Lab 1 – Cisco Switch 2960 Basic Configuration

Centro Avançado de Telecomunicações
2022/2023

Lab 1 – Cisco Switch 2960 Basic Configuration

Topology

Objectives

Part 1:Access a Cisco Switch through the Serial Console Port.

Part 2:Initialize the Switch and Reload.

Part 3:Configuring a Switch Management Address.

Part 4:Configure an IP address on PC-A.

Part 5: Display and Configure Basic Device Settings

Required Resources

- Switch (Cisco 2960 Model)
- PC (With a terminal emulation program, such as Putty)
- Rollover (DB-9 to RJ-45) console cable to configure the switch or router via the RJ-45 console port
- Straight-Through UTP Ethernet Cable

Part 1: Access a Cisco Switch through the Serial Console Port

You will connect a PC to a Cisco switch using a rollover console cable. This connection will allow you to access the CLI and display settings or configure the switch.

You will connect a PC to a Cisco switch using a rollover console cable. This connection will allow you to access the CLI and display settings or configure the switch.

Step 1: Connect a Cisco switch and computer using a rollover console cable.

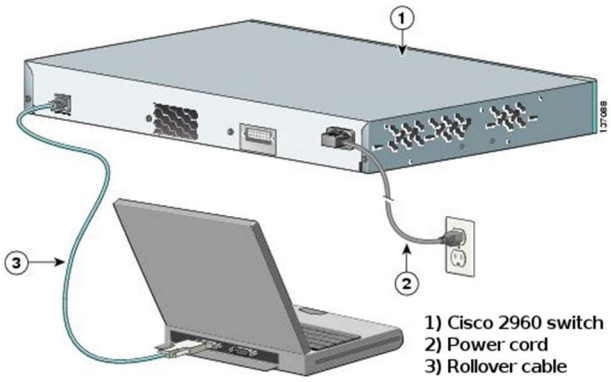
a. Connect the rollover console cable to the RJ-45 console port of the switch.

b. Connect the other cable end to the serial COM port on the computer.

Note: Serial COM ports are no longer available on most computers. A USB-to-DB9 adapter can be used with the rollover console cable for console connection between the computer and a Cisco device. USB-to-DB9 adapters can be purchased at any computer electronics store.

Note: If using a USB-to-DB9 adapter to connect to the COM port, you may be required to install a driver for the adapter provided by the manufacturer of your computer. To determine the COM port used by the adapter, please see Part 3 Step 4. The correct COM port number is required to connect to the Cisco IOS device using a terminal emulator in Step 2.

c. Turn on the Cisco switch and computer.



Step 2: Configure Putty Client to establish a console session with the switch.

a. In the New Connection dialog box, click the **Serial** radio button. Verify that the correct COM port is selected and click **OK** to continue.

b. From the Putty **Setup** menu, choose the **Serial port…** to verify the serial settings. The default parameters for the console port are 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control. The Putty default settings match the console port settings for communications with the Cisco IOS switch.

c. When you can see the terminal output, you are ready to configure a Cisco switch. The following console example displays the terminal output of the switch while it is loading.

Part 2: Initialize the Switch and Reload

Step 1: Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Step 2: Determine if there have been any virtual local-area networks (VLANs) created.

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

```
Switch# show flash
```

[output]

Step 3: Delete the VLAN file.

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

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

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

b. When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

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

Step 4: Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

```
Switch# erase startup-config
```

[output]

Step 5: Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

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

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

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

Step 6: Bypass the initial configuration dialog.

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

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

Reflection

1. Why is it necessary to erase the startup configuration before reloading the switch?

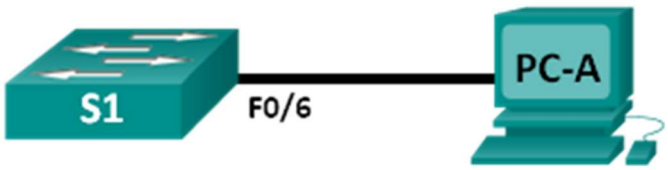
   _____

2. You find a couple configurations issues after saving the running configuration to the startup configuration, so you make the necessary changes to fix those issues. If you were to reload the device now, what configuration would be restored to the device after the reload?

   _____

Part 3: Configuring a Switch Management Address

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
SWX	VLAN 1	192.168.199.X	255.255.255.0
PC-A	NIC	192.168.199.yy	255.255.255.0

Where “X” is your Group ID [1-8]

Cisco switches have a special interface, known as a switch virtual interface (SVI). The SVI can be configured with an IP address, commonly referred to as the management address. The management address is used for remote access to the switch to display or configure settings.

In this lab, you will build a simple network using Ethernet LAN cabling and access a Cisco switch using the console and remote access methods. You will configure basic switch settings, IP addressing, and 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

Step 1: Set the SVI IP address to allow remote switch management.

a. Enter global configuration mode to set the SVI IP address to allow remote switch management.

```
S1# config t
S1#(config)# interface vlan 1
S1(config-if)# ip address 192.168.199.X  255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.199.254
```

Step 2: Display the S1 device configuration.

Issue the **show run** command to display and verify your switch configuration.

[output]

Step 3: Enter local passwords.

To prevent unauthorized access to the switch, passwords must be configured.

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# enable secret class
```

a. Restrict console port access. The default configuration is to allow all console connections with no password needed.

```
S1(config)# line con 0
```

```
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

b. Configure the VTY line 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.

```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
```

Part 4: Configure an IP address on PC-A.

Step 1: Assign the IP address and subnet mask to the PC.

a. Assign the IP address and subnet mask to the PC, as shown in the Addressing Table. The procedure for assigning an IP address on a PC running Windows 10 is described below:

1) Click the **Windows Start** icon > **Control Panel**.
2) Click **View By:** > **Category**.
3) Choose **View network status and tasks** > **Change adapter settings**.
4) Right-click **Local Area Network Connection** and select **Properties**.
5) Choose **Internet Protocol Version 4 (TCP/IPv4)**, click **Properties**.
6) Click the **Use the following IP address** radio button and enter the IP address and subnet mask.

Step 2: Display the status of the connected interfaces on the switch.

To check the status of the connected interfaces, use the **show ip interface brief** command. Press the spacebar to advance to the end of the list.

```
S1# show ip interface brief
```

[output]

Step 3: Record the interface status for the following interfaces.

Why are some FastEthernet ports on the switches are up and others are down?

_____

_____

Step 4: Test end-to-end connectivity.

Open a command prompt window (cmd.exe) on PC-A by clicking the **Windows Start** icon and entering **cmd** into the **Search for programs and files** field. Verify the IP address of PC-A by using the **ipconfig /all** command. This command displays the PC hostname and the IPv4 address information. Ping PC-A's address and the management address of S1.

a. Ping the PC-A address first.

```
C:\Users\NetAcad> ping 192.168.199.yy
```

b. Ping the SVI management address of S1.

```
C:\Users\NetAcad> ping 192.168.199.X
```

If ping results are not successful, troubleshoot the basic device configurations. You should check both the physical cabling and IP addressing if necessary.

[output]

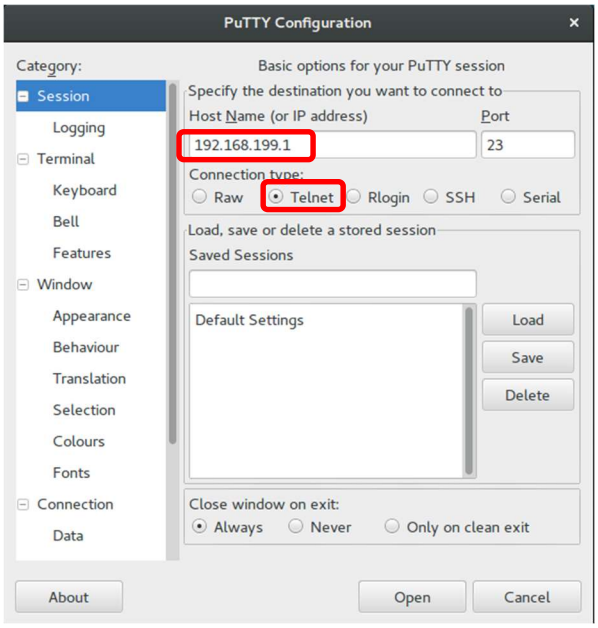
Step 5: Test and verify the remote management of S1.

You will now use Telnet to remotely access the switch S1 using the SVI management address. 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. Telnet is not a secure protocol. However, you will use it in this lab to test remote access. All information sent by Telnet, including passwords and commands, is sent across the session in plaintext. In subsequent labs, you will use SSH to remotely access network devices.

a. With the command prompt window still open on PC-A, issue a Telnet command to connect to S1 via the SVI management address.

```
C:\Users\NetAcad> telnet 192.168.199.X
```

b. Or open putty and enter the IP Address configured on the previous step and select telnet connection.



Step 6: Save the configuration file.

a. From your Telnet session, issue the **copy run start** command at the prompt.

```
S1# copy run start
Destination filename [startup-config]? [Enter]
Building configuration ..
S1#
```

b. Exit the Telnet session by typing **quit**. You will be returned to the Windows command prompt.

Reflection

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

_____

Part 5: Display and Configure Basic Device Settings

In this section, you are introduced to the user and privileged executive modes. You will determine the IOS version, display the clock settings, and configure the clock on the switch.

Step 1: Display the switch IOS image version.

a. While you are in the user EXEC mode, display the IOS version for your switch and other useful switch information.

```
Switch> show version
```

[output]

Which IOS image version is currently in use by your switch?

_____

What is the name of the IOS image that the switch is running?

_____

How much dynamic random access memory (DRAM) does the switch have?

_____

How much nonvolatile random-access memory (NVRAM) does the switch have?

_____

What is the model number of the switch?

_____

Step 2: Configure the clock.

As you learn more about networking, you will see that configuring the correct time on a Cisco switch can be helpful when you are troubleshooting problems. The following steps manually configure the internal clock of the switch.

a. Display the current clock settings.

```
Switch> show clock
```

[output]

b. The clock setting is changed from within the privileged EXEC mode. Enter the privileged EXEC mode by typing **enable** at the user EXEC mode prompt.

```
Switch> enable
```

c. Configure the clock setting. The question mark (?) provides help and allows you to determine the expected input for configuring the current time, date, and year. Press Enter to complete the clock configuration.

```
Switch# clock set ?
Switch#
*Oct 26 15:08:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:31:43
UTC Mon Mar 1 1993 to 15:08:00 UTC Fri Oct 26 2012, configured from console by
console.
```

d. Enter the **show clock** command to verify that the clock setting has updated.

```
Switch# show clock
```

[output]

Step 3: Enter configuration mode.

Use the **configuration terminal** command to enter configuration mode.

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

The prompt changed to reflect global configuration mode.

Step 4: Give the switch a name.

Use the **hostname** command to change the switch name to **Sx,** where "x" is your group ID [1-8].

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

Step 5: Prevent unwanted DNS lookups.

To prevent the switch from attempting to translate incorrectly entered commands as though they were hostnames, disable the Domain Name System (DNS) lookup.

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

Step 6: Enter a login MOTD banner.

A login banner, known as the message of the day (MOTD) banner, should be configured to warn anyone accessing the switch that unauthorized access will not be tolerated.

The **banner motd** command requires the use of delimiters to identify the content of the banner message. The delimiting character can be any character as long as it does not occur in the message. For this reason, symbols, such as the **#**, are often used.

```
S1(config)# banner motd #
Unauthorized access is strictly prohibited. #
```

```
S1(config)# exit
S1#
```

Step 7: Save the configuration.

Use the **copy** command to save the running configuration to the startup file on non-volatile random access memory (NVRAM).

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

Step 8: Verify your access setting by moving between modes.

```
S1# exit
Unauthorized access is strictly prohibited.
S1>
```

What shortcut keys are used to go directly from global configuration mode to privileged EXEC mode?

_____

Return to privileged EXEC mode from user EXEC mode.

```
S1> enable
Password: class
S1#
```

Note: The password will not show up on the screen when entering.

Step 9: Display the current configuration.

The **show running-config** command displays the entire running configuration, one page at a time. Use the spacebar to advance paging. Identify the commands configured in Steps 1 – 7.

```
S1# show running-config
```

[output]