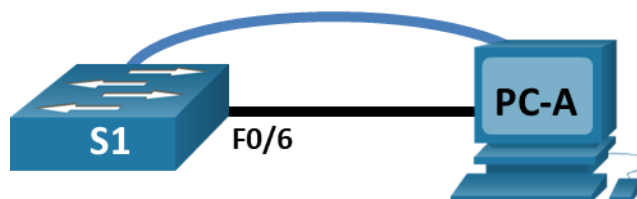


Packet Tracer - Basic Switch Configuration - Physical Mode

Topology



Addressing Table

Device	Interface	IP Address / Prefix
S1	VLAN 99	192.168.1.2 /24
		2001:db8:acad:1::2 /64
		fe80::2
PC-A	NIC	192.168.1.10 /24
		2001:db8:acad:1::10 /64

Objectives

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

Part 2: Configure Basic Network Device Settings

Part 3: Verify and Test Network Connectivity

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 on VLAN 1 have access to the SVI IP address.

In this activity, you will build a simple topology using Ethernet LAN cabling to 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 use a management IP address for remote switch management. The topology consists of one switch and two hosts using only Ethernet and console ports. You will verify network connectivity and manage a MAC address table using two end devices.

Instructions

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.

- From the shelf, click and drag switch **S1** and place it on the left side of the table.
- From the shelf, click and drag the device **PC-A** and place it on the right side of the table. Power on PC-A.
- Connect a console cable from device **PC-A** to switch **S1**, as shown in the topology. Do not connect the device PC-A Ethernet cable at this time.
- From the **Desktop** tab of PC-A, use **Terminal** to connect to the switch.

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?

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 of 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 activity.

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

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

- Verify that there is a clean default configuration file on the switch by issuing the **show running-config** privileged EXEC mode command. Examine the current running configuration file.

How many GigabitEthernet interfaces does the switch have?

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

- Examine the startup configuration file in NVRAM.

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

Why does this message appear?

- 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 an Ethernet cable from PC-A to GigabitEthernet1/0/6 on the switch. Allow time for the switch and PC to negotiate duplex and speed parameters. Examine the IP properties of the SVI VLAN 1.

What output do you see?

- g. Enter global configuration and enable the SVI VLAN 1 interface.

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

What output do you see?

- i. 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 Ethernet MAC address of this switch?

- j. Examine the default properties of the GigabitEthernet1/0/6 interface used by PC-A.

```
Switch# show interface gig1/0/6
```

Is the interface up or down?

What event would make an interface go down?

What is the MAC address of the interface?

What is the speed and duplex setting of the interface?

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

```
Switch# show vlan
```

What is the name of VLAN 1?

Which ports are in VLAN 1?

Is VLAN 1 active?

What type of VLAN is the default VLAN?

- I. 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, 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. Next, 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. An IPv6 address can also be configured on the SVI interface. Use the IPv6 addresses listed in the **Addressing Table**.

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.

To establish connectivity between the host and the switch, the ports used by the host must be in the same VLAN as the switch. After a few seconds, VLAN 99 comes up because at least one active port (Fa0/6 with PC-A attached) is now assigned to VLAN 99.

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

- e. 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.
- 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 use Telnet to access the switch.

Why is the **login** command required?

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 to function; however, you should enter **192.168.1.1** and **fe80::1** to simulate a router attached to S1.

- a. Navigate to the **Desktop** tab.
- b. Click **IP Configuration**.
- c. Verify that the **Static** IP Configuration radial button is selected.
- d. Enter the IPv4 address, subnet mask, and default gateway.
- e. Verify that the **Static** IPv6 Configuration radial button is selected.
- f. Enter the IPv6 address, prefix, and default gateway
- g. Click the **X** to close the **IP Configuration** 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 remote management capability of the switch.

Step 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.

- 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 : 2424 bytes
!
version 16.3.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
```

```
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil!
no ip cef
no ipv6 cef
!
!
no ip domain-lookup
!
<output omitted>
!
interface GigabitEthernet1/0/6
  switchport access vlan 99
!
<output omitted>
!
interface GigabitEthernet1/0/24
  switchport access vlan 99
!
<output omitted>
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan99
  mac-address 00e0.f795.d201
  ip address 192.168.1.2 255.255.255.0
  ipv6 address FE80::2 link-local
  ipv6 address 2001:DB8:ACAD:1::2/64
!
ip default-gateway 192.168.1.1
ip classless
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
  password 7 0822455D0A16
  logging synchronous
  login
line vty 0 4
  password 7 0822455D0A16
  login
line vty 5 15
  password 7 0822455D0A16
  login
!
end
```

- b. Verify the management VLAN 99 settings.

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

What is the bandwidth on this interface?

What is the VLAN 99 state?

What is the line protocol state?

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

Verify that PC-A can ping the IPv4 and IPv6 address for S1.

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

```
C:\> ping 2001:db8:acad: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 activity, 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 the 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 in plaintext. In subsequent activities, you will use SSH to remotely access network devices.

- Open the **Desktop** tab on PC-A.
- Scroll down in the listing of apps and click the **Telnet/SSH Client**.
- Set the **Connection Type** to be **Telnet**.
- Enter the SVI management address to connect to S1 and click **Connect**.
- 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**.
- Save the configuration.
- Type **exit** to end the Telnet session. Click **No** to the pop-up.

Step 4: Deploy switch S1 on the production network.

You will now install switch S1 on the production network and disconnect the console cable. Telnet will be used to remotely access the switch and complete any additional configuration and verification. In subsequent activities, you will use SSH to remotely access network devices.

- Move switch **S1** to the **Rack**.
- Right-click switch **S1** and select **Inspect Rear**.
- Click and drag the **console cable** to the **peg board**.

Reflection Questions

1. Why should you configure the vty password for the switch?
2. Why change the default VLAN 1 to a different VLAN number?
3. How can you prevent passwords from being sent in plaintext?