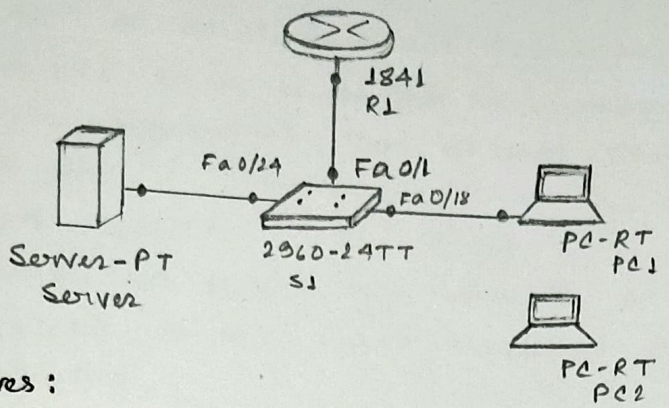
Assignment - 06

Configuring and Troubleshooting a Switched Network

Topology Diagram:



Objectives:

- Establish console connection to the switch.
- Configure the host name and VLAN1.
- Use the help feature to configure the clock.
- Configure the passwords and console/Telnet access.
- Configure login banners.
- Configure the router.
- Solve duplex and speed mismatch problems.
- Configure port security
- Manage the switch configuration file.

Background / Preparation:

In this Packet Tracer Skills Integration Challege activity, you will configure basic switch management, including general maintenance commands, passwords, and port security. This activity provides you an opportunity to review previously acquired skills.

Addressing Table:

Device	Interface	IP Address	Subnet Mask
R1	Fa 0/0	172.17.99.1	255.255.255.0
S1	Fa 0/1	172.17.99.11	255.255.255.0
PC1	NIC	172.17.99.21	255.255.255.0
PC2	NIC	172.17.99.22	255.255.255.0
Server	NIC	172.17.99.31	255.255.255.0

Step 1: Establish a console connection to a switch.

For this activity, direct access to the S1 config and CLI tabs is disabled. You must establish a console session through PC1.

a. Connect a console cable from PC1 to S1.

b. From PC1, open a terminal window and use the default terminal configuration. You should now have access to the CLI for S1.

c. Check results.

Your completion percentage should be 8%. If not, click Check Results to see which required components are not yet completed.

Step 2: Configure the host name and VLAN1.

a. Configure the switch host name as S1.

b. Configure port fa 0/1. Set the mode on Fast Ethernet 0/1 to access mode.

i. S1(config)# interface fastethernet 0/1

ii. S1(config)# switchport mode access

c. Configure IP connectivity on S1 using VLAN1.

i. S1(config)# interface vlan 1

ii. S1(config)# ip address 172.17.99.11 255.255.255.0

iii. S1(config-if)# no shutdown

d. Configure the default gateway for S1 and then test connectivity. S1 should be able to ping R1.

e. Check results.

Your completion percentage should be 31%. If not, click Check Results to see which required components are not yet completed. Also, make sure that interface VLAN1 is active.

Step 3: Configure the current time using Help.

a. Configure the clock to the current time. At the privileged EXEC prompt, enter clock ?

b. Use Help to discover the steps required to set the current time.

c. Use the show clock command to verify that the clock is

now set to the current time. Packet Tracer may not correctly simulate the time you entered.

Packet Tracer does not grade this command, so the completion percentage does not change.

Step 4: Configure passwords.

a. Use the encrypted form of the privileged EXEC mode password and set the password to class.

b. Configure the passwords for console and Telnet. Set both the console and vty password to cisco and required users to log in.

c. View the current configuration on S1. Notice that the line passwords are shown in clear text. Enter the command to encrypt these passwords.

d. Check results.

Your completion percentage should be 42%. If not, click Check Results to see which required components are not yet completed.

Step 5: Configure the login banner.

If you do not enter the banner text exactly as specified Packet Tracer does not grade your command correctly. These commands are case-sensitive. Also make sure that you do not include any spaces before or after the text.

a. Configure the message-of-the-day banner on S1 to display as Authorized access only. (Do not include the period.)

b. Check results.

Your completion percentage should be 48%. If not, click Check Results to see which required components are not yet completed.

Step 6: Configure the router:

Routers and switches share many of the same commands. Configure the router with the same basic commands you used on S1.

a. Access the CLI for R1 by clicking the device.
b. Do the following on R1:
• Configure the hostname of the router as R1.
• Configure the encrypted form of the privileged EXEC mode password and set the password to class.
• Set the console and vty password to cisco and require users to log in.
• Encrypt the console and vty passwords.
• Configure the message-of-the-day as Authorized Access Only. (Do not include the period.)
c. Check results.
Your completion percentage should be 65%. If not, click Check Results to see which required components are not yet completed.

Step 7: Solve a mismatch between duplex and speed.
a. PC1 and Server currently do not have access through S1 because the duplex and speed are mismatched.
b. Verify connectivity.
c. Both PC1 and Server should now be able to ping S1, R1 and each other.
d. Check Results.
Your completion percentage should be 73%. If not, click Check Results to see which required components are not yet completed.

Step 8: Configure port security:
a. Use the following policy to establish port security on the port used by PC1:
• Enable port security
• Allow only one MAC address
• Configure the first learned MAC address to "stick" to the configuration.
Only enabling port security is graded by Packet Tracer and counted toward the completion precentage.

However, all the port security tasks listed above are required to complete this activity successfully.

b. Verify that port security is enabled for Fa0/18. Your output should look like the following output. Notice that S1 has not yet learned a MAC address for this interface. What command this output?

S1# _____

Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
Secure Static Address Aging : Disabled
Maximum MAC Address 1
Total MAC Address 0
Configured MAC Address 0
Sticky MAC Address 0
Last Source Address : Vlan : 0000.0000.0000 : 0
Security Violation Count 0

c. Force S1 to learn the MAC address for PC1. Send a ping from PC1 to S1. Then verify that S1 added the MAC address for PC1 to the running configuration.

!
interface FastEthernet 0/18
<output omitted>
switchport port-security mac-address sticky 0060.3EE6.1650
<output omitted>
!

d. Test port security. Remove the Fast Ethernet connection between S1 and PC1. Connect PC2 to Fa0/18.

Wait for the link lights to turn green. If necessary, send a ping from PC2 to S1 to cause the port of shut down.

Port security should show the following results:

Port Security : Enabled
Port Status : Secure-shutdown
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
Secure Static Address Aging : Disabled
Maximum MAC Address : 1
Total MAC Address 1
Configured MAC
Address : 1
Sticky MAC Addresses 0
Last Source Address : Vlan : 0DD0.BADB.5193 : 99 Security
violation Count 1

e. Viewing the Fa0/18 interface shows that the protocol is down (err-disabled), which also indicates a security violation

S1 # show interface Fa0/18
Fast Ethernet 0/18 is down, line protocol is down (err-disable
(output omitted)

f. Reconnect PC1 and re-enable the port. To re-enable the port, disconnect PC2 from Fa0/18 and reconnect PC1. Interface Fa0/18 must be manually re enabled with the no shutdown command before returning to the active state.

g. Check results.

Your completion Percentage should be 77 %. If not, click Check Results to see which required components are not yet completed.

Step 9: Secure unused Ports.

a. Disable all ports that are currently not used on S1. Packet Tracer grades the status of the following ports: Fa0/2, Fa0/3, Fa0/4, Gig1/1, and Gig1/2.

b. Check results

Your completion percentage should be 8%. If not, click Check Results to see which required components are not yet completed.

Step 10: Manage the switch configuration file.

a. Save the current configuration for S1 and R1 to NVRAM.

b. Back up the startup configuration file on S1 and R1 by uploading them to Server.

Verify that Server has the R1-config and S1-config files.

c. Check Results.

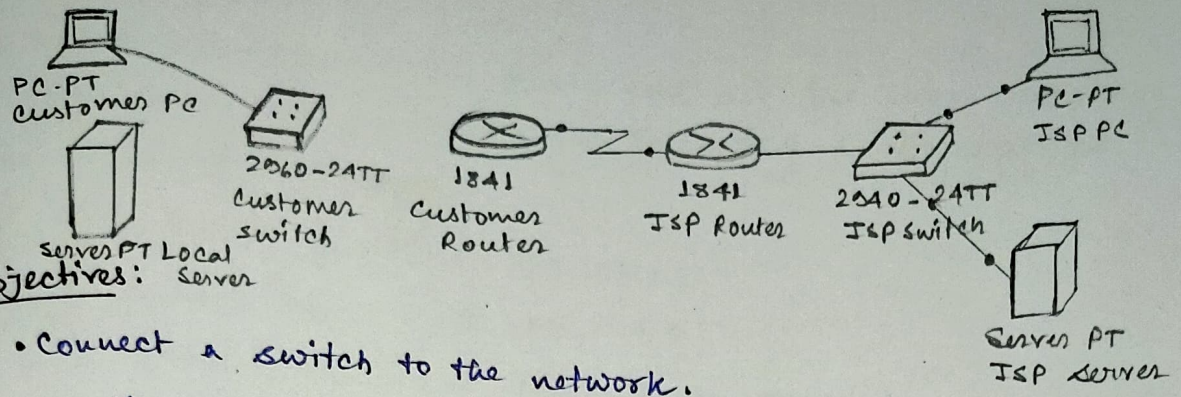
Your completion Percentage should be 100%. If not, click Check Results to see which required components are not yet completed.

4/4/23

Assignment - 07

Connection a Switch

Topology Diagram:



Objectives:

- Connect a switch to the network.
- Verify the configuration on the switch.

Background:

In this activity, you will verify the configuration on the customer Cisco Catalyst 2960 switch. The switch is already configured with all the basic necessary information for connecting to the LAN at the customer site. The switch is currently not connected to the network. You will connect the switch to the customer workstation, the customer server, and customer router. You will verify that the switch has been connected and configured successfully by pinging the LAN interface of the customer router.

Step 1: Connect the switch to the LAN

a. Using the proper cable, connect the Fast Ethernet 0/0 on customer Router to the Fast Ethernet 0/1 on customer Switch.

b. Using the proper cable, connect the customer PC to the customer switch on port Fast Ethernet 0/2

c. Using the proper cable, connect the Local Server to the customer switch on port Fast Ethernet 0/3.

Step 2: Verify the switch configuration.

a. From the customer PC, use the terminal emulation software to connect to the console of the customer

b. Use the console connection and terminal utility on the customer PC to verify the configurations. Use cisco as the console password.

c. Enter privileged EXEC mode and use the show running-config command to verify the following configurations. The password is cisco123.

a. VLAN1 IP address = 192.168.1.5
b. Subnet mask = 255.255.255.0
c. Password required for console access
d. Password required for vty access
e. Password enabled for privileged EXEC mode
f. Secret enabled for privileged EXEC mode

d. Verify IP connectivity between the Cisco Catalyst 2960 switch and the cisco 1841 router by initiating a ping to 192.168.1.1 from the switch CLI.

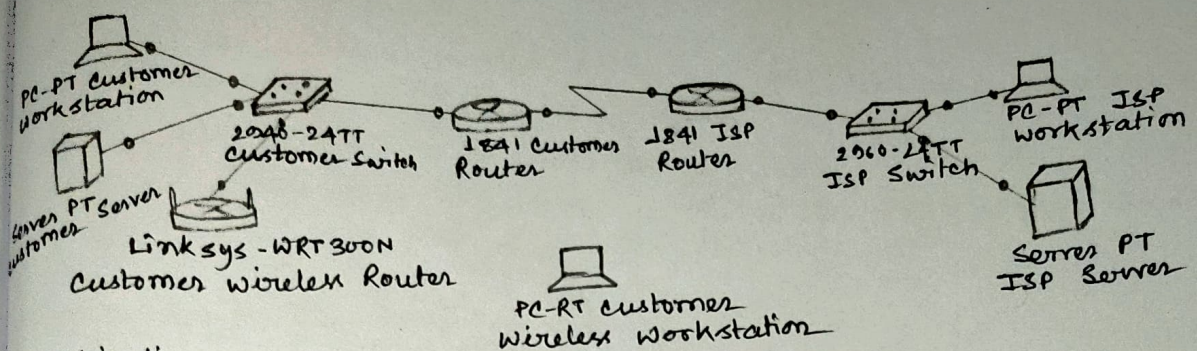
e. Click the Check Results button at the bottom of this instruction window to check your work.

11/4/23

Assignment 08

Configuring WEP on a Wireless Router

Topology Diagram:



Objectives:

Configure WEP security between a workstation and a Linksys wireless router.

Background:

You have been asked to go back to a business customer and install a new Linksys wireless router for the customer office. The customer company has some new personnel who will be using wireless computers to save money on adding additional wired connections to the building. The business is concerned about the security of the network because they have financial and highly classified data being transmitted over the network. Your job is to configure the security on the router to protect the data.

Step 1: Configure the Linksys wireless router to require WEP.

a. Click the Customer Wireless Router icon. Then click the GUI tab to access the router web management interface.

b. Click the Wireless menu option and change the Network Name (SSID) from Default to Customer Wireless. Leave the other settings with their default options.

c. Click the Save Settings button at the bottom of the Basic Wireless Settings window.

d. Click the Wireless Security submenu under the Wireless menu to display the current wireless security parameters.

e. From the Security mode drop down menu, select WEP.

f. In the Key1 text box, type 1a2b3c4d5e. This will be the new WEP pre shared key to access the wireless network.

g. Click the Save Settings button at the bottom of the Wireless Security window.

Step 2: Configure WEP on the customer wireless workstation:

a. Click the Customer Wireless Workstation.

b. Click the config tab

c. Click the Wireless button to display the current wireless configuration settings on the workstation.

d. Change the SSID to Customer Wireless.

e. Change the Security Mode to WEP. Enter 1a2b3c4d5e in the key text box, and then close the window.

Step 3: Verify the configuration.

After you configure the correct WEP key and SSID on the customer wireless workstation, notice that there is a wireless connection between the workstation and the wireless router.

a. Click the Customer Wireless Workstation.

b. Click the Desktop tap to view the applications that are available.

c. Click on the Command Prompt application to bring up the command prompt.

d. Type ipconfig/all and press Enter to view the current Network configuration settings.

e. Type ping 192.168.2.1 to verify connectivity to the LAN interface of the customer wireless router.

f. Close the command prompt window

g. Open the Command web browser.

h. In the address bar of the web browser window, type http://192.168.1.10. Press Enter. The Intranet web page that is running on the customer server appears. You have just verified that the customer wireless work station has connectivity to the rest of the customer network.

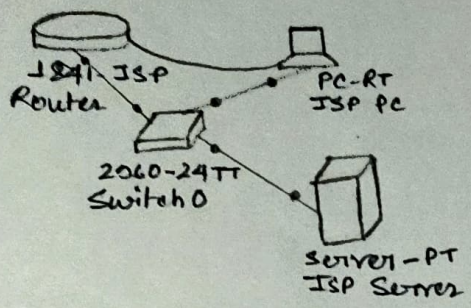
i. Click the Check Results button at the bottom of this instruction window to check your work.

25/4/23

Assignment 09

Using the Cisco IOS show commands

Topology Diagram:



Objectives:

Use the Cisco IOS show commands.

Background:

The Cisco IOS show commands are used extensively when working with Cisco equipment. In this activity, you will use the show commands on a router that is located at an ISP.

Step 1: Connect to the ISP Cisco 1841 router.

Use the terminal emulation software on ISP PC to connect to the Cisco 1841 router. The ISP Router> prompt indicates that you are in user EXEC mode. Now type enable at the prompt. The ISP Router# prompt indicates that you are in privilleged EXEC mode.

Step 2: Explore the show commands.

Use the information displayed by these show commands to answer the question in the Reflection section.

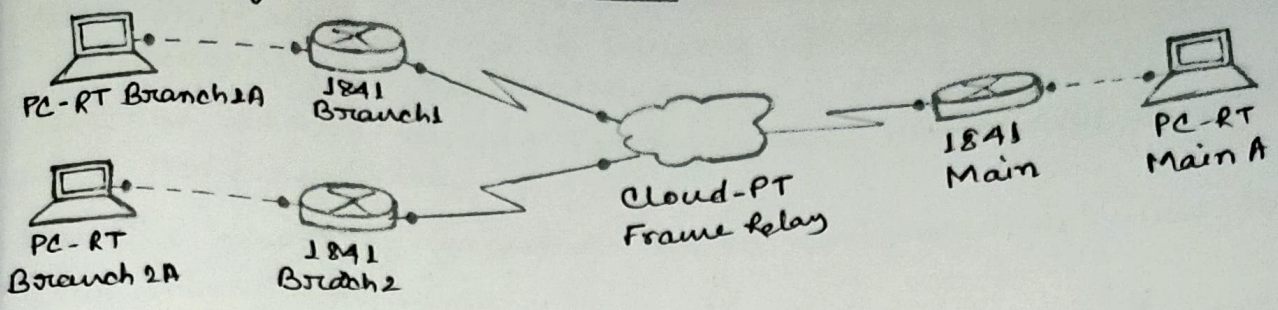
a. Type show arp.
b. Type show flash.
c. Type show ip route.
d. Type show interface
e. Type show protocols
f. Type show users.
g. Type show version.

Sudh
25/4/23

the
f. L
statu
h. Use
relay

Assignment 10

Examining WAN Connections:



Objective:

The show commands are very powerful commands for troubleshooting and monitoring networks. They give a static image of the network at a given time. The use of a variety of show commands will give a clear picture of how the networking is communicating and transferring data.

Background:

The physical topology of the network has been designed using Frame Relay. To test the network connectivity, use a variety of show commands.

Required file: Examining WAN connections.pka

Step 1: Examine the configuration of Branch1 and Branch2.

a. Click on Branch1 and use various show commands to view the connectivity to the network.

b. Use the show running-configuration command to view the router configuration.

c. Use the show ip interface brief command to view the status of the interfaces.

d. Use the various show frame-relay map, show frame-relay pvc and show frame-relay lmi commands to see the status of the frame-relay circuit.

e. Click on Branch2 and use various show commands to view the connectivity to the network.

f. Use the show running-configuration command to view the router status configurations.

g. Use the show ip interface brief command to view the status of the interfaces.

h. Use the various show frame-relay map, show frame-relay pvc, and show frame relay lmi commands to see the status of the Frame-relay circuit

Step 2: Examine the configuration of Main.

a. Click on Main and use a variety of show commands to view the connectivity to the network.

b. Use the show running configuration command to view the router configuration.

c. Use the show ip interface brief command to view the status of the interfaces.

d. To view the status of the frame-relay configurations use the show frame-relay lmi, show frame relay map, and show frame-relay pvc commands.

09/08/23