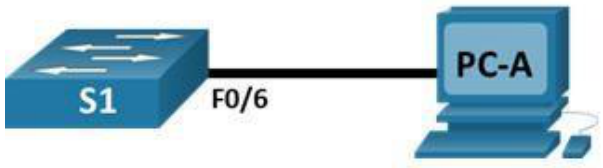
Lab 1.1.7 - Basic Switch Configuration

This lab has been updated for use on NETLAB+.
www.netdevgroup.com

Topology



Addressing Table

Device	Interface	IP Address / Prefix
S1	VLAN 99	192.168.1.2 /24
		2001:db8:acad::2 /64
		fe80::2
PC-A	NIC	192.168.1.10 /24
		2001:db8:acad::3 /64
		fe80::3

Objectives

Part 1: 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. **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 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.

The **default bias** template used by the Switch Database Manager (SDM) does not provide IPv6 address capabilities. Verify that SDM is using either the **dual-ipv4-and-ipv6** template or the **lanbase-routing** template. The new template will be used after reboot even if the configuration is not saved.

```
S1# show sdm prefer
```

Use the following commands to assign the **dual-ipv4-and-ipv6** template as the default SDM template.

```
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

Part 1: Verify the Default Switch Configuration

In Part 1, you will verify default switch settings.

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

a. At this time, it is important to keep PC-A disconnected from the network. Do not activate interface F0/6 on S1 at this time. This has the same effect as not connecting PC-A to S1.

b. Click on the Switch to access the Console port in order to initially configure the switch.

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.

a. Examine the current running configuration file.

How many FastEthernet interfaces does a 2960 switch have?

24

How many Gigabit Ethernet interfaces does a 2960 switch have?

2

b. Use the **show interface vlan 1** command to examine the characteristics of the SVI for VLAN 1.

Is there an IP address assigned to VLAN 1?

no

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

001e.147c.2dc0

Is this interface up?

yes

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

What output do you see?

no output

d. In configuration mode, activate interface F0/6 on S1 with a **no shutdown** command. This effectively connects PC-A to switch S1, and then examine the IP properties of the SVI VLAN 1. Allow time for the switch and PC to negotiate duplex and speed parameters.

What output do you see?

interface resets

e. From privileged exec mode, run the **show version** command to examine the Cisco IOS version information of the switch.

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

Version 15.0

What is the system image filename?

flash:/c2960-lanbasek9-mz.150-2.SE4.bin

What is the base MAC address of this switch?
00:1E:14:7C:2D:80

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

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

Is the interface up or down?

Up

What is the MAC address of the interface?

001e.147c.2d86

g. Using the **show vlan** command, examine the default VLAN settings of the switch.

What is the default name of VLAN 1?

default

Which ports are in VLAN 1?

All of them

Is VLAN 1 active?

Yes

What type of VLAN is the default VLAN?

enet

h. 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?

.bin

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.

a. 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. #
```

b. 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. In global configuration mode, enter **vlan 99** to create the vlan. Enter the command **name Management** to give the VLAN a name.

Then 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 VLAN 99. IPv6 address can also be configured on the SVI interface. Use the IPv6 addresses listed in the Addressing Table.

See 1.1.6 in the reading for examples on how to set the IP address on VLAN 99.

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.

c. Assign all user ports to VLAN 99. *An example command of how to do this is found in 3.3.5 in the reading*. To save time, use the range command to assign all the ports at once to VLAN 99. This command would be **interface range f0/1-24,g0/1-2** then issue the commands:

switchport mode access

switchport access vlan 99

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.VLAN 1 interface goes down because none of the ports are assigned to VLAN 1.

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

e. Configure the default gateway for S1 using the command **ip default gateway 192.168.1.1** 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.

f. 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
```

g. 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.

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** and **fe80::1** to simulate a router attached to S1.

1) Navigate to the **Control Panel**.

2) In the Category view, select **View network status and tasks**.

3) Click **Change adapter settings** on the left panel.
4) Right-click an **Ethernet** interface, and choose **Properties**.
5) Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
6) Click the **Use the following IP address** radio button and enter the IP address and subnet mask and click **OK**.
7) Select **Internet Protocol Version 6 (TCP/IPv6)** and click **Properties**.
8) Click the **Use the following IPv6 address** radio button and enter the IPv6 address and prefix and click **OK** to continue
9) Click **OK** to exit the Properties window.

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 1: Display the switch configuration.

Click on the switch to access the console port 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.

a. 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 15.2 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 5 $1$mtvC$6NC.1VKr3p6bj7YGE.jNg0
!
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 192.168.1.2
255.255.255.0 ipv6 address FE80::2
link-local ipv6 address
2001:DB8:ACAD::2/64 ! ip default-
gateway 192.168.1.1
 ip http server ip http secure-
server !
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password 7
 00071A150754 logging
 synchronous login
line vty 0 4
 password 7
 121A0C041104 login
line vty 5 15
 password 7
121A0C041104 login !
end
```

b. Verify the management VLAN 99 settings.

```
S1# show interface vlan 99
```

What is the bandwidth on this interface?

1000000

What is the VLAN 99 state?

up

What is the line protocol state?

up

Step 2: Test end-to-end connectivity with ping.

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

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

b. 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 3: 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 this step, you will use Telnet to remotely access switch S1 using its SVI management address. In subsequent labs, you will use SSH to remotely access network devices.

a. From PC1, open Tera Term.

b. Select the Telnet service and enter the SVI management address of S1 as the target. The password is **cisco**.

c. After entering the password **cisco**, you will be at the user EXEC mode prompt. Access privileged EXEC mode using the **enable** command and providing the secret password **class**.

d. Save the configuration.

e. Type **exit** to end the Telnet 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. ***Type your answers here.***

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?

2

How many MAC addresses are there in total?

20

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

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

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

c. View the MAC address entry for PC-A. The MAC address formatting for the command is xxxx.xxxx.xxxx.

```
S1# show mac address-table address <PC-A MAC here>
```

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 MAC addresses are there?

20

How many dynamic addresses are there?

1

c. Examine the MAC table again.

More than likely, an application running on PC-A has already sent a frame out the NIC to S1. Look at the MAC address table again in privileged EXEC mode to see if S1 has relearned the MAC address of PC-A.

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

How many dynamic addresses are there?

2

Why did this change from the last display?

Because the connection between them allows the pc to send out signals and that allows the mac address to be optained

If S1 has not yet relearned the MAC address for PC-A, ping the VLAN 99 IP address of the switch from PC-A, and then repeat the **show mac address-table** command.

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 99 interface
fastethernet 0/6
```

e. Verify the MAC address table entries.

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

How many total MAC addresses are there?

23

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 99 interface
fastethernet 0/6
```

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

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

How many total static MAC addresses are there?

22

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>
```

Router and Switch Interface Summary Table

Router / Switch Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Router / Switch Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
2960	Fast Ethernet 0/1 (F0/1)	Fast Ethernet 0/2 (F0/2)	n/a	n/a
3560	Fast Ethernet 0/1 (F0/1)	Fast Ethernet 0/2 (F0/2)	n/a	n/a
3650	Gigabit Ethernet 1/0/1 (G1/0/1)	Gigabit Ethernet 1/0/2 (G1/0/2)	n/a	n/a
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (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.