ELEC472

Advanced Telecommunication Networks

Lab Manual

Document No. ECE-L002-002

Revision Date: 2020.03.27

Department of Electrical and Computer Engineering
Concordia University

S-EV005.139
1455 de Maisonneuve Blvd. West
Montreal, Quebec, H4G 1M8 Canada
Web Site: www. ece.concordia.com/~netlab

Table of Contents

Contents

List of Figures

List of Tables

LAB RULES

LABORATORY RULES

Considering the large number of students attending the labs and in order for the lab to operate properly, students are asked to abide the following rules:

1. No eating or drinking is permitted in the laboratory.
2. Overcoats and briefcases are not permitted in the laboratory.
3. Students should bring their own lab manuals.
4. Students are not allowed to do any kind of physical modifications in network lab. Ex. Connecting or disconnecting cables, inserting or removing modules, etc.
5. Students should not install applications or copy files on lab computers.
6. All damaged or malfunctioning equipment and cables must be reported immediately to the demonstrator.
7. All required data or diagrams must be captured and saved on to the student's Home Directories. This information should be presented to the demonstrator and they will not be backed up or preserved after the end of the corresponding lab session.
8. No more than three students are allowed to occupy one laboratory workstation.
9. After your laboratory session is completed, no file or data should remain on computers. Close you router sessions and log off the computers.
10. Work groups are identified in the beginning of each lab experiment. Students should follow the group activity guidelines. Each group is responsible for the observations or results which are mentioned in the experiments.
11. Students should not turn on or off the routers or computers. All equipment should be continuously "on" during the lab session. To reset a router or modify a command, you should contact the demonstrator.
12. No command should be entered on routers other than what are specified in experiments. It is especially prohibited to erase the flash memory of routers or router configurations.
13. If it is needed to save the router configuration for further use, it should be done in the student's Home Directory.
14. Each lab experiment should be finished in its corresponding session. It is not possible to return to the lab after the session is done.
15. Tables must be left clean at the end of each lab session.

ORGANIZATION OF THE MANUAL

This manual contains five experiments; each experiment consists of the following sections:

- Objective
- Setup
- Tasks and multiple steps within each task
- Completions criteria

The first part gives the objective of the experiment. The second part provides the required preparations before starting the experiment. The third part consists of multiple tasks and each task includes steps which should be followed as specified. Completion criteria specify the activities that should have been done before finishing a lab session.

Some “paper labs” are included in this manual. They are not mandatory work in lab teaching, just designed for you to understand some concepts before you start incoming experiments.

You can find a useful introduction to Cisco IOS that includes general information about configuring a Cisco Router as Appendix A. You can also find a complete description of commands used in lab experiments on lab computers or Cisco web site: www.cisco.com

EXPERIMENT EXECUTION

Each experiment should be studied in advance and the introduction and related materials must be reviewed before conducting the experiment. Each task should be completed by all groups before proceeding to the next task. Steps within each task must be executed in the order specified but no coordination is required between groups. All of the required diagrams should be captured and copied to be presented in the report. Questions introduced in each task should be answered later in the report. These questions are based on lab observations and theoretical material. Marks will be assigned to group members according to their participation during the performance of the experiments and based on their reports. It is important to show the demonstrator that you are working with the group and understand the operation of all modules.

No physical modifications are required and routers should be ‘on’ during the whole session. All the required commands to conduct an experiment are provided and there is no need to use any other configuration commands without the approval of lab demonstrator. “show” or “debug” commands can be used by students at any time required. Use of “erase” commands are forbidden.

LAB REPORT

Each lab report should be divided into five parts as follows:

Cover page: Student name and ID

Objectives: They have to be stated clearly.

Introduction: It should be brief and written clearly in your own terms and not copied from the experiment document provided. Explain the relevant theory used in the experiments.

Results & Questions: Experimental results should be broken down into sections as in the lab manual. Each diagram should be discussed thoroughly and questions should be answered in detail.

Discussion: You must also add a Discussion section to each part of the lab experiment for providing information about your observations and the resulted technical facts.

Conclusions: In this section, a detailed conclusion of activities and the technical facts that have been learned should be provided.

GRADING SCHEME

There are four experiments for this semester, each lab report (#1 to #4) will be marked out of twenty-five. Late lab reports will be penalized for 20% for each late day. The grading scheme is as follows:

Pre-lab preparation **	2/20
Participation **	2/20
Objectives and brief introduction	2/20
Results presentation	4/20
Discussion and questions	4/20
Post lab	4/20
Conclusions	2/20

** It is important that students prepare themselves for each experiment by reading the instructions and theory before conducting the experiment. Participation means that each student should work on all tasks and steps by doing the configuration and interpreting results.

SUBMISSION OF LAB REPORT

The lab reports must be submitted individually.

INTRODUCTION

LAB LAYOUT

The bellowed diagram shows the layout of Network Lab.

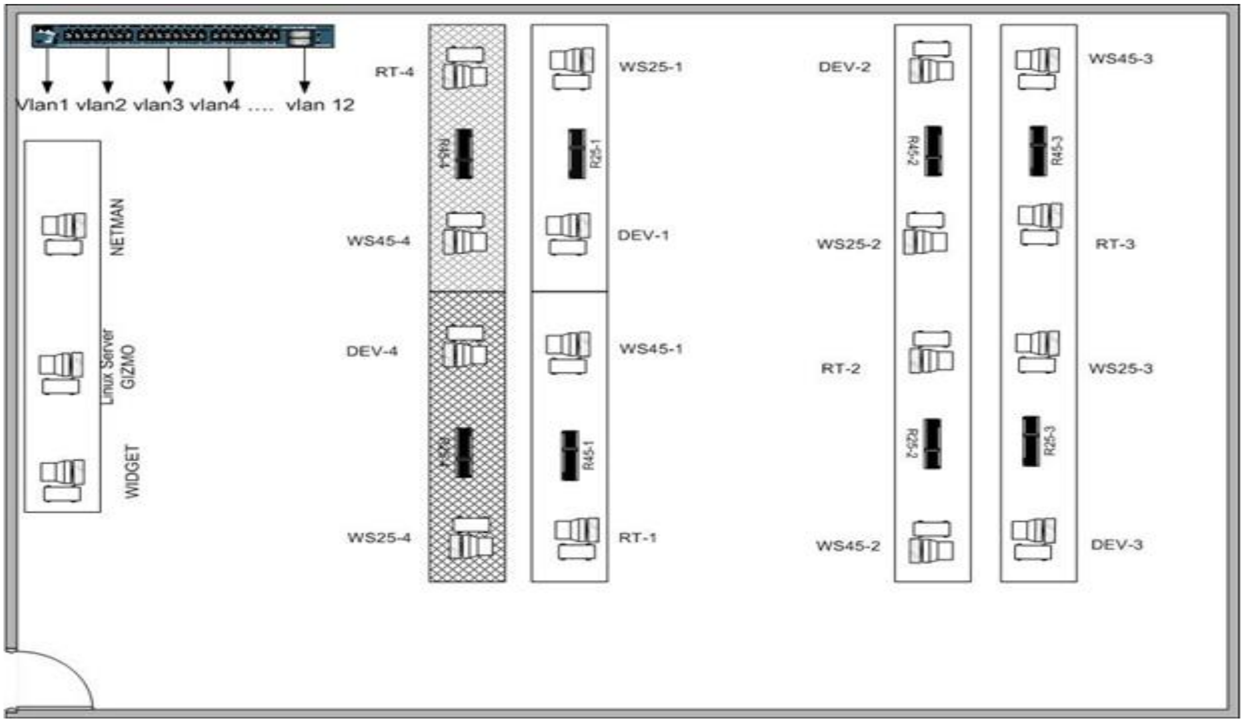


Figure 0.1: Laboratory Layout

IP ASSIGNMENT

Currently VLAN definition is relied on the network configuration, see above section about the current diagram of the Network Lab:

The flowing table lists most of the cables and IP assignments in above diagram. The detailed description for each section (VLAN) will be introduced in the next chapters.

Table 1: Lab Cabling and IP assignment

Device		IP Address
Gismo/Gizmo	Linux Server	192.168.20.18,
Widget	Gateway	192.168.20.19
Netman	Virtual Server	192.168.20.20
Solarwinds	Windows server	192.168.20.21
DEV-1		192.168.20.69
DEV-2		192.168.20.85
DEV-3		192.168.20.101

DEV-4		192.168.20.117
RT-4		192.168.20.166
RT-3		192.168.20.165
RT-2		192.168.20.149
RT-1		192.168.20.133
WS45-1		192.168.20.132
WS45-2		192.168.20.148
WS45-3		192.168.20.164
WS45-4		192.168.20.180
WS25-1		192.168.20.68
WS25-2		192.168.20.84
WS25-3		192.168.20.100
WS25-4		192.168.20.116
R25-1	GigabitEthernet0/0	192.168.20.67
	GigabitEthernet0/1	192.169.25.1
	Serial0/0/0	10.0.15.5
	Serial0/0/1	10.0.15.9
R25-2	GigabitEthernet0/0	192.168.20.83
	GigabitEthernet0/1	192.169.25.2
	Serial0/0/0	10.0.15.17
	Serial0/0/1	10.0.15.14
R25-3	GigabitEthernet0/0	192.168.20.99
	GigabitEthernet0/1	192.169.25.3
	Serial0/0/0	10.0.15.22
	Serial0/0/1	10.0.15.25
R25-4	GigabitEthernet0/0	192.168.20.115
	GigabitEthernet0/1	192.169.25.4
	Serial0/0/0	10.0.15.33
	Serial0/0/1	10.0.15.30
R45-1	GigabitEthernet0/0	192.168.20.131
	GigabitEthernet0/1	192.168.45.1
	Serial0/0/0	10.0.15.6/[29]
	Serial0/0/1	10.0.15.13
R45-2	GigabitEthernet0/0	192.168.20.147
	GigabitEthernet0/1	192.168.45.2
	Serial0/0/0	10.0.15.10
	Serial0/0/1	10.0.15.26
R45-3	GigabitEthernet0/0	192.168.20.163
	GigabitEthernet0/1	192.168.45.3
	Serial0/0/0	10.0.15.21
	Serial0/0/1	10.0.15.18
R45-4	GigabitEthernet0/0	192.168.20.179
	GigabitEthernet0/1	192.168.45.4
	Serial0/0/0	10.0.15.34
	Serial0/0/1	10.0.15.6

EXPERIMENT#1: WORKSTATION FOUNDATIONS

INTRODUCTION

In this lab we are going to learn about basic networking tools and devices and how to configure them.

First, you need to know exactly what an internetwork is: You create an internetwork when you take two or more LANs or WANs and connect them via a router, and configure a logical network addressing scheme with a protocol like IP.

The challenge in the networking world is to break a large network into small interconnected networks, and we do that to minimize the effect of network congestion, the procedure of dividing the network is called segmentation, it is accomplished using routers and switches. The possible causes of traffic congestion are:

- Large number of hosts in a broadcast domain.
- Multicasting
- Low bandwidth
- Broadcast storms

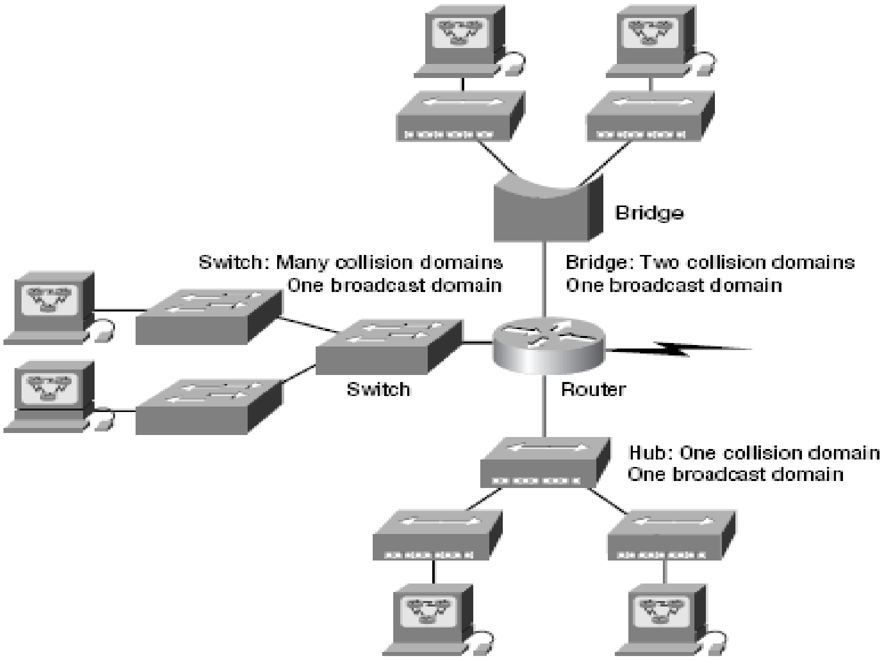

Bridge
Switch: Many collision domains
One broadcast domain
Bridge: Two collision domains
One broadcast domain
Switch
Router
Hub: One collision domain
One broadcast domain

Figure 0.2: Network Devices

Routers are used to connect networks together and route packets of data from one network to another. Routers, by default, break up a broadcast domain, which is the set of all devices on a network segment that hear all broadcasts sent on that segment. Breaking up a broadcast domain is important because when a host or server sends a network broadcast, every device on the network must read and process that broadcast—unless you've got a router. When the router's interface receives this broadcast, it can respond by basically saying "No thanks, go to your own network," and discard the broadcast without forwarding it on to other networks. Even though routers are known for breaking up broadcast domains by default, it's important to remember that they also break up collision domains as well.

Conversely, switches aren't used to create internetworks; they're employed to add functionality to an internetwork LAN. The main purpose of a switch is to make a LAN work better—to optimize its performance—providing more bandwidth for the LAN's users. And switches don't forward packets to other networks like routers do. Instead, they only "switch" frames from one port to another within the switched network.

PRELAB

After you read the whole experiment, do the following:

1. Find the IP address of your laptop or PC and take a screenshot of that.
2. Install Packet Tracer on your laptop or PC and take a screenshot of that. The download link can be found at : http://ccna-v5.net/2015/06/cisco-packet-tracer-6-2-full-windows-with-tutorial-free-download.html

DYNAMIC DHCP LAB

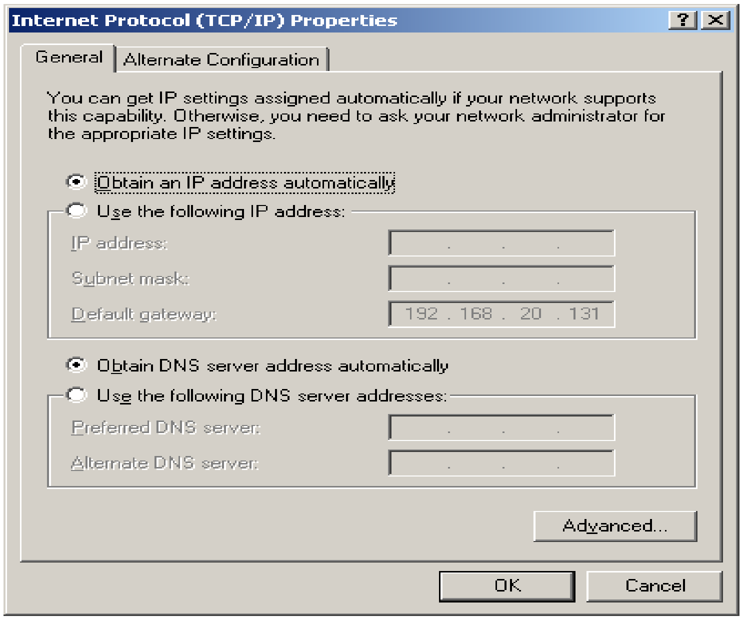
Objective:
To learn about DHCP and how it works with a workstation.

Materials and Tools:
Workstation on network with DHCP server

Background:
Most workstations connected to networks use a DHCP server from which to obtain their IP address automatically. In this lab you will learn how to release and renew the IP address and mask from your workstation using DOS commands and windows utilities.

Step-By-Step Instructions:
1. Enable DHCP in Windows workstation

Try to find and open the following window to check your workstation network setups. You may use Window Help to open it.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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: 192 . 168 . 20 . 131

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 0.1: Windows DHCP checkup

Confirm to select 'Obtain an IP automatically"

2. Use the command 'ipconfig'

Open up a DOS window, then type "ipconfig" to see your IP settings using DOS. From DOS you should see something like this:

```
C:\Documents and Settings\ELEC472>ipconfig

Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix. . :netlab
IP Address. . . . . . . . . . . . :192.168.20.132
Subnet Mask  . . . . . . . :  . . :255.255.255.0
Default Gateway. . . . . . . . . .:192.168.20.131
```

It's always a good idea to get a snapshot of the settings before you start changing them in case we need to put them back in later. Write down the IP address of the workstation, you will use it later.

```
C:\Documents and Settings\Elec472>ipconfig /?
```

From DOS we can now type 'ipconfig /release' to "let go" of our IP address. After doing that you should see:

```
C:\Documents and Settings\Elec472>ipconfig /release
IP address successfully released for adapter "Local Area
Connection"
```

Then we can use '*ipconfig /renew_all*'or *ipconfig /renew* to "get a new one" from the DHCP server.

You should see:

```
C:\Documents and Settings\Elec472>ipconfig /renew
Windows IP Configuration Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix. . :netlab
IP Address. . . . . . . . . . . . :192.168.20.132
Subnet Mask  . . . . . . . :   . . :255.255.255.0
Default Gateway. . . . . . . . . .:192.168.20.131
```

3. Use the command 'ping'

In the network world, 'ping' is king. This simple command can help you check the network connection.

- Try the command "*ping /?*" and real the help information.
- Use the command '*ping 192.168.20.19*' or '*ping widget.netlab*'

4. Use the command '*tracert*'

The ***tracert*** command traces the path by sending Internet Control Message Protocol (ICMP) Echo Request and Echo Reply messages (similar to the ***ping*** command) to produce command-line report output about each router that is crossed and the roundtrip time (RTT) for each hop. Packet filtering policies on routers, firewalls, or other types of security gateways might prevent the forwarding of this traffic. To trace a path by using the ***tracert*** command

- Open Command Prompt, and type the following:
- ***tracert*** *host_name (widget.netlab)* Or, type ***tracert*** *ip_address(192.168.20.19)* where *host_name* or *ip_address* is the host name or IP address, respectively, of the remote computer.

Notes: If ***tracert*** is unsuccessful, you can use the command output to help determine at which intermediate router forwarding failed or was slowed. For details about packet forwarding and packet loss at each router and link in the path, use the ***pathping*** command.

Questions:

1. Can I ping my workstation itself? How?
2. How does DHCP work?

So What Have You Learned Here?

You have learned how to release and renew the DHCP address from a workstation. In later labs you will work more with DHCP and need to know how it works. Here you also learn some helpful commands, '*ping*', '*tracert*' or '*pathping*'

CONSOLE PORT – ROUTER LOCAL ACCESS

Objectives:

Learn how to set up a router and login through a router console port from a workstation using the *HyperTerminal* or *Putty* program.

Tools and Materials:

Workstation with *HyperTerminal and Putty program*, Cisco router, a rollover cable (or called console cable.)

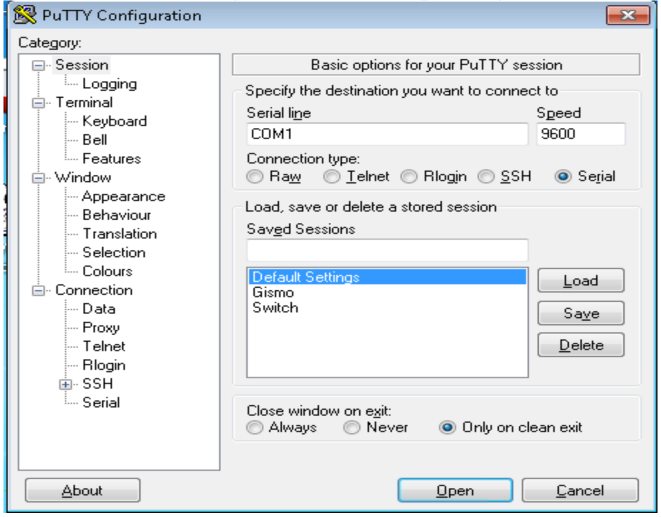
Background:

This lab is designed to show you how to set up a terminal program, how to connect a router console port and how to access the router.

1.1.1 PUTTY

PuTTY is an implementation of Telnet and SSH for Windows and Unix platforms, along with an `xterm` terminal emulator.

1. Connect the router from the ***console port*** to COM1 on your workstation using a rollover cable, then you can run HyperTerminal and connect to the router.
2. Click the icon 'Putty' on the desktop, Putty window will be shown.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM1

Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

Saved Sessions

Default Settings
Gismo
Switch

Close window on exit: ○ Always ○ Never ● Only on clean exit

3. Select the connection type as ***Serial*** and confirm to use the Serial port ***COM1*** and Speed at ***9600***.
4. Click the button 'Open', press the key 'Enter'.
5. Type '?" and more.

SUMMARY:

Learn about some more communication software. HyperTerminal and Putty are going to be used quite a lot throughout the rest of this manual.

TELNET – ROUTER REMOTE ACCESS

Objective:

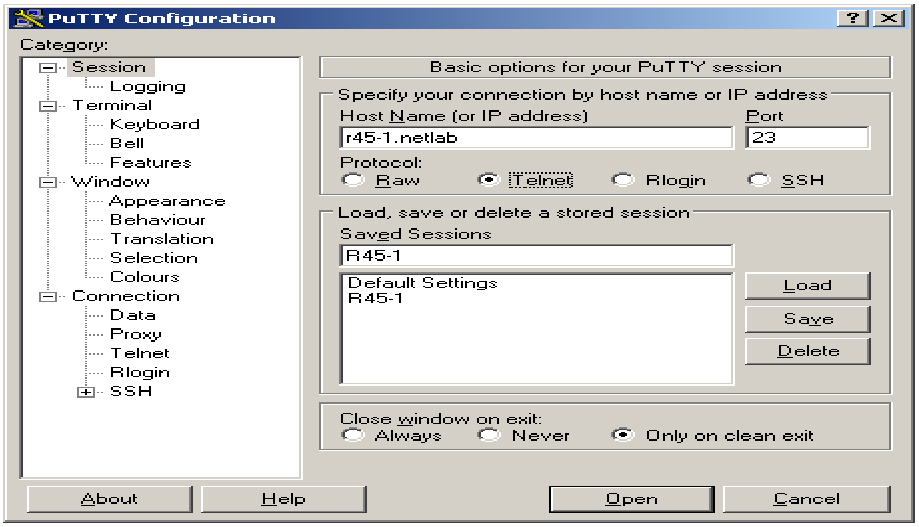
To learn how to use terminal emulation (TELNET) software for a router connectivity.

Background:

In lab you have known how to connect a router via HyperTerminal or Putter, now you will learn how to access a router by TELNET remotely.

1.1.2 TELNET BY PUTTY

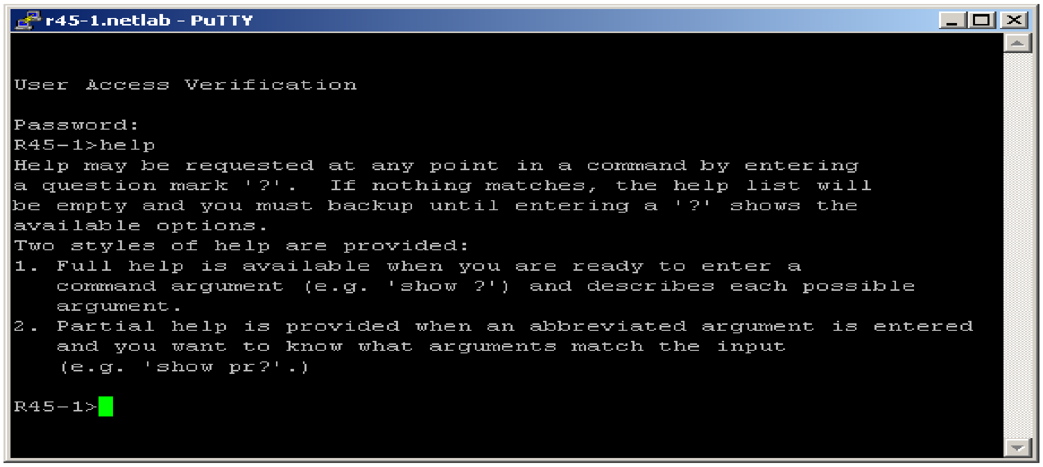
To open the Putty telnet application, click the 'Putty' icon on Desktop or launch from ***"Start-> All Programs->Putty".***



Host Name (or IP address): r45-1.netlab
Port: 23
Protocol: ○ Raw ● Telnet ○ Rlogin ○ SSH
Saved Sessions: R45-1
Default Settings
R45-1
Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 0.2: Putty Interface

Input the router domain name, such as 'r45-1.netlab' or its ip address which you get from DHCP section, and save it as a session. Choose the protocol 'Telnet', and then try to open a connection. Input your Telnet password: **colab**, the following window shows up:



```
User Access Verification

Password:
R45-1>help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)

R45-1>
```

Telnet to a router: input the router domain name, such as 'r45-1.netlab' or it ip address, then try to set a

connection with your router.
Find your peer workstation from the following table:

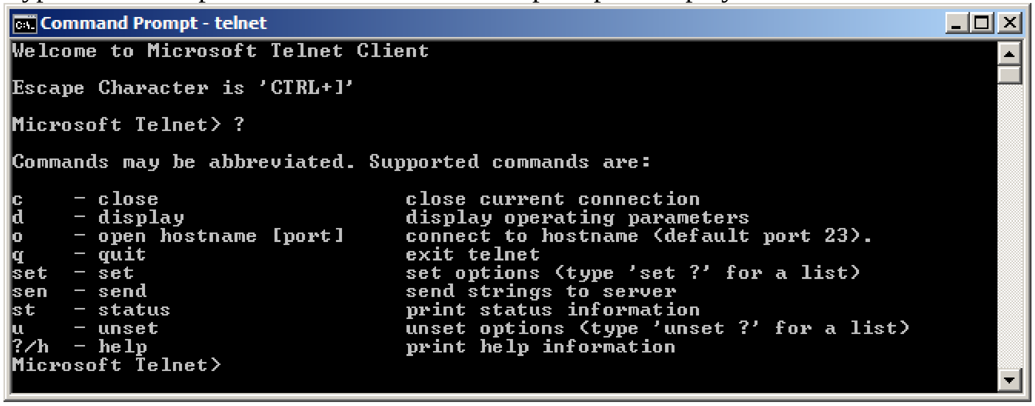
Table 2: Router and its Workstation

Router	Workstation-1	Workstation-2	Vlans
R25-1	WS25-1	DEV-1	Vlan 5
R25-2	WS25-2	DEV-2	Vlan 6
R25-3	WS25-3	DEV-3	Vlan 7
R25-4	WS25-4	DEV-4	Vlan 8
R45-1	WS45-1	RT-1	Vlan 9
R45-2	WS45-2	RT-2	Vlan 10
R45-3	WS45-3	RT-3	Vlan 11
R45-4	WS45-4	RT-4	Vlan 12

1.1.3 TELNET BY MICROSOFT TELNET

To open a Telnet session:

- Click **Start**.
- Enter **cmd** in the **Search** field in the **Start** menu. A command prompt is displayed.
- Type **telnet** and press ENTER. The **Telnet>** prompt is displayed.



```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> ?

Commands may be abbreviated. Supported commands are:

c    - close                    close current connection
d    - display                  display operating parameters
o    - open hostname [port]     connect to hostname (default port 23).
q    - quit                     exit telnet
set  - set                      set options (type 'set ?' for a list)
sen  - send                     send strings to server
st   - status                   print status information
u    - unset                    unset options (type 'unset ?' for a list)
?/h  - help                     print help information
Microsoft Telnet>
```

- Or by using the router name, you can input the full telnet command, for example ‘telnet r25-1.labnet”. Note: use your own router name to replace ‘r25-1’.

Try to connect your router by its name or ip.

Supplemental Labs or Challenge Activities:

1. Read the tutorials on how to use telnet and its associated websites.
2. How to use Telnet to save your work?
3. Compare the HyperTerminal and Telnet when you are working with a router.

Summary

Learn about Telnet utilities that can be used to connect your router. In the following labs, you can choose your favorite tool to talk with your router.

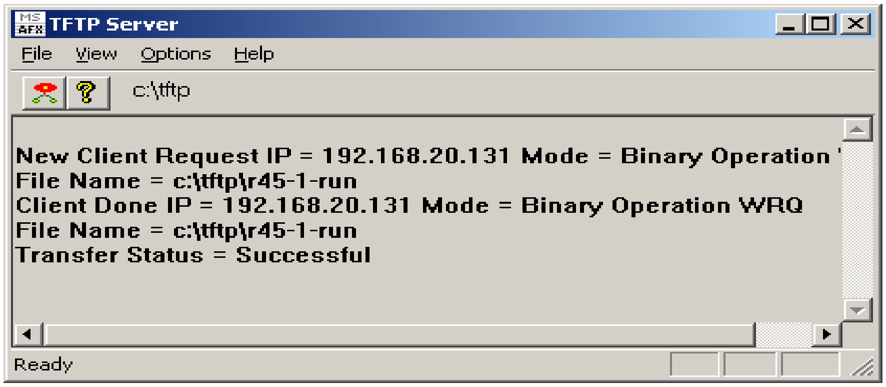
TFTP SERVER

Objective:
To learn the basics about file transfer programs.

Background:
The File Transfer Program (FTP) has probably been used by nearly everyone who uses the web, whether they know it or not. This program is used to transfer files from one computer to another. The Trivial File Transfer Program (TFTP) is a similar program but is used for more specific applications like downloading software to a router. Here you will learn how to use TFTP and its basic commands to upload and download a file. You also will learn how to save your file into your 'home' from Network lab. In a later lab you will use the similar TFTP program to download an operating system to a router.

Step-by-Step Instructions:
A. Check the TFTP server on your workstation.

You can find a Tftp.lnk on your desktop, click it to check its status. Remember its root directory.



c:\tftp

```
New Client Request IP = 192.168.20.131 Mode = Binary Operation
File Name = c:\tftp\r45-1-run
Client Done IP = 192.168.20.131 Mode = Binary Operation WRQ
File Name = c:\tftp\r45-1-run
Transfer Status = Successful
```

Ready

Figure 0.3: TFTP Server

B. Connect to your router by HyperTerminal or Telnet

C. Use the command

```
R45-1>enable
Password:xxxx

R45-1#show running-config
```

You will see current running configuration in your router. Let's save it now. It may be good idea for you to save a copy at the beginning.
Note: Here you may not understand these commands. That is no problem, you shall learn about them in Experiment #2.

D. Use the following command:

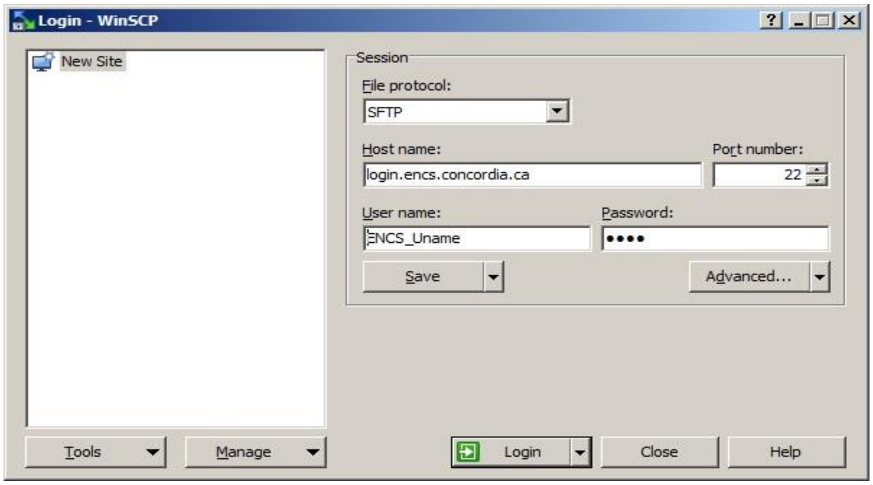
```
R45-1#copy running-config tftp://192.168.20.132/r45-1-run
```

Note: check out your workstation IP first, then use it in above command. You should change the router and workstation name in command line according to the router that you are working with.
192.168.20.132 – IP address of the router you are working with (your WorkStation IP);
r45-1-run: the file name that you want to save.

E. Check the message shown in TFTP server, and confirm file that you named is already saved on your desktop.

SECURE FILE TRANSFER

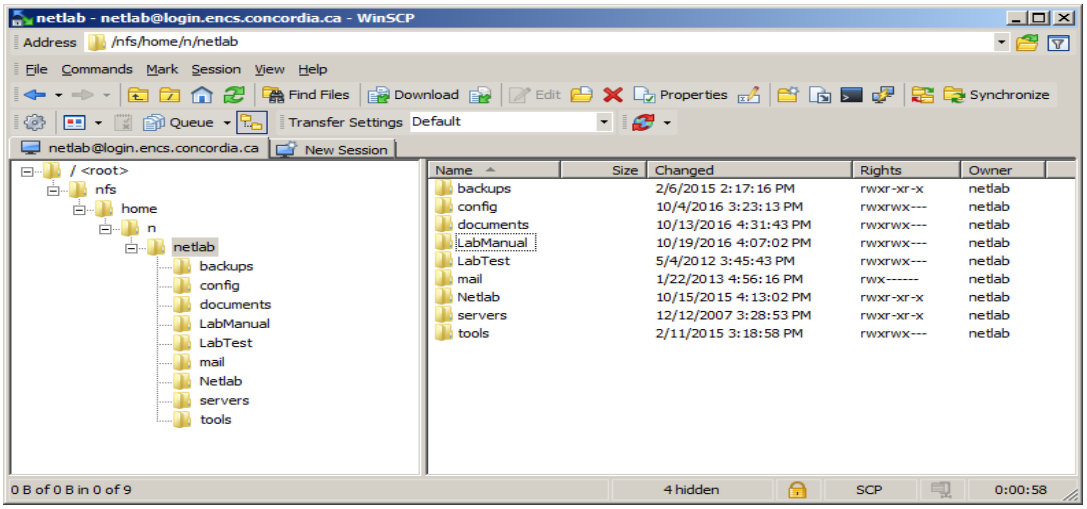
The tool – WinSCP has been installed on every workstation. To run this tool, click the icon or from 'Start -> Programs ->WinSCP", you would see the following window:



File protocol: SFTP
Host name: login.encs.concordia.ca
Port number: 22
User name: ENCS_Uname
Password: ••••

Figure 0.4: WinSCP File Transfer

input Host name as: ***login.encs.concordia.ca*** and your ENCS ID, press "Login", you need to input your password. You shall see your ENCS /home directory on the right window.



Address /nfs/home/n/netlab

Transfer Settings Default

Name	Size	Changed	Rights	Owner
backups		2/6/2015 2:17:16 PM	rwxr-xr-x	netlab
config		10/4/2016 3:23:13 PM	rwxrwx---	netlab
documents		10/13/2016 4:31:43 PM	rwxrwx---	netlab
LabManual		10/19/2016 4:07:02 PM	rwxrwx---	netlab
LabTest		5/4/2012 3:45:43 PM	rwxrwx---	netlab
mail		1/22/2013 4:56:16 PM	rwx------	netlab
Netlab		10/15/2015 4:13:02 PM	rwxr-xr-x	netlab
servers		12/12/2007 3:28:53 PM	rwxr-xr-x	netlab
tools		2/11/2015 3:18:58 PM	rwxrwx---	netlab

0 B of 0 B in 0 of 9 4 hidden SCP 0:00:58

It is suggested that you to create a sub-directory called ‘netlab’ to save your files used in ECE Network Lab.
Find the router configuration file and save to your /home. Actually you can save and copy your another files by this tool.

Note: you should keep in mind; the file you save on the workstation might be changed and copied by other students. So don’t rely on the file that you saved in last lab.

Supplemental Labs or Challenge Activities:
So What Have You Learned Here?

- How to save router configuration to a workstation, how to copy it back?

- How to save files in the lab to ENCS server and how to retrieve them back.

NETWORK PACKET ANALYZER: WIRESHARK

Objective:

Learn how use Wireshark- a free a network packet analyzer (or called protocol inspector).

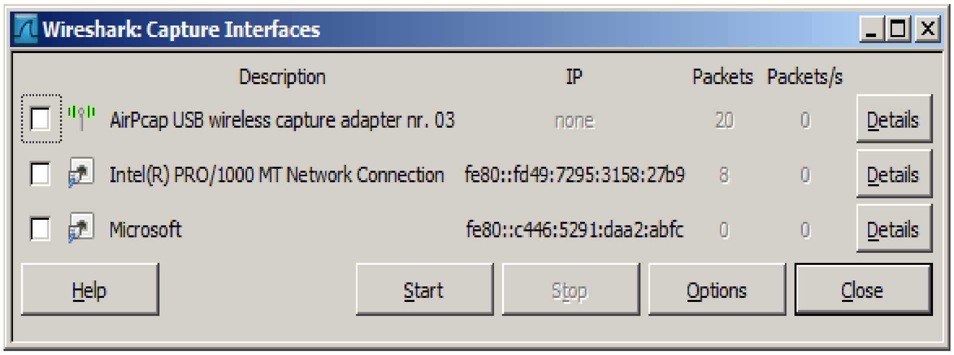
Introduction

Wireshark is a network packet analyzer that intercepts, captures and logs information about packets passing through a network interface. This is useful for analyzing network problems, detecting network intrusions, network misuse, and other security problems, monitor usage and gather statistics, and many other applications..

* You will need to run Wireshark with root/Administrator privileges in order to perform live capture on your network interface.

1.1.4 CAPTURE A PACKAGE

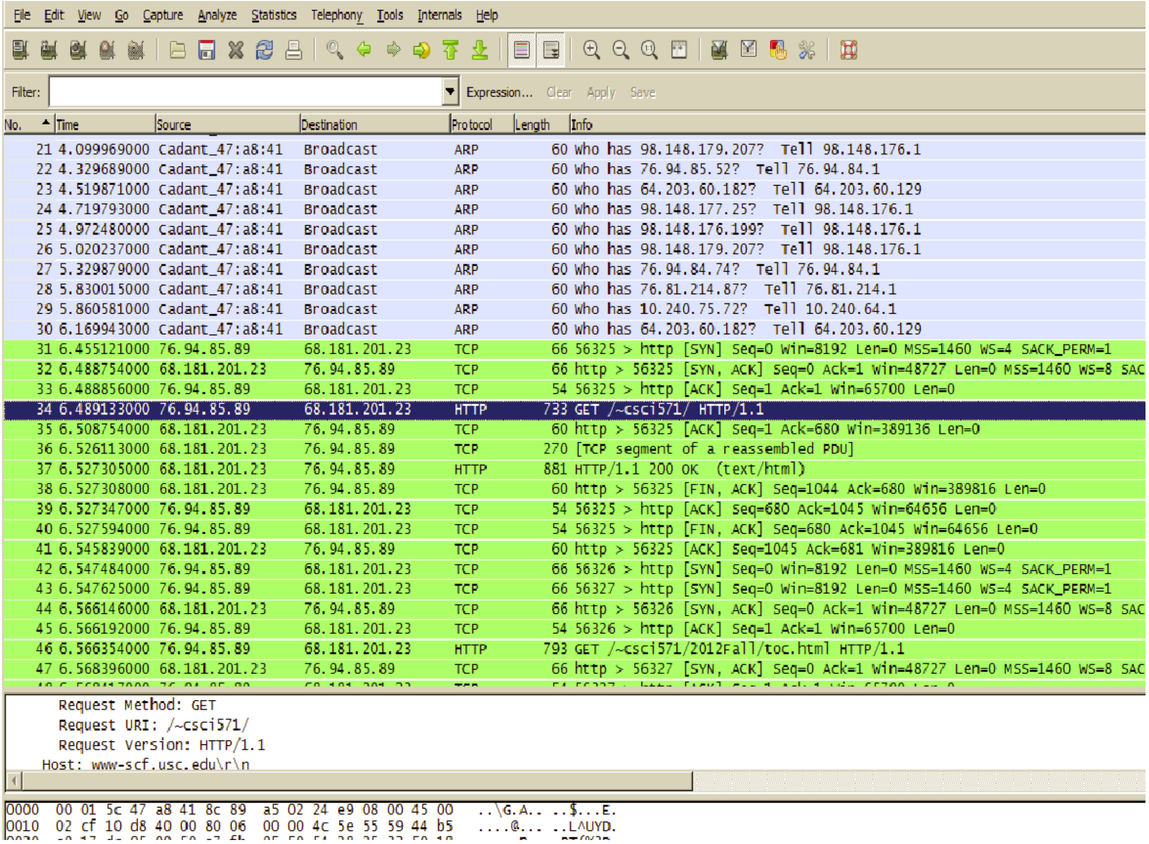
1. Click the icon of Wireshark to run Wireshark.
2. Under the “Capture” header, select the “Interface List” option; or click on the “Interfaces” button on the toolbar:



	Description	IP	Packets	Packets/s	
□	AirPcap USB wireless capture adapter nr. 03	none	20	0	Details
□	Intel(R) PRO/1000 MT Network Connection	fe80::fd49:7295:3158:27b9	8	0	Details
□	Microsoft	fe80::c446:5291:daa2:abfc	0	0	Details

This will bring up a list of network interfaces that Wireshark is able to capture packets from: Select the network adapter (wired or wireless) that you are currently using to connect to the Internet, and hit the “Start” button. This will take you to the main window, see the following figure.

Wireshark is now capturing live network activity on your network interface. Notice that the list of packets is color-coded to highlight different types of network traffic.
Open your web browser and navigate to a few random web pages – observe that the network packets corresponding to your web browsing activity are captured and show up in Wireshark as well.


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time        Source            Destination      Protocol Length Info
   21 4.099969000 Cadant_47:a8:41   Broadcast        ARP        60 Who has 98.148.179.207?  Tell 98.148.176.1
   22 4.329689000 Cadant_47:a8:41   Broadcast        ARP        60 Who has 76.94.85.52?  Tell 76.94.84.1
   23 4.519871000 Cadant_47:a8:41   Broadcast        ARP        60 Who has 64.203.60.182?  Tell 64.203.60.129
   24 4.719793000 Cadant_47:a8:41   Broadcast        ARP        60 Who has 98.148.177.25?  Tell 98.148.176.1
   25 4.972480000 Cadant_47:a8:41   Broadcast        ARP        60 Who has 98.148.176.199?  Tell 98.148.176.1
   26 5.020237000 Cadant_47:a8:41   Broadcast        ARP        60 Who has 98.148.179.207?  Tell 98.148.176.1
   27 5.329879000 Cadant_47:a8:41   Broadcast        ARP        60 Who has 76.94.84.74?  Tell 76.94.84.1
   28 5.830015000 Cadant_47:a8:41   Broadcast        ARP        60 Who has 76.81.214.87?  Tell 76.81.214.1
   29 5.860581000 Cadant_47:a8:41   Broadcast        ARP        60 Who has 10.240.75.72?  Tell 10.240.64.1
   30 6.169943000 Cadant_47:a8:41   Broadcast        ARP        60 Who has 64.203.60.182?  Tell 64.203.60.129
   31 6.455121000 76.94.85.89       68.181.201.23    TCP        66 56325 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
   32 6.488754000 68.181.201.23     76.94.85.89      TCP        66 http > 56325 [SYN, ACK] Seq=0 Ack=1 Win=48727 Len=0 MSS=1460 WS=8 SAC
   33 6.488856000 76.94.85.89       68.181.201.23    TCP        54 56325 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0
   34 6.489133000 76.94.85.89       68.181.201.23    HTTP      733 GET /~csci571/ HTTP/1.1
   35 6.508754000 68.181.201.23     76.94.85.89      TCP        60 http > 56325 [ACK] Seq=1 Ack=680 Win=389136 Len=0
   36 6.526113000 68.181.201.23     76.94.85.89      TCP       270 [TCP segment of a reassembled PDU]
   37 6.527305000 68.181.201.23     76.94.85.89      HTTP      881 HTTP/1.1 200 OK  (text/html)
   38 6.527308000 68.181.201.23     76.94.85.89      TCP        60 http > 56325 [FIN, ACK] Seq=1044 Ack=680 Win=389816 Len=0
   39 6.527347000 76.94.85.89       68.181.201.23    TCP        54 56325 > http [ACK] Seq=680 Ack=1045 Win=64656 Len=0
   40 6.527594000 76.94.85.89       68.181.201.23    TCP        54 56325 > http [FIN, ACK] Seq=680 Ack=1045 Win=64656 Len=0
   41 6.545839000 68.181.201.23     76.94.85.89      TCP        60 http > 56325 [ACK] Seq=1045 Ack=681 Win=389816 Len=0
   42 6.547484000 76.94.85.89       68.181.201.23    TCP        66 56326 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
   43 6.547625000 76.94.85.89       68.181.201.23    TCP        66 56327 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
   44 6.566146000 68.181.201.23     76.94.85.89      TCP        66 http > 56326 [SYN, ACK] Seq=0 Ack=1 Win=48727 Len=0 MSS=1460 WS=8 SAC
   45 6.566192000 76.94.85.89       68.181.201.23    TCP        54 56326 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0
   46 6.566354000 76.94.85.89       68.181.201.23    HTTP      793 GET /~csci571/2012Fall/toc.html HTTP/1.1
   47 6.568396000 68.181.201.23     76.94.85.89      TCP        66 http > 56327 [SYN, ACK] Seq=0 Ack=1 Win=48727 Len=0 MSS=1460 WS=8 SAC
```

```
      Request Method: GET
      Request URI: /~csci571/
      Request Version: HTTP/1.1
    Host: www-scf.usc.edu\r\n
```

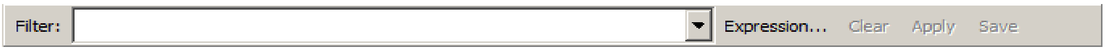
```
0000  00 01 5c 47 a8 41 8c 89  a5 02 24 e9 08 00 45 00   ..\G.A.. ..$...E.
0010  02 cf 10 d8 40 00 80 06  00 00 4c 5e 55 59 44 b5   ....@... ..L^UYD.
```

3. Open a terminal by ‘Start ->Run ->cmd”, input the command *ping 192.108.20.146* or other ip commands ‘tracert’. See what you get in Wireshark Window, By default, the list of captured packets will keep scrolling automatically during a live capture. You can toggle this on/off using the AutoScroll toggle button in the toolbar:
4. Press the stop capture button: to stop capturing and try to analysis the packages.

1.1.5 FILTERING THE PACKET LIST

In the previous section, you’ve captured all kinds of network traffic from a couple minutes of network activity – this could include traffic on many different protocols such as ARP, TCP, UDP, DNS, HTTP, etc.

You may not be interested in all of these, depending on what you are trying to achieve. Fortunately, Wireshark allows you to filter the list based on different criteria using the “Filter” toolbar:



Filter toolbar

For the purposes of this exercise, you are going to look at the HTTP traffic that occurs when browsing the web.

1. In the filter toolbar, type “http” and then click on “Apply”. The window will now list only captured packets related to HTTP traffic.
2. Start Capture again.
3. Open your web browser and navigate to web pages at http://192.168.20.19 – observe that the network packets corresponding to your web browsing activity are captured and show up in Wireshark as well.
4. After letting the capture run for a couple of minutes, press the stop capture button: , analysis the packages

Supplemental Labs or Challenge Activities:

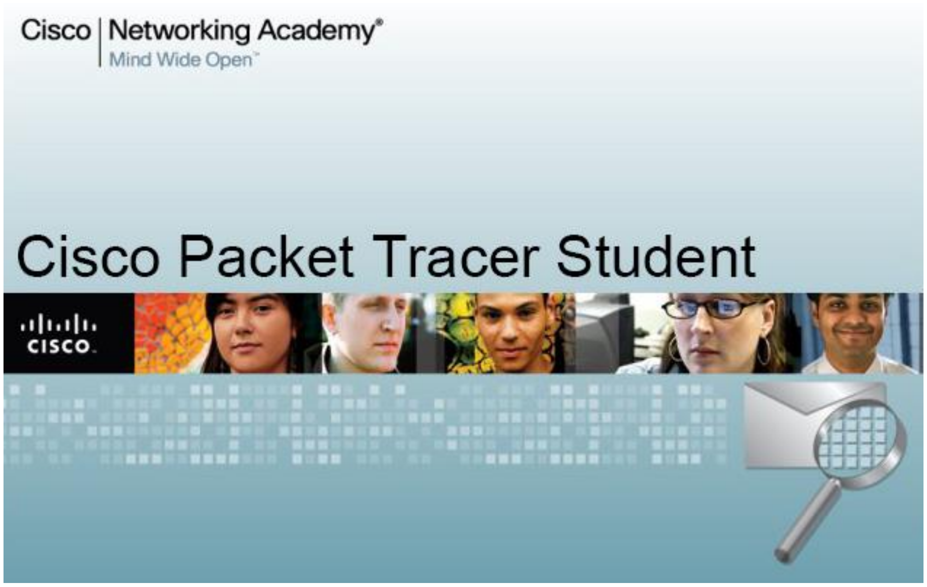
- Go to the Wireshark website and find the sample packets https://www.wireshark.org/.
- Get the one on IPv6. How does it differ from IPv4?

Using your protocol inspector find out how much they can really see and cannot see actually?

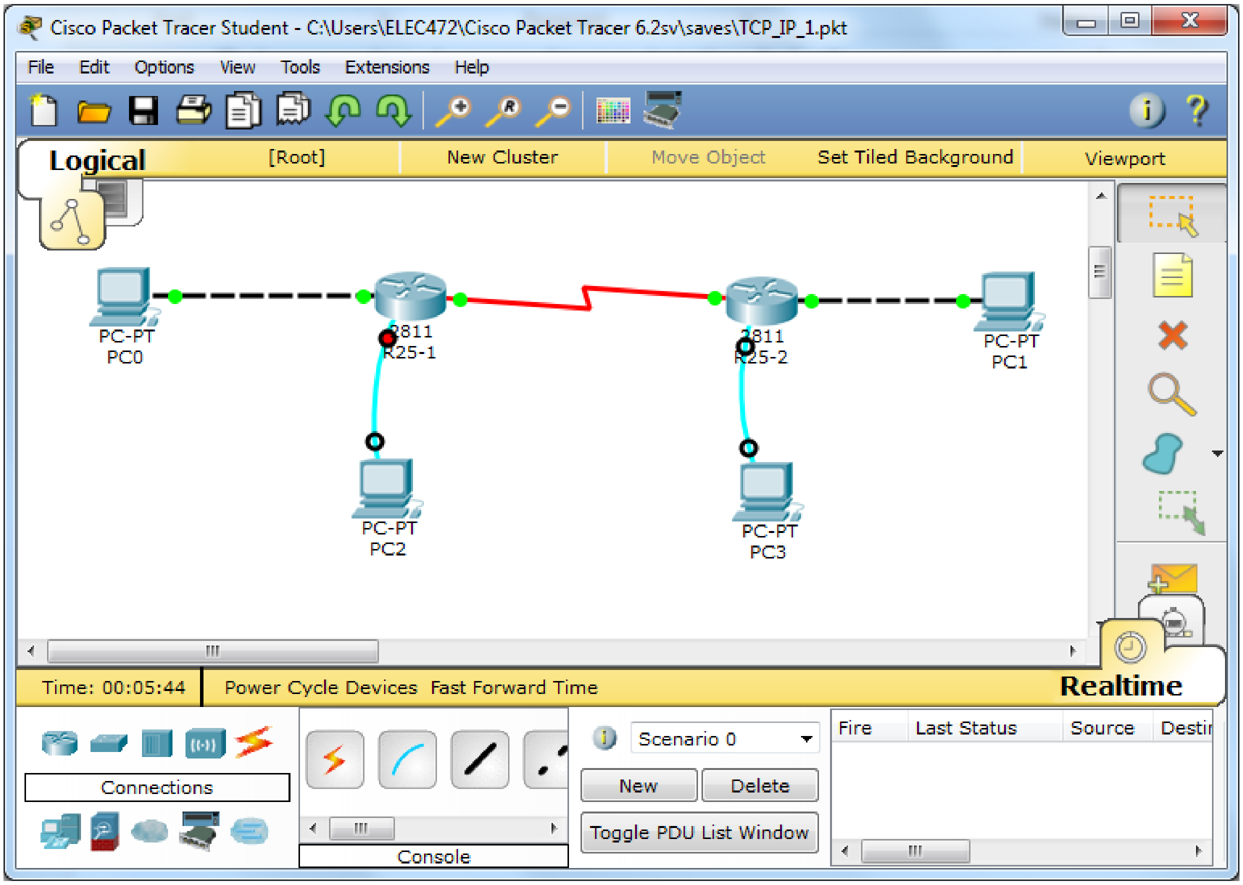
CISCO PACKET TRACER

The best way to learn about networking is to do it. Cisco Packet Tracer, an innovative network configuration simulation tool that helps you improve your networking configuration skills from your desktop or mobile device. We use Packet Tracer to:

- Improve network skills.
- Prepare for a certification exam.
- Practice what you learn in networking courses.



Try to draw a network with the workstations and routers. For example:



What Have You Learned Here?

In almost every lab you will be using a workstation, you may have to know its network setting no matter how these settings have been set up, to know how to use some basic network tools.

POST-LAB

Do the following task(s) and take a snapshot for each part and include it in your report.

1. Find the IP address of the following websites by using PING command :
    a. GMAIL (gmail.com)
    b. CONCORDIA UNIVERSITY (concordia.ca)
    c. FACEBOOK (facebook.com)
    d. TWITTER (twitter.com)
    e. YOUTUBE (youtube.com)

EXPERIMENT #2: ROUTER FOUNDATIONS

This lab is designed to help the students know more about a router. It will help them become familiar with basic router configuration commands. (Check on the status of interfaces, enable and disable interfaces, set passwords, etc.)

QUICK OVERVIEW THE ROUTERS - CISCO 3900

This paper lab requires you to read the documents from Cisco and understand the equipment in the lab that you will work with.
The modular Cisco 3900 Series Multi-service Access Routers leverage network modules (NMs),WAN Interface Cards (WICs), and Advanced Integration Modules (AIMs) from the Cisco 1700, 2600, and 3600 Series Routers for WAN Access, Voice Gateway, Security, Content, Circuit Emulation, and Dial applications. In addition, the Cisco 3925 and Cisco 3945 introduce a new, doublewide form factor, which provides support for the high density services modules (HDSM's). The Cisco 3945 with four network module slots can accept up to two HDSM's by removing the center guides between each pair of adjacent NM slots. The Cisco 3925, with two network module slots can accept a single HDSM in the upper network module slot by removing the blank panel and still have an available network module slot. By utilizing the new HDSM capability the Cisco 3900 Series routers are able to integrate higher port density and new, high performance services.

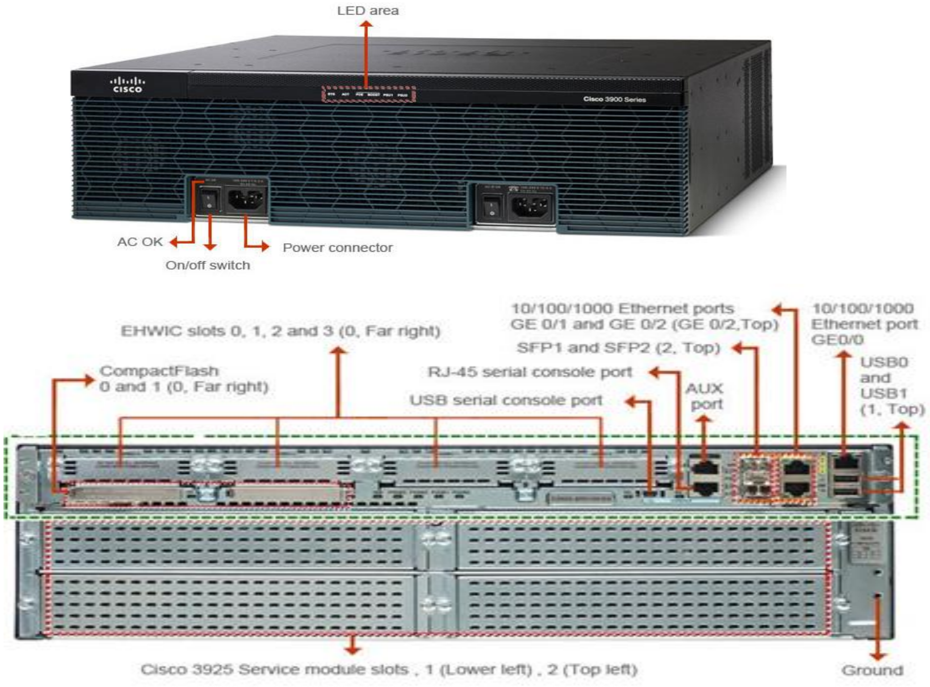

LED area
AC OK
On/off switch
Power connector
10/100/1000 Ethernet ports GE 0/1 and GE 0/2 (GE 0/2,Top)
10/100/1000 Ethernet port GE0/0
EHWIC slots 0, 1, 2 and 3 (0, Far right)
SFP1 and SFP2 (2, Top)
USB0 and USB1 (1, Top)
CompactFlash 0 and 1 (0, Far right)
RJ-45 serial console port
AUX port
USB serial console port
Cisco 3925 Service module slots , 1 (Lower left) , 2 (Top left)
Ground

Figure 0.1: 3925/3945 Multiservice Access Router

Key features for the Cisco 3925 and 3945:

- Modular Services Performance Engine (SPE) 100, which can be upgraded for even higher performance as next-generation WAN environments evolve
- 3 integrated 10/100/1000 Ethernet ports with 2 ports capable of RJ-45 or SFP connectivity
- 4 service module slots
- 4 Enhanced High-Speed WAN Interface Card (EHWIC) slots
- 4 onboard digital signal processor (DSP) slots
- 1 Internal Services Module slot
- Dual integrated power supplies
- Fully integrated power distribution to modules supporting 802.3af Power over Ethernet
- Integrated threat control using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, and Cisco IOS Content Filtering
- Unified Communications
- High-density-packet voice DSP module, optimized for voice and video support
- Support for Cisco Communications Manager Express and Survivable Remote Site Telephony

Supplemental Lab:

1. List some 3 service from 3925/3945 ‘multiservice’
2. Draw a diagram of 3925/3945 typical application.

PRELAB

After reading the whole experiment, do the following and take a snapshot for each part:

1. Open the Packet Tracer software and build a network topology that has three routers and three PCs. Take a screenshot of the built network. Save this file as we will be using it in the upcoming experiments.
2. Apply the basic commands (**except Static Routing**) shown in Experiment 2 on each router and take a snapshot of that.
    a. Find the available commands on the user mode.
    b. Change the name of each router to **YOURNAME_n** where n is 1 for the first router, 2 for the second router, and 3 for the third router.

BASIC ROUTER COMMANDS

Objective

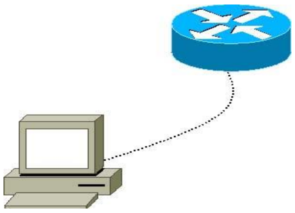
To become familiar with basic router commands including how to get help.

Background

In this lab we take you into the mysterious world of the router. In this lab you will become familiar with the help commands, the types of prompts you will use, and some basic router commands.

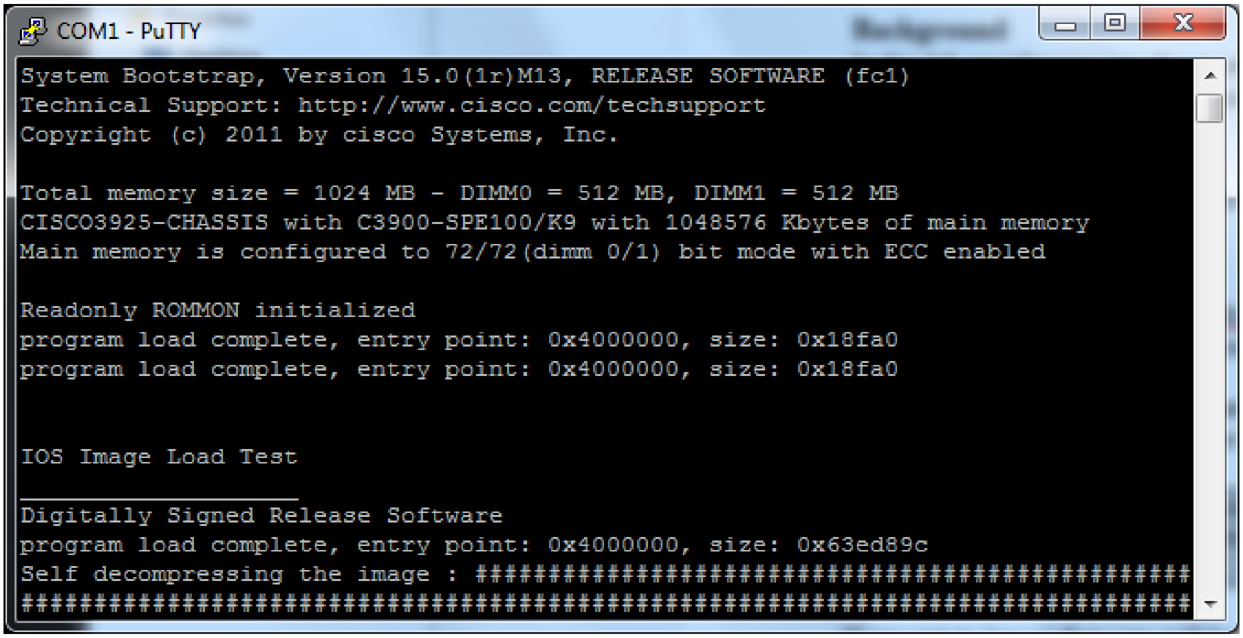
Lab Design:

Set a workstation as a router console by serial cable connecting.



Step-by-Step Instructions:

1. Open a terminal session Putty on the workstation.
2. Turn the power on to the router and watch the text as the router boots.



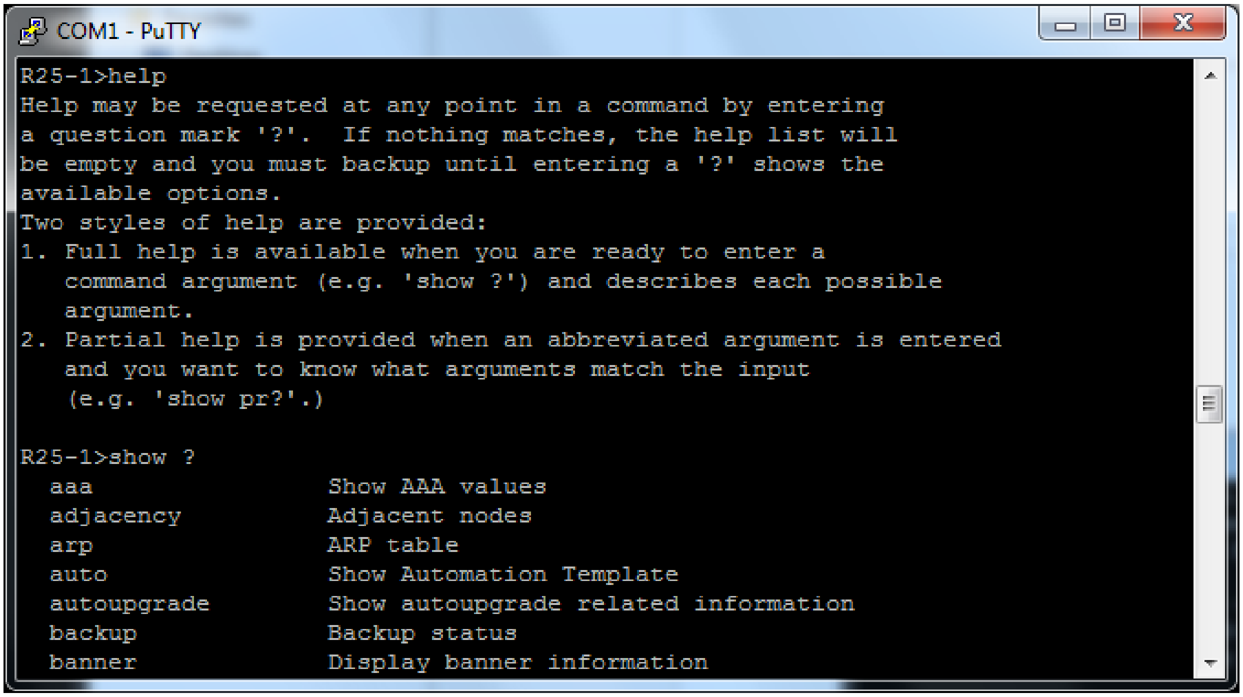
```
System Bootstrap, Version 15.0(1r)M13, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.

Total memory size = 1024 MB - DIMM0 = 512 MB, DIMM1 = 512 MB
CISCO3925-CHASSIS with C3900-SPE100/K9 with 1048576 Kbytes of main memory
Main memory is configured to 72/72(dimm 0/1) bit mode with ECC enabled

Readonly ROMMON initialized
program load complete, entry point: 0x4000000, size: 0x18fa0
program load complete, entry point: 0x4000000, size: 0x18fa0


IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x4000000, size: 0x63ed89c
Self decompressing the image : #################################################
################################################################################
```

Press RETURN to get started. To see what options are available for us at the user prompt we can “ask” our router for help. Computer devices are like that…if we get stuck, then we can ask it for help. On your workstation if you want some help then you can use your pull-down menus or even use the task bar help option (Start>help). Routers are helpful too. The phrase “easy when you know how” really applies. To get help you should start with the generic “**`help`**.” Then press enter, you should see something like this:



```
R25-1>help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)

R25-1>show ?
  aaa                  Show AAA values
  adjacency            Adjacent nodes
  arp                  ARP table
  auto                 Show Automation Template
  autoupgrade          Show autoupgrade related information
  backup               Backup status
  banner               Display banner information
```

```
router>help

Help may be requested at any point in a command by entering a
question mark '?'.  If nothing matches, the help list will be
empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a command
argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is
entered and you want to know what arguments match the input (e.g.
'show pr?'.)Router>
```

Ok…so that didn't give you much. Most computers or network systems the command "help" works very well. So remember it and use it when appropriate. There is a better way to get help using the question mark on Cisco devices. Try typing this (and press enter):

```
router>?
Exec commands:
  <0-4>/<0-4>      Enter card slot/sublot number
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  clear            Reset functions
  connect          Open a terminal connection
  credential       load the credential info from file system
  crypto           Encryption related commands.
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection

-------More---------
```

Then the router is waiting for you to press enter to continue. This just stops what's on the screen for you to be able to read it. If you hit any other key it will take you back to the prompt without showing the rest of the information.

Now let's move on to the next type of prompt: the privileged mode prompt.

To get to the privileged prompt you need to type either "**enable**" or "**en**" for a shortcut. Many commands can be short-cut but for now get used to using the entire command. As you progress through these labs and get comfortable with the commands then you can start abbreviating the commands.

```
router>enable
router#
```

Notice how the prompt changes from a carat to a pound sign. This is a visual cue to you that you are at the privileged mode prompt. To switch back to the user mode prompt simply type "**disable**." Actually you can also type "**exit**" here and it will do the same thing, but "**disable**" is the technically most correct answer for how to get from the privileged mode prompt to the user mode prompt. Try both and see for yourself.

Now let's get back to exploring the privileged mode prompt command options. Just like we did at the user mode prompt we can request help for seeing all available command options with a question mark:

```
router# ?
```

Write down what you see on the worksheet entitled “privileged mode ? Options.” Like the user mode prompts some of the commands you will be using more than the others.

Check router configuration

Let’s try using a couple of those commands. Type “***show run***” and look at the output. This is actually the current running configuration script for your router. You will learn more about this in the next couple of labs.

Reboot Router

Type “***reload***” and hit enter. You will need to hit enter one more time and the system will “reload” or in geek terms it will “reboot”.

Shortcuts with router commands.

These are designed to help you more accurately work with your router. You can use the up and down arrows to view the previous commands. We did this earlier in part 1 with our workstation DOS prompt and the DOSKEY commands. If you do not see anything when you use the up arrow it may because you have not used any commands at that specific prompt mode. Next, lets look at some keystroke shortcuts. Suppose you typed a command similar to what you need to use next. Ping will be a good example here…supposes we wanted to ping to destinations 192.168.1.1 and 192.168.1.2. We could try it this way:

```
 router#ping 192.168.20.18 (typed)
 router#ping 192.168.20.20 (typed)
```

Or we could do it this way:

```
 router#ping 192.168.20.18 (typed)
 router#ping 192.168.20.18 (used the up arrow)
 router#ping 192.168.20. (Back space one character)
 router#ping 192.168.20.18 (typed in “2”)
```

In this manner we used less keystrokes and we have reduced the possibility of a typing error on the second ping command. These types of short cuts are ok. You can use keystroke commands to move back and forth more quickly on the command line.

Another way to view the progression of commands is using the “show history” command. The up arrow will only show you those commands one at a time, but

```
router#show history
```

the *show history* will show you the last 15 commands (default) you used. Heck, you can even change how many previous commands will be stored. Let’s try that now:

```
router#terminal history size 5
```

Using this command will set the number of commands retained in the history buffer to 5. If you were to “show history” then you would see the previous 5 commands. This number can range from 0 to 256. (Sounds like a good CCNA question doesn’t it?).
Ok. We are still moving with our prompts. Before we can make any changes to our router we need to be at the configuration mode prompt.

```
router#config
Configuring from terminal, memory, or network [terminal]?
router#terminal
router(config)#
```

Or we can just by-pass that second statement by combining the two statements:

```
router#config t
router(config)#
```

Change the name of our router.

We do this from the privileged mode prompt using the command “hostname.” Let’s change it to our name.

```
router(config)#hostname matt
matt(config)#
```

Notice how the prompt changes immediately to our new hostname.
To leave the configuration mode, just type exit.

```
matt(config)#exit
matt#
```

Save your work **(Important!)**

You can save your work to the file that is loaded when our router starts. Or you can save the work to TFTP server. Right now our changes are in a file called “running-configuration.” Here you can type in some changes and see if those changes have the desired effects. Let’s try to save it to TFTP sever.

```
Matt#copy running-configuration tftp://192.168.20.132/r45-1-matt-
run
```

Note: You should change the router and workstation name in command line according to the router that you are working with.

- 192.168.20.132 – IP address of the router you are working with;
- r45-1-matt-run: the file name that you want to save.

Restore your work

We can restore our work from the file that has been loaded to TFTP server.

Use *Window WordPad* to open the file ‘r45-1-matt-run‘, which is uploaded by you. Change the line ‘`hostname Matt`’ to the original name, let’s say ‘`hostname R45-1`’, save you change.

Let’s try to get it back to router from TFTP sever.

```
Matt#copy tftp://192.168.20.132/r45-1-matt-run run
```

Question: why ‘**run**’ instead of ‘**running-configuration”?**

With prompts?

One other type of prompt is called the “global mode prompt.” From here we make changes to various parts of the router. For example, when we want to configure an interface we first must be in the “interface global mode prompt.” I know, lots of jargon. It really makes more sense after you have done it a couple of times. Let’s look at the various types of global mode prompts and the sequence from the user mode prompt we took to get here (you do not have to type these in…just look at them):

Router	r45-1>**en** r45-1#**conf t** r45-1(config)#
Interface	r45-1(config)#**int ge0/0** r45-1(config-if)#
Sub-interface	r45-1(config)#**int ge0/0.1** r45-1(config-subif)#
Router	r45-1(config)#**router rip** r45-1(config-router)#
Console line	r45-1(config)#**line vty 0 4** r45-1(config-line)#

Your interface name and number can vary with your model. For example the 3900 routers use “ge0” for the first Ethernet. You can also use the show interface command (be sure you are not in config mode) too.

Other modes you may use include: controller, map-list, route-map, ipx router and map-class. Use your knowledge of help commands to figure out what those prompts would look like.

Supplemental Labs or Challenge Activity:

1. Try going through the initial configuration setup (put in yes instead of no). See how it differs. Its actually very nice but don’t get too attached to it. You will learn more by configuring your router using the command line interface (CLI).
2. What are the other options available with the copy command?
3. If your router is already started then how would you get the router setup script back?

So What Have I Learned Here?

In this lab you learned basic router steps including getting help. I guarantee you will be using the help function many more times during your training. In the next lab we will look a bit deeper into how the router boots. I actually had a lot of fun writing that one…there is some information in there you won’t find in any books or documentation anywhere.

User Mode Options

Command	Description

Privileged Model Options Router Boot Sequence

Command	Description

BASIC ROUTER CONFIGURATION

Objectives:

To learn a method for configuring basic router commands that you will use many times.

Background:

During your real work, you may be setting up many routers with many different router configurations. It is a good idea to learn to set up routers in "steps."

a. Step 1—start with setting up the "router basics"
b. Step 2—configure interfaces
c. Step 3—configure routing protocols
d. Step 4—add any other items (ACL's, security, routes, etc.)

In this lab you will learn about step 1: configuring the router's name, configuring vty lines, console lines, and setting up passwords. With Experiment #3-5, you shall learn how to configure interface, and routing protocol.

Tools and Materials:

Cisco router and Workstation

Step-by-Step Instructions:

1. Boot up the router and do not use the setup program. Oh sure, setup is easy, but you need to learn it

all from the command line. Enter the privileged mode:

```
Router>enable (or just “en”)

Router#
```

Since no enable password is set yet, the router does not ask for a password.

2. Enter configuration mode:

```
RouterA#configure (or just “config t”)
RouterA#terminal
RouterA(config)#
```

3.Configure the vty lines with a password “colab.” These are the available Telnet ports for use from the Internet or from other networking devices on your network. Without a password no one will be able to telnet into the router.

```
RouterA(config)#line vty 0 4
RouterA(config-line)#password colab
RouterA(config-line)#login
RouterA(config-line)#exit
```

4. Configure the console line so messages will not interrupt what you are typing and so your session does not time out:

```
RouterA(config)#line con 0
RouterA(config-line)#logging synchronous
RouterA(config-line)#exec-timeout 0 0
RouterA(config-line)#exit
```

Try to change **`exec-timeout` to 0 1.** This will cause your router session to time out every 1 second (it can take up to about 5 minutes to start though). There are only two ways to fix it: router recovery or press the “down” arrow key while you change the exec timeout to a higher number with your other hand at the same time. Doing this generates a continuous interrupt request to the CPU and the session, therefore, does not time out. Logging synchronous is a nice command. When you are configuring a router sometimes messages will interrupt your work. Without this command in your script when you are interrupted you will have to remember exactly what you typed when you were interrupted. With this command the router will “refresh” what you typed on the current line.

5. Configure the secret password “concis” and the enable password “class.” The enable secret password is used to get from user mode into privileged mode. The enable password is something that shows up from time to time on tests and whether you know how to configure it or not.

```
RouterA(config)#enable secret concis
RouterA(config)#enable password class
```

To see what you have done so far you can always look at the running-configuration file:
Once you have determined that your configuration is what you would like on your router you need to save it to your startup-configuration file. Otherwise if your router is re-booted or you loose power then your configuration will be lost.

```
RouterA(config)#exit (or use control+Z to get all the way out)
RouterA#sh ru (short for show run)
```

Now you know how to save your configuration.

So what if you made a mistake when you are typing something? Some things you can just re-type and they will be changed (like hostname) and some others you can un-do just by typing the word "no" and repeating the errant command.

```
RouterA(config)#hostname mark (darn! We wanted "r45-1")
Mark(config)#hostname r45-1 (just type in "r45-1")
r45-1(config)#

r45-1(config)#line vty 0 4
r45-1(config-line)#password csico (darn! We wanted "colab")
r45-1(config-line)#no password csico
r45-1(config-line)#password colab
```

Supplemental Lab or Challenge Activity:

When doing this, you generally do not want to abbreviate too many commands…it can really mess things up when you have an inaccurate command or forget to put an exit here or there. Practice makes perfect. For now you should probably forget about this little tip and just get used to typing all of this in by hand.

6. Configure the IP address on all of your router interfaces as it is defined in the above table. You need to do this in interface configuration mode as follows:

For Fast Ethernet (GigabitEthernet) interfaces:

```
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip address ip-address  subnet-mask
```

```
Router(config)#interface GigabitEthernet 0/1
Router(config-if)#ip address ip-address  subnet-mask
```

For serial interfaces:

```
Router(config)#interface serial 0/0/0
Router(config-if)#ip address ip-address  subnet-mask
Router(config)#interface serial 0/0/1
Router(config-if)#ip address ip-address  subnet-mask
```

So What Have You Learned Here?

In this lab you have learned how to set up the basics on a router. You will be using this information pretty much. After a while this will become automatic to you. In the next lab we will put this to use by learning about configuring router interface.

NETWORK DISCOVERY ON A ROUTER

Objective:

To learn how to configure a router IP interface and how to check the sub-networks on a router.

Step-By-Step Instructions:

1. Open HyperTerminal or Telnet to connect your router. You can find the router ip from the Table 1.
2. Enter Enable mode by using enable secret:

```
R25-1>enable
password>concis
r25-1#
```

3. Check the interface setting on router

```
R25-1#show ip interface
password#
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.20.67/28
  Broadcast address is 255.255.255.255
  Address determined by DHCP
  . . .
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.25.1/28
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory

  . . .
Serial0/0/0 is up, line protocol is up
  Internet address is 10.0.15.5/30
  Broadcast address is 255.255.255.255

. . .
Serial0/0/1 is up, line protocol is up
```

```
  Internet address is 10.0.15.9/30
  Broadcast address is 255.255.255.255

. . .
Loopback0 is up, line protocol is up
  Internet address is 192.168.18.5/30
  Broadcast address is 255.255.255.255
  Address determined by configuration file
```

Please record the ip setting on your router into the following table:

Router:________	GigabitEthernet0/0	
	GigabitEthernet0/1	
	Serial0/0/0	
	Serial0/0/1	

4. Check the routing tables and confirm your record again:

```
R25-1#show ip route
Codes: 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 i - IS-IS,
su - IS-IS summary, 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 192.168.20.65 to network 0.0.0.0

     192.168.25.0/28 is subnetted, 1 subnets
C       192.168.25.0 is directly connected, GigabitEthernet0/1

     192.168.20.0/28 is subnetted, 1 subnets
C       192.168.20.64 is directly connected, GigabitEthernet0/0

     10.0.0.0/30 is subnetted, 2 subnets
C       10.0.15.4 is directly connected, Serial0/0/0
C       10.0.15.8 is directly connected, Serial0/0/1

     192.168.18.0/30 is subnetted, 1 subnets
C       192.168.18.4 is directly connected, Loopback0

S*   0.0.0.0/0 [254/0] via 192.168.20.65
```

QUESTIONS:

Please Use Cisco Packet Tracer to draw a network diagram in the below frame for your router by using Cisco icons. On your diagram, try to show all subnets connected to your router by the different interface.

- Figure out how many ip addresses available for each sub-network.
- Find out which equipment are connected to your router from Table 1.

5. Configure ip interface on a router.

Here let’s change the ip setting on GigabitEthernet 0/1. Please input the following commands:

```
R25-1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R25-1(config)#in
R25-1(config)#interface fa
R25-1(config)#interface GigabitEthernet 0/1
R25-1(config-if)#ip address 192.168.25.X 255.255.255.0
R25-1(config-if)#^Z
R25-1#
```

Once press ‘Ctrl+z’, you are out configuration mode. Please use the “show ip interface” to check your new configuration.

STATIC ROUTING

Objective:

To learn how to use static routing on a router.

Background:

In this lab you will be presented how to configure the static routing tables.

Step-By-Step Instructions:

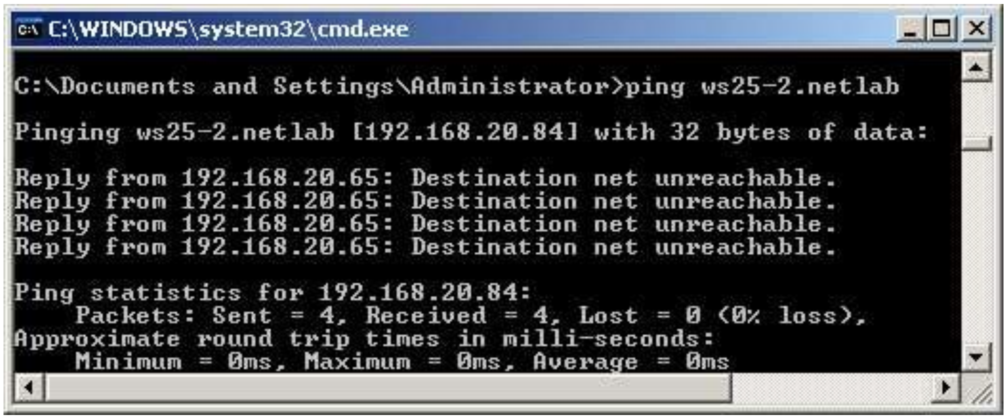
1. If you are already connecting a router, skip this step. Otherwise open HyperTerminal or Telnet to connect your router. You can find the router ip from the Table 1.
2. Enter Enable mode by using enable secret.
3. Try to reach other router (your neighbors) by ping: You can try to ping all routers **r25-1/2/3/4** and **r45-1/2/3/4**, including yourself, see what happens.

```
R25-1#ping r25-2
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.20.83, timeout is 2
seconds:
U.U.U
```

```
Success rate is 0 percent (0/5)
```

Try to reach other workstation by ping: You can try to ping all workstation '**ws25-1/2/3/4.netlab**' and '**ws45-1/2/3/4.netlab**', including yourself, see what happens.



C:\WINDOWS\system32\cmd.exe

```
C:\Documents and Settings\Administrator>ping ws25-2.netlab

Pinging ws25-2.netlab [192.168.20.84] with 32 bytes of data:

Reply from 192.168.20.65: Destination net unreachable.
Reply from 192.168.20.65: Destination net unreachable.
Reply from 192.168.20.65: Destination net unreachable.
Reply from 192.168.20.65: Destination net unreachable.

Ping statistics for 192.168.20.84:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

4. Check your routing table by the command "show ip route". You should get the similar message as the following:

```
R25-1#show ip route
Gateway of last resort is 192.168.20.65 to network 0.0.0.0

     192.168.25.0/28 is subnetted, 1 subnets
C       192.168.25.0 is directly connected, GigabitEthernet0/1

     192.168.20.0/28 is subnetted, 1 subnets
C       192.168.20.64 is directly connected, GigabitEthernet0/0

     10.0.0.0/30 is subnetted, 2 subnets
C       10.0.15.4 is directly connected, Serial0/0/0
C       10.0.15.8 is directly connected, Serial0/0/1

     192.168.18.0/30 is subnetted, 1 subnets
C       192.168.18.4 is directly connected, Loopback0
```

Questions:

- How many routers/workstations can you reach?
- How many routes are connected to your router directly? (You get this from last lab).
- Why can't your router reach the directly-connected routers?
- If the ping packet doesn't reach its destination, where does it go on a router?

Find neighbors.

First at all, let's find which routes are connected, use the following commands:

```
R45-1#show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID  Local Intrfce   Holdtme   Capability  Platform  Port
ID

R25-3        Gig 0/1        139      R S       3925      Gig 0/1
R45-2        Ser 0/1        131      R S       3945      Ser 0/0/0
R45-1        Ser 0/0        134      R S       3945      Ser 0/0/0
R25-2.netlab Gig 0/1        127      R S       3925      Gig 0/1
```

List sub-networks which you want to reach

According the above commands and Table 1, fill in the following table. You may have to ask the other groups to get their gateway ip.

R/WS	IP address	Mask	Gateway	Connected(y/n)
R25-1/WS25-1				
R25-2/WS25-2				
R25-3/WS25-3				
R25-4/WS25-4				
R45-1/WS45-1				
R45-2/WS45-2				
R45-3/WS45-3				
R45-4/WS45-4				

Configure static routing table

In this step, we will try to set the static routing table by using the command ‘ip route’ that takes three parameters: the network address that you want to reach, the subnet mask, and your interface used to reach that network.

GigabitEthernet0/1

```
R25-1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R25-1(config)#ip route 192.168.20.xx 255.255.255.240
GigabitEthernet 0/1
R25-1(config)#ip route 192.168.20.xx 255.255.255.240
GigabitEthernet 0/1
R25-1(config)#^Z
```

If you have known the next hop ip (your neighbor’s gateway ip), you also can use the following command:

```
R25-1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
R25-1(config)#ip route 192.168.20.xx 255.255.255.240 192.168.25.x
R25-1(config)#ip route 192.168.20.xx 255.255.255.240 192.168.25.x
R25-1(config)#^Z
```

You may have to modify the ip according your router settings.

Serial0/0/0

```
R25-1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R25-1(config)#ip route 192.168.20.xx 255.255.255.240 10.0.15.x
R25-1(config)#^Z
```

Or

```
R25-1(config)#ip route 192.168.20.128 255.255.255.240 serial
0/0/0
```

Serial0/0/1

```
R25-1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R25-1(config)#ip route 192.168.20.xx 255.255.255.240 10.0.15.X
R25-1(config)#^Z
```

Or

```
R25-1(config)#ip route 192.168.20.xx 255.255.255.240 serial 0/0/1
```

Check routing table:

Use the command ‘show ip route”, you can check your static routing table, the similar message is shown as the bellows:

```
     192.168.25.0/28 is subnetted, 1 subnets
C       192.168.25.0 is directly connected, GigabitEthernet0/1
     192.168.20.0/28 is subnetted, 5 subnets
S       192.168.20.96 [1/0] via 192.168.25.3
S       192.168.20.80 [1/0] via 192.168.25.2
C       192.168.20.64 is directly connected, GigabitEthernet0/0
S       192.168.20.144 [1/0] via 10.0.15.10
S       192.168.20.128 [1/0] via 10.0.15.8
                       [1/0] via 10.0.15.6
     10.0.0.0/30 is subnetted, 2 subnets
C       10.0.15.4 is directly connected, Serial0/0/0
C       10.0.15.8 is directly connected, Serial0/0/1
     192.168.18.0/30 is subnetted, 1 subnets
C       192.168.18.4 is directly connected, Loopback0
```

Ping the neighbor routers and workstations as Step 3. See how many of them can you reach.
Configure the default gateway:

In Network Lab, all the servers are set in a VLAN 192.168.20.16/28. If your router wants to talk with a server, how does the router forward the packets? The same question is how to connect those networks that are not in lab?

The answer is to setup a default gateway on your router. Once the destination IP of an IP package is not in routing list, this packet shall be forwarded to the default gateway. Now let's configure the default gateway on your router.

```
R25-1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R25-1(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.XX
R25-1(config)#^Z
```

Table 3: Default Gateways on Routers

Router	Default Gateway
R25-1	192.168.20.65
R25-2	192.168.20.81
R25-3	192.168.20.97
R25-4	192.168.20.113
R45-1	192.168.20.129
R45-2	192.168.20.145
R45-3	192.168.20.161
R45-4	192.168.20.177

Check the setting of the default gateway by the command 'show ip route' , you may find the following message:

```
Gateway of last resort is 192.168.20.65 to network 0.0.0.0
```

Try to ping the servers on router:

```
Ping 192.168.20.18
ping 192.168.20.19
```

Try to ping and trace the servers on workstation:

```
ping 192.168.20.18
tracert 192.168.20.19
tracert 216.239.37.99
```

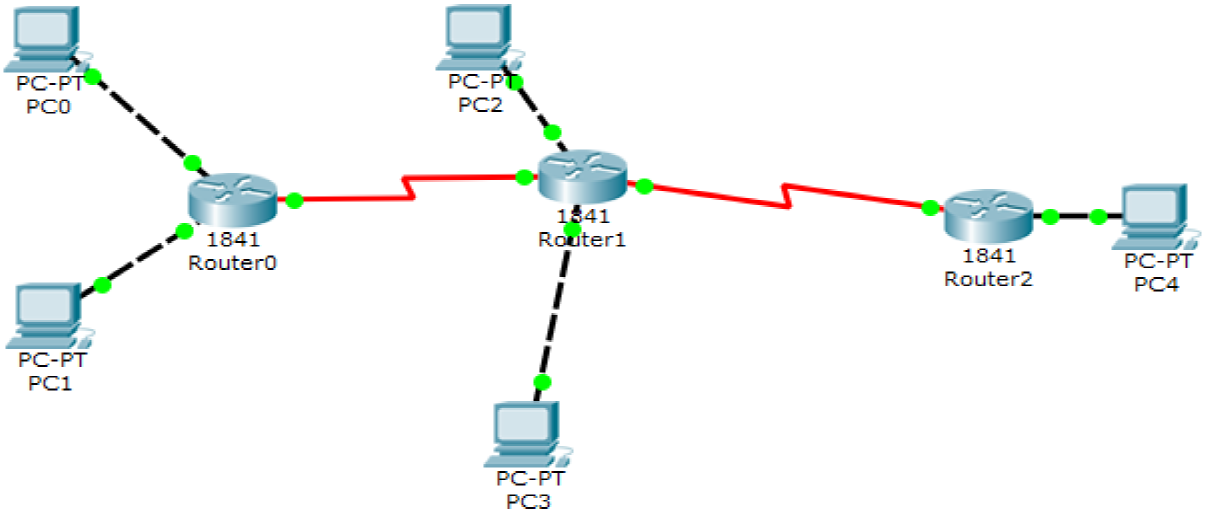
Question:

- Please list some advantage and disadvantage of Static Routing

POST-LAB

Do the following task(s) and take a snapshot for each part and include it in your report.

1. Configure the IP address on all interfaces of each router as in the following diagram and tables.
2. Configure static routing on the network by using the commands applied in the lab.
3. Show the routing table of each router.
4. Ping all the workstations of your network.



Router	Interface	IP Address	Subnet Mask
Router0	GE 0/0	1.168.0.1	255.0.0.0
	GE 0/1	128.168.0.1	255.255.0.0
	S0/0/0	10.0.0.1	255.0.0.0
Router1	GE 0/0	192.168.0.1	255.255.255.0
	GE 0/1	126.168.1.1	255.0.0.0
	S0/0/0	10.0.0.2	255.0.0.0
	S0/0/1	128.0.0.1	255.255.0.0
Router2	GE 0/0	191.168.1.1	255.255.0.0
	S0/0/0	128.0.0.3	255.255.0.0

WorkStation	IP Address	Subnet Mask	Gateway
PC0	1.168.0.2	255.0.0.0	1.168.0.1
PC1	128.168.0.2	255.255.0.0	128.168.0.1
PC2	192.168.0.2	255.255.255.0	192.168.0.1
PC3	126.168.1.2	255.0.0.0	126.168.1.1
PC4	191.168.1.2	255.255.0.0	191.168.1.1

EXPERIMENT #3: ADVANCED ROUTING AND MONITORING

ROUTING PROTOCOL – RIP AND OSPF

Objective

Complete the following lab experiment to review basic router configurations and learn the network lab topology. You will complete the following tasks:

- Configuring the routers with a basic configuration by using the RIP routing protocol.
- Verifying lab connectivity and network topology.
- Understanding OSPF routing protocol.
- Comparing OSPF & RIP.
- Implementing OSPF on the routers.
- Overview & Using of SolarWinds software.

Command List

You can find the required commands in each step.

PRELAB

After reading the whole experiment, do the following and take a snapshot for each part:

1. Fill in Table showed in Task A step 7 by finding the classful address and the subnet address.
2. Open the Packet Tracer and use the saved network topology to configure the IP address on all your routers interfaces as in the following table.
3. Apply the RIP v2 routing protocol on each router by following the steps explained in the experiment.

<u>Task A: Basic Router Configuration</u>

Step 1 Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to “Router#”.

```
Router>enable
Password:concis
Router#
```

Step 2 Execute the following command in global configuration mode:

```
Router#config t
Router(config)#no ip domain-lookup
Router(config)#end
```

This command prevents your router from taking a mistaken command as a host/network name.

Step 3 Configure the serial interface bandwidth as 64 Kbps. As you know, clock rate can only be set on DCE interfaces.

For Serial 0/0/0

```
Router#config t
Router(config)#interface serial0/0/0
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
Router(config-if)#^z
```

For Serial 0/0/1

```
Router#config t
Router(config)#interface serial0/0/1
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
Router(config-if)#^z
```

Questions:

- What is the serial interface used for in data communications?
- What do DTE and DCE stand for? Why should we only setup clock rate and bandwidth on DCE?
- What is the clock rate command for? Bandwidth command is used to define the interface bandwidth for routing protocols that use bandwidth as a route metric. ex. OSPF routing protocol.

Step 4 Determine the Serial cable types attached to your router by executing the following command.

```
Router#show controller serial0/0/0
Router#show controller serial0/0/1
```

- What are the cable types connected to Serial0/0/0 and Serial0/0/1 of your router? …………………………………………………………
- What is the interface clock rate? ……………………………………

Step 5 Execute the following command to check the serial interface specification.

```
Router#show interface serial0/0/0
Router#show interface serial0/0/1
```

Step 6 Check the Ethernet interfaces on your router.

```
Router#show interface GigabitEthernet0/0
Router#show interface GigabitEthernet0/1
```

Set or verify that the Ethernet interfaces are “up” on physical and data link layers.

Verify the Ethernet interface types. It is …………………….

Verify the Ethernet interface speed. It is ……………………..

Verify the Queuing strategy. It is ………………

Step 7 Using the given IP address and subnet mask; determine the class-full network address and subnet address. Write them in the following table.

Router	Interface	IP Address	Subnet Mask	Classfull Address	Subnet Address
R25-1	GigabitEthernet 0/0	192.168.20.67	255.255.255.240		
	GigabitEthernet 0/1	192.168.25.1	255.255.255.240		
	S0/0/0	10.0.15.5	255.255.255.252		
	S0/0/1	10.0.15.9	255.255.255.252		
	Loopback0/0	192.168.18.5	255.255.255.252		
R25-2	GigabitEthernet 0/0	192.168.20.83	255.255.255.240		
	GigabitEthernet 0/1	192.168.25.2	255.255.255.240		
	S0/0/0	10.0.15.17	255.255.255.252		
	S0/0/1	10.0.15.14	255.255.255.252		
	Loopback0/0	192.168.18.13	255.255.255.252		
R25-3	GigabitEthernet 0/0	192.168.20.99	255.255.255.240		
	GigabitEthernet 0/1	192.168.25.3	255.255.255.240		
	S0/0/0	10.0.15.22	255.255.255.252		
	S0/0/1	10.0.15.25	255.255.255.252		
	Loopack0/0	192.168.18.17	255.255.255.252		
R25-4	GigabitEthernet 0/0	192.168.20.115	255.255.255.240		
	GigabitEthernet 0/1	192.168.25.4	255.255.255.240		
	S0/0/0	10.0.15.33	255.255.255.252		
	S0/0/1	10.0.15.30	255.255.255.252		
	Loopack0/0	192.168.18.29	255.255.255.252		
R45-1	GigabitEthernet 0/0	192.168.20.131	255.255.255.240		
	GigabitEthernet 0/1	192.168.45.1	255.255.255.240		
	S0/0/0	10.0.15.29[6]	255.255.255.252		
	S0/0/1	10.0.15.13	255.255.255.252		
	Loopack0/0	192.168.18.9	255.255.255.252		
R45-2	GigabitEthernet 0/0	192.168.20.147	255.255.255.240		
	GigabitEthernet 0/1	192.168.45.2	255.255.255.240		
	S0/0/0	10.0.15.10	255.255.255.252		
	S0/0/1	10.0.15.26	255.255.255.252		
	Loopack0/0	192.168.18.21	255.255.255.252		
R45-3	GigabitEthernet 0/0	192.168.20.163	255.255.255.240		
	GigabitEthernet 0/1	192.168.45.3	255.255.255.240		
	S0/0/0	10.0.15.21	255.255.255.252		
	S0/0/1	10.0.15.18	255.255.255.252		
	Loopack0/0	192.168.18.25	255.255.255.252		
R45-4	GigabitEthernet 0/0	192.168.20.179	255.255.255.240		

	GigabitEthernet 0/1	192.168.45.4	255.255.255.240		
	S0/0/0	10.0.15.34	255.255.255.252		
	S0/0/1	10.0.15.6	255.255.255.252		
	Loopack0/0	192.168.18.33	255.255.255.252		

Step 8 Configure the IP address on all of your router interfaces as it is defined in the above table. You need to do this in interface configuration mode as follows:

For Fast Ethernet interfaces:

USE THE ABOVE TABLE IN ORDER TO FIND YOUR CORRESPONDING IP-ADDRESS AND SUBNET MASK AND REPLACE THEM IN THE FOLLOWING UNDERLINED COMMANDS.

```
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip address ip-address  subnet-mask
```

```
Router(config)#interface GigabitEthernet 0/1
Router(config-if)#ip address ip-address  subnet-mask
```

For serial interfaces:

```
Router(config)#interface serial 0/0/0
Router(config-if)#ip address ip-address  subnet-mask
```

```
Router(config)#interface serial 0/0/1
Router(config-if)#ip address ip-address  subnet-mask
```

Task B: Check router connectivity and network topology

Step 1 Using the Cisco Discovery Protocol (CDP) verify that your router can see all its connected neighbors. This is a data link layer protocol that provides information about all the neighbor routers.

```
Router#show cdp neighbors detail
```

Fill in the table below using the CDP command output. (Ask other groups about their router connectivity to fill up the table).

From R25-1:	
Device ID	Local Interface

From R25-2:	
Device ID	Local Interface
From R25-3:	
Device ID	Local Interface
From R25-4:	
Device ID	Local Interface
From R45-1:	
Device ID	Local Interface
From R45-2:	
Device ID	Local Interface
From R45-3:	
Device ID	Local Interface
From R45-4:	
Device ID	Local Interface

Step-2 Draw the network diagram clearly in your report. On the diagram, identify the router names, interfaces, host computers connected to the GigabitEthernet interfaces and the IP address of each interface.

Task C: Enable RIP routing

Step 1 Enable RIP routing in your router by using the following commands and substituting the *network address* with class C address that you obtained in step 7 of Task A.

```
Router(config)# ip routing

Router(config)#router rip
Router(config)#version 2
Router(config-router)#network classfull-network-address
Router(config)#no auto-summary
```

Task D: Verify the routing table

Step 1 Display the routing table and verify that you have valid routes and connectivity to all the other routers in the network. Use the following command:

```
Router#show ip route
```

Step 2 Make sure that you can successfully ping all of the other routers in your network by pinging their Loopback IP address. Ex. Ping 192.168.18.5

Step 3 Examine the routing table of your router and answer the following questions:

```
Router#show ip route rip
```

What are the routes to each of the following networks and how many hops are they away?

192.168.20.64 via router/s ……………………and ………….hops away.
192.168.20.80 via router/s ……………………and ………….hops away.
192.168.20.96 via router/s ……………………and ………….hops away.
192.168.20.112 via router/s ……………………and ………….hops away.
192.168.20.128 via router/s ……………………and ………….hops away.
192.168.20.144 via router/s ……………………and ………….hops away.
192.168.20.160 via router/s ……………………and ………….hops away.
192.168.20.176 via router/s ……………………and ………….hops away.

By comparing the routing table with network topology, discuss the algorithm that RIP is using to find out the network topology and if it is finding the optimized routes in your network.

- What information does your router have about network 192.168.45.0? Is this information correct?

- What information does your router have about the Loopback interface of other routers? Is this information correct?

Step 4 Issue the following command to capture RIP routing updates.

```
Router(config)#logging console debugging
Router#debug ip rip events
```

Check the routing updates sent by your router through its interfaces:

- What is/are the destination address/es of these updates? What does it mean?
- How long it takes for the router to send two consecutive updates via interface S0/0?

Step 5 Save the current configuration of your router and exit.

```
Router#copy running-config startup-config
Router(config)# no logging console debugging
Router#no debug all
Router#disable
```

<u>Command List</u>

In this lab experiment, you used the following commands. Use this list if necessary for configuration command assistance.

Command	Description
Show hostname	View router’s hostname
Show controllers s0/x GigabitEthernet 0/x	View the interface physical specification.
Show interface s0/x GigabitEthernet 0/x	View the interface specifications in both physical and datalink layers.
Interface s0/x GigabitEthernet 0/x	Executed in global configuration mode. Enter the interface configuration mode.
ip address ip-address subnet-mask	Executed in interface configuration mode. It defines the interface ip address.
Show cdp neighbor	It verifies the neighboring router specification.
Ip routing	Enable ip routing
Router rip	Executed in global configuration mode. Enable rip routing.
Network classful-network-address	Executed in router configuration mode. Define the networks participating in routing process.
ip host name ip-address	Define an ip host list in your router.
Show ip route	View the routing table.
Show ip route rip	View the rip routes in your routing table.

UNDERSTANDING OSPF

OSPF Introduction

- OSPF was developed by the internet community to answer the need to a highly functional and non-proprietary Internal Gateway Protocol (IGP) for TCP/IP.
- Some Differences between OSPF with RIP:
- The rapid expansion of networks has pushed RIP to its limits. There are some limitations in RIP that can cause problems in large networks. Some of them are mentioned here:
- RIP has a limit of 15 hops. A RIP network that spans more than 15 hops (15 routers) is considered unreachable.
- Periodic broadcasts of the full routing table will consume a large amount of bandwidth. This is a major problem with large networks especially on slow links and WAN clouds.
- RIP converges slower than OSPF. In large networks convergence gets to be in the order of minutes. Slow convergence is inappropriate in large environments and could cause routing inconsistencies.
- RIP networks are flat networks. There is no concept of areas or boundaries.
- OSPF, on the other hand, addresses most of the issues presented above:
- With OSPF, there is no limitation on the hop count.

Comparing OSPF with RIP

The rapid expansion of networks has pushed RIP to its limits. There are some limitations in RIP that can cause problems in large networks. Some of them are mentioned here:

- RIP has a limit of 15 hops. A RIP network that spans more than 15 hops (15 routers) is considered unreachable.
- Periodic broadcasts of the full routing table will consume a large amount of bandwidth. This is a major problem with large networks especially on slow links and WAN clouds.
- RIP converges slower than OSPF. In large networks convergence gets to be in the order of minutes. Slow convergence is inappropriate in large environments and could cause routing inconsistencies.
- RIP has no concept of network delays and link costs. Routing decisions are based on hop counts. The path with the lowest hop count to the destination is always preferred even if the longer path has a better aggregate link bandwidth.
- RIP networks are flat networks. There is no concept of areas or boundaries.

OSPF CONFIGURATION

Complete the following lab experiment to review and configure OSPF in a single area network.

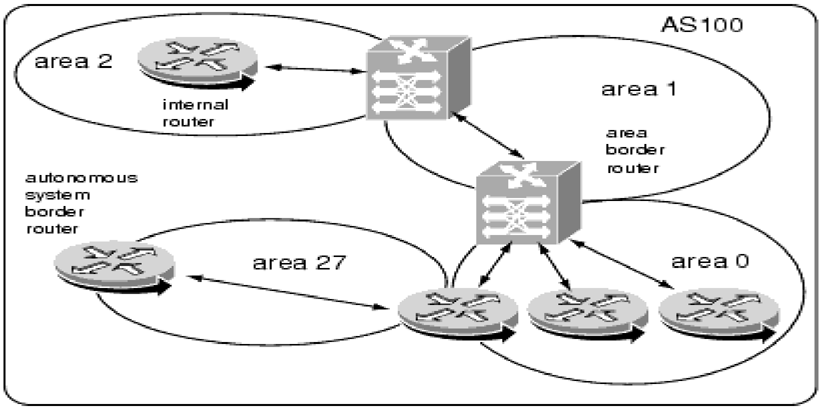


Figure 0.1: OSPF configuration

In this experiment, students will work in the following groups:

- ✓ Group 1: R25-1 & R45-1
- ✓ Group 2: R25-2 & R45-2
- ✓ Group 3: R25-3 & R45-3
- ✓ Group 4: R25-4 & R45-4

OSPF was developed by the internet community to answer the need to a highly functional and non-proprietary Internal Gateway Protocol (IGP) for TCP/IP. OSPF is a link-state routing protocol, which is different from the Bellman-Ford vector based algorithm used in RIP.

First execute the following commands:

```
Rx-x>enable
   Password: concis
Rx-x#
Rx-x#configure terminal
Rx-x(config)#no ip domain-lookup
Rx-x(config)#end
```

(Note: The command ‘no ip domain-lookup’ prevents your router from taking a mistaken command as a host/network name)

Step 1: Remove RIP routing by using the following command in global configuration mode:

```
Rx-x#configure terminal
```

OR

```
Rx-x#conf t
Rx-x(config)#no router rip
```

Step 2: Check all the network addresses connected to your router along with their subnet mask

And write them in the following table. You can use the following command:

```
Rx-x# show interfaces
```

Define the OSPF mask for each network as it was discussed in introduction section and write it in the following table. (OSPF mask is the 1's complement of the subnet mask *).

Network Address/Subnet Address	OSPF Mask

(*The **mask** contains wild card bits where 0 is a match and 1 is a "do not care" bit, e.g. 0.0.255.255 indicates a match in the first two bytes of the network number. You can consider the mask as the inverse of subnet mask while you add a specific network to OSPF routing process.)

Step 3: Enable OSPF with process ID 1 on your router by using the following commands:

```
Rx-x(config)#ip routing
Rx-x(config)#router ospf 1
```

（*The OSPF process-id is a numeric value local to the router. It does not have to match process-ids on other routers.)

Step 4: Use the network address and OSPF masks from the table you completed in Step 2. Introduce each of them to OSPF by using the following command. You need to use the addresses you calculated in Experiment 4.

```
Rx-x(config-router)#network subnet-address OSPF-mask area 0
```

(ex: network 192.168.20.64 0.0.0.15 area 0)

With this command, you also put the interfaces in the backbone area which is "area 0".

Note: The area-id is the area number that you want the interface to be in. The area-id can be an integer between 0 and 4294967295 or can take a form similar to an IP address A.B.C.D. In an OSPF network, an area 0 must exist and it works as the backbone area. Other areas can be added while needed and they should be directly connected to area 0.

Step 5 Display the routing table and verify that you have full connectivity within the network. Make sure that you can successfully ping all of the other routers Loopback addresses within the network. You can use the following command:

```
Rx-x#show ip route ospf
```

Step 6 Examine the routing table:

What is OSPF routing metric based on? …………………………………….

Which interface your router uses to send traffic to each of the following networks?

Network	Interface
192.168.20.64/28	
192.168.20.80/28	
192.168.20.96/28	
192.168.20.112/28	
192.168.20.128/28	
192.168.20.144/28	
192.168.20.160/28	
192.168.20.176/28	
192.168.45.0/28	
192.168.25.0/28	
10.0.15.4/30	
10.0.15.8/30	
10.0.15.12/30	
10.0.15.16/30	
10.0.15.20/30	
10.0.15.24/30	
10.0.15.28/30	
10.0.15.32/30	
192.168.18.4/30	
192.168.18.8/30	
192.168.18.12/30	
192.168.18.16/30	
192.168.18.20/30	
192.168.18.24/30	
192.168.18.28/30	
192.168.18.32/30	

Verify the routing table for load balanced routes and write them in the following table. Does OSPF load balance by default?

____

____

____

Step 7 Make sure that you have finished the entire configuration in previous steps and save the current configuration of your router to NVRAM by using the following command:

```
Rx-x#copy running-config startup-config
```

Network Performance Measurement Tool - SolarWinds

SolarWinds, has an array of IT management, monitoring, and discovery tools to measure network performance and capabilities. **SolarWinds VoIP and Network Quality Manager** used as an IP SLA network monitoring solution that can provide different Voice over IP network measurements. In this lab we will use this package to monitor and measure network performance parameter of real time traffic and test the traffic discrimination technique effect on the network performance.

Internet Protocol Service Level Agreement (IP SLA) technology offers a cost-effective and efficient response to the needs of enterprises of all sizes. SolarWinds VoIP and Network Quality Manager collect IP SLA-specific data and provide presentation tools that enable IP SLA network monitoring and real-time status reporting. IP SLA operations provide immediate insight into network **Quality of Service (QoS)**, including ***packet loss***, ***latency***, ***jitter***, and ***mean opinion score (MOS)*** metrics. VoIP and Network Quality Manager deploys **Cisco IP SLA operations** to generate various types of network traffic including DNS requests, DHCP IP allocation, FTP and HTTP requests, TCP connect, ICMP and UDP Echo, and simulated VoIP traffic between devices on your network using the jitter codec you specify. Cisco IP SLAs provide real-time and historical performance statistics that VoIP and Network Quality Manager presents in the readily customizable Web Console.

By using SolarWinds, measure the network performance as following:

- Open the chrome explorer fill into the URL http://192.168.20.21, a username and password will requested use your Router name in small letter for both, for example username: r25-1 password:r25-1.
- Click the VoIP & Network Quality tab in the Modules menu bar, and then click VoIP & Quality Settings at the top right of the view.
- Under ALL IP SLA Operations, you will find the running operation of network performance, export the measure performance for your router based on the below table.

Router Name	Type of Traffic1	Type of Traffic2	Type of Traffic3
R25-1	VoIP(R25-1, R25-2) Voice(16400), Video(50505)	FTP (R25-1, 192.168.20.132)	UDP Ehco(R25-1, R25-2)
R25-2	VoIP(R25-2, R25-3) Voice(16400), Video(50505)	FTP (R25-2, 192.168.20.148)	UDP Ehco (R25-2, R25-3)
R25-3	VoIP(R25-3, R25-4) Voice(16400), Video(50505)	FTP (R25-3, 192.168.20.164)	UDP Ehco (R25-3, R25-4)
R25-4	VoIP(R25-4, R25-1) Voice(16400), Video(50505)	FTP (R25-4, 192.168.20.180)	UDP Ehco (R25-4, R25-1)
R45-1	VoIP(R25-2, R25-1) Voice(16400), Video(50505)	FTP (R25-1, 192.168.20.132)	UDP Ehco (R25-1, R25-2)
R45-2	VoIP(R25-3, R25-2) Voice(16400), Video(50505)	FTP (R25-2, 192.168.20.148)	UDP Ehco (R25-2, R25-3)
R45-3	VoIP(R25-4, R25-3) Voice(16400), Video(50505)	FTP (R25-3, 192.168.20.164)	UDP Ehco (R25-3, R25-4)
R45-4	VoIP(R25-1, R25-4) Voice(16400), Video(50505)	FTP (R25-4, 192.168.20.180)	UDP Ehco (R25-4, R25-1)

The operations are configured as following information:

	Parameters					
	Round Trip Time Thresholds					

Operation traffic type	Warning	Critical	Maximum	freq	Codec	MOS	Jitter Threshold	Port number
ICMP (UDP Echo)	500ms	1000ms	1500ms	300s	-	-	-	7
FTP	5000ms	6000ms	8000ms	300s	-	-	-	21,20
VoIP voice	1000ms	2000ms	3000ms	300s	GSM 729A	3.75, 3.5	30,50,100ms	16400
VoIP video	1000ms	2000ms	3000ms	300s	GSM 711ULAW	3.75, 3.5	30,50,100ms	50505

Note: indicate the MOS how voice is accepted.

What is the average round trip latency for five consecutive ftp requests?
How much is the average source to destination jitter for voice traffic in a period of 5 minutes?
How much is the destination to source jitter for voice traffic in a period of 5 minutes? Do you see much variance in voice jitter during a long period of time? Why?

How much is the average round trip latency for voice traffic in a period of 5 minutes?
How much is the average error occurrence in a period of 5 minutes?

COMPLETION CRITERIA

At the end of this lab,

- All the classroom routers should have full connectivity to each other and you should be able to ping all the existing interfaces on routers.
- All the classroom routers should have full connectivity by using the OSPF protocol and you should be able to ping all the loopback interfaces. You should have defined different traffic types in SolarWinds and measured the network performance including round trip delay and jitter for the corresponding traffic type.

POST-LAB

Do the following task(s) and take a snapshot for each part and include it in your report.

1. Open the Packet Tracer and use the saved network topology.
2. Configure OSPF on the network by using the commands applied in the lab.
3. Show the routing table of each router.
4. Ping all the workstations of your network.

EXPERIMENT #4: NETWORK PERFORMANCE

INTRODUCTION

Network performance refers to measures of service quality of a telecommunications product as seen by the customer. The following measures are often considered important:

- Bandwidth commonly measured in bits/second is the maximum rate that information can be transferred
- Throughput the actual rate that information is transferred
- Latency the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses
- Jitter variation in the time of arrival at the receiver of the information
- Error rate the number of corrupted bits expressed as a percentage or fraction of the total sent

However, throughput, latency, the type of information transmitted, and the way that information is applied all affect the perceived speed of a connection.

Priority Queuing (PQ)

Priority Queuing allows you to prioritize traffic in a network. You can have a maximum of four traffic priorities. Packet filters can be identified to classify traffic and put them in each relevant queue. The queue with the highest priority will be served first until it is empty, then the lower priority queues are served in sequence.

PQ gives a high priority queue absolute preferential over lower priority queues; important traffic in the highest priority queue have precedence over traffic in the lower priority queues. Packets are classified based on user-specified criteria like source/destination address and TCP/UDP port number. Each packet will be placed in one of the four priority output queues, high, medium, normal and low based on the assigned priority. Packets that are not classified by priority get into the normal queue. Figure 1 illustrates this process:

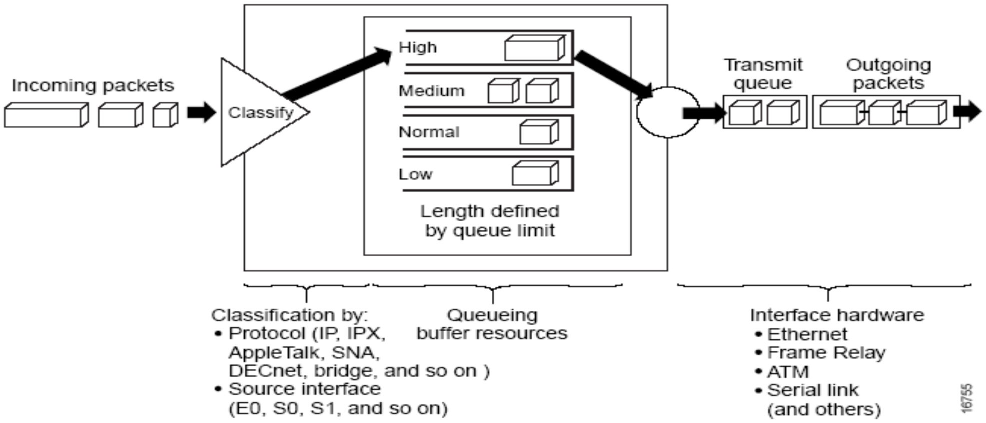

Incoming packets
Classify
High
Medium
Normal
Low
Length defined by queue limit
Transmit queue
Outgoing packets
Classification by:
• Protocol (IP, IPX, AppleTalk, SNA, DECnet, bridge, and so on)
• Source interface (E0, S0, S1, and so on)
Queueing buffer resources
Interface hardware
• Ethernet
• Frame Relay
• ATM
• Serial link (and others)
16755

Figure 1: Priority Queuing

Priority queues on an interface are scanned for packets in descending order of priority. The packets in the highest priority queue are chosen first for transmission, then the packets in the lower priority queue and so on. This procedure is repeated every time a packet is to be sent. The maximum length of a queue is defined by the length limit. When a queue is longer than the queue limit, all additional packets are dropped.

Packet Classification for Priority Queuing

A priority list identifies the rules that describe how packets should be assigned to one of the four priority queues. A default priority queue or queue size limits can also be identified. Protocol type, incoming interface, packet size, fragments and access list can classify packets.

Why Use Priority Queuing?

PQ provides absolute preferential treatment to high priority traffic, ensuring that mission-critical traffic receives priority treatment. In addition, PQ provides a faster response time than other queuing methods. Although you can enable priority output queuing for any interface, it is best used for low-bandwidth, congested serial interfaces.

Restrictions on using PQ

When choosing to use PQ, consider that because lower priority traffic is often denied bandwidth in favor of higher priority traffic, use of PQ could, in the worst case, result in lower priority traffic never being sent.

Weighted Round Robin scheduling as Custom Queuing

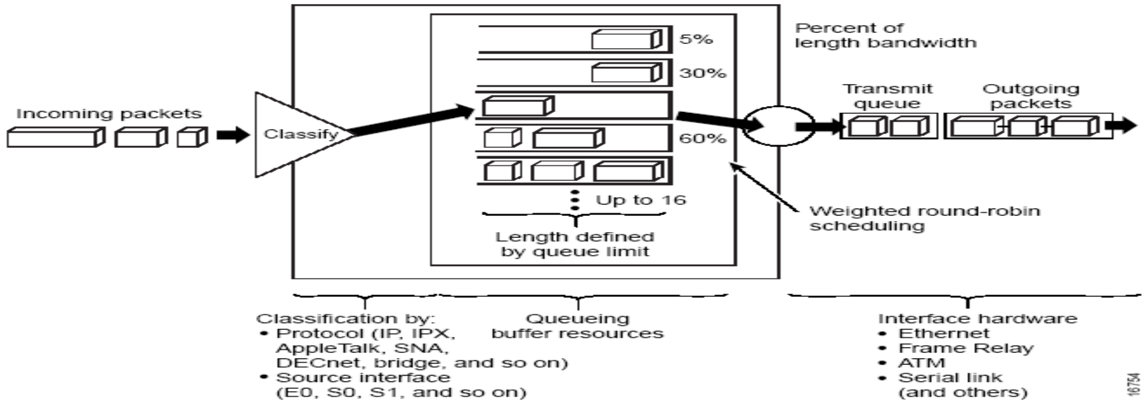
Custom Queuing allows you to define a certain number of bytes to be transferred from a queue each time the queue is serviced. Queues are serviced on a round robin basis. This allows you to share bandwidth among applications.

How Custom Queue Works

Custom Queue handles traffic by specifying the number of packets or bytes being served for each queue. It services queues by cycling through them in round robin fashion, sending the portion of bandwidth allocated to each queue before moving to the next queue. The byte count or bandwidth assigned to each queue can be seen as weight. If a queue is empty, router will send packets from the next queue which contains packets. When CQ is enabled on an interface, the system maintains 17 output queues for that interface. You can specify queues 1 through 16. Associated with each output queue is a configurable byte count, which specifies how many bytes of data the system should deliver from the current queue before it moves on to the next queue.

Queue number 0 is the system queue; it is emptied before any of the queues numbered 1 through 16 are processed. The system queue serves high priority packets, such as signaling packets. Other traffic cannot be configured to use this queue. For queue numbers 1 through 16, the system cycles through the queues sequentially (in a round-robin fashion), transmitting the configured byte count from each queue in each cycle and moving on to the next one. When a particular queue is being processed, packets are sent until the number of bytes sent exceeds the queue byte count or the queue is empty. Bandwidth used by a particular queue can be indirectly specified only in terms of byte count and queue length.

The following figure shows how CQ works:


Incoming packets
Classify
5%
30%
60%
Up to 16
Length defined by queue limit
Percent of length bandwidth
Transmit queue
Outgoing packets
Weighted round-robin scheduling
Classification by:
• Protocol (IP, IPX, AppleTalk, SNA, DECnet, bridge, and so on)
• Source interface (E0, S0, S1, and so on)
Queueing buffer resources
Interface hardware
• Ethernet
• Frame Relay
• ATM
• Serial link (and others)
16754

CQ ensures that no application or specified group of applications achieves more than a predetermined proportion of overall capacity when the line is under stress. Like PQ, CQ is statically configured and does not automatically adapt to changing network conditions.

What is Byte Count?

The router sends packets from a particular queue until the byte count is exceeded. Once the byte count value is exceeded, the packet that is currently being sent will be completely sent. Therefore, if you set the byte count to 100 bytes and the packet size of your protocol is 1024 bytes, then every time this queue is serviced, 1024 bytes will be sent, not 100 bytes.

For example, suppose one protocol has 500-byte packets, another has 300-byte packets, and a third has 100-byte packets. If you want to split the bandwidth evenly across all three protocols, you might choose to specify byte counts of 200, 200, and 200 for each queue. However, this configuration does not result in a 33/33/33 ratio. When the router services the first queue, it sends a single 500-byte packet; when it services the second queue, it sends a 300-byte packet; and when it services the third queue, it sends two 100-byte packets. The effective ratio is 50/30/20.

Thus, setting the byte count too low can result in an unintended bandwidth allocation. However, very large byte counts will produce a “jerky” distribution. That is, if you assign 10 KB, 10 KB, and 10 KB to three queues in the example given, each protocol is serviced promptly when its queue is the one being serviced, but it may be a long time before the queue is serviced again. A better solution is to specify 500-byte, 600-byte, and 500-byte counts for the queue. This configuration results in a ratio of 31/38/31, which may be acceptable.

In order to service queues in a timely manner and ensure that the configured bandwidth allocation is as close as possible to the required bandwidth allocation, you must determine the byte count based on the packet size of each protocol; otherwise your percentages may not match what you configure.

Determining the Byte Count

To determine the correct byte counts, perform the following tasks:

1. For each queue, divide the percentage of bandwidth you want to allocate to the queue by the packet size, in bytes. The ratios are: 20:1086, 60:291, 20:831 or 0.01842, 0.20619, 0.02407
2. Normalize the numbers by dividing by the lowest number: 1, 11.2, 1.3
3. The result is the ratio of the number of packets that must be sent so that the percentage of bandwidth each protocol uses is approximately 20, 60, and 20 percent.
4. A fraction in any of the ratio values means an additional packet is sent. Round up the numbers to the next whole number to obtain the actual packet count. In this example, the actual ratio is 1 packet, 12 packets, and 2 packets.
5. Convert the packet number ratio into byte counts by multiplying each packet count by the corresponding packet size. In this example, the number of packets sent is one 1086-byte packet, twelve 291-byte packets, and two 831-byte packets, or 1086, 3492, and 1662 bytes, respectively, from the each queue. These are the byte counts you would specify in your custom queuing configuration.
6. To determine the bandwidth distribution this ratio represents, first determine the total numbers of bytes sent after all three queues are serviced: (1×1086) + (12×291) + (2×831) = 1086 + 3492 + 1662 = 6240
7. Then determine the percentage of the total number of bytes sent from each queue: 1086 ÷ 6240, 3492÷6240, 1662÷6240 = 17.4%, 56%, and 26.6%

As you can see, this is close to the desired ratio of 20:60:20.

Window Size

Window size also affects the bandwidth distribution. If the window size of a particular protocol is set to one, then that protocol will not place another packet into the queue until it receives an acknowledgment. The CQ algorithm moves to the next queue if the byte count is exceeded or no packets are in that queue. Therefore, with a window size of one, only one frame will be sent each time. If your frame count is set to 2 kilobytes, and your frame size is 256 bytes, then only 256 bytes will be sent each time this queue is serviced.

PRELAB

After reading the whole experiment, do the following and take a snapshot for each part:

> Calculate the byte count, needed to be transferred from each of four queues so that you assign 40% of bandwidth to Video-1, 20% to Video-2, 25% to Voice-1 and 15% to Voice-2. Considering that the average packet size for video traffic is 1070 Bytes and for voice traffic which is 206 Bytes, settings should do be done. (You can refer to introduction of this experiment, determining the byte count section).

Complete the following lab experiment to configure traffic scheduling in network. In this experiment, students will work in the following groups:

1. Group 1: R25-1 & R45-1
2. Group 2: R25-2 & R45-2
3. Group 3: R25-3 & R45-3
4. Group 3: R25-4 & R45-4

Groups should start each task by coordinating with lab instructor. All groups should start each task at the same time. Whenever you obtain performance diagrams, you should capture and present them in your report**. After doing any configuration, you should use the corresponding "show" commands to check that your configuration is correct and applied properly.** Incorrectness of your configurations directly affects the results of all groups.

TASKS

1.1.6 TASK 1: CHECK THE NETWORK PERFORMANCE WITH FIFO QUEUING

Complete the following steps.

Step 1 Examine your router interfaces by using the following commands:

```
Rx-x#show interface serial0/0/x
Rx-x#show interface GigabitEthernet0/x
```

What are the Queuing Strategies? ……………………

How many queues exist on each interface? What is the purpose of each queue?

Check and describe the information available on each queue. Append this information to your report.

You need to change the OSPF routing preferences to select serial interfaces the prefer interface to forwards traffics between the routers**.**

```
Rx-x(config)# interface  GE 0/x     x=0,1
Rx-x(config)# ip ospf cost 60000
```

Step 2 use SolarWinds to measure the network performance.

Open the chrome explorer fill into the URL http://192.168.20.21, a username and password will be requested use your router name in small letter for both, for example username: r25-1 password:r25-1.

Click the VoIP & Network Quality tab in the Modules menu bar, and then click VoIP & Quality Settings at the top right of the view.

Under ALL IP SLA Operations, you will find the running operation of network performance, export the measure performance for your POD based on the below table.

Router Name	Type of Traffic1	Type of Traffic2	Type of Traffic3
R25-1	VoIP(R25-1, R25-2) Voice(16400), Video(50505)	FTP (R25-1, 192.168.20.132)	UDP Ehco(R25-1, R25-2)
R25-2	VoIP(R25-2, R25-3) Voice(16400), Video(50505)	FTP (R25-2, 192.168.20.148)	UDP Ehco (R25-2, R25-3)
R25-3	VoIP(R25-3, R25-4) Voice(16400), Video(50505)	FTP (R25-3, 192.168.20.164)	UDP Ehco (R25-3, R25-4)
R25-4	VoIP(R25-4, R25-1) Voice(16400), Video(50505)	FTP (R25-4, 192.168.20.180)	UDP Ehco (R25-4, R25-1)
R45-1	VoIP(R25-2, R25-1) Voice(16400), Video(50505)	FTP (R25-1, 192.168.20.132)	UDP Ehco (R25-1, R25-2)

R45-2	VoIP(R25-3, R25-2)
	Voice(16400), Video(50505)
		FTP (R25-2,
		192.168.20.148)
			UDP Ehco (R25-2, R25-3)

R45-3	VoIP(R25-4, R25-3)
	Voice(16400), Video(50505)
		FTP (R25-3,
		192.168.20.164)
			UDP Ehco (R25-3, R25-4)

R45-4	VoIP(R25-1, R25-4)
	Voice(16400), Video(50505)
		FTP (R25-4,
		192.168.20.180)
			UDP Ehco (R25-4, R25-1)

1.1.7 TASK 2: CONFIGURE PRIORITY QUEUING

Step 1 Configure a Priority Queue in your router by executing the following commands in global configuration mode:

```
Rx-x#configure terminal
Rx-x(config)#Priority-list 1 protocol ip high udp 16400
Rx-x(config)#Priority-list 1 protocol ip medium tcp echo
Rx-x(config)#Priority-list 1 protocol ip normal udp 50505
Rx-x(config)#Priority-list 1 protocol ip low tcp ftp-data
```

According to the PQ definition, voice traffic destined to UDP port 16400 has the highest priority. The second important traffic is the TCP echo traffic generated by ping command. Traffic in “normal” queue is Video, which is sent to the UDP port 50505, and FTP traffic has the lowest priority.

Step 5 Enter the following command in your routers in interface configuration mode on all **serial** interfaces.

```
Rx-x(config-if)#Priority-group 1
```

By entering this command, you activated priority queuing on all serial interfaces and priority list 1 is activated on the out-going packets in each serial interface.

1.1.8 TASK 3: MONITOR NETWORK PERFORMANCE WITH PRIORITY QUEUE

Use the SolarWinds tool to capture network performance metrics.

1.1.9 TASK 4: CONFIGURING CUSTOM QUEUING

Complete the following steps:

Step 1 Change the queuing strategy on all router interfaces to FIFO by entering the following command in interface configuration mode:

```
Rx-x(config-if)#no priority-group 1
Rx-x(config-if)#no fair-queue
```

Start exporting the graph from SolarWinds as a PDF files. Please wait at least 5 minutes to make sure the sampling time is enough and captured.

1.1.10 TASK 5: CONFIGURE WEIGHTED ROUND ROBIN

Step 1 Calculate the byte count, needed to be transferred from each of four queues so that you assign 40% of bandwidth to Video-1, 20% to Video-2, 25% to Voice-1 and 15% to Voice-2. Considering that the average packet size for video traffic is 1070 Bytes and for voice traffic which is 206 Bytes, settings should do be done. (You can refer to introduction of this experiment, determining the byte count section).

Step 2 Configure the WRR by executing the following commands in global configuration mode and enter the results of your calculation as the “no-of-bytes” in the corresponding commands:

```
Rx-x(config)#queue-list 5 protocol ip 1 udp 50505
Rx-x(config)#queue-list 5 protocol ip 2 udp 50509
Rx-x(config)#queue-list 5 protocol ip 3 udp 16400
Rx-x(config)#queue-list 5 protocol ip 4 udp 16409

Rx-x(config)#queue-list 5 queue 1 byte-count no_of_bytes
Rx-x(config)#queue-list 5 queue 2 byte-count no_of_bytes
Rx-x(config)#queue-list 5 queue 3 byte-count no_of_bytes
Rx-x(config)#queue-list 5 queue 4 byte-count no_of_bytes
```

Step 3 Enter the following command in your routers in interface configuration mode on all **serial** interfaces.

```
Rx-x(config-if)#custom-queue-list 5
```

By entering this command, you activated custom queuing on all serial interfaces.

1.1.11 TASK 8: CHECK NETWORK PERFORMANCE WITH WRR

Step 1 Check each of delay, jitter and error graphs for voice and video for a period of 10 minutes and capture them to answer the following questions:

- Compare the graphs obtained for Tasks 1,2 and 4. What differences do you see? Describe the changes happened based on the specifications of custom queuing.
- Compare graphs for Voice and Video, what are the differences? Why?
- Does Voice or Video traffic see major changes while applying WRR? Why?
- Check the error rate for Voice and Video traffics and try to explain the reason for major changes in error rate.

Step 2 Remove “custom-queue-list” commands from all interfaces and stop collectors.

COMPLETION CRITERIA

At the end of this lab, you should have obtained clear and describable curves for each task and you should have all the required information to answer the questions.

POST-LAB

Do the following task(s) and take a snapshot for each part and include it in your report.

1. Open the Packet Tracer and use the saved network topology.
2. Configure the priority queuing on each router by using the commands applied in the lab.