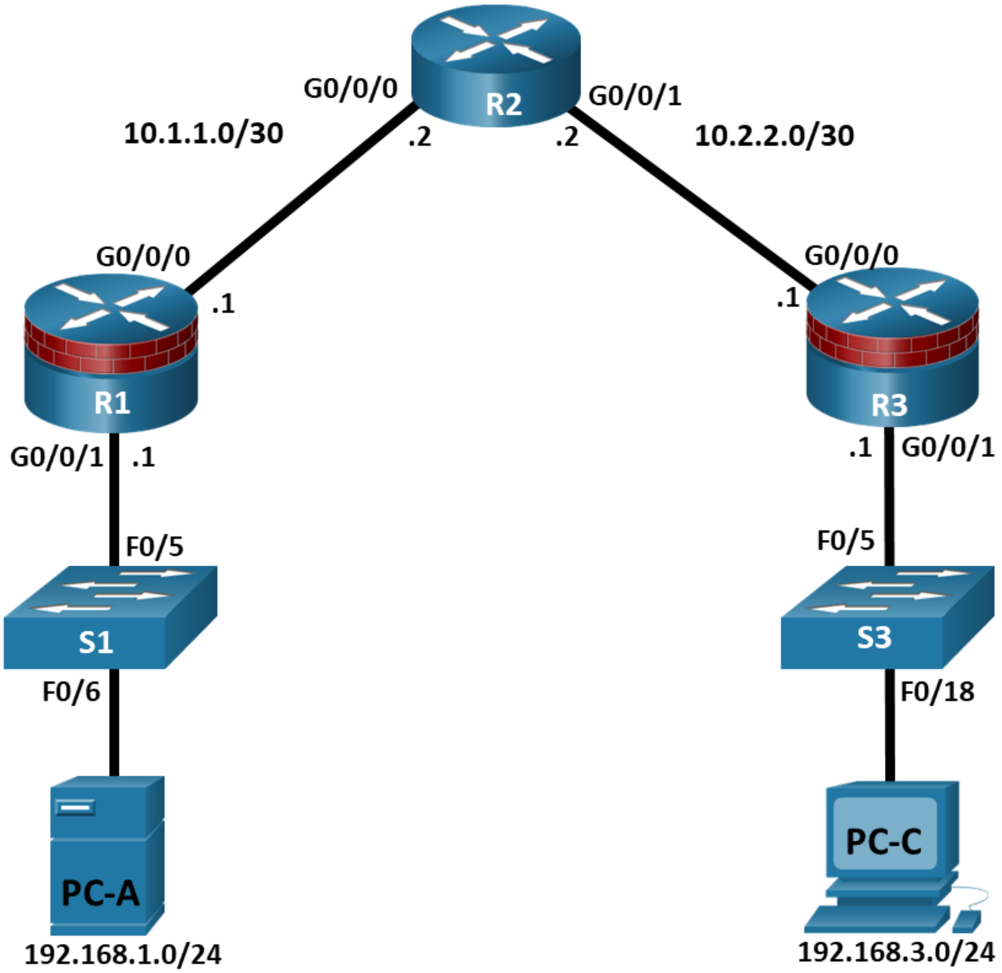
Lab - Configure Administrative Roles

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
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.