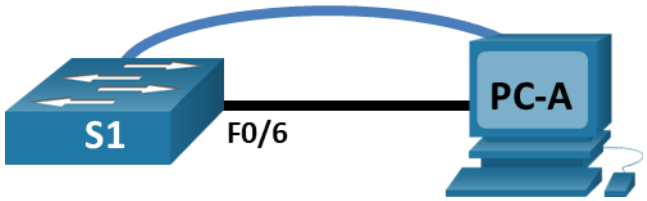
Shaun Lim
Aldrich Go
Dave Bolima
Amienz Arago

Lab 2.1 - Basic Switch Configuration

Topology



Addressing Table

Device	Interface	IP Address / Prefix
S1	VLAN 1	192.168.1.2 /24
PC-A	NIC	192.168.1.10 /24

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 SSH.

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.

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, message of the day (MOTD) banner, 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.

Required Resources

- 1 Switch (Cisco 2960)
- 1 PC
- 1 Console cable to configure the Cisco IOS device via the console port
- 1 Ethernet cable as shown in the topology

Part 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.

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

a. Connect the console cable as shown in the topology. **Do not connect the PC-A Ethernet cable at this time.**

b. Connect to the switch from PC-A using the terminal emulation program from its desktop.

Why must you use a console connection to initially configure the switch? Why is it not possible to connect to the switch via Telnet or SSH?

Since the switch is not yet configured, we cannot use Telnet or SSH, since these two protocols need an IP address and protocol configured already.

Step 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.

a. Assuming the switch had no configuration file stored in nonvolatile random-access memory (NVRAM), A console connection using a 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.

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

b. Examine the current running configuration file using the command **show running-configuration**.

How many FastEthernet interfaces does a 2960 switch have?	24
How many Gigabit Ethernet interfaces does a 2960 switch have?	2
What is the range of values shown for the vty lines?	0-15

a. Examine the startup configuration file in NVRAM using the command **show startup-configuration**.

Why does this message appear?

The message “startup-config is not present” is there because we haven’t saved any configuration yet to the NVRAM.

b. Examine the characteristics of the SVI for VLAN 1 using the command **show interface vlan 1**.

Is there an IP address assigned to VLAN 1?	no
What is the MAC address of this SVI?	0024.9850.db40
Is this interface up?	No

a. Examine the IP properties of the SVI VLAN 1.

What interface and IP processing status do you see?

There is none yet

b. Connect a straight-through 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. Use the command **show interface vlan 1** again

What interface status do you see this time?

Vlan1 is up, line protocol is up

c. Examine the Cisco IOS version information of the switch using the command **show version**.

What is the Cisco IOS version that the switch is running?	Version 15.0(2)SE4

What is the system image filename?	flash:c2960-lanbasek9-mz.150-2.SE4/c2960-lanbasek9-mz.150-2.SE4.bin"
What is the base MAC address of this switch?	00:24:98:50:DB:00

d. Examine the default properties of the FastEthernet interface used by PC-A.

```
Switch# show interface f0/6
```

Is the interface up or down?	Up (FastEthernet0/6 is up, line protocol is up (connected))
What is the MAC address of the interface?	0024.9850.db06
What is the speed and duplex setting of the interface?	Full-duplex, 100Mb/s, media type is 10/100BaseTX

What event would make an interface go up?

The interface must be administratively up and there should be a physical connection to a port.

e. Temporarily disconnect PC-A from S1 and reconnect it to Fa0/6 using a crossover cable. Reexamine the status of Fa0/6

Is the interface up or down?	Up

Why can the switch successfully establish an active link with PC-A regardless if using it's connected using a straight-through or crossover cable?

Because the switch has auto-mdix.

f. Examine the default VLAN settings of the switch using the command **show vlan**.

What is the default name of VLAN 1?	default

Which ports are in VLAN 1?	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
What type of VLAN is the default VLAN?	enet
Is VLAN 1 active?	Yes

g. 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?	c2960-lanbasek9-mz.150-2.SE4

Part 2: Configure Basic Network Device Settings

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

Step 1: Configure basic switch settings.

g. Enter global configuration mode on S1. 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
banner motd #
Unauthorized access is strictly prohibited. #
```

h. 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.

Set the IP address of the switch to 192.168.1.2 with a subnet mask of 255.255.255.0 on the internal virtual interface

i. 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 192.168.1.1, set the default gateway for the switch.

j. Enable SSH for remote management of the S1. Configure the domain name to be **ITNET.edu.ph** and create an RSA key for encrypting data. When prompted, set the key length to **1024** bits.

```
S1(config)# ip domain-name ITNET.edu.ph
S1(config)# crypto key generate rsa
The name for the keys will be: S1.ITNET.edu.ph
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:1024
```

k. Create a local user account. Set the user name to **administrator** with **cisco** as the secret password. This will be later used as login credentials when doing remote management on the switch through its VTY lines

```
S1(config)# username administrator secret cisco
```

l. Configure the VTY lines to check the local username database for login credentials and to only allow SSH for remote access.

```
S1(config)# line vty 0 15
S1(config-line)# login local
S1(config-line)# transport input ssh
```

m. Console port access should also be restricted with a password. Use **cisco** as the console login password in this activity. 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)# logging synchronous
```

Step 2: Configure an IP address on PC-A.

Assign the IP address and subnet mask to the PC as shown in the Addressing Table. An abbreviated version of the procedure is described here. A default gateway is not required for this topology; however, you can enter **192.168.1.1** to simulate a router attached to S1.

1) Navigate to the **IP Configuration** menu.
2) Under the **IP Configuration** pane, set the addressing method to **Static**.
3) Enter the specified IP address and subnet mask settings of PC-A and close the menu.

Part 3: 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.

Step 3: 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.

Step 4: Test end-to-end connectivity with ping.

g. From the command prompt on PC-A, ping the address of PC-A first.

```
C:\> ping 192.168.1.10
```

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

```
C:\> ping 192.168.1.2
```

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.

Step 5: Test and verify remote management of S1.

You will now use SSH 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 SSH to remotely access switch S1 using its SVI management address.

g. Open the command prompt of PC-A from its desktop.

h. Attempt to log in using SSH.

Open another PuTTY session using SSH as the connection type. Input the IP address of the switch and click Open to begin

i. When prompted, enter the administrator username for ‘login as’ then the password

j. Upon successful login, enter privileged EXEC mode and save the configuration.

k. Type **exit** to end the SSH session.

Part 4: 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.

Step 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.

Step 2: Determine the MAC addresses that the switch has learned.

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

```
S1# show mac address-table
```

How many dynamic addresses are there?	1
How many MAC addresses are there in total?	21
Does the dynamic MAC address match the MAC address of PC-A?	Yes

Step 3: List the show mac address-table options.

a. Display the MAC address table options.

```
S1# show mac address-table ?
```

How many options are available for the **show mac address-table** command?	13

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

```
S1# show mac address-table dynamic
```

How many dynamic addresses are there?	1

Step 4: Set up a static MAC address.

a. Clear the MAC address table.

To remove the existing MAC addresses, use the **clear mac address-table dynamic** command in privileged EXEC mode.

```
S1# clear mac address-table dynamic
```

b. Verify that the MAC address table was cleared.

```
S1# show mac address-table
```

How many static addresses are there?	20
How many dynamic addresses are there?	1

c. Ping the VLAN 1 IP address of the switch from PC-A, and then repeat the **show mac address-table** command

```
S1# show mac address-table
```

How many dynamic addresses are there?	1

Why did this change from the last display?

It did not change because we used an SSH connection. If we used the console cable connection, it would be 0.

d. 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 1 interface
fastethernet 0/6
```

e. Verify the MAC address table entries.

```
S1# show mac address-table
```

How many MAC addresses are there in total?	21
How many static addresses are there?	21

f. 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 0050.56BE.6C89 is used in the example only. Use the MAC address for PC-A.

```
S1(config)# no mac address-table static 0050.56BE.6C89 vlan 1 interface
fastethernet 0/6
```

g. Verify that the static MAC address has been cleared.

```
S1# show mac address-table
```

How many total static addresses are there?	20

Reflection Questions

1. Why is it recommended to enable the management interface of the switch even if it can be configured using a console cable anyway?

   The console cable only allows for a direct connection and accessing it if it does not have prior configurations. However, enabling the management interface of the switch allows remote access to the switch, allowing for greater flexibility.

2. Why should SSH be used instead of Telnet for remote management of network devices?

   SSH is more secure than Telnet since Telnet is only plain-text while SSH is encrypted.

3. Why configure a static MAC address on a port interface?

   To specify which ports a host can connect to, meaning it can distinguish from “fake” mac addresses that could potentially be from malicious sources.

Appendix A: Initialize and Reload a Switch

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

```
Switch> enable
Switch#
```

b. Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash
Directory of flash:/

    2  -rwx        1919   Mar 1 1993 00:06:33 +00:00  private-config.text
    3  -rwx        1632   Mar 1 1993 00:06:33 +00:00  config.text
    4  -rwx       13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
    6  -rwx         616   Mar 1 1993 00:07:13 +00:00  vlan.dat

32514048 bytes total (20886528 bytes free)
```

c. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

d. You are prompted to verify the filename. If you have entered the name correctly, press Enter; otherwise, you can change the filename.

You are prompted to confirm deletion of this file. Press Enter to confirm.

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

e. Use the **erase startup-config** command to erase the startup configuration file from NVRAM. You are prompted to remove the configuration file. Press Enter to confirm.

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

f. Reload the switch to remove any old configuration information from memory. You will then receive a prompt to confirm reloading of the switch. Press Enter to proceed.

```
Switch# reload
Proceed with reload? [confirm]
```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Respond by typing **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

g. After the switch reloads, you should see a prompt to enter the initial configuration dialog. Respond by entering **no** at the prompt and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```