The University of Jordan, Comp. Eng. Dept.

Networks lab: Handout: Experiment 8 Configuration of Basic and Real Devices (Theory and Practice)

Instructors: Prof. Khalid A. Darabkh and Eng. Muna Al-Akhras

Parts Involved: Basic device configuration and Real devices configuration.

Part I: Basic device configuration:

It is important to highlight the following:

- Common configuration tasks include setting the hostname, access passwords, and Message of the Day Banner (MOTD banner).
- Configuration changes are effective immediately.
- Configuration changes must be saved in non-volatile RAM (NVRAM) to be persistent across reboot.
- Configuration changes may also be saved off-line in a text file for auditing or device replacement.
- Cisco IOS switch configuration is similar to Cisco IOS router configuration.

Important Note: All configuration commands discussed in this experiment are applied for switches and routers in the same manner except for configuring router interfaces since the switch ports don't accept IP address configuration.

1. **Device Hostname:** You can change the device hostname displayed in the command prompt from the default name to another character string. When you give the device a unique hostname, you can easily identify the device from the command-line interface (CLI) prompt.
   - ✓ From the privileged exec mode, enter global configuration mode:

     ```
     Router# configure terminal
     Router(config)#
     ```
   - ✓ Set the device hostname to Network_Lab:

     ```
     Router(config)# hostname Network_Lab
     Network_Lab(config)#
     ```
2. **MOTD:** MOTD banner is displayed before the user login prompt on the device. This message can contain any information that you want to display for users of the device.

   ```
   Router(config)# banner motd % Enter Any TEXT message End%
   ```

   In production networks, banner content may have a significant legal impact on the organization. For example, a friendly "Welcome" message may be interpreted by a court that an attacker has been granted permission to hack into the router. A banner should include information about authorization, penalties for unauthorized access, connection logging, and applicable local laws. The corporate security policy should provide policy on all banner messages.
3. **Cisco router password access:** Access passwords are set for **the privileged exec mode** and **user entry point such as console, aux, and virtual lines.** The privileged exec mode password is the most critical password, since it controls access to the configuration mode.
   - ➢ **Configure the privileged exec password:** Cisco IOS supports two commands that set access to the privileged exec mode.

  - The first command contains weak cryptography and should never be used if the enable secret command is available.

    ```
    Router(config)# enable password class
    ```

  - The enable secret command uses a very secure MD5 cryptographic hash algorithm. Password security relies on the password algorithm, and the password. In production environments, strong passwords should be used at all times. A strong password consists of at least nine characters of upper and lower case letters, numbers, and symbols. In a lab environment, we will use weak passwords. Set the privileged exec password to cisco.

    ```
    Router(config)# enable secret cisco
    ```

- **Configure the console password:** The console password controls console access to the router.

  ```
  Router(config)# line console 0
  Router(config-line)# password class
  Router(config-line)# login
  ```

- **Configure the virtual line password:** The virtual line password controls **Telnet access** to the router. In early Cisco IOS versions, only five virtual lines could be set, 0 through 4. In newer Cisco IOS versions, the number has been expanded. Unless a telnet password is set, access on that virtual line is blocked. There are 16 virtual lines that can be configured on a Cisco switch, 0 through 15.

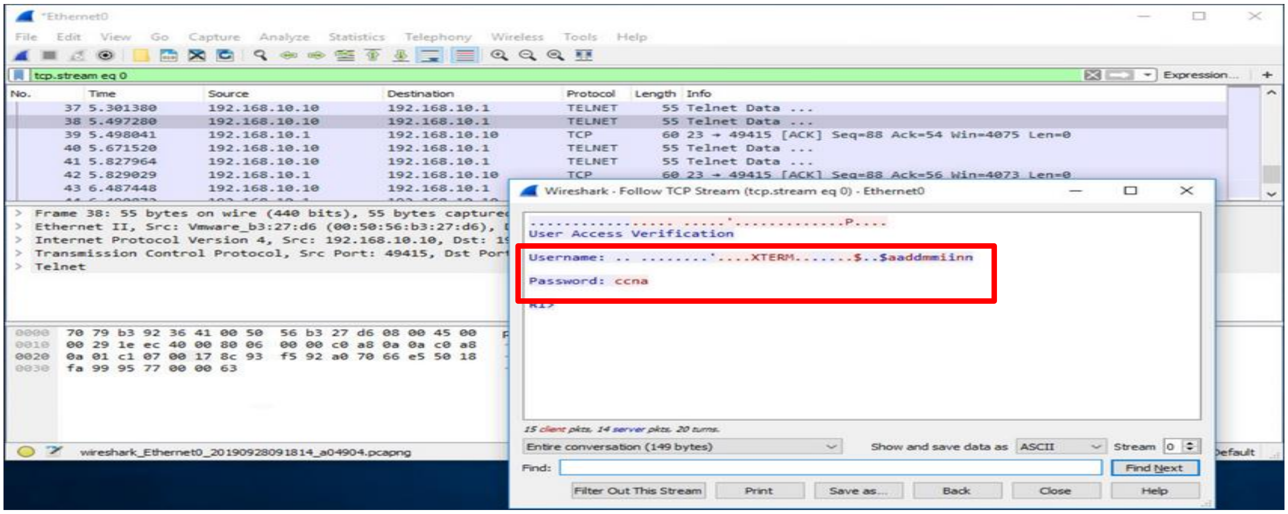
  ```
  Router(config-line)# line vty 0 4
  Router(config-line)# password class
  Router(config-line)# login
  ```

- **Encrypt passwords:** When you use the `show run` command, the console and virtual line passwords appear in plain text. Thus, to encrypt the plain text passwords, use the following command, the effect of this command that the passwords are hidden using a weak encryption algorithm.

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

4. Configuring Secure Shell (SSH)

You might not always have direct access to your switch or router when you need to configure it. You need to be able to access it remotely and it is imperative that your access is secure. Telnet uses TCP port 23. It is an older protocol that uses unsecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices. A threat actor can monitor packets using Wireshark. For example, Figure 1 presents how the threat actor captured the username admin and password ccna from a Telnet session.



*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Wireshark - Follow TCP Stream (tcp.stream eq 0) - Ethernet0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Default

```
tcp.stream eq 0
No.   Time        Source          Destination     Protocol  Length Info
   37 5.301380    192.168.10.10   192.168.10.1    TELNET    55 Telnet Data ...
   38 5.497280    192.168.10.10   192.168.10.1    TELNET    55 Telnet Data ...
   39 5.498041    192.168.10.1    192.168.10.10   TCP       60 23 → 49415 [ACK] Seq=88 Ack=54 Win=4075 Len=0
   40 5.671520    192.168.10.10   192.168.10.1    TELNET    55 Telnet Data ...
   41 5.827964    192.168.10.10   192.168.10.1    TELNET    55 Telnet Data ...
   42 5.829029    192.168.10.1    192.168.10.10   TCP       60 23 → 49415 [ACK] Seq=88 Ack=56 Win=4073 Len=0
   43 6.487448    192.168.10.10   192.168.10.1

> Frame 38: 55 bytes on wire (440 bits), 55 bytes capture
> Ethernet II, Src: Vmware_b3:27:d6 (00:50:56:b3:27:d6),
> Internet Protocol Version 4, Src: 192.168.10.10, Dst: 1
> Transmission Control Protocol, Src Port: 49415, Dst Port
> Telnet

0000  70 79 b3 92 36 41 00 50  56 b3 27 d6 08 00 45 00
0010  00 29 1e ec 40 00 80 06  00 00 c0 a8 0a 0a c0 a8
0020  0a 01 c1 07 00 17 8c 93  f5 92 a0 70 66 e5 50 18
0030  fa 99 95 77 00 00 63

wireshark_Ethernet0_20190928091814_a04904.pcapng
```

```
..................  .....'..............P....
User Access Verification

Username: ..  .........'....XTERM.......$..$aaddmmiinn

Password: ccna

R1>
```

15 client pkts, 14 server pkts, 20 turns.

Entire conversation (149 bytes) | Show and save data as ASCII | Stream 0

Figure 1: Unsecure Telnet password

To enable SSH, The IOS filename must includes the combination “**k9**” which indicated that it supports cryptographic (encrypted) features and capabilities. The example below shows the output of the `show version` command.

```
Switch# show System image file is "flash:c2960-lanbasek9-mz.150-2.SE4.bin" version
```

➢ **Configuring SSH:**

a. **Verify SSH support:** Use the `show ip ssh` command to verify that the switch supports SSH. If the switch is not running an IOS that supports cryptographic features, this command is unrecognized.

b. **Configure the IP domain,** use the following command:

```
Switch(config)# ip domain-name cisco.com
```

c. **Generate RSA key pairs:** Use the `crypto key generate rsa` global configuration mode command to enable the SSH server on the switch and generate an RSA key pair. When generating RSA keys, the administrator is prompted to enter a modulus length. The sample configuration in the figure uses a modulus size of 1,024 bits. A longer modulus length is more secure, but it takes longer to generate and to use.

```
Switch(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024
```

d. **Configure user authentication:**The SSH server can authenticate users locally or using an authentication server. To use the local authentication method, create a username and password pair using the **username** username **secret** password global configuration mode command. In the example, the user admin is assigned the password ccna.

```
Switch(config)# username admin secret ccna
```

e. **Configure the vty lines:** Enable the SSH protocol on the vty lines by using the `transport input ssh` line configuration mode command. The Catalyst 2960 has vty lines ranging from 0 to 15. This configuration prevents non-SSH (such as Telnet) connections and limits the switch to accept only SSH connections. Use the line vty global configuration mode command and then the login local line configuration mode command to require local authentication for SSH connections from the local username database.

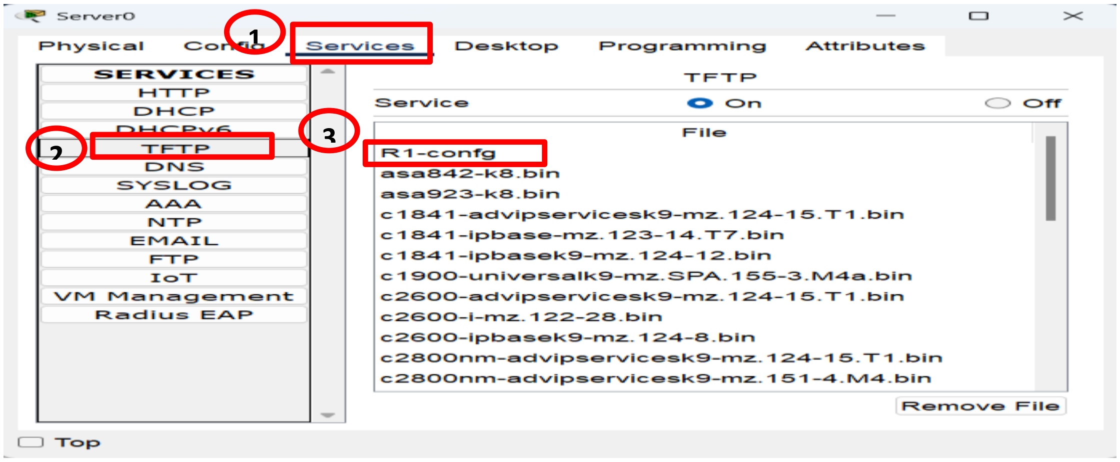
```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

5. Using TFTP server to save configuration files

a. From the privileged EXEC prompt, issue the `copy running-config tftp` command. Follow the prompts:

```
Router1#copy running-config tftp:
Address or name of remote host []?<enter TFTP server IP address>
Destination filename [router1-confg]? <ENTER>
!!
667 bytes copied in 0.036 secs (18528 bytes/sec)
```

b. Verify a successful upload transfer. Check the TFTP server, and do the steps as shown in Figure 2.



TFTP

Service ● On ○ Off

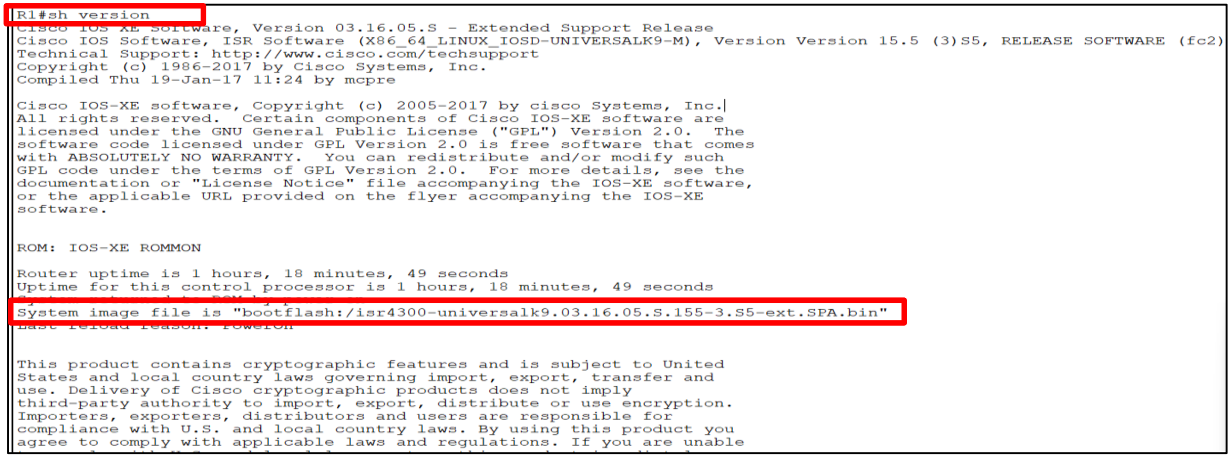
File
R1-confg
asa842-k8.bin
asa923-k8.bin
c1841-advipservicesk9-mz.124-15.T1.bin
c1841-ipbase-mz.123-14.T7.bin
c1841-ipbasek9-mz.124-12.bin
c1900-universalk9-mz.SPA.155-3.M4a.bin
c2600-advipservicesk9-mz.124-15.T1.bin
c2600-i-mz.122-28.bin
c2600-ipbasek9-mz.124-8.bin
c2800nm-advipservicesk9-mz.124-15.T1.bin
c2800nm-advipservicesk9-mz.151-4.M4.bin

Figure 2: Saving the configuration file in the TFTP server

c. You can save a back up of the startup-config file in the same way (`copy startup-config tftp`).

6. Using TFTP server to save IOS Images

a. Similar to uploading a configuration files, the IOS can also be stored off-line for future use. **To discover the IOS filename,** issue the Cisco IOS command `show version`. The filename is highlighted, below as shown in Figure 3 :



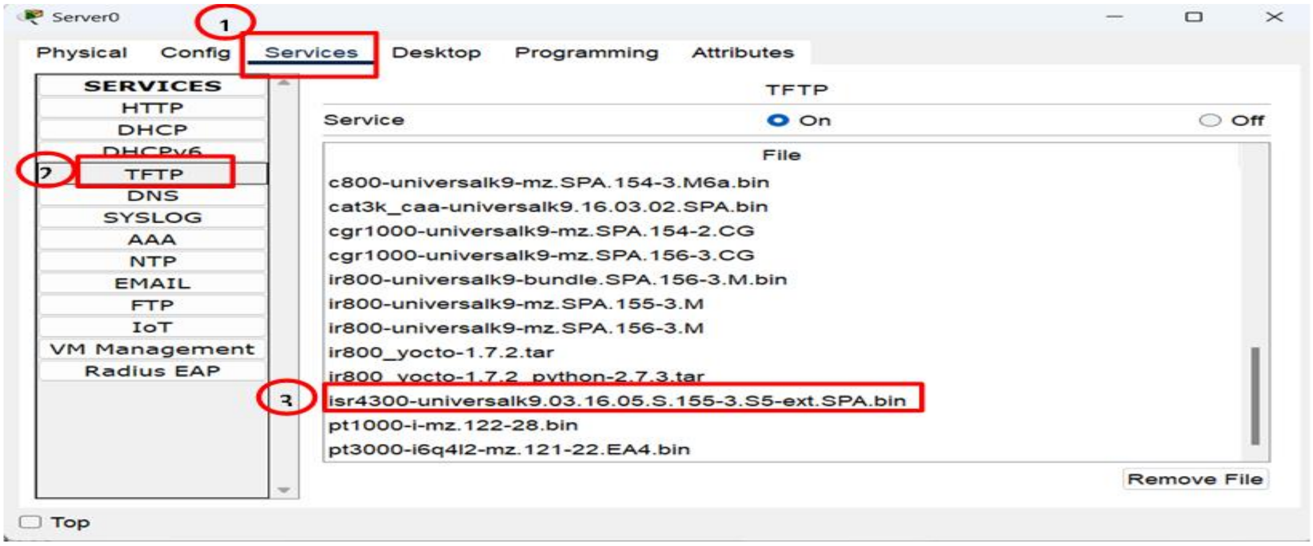
```
R1#sh version
Cisco IOS XE Software, Version 03.16.05.S - Extended Support Release
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version Version 15.5 (3)S5, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Thu 19-Jan-17 11:24 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2017 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
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.


ROM: IOS-XE ROMMON

Router uptime is 1 hours, 18 minutes, 49 seconds
Uptime for this control processor is 1 hours, 18 minutes, 49 seconds
System returned to ROM by power-on
System image file is "bootflash:/isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin"
Last reload reason: PowerOn


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
```

Figure 3: The name of the IOS image

b. Or enter `show flash` command to **view the IOS filename.** Highlight the filename and copy it, later when you are prompted to enter the flash file name use the mouse right click and select paste to host. The commands to upload the IOS are similar to uploading the configuration file:

```
Router1# copy flash tftp
Source filename []? isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin
Address or name of remote host []? <enter TFTP server IP address>
Destination filename [isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin]?<enter>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
22063220 bytes copied in 59.564 secs (370412 bytes/sec)
Router1#
```

c. Verify a successful upload transfer. Check the TFTP server, and do the steps as shown in Figure 4.



TFTP

Service ● On ○ Off

File
c800-universalk9-mz.SPA.154-3.M6a.bin
cat3k_caa-universalk9.16.03.02.SPA.bin
cgr1000-universalk9-mz.SPA.154-2.CG
cgr1000-universalk9-mz.SPA.156-3.CG
ir800-universalk9-bundle.SPA.156-3.M.bin
ir800-universalk9-mz.SPA.155-3.M
ir800-universalk9-mz.SPA.156-3.M
ir800_yocto-1.7.2.tar
ir800_yocto-1.7.2_python-2.7.3.tar
isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin
pt1000-i-mz.122-28.bin
pt3000-i6q4l2-mz.121-22.EA4.bin

Figure 4: Saving the IOS image in the TFTP server

7. Use TFTP to restore Configuration files and IOS Images

Assume that the configuration on the router **has become corrupt, then you must restore the files or the IOS image by** copying the backup startup or configuration files from the TFTP server to the running-config or startup-config of the router. To simulate this:

a. change the hostname of the router from "Router1" to "Router".

b. Issue the following command to copy the startup-config file from the TFTP server to the router.

```
Router#copy tftp running-config
Address or name of remote host []?<enter TFTP server IP address>
Source filename []? startup-config
Destination filename [running-config]? <Enter>
Accessing tftp://192.168.14.2/startup-config...
Loading startup-config from 192.168.14.2 (via FastEthernet0): !
[OK - 667 bytes]
667 bytes copied in 9.584 secs (70 bytes/sec)
Router1#
```

c. To restore the IOS image from the TFTP server, use the following command

```
Router1#copy tftp flash
Router#copy tftp: flash:
Address or name of remote host []? <enter TFTP server IP address>
Source filename []? isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin
Destination filename [isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin]?<Enter>
```

```
%Warning:There is a file already existing with this name
Do you want to over write? [confirm] <Enter>

Accessing tftp://192.168.1.2/isr4300-universalk9.03.16.05.S.155-3.S5-
ext.SPA.bin...
Loading isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin from 192.168.1.2:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 486899872 bytes]
486899872 bytes copied in 7.649 secs (205068 bytes/sec)
Router#
```

8. Saving the router's configuration files

Cisco IOS refers to RAM configuration storage as running-configuration, and NVRAM configuration storage as startup-configuration. For configurations to survive rebooting or power restarts, the RAM configuration must be copied into NVRAM. This does not occur automatically, NVRAM must be manually updated after any changes are made.

- ➢ **Compare router RAM and NVRAM configurations.**
- ✓ Display the contents of NVRAM using this command: `Router1# show startup-config`. If the output of NVRAM is missing, it is because there is no saved configuration, as shown below.

```
Router1# show startup-config
startup-config is not present
```

- ✓ Display the contents of RAM.

```
Router1#show running-config
<Display the content of this file>
```

- ➢ **Save RAM configuration to NVRAM.**
- ✓ For a configuration to be used the next time the router is powered on or reloaded, it must be manually saved in NVRAM. Save the RAM configuration to NVRAM:

```
Router1# copy running-config startup-config
Destination filename [startup-config]? <ENTER>
Building configuration...
[OK]
Router1#
```

- ➢ **To erase the NVRAM configuration file:**

```
Router1# erase startup-config
Erasing the nvram filesystem will remove all
configuration files! Continue? [confirm] <ENTER>
[OK]
Erase of nvram: complete
```

- ➢ **Reload the router:**

```
Router1# reload
Proceed with reload? [confirm] <ENTER>
```

Part II: Configuring IPv4 and IPv6 with routing protocols (Real devices):

A. Real Devices Configuration:

For real devices configuration, please consider the network topology shown in Figure 2.1.

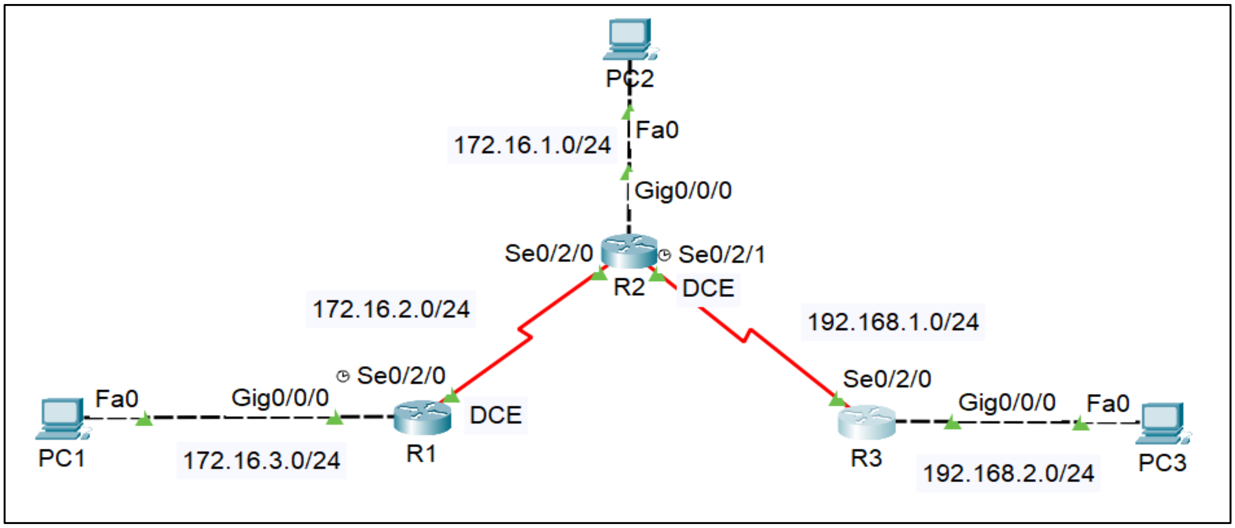


Fig 2.1 Network topology considered in the lab sheet

Steps to configure the router and routing protocols:

The following figure (i.e., Figure 2.2) shows the router interfaces.

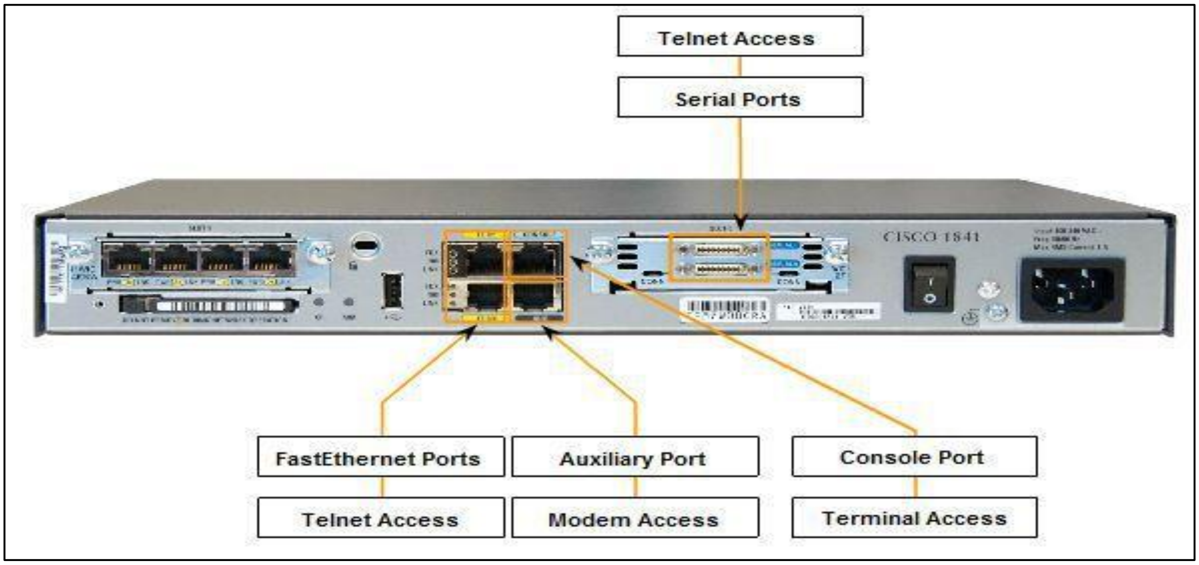


Fig 2.2. Router interfaces

1. **Cable the network topology** as shown in the lab sheet, and as shown in Figure 2.1, with:
    - UTP straight-through Ethernet cables between Ethernet interfaces of the (PCs and routers), as shown in Figure 2.3.

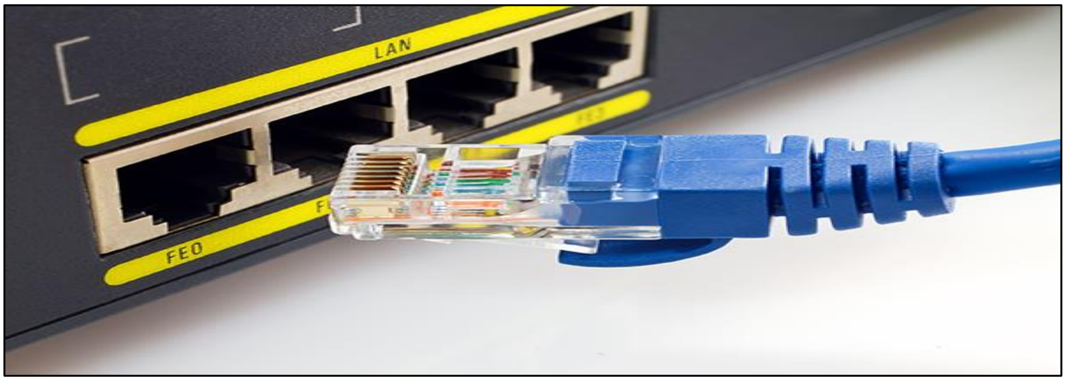


Fig 2.3. Ethernet cable between LAN router interfaces and PCs.

- Serial cables between the two routers, as shown in Figures 2.4 and 2.5.

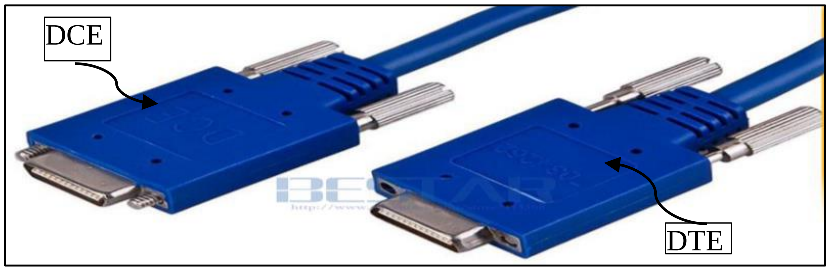


Fig 2.4. Serial cable between WAN router interfaces.

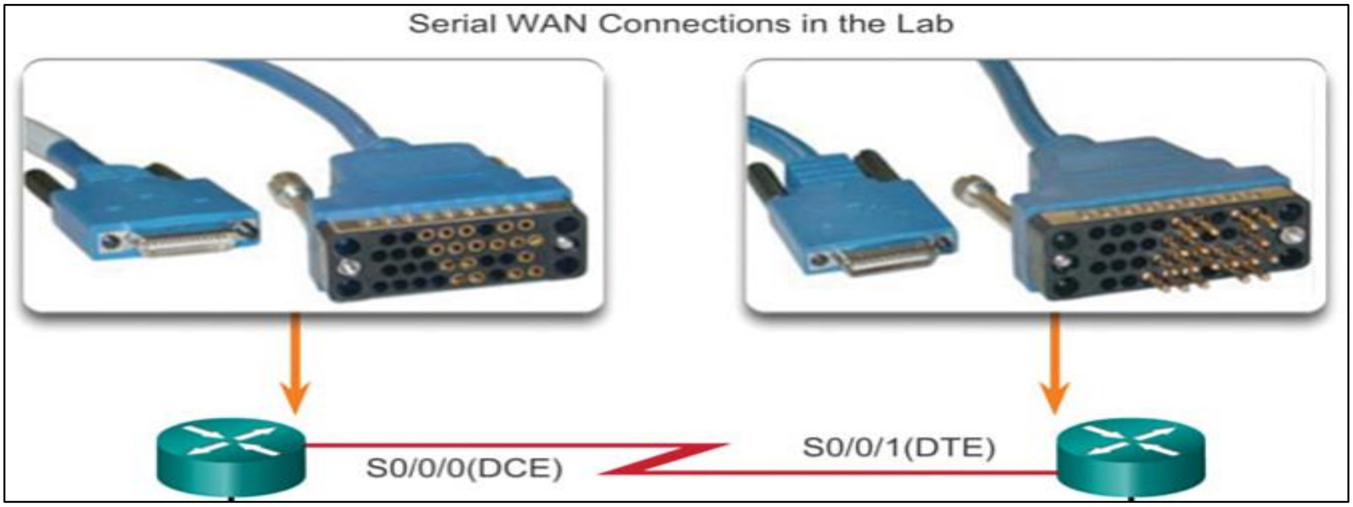


Fig 2.5. Serial cable's connection between WAN router interfaces.

- Console (rollover) cable for configuration between the COM ports of routers and PCs, as shown in Figure 2.6.

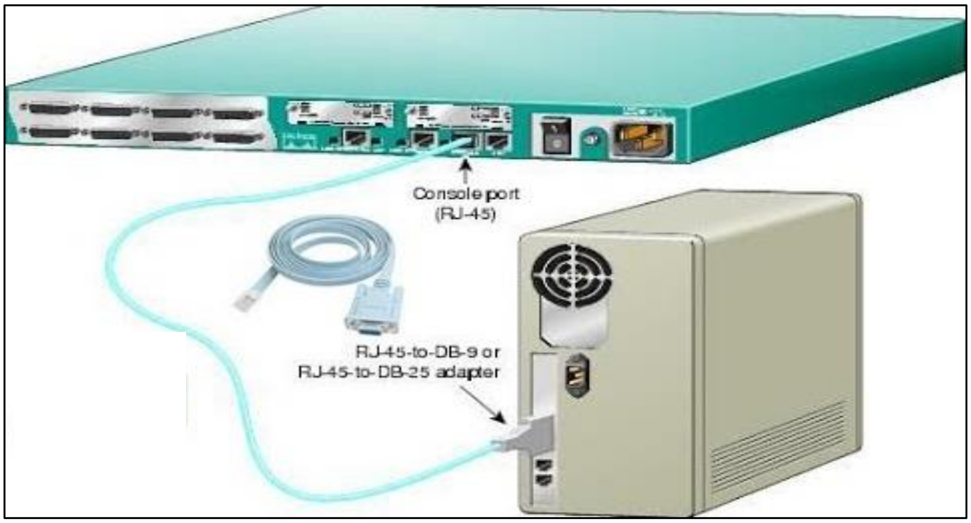


Fig 2. 6. Console cable’s connection between router interface and PC.

2. **Establish a Console Session using Putty**. Select appropriate serial port that your console cable is connected to (Device Manager →Ports (COM&LPT).

Step 1: Connect a Cisco router and computer using a rollover console cable.

- Connect the rollover console cable to the RJ-45 console port of the router, as shown in Figure 2.7.
- Connect the other cable end to the serial COM port on the computer.
- Turn on the Cisco router and computer by connecting the power cables.

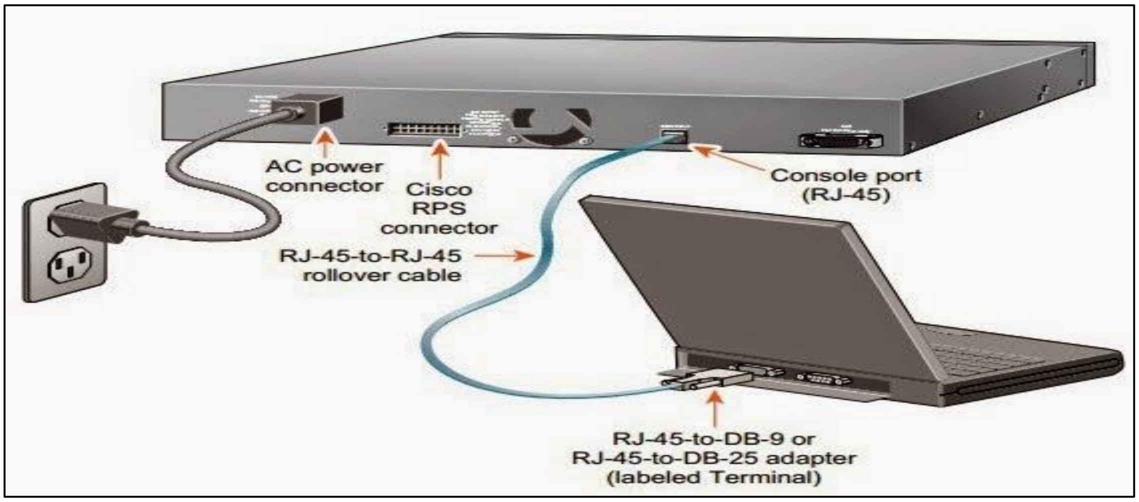


Fig 2.7. Rollover console cable connection.

Step 2: Configure Putty to establish a console session with the router.

- Determine the correct COM (serial) port being used to connect your PC to your router over the console cable, as as shown in Figure 2.8. Go to the computer icon, right click, proprties, device manger. Ports (COM & LPT).

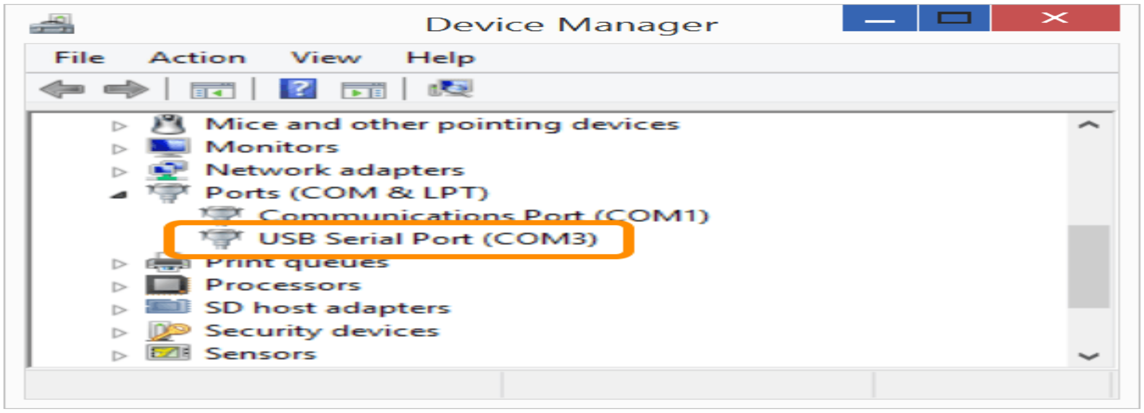
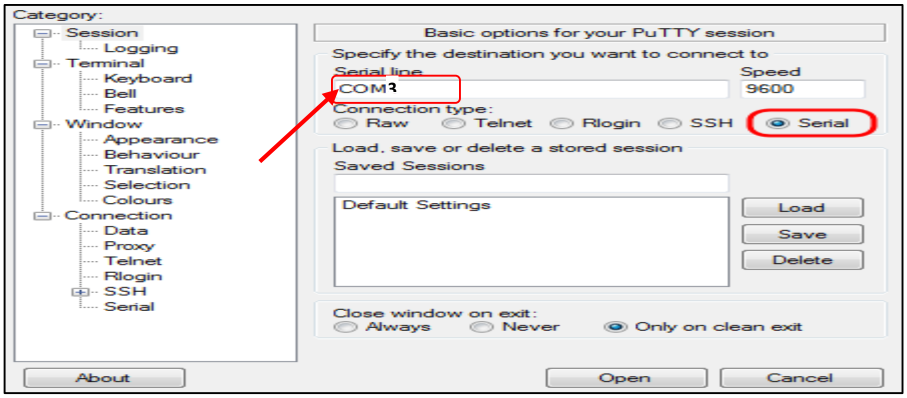


Fig 2.8. Selecting the appropriate COM prot.

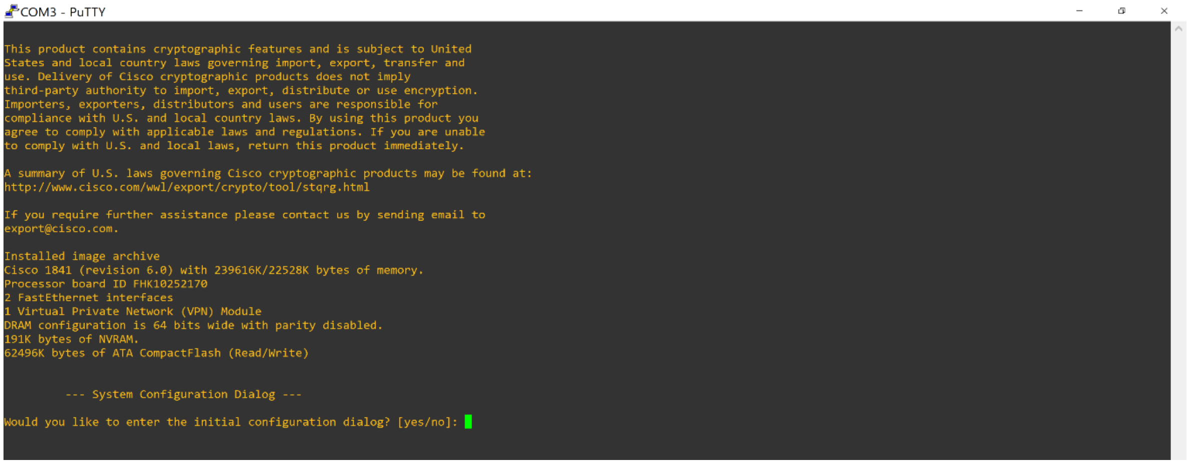
- Start Putty by clicking on its icon on desktop and click Open to continue, as shown in Figure 2.9.



Serial line: COM3
Speed: 9600
Connection type: ● Serial

Fig 2.9. Verify the correct COM port in Putty

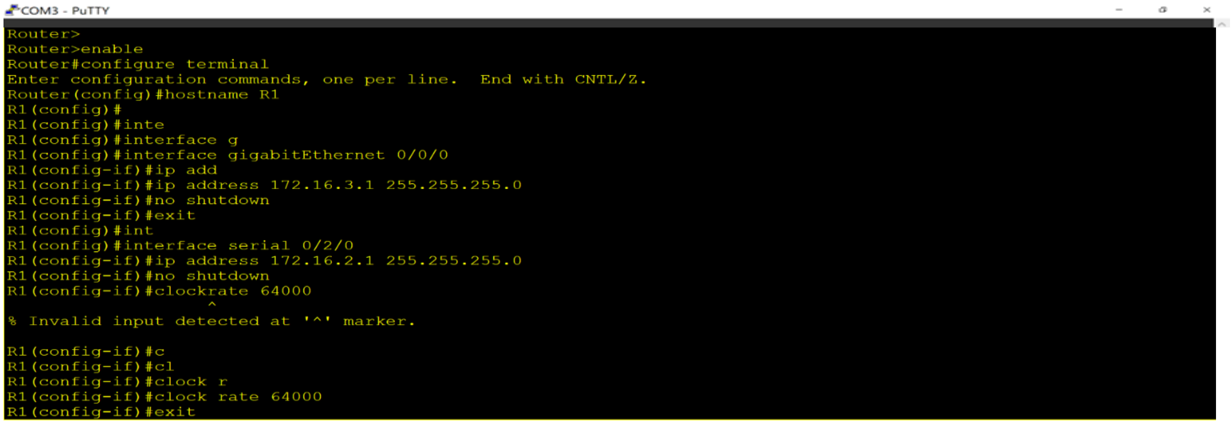
Step 3: You should see a response from the router on the screen (press enter several times). If you were asked "Continue with configuration dialog? [yes/no]: ", press no, as shown in Figure 2.10. Verify a clean configuration file with the privileged exec command `show running-config`. If a configuration file was previously saved, it will have to be removed.



```
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.

Installed image archive
Cisco 1841 (revision 6.0) with 239616K/22528K bytes of memory.
Processor board ID FHK10252170
2 FastEthernet interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
62496K bytes of ATA CompactFlash (Read/Write)


         --- System Configuration Dialog ---

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

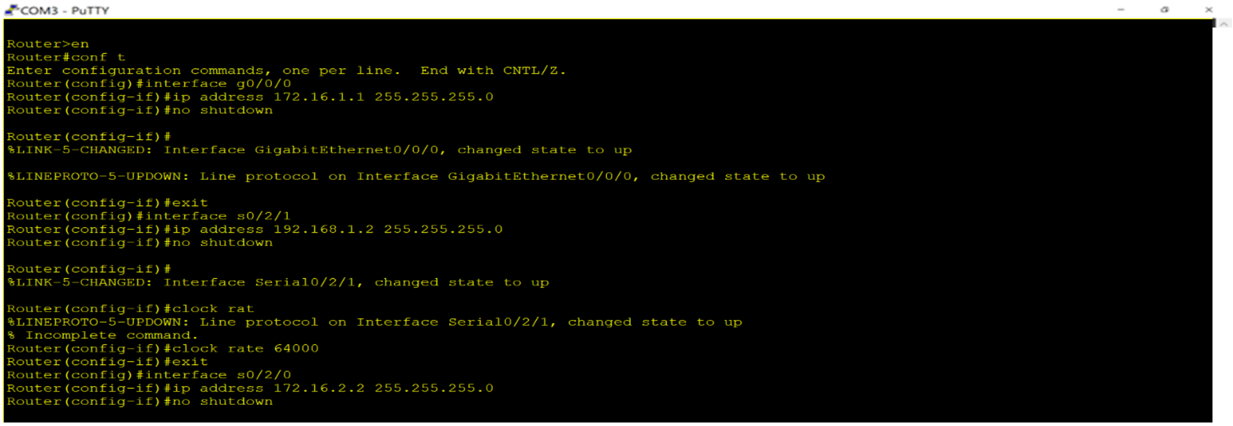
Fig 2.10. Router screen in putty.

3. **Configuring the routers' interfaces:** From the user exec mode, enter privileged exec mode, as shown in Figures 2.11, 2.12, and 2.13, configure the routers interfaces (R1, R2, and R3) with the correct ip address as shown the addressing table in the lab sheet.



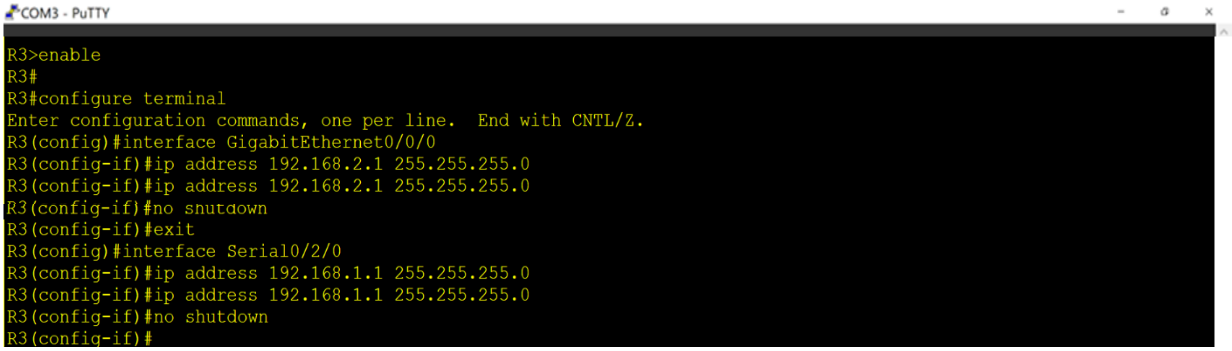
```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
R1(config)#inte
R1(config)#interface g
R1(config)#interface gigabitEthernet 0/0/0
R1(config-if)#ip add
R1(config-if)#ip address 172.16.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#int
R1(config)#interface serial 0/2/0
R1(config-if)#ip address 172.16.2.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#clockrate 64000
                   ^
% Invalid input detected at '^' marker.

R1(config-if)#c
R1(config-if)#cl
R1(config-if)#clock r
R1(config-if)#clock rate 64000
R1(config-if)#exit
```

Fig 2.11. Configuring IP addresses of R1 interfaces.



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface g0/0/0
Router(config-if)#ip address 172.16.1.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

Router(config-if)#exit
Router(config)#interface s0/2/1
Router(config-if)#ip address 192.168.1.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/1, changed state to up

Router(config-if)#clock rat
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed state to up
% Incomplete command.
Router(config-if)#clock rate 64000
Router(config-if)#exit
Router(config)#interface s0/2/0
Router(config-if)#ip address 172.16.2.2 255.255.255.0
Router(config-if)#no shutdown
```

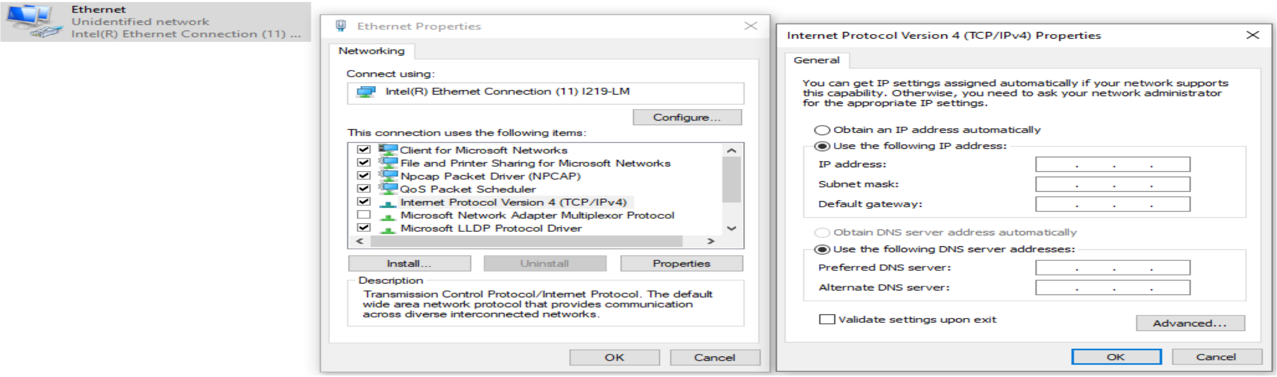
Fig 2.12. Configuring IP addresses of R2 interfaces.



```
R3>enable
R3#
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface GigabitEthernet0/0/0
R3(config-if)#ip address 192.168.2.1 255.255.255.0
R3(config-if)#ip address 192.168.2.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface Serial0/2/0
R3(config-if)#ip address 192.168.1.1 255.255.255.0
R3(config-if)#ip address 192.168.1.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#
```

Fig 2.13. Configuring IP addresses of R3 interfaces.

4. **Configure the host computer IP address**: (Control Panel→Network and Internet→Network and Sharing Center→Change Adapter settings→Right-click on the Local Area Connection icon, and select Properties→Highlight the Internet Protocol (TCP/IPv4) field, and select Properties). Configure IP address, subnet mask, and default gateway, and then Highlight the Internet Protocol (TCP/IPv6) field, and select Properties). Configure IPv6 address, prefix length, and default gateway as shown in Figures 2.14 – 2.18. Open a command prompt from start search for **cmd** and verify network settings with the **ipconfig** command.



Ethernet
Unidentified network
Intel(R) Ethernet Connection (11) ...

Ethernet Properties

Networking

Connect using:
Intel(R) Ethernet Connection (11) I219-LM

Configure...

This connection uses the following items:
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Npcap Packet Driver (NPCAP)
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Install... Uninstall Properties

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

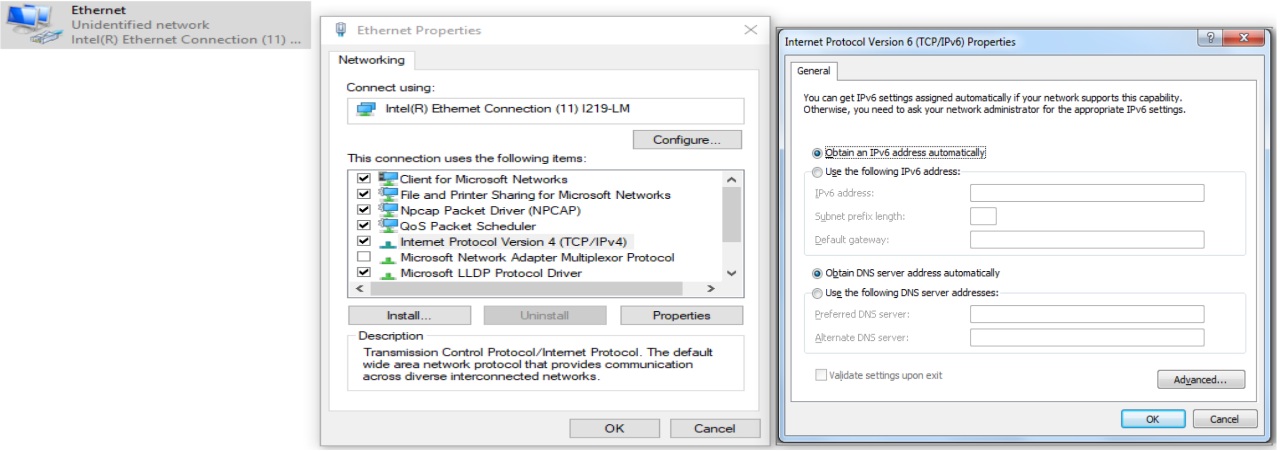
○ Obtain an IP address automatically
● Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

☐ Validate settings upon exit Advanced...

OK Cancel

Fig 2.14. Configure static IPv4 address for PCs.



Ethernet
Unidentified network
Intel(R) Ethernet Connection (11) ...

Ethernet Properties

Networking

Connect using:
Intel(R) Ethernet Connection (11) I219-LM

Configure...

This connection uses the following items:
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Npcap Packet Driver (NPCAP)
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Install... Uninstall Properties

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

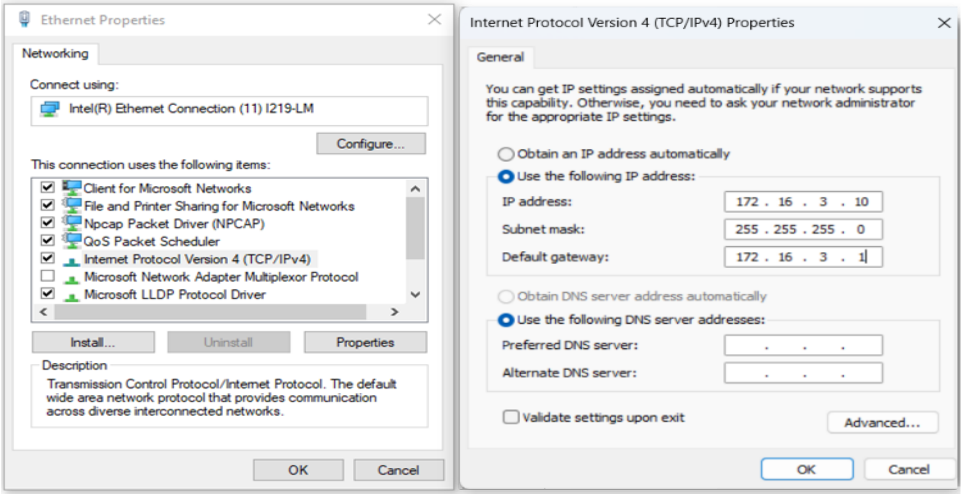
● Obtain an IPv6 address automatically
○ Use the following IPv6 address:
IPv6 address:
Subnet prefix length:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

☐ Validate settings upon exit Advanced...

OK Cancel

Fig 2.15. Configure static IPv6 address for PCs.



Ethernet Properties

Networking

Connect using:
Intel(R) Ethernet Connection (11) I219-LM

Configure...

This connection uses the following items:
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Npcap Packet Driver (NPCAP)
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Install... Uninstall Properties

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

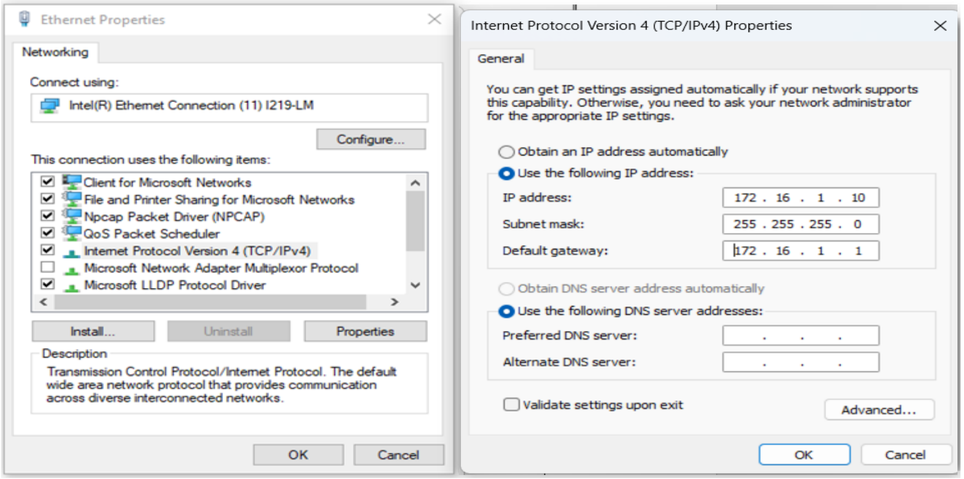
○ Obtain an IP address automatically
● Use the following IP address:
IP address: 172 . 16 . 3 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 172 . 16 . 3 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

☐ Validate settings upon exit Advanced...

OK Cancel

Fig 2.16. Configure static IPv4 address for PC1.



Connect using: Intel(R) Ethernet Connection (11) I219-LM

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Npcap Packet Driver (NPCAP)
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Description: Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

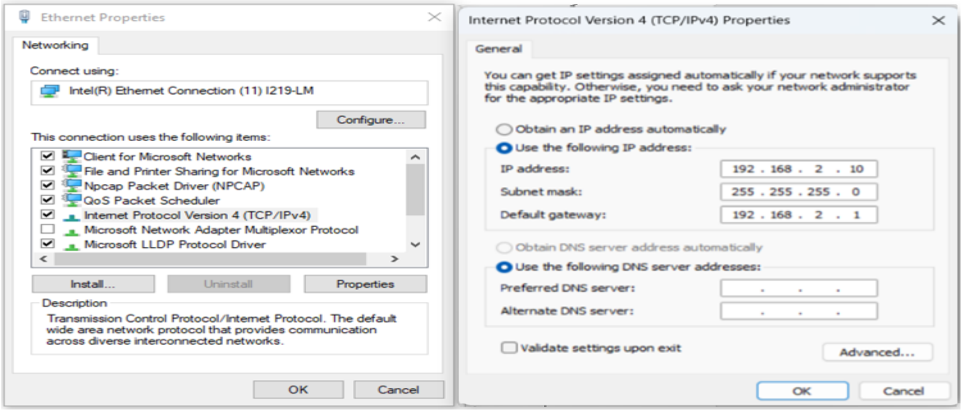
IP address: 172 . 16 . 1 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 172 . 16 . 1 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

☐ Validate settings upon exit

Fig 2.17. Configure static IPv4 address for PC2.



Connect using: Intel(R) Ethernet Connection (11) I219-LM

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Npcap Packet Driver (NPCAP)
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Description: Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 2 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 2 . 1

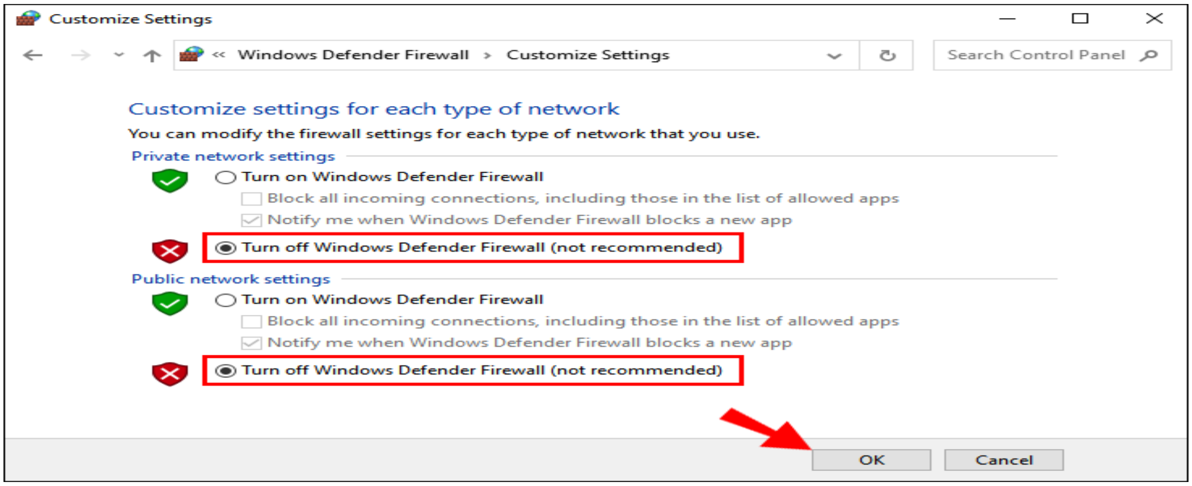
○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

☐ Validate settings upon exit

Fig 2.18. Configure static IPv4 address for PC3.

5. **Test connectivity between end devices and their gateways** and then the directly connected network in the routing table (make sure the firewall is turned off, as shown in Figure 2.19).



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Defender Firewall
☐ Block all incoming connections, including those in the list of allowed apps
☑ Notify me when Windows Defender Firewall blocks a new app
● Turn off Windows Defender Firewall (not recommended)

Public network settings

○ Turn on Windows Defender Firewall
☐ Block all incoming connections, including those in the list of allowed apps
☑ Notify me when Windows Defender Firewall blocks a new app
● Turn off Windows Defender Firewall (not recommended)

Fig 2.19. Turn off firewall in windows.

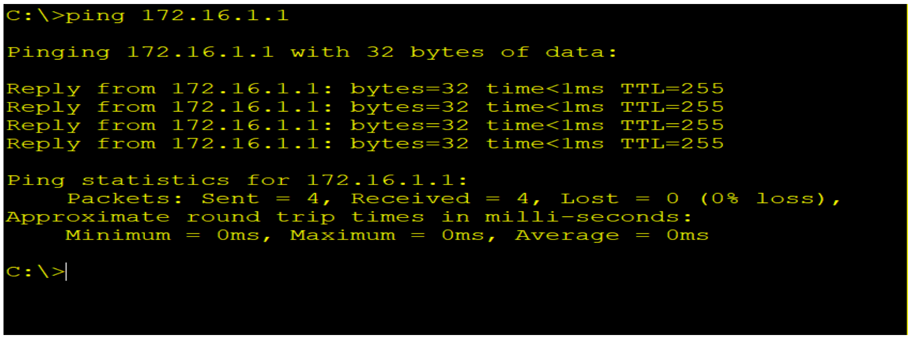
Use the **ping** command to verify network connectivity with the router. From the router hyperterminal session issue the following command.

```
Router1(config)# ping <enter the host PC IP address>.
```

And from the command prompt window on the host computer, issue the following command.

```
C:\Users\hp> ping <enter Router's g0/0 IP Address >
```

Figure 2.20 presents the successful ping of the default gateway from PC2.



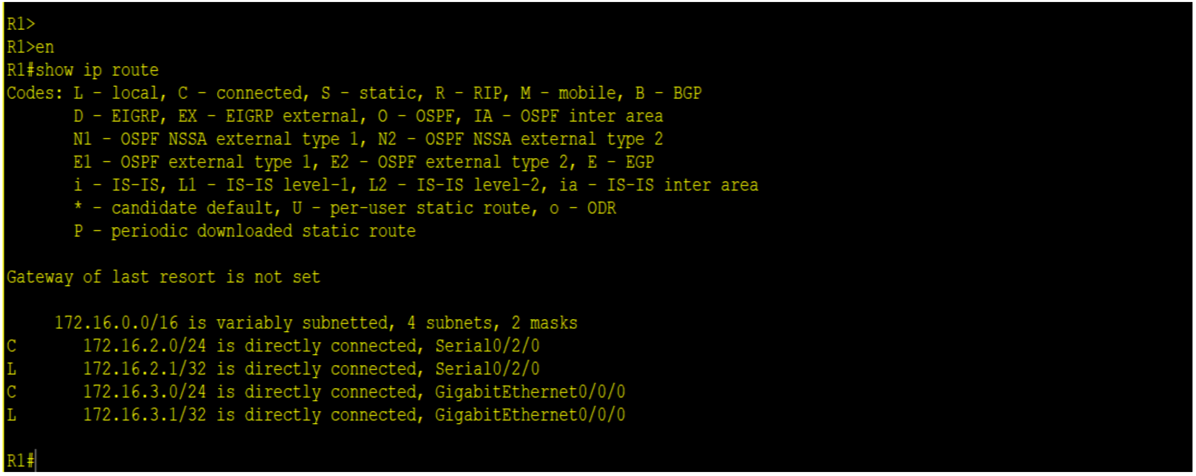
```
C:\>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Reply from 172.16.1.1: bytes=32 time<1ms TTL=255
Reply from 172.16.1.1: bytes=32 time<1ms TTL=255
Reply from 172.16.1.1: bytes=32 time<1ms TTL=255
Reply from 172.16.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fig 2. 20. ping the default gateway from PC2

If ping replies are not successful troubleshoot the connection:

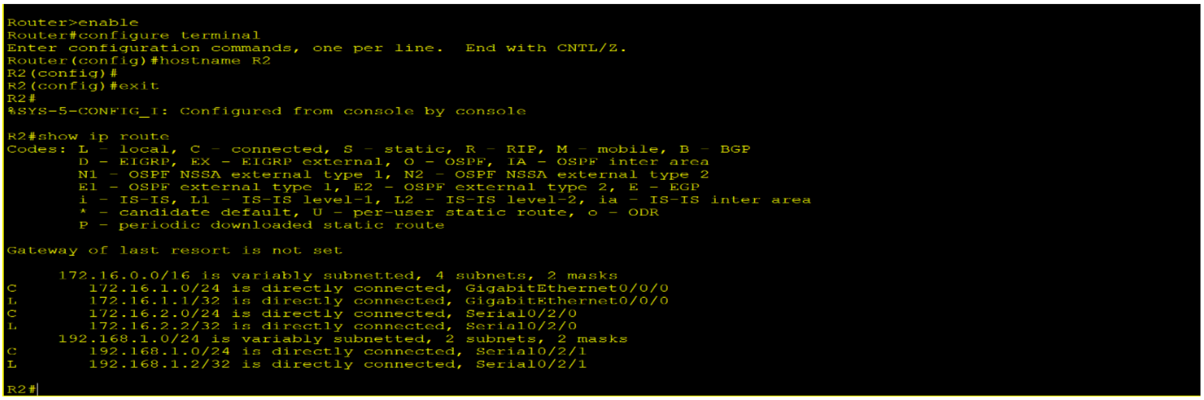
- Verify the Router`s interface status using the command: `Router1# show ip interface brief` The up in the Status column shows that this interface is operational at Layer 1. The up in the Protocol column indicates that the Layer 2 protocol is operational. If you find administratively down in the Status column, then this interface was not enabled with the no shutdown command.
- Verify host computer configuration with the **ipconfig** command.
- Verify the cable connection between the router Ethernet interface and the host computer. Ethernet card is crossover cable.

6. **View the routing table on each router before adding any routing protocols** to verify how the routing table will be changed. Figures 2.21 -2.23 demonstrates the routing tables of the R1, R2, and R3 respectively before adding the static routes.



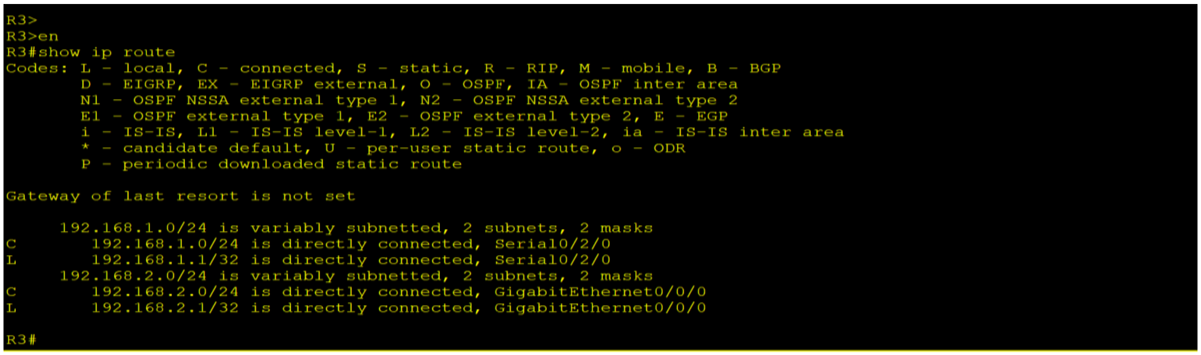
```
R1>
R1>en
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.2.0/24 is directly connected, Serial0/2/0
L       172.16.2.1/32 is directly connected, Serial0/2/0
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.3.1/32 is directly connected, GigabitEthernet0/0/0

R1#
```

Fig 2.21.   The routing table of R1 before configuring static routes.



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.1.1/32 is directly connected, GigabitEthernet0/0/0
C       172.16.2.0/24 is directly connected, Serial0/2/0
L       172.16.2.2/32 is directly connected, Serial0/2/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Serial0/2/1
L       192.168.1.2/32 is directly connected, Serial0/2/1

R2#
```

Fig 2.22. The routing table of R2 before configuring static routes.



```
R3>
R3>en
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Serial0/2/0
L       192.168.1.1/32 is directly connected, Serial0/2/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0/0

R3#
```

Fig 2. 23. The routing table of R3 before configuring static routes.

Important Note: Some parts of this handout have been collected from several trustable sites, books, and published slides and the other parts have been prepared and written by the instructors. As a matter of fact, this handout is made to be so straight forward, understandable, and so attractive whereas the students can do the required activities and solve the problems in a systematic and easy way, but still the instructors are expected to discuss some important material during the labs' sessions.