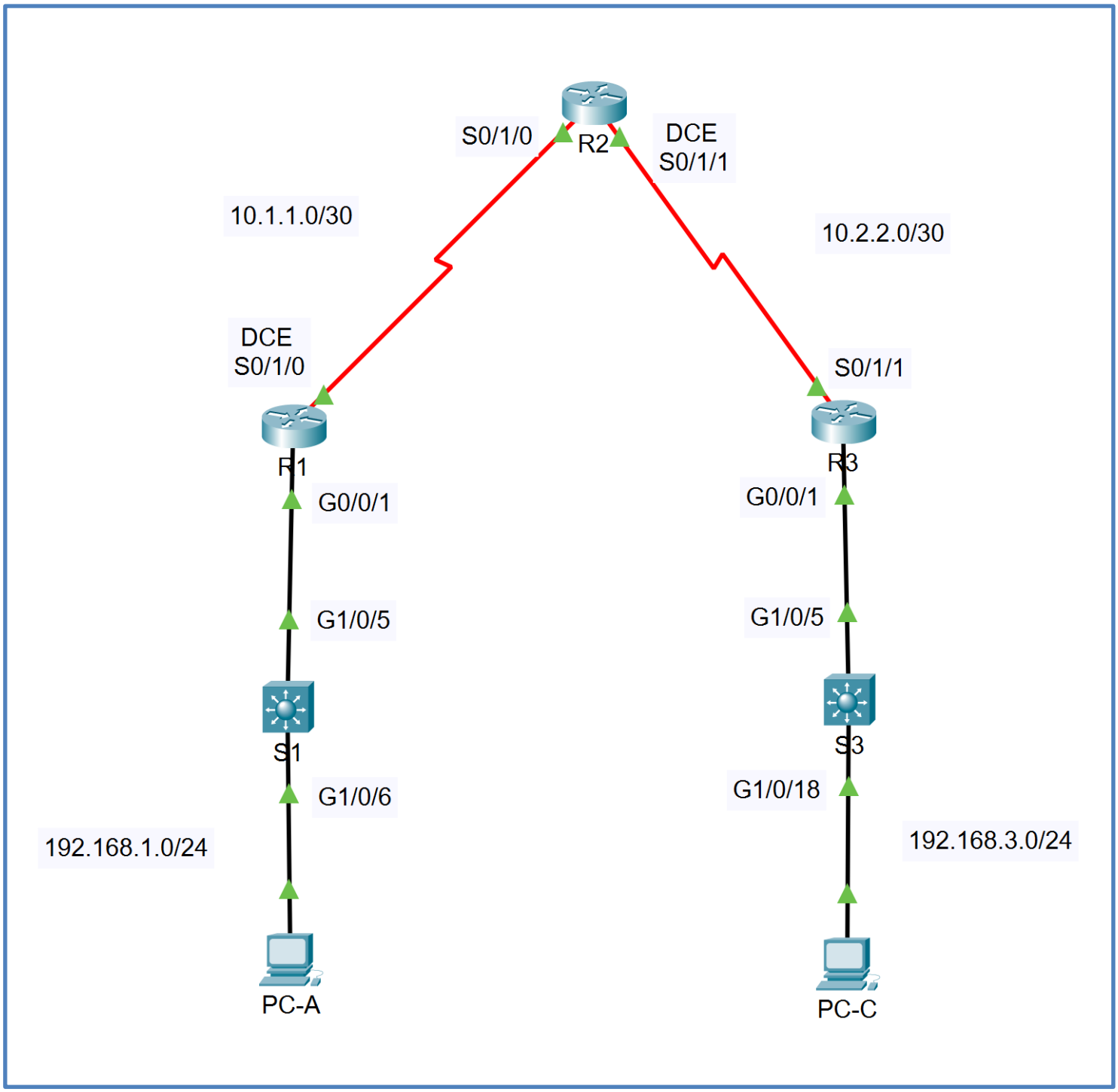
Lab Activity: CCP Configuration:

There are two LANs and two site-to-site WANs in following the topology. Please develop the following topology on the physical pod/rack in the lab room.



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 G1/0/5
	S0/1/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/1/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/1/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/0/1	192.168.3.1	255.255.255.0	N/A	S3 G1/0/5
	S0/1/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 G1/0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 G1/0/18

Objectives

Part 1: Initialize and Reload Network Devices

- Initialize the router and reload
- Initialize the switch and reload

Part 2: Basic Network Device Configuration

- Cable the network as shown in the topology
- Initialize network devices
- Configure basic IP addressing for routers and PCs
- Configure routing
- Verify connectivity between hosts and routers

Part 3: Configure CCP Access for Routers

- Enable a secure HTTP server
- Create a user account with privilege level 15
- Configure SSH and Telnet access for local login

Part 4: Basic CCP Configuration

- Install CCP
- Manage communities
- Discover router devices

Background/Scenario

Cisco Configuration Professional (CCP) is a Windows-based device management tool for Integrated Service Routers (ISRs). CCP simplifies router configurations through easy-to-

use wizards. The objective of this lab is to verify the routers and PCs are configured properly for use with CCP.

Note: The router commands and output in this lab are from a Cisco 1841 with Cisco IOS Release 15.1(4)M8 (Advanced IP Services image). Other routers and Cisco IOS versions can be used. See the Router Interface Summary Table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

Note: Make sure the routers and switches have been erased and have no startup configurations.

Required Resources:

- Two Layer-3/Multilayer Switches (Cisco Catalyst 1000 Series with Cisco IOS Release 15.1+ image)
- Three routers (Cisco 4221 with Cisco IOS Release 17.6+ image)
- Two PCs (Windows with Terminal Emulation Program)
- Cables:
    - Console cables to configure the Cisco IOS devices through the console port.
    - Ethernet and serial cables as shown in the topology.

CCP Notes:

- To run CCP, it may be necessary to temporarily disable antivirus programs and O/S firewalls. Make sure all pop-up blockers are turned off in the browser.

CCP Related Hardware and Software Information:

IOS Images:

For the latest compatible IOS images, search for **NetAcad Maintenance – Image & Hardware Spport.xls** in the NetAcad Maintenance under Equipment Information on NetSpace.

Interface Cards:

Interfaces	Part Numbers
WAN Interface Cards (WICs)	WIC-1T, WIC-2A/S, WIC-2T
High-speed WICs (HWICs)	HWIC-4ESW-POE, HWIC-2A/S, HWIC-2T, HWIC-4ESW

The following table summarizes the minimum PC requirements to run CCP:

PC operating systems	Windows 7 Windows Vista: Business Edition and Ultimate Edition Mac OSX 10.5.6 running Windows XP using VMWare 2.0
Other software	Sun JRE 1.5.0_11 up to 1.6.0_16 Adobe Flash Player Version 10.0.12.36 and later
PC hardware	Minimum 2-GHz processor 1-GB DRAM minimum; 2 GB recommended Screen Resolution: 1024 x 768 Free disk space of 400 MB
Browser requirements	Microsoft IE 6.0 or later

The following JRE settings are needed for Cisco CP to function properly:

1) Go to **Start** > **Control Panel** > **Java**.
2) Click **View** under Java Applet Runtime Settings.
3) Select your JRE in use.

In addition, if JRE is upgraded to versions 1.6.0_11 or above, the following settings are needed after Cisco CP installation.

4) Go to **Start** > **Control Panel** > **Java** > **Advanced** tab.
5) Click **Java Plug-in** tree.
6) Uncheck the check box for **Enable Next-generation Java Plug-in**.
7) Restart Cisco CP.

Link to release notes for CCP:

CCP version 2.5:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/v2_5/rlsnts/ccp_rel_notes.html

CCP version 2.6:

http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_configuration_professional/v2_6/rlsnts/ccp_rel_notes.html

CCP version 2.7:

http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_configuration_professional/v2_7/rlsnts/ccp_v27_rel_notes.html

Part 1: Initialize and Reload Network Devices

Task 1: Initialize the router and reload.

Step 1: Connect to the router.

Console into the router and enter privileged EXEC mode using the **enable** command.

```
Router> enable
Router#
```

Step 2: Erase the startup configuration file from NVRAM.

Type the **erase startup-config** command to remove the startup configuration from NVRAM.

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

Step 3: Reload the router.

Issue the **reload** command to remove old configurations from memory. When prompted to proceed with reload, press Enter to confirm the reload. Pressing any other key will abort the reload.

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


*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload
Reason: Reload Command.
```

You may receive a prompt to save the running configuration prior to reloading the router. Respond by typing **no** and press **Enter**.

```
System configuration has been modified. Save? [yes/no]: no
```

Step 4: Bypass the initial configuration dialog.

After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press **Enter**.

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

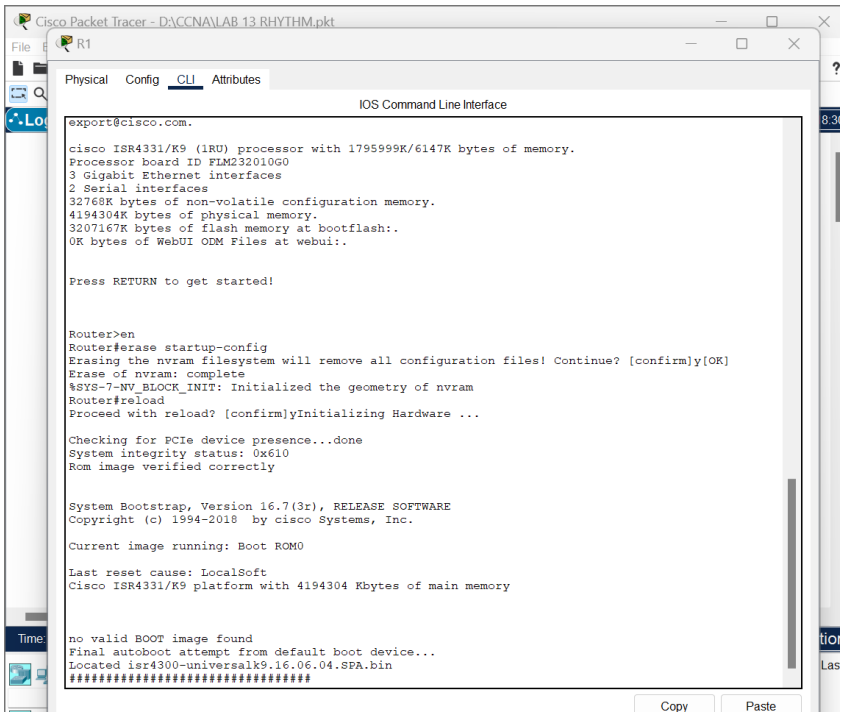
Step 5: Terminate the autoinstall program.

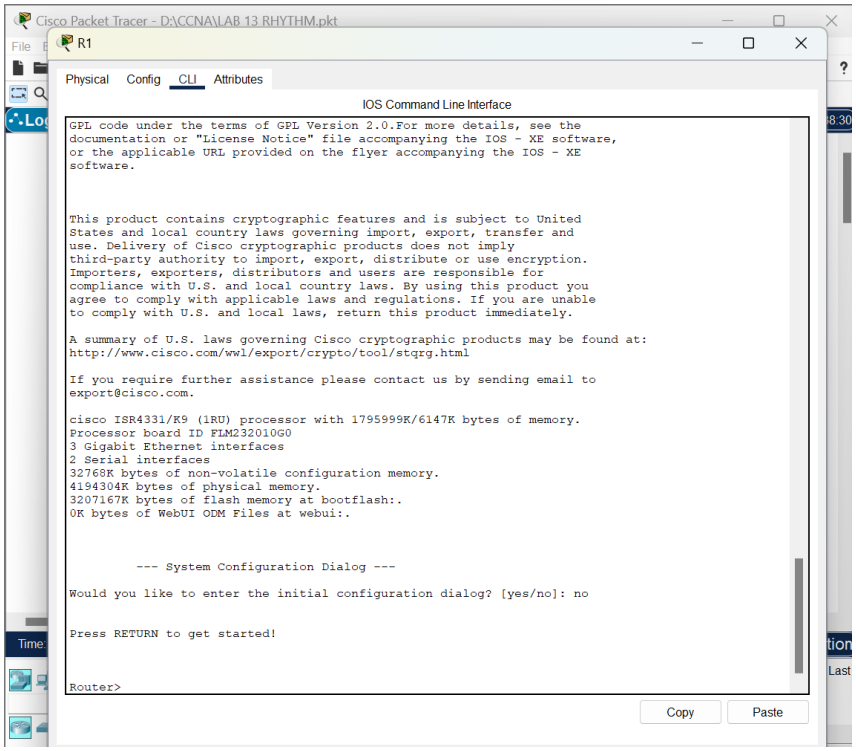
You will be prompted to terminate the autoinstall program. Respond **yes** and then press **Enter**. This step only applicable on real device not on virtual device.

```
Would you like to terminate autoinstall? [yes]: yes
```

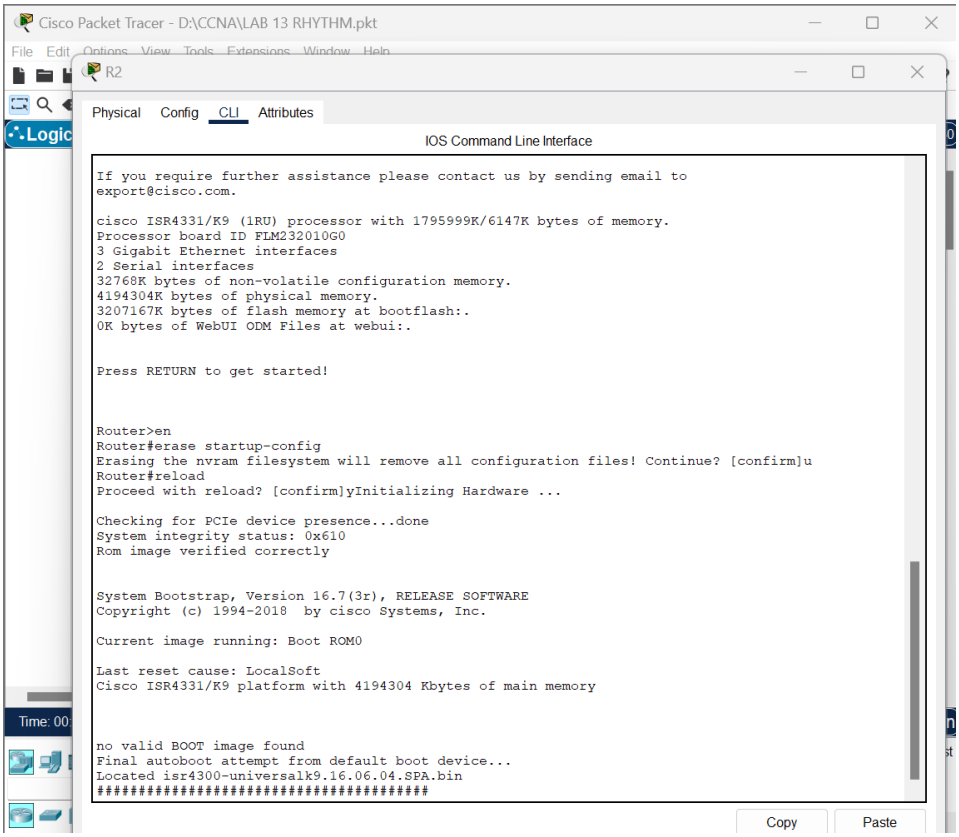
Router>

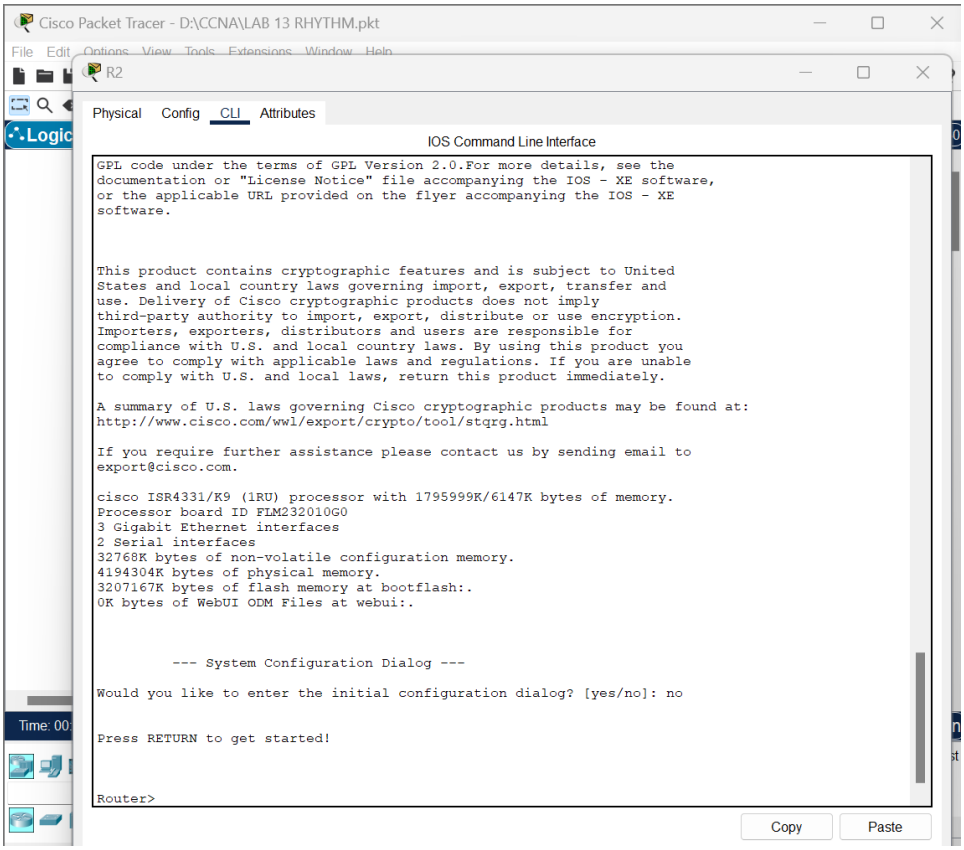
R1:


Cisco Packet Tracer - D:\CCNA\LAB 13 RHYTHM.pkt
R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
export@cisco.com.
cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0
3 Gigabit Ethernet interfaces
2 Serial interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.
Press RETURN to get started!
Router>en
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]yInitializing Hardware ...
Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly
System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.
Current image running: Boot ROM0
Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory
no valid BOOT image found
Final autoboot attempt from default boot device...
Located isr4300-universalk9.16.06.04.SPA.bin
Copy
Paste

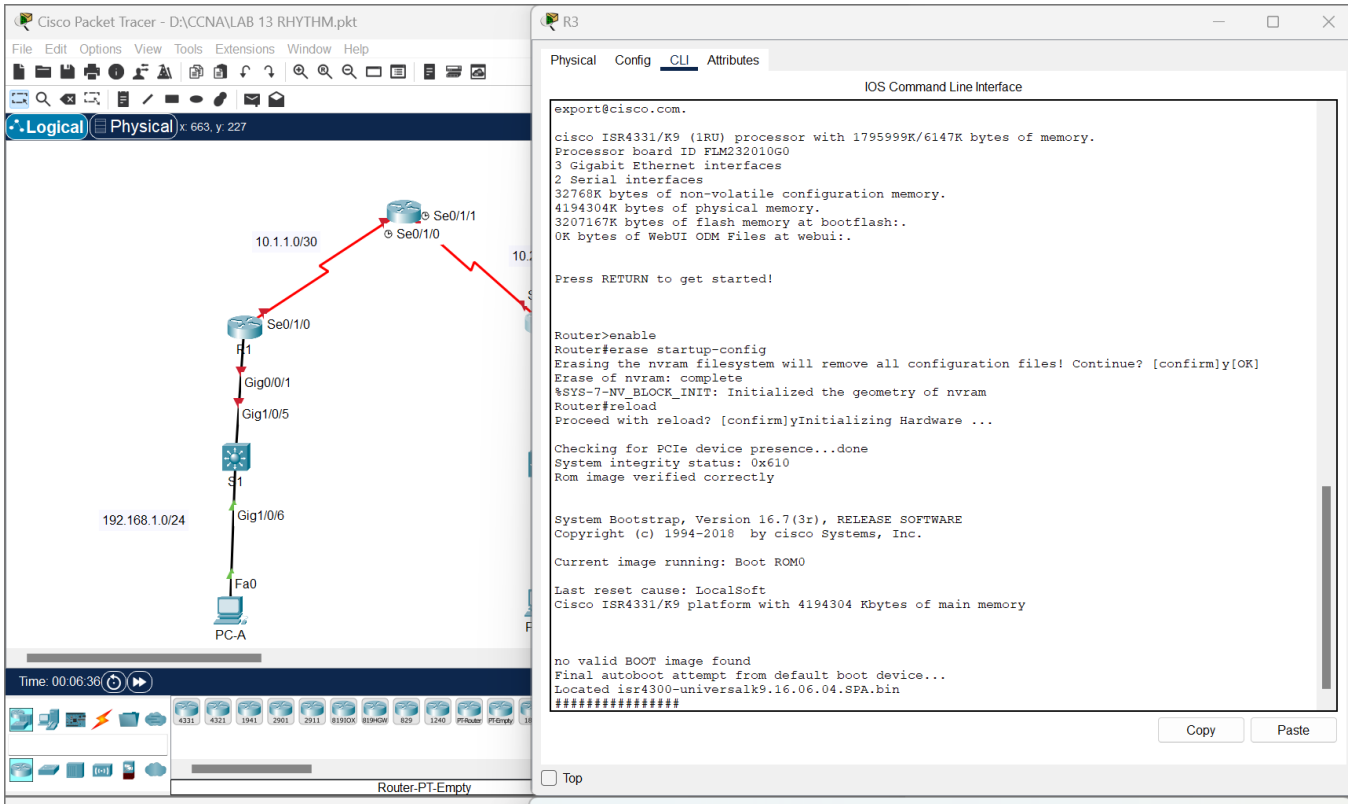

Cisco Packet Tracer - D:\CCNA\LAB 13 RHYTHM.pkt
R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
GPL code under the terms of GPL Version 2.0.For more details, see the
documentation or "License Notice" file accompanying the IOS - XE software,
or the applicable URL provided on the flyer accompanying the IOS - XE
software.
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0
3 Gigabit Ethernet interfaces
2 Serial interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>
Copy
Paste

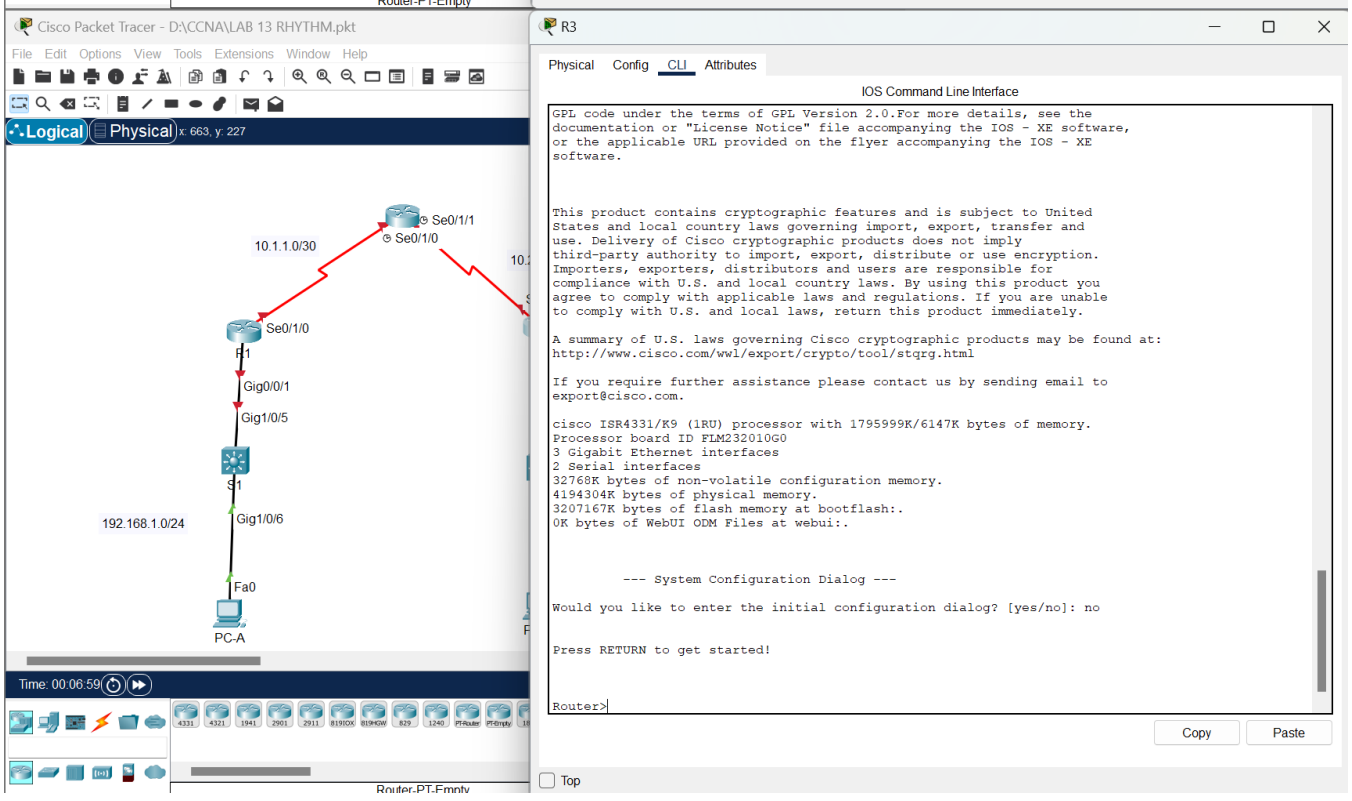
R2


Cisco Packet Tracer - D:\CCNA\LAB 13 RHYTHM.pkt
File Edit Options View Tools Extensions Window Help
R2
Physical Config CLI Attributes
IOS Command Line Interface
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0
3 Gigabit Ethernet interfaces
2 Serial interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.
Press RETURN to get started!
Router>en
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]u
Router#reload
Proceed with reload? [confirm]yInitializing Hardware ...
Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly
System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.
Current image running: Boot ROM0
Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory
no valid BOOT image found
Final autoboot attempt from default boot device...
Located isr4300-universalk9.16.06.04.SPA.bin
Copy
Paste


Cisco Packet Tracer - D:\CCNA\LAB 13 RHYTHM.pkt
File Edit Options View Tools Extensions Window Help
R2
Physical Config CLI Attributes
IOS Command Line Interface
GPL code under the terms of GPL Version 2.0.For more details, see the
documentation or "License Notice" file accompanying the IOS - XE software,
or the applicable URL provided on the flyer accompanying the IOS - XE
software.
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0
3 Gigabit Ethernet interfaces
2 Serial interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>
Copy
Paste

R3


Cisco Packet Tracer - D:\CCNA\LAB 13 RHYTHM.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 663, y: 227
Se0/1/1
Se0/1/0
10.1.1.0/30
Se0/1/0
R1
Gig0/0/1
Gig1/0/5
S1
192.168.1.0/24
Gig1/0/6
Fa0
PC-A
Time: 00:06:36
Router-PT-Empty
R3
Physical Config CLI Attributes
IOS Command Line Interface
export@cisco.com.
cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0
3 Gigabit Ethernet interfaces
2 Serial interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.
Press RETURN to get started!
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]yInitializing Hardware ...
Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly
System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.
Current image running: Boot ROM0
Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory
no valid BOOT image found
Final autoboot attempt from default boot device...
Located isr4300-universalk9.16.06.04.SPA.bin
#################
Copy
Paste
Top


Cisco Packet Tracer - D:\CCNA\LAB 13 RHYTHM.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 663, y: 227
Se0/1/1
Se0/1/0
10.1.1.0/30
Se0/1/0
R1
Gig0/0/1
Gig1/0/5
S1
192.168.1.0/24
Gig1/0/6
Fa0
PC-A
Time: 00:06:59
Router-PT-Empty
R3
Physical Config CLI Attributes
IOS Command Line Interface
GPL code under the terms of GPL Version 2.0.For more details, see the
documentation or "License Notice" file accompanying the IOS - XE software,
or the applicable URL provided on the flyer accompanying the IOS - XE
software.
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0
3 Gigabit Ethernet interfaces
2 Serial interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>
Copy
Paste
Top

Task 2: Initialize the switch and reload.

Step 1: Connect to the switch.

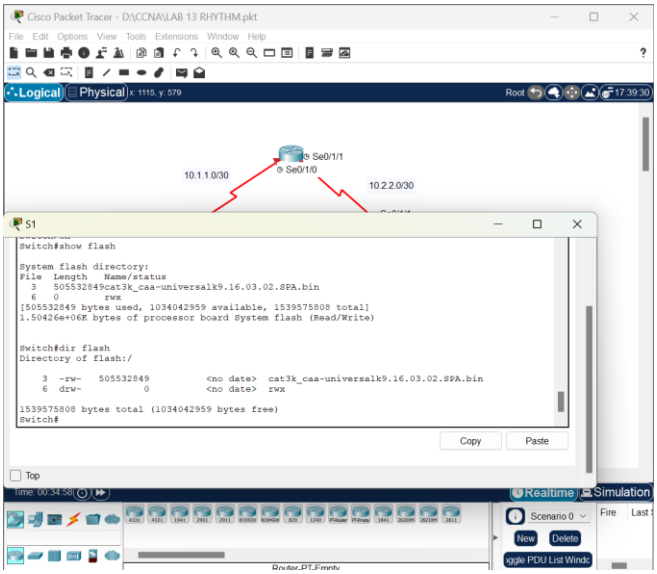
Console into the switch and enter privileged EXEC mode.

Switch> **enable**
Switch#

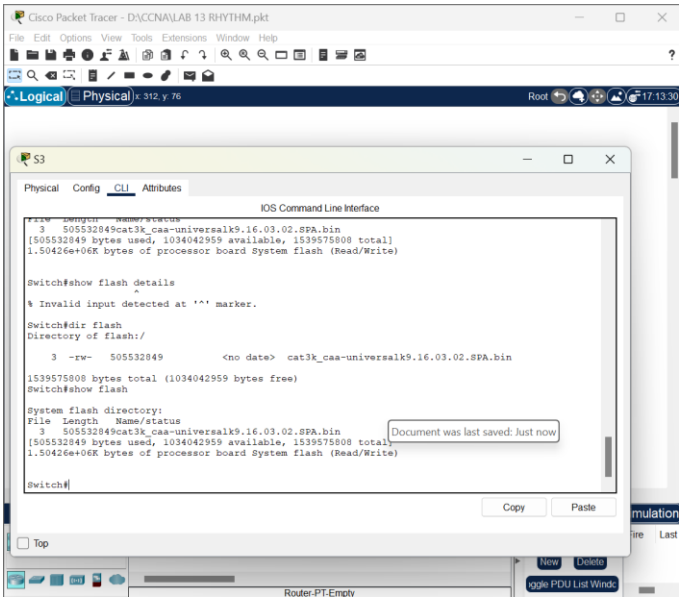
Step 2: Determine if there have been any virtual LANs (VLANs) created.

Use the **show flash** command to determine if any VLANs have been created on the switch.

S1



S2



```
Switch# show flash

Directory of flash:/

    2  -rwx        1919   Mar 1 1993 00:06:33 +00:00  private-
config.text
    3  -rwx        1632   Mar 1 1993 00:06:33 +00:00
config.text
    4  -rwx       13336   Mar 1 1993 00:06:33 +00:00  multiple-
fs
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-
lanbasek9-mz.150-2.SE.bin
    6  -rwx         616   Mar 1 1993 00:07:13 +00:00  vlan.dat

32514048 bytes total (20886528 bytes free)
Switch#
```

There is no vlan.dat in flash so no need to follow step 3 a,b

Step 3: Delete the VLAN file.

a. If the **vlan.dat** file was found in flash delete this file.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

You will be prompted to verify the file name. At this point, you can change the file name or press **Enter** if you have entered the name correctly.

b. When you are prompted to delete this file, press **Enter** to confirm the deletion. Pressing any other key will abort the deletion.

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Step 4: Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When prompted to remove the configuration file, press **Enter** to confirm the erase. (Pressing any other key will abort the operation.)

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

```
Switch#
```

Step 5: Reload the switch.

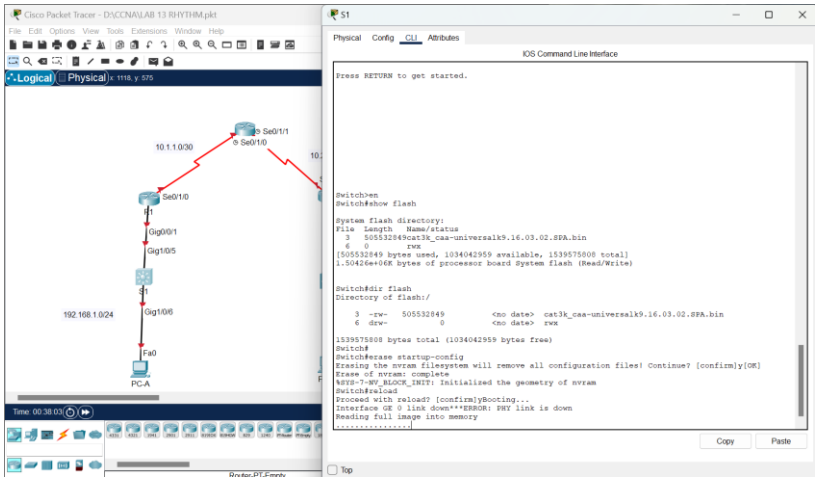
Reload the switch to remove old configuration information from memory. When prompted to reload the switch, press **Enter** to proceed with the reload. Pressing any other key will abort the reload.

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

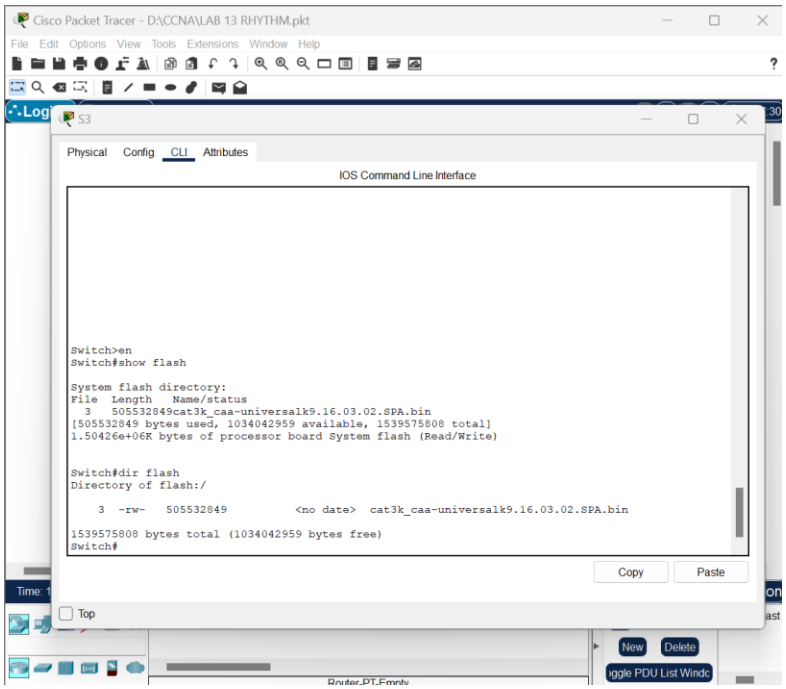
Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press **Enter**.

```
System configuration has been modified. Save? [yes/no]: no
```

S1



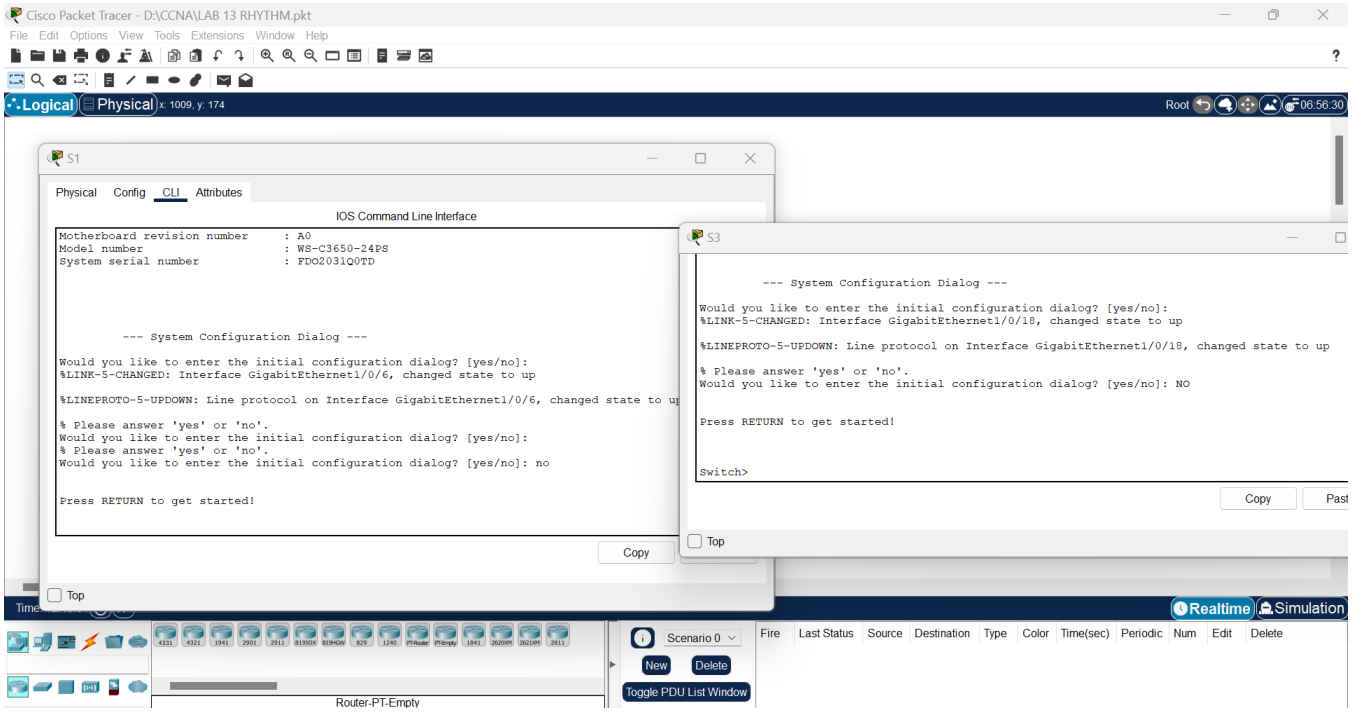
S3



Step 6: Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press **Enter**.

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

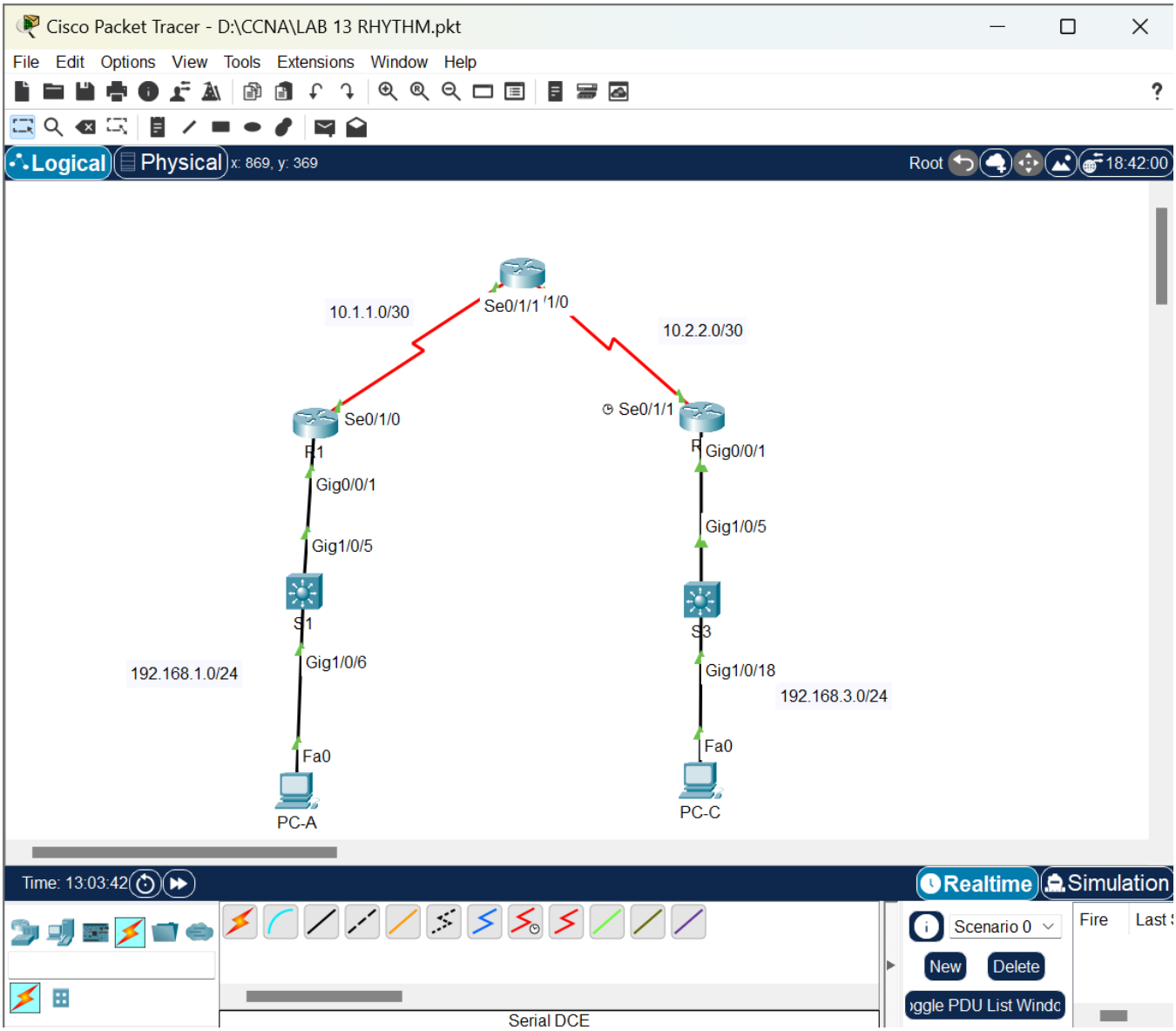


Part 2: Basic Network Device Configuration

In Part 2 of this lab, you will set up the network topology and configure basic settings such as interface IP addresses and routing.

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 each router.

a. Configure host names as shown in the topology.

b. Configure the interface IP addresses as shown in the IP Addressing Table.

c. Configure a clock rate for the routers with a DCE serial cable attached to their serial interface.

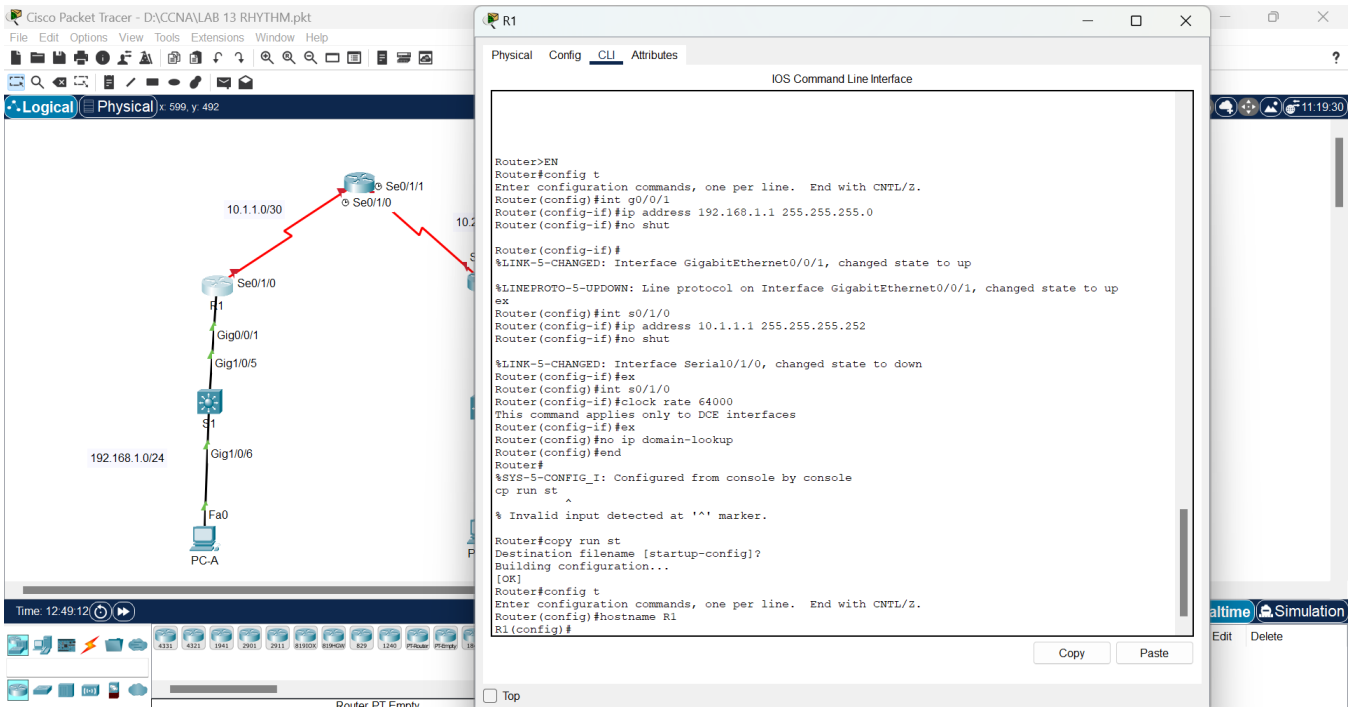
R1(config)# **interface S0/1/0**

R1(config-if)# **clock rate 64000**

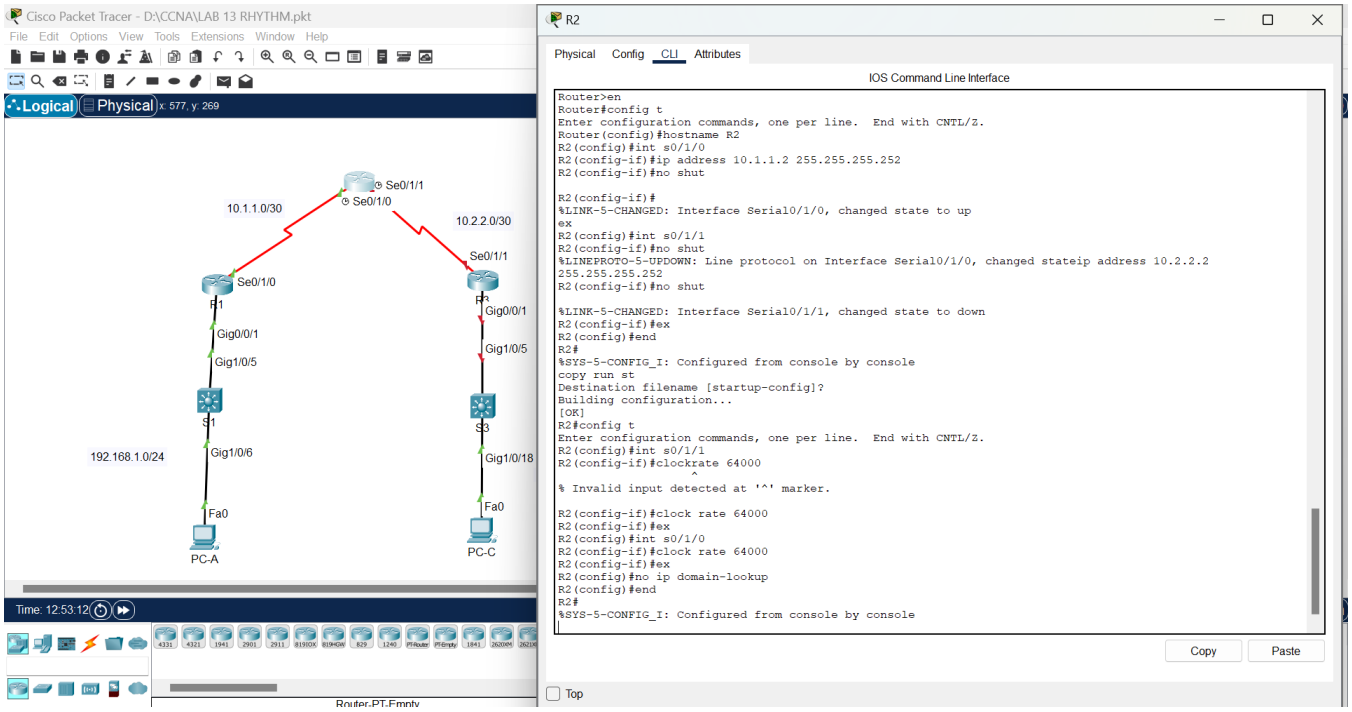
d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

R1(config)# **no ip domain-lookup**

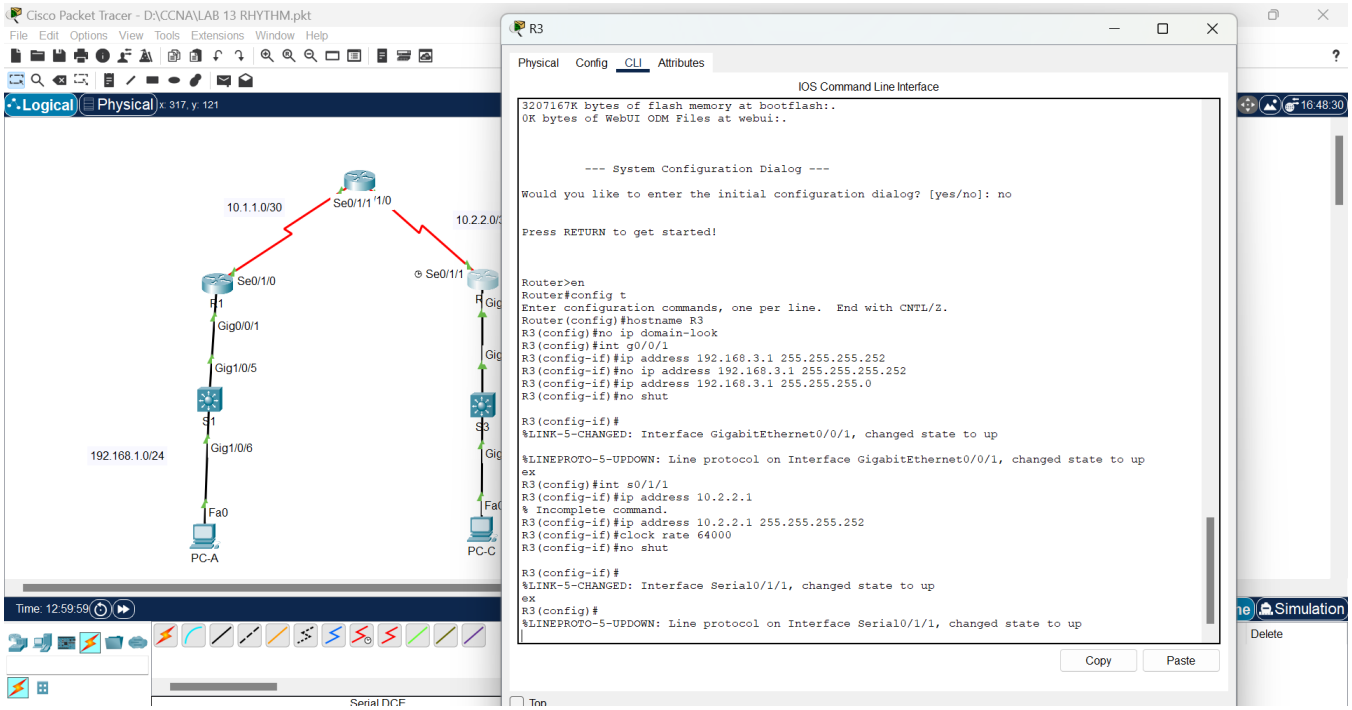
R1



R2


Cisco Packet Tracer - D:\CCNA\LAB 13 RHYTHM.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 577, y: 269
10.1.1.0/30
10.2.2.0/30
Se0/1/1
Se0/1/0
R1
R2
Gig0/0/1
Gig1/0/5
S1
S3
192.168.1.0/24
Gig1/0/6
Gig1/0/18
Fa0
PC-A
PC-C
Time: 12:53:12
Router-PT-Empty
R2
Physical Config CLI Attributes
IOS Command Line Interface
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int s0/1/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
ex
R2(config)#int s0/1/1
R2(config-if)#no shut
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed stateip address 10.2.2.2
255.255.255.252
R2(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
R2(config-if)#ex
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
copy run st
Destination filename [startup-config]?
Building configuration...
[OK]
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/1/1
R2(config-if)#clockrate 64000
^
% Invalid input detected at '^' marker.
R2(config-if)#clock rate 64000
R2(config-if)#ex
R2(config)#int s0/1/0
R2(config-if)#clock rate 64000
R2(config-if)#ex
R2(config)#no ip domain-lookup
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
Copy
Paste
Top

R3

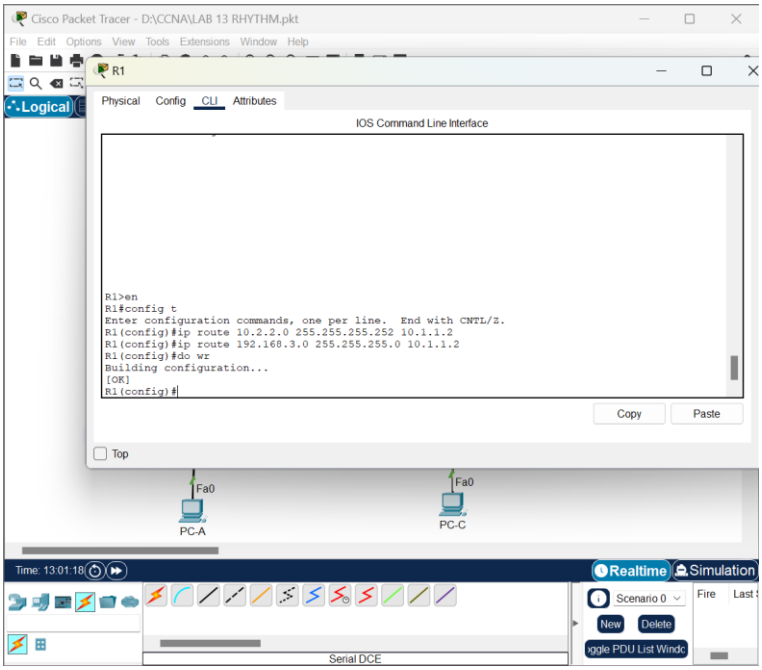

Cisco Packet Tracer - D:\CCNA\LAB 13 RHYTHM.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 317, y: 121
10.1.1.0/30
Se0/1/0
R1
Gig0/0/1
Gig1/0/5
S1
192.168.1.0/24
Gig1/0/6
Fa0
PC-A
PC-C
Time: 12:59:59
Serial DCE
R3
Physical Config CLI Attributes
IOS Command Line Interface
3207167K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#no ip domain-look
R3(config)#int g0/0/1
R3(config-if)#ip address 192.168.3.1 255.255.255.252
R3(config-if)#no ip address 192.168.3.1 255.255.255.252
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
ex
R3(config)#int s0/1/1
R3(config-if)#ip address 10.2.2.1
% Incomplete command.
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#clock rate 64000
R3(config-if)#no shut
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up
ex
R3(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up
Copy
Paste
Top
16:48:30
Simulation
Delete

Step 3: Configure routing on the routers.

Configure the static routing on routers R1 and R3 as below:

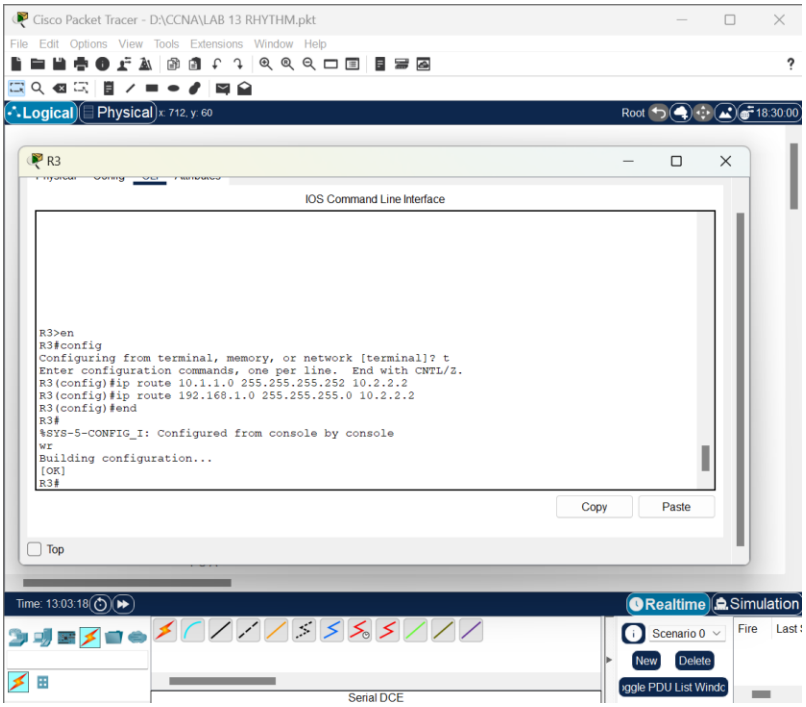
R1(config)# **ip route 10.2.2.0 255.255.255.252 10.1.1.2**

R1(config)# **ip route 192.168.3.0 255.255.255.0 10.1.1.2**



R3(config)# **ip route 10.1.1.0 255.255.255.252 10.2.2.2**

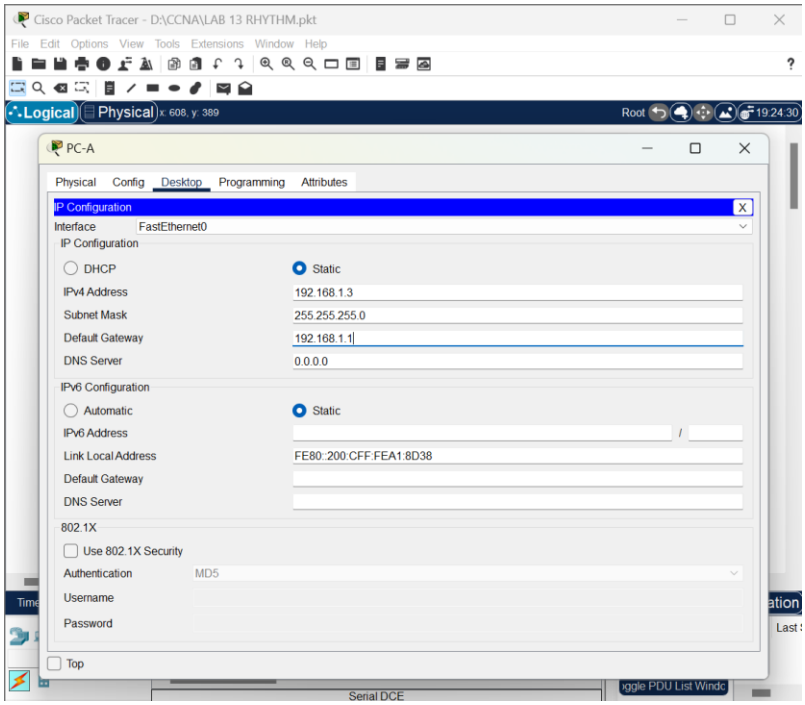
R3(config)# **ip route 192.168.1.0 255.255.255.0 10.2.2.2**



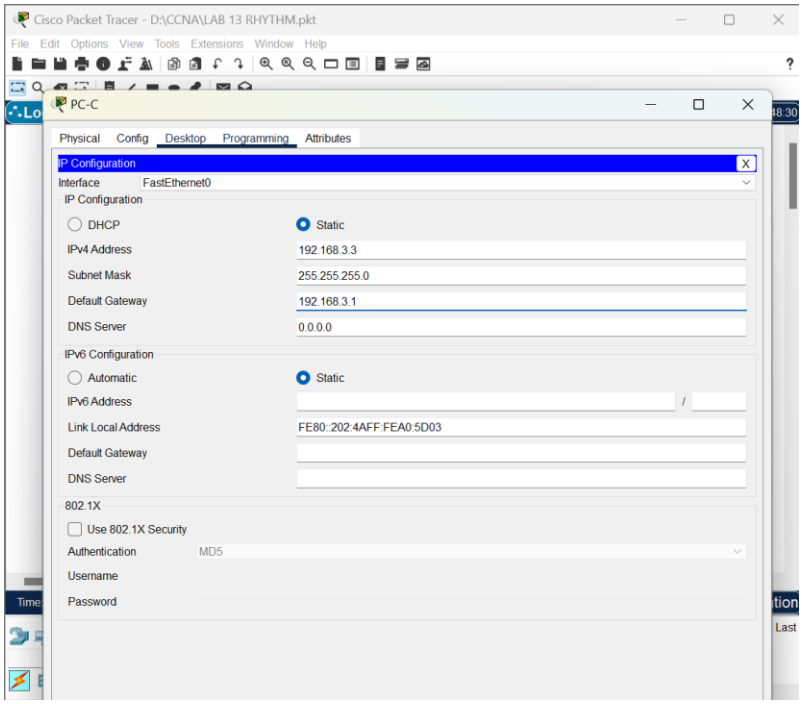
Step 4: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C, as shown in the IP addressing table.

PC-A

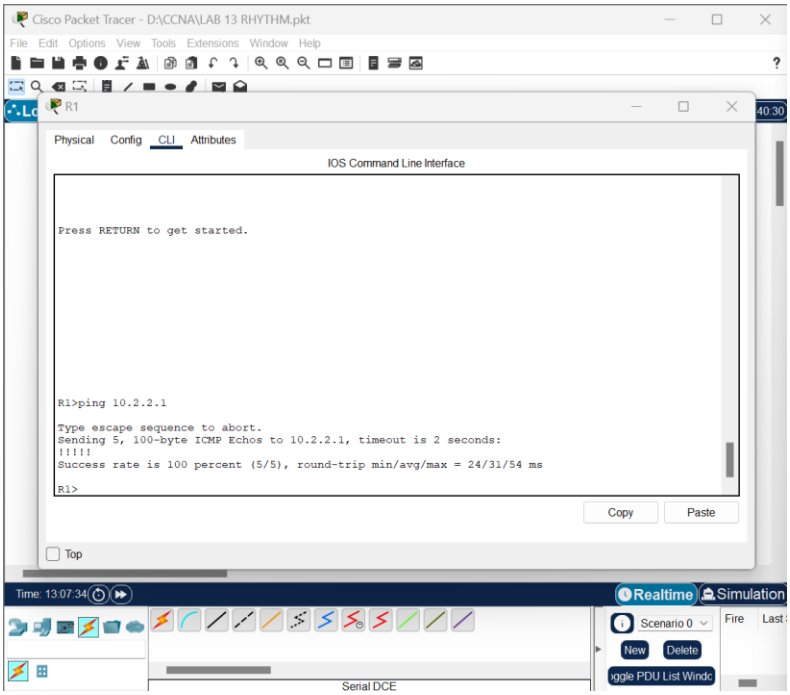


PC-C



Step 5: Verify connectivity between PC-A and R3.

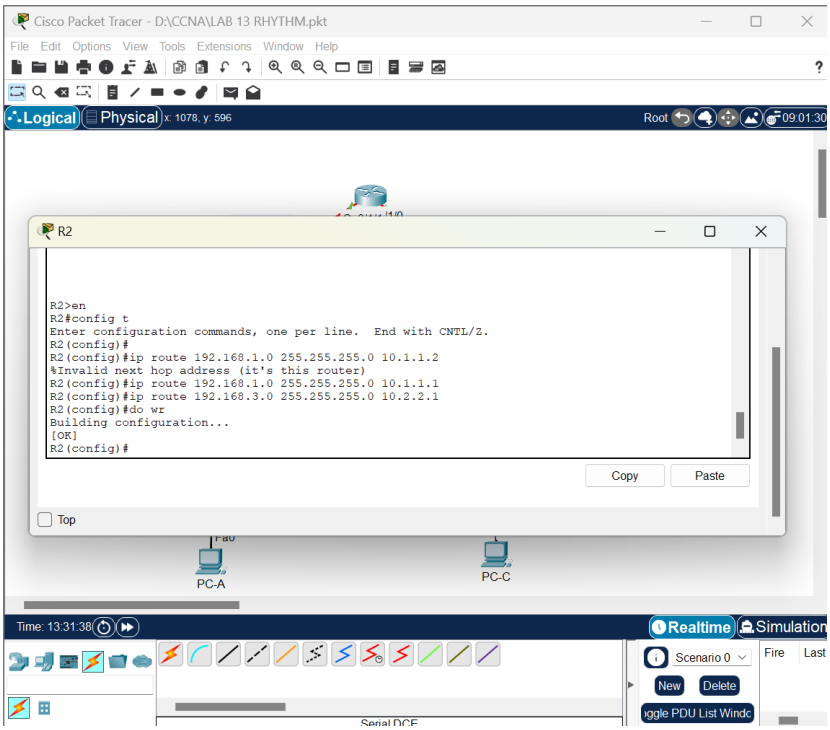
a. Ping from R1 to R3.

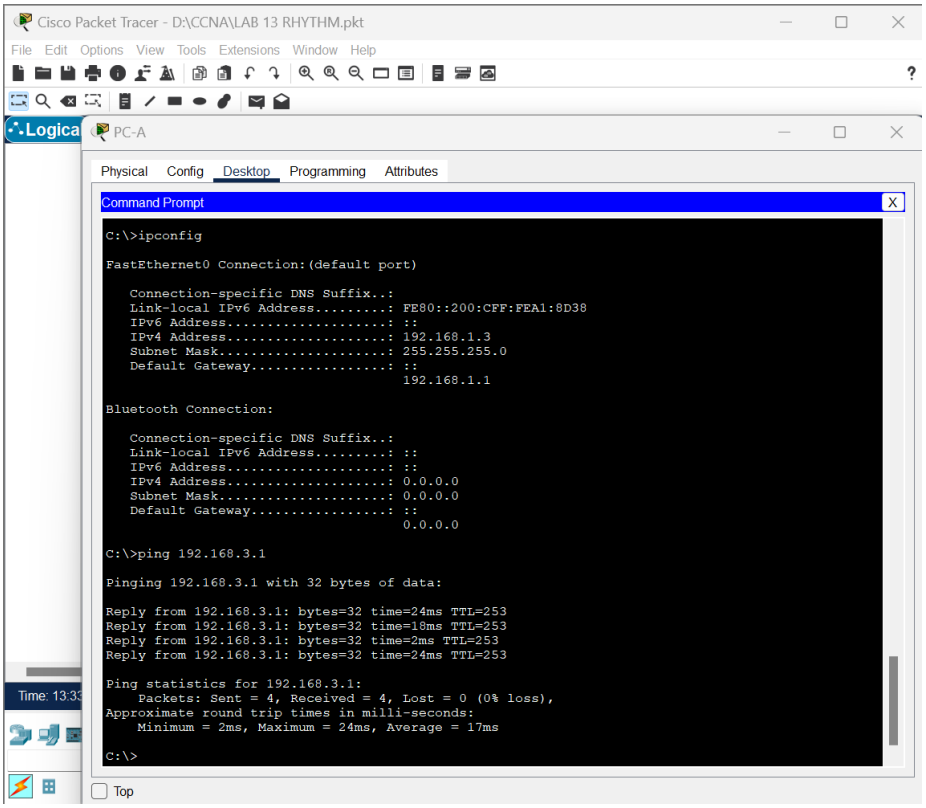


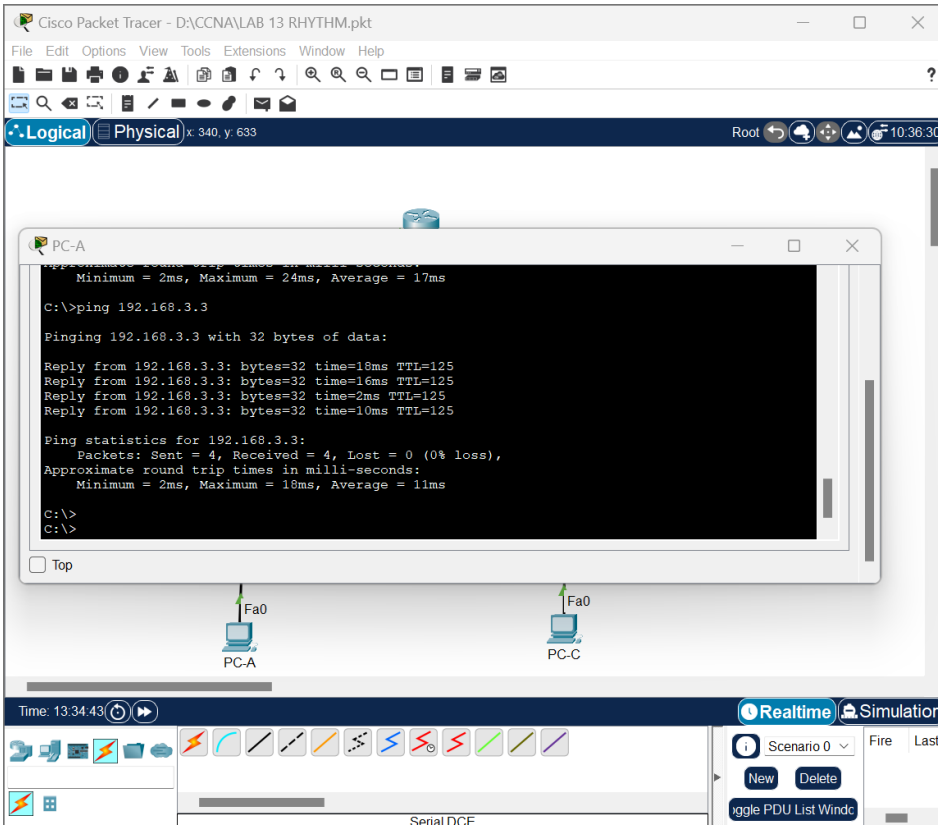
If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

After Troubleshoot







If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C, you have demonstrated that static routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to help identify routing protocol-related problems.

Part 3: Router Access for CCP

In Part 3 of this lab, you will set up a router for use with CCP by enabling a secure HTTP server, creating a privileged user account and configuring a SSH and Telnet access.

Step 1: Connect to your router through Telnet, SSH or the console.

Enter the global configuration mode using the command:

Router> **enable**
Router# **configure terminal**

Step 2: Enable the router as an HTTP server.

a. Enable HTTP server.

Router(config)# **ip http server**

b. For a secure connection, enable the secure HTTP server.

Router(config)# **ip http secure-server**
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

R1(config)#
*Jan 1 17:23:44.103: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jan 1 17:23:44.215: %PKI-4-NOAUTOSAVE: Configuration was modified. Issue "write memory" to save new certificate

Note: A secure HTTP server can only be enabled for cryptography-enabled Cisco IOS Software images. It is also possible to connect using an unsecure connection if the command **ip http server** is configured; however, this is an unsecure connection and not recommended for production environments.

c. Configure authentication for HTTP access using the local authentication.

Router(config)# **ip http authentication local**

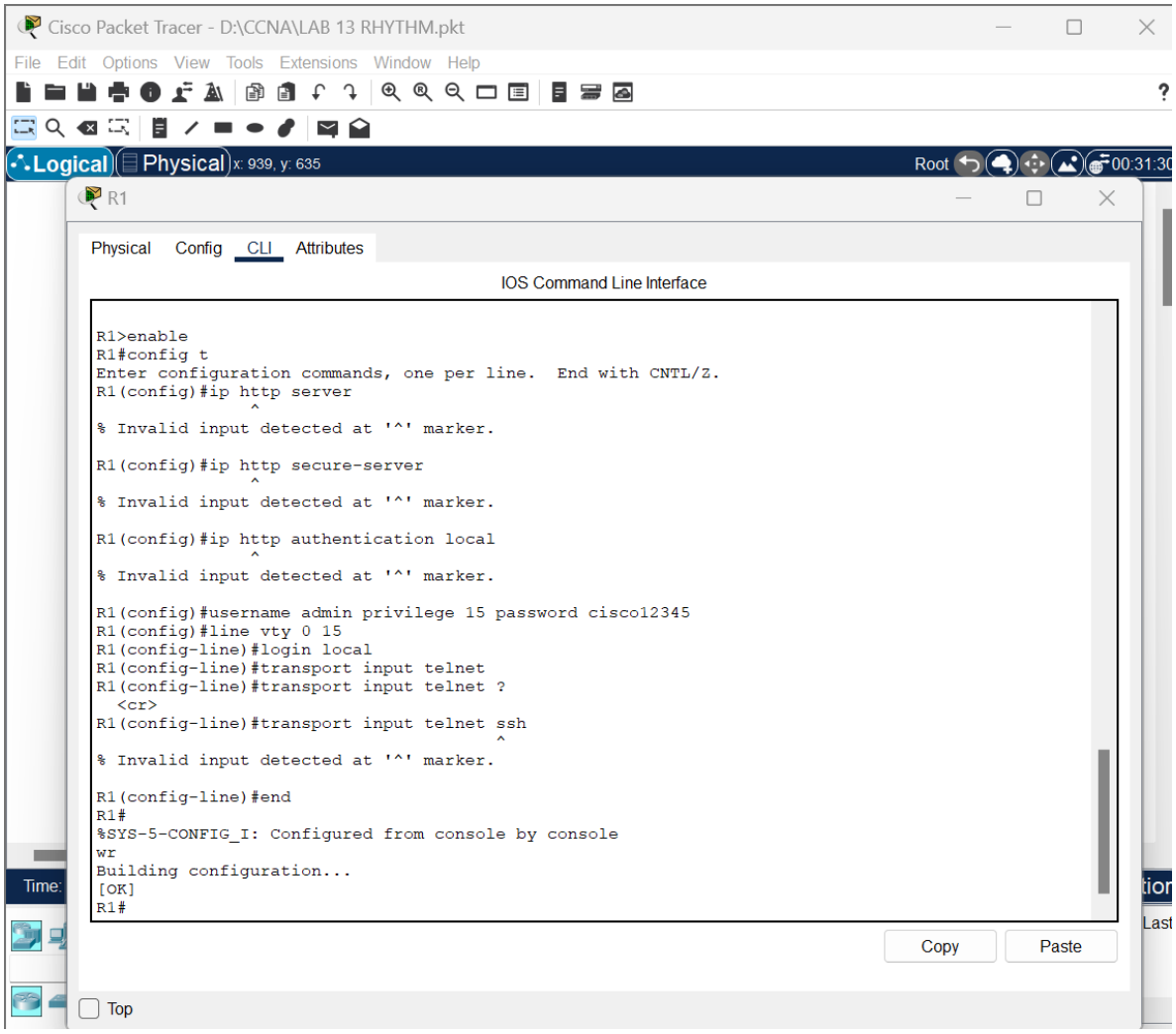
Step 3: Create a user with privilege level 15.

Router(config)# **username admin privilege 15 password cisco12345**

Step 4: Configure SSH and Telnet for local login.

Router(config)# **line vty 0 15**

Router(config-line)# **login local**
Router(config-line)# **transport input telnet**
Router(config-line)# **transport input telnet ssh**
Router(config-line)# **exit**



As shown in the picture ip http server, ip http secure-server, ip http authentication local is not working this commands will working on real time devices only.

Part 4: Java Settings on PCs

The next-generation Java Plug-in must be enabled, and the security setting must be set to Medium for the CCP configuration of IPS. To support CCP configuration of IPS, the PC should be running Java JRE version 6 or newer to set the Java heap to 256 MB. This is done using the runtime parameter –Xmx256m. The latest JRE for Windows can be downloaded from Oracle Corporation at http://www.oracle.com/.

Step 1: Enable next-generation Java Plug-in.

a. Open the **Control Panel**, select **Java** to access the Java Control Panel.

b. In the Java Control Panel, click the **Advanced** tab.

c. Locate the heading Java Plug-in. Select the checkbox to **Enable the next-generation Plug-in**, which requires browser restart.

d. Click **Apply**.

e. Click **Yes** to allow the changes. Then click **OK** to acknowledge the changes.

Step 2: Change the Java security settings.

a. Click the **Security** tab.

b. Change the Security Level to **Medium** by moving the slider.

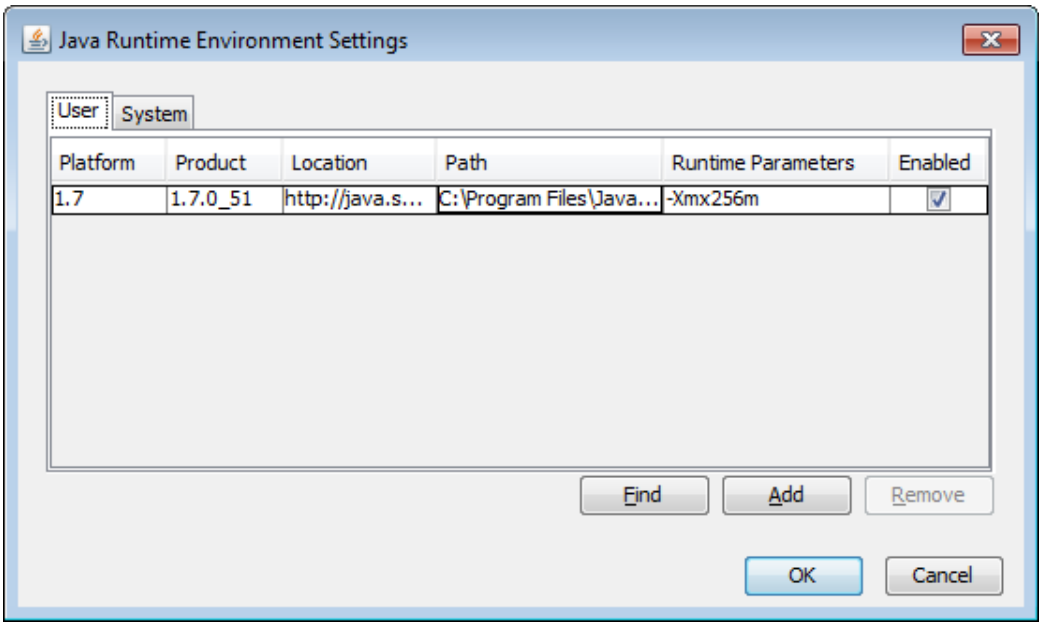
c. Click **Apply**.

Step 3: Change the Java Applet Runtime settings.

a. Click the **Java** tab and click the **View** button to change the Java Applet Runtime Settings.

b. Double-click the **Runtime Parameters** box. Type **–Xmx256m** in the box.

c. Click **OK**. Click **OK** again to exit the Java Control Panel.



Step 4: Restart all web browsers, including CCP if opened for the changes to take effect.

Part 5: CCP Installation and Initial Setup

Step 1: Install CCP.

Note: This section can be skipped if CCP is already installed on your PC.

a. Download CCP 2.5 from Cisco's website:

http://www.cisco.com/cisco/software/release.html?mdfid=281795035&softwareid=282159854&release=2.5&rellifecycle=&relind=AVAILABLE&reltype=all

Note: Be sure to select the correct CCP file and not CCP Express. If there is a more current release of CCP, you may choose to download it. However, the labs in this course are based on CCP 2.5.

b. Choose the file **cisco-config-pro-k9-pkg-2_5-en.zip**.

Note: Choose the PC-based version, not the Express version.

c. Agree to the terms and conditions. Download and save the file to the desired location.

d. Open the zip file and run the CCP executable.

e. Follow the on-screen instructions to install CCP 2.5 on your PC.

Step 2: Run CCP as Administrator.

If CCP is installed on a PC that uses the Microsoft Windows Vista operating system or the Microsoft Windows 7 operating system, CCP may fail to launch. Two possible solutions are listed below:

a. Option 1: Run as Administrator settings:

1) Right click on the CCP icon or menu item and select **Properties**.

2) While in the **Properties** dialog box, select the **Compatibility** tab. In this tab, select the checkbox for **Run this program as administrator** in Privilege Level section.

3) Click **OK**.

b. Option 2: Run as Administrator for each launch:

1) Right click on the CCP icon or menu item and select **Run as Administrator**.

2) For more information, please refer to the Cisco CP Quick Start Guide or search for "run as administrator" for your operating system on the internet.

Note: It may be necessary to temporarily disable antivirus programs and O/S firewalls to run CCP.

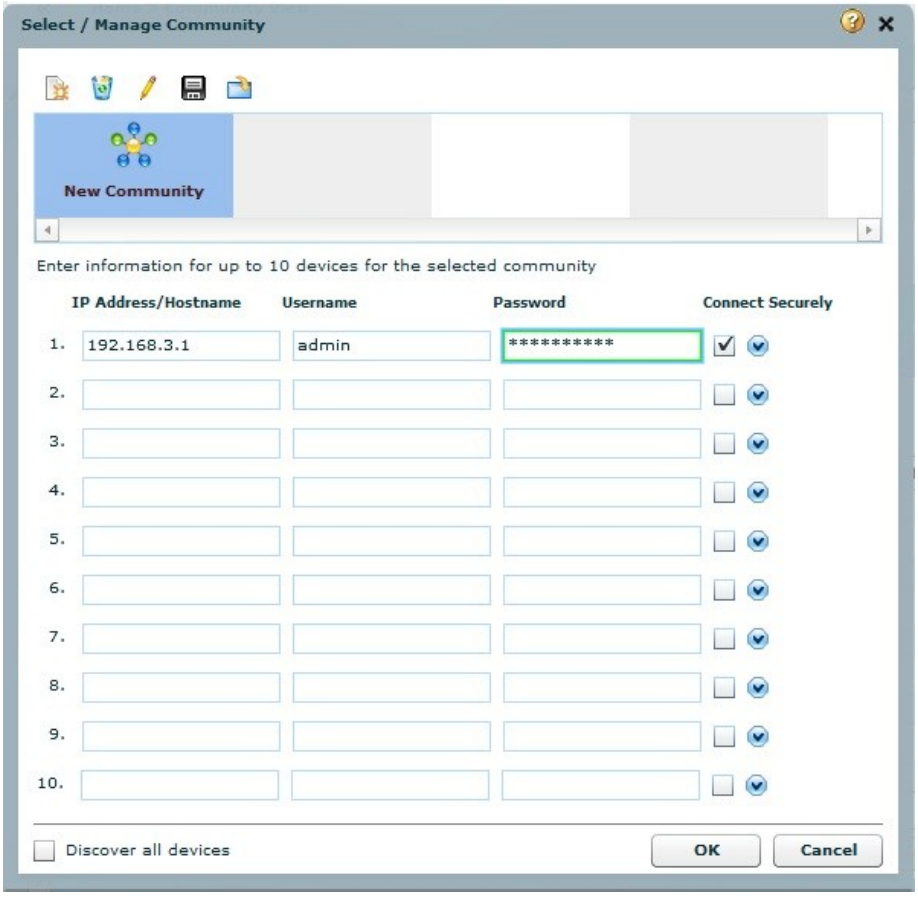
Step 3: Create/Manage Communities.

CCP 2.5 can discover up to 10 devices in a community. If desired, the information for both R1 and R3 can be included in one community if the PC has network connectivity to the routers. Only R3 is discovered on PC-C in this section.

a. On PC-C, start CCP: **Start** > **Cisco Configuration Professional**.

b. In the Select/Manage Community window, input into the appropriate fields the R3 IP address 192.168.3.1, the username **admin**, and the password **cisco12345**. The checkbox **Connect Securely** can be selected for a more secure connection to the device. This requires the configuration of the command **ip http secure-server**.

c. Click **OK** to continue.

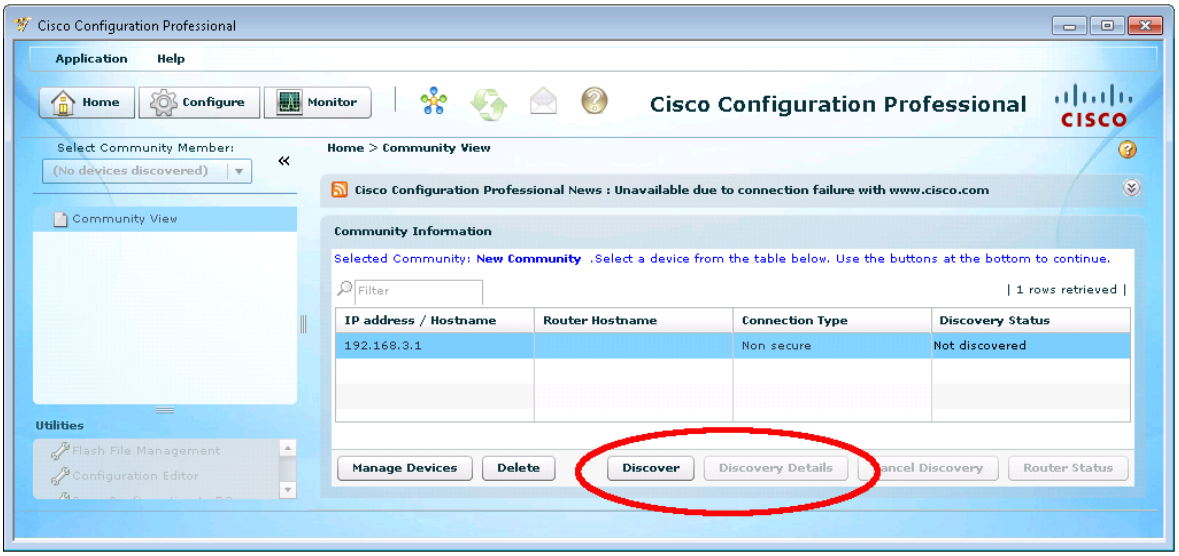


Step 4: Discovery Router Devices.

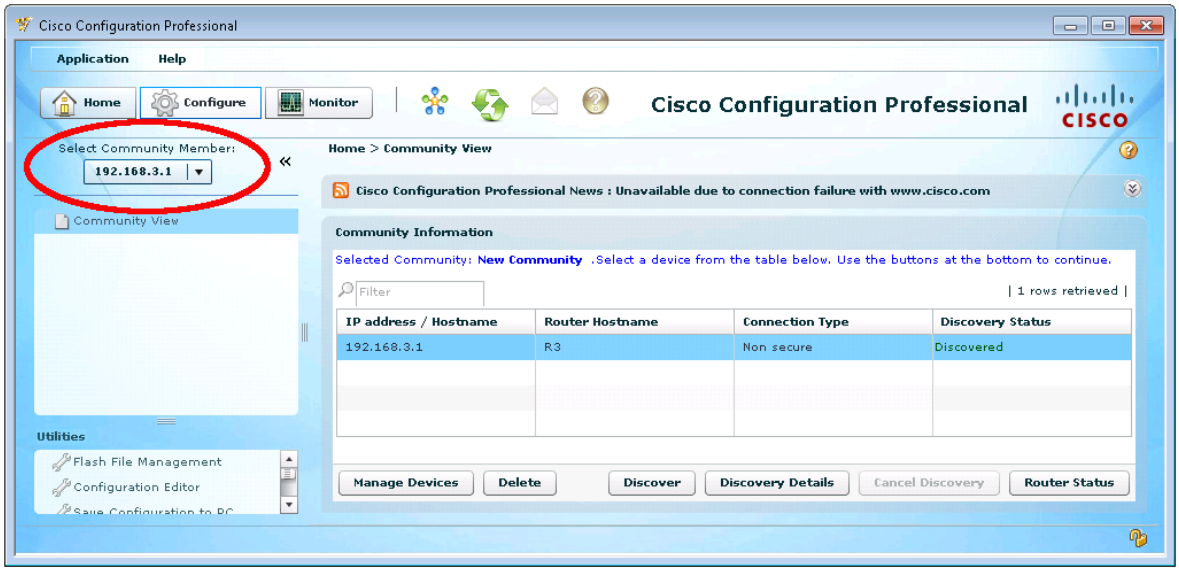
a. Click **Discover** on the dashboard to discover and connect to R3. If discovery fails, click the **Discovery Details** button to determine the problem so you can resolve the issue.

When connecting securely, you must accept the certificate when the Security Certificate Alert window displays to establish a connection to the device. CCP uses the Internet Explorer (IE) browser. Be sure IE settings are set to allow pop-up windows.

Note: If you experience problems with accepting the security certificate, you can connect using an unsecure connection. The command **ip http server** must be configured on the router and the checkbox **Connect Securely** (from step 2 above) must be unchecked. Keep in mind, this is an unsecure connection and not recommended in a production environment.



b. After the router has been discovered by CCP, you are ready to configure your Select Community Member. In this example, the Select Community Member is 192.168.3.1.



c. After the successful discovery of the device, configure the device as directed in the respective labs.