Shaheed Zulfikar Ali Bhutto
Institute of Science & Technology

Computer Networks and Data Communications

(CSCL 3205)

Laboratory Manual

(Spring 2024)

Student Name: Sabih Ul Hassan

Roll No: 2112126

Section: BSCS VI-A

Lab Instructor:
Idrees Darbar

Experiment#02

Lab# 2.1:- Packet Tracer - Navigating the IOS

Topology

Objectives

Part 1: Basic Connections, Accessing the CLI and Exploring Help

Part 2: Exploring EXEC Modes

Part 3: Setting the Clock

Background

In this activity, you will practice skills necessary for navigating the Cisco IOS, including different user access modes, various configuration modes, and common commands you use on a regular basis. You also practice accessing the context-sensitive Help by configuring the **clock** command.

Part 1: Basic Connections, Accessing the CLI and Exploring Help

In Part 1 of this activity, you connect a PC to a switch using a console connection and explore various command modes and Help features.

Step 1: Connect PC1 to S1 using a console cable.

a. Click the **Connections** icon (the one that looks like a lightning bolt) in the lower left corner of the Packet Tracer window.

b. Select the light blue Console cable by clicking it. The mouse pointer will change to what appears to be a connector with a cable dangling off of it.

c. Click **PC1**; a window displays an option for an RS-232 connection.

d. Drag the other end of the console connection to the S1 switch and click the switch to bring up the connection list.

e. Select the Console port to complete the connection.

Step 2: Establish a terminal session with S1.

a. Click **PC1** and then select the **Desktop** tab.

b. Click the **Terminal** application icon; verify that the Port Configuration default settings are correct.

What is the setting for bits per second? 960

c. Click **OK**.

d. The screen that appears may have several messages displayed. Somewhere on the display there should be a Press RETURN to get started! message. Press **ENTER**.

What is the prompt displayed on the screen? Switch

Step 3: Explore the IOS Help.

a. The IOS can provide help for commands depending on the level being accessed. The prompt currently being displayed is called **User EXEC** and the device is waiting for a command. The most basic form of help is to type a question mark (?) at the prompt to display a list of commands.

S1> **?**

Which command begins with the letter 'C'? Connect

b. At the prompt, type **t**, followed by a question mark (**?**).

S1> **t?**

Which commands are displayed? Terminal

c. At the prompt, type **te**, followed by a question mark (**?**).

S1> **te?**

Which commands are displayed? Telnet

This type of help is known as **context-sensitive** Help, providing more information as the commands are expanded.

Part 2: Exploring EXEC Modes

In Part 2 of this activity, you switch to privileged EXEC mode and issue additional commands.

Step 1: Enter privileged EXEC mode.

a. At the prompt, type the question mark (**?**).

S1> **?**

What information is displayed that describes the **enable** command? Description of the enable command.

b. Type **en** and press the **Tab** key.

S1> **en<Tab>**

What displays after pressing the **Tab** key? "enable"

This is called command completion or tab completion. When part of a command is typed, the **Tab** key can be used to complete the partial command. If the characters typed are enough to make the command unique, as in the case with the **enable** command, the remaining portion is displayed.

What would happen if you were to type **te<Tab>** at the prompt?
If you were to type "te<Tab>", nothing would occur because there isn't a command that starts with "te" and is distinct enough to trigger tab completion.

c. Enter the **enable** command and press **ENTER**. How does the prompt change?
The prompt changes from "S1>" to "S1#"

d. When prompted, type the question mark (**?**).

S1# **?**

Previously there was one command that started with the letter 'C' in user EXEC mode. How many commands are displayed now that privileged EXEC mode is active? (**Hint**: you could type c? to list just the commands beginning with 'C'.)
Clear, clock, configure, connect, and copy

Step 2: Enter Global Configuration mode.

a. One of the commands starting with the letter 'C' is **configure** when in Privileged EXEC mode. Type either the full command or enough of the command to make it unique along with the <**Tab**> key to issue the command and press **<ENTER>**.

S1# **configure**

What is the message that is displayed?
S1(config)#

b. Press the **<ENTER>** key to accept the default parameter enclosed in brackets **[terminal]**.

How does the prompt change? S1(config)#

c. This is called global configuration mode. This mode will be explored further in upcoming activities and labs. For now exit back to Privileged EXEC mode by typing **end**, **exit** or **Ctrl-Z**.

S1(config)# **exit**
S1#

Part 3: Setting the Clock

Step 1: Use the clock command.

a. Use the **clock** command to further explore Help and command syntax. Type **show clock** at the privileged EXEC prompt.

S1# **show clock**

What information is displayed? What is the year that is displayed?
Usually, the displayed information includes both the present date and time.

b. Use the context-sensitive Help and the **clock** command to set the time on the switch to the current time. Enter the command **clock** and press **ENTER**.

S1# **clock<ENTER>**

What information is displayed? It would show a message indicating an unfinished command, signaling the need for additional parameters.

c. The % Incomplete command message is returned by the IOS indicating that the **clock** command needs further parameters. Any time more information is needed help can be provided by typing a space after the command and the question mark (?).

S1# **clock ?**

What information is displayed? It will show details regarding the options and parameters accessible for the clock command.

d. Set the clock using the **clock set** command. Continue proceeding through the command one step at a time.

S1# **clock set ?**

What information is being requested? <1-31>: Day of the month, MONTH: Month of the year

What would have been displayed if only the **clock set** command had been entered and no request for help was made by using the question mark? Either an error message or a message indicating an incomplete command would probably be shown.

e. Based on the information requested by issuing the **clock set ?** command, enter a time of 3:00 p.m. by using the 24-hour format of 15:00:00. Check to see if further parameters are needed.

S1# **clock set 15:00:00 ?**

The output returns the request for more information:
<1-31> Day of the month
MONTH Month of the year

f. Attempt to set the date to 01/31/2035 using the format requested. It may be necessary to request additional help using the context-sensitive Help to complete the process. When finished, issue the **show clock** command to

display the clock setting. The resulting command output should display as:

S1# **show clock**

*15:0:4.869 UTC Tue Jan 31 2035

g. If you were not successful, try the following command to obtain the output above:

S1# **clock set 15:00:00 31 Jan 2035**

Step 2: Explore additional command messages.

a. The IOS provides various outputs for incorrect or incomplete commands as experienced in earlier sections. Continue to use the **clock** command to explore additional messages that may be encountered as you learn to use the IOS.

b. Issue the following command and record the messages:

S1# **cl**

What information was returned? Executing this command is likely to lead to an "Ambiguous command" error message.

S1# **clock**

What information was returned? It could potentially request additional parameters, contingent upon the particular configuration and needs.

S1# **clock set 25:00:00**

What information was returned?

Executing this command would typically lead to an "Invalid input detected at '^' marker" error message, signaling that the provided time is invalid as it exceeds 24 hours.

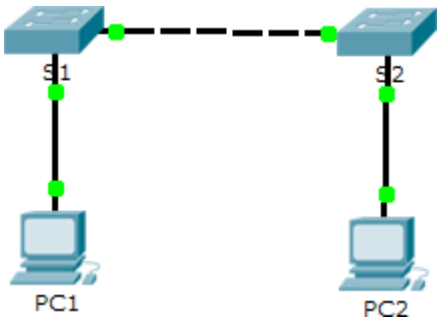
S1# **clock set 15:00:00 32**

What information was returned?

Similarly, executing this command is also likely to lead to an "Invalid input detected at '^' marker" error message because the specified day (32) is invalid. Days should fall within the range of 1 to 31.

Lab# 2.2:- Configuring Initial Switch Settings

Topology



Objectives

Part 1: Verify the Default Switch Configuration

Part 2: Configure a Basic Switch Configuration

Part 3: Configure a MOTD Banner

Part 4: Save Configuration Files to NVRAM

Part 5: Configure S2

Background

In this activity, you will perform basic switch configurations. You will secure access to the command-line interface (CLI) and console ports using encrypted and plain text passwords. You will also learn how to configure messages for users logging into the switch. These banners are also used to warn unauthorized users that access is prohibited.

Part 4: Verify the Default Switch Configuration

Step 1: Enter privileged mode.

You can access all switch commands from privileged mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use.

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.

a. Click **S1** and then the **CLI** tab. Press **<Enter>**.

b. Enter privileged EXEC mode by entering the **enable** command:

Switch> **enable**
Switch#

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Step 2: Examine the current switch configuration.

a. Enter the **show running-config** command.

Switch# **show running-config**

b. Answer the following questions:

How many FastEthernet interfaces does the switch have? 24

How many Gigabit Ethernet interfaces does the switch have? 2

What is the range of values shown for the vty lines? 0 to 15

Which command will display the current contents of non-volatile random-access memory (NVRAM)?
Show startup-config.

Why does the switch respond with startup-config is not present?
The switch replies with "startup-config is not present" because there isn't a saved configuration in the non-volatile RAM (NVRAM).

Part 5: Create a Basic Switch Configuration

Step 1: Assign a name to a switch.

To configure parameters on a switch, you may be required to move between various configuration modes. Notice how the prompt changes as you navigate through the switch.

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# exit
S1#
```

Step 2: Secure access to the console line.

To secure access to the console line, access config-line mode and set the console password to **letmein**.

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# line console 0
S1(config-line)# password letmein
S1(config-line)# login
S1(config-line)# exit
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Why is the **login** command required?
To enforce password authentication.

Step 3: Verify that console access is secured.

Exit privileged mode to verify that the console port password is in effect.

```
S1# exit
Switch con0 is now available
Press RETURN to get started.

User Access Verification
Password:
S1>
```

Note: If the switch did not prompt you for a password, then you did not configure the **login** parameter in Step 2.

Step 4: Secure privileged mode access.

Set the **enable** password to **c1$c0**. This password protects access to privileged mode.

Note: The **0** in **c1$c0** is a zero, not a capital O. This password will not grade as correct until after you encrypt it in Step 8.

S1> **enable**
S1# **configure terminal**
S1(config)# **enable password c1$c0**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#

Step 5: Verify that privileged mode access is secure.

a. Enter the **exit** command again to log out of the switch.

b. Press **<Enter>** and you will now be asked for a password:

User Access Verification
Password:

c. The first password is the console password you configured for **line con 0**. Enter this password to return to user EXEC mode.

d. Enter the command to access privileged mode.

e. Enter the second password you configured to protect privileged EXEC mode.

f. Verify your configurations by examining the contents of the running-configuration file:

S1# **show running-config**

Notice how the console and enable passwords are both in plain text. This could pose a security risk if someone is looking over your shoulder.

Step 6: Configure an encrypted password to secure access to privileged mode.

The **enable password** should be replaced with the newer encrypted secret password using the **enable secret** command. Set the enable secret password to **itsasecret**.

S1# **config t**
S1(config)# **enable secret itsasecret**
S1(config)# **exit**
S1#

Note: The **enable secret** password overrides the **enable** password. If both are configured on the switch, you must enter the **enable secret** password to enter privileged EXEC mode.

Step 7: Verify that the enable secret password is added to the configuration file.

a. Enter the **show running-config** command again to verify the new **enable secret** password is configured.

Note: You can abbreviate **show running-config** as
S1# **show run**

b. What is displayed for the **enable secret** password? enable secret 5 1mERr$ILwq/b7kc.7X/ejA4Aosn0

c. Why is the **enable secret** password displayed differently from what we configured?
The display of the enable secret password differs because it is encrypted within the configuration file for security reasons.

Step 8: Encrypt the enable and console passwords.

As you noticed in Step 7, the **enable secret** password was encrypted, but the **enable** and **console** passwords were still in plain text. We will now encrypt these plain text passwords using the **service password-encryption** command.

S1# **config t**

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

S1(config)# **exit**

If you configure any more passwords on the switch, will they be displayed in the configuration file as plain text or in encrypted form? Explain why?

Passwords set on the switch subsequent to enabling the service password-encryption feature will appear in encrypted form within the configuration file. This occurs because the service password-encryption command encrypts all passwords configured on the device, irrespective of the method employed to establish them.

Part 6: Configure a MOTD Banner

Step 1: Configure a message of the day (MOTD) banner.

The Cisco IOS command set includes a feature that allows you to configure messages that anyone logging onto the switch sees. These messages are called message of the day, or MOTD banners. Enclose the banner text in quotations or use a delimiter different from any character appearing in the MOTD string.

S1# **config t**

S1(config)# **banner motd "This is a secure system. Authorized Access Only!"**

S1(config)# **exit**

%SYS-5-CONFIG_I: Configured from console by console

S1#

When will this banner be displayed?

Whenever someone logs onto the switch, this banner will be presented.

Why should every switch have a MOTD banner?

A MOTD banner serves as a crucial tool for conveying essential warnings or messages to users accessing the system. Its presence promotes security and compliance by ensuring users are aware of network rules and regulations.

Part 7: Save Configuration Files to NVRAM

Step 1: Verify that the configuration is accurate using the show run command.

Step 2: Save the configuration file.

You have completed the basic configuration of the switch. Now back up the running configuration file to NVRAM to ensure that the changes made are not lost if the system is rebooted or loses power.

S1# **copy running-config startup-config**

Destination filename [startup-config]?**[Enter]**

Building configuration...

[OK]

What is the shortest, abbreviated version of the **copy running-config startup-config** command? Copy run start

Step 3: Examine the startup configuration file.

Which command will display the contents of NVRAM? show startup-config

Are all the changes that were entered recorded in the file? Yes

Part 8: Configure S2

You have completed the configuration on S1. You will now configure S2. If you cannot remember the commands, refer to Parts 1 to 4 for assistance.

Configure S2 with the following parameters:

a. Name device: **S2**

b. Protect access to the console using the **letmein** password.

c. Configure an enable password of **c1$c0** and an enable secret password of **itsasecret**.

d. Configure a message to those logging into the switch with the following message:

Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.

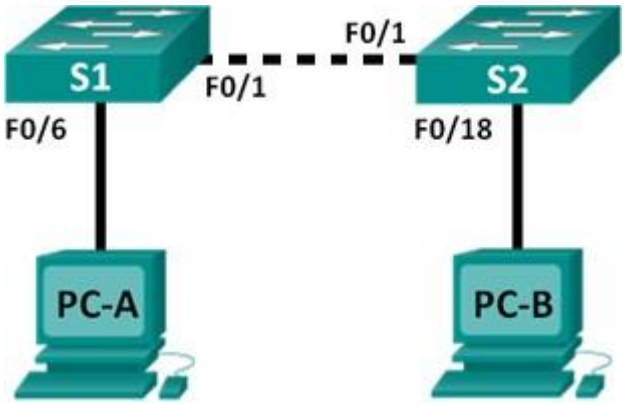
e. Encrypt all plain text passwords.

f. Ensure that the configuration is correct.

g. Save the configuration file to avoid loss if the switch is powered down.

Lab# 2.3: - Implement Basic Connectivity

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC-A	NIC	192.168.1.1	255.255.255.0
PC-**B**	NIC	192.168.1.2	255.255.255.0

Objectives

Part 1: Perform a Basic Configuration on S1 and S2

Part 2: Configure the PCs

Part 3: Configure the Switch Management Interface

Background

In this activity you will first perform basic switch configurations. Then you will implement basic connectivity by configuring IP addressing on switches and PCs. When the IP addressing configuration is complete, you will use various **show** commands to verify configurations and use the **ping** command to verify basic connectivity between devices.

Part 9: Perform a Basic Configuration on S1 and S2

Complete the following steps on S1 and S2.

Step 1: Configure S1 with a hostname.

a. Click **S1**, and then click the **CLI** tab.

b. Enter the correct command to configure the hostname as **S1**.

Step 2: Configure the console and privileged EXEC mode passwords.

a. Use **cisco** for the console password.

b. Use **class** for the privileged EXEC mode password.

Step 3: Verify the password configurations for S1.

How can you verify that both passwords were configured correctly?

To validate passwords, try accessing privileged EXEC mode and examine the configuration for encryption. You can also utilize commands like "show running-config" or "show startup-config" to inspect the configuration and verify if passwords are encrypted.

Step 4: Configure a message of the day (MOTD) banner.

Use an appropriate banner text to warn unauthorized access. The following text is an example:

Authorized access only. Violators will be prosecuted to the full extent of the law.

Step 5: Save the configuration file to NVRAM.

Which command do you issue to accomplish this step?

The command to store the configuration file to NVRAM is "copy running-config startup-config" or its shortened version "copy run start".

Step 6: Repeat Steps 1 to 5 for S2.

Part 10: Configure the PCs

Configure PC1 and PC2 with IP addresses.

Step 1: Configure both PCs with IP addresses.

a. Click **PC-A**, and then click the **Desktop** tab.

b. Click **IP Configuration**. In the **Addressing Table** above, you can see that the IP address for PC1 is 192.168.1.1 and the subnet mask is 255.255.255.0. Enter this information for PC1 in the **IP Configuration** window.

c. Repeat steps 1a and 1b for PC-B.

Step 2: Test connectivity to switches.

a. Click **PC1**. Close the **IP Configuration** window if it is still open. In the **Desktop** tab, click **Command Prompt**.
.

b. Type the **ping** command and the IP address for S1, and press **Enter**.

Packet Tracer PC Command Line 1.0
PC> **ping 192.168.1.253**

Were you successful? Why or why not?

The attempt was unsuccessful as all four packets sent to the IP address 192.168.1.253 timed out.

Part 11: Configure the Switch Management Interface

Configure S1 and S2 with an IP address.

Step 1: Configure S1 with an IP address. Also configure Virtual Terminal Line (VTY):

Switches can be used as a plug-and-play device, meaning they do not need to be configured for them to work. Switches forward information from one port to another based on Media Access Control (MAC) addresses. If this is the case, why would we configure it with an IP address?

Enables administrators to manage and monitor systems remotely over the network, simplifying configuration and troubleshooting processes without requiring physical access.

a. Use the following commands to configure S1 with an IP address.

S1 #**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# **interface vlan 1**
S1(config-if)# **ip address 192.168.1.253 255.255.255.0**
S1(config-if)# **no shutdown**
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#
S1(config-if)# **exit**
S1#

Why do you need to enter the **no shutdown** command?

This command activates the VLAN interface, which is initially administratively shut down, thereby permitting the passage of traffic through it.

b. Configure the virtual terminal (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#
```

Step 2: Configure S2 with an IP addresses.

Use the information in the addressing table to configure S2 with an IP address.

Step 3: Verify the IP address configuration on S1 and S2.

Use the **show ip interface brief** command to display the IP address and status of the all the switch ports and interfaces. Alternatively, you can also use the **show running-config** command.

Step 4: Save configurations for S1 and S2 to NVRAM.

Which command is used to save the configuration file in RAM to NVRAM? copy running-config startup-config or copy run start

Step 5: Verify network connectivity.

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure. Ping S1's and S2's IP address from PC1 and PC2.

a. Click **PC-A**, and then click the **Desktop** tab.

b. Click **Command Prompt**.

c. Ping the IP address for PC-B.

d. Ping the IP address for S1.

e. Ping the IP address for S2.

Note: You can also use the same **ping** command on the switch CLI and on PC-B.

All pings should be successful. If your first ping result is 80%, retry; it should now be 100%. You will learn why a ping may fail the first time later in your studies. If you are unable to ping any of the devices, recheck your configuration for errors.

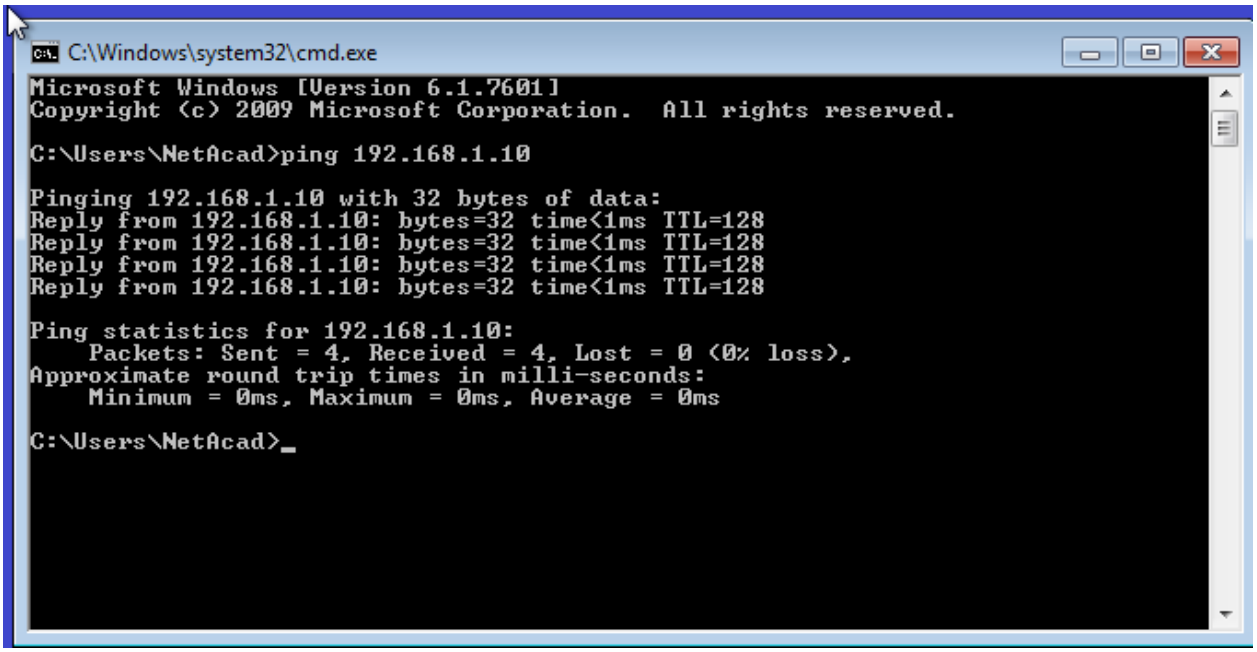
Step 6: Test end-to-end connectivity.

Open a command prompt window (cmd.exe) on PC-A by clicking the **Windows Start** icon and enter **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 own address and the management address of S1.

a. Ping your own PC-A address first.

C:\Users\NetAcad> **ping 192.168.1.1**

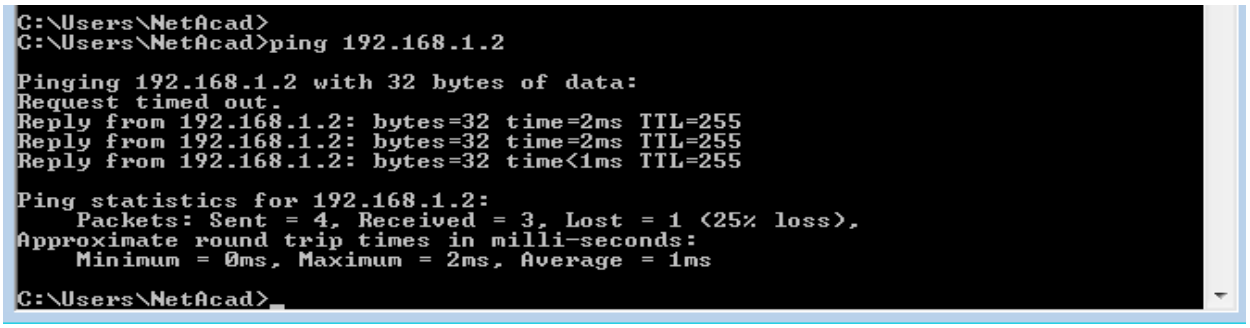
Your output should be similar to the following screen:



b. 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.



Step 7: Test and verify 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 plain text. In subsequent labs, you will use Secure Shell (SSH) to remotely access network devices.

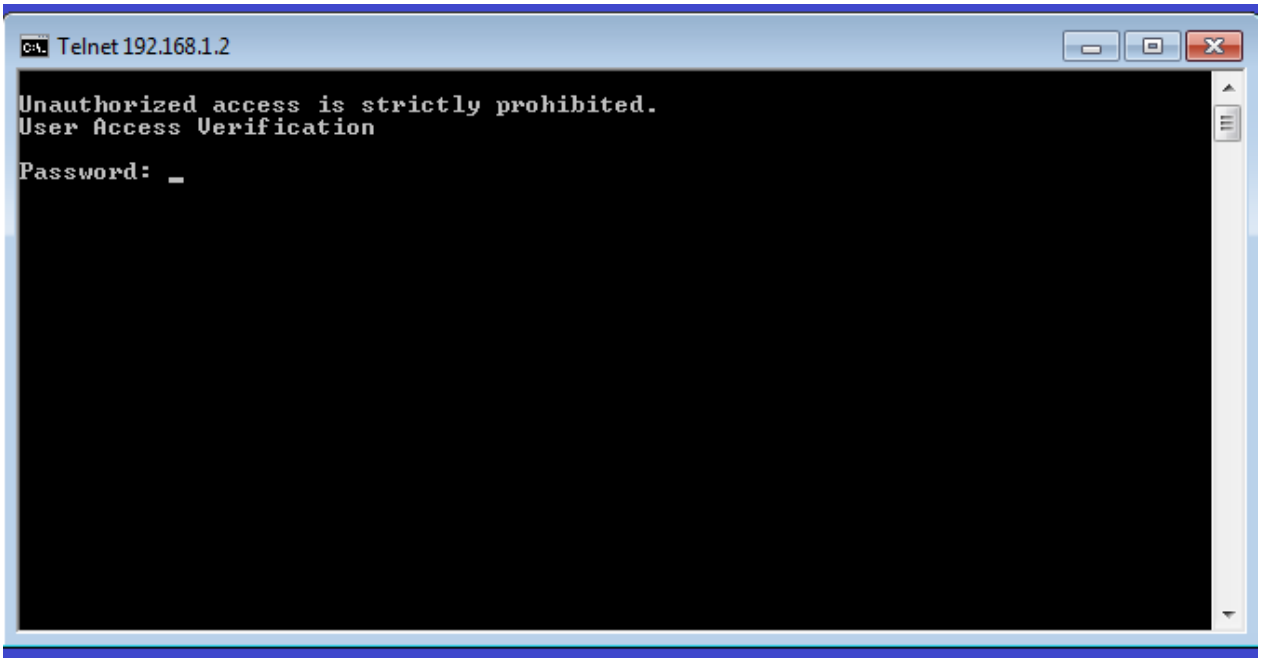
Note: Windows 7 does not natively support Telnet. The administrator must enable this protocol. To install the Telnet client, open a command prompt window and type **pkgmgr /iu:"TelnetClient"**.

C:\Users\NetAcad> **pkgmgr /iu:"TelnetClient"**

a. 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 192.168.1.253**

Your output should be similar to the following screen:



b. 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.

Reflection

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

The console connection offers direct access for initial configuration without depending on network connectivity. Console access ensures a secure method of configuration, particularly in environments where network connectivity or remote access services might not be configured or secured yet.

Lab's Evaluation Sheet

Students Registration No:	2112126
Date Performed:	25th February 2024
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	Student's Behavior	2.5	
2	Lab Performance	2.5	
3	On Time Submission	5	
4	Home Activity	10	
	Net Result	20	

Examined By: (Instructor's Name & Initial's)

Date