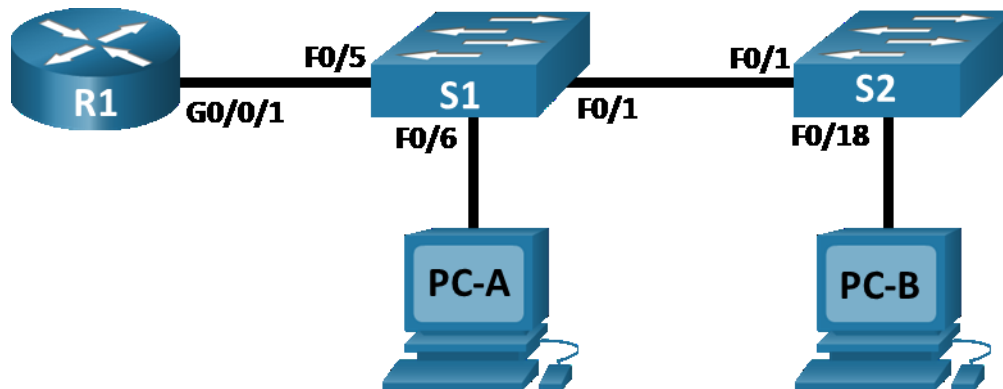


## Lab - Implement Inter-VLAN Routing

### Topology



### Addressing Table

| Device | Interface   | IP Address    | Subnet Mask   | Default Gateway |
|--------|-------------|---------------|---------------|-----------------|
| R1     | G0/0/1.10   | 192.168.10.1  | 255.255.255.0 | N/A             |
|        | G0/0/1.20   | 192.168.20.1  | 255.255.255.0 |                 |
|        | G0/0/1.30   | 192.168.30.1  | 255.255.255.0 |                 |
|        | G0/0/1.1000 | N/A           | N/A           |                 |
| S1     | VLAN 10     | 192.168.10.11 | 255.255.255.0 | 192.168.10.1    |
| S2     | VLAN 10     | 192.168.10.12 | 255.255.255.0 | 192.168.10.1    |
| PC-A   | NIC         | 192.168.20.3  | 255.255.255.0 | 192.168.20.1    |
| PC-B   | NIC         | 192.168.30.3  | 255.255.255.0 | 192.168.30.1    |

### VLAN Table

| VLAN | Name        | Interface Assigned   |
|------|-------------|--|
| 10   | Management  | S1: VLAN 10<br>S2: VLAN 10                                   |
| 20   | Sales       | S1: F0/6   |
| 30   | Operations  | S2: F0/18  |
| 999  | Parking_Lot | S1: F0/2-4, F0/7-24, G0/1-2<br>S2: F0/2-17, F0/19-24, G0/1-2 |
| 1000 | 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 improve network performance by separating large Layer 2 broadcast domains into smaller ones. VLANs can also be used as a security measure by separating sensitive data traffic from the rest of the network. 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. Adding an inter-VLAN router allows the organization to segregate and separate broadcast domains while simultaneously allowing them to communicate with each other.

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.

### 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. Set the clock on the switch.
- i. Save 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 and 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 the switch to the Parking\_Lot 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.

- Assign used ports to the appropriate VLAN (specified in the VLAN table above) and configure them for static access mode.
- 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 on switch S1 and S2.

- Configure static trunking on interface F0/1 for both switches.
- Set the native VLAN to 1000 on both switches.
- Specify that VLANs 10, 20, 30, and 1000 are allowed to cross the trunk.
- Verify trunking ports, the Native VLAN and allowed VLANs across the trunk.

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

- Configure S1's interface F0/5 with the same trunk parameters as F0/1. This is the trunk to the router.
- Save the running configuration to the startup configuration file.
- Verify trunking.

What happens if G0/0/1 on R1 is down?

## Part 4: Configure Inter-VLAN Routing on the Router

### Step 1: Configure the router.

- Activate interface G0/0/1 as necessary on the router.
- 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.
- Verify the sub-interfaces are operational

### Step 2: Complete the following tests from PC-A. All should be successful.

**Note:** You may have to disable the PC firewall for pings to work

- Ping from PC-A to its default gateway.
- Ping from PC-A to PC-B
- Ping from PC-A to S2

### Step 3: Complete the following test from PC-B

From the Command Prompt window on PC-B, issue the **tracert** command to the address of PC-A.

What intermediate IP addresses are shown in the results?

### Router Interface Summary Table

| Router Model | Ethernet Interface #1              | Ethernet Interface #2              | Serial Interface #1   | Serial Interface #2   |
|--------------|------------------------------------|------------------------------------|-----------------------|-----------------------|
| 1800         | Fast Ethernet 0/0<br>(F0/0)        | Fast Ethernet 0/1<br>(F0/1)        | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900         | Gigabit Ethernet 0/0<br>(G0/0)     | Gigabit Ethernet 0/1<br>(G0/1)     | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801         | Fast Ethernet 0/0<br>(F0/0)        | Fast Ethernet 0/1<br>(F0/1)        | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811         | Fast Ethernet 0/0<br>(F0/0)        | Fast Ethernet 0/1<br>(F0/1)        | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900         | Gigabit Ethernet 0/0<br>(G0/0)     | Gigabit Ethernet 0/1<br>(G0/1)     | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 4221         | Gigabit Ethernet 0/0/0<br>(G0/0/0) | Gigabit Ethernet 0/0/1<br>(G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 4300         | Gigabit Ethernet 0/0/0<br>(G0/0/0) | Gigabit Ethernet 0/0/1<br>(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.