**Experiment 1**

**Aim:** To construct and understand RJ45 connectors.

**Theory:** T568A and T568B are two standards for wiring twisted-pair Ethernet cables using 8-position, 8-contact (8P8C) connectors, commonly known as RJ45 connectors. The main difference between the two is the order of the green and orange wire pairs. T568A arranges the wires with the white/green and green pair first, while T568B places the white/orange and orange pair first. Both standards are functionally equivalent, providing the same electrical performance, and can be used interchangeably. However, it's important to use the same standard on both ends of a cable for a straight-through connection. T568B is more widely used in North America, while T568A is common in government installations and in Europe.

**Tools and Materials Needed:**

1. Twisted-pair cable (Cat5, Cat5e, Cat6)
2. RJ45 connectors
3. Cable stripper
4. Crimping tool
5. Cable tester (optional but recommended)

**T568A Wiring Standard:**

The T568A standard arranges the wires as follows, from Pin 1 to Pin 8:

1. White/Green
2. Green
3. White/Orange
4. Blue
5. White/Blue
6. Orange
7. White/Brown
8. Brown

**T568B Wiring Standard:**

The T568B standard arranges the wires as follows, from Pin 1 to Pin 8:

1. White/Orange
2. Orange
3. White/Green
4. Blue
5. White/Blue
6. Green
7. White/Brown
8. Brown

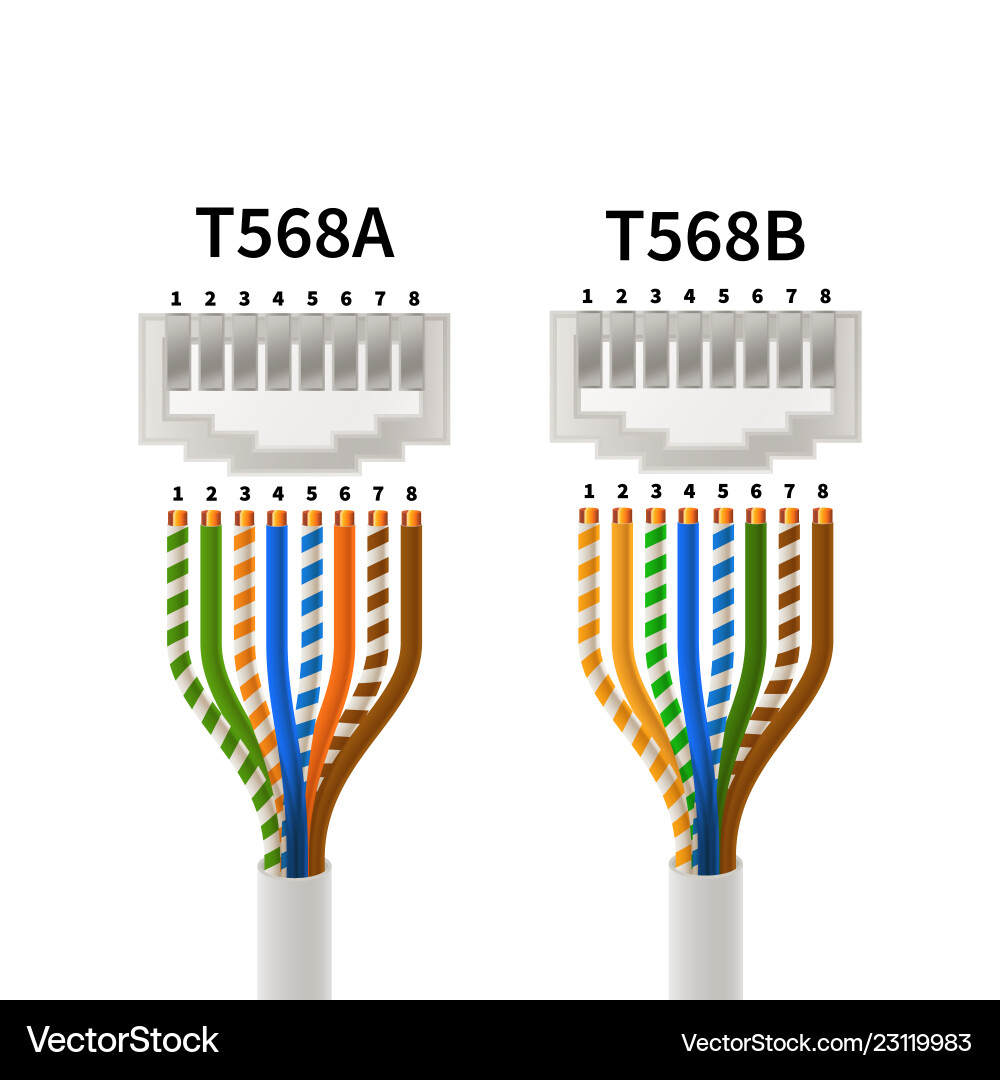
**Building a Straight-Through Cable:**

1. Strip the Cable: Remove about 1-2 inches of the outer jacket of the Ethernet cable, exposing the twisted pairs inside.
2. Untwist and Arrange Wires: Untwist the pairs and arrange them according to either the T568A or T568B standard, ensuring that the wires are straightened out and in the correct order.
3. Trim the Wires: Trim the wires evenly, leaving about 0.5 inches exposed beyond the jacket.
4. Insert Wires into the RJ45 Connector: With the clip side down, insert the wires into the RJ45 connector, making sure each wire goes into its correct slot.
5. Crimp the Connector: Use the crimping tool to secure the connector onto the cable, ensuring a firm connection.
6. Repeat for the Other End: Repeat the process for the other end of the cable, using the same wiring standard (T568A or T568B) to create a straight-through cable.
7. Test the Cable: Optionally, use a cable tester to verify that the connections are correct and that the cable is functioning properly.

**Building a Crossover Cable:**

A crossover cable is used to connect similar devices, such as two computers or two switches, directly. It involves wiring one end with T568A and the other end with T568B.

1. Prepare the Cable: As before, strip the cable jacket and untwist the pairs.
2. Wiring One End (T568A): Follow the T568A wiring standard for the first connector.
3. Wiring the Other End (T568B): Follow the T568B wiring standard for the second connector.
4. Crimp the Connectors: Securely crimp both connectors onto the cable.
5. Test the Cable: Use a cable tester to ensure that the crossover wiring is correct and the cable is functional.



**Experiment 2**

**Aim:** Navigate the IOS (Packet Tracer 2.3.7)

**Theory:** In this exercise, the objective is to familiarize with the Cisco IOS by learning to access and navigate the Command Line Interface (CLI). This includes establishing basic connections, exploring different EXEC modes (User and Privileged), and using the Help system to understand commands. Additionally, the exercise involves practical tasks such as setting the system clock, demonstrating how to apply basic configuration commands.

**Instructions:**

* **Part 1: Establish Basic Connections, Access the CLI, and Explore Help**

**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 from it.

c.     Click **PC1**. A window displays an option for an RS-232 connection. Connect the cable to the RS-232 port.

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

e.     Select the **Console** port to complete the connection.

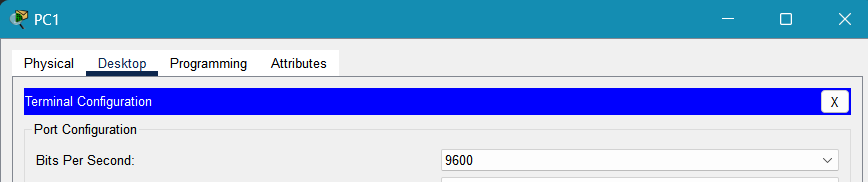
**Step 2: Establish a terminal session with S1.**

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

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

Question:

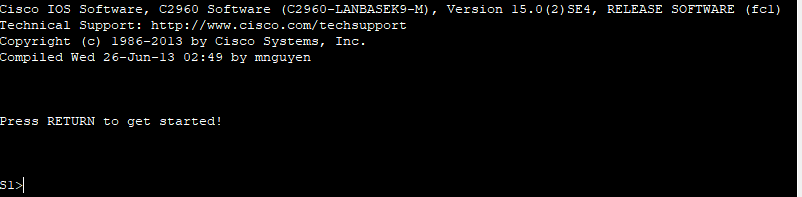
What is the setting for bits per second?



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

Question:

What is the prompt displayed on the screen?



**Step 3: Explore the IOS Help.**

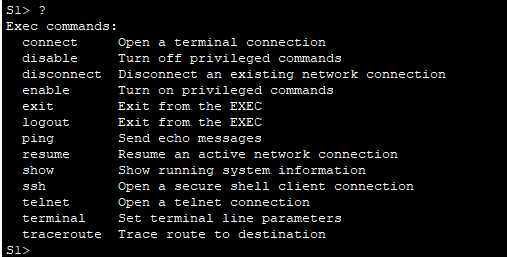
a.     The IOS can provide help for commands depending on the level accessed. The prompt currently displayed is called **User EXEC**, and the device is waiting for a command. The most basic form of help is to type a question mark (?) at the prompt to display a list of commands.

*Open Configuration Window*

S1> **?**

Question:

Which command begins with the letter ‘C’?



b.     At the prompt, type t and then a question mark (?).

S1> **t?**

Question:

Which commands are displayed?



At the prompt, type te and then a question mark (?).

S1> **te?**

Question:

Which commands are displayed?



This type of help is known as context-sensitive help. It provides more information as the commands are expanded.

* **Part 2: Explore EXEC Modes**

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

**Step 1: Enter privileged EXEC mode.**

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

S1> **?**

Question:

What information is displayed for the **enable** command?



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

S1> **en<Tab>**

Question:

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



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 of the **enable** command, the remaining portion of the command is displayed.

Question:

What would happen if you typed **te<Tab>**at the prompt?



c.     Enter the **enable** command and press ENTER.

Question:

How does the prompt change?



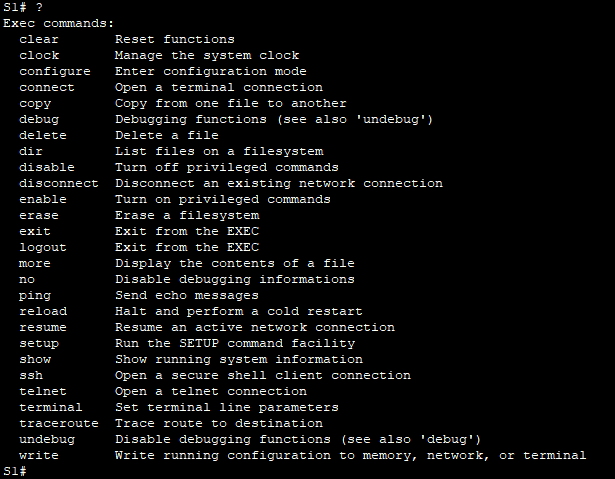
d.     When prompted, type the question mark (**?**).

S1# **?**

One command starts with the letter ‘C’ in user EXEC mode.

Question:

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’.)



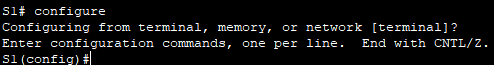
**Step 2: Enter Global Configuration mode**

a.     When in privileged EXEC mode, one of the commands starting with the letter ‘C’ is **configure**. Type either the full command or enough of the command to make it unique. Press the <**Tab**> key to issue the command and press ENTER.

S1# **configure**

Question:

What is the message that is displayed?



b.     Press Enter to accept the default parameter that is enclosed in brackets **[terminal]**.

Question:

How does the prompt change?



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

S1(config)# **exit**

S1#

* **Part 3: Set 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**

Question:

What information is displayed? What is the year that is displayed?



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>**

Question

What information is displayed?



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

S1# **clock ?**

Question:

What information is displayed?



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

S1# **clock set ?**

Questions:

What information is being requested?

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?



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 more parameters are needed.

S1# **clock set 15:00:00 ?**

The output returns a 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 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. 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 commands and record the messages:

S1# **cl<tab>**

Questions:

What information was returned?



S1# **clock**

Question:

What information was returned?



S1# **clock set 25:00:00**

Question:

What information was returned?

A screen shot of a computer

Description automatically generated

S1# **clock set 15:00:00 32**

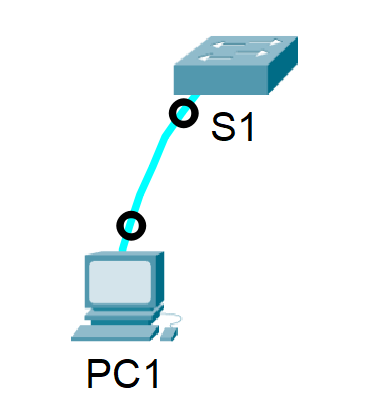
Question:

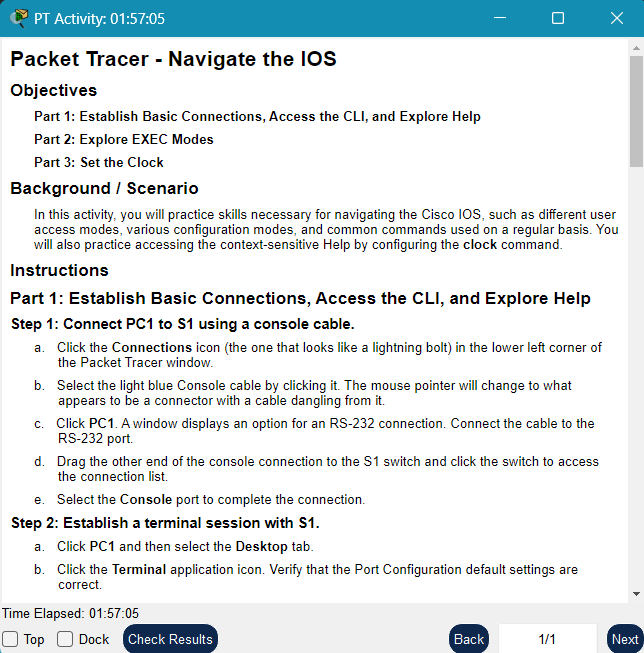
What information was returned?

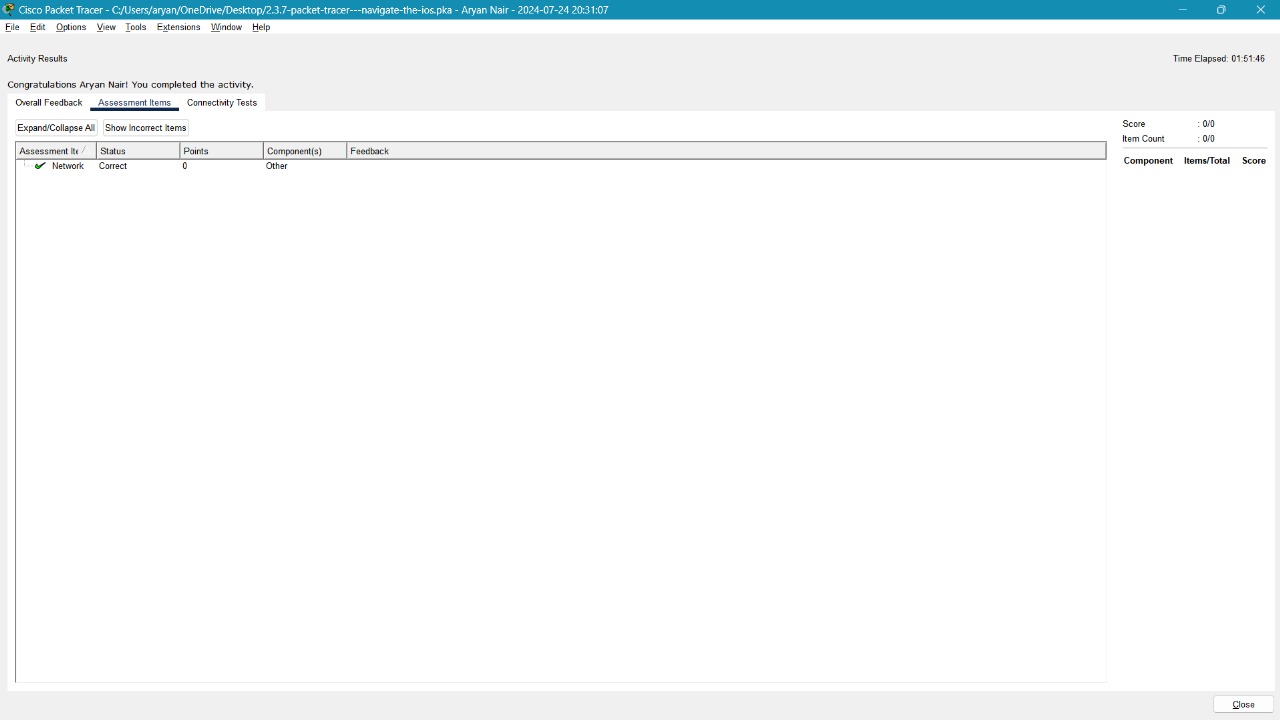
A screen shot of a black background

Description automatically generated

**Result:**

****





**Experiment 3**

**Aim:** Configure Initial Switch Settings (Packet Tracer 2.5.5)

**Theory:** In this exercise, the goal is to understand and apply basic configurations to a network switch. The exercise begins with verifying the default switch settings to establish a baseline. Next, it involves configuring fundamental settings such as hostname, passwords, and VLANs, which are essential for securing and managing the network environment. A Message of the Day (MOTD) banner is configured to provide important information or warnings to users accessing the switch. The final steps include saving the configuration changes to NVRAM to ensure they persist after a reboot and configuring an additional switch, S2, to replicate the setup and ensure network consistency.

**Instructions:**

* **Part 1: Verify the Default Switch Configuration**

**Step 1: Enter privileged EXEC mode.**

You can access all switch commands from privileged EXEC 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 the commands available in user EXEC mode, many additional commands, and the **configure**command through which access to the configuration modes is gained.

a.     Click S1 and then the CLI tab. Press Enter.

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

*Open Configuration Window for S1*

Switch> **enable**

Switch#

Notice that the prompt changed to reflect privileged EXEC mode.

**Step 2: Examine the current switch configuration.**

Enter the show running-config command.

Switch# **show running-config**

Answer the following questions:

How many Fast Ethernet interfaces does the switch have?

How many Gigabit Ethernet interfaces does the switch have?

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

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

Why does the switch respond with “startup-config is not present?”

* **Part 2: 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#

Question:

Why is the **login** command required?

**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 configuration by examining the contents of the running-configuration file:

S1# **show running-config**

Notice that the console and enable passwords are both in plain text. This could pose a security risk if someone is looking over your shoulder or obtains access to config files stored in a backup location.

**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.**

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**

Questions:

What is displayed for the enable secret password?

Why is the enable secret password displayed differently from what we configured?

**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**

Question:

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.

* **Part 3: 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#

Questions:

When will this banner be displayed?

Why should every switch have a MOTD banner?

* **Part 4: Save and Verify Configuration Files to NVRAM**

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

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]

*Close Configuration Window for S1*

Questions:

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

Examine the startup configuration file.

Which command will display the contents of NVRAM?

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

* **Part 5: 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:**

*Open Configuration Window for S2*

a.     Device name: **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**.

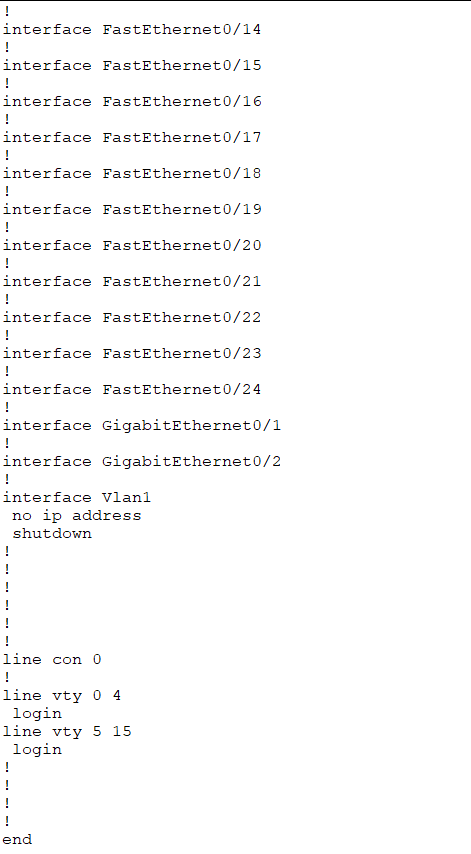
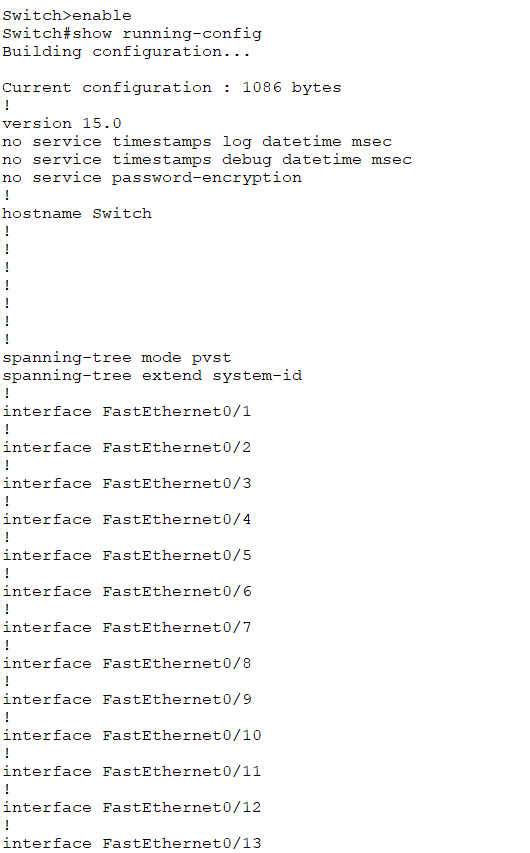
d.     Configure an appropriate message to those logging into the switch.

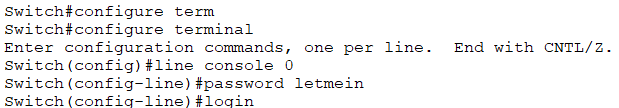
e.     Encrypt all plain text passwords.

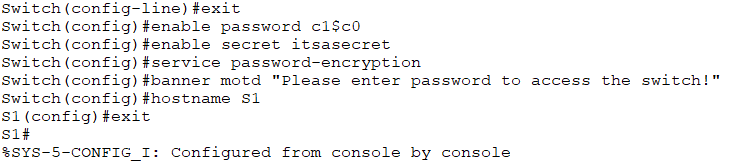
f.      Ensure that the configuration is correct.

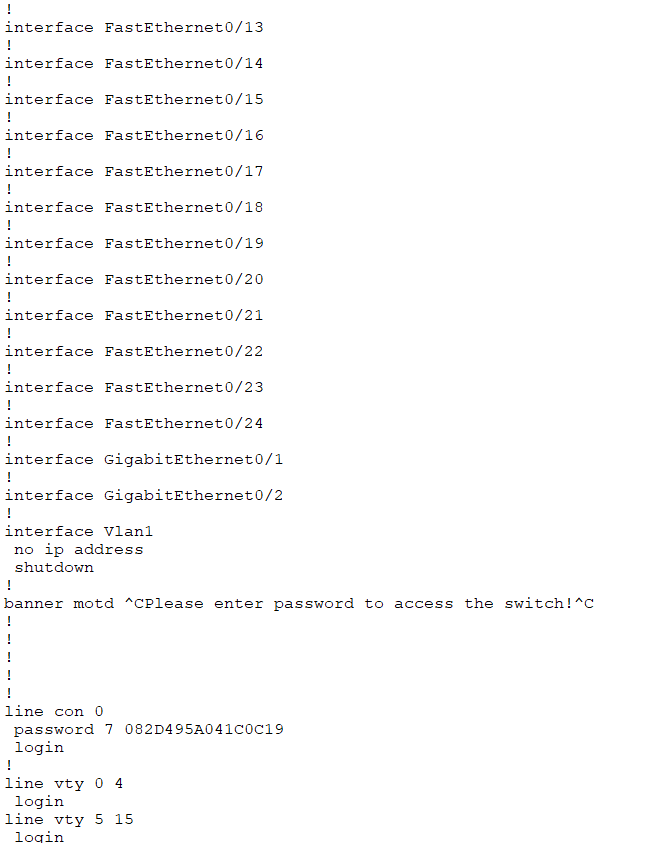
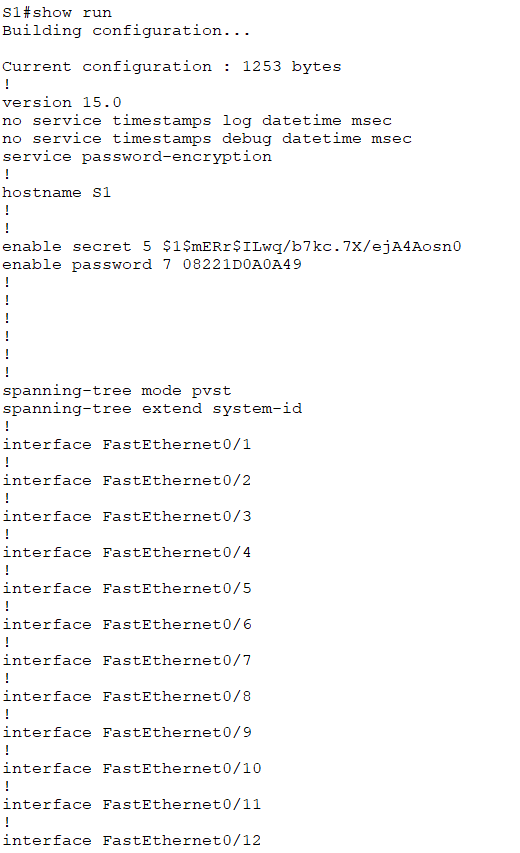
g.     Save the configuration file to avoid loss if the switch is powered down.

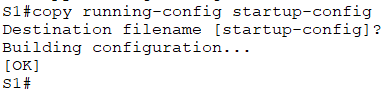
**Commands:**

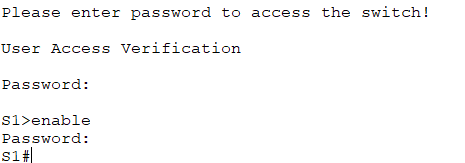




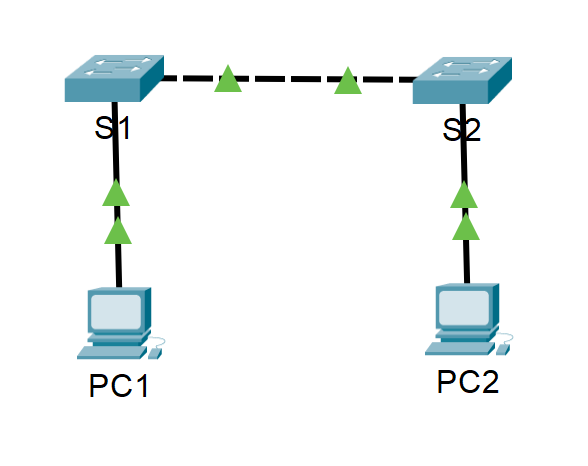


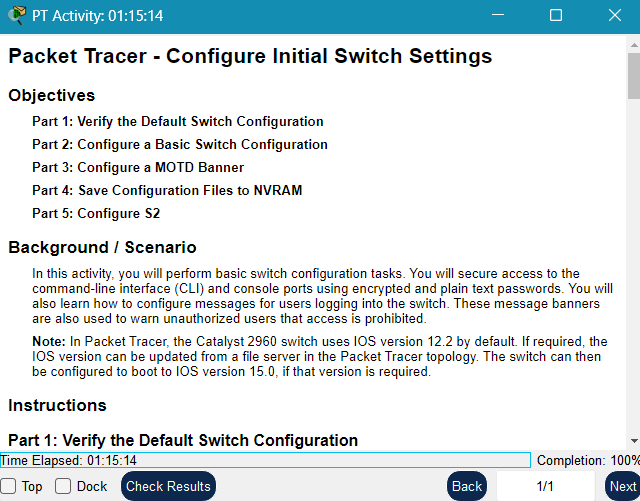


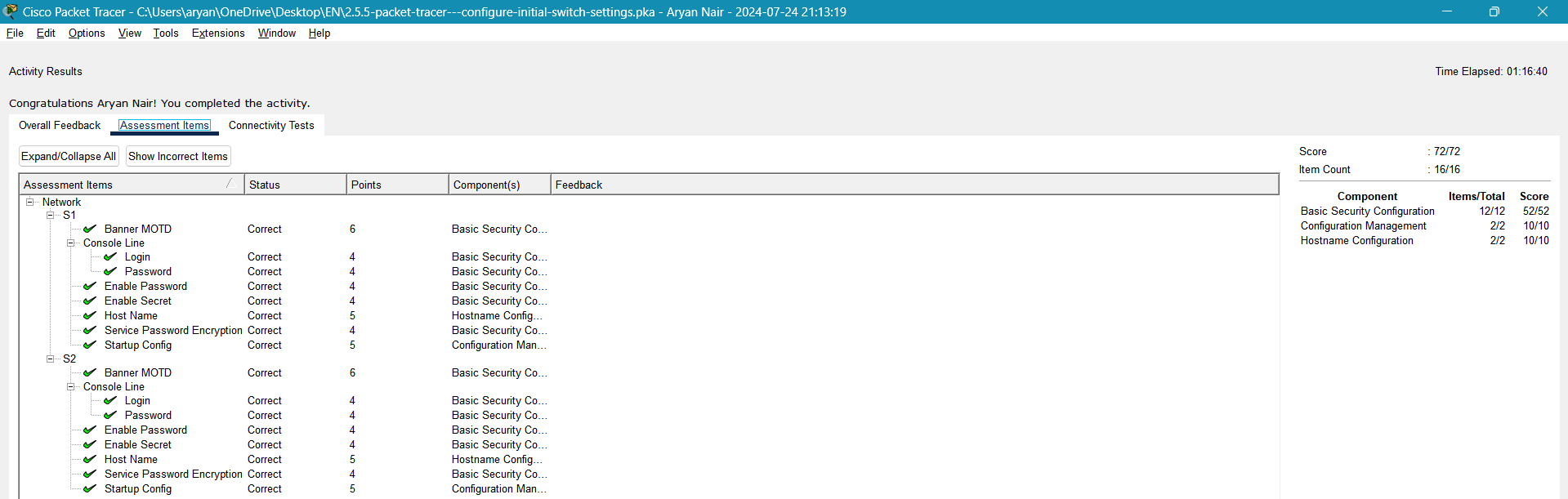


****

**Result:**







**Experiment 4**

**Aim:** Configure Initial Switch Settings (Packet Tracer 2.7.6)

**Theory:** In Packet Tracer, establishing basic connectivity involves configuring switches (S1 and S2) and PCs (PC1 and PC2) with appropriate settings. First, each switch is given a hostname and secured with console and privileged EXEC mode passwords. A warning banner is added for unauthorized access, and configurations are saved to NVRAM. Next, PCs are configured with IP addresses (192.168.1.1 for PC1 and 192.168.1.2 for PC2), allowing them to communicate within the network. The switch management interfaces are configured with IP addresses, enabling remote management. Finally, network connectivity is verified using the ping command, ensuring that all devices can communicate successfully. This process ensures the foundational setup for a functioning network.

**Instructions:**

* **Part 1: 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 encrypted 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.**

Question:

How can you verify that both passwords were configured correctly?

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 4: Save the configuration file to NVRAM.**

Question:

Which command do you issue to accomplish this step?

**Step 5: Repeat Steps 1 to 5 for S2.**

* **Part 2: Configure the PCs**

Configure PC1 and PC2 with IP addresses.

**Step 1: Configure both PCs with IP addresses.**

a.     Click PC1 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 PC2.

**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**

Question:

* **Part 3: Configure the Switch Management Interface**

Configure S1 and S2 with an IP address.

**Step 1: Configure S1 with an IP address.**

Switches can be used as plug-and-play devices. This means that they do not need to be configured for them to work. Switches forward information from one port to another based on MAC addresses.

Question:

If this is the case, why would we configure it with an IP address?

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#

Question:

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

**Step 2: Configure S2 with an IP address.**

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 all the switch ports and interfaces. You can also use the **show running-config** command.

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

Question:

Which command is used to save the configuration file in RAM to NVRAM?

**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 and S2 from PC1 and PC2.

a.     Click PC1 and then click the Desktop tab.

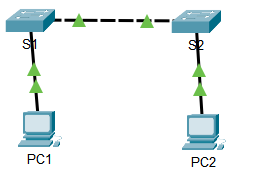
b.     Click Command Prompt.

c.     Ping the IP address for PC2.

d.     Ping the IP address for S1.

e.     Ping the IP address for S2.

**Result:**

****

A screenshot of a computer

Description automatically generated

