

Institute of Computer Technology

B. Tech Computer Science and Engineering

Sub: Computer Networks

Course Code:-2CSE502

Sem-V(CS)

Class:-A

Practical:5

Aim:

To configure and utilize Telnet (teletype network), SSH (Secure Socket Shell) and FTP (File Transfer Protocol) in a network.

Scenario:

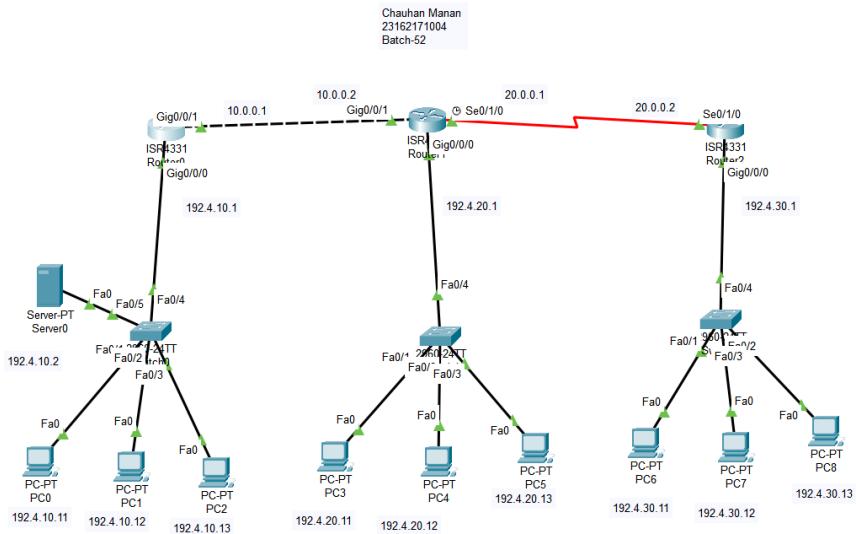
Design the network of an organization having 3 different departments. Make sure the below mentioned requirements must be fulfilled.

- 1) Create 3 users which will be able to get the access of the router using Telnet.
- 2) Create a single password to get the access of the router using Telnet. Configure in such a way at a time 2 users can access router at a time.
- 3) Create 3 users which will be able to get the access of the router using SSH. Configure in such a way at a time 2 users can access router at a time.

4) Create FTP server and perform the operation to upload and download a file from one department to other department.

Procedure:

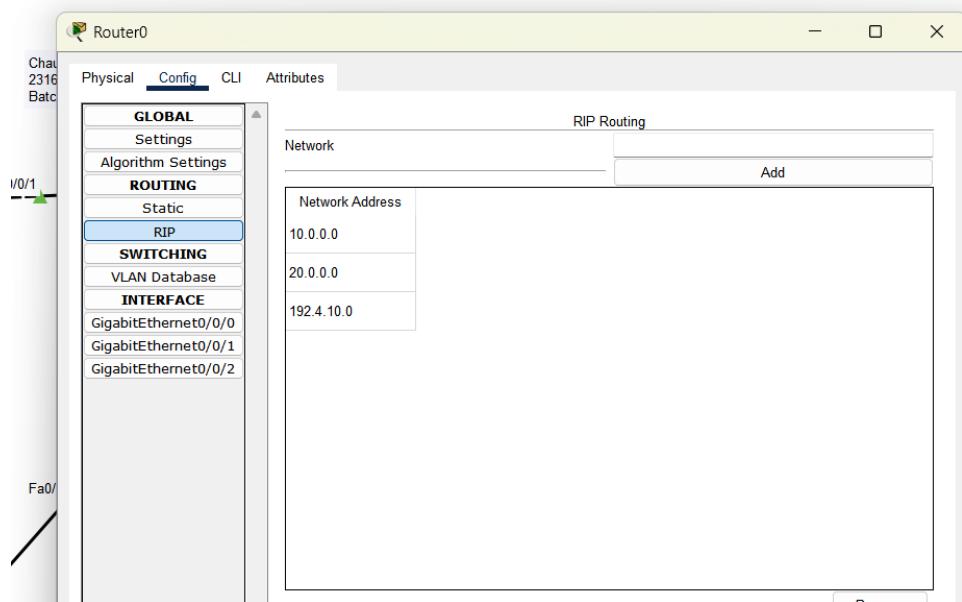
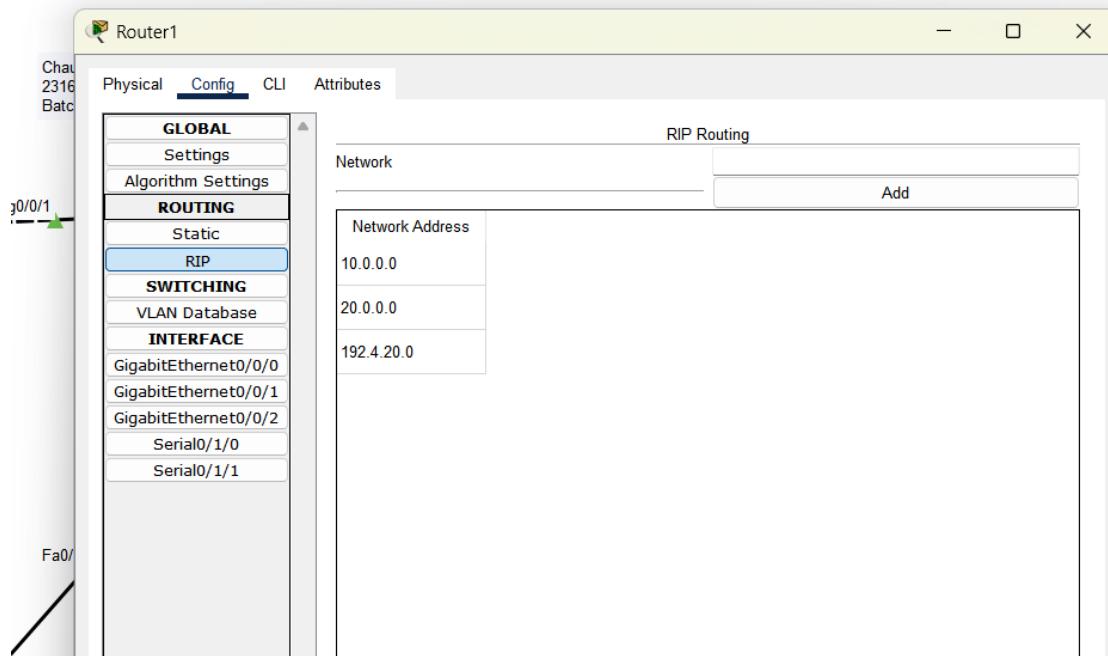
1) Create network as given below:

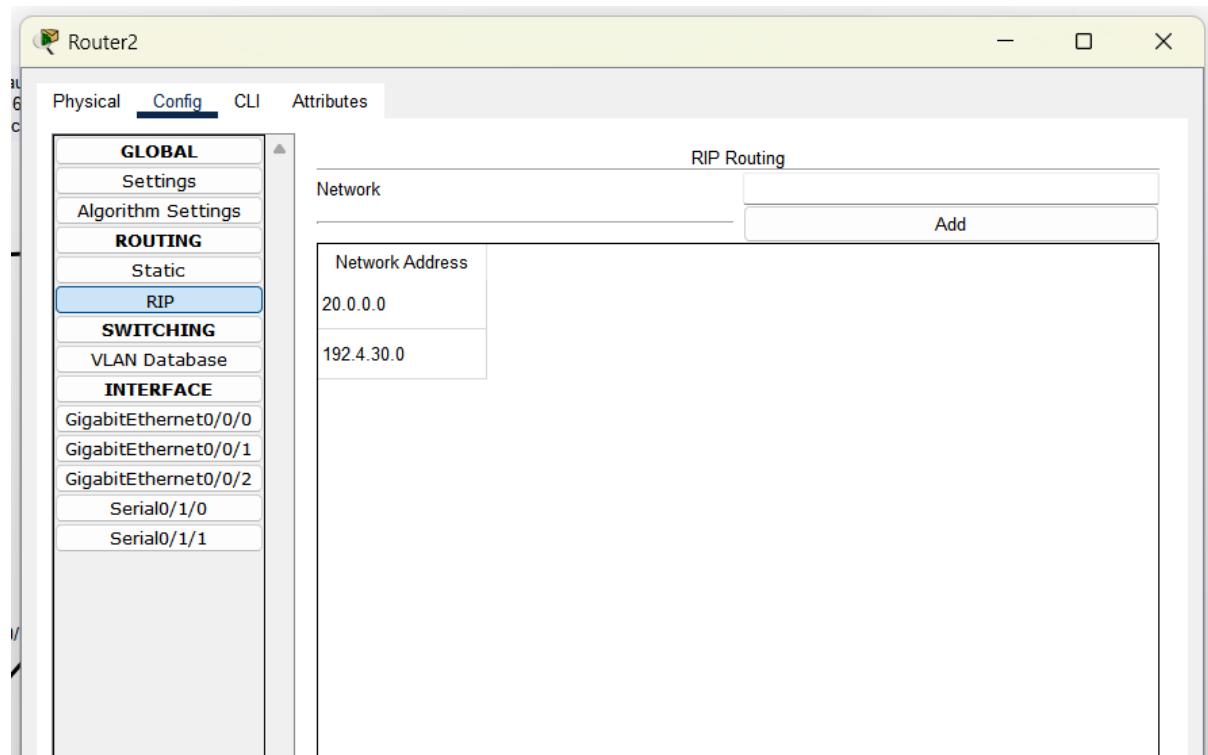


IP Address of devices(PC, Router and Server)

Department	Device / Router Interface	IP Address	Subnet Mask	Default Gateway
Dept. 1	Server (Fa0)	192.4.10.2	255.255.255.0	192.4.10.1
	PC0	192.4.10.11	255.255.255.0	192.4.10.1
	PC1	192.4.10.12	255.255.255.0	192.4.10.1
	PC2	192.4.10.13	255.255.255.0	192.4.10.1
	Router0 G0/0/0 (LAN)	192.4.10.1	255.255.255.0	—
	Router0 G0/0/1 (WAN)	10.0.0.1	255.0.0.0	—
Dept. 2	PC3	192.4.20.11	255.255.255.0	192.4.20.1
	PC4	192.4.20.12	255.255.255.0	192.4.20.1
	PC5	192.4.20.13	255.255.255.0	192.4.20.1
	Router1 G0/0/0 (LAN)	192.4.20.1	255.255.255.0	—
	Router1 G0/0/1 (WAN)	10.0.0.2	255.0.0.0	—
	Router1 S0/1/0 (WAN)	20.0.0.1	255.0.0.0	—
Dept. 3	PC6	192.4.30.11	255.255.255.0	192.4.30.1
	PC7	192.4.30.12	255.255.255.0	192.4.30.1
	PC8	192.4.30.13	255.255.255.0	192.4.30.1
	Router2 G0/0/0 (LAN)	192.4.30.1	255.255.255.0	—
	Router2 S0/1/0 (WAN)	20.0.0.2	255.0.0.0	—

3) Configure dynamic routing table (RIP in routers):





4) Configure TELNET on Router0:

The image shows two windows from Cisco Packet Tracer. The top window, titled 'Router0', displays the IOS Command Line Interface. The bottom window, titled 'PC4', displays the Command Prompt interface.

Router0 (IOS Command Line Interface):

```
Router#  
Router#  
Router#  
Router#  
Router#  
Router#  
Router#  
Router#  
Router#  
Router#enable sec secl  
^  
% Invalid input detected at '^' marker.  
  
Router#enable secret secl  
^  
% Invalid input detected at '^' marker.  
  
Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#enable secret secl  
The enable secret you have chosen is the same as your enable password.  
This is not recommended. Re-enter the enable secret.  
Router(config)#enable secret sec  
Router(config)#username usr1 password psw1  
Router(config)#username usr2 password psw2  
Router(config)#username usr3 password psw3  
Router(config)#line vty 0 1  
Router(config-line)#password secl  
Router(config-line)#login local  
Router(config-line)#transport input telnet  
Router(config-line)#exit
```

PC4 (Command Prompt):

```
Cisco Packet Tracer PC Command Line 1.0  
C:\>telnet 192.4.10.1  
Trying 192.4.10.1 ...Open  
  
User Access Verification  
  
Username: usr1  
Password:  
Router>en  
Password:  
Password:  
Router#do show user  
^  
% Invalid input detected at '^' marker.  
  
Router#show user  
Line User Host(s) Idle Location  
0 con 0 idle 00:01:03  
* 4 vty 0 usr1 idle 00:00:00 192.4.20.12  
  
Interface User Mode Idle Peer Address  
Router#
```

5) Configure SSH on Router1

```
R1>
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname Man
Man(config)#enable secret man
Man(config)#ip domain name ma
Man(config)#crypto key generate rsa
% You already have RSA keys defined named R1.man .
% Do you really want to replace them? [yes/no]: y
The name for the keys will be: Man.ma
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Man(config)#ip ssh version 2
*Mar 1 3:37:51.912: %SSH-5-ENABLED: SSH 2 has been enabled
Man(config)#line vty 0 1
Man(config-line)#transport input ssh
Man(config-line)#login local
Man(config-line)#exit
Man(config)#
```

Conv Past

```
C:\>
C:\>ssh -l usrl 192.4.20.1

Password:

Man>en
Password:
Man#
```

6) Configure FTP on Server

The screenshot shows the 'Server0' configuration interface with the 'Services' tab selected. On the left sidebar, under the 'SERVICES' section, the 'FTP' option is highlighted. The main panel displays the 'FTP' configuration. The 'Service' status is set to 'On'. In the 'User Setup' section, a user named 'man-ftp' is configured with password '123'. Under the 'Permission' column, the user has 'RWDNL' permissions. Below this, a file list titled 'File' shows four entries: 'asa842-k8.bin', 'asa923-k8.bin', 'c1841-advipservicesk9-mz.124-15.T1.bin', and 'c1841-ipbase-mz.123-14.T7.bin'.

Username	Password	Permission
1 man-ftp	123	RWDNL

PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.4.10.2
Trying to connect...192.4.10.2
Connected to 192.4.10.2
220- Welcome to PT Ftp server
Username:man-ftp
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put man.txt

Writing file man.txt to 192.4.10.2:
File transfer in progress...

[Transfer complete - 12 bytes]

12 bytes copied in 0.079 secs (151 bytes/sec)
ftp>dir

Listing /ftp directory from 192.4.10.2:
 0 : asa842-k8.bin          5571584
 1 : asa923-k8.bin          30468096
 2 : cl841-advpipservicesk9-mz.124-15.T1.bin 33591768
 3 : cl841-ipbase-mz.123-14.T7.bin   13832032
 4 : cl841-ipbasek9-mz.124-12.bin  16599160
 5 : cl900-universalk9-mz.SPA.155-3.M4a.bin 33591768
 6 : c2600-advpipservicesk9-mz.124-15.T1.bin 33591768
 7 : c2600-i-mz.122-28.bin    5571584
 8 : c2600-ipbasek9-mz.124-8.bin 13169700
 9 : c2800nm-advpipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advpipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin   5571584
12 : c2800nm-ipbasek9-mz.124-8.bin  15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin  3058048
15 : c2950-i6q412-mz.121-22.EA8.bin 3117390
16 : c2960-lanbase-mz.122-25.FX.bin  4414921
17 : c2960-lanbase-mz.122-25.SE1.bin 4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
19 : c3560-advpipservicesk9-mz.122-37.SE1.bin 8662192
20 : c3560-advpipservicesk9-mz.122-46.SE.bin 10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin 33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin 83029236
23 : cat3k_caa-universalk9.16.03.02.SPA.bin 505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG 159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG 184530138
26 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
27 : ir800-universalk9-mz.SPA.155-3.M    61750062
28 : ir800-universalk9-mz.SPA.156-3.M    63753767
29 : ir800_yocto-1.7.2.tar    2877440
30 : ir800_yocto-1.7.2_python-2.7.3.tar 6912000
31 : man.txt                  12
32 : pt1000-i-mz.122-28.bin  5571584
33 : pt3000-i6q412-mz.121-22.EA4.bin 3117390
ftp>
```

Top

```

PC7
Physical Config Desktop Programming Attributes
Composed Prompt X

Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.4.10.2
Trying to connect...192.4.10.2
Connected to 192.4.10.2.
220- Welcome to rf ftp server
Username:man
331- Username ok, need password
Password:
230- Logged in
(pasive mode On)
ftp>get man.txt
Reading file man.txt from 192.4.10.2:
File transfer in progress...
[Transfer complete - 12 bytes]
12 bytes copied in 0.016 secs (857 bytes/sec)
ftp>dir
Listing /tmp directory from 192.4.10.2:
0 : asa923-k8.bin
1 : ASA923-K8.bin
2 : C1841-advisorieservicesk9-mz.124-15.T1.bin
3 : C1841-advisorieservicesk9-mz.124-15.T1.bin
4 : C1841-ipbasek9-mz.124-12.bin
5 : C1900-universalk9-mz.SPA.155-3-M.a.bin
6 : C2400-advisorieservicesk9-mz.124-15.T1.bin
7 : C2400-advisorieservicesk9-mz.124-15.T1.bin
8 : C2400-ipbasek9-mz.124-8.bin
9 : C2500nm-advisorieservicesk9-mz.124-15.T1.bin
10 : C2500nm-advisorieservicesk9-mz.124-15.T1.bin
11 : C2500nm-ipbasek9-mz.124-8.bin
12 : C2500nm-ipbasek9-mz.124-8.bin
13 : C2900-universalk9-mz.SPA.155-3-M.a.bin
14 : C2900-universalk9-mz.124-15.T1.bin
15 : C2950-16q12-ms.121-22.EA8.bin
3117390
16 : C2960-lanbase-ms.122-25.FX.bin
4114921
17 : C2960-lanbase-ms.122-25.FX.bin
4114921
18 : C2960-lanbasek9-ms.150-2-EA4.bin
4670453
19 : C3560-advisorieservicesk9-ms.122-37.SE1.bin
8662192
20 : C3560-advisorieservicesk9-ms.122-46.SE.bin
10713279
21 : C3560-advisorieservicesk9-ms.122-46.SE.bin
3117390
22 : C800-universalk9-ms.SPA.155-3-M6a.bin
83029236
23 : cae3k_cae-universalk9_1.03.02.SPA.bin
505532849
24 : cpe1000-universalk9-mz.SPA.154-2-100
159978752
25 : cpe1000-universalk9-mz.SPA.154-2-100.CG
154517138
26 : i2800-universalk9-dumble-mz.SPA.155-3.M.bin
610968869
27 : i2800-universalk9-mz.SPA.155-3.M
61750062
28 : i2800-universalk9-mz.SPA.156-3.M
6373777
29 : i2800_yocto-1.7.2.yar
2877440
30 : i2800_yocto-1.7.2_python-2.7.3.tar
6912000
31 : i2800.yar
1
32 : pt2900-16q12-ms.122-28.bin
5571584
33 : pt2900-16q12-ms.121-22.EA8.bin
3117390
ftp>

```

Conclusion:

In this practical, we successfully configured and verified Telnet, SSH, and FTP services in a network with three departments.

- Telnet was implemented with three users and a common password, allowing a maximum of two simultaneous sessions.
- SSH was configured with three secure users, ensuring encrypted remote access with a limit of two concurrent sessions.
- FTP server was set up in Dept. 1, and file upload/download between different departments was tested successfully.

Thus, the organization's network was able to achieve remote router access (Telnet & SSH) and secure file sharing (FTP) while meeting all given requirements.