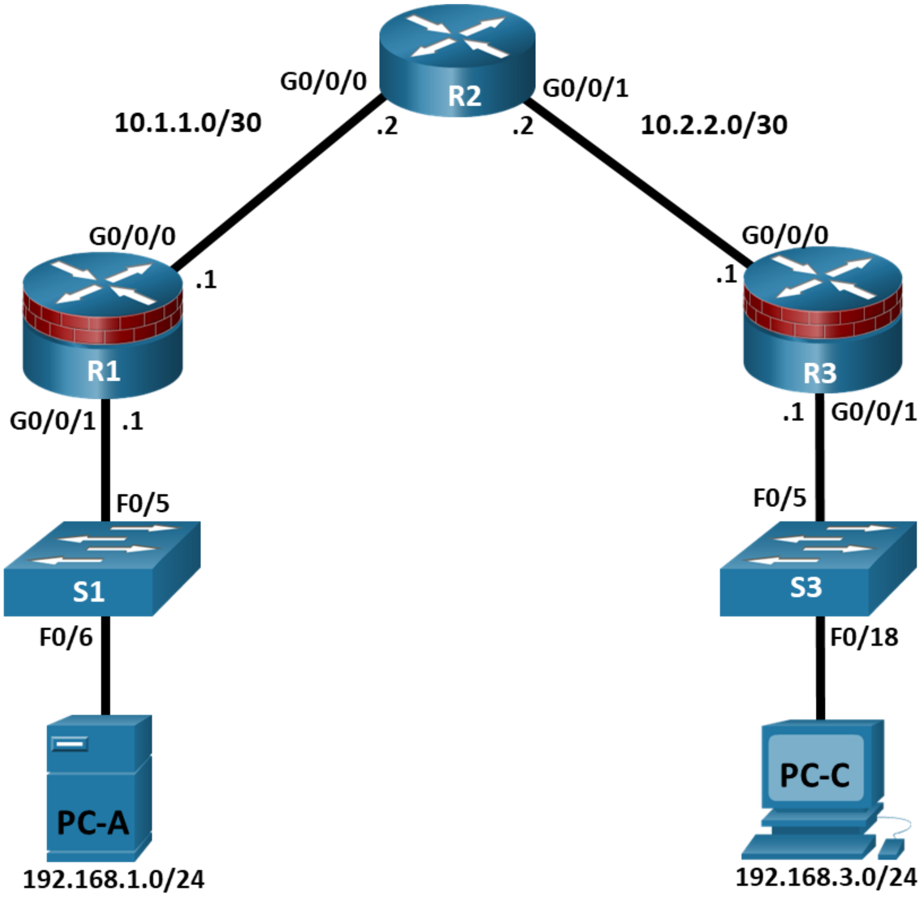
[Title]

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
R2	G0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	G0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objectives

Part 1: Configure Basic Device Settings

- Cable the network as shown in the topology.
- Configure basic IP addressing for routers and PCs.
- Configure OSPF routing.
- Configure PC hosts.
- Verify connectivity between hosts and routers.

Part 2: Configure and Encrypt Passwords on Routers R1 and R3

- Configure encrypted password for console, auxiliary port, and virtual access lines.
- Encrypt clear text passwords
- Configure a warning message banner

Part 3: Configure Enhanced Username Password Security on Routers R1 and R3

- Create new user accounts
- Log in using the user accounts

Part 4: Configure the SSH Server on Routers R1 and R3

- Configure a domain name
- Generate RSA encryption key
- Configure and verify SSH configurations

Background / Scenario

The router is a critical component in any network. It controls the movement of data into and out of the network and between devices within the network. It is particularly important to protect network routers because the failure of a routing device could make sections of the network, or the entire network, inaccessible. Controlling access to routers and enabling reporting on routers is critical to network security and should be part of a comprehensive security policy.

In this lab, you will build a multi-router network and configure the routers and hosts. Use various CLI tools to secure local and remote access to the routers, analyze potential vulnerabilities, and take steps to mitigate them. Enable management reporting to monitor router configuration changes.

Note: The routers used with hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.6 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960+ with Cisco IOS Release 15.2(7) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Before you begin, ensure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 2 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 2 PCs (Windows OS with a terminal emulation program, such as PuTTY or Tera Term installed)

- Console cables to configure Cisco networking devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Device Settings

In this part, set up the network topology and configure basic settings, such as interface IP addresses.

Step 1: Cable the network.

Attach the devices, as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

a. Console into the router and enable privileged EXEC mode.

```
Router> enable
Router# configure terminal
```

b. Configure host names as shown in the topology.

```
R1(config)# hostname R1
```

c. Configure interface IP addresses as shown in the IP Addressing Table.

```
R1(config)# interface g0/0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# no shutdown

R1(config)# interface g0/0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

d. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup. R1 is shown here as an example.

```
R1(config)# no ip domain-lookup
```

Step 3: Configure OSPF routing on the routers.

a. Use the **router ospf** command in global configuration mode to enable OSPF on R1.

```
R1(config)# router ospf 1
```

b. Configure the **network** statements for the networks on R1. Use an area ID of 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

c. Configure OSPF on R2 and R3.

```
R2(config)# router ospf 1
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config)# router ospf 1
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

```
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
```

d. Issue the **passive-interface** command to change the G0/0/1 interface on R1 and R3 to passive.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0/1

R3(config)# router ospf 1
R3(config-router)# passive-interface g0/0/1
```

Step 4: Verify OSPF neighbors and routing information.

a. Issue the **show ip ospf neighbor** command to verify that each router lists the other routers in the network as neighbors.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.2.2          1   FULL/BDR        00:00:37    10.1.1.2
GigabitEthernet0/0/0
```

b. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, GigabitEthernet0/0/0
L        10.1.1.1/32 is directly connected, GigabitEthernet0/0/0
O        10.2.2.0/30 [110/2] via 10.1.1.2, 00:01:11, GigabitEthernet0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
O     192.168.3.0/24 [110/3] via 10.1.1.2, 00:01:07, GigabitEthernet0/0/0
```

Step 5: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C as shown in the IP Addressing Table.

Step 6: Verify connectivity between PC-A and PC-C.

a. Ping from R1 to R3.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A, on the R1 LAN, to PC-C, on the R3 LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C you have demonstrated that OSPF routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run, show ip ospf neighbor,** and **show ip route** commands to help identify routing protocol-related problems.

Step 7: Save the basic running configuration for each router.

Save the basic running configuration for the routers as text files on your PC. These text files can be used to restore configurations later in the lab.

Part 2: Configure and Encrypt Passwords on Routers R1 and R3

In this part, you will:

- Configure encrypted passwords.
- Configure a login warning banner.
- Configure enhanced username password security.
- Configure enhanced virtual login security.

Note: Perform all tasks on both R1 and R3. The procedures and output for R1 are shown here.

Step 1: Configure encrypted passwords on routers R1 and R3.

a. Configure the enable secret encrypted password on both routers. Use the type 9 (SCRYPT) hashing algorithm.

```
R1(config)# enable algorithm-type scrypt secret cisco12345
```

How does configuring an enable secret password help to protect a router from being compromised by an attack?

b. Use the **security passwords** command to set a minimum password length of 10 characters.

```
R1(config)# security passwords min-length 10
```

Step 2: Configure basic console, auxiliary port, and virtual access lines.

Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

a. Configure a console password and enable login for routers. For additional security, the **exec-timeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the **exec-timeout** command can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

```
R1(config)# line console 0
R1(config-line)# password ciscocon
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```

When you configured the password for the console line, what message was displayed?

b. Configure a new password of **ciscoconpass** for the console.

c. Configure a password for the AUX port for router R1.

```
R1(config)# line aux 0
R1(config-line)# password ciscoauxpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

d. Telnet from R2 to R1.

```
R2> telnet 10.1.1.1
```

Were you able to login? Explain.

What messages were displayed?

e. Configure the password on the vty lines for router R1.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# transport input telnet
R1(config-line)# login
```

f. Telnet from R2 to R1 again.

Were you able to login this time?

g. Enter privileged EXEC mode and issue the **show run** command.

Can you read the enable secret password? Explain.

Can you read the console, aux, and vty passwords? Explain.

Step 3: Encrypt clear text passwords.

a. Use the **service password-encryption** command to encrypt the console, aux, and vty passwords.

```
R1(config)# service password-encryption
```

b. Issue the **show run** command.

Can you read the console, aux, and vty passwords? Explain.

At what level (number) is the default enable secret password encrypted?

At what level (number) are the other passwords encrypted?

Which level of encryption is harder to crack. Explain.

Step 4: Configure a warning message to display prior to login.

a. Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner using the **banner motd** command. When a user connects to one of the routers, the MOTD banner appears before the login prompt. In this example, the dollar sign ($) is used to start and end the message.

```
R1(config)# banner motd $Unauthorized access strictly prohibited!$
R1(config)# exit
```

b. Issue the **show run** command.

What does the $ convert to in the output?

c. Telnet to R1 from R2 again. Notice the MOTD banner.

d. Repeat the configuration portion of previous steps on router R3.

Part 3: Configure Enhanced Username Password Security on Routers R1 and R3

Step 1: Investigate the options for the username command.

In global configuration mode, enter the following command:

```
R1(config)# username user01 algorithm-type ?
```

What options are available?

Step 2: Create a new user account with a secret password.

a. Create a new user account with SCRYPT hashing to encrypt the password.

```
R1(config)# username user01 algorithm-type scrypt secret user01pass
```

b. Exit global configuration mode and save your configuration.

c. Display the running configuration.

Which hashing method is used for the password?

Step 3: Test the new account by logging in to the console.

a. Set the console line to use the locally defined login accounts.

```
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# end
R1# exit
```

b. Exit to the initial router screen which displays: R1 con0 is now available, Press RETURN to get started.

c. Log in using the previously defined username **user01** and the password **user01pass**.

What is the difference between logging in at the console now and previously?

d. After logging in, issue the **show run** command.

   Were you able to issue the command? Explain.

e. Enter privileged EXEC mode using the **enable** command.

   Were you prompted for a password? Explain.

Part 4: Configure the SSH Server on Routers R1 and R3

In this part, use the CLI to configure the router to be managed securely using SSH instead of Telnet. Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals.

Note: For a router to support SSH, it must be configured with local authentication, (AAA services, or username) or password authentication. In this task, you configure an SSH username and local authentication.

Step 1: Configure a domain name.

Enter global configuration mode and set the domain name.

```
R1# conf t
R1(config)# ip domain-name netsec.com
```

Step 2: Configure a privileged user for login from the SSH client.

a. Use the **username** command to create the user ID with the highest possible privilege level and a secret password.

```
R1(config)# username admin privilege 15 algorithm-type scrypt secret
cisco12345
```

   Note: Usernames are not case sensitive by default.

b. Exit to the initial router login screen. Log in with the username admin and the associated password.

   What was the router prompt after you entered the password?

Step 3: Configure the incoming vty lines.

Specify a privilege level of **15** so that a user with the highest privilege level (15) will default to privileged EXEC mode when accessing the vty lines. Other users will default to user EXEC mode. Use the local user accounts for mandatory login and validation and accept only SSH connections.

```
R1(config)# line vty 0 4
R1(config-line)# privilege level 15
R1(config-line)# login local
```

```
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Note: The **login local** command should have been configured in a previous step. It is included here to provide all commands if you are doing this for the first time.

Note: If you add the keyword **telnet** to the **transport input** command, users can log in using Telnet as well as SSH, however, the router will be less secure. If only SSH is specified, the connecting host must have an SSH client installed.

Step 4: Erase existing key pairs on the router.

```
R1(config)# crypto key zeroize rsa
```

Note: If no keys exist, you might receive this message: `% No Signature RSA Keys found in configuration`.

Step 5: Generate the RSA encryption key pair for the router.

The router uses the RSA key pair for authentication and encryption of transmitted SSH data.

a. Configure the RSA keys with **1024** for the number of modulus bits. The default is 512, and the range is from 360 to 2048.

```
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.netsec.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Dec 16 21:24:16.175: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

a. Issue the **ip ssh version 2** command to force the use of SSH version 2.

```
R1(config)# ip ssh version 2
R1(config)# exit
```

Note: The details of encryption methods are covered in later module.

Step 6: Verify the SSH configuration.

a. Use the **show ip ssh** command to see the current settings.

```
R1# show ip ssh
```

b. Fill in the following information based on the output of the **show ip ssh** command.

SSH version enabled:

Authentication timeout:

Authentication retries:

Step 7: Configure SSH timeouts and authentication parameters.

a. The default SSH timeouts and authentication parameters can be altered to be more restrictive using the following commands.

```
R1(config)# ip ssh time-out 90
R1(config)# ip ssh authentication-retries 2
```

b. Use the **show ip ssh** command to see the current settings.

c. Save the running-config to the startup-config.

```
R1# copy running-config startup-config
```

d. Repeat the configuration portion of previous steps on router R3.

Step 8: Verify SSH connectivity to R1 from PC-A.

a. From PC-A, SSH into router R1 using the terminal emulation software by selecting the SSH option and providing the IP address of R1. Confirm that you will trust the host (R1) when prompted in the security alert.

b. Enter the **admin** username and password **cisco12345** when prompted.

c. At the R1 privileged EXEC prompt, enter the **show users** command.

```
R1# show users
```

What users are connected to router R1 at this time?

d. Close the SSH session window.

e. Try to open a Telnet session to your router from PC-A. Were you able to open the Telnet session? Explain.

f. Open a PuTTY SSH session to the router from PC-A. Enter the **user01** username and password **user01pass** in the PuTTY window to try connecting for a user who does not have privilege level of 15.

If you were able to login, what was the prompt?

g. Use the **enable** command to enter privilege EXEC mode and enter the enable secret password **cisco12345**.

Reflection

1. Explain the importance of securing router access and monitoring network devices.

2. What advantages does SSH have over Telnet?

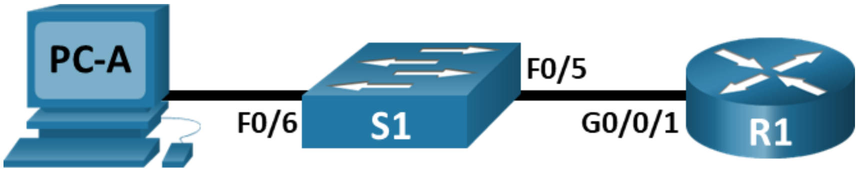
Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

[Title]

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.254	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure the Router for SSH Access

Part 3: Configure the Switch for SSH Access

Part 4: SSH from the CLI on the Switch

Background / Scenario

In the past, Telnet was the most common network protocol used to remotely configure network devices. Telnet does not encrypt the information between the client and server. This allows a network sniffer to intercept passwords and configuration information.

Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals. SSH is most often used to log in to a remote device and execute commands. However, it can also transfer files using the associated Secure FTP (SFTP) or Secure Copy (SCP) protocols.

The network devices that are communicating must be configured to support SSH in order for SSH to function. In this lab, you will enable the SSH server on a router and then connect to that router using a PC with an SSH client installed. On a local network, the connection is normally made using Ethernet and IP.

Note: The routers used with hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 1 Switch (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 1 PC (Windows OS with a terminal emulation program, such as Tera Term or PuTTy installed)
- Console cables to configure the Cisco IOS devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the router.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the router and switch.

Step 3: Configure the router.

a. Console into the router and enable privileged EXEC mode.

b. Enter configuration mode.

c. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

d. Assign **class** as the privileged EXEC encrypted password using the type 8 (PBKDF2) hashing algorithm.

e. Assign **cisco** as the console password and enable login.

f. Assign **cisco** as the VTY password and enable login.

g. Encrypt the plaintext passwords.

h. Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.

i. Configure and activate the G0/0/1 interface on the router using the information contained in the Addressing Table.

j. Save the running configuration to the startup configuration file.

Step 4: Configure PC-A.

a. Configure PC-A with an IP address and subnet mask.

b. Configure a default gateway for PC-A.

Step 5: Verify network connectivity.

Ping R1 from PC-A. If the ping fails, troubleshoot the connection.

Part 2: Configure the Router for SSH Access

Using Telnet to connect to a network device is a security risk because all the information is transmitted in a clear text format. SSH encrypts the session data and provides device authentication; therefore, SSH is recommended for remote connections. In Part 2, you will configure the router to accept SSH connections over the VTY lines.

Step 1: Configure device authentication.

The device name and domain are used as part of the crypto key when it is generated. Therefore, these names must be entered prior to issuing the **crypto key** command.

a. Configure device name.

b. Configure the domain for the device.

Step 2: Configure the encryption key method.

Step 3: Configure a local database username.

a. Configure a username using **admin** as the username and **Adm1nP@55** as the password using the type 8 (PBKDF2) hashing algorithm.

Step 4: Enable SSH on the VTY lines.

a. Enable SSH on the inbound VTY lines using the **transport input** command.

b. Change the login method to use the local database for user verification.

Step 5: Save the running configuration to the startup configuration file.

Step 6: Establish an SSH connection to the router.

a. Start Tera Term from PC-A.

b. Establish an SSH session to R1. Use the username **admin** and password **Adm1nP@55**. You should be able to establish an SSH session with R1.

Part 3: Configure the Switch for SSH Access

In Part 3, you will configure the switch to accept SSH connections. After the switch has been configured, establish an SSH session using Tera Term.

Step 1: Configure the basic settings on the switch.

a. Console into the switch and enable privileged EXEC mode.

b. Enter configuration mode.

c. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

d. Assign **class** as the privileged EXEC encrypted password using the type 8 (PBKDF2) hashing algorithm.

e. Assign **cisco** as the console password and enable login.

f. Assign **cisco** as the VTY password and enable login.

g. Encrypt the plain text passwords.

h. Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.

i. Configure and activate the VLAN 1 interface on the switch according to the Addressing Table.

j. Save the running configuration to the startup configuration file.

Step 2: Configure the switch for SSH connectivity.

Use the same commands that you used to configure SSH on the router in Part 2 to configure SSH for the switch.

a. Configure the device name as listed in the Addressing Table.

b. Configure the domain for the device.

c. Configure the encryption key method.

d. Configure a local database username using the type 8 (PBKDF2) hashing algorithm.

e. Enable Telnet and SSH on the VTY lines.

f. Change the login method to use the local database for user verification.

Step 3: Establish an SSH connection to the switch.

Start Tera Term from PC-A, and then SSH to the SVI interface on S1.

Are you able to establish an SSH session with the switch?

Part 4: SSH From the CLI on the Switch

The SSH client is built into the Cisco IOS and can be run from the CLI. In Part 4, you will SSH to the router from the CLI on the switch.

Step 1: View the parameters available for the Cisco IOS SSH client.

Use the question mark (**?**) to display the parameter options available with the **ssh** command.

```
S1# ssh ?
  -c     Select encryption algorithm
  -l     Log in using this user name
  -m     Select HMAC algorithm
  -o     Specify options
  -p     Connect to this port
  -v     Specify SSH Protocol Version
  -vrf   Specify vrf name
  WORD   IP address or hostname of a remote system
```

Step 2: SSH to R1 from S1.

a. You must use the **–l admin** option when you SSH to R1. This allows you to log in as user **admin**. When prompted, enter **Adm1nP@55** for the password.

```
S1# ssh -l admin 192.168.1.1
Password:
Authorized Users Only!
R1>
```

b. You can return to S1 without closing the SSH session to R1 by pressing **Ctrl**+**Shift**+**6**. Release the **Ctrl**+**Shift**+**6** keys and press **x**. The switch privileged EXEC prompt displays.

```
R1>
S1#
```

c. To return to the SSH session on R1, press Enter on a blank CLI line. You may need to press Enter a second time to see the router CLI prompt.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]

R1>
```

d. To end the SSH session on R1, type **exit** at the router prompt.

```
R1# exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

What versions of SSH are supported from the CLI?

Reflection Question

How would you provide multiple users, each with their own username, access to a network device?

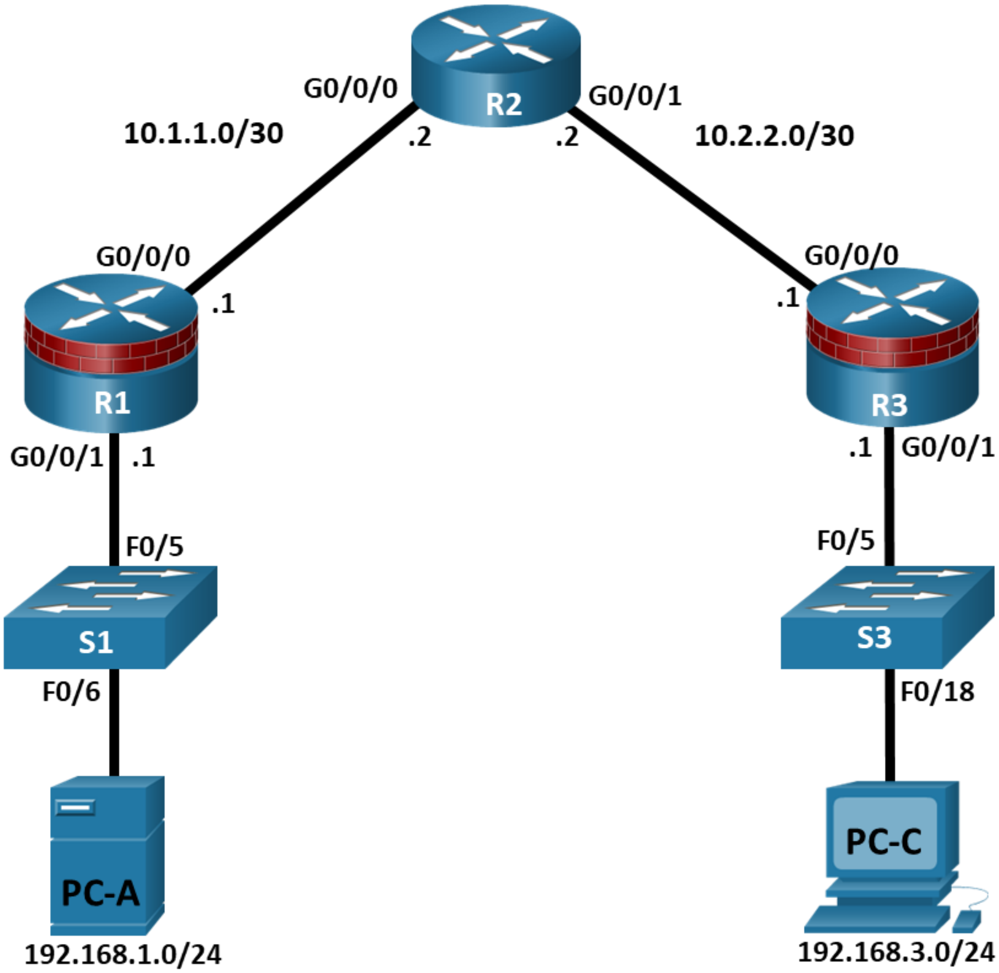
Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

[Title]

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
R2	G0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	G0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objectives

Part 1: Configure Basic Device Settings

- Cable the network as shown in the topology.
- Configure basic IP addressing for routers and PCs.
- Configure OSPF routing.
- Configure PC hosts.
- Verify connectivity between hosts and routers.

Part 2: Configure Administrative Roles

- Create multiple role views and grant varying privileges.
- Verify and contrast views.

Background / Scenario

The router is a critical component in any network. It controls the movement of data into and out of the network and between devices within the network. It is particularly important to protect network routers because the failure of a routing device could make sections of the network, or the entire network, inaccessible. Controlling access to routers and enabling reporting on routers is critical to network security and should be part of a comprehensive security policy.

In this lab, you will build a multi-router network and configure the routers and hosts. You will configure administrative roles with different privilege levels.

Note: The routers used with hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.6 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960+ with Cisco IOS Release 15.2(7) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Before you begin, ensure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 2 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 2 PCs (Windows OS with a terminal emulation program, such as PuTTY or Tera Term installed)
- Console cables to configure Cisco networking devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Device Settings

In this part, set up the network topology and configure basic settings, such as interface IP addresses.

Step 1: Cable the network.

Attach the devices, as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

a. Console into the router and enable privileged EXEC mode.

```
Router> enable
Router# configure terminal
```

Configure host names as shown in the topology.

```
R1(config)# hostname R1
```

Configure interface IP addresses as shown in the IP Addressing Table.

```
R1(config)# interface g0/0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# no shutdown

R1(config)# interface g0/0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

b. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup. R1 is shown here as an example.

```
R1(config)# no ip domain-lookup
```

Step 3: Configure OSPF routing on the routers.

a. Use the **router ospf** command in global configuration mode to enable OSPF on R1.

```
R1(config)# router ospf 1
```

b. Configure the **network** statements for the networks on R1. Use an area ID of 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

c. Configure OSPF on R2 and R3.

```
R2(config)# router ospf 1
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config)# router ospf 1
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
```

d. Issue the **passive-interface** command to change the G0/0/1 interface on R1 and R3 to passive.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0/1

R3(config)# router ospf 1
R3(config-router)# passive-interface g0/0/1
```

Step 4: Verify OSPF neighbors and routing information.

a. Issue the **show ip ospf neighbor** command to verify that each router lists the other routers in the network as neighbors.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.2.2          1   FULL/BDR        00:00:37    10.1.1.2
GigabitEthernet0/0/0
```

b. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, GigabitEthernet0/0/0
L        10.1.1.1/32 is directly connected, GigabitEthernet0/0/0
O        10.2.2.0/30 [110/2] via 10.1.1.2, 00:01:11, GigabitEthernet0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
O     192.168.3.0/24 [110/3] via 10.1.1.2, 00:01:07, GigabitEthernet0/0/0
```

Step 5: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C as shown in the IP Addressing Table.

Step 6: Verify connectivity between PC-A and PC-C.

a. Ping from R1 to R3.

   If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A, on the R1 LAN, to PC-C, on the R3 LAN.

   If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C you have demonstrated that OSPF routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run, show ip ospf neighbor,** and **show ip route** commands to help identify routing protocol-related problems.

Step 7: Save the basic running configuration for each router.

Save the basic running configuration for the routers as text files on your PC. These text files can be used to restore configurations later in the lab.

Part 2: Configure Administrative Roles

In this part of lab, you will:

- Create multiple administrative roles, or views, on routers R1 and R3.
- Grant each view varying privileges.
- Verify and contrast the views.

The role-based CLI access feature allows the network administrator to define views, which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (config) mode commands. Views restrict user access to the Cisco IOS CLI and configuration information. A view can define which commands are accepted and what configuration information is visible.

Note: Perform all tasks on both R1 and R3. The procedures and output for R1 are shown here.

If an administrator wants to configure another view to the system, the system must be in root view. When a system is in root view, the user has the same access privileges as a user who has level-15 privileges, but the root view user can also configure a new view and add or remove commands from the view. When you are in a CLI view, you have access only to the commands that have been added to that view by the root view user.

Step 1: Enable AAA on router R1.

To define views, enable AAA on the router.

```
R1# configure terminal
R1(config)# aaa new-model
```

Step 2: Configure privileged EXEC mode password.

A privileged EXEC mode password is required to access the root view. The password **cisco12345** is used in this example.

```
R1(config)# enable secret cisco12345
R1# exit
```

Step 3: Enable the root view.

Use the command **enable view** to enable the root view.

```
R1# enable view
Password: cisco12345
```

Step 4: Create the admin1 view, establish a password, and assign privileges.

a. The admin1 user is the top-level user below root that is allowed to access this router. It has the most authority. The admin1 user can use all **show**, **config**, and **debug** commands. Use the following command to create the admin1 view while in the root view.

```
R1# configure terminal
R1(config)# parser view admin1
R1(config-view)#
```

Note: To delete a view, use the command **no parser view** ***viewname***.

b. Associate the admin1 view with an encrypted password.

```
R1(config-view)# secret admin1pass
R1(config-view)#
```

c. Review the commands that can be configured in the admin1 view. Use the **commands ?** command to see available commands. The following is a partial listing of the available commands.

```
R1(config-view)# commands ?
  RITE-profile           Router IP traffic export profile command mode
  RMI Node Config        Resource Policy Node Config mode
  RMI Resource Group     Resource Group Config mode
  RMI Resource Manager   Resource Manager Config mode
  RMI Resource Policy    Resource Policy Config mode
  SASL-profile           SASL profile configuration mode
  aaa-attr-list          AAA attribute list config mode
  aaa-user               AAA user definition
  accept-dialin          VPDN group accept dialin configuration mode
  accept-dialout         VPDN group accept dialout configuration mode
  address-family         Address Family configuration mode
<output omitted>
```

d. Add all **config**, **show**, and **debug** commands to the admin1 view and then exit from view configuration mode.

```
R1(config-view)# commands exec include all show
R1(config-view)# commands exec include all config terminal
R1(config-view)# commands exec include all debug
R1(config-view)# end
```

e. Verify the admin1 view.

```
R1# enable view admin1
Password: admin1pass

R1# show parser view
Current view is 'admin1'
```

f. Examine the commands available in the admin1 view.

```
R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  configure    Enter configuration mode
  debug        Debugging functions (see also 'undebug')
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  show           Show running system
```

Note: There may be more EXEC commands available than are displayed. This depends on your device and the IOS image used.

g. Examine the **show** commands available in the admin1 view.

```
R1# show ?
  aaa                        Show AAA values
  access-expression          List access expression
  access-lists               List access lists
  acircuit                   Access circuit info
  adjacency                  Adjacent nodes
  aliases                    Display alias commands
  alignment                  Show alignment information
  appfw                      Application Firewall information
  archive                    Archive functions
  arp                        ARP table
<output omitted>
```

Step 5: Create the admin2 view, establish a password, and assign privileges.

a. The admin2 user is a junior administrator in training who is allowed to view all configurations but is not allowed to configure the routers or use debug commands.

b. Use the **enable view** command to enable the root view, and enter the enable secret password **cisco12345**.

```
R1# enable view
Password: cisco12345
```

c. Use the following command to create the admin2 view.

```
R1# configure terminal
R1(config)# parser view admin2
```

d. Associate the admin2 view with a password.

```
R1(config-view)# secret admin2pass
```

e. Add all **show** commands to the view, and then exit from view configuration mode.

```
R1(config-view)# commands exec include all show
R1(config-view)# end
```

f. Verify the admin2 view.

```
R1# enable view admin2
Password: admin2pass

R1# show parser view
Current view is ‘admin2’
```

g. Examine the commands available in the admin2 view.

```
R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  show         Show running system information
```

Note: There may be more EXEC commands available than are displayed. This depends on your device and the IOS image used.

What is missing from the list of admin2 commands that is present in the admin1 commands?

Step 6: Create the tech view, establish a password, and assign privileges.

a. The tech user typically installs end-user devices and cabling. Tech users are only allowed to use selected **show** commands.

b. Use the enable **view** command to enable the root view, and enter the enable secret password **cisco12345**.

```
R1# enable view
Password: cisco12345
```

c. Use the following command to create the tech view.

```
R1(config)# parser view tech
```

d. Associate the tech view with a password.

```
R1(config-view)# secret techpasswd
```

e. Add the following **show** commands to the view and then exit from view configuration mode.

```
R1(config-view)# commands exec include show version
R1(config-view)# commands exec include show interfaces
R1(config-view)# commands exec include show ip interface brief
R1(config-view)# commands exec include show parser view
R1(config-view)# end
```

f. Verify the tech view.

```
R1# enable view tech
Password: techpasswd

R1# show parser view
Current view is 'tech'
```

g. Examine the commands available in the tech view.

```
R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  show         Show running system information
```

Note: There may be more EXEC commands available than are displayed. This depends on your device and the IOS image used.

h. Examine the **show** commands available in the tech view.

```
R1# show ?
  banner      Display banner information
  flash0:     display information about flash0: file system
  flash1:     display information about flash1: file system
  flash:      display information about flash: file system
  interfaces  Interface status and configuration
  ip          IP information
  parser      Display parser information
  usbflash0:  display information about usbflash0: file system
  version     System hardware and software status
```

Note: There may be more EXEC commands available than are displayed. This depends on your device and the IOS image used.

i. Issue the **show ip interface brief** command.

Were you able to do it as the tech user? Explain.

j. Issue the **show ip route** command.

Were you able to do it as the tech user?

k. Return to root view with the **enable view** command.

```
R1# enable view
Password: cisco12345
```

l. Issue the **show run** command to see the views you created.

For tech view, why are the **show** and **show ip** commands listed as well as **show ip interface** and **show ip interface brief**?

m. Configure the same administrative roles on router R3.

Step 7: Save the configuration on routers R1 and R3.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

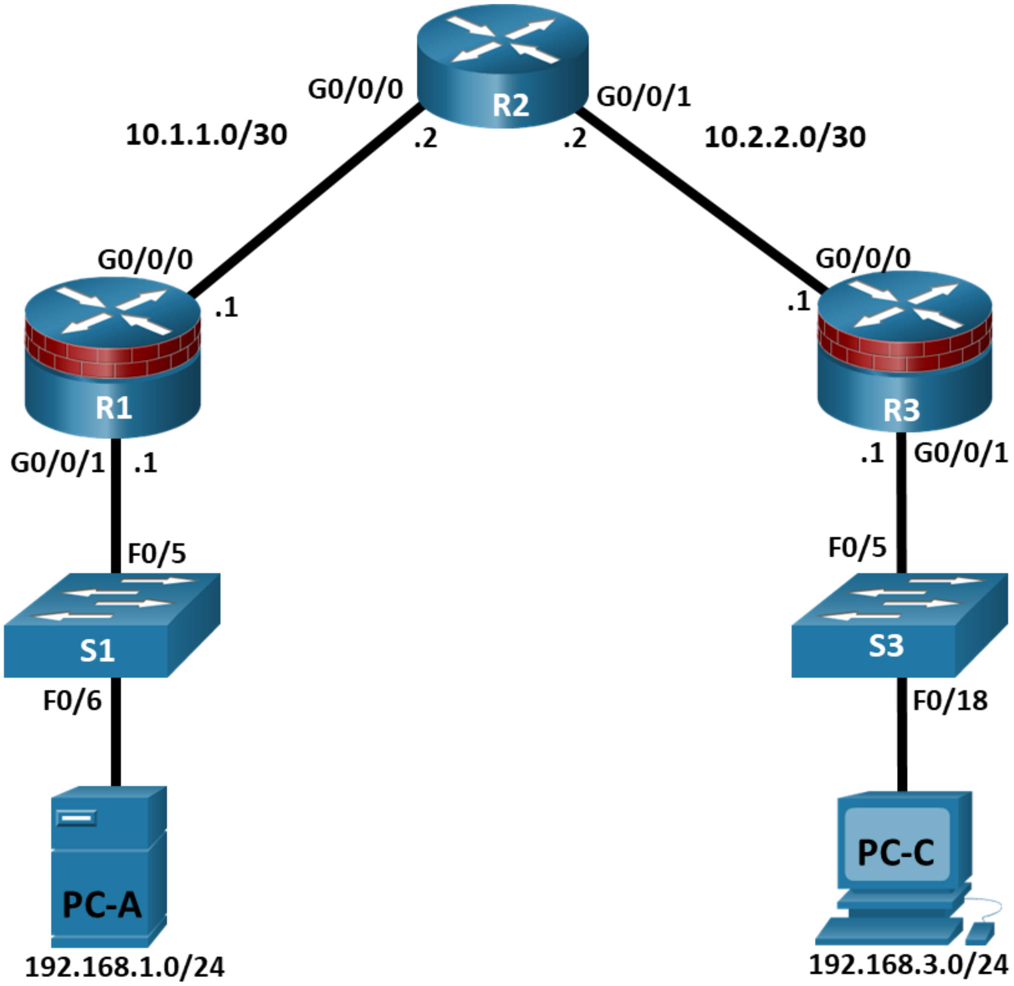
Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

[Title]

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
R2	G0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	G0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objectives

Part 1: Configure Basic Device Settings

- Cable the network as shown in the topology.
- Configure basic IP addressing for routers and PCs.
- Configure OSPF routing.
- Configure PC hosts.
- Verify connectivity between hosts and routers.

Part 2: Configure Automated Security Features

- Lock down a router using AutoSecure and verify the configuration.
- Contrast using AutoSecure with manually securing a router using the command line.

Background / Scenario

The router is a critical component in any network. It controls the movement of data into and out of the network and between devices within the network. It is particularly important to protect network routers because the failure of a routing device could make sections of the network, or the entire network, inaccessible. Controlling access to routers and enabling reporting on routers is critical to network security and should be part of a comprehensive security policy.

In this lab, you will build a multi-router network and configure the routers and hosts. You will use automated security features on router R3.

Note: The routers used with hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.6 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960+ with Cisco IOS Release 15.2(7) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Before you begin, ensure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 2 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 2 PCs (Windows OS with a terminal emulation program, such as PuTTY or Tera Term installed)
- Console cables to configure Cisco networking devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Device Settings

In this part, set up the network topology and configure basic settings, such as interface IP addresses.

Step 1: Cable the network.

Attach the devices, as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

a. Console into the router and enable privileged EXEC mode.

```
Router> enable
Router# configure terminal
```

Configure host names as shown in the topology.

```
R1(config)# hostname R1
```

Configure interface IP addresses as shown in the IP Addressing Table.

```
R1(config)# interface g0/0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# no shutdown

R1(config)# interface g0/0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

b. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup. R1 is shown here as an example.

```
R1(config)# no ip domain-lookup
```

Step 3: Configure OSPF routing on the routers.

a. Use the **router ospf** command in global configuration mode to enable OSPF on R1.

```
R1(config)# router ospf 1
```

b. Configure the **network** statements for the networks on R1. Use an area ID of 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

c. Configure OSPF on R2 and R3.

```
R2(config)# router ospf 1
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config)# router ospf 1
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
```

d. Issue the **passive-interface** command to change the G0/0/1 interface on R1 and R3 to passive.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0/1

R3(config)# router ospf 1
R3(config-router)# passive-interface g0/0/1
```

Step 4: Verify OSPF neighbors and routing information.

a. Issue the **show ip ospf neighbor** command to verify that each router lists the other routers in the network as neighbors.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.2.2          1   FULL/BDR        00:00:37    10.1.1.2
GigabitEthernet0/0/0
```

b. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, GigabitEthernet0/0/0
L        10.1.1.1/32 is directly connected, GigabitEthernet0/0/0
O        10.2.2.0/30 [110/2] via 10.1.1.2, 00:01:11, GigabitEthernet0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
O     192.168.3.0/24 [110/3] via 10.1.1.2, 00:01:07, GigabitEthernet0/0/0
```

Step 5: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C as shown in the IP Addressing Table.

Step 6: Verify connectivity between PC-A and PC-C.

a. Ping from R1 to R3.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A, on the R1 LAN, to PC-C, on the R3 LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C you have demonstrated that OSPF routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run, show ip ospf neighbor,** and **show ip route** commands to help identify routing protocol-related problems.

Part 2: Configure Basic Security Settings on R1

In this part, copy and paste the following commands into R1 to configure basic security settings.

```
enable
```

```
configure terminal
service password-encryption
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
ip domain name netsec.com
username user01 algorithm-type scrypt secret user01pass
username admin privilege 15 algorithm-type scrypt secret adminpasswd
banner motd " Unauthorized access is strictly prohibited! "
line con 0
 exec-timeout 5 0
login local
 logging synchronous
line aux 0
 exec-timeout 5 0
login local
line vty 0 4
 exec-timeout 5 0
 privilege level 15
transport input ssh
 login local
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
```

Part 3: Configure Automated Security Features

In this part, you will do as follows:

- Use AutoSecure to secure R3.
- Review router security configurations with CLI.

By using a single command in CLI mode, the AutoSecure feature allows you to disable common IP services that can be exploited for network attacks. It can also enable IP services and features that can aid in the defense of a network when under attack. AutoSecure simplifies the security configuration of a router and hardens the router configuration.

Step 1: Use the AutoSecure Cisco IOS feature on R3.

a. Enter privileged EXEC mode using the **enable** command.

b. Issue the **auto secure** command on R3 to lock down the router. R2 represents an ISP router, so assume that R3 G0/0/0 is connected to the internet when prompted by the AutoSecure questions. Respond to the AutoSecure questions as shown in the following output. The responses are bolded.

```
R3# auto secure
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router but it will not make router absolutely secure
```

```
from all security attacks ***

All the configuration done as part of AutoSecure will be
shown here. For more details of why and how this configuration
is useful, and any possible side effects, please refer to Cisco
documentation of AutoSecure.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

If this device is being managed by a network management station,
AutoSecure configuration may block network management traffic.
Continue with AutoSecure? [no]: yes

Gathering information about the router for AutoSecure


Is this router connected to internet? [no]: yes
Enter the number of interfaces facing internet [1]:
Interface                IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0/0     10.2.2.1        YES manual up
up
GigabitEthernet0/0/1     192.168.3.1     YES manual up
up
Serial0/1/0              unassigned      YES unset  up
up
Serial0/1/1              unassigned      YES unset  up
up
Enter the interface name that is facing internet: GigabitEthernet0/0/0

Securing Management plane services..

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Here is a sample Security Banner to be shown
```

```
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

Enter the security banner {Put the banner between
k and k, where k is any character}:
# Unauthorized Access Prohibited #
Enable secret is either not configured or
 is the same as the enable password
Enter the new enable secret: cisco12345
Confirm the enable secret : cisco12345
Enter the new enable password: 12345cisco
Confirm the enable password: 12345cisco

Configuration of local user database
Enter the username: admin
Enter the password: adminpasswd
Confirm the password: adminpasswd
Configuring AAA local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 60

Maximum Login failures with the device: 2

Maximum time period for crossing the failed login attempts: 30

Configure SSH server? [yes]: [Enter]
Enter the domain-name: www.netsec.com

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply

Securing Forwarding plane services..

Enabling unicast rpf on all interfaces connected
to internet

Configure CBAC Firewall feature? [yes/no]: no

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
banner motd ^C  Unauthorized Access Prohibited ^C
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$lubv$Rdx4gHUcijbxV7p2z76/71
enable password 7 110A1016141D5D5B5C737B
username admin password 7 02050D4808095E731F1A5C
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
```

```
line tty 1
 login authentication local_auth
 exec-timeout 15 0
login block-for 60 attempts 2 within 30
ip domain-name www.netsec.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
int GigabitEthernet0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
int GigabitEthernet0/0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
ip access-list extended 100
 permit udp any any eq bootpc
interface GigabitEthernet0/0/0
 ip verify unicast source reachable-via rx 100
!
end


Apply this configuration to running-config? [yes]: [Enter]


Applying the config generated to running-config


 WARNING: Command has been added to the configuration using a type 5
password. However, type 5 passwords will soon be deprecated. Migrate to
a supported password type
```

```
 WARNING: Command has been added to the configuration using a type 7
password. However, type 7 passwords will soon be deprecated. Migrate to
a supported password type

 WARNING: Command has been added to the configuration using a type 7
password. However, type 7 passwords will soon be deprecated. Migrate to
a supported password typeThe name for the keys will be:
R3.www.netsec.com


% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 0 seconds)


R3#
```

Note: The questions asked and the output may vary depend on the features on the IOS image and device.

Step 2: Establish an SSH connection from PC-C to R3.

a. Start PuTTy or another SSH client, and log in with the **admin** account and password **adminpasswd** created when AutoSecure was run. Enter the IP address of the R3 G0/0/1 interface **192.168.3.1**.

b. Because SSH was configured using AutoSecure on R3, you will receive a PuTTY security warning. Click **Yes** to connect anyway.

c. Enter privileged EXEC mode with password **cisco12345**, and verify the R3 configuration using the **show run** command.

Step 3: Contrast the AutoSecure-generated configuration of R3 with the manual configuration of R1.

1. What security-related configuration changes were performed on R3 by AutoSecure that were not performed in previous sections of the lab on R1?

2. What security-related configuration changes were performed in previous sections of the lab that were not performed by AutoSecure?

3. Identify at least five unneeded services that were locked down by AutoSecure and at least three security measures applied to each interface.

   Note: Some of the services listed as being disabled in the AutoSecure output above might not appear in the **show running-config** output because they are already disabled by default for this router and Cisco IOS version.

   Services disabled include:

   For each interface, the following were disabled:

4. What are some advantages to using AutoSecure?

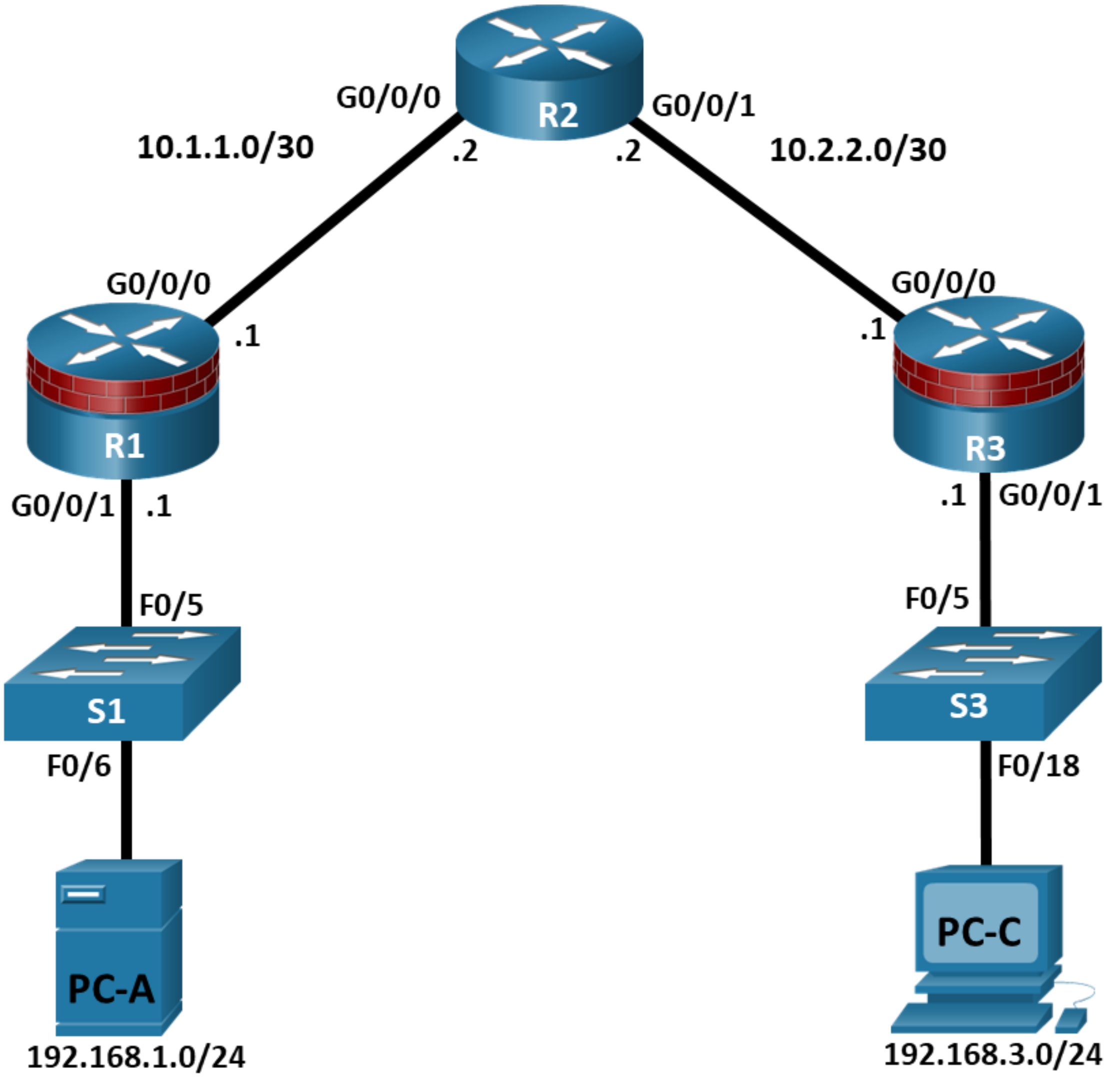
Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

[Title]

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
R2	G0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	G0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objectives

Part 1: Configure Basic Device Settings

- Cable the network as shown in the topology.
- Configure basic IP addressing for routers and PCs.
- Configure OSPF routing.
- Configure PC hosts.
- Verify connectivity between hosts and routers.

Part 2: Secure the Control Plane

- Configure OSPF Authentication using SHA256
- Verify OSPF Authentication

Background / Scenario

The router is a critical component in any network. It controls the movement of data into and out of the network and between devices within the network. It is particularly important to protect network routers because the failure of a routing device could make sections of the network, or the entire network, inaccessible. Controlling access to routers and enabling reporting on routers is critical to network security and should be part of a comprehensive security policy.

In this lab, you will build a multi-router network and configure the routers and hosts. You will configure administrative roles with different privilege levels.

Note: The routers used with hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.6 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960+ with Cisco IOS Release 15.2(7) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Before you begin, ensure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 2 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 2 PCs (Windows OS with a terminal emulation program, such as PuTTY or Tera Term installed)
- Console cables to configure Cisco networking devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Device Settings

In this part, set up the network topology and configure basic settings, such as interface IP addresses.

Step 1: Cable the network.

Attach the devices, as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

a. Console into the router and enable privileged EXEC mode.

```
Router> enable
Router# configure terminal
```

Configure host names as shown in the topology.

```
R1(config)# hostname R1
```

Configure interface IP addresses as shown in the IP Addressing Table.

```
R1(config)# interface g0/0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# no shutdown

R1(config)# interface g0/0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

b. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup. R1 is shown here as an example.

```
R1(config)# no ip domain-lookup
```

Step 3: Configure OSPF routing on the routers.

a. Use the **router ospf** command in global configuration mode to enable OSPF on R1.

```
R1(config)# router ospf 1
```

b. Configure the **network** statements for the networks on R1. Use an area ID of 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

c. Configure OSPF on R2 and R3.

```
R2(config)# router ospf 1
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config)# router ospf 1
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
```

d. Issue the **passive-interface** command to change the G0/0/1 interface on R1 and R3 to passive.

```
R1(config)# router ospf 1
```

```
R1(config-router)# passive-interface g0/0/1

R3(config)# router ospf 1
R3(config-router)# passive-interface g0/0/1
```

Step 4: Verify OSPF neighbors and routing information.

a. Issue the **show ip ospf neighbor** command to verify that each router lists the other routers in the network as neighbors.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.2.2          1   FULL/BDR        00:00:37    10.1.1.2        
GigabitEthernet0/0/0
```

b. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, GigabitEthernet0/0/0
L        10.1.1.1/32 is directly connected, GigabitEthernet0/0/0
O        10.2.2.0/30 [110/2] via 10.1.1.2, 00:01:11, GigabitEthernet0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
O     192.168.3.0/24 [110/3] via 10.1.1.2, 00:01:07, GigabitEthernet0/0/0
```

Step 5: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C as shown in the IP Addressing Table.

Step 6: Verify connectivity between PC-A and PC-C.

a. Ping from R1 to R3.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A, on the R1 LAN, to PC-C, on the R3 LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C you have demonstrated that OSPF routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run, show ip ospf neighbor,** and **show ip route** commands to help identify routing protocol-related problems.

Step 7: Save the basic running configuration for each router.

Save the basic running configuration for the routers as text files on your PC. These text files can be used to restore configurations later in the lab.

Part 2: Configure OSPF Routing Protocol Authentication using SHA256 Hashing.

Step 1: Configure a key chain on all three routers.

a. Assign a key chain name and number.

```
R1(config)# key chain NetAcad
R1(config-keychain)# key 1
```

b. Assign the authentication key string.

```
R1(config-keychain-key)# key-string NetSeckeystring
```

c. Configure the encryption algorithm to be used for authentication, use SHA256 encryption.

```
R1(config-keychain-key)# cryptographic-algorithm hmac-sha-256
```

Step 2: Configure the GigabitEthernet interfaces to use OSPF authentication.

a. Use the **ip ospf authentication** command to assign the key-chain to the GigabitEthernet0/0/0 interface on R1 and R3.

```
R1(config)# interface g0/0/0
R1(config-if)# ip ospf authentication key-chain NetAcad
R1(config)#
*Jan 31 00:34:49.172: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on
GigabitEthernet0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired


R3(config)# interface g0/0/0
R3(config-if)# ip ospf authentication key-chain NetAcad
R3(config)#
*Jan 31 00:32:31.998: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on
GigabitEthernet0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

b. Use the **ip ospf authentication** command to assign the key-chain to both GigabitEthernet interfaces on R2.

```
R2(config)# interface g0/0/0
R2(config-if)# ip ospf authentication key-chain NetAcad
R2(config)# interface g0/0/1
R2(config-if)# ip ospf authentication key-chain NetAcad
R2(config-if)#
*Jan 31 00:37:48.379: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on
GigabitEthernet0/0/0 from LOADING to FULL, Loading Done
*Jan 31 00:38:04.829: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on
GigabitEthernet0/0/1 from LOADING to FULL, Loading Done
```

Step 3: Verify OSPF Routing and Authentication is Correct.

a. Issue the show **ip ospf interface** command to verify that Authentication Key has been assigned to the GigabitEthernet interfaces on all routers.

```
R1# show ip ospf interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.1/30, Interface ID 5, Area 0
  Attached via Network Statement
  Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.1.1, Interface address 10.1.1.1
  Backup Designated router (ID) 10.2.2.2, Interface address 10.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 3
  Last flood scan time is 0 msec, maximum is 1 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-256 - key chain NetAcad
```

b. Issue the **show ip ospf neighbor** command to verify that each router lists the other routers in the network as neighbors.

```
R2# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.3.1       1   FULL/DR         00:00:37    10.2.2.1
GigabitEthernet0/0/1
192.168.1.1       1   FULL/DR         00:00:37    10.1.1.1
GigabitEthernet0/0/0
```

c. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

```
R3# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O        10.1.1.0/30 [110/2] via 10.2.2.2, 00:08:15, GigabitEthernet0/0/0
C        10.2.2.0/30 is directly connected, GigabitEthernet0/0/0
L        10.2.2.1/32 is directly connected, GigabitEthernet0/0/0
O     192.168.1.0/24 [110/3] via 10.2.2.2, 00:08:12, GigabitEthernet0/0/0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.3.1/32 is directly connected, GigabitEthernet0/0/1
```

d. Use the **ping** command to verify connectivity between PC-A and PC-C.

If the pings are not successful, troubleshoot before continuing.

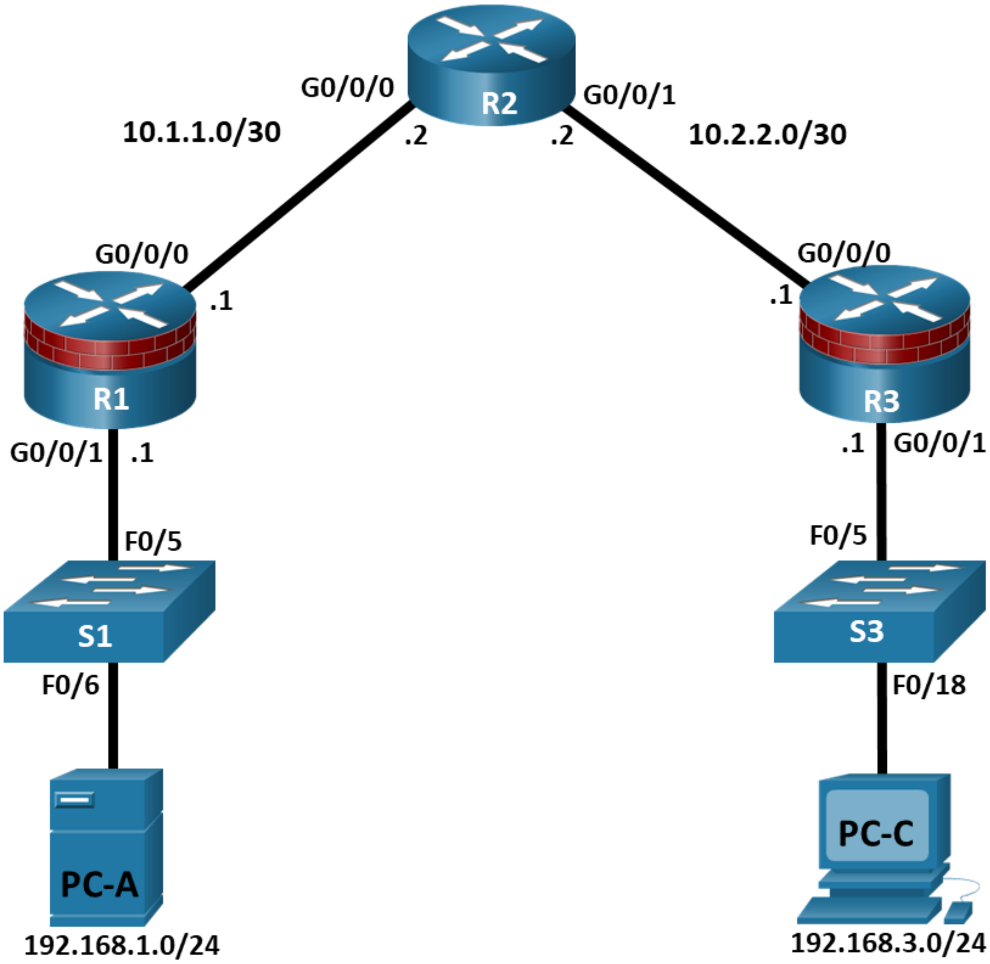
Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

[Title]

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
R2	G0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	G0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure SNMPv3 Security using an ACL.

Part 3: Configure a router as a synchronized time source for other devices using NTP.

Part 4: Configure syslog support on a router.

Background / Scenario

The router is a critical component in any network. It controls the movement of data into and out of the network and between devices within the network. It is particularly important to protect network routers because the failure of a routing device could make sections of the network, or the entire network, inaccessible. Controlling access to routers and enabling reporting on routers is critical to network security and should be part of a comprehensive security policy.

In this lab, you will build a multi-router network and configure the routers and hosts. You will configure SNMP, NTP, and syslog support to monitor router configuration changes.

Note: The routers used with hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.6 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960+ with Cisco IOS Release 15.2(7) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Before you begin, ensure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 2 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 2 PCs (Windows OS with a terminal emulation program, such as PuTTY or Tera Term installed)
- Console cables to configure Cisco networking devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Device Settings

In this part, set up the network topology and configure basic settings, such as interface IP addresses.

Step 1: Cable the network.

Attach the devices, as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

a. Console into the router and enable privileged EXEC mode.

```
Router> enable
Router# configure terminal
```

b. Configure host names as shown in the topology.

```
R1(config)# hostname R1
```

c. Configure interface IP addresses as shown in the IP Addressing Table.

```
R1(config)# interface g0/0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# no shutdown

R1(config)# interface g0/0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

d. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup. R1 is shown here as an example.

```
R1(config)# no ip domain-lookup
```

Step 3: Configure OSPF routing on the routers.

a. Use the **router ospf** command in global configuration mode to enable OSPF on R1.

```
R1(config)# router ospf 1
```

b. Configure the **network** statements for the networks on R1. Use an area ID of 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

c. Configure OSPF on R2 and R3.

```
R2(config)# router ospf 1
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config)# router ospf 1
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
```

d. Issue the **passive-interface** command to change the G0/0/1 interface on R1 and R3 to passive.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0/1

R3(config)# router ospf 1
R3(config-router)# passive-interface g0/0/1
```

Step 4: Verify OSPF neighbors and routing information.

a. Issue the **show ip ospf neighbor** command to verify that each router lists the other routers in the network as neighbors.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.2.2          1   FULL/BDR        00:00:37    10.1.1.2
GigabitEthernet0/0/0
```

b. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, GigabitEthernet0/0/0
L        10.1.1.1/32 is directly connected, GigabitEthernet0/0/0
O        10.2.2.0/30 [110/2] via 10.1.1.2, 00:01:11, GigabitEthernet0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
O     192.168.3.0/24 [110/3] via 10.1.1.2, 00:01:07, GigabitEthernet0/0/0
```

Step 5: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C as shown in the IP Addressing Table.

Step 6: Verify connectivity between PC-A and PC-C.

a. Ping from R1 to R3.

   If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A, on the R1 LAN, to PC-C, on the R3 LAN.

   If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C you have demonstrated that OSPF routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run, show ip ospf neighbor,** and **show ip route** commands to help identify routing protocol-related problems.

Step 7: Save the basic running configuration for each router.

Save the basic running configuration for the routers as text files on your PC. These text files can be used to restore configurations later in the lab.

Part 2: Configure SNMPv3 Security using an ACL.

Simple Network Management Protocol (SNMP) enables network administrators to monitor network performance, mange network devices, and troubleshoot network problems. SNMPv3 provides secure access by authenticating and encrypting SNMP management packets over the network. You will configure SNMPv3 using an ACL on R1.

Step 1: Configure an ACL on R1 that will restrict access to SNMP on the 192.168.1.0 LAN.

a. Create a standard access-list named **PERMIT-SNMP**.

```
R1(config)# ip access-list standard PERMIT-SNMP
```

b. Add a permit statement to allow only packets on R1's LAN.

```
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
```

Step 2: Configure the SNMP view.

Configure a SNMP view called **SNMP-RO** to include the ISO MIB family.

```
R1(config)# snmp-server view SNMP-RO iso included
```

Step 3: Configure the SNMP group.

Call the group name **SNMP-G1**, and configure the group to use SNMPv3 and require both authentication and encryption by using the **priv** keyword. Associate the view you created in Step 2 to the group, giving it read only access with the **read** parameter. Finally specify the ACL **PERMIT-SNMP**, configured in Step 1, to restrict SNMP access to the local LAN.

```
R1(config)# snmp-server group SNMP-G1 v3 priv read SNMP-RO access
PERMIT-SNMP
```

Step 4: Configure the SNMP user.

Configure an **SNMP-Admin** user and associate the user to the **SNMP-G1** group you configured in Step 3. Set the authentication method to **SHA** and the authentication password to **Authpass**. Use AES-128 for encryption with a password of **Encrypass**.

```
R1(config)# snmp-server user SNMP-Admin SNMP-G1 v3 auth sha Authpass
priv aes 128 Encrypass
R1(config)# end
```

Step 5: Verify your SNMP configuration.

a. Use the **show snmp group** command in privilege EXEC mode to view the SNMP group configuration. Verify that your group is configured correctly.

Note: If you need to make changes to the group, use the command **no snmp group** to remove the group from the configuration and then re-add it with the correct parameters.

```
R1# show snmp group
groupname: ILMI                             security model:v1
contextname: <no context specified>         storage-type: permanent
readview : *ilmi                            writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                             security model:v2c
contextname: <no context specified>         storage-type: permanent
readview : *ilmi                            writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: SNMP-G1                          security model:v3 priv
```

```
contextname: <no context specified>          storage-type: nonvolatile
readview : SNMP-RO                           writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active      access-list: PERMIT-SNMP
```

b. Use the command **show snmp user** to view the SNMP user information.

Note: The **snmp-server user** command is hidden from view in the configuration for security reasons. However, if you need to make changes to a SNMP user, you can issue the command **no snmp-server user** to remove the user from the configuration, and then re-add the user with the new parameters.

```
R1# show snmp user

User name: SNMP-Admin
Engine ID: 800000090300707 9B3923640
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: SNMP-G1
```

Part 3: Configure a Synchronized Time Source Using NTP.

R2 will be the master NTP clock source for routers R1 and R3.

Note: R2 could also be the master clock source for switches S1 and S3, but it is not necessary to configure them for this lab.

Step 1: Set Up the NTP Master using Cisco IOS commands.

R2 is the master NTP server in this lab. All other routers and switches learn the time from it, either directly or indirectly. For this reason, you must ensure that R2 has the correct Coordinated Universal Time set.

a. Use the **show clock** command to display the current time set on the router.

```
R2# show clock
*18:18:25.443 UTC Sun Jan 31 2021
```

b. To set the time on the router, use the **clock set** *time* command.

```
R2# clock set 11:17:00 Jan 31 2021
R2#
*Jan 31 11:17:00.001: %SYS-6-CLOCKUPDATE: System clock has been updated
from 18:19:03 UTC Sun Jan 31 2021 to 11:17:00 UTC Sun Jan 31 2021,
configured from console by console.
Jan 31 11:17:00.001: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has
been set.
```

c. Configure NTP authentication by defining the authentication key number, hashing type, and password that will be used for authentication. The password is case sensitive.

```
R2# config t
R2(config)# ntp authentication-key 1 md5 NTPpassword
```

d. Configure the trusted key that will be used for authentication on R2.

```
R2(config)# ntp trusted-key 1
```

e. Enable the NTP authentication feature on R2.

```
R2(config)# ntp authenticate
```

f. Configure R2 as the NTP master using the **ntp master** *stratum-number* command in global configuration mode. The stratum number indicates the distance from the original source. For this lab, use a stratum number of **3** on R2. When a device learns the time from an NTP source, its stratum number becomes one greater than the stratum number of its source.

```
R2(config)# ntp master 3
```

Step 2: Configure R1 and R3 as NTP clients using the CLI.

a. Issue the **debug ntp all** command to see NTP activity on R1 as it synchronizes with R2. Review the debug messages as you proceed through this step.

```
R1# debug ntp all
NTP events debugging is on
NTP core messages debugging is on
NTP clock adjustments debugging is on
NTP reference clocks debugging is on
NTP packets debugging is on
```

b. Configure NTP authentication by defining the authentication key number, hashing type, and password that will be used for authentication.

```
R1# config t
R1(config)# ntp authentication-key 1 md5 NTPpassword
R1(config)#
*Jan 31 18:41:23.707: NTP Core(INFO): keys initilized.
*Jan 31 18:41:23.712: NTP Core(NOTICE): proto: precision =  usec
*Jan 31 18:41:23.712: %NTP : Drift Read Failed (String Error).
*Jan 31 18:41:23.712: NTP Core(DEBUG): drift value read: 0.000000000
*Jan 31 18:41:23.712: NTP Core(NOTICE): ntpd  PPM
*Jan 31 18:41:23.712: NTP Core(NOTICE): trans state : 1
*Jan 31 18:41:23.712: NTP: Initialized interface GigabitEthernet0/0/0
*Jan 31 18:41:23.712: NTP: Initialized interface GigabitEthernet0/0/1
*Jan 31 18:41:23.712: NTP: Initialized interface LIIN0
R1(config)#
*Jan 31 18:41:23.713: NTP Core(INFO): more memory added for keys.
*Jan 31 18:41:23.713: NTP Core(INFO): key (1) added.
```

c. Configure the trusted key that will be used for authentication. This command provides protection against accidentally synchronizing the device to a time source that is not trusted.

```
R1(config)# ntp trusted-key 1
R1(config)#
*Jan 31 18:43:56.191: NTP Core(INFO): key (1) marked as trusted.
```

d. Enable the NTP authentication feature.

```
R1(config)# ntp authenticate
R1(config)#
*Jan 31 18:44:33.482: NTP Core(INFO): 0.0.0.0 C01C 0C clock_step
```

e. R1 and R3 will become NTP clients of R2. Use the command **ntp server** *hostname*. The host name can also be an IP address.

Note: The command **ntp update-calendar** may be necessary to periodically updates the calendar with the NTP time for other IOS images.

```
R1(config)# ntp server 10.1.1.2
R1(config)#
*Jan 31 18:45:29.714: NTP message sent to 10.1.1.2, from interface
'GigabitEthernet0/0/0' (10.2.2.1).
*Jan 31 18:45:29.715: NTP message received from 10.1.1.2 on interface
'GigabitEthernet0/0/0' (10.2.2.1).
*Jan 31 18:45:29.716: NTP Core(DEBUG): ntp_receive: message received
*Jan 31 18:45:29.716: NTP Core(DEBUG): ntp_receive: peer is 0x80007FA135BB32F8,
next action is 1.
*Jan 31 18:45:29.716: NTP Core(DEBUG): Peer becomes reachable, poll set to 6.

*Jan 31 18:45:29.716: NTP Core(INFO): 10.1.1.2 8014 84 reachable
*Jan 31 18:45:29.716: NTP Core(INFO): 10.1.1.2 962A 8A sys_peer
R1(config)#
*Jan 31 18:45:29.716: NTP: step(0xFFFF9D56.B5A1C9F4): local_offset =
0x00000000.00000000, curtime = 0xE3C17949.B74BC8A0
*Jan 31 11:44:32.426: NTP Core(NOTICE): time reset -25257.290500 s
*Jan 31 11:44:32.426: NTP Core(NOTICE): trans state : 4
*Jan 31 11:44:32.426: NTP Core(INFO): 0.0.0.0 C62C 0C clock_step
*Jan 31 11:44:32.426: NTP Core(INFO): 0.0.0.0 C03C 0C clock_step
*Jan 31 11:44:33.423: NTP message sent to 10.1.1.2, from interface
'GigabitEthernet0/0/0' (10.2.2.1).
*Jan 31 11:44:33.424: NTP message received from 10.1.1.2 on interface
'GigabitEthernet0/0/0' (10.2.2.1).
*Jan 31 11:44:33.424: NTP Core(DEBUG): ntp_receive: message received
*Jan 31 11:44:33.424: NTP Core(DEBUG): ntp_receive: peer is 0x80007FA135BB32F8,
next action is 1.
*Jan 31 11:44:33.424: NTP Core(DEBUG): Peer becomes reachable, poll set to 6.

*Jan 31 11:44:33.424: NTP Core(INFO): 10.1.1.2 8034 84 reachable
*Jan 31 11:44:33.425: NTP Core(INFO): 10.1.1.2 964A 8A sys_peer
```

f. Issue the **undebug all** or the **no debug ntp all** command to turn off debugging.

```
R1# undebug all
```

g. Verify that R1 has made an association with R2 with the **show ntp associations** command. You can also use the more verbose version of the command by adding the **detail** argument. It might take some time for the NTP association to form.

```
R1# show ntp associations

address     ref clock    st  when  poll reach  delay  offset   disp
~10.1.1.2  127.127.1.1   3    14    64     3  0.000  -280073  3939.7
*sys.peer, # selected, +candidate, -outlyer, x falseticker, ~ configured
```

h. Verify the time on R1 after it has made an association with R2.

```
R1# show clock
*11:49:27.709 UTC Sun Jan 31 2021
```

i. Repeat the NTP configurations to configure R3 as an NTP client.

Part 4: Configure syslog Support on R1 and PC-A.

Step 1: Install and start the syslog server.

Free or trial versions of syslog server can be downloaded from the Internet. Use a web browser to search for “free windows syslog server” and refer to the software documentation for more information. Your instructor may also recommend a suitable syslog server for classroom use.

If a syslog server is not currently installed on the host, download a syslog server and install it on PC-A. If it is already installed, go to the next step.

Step 2: Configure R1 to log messages to the syslog server using the CLI.

a. Start the syslog server.

b. Verify that you have connectivity between R1 and PC-A by pinging the R1 G0/0/1 interface IP address 192.168.1.1. If it is not successful, troubleshoot as necessary before continuing.

c. NTP was configured in a previous part to synchronize the time on the network. Displaying the correct time and date in syslog messages is vital when using syslog to monitor a network. If the correct time and date of a message is not known, it can be difficult to determine what network event caused the message.

   Verify that the timestamp service for logging is enabled on the router using the **show run** command. Use the following command if the timestamp service is not enabled.

```
R1(config)# service timestamps log datetime msec
```

d. Configure the syslog service on the router to send syslog messages to the syslog server.

```
R1(config)# logging host 192.168.1.3
```

Step 3: Configure the logging severity level on R1.

Logging traps can be set to support the logging function. A trap is a threshold that when reached, triggers a log message. The level of logging messages can be adjusted to allow the administrator to determine what kinds of messages are sent to the syslog server. Routers support different levels of logging. The eight levels range from 0 (emergencies), indicating that the system is unstable, to 7 (debugging), which sends messages that include router information.

Note: The default level for syslog is 6, informational logging. The default for console and monitor logging is 7, debugging.

a. Use the **logging trap** command to determine the options for the command and the various trap levels available.

```
R1(config)# logging trap ?
<0-7>          Logging severity level
alerts         Immediate action needed           (severity=1)
critical       Critical conditions               (severity=2)
debugging      Debugging messages                (severity=7)
emergencies    System is unusable                (severity=0)
errors         Error conditions                  (severity=3)
informational  Informational messages            (severity=6)
notifications  Normal but significant conditions (severity=5)
warnings       Warning conditions                (severity=4)
<cr>
```

b. Define the level of severity for messages sent to the syslog server. To configure the severity levels, use either the keyword or the severity level number (0–7).

Severity Level	Keyword	Meaning
0	emergencies	System is unusable
1	alerts	Immediate action required
2	critical	Critical conditions
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant condition
6	informational	Informational messages
7	debugging	Debugging messages

Note: The severity level includes the level specified and anything with a lower severity number. For example, if you set the level to 4, or use the keyword **warnings**, you capture messages with severity level 4, 3, 2, 1, and 0.

c. Use the **logging trap** command to set the severity level for R1.

```
R1(config)# logging trap warnings
```

What is the problem with setting the level of severity too high or too low?

If the command **logging trap critical** were issued, which severity levels of messages would be logged?

Step 4: Display the current status of logging for R1.

a. Use the **show logging** command to see the type and level of logging enabled.

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0
flushes, 0 overruns, xml disabled, filtering disabled)


No Active Message Discriminator.




No Inactive Message Discriminator.



    Console logging: level debugging, 72 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 72 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level warnings, 54 message lines logged
        Logging to 192.168.1.3  (udp port 514, audit disabled,
              link up),
              3 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging Source-Interface:       VRF Name:
<output omitted>
```

At what level is console logging enabled?

At what level is trap logging enabled?

What is the IP address of the syslog server?

What port is syslog using?

Step 5: Make changes to the router and monitor syslog results on the PC.

a. Verify that the syslog server is already started on PC-A. Start the server as necessary.

b. To verify that syslog server is logging the message, disable and enable R1's G0/0/0 interface.

```
R1(config)# interface g0/0/0
R1(config-if)# shut
.Jan 31 12:02:50.376: %LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed
state to administratively down
.Jan 31 12:02:51.376: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to down
R1(config-if)# no shut
.Jan 31 12:03:11.302: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.4
port 514 started - CLI initiated
.Jan 31 12:03:14.365: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed
state to up
.Jan 31 12:03:15.365: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to up
.Jan 31 12:03:59.894: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on
GigabitEthernet0/0/0 from LOADING to FULL, Loading Done
```

c. Navigate to PC-A to view the syslog messages.

Router Interface Summary Table

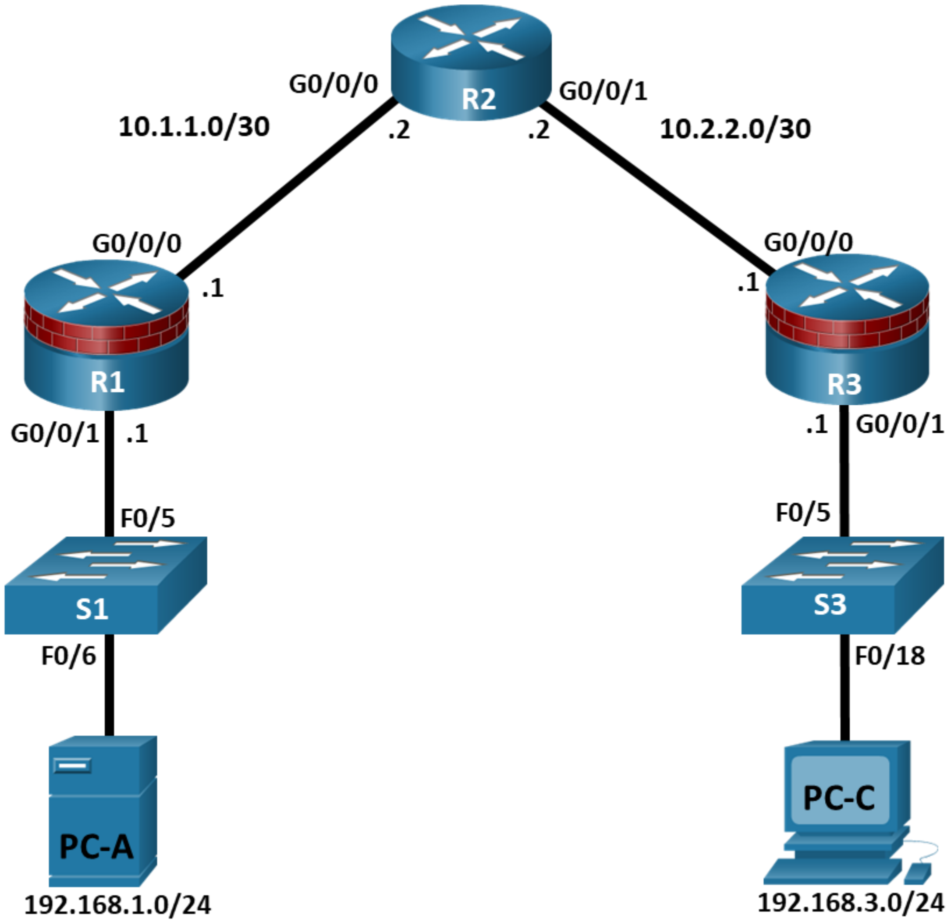
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

[Title]

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
R2	G0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	G0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objectives

Part 1: Configure Basic Device Settings

- Configure basic settings such as host name, interface IP addresses, and access passwords.
- Configure static routing.

Part 2: Configure Local Authentication for Console Access

- Configure a local database user and local access for the console line.
- Test the configuration.

Part 3: Configure Local Authentication for Remote Access

- Configure domain name
- Configure encryption key
- Enable SSH on vty

Part 4: Configure Local Authentication Using AAA on R3

- Configure the local user database using Cisco IOS.
- Configure AAA local authentication using Cisco IOS.
- Test the configuration.

Part 5: Observe AAA Authentication Using Cisco IOS Debug

Background / Scenario

The most basic form of router access security is to create passwords for the console, vty, and aux lines. A user is prompted for only a password when accessing the router. Configuring a privileged EXEC mode enable secret password further improves security, but still only a basic password is required for each mode of access.

In addition to basic passwords, specific usernames or accounts with varying privilege levels can be defined in the local router database that can apply to the router as a whole. When the console, vty, or aux lines are configured to refer to this local database, the user is prompted for a username and a password when using any of these lines to access the router.

Additional control over the login process can be achieved using authentication, authorization, and accounting (AAA). For basic authentication, AAA can be configured to access the local database for user logins, and fallback procedures can also be defined. However, this approach is not very scalable because it must be configured on every router. When a user attempts to log in, the router references the external server database to verify that the user is logging in with a valid username and password.

In this lab, you build a multi-router network and configure the routers and hosts. You will then use CLI commands to configure routers with basic local authentication by means of AAA.

Note: The routers used with hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.6 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960+ with Cisco IOS Release 15.2(7) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Before you begin, ensure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 2 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 2 PCs (Windows OS with a terminal emulation program, such as PuTTY or Tera Term installed)
- Console cables to configure Cisco networking devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Device Settings

In this part of the lab, you set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

All steps should be performed on routers R1 and R3. Only steps 1, 2, 3 and 6 need to be performed on R2. The procedure for R1 is shown here as an example.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and then cable as necessary.

Step 2: Configure basic settings for each router.

a. Configure host names as shown in the topology.

b. Configure the interface IP addresses as shown in the IP addressing table.

c. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup.

```
R1(config)# no ip domain-lookup
```

Step 3: Configure static routing on the routers.

a. Configure a static default route from R1 to R2 and from R3 to R2.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

```
R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

b. Configure a static route from R2 to the R1 LAN and from R2 to the R3 LAN.

```
R2(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1
R2(config)# ip route 192.168.3.0 255.255.255.0 10.2.2.1
```

Step 4: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C, as shown in the IP addressing table.

Step 5: Verify connectivity between PC-A and R3.

a. Ping from R1 to R3.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C, you have demonstrated that static routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to help identify routing protocol-related problems.

Step 6: Save the basic running configuration for each router.

Step 7: Configure and encrypt passwords on R1 and R3.

Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

For this step, configure the same settings for R1 and R3. Router R1 is shown here as an example.

a. Configure a minimum password length.

Use the **security passwords** command to set a minimum password length of 10 characters.

```
R1(config)# security passwords min-length 10
```

b. Configure a password for the privileged EXEC mode on both routers. Use the type 8 (PDKDF2) hashing algorithm.

```
R1(config)# enable algorithm-type sha256 secret cisco12345
```

Step 8: Configure the basic console, auxiliary port, and vty lines.

a. Configure a console password and enable login for router R1. For additional security, the **exec-timeout** command causes the line to log out after **5** minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the exec timeout can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

```
R1(config)# line console 0
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```

b. Configure a password for the aux port for router R1.

```
R1(config)# line aux 0
R1(config-line)# password ciscoauxpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

c. Configure the password on the vty lines for router R1.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

d. Encrypt the console, aux, and vty passwords.

```
R1(config)# service password-encryption
```

e. Issue the **show run | section line** command.

Can you read the console, aux, and vty passwords? Explain.

Step 9: Configure a login warning banner on routers R1 and R3.

a. Configure a warning to unauthorized users using a message-of-the-day (MOTD) banner with the **banner motd** command. When a user connects to the router, the MOTD banner appears before the login prompt. In this example, the dollar sign ($) is used to start and end the message.

```
R1(config)# banner motd $Unauthorized access strictly prohibited!$
R1(config)# exit
```

b. Exit privileged EXEC mode by using the **disable** or **exit** command and press **Enter** to get started.

If the banner does not appear correctly, re-create it using the **banner motd** command.

Step 10: Save the basic configurations on all routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1# copy running-config startup-config
```

Part 2: Configure Local Authentication for Console Access

In this part of lab, you configure a local username and password and change the access for the console, aux, and vty lines to reference the router's local database for valid usernames and passwords. Perform all steps on R1 and R3. The procedure for R1 is shown here.

Step 1: Configure the local user database.

a. Create a local user account using the type 8 (PDKDF2) hashing algorithm to encrypt the password.

```
R1(config)# username user01 algorithm-type sha256 secret user01pass
```

b. Exit global configuration mode and display the running configuration.

Can you read the user's password?

Step 2: Configure local authentication for the console line and login.

a. Set the console line to use the locally defined login usernames and passwords.

```
R1(config)# line console 0
R1(config-line)# login local
```

b. Exit to the initial router screen that displays:

```
R1 con0 is now available.

Press RETURN to get started.
```

c. Log in using the **user01** account and password previously defined.

What is the difference between logging in at the console now and previously?

d. After logging in, issue the **show run** command.

Were you able to issue the command? Explain.

e. Enter privileged EXEC mode using the **enable** command.

Were you prompted for a password? Explain.

Part 3: Configure Local Authentication for Remote Access

In this part, you will use SSH for remote access to R1 using local user database.

Step 1: Configure a domain name for the device.

Step 2: Configure the encryption key method.

Step 3: Enable SSH on the vty lines.

a. Enable SSH on the inbound vty lines using the **transport input** command.

b. Change the login method to use the local database for user verification.

c. From PC-A, establish an SSH session with R1.

Were you prompted for a user account? Explain.

d. While connected to R1 via SSH, access privileged EXEC mode with the **enable** command.

What password did you use?

e. For added security, set the aux port to use the locally defined login accounts.

```
R1(config)# line aux 0
R1(config-line)# login local
```

Step 4: Save the configuration on R1.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1# copy running-config startup-config
```

Step 5: Perform steps 1 through 4 on R3 and save the configuration.

Part 4: Configure Local Authentication Using AAA on R3

Step 1: Configure the local user database.

a. Create a local user account with PDKDF2 hashing to encrypt the password.

```
R3(config)# username Admin01 privilege 15 algorithm-type sha256 secret
Admin01pass
```

b. Exit global configuration mode and display the running configuration.

Can you read the user’s password?

Step 2: Enable AAA services.

On R3, enable services with the global configuration **aaa new-model** command. Because you are implementing local authentication, use local authentication as the first method, and no authentication as the secondary method.

If you were using an authentication method with a remote server, such as TACACS+ or RADIUS, you would configure a secondary authentication method for fallback if the server is unreachable. Normally, the secondary method is the local database. In this case, if no usernames are configured in the local database, the router allows all users login access to the device.

```
R3(config)# aaa new-model
```

Step 3: Implement AAA services for console access using the local database.

a. Create the default login authentication list by issuing the **aaa authentication login default** *method1[method2][method3]* command with a method list using the **local** and **none** keywords.

```
R3(config)# aaa authentication login default local-case none
```

Note: If you do not set up a default login authentication list, you could get locked out of the router and be forced to use the password recovery procedure for your specific router.

Note: The **local-case** parameter is used to make usernames case-sensitive.

b. Exit to the initial router screen that displays:

```
R3 con0 is now available


Press RETURN to get started.
```

Log in to the console as **Admin01** with a password of **Admin01pass**. Remember that usernames and passwords are both case-sensitive now.

Were you able to log in? Explain.

Note: If your session with the console port of the router times out, you might have to log in using the default authentication list.

c. Exit to the initial router screen that displays:

d. Attempt to log in to the console as **baduser** with any password.

Were you able to log in? Explain.

If no user accounts are configured in the local database, which users are permitted to access the device?

Step 4: Create an AAA authentication profile for SSH using the local database.

a. Create a unique authentication list for SSH access to the router. This does not have the fallback of no authentication, so if there are no usernames in the local database, SSH access is disabled. To create an authentication profile that is not the default, specify a list name of SSH_LINES and apply it to the vty lines.

```
R3(config)# aaa authentication login SSH_LINES local
R3(config)# line vty 0 4
R3(config-line)# login authentication SSH_LINES
```

b. Verify that this authentication profile is used by opening an SSH session from PC-C to R3. Log in as **Admin01** with a password of **Admin01pass**.

Were you able to login? Explain.

c. Exit the SSH session.

d. Attempt to log in as **baduser** with any password.

Were you able to login? Explain.

Part 5: Observe AAA Authentication Using Cisco IOS Debug

In this part, you use the **debug** command to observe successful and unsuccessful authentication attempts.

Step 1: Verify that the system clock and debug time stamps are configured correctly.

a. From the R3 user or privileged EXEC mode prompt, use the **show clock** command to determine what the current time is for the router. If the time and date are incorrect, set the time from privileged EXEC mode with the command **clock set HH:MM:SS DD month YYYY.** An example is provided here for R3.

```
R3# clock set 14:15:00 03 February 2021
```

b. Verify that detailed time-stamp information is available for your debug output using the **show run** command. This command displays all lines in the running config that include the text “timestamps”.

```
R3# show run | include timestamps
service timestamps debug datetime msec
service timestamps log datetime msec
```

c. If the **service timestamps debug** command is not present, enter it in global config mode.

```
R3(config)# service timestamps debug datetime msec
R3(config)# exit
```

d. Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R3# copy running-config startup-config
```

Step 2: Use debug to verify user access.

a. Activate debugging for AAA authentication.

```
R3# debug aaa authentication
AAA Authentication debugging is on
```

b. Start an SSH session from R2 to R3. Log in with username **Admin01** and password **Admin01pass**.

```
R2# ssh -l Admin01 10.2.2.1
```

c. Navigate back R3. Observe the AAA authentication events in the console session window. Debug messages similar to the following should be displayed.

```
R3#
Feb  3 14:15:57.653: AAA/BIND(00000FB5): Bind i/f
Feb  3 14:15:57.653: AAA/AUTHEN/LOGIN (00000FB5): Pick method list 'SSH_LINES'
R3#
Feb  3 14:16:01.966: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Admin01]
[Source: 10.2.2.2] [localport: 22] at 14:16:01 UTC Wed Feb 3 2021
```

d. From the SSH window on R2, enter privileged EXEC mode. Use the enable secret password of **cisco12345**. Debug messages similar to the following should be displayed. In the third entry, note the username (Admin01), virtual port number (tty866), and remote SSH client address (10.2.2.2). Also note that the last status entry is “PASS.”

```
Feb  3 14:19:51.146: AAA: parse name=tty866 idb type=-1 tty=-1
Feb  3 14:19:51.146: AAA: name=tty866 flags=0x11 type=5 shelf=0 slot=0
adapter=0 port=866 channel=0
Feb  3 14:19:51.146: AAA/MEMORY: create_user (0x7FD084CE0FF0) user='Admin01'
ruser='NULL' ds0=0 port='tty866' rem_addr='10.2.2.2' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0', vrf= (id=0)
Feb  3 14:19:51.146: AAA/AUTHEN/START (402765494): port='tty866' list=''
action=LOGIN service=ENABLE
Feb  3 14:19:51.146: AAA/AUTHEN/START (402765494): non-console enable - default
to enable password
Feb  3 14:19:51.147: AAA/AUTHEN/START (402765494): Method=ENABLE
R3#
Feb  3 14:19:51.147: AAA/AUTHEN (402765494): status = GETPASS
R3#
Feb  3 14:19:54.156: AAA/AUTHEN/CONT (402765494): continue_login
(user='(undef)')
Feb  3 14:19:54.156: AAA/AUTHEN (402765494): status = GETPASS
Feb  3 14:19:54.156: AAA/AUTHEN/CONT (402765494): Method=ENABLE
Feb  3 14:19:54.259: AAA/AUTHEN (402765494): status = PASS
Feb  3 14:19:54.259: AAA/MEMORY: free_user (0x7FD084CE0FF0) user='NULL'
ruser='NULL' port='tty866' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE
priv=15 vrf= (id=0)
```

e. From the SSH window, exit privileged EXEC mode using the **disable** command. Try to enter privileged EXEC mode again, but use a bad password this time. Observe the debug output on R3, noting that the status is “FAIL” this time.

```
Feb  3 14:24:20.274: AAA: parse name=tty866 idb type=-1 tty=-1
Feb  3 14:24:20.274: AAA: name=tty866 flags=0x11 type=5 shelf=0 slot=0
adapter=0 port=866 channel=0
Feb  3 14:24:20.274: AAA/MEMORY: create_user (0x7FD08991D130) user='Admin01'
ruser='NULL' ds0=0 port='tty866' rem_addr='10.2.2.2' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0', vrf= (id=0)
Feb  3 14:24:20.274: AAA/AUTHEN/START (1943266075): port='tty866' list=''
action=LOGIN service=ENABLE
Feb  3 14:24:20.274: AAA/AUTHEN/START (1943266075): non-console enable -
default to enable password
Feb  3 14:24:20.274: AAA/AUTHEN/START (1943266075): Method=ENABLE
R3#
Feb  3 14:24:20.275: AAA/AUTHEN (1943266075): status = GETPASS
R3#
Feb  3 14:24:22.276: AAA/AUTHEN/CONT (1943266075): continue_login
(user='(undef)')
Feb  3 14:24:22.276: AAA/AUTHEN (1943266075): status = GETPASS
Feb  3 14:24:22.276: AAA/AUTHEN/CONT (1943266075): Method=ENABLE
Feb  3 14:24:22.379: AAA/AUTHEN(1943266075): password incorrect
Feb  3 14:24:22.379: AAA/AUTHEN (1943266075): status = FAIL
Feb  3 14:24:22.379: AAA/MEMORY: free_user (0x7FD08991D130) user='NULL'
ruser='NULL' port='tty866' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE
priv=15 vrf= (id=0)
R3#
```

f. Exit the SSH session to the router R3. Then try to open an SSH session to the router again, but this time try to log in with the username **Admin01** and a bad password. From the console window, the debug output should look similar to the following.

```
Feb  3 14:26:40.960: AAA/BIND(00000FB9): Bind i/f
Feb  3 14:26:40.960: AAA/AUTHEN/LOGIN (00000FB9): Pick method list 'SSH_LINES'
```

What message was displayed on the SSH client screen?

g. Turn off all debugging using the **undebug all** command at the privileged EXEC prompt.

Reflection

1. Why would an organization want to use a centralized authentication server rather than configuring users and passwords on each individual router?

2. Contrast local authentication and local authentication with AAA.

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

[Title]

Objectives

Part 1: Prepare a Personal Computer for Virtualization

Part 2: Import a Virtual Machine into VirtualBox Inventory

Background / Scenario

Computing power and resources have increased tremendously over the last 10 years. A benefit of having multicore processors and large amounts of RAM is the ability to use virtualization. With virtualization, one or more virtual computers operate inside one physical computer. Virtual computers that run within physical computers are called virtual machines. Virtual machines are often called guests, and physical computers are often called hosts. Anyone with a modern computer and operating system can run virtual machines.

A virtual machine image file has been created for you to install on your computer. In this lab, you will download and import this image file into a desktop virtualization application, such as VirtualBox. When opened in the player software, this fille will permit you to run a Linux guest computer that can be accessed directly from your host operating system.

This virutal machine will be used later in the course.

Required Resources

- Host computer with a minimum of 8 GB of RAM and 20GB of free disk space
- High-speed internet access to download Oracle VirtualBox and the virtual machine image file

Instructions

Part 1: Prepare a Host Computer for Virtualization

In Part 1, you will download and install desktop virtualization software, and also download an image file that can be used to complete several of the labs throughout the course. For this lab, the virtual machine is running a Linux OS.

Step 1: Download and install VirtualBox.

VMware Player and Oracle VirtualBox are two virtualization programs that you can download and install to support the image file. In this lab, you will use VirtualBox.

a. Navigate to http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html.

b. Choose and download the appropriate installation file for your operating system.

c. When you have downloaded the VirtualBox installation file, run the installer and accept the default installation settings.

Step 2: Download the Virtual Machine image file.

The image file was created in accordance with the Open Virtualization Format (OVF). OVF is an open standard for packaging and distributing virtual appliances. An OVF package has several files placed into one directory. This directory is then distributed as an OVA package. This package contains all the OVF files necessary for the deployment of the virtual machine. The virtual machine used in this lab was exported in accordance with the OVF standard.

a. Navigate to the Network Security Virtual Machine (VM) page on netacad.com.

b. Download the **security_workstation.ova** image file and note the location of the downloaded VM file.

Note: Your browser may ask if you wish to open the file with the VirtualBox program. Select **Save** instead to follow the instructions in Part 2.

Part 2: Import the Virtual Machine into the VirtualBox Inventory

In Part 2, you will import the virtual machine image into VirtualBox and start the virtual machine.

Step 1: Import the virtual machine file into VirtualBox.

a. Open **VirtualBox**. Click **File > Import Appliance...** to import the virtual machine image.

b. In the Appliance to import window, specify the location of the .OVA file and click **Next**.

c. The Appliance window presents the settings suggested in the OVA archive. Review the default settings and change if necessary. Normally, the default settings are appropriate. Click **Import** to continue.

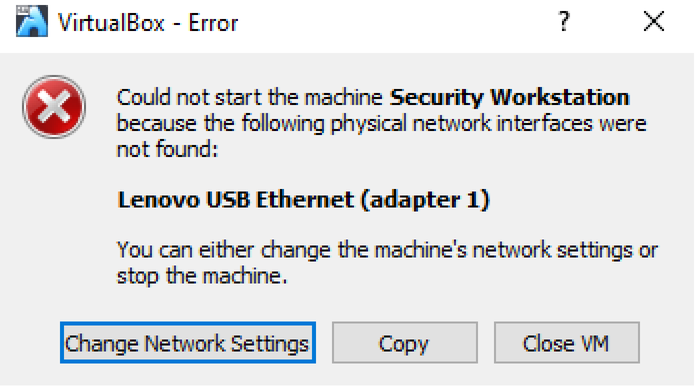
d. When the import process is complete, you will see the new Virtual Machine added to the VirtualBox inventory in the left panel. The virtual machine is now ready to use.

Step 2: Start the virtual machine and log in.

a. Click the Security Workstation virtual machine.

b. Click the green arrow **Start** button at the top portion of the VirtualBox application window. If you get the following error dialog box, click **Change Network Settings** and set your Bridged Adapter.

Click the dropdown list next to the Name and choose your network adapter (this will vary for each computer).



VirtualBox - Error

Could not start the machine **Security Workstation** because the following physical network interfaces were not found:

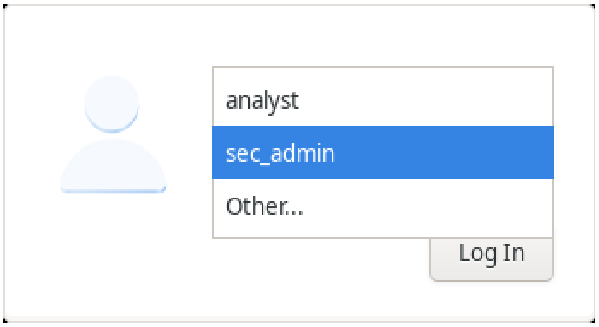
Lenovo USB Ethernet (adapter 1)

You can either change the machine's network settings or stop the machine.

Note: If your network is not configured with DHCP services, click **Change Network Settings** and select **NAT** in the **Attached to** dropdown box. The network settings can also be accessed via **Settings** in the Oracle VirtualBox Manager or in the virtual machine menu by selecting **Devices** > **Network** > **Network Settings**. You may need to disable and enable the network adaptor for the change to take effect.

c. Click **OK**. A new window will appear and the virtual machine boot process will start.

d. When the boot process is complete, the virtual machine will ask for a username and password. Select **sec_admin** in the drop-down menu.



Use the following credentials to log in to the virtual machine:

Username: **sec_admin**

Password: **net_secPW**

You will be presented with a desktop environment with a launcher bar at the bottom, icons on the desktop, and an application menu at the top.

Note: Notice the keyboard and mouse focus. When you click inside the virtual machine window, your mouse and keyboard will operate the guest operating system. Your host operating system will no longer detect keystrokes or mouse movements. Move your mouse outside of the VirtualBox window to control your host operating system. If you are unable to move the mouse out of the VirtualBox window, press the **right CTRL** key to return keyboard and mouse focus to the host operating system.

Step 3: Familiarize yourself with the Virtual Machine.

The virtual machine that you just installed will be used to complete several of the labs in this course. Familiarize yourself with the icons in the list below:

The launcher bar icons are (from left to right):

- Show the desktop
- Terminal emulator
- File manager application
- Web browser application (Firefox)
- File search tool
- Current user's home directory

a. Open the **Terminal Emulator** application. Type **ip address** at the prompt to determine the IP address of your virtual machine.

```
[sec_admin@Workstation ~]$ ip address
```

What are the IP addresses assigned to your virtual machine?

b. Locate and launch the web browser application.

Can you navigate to your favorite search engine?

Step 4: Run scripts.

In this step, you will run two scripts that were created for this course. A script is a plain text file that contains a set of commands that execute when the script filename is entered at the terminal prompt.

a. Open a terminal using the **Terminal Emulator** application.

b. Navigate to the scripts folder.

```
[sec_admin@Workstation ~]$ cd lab.support.files/scripts/
[sec_admin@Workstation scripts]$
```

c. You can list the files in the folder by entering **ls** at the promp.t

```
[sec_admin@Workstation scripts]$ ls
configure_as_dhcp.sh  configure_as_static.sh  net_configuration_files
```

d. To run a script that changes the IP address to a static IP address of 192.168.1.11, enter **./configure_as_static.sh**. Enter **net_secPW** as the password when prompted.

```
[sec_admin@Workstation scripts]$ ./configure_as_static.sh
[sudo] password for sec_admin:
Configuring the NIC as:
IP: 192.168.1.11/24
GW: 192.168.1.1

IP Configuration successful.
```

e. Verify the static IP address by typing **ip address** at the terminal prompt.

```
[sec_admin@Workstation scripts]$ ip address
<output omitted>
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:8a:4b:dd brd ff:ff:ff:ff:ff:ff
    inet 192.168.192.183/24 brd 192.168.192.255 scope global dynamic eth0
       valid_lft 1774sec preferred_lft 1774sec
    inet6 fe80::a00:27ff:fe8a:4bdd/64 scope link
       valid_lft forever preferred_lft forever
```

f. To return to using DHCP to get an IP address, enter **./configure_as_dhpc.sh** at the prompt.

```
[sec_admin@Workstation scripts]$ ./configure_as_dhcp.sh
[sudo] password for sec_admin:
Configuring the NIC to request IP info via DHCP...
Requesting IP information...
IP Configuration successful.
```

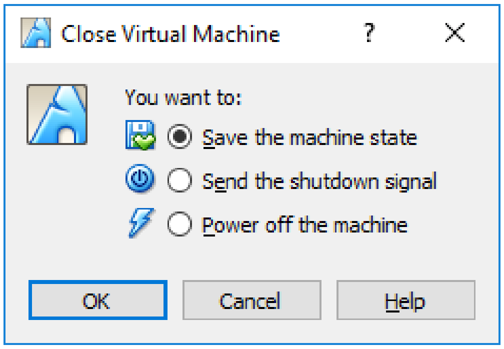
Step 5: Shut down the VM.

When you are done with the VM, you can save the state of the VM for future use or shut down the VM.

Closing the VM using GUI:

From the VirtualBox **File** menu, choose **Close...**

Click the **Save the machine state** radio button and click **OK**. The next time you start the virtual machine, you will be able to resume working in the operating system in its current state.



Close Virtual Machine

You want to:

● Save the machine state

○ Send the shutdown signal

○ Power off the machine

The other two options are:

Send the shutdown signal: simulates pressing the power button on a physical computer and selecting shut down

Power off the machine: simulates pulling the plug on a physical computer or holding down the power button until the computer turns off

Closing the VM using CLI:

To shut down the VM using the command line, you can use the menu options inside the VM or enter **sudo shutdown -h now** command in a terminal window and provide the password **net_secPW** when prompted.

Rebooting the VM:

If you want to reboot the VM, you can use the menu options inside the VM or enter **sudo reboot** command in a terminal and provide the password **net_secPW** when prompted.

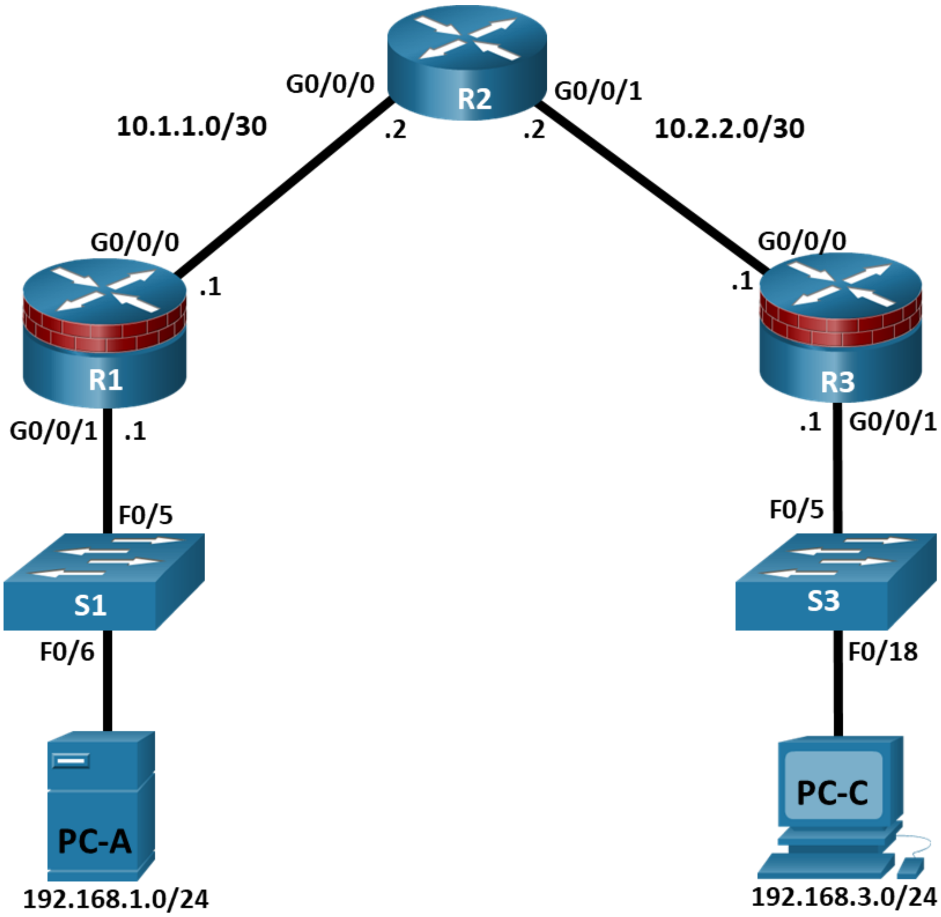
Note: You can use the web browser in this virtual machine to research security issues. By using the virtual machine, you may prevent malware from being installed on your host computer.

Reflection

What are the advantages and disadvantages of using a virtual machine?

[Title]

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
R2	G0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	G0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
RADIUS Server on PC-A	NIC	192.168.1.11	255.255.255.0	192.168.1.1	N/A
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure Centralized Authentication Using AAA and RADIUS

- Enable AAA.
- Configure the default login authentication list.
- Specify a RADIUS server.

Part 3: Configure Centralized Authentication Using AAA and RADIUS

- Test the AAA RADIUS configuration.
- Change the RADIUS port numbers

Background / Scenario

The most basic form of router access security is to create passwords for the console, vty, and aux lines. A user is prompted for only a password when accessing the router. Configuring a privileged EXEC mode secret password further improves security, but still only a basic password is required for each mode of access. Local databases with usernames with varying privilege levels can also be used and the users will be prompted for usernames and passwords to access the devices.

In addition to basic passwords and local authentication, additional control over the login process can be achieved using authentication, authorization, and accounting (AAA). For basic authentication, AAA can be configured to access the local database for user logins, and fallback procedures can also be defined. However, this approach is not very scalable because it must be configured on every router. To take full advantage of AAA and achieve maximum scalability, AAA is used in conjunction with an external TACACS+ or RADIUS server database. When a user attempts to log in, the router references the external server database to verify that the user is logging in with a valid username and password.

In this lab, you build a multi-router network and configure the routers and hosts. You will access RADIUS software on an external computer and use AAA to authenticate users with the RADIUS server.

Note: The routers used with hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.6 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960+ with Cisco IOS Release 15.2(7) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Before you begin, ensure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 2 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 2 PCs (Windows OS with a terminal emulation application and virtualization software, such as VirtualBox installed)
- 1 Security Workstation Virtual Machine with RADIUS server already installed
- Console cables to configure Cisco networking devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Device Settings

In this part, you set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

The initial router configurations are provided and the configurations for the switches are optional.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and then cable as necessary.

Step 2: Load the configurations.

In this step, you will copy and paste the configurations into each router.

Router R1

```
enable
config terminal
no ip domain lookup
enable algorithm-type sha256 secret cisco12345
username user01 algorithm-type sha256 secret user01pass
username admin privilege 15 algorithm-type sha256 secret cisco12345
ip domain-name netsec.com
host R1
interface GigabitEthernet0/0/0
 ip address 10.1.1.1 255.255.255.252
 no shutdown
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 no shutdown
router ospf 1
 passive-interface GigabitEthernet0/0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 10.1.1.2
line con 0
```

```
 login local
 logging synchronous
 exec-timeout 5 0
line aux 0
 login local
 exec-timeout 5 0
line vty 0 4
 login local
 exec-timeout 5 0
 transport input ssh
crypto key generate rsa general-key modulus 1024
end
```

Router R2

```
enable
config terminal
no ip domain lookup
host R2
enable algorithm-type sha256 secret cisco12345
username user01 algorithm-type sha256 secret user01pass
username admin privilege 15 algorithm-type sha256 secret cisco12345
ip domain-name netsec.com
interface GigabitEthernet0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
interface GigabitEthernet0/0/1
ip address 10.2.2.2 255.255.255.252
 no shutdown
router ospf 1
 passive-interface GigabitEthernet0/0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
ip route 192.168.1.0 255.255.255.0 10.1.1.1
ip route 192.168.3.0 255.255.255.0 10.2.2.1
line con 0
 login local
 logging synchronous
 exec-timeout 5 0
line aux 0
 login local
 exec-timeout 5 0
line vty 0 4
 login local
 exec-timeout 5 0
 transport input ssh
crypto key generate rsa general-key modulus 1024
```

```
end
```

Router R3

```
enable
config terminal
no ip domain lookup
enable algorithm-type sha256 secret cisco12345
username user01 algorithm-type sha256 secret user01pass
username admin privilege 15 algorithm-type sha256 secret cisco12345
ip domain-name netsec.com
host R3
interface GigabitEthernet0/0/0
 ip address 10.2.2.1 255.255.255.252
 no shutdown
interface GigabitEthernet0/0/1
 ip address 192.168.3.1 255.255.255.0
 no shutdown
router ospf 1
 passive-interface GigabitEthernet0/0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 10.2.2.2
line con 0
 login local
 logging synchronous
 exec-timeout 5 0
line aux 0
 login local
 exec-timeout 5 0
line vty 0 4
 login local
 exec-timeout 5 0
 transport input ssh
crypto key generate rsa general-key modulus 1024
end
```

Step 3: Configure the PCs.

PC-A will function as the RADIUS server for this lab. A virtual machine with a RADIUS server is setup for use in this course. You can deploy the virtual machine on PC-A by following **Lab - Installing the Virtual Machine** if you have not done so already. You may choose to download, install, and configure a RADIUS server for your use if desired.

a. Assign the IP address and default gateway on PC-C according to the Addressing Table.

b. If you have not already deployed the virtual machine **Security Workstation VM**, please go back to **Lab - Installing the Virtual Machine**.

c. Start VirtualBox and verify that the Security Workstation is using the Bridged Adapter in the Network Settings.

d. Start the Security Workstation VM. Log into the VM as **sec_admin** with the password **net_secPW**. Select the user **sec_admin** from the dropdown list if necessary.

e. From the menu bar at the bottom of the Desktop, click **Terminal Emulator**.

f. Within the terminal emulator window, you will configure this virtual machine with an IP address of 192.168.1.11 by running a script. When prompted for a password, use the password **net_secPW**.

```
[sec_admin@Workstation ~]$ cd ~/lab.support.files/scripts/
[sec_admin@Workstation scripts]$ ./configure_as_static.sh
[sudo] password for sec_admin:
Configuing the NIC as:
IP: 192.168.1.11/24
GW: 192.168.1.1

IP Configuration successful.
```

g. Enter **ip addr** at the prompt to verify the assigned static IP address on Security Workstation VM.

```
[sec_admin@Workstation scripts]$ ip addr
<output omitted>
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 00:50:56:9c:c5:37 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.11/24 brd 192.168.1.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe9c:5248/64 scope link
       valid_lft forever preferred_lft forever
```

h. Ping the gateway IP address (R1's G0/0/0, 192.168.1.1) from Security Workstation VM.

```
[sec_admin@Workstation scripts]$ ping -c 4 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.605 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.661 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.654 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.641 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3042ms
rtt min/avg/max/mdev = 0.605/0.640/0.661/0.021 ms
```

Step 4: Verify connectivity.

a. Test connectivity by pinging from Security Workstation VM to PC-C. If the pings are not successful, troubleshoot the router and PC configurations until they are.

b. From Security Workstation VM terminal, establish an SSH session with R1 using the username **user01** and password **user01pass**. Enter **yes** when prompted if you are sure you want to continue connecting.

```
[sec_admin@Workstation scripts]$ ssh -l user01 192.168.1.1
```

c. Exit the SSH session when finished. Establish another SSH with R1 using the username **admin** and password **cisco12345**.

d. Exit the SSH session when finished. Now you have verified end-to-end connectivity and Security Workstation VM can communicate with router R1.

Part 2: Configure Centralized Authentication Using AAA and RADIUS

In this part, you will configure R1 to use AAA services to authenticate users. The RADIUS server is already configured with one user **RadUser** with the password **RadUserpass** and the secret shared key **$trongKey**.

Step 1: Enable AAA on R1.

Open a console on R1 and use the **aaa new-model** command in global configuration mode to enable AAA.

```
R1(config)# aaa new-model
```

Step 2: Configure the default login authentication list.

Configure the list to first use RADIUS for the authentication service, and then the fallback, **none**. If no RADIUS server can be reached and authentication cannot be performed, the router globally allows access without authentication. This is a safeguard measure in case the router starts up without connectivity to an active RADIUS server.

```
R1(config)# aaa authentication login default group radius none
```

Note: You could alternatively configure local authentication as the backup authentication method.

Note: If you do not set up a default login authentication list, you could get locked out of the router and need to use the password recovery procedure for your specific router.

Step 3: Specify a RADIUS server.

a. Use the **radius server** command to enter RADIUS server configuration mode.

```
R1(config)# radius server NetSec
```

b. Use the **?** to view the sub-mode commands available for configuring a RADIUS server.

```
R1(config-radius-server)# ?
RADIUS server sub-mode commands:
  address          Specify the radius server address
  automate-tester  Configure server automated testing.
  backoff          Retry backoff pattern(Default is retransmits with constant
                   delay)
  exit             Exit from RADIUS server configuration mode
  key              Per-server encryption key
  no               Negate a command or set its defaults
  non-standard     Attributes to be parsed that violate RADIUS standard
  pac              Protected Access Credential key
  retransmit       Number of retries to active server (overrides default)
  timeout          Time to wait (in seconds) for this radius server to reply
                   (overrides default)
```

c. Use the **address** command to configure the IP address of the RADIUS server.

```
R1(config-radius-server)# address ipv4 192.168.1.11
```

d. The **key** command is used for the secret password that is shared between the RADIUS server and the router (R1 in this case) and is used to authenticate the connection between the router and the server before the user authentication process takes place. Use the secret password of

$trongPass that has been configured on the Radius server. Remember that passwords are case-sensitive.

```
R1(config-radius-server)# key $trongPass
R1(config-radius-server)# end
```

Note: For the purposes of this lab, an unencrypted password is configured. In the future, IOS will require encrypted passwords.

Part 3: Test the AAA RADIUS Configuration.

Step 1: Start the RADIUS Server and verify operation.

a. At the Security Workstation terminal, start the RADIUS server by entering the **sudo systemctl start freeradius.service** command. Enter the password **net_secPW** as necessary.

```
[sec_admin@Workstation ~]$ sudo systemctl start freeradius.service
```

b. Verify that the server is running, enter the command **sudo systemctl status freeradius.service** at the terminal prompt.

```
[sec_admin@Workstation ~]$ sudo systemctl status freeradius.service
? freeradius.service - FreeRADIUS high performance RADIUS server.
     Loaded: loaded (/usr/lib/systemd/system/freeradius.service; disabled;
vendor preset: disabled)
     Active: active (running) since Sun 2021-02-14 22:14:07 EST; 18min ago
       Docs: man:radiusd(8)
             man:radiusd.conf(5)
             https://wiki.freeradius.org/Home
             https://networkradius.com/freeradius-documentation/
    Process: 890 ExecStartPre=/usr/bin/radiusd -C (code=exited,
status=0/SUCCESS)
    Process: 893 ExecStart=/usr/bin/radiusd -d /etc/raddb (code=exited,
status=0/SUCCESS)
   Main PID: 895 (radiusd)
      Tasks: 6 (limit: 1113)
     Memory: 77.5M
     CGroup: /system.slice/freeradius.service
             mq895 /usr/bin/radiusd -d /etc/raddb

Feb 14 22:14:07 Workstation systemd[1]: Starting FreeRADIUS high performance
RADIUS server....
Feb 14 22:14:07 Workstation systemd[1]: Started FreeRADIUS high performance
RADIUS server..
```

Step 2: Test your configuration.

You can test and verify your RADIUS server configurations on your router before exiting the router by using the **test aaa** command. The output message indicates that there is no authoritative response from the RADIUS sever.

```
R1# test aaa group radius RadUser RadUserpass legacy
Attempting authentication test to server-group radius using radius
No authoritative response from any server
```

You may also see messages similar to the following may display after the attempted tests indicating that the RADIUS server at 192.168.1.11 is not communicating with the router.

```
*Feb 15 02:30:26.504: %RADIUS-4-RADIUS_DEAD: RADIUS server
192.168.1.11:1645,1646 is not responding.
*Feb 15 02:30:26.504: %RADIUS-4-RADIUS_ALIVE: RADIUS server
192.168.1.11:1645,1646 is being marked alive.
```

Step 3: Troubleshoot router-to-RADIUS server communication.

The **show radius server-group radius** command indicates that the router is using UDP ports 1645 and 1646 for communications.

```
R1# show radius server-group radius
Server group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
    Server(192.168.1.11:1645,1646) Transactions:
    Authen: 32  Author: 0       Acct: 0
    Server_auto_test_enabled: FALSE
     Keywrap enabled: FALSE
```

RFC 2865 officially assigned port numbers 1812 and 1813 for RADIUS. This indicates that the router and RADIUS server are not communicating on the same ports.

Step 4: Change the RADIUS port numbers on R1 to match the RADIUS server.

Unless specified otherwise, the Cisco IOS RADIUS configuration defaults to UDP port numbers 1645 and 1646. Either the router Cisco IOS port numbers must be changed to match the port number of the RADIUS server or the RADIUS server port numbers must be changed to match the port numbers of the Cisco IOS router.

a. Re-issue the address sub-mode command again. This time specify port numbers **1812** and **1813**, along with the IPv4 address**.**

```
R1(config)# radius server NetSec
R1(config-radius-server)# address ipv4 192.168.1.11 auth-port 1812
acct-port 1813
```

b. Test the router to RADIUS server communications again by using the **test aaa** command.

```
R1# test aaa group radius RadUser RadUserpass legacy
Attempting authentication test to server-group radius using radius
User was successfully authenticated.
```

Step 5: Test your configuration by logging into the console on R1.

a. Exit to the initial router screen that displays: R1 con0 is now available, Press **RETURN** to get started.

b. Log in again with the username of **RadUser** and password of **RadUserpass**.

Were you able to login? Was there any delay this time?

c. Log in again using an invalid username of **Userxxx** and the password of **Userxxxpass**.

Were you able to login?

What message was displayed on the router?

d. Log in again using the local user credentials, **admin** / **cisco12345** or **user01** / **user01pass**.

Were you able to log in? Explain.

Type your answers here.

Step 6: Create an authentication method list for SSH and test it.

a. Log back into R1 as necessary.

b. Create a unique authentication method list for SSH access to the router. This does not have the fallback of no authentication, so if there is no access to the RADIUS server, SSH access is disabled. Name the authentication method list **SSH_LINES**.

```
R1(config)# aaa authentication login SSH_LINES group radius
```

c. Apply the list to the vty lines on the router using the **login authentication** command.

```
R1(config)# line vty 0 4
R1(config-line)# login authentication SSH_LINES
```

d. Establish an SSH session from PC-C to R1 (10.1.1.1) and log in with the username **RadUser** and the password of **RadUserpass**. Were you able to gain access to log in? Explain.

e. Establish an SSH session from PC-C to R1 again. Log in with the username **user01** and the password of **user01pass**. Were you able to log in? Explain.

Reflection

1. Why would an organization want to use a centralized authentication server rather than configuring users and passwords on each individual router?

2. Contrast local authentication and local authentication with AAA.

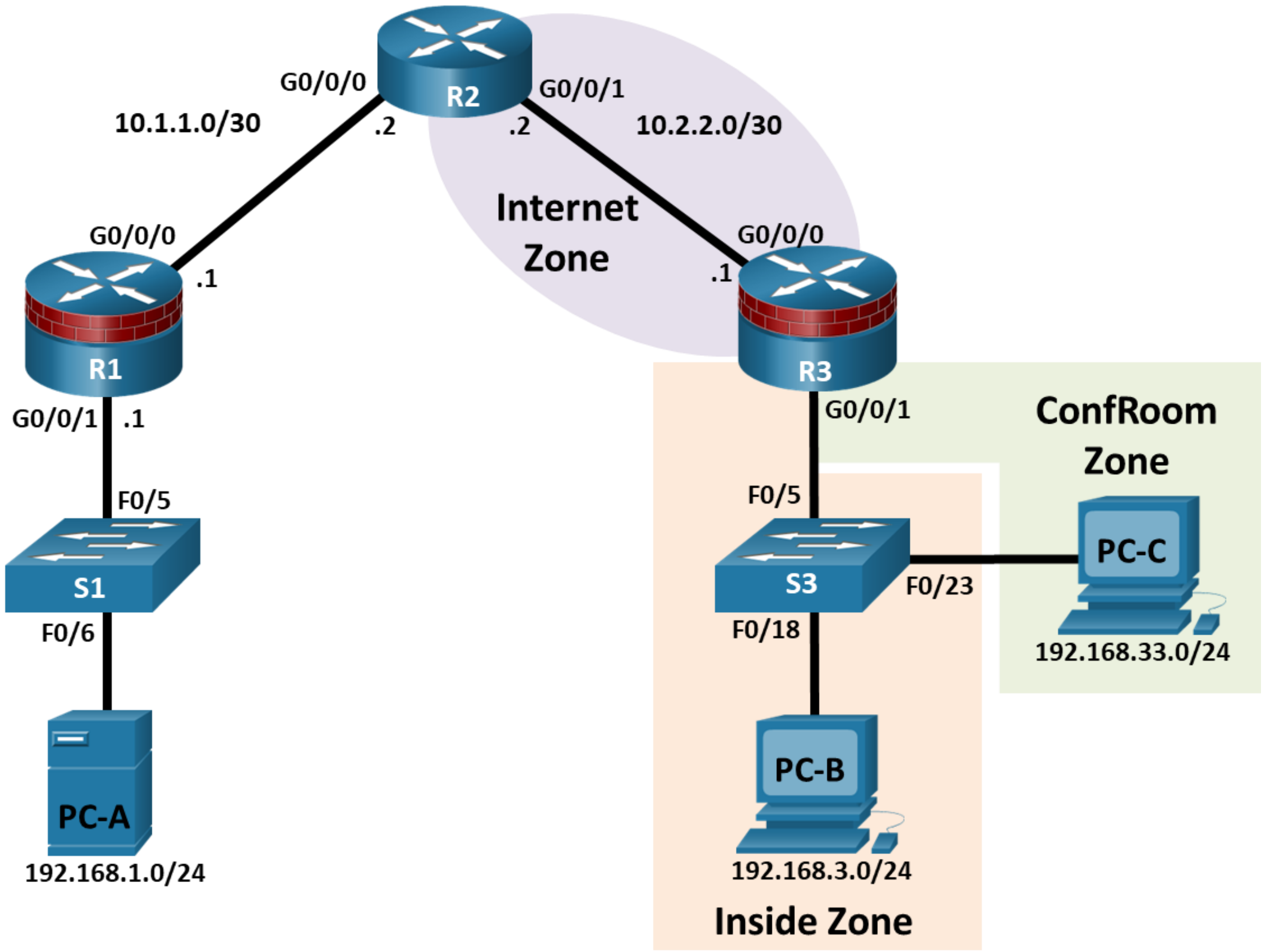
Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

[Title]

Topology



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
R2	G0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	G0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
	G0/0/1.3	192.168.3.1	255.255.255.0	N/A	S3 F0/5

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
	G0/0/1.33	192.168.33.1	255.255.255.0	N/A	S3 F0/5
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-B	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18
PC-C	NIC	192.168.33.3	255.255.255.0	192.168.33.1	S3 F0/23

Objectives

Part 1: Basic Device Configuration

- Configure host names, interface IP addresses, and access passwords on routers.
- Configure the static routes to enable end-to-end connectivity on routers.
- Configure access and trunk ports on a switch.

Part 2: Configuring a Zone-Based Policy Firewall (ZPF)

- Use the CLI to configure a Zone-Based Policy Firewall.
- Use the CLI to verify the configuration.

Part 3: Verify ZPF Firewall Functionality

Background

The most basic form of a Cisco IOS firewall uses access control lists (ACLs) to filter IP traffic and monitor established traffic patterns. A traditional Cisco IOS firewall is an ACL-based firewall.

The newer Cisco IOS Firewall implementation uses a zone-based approach that operates as a function of interfaces instead of access control lists. A Zone-Based Policy Firewall (ZPF) allows different inspection policies to be applied to multiple host groups connected to the same router interface. It can be configured for extremely advanced, protocol specific, granular control. It prohibits traffic via a default deny-all policy between different firewall zones. ZPF is suited for multiple interfaces that have similar or varying security requirements.

In this lab, you build a multi-router network, configure the routers and PC hosts, and configure a Zone-Based Policy Firewall using the Cisco IOS command line interface (CLI).

Note: The routers used with hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960+ with Cisco IOS Release 15.2(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 2 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 3 PCs (Windows OS with a terminal emulation program, such as Tera Term or PuTTy installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Instructions

Part 1: Basic Device Configuration

In this part of this lab, you set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

Note: All tasks should be performed on routers R1, R2, and R3. The procedures are shown for only one of the routers.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Disable DNS lookup.

To prevent the router from attempting to translate incorrectly entered commands, disable DNS lookup.

Step 3: Configure basic settings for each router.

a. Configure host names as shown in the topology.

b. Configure the interface IP addresses as shown in the IP addressing table. The IP address configuration for router R3 is provided below.

```
R3(config)# interface GigabitEthernet0/0/0
R3(config-if)# ip address 10.2.2.1 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# interface GigabitEthernet0/0/1
R3(config-if)# no shutdown
R3(config-if)# interface GigabitEthernet0/0/1.3
R3(config-if)# encapsulation dot1Q 3
R3(config-if)# ip address 192.168.3.1 255.255.255.0
R3(config-if)#interface GigabitEthernet0/0/1.33
R3(config-if)# encapsulation dot1Q 33
R3(config-if)# ip address 192.168.33.1 255.255.255.0
```

Step 4: Configure static routes on R1, R2, and R3.

a. To achieve end-to-end IP reachability, proper static routes must be configured on R1, R2 and R3. R1 and R3 are stub routers, and as such, only need a default route pointing to R2. R2, behaving as the ISP, must know how to reach R1's and R3's internal networks before end-to-end IP reachability is achieved. Below is the static route configuration for R1, R2 and R3. On R1, use the following command:

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

b. On R2, use the following commands.

```
R2(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1
R2(config)# ip route 192.168.3.0 255.255.255.0 10.2.2.1
R2(config)# ip route 192.168.33.0 255.255.255.0 10.2.2.1
```

c. On R3, use the following command.

```
R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

Step 5: Configure S3.

a. Configure trunk link:

```
S3(config)# interface f0/5
S3(config-if)# switchport mode trunk
```

b. Configure access ports.

```
S3(config)# interface f0/18
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 3
S3(config-if)# interface f0/23
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 33
```

Step 6: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A, PC-B, and PC-C as shown in the IP addressing table.

Step 7: Verify basic network connectivity.

a. Ping from R1 to R3.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-B and PC-C on the R3 LANs.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C, you have demonstrated that the end-to-end IP reachability has been achieved. If you cannot ping but the device interfaces are UP and IP addresses are correct, use the **show interface**, **show ip interface,** and **show ip route** commands to help identify problems.

Step 8: Configure a user account, encrypted passwords and crypto keys for SSH.

Note: Passwords in this task are set to a minimum of 10 characters, but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

a. Configure a minimum password length using the **security passwords** command to set a minimum password length of 10 characters.

```
R1(config)# security passwords min-length 10
```

b. Configure a domain name.

```
R1(config)# ip domain-name netsec.com
```

c. Configure crypto keys for SSH

```
R1(config)# crypto key generate rsa general-keys modulus 1024
```

d. Configure an admin01 user account using **algorithm-type scrypt** for encryption and a password of cisco12345.

```
R1(config)# username admin01 algorithm-type scrypt secret cisco12345
```

e. Configure line console 0 to use the local user database for logins. For additional security, the **exec-timeout** command causes the line to log out after **5** minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the **exec-timeout** command can be set to **0 0**, which prevents it from expiring; however, this is not considered to be a good security practice.

```
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
```

f. Configure line aux 0 to use the local user database for logins.

```
R1(config)# line aux 0
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
```

g. Configure line vty 0 4 to use the local user database for logins and restrict access to SSH connections only.

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exec-timeout 5 0
```

h. Configure the enable password with strong encryption.

```
R1(config)# enable algorithm-type scrypt secret class12345
```

Step 9: Save the basic running configuration for all three routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1# copy running-config startup-config
```

Part 2: Configuring a Zone-Based Policy Firewall (ZPF)

In this part, you will create a zone-based policy firewall on R3 using the command line interface (CLI), making it act not only as a router but also as a firewall. R3 is currently responsible for routing packets for the three networks connected to it. R3's interface roles are configured as follows:

G0/0/0 is connected to the Internet. Because this is a public network, it is considered an untrusted network and should have the lowest security level.

G0/0/1.3 is connected to the internal network. Only authorized users have access to this network. In addition, vital institution resources also reside in this network. The internal network is to be considered a trusted network and should have the highest security level.

G0/0/1.33 is connected to a conference room. The conference room is used to host meetings with people who are not part of the organization.

The security policy to be enforced by R3 when it is acting as a firewall dictates that:

- No traffic initiated from the Internet should be allowed into the internal or conference room networks.
- Returning Internet traffic (return packets coming from the Internet into the R3 site, in response to requests originating from any of the R3 networks) should be allowed.
- Computers in the R3 internal network are considered *trusted* and are allowed to initiate any type traffic (TCP, UDP or ICMP based traffic).
- Computers in the R3 conference room network are considered *untrusted* and are allowed to initiate only web traffic (HTTP or HTTPS) to the Internet.
- No traffic is allowed between the internal network and the conference room network. There is no guarantee regarding the condition of guest computers in the conference room network.

Such machines could be infected with malware and might attempt to send out spam or other malicious traffic.

Step 1: Verify end-to-end network connectivity.

In this step, you will verify end-to-end network connectivity before implementing ZPF.

a. Ping from R1 to R3 using both of R3's G0/0/1 interface IP addresses (192.168.3.1 and 192.168.33.1).

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 conference room LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

c. Ping from PC-A on the R1 LAN to PC-B on the R3 internal LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Display the R3 running configurations.

In this step, you will verify R3 running configurations before implementing ZPF.

a. Issue the **show ip interface brief** command on R3 to verify the correct IP addresses were assigned. Use the Address Table to verify the addresses.

b. Issue the **show ip route** command on R3 to verify it has a static default route pointing to R2's G0/0/1 interface.

c. Issue the **show run** command to review the current basic configuration on R3.

Step 3: Creating the security zones.

A security zone is a group of interfaces with similar security properties and requirements. For example, if a router has three interfaces connected to internal networks, all three interfaces can be placed under the same zone named "internal". Because all security properties are configured to the zone instead of to the individual router interfaces, the firewall design is much more scalable.

In this lab, the R3 site has three interfaces; one connected to an internal trusted network, one connected to the conference room network and another connected to the internet. Because all three networks have different security requirements and properties, we will create three different security zones.

Security zones are created in global configuration mode, and the command allows for zone name definition. In R3, create three zones named **INSIDE**, **CONFROOM** and **INTERNET**:

```
R3(config)# zone security INSIDE
R3(config)# zone security CONFROOM
R3(config)# zone security INTERNET
```

Step 4: Creating Security Policies

Before ZPF can decide if some specific traffic should be allowed or denied, it must be told *what* traffic is to be considered. Cisco IOS uses class-maps to select traffic. *Interesting traffic* is a common denomination for traffic that has been selected by a class-map.

While class-maps select traffic, it is not their job to decide what happens to the selected traffic; Policy-maps decide the *fate* of the selected traffic.

ZPF traffic policies are defined as policy-maps and use class-maps to select traffic. In other words, class-maps define *what* traffic is to be policed while policy-maps define the *action* to be taken upon the selected traffic.

Policy-maps can drop, pass or inspect traffic. Because we want the firewall to *watch* traffic moving in the direction of zone-pairs, we will create inspect policy-maps. Inspect policy-maps allow for dynamic handling of the return traffic.

First, you will create class-maps. After the class-maps are created, you will create policy-maps and attach the class-maps to the policy-maps.

a. Create an inspect class-map to match traffic to be allowed from the INSIDE zone to the **INTERNET** zone. Because we trust the INSIDE zone, we allow all the main protocols.

   In the commands below, the first line creates an inspect class-map. The **match-any** keyword instructs the router that any of the **match** protocol statements will qualify as a successful match resulting in a policy being applied. The result is a match for TCP or UDP or ICMP packets.

   The **match** commands refer to specific Cisco NBAR supported protocols. For more information, perform an internet search for Cisco NBAR.

```
R3(config)# class-map type inspect match-any INSIDE_PROTOCOLS
R3(config-cmap)# match protocol tcp
R3(config-cmap)# match protocol udp
R3(config-cmap)# match protocol icmp
```

b. Similarly, create a class-map to match the traffic to be allowed from the **CONFROOM** zone to the **INTERNET** zone. Because we do not fully trust the **CONFROOM** zone, we must limit what the server can send out to the Internet:

```
R3(config)# class-map type inspect match-any CONFROOM_PROTOCOLS
R3(config-cmap)# match protocol http
R3(config-cmap)# match protocol https
R3(config-cmap)# match protocol dns
```

c. Now that the class-maps are created, you can create the policy-maps.

   In the commands below, the first line creates an inspect policy-map named **INSIDE_TO_INTERNET**. The second line binds the previously created **INSIDE_PROTOCOLS** class-map to the policy-map. All packets matched by the **INSIDE_PROTOCOLS** class-map will be subjected to the action taken by the **INSIDE_TO_INTERNET** policy-map. Finally, the third line defines the actual action this policy-map will apply to the matched packets. In this case, the matched packets will be inspected.

   The next three lines creates a similar policy-map named **CONFROOM_TO_INTERNET** and attaches the **CONFROOM_PROTOCOLS** class-map.

   The commands are as follows:

```
R3(config)# policy-map type inspect INSIDE_TO_INTERNET
R3(config-pmap)# class type inspect INSIDE_PROTOCOLS
R3(config-pmap-c)# inspect
R3(config)# policy-map type inspect CONFROOM_TO_INTERNET
R3(config-pmap)# class type inspect CONFROOM_PROTOCOLS
R3(config-pmap-c)# inspect
```

Step 5: Create the Zone Pairs

A zone pair allows you to specify a unidirectional firewall policy between two security zones.

For example, a commonly used security policy dictates that the internal network can initiate any traffic towards the Internet but no traffic originating from the Internet should be allowed to reach the internal network.

This traffic policy requires only one zone pair, **INTERNAL to INTERNET**. Because zone-pairs define unidirectional traffic flow, another zone-pair must be created if Internet-initiated traffic must flow in the **INTERNET to INTERNAL** direction.

Notice that Cisco ZPF can be configured to inspect traffic that moves in the direction defined by the zone pair. In that situation, the firewall *watches* the traffic and dynamically creates rules allowing the return or related traffic to flow back through the router.

To define a zone pair, use the **zone-pair security** command. The direction of the traffic is specified by the source and destination zones.

For this lab, you will create two zone-pairs:

INSIDE_TO_INTERNET: Allows traffic leaving the internal network towards the Internet.

CONFROOM_TO_INTERNET: Allows Internet access from the ConfRoom network.

a. Creating the zone-pairs:

```
R3(config)# zone-pair security INSIDE_TO_INTERNET source INSIDE
destination INTERNET
R3(config)# zone-pair security CONFROOM_TO_INTERNET source CONFROOM
destination INTERNET
```

b. Verify the zone-pairs were correctly created by issuing the **show zone-pair security** command. Notice that no policies are associated with the zone-pairs yet. The security policies will be applied to zone-pairs in the next step.

```
R3# show zone-pair security
Zone-pair name INSIDE_TO_INTERNET
    Source-Zone INSIDE  Destination-Zone INTERNET
    service-policy not configured
Zone-pair name CONFROOM_TO_INTERNET
    Source-Zone CONFROOM  Destination-Zone INTERNET
    service-policy not configured
```

Step 6: Applying Security Policies

a. As the last configuration step, apply the policy-maps to the zone-pairs:

```
R3(config)# zone-pair security INSIDE_TO_INTERNET
R3(config-sec-zone-pair)# service-policy type inspect
INSIDE_TO_INTERNET
R3(config)# zone-pair security CONFROOM_TO_INTERNET
R3(config-sec-zone-pair)# service-policy type inspect
CONFROOM_TO_INTERNET
```

b. Issue the **show zone-pair security** command once again to verify the zone-pair configuration. Notice that the service-polices are now displayed:

```
R3# show zone-pair security
Zone-pair name INSIDE_TO_INTERNET
    Source-Zone INSIDE  Destination-Zone INTERNET
    service-policy INSIDE_TO_INTERNET
Zone-pair name CONFROOM_TO_INTERNET
    Source-Zone CONFROOM  Destination-Zone INTERNET
    service-policy CONFROOM_TO_INTERNET
```

c. To obtain more information about the zone-pairs, their policy-maps, the class-maps and match counters, use the **show policy-map type inspect zone-pair** command:

```
R3# show policy-map type inspect zone-pair
Zone-pair: CONFROOM_TO_INTERNET
  Service-policy inspect : CONFROOM_TO_INTERNET

    Class-map: CONFROOM_PROTOCOLS (match-any)
      Match: protocol http
      Match: protocol https
      Match: protocol dns
      Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
  Zone-pair: INSIDE_TO_INTERNET
  Service-policy inspect : INSIDE_TO_INTERNET

    Class-map: INSIDE_PROTOCOLS (match-any)
      Match: protocol tcp
      Match: protocol udp
      Match: protocol icmp
      Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes <output omitted>
```

Step 7: Assign Interfaces to the Proper Security Zones

Interfaces (physical and logical) are assigned to security zones with the **zone-member security** interface command.

a. Assign R3’s G0/0 to the **CONFROOM** security zone:

```
R3(config)# interface g0/0/1.33
R3(config-if)# zone-member security CONFROOM
```

b. Assign R3’s G0/1 to the INSIDE security zone:

```
R3(config)# interface g0/0/1.3
R3(config-if)# zone-member security INSIDE
```

c. Assign R3’s S0/0/1 to the **INTERNET** security zone:

```
R3(config)# interface g0/0/0
R3(config-if)# zone-member security INTERNET
```

Step 8: Verify Zone Assignment

a. Issue the show zone security command to ensure the zones were properly created, and the interfaces were correctly assigned:

```
R3# show zone security
zone self
  Description: System defined zone

zone service
  Description: System defined zone

zone INSIDE
  Member Interfaces:
    GigabitEthernet0/0/1.3

zone CONFROOM
  Member Interfaces:
    GigabitEthernet0/0/1.33

zone INTERNET
  Member Interfaces:
    GigabitEthernet0/0/0
```

b. Even though no commands were issued to create a “self” zone, the output above still displays it.

Why is R3 displaying a zone named “self”? What is the significance of this zone?

Part 3: Verify ZPF Firewall Functionality

Step 1: Traffic originating on the Internet

a. To test the firewall’s effectiveness, ping PC-B from PC-A. In PC-A, open a command prompt and issue a ping to 192.168.3.3.

```
PC-A:\> ping 192.168.3.3
```

Was the ping successful? Explain.

b. Ping PC-C from PC-A. In PC-A, open a command window and ping 192.168.33.3.

```
PC-A:\> ping 192.168.33.3
```

Was the ping successful? Explain.

c. Ping PC-A from PC-B. In PC-B, open a command window and issue a ping to 192.168.1.3.

```
PC-B:\> ping 192.168.1.3
```

Was the ping successful? Explain.

d. Ping PC-A from PC-C. In PC-C, open a command window and ping 192.168.1.3

```
PC-C:\> ping 192.168.1.3
```

Was the ping successful? Explain.

Step 2: The Self Zone Verification

a. From PC-A ping R3's G0/0/1.3 interface:

```
PC-A:\> ping 192.168.3.1
```

Was the ping successful? Is this the correct behavior? Explain.

b. From PC-C ping R3's G0/0/1.3 interface:

```
PC-C:\> ping 192.168.3.1
```

Was the ping successful? Is this the correct behavior? Explain.

Challenge (optional)

Create the proper zone-pair, class-maps, and policy-maps and configure R3 to prevent Internet originating traffic from reaching the Self Zone.

Appendix – Multiple Interfaces under the Same Zone (optional)

One benefit of ZPF firewalls is that they scale well compared to the classic firewall. If a new interface with the same security requirements is added to the firewall, the administrator can simply add the new interface as a member of an existing security zone. However, some IOS versions will not allow devices connected to different interfaces of the same zone to communicate by default. In those cases, a zone-pair must be created using the same zone as source and destination.

Traffic between similarly zoned interfaces will always be bidirectional due to the fact that the zone-pair's source and destination zones are the same. Because of that, there is no need to inspect traffic to allow for automatic return traffic handling; return traffic will always be allowed because it will always conform to the zone-pair definition. In this case, the policy-map should have a **pass** action instead of **inspect**. Because of the **pass** action, the router will not inspect packets matched by the policy-map, it will simply forward it to its destination.

In the context of this lab, if R3 had a G0/0/1.2 interface also assigned to the INSIDE zone, and the router IOS version did not support allowing traffic between interfaces configured to the same zone, the extra configuration would look like this:

New zone-pair: **Inside to Inside**; allows routing of traffic among the internal trusted interfaces.

Creating the policy-map (notice that no explicit class-map is needed because we use the default “catch-all” class):

```
R3(config)# policy-map type inspect inside
R3(config-pmap)# class class-default
R3(config-pmap-c)# pass
```

Creating the zone-pair and assigning the new policy-map to it. Notice that the INSIDE zone is both the source and the destination of the zone-pair:

```
R3(config)# zone-pair security INSIDE source INSIDE destination INSIDE
R3(config-sec-zone-pair)# service-policy type inspect inside
```

To verify the existence of the new pair, use **show zone-pair security:**

```
R3# show zone-pair security
Zone-pair name INSIDE_TO_INTERNET
    Source-Zone INSIDE Destination-Zone INTERNET
    service-policy INSIDE_TO_INTERNET
Zone-pair name CONFROOM_TO_INTERNET
    Source-Zone CONFROOM  Destination-Zone INTERNET
    service-policy CONFROOM_TO_INTERNET
Zone-pair name INSIDE
    Source-Zone INSIDE Destination-Zone INSIDE
    service-policy inside
```

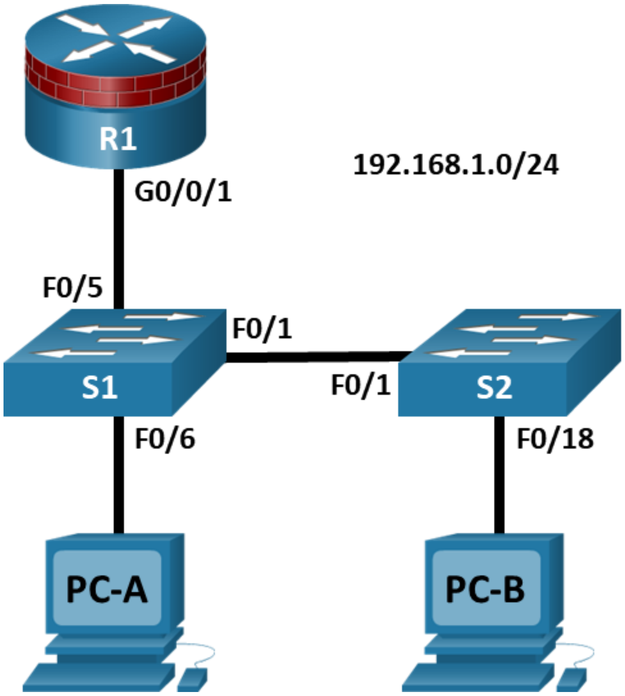
Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

[Title]

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A	N/A
S2	VLAN 1	192.168.1.3	255.255.255.0	N/A	N/A
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1	S1 F0/6
PC-B	NIC	192.168.1.11	255.255.255.0	192.168.1.1	S2 F0/18

Objectives

Part 1: Configure Basic Switch Settings

- Build the topology.
- Configure the hostname, IP address, and access passwords.

Part 2: Configure Secure Trunks Ports

- Configure trunk port mode.
- Change the native VLAN for trunk ports.
- Verify trunk configuration.
- Disable trunking.

Part 3: Protect Against STP Attacks

- Enable PortFast and BPDU guard.

- Verify BPDU guard.
- Enable root guard.
- Enable loop guard.

Part 4: Configure Port Security and Disable Unused Ports

- Configure and verify port security.
- Disable unused ports.
- Move ports from default VLAN 1 to alternate VLAN.
- Configure the PVLAN Edge feature on a port.

Background / Scenario

The Layer 2 infrastructure consists mainly of interconnected Ethernet switches. Most end-user devices, such as computers, printers, IP phones, and other hosts, connect to the network via Layer 2 access switches. As a result, switches can present a network security risk. Similar to routers, switches are subject to attack from malicious internal users. The switch Cisco IOS software provides many security features that are specific to switch functions and protocols.

In this lab, you will configure various switch protection measures, including access port security and Spanning Tree Protocol (STP) features, such as BPDU guard and root guard.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.6 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960+ with Cisco IOS Release 15.2(7) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Before you begin, ensure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 1 Router (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 2 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 2 PCs (Windows OS with a terminal emulation program, such as PuTTY or Tera Term installed)
- Console cables to configure Cisco networking devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Switch Settings

In Part 1, you will set up the network topology and configure basic settings, such as the hostnames, IP addresses, and device access passwords.

Step 1: Cable the network as shown in the topology.

Attach the devices, as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for the router and each switch.

Perform all tasks on R1, S1, and S2. The procedure for S1 is shown here as an example.

Configure hostnames, as shown in the topology.

Configure interface IP addresses, as shown in the IP Addressing Table. The following configuration displays the VLAN 1 management interface on S1:

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
```

Prevent the router or switch from attempting to translate incorrectly entered commands by disabling DNS lookup. S1 is shown here as an example.

```
S1(config)# no ip domain-lookup
```

HTTP access to the switch is enabled by default. Prevent HTTP access by disabling the HTTP server and HTTP secure server.

```
S1(config)# no ip http server
S1(config)# no ip http secure-server
```

Note: The switch must have a cryptography IOS image to support the **ip http secure-server** command. HTTP access to the router is disabled by default.

Configure the enable secret password.

```
S1(config)# enable algorithm-type scrypt secret cisco12345
```

Configure console password.

```
S1(config)# line console 0
S1(config-line)# password ciscoconpass
S1(config-line)# exec-timeout 5 0
S1(config-line)# login
S1(config-line)# logging synchronous
```

Step 3: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-B, as shown in the Addressing Table.

Step 4: Verify basic network connectivity.

a. Ping from PC-A and PC-B to the R1 G0/0/1 interface at IP address **192.168.1.1**.

If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A to PC-B.

If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

Step 5: Save the basic configurations for the router and both switches.

Save the running configuration to the startup configuration from the privileged EXEC mode prompt.

```
S1# copy running-config startup-config
```

Part 2: Configure Secure Trunk Ports

In this part, you will configure trunk ports, change the native VLAN for trunk ports, and verify trunk configuration.

Securing trunk ports can help stop VLAN hopping attacks. The best way to prevent a basic VLAN hopping attack is to explicitly disable trunking on all ports except the ports that specifically require trunking. On the required trunking ports, disable DTP (auto trunking) negotiations and manually enable trunking. If no trunking is required on an interface, configure the port as an access port. This disables trunking on the interface.

Note: Tasks should be performed on S1 or S2, as indicated.

Step 1: Configure S1 as the root switch.

For the purposes of this lab, S2 is currently the root bridge. You will configure S1 as the root bridge by changing the bridge ID priority level.

a. From the console on S1, enter global configuration mode.

b. The default priority for S1 and S2 is 32769 (32768 + 1 with System ID Extension). Set S1 priority to **0** so that it becomes the root switch.

```
S1(config)# spanning-tree vlan 1 priority 0
S1(config)# exit
```

Note: You can also use the **spanning-tree vlan 1 root primary** command to make S1 the root switch for VLAN 1.

c. Issue the **show spanning-tree** command to verify that S1 is the root bridge, to see the ports in use, and to see their status.

```
S1# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    1
             Address     001d.4635.0c80
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    1      (priority 0 sys-id-ext 1)
             Address     001d.4635.0c80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
```

What is the S1 priority?

Which ports are in use and what is their status?

Step 2: Configure trunk ports on S1 and S2.

a. Configure port F0/1 on S1 as a trunk port.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

Note: If performing this lab with a 3560 switch, the user must first enter the **switchport trunk encapsulation dot1q** command.

b. Configure port F0/1 on S2 as a trunk port.

```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```

c. Verify that S1 port F0/1 is in trunking mode with the **show interfaces trunk** command.

```
S1# show interfaces trunk

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

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
```

Step 3: Change the native VLAN for the trunk ports on S1 and S2.

a. Changing the native VLAN for trunk ports to an unused VLAN helps prevent VLAN hopping attacks.

From the output of the **show interfaces trunk** command in the previous step, what is the current native VLAN for the S1 F0/1 trunk interface?

b. Set the native VLAN on the S1 F0/1 trunk interface to an unused VLAN 99.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
```

c. The following message should display after a brief period of time:

```
02:16:28: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/1 (99), with S2 FastEthernet0/1 (1).
```

What does the message mean?

d. Set the native VLAN on the S2 F0/1 trunk interface to VLAN 99.

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# end
```

Step 4: Prevent the use of DTP on S1 and S2.

Setting the trunk port to **nonegotiate** also helps to mitigate VLAN hopping by turning off the generation of DTP frames.

```
S1(config)# interface f0/1
```

```
S1(config-if)# switchport nonegotiate

S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```

Step 5: Verify the trunking configuration on port F0/1.

```
S1# show interfaces f0/1 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1

S1# show interfaces f0/1 switchport

Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Inactive)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Step 6: Verify the configuration with the show run command.

Use the **show run** command to display the running configuration, beginning with the first line that has the text string “0/1” in it.

```
S1# show run | begin 0/1
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate

<output omitted>
```

Step 7: Disable trunking on S1 access ports.

a. On S1, configure F0/5, the port to which R1 is connected, as access mode only.

```
S1(config)# interface f0/5
S1(config-if)# switchport mode access
```

b. On S1, configure F0/6, the port to which PC-A is connected, as access mode only.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
```

Step 8: Disable trunking on S2 access ports.

On S2, configure F0/18, the port to which PC-B is connected, as access mode only.

```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
```

Part 3: Protect Against STP Attacks

Network attackers hope to spoof their system, or a rogue switch that they add to the network, as the root bridge in the topology by manipulating the STP root bridge parameters. If a port that is configured with PortFast receives a BPDU, STP can put the port into the blocking state by using a feature called BPDU guard.

The topology has only two switches and no redundant paths, but STP is still active. In this part, you will enable switch security features that can help reduce the possibility of an attacker manipulating switches via STP-related methods.

Step 1: Enable portfast.

PortFast is configured on access ports that connect to a single workstation or server, which enables them to become active more quickly.

a. Enable PortFast on the S1 F0/5 access port.

```
S1(config)# interface f0/5
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single host.
Connecting hubs, concentrators, switches, bridges, etc... to this interface
when portfast is enabled, can cause temporary bridging loops. Use with CAUTION
```

```
%Portfast has been configured on FastEthernet0/5 but will only
 have effect when the interface is in a non-trunking mode.
```

b. Enable PortFast on the S1 F0/6 access port.

```
S1(config)# interface f0/6
S1(config-if)# spanning-tree portfast
```

c. Enable PortFast on the S2 F0/18 access ports.

```
S2(config)# interface f0/18
S2(config-if)# spanning-tree portfast
```

Step 2: Enable BPDU guard.

BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports.

a. Enable BPDU guard on the switch port F0/6.

```
S1(config)# interface f0/6
S1(config-if)# spanning-tree bpduguard enable

S2(config)# interface f0/18
S2(config-if)# spanning-tree bpduguard enable
```

Note: PortFast and BPDU guard can also be enabled globally with the **spanning-tree portfast default** and **spanning-tree portfast bpduguard** commands in global configuration mode.

Note: BPDU guard can be enabled on all access ports that have PortFast enabled. These ports should never receive a BPDU. BPDU guard is best deployed on user-facing ports to prevent rogue switch network extensions by an attacker. If a port is enabled with BPDU guard and receives a BPDU, it is disabled and must be manually re-enabled. An **err-disable timeout** can be configured on the port so that it can recover automatically after a specified time period.

b. Verify that BPDU guard is configured by using the **show spanning-tree interface f0/6 detail** command on S1.

```
S1# show spanning-tree interface f0/6 detail

Port 6 (FastEthernet0/6) of VLAN0001 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.6.
   Designated root has priority 1, address 001d.4635.0c80
   Designated bridge has priority 1, address 001d.4635.0c80
   Designated port id is 128.6, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast mode
   Link type is point-to-point by default
   Bpdu guard is enabled
   BPDU: sent 3349, received 0
```

Step 3: Enable root guard.

Root guard is another option to help prevent rogue switches and spoofing. Root guard can be enabled on all ports on a switch that are not root ports. It is normally enabled only on ports connecting to edge switches where a superior BPDU should never be received. Each switch should have only one root port, which is the best path to the root switch.

a. The following command configures root guard on S2 interface G0/1. Normally, this is done if another switch is attached to this port. Root guard is best deployed on ports that connect to switches that should not be the root bridge. In the lab topology, S1 F0/1 would be the most logical candidate for root guard. However, S2 G0/1 is shown here as an example, as Gigabit ports are more commonly used for inter-switch connections.

```
S2(config)# interface g0/1
S2(config-if)# spanning-tree guard root
```

b. Issue the **show run | begin Gig** command to verify that root guard is configured.

```
S2# show run | begin Gig
interface GigabitEthernet0/1
 spanning-tree guard root
```

Note: The S2 Gi0/1 port is not currently up, so it is not participating in STP. Otherwise, you could use the **show spanning-tree interface Gi0/1 detail** command.

Note: The expression in the command **show run | begin** is case-sensitive.

c. If a port that is enabled with BPDU guard receives a superior BPDU, it enters a root-inconsistent state. Use the **show spanning-tree inconsistentports** command to determine if there are any ports currently receiving superior BPDUs that should not be.

```
S2# show spanning-tree inconsistentports

Name                 Interface              Inconsistency
-------------------- ---------------------- ------------------
Number of inconsistent ports (segments) in the system : 0
```

Note: Root guard allows a connected switch to participate in STP as long as the device does not try to become the root. If root guard blocks the port, subsequent recovery is automatic. The port returns to the forwarding state if the superior BPDUs stop.

Step 4: Enable loop guard.

The STP loop guard feature provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the STP blocking port) no longer receives STP BPDUs. Having all ports in forwarding state will result in forwarding loops. If a port enabled with loopguard stops hearing BPDUs from the designated port on the segment, it goes into the loop inconsistent state instead of transitioning into forwarding state. Loop inconsistent is basically blocking, and no traffic is forwarded. When the port detects BPDUs again it automatically recovers by moving back into blocking state.

a. Loop guard should be applied to non-designated ports. Therefore, the global command can be configured on non-root switches.

```
S2(config)# spanning-tree loopguard default
```

b. Verify Loopguard configuration.

```
S2# show spanning-tree summary
Switch is in pvst mode

Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
```

```
Loopguard Default            is enabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                     0         0        0          3          3
---------------------- -------- --------- -------- ---------- ---------
```

Part 4: Configure Port Security and Disable Unused Ports

Switches can be subject to a CAM table, also known as a MAC address table, overflow, MAC spoofing attacks, and unauthorized connections to switch ports. In this task, you will configure port security to limit the number of MAC addresses that can be learned on a switch port and disable the port if that number is exceeded.

Step 1: Record the R1 G0/0/1 MAC address.

From the R1 CLI, use the **show interface** command and record the MAC address of the interface.

```
R1# show interfaces g0/0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e1 (bia
fc99.4775.c3e1)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
<Output Omitted>
```

What is the MAC address of the R1 G0/0/1 interface?

Step 2: Configure basic port security.

This procedure should be performed on all access ports that are in use. S1 port F0/5 is shown here as an example.

a. From the S1 CLI, enter interface configuration mode for the port that connects to the router (Fast Ethernet 0/5).

```
S1(config)# interface f0/5
```

b. Shut down the switch port.

```
S1(config-if)# shutdown
```

c. Enable port security on the port.

```
S1(config-if)# switchport port-security
```

Note: A switch port must be configured as an access port to enable port security.

Note: Entering just the **switchport port-security** command sets the maximum MAC addresses to **1** and the violation action to **shutdown**. The **switchport port-security maximum** and **switchport port-security violation** commands can be used to change the default behavior.

d. Configure a static entry for the MAC address of R1 G0/0/1 interface recorded in Step 1.

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

Note: *xxxx.xxxx.xxxx* is the actual MAC address of the router G0/0/1 interface.

Note: You can also use the **switchport port-security mac-address sticky** command to add all the secure MAC addresses that are dynamically learned on a port (up to the maximum set) to the switch running configuration.

e. Enable the switch port.

```
S1(config-if)# no shutdown
```

Step 3: Verify port security on S1 F0/5.

a. On S1, issue the **show port-security** command to verify that port security has been configured on S1 F0/5.

```
S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

What is the Security Violation Count?

What is the status of the F0/5 port?

What is the Last Source Address and VLAN?

b. From the R1 CLI, ping PC-A to verify connectivity. This also ensures that the R1 G0/0/1 MAC address is learned by the switch.

```
R1# ping 192.168.1.10
```

c. Now, violate security by changing the MAC address on the router interface. Enter interface configuration mode for the Fast Ethernet 0/1. Configure a MAC address for the interface on the interface, using **aaaa.bbbb.cccc** as the address.

```
R1(config)# interface g0/0/1
R1(config-if)# mac-address aaaa.bbbb.cccc
R1(config-if)# end
```

Note: You can also change the PC MAC address attached to S1 F0/6 and achieve similar results to those shown here.

From the R1 CLI, ping PC-A. Was the ping successful? Explain.

d. On S1 console, observe the messages when port F0/5 detects the violating MAC address.

```
*Jan 14 01:34:39.750: %PM-4-ERR_DISABLE: psecure-violation error detected on
Fa0/5, putting Fa0/5 in err-disable state
*Jan 14 01:34:39.750: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address aaaa.bbbb.cccc on port FastEthernet0/5.
*Jan 14 01:34:40.756: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/5, changed state to down
*Jan 14 01:34:41.755: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state
to down
```

e. On the switch, use the **show port-security** commands to verify that port security has been violated.

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
      Fa0/5            1           1                 1         Shutdown
----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : aaaa.bbbb.cccc:1
Security Violation Count   : 1

S1# show port-security address
Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
   1    fc99.4775.c3e1    SecureConfigured              Fa0/5         -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

f. Remove the hard-coded MAC address from the router and re-enable the G0/0/1 interface.

```
R1(config)# interface g0/0/1
R1(config-if)# no mac-address aaaa.bbbb.cccc
```

Note: This will restore the original GigabitEthernet interface MAC address.

From R1, try to ping the PC-A again at 192.168.1.10. Was the ping successful? Explain.

Step 4: Clear the S1 F0/5 error disabled status.

a. From the S1 console, clear the error and re-enable the port using the commands shown in the example. This will change the port status from Secure-shutdown to Secure-up.

```
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

Note: This assumes the device/interface with the violating MAC address has been removed and replaced with the original device/interface configuration.

b. From R1, ping PC-A again. You should be successful this time.

```
R1# ping 192.168.1.10
```

Step 5: Remove basic port security on S1 F0/5.

From the S1 console, remove port security on F0/5. This procedure can also be used to re-enable the port, but **port security** commands must be reconfigured.

```
S1(config)# interface f0/5
S1(config-if)# no switchport port-security
S1(config-if)# no switchport port-security mac-address fc99.4775.c3e1
```

You can also use the following commands to reset the interface to its default settings:

```
S1(config)# default interface f0/5
S1(config)# interface f0/5
```

Note: This **default interface** command also requires that you reconfigure the port as an access port to re-enable the security commands.

Step 6: (Optional) Configure port security for VoIP.

This example shows a typical port security configuration for a voice port. Three MAC addresses are allowed and should be learned dynamically. One MAC address is for the IP phone, one is for the switch, and one is for the PC connected to the IP phone. Violations of this policy result in the port being shut down. The aging timeout for the learned MAC addresses is set to two hours.

The following example displays S2 port F0/18:

```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport port-security
S2(config-if)# switchport port-security maximum 3
S2(config-if)# switchport port-security violation shutdown
S2(config-if)# switchport port-security aging time 120
```

Step 7: Disable unused ports on S1 and S2.

As a further security measure, disable ports that are not being used on the switch.

a. Ports F0/1, F0/5, and F0/6 are used on S1. The remaining Fast Ethernet ports and the two Gigabit Ethernet ports will be shut down.

```
S1(config)# interface range f0/2 - 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 - 2
S1(config-if-range)# shutdown
```

b. Ports F0/1 and F0/18 are used on S2. The remaining Fast Ethernet ports and the Gigabit Ethernet ports will be shut down.

```
S2(config)# interface range f0/2 – 17, f0/19 – 24, g0/1 - 2
S2(config-if-range)# shutdown
```

Step 8: Move active ports to a VLAN other than the default VLAN 1.

As a further security measure, you can move all active end-user ports and router ports to a VLAN other than the default VLAN 1 on both switches.

a. Configure a new VLAN for users on each switch using the following commands:

```
S1(config)# vlan 20
S1(config-vlan)# name Users

S2(config)# vlan 20
S2(config-vlan)# name Users
```

b. Add the current active access (non-trunk) ports to the new VLAN.

```
S1(config)# interface f0/6
S1(config-if-range)# switchport access vlan 20

S2(config)# interface f0/18
S2(config-if)# switchport access vlan 20
```

Note: This will prevent communication between end-user hosts and the management VLAN IP address of the switch, which is currently VLAN 1. The switch can still be accessed and configured using the console connection.

Note: To provide SSH access to the switch, a specific port can be designated as the management port and added to VLAN 1 with a specific management workstation attached. A more elaborate solution is to create a new VLAN for switch management (or use the existing native trunk VLAN 99), and configure a separate subnet for the management and user VLANs.

Step 9: Configure a port with the PVLAN Edge feature.

Some applications require that no traffic be forwarded at Layer 2 between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor. In such an environment, the use of the Private VLAN (PVLAN) Edge feature, also known as protected ports, ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch. The PVLAN Edge feature can only be implemented for ports on the same switch and is locally significant.

For example, to prevent traffic between host PC-A on S1 (port F0/6) and a host on another S1 port (e.g. port F0/7, which was previously shut down), you could use the **switchport protected** command to activate the PVLAN Edge feature on these two ports. Use the **no switchport protected** interface configuration command to disable protected port.

a. Configure the PVLAN Edge feature in interface configuration mode using the following commands:

```
S1(config)# interface f0/6
S1(config-if)# switchport protected
S1(config-if)# interface f0/7
S1(config-if)# switchport protected
S1(config-if)# no shut
S1(config-if)# end
```

b. Verify that the PVLAN Edge Feature (protected port) is enabled on F0/6.

```
S1# show interfaces f0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 20 (Users)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

c. Deactivate protected port on interfaces F0/6 and F0/7 using the following commands:

```
S1(config)# interface range f0/6 - 7
S1(config-if-range)# no switchport protected
```

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.