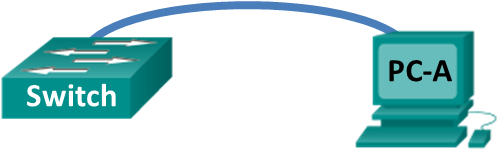
Lab 2.1.4.7 Establishing a Console Session



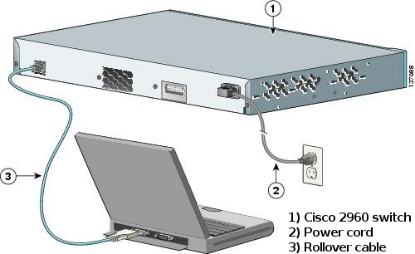
1. Objectives

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

Part 2: Display and Configure Basic Device Settings

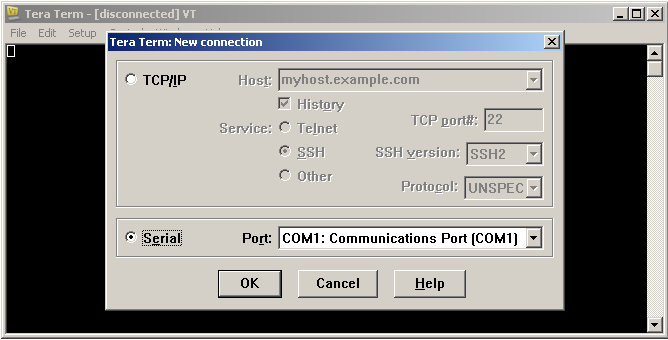
1. Background / Scenario

Various models of Cisco routers and switches are used in all types of networks. These devices are managed using a local console connection or a remote connection. In this lab, you will learn how to access a Cisco device via a direct local connection to the console port, using the terminal emulation program called **Tera Term**. Using **Tera Term** is the most basic way to access a router for checking or changing its configuration. After you have established a console connection with the Cisco device, you can display or configure device settings. You will only display settings and configure the clock in this lab.

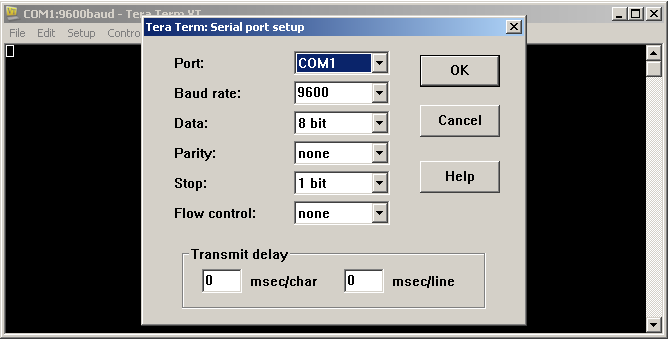
* 1. Connect a Cisco switch and computer using a rollover console cable.
     1. Connect the rollover console cable to the RJ-45 console port of the switch.
     2. Connect the other cable end to the serial COM port on the computer.
     3. Turn on the Cisco switch and computer.
  2. Establish a console session with the switch.

**Tera Term** is a terminal emulation program. This program allows you to access the terminal output of the switch. It also allows you to configure the switch.

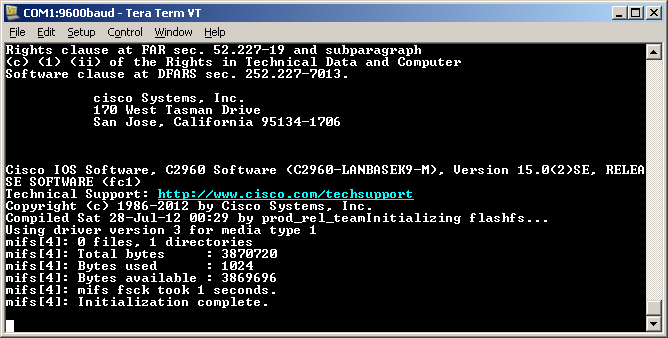
1. Start **Tera Term** by clicking the **Windows Start** button located in the task bar. Locate **Tera Term** under **All Programs**.
2. In the New Connection dialog box, click the **Serial** radio button. Verify that the correct COM port is selected and click **OK** to continue.



1. From the **Tera Term** **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 **Tera Term** default settings match the console port settings for communications with the Cisco IOS switch.



* + 1. 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.



* 1. 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.

* + 1. After the switch has completed its startup process, the following message is displayed. Enter **n** to continue**.**

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

**Note**: If you do not see the above message, please contact your instructor to reset your switch to the initial configuration.

* + 1. While you are in the user EXEC mode, display the IOS version for your switch.
  1. Display the IOS version and other useful switch information.

Use the **show version** command to display the IOS version that the switch is running, along with other useful information. Again, you will need to use the spacebarto advance through the displayed information.

Switch> **show version**

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2012 by Cisco Systems, Inc.

Compiled Sat 28-Jul-12 00:29 by prod\_rel\_team

ROM: Bootstrap program is C2960 boot loader

BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE (fc1)

Switch uptime is 1 hour, 38 minutes

System returned to ROM by power-on

**System image file is "flash:/c2960-lanbasek9-mz.150-2.SE.bin"**

This product contains cryptographic features and is subject to United

States and local country laws governing import, export, transfer and

use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for

compliance with U.S. and local country laws. By using this product you

agree to comply with applicable laws and regulations. If you are unable

to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to

export@cisco.com.

cisco WS-C2960-24TT-L (PowerPC405) processor (revision R0) with 65536K bytes of memory.

Processor board ID FCQ1628Y5LE

Last reset from power-on

1 Virtual Ethernet interface

24 FastEthernet interfaces

2 Gigabit Ethernet interfaces

The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.

Base ethernet MAC Address : 0C:D9:96:E2:3D:00

Motherboard assembly number : 73-12600-06

Power supply part number : 341-0097-03

Motherboard serial number : FCQ16270N5G

Power supply serial number : DCA1616884D

Model revision number : R0

Motherboard revision number : A0

Model number : WS-C2960-24TT-L

System serial number : FCQ1628Y5LE

Top Assembly Part Number : 800-32797-02

Top Assembly Revision Number : A0

Version ID : V11

CLEI Code Number : COM3L00BRF

Hardware Board Revision Number : 0x0A

Switch Ports Model SW Version SW Image

------ ----- ----- ---------- ----------

\* 1 26 WS-C2960-24TT-L 15.0(2)SE C2960-LANBASEK9-M

* + 1. Which IOS image version is currently in use by your switch?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. 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.

* + 1. Display the current clock settings.

Switch> **show clock**

\*00:30:05.261 UTC Mon Mar 1 1993

* + 1. 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**

* + 1. 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 ?**

hh:mm:ss Current Time

Switch# **clock set 15:15:00 ?**

MONTH Month of the year

<1-31> Day of the month

Switch# **clock set 15:15:00 Feb 16 ?**

<1993-2035> Year

Switch# **clock set 15:15:00 Feb 16 2021**

Switch#

* + 1. Enter the **show clock** command to verify that the clock setting has updated.

Switch# **show clock**

15:15:04.213 UTC Tue Feb 16 2021

Lab 2.3.3.3 Building a Simple Network



|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask |
| PC-A | NIC | 192.168.1.10 | 255.255.255.0 |
| PC-B | NIC | 192.168.1.11 | 255.255.255.0 |

1. Objectives

Part 1: Set Up the Network Topology (Ethernet only)

Part 2: Configure PC Hosts

Part 3: Configure and Verify Basic Switch Settings

1. Background / Scenario

Networks are constructed of three major components: hosts, switches, and routers. In this lab, you will build a simple network with two hosts and two switches. You will also configure basic settings including hostname, local passwords, and login banner. Use **show** commands to display the running configuration, IOS version, and interface status. Use the **copy** command to save device configurations. You will apply IP addressing for this lab to the PCs to enable communication between these two devices. Use the **ping** utility to verify connectivity.

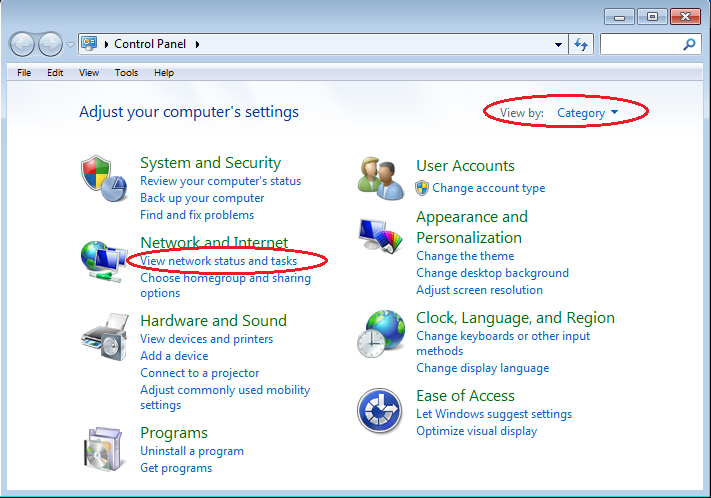
1. Set Up the Network Topology (Ethernet only)

In Part 1, you will cable the devices together according to the network topology.

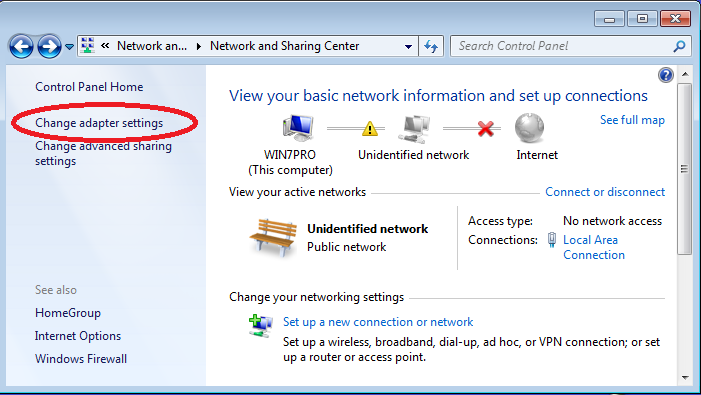
* 1. Connect the PCs to their respective switches.
     1. Connect one end of the second Ethernet cable to the NIC port on PC-A. Connect the other end of the cable to F0/6 on S1. After connecting the PC to the switch, you should see the light for F0/6 turn amber and then green, indicating that PC-A has been connected correctly.
     2. Connect one end of the last Ethernet cable to the NIC port on PC-B. Connect the other end of the cable to F0/18 on S2. After connecting the PC to the switch, you should see the light for F0/18 turn amber and then green, indicating that the PC-B has been connected correctly.
  2. Connect the two switches.

Connect one end of an Ethernet cable to F0/1 on S1 and the other end of the cable to F0/1 on S2. You should see the lights for F0/1 on both switches turn amber and then green. This indicates that the switches have been connected correctly.

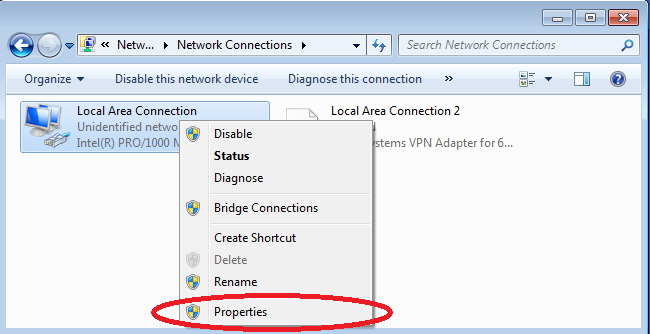
1. Configure PC Hosts
   1. Configure static IP address information on the PCs.
      1. Click the **Windows Start** icon and then select **Control Panel**.
      2. In the **Network and Internet** section, click the **View network status and tasks** link. **Note**: If the Control Panel displays a list of icons, click the drop-down option next to the **View by**: and change this option to display by **Category**.



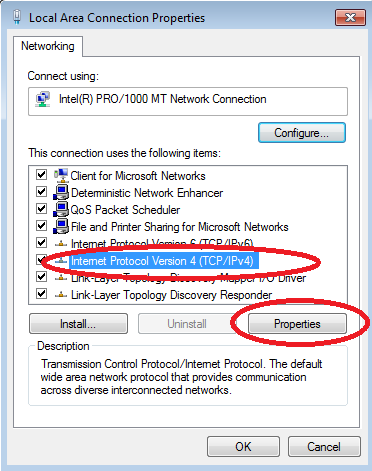
* + 1. In the left pane of the **Network and Sharing Center** window, click the **Change adapter settings** link.



* + 1. The Network Connections window displays the available interfaces on the PC. Right-click the **Local Area Connection** interface and select **Properties**.

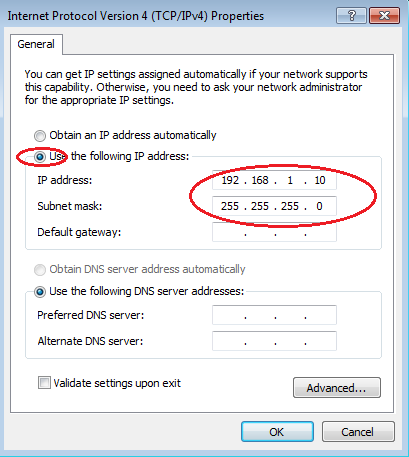


* + 1. Select the **Internet Protocol Version 4 (TCP/IPv4)** option and then click **Properties**.



**Note**: You can also double-click **Internet Protocol Version 4 (TCP/IPv4**) to display the Properties window.

* + 1. Click the **Use the following IP address** radio button to manually enter an IP address, subnet mask, and default gateway.

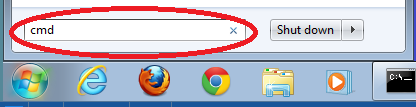


**Note**: In the above example, the IP address and subnet mask have been entered for PC-A. The default gateway has not been entered, because there is no router attached to the network. Refer to the Addressing Table on page 1 for PC-B’s IP address information.

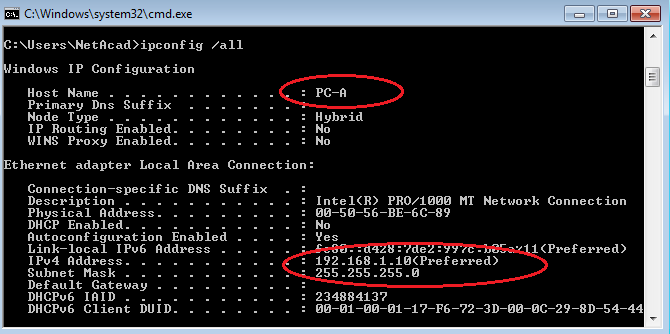
* + 1. After all the IP information has been entered, click **OK**. Click **OK** on the Local Area Connection Properties window to assign the IP address to the LAN adapter.
    2. Repeat the previous steps to enter the IP address information for PC-B.
  1. Verify PC settings and connectivity.

Use the command prompt (**cmd.exe**) window to verify the PC settings and connectivity.

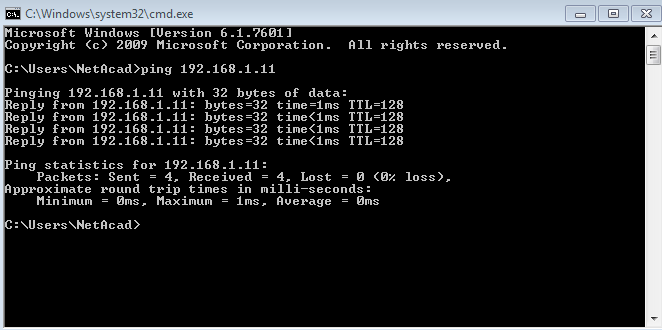
* + 1. From PC-A, click the **Windows Start** icon, type **cmd** in the **Search programs and files** box, and then press Enter.



* + 1. The cmd.exe window is where you can enter commands directly to the PC and view the results of those commands. Verify your PC settings by using the **ipconfig /all** command. This command displays the PC hostname and the IPv4 address information.



* + 1. Type **ping 192.168.1.11** and press Enter.



Were the ping results successful? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If not, troubleshoot as necessary.

1. Configure and Verify Basic Switch Settings
   1. Enter privileged EXEC mode.

You can access all switch commands in privileged EXEC mode. The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained. Enter privileged EXEC mode by entering the **enable** command.

Switch> **enable**

Switch#

The prompt changed from **Switch>** to **Switch#** which indicates privileged EXEC mode.

* 1. 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.

* 1. Give the switch a name.

Use the **hostname** command to change the switch name to **S1** or **S2**.

Switch(config)# **hostname S1**

S1(config)#

* 1. 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**

* 1. Enter local passwords.

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

* + 1. Configure the switch password access to privileged EXEC mode.

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

* + 1. Restrict console port access. The default configuration is to allow all console connections with no password needed. Configure the console password.

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

S1(config-line)# **password cisco**

S1(config-line)# **login**

S1(config-line)# **exit**

S1(config)#

* 1. 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 #**

Enter TEXT message. End with the character '#'.

**Unauthorized access is strictly prohibited and prosecuted to the full extent of the law. #**

S1(config)# **exit**

S1#

What shortcut keys are used to go directly from global configuration mode **S1(config)#** to privileged EXEC mode **S1#**?

* 1. 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]

* 1. 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. The commands configured in Steps 1 – 8 are highlighted below.

S1# **show running-config**

Building configuration...

Current configuration : 1409 bytes

!

! Last configuration change at 03:49:17 UTC Mon Mar 1 1993

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no 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>**

!

banner motd ^C

Unauthorized access is strictly prohibited and prosecuted to the full extent of the law. ^C

!

line con 0

password cisco

login

line vty 0 4

login

line vty 5 15

login

!

end

* 1. 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**

Interface IP-Address OK? Method Status Protocol

Vlan1 unassigned YES unset up up

FastEthernet0/1 unassigned YES unset up up

FastEthernet0/2 unassigned YES unset down down

FastEthernet0/3 unassigned YES unset down down

FastEthernet0/4 unassigned YES unset down down

FastEthernet0/5 unassigned YES unset down down

FastEthernet0/6 unassigned YES unset up up

FastEthernet0/7 unassigned YES unset down down

FastEthernet0/8 unassigned YES unset down down

FastEthernet0/9 unassigned YES unset down down

FastEthernet0/10 unassigned YES unset down down

FastEthernet0/11 unassigned YES unset down down

FastEthernet0/12 unassigned YES unset down down

FastEthernet0/13 unassigned YES unset down down

FastEthernet0/14 unassigned YES unset down down

FastEthernet0/15 unassigned YES unset down down

FastEthernet0/16 unassigned YES unset down down

FastEthernet0/17 unassigned YES unset down down

FastEthernet0/18 unassigned YES unset down down

FastEthernet0/19 unassigned YES unset down down

FastEthernet0/20 unassigned YES unset down down

FastEthernet0/21 unassigned YES unset down down

FastEthernet0/22 unassigned YES unset down down

FastEthernet0/23 unassigned YES unset down down

FastEthernet0/24 unassigned YES unset down down

GigabitEthernet0/1 unassigned YES unset down down

GigabitEthernet0/2 unassigned YES unset down down

* 1. Record the interface status for the following interfaces.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Interface | S1 | | S2 | |
| Status | Protocol | Status | Protocol |
| F0/1 |  |  |  |  |
| F0/6 |  |  |  |  |
| F0/18 |  |  |  |  |

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

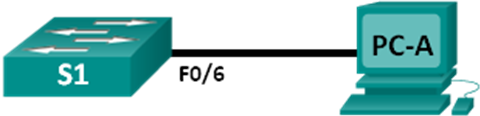
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. What could prevent a ping from being sent between the PCs?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Lab 2.3.3.4 Configuring a Switch Management Address

Topology



1. Addressing Table

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask |
| S1 | VLAN 1 | 192.168.1.2 | 255.255.255.0 |
| PC-A | NIC | 192.168.1.10 | 255.255.255.0 |

1. Objectives

Part 1: Configure a Basic Network Device

Part 2: Verify and Test Network Connectivity

1. Background / Scenario

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.

1. Configure a Basic Network Device
   1. Configure basic switch settings.

In this step, you will configure basic switch settings, such as hostname, and configure an IP address for the SVI. Assigning an IP address on the switch is only the first step. As the network administrator, you must specify how the switch will be managed. Telnet and SSH are two of the most common management methods. However, Telnet is a very insecure protocol. All information flowing between the two devices is sent in plaintext. Passwords and other sensitive information can be easily viewed if captured by a packet sniffer.

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 192.168.1.2 255.255.255.0**

S1(config-if)# **no shut**

S1(config-if)# **exit**

S1(config)#

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**

S1#

* 1. Configure an IP address on PC-A.

Assign the IP address and subnet mask to the PC, as shown in the Addressing Table.

1. Verify and Test Network Connectivity

You will now 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.

* 1. Display the S1 device configuration.

Return to your console connection using **Hyperterminal** on PC-A. Issue the **show run** command to display and verify your switch configuration. A sample configuration is shown below. The settings you configured are highlighted in yellow. The other configuration settings are IOS defaults.

S1# **show run**

Building configuration...

Current configuration : 1508 bytes

!

! Last configuration change at 00:06:11 UTC Mon Mar 1 1993

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no 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

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

!

interface FastEthernet0/1

!

interface FastEthernet0/2

<output omitted>

interface FastEthernet0/24

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface Vlan1

ip address 192.168.1.2 255.255.255.0

!

ip http server

ip http secure-server

!

banner motd ^C

Unauthorized access is strictly prohibited. ^C

!

line con 0

password cisco

login

line vty 0 4

password cisco

login

line vty 5 15

login

!

end

Verify the status of your SVI management interface. Your VLAN 1 interface should be up/up and have an IP address assigned. Notice that switch port **F0/6** is also up because PC-A is connected to it. Because all switch ports are initially in VLAN 1, by default, you can communicate with the switch using the IP address you configured for VLAN 1.

S1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Vlan1 192.168.1.2 YES manual up up

FastEthernet0/1 unassigned YES unset down down

FastEthernet0/2 unassigned YES unset down down

FastEthernet0/3 unassigned YES unset down down

FastEthernet0/4 unassigned YES unset down down

FastEthernet0/5 unassigned YES unset down down

FastEthernet0/6 unassigned YES unset up up

FastEthernet0/7 unassigned YES unset down down

FastEthernet0/8 unassigned YES unset down down

FastEthernet0/9 unassigned YES unset down down

FastEthernet0/10 unassigned YES unset down down

FastEthernet0/11 unassigned YES unset down down

FastEthernet0/12 unassigned YES unset down down

FastEthernet0/13 unassigned YES unset down down

FastEthernet0/14 unassigned YES unset down down

FastEthernet0/15 unassigned YES unset down down

FastEthernet0/16 unassigned YES unset down down

FastEthernet0/17 unassigned YES unset down down

FastEthernet0/18 unassigned YES unset down down

FastEthernet0/19 unassigned YES unset down down

FastEthernet0/20 unassigned YES unset down down

FastEthernet0/21 unassigned YES unset down down

FastEthernet0/22 unassigned YES unset down down

FastEthernet0/23 unassigned YES unset down down

FastEthernet0/24 unassigned YES unset down down

GigabitEthernet0/1 unassigned YES unset down down

GigabitEthernet0/2 unassigned YES unset down down

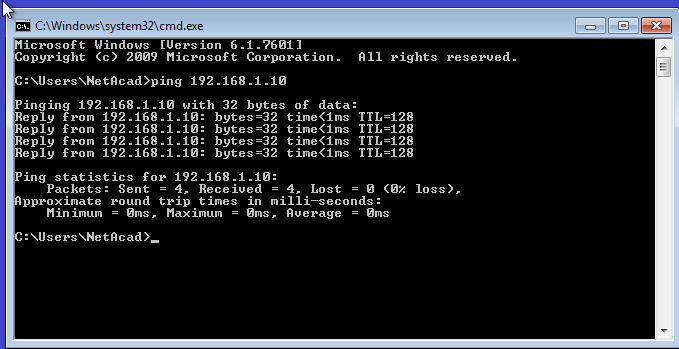
* 1. Test end-to-end connectivity.

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.

Ping the PC-A address first.

C:\Users\NetAcad> **ping 192.168.1.10**

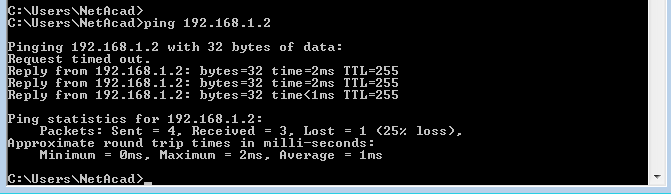
Your output should be similar to the following screen:



Ping the SVI management address of **S1**.

C:\Users\NetAcad> **ping 192.168.1.2**

Your output should be similar to the following screen. If ping results are not successful, troubleshoot the basic device configurations. You should check both the physical cabling and IP addressing if necessary.



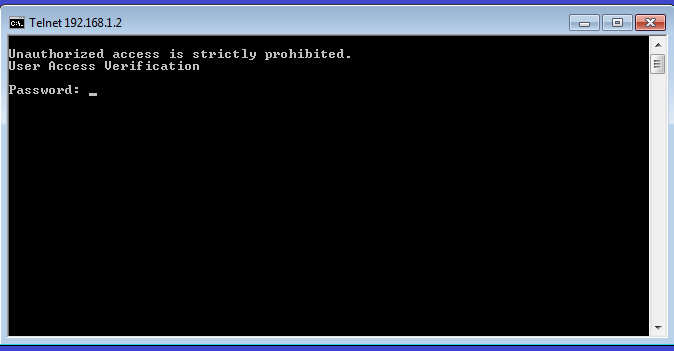
* 1. Test and verify the remote management of S1.

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.

With the command prompt 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\NetAcad> **telnet 192.168.1.2**

Your output should be similar to the following screen:



After entering the **cisco** password, you will be at the user EXEC mode prompt. Type **enable** at the prompt. Enter the **class** password to enter privileged EXEC mode and issue a **show run** command.

* 1. Save the configuration file.

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#

* 1. 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.)

S1# **erase startup-config**

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

S1#

* 1. 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.)

S1# **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**

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