Lab 9 - Hardware Lab - Configure CDP, LLDP, NTP and create a backup **and create a backup configuration file**

Topology

Note: for students in lab E202 ONLY

There is a different model of switch in this lab. Instead of connecting to Gigabit Ethernet ports you will need to connect to FastEtherent ports on switches S1 and S2. You will need to substitute with the following:

S1: G1/0/10 -> F0/10

S1: G1/0/15 -> F0/15

S2: G1/0/7 -> F0/7

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Loopback1	172.16.1.1	255.255.255.0	N/A
	G0/0/1	10.22.0.1	255.255.255.0	
S1	SVI VLAN 1	10.22.0.2	255.255.255.0	10.22.0.1
S2	SVI VLAN 1	10.22.0.3	255.255.255.0	10.22.0.1

Please note: users in E202 the ports on the switch will be different e.g. Fast Ethernet ports instead of Gigabit Ethernet. Swap these: e.g. G1/0/10 will be F0/10, G1/0/15 will be F0/15 and so on.

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Network Discovery with CDP

Part 3: Network Discovery with LLDP

Part 4: Configure and Verify NTP

Part 5: Create a Backup Configuration File

Background / Scenario

Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol for network discovery on the data link layer. It can share information such as device names and IOS versions with other physically connected Cisco devices. Link Layer Discovery Protocol (LLDP) is vendor-neutral protocol using on the data link layer for network discovery. It is mainly used with network devices in the local area network (LAN). The network devices advertise information, such as their identities and capabilities to their neighbors.

Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients. NTP uses the User Datagram Protocol (UDP) as its transport protocol. By default, NTP communications use Coordinated Universal Time (UTC).

An NTP server usually receives its time from an authoritative time source, such as an atomic clock attached to a time server. It then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of each other.

In this lab, you must document the ports that are connected to other switches using CDP and LLDP. You will document your findings in a network topology diagram.

Note: Ensure that the routers and switches have been erased and have no startup configurations. If you are unsure contact your instructor.

Required Resources

- 1 Router e.g.(Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 2 Switches e.g (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable) or Cisco Catalyst 1000 Series
- 2 PCs (Windows with a terminal emulation program, such as Putty)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the router and switches.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for the router.

a. Assign a device name to the router.

```
router(config)# hostname R1
```

b. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

```
R1(config)# no ip domain lookup
```

c. Assign **class** as the privileged EXEC encrypted password.

```
R1(config)# enable secret class
```

d. Assign **cisco** as the console password and enable login.

```
R1(config)# line console 0
```

```
R1(config-line)# password cisco
R1(config-line)# login
```

e. Assign **cisco** as the VTY password and enable login. Also, enable remote telnet access only (although please note this is insecure protocol – using for test purposes only).

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# transport input telnet
R1(config-line)# login
```

f. Encrypt the plaintext passwords.

```
R1(config)# service password-encryption
```

g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

```
R1(config)# banner motd $ Authorized Users Only! $
```

h. Configure interfaces as listed in the table above

```
R1(config-if)# interface g0/0/1
R1(config-if)# ip address 10.22.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# end
R1# exit

Authorized Users Only!
User Access Verification
Password:
```

Now enter your passwords you configured for console.

Also, enter your enable password to gain access back to privileged mode.

```
R1>en
Password:
R1#
```

Step 3: Configure basic settings for each switch.

a. Assign a device name to the switch.

```
switch(config)# hostname S1
switch(config)# hostname S2
```

b. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

```
S1(config)# no ip domain-lookup
S2(config)# no ip domain-lookup
```

c. Assign **class** as the privileged EXEC encrypted password.

```
S1(config)# enable secret class
S2(config)# enable secret class
```

d. Assign **cisco** as the console password and enable login.

```
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login

S2(config)# line console 0
S2(config-line)# password cisco
S2(config-line)# login
```

e. Assign **cisco** as the VTY password and enable login.

```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login

S2(config)# line vty 0 15
S2(config-line)# password cisco
S2(config-line)# login
```

f. Encrypt the plaintext passwords.

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

S2(config)# service password-encryption
```

g. Create a banner that warns anyone accessing the device sees the banner message “Authorized Users Only !”.

```
S1(config)# banner motd $ Authorized Users Only! $

S2(config)# banner motd $ Authorized Users Only! $
```

Use the command:

```
S1# show version
S2# show version
```

Answer the following questions:

What is the switch **uptime**?

How many **ports** are on this switch?

(review the output carefully)

Answers will vary. In this example, look for the switch uptime.
Output should show
S1 uptime is x hour, x minutes

Down the bottom of the output it will show the amount of Ports available and model of switch.

Part 2: Network Discovery with CDP

On Cisco devices, CDP is enabled by default. You will use CDP to discover the ports that are currently connected.

a. On R1, use the **show cdp** command to determine how many interfaces are CDP enabled, and of those how many are up and how many are down.

Answers will vary depending if there was configuration on your router. If your router was erased you will likely see the below. Note: this will depend on your router model. E.g. for Cisco Router 4221

```
-------------------------

Global CDP information:
       Sending CDP packets every 60 seconds
       Sending a holdtime value of 180 seconds
       Sending CDPv2 advertisements is enabled

On R1, use the show cdp interface command to
R1# show cdp interface
 <output omitted>

cdp enabled interfaces : 2
 interfaces up          : 1
 interfaces down        : 1
```

How many interfaces are participating in the CDP advertisement? Which interfaces are up?

Answers may vary. In the output above, two interfaces are participating in CDP. One is up, one is down. Note: again this will depend on your router initial configuration however, if you have configured up to this point you will likely see G0/0/0 as administratively down and G0/0/1 as up. Note: G0/0/1 is where you assigned an IPv4 address and enabled the interface above.

On R1, use the appropriate **show cdp neighbors** command to view neighbors.

```
R1# show cdp neighbors
```

Answers may vary (depending on your hardware in the lab). You should see S1 under Device ID column.

b. On R1, use the appropriate **show cdp** command to determine the IOS version used on S1.

```
R1# show cdp entry S1
```

Answers may vary (depending on your hardware in the lab). In this sample example, it's showing output for a C2969 switch but your setup/hardware may differ.

```
-------------------------
Device ID: S1
Entry address(es):
Platform: cisco WS-C2960+24LC-L,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/0/1,  Port ID (outgoing port): FastEthernet0/5
Holdtime : 125 sec
```

```
Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.2(4)E8, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Fri 15-Mar-19 17:28 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
```

Notice there is no current Entry addresses (IP addresses) configured on S1.

What IOS version is S1 using?

Answers may vary. S1 in this example is using IOS Version 15.2(4)E8

Note if you are in lab E125 the switches are C1000 so IOS Version will likely be 15.2(7) E6

c. On S1, use the appropriate **show cdp** command to determine how many CDP packets have been output.

```
S1# show cdp traffic
CDP counters :
        Total packets output: 179, Input: 148
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0,
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 179, Input: 148
```

How many packets has CDP output since the last counter reset?

Answers may vary. In this example, CDP has output 179 packets

d. Configure the SVI for VLAN 1 on S1 and S2 using the IP addresses specified in the Addressing Table above. Configure the default gateway on each switch based on the Address Table.

```
S1(config)# interface vlan 1
S1(config-if)# ip address 10.22.0.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# ip default-gateway 10.22.0.1

S2(config)# interface vlan 1
S2(config-if)# ip address 10.22.0.3 255.255.255.0
S2(config-if)# no shutdown
S2(config-if)# exit
S2(config)# ip default-gateway 10.22.0.1
```

e. On R1, issue the **show cdp entry S1** command.

What additional information is now available?

The output includes the management IP address for VLAN 1 SVI on S1 that was just configured. Note: you may need to wait a minute to see the output change.

```
R1# show cdp entry S1
-------------------------
Device ID: S1
Entry address(es):
  IP address: 10.22.0.2
Platform: cisco WS-C2960+24LC-L,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/0/1,  Port ID (outgoing port): FastEthernet0/5
Holdtime : 133 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.2(4)E8, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Fri 15-Mar-19 17:28 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
Management address(es):
  IP address: 10.22.0.2
```

Notice there is now current entry addresses (IP addresses) configured on S1.

f. Telnet from S1 to R1.

```
S1# telnet 10.22.0.1
Trying 10.22.0.1 … Open
Authorized Users Only!
User Access Verification
Password:Enter password.
R1> enable
Password:  Enter password.
R1#
```

You have now used the telnet protocol to remotely access R1. Type exit to return to S1.

```
R1# exit
[Connection to 10.22.0.1 closed by foreign host]
S1#
```

```
S1# show cdp neighbors
```

Note: you should be able to see S2 and R1 from output.

Note how it shows the capabilities of both devices. I.e it shows a legend code to show R S for the Router (R1). This means that it has router and switch capabilities

Note the Switch(S2) does not indicate the R capability.

```
S1# show cdp neighbors detail
```

Take note of the differences between the two commands.

Before proceeding, go to the "Lab 9 - Hardware Activity (1%) - 2025" quiz on the Brightspace page and enter your answer for question 1,2 & 3. Leave the quiz open while you complete the rest of the lab sheet.

g. Disable CDP globally on all devices.

```
R1(config)# no cdp run
S1(config)# no cdp run
S2(config)# no cdp run
```

Note the following output after you have disabled CDP globally.

```
R1# show cdp neighbors
%CDP is not enabled
```

Part 3: Network Discovery with LLDP (802.1AB)

Link Layer Discovery Protocol (LLDP) is an industry standard alternative to CDP. You will use LLDP to discover the ports that are currently connected.

```
R1# show lldp
%LLDP is not enabled
```

a. Enter the appropriate **lldp** command to enable LLDP on all devices in the topology.

```
R1(config)# lldp run
S1(config)# lldp run
S2(config)# lldp run

R1# show lldp
Global LLDP Information:
      Status: ACTIVE
      <output omitted>
```

b. On S1, issue the appropriate **lldp** command to give you detailed information on S2.

```
S1# show lldp entry S2

Capability codes:
```

```
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
----------------------------------------------
Local Intf: Gi1/0/15
Chassis id: c025.5cd7.ef00
Port id: Gi1/0/7
Port Description: FastEthernet0/1
System Name: S2

System Description:
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.2(4)E8, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Fri 15-Mar-19 17:28 by prod_rel_team

Time remaining: 109 seconds
System Capabilities: B
Enabled Capabilities: B
Management Addresses:
    IP: 10.22.0.3
Auto Negotiation - supported, enabled
Physical media capabilities:
    100base-TX(FD)
    100base-TX(HD)
    10base-T(FD)
    10base-T(HD)
Media Attachment Unit type: 16
Vlan ID: 1


Total entries displayed: 1
```

What is the chassis ID for switch S2?

Answers will vary. In the sample example above, the chassis ID for S2 is c025.5cd7.ef00. Knowing the chassis ID may help in detecting unauthorized switches added to the network. They may be used for inventory tracking and asset management.

c. Console into all the devices and use the LLDP commands necessary for you to draw the physical network topology from only the show command output.

```
S1# show lldp neighbor
```

Answers will vary, but the main command to use is show lldp neighbor. The idea is to visualize the network topology from only the LLDP outputs.

Part 4: Configure NTP

In Part 4, you will configure R1 as the NTP server and S1 and S2 as NTP clients of R1. Synchronized time is important for syslog and debug functions. If the time is not synchronized, it is difficult to determine what network event caused the message.

Step 1: Display the current time.

```
R1# show clock
*17:11:14.669 UTC Wed Mar 26 2025

R1# show clock detail
*17:11:14.913 UTC Wed Mar 26 2025
No time source
```

Issue the **show clock detail** command to display the current time on R1. Record the information regarding the current time displayed in the following table.

Date	Time	Time Zone	Time Source
Answer will vary.	**Answer will vary.**	**Answer will vary.**	**Answer will vary.**

Step 2: Set the time.

Use the appropriate command to set the time on R1 **(if it is incorrect).** The time entered should be in UTC.

```
R1# clock set 17:00:00 26 March 2025

R1# show clock detail
*17:00:00.913 UTC Wed Mar 26 2025
Time source is user configuration
```

Step 3: Configure the NTP master.

First check the status of NTP.

```
R1# show ntp status
*NTP is not enabled
```

Configure R1 as the NTP master with a stratum level of 4.

```
R1(config)# ntp master 4

R1# show ntp status
Clock is unsynchronized, stratum 4, reference is
<output omitted>
```

Step 4: Configure the NTP client.

a. Issue the appropriate command on S1 and S2 to see the configured time. Record the current time displayed in the following table.

```
S1# show clock detail
*16:57:00.913 UTC Wed Mar 26 2025
Time source is hardware calendar
```

Date	Time	Time Zone
Answer will vary.	**Answer will vary.**	**Answer will vary.**

b. Check NTP status of switches.

```
S1# show ntp status
*NTP is not enabled
```

c. Configure S1 and S2 as NTP clients. Use the appropriate NTP commands to obtain time from R1's G0/0/1 interface, as well as to periodically update the calendar or hardware clock on the switch.

```
S1(config)# ntp server 10.22.0.1
S1(config)# ntp update-calendar

S2(config)# ntp server 10.22.0.1
S2(config)# ntp update-calendar

S1# show ntp status
Clock is unsynchronized, stratum 16, no reference clock…
```

Step 5: Verify NTP configuration.

a. Use the appropriate **show** command to verify that S1 and S2 are synchronized with R1.

Note: It could take a few minutes before the switches are synchronized with R1.

```
S1# show ntp status | include Clock

Clock is synchronized, stratum 5, reference is 10.22.0.1

S2# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~10.22.0.1       127.127.1.1      4      4     64     3  3.194   4.629 63.914
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Please note: it can take some time before this changes from st 16 to change to st 4. You DO NOT need to wait for this to update. IMPORTANT: Please move onto the next task.

Reflection Question

Within a network, on which interfaces should you not use discovery protocols? Explain.

Discovery protocols should not be used on interfaces that are facing the external networks because these protocols provide insights about the internal network. This information allows attackers to gain valuable information about the internal network and can be used to exploit the network.

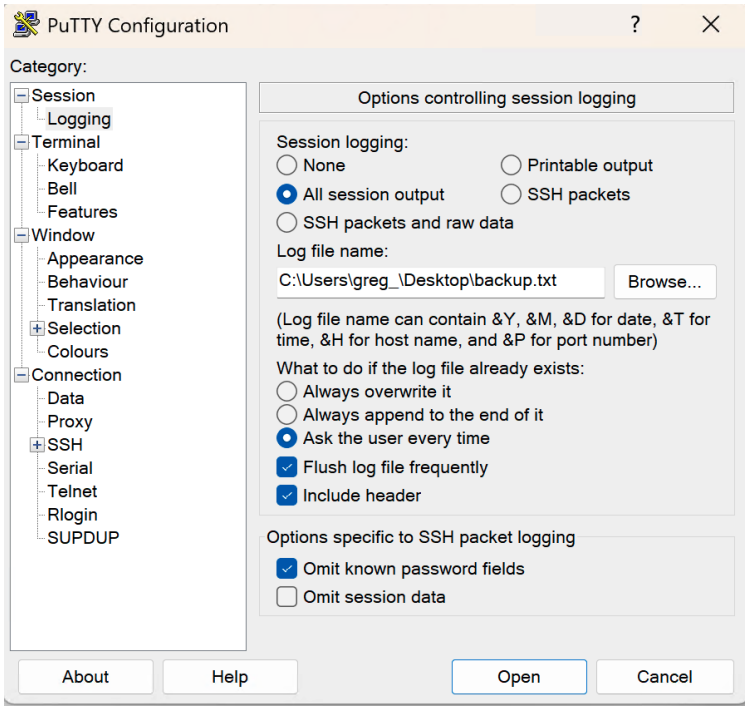
Part 5: Create a Backup Configuration File

In Putty or other terminal emulation program, you can create a log of your commands and output to a device via a connection. In this part, you will record your interaction with a device using the logging feature of Putty.

Step 1: Create a log file.

a. Open a new Putty window.

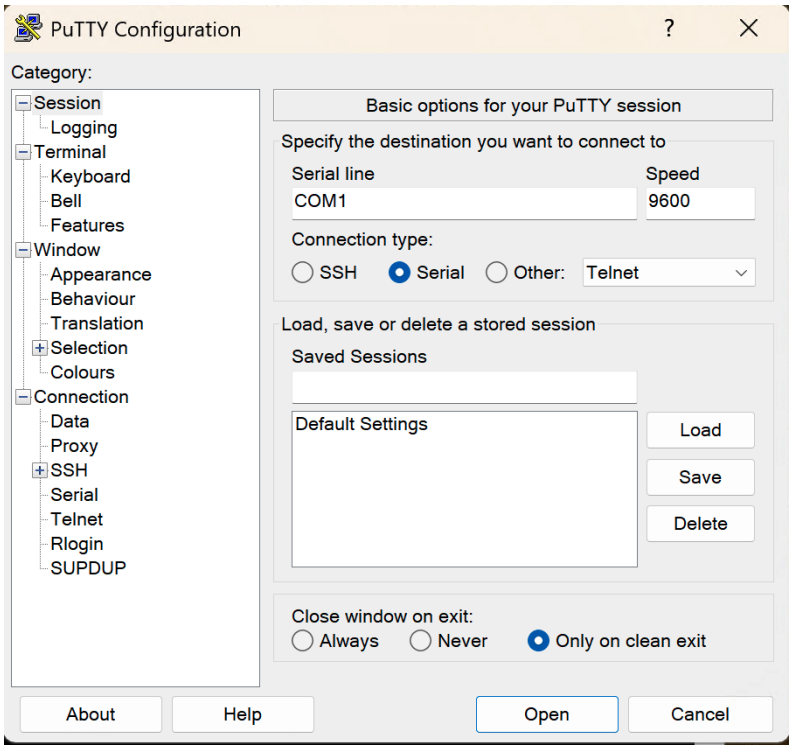
b. Click on Logging (under Session category.)

c. 

d. Select **All session output**.

e. Note: **I change the log file extension and location.**

f. Click back to Session and open serial connection to your Router (ensuring that COM port is correct – NOTE you may need to change the COM port connected to your PC).

g. 

h. Click open.

i. Once you connect.

j. Enter privileged EXEC mode.

```
R1# terminal length 0
This ensures you don't need to hit enter after number of lines of
configuration.
Normally, when you run a long command like show running-config, the output
stops after 24 lines (the default page size) and waits for you to press Space
or Enter to continue.
Setting terminal length 0 removes this pause, displaying the entire output in
one go.
```

k. Run the following command to display the router running-configuration.

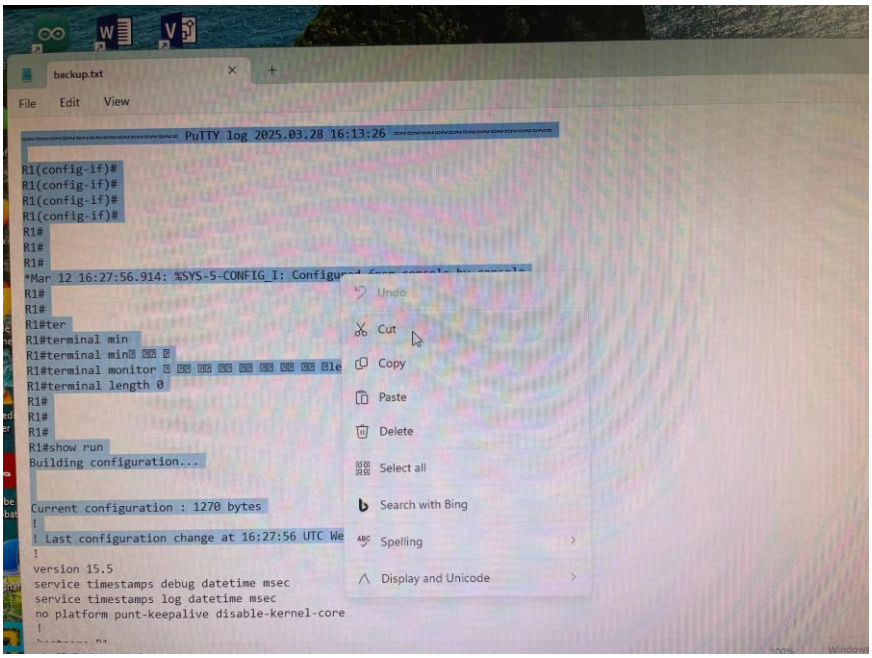
```
R1# show running-config
```

l. After the output completes, **close PuTTY.**

m. The configuration will be saved in the log file you selected (in my example I selected the Desktop).

n. This method is useful for quick manual backups.

o. Note: you may open up the file (for me it is a file called backup.txt on my desktop). Here you will see the full configuration.



p. You will see something similar to the above. You may delete the first number of commands and save the file.

q. Note: I delete the initial commands in the file (all the way down to ! Last configuration…

r. We are really interested in just having the configuration only in this file.

Also Note: You can use this feature to capture the output from several commands in sequence and use it for network documentation purposes.

Part 2: Use a Backup Configuration File to Restore a Router Configuration

Step 1: Erase the router startup-configuration and reload it.

a. From privileged EXEC mode erase the startup configuration.

```
R1# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
```

b. Reload the router.

```
R1# reload
Proceed with reload? [confirm]
```

c. You may receive the following message. System configuration has been modified Save? Type **no**; Proceed with reload. Press **enter**.

d. After the reboot, you should see the System Configuration Dialog prompt, indicating an unconfigured router. Type **no** and press **enter**

```
        --- System Configuration Dialog ---

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

```
Press RETURN to get started!
<output omitted>
```

e. Note there is no longer any configuration in the running configuration.

f. Enter privileged EXEC mode and enter a **show running-config** command to **verify** that all of the previous configurations were erased.

```
Router>en
Router# show run
```

Step 2: Edit the saved configuration backup file to prepare it for restoring the router configuration.

To restore the router configuration from a saved running configuration backup file, you must edit the text.

a. Open the **backup.txt** text file (you saved this to the Desktop in Part 5.)

b. Ensure you have removed any initial connection information in the text file and initial commands.

Step 3: Restore the router configuration.

You can restore the edited running configuration directly to the console terminal in router global configuration mode, and the configurations are entered as if they were commands entered individually at the command prompt.

Method: Manual Paste (Recommended for Small Configs only)

If your configuration file is not too large, you can simply copy and paste it into the router.

Steps:

a. Open PuTTY and connect to the router via SSH or Telnet.

b. Enter global configuration mode:

```
R1# enable
R1# configure terminal
```

c. Open your edited configuration file in **Notepad** or any text editor.

d. **Copy the entire configuration** (CTRL + A and then CTRL + C) .

e. Right-click in PuTTY (or press Shift + Insert) to **paste**.

f. Press Enter to ensure all commands are applied.

Note: you can now run

```
R1# show run
```

Notice, your hostname has returned to R1 and all your configuration is back in the running-config.

```
At this point, we have successfully restored our configuration. One item to check
you may need to do a no shutdown on any interfaces (as default state on some
routers is to have these as administratively down.)
You could check this by
```

```
R1# show ip int brief
```

You could then do a no shutdown on the interface if they were administratively down.

```
R1# conf t
R1# int g0/0/1
R1# no shut
```

Well done you have completed the Lab 9 Hands-on activity. Now you can attempt Q4 and Q5 of the remaining questions in Lab 9 - Hardware Activity (1%) -2025 on Brightspace and submit your lab.

Once this is complete, open Lab 9 - Backing Up and Upgrading Network Devices (PT Activity)-2025– this is a Packet Tracer activity and complete.

Once all members have completed the hardware activity, please remove any cables you connected to both switches and router.