

# Lab – Exploring Cisco IOS and Configuring Basic Switch Settings

## Topology



## Addressing 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

## 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.

### Part 5 : Configure and Verify SSH Access on S1

### Part 6 : Configure Router as Gateway for Switch network

### Part 7 : Configure and Verify Security Features on S1

## Background / Scenario

Cisco switches can be configured with a special IP address known as Switched 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.

## Lab – Exploring Cisco IOS and Configuring Basic Switch Settings

---

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, 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.

### 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. Cable the console connection as shown in the topology. Do not connect the PC-A Ethernet cable at this time.
- b. Create a console connection to the switch from PC-A using Putty. In Ubuntu Open a Terminal windows and type **gksudo putty** – Enter password and Putty GUI will appear.

#### 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.

If there is a configuration saved in NVRAM on the router or switch you should initialize the router/switch using the following procedure.

#### NOTE:

If you are prompted to enter initial dialog configuration that means there is no saved configuration and you DO NOT need to initialise the router/switch.

### Initializing and Reloading a Router and Switch

#### Step 1: Initialize and reload the router.

- a. Console into the router and enable privileged EXEC mode.

```
Router> enable
Router#
```

- b. Enter the **erase startup-config** command to remove the startup configuration from NVRAM.

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

## Lab – Exploring Cisco IOS and Configuring Basic Switch Settings

---

- c. Issue the **reload** command to remove an old configuration from memory. When prompted to Proceed with reload?, press Enter. (Pressing any other key aborts the reload.)

```
Router# reload
Proceed with reload? [confirm]
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

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

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

- d. After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press Enter.

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

- e. Another prompt asks to terminate autoinstall. Respond by typing **yes** press Enter.

```
Would you like to terminate autoinstall? [yes]: yes
```

### Step 2: Initialize and reload the 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)
Switch#
```

- 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.

- e. You are prompted to confirm to delete this file. Press Enter to confirm.

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

- f. 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#
```

## Lab – Exploring Cisco IOS and Configuring Basic Switch Settings

---

- g. Reload the switch to remove any old configuration information from memory. You will then receive a prompt to confirm to reload 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
```

- h. 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>
```

### Verify the default switch configuration

- 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
```

- c. Examine the startup configuration file in NVRAM.

```
Switch# show startup-config
startup-config is not present
```

Why do you think this message appears?

- d. Examine the characteristics of the SVI for VLAN 1.

```
Switch# show interface vlan1
```

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

```
Switch# show ip interface vlan1
```

- 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
```

- g. Examine the Cisco IOS version information of the switch.

```
Switch# show version
```

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

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

- i. Examine the default VLAN settings of the switch.

```
Switch# show vlan
```

## Lab – Exploring Cisco IOS and Configuring Basic Switch Settings

---

- 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.

## Part 2: Configure Basic Network Device Settings

In Part 2, you 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.

In this step, you will configure the PC and basic switch settings, such as hostname and an IP address for the switch management SVI. Assigning an IP address on the switch is only the first step. As the network administrator, you must specify how the switch is managed. Telnet and SSH are the two most common management methods. However, Telnet is not a secure protocol. All information flowing between the two devices is sent in plain text. Passwords and other sensitive information can be easily looked at if captured by a packet sniffer.

- 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#
```

- 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.

- Assign the switch hostname.

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

- Configure password encryption.

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

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

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

- Prevent unwanted DNS lookups.

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

- Configure a MOTD banner.

```
S1(config)# banner motd #
Enter Text message. End with the character `#'.
Unauthorized access is strictly prohibited. #
```

- Verify your access settings by moving between modes.

```
S1(config)# exit
S1#
*Mar  1 00:19:19.490: %SYS-5-CONFIG_I: Configured from console by console
S1# exit
S1 con0 is now available
Press RETURN to get started.
Unauthorized access is strictly prohibited.
S1>
```

## Lab – Exploring Cisco IOS and Configuring Basic Switch Settings

---

- 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 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 192.168.1.2 255.255.255.0
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
```

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

## Lab – Exploring Cisco IOS and Configuring Basic Switch Settings

---

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
```

- m. Configure the IP 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. It does respond to pings from a remote network. 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.

```
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#
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

### 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. A default gateway is not required for this topology; however, you can enter **192.168.1.1** to simulate a router attached to S1.

To change IP address of a PC in Ubuntu.

1. Edit Network Connections.
2. Select Manual and Click Add.
3. Type in your local IP address / Netmask / Gateway.
4. Click Save.
5. Open a Terminal window.
6. Type **ifconfig** (Note name of network connection, eth0, eth1, etc.).
7. Type **sudo ifconfig eth0 down** (Replace eth0 if it is a different name).
8. Enter Cisco Student password (C1sc0:d04).
9. The Network Connection should Disconnect and Reconnect with the new IP address.



10. If not, type ***sudo ifconfig eth0 up***
11. Repeat above steps when switching back to Automatic (DHCP) in Network Connections.

### 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.

From your console connection on PC-A, display and verify your 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 displays 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
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
no ip route-cache
```

## Lab – Exploring Cisco IOS and Configuring Basic Switch Settings

---

```
!  
interface Vlan99  
ip address 192.168.1.2 255.255.255.0  
no ip route-cache  
!  
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 104D000A0618  
logging synchronous  
login  
line vty 0 4  
password 7 14141B180F0B  
login  
line vty 5 15  
password 7 14141B180F0B  
login  
!  
end  
  
S1#
```

### b. 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 192.168.1.2/24  
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
```

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

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

```
C:\Users\User1> ping 192.168.1.10
```

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

```
C:\Users\User1> 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. You should check both the physical cabling and logical addressing if necessary.

### 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. You can use Telnet from the command line in Ubuntu or from the Putty application. **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"**.

- 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
```

- After entering the password **cisco**, you will be at the user EXEC mode prompt. Access privileged EXEC mode.
- 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#
```

## Part 4: Manage the MAC Address Table

In Part 4, you will determine the MAC address 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.

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

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

- Display the MAC address table options.

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

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

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

- 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.

- Clear the MAC address table.

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

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

- Verify that the MAC address table was cleared.

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

- Examine the MAC table again.

More than likely, an application running on your PC 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 for PC-A.

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

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.

- 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 your 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
```

## Lab – Exploring Cisco IOS and Configuring Basic Switch Settings

---

- e. Verify the MAC address table entries.

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

- 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 your 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
```

## Part 5: Configure and Verify SSH Access on S1

### Step 1: Configure SSH access on S1.

- a. Enable SSH on S1. From global configuration mode, create a domain name of **CCNA-Lab.com**.  
S1(config)# **ip domain-name CCNA-Lab.com**
- b. Create a local user database entry for use when connecting to the switch via SSH. The user should have administrative level access.

**Note:** The password used here is NOT a strong password. It is merely being used for lab purposes.

```
S1(config)# username admin privilege 15 secret sshadmin
```

- c. Configure the transport input for the vty lines to allow SSH connections only, and use the local database for authentication.

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

- d. Generate an RSA crypto key using a modulus of 1024 bits.

```
S1(config)# crypto key generate rsa modulus 1024  
The name for the keys will be: S1.CCNA-Lab.com  
  
% The key modulus size is 1024 bits  
% Generating 1024 bit RSA keys, keys will be non-exportable...  
[OK] (elapsed time was 3 seconds)
```

```
S1(config)#  
S1(config)# end
```

- e. Verify the SSH configuration and answer the questions below.

```
S1# show ip ssh
```

### Step 2: Modify the SSH configuration on S1.

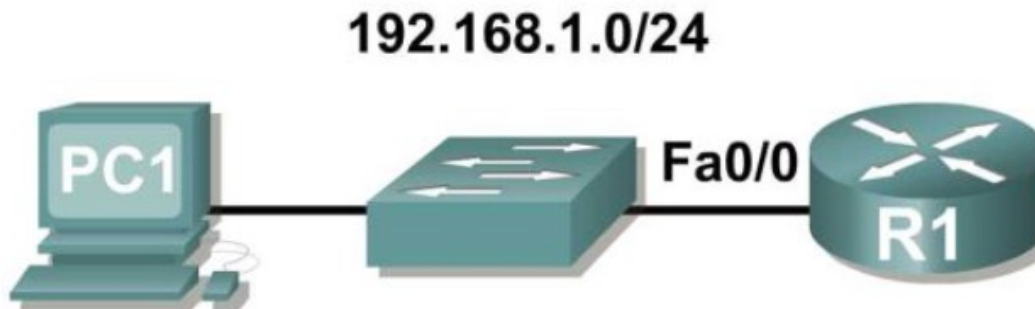
Modify the default SSH configuration.

```
S1# config t  
S1(config)# ip ssh time-out 75  
S1(config)# ip ssh authentication-retries 2
```

### Step 3: Verify the SSH configuration on S1.

- a. Using SSH client software on PC-A (e.g. Putty), open an SSH connection to S1. If you receive a message on your SSH client regarding the host key, accept it. Log in with **admin** for username and **cisco** for the password.
- b. Type **exit** to end the SSH session on S1.

## Part 6: Configure Router as Gateway for Switch network



### 1. Configure the router.

- i) Console into the router and enable privileged EXEC mode.

```
Router> enable
Router#
```

- ii) Enter into global configuration mode.

```
Router# config terminal
Router(config)#
```

- iii) Assign a device name to the router.

```
Router(config)# hostname R1
```

- iv) Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.

- v) Encrypt the clear text passwords.

```
R1(config)# service password-encryption
```

- vi) Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

```
R1(config)# banner motd #Unauthorized access prohibited!#
```

- vii) Configure an IP address and interface description. Activate both interfaces on the router.

```
R1(config)# int Fa 0/0
R1(config-if)# description Connection to Switch1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
```

- a. Save the running configuration to the startup configuration file.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

What would be the result of reloading the router prior to completing the **copy running-config startup-config** command?

## Part 7: Configure and Verify Security Features on S1

You should always shut down unused ports, turn off certain services running on the switch, and configure port security based on MAC addresses. Switches can be subject to MAC address table overflow attacks, MAC spoofing attacks, and unauthorized connections to switch ports. You will configure port security to limit the number of MAC addresses that can be learned on a switch port and disable the port if that number is exceeded.

### Step 1: Configure general security features on S1.

- Configure a message of the day (MOTD) banner on S1 with an appropriate security warning message.
- Issue a **show ip interface brief** command on S1. What physical ports are up?

- 
- Shut down all unused physical ports on the switch. Use the **interface range** command.

```
S1(config)# interface range f0/1 - 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 - 2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

- Issue the **show ip interface brief** command on S1. What is the status of ports F0/1 to F0/4?
- Issue the **show ip http server status** command.  
What is the HTTP server status? What server port is it using?  
What is the HTTP secure server status? What secure server port is it using?
- HTTP sessions send everything in plain text. You will disable the HTTP service running on S1.  

```
S1(config)# no ip http server
```
- From PC-A, open a web browser session to `http://192.168.1.10`. What was your result?
- From PC-A, open a secure web browser session at `https://192.168.1.10`. Accept the certificate. Log in with no username and a password of **class**. What was your result?
- Close the web session on PC-A.

### Step 2: Configure and verify port security on S1.

- Connect another device (e.g. your laptop) into the G0/1 port. From the Switch CLI, use the **show interface g0/1** command and record the MAC address of the interface.
- From the S1 CLI, issue a **show mac address-table** command from privileged EXEC mode. Find the dynamic entries for the connected ports and record them.
- Configure basic port security.

- From the S1 CLI, enter interface configuration mode for the port that connects the PC e.g. F0/5

```
S1(config)# interface f0/5
```

- Shut down the port.

```
S1(config-if)# shutdown
```

- Enable port security on F0/5.

```
S1(config-if)# switchport port-security
```



## Lab – Exploring Cisco IOS and Configuring Basic Switch Settings

**Note:** Entering the **switchport port-security** command sets the maximum MAC addresses to 1 and the violation action to shutdown. The **switchport port-security maximum** and **switchport port-security violation** commands can be used to change the default behavior.

- 4) Configure a static entry for the MAC address of the PC/laptop connected into G0/1 interface recorded in Step 2a.

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

(xxxx.xxxx.xxxx is the actual MAC address of the router G0/1 interface)

**Note:** Optionally, you can use the **switchport port-security mac-address sticky** command to add all the secure MAC addresses that are dynamically learned on a port (up to the maximum set) to the switch running configuration.

- 5) Enable the switch port.

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

```
S1(config-if)# end
```

- d. Verify port security on S1 F0/5 by issuing a **show port-security interface** command.

```
S1# show port-security interface f0/5  
Port Security           : Enabled  
Port Status             : Secure-up  
Violation Mode          : Shutdown  
Aging Time              : 0 mins  
Aging Type              : Absolute  
SecureStatic Address Aging : Disabled  
Maximum MAC Addresses   : 1  
Total MAC Addresses     : 1  
Configured MAC Addresses : 1  
Sticky MAC Addresses    : 0  
Last Source Address:Vlan : 0000.0000.0000:0  
Security Violation Count : 0
```

What is the port status of F0/5?

- e. Ping PC-A to verify connectivity.
- f. You will now violate security by connecting a different device/MAC address into the port fa0/5
- g. Try send a ping to the switch from this newly connected device. Was the ping successful? Why or why not?
- h. On the switch, verify port security with the following commands shown below.

```
S1# show port-security  
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action  
              (Count)          (Count)          (Count)  
-----  
Fa0/5          1              1              1              Shutdown  
-----  
Total Addresses in System (excluding one mac per port) :0  
Max Addresses limit in System (excluding one mac per port) :8192
```

```
S1# show port-security interface f0/5  
Port Security           : Enabled  
Port Status             : Secure-shutdown  
Violation Mode          : Shutdown  
Aging Time              : 0 mins
```

## Lab – Exploring Cisco IOS and Configuring Basic Switch Settings

```
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : aaaa.bbbb.cccc:99
Security Violation Count : 1
```

S1# **show interface f0/5**

```
FastEthernet0/5 is down, line protocol is down (err-disabled)
Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
```

S1# **show port-security address**

```
Secure Mac Address Table
-----
Vlan      Mac Address      Type                Ports      Remaining Age
(mins)
-----
  99      30f7.0da3.1821   SecureConfigured   Fa0/5      -
-----
Total Addresses in System (excluding one mac per port) :0
Max Addresses limit in System (excluding one mac per port) :8192
```

- i. Clear the S1 F0/5 error disabled status.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

**Note:** There may be a delay while the port states converge.

- j. Issue the **show interface f0/5** command on S1 to verify F0/5 is no longer in error disabled mode.

```
S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
```

- k. From the R1 command prompt, ping PC-A again. You should be successful.

## Reflection

1. Why should you configure the vty lines for the switch?
2. Why change the default VLAN 1 to a different VLAN number?
3. Why should unused ports on a switch be disabled?