Lab - Configure IPv4 and IPv6 Static and Default Routes

Topology
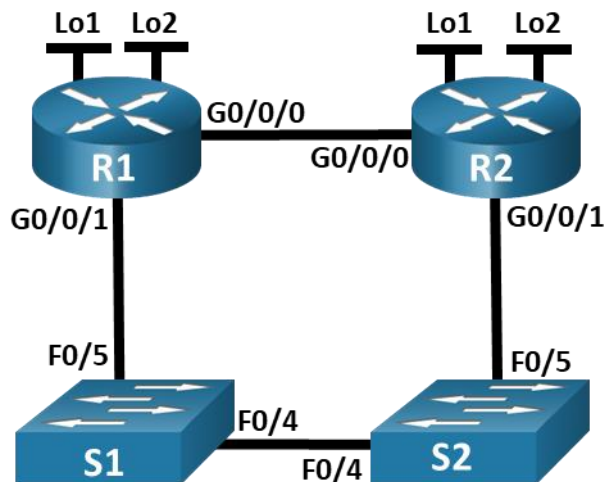
Addressing Table

Device	Interface	IP Address / Prefix
R1	G0/0/0	172.16.1.1 /24
		2001:db8:acad:2::1 /64
		fe80::1
	G0/0/1	192.168.1.1 /24
		2001:db8:acad:1::1 /64
		fe80::1
	Loopback1	10.1.0.1 /24
		2001:db8:acad:10::1 /64
		fe80::1
	Loopback2	209.165.200.225 /27
		2001:db8:acad:209::1 /64
		fe80::1
R2	G0/0/0	172.16.1.2 /24
		2001:db8:acad:2::2 /64
		fe80::2

Device	Interface	IP Address / Prefix
	G0/0/1	192.168.1.2 /24
		2001:db8:acad:1::2 /64
		fe80::2
	Loopback1	10.2.0.1 /24
		2001:db8:acad:11::2 /64
		fe80::2
	Loopback2	209.165.200.193 /27
		2001:db8:acad:210::1 /64
		fe80::2

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure and verify IP and IPv6 addressing on R1 and R2

Part 3: Configure and verify static and default routing for IPv4 on R1 and R2

Part 4: Configure and verify static and default routing for IPv6 on R1 and R2

Background / Scenario

Static and Default routing are the simplest forms of network routing and configured manually. They are fixed, meaning that they do not change dynamically to meet changing network conditions. They are either valid and made available to the routing table or invalid and not made available to the routing table. Static routes have an administrative distance of one by default. However, static and default routes can be configured with an administrator-defined administrative distance. This capability allows the administrator to put the static or default route in reserve, and only make it available to the routing table when routes with lower administrative distances (usually generated by dynamic routing protocols) are no longer valid.

Note: In this lab you will configure static, default, and floating default routes for both IPv4 and IPv6 which may not reflect networking best practices.

Note: The routers used with CCNA 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: Ensure that the routers and switches have been erased and have no startup configurations. If you are unsure contact your instructor.

Required Resources

- 2 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(2) lanbasek9 image or comparable)
- 1 PC (Windows with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Instructions

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and switches.

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 each router.

a. Assign a device name to the router.

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

c. Assign **class** as the privileged EXEC encrypted password.

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

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

f. Encrypt the plaintext passwords.

g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

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

Step 3: Configure basic settings for each switch.

a. Assign a device name to the switch.

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

c. Assign **class** as the privileged EXEC encrypted password.

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

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

f. Encrypt the plaintext passwords.

g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

h. Shutdown all interfaces that will not be used.

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

Issuing the command **show cdp neighbors** at this point on R1 or R2 results in an empty list. Explain.

Part 2: Configure and verify IPv4 and IPv6 addressing on R1 and R2

In Part 2, you will configure and verify the IPv4 and IPv6 addresses on R1 and R2. Use the table above for the information necessary to complete this part.

Step 1: Configure IP addresses for both routers.

a. Enable IPv6 Unicast Routing on both routers.

b. Configure the IP address for all the interfaces according to the Addressing Table.

Step 2: Verify addressing

    a.   Issue the command to verify IPv4 assignments to the interfaces.

    b.   Issue the command to verify IPv6 assignments to the interfaces.

Step 3: Save your configuration

Save the running configuration to the startup configuration file on both routers.

Part 3: Configure and verify static and default routing for IPv4 on R1 and R2

In Part 3, you will configure static and default routing on R1 and R2 to enable full connectivity between the routers using IPv4. Once again, the static routing being used here is not meant to represent best practice, but to assess your ability to complete the required configurations.

Step 1: On R1, configure a static route to R2's Loopback1 network, using R2's G0/0/1 address as the next hop.

    a.   Use the **ping** command to ensure that R2's G0/0/1 interface is reachable.

    b.   Configure a static route for R2's Loopback1 network via R2's G0/0/1 address.

        R1(config)# ip route 10.2.0.0 255.255.255.0 192.168.1.2

Step 2: On R1, configure a static default route via R2's G0/0/0 address.

    a.   Use the **ping** command to ensure that R2's G0/0/0 interface is reachable.

    b.   Configure a static default route via R2's G0/0/0 address.

        R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.2

Step 3: On R1, configure a floating static default route via R2's G0/0/1 address.

Configure a floating static default route with an AD of 80 via R2's G0/0/1 address.

        R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.2 80

Step 4: On R2, configure a static default route via R1's G0/0/0 address

    a.   Use the **ping** command to ensure that R1's G0/0/0 interface is reachable.

    b.   Configure a static default route via R1's G0/0/0 address.

        R2(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.1

Step 5: Verify that the routes are operational.

    a.   Use the **show ip route** command to ensure that R1's routing table shows the static and default routes.

    b.   On R1, issue the command **traceroute 10.2.0.1**. The output should show that the next hop is 192.168.1.2.

    c.   On R1, issue the command **traceroute 209.165.200.193**. The output should show that the next hop is 172.16.1.2.

    d.   Issue the **shutdown** command on R1 G0/0/0.

    e.   Demonstrate that the floating static route is working. First, issue the **show ip route static** command. You should see two static routes. A default static route with an AD of 80 and a static route to the 10.2.0.0/24 network with an AD of 1.

f.   Demonstrate the floating static route is working by issuing the **traceroute 209.165.200.193** command. The traceroute will show the next hop as 192.168.1.2.

g.   Issue the **no shutdown** command on R1 G0/0/0.

Part 4: Configure and verify static and default routing for IPv6 on R1 and R2

In Part 4, you will configure static and default routing on R1 and R2 to enable full connectivity between the routers using IPv6. Once again, the static routing being used here is not meant to represent best practice, but to assess your ability to complete the required configurations.

Step 1: On R2, configure a static route to R1's Loopback1 network, using R1's G0/0/1 address as the next hop.

a.   Use the **ping** command to ensure that R1's G0/0/1 interface is reachable.

b.   Configure a static route for R1's Loopback1 network via R1's G0/0/1 address.

```
R2(config)# ipv6 route 2001:db8:acad:10::/64 2001:db8:acad:1::1
```

Step 2: On R2, configure a static default route via R1's G0/0/0 address.

a.   Use the **ping** command to ensure that R1's G0/0/0 interface is reachable.

b.   Configure a static default route via R1's G0/0/0 address.

```
R2(config)# ipv6 route ::/0 2001:db8:acad:2::1
```

Step 3: On R2, configure a floating static default route via R1's G0/0/1 address.

Configure a floating static default route with an AD of 80 via R2's G0/0/1 address.

```
R2(config)# ipv6 route ::/0 2001:db8:acad:1::1 80
```

Step 4: On R1, configure a static default route via R1's G0/0/0 address.

a.   Use the **ping** command to ensure that R2's G0/0/0 interface is reachable.

b.   Configure a static default route via R2's G0/0/0 address.

```
R1(config)# ipv6 route ::/0 2001:db8:acad:2::2
```

Step 5: Verify that the routes are operational.

a.   Use the **show ipv6 route** command to ensure that R2's routing table shows the static and default routes.

b.   On R2, issue the command **traceroute 2001:db8:acad:10::1**. The output should show that the next hop is 2001:db8:acad:1::1.

c.   On R2, issue the command **traceroute 2001:db8:acad:209::1**. The output should show that the next hop is 2001:db8:acad:2::1.

d.   Issue the **shutdown** command on R2 G0/0/0.

e.   Demonstrate the floating static route is working. First issue the **show ipv6 route static** command. You should see two static routes. A default static route with an AD of 80 and a static route to the 2001:db8:acad:10::/64 network with an AD of 1.

f.   Lastly, demonstrate that the floating static route is working by issuing the **traceroute 2001:db8:acad:209::1** command. The traceroute will show the next hop as 2001:db8:acad:1::1.

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
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)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	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.