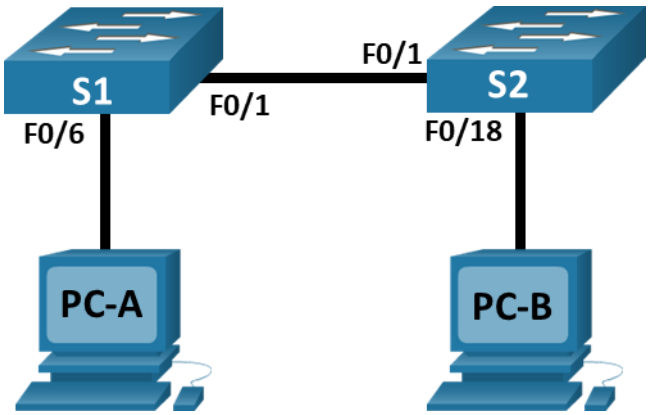
Lab - Basic Switch and End Device Configuration

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.1	255.255.255.0
S2	VLAN 1	192.168.1.2	255.255.255.0
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

Objectives

- Set Up the Network Topology
- Configure PC Hosts
- Configure and Verify Basic Switch Settings

Background / Scenario

In this lab, you will build a simple network with two hosts and two switches. You will also configure basic settings including hostname, local passwords, and login banner. Use **show** commands to display the running configuration, IOS version, and interface status. Use the **copy** command to save device configurations.

You will apply IP addressing for this lab to the PCs and switches to enable communication between the devices. Use the **ping** utility to verify connectivity.

Note: The switches used 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. Refer to Appendix A for the procedure to initialize and reload a switch.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 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

Instructions

Step 1: Set Up the Network Topology

In this step, you will cable the devices together according to the network topology.

a. Power on the devices.

b. Connect the two switches.

c. Connect the PCs to their respective switches.

d. Visually inspect network connections.

Step 2: Configure PC Hosts

a. Configure static IP address information on the PCs according to the Addressing Table.

b. Verify PC settings and connectivity.

Step 3: Configure and Verify Basic Switch Settings

a. Console into the switch. Enter the global configuration mode.

b. Give the switch a name according to the Addressing Table.

c. Prevent unwanted DNS lookups.

d. Enter local passwords. Use **class** as the privileged EXEC password and **cisco** as the password for console access.

e. Configure and enable the SVI according to the Addressing Table.

f. Enter a login MOTD banner to warn about unauthorized access.

g. Save the configuration.

h. Display the current configuration.

i. Display the IOS version and other useful switch information.

j. Display the status of the connected interfaces on the switch.

k. Configure switch S2.

l. Record the interface status for the following interfaces.

Interface	S1 Status	S1 Protocol	S2 Status	S2 Protocol
F0/1	Up	Up	Up	Up
F0/6	Up	Up	Down	Down
F0/18	Down	Down	Up	Up
VLAN 1	Up	Up	Up	Up

m. From a PC, ping S1 and S2. The pings should be successful.

n. From a switch, ping PC-A and PC-B. The pings should be successful.

Reflection Question

Why some FastEthernet ports on the switches are up and others are down?

The FastEthernet ports are usually up when cables are connected to them. Ports that have a cable connected to them can also be administratively taken down. Ports without cables can be administratively taken down to prevent those ports from being used by potentially unauthorized users.

What could prevent a ping from being sent between the PCs?

Many things could prevent a ping. For example, an incorrect IP address, a machine that is not turned on (router, switch, or PC), the cables being disconnected, firewall that blocks ICMP, or a port that has been administratively taken down.