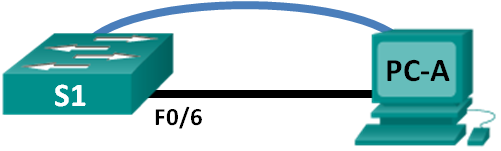
EE3009 Lab 2-1 (Sem B 2020/2021)

5.1.1.6 – Configuring Basic Switch Settings – PT

1. Topology



1. Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| S1 | VLAN 99 | 192.168.2.2 | 255.255.255.0 | 192.168.2.1 |
| PC-A | NIC | 192.168.2.10 | 255.255.255.0 | 192.168.2.1 |

1. Objectives

Part 1: Cable the Network and Verify the Default Switch Configuration

Part 2: Configure Basic Network Device Settings

* Configure basic switch settings.
* Configure the PC IP address.

Part 3: Verify and Test Network Connectivity

* Display device configuration.
* Test end-to-end connectivity with ping.
* Test remote management capabilities with Telnet.
* Save the switch running configuration file.

Part 4: Manage the MAC Address Table

* Record the MAC address of the host.
* Determine the MAC addresses that the switch has learned.
* List the **show mac address-table** command options.
* Set up a static MAC address.

1. Background / Scenario

Cisco switches can be configured with a special IP address known as the switch virtual interface (SVI). The SVI, or management address, can be used for remote access to the switch to display or configure settings. If the VLAN 1 SVI is assigned an IP address, by default all ports in VLAN 1 have access to the SVI IP address.

In this lab, you will build a simple topology using Ethernet LAN cabling and access a Cisco switch using the console and remote access methods. You will examine default switch configurations before configuring basic switch settings. These basic switch settings include device name, interface description, local passwords, IP addressing, and static MAC address. You will also demonstrate the use of a management IP address for remote switch management. The topology consists of one switch and one host using only Ethernet and console ports.

1. Cable the Network and Verify the Default Switch Configuration

In Part 1, you will set up the network topology and verify default switch settings.

* 1. Cable the network as shown in the topology. (Ethernet only)
  2. Verify the default switch configuration.

In this step, you will examine the default switch settings, such as current switch configuration, IOS information, interface properties, VLAN information, and flash memory.

You can access all the switch IOS commands in privileged EXEC mode. Access to privileged EXEC mode should be restricted by password protection to prevent unauthorized use because it provides direct access to global configuration mode and commands used to configure operating parameters. You will set passwords later in this lab.

The privileged EXEC mode command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes is gained. Use the **enable** command to enter privileged EXEC mode.

* + 1. Assuming the switch had no configuration file stored in nonvolatile random-access memory (NVRAM), A console connection using Tera Term or other terminal emulation program will place you at the user EXEC mode prompt on the switch with a prompt of Switch>. Use the **enable** command to enter privileged EXEC mode.

Switch> **enable**

Switch#

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Verify that there is a clean default configuration file on the switch by issuing the **show running-config** privileged EXEC mode command. If a configuration file was previously saved, it must be removed. Depending on the switch model and IOS version, your configuration may look slightly different. However, there should be no configured passwords or IP address. If your switch does not have a default configuration, erase and reload the switch.

**Note**: Appendix A details the steps to initialize and reload a switch.

* + 1. Examine the current running configuration file.

Switch# **show running-config**

How many FastEthernet interfaces does a 2960 switch have? \_\_\_\_\_\_\_\_

How many Gigabit Ethernet interfaces does a 2960 switch have? \_\_\_\_\_\_\_\_

What is the range of values shown for the vty lines? \_\_\_\_\_\_\_\_

* + 1. Examine the startup configuration file in NVRAM.

Switch# **show startup-config**

startup-config is not present

Why does this message appear? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Examine the characteristics of the SVI for VLAN 1.

Switch# **show interface vlan1**

Is there an IP address assigned to VLAN 1? \_\_\_\_\_\_\_\_

What is the MAC address of this SVI? Answers will vary. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Is this interface up?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Examine the IP properties of the SVI VLAN 1.

Switch#config t

Switch(config)#int vlan 1

Switch(config-if)#no shut

Switch(config-if)#end

Switch# **show ip interface vlan1**

What output do you see?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Connect an Ethernet cable from PC-A to port 6 on the switch and examine the IP properties of the SVI VLAN 1. Allow time for the switch and PC to negotiate duplex and speed parameters.

Switch# **show ip interface vlan1**

What output do you see?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Examine the Cisco IOS version information of the switch.

Switch# **show version**

What is the Cisco IOS version that the switch is running? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the system image filename? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the base MAC address of this switch? Answers will vary. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Examine the default properties of the FastEthernet interface used by PC-A.

Switch# **show interface f0/6**

Is the interface up or down? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What event would make an interface go up? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the MAC address of the interface? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the speed and duplex setting of the interface? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Examine the default VLAN settings of the switch.

Switch# **show vlan**

What is the default name of VLAN 1? \_\_\_\_\_\_\_\_\_\_\_\_

Which ports are in VLAN 1? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Is VLAN 1 active? \_\_\_\_\_\_\_\_\_\_\_\_

What type of VLAN is the default VLAN? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Examine flash memory.

Issue one of the following commands to examine the contents of the flash directory.

Switch# **show flash**

Switch# **dir flash:**

Files have a file extension, such as .bin, at the end of the filename. Directories do not have a file extension.

What is the filename of the Cisco IOS image? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Configure Basic Network Device Settings

In Part 2, you will configure basic settings for the switch and PC.

* 1. Configure basic switch settings.
     1. Copy the following basic configuration and paste it into S1 while in global configuration mode.

no ip domain-lookup

hostname S1

service password-encryption

enable secret class

* + 1. Set the SVI IP address of the switch. This allows remote management of the switch.

Before you can manage S1 remotely from PC-A, you must assign the switch an IP address. The default configuration on the switch is to have the management of the switch controlled through VLAN 1. However, a best practice for basic switch configuration is to change the management VLAN to a VLAN other than VLAN 1.

For management purposes, use VLAN 99. The selection of VLAN 99 is arbitrary and in no way implies that you should always use VLAN 99.

First, create the new VLAN 99 on the switch. Then set the IP address of the switch to 192.168.2.2 with a subnet mask of 255.255.255.0 on the internal virtual interface VLAN 99.

S1# **configure terminal**

S1(config)# **vlan 99**

S1(config-vlan)# **exit**

S1(config)# **interface vlan99**

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down

S1(config-if)# **ip address 192.168.2.2 255.255.255.0**

S1(config-if)# **no shutdown**

S1(config-if)# **exit**

S1(config)#

Notice that the VLAN 99 interface is in the down state even though you entered the **no shutdown** command. The interface is currently down because no switch ports are assigned to VLAN 99.

* + 1. Assign all user ports to VLAN 99.

S1(config)# **interface range f0/1 – 24,g0/1 - 2**

S1(config-if-range)# **switchport access vlan 99**

S1(config-if-range)# **exit**

S1(config)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

To establish connectivity between the host and the switch, the ports used by the host must be in the same VLAN as the switch. Notice in the above output that the VLAN 1 interface goes down because none of the ports are assigned to VLAN 1. After a few seconds, VLAN 99 comes up because at least one active port (F0/6 with PC-A attached) is now assigned to VLAN 99.

* + 1. Issue the **show vlan brief** command to verify that all ports are in VLAN 99.

S1# **show vlan brief**

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active

99 VLAN0099 active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

Gi0/1, Gi0/2

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

* + 1. Configure the default gateway for S1. If no default gateway is set, the switch cannot be managed from a remote network that is more than one router away. Although this activity does not include an external IP gateway, assume that you will eventually connect the LAN to a router for external access. Assuming that the LAN interface on the router is 192.168.2.1, set the default gateway for the switch.

S1(config)# **ip default-gateway 192.168.2.1**

S1(config)#

* + 1. Console port access should also be restricted. The default configuration is to allow all console connections with no password needed. To prevent console messages from interrupting commands, use the **logging synchronous** option.

S1(config)# **line con 0**

S1(config-line)# **password conpass**

S1(config-line)# **login**

S1(config-line)# **logging synchronous**

S1(config-line)# **exit**

S1(config)#

* + 1. Configure the virtual terminal (vty) lines for the switch to allow Telnet access. If you do not configure a vty password, you will not be able to Telnet to the switch.

S1(config)# **line vty 0 15**

S1(config-line)# **password vtypass**

S1(config-line)# **login**

S1(config-line)# **end**

S1#

\*Mar 1 00:06:11.590: %SYS-5-CONFIG\_I: Configured from console by console

Why is the **login** command required? **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* 1. Configure an IP address on PC-A.

Assign the IP address and subnet mask to the PC as shown in the Addressing Table. A default gateway is not required for this topology; however, you can enter **192.168.2.1** to simulate a router attached to S1.

1. Verify and Test Network Connectivity

In Part 3, you will verify and document the switch configuration, test end-to-end connectivity between PC-A and S1, and test the switch’s remote management capability.

* 1. Display the switch configuration.

Use the console connection on PC-A to display and verify the switch configuration. The **show run** command displays the entire running configuration, one page at a time. Use the spacebar to advance paging.

* + 1. A sample configuration is shown here. The settings you configured are highlighted in yellow. The other configuration settings are IOS defaults.

S1# **show run**

Building configuration...

Current configuration : 2206 bytes

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname S1

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

system mtu routing 1500

!

!

no ip domain-lookup

!

**<output omitted>**

!

interface FastEthernet0/24

switchport access vlan 99

!

interface GigabitEthernet0/1

switchport access vlan 99

!

interface GigabitEthernet0/2

switchport access vlan 99

!

interface Vlan1

no ip address

no ip route-cache

!

interface Vlan99

ip address 192.168.2.2 255.255.255.0

no ip route-cache

!

ip default-gateway 192.168.2.1

ip http server

ip http secure-server

!

line con 0

password 7 104D000A0618

logging synchronous

login

line vty 0 4

password 7 14141B180F0B

login

line vty 5 15

password 7 14141B180F0B

login

!

end

S1#

* + 1. Verify the management VLAN 99 settings.

S1# **show interface vlan 99**

Vlan99 is up, line protocol is up

Hardware is EtherSVI, address is 0cd9.96e2.3d41 (bia 0cd9.96e2.3d41)

Internet address is 192.168.2.2/24

MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00

Last input 00:00:06, output 00:08:45, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

175 packets input, 22989 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicast)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

1 packets output, 64 bytes, 0 underruns

0 output errors, 0 interface resets

0 output buffer failures, 0 output buffers swapped out

What is the bandwidth on this interface? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the VLAN 99 state? \_\_\_\_\_\_\_\_\_

What is the line protocol state? \_\_\_\_\_\_\_\_\_

* 1. Test end-to-end connectivity with ping.
     1. From the command prompt on PC-A, ping the address of PC-A first.

C:\> **ping 192.168.2.10**

* + 1. From the command prompt on PC-A, ping the SVI management address of S1.

C:\> **ping 192.168.2.2**

Because PC-A needs to resolve the MAC address of S1 through ARP, the first packet may time out. If ping results continue to be unsuccessful, troubleshoot the basic device configurations. Check both the physical cabling and logical addressing.

* 1. Test and verify remote management of S1.

You will now use Telnet to remotely access the switch. In this lab, PC-A and S1 reside side by side. In a production network, the switch could be in a wiring closet on the top floor while your management PC is located on the ground floor. In this step, you will use Telnet to remotely access switch S1 using its SVI management address. Telnet is not a secure protocol; however, you will use it to test remote access. With Telnet, all information, including passwords and commands, are sent across the session in plain text. In subsequent labs, you will use SSH to remotely access network devices.

* + 1. Telnet to S1 via the SVI management address. The password is **vtypass**.

**At “Desktop” of PC-A , select Telnet and the host ip is 192.168.2.2**

* + 1. After entering the password **vtypass**, you will be at the user EXEC mode. Access privileged EXEC mode using the **enable** command and providing the secret password **class**.
    2. If not successful, troubleshoot.
    3. End the Telnet session.
  1. Save the switch running configuration file.

Save the configuration.

S1# **copy running-config startup-config**

Destination filename [startup-config]? **[Enter]**

Building configuration...

[OK]

S1#

1. Manage the MAC Address Table

In Part 4, you will determine the MAC addresses that the switch has learned, set up a static MAC address on one interface of the switch, and then remove the static MAC address from that interface.

* 1. Record the MAC address of the host.

Open a command prompt on PC-A and issue the **ipconfig /all** command to determine and record the Layer 2 (physical) addresses of the NIC.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Determine the MAC addresses that the switch has learned.

Display the MAC addresses using the **show mac address-table** command.

S1# **show mac address**

How many dynamic addresses are there? \_\_\_\_\_\_\_\_\_\_\_\_

How many MAC addresses are there in total? \_\_\_\_\_\_\_\_\_\_\_\_

Does the dynamic MAC address match the MAC address of PC-A? \_\_\_\_\_\_\_\_\_\_\_\_

* 1. List the show mac address-table options.
     1. Display the MAC address table options.

S1# **show mac address ?**

How many options are available for the **show mac address** command? \_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Issue the **show mac address-table dynamic** command to display only the MAC addresses that were learned dynamically.

S1# **show mac address dynamic**

How many dynamic addresses are there? \_\_\_\_\_\_\_\_\_\_\_\_

* 1. Set up a static MAC address.
     1. Set up a static MAC address.

To specify which ports a host can connect to, one option is to create a static mapping of the host MAC address to a port.

Set up a static MAC address on F0/6 using the address that was recorded for PC-A in Part 4, Step 1. The MAC address 0050.56BE.6C89 is used as an example only. You must use the MAC address of PC-A, which is different than the one given here as an example.

S1(config)# **mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/6**

* + 1. Verify the MAC address table entries.

S1# **show mac address-table**

How many total MAC addresses are there? \_\_\_\_\_\_\_\_\_\_

How many static addresses are there? \_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Remove the static MAC entry. Enter global configuration mode and remove the command by putting a **no** in front of the command string.

**Note**: The MAC address **000B.BE33.B95B** is used in the example only. Use the MAC address for PC-A.

S1(config)# **no mac address-table static 000B.BE33.B95B vlan 99 interface fastethernet 0/6**

* + 1. Verify that the static MAC address has been cleared.

S1# **show mac address**

How many total static MAC addresses are there? \_\_\_\_\_\_\_\_\_\_\_\_

1. ☞ Save your Packet Tracer file and upload to Canvas.