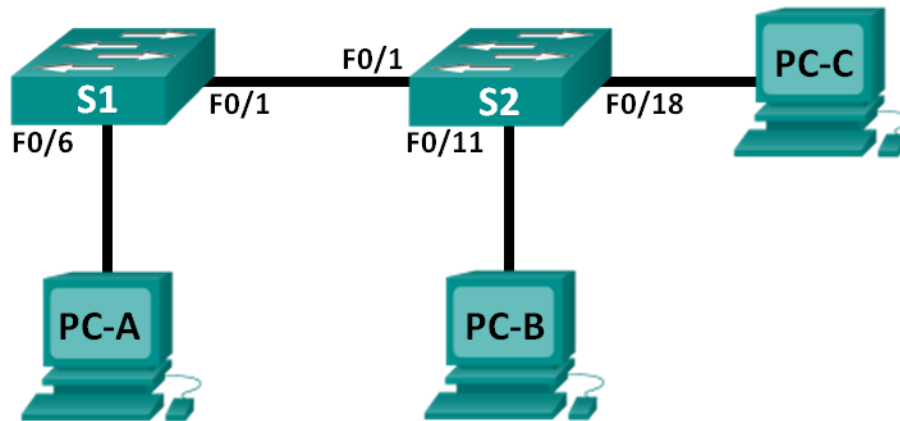


Lab - Troubleshooting VLAN Configurations

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
S2	VLAN 1	192.168.1.3	255.255.255.0	N/A
PC-A	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Switch Port Assignment Specifications

Ports	Assignment	Network
F0/1	802.1Q Trunk	N/A
F0/6-12	VLAN 10 – Students	192.168.10.0/24
F0/13-18	VLAN 20 – Faculty	192.168.20.0/24
F0/19-24	VLAN 30 – Guest	192.168.30.0/24

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot VLAN 10

Part 3: Troubleshoot VLAN 20

Background / Scenario

VLANs provide logical segmentation within an internetwork and improve network performance by separating large broadcast domains into smaller ones. By separating hosts into different networks, VLANs can be used

to control which hosts can communicate. In this lab, a school has decided to implement VLANs in order to separate traffic from different end users. The school is using 802.1Q trunking to facilitate VLAN communication between switches.

The S1 and S2 switches have been configured with VLAN and trunking information. Several errors in the configuration have resulted in connectivity issues. You have been asked to troubleshoot and correct the configuration errors and document your work.

Note: The switches used with this lab are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

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

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with 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

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the switches with some basic settings, such as passwords and IP addresses. Preset VLAN-related configurations, which contain errors, are provided for you for the initial switch configurations. You will also configure the IP settings for the PCs in the topology.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the switches as necessary.

Step 4: Configure basic settings for each switch.

- a. Disable DNS lookup.
- b. Configure IP address in Addressing Table.
- c. Assign **cisco** as the console and vty passwords and enable login for console and vty lines.
- d. Assign **class** as the privileged EXEC password.
- e. Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 5: Load switch configurations.

The configurations for the switches S1 and S2 are provided for you. There are errors within these configurations, and it is your job to determine the incorrect configurations and correct them.

Switch S1 Configuration:

```
hostname S1
vlan 10
name Students
vlan 2
```

```
!vlan 20
name Faculty
vlan 30
name Guest
interface range f0/1-24
switchport mode access
shutdown
interface range f0/7-12
switchport access vlan 10
interface range f0/13-18
switchport access vlan 2
interface range f0/19-24
switchport access vlan 30
end
```

Switch S2 Configuration:

```
hostname S2
vlan 10
Name Students
vlan 20
Name Faculty
vlan 30
Name Guest
interface f0/1
switchport mode trunk
switchport trunk allowed vlan 1,10,2,30
interface range f0/2-24
switchport mode access
shutdown
interface range f0/13-18
switchport access vlan 20
interface range f0/19-24
switchport access vlan 30
shutdown
end
```

Step 6: Copy the running configuration to the startup configuration.

Part 2: Troubleshoot VLAN 10

In Part 2, you must examine VLAN 10 on S1 and S2 to determine if it is configured correctly. You will troubleshoot the scenario until connectivity is established.

Step 1: Troubleshoot VLAN 10 on S1.

- a. Can PC-A ping PC-B?
- b. After verifying that PC-A was configured correctly, examine the S1 switch to find possible configuration errors by viewing a summary of the VLAN information. Enter the **show vlan brief** command.
- c. Are there any problems with the VLAN configuration?

Lab - Troubleshooting VLAN Configurations

- d. Examine the switch for trunk configurations using the **show interfaces trunk** and the **show interface f0/1 switchport** commands.
- e. Are there any problems with the trunking configuration?
- f. Examine the running configuration of the switch to find possible configuration errors.
Are there any problems with the current configuration?
- g. Correct the errors found regarding F0/1 and VLAN 10 on S1. Record the commands used in the space below.
- h. Verify the commands had the desired effects by issuing the appropriate **show** commands.
- i. Can PC-A ping PC-B?

Step 2: Troubleshoot VLAN 10 on S2.

- a. Using the previous commands, examine the S2 switch to find possible configuration errors.
Are there any problems with the current configuration?
- b. Correct the errors found regarding interfaces and VLAN 10 on S2. Record the commands below.
- c. Can PC-A ping PC-B?

Part 3: Troubleshoot VLAN 20

In Part 3, you must examine VLAN 20 on S1 and S2 to determine if it is configured correctly. To verify functionality, you will reassign PC-A into VLAN 20, and then troubleshoot the scenario until connectivity is established.

Step 1: Assign PC-A to VLAN 20.

- a. On PC-A, change the IP address to 192.168.20.2/24 with a default gateway of 192.168.20.1.
- b. On S1, assign the port for PC-A to VLAN 20. Write the commands needed to complete the configuration.

Lab - Troubleshooting VLAN Configurations

- c. Verify that the port for PC-A has been assigned to VLAN 20.
- d. Can PC-A ping PC-C?

Step 2: Troubleshoot VLAN 20 on S1.

- a. Using the previous commands, examine the S1 switch to find possible configuration errors.
Are there any problems with the current configuration?

- b. Correct the errors found regarding VLAN 20.
- c. Can PC-A ping PC-C?

Step 3: Troubleshoot VLAN 20 on S2.

- a. Using the previous commands, examine the S2 switch to find possible configuration errors.
Are there any problems with the current configuration?

- b. Correct the errors found regarding VLAN 20. Record the commands used below.

- c. Can PC-A ping PC-C?

Note: It may be necessary to disable the PC firewall to ping between PCs.

Reflection

1. Why is a correctly configured trunk port critical in a multi-VLAN environment?

2. Why would a network administrator limit traffic for specific VLANs on a trunk port?