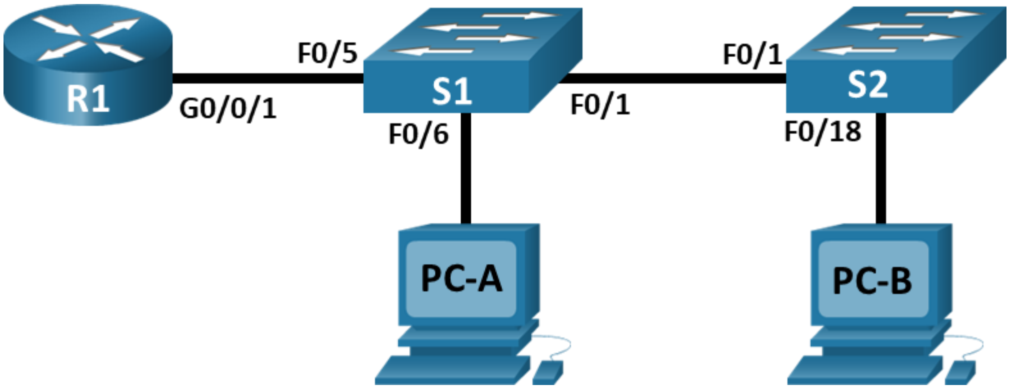
Lab - Configure Router-on-a-Stick Inter-VLAN Routing

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/1.3	192.168.3.1	255.255.255.0	N/A
	G0/0/1.4	192.168.4.1	255.255.255.0	
	G0/0/1.8	N/A	N/A	
S1	VLAN 3	192.168.3.11	255.255.255.0	192.168.3.1
S2	VLAN 3	192.168.3.12	255.255.255.0	192.168.3.1
PC-A	NIC	192.168.3.3	255.255.255.0	192.168.3.1
PC-B	NIC	192.168.4.3	255.255.255.0	192.168.4.1

VLAN Table

VLAN	Name	Interface Assigned
3	Management	S1: VLAN 3 S2: VLAN 3 S1: F0/6
4	Operations	S2: F0/18
7	ParkingLot	S1: F0/2-4, F0/7-24, G0/1-2 S2: F0/2-17, F0/19-24, G0/1-2
8	Native	N/A

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Create VLANs and Assign Switch Ports

Part 3: Configure an 802.1Q Trunk between the Switches

Part 4: Configure Inter-VLAN Routing on the Router

Part 5: Verify Inter-VLAN Routing is working

Background / Scenario

Modern switches use virtual local-area networks (VLANs) to provide segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. In general, VLANs make it easier to design a network to support the goals of an organization. Communication between VLANs requires a device operating at Layer 3 of the OSI model. Routers in VLAN topologies provide additional security and traffic flow management.

VLAN trunks are used to span VLANs across multiple devices. Trunks allow the traffic from multiple VLANS to travel over a single link, while keeping the VLAN identification and segmentation intact. A particular kind of inter-VLAN routing, called “Router-On-A-Stick”, uses a trunk from the router to the switch to enable all VLANs to pass to the router.

In this lab, you will create VLANs on both switches in the topology, assign VLANs to switch access ports, verify that VLANs are working as expected, create VLAN trunks between the two switches and between S1 and R1, and configure Inter-VLAN routing on R1 to allow hosts in different VLANs to communicate, regardless of which subnet the host resides.

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

- 1 Router (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)
- 2 PCs (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 the router.

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

b. Enter configuration mode.

c. Assign a device name to the router.

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

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

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

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

h. Encrypt the plaintext passwords.

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

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

k. Set the clock on the router.

   Note: Use the question mark (**?**) to help with the correct sequence of parameters needed to execute this command.

Step 3: Configure basic settings for each switch.

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

b. Enter configuration mode.

c. Assign a device name to the switch.

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

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

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

g. Assign **cisco** as the vty password and enable login.

h. Encrypt the plaintext passwords.

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

j. Set the clock on the switch.

   Note: Use the question mark (**?**) to help with the correct sequence of parameters needed to execute this command.

k. Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Part 2: Create VLANs and Assign Switch Ports

In Part 2, you will create VLANs, as specified in the table above, on both switches. You will then assign the VLANs to the appropriate interface. The **show vlan** command is used to verify your configuration settings. Complete the following tasks on each switch.

Step 1: Create VLANs on both switches.

a. Create and name the required VLANs on each switch from the table above.

b. Configure the management interface and default gateway on each switch using the IP address information in the Addressing Table.

c. Assign all unused ports on both switches to the ParkingLot VLAN, configure them for static access mode, and administratively deactivate them.

Note: The interface range command is helpful to accomplish this task with as few commands as necessary.

Step 2: Assign VLANs to the correct switch interfaces.

a. Assign used ports to the appropriate VLAN (specified in the VLAN table above) and configure them for static access mode. Be sure to do this on both switches

b. Issue the **show vlan brief** command and verify that the VLANs are assigned to the correct interfaces.

Part 3: Configure an 802.1Q Trunk Between the Switches

In Part 3, you will manually configure interface F0/1 as a trunk.

Step 1: Manually configure trunk interface F0/1.

a. Change the switchport mode on interface F0/1 to force trunking. Make sure to do this on both switches.

b. As a part of the trunk configuration, set the native VLAN to 8 on both switches. You may see error messages temporarily while the two interfaces are configured for different native VLANs.

c. As another part of trunk configuration, specify that VLANs 3, 4, and 8 are only allowed to cross the trunk.

d. Issue the **show interfaces trunk** command to verify trunking ports, the Native VLAN and allowed VLANs across the trunk.

Step 2: Manually configure S1’s trunk interface F0/5

a. Configure the F0/5 on S1 with the same trunk parameters as F0/1. This is the trunk to the router.

b. Save the running configuration to the startup configuration file on S1 and S2.

c. Issue the **show interfaces trunk** command to verify trunking.

Why does F0/5 not appear in the list of trunks?

S1 port 5 will not be displayed because the GigabitEthernet 0/0/1 interface status on the router is administratively down.

Part 4: Configure Inter-VLAN Routing on the Router

a. Activate interface G0/0/1 on the router.

b. Configure sub-interfaces for each VLAN as specified in the IP addressing table. All sub-interfaces use 802.1Q encapsulation. Ensure the sub-interface for the native VLAN does not have an IP address assigned. Include a description for each sub-interface.

c. Use the **show ip interface brief** command to verify the sub-interfaces are operational.

Part 5: Verify Inter-VLAN Routing is Working

Step 1: Complete the following tests from PC-A. All should be successful.

Note: You may have to disable the PC firewall for pings to be successful.

a. Ping from PC-A to its default gateway.

b. Ping from PC-A to PC-B

c. Ping from PC-A to S2

Step 2: Complete the following test from PC-B.

From the command prompt on PC-B, issue the tracert command to the address of PC-A.

What intermediate IP addresses are shown in the results?

The tracert output shows two entries in the results. The first hop is G0/0/1.4 on the R1 interface address, which is the Gateway address for PC-B. The second hop is PC-A's address.

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.