Experiment No. 4

VERIFY AND TEST NETWORK CONNECTIVITY

OBJECTIVE:

Part 1:

- Cable the Network and Verify the Default Switch Configuration

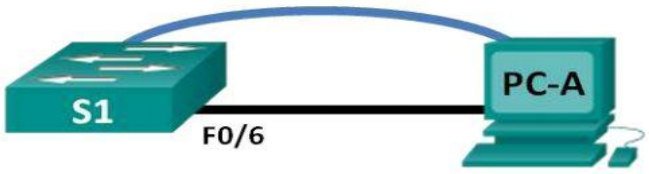
Part 2:

- 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.

TOPOLOGY:



ADDRESSTING TABLE:

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

BACKGROUND SCENARIO:

Cisco switches can be configured with a special IP address known as 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 management 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, and message of the day (MOTD) banner, IP addressing, setting up a static MAC address, and demonstrating 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.

Note: Make sure that the switch has been erased and has no startup configuration. Refer to Appendix A for the procedures to initialize and reload devices.

REQUIRED RESOURCES:

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term, and Telnet capability)
- Console cable to configure the Cisco IOS device via the console port
- Ethernet cable as shown in the topology

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

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

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

Step 2: Verify the default switch configuration.

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), you will be 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 a clean configuration file with the show running-config privileged EXEC mode command. If a configuration file was previously saved, it must be removed. Depending on 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.

b. 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?

c. Examine the startup configuration file in NVRAM.

Switch# show startup-config

startup-config is not present, Why does this message appear?

d. 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?

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

Switch# show ip interface vlan1

What output do you see?

f. Connect PC-A Ethernet cable 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?

g. 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?

h. 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?

i. Examine the default VLAN settings of the switch.

Switch# show vlan

What is the default name of VLAN 1?
Which ports are in this VLAN?
Is VLAN 1 active?
What type of VLAN is the default VLAN?

j. 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?

Part 2: Configure Basic Network Device Settings

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

Step 1: Configure basic switch settings including hostname, local passwords, MOTD banner, management address, and Telnet access.

a. Assuming the switch had no configuration file stored in NVRAM, verify you are at privileged EXEC mode.
Enter enable if the prompt has changed back to Switch>.

Switch> enable
Switch#

b. Enter global configuration mode.

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#

The prompt changed again to reflect global configuration mode.

c. Assign the switch hostname.

Switch(config)# hostname S1
S1(config)#

d. Configure password encryption.

S1(config)# service password-encryption
S1(config)#

e. Assign class as the secret password for privileged EXEC mode access.

S1(config)# enable secret class
S1(config)#

f. Prevent unwanted DNS lookups.

S1(config)# no ip domain-lookup
S1(config)#

g. Configure a MOTD banner.

S1(config)# banner motd #

Enter Text message. End with the character '#'. Unauthorized access is strictly prohibited. #

h. Verify your access settings by moving between modes.

S1(config)# exit
S1# exit

S1 con0 is now available
Press RETURN to get started.
Unauthorized access is strictly prohibited.

S1>

i. Go back to privileged EXEC mode from user EXEC mode. Enter class as the password when prompted.

S1> enable
Password:
S1#

Note: The password does not display when entering.

j. Enter global configuration mode to 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 192.168.1.2 with 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 192.168.1.2 255.255.255.0
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.

k. 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.

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

S1# show vlan brief

m. Configure the IP default gateway for S1.

S1(config)# ip default-gateway 192.168.1.1
S1(config)#

n. 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 cisco
S1(config-line)# login
S1(config-line)# logging synchronous
S1(config-line)# exit
S1(config)#

o. Configure the virtual terminal (vty) lines for the switch to allow Telnet access. If you do not configure a vty password, you are unable to telnet to the switch.

S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#

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) Click the Windows Start icon > Control Panel.
2) Click View By: and choose Small icons.
3) Choose Network and Sharing Center > Change adapter settings.
4) Select Local Area Network Connection, right click and choose Properties.
5) Choose Internet Protocol Version 4 (TCP/IPv4) > Properties.
6) Click the Use the following IP address radio button and enter the IP address and subnet mask.

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.

S1# show run

b. Verify the management VLAN 99 settings.

S1# show interface vlan 99

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

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

C:\Users\User1> ping 192.168.1.10

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

C:\Users\User1> ping 192.168.1.2

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 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. Note: If you are using Windows 7, the administrator may need to enable the Telnet protocol. To install the Telnet client, open a cmd window and type pkgmgr /iu:"TelnetClient". An example is shown below.

C:\Users\User1> pkgmgr /iu:"TelnetClient"

a. With the cmd window still open on PC-A, issue a Telnet command to connect to S1 via the SVI management address. The password is cisco.

C:\Users\User1> telnet 192.168.1.2

b. After entering the password cisco, you will be at the user EXEC mode prompt. Access privileged EXEC mode.

c. Type exit to end the Telnet session.

Step 4: Save the switch running configuration file.

Save the configuration.

S1# copy running-config startup-config

Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
S1#

CONCLUSION & COMMENTS: