer within the same network as the router. The IP address of **Admin** is outside the new range of the **DHCP** server.
f. Close the **Admin** web browser.
g. In **Admin Desktop** tab, click **Command Prompt**.
h. Type **ipconfig /renew** to force Admin re-acquire its IP information via **DHCP**.
i. Renew the IP address on other laptop.

Result: *Configured and Verified a Wireless Network successfully.*

EXERCISE NO.4

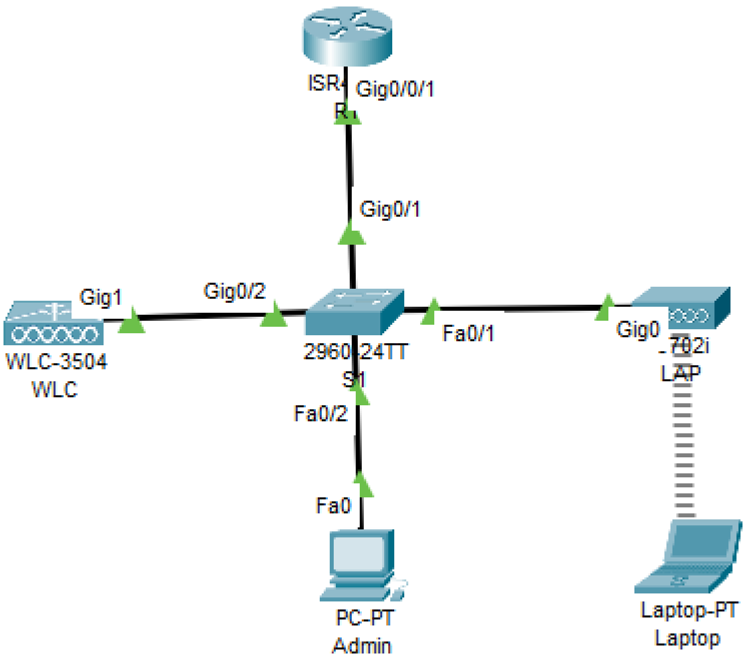
Configure a Basic WLAN on the WLC

-Monitor the WLC

-Create a Wireless LAN

-Connect a Host to the WLAN

TOPOLOGY



DEVICE MODELS

DEVICE NAME	MODEL
R1	ISR4331
S1	2960
WLC	WLC-3504
LAP	3702i

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
R1	G0/0/1	192.168.1.1	255.255.255.0	Not Applicable	Connected to S1 G0/1
WLC	Management	192.168.1.2	255.255.255.0	192.168.1.1	WLC Management
LAP	NIC	DHCP			Connected to S1 Fa0/1
Admin	NIC	DHCP			Connected to S1 Fa0/2
Laptop	NIC	DHCP			Wirelessly Connected to LAP

Router R1 Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#interface g0/0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
R1(config)#ip dhcp pool DHCP_Pool
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#end
R1#copy run start
```

Configure the WLC

Go to **Admin** PC -> **Desktop** -> **Web Browser**
Type **192.168.1.2** and click go (Need to wait nearly 1 minute to get the Page)

Create admin username: admin
Create admin password: Cisco123
Confirm admin password: Cisco123
Then click Start

Setup Your Controller as follows

System Name: WLC
Management IP Address: 192.168.1.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1
(Note: Leave other options as default)
Then click Next

Create your Wireless Networks as follows

Network Name: CP08
Security: WPA2 Personal
Passphrase: Cisco123
Confirm Passphrase: Cisco123
(Note: Leave other options as default)
Then click Next

Advanced Settings as default then click Next

Please confirm settings and apply (There will be a reboot message, click Ok)
Close the Admin Window

Monitor the WLC

Wait until STP has converged on the network. You can click the Packet Tracer Fast Forward Time button to speed up the process. Continue when all link lights are green.

Go the desktop of Admin PC and open a browser. Enter the management IP address 192.168.1.1 of WLC into the address bar. You must specify the HTTPS protocol.

Click Login and enter the following credentials:

User Name: admin

Password: Cisco123.

After a short delay, you will see the WLC Monitor Summary screen.

Create and enable the WLAN. (Remove Existing WLANs)

Click WLANs in the WLC menu bar. Locate the dropdown box in the upper right had corner of the WLANs screen. It will say Create New. Click Go to create a new WLAN.

Enter the Profile Name of the new WLAN. Use the profile name NTTF. Assign an SSID of CP08 to the WLAN. Hosts will need to use this SSID to join the network.

Select the ID for the WLAN. This value is a label that will be used to identify the WLAN is other displays. Select a value of 5 to keep it consistent with the VLAN number and SSID. This is not a requirement but it helps with understanding the topology.

Click Apply so that the settings go into effect.

Now that the WLAN has been created, you can configure features of the network. Click Enabled to make the WLAN functional. It is a common mistake to accidentally skip this step.

Click the Advanced tab.

Scroll down to the FlexConnect portion of the page. Click to enable FlexConnect Local Switching and FlexConnect Local Auth.

Click Apply to enable the new WLAN. If you forget to do this, the WLAN will not operate.

Secure the WLAN.

In the WLANs Edit screen for the NTTF WLAN, click the Security tab. Under the Layer 2 tab, select WPA+WPA2 from the Layer 2 Security drop down box. This will reveal the WPA parameters.

Click the checkbox next to WPA2 Policy. This will reveal additional security settings. Under Authentication Key Management, enable PSK.

Now you can enter the pre-shared key that will be used by hosts to join the WLAN. Use Cisco123 as the passphrase.

Click Apply to save these settings.

Note: It is not a good practice to reuse passwords when configuring security. We have reused passwords in this activity to simplify configuration.

Connect a Host to the WLAN

Open Laptop, select Physical tab, power off Laptop, remove Ethernet module, and add Linksys-WPC300N module

Go to the desktop of Laptop and click the PC Wireless tile.

Click the Connect tab. After a brief delay you should see the SSID for the WLAN appear in the table of wireless network names. Select the CP08 network and click the Connect button.

Enter the pre-shared key that you configured for the WLAN and click Connect.

Click the Link Information tab. You should see a message that confirms that you have successfully connected to the access point. You should also see a wireless wave in the topology showing the connection to LAP.

Click the More Information button to see details about the connection.
Close the PC Wireless app and open the IP Configuration app. Verify that Wireless Host has received a non-APIPA IP address over DHCP. If not, click the Fast Forward Time button a few times.
From Wireless Host, ping the WLAN default gateway and the Server to verify that the laptop has full connectivity.

Result: *Configured and Verified a Basic WLAN on the WLC.*

EXERCISE NO.5

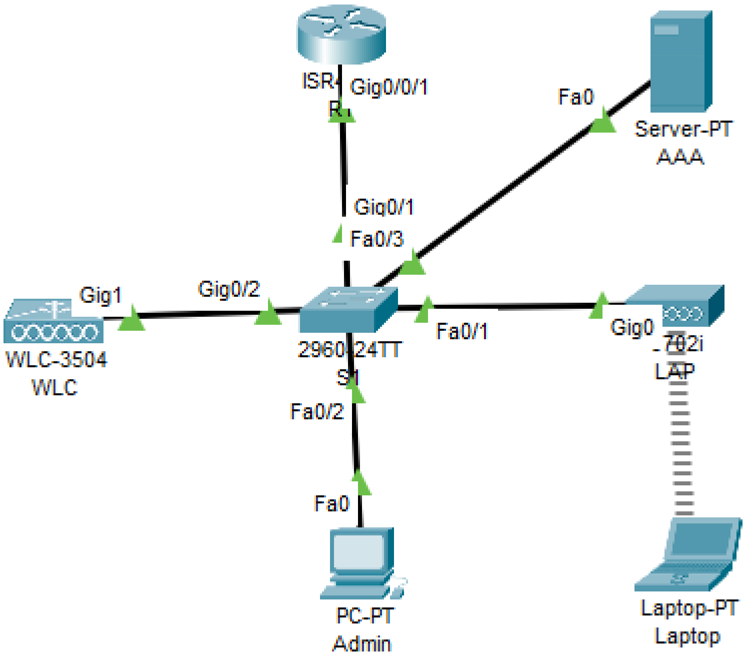
Configure a WPA2 Enterprise WLAN on the WLC

-Create a new WLAN

-Configure a DHCP Scope and SNMP

-Connect Hosts to the Network

TOPOLOGY



DEVICE MODELS

DEVICE	MODEL
R1	ISR4331
S1	2960
WLC	WLC-3504
LAP	3702i

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
R1	G0/0/1	192.168.1.1	255.255.255.0	Not Applicable	Connected to S1 G0/1
WLC	Management	192.168.1.2	255.255.255.0	192.168.1.1	WLC Management
LAP	NIC	DHCP			Connected to S1 Fa0/1
Admin	NIC	DHCP			Connected to S1 Fa0/2
AAA	NIC	192.168.1.3	255.255.255.0	192.168.1.1	Connected to S1 Fa0/3
Laptop	NIC	DHCP			Connected Wirelessly to LAP

Router R1 Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#interface g0/0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
R1(config)#ip dhcp pool DHCP_Pool
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#end
R1#copy run start
```

Configure the WLC

Go to **Admin** PC -> **Desktop** -> **Web Browser**
Type **192.168.1.2** and click go (Need to wait nearly 1 minute to get the Page)

Create admin username: admin
Create admin password: Cisco123
Confirm admin password: Cisco123
Then click Start

Setup Your Controller as follows

System Name: WLC
Management IP Address: 192.168.1.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1
(Note: Leave other options as default)
Then click Next

Create your Wireless Networks as follows

Network Name: CP08
Security: WPA2 Personal
Passphrase: Cisco123
Confirm Passphrase: Cisco123
(Note: Leave other options as default)
Then click Next

Advanced Settings as default then click Next

Please confirm settings and apply (There will be a reboot message, click Ok)
Close the Admin Window

Configure AAA Service

Go to AAA Server -> Services -> AAA
Service: On
In Network Configuration
Client Name: WLC
Client IP: 192.168.1.2
Secret: Cisco123
ServerType: Radius
Then Click on Add

User Setup
Username: admin
Password: admin
Then Click on Add

Configure the WLC to use a RADIUS server.

WPA2-Enterprise uses an external RADIUS server to authenticate WLAN users. Individual user accounts with unique usernames and passwords can be configured on the RADIUS server. Before the WLC can use the services of the RADIUS server, the WLC must be configured with the server address.
Click the **Security** menu on the WLC.
Click the **New** button and enter the IP address of the RADIUS server in the Server IP Address field.
The RADIUS server will authenticate the WLC before it will allow the WLC to access the user account information that is on the server. This requires a shared secret value. Use **Cisco123**. Confirm the shared secret and click **Apply**.

Create and enable the WLAN. (Remove Existing WLANs)

Click **WLANs** in the WLC menu bar. Locate the dropdown box in the upper right had corner of the WLANs screen. It will say **Create New**. Click **Go** to create a new WLAN.
Enter the Profile Name of the new WLAN. Use the profile name **NTTF**. Assign an **SSID** of **CP08** to the WLAN. Hosts will need to use this SSID to join the network.
Select the ID for the WLAN. This value is a label that will be used to identify the WLAN is other displays. Select a value of 5 to keep it consistent with the VLAN number and SSID. This is not a requirement but it helps with understanding the topology.
Click Apply so that the settings go into effect.
Now that the WLAN has been created, you can configure features of the network. Click Enabled to make the WLAN functional. It is a common mistake to accidentally skip this step.
Click the Advanced tab.
Scroll down to the **FlexConnect** portion of the page. Click to enable **FlexConnect** Local Switching and **FlexConnect Local Auth**.
Click **Apply** to enable the new WLAN. If you forget to do this, the WLAN will not operate.

Configure WLAN security.

Instead of WPA2-PSK, we will configure the new WLAN to use **WPA2-Enterprise**.
Click the WLAN ID of the newly created WLAN to continue configuring it, if necessary.
Click the Security tab. Under the Layer 2 tab, select **WPA+WPA2** from the drop-down box.
Under WPA+WPA2 Parameters, enable **WPA2 Policy**. Click **802.1X** under Authentication Key Management. This tells the WLC to use the 802.1X protocol to authenticate users externally.
Click the **AAA Servers** tab. Open the drop-down next to Server 1 in the Authentication Servers column and select the server that we configured.
Click **Apply** to enact this configuration. You have now configured the WLC to use the RADIUS sever to authenticate users that attempt to connect to the WLAN.

Configure SNMP

Click the **Management** menu in the WLC GUI and expand the entry for **SNMP** in the left-hand menu.
Click Trap **Receivers** and then **New**…
Enter the community string as **WLAN_SNMP** and the IP address of the server at **192.168.1.3**.
Click **Apply** to finish the configuration.

Configure a host to connect to the enterprise network.

In the Packet Tracer PC Wireless client app, you must configure a WLAN Profile in order to attach to a WPA2-Enterprise WLAN.
Click **Laptop** and open the **PC Wireless** app.
Click the **Profiles** tab and then click **Edit**.
Highlight the Wireless Network Name for the WLAN that we created earlier and click Advanced Setup.
Verify that the SSID for the wireless LAN is present and then click Next. Wireless Host should see **CP08**.
Verify that the **DHCP** network setting is selected and click Next.
In the Security drop down box, select **WPA2-Enterprise**. Click Next.
Enter login **admin** and the password **admin** and click **Next**.
Verify the Profile Settings and click Save.
Then Click **Connect** to Network
Confirm that Wireless Host has connected to the WLAN. Wireless Host should receive an IP address from the DHCP server

Test Connectivity.

Close the PC Wireless app.
Open a command prompt and confirm that Wireless Host laptop has obtained an IP address from the WLAN network. From Wireless Host, ping the WLAN default gateway and the Server to verify that the laptop has full connectivity.

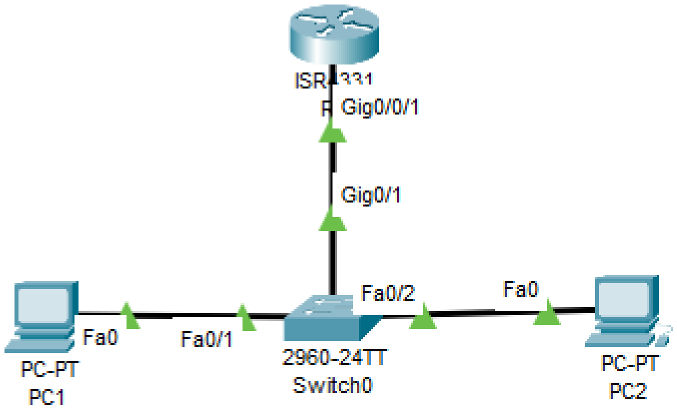
Result: *Configured and Verified a WPA2 Enterprise WLAN on the WLC.*

EXERCISE NO.6

Basic Router Configuration Review

- -Assign static IPv4 and IPv6 addresses to the PC interfaces.
- -Configure basic router settings.
- -Configure the router for SSH.
- -Verify network connectivity

TOPOLOGY



DEVICES MODEL

DEVICE	MODEL
R1	ISR4331
Switch0	2960

ADDRESSING TABLE

Device	Interface	IPv6 Address/Prefix		Default Gateway	Description
		IP Address	Subnet Mask		
R1	G0/0/1	192.168.1.1	255.255.255.0	Not Applicable	Connected to S1 G0/1
		2001:DB8:ACAD:1::1/64		Not Applicable	
		FE80::1			Link Local IPv6 Address
PC1	NIC	192.168.1.10	255.255.255.0	192.168.1.1	Connected to S1 Fa0/1
		2001:DB8:ACAD:1::A/64		FE80::1	
PC2	NIC	192.168.1.11	255.255.255.0	192.168.1.1	Connected to S1 Fa0/2
		2001:DB8:ACAD:1::B/64		FE80::1	

Router R1 Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#ip domain-name ccna.com
R1(config)#banner motd "Unauthorized access is strictly prohibited"
R1(config)#service password-encryption
R1(config)#enable secret class
R1(config)#username admin password cisco
R1(config)#ipv6 unicast-routing
R1(config)#crypto key generate rsa
1024
R1(config)#ip ssh version 2
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#loggin synchronous
R1(config-line)#line vty 0 15
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#loggin synchronous

R1(config-line)#exit
R1(config)#interface g0/0/1
R1(config-if)#description Connected S1 G0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#end
R1#copy run start
```

PC1 IP Configuration
IPv4 Address: 192.168.1.9
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PC1 IPv6 Configuration
IPv6 Address: 2001:DB8:ACAD:1::A/64
Default Gateway: FE80::1

PC2 IP Configuration
IPv4 Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PC2 IPv6 Configuration
IPv6 Address: 2001:DB8:ACAD:1::B/64
Default Gateway: FE80::1

Verification Commands Used:

```
R1#show ip interface brief
R1#show running-config
```

Result: *Configured and Verified a Basic Router Configuration Review.*

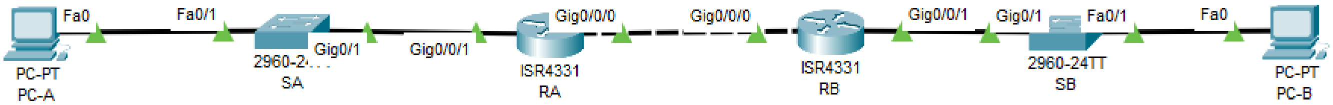
EXERCISE NO.7

Configure IPv4 Static Routes

-Configure Directly Connected Static Routes

-Configure Default Static Routes

TOPOLOGY



DEVICE MODEL

DEVICE	MODEL
RA, RB	ISR4331
SA, SB	2960

ADDRESSING TABLE

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
RA	G0/0/0	10.1.1.1	255.255.255.252	Not Applicable	Connected to RB G0/0/0
	G0/0/1	192.168.1.1	255.255.255.0	Not Applicable	Connected to S1 G0/1
RB	G0/0/0	10.1.1.2	255.255.255.252	Not Applicable	Connected to RA G0/0/0
	G0/0/1	192.168.2.1	255.255.255.0	Not Applicable	Connected to S2 G0/1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1	Connected to S1 Fa0/1
PC-B	NIC	192.168.2.10	255.255.255.0	192.168.2.1	Connected to S2 Fa0/1

Router RA Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RA

RA(config)#interface g0/0/0
RA(config-if)#ip address 10.1.1.1 255.255.255.252
RA(config-if)#no shutdown

RA(config-if)#interface g0/0/1
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#no shutdown
RA(config-if)#exit
RA(config)#ip route 192.168.2.0 255.255.255.0 g0/0/0

RA(config)#exit
RA#copy run start
```

Router RB Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RB

RB(config)#interface g0/0/0
RB(config-if)#ip address 10.1.1.2 255.255.255.252
RB(config-if)#no shutdown

RB(config-if)#interface g0/0/1
RB(config-if)#ip address 192.168.2.1 255.255.255.0
RB(config-if)#no shutdown
RB(config-if)#exit

RB(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.1

RB(config)#exit
RB#copy run start
```

PC-A IP Configuration
IPv4 Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PC-B IP Configuration
IPv4 Address: 192.168.2.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1

Verification Commands Used:

```
R1#show ip interface brief
R1#show ip route
R1#show running-config
```

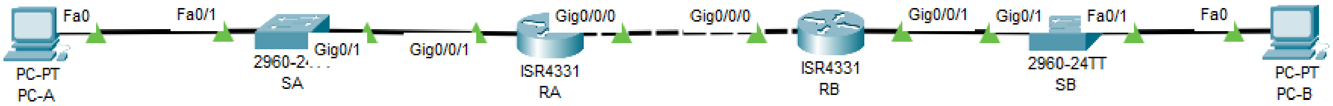
Result: *Configured and Verified IPv4 Static Routes.*

EXERCISE NO.8

Configure IPv6 Static Routes

- Configure Directly Connected Static Routes
- Configure Default Static Routes

TOPOLOGY



Addressing Table

Device	Interface	IPV6 Address/Prefix	Default Gateway	Description
RA	G0/0/0	2001:DB8:ACAD:B::1/64	Not Applicable	Connected to RB G0/0/0
	G0/0/1	2001:DB8:ACAD:A::1/64	Not Applicable	Connected to S1 G0/1
	FE80::1			Link Local IPv6 for RA Interfaces
RB	G0/0/0	2001:DB8:ACAD:B::2/64	Not Applicable	Connected to RA G0/0/0
	G0/0/1	2001:DB8:ACAD:C::1/64	Not Applicable	Connected to S2 G0/1
	FE80::2			Link Local IPv6 for RB Interfaces
PC-A	NIC	2001:DB8:ACAD:A::F/64	FE80::1	Connected to S1 Fa0/1
PC-B	NIC	2001:DB8:ACAD:C::F/64	FE80::2	Connected to S2 Fa0/1

Router RA Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RA
RA(config)#ipv6 unicast-routing

RA(config)#interface g0/0/0
RA(config-if)#ipv6 address 2001:DB8:ACAD:B::1/64
RA(config-if)#ipv6 address FE80::1 link-local
RA(config-if)#no shutdown

RA(config-if)#interface g0/0/1
RA(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
RA(config-if)#ipv6 address FE80::1 link-local
RA(config-if)#no shutdown

RA(config-if)#exit
RA(config)#ipv6 route 2001:DB8:ACAD:C::/64 g0/0/0 2001:DB8:ACAD:B::2

RA(config)#exit
RA#copy run start
```

Router RB Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RB
RB(config)#ipv6 unicast-routing

RB(config)#interface g0/0/0
RB(config-if)#ipv6 address 2001:DB8:ACAD:B::2/64
RB(config-if)#ipv6 address FE80::2 link-local
RB(config-if)#no shutdown

RB(config-if)#interface g0/0/1
RB(config-if)#ipv6 address 2001:DB8:ACAD:C::1/64
RB(config-if)#ipv6 address FE80::2 link-local
RB(config-if)#no shutdown
RB(config-if)#exit

RB(config)#ipv6 route ::/0 2001:DB8:ACAD:B::1

RB(config)#exit
RB#copy run start
```

PC-A IP Configuration
IPv6 Address: *2001:DB8:ACAD:A::F*
/64
Default Gateway: FE80::1

PC-B IP Configuration
IPv6 Address: *2001:DB8:ACAD:C::F*
/64
Default Gateway: FE80::2

Verification Commands Used:

```
R1#show ipv6 interface brief
R1#show ipv6 route
R1#show running-config
```

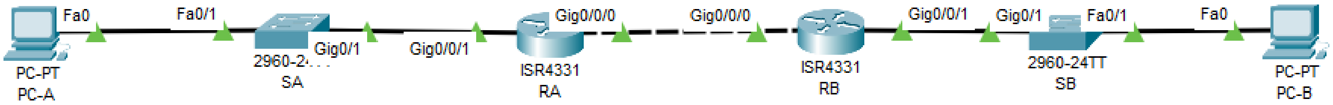
Result: *Configured and Verified IPv6 Static Routes.*

EXERCISE NO.9

Point-to-Point Single-Area OSPFv2 Configuration

- -Configure Router IDs.
- -Configure Networks for OSPF Routing.
- -Configure Passive Interfaces.
- -Verify OSPF configuration.

TOPOLOGY



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
RA	G0/0/0	10.1.1.1	255.255.255.252	Not Applicable	Connected to RB G0/0/0
	G0/0/1	192.168.1.1	255.255.255.0	Not Applicable	Connected to S1 G0/1
RB	G0/0/0	10.1.1.2	255.255.255.252	Not Applicable	Connected to RA G0/0/0
	G0/0/1	192.168.2.1	255.255.255.0	Not Applicable	Connected to S2 G0/1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1	Connected to S1 Fa0/1
PC-B	NIC	192.168.2.10	255.255.255.0	192.168.2.1	Connected to S2 Fa0/1

Router RA Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RA

RA(config)#interface g0/0/0
RA(config-if)#ip address 10.1.1.1 255.255.255.252
RA(config-if)#no shutdown

RA(config-if)#interface g0/0/1
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#no shutdown

RA(config-if)#exit
RA(config)#router ospf 1
RA(config-router)#router-id 1.1.1.1
RA(config-router)#network 10.1.1.0 0.0.0.3 area 0
RA(config-router)#network 192.168.1.0 0.0.0.255 area 0
RA(config-router)#passive-interface g0/0/1
RA(config-router)#end
RA#copy run start
```

Router RB Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RB

RB(config)#interface g0/0/0
RB(config-if)#ip address 10.1.1.2 255.255.255.252
RB(config-if)#no shutdown

RB(config-if)#interface g0/0/1
RB(config-if)#ip address 192.168.2.1 255.255.255.0
RB(config-if)#no shutdown
RB(config-if)#exit

RB(config)#router ospf 1
RB(config-router)#router-id 2.2.2.2
RB(config-router)#network 10.1.1.0 0.0.0.3 area 0
RB(config-router)#network 192.168.2.0 0.0.0.255 area 0
RB(config-router)#passive-interface g0/0/1

RB(config-router)#end
RB#copy run start
```

PC-A IP Configuration

IPv4 Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PC-B IP Configuration

IPv4 Address: 192.168.2.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1

Verification Commands Used:

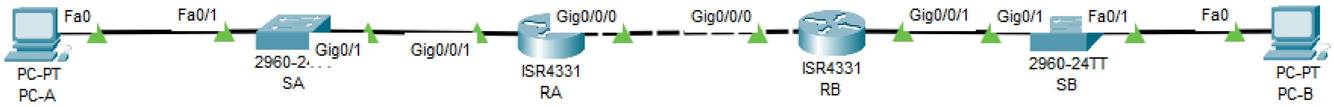
```
RA#show ip interface brief
RA#show ip ospf neighbour
RA#show ip ospf database
RA#show ip route
RA#show running-config
```

Result: *Configured and Verified Point-to-Point Single-Area OSPFv2.*

EXERCISE NO.10

Modify Single-Area OSPFv2
- Modify OSPF Default Settings
- Verify Connectivity

TOPOLOGY



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
RA	G0/0/0	10.1.1.1	255.255.255.252	Not Applicable	Connected to RB G0/0/0
	G0/0/1	192.168.1.1	255.255.255.0	Not Applicable	Connected to S1 G0/1
RB	G0/0/0	10.1.1.2	255.255.255.252	Not Applicable	Connected to RA G0/0/0
	G0/0/1	192.168.2.1	255.255.255.0	Not Applicable	Connected to S2 G0/1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1	Connected to S1 Fa0/1
PC-B	NIC	192.168.2.10	255.255.255.0	192.168.2.1	Connected to S2 Fa0/1

Router RA Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RA
RA(config)#interface g0/0/0
RA(config-if)#ip address 10.1.1.1 255.255.255.252
RA(config-if)#no shutdown

RA(config-if)#interface g0/0/1
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#no shutdown

RA(config-if)#exit
RA(config)#router ospf 1
RA(config-router)#router-id 1.1.1.1
RA(config-router)#network 10.1.1.0 0.0.0.3 area 0
RA(config-router)#network 192.168.1.0 0.0.0.255 area 0
RA(config-router)#passive-interface g0/0/1

RA(config-router)#int g0/0/0
RA(config-if)#ip ospf hello-interval 15
RA(config-if)#ip ospf dead-interval 60
RA(config-if)#end
RA#copy run start
```

Router RB Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RB

RB(config)#interface g0/0/0
RB(config-if)#ip address 10.1.1.2 255.255.255.252
RB(config-if)#no shutdown

RB(config-if)#interface g0/0/1
RB(config-if)#ip address 192.168.2.1 255.255.255.0
RB(config-if)#no shutdown
RB(config-if)#exit

RB(config)#router ospf 1
RB(config-router)#router-id 2.2.2.2
RB(config-router)#network 10.1.1.0 0.0.0.3 area 0
RB(config-router)#network 192.168.2.0 0.0.0.255 area 0
RB(config-router)#passive-interface g0/0/1

RB(config-router)#interface g0/0/0
RB(config-if)#ip ospf hello-interval 15
RB(config-if)#ip ospf dead-interval 60

RB(config-if)#end
RB#copy run start
```

PC-A IP Configuration

IPv4 Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PC-B IP Configuration

IPv4 Address: 192.168.2.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1

Verification Commands Used:

```
RA#show ip interface brief
RA#show ip ospf neighbour
RA#show ip ospf database
RA#show ip ospf interface g0/0/0
RA#show ip route
RA#show running-config
```

Result: *Configured, Modified and Verified Single-Area OSPFv2.*

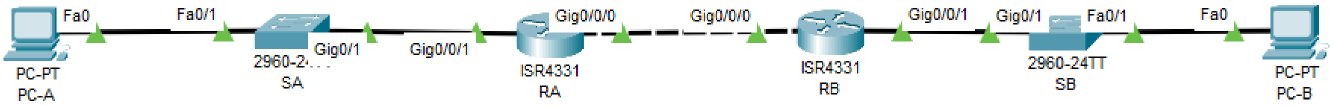
EXERCISE NO.11

Propagate a Default Route in OSPFv2

-Propagate a Default Route

-Verify Connectivity

TOPOLOGY



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
RA	G0/0/0	10.1.1.1	255.255.255.252	Not Applicable	Connected to RB G0/0/0
	G0/0/1	192.168.1.1	255.255.255.0	Not Applicable	Connected to S1 G0/1
RB	G0/0/0	10.1.1.2	255.255.255.252	Not Applicable	Connected to RA G0/0/0
	G0/0/1	192.168.2.1	255.255.255.0	Not Applicable	Connected to S2 G0/1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1	Connected to S1 Fa0/1
PC-B	NIC	192.168.2.10	255.255.255.0	192.168.2.1	Connected to S2 Fa0/1

Router RA Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RA
RA(config)#interface g0/0/0
RA(config-if)#ip address 10.1.1.1 255.255.255.252
RA(config-if)#no shutdown

RA(config-if)#interface g0/0/1
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#no shutdown

RA(config-if)#exit
RA(config)#router ospf 1
RA(config-router)#router-id 1.1.1.1
RA(config-router)#network 10.1.1.0 0.0.0.3 area 0
RA(config-router)#network 192.168.1.0 0.0.0.255 area 0
RA(config-router)#passive-interface g0/0/1

RA(config-router)#end
RA#copy run start
```

Router RB Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RB

RB(config)#interface g0/0/0
RB(config-if)#ip address 10.1.1.2 255.255.255.252
RB(config-if)#no shutdown

RB(config-if)#interface g0/0/1
RB(config-if)#ip address 192.168.2.1 255.255.255.0
RB(config-if)#no shutdown

RB(config-if)#interface loopback 0
RB(config-if)#ip address 201.19.1.1 255.255.255.0
RB(config-if)#exit

RB(config)#ip route 0.0.0.0 0.0.0.0 loopback 0

RB(config)#router ospf 1
RB(config-router)#router-id 2.2.2.2
RB(config-router)#network 10.1.1.0 0.0.0.3 area 0
RB(config-router)#network 192.168.2.0 0.0.0.255 area 0
RB(config-router)#passive-interface g0/0/1
RB(config-router)#default-information originate
RB(config-router)#end
RB#copy run start
```

PC-A IP Configuration

IPv4 Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PC-B IP Configuration

IPv4 Address: 192.168.2.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1

Verification Commands Used:

```
RA#show ip interface brief
RA#show ip ospf neighbour
RA#show ip ospf database
RA#show ip ospf interface g0/0/0
RA#show ip route
RA#show running-config
```

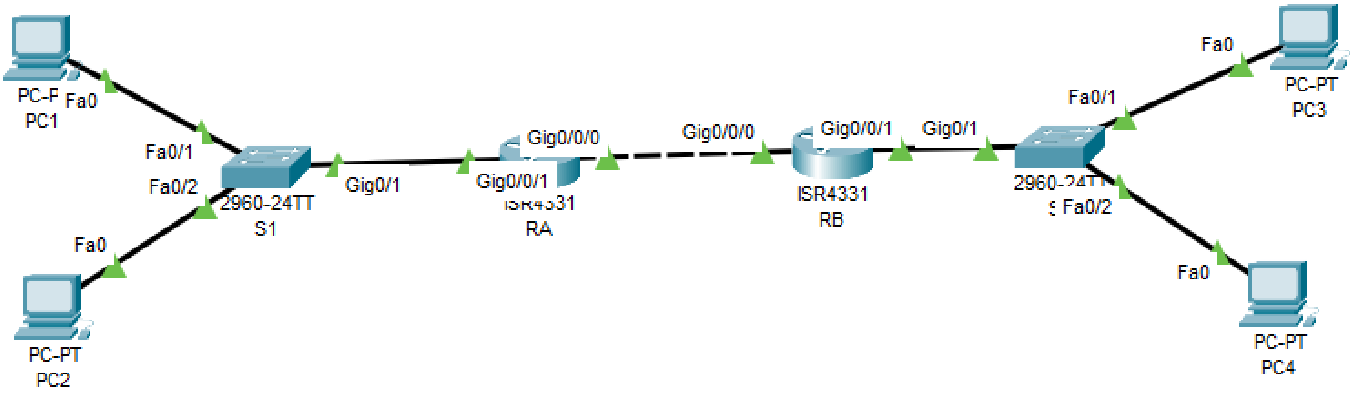
Result: *Configure and verified Propagate a Default Route in OSPFv2.*

EXERCISE NO.12

Configure Numbered Standard IPv4 ACLs

- Plan an ACL Implementation
- Configure, Apply, and Verify a Standard ACL

TOPOLOGY



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
RA	G0/0/0	10.1.1.1	255.255.255.252	Not Applicable	Connected to RB G0/0/0
	G0/0/1	192.168.1.1	255.255.255.0	Not Applicable	Connected to S1 G0/1
RB	G0/0/0	10.1.1.2	255.255.255.252	Not Applicable	Connected to RA G0/0/0
	G0/0/1	192.168.2.1	255.255.255.0	Not Applicable	Connected to S2 G0/1
PC1	NIC	192.168.1.10	255.255.255.0	192.168.1.1	Connected to S1 Fa0/1
PC2	NIC	192.168.1.11	255.255.255.0	192.168.1.1	Connected to S1 Fa0/2
PC3	NIC	192.168.2.10	255.255.255.0	192.168.2.1	Connected to S2 Fa0/1
PC4	NIC	192.168.2.11	255.255.255.0	192.168.2.1	Connected to S2 Fa0/2

Router RA Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RA

RA(config)#interface g0/0/0
RA(config-if)#ip address 10.1.1.1 255.255.255.252
RA(config-if)#no shutdown

RA(config-if)#interface g0/0/1
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#no shutdown

RA(config-if)#exit
RA(config)#router ospf 1
RA(config-router)#router-id 1.1.1.1
RA(config-router)#network 10.1.1.0 0.0.0.3 area 0
RA(config-router)#network 192.168.1.0 0.0.0.255 area 0
RA(config-router)#passive-interface g0/0/1

RA(config-router)#end
RA#copy run start
```

Router RB Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RB

RB(config)#interface g0/0/0
RB(config-if)#ip address 10.1.1.2 255.255.255.252
RB(config-if)#no shutdown

RB(config-if)#interface g0/0/1
RB(config-if)#ip address 192.168.2.1 255.255.255.0
RB(config-if)#no shutdown
RB(config-if)#exit

RB(config)#router ospf 1
RB(config-router)#router-id 2.2.2.2
RB(config-router)#network 10.1.1.0 0.0.0.3 area 0
RB(config-router)#network 192.168.2.0 0.0.0.255 area 0
RB(config-router)#passive-interface g0/0/1
RB(config-router)#exit

RB(config)#access-list 1 deny host 192.168.1.10
RB(config)#access-list 1 permit any
RB(config)#interface g0/0/1
RB(config-if)#ip access-group 1 out
RB(config-if)#end
RB#copy run start
```

PC1 IP Configuration
IPv4 Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PC2 IP Configuration
IPv4 Address: 192.168.1.11
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PC3 IP Configuration
IPv4 Address: 192.168.2.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1

PC4 IP Configuration
IPv4 Address: 192.168.2.11
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1

Verification Commands Used:

```
RB#show ip interface brief
RB#show access-lists
RB#show ip route
RB#show running-config
```

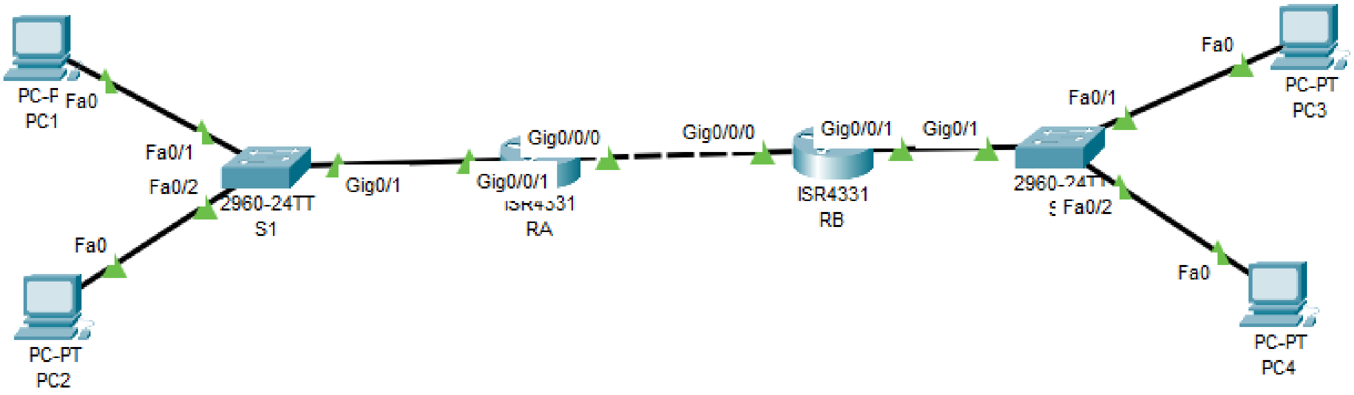
Result: *Configured and Verified* Numbered Standard IPv4 ACLs*.*

EXERCISE NO.13

Configure Named Standard IPv4 ACLs

- Configure and Apply a Named Standard ACL
- Verify the ACL Implementation

TOPOLOGY



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
RA	G0/0/0	10.1.1.1	255.255.255.252	Not Applicable	Connected to RB G0/0/0
	G0/0/1	192.168.1.1	255.255.255.0	Not Applicable	Connected to S1 G0/1
RB	G0/0/0	10.1.1.2	255.255.255.252	Not Applicable	Connected to RA G0/0/0
	G0/0/1	192.168.2.1	255.255.255.0	Not Applicable	Connected to S2 G0/1
PC1	NIC	192.168.1.10	255.255.255.0	192.168.1.1	Connected to S1 Fa0/1
PC2	NIC	192.168.1.11	255.255.255.0	192.168.1.1	Connected to S1 Fa0/2
PC3	NIC	192.168.2.10	255.255.255.0	192.168.2.1	Connected to S2 Fa0/1
PC4	NIC	192.168.2.11	255.255.255.0	192.168.2.1	Connected to S2 Fa0/2

Router RA Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RA

RA(config)#interface g0/0/0
RA(config-if)#ip address 10.1.1.1 255.255.255.252
RA(config-if)#no shutdown

RA(config-if)#interface g0/0/1
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#no shutdown

RA(config-if)#exit
RA(config)#router ospf 1
RA(config-router)#router-id 1.1.1.1
RA(config-router)#network 10.1.1.0 0.0.0.3 area 0
RA(config-router)#network 192.168.1.0 0.0.0.255 area 0
RA(config-router)#passive-interface g0/0/1

RA(config-router)#end
RA#copy run start
```

Router RB Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RB

RB(config)#interface g0/0/0
RB(config-if)#ip address 10.1.1.2 255.255.255.252
RB(config-if)#no shutdown

RB(config-if)#interface g0/0/1
RB(config-if)#ip address 192.168.2.1 255.255.255.0
RB(config-if)#no shutdown
RB(config-if)#exit

RB(config)#router ospf 1
RB(config-router)#router-id 2.2.2.2
RB(config-router)#network 10.1.1.0 0.0.0.3 area 0
RB(config-router)#network 192.168.2.0 0.0.0.255 area 0
RB(config-router)#passive-interface g0/0/1
RB(config-router)#exit

RB(config)#ip access-list standard My_ACL
RB(config-std-nacl)#deny host 192.168.1.10
RB(config-std-nacl)#permit any
RB(config-std-nacl)#interface g0/0/1
RB(config-if)#ip access-group My_ACL out

RB(config-if)#end
RB#copy run start
```

PC1 IP Configuration
IPv4 Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PC2 IP Configuration
IPv4 Address: 192.168.1.11
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PC3 IP Configuration
IPv4 Address: 192.168.2.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1

PC4 IP Configuration
IPv4 Address: 192.168.2.11
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1

Verification Commands Used:

```
RB#show ip interface brief
RB#show access-lists
RB#show ip route
RB#show running-config
```

Result: *Configured and Verified* Named Standard IPv4 ACLs*.*

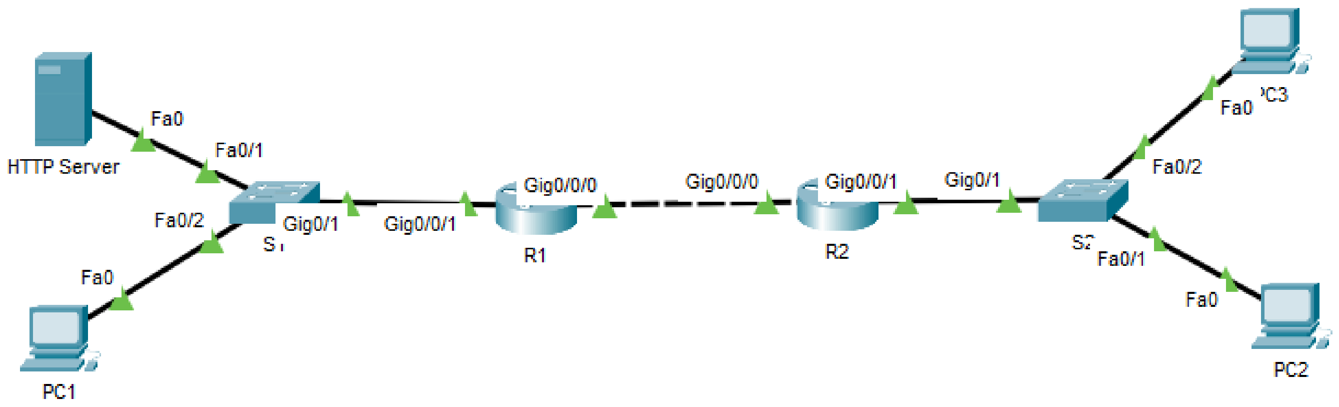
EXERCISE NO.14

Configure Extended IPv4 ACLs

-Configure, Apply and Verify an Extended Numbered ACL

-Configure, Apply and Verify an Extended Named ACL

TOPOLOGY



DEVICE MODEL

DEVICE	MODEL
R1, R2	ISR4331
S1, S2	2960

ADDRESSING TABLE

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
RA	G0/0/0	10.1.1.1	255.255.255.252	Not Applicable	Connected to RB G0/0/0
	G0/0/1	192.168.1.1	255.255.255.0	Not Applicable	Connected to S1 G0/1
RB	G0/0/0	10.1.1.2	255.255.255.252	Not Applicable	Connected to RA G0/0/0
	G0/0/1	192.168.2.1	255.255.255.0	Not Applicable	Connected to S2 G0/1
PC1	NIC	192.168.1.10	255.255.255.0	192.168.1.1	Connected to S1 Fa0/2
HTTP Server	NIC	192.168.1.254	255.255.255.0	192.168.1.1	Connected to S1 Fa0/1
PC2	NIC	192.168.2.10	255.255.255.0	192.168.2.1	Connected to S2 Fa0/1
PC3	NIC	192.168.2.11	255.255.255.0	192.168.2.1	Connected to S2 Fa0/2

Router RA Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RA
```

```
RA(config)#interface g0/0/0
RA(config-if)#ip address 10.1.1.1 255.255.255.252
RA(config-if)#no shutdown
RA(config-if)#interface g0/0/1
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#no shutdown

RA(config-if)#exit
RA(config)#router ospf 1
RA(config-router)#router-id 1.1.1.1
RA(config-router)#network 10.1.1.0 0.0.0.3 area 0
RA(config-router)#network 192.168.1.0 0.0.0.255 area 0
RA(config-router)#passive-interface g0/0/1

RA(config-router)#end
RA#copy run start
```

Router RB Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RB

RB(config)#interface g0/0/0
RB(config-if)#ip address 10.1.1.2 255.255.255.252
RB(config-if)#no shutdown

RB(config-if)#interface g0/0/1
RB(config-if)#ip address 192.168.2.1 255.255.255.0
RB(config-if)#no shutdown
RB(config-if)#exit

RB(config)#router ospf 1
RB(config-router)#router-id 2.2.2.2
RB(config-router)#network 10.1.1.0 0.0.0.3 area 0
RB(config-router)#network 192.168.2.0 0.0.0.255 area 0
RB(config-router)#passive-interface g0/0/1
RB(config-router)#exit

RB(config)#access-list 110 deny tcp host 192.168.2.10 host 192.168.1.254 eq www
RB(config)#access-list 110 permit ip any any
RB(config)#interface g0/0/1
RB(config-if)#ip access-group 110 in
RB(config)#ip access-list extended DENY_FTP
RB(config-ext-nacl)#deny tcp host 192.168.2.11 host 192.168.1.254 eq ftp
RB(config-ext-nacl)#permit ip any any
RB(config-ext-nacl)#interface g0/0/0
RB(config-if)#ip access-group DENY_FTP out

RB(config-if)#end
RB#copy run start
```

PC1 IP Configuration
IPv4 Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

HTTP Server IP Configuration
IPv4 Address: 192.168.1.254
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PC3 IP Configuration
IPv4 Address: 192.168.2.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1

PC4 IP Configuration
IPv4 Address: 192.168.2.11
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1

Verification Commands Used:

```
RB#show ip interface brief
RB#show access-lists
RB#show ip route
RB#show running-config
```

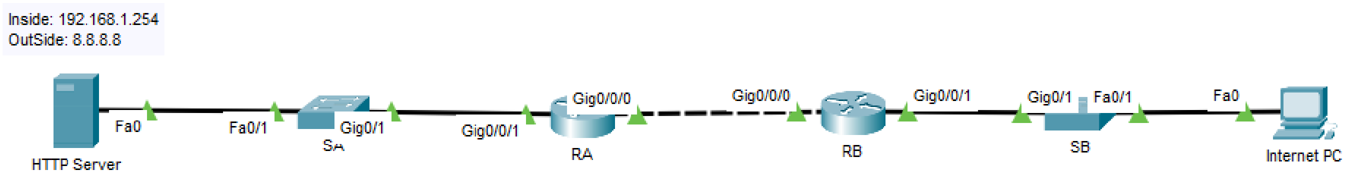
Result: *Configured and Verified* Named and Numbered Extended IPv4 ACLs.

EXERCISE NO.15

Configure Static NAT

- -Configure Static NAT
- -Test Access with NAT

TOPOLOGY



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
RA	G0/0/0	10.1.1.1	255.255.255.252	Not Applicable	Connected to RB G0/0/0
	G0/0/1	192.168.1.1	255.255.255.0	Not Applicable	Connected to S1 G0/1
RB	G0/0/0	10.1.1.2	255.255.255.252	Not Applicable	Connected to RA G0/0/0
	G0/0/1	192.168.2.1	255.255.255.0	Not Applicable	Connected to S2 G0/1
HTTP Server	NIC	192.168.1.254	255.255.255.0	192.168.1.1	Connected to S1 Fa0/1
Internet PC	NIC	192.168.2.10	255.255.255.0	192.168.2.1	Connected to S2 Fa0/1

Router RA Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RA

RA(config)#interface g0/0/0
RA(config-if)#ip address 10.1.1.1 255.255.255.252
RA(config-if)#no shutdown
RA(config-if)#interface g0/0/1
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#no shutdown

RA(config-if)#exit
RA(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0
RA(config)#ip nat inside source static 192.168.1.254 8.8.8.8
RA(config)#interface g0/0/1
RA(config-if)#ip nat inside
RA(config)#interface g0/0/0
RA(config-if)#ip nat outside
RA(config-if)#end
RA#copy run start
```

Router RB Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RB

RB(config)#interface g0/0/0
RB(config-if)#ip address 10.1.1.2 255.255.255.252
RB(config-if)#no shutdown

RB(config-if)#interface g0/0/1
RB(config-if)#ip address 192.168.2.1 255.255.255.0
RB(config-if)#no shutdown
RB(config-if)#exit

RB(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0

RB(config)#exit
RB#copy run start
```

HTTP Server IP Configuration
IPv4 Address: 192.168.1.254
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

Internet PC IP Configuration
IPv4 Address: 192.168.2.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1

Verification Commands Used:

```
RA#show ip interface brief
RA#show ip nat translation
RA#show ip route
RA#show running-config
```

Ping from Internet PC to HTTP Server using 8.8.8.8 and the ping should succeed

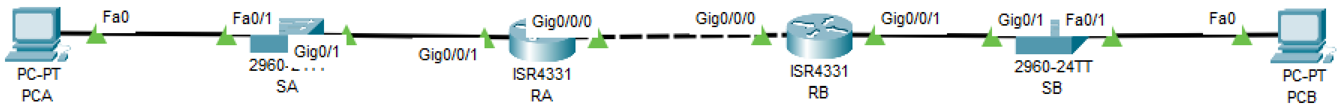
Result: *Configured and Verified Static NAT.*

EXERCISE NO.16

Configure Dynamic NAT

- -Configure Dynamic NAT
- -Verify NAT Implementation

TOPOLOGY



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
RA	G0/0/0	10.1.1.1	255.255.255.252	Not Applicable	Connected to RB G0/0/0
	G0/0/1	192.168.1.1	255.255.255.0	Not Applicable	Connected to S1 G0/1
RB	G0/0/0	10.1.1.2	255.255.255.252	Not Applicable	Connected to RA G0/0/0
	G0/0/1	192.168.2.1	255.255.255.0	Not Applicable	Connected to S2 G0/1
PCA	NIC	192.168.1.10	255.255.255.0	192.168.1.1	Connected to S1 Fa0/1
PCB	NIC	192.168.2.10	255.255.255.0	192.168.2.1	Connected to S2 Fa0/1

Router RA Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RA

RA(config)#interface g0/0/0
RA(config-if)#ip address 10.1.1.1 255.255.255.252
RA(config-if)#no shutdown
RA(config-if)#interface g0/0/1
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#no shutdown

RA(config-if)#exit
RA(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0
RA(config)#access-list 1 permit 192.168.1.0 0.0.0.255
RA(config)#ip nat pool DYNAMIC_NAT 201.198.1.1 201.198.1.2 netmask 255.255.255.252
RA(config)#ip nat inside source list 1 pool DYNAMIC_NAT
RA(config)#interface g0/0/1
RA(config-if)#ip nat inside
RA(config)#interface g0/0/0
RA(config-if)#ip nat outside
RA(config-if)#end
RA#copy run start
```

Router RB Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RB

RB(config)#interface g0/0/0
RB(config-if)#ip address 10.1.1.2 255.255.255.252
RB(config-if)#no shutdown

RB(config-if)#interface g0/0/1
RB(config-if)#ip address 192.168.2.1 255.255.255.0
RB(config-if)#no shutdown
RB(config-if)#exit

RB(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0

RB(config)#exit
RB#copy run start
```

PCA IP Configuration
IPv4 Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PCB IP Configuration
IPv4 Address: 192.168.2.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1

Verification Commands Used:

```
RA#show ip interface brief
RA#show ip nat translation
RA#show ip route
RA#show running-config
```

Result: *Configured and Verified Dynamic NAT.*

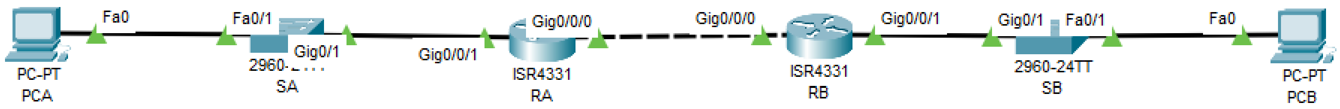
EXERCISE NO.17

Configure PAT

-Configure PAT using an Interface

-Verify PAT Interface Implementation

TOPOLOGY



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
RA	G0/0/0	201.198.1.1	255.255.255.252	Not Applicable	Connected to RB G0/0/0
	G0/0/1	192.168.1.1	255.255.255.0	Not Applicable	Connected to S1 G0/1
RB	G0/0/0	201.198.1.2	255.255.255.252	Not Applicable	Connected to RA G0/0/0
	G0/0/1	192.168.2.1	255.255.255.0	Not Applicable	Connected to S2 G0/1
PCA	NIC	192.168.1.10	255.255.255.0	192.168.1.1	Connected to S1 Fa0/1
PCB	NIC	192.168.2.10	255.255.255.0	192.168.2.1	Connected to S2 Fa0/1

Router RA Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RA

RA(config)#interface g0/0/0
RA(config-if)#ip address 201.198.1.1 255.255.255.252
RA(config-if)#no shutdown
RA(config-if)#interface g0/0/1
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#no shutdown

RA(config-if)#exit
RA(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0
RA(config)#access-list 1 permit 192.168.1.0 0.0.0.255
RA(config)# ip nat inside source list 1 interface g0/0/0 overload
RA(config)#interface g0/0/1
RA(config-if)#ip nat inside
RA(config)#interface g0/0/0
RA(config-if)#ip nat outside
RA(config-if)#end
RA#copy run start
```

Router RB Configuration

```
Router>enable
Router#configure terminal
Router(config)#hostname RB

RB(config)#interface g0/0/0
RB(config-if)#ip address 201.198.1.2 255.255.255.252
RB(config-if)#no shutdown

RB(config-if)#interface g0/0/1
RB(config-if)#ip address 192.168.2.1 255.255.255.0
RB(config-if)#no shutdown
RB(config-if)#exit

RB(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0

RB(config)#exit
RB#copy run start
```

PCA IP Configuration

IPv4 Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PCB IP Configuration

IPv4 Address: 192.168.2.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1

Verification Commands Used:

```
RA#show ip interface brief
RA#show ip nat translation
RA#show ip route
RA#show running-config
```

Result: *Configured and Verified PAT.*

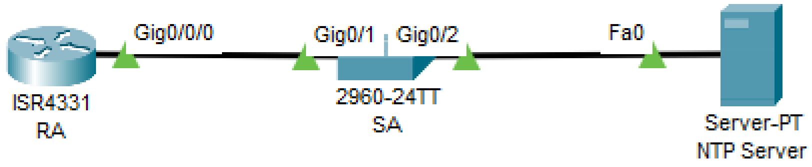
EXERCISE NO.18

Configure and Verify NTP

-Configure the NTP Clients

-Verify NTP settings

TOPOLOGY



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
RA	G0/0/0	192.168.1.1	255.255.255.250	Not Applicable	Connected to SA G0/1
NTP Server	NIC	192.168.1.10	255.255.255.0	192.168.1.1	Connected to SA G0/2

Verify Clock

```
Router>enable
Router#show clock
```

Router RA Configuration

```
Router#configure terminal
Router(config)#hostname RA
RA(config)#interface g0/0/0
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#no shutdown
RA(config-if)#exit

RA (config)#ntp server 192.168.1.10
RA(config)#exit
RA#copy run start
```

NTP Server IP Configuration

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

Verification Commands Used:

```
RA#show clock
RA#show ntp status
```

Result: *Configured and Verified NTP.*

EXERCISE No.19

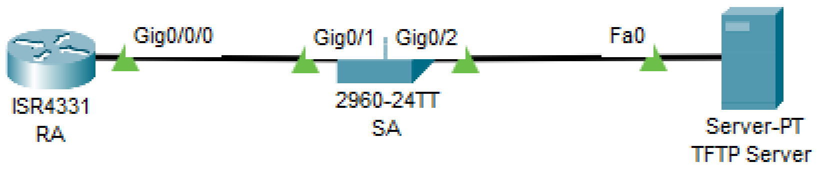
Back Up Configuration Files

-Establish Connectivity to TFTP Server

-Transfer the Configuration File from TFTP Server

-Backup Configuration and IOS to TFTP Server

TOPOLOGY



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Description
RA	G0/0/0	192.168.1.1	255.255.255.250	Not Applicable	Connected to SA G0/1
TFTP Server	NIC	192.168.1.10	255.255.255.0	192.168.1.1	Connected to SA G0/2

TFTP Server IP Configuration

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

Router RA Configuration

```
Router#configure terminal
Router(config)#hostname RA

RA(config)#interface g0/0/0
RA(config-if)#ip address 192.168.1.1 255.255.255.0
RA(config-if)#no shutdown
RA(config-if)#end
RA#copy run start
```

Test the Connectivity to TFTP Server (ping 192.168.1.10)

Transfer Backup Configuration *file from RA to TFTP*

```
RA#copy running-config tftp:
Address or name of remote host []? 192.168.1.10
Destination filename [RA-confg]? (Press Enter)
```

Backup Configuration and IOS to TFTP Server

```
RA#show flash: (Copy the IOS file name with extension .bin)

RA#copy flash: tftp:
Source filename []? isr4300-universalk9.16.06.04.SPA.bin
Address or name of remote host []? 192.168.1.10
Destination filename [isr4300-universalk9.16.06.04.SPA.bin]? (Press Enter)
```

Verify that Configuration files and IOS copied to TFTP:

Go to TFTP Server → Services → TFTP and check the following files are available in the list

RA-confg
isr4300-universalk9.16.06.04.SPA.bin

Transfer the Configuration File from TFTP Server

```
RA#configure terminal
RA(config)#hostname RB
RB(config)#exit
RB#copy tftp: running-config
Address or name of remote host []? 192.168.1.10
Source filename []? RA-confg
Destination filename [running-config]?
RA#copy run start
```

Result: Established Connectivity to TFTP Server and Transferred the Configuration File from TFTP Server, and Backup Configuration and IOS to TFTP Server