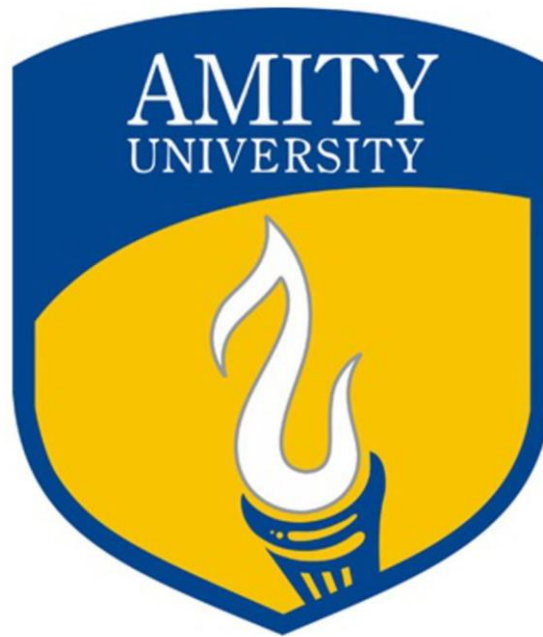


**Exploring The Networks  
Laboratory Manual  
B.Tech (CS&E) Vth Semester  
Academic Year (2018-2019)**



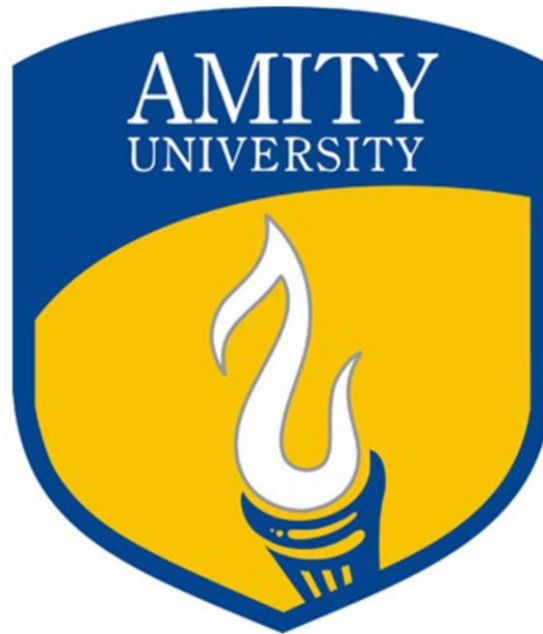
**Prepared & Maintain by  
Mr. Vineet Singh  
Assistant Professor**

**Department of Computer Science & Engineering  
Amity School of Engineering & Technology  
Amity University Lucknow Campus**

## Contents

1. <b>List of Practicals</b> .....	4
2. <b>INDEX</b> .....	5
3. <b>Lab 1: Observing TCP and UDP using Netstat</b> .....	6
4. <b>Lab 2: Using Wireshark™ to View Protocol Data Units</b> .....	11
5. <b>Lab 3: Examining a Device's Gateway</b> .....	21
6. <b>Lab 4: Examining a Route</b> .....	29
7. <b>Lab 5: Ping and Traceroute</b> .....	36
8. <b>Lab 6: Examining ICMP Packets</b> .....	44
9. <b>Lab 7: IPv4 Address Subnetting</b> .....	53
10. <b>Lab 8: Subnet and Router Configuration</b> .....	59
11. <b>Lab 9: Media Connectors Lab Activity</b> .....	62
12. <b>Lab 10: Basic Cisco Device Configuration</b> .....	68

**Exploring The Networks  
Laboratory Record  
B.Tech (CS&E) Vth Semester  
Academic Year (2018-2019)**



**Submitted By**

**Name:** \_\_\_\_\_

**Enrol No:** \_\_\_\_\_

**Department of Computer Science & Engineering  
Amity School of Engineering & Technology  
Amity University Lucknow Campus**

## List of Practicals

### Introduction to Networks Lab

#### 1 Observing TCP and UDP using Netstat

Explain common **netstat** command parameters and outputs.

#### 2 TCP/IP Transport Layer Protocols, TCP and UDP

Identify TCP header fields and operation using a Wireshark FTP session capture.

Identify UDP header fields and operation using a Wireshark TFTP session capture

#### 3 Examining a Device's Gateway

Understand and explain the purpose of a gateway address.

Understand how network information is configured on a Windows computer.

Troubleshoot a hidden gateway address problem

#### 4 Examining a Route

Use the **route** command to modify a Windows computer routing table.

Use a Windows Telnet client command **telnet** to connect to a Cisco router.

Examine router routes using basic Cisco IOS commands.

#### 5 Ping and Traceroute

Use the **ping** command to verify simple TCP/IP network connectivity.

Use the **tracert/traceroute** command to verify TCP/IP connectivity.

#### 6 Examining ICMP Packets

Understand the format of ICMP packets.

Use Wireshark to capture and examine ICMP messages.

#### 7 IPv4 Address Subnetting

##### Scenario

When given an IP address, network mask, and subnetwork mask, you will be able to determine other information about the IP address such as:

- The subnet address of this subnet
- The broadcast address of this subnet
- The range of host addresses for this subnet
- The maximum number of subnets for this subnet mask
- The number of hosts for each subnet
- The number of subnet bits
- The number of this subnet

#### 8 Subnet and Router Configuration

Subnet an address space per given requirements.

Assign appropriate addresses to interfaces and document.

Configure and activate Serial and FastEthernet interfaces.

Test and verify configurations.

Reflect upon and document the network implementation

#### 9 Media Connectors Lab Activity

Become familiar with the most common functions of a cable tester.

Test different cables for type and wiring problems

#### 10 Basic Cisco Device Configuration

Configure Cisco router global configuration settings.

Configure Cisco router interfaces.

Save the router configuration file.

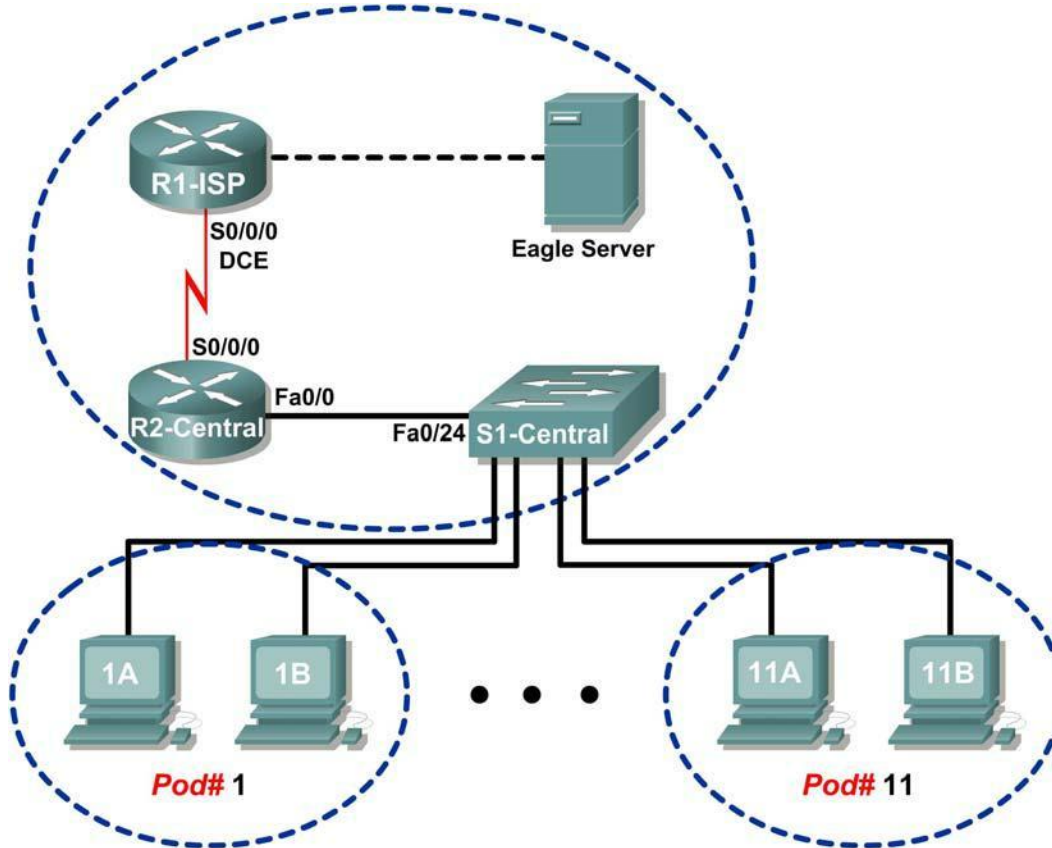
Configure a Cisco switch

**INDEX**

<b>S.No</b>	<b>Name Of Lab Work</b>	<b>Date</b>	<b>Signature of Faculty</b>
1	Observing TCP and UDP using Netstat		
2	TCP/IP Transport Layer Protocols, TCP and UDP		
3	Examining a Device's Gateway		
4	Examining a Route		
5	Ping and Traceroute		
6	Examining ICMP Packets		
7	IPv4 Address Subnetting		
8	Subnet and Router Configuration		
9	Media Connectors Lab Activity		
10	Basic Cisco Device Configuration		

# Lab 1: Observing TCP and UDP using Netstat

## Topology Diagram



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	10.10.10.6
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	N/A	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	N/A
hostPod#A	N/A	172.16.Pod#.1	255.255.0.0	172.16.255.254
hostPod#B	N/A	172.16.Pod#.2	255.255.0.0	172.16.255.254
S1-Central	N/A	172.16.254.1	255.255.0.0	172.16.255.254

## Learning Objectives

- Explain common `netstat` command parameters and outputs.
- Use `netstat` to examine protocol information on a pod host computer.

## Background

`netstat` is an abbreviation for the network statistics utility, available on both Windows and Unix / Linux computers. Passing optional parameters with the command will change output information. `netstat` displays incoming and outgoing network connections (TCP and UDP), host computer routing table information, and interface statistics.

## Scenario

In this lab the student will examine the `netstat` command on a pod host computer, and adjust `netstat` output options to analyze and understand TCP/IP Transport Layer protocol status.

## Task 1: Explain common `netstat` command parameters and outputs.

Open a terminal window by clicking on Start | Run. Type `cmd`, and press **OK**.

To display help information about the `netstat` command, use the `/?` options, as shown:

```
C:\> netstat /? <ENTER>
```

Use the output of the `netstat /?` command as reference to fill in the appropriate option that best matches the description:

Option	Description
	Display all connections and listening ports.
	Display addresses and port numbers in numerical form.
	Redisplay statistics every five seconds. Press CTRL+C to stop redisplaying statistics.
	Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, proto may be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
	Redisplay all connections and listening ports every 30 seconds.
	Display only open connections. This is a tricky problem.

When `netstat` statistics are displayed for TCP connections, the TCP state is displayed. During the life of a TCP connection, the connection passes through a series of states. The following table

is a summary of TCP states, compiled from RFC 793, Transmission Control Protocol, September, 1981, as reported by `netstat`:

State	Connection Description
LISTEN	The local connection is waiting for a connection request from any remote device.
ESTABLISHED	The connection is open, and data may be exchanged through the connection. This is the normal state for the data transfer phase of the connection.
TIME-WAIT	The local connection is waiting a default period of time after sending a connection termination request before closing the connection. This is a normal condition, and will normally last between 30 - 120 seconds.
CLOSE-WAIT	The connection is closed, but is waiting for a termination request from the local user.
SYN-SENT	The local connection is waiting for a response after sending a connection request. The connection should transition quickly through this state.
SYN RECEIVED	The local connection is waiting for a confirming connection request acknowledgment. The connection should transition quickly through this state. Multiple connections in SYN_RECEIVED state may indicate a TCP SYN attack.

IP addresses displayed by `netstat` fall into several categories:

IP Address	Description
127.0.0.1	This address refers to the local host, or this computer.
	ANY
Remote Address	The address of the remote device that has a connection with this computer.

## Task 2: Use `netstat` to Examine Protocol Information on a Pod Host Computer.

### Step 1: Use `netstat` to view existing connections.

From the terminal window in Task 1, above, issue the command `netstat -a`:

```
C:\> netstat -a <ENTER>
```

A table will be displayed that lists protocol (TCP and UDP), Local address, Foreign address, and State information. Addresses and protocols that can be translated into names are displayed.

The `-n` option forces `netstat` to display output in raw format. From the terminal window, issue the command `netstat -an`:

```
C:\> netstat -an <ENTER>
```

Use the window vertical scroll bar to go back and forth between the outputs of the two commands. Compare outputs, noting how well-known port numbers are changed to names.



Write down three TCP and three UDP connections from the `netstat -a` output, and the corresponding translated port numbers from the `netstat -an` output. If there are fewer than three connections that translate, note that in your table.

Connection	Proto	Local Address	Foreign Address	State

Refer to the following `netstat` output. A new network engineer suspects that his host computer has been compromised by an outside attack against ports 1070 and 1071. How would you respond?

```
C:\> netstat -n
Active Connections
Proto Local Address          Foreign Address        State
TCP   127.0.0.1:1070         127.0.0.1:1071        ESTABLISHED
TCP   127.0.0.1:1071         127.0.0.1:1070        ESTABLISHED
C:\>
```

**Step 2: Establish multiple concurrent TCP connections and record netstat output.**

In this task, several simultaneous connections will be made with Eagle Server. The venerable `telnet` command will be used to access Eagle Server network services, thus providing several protocols to examine with `netstat`.

Open an additional four terminal windows. Arrange the windows so that all are visible. The four terminal windows that will be used for telnet connections to Eagle Server can be relatively small, approximately 1/2 screen width by 1/4 screen height. The terminal windows that will be used to collect connection information should be 1/2 screen width by full screen height.

Several network services on Eagle Server will respond to a telnet connection. We will use:

- DNS- domain name server, port 53
- FTP- FTP server, port 21
- SMTP- SMTP mail server, port 25
- TELNET- Telnet server, port 23

Why should telnet to UDP ports fail?

---

---

To close a telnet connection, press the <CTRL> ] keys together. That will bring up the telnet prompt, `Microsoft Telnet>`. Type `quit` <ENTER> to close the session.

In the first telnet terminal window, telnet to Eagle Server on port 53. In the second terminal window, telnet on port 21. In the third terminal window, telnet on port 25. In the fourth terminal window, telnet on port 23. The command for a telnet connection on port 21 is shown below:

```
C:\> telnet eagle-server.example.com 53
```

In the large terminal window, record established connections with Eagle Server. Output should look similar to the following. If typing is slow, a connection may close before all connections have been made. Eventually, connections should terminate from inactivity.

Proto	Local Address	Foreign Address	State
TCP	192.168.254.1:1688	192.168.254.254:21	ESTABLISHED
TCP	192.168.254.1:1691	192.168.254.254:25	ESTABLISHED
TCP	192.168.254.1:1693	192.168.254.254:53	ESTABLISHED
TCP	192.168.254.1:1694	192.168.254.254:23	ESTABLISHED

### Task 3: Reflection.

The `netstat` utility displays incoming and outgoing network connections (TCP and UDP), host computer routing table information, and interface statistics.

### Task 4: Challenge.

Close Established sessions abruptly (close the terminal window), and issue the `netstat -an` command. Try to view connections in stages different from ESTABLISHED.

### Task 5: Cleanup.

Unless directed otherwise by the instructor, turn off power to the host computers. Remove anything that was brought into the lab, and leave the room ready for the next class.

## Lab 2: Using Wireshark™ to View Protocol Data Units

### Learning Objectives

- Be able to explain the purpose of a protocol analyzer (Wireshark).
- Be able to perform basic PDU capture using Wireshark.
- Be able to perform basic PDU analysis on straightforward network data traffic.
- Experiment with Wireshark features and options such as PDU capture and display filtering.

### Background

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. Before June 2006, Wireshark was known as Ethereal.

A packet sniffer (also known as a network analyzer or protocol analyzer) is computer software that can intercept and log data traffic passing over a data network. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications.

Wireshark is programmed to recognize the structure of different network protocols. This enables it to display the encapsulation and individual fields of a PDU and interpret their meaning.

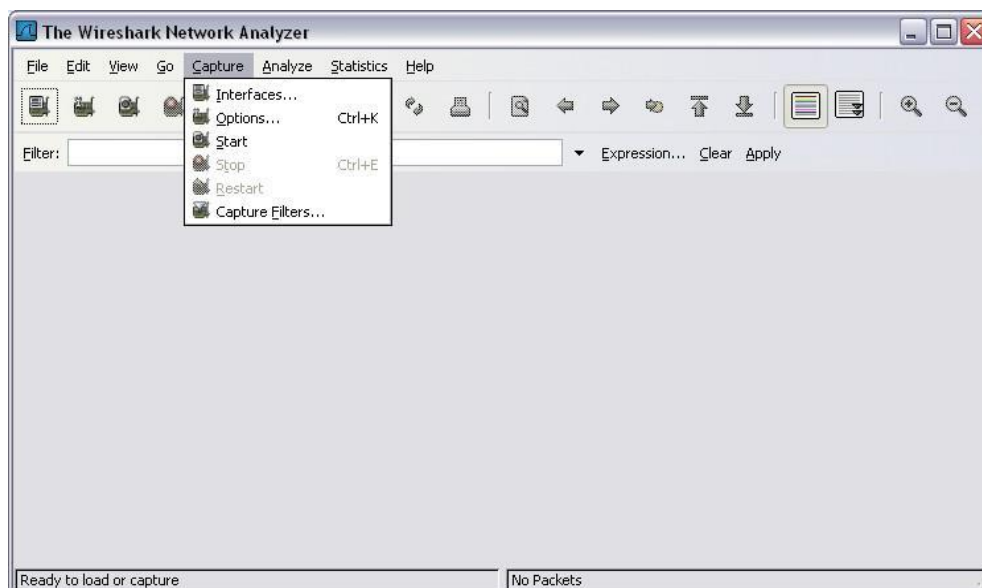
It is a useful tool for anyone working with networks and can be used with most labs in the CCNA courses for data analysis and troubleshooting.

For information and to download the program go to - <http://www.Wireshark.org>

### Scenario

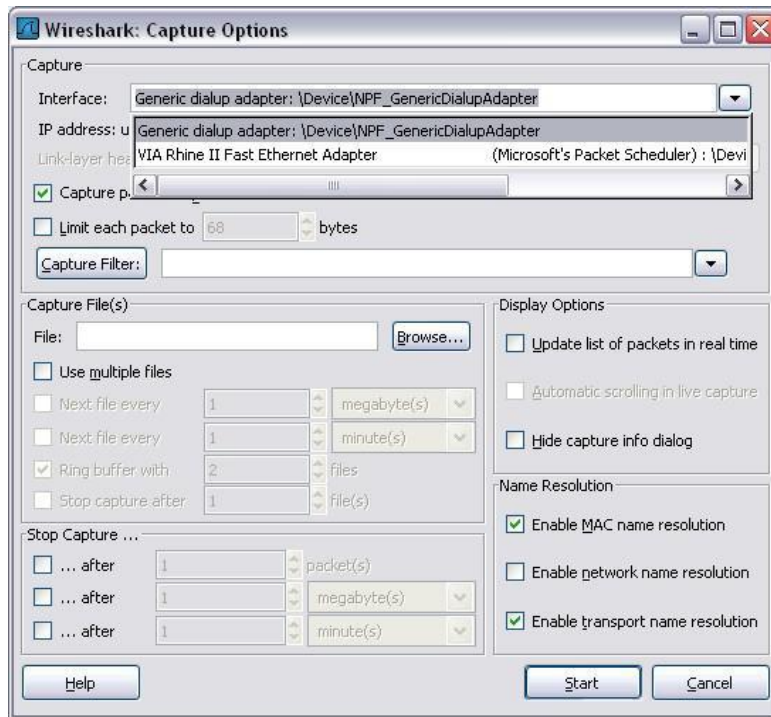
To capture PDUs the computer on which Wireshark is installed must have a working connection to the network and Wireshark must be running before any data can be captured.

When Wireshark is launched, the screen below is displayed.



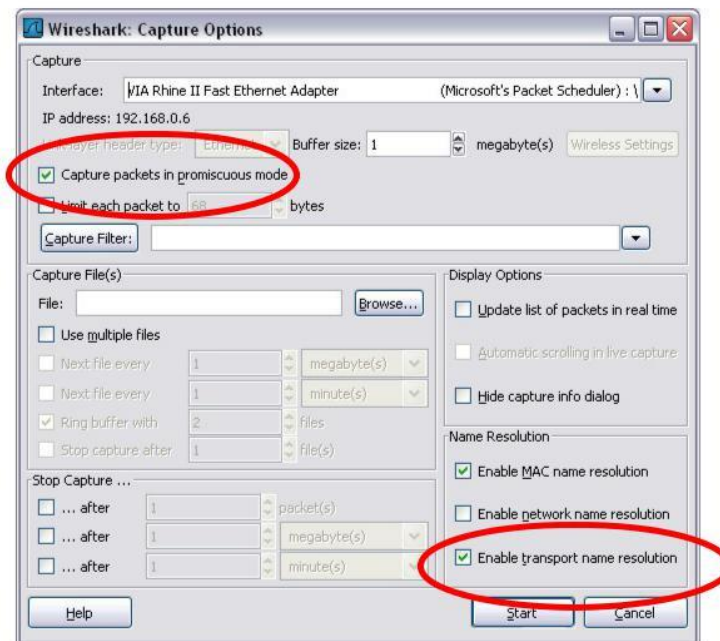
To start data capture it is first necessary to go to the **Capture** menu and select the **Options** choice.

The **Options** dialog provides a range of settings and filters which determines which and how much data traffic is captured.



First, it is necessary to ensure that Wireshark is set to monitor the correct interface. From the **Interface** drop down list, select the network adapter in use. Typically, for a computer this will be the connected Ethernet Adapter.

Then other Options can be set. Among those available in **Capture Options**, the two highlighted below are worth examination.



### Setting Wireshark to capture packets in promiscuous mode

If this feature is NOT checked, only PDUs destined for this computer will be captured.

If this feature is checked, all PDUs destined for this computer AND all those detected by the computer NIC on the same network segment (i.e., those that "pass by" the NIC but are not destined for the computer) are captured.

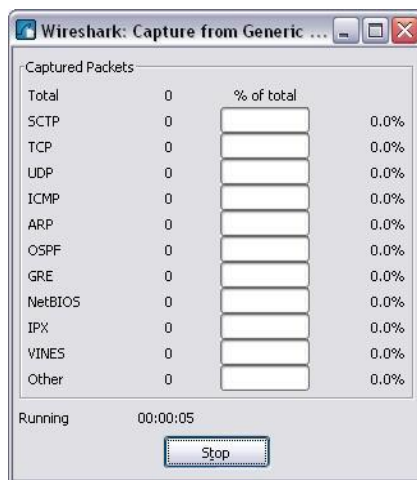
Note: The capturing of these other PDUs depends on the intermediary device connecting the end device computers on this network. As you use different intermediary devices (hubs, switches, routers) throughout these courses, you will experience the different Wireshark results.

### Setting Wireshark for network name resolution

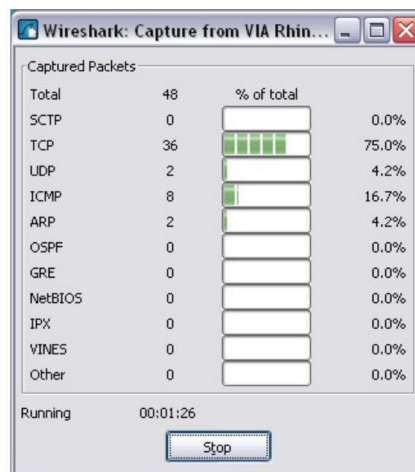
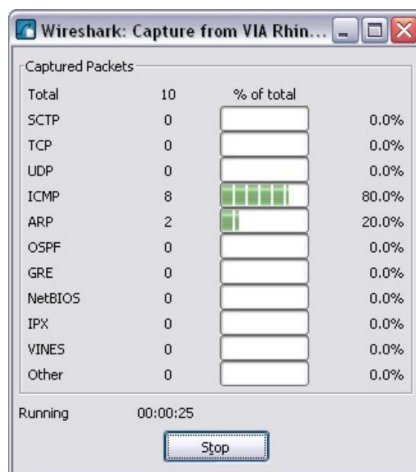
This option allows you to control whether or not Wireshark translates network addresses found in PDUs into names. Although this is a useful feature, the name resolution process may add extra PDUs to your captured data perhaps distorting the analysis.

There are also a number of other capture filtering and process settings available.

Clicking on the **Start** button starts the data capture process and a message box displays the progress of this process.



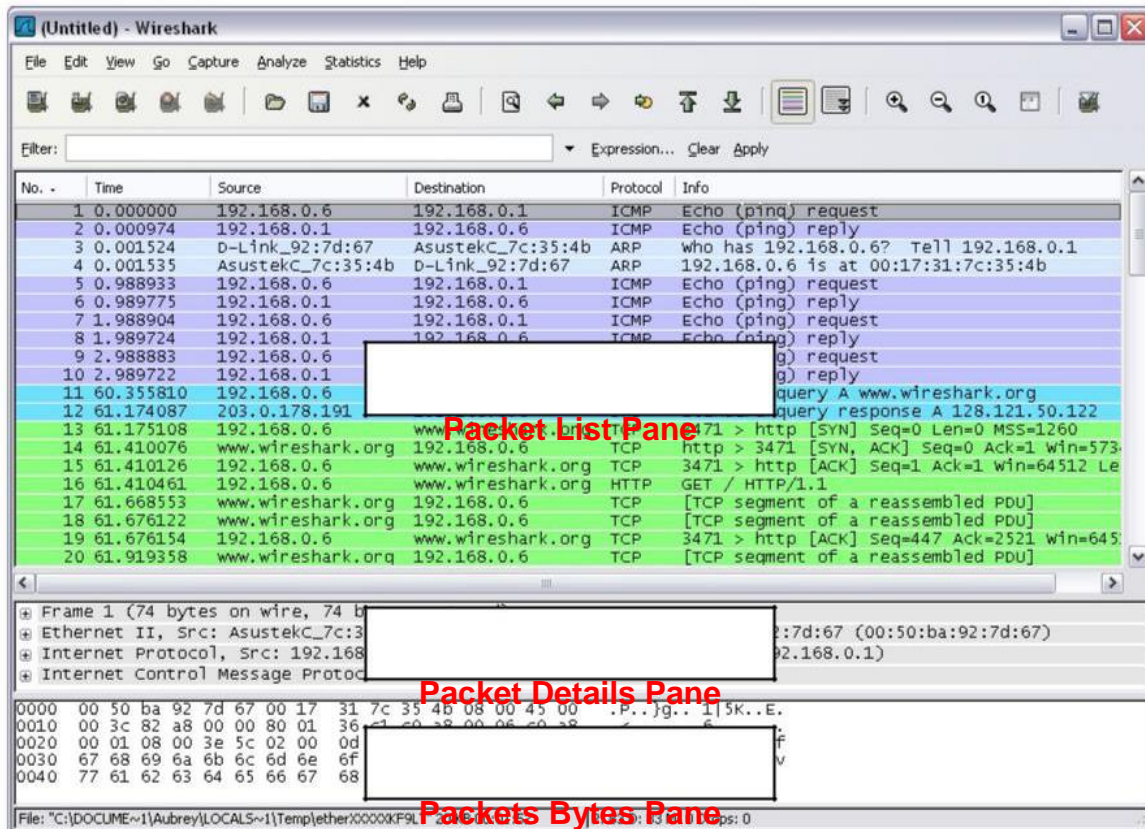
As data PDUs are captured, the types and number are indicated in the message box



The examples above show the capture of a ping process and then accessing a web page.

When the **Stop** button is clicked, the capture process is terminated and the main screen is displayed.

This main display window of Wireshark has three panes.



The PDU (or Packet) List Pane at the top of the diagram displays a summary of each packet captured. By clicking on packets in this pane, you control what is displayed in the other two panes.

The PDU (or Packet) Details Pane in the middle of the diagram displays the packet selected in the Packet List Pane in more detail.

The PDU (or Packet) Bytes Pane at the bottom of the diagram displays the actual data (in hexadecimal form representing the actual binary) from the packet selected in the Packet List Pane, and highlights the field selected in the Packet Details Pane.

Each line in the Packet List corresponds to one PDU or packet of the captured data. If you select a line in this pane, more details will be displayed in the "Packet Details" and "Packet Bytes" panes. The example above shows the PDUs captured when the ping utility was used and <http://www.Wireshark.org> was accessed. Packet number 1 is selected in this pane.

The Packet Details pane shows the current packet (selected in the "Packet List" pane) in a more detailed form. This pane shows the protocols and protocol fields of the selected packet. The protocols and fields of the packet are displayed using a tree, which can be expanded and collapsed.

The Packet Bytes pane shows the data of the current packet (selected in the "Packet List" pane) in what is known as "hexdump" style. In this lab, this pane will not be examined in detail. However, when a more in- depth analysis is required this displayed information is useful for examining the binary values and content of PDUs.



The information captured for the data PDUs can be saved in a file. This file can then be opened in Wireshark for analysis some time in the future without the need to re-capture the same data traffic again. The information displayed when a capture file is opened is the same as the original capture.

When closing a data capture screen or exiting Wireshark you are prompted to save the captured PDUs.



Clicking on **Continue without Saving** closes the file or exits Wireshark without saving the displayed captured data.

### Task 1: Ping PDU Capture

**Step 1: After ensuring that the standard lab topology and configuration is correct, launch Wireshark on a computer in a lab pod.**

Set the Capture Options as described above in the overview and start the capture process.

From the command line of the computer, ping the IP address of another network connected and powered on end device on in the lab topology. In this case, ping the Eagle Server at using the command ping **192.168.254.254**.

After receiving the successful replies to the ping in the command line window, stop the packet capture.

**Step 2: Examine the Packet List pane.**

The Packet List pane on Wireshark should now look something like this:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Cont. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
2	2.000032	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
3	4.000059	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
4	4.072858	QuantaCo_bd:0c:7c	Broadcast	ARP	who has 10.1.1.254? Tell 10.1.1.1
5	4.073609	Cisco_cf:66:40	QuantaCo_bd:0c:7c	ARP	10.1.1.254 is at 00:0c:85:cf:66:40
6	4.073626	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
7	4.074122	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
8	5.067535	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
9	5.068007	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
10	6.000113	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
11	6.067548	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
12	6.068019	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
13	6.084103	Cisco_9f:6c:c9	Cisco_9f:6c:c9	LOOP	Reply
14	7.067603	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
15	7.068131	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
16	8.000126	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
17	9.975700	Cisco_9f:6c:c9	CDP/VTP/DTP/PAgp/u	DTP	Dynamic Trunking Protocol
18	10.000134	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =

Look at the packets listed above; we are interested in packet numbers 6, 7, 8, 9, 11, 12, 14 and 15.

Locate the equivalent packets on the packet list on your computer.

If you performed Step 1A above match the messages displayed in the command line window when the ping was issued with the six packets captured by Wireshark.

From the Wireshark Packet List answer the following:

What protocol is used by ping? \_\_\_\_\_

What is the full protocol name? \_\_\_\_\_

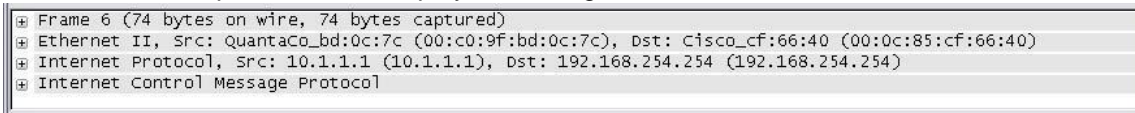
What are the names of the two ping messages? \_\_\_\_\_

Are the listed source and destination IP addresses what you expected? Yes / No

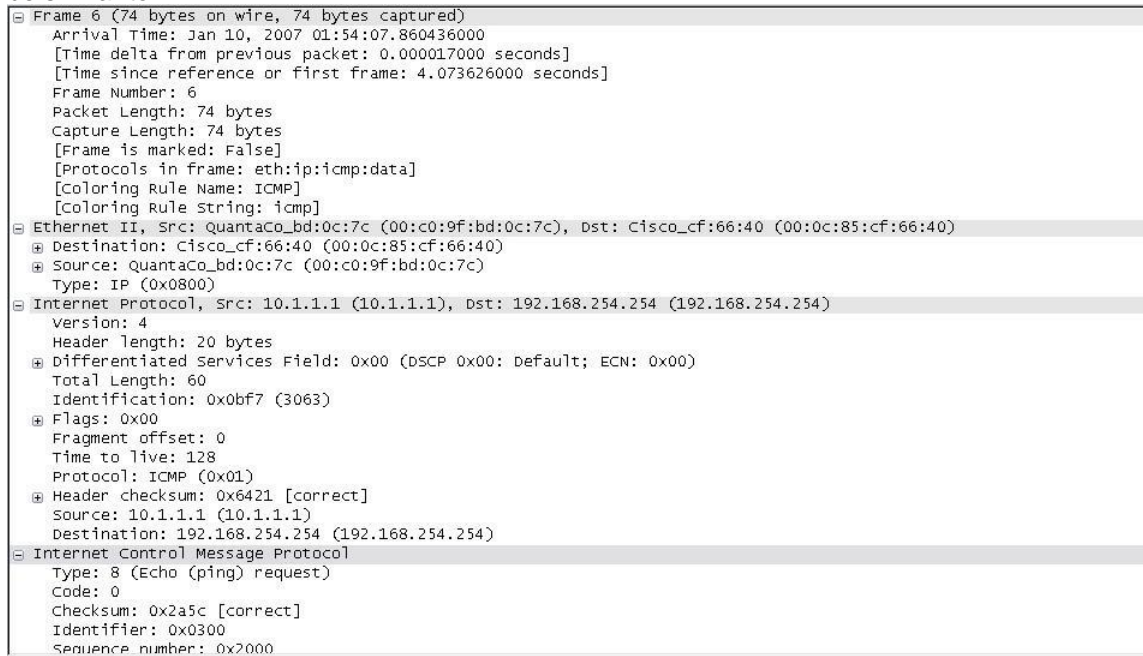
Why? \_\_\_\_\_

**Step 3: Select (highlight) the first echo request packet on the list with the mouse.**

The Packet Detail pane will now display something similar to:



Click on each of the four "+" to expand the information. The packet Detail Pane will now be similar to:





As you can see, the details for each section and protocol can be expanded further. Spend some time scrolling through this information. At this stage of the course, you may not fully understand the information displayed but make a note of the information you do recognize.

Locate the two different types of 'Source' and 'Destination'. Why are there two types?

---

What protocols are in the Ethernet frame?

---

As you select a line in the Packets Detail pane all or part of the information in the Packet Bytes pane also becomes highlighted.

For example, if the second line (+ Ethernet II) is highlighted in the Details pane the Bytes pane now highlights the corresponding values.



This shows the particular binary values that represent that information in the PDU. At this stage of the course, it is not necessary to understand this information in detail.

**Step 4: Go to the File menu and select Close.**

Click on **Continue without Saving** when this message box appears.



**Task 2: FTP PDU Capture**

**Step 1: Start packet capture.**

Assuming Wireshark is still running from the previous steps, start packet capture by clicking on the **Start** option on the **Capture** menu of Wireshark.

At the command line on your computer running Wireshark, enter [ftp 192.168.254.254](#)

When the connection is established, enter **anonymous** as the user without a password.

Userid: **anonymous**

Password: <ENTER>

You may alternatively use login with userid **cisco** and with password **cisco**.

When successfully logged in enter **get /pub/eagle\_labs/eagle1/chapter1/gaim-1.5.0.exe** and press the enter key <ENTER>. This will start downloading the file from the ftp server. The output will look similar to:

```
C:\Documents and Settings\ccna1>ftp eagle-
server.example.com Connected to eagle-server.example.com.
220 Welcome to the eagle-server FTP service.
User (eagle-server.example.com:(none)):
anonymous 331 Please specify the password.
Password:<ENTER>
230 Login successful.
ftp> get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for
pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe (6967072 bytes).
226 File send OK.
ftp: 6967072 bytes received in 0.59Seconds 11729.08Kbytes/sec.
```

When the file download is complete enter **quit**

```
ftp> quit
221 Goodbye.
C:\Documents and Settings\ccna1>
```

When the file has successfully downloaded, stop the PDU capture in Wireshark.

### **Step 2: Increase the size of the Wireshark Packet List pane and scroll through the PDUs listed.**

Locate and note those PDUs associated with the file download. These will be the PDUs from the Layer 4 protocol TCP and the Layer 7 protocol FTP. Identify the three groups of PDUs associated with the file transfer.

If you performed the step above, match the packets with the messages and prompts in the FTP command line window.

The first group is associated with the "connection" phase and logging into the server. List examples of messages exchanged in this phase.

---

Locate and list examples of messages exchanged in the second phase that is the actual download request and the data transfer.

---



---

The third group of PDUs relate to logging out and "breaking the connection". List examples of messages exchanged during this process.

Locate recurring TCP exchanges throughout the FTP process. What feature of TCP does this indicate?

---

---

### Step 3: Examine Packet Details.

Select (highlight) a packet on the list associated with the first phase of the FTP process. View the packet details in the Details pane.

What are the protocols encapsulated in the frame?

---

Highlight the packets containing the user name and password. Examine the highlighted portion in the Packet Byte pane.

What does this say about the security of this FTP login process?

---

Highlight a packet associated with the second phase. From any pane, locate the packet containing the file name.

The filename is: \_\_\_\_\_

Highlight a packet containing the actual file content - note the plain text visible in the Byte pane.

Highlight and examine, in the Details and Byte panes, some packets exchanged in the third phase of the file download.

What features distinguish the content of these packets?

---

When finished, close the Wireshark file and continue without saving

## Task 3: HTTP PDU Capture

### Step 1: Start packet capture.

Assuming Wireshark is still running from the previous steps, start packet capture by clicking on the **Start** option on the **Capture** menu of Wireshark.

**Note:** Capture Options do not have to be set if continuing from previous steps of this lab.

Launch a web browser on the computer that is running Wireshark. Enter the URL of the Eagle Server of **example.com** or enter the IP address-192.168.254.254. When the webpage has fully downloaded, stop the Wireshark packet capture.

### Step 2: Increase the size of the Wireshark Packet List pane and scroll through the PDUs listed.

Locate and identify the TCP and HTTP packets associated with the webpage download.

Note the similarity between this message exchange and the FTP exchange.

**Step 3: In the Packet List pane, highlight an HTTP packet that has the notation "(text/html)" in the Info column.**

In the Packet Detail pane click on the "+" next to "Line-based text data: html"  
When this information expands what is displayed?

---

Examine the highlighted portion of the Byte Panel.  
This shows the HTML data carried by the packet.

When finished close the Wireshark file and continue without saving

### **Task 4: Reflection**

Consider the encapsulation information pertaining to captured network data Wireshark can provide. Relate this to the OSI and TCP/IP layer models. It is important that you can recognize and link both the protocols represented and the protocol layer and encapsulation types of the models with the information provided by Wireshark.

### **Task 5: Challenge**

Discuss how you could use a protocol analyzer such as Wireshark to:

(1) Troubleshoot the failure of a webpage to download successfully to a browser on a computer.

and

(2) Identify data traffic on a network that is requested by users.

---

---

---

---

---

---

---

---

---

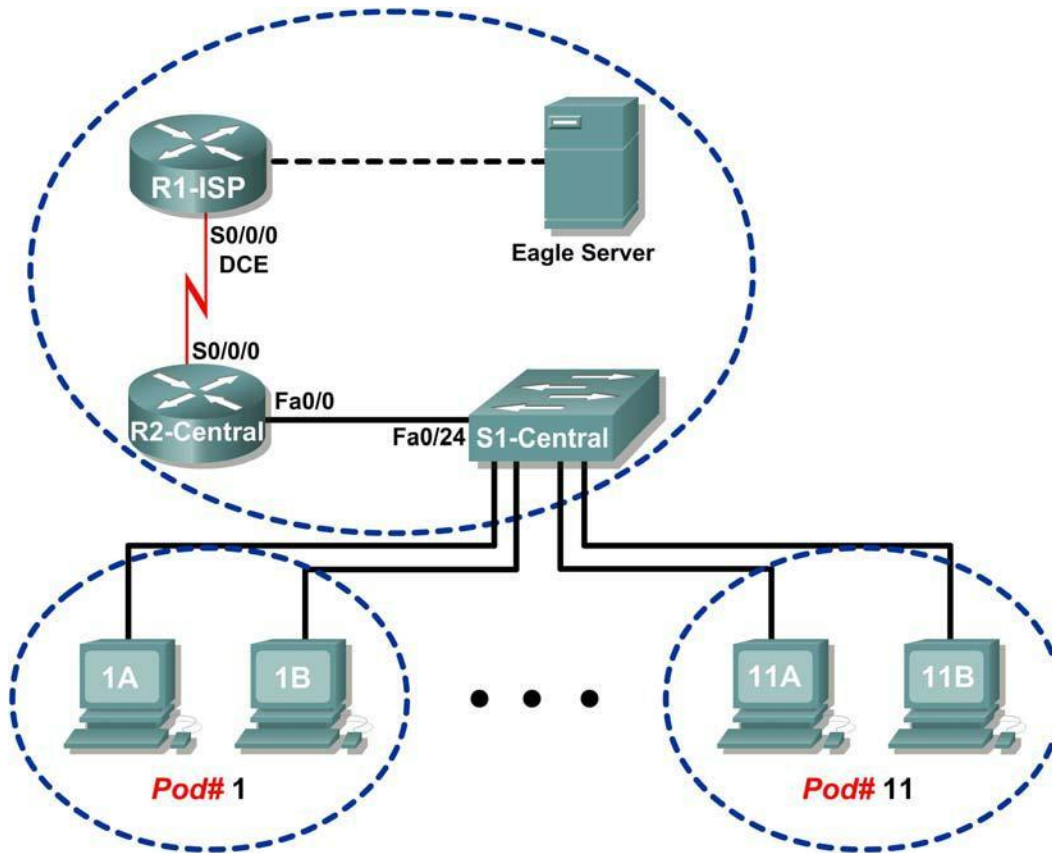
---

### **Task 6: Cleanup**

Unless instructed otherwise by your instructor, exit Wireshark and properly shutdown the computer.

### Lab 3: Examining a Device's Gateway

#### Topology Diagram



#### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	10.10.10.6
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	N/A	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	N/A
hostPod#A	N/A	172.16.Pod#.1	255.255.0.0	172.16.255.254
hostPod#B	N/A	172.16.Pod#.2	255.255.0.0	172.16.255.254
S1-Central	N/A	172.16.254.1	255.255.0.0	172.16.255.254

## Learning Objectives

Upon completion of this lab, you will be able to:

- Understand and explain the purpose of a gateway address.
- Understand how network information is configured on a Windows computer.
- Troubleshoot a hidden gateway address problem.

## Background

An IP address is composed of a network portion and a host portion. A computer that communicates with another device must first know how to reach the device. For devices on the same local area network (LAN), the host portion of the IP address is used as the identifier. The network portion of the destination device is the same as the network portion of the host device.

However, devices on different networks have different source and destination network numbers. The network portion of the IP address is used to identify when a packet must be sent to a gateway address, which is assigned to a network device that forwards packets between distant networks.

A router is assigned the gateway address for all the devices on the LAN. One purpose of a router is to serve as an entry point for packets coming into the network and exit point for packets leaving the network.

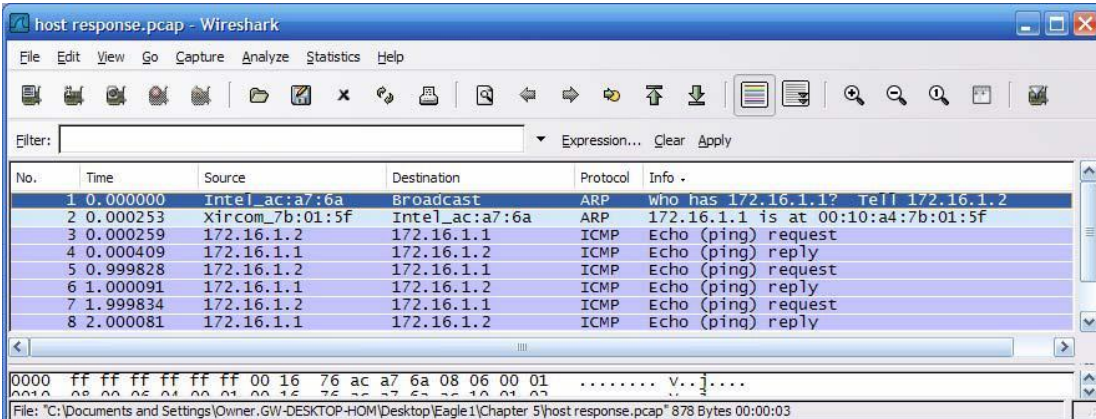
Gateway addresses are very important to users. Cisco estimates that 80 percent of network traffic will be destined to devices on other networks, and only 20 percent of network traffic will go to local devices. This is called the 80/20 rule. Therefore, if a gateway cannot be reached by the LAN devices, users will not be able to perform their job.

## Scenario

Pod host computers must communicate with Eagle Server, but Eagle Server is located on a different network. If the pod host computer gateway address is not configured properly, connectivity with Eagle Server will fail.

Using several common utilities, network configuration on a pod host computer will be verified.

## Task 1: Understand and Explain the Purpose of a Gateway Address.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Intel_ac:a7:6a	Broadcast	ARP	Who has 172.16.1.1? Tell 172.16.1.2
2	0.000253	Xircom_7b:01:5f	Intel_ac:a7:6a	ARP	172.16.1.1 is at 00:10:a4:7b:01:5f
3	0.000259	172.16.1.2	172.16.1.1	ICMP	Echo (ping) request
4	0.000409	172.16.1.1	172.16.1.2	ICMP	Echo (ping) reply
5	0.999828	172.16.1.2	172.16.1.1	ICMP	Echo (ping) request
6	1.000091	172.16.1.1	172.16.1.2	ICMP	Echo (ping) reply
7	1.999834	172.16.1.2	172.16.1.1	ICMP	Echo (ping) request
8	2.000081	172.16.1.1	172.16.1.2	ICMP	Echo (ping) reply

0000 ff ff ff ff ff ff 00 16 76 ac a7 6a 08 06 00 01 ..... V..]....  
 0010 08 00 05 04 00 01 00 16 76 ac a7 6a 08 06 00 01 ..... V..]....

File: "C:\Documents and Settings\Owner.GW-DESKTOP-HOM\Desktop\Eagle1\Chapter 5\host response.pcap" 878 Bytes 00:00:03

Figure 1. Communication Between LAN Devices

For local area network (LAN) traffic, the gateway address is the address of the Ethernet device. Figure 1 shows two devices on the same network communicating with the **ping** command. Any device that has the same network address—in this example, 172.16.0.0—is on the same LAN. Referring to Figure 1, what is the MAC address of the network device on IP address 172.16.1.1?

There are several Windows commands that will display a network gateway address. One popular command is **netstat -r**. In the following transcript, the **netstat -r** command is used to view the gateway addresses for this computer. The top highlight shows what gateway address is used to forward all network packets destined outside of the LAN. The "quad-zero" Network Destination and Netmask values, 0.0.0.0 and 0.0.0.0, refer to *any* network not specifically known. For any non-local network, this computer will use 172.16.255.254 as the default gateway. The second yellow highlight displays the information in human-readable form. More specific networks are reached through other gateway addresses. A local interface, called the loopback interface, is automatically assigned to the 127.0.0.0 network. This interface is used to identify the local host to local network services. Refer to the gray highlighted entry. Finally, any device on network 172.16.0.0 is accessed through gateway 172.16.1.2, the IP address for this Ethernet interface. This entry is highlighted in green.

```
C:\>netstat -r

Route Table
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x20005 ...00 16 76 ac a7 6a Intel(R) 82562V 10/100 Network
Connection
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface
Metric
    0.0.0.0             0.0.0.0         172.16.255.254  172.16.1.2      1
    127.0.0.0           255.0.0.0       127.0.0.1       127.0.0.1      1
    172.16.0.0          255.255.0.0     172.16.1.2      172.16.1.2     20
    172.16.1.2         255.255.255.255  127.0.0.1       127.0.0.1     20
    172.16.255.255     255.255.255.255  172.16.1.2      172.16.1.2     20
    255.255.255.255     255.255.255.255  172.16.1.2      172.16.1.2     1
Default Gateway:      172.16.255.254
=====
Persistent Routes:
None
C:\>
```

**Step 1: Open a terminal window on a pod host computer.**

What is the default gateway address?

**Step 2: Use the ping command to verify connectivity with IP address 127.0.0.1.**

Was the ping successful? \_\_\_\_\_

**Step 3: Use the ping command to ping different IP addresses on the 127.0.0.0 network, 127.10.1.1, and 127.255.255.255.**

Were responses successful? If not, why?

---



---

A default gateway address permits a network device to communicate with other devices on different networks. In essence, it is the door to other networks. All traffic destined to different networks must go through the network device that has the default gateway address.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Intel_ac:a7:6a	Broadcast	ARP	Who has 172.16.255.254? Tell 172.16.1.2
2	0.000653	Cisco_cf:66:40	Intel_ac:a7:6a	ARP	172.16.255.254 is at 00:0c:85:cf:66:40
3	0.000659	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
4	0.001808	192.168.254.254	172.16.1.2	ICMP	Echo (ping) reply
5	1.000568	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
6	1.001013	192.168.254.254	172.16.1.2	ICMP	Echo (ping) reply
7	2.000567	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
8	2.001014	192.168.254.254	172.16.1.2	ICMP	Echo (ping) reply
9	3.000577	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
10	3.001009	192.168.254.254	172.16.1.2	ICMP	Echo (ping) reply

**Figure 2. Communication Between Devices on Different Networks**

As shown in Figure 2, communication between devices on different networks is different than on a LAN. Pod host computer #2, IP address 172.16.1.2, initiates a ping to IP address 192.168.254.254. Because network 172.16.0.0 is different from 192.168.254.0, the pod host computer requests the MAC address of the default gateway device. This gateway device, a router, responds with its MAC address. The computer composes the Layer 2 header with the destination MAC address of the router and places frames on the wire to the gateway device.

Referring to Figure 2, what is the MAC address of the gateway device?

---

Referring to Figure 2, what is the MAC address of the network device with IP address 192.168.254.254?

---



## Task 2: Understand how Network Information is Configured on a Windows Computer.

Many times connectivity issues are attributed to wrong network settings. In troubleshooting connectivity issues, several tools are available to quickly determine the network configuration for any Windows computer.

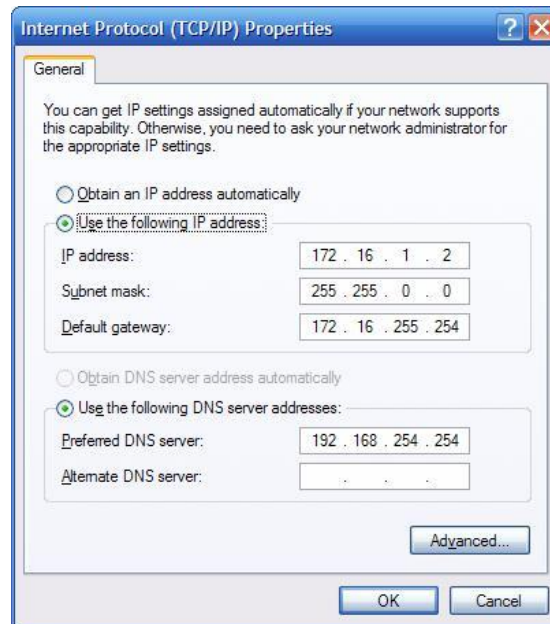


Figure 3. Network Interface with Static IP Address

### Step 1: Examine network properties settings.

One method that may be useful in determining the network interface IP properties is to examine the pod host computer's Network Properties settings. To access this window:

1. Click **Start > Control Panel > Network Connections**.
2. Right-click **Local Area Connection**, and choose **Properties**.
3. On the **General** tab, scroll down the list of items in the pane, select **Internet Protocol (TCP/IP)**, and click the **Properties** button. A window similar to the one in Figure 3 will be displayed.

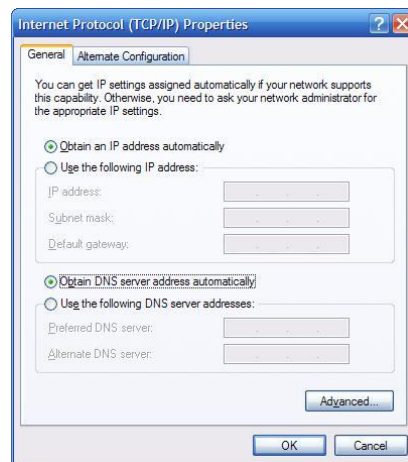


Figure 4. Network Interface with Dynamic IP Address

However, a dynamic IP address may be configured, as shown in Figure 4. In this case, the Network Properties settings window is not very useful for determining IP address information. A more consistently reliable method for determining network settings on a Windows computer is to use the `ipconfig` command:

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . . . :
    1 IP Address. . . . . : 172.16.1.2
    2 Subnet Mask . . . . . : 255.255.0.0
    3 Default Gateway . . . . . : 172.16.255.254
```

- IP address for this pod host computer
- Subnet mask
- Default gateway address

There are several options available with the `ipconfig` command, accessible with the command `ipconfig /?`. To show the most information about the network connections, use the command `ipconfig /all`.

```
C:\>ipconfig /all
Windows IP Configuration
    Host Name . . . . . : GW-desktop-hom
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Intel(R) 82562V 10/100
Network Connection
    Physical Address. . . . . : 00-16-76-AC-A7-6A
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 172.16.1.2
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 172.16.255.254
    1 DNS Servers . . . . . : 192.168.254.254
C:\>
```

- Domain name server IP address

**Step 2:** Using the command `ipconfig /all`, fill in the following table with information from your pod host computer:

Description	Address
IP Address	
Subnet Mask	
Default Gateway	
DNS Server	

**Task 3: Troubleshoot a Hidden Gateway Address Problem.**

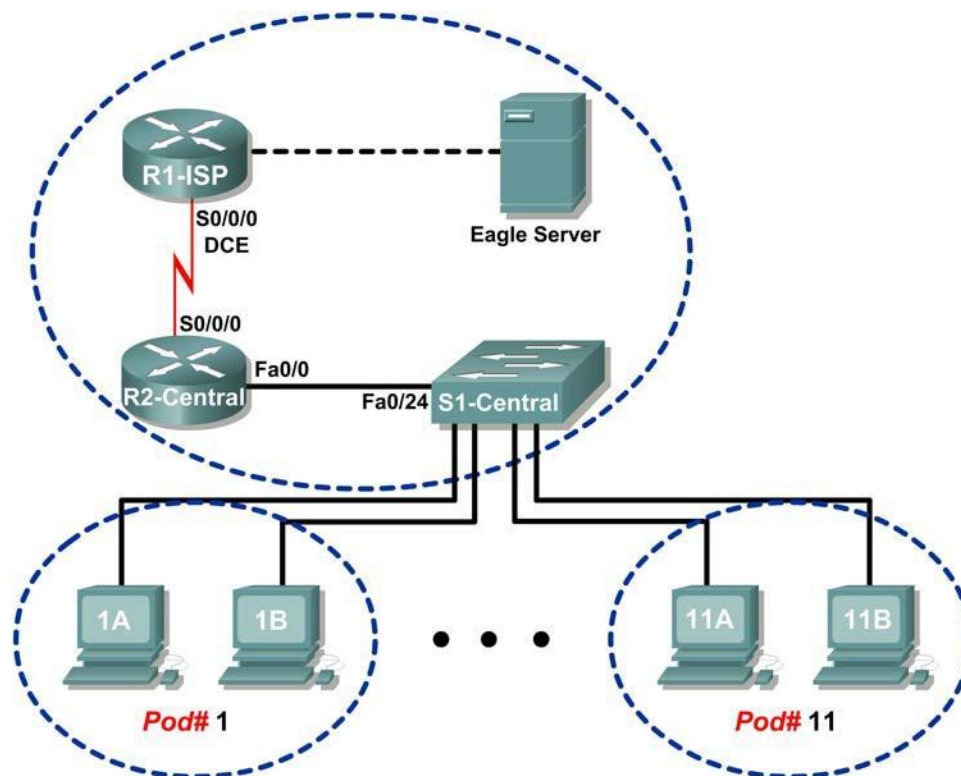


Figure 5. Topology Diagram

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.4	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.3	255.255.255.252	10.10.10.4
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	N/A	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	N/A
hostPod#A	N/A	172.16.Pod#.1	255.255.0.0	172.16.255.254
hostPod#B	N/A	172.16.Pod#.2	255.255.0.0	172.16.255.254
S1-Central	N/A	172.16.254.1	255.255.0.0	172.16.255.254

Table 1. Logical Address Assignments

When troubleshooting network issues, a thorough understanding of the network can often assist in identifying the real problem. Refer to the network topology in Figure 5 and the logical IP address assignments in Table 1.

As the 3rd shift help desk Cisco engineer, you are asked for assistance from the help desk technician. The technician received a trouble ticket from a user on computer host-1A, complaining that computer host-11B, `host-11B.example.com`, does not respond to pings. The technician verified the cables and network settings on both computers, but nothing unusual was found. You check with the corporate network engineer, who reports that R2-Central has been temporarily brought down for a hardware upgrade.

Nodding your head in understanding, you ask the technician to ping the IP address for host-11B, 172.16.11.2 from host-1A. The pings are successful. Then, you ask the technician to ping the gateway IP address, 172.16.254.254, and the pings fail.

What is wrong?

---

---

You instruct the help desk technician to tell the user to use the IP address for host-11B temporarily, and the user is able to establish connectivity with the computer. Within the hour the gateway router is back on line, and normal network operation resumes.

#### **Task 4: Reflection**

A gateway address is critical to network connectivity, and in some instances LAN devices require a default gateway to communicate with other devices on the LAN.

Using Windows command line utilities such as `netstat -r` and `ipconfig /all` will report gateway settings on host computers.

#### **Task 5: Challenge**

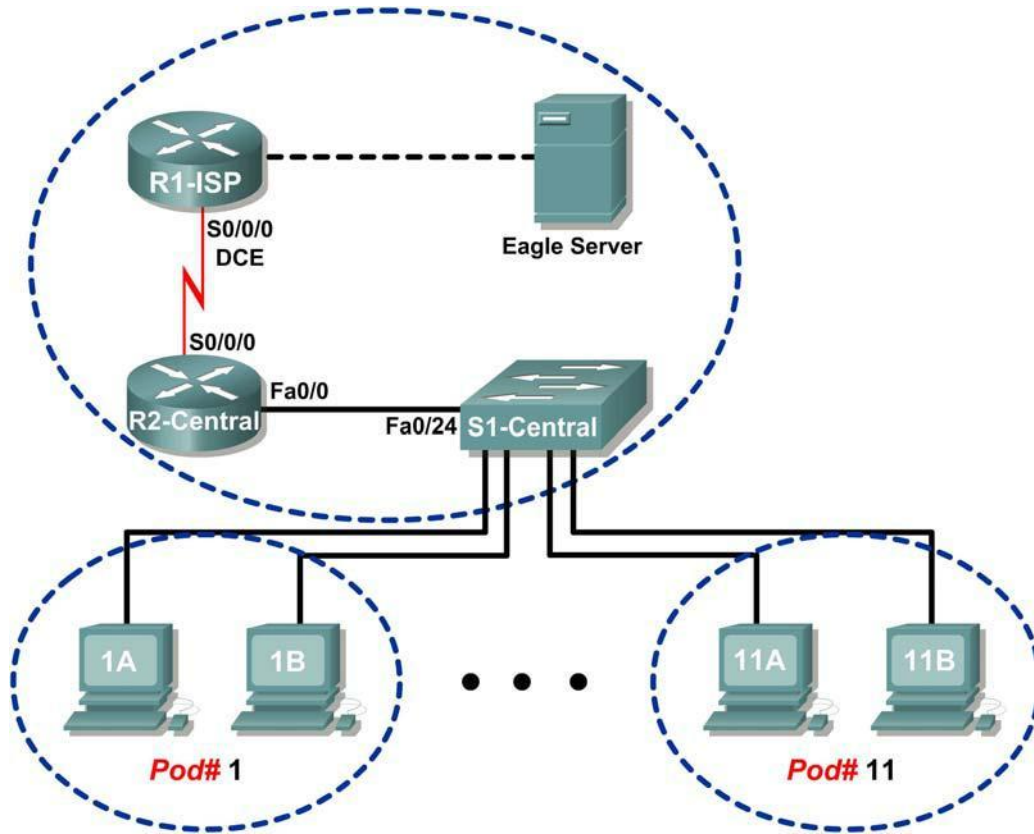
Use Wireshark to capture a ping between two pod host computers. It may be necessary to restart the host computer to flush the DNS cache. First, use the hostname of the destination pod computer for DNS to reply with the destination IP address. Observe the communication sequence between network devices, especially the gateway. Next, capture a ping between network devices using only IP addresses. The gateway address should not be needed.

#### **Task 6: Clean Up**

Unless directed otherwise by the instructor, turn off power to the host computers. Remove anything that was brought into the lab, and leave the room ready for the next class.

## Lab 4: Examining a Route

### Topology Diagram



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	10.10.10.6
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	N/A	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	N/A
hostPod#A	N/A	172.16.Pod#.1	255.255.0.0	172.16.255.254
hostPod#B	N/A	172.16.Pod#.2	255.255.0.0	172.16.255.254
S1-Central	N/A	172.16.254.1	255.255.0.0	172.16.255.254

## Learning Objectives

Upon completion of this lab, you will be able to:

- Use the `route` command to modify a Windows computer routing table.
- Use a Windows Telnet client command `telnet` to connect to a Cisco router.
- Examine router routes using basic Cisco IOS commands.

## Background

For packets to travel across a network, a device must know the route to the destination network. This lab will compare how routes are used in Windows computers and the Cisco router.

Some routes are added to routing tables automatically, based upon configuration information on the network interface. The device considers a network directly connected when it has an IP address and network mask configured, and the network route is automatically entered into the routing table. For networks that are not directly connected, a default gateway IP address is configured that will send traffic to a device that should know about the network.

## Scenario

Using a pod host computer, examine the routing table with the `route` command and identify the different routes and gateway IP address for the route. Delete the default gateway route, test the connection, and then add the default gateway route back to the host table.

Use a pod host computer to telnet into R2-Central, and examine the routing table.

## Task 1: Use the `route` Command to Modify a Windows Computer Routing Table.

```
C:\>netstat -r

Route Table
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x20005 ...00 16 76 ac a7 6a Intel(R) 82562V 10/100 Network Connection
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface Metric
0.0.0.0                0.0.0.0         172.16.255.254  172.16.1.2     1
127.0.0.0              255.0.0.0       127.0.0.1      127.0.0.1     1
172.16.0.0             255.255.0.0     172.16.1.2    172.16.1.2    20
172.16.1.2            255.255.255.255 127.0.0.1     127.0.0.1     20
172.16.255.255        255.255.255.255 172.16.1.2    172.16.1.2    20
255.255.255.255       255.255.255.255 172.16.1.2    172.16.1.2    1
Default Gateway:      172.16.255.254
=====
Persistent Routes:
None
C:\>
```

Figure 1. Output of the `netstat` Command

Shown in Figure 1, output from the `netstat -r` command is useful to determine route and gateway information.

### Step 1: Examine the active routes on a Windows computer.

A useful command to modify the routing table is the `route` command. Unlike the `netstat -r` command, the `route` command can be used to view, add, delete, or change routing table entries. To view detailed information about the `route` command, use the option `route /?`.

An abbreviated option list for the `route` command is shown below:

```

route PRINT          Prints active routes
route ADD           Adds a route:
                      route ADD network MASK mask gateway
route DELETE       Deletes a route:
                      route DELETE network
route CHANGE      Modifies an existing route

```

To view active routes, issue the command `route PRINT`:

```

C:\ >route PRINT
=====
=
Interface List
0x1 ..... MS TCP Loopback interface
0x70003 ...00 16 76 ac a7 6a .Intel(R) 82562V 10/100 Network Connection
=====
=
=
Active Routes:
Network Destination    Netmask          Gateway          Interface Metric
      0.0.0.0             0.0.0.0         172.16.255.254   172.16.1.2     1
      127.0.0.0           255.0.0.0       127.0.0.1        127.0.0.1     1
      172.16.0.0          255.255.0.0     172.16.1.2       172.16.1.2    20
      172.16.1.2          255.255.255.255 127.0.0.1        127.0.0.1    20
      172.16.255.255      255.255.255.255 172.16.1.2       172.16.1.2    20
      255.255.255.255     255.255.255.255 172.16.1.2       172.16.1.2     1
Default Gateway:       172.16.255.254
=====
=
Persistent Routes:
    None
C:\>

```

Verify network connectivity to Eagle Server:

```

C:\> ping eagle-server.example.com
Pinging eagle-server.example.com [192.168.254.254] with
32 bytes of data:

Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63

Ping statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average =
0ms C:\>

```

What is the gateway address to `eagle-server.example.com`?

---

**Step 2: Delete a route from the Windows computer routing table.**

How important is the default gateway route? Delete the gateway route, and try to ping Eagle Server. The syntax to remove the default gateway route is:

```
route DELETE network  
  
C: /> route DELETE 0.0.0.0
```

Examine the active routing table and verify that the default gateway route has been removed: What is the default gateway IP address?

---

Try to ping Eagle Server. What are the results?

---

If the default gateway IP address is removed, how can the DNS server be reached to resolve `eagle-server.example.com`?

Can other LAN devices be reached, such as `172.16.255.254`?

---

**Step 3: Insert a route into the Windows computer routing table.**

In the following configuration, use the IP address assigned to your host pod interface. The syntax to add a route to the Windows computer routing table is:

```
route ADD network MASK mask gateway-IP address  
  
C: /> route ADD 0.0.0.0 MASK 0.0.0.0 172.16.255.254
```

Examine the active routing table, and verify that the default gateway route has been restored:

Has the default gateway route been restored? \_\_\_\_\_:

Try to ping Eagle Server. What are the results?

---

**Task 2: Use a Windows Telnet Client Command `telnet` to Connect to a Cisco Router.**

In this task, you will telnet into the R2-Central router and use common IOS commands to examine the router routing table. Cisco devices have a Telnet server and, if properly configured, will permit remote logins. Access to the router is restricted, however, and requires a username and password. The password for all usernames is `cisco`. The username depends on the pod.



Username `ccna1` is for users on pod 1 computer, `ccna2` is for students on pod 2 computers, and so on.

### Step 1: Using the Windows Telnet client, log in to a Cisco router.

Open a terminal window by clicking **Start > Run**. Type `cmd`, and click **OK**. A terminal window and prompt should be available. The Telnet utility has several options and can be viewed with the `telnet /?` command. A username and password will be required to log in to the router. For all usernames, the corresponding password is `cisco`.

Pod Number	Username
1	ccna1
2	ccna2
3	ccna3
4	ccna4
5	ccna5
6	ccna6
7	ccna7
8	ccna8
9	Ccna9
10	ccna10
11	ccna11

To start a Telnet session with router R2-central, type the command:

```
C: /> telnet 172.16.255.254 <ENTER>
```

A login window will prompt for a username, as shown below. Enter the applicable username, and press **<ENTER>**. Enter the password, `cisco`, and press **<ENTER>**. The router prompt should be visible after a successful login.

```
*****
                This is Eagle 1 lab router R2-Central.
                Authorized access only.
*****

User Access Verification

Username: ccna1
Password: cisco (hidden)
R2-Central#
```

At the prompt, `R2-Central#`, a successful Telnet login has been created. Only limited permissions for `ccnax` usernames are available; therefore, it is not possible to modify router settings or view the configuration. The purpose of this task was to establish a Telnet session, which has been accomplished. In the next task, the router routing table will be examined.

### Task 3: Examine Router Routes using Basic Cisco IOS Commands.

As with any network device, gateway addresses instruct the device about how to reach other networks when no other information is available. Similar to the host computer default gateway IP address, a router may also employ a default gateway. Also similar to a host computer, a router is knowledgeable about directly connected networks.

This task will not examine Cisco IOS commands in detail but will use a common IOS command to view the routing table. The syntax to view the routing table is:

```
show ip route <ENTER>
```

### Step 1: Enter the command to display the router routing table.

The route information displayed is much more detailed than the route information on a host computer. This is to be expected, because the job of a router is to route traffic between networks. The information required of this task, however, is not difficult to glean. Figure 2 shows the routing table for R2-Central.

```
R2-Central#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 10.10.10.6 to network 0.0.0.0

C    172.16.0.0/16 is directly connected, FastEthernet0/0
     10.0.0.0/30 is subnetted, 1 subnets
C      10.10.10.4 is directly connected, Serial10/2/0
S*   0.0.0.0/0 [1/0] via 10.10.10.6
R2-Central#
```

Figure 2. Output of the Cisco IOS show ip route Command

The Codes section shown in Figure 3 provides an explanation for the symbols to the left of each route entry.

```
R2-Central#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

4 Gateway of last resort is 10.10.10.6 to network 0.0.0.0

1 C    172.16.0.0/16 is directly connected, FastEthernet0/0
     10.0.0.0/30 is subnetted, 1 subnets
1 C      10.10.10.4 is directly connected, Serial10/2/0
2 3 S*   0.0.0.0/0 [1/0] via 10.10.10.6
R2-Central#
```

Figure 3. Explanation of Codes

- C denotes directly connected networks and the interface that supports the connection.
- S denotes a static route, which is manually entered by the Cisco network engineer.
- Because the route is "quad-zero," it is a candidate default route.
  - If there is no other route in the routing table, use this gateway of last resort IP address to forward packets.

How is IP mask information displayed in a router routing table?

What would the router do with packets destined to 192.168.254.254?

---

---

When finished examining the routing table, exit the router with the command `exit` <ENTER>. The telnet client will also close the connection with the telnet escape sequence <CTRL> ] and `quit`. Close the terminal window.

#### Task 4: Reflection

Two new Windows commands were used in this lab. The `route` command was used to view, delete, and add route information on the pod host computer.

The Windows Telnet client, `telnet`, was used to connect to a lab router, R2-Central. This technique will be used in other labs to connect to Cisco network devices.

The router routing table was examined with the Cisco IOS command `show ip route`. Routes for directly connected networks, statically assigned routes, and gateway of last resort information are displayed.

#### Task 5: Challenge

Other Cisco IOS commands can be used to view IP address information on a router. Similar to the Windows `ipconfig` command, the Cisco IOS command `show ip interface brief` will display IP address assignments.

```
R2-Central#show ip interface brief
Interface          IP-Address      OK? Method Status
Protocol
FastEthernet0/0    172.16.255.254 YES manual up
FastEthernet0/1    unassigned      YES unset  administratively down
down
Serial10/2/0       10.10.10.5      YES manual up
Serial10/2/1       unassigned      YES unset  administratively down
down
R2-Central#
```

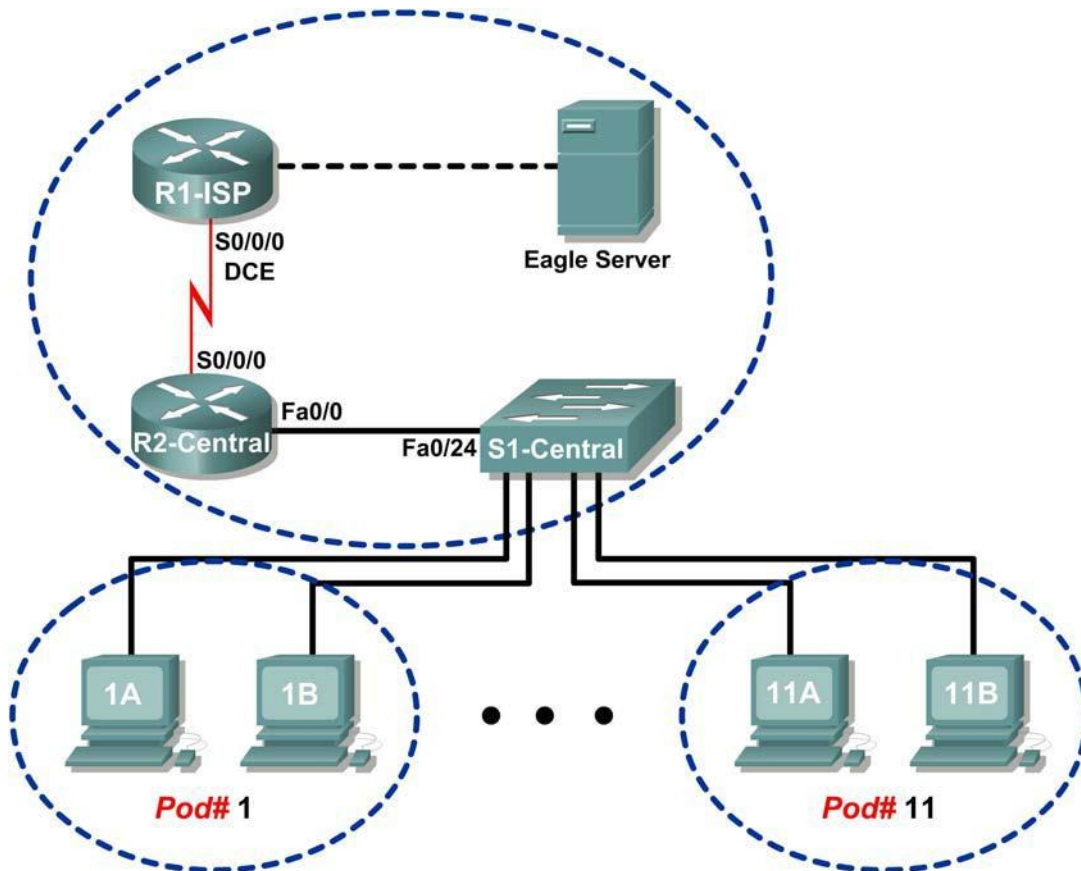
Using Windows commands and the Cisco IOS commands in this lab, compare network information output. What was missing? What critical network information was similar?

---

---

## Lab 5: Ping and Traceroute

### Topology Diagram



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	10.10.10.6
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	N/A	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	N/A
hostPod#A	N/A	172.16.Pod#.1	255.255.0.0	172.16.255.254
hostPod#B	N/A	172.16.Pod#.2	255.255.0.0	172.16.255.254
S1-Central	N/A	172.16.254.1	255.255.0.0	172.16.255.254

## Learning Objectives

Upon completion of this lab, you will be able to:

- Use the `ping` command to verify simple TCP/IP network connectivity.
- Use the `tracert/traceroute` command to verify TCP/IP connectivity.

## Background

Two tools that are indispensable when testing TCP/IP network connectivity are `ping` and `tracert`. The `ping` utility is available on Windows, Linux, and Cisco IOS, and tests network connectivity. The `tracert` utility is available on Windows, and a similar utility, `traceroute`, is available on Linux and Cisco IOS. In addition to testing for connectivity, `tracert` can be used to check for network latency.

For example, when a web browser fails to connect to a web server, the problem can be anywhere between client and the server. A network engineer may use the `ping` command to test for local network connectivity or connections where there are few devices. In a complex network, the `tracert` command would be used. Where to begin connectivity tests has been the subject of much debate; it usually depends on the experience of the network engineer and familiarity with the network.

The Internet Control Message Protocol (ICMP) is used by both `ping` and `tracert` to send messages between devices. ICMP is a TCP/IP Network layer protocol, first defined in RFC 792, September, 1981. ICMP message types were later expanded in RFC 1700.

## Scenario

In this lab, the `ping` and `tracert` commands will be examined, and command options will be used to modify the command behavior. To familiarize the students with the use of the commands, devices in the Cisco lab will be tested.

Measured delay time will probably be less than those on a production network. This is because there is little network traffic in the Eagle 1 lab.

## Task 1: Use the `ping` Command to Verify Simple TCP/IP Network Connectivity.

The `ping` command is used to verify TCP/IP Network layer connectivity on the local host computer or another device in the network. The command can be used with a destination IP address or qualified name, such as `eagle-server.example.com`, to test domain name services (DNS) functionality. For this lab, only IP addresses will be used.

The `ping` operation is straightforward. The source computer sends an ICMP echo request to the destination. The destination responds with an echo reply. If there is a break between the source and destination, a router may respond with an ICMP message that the host is unknown or the destination network is unknown.

### Step 1: Verify TCP/IP Network layer connectivity on the local host computer.

```
C:\> ipconfig

Windows IP Configuration
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 172.16.1.2
    Subnet Mask . . . . .             : 255.255.0.0
    Default Gateway . . . . .         : 172.16.255.254

C:\>
```

Figure 1. Local TCP/IP Network Information

1. Open a Windows terminal and determine IP address of the pod host computer with the `ipconfig` command, as shown in Figure 1.

The output should look the same except for the IP address. Each pod host computer should have the same network mask and default gateway address; only the IP address may differ. If the information is missing or if the subnet mask and default gateway are different, reconfigure the TCP/IP settings to match the settings for this pod host computer.

2. Record information about local TCP/IP network information:

TCP/IP Information	Value
IP Address	
Subnet Mask	
Default Gateway	

```

C:\> ping 172.16.1.2
Pinging 172.16.1.1 with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
    
```

Figure 2. Output of the ping Command on the Local TCP/IP Stack

3. Use the `ping` command to verify TCP/IP Network layer connectivity on the local host computer.

By default, four ping requests are sent to the destination and reply information is received. Output should look similar to that shown in Figure 2.

- Destination address, set to the IP address for the local computer.

- Reply information:

- bytes—size of the ICMP packet.

- time—elapsed time between transmission and reply.

- TTL—default TTL value of the DESTINATION device, minus the number of routers in the path. The maximum TTL value is 255, and for newer Windows machines the default value is 128.

- Summary information about the replies:

- Packets Sent—number of packets transmitted. By default, four packets are sent.

- Packets Received—number of packets received.

- Packets Lost —difference between number of packets sent and received.

- Information about the delay in replies, measured in milliseconds. Lower round trip times indicate faster links. A computer timer is set to 10 milliseconds. Values faster than 10 milliseconds will display 0.

- Fill in the results of the `ping` command on your computer:

Field	Value
Size of packet	
Number of packets sent	
Number of replies	
Number of lost packets	
Minimum delay	
Maximum delay	
Average delay	

**Step 2: Verify TCP/IP Network layer connectivity on the LAN.**

```
C:\> ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:
Reply from 172.16.255.254: bytes=32 time=1ms TTL=255
Reply from 172.16.255.254: bytes=32 time<1ms TTL=255
Reply from 172.16.255.254: bytes=32 time<1ms TTL=255
Reply from 172.16.255.254: bytes=32 time<1ms TTL=255
Ping statistics for 172.16.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average =
0ms C:\>
```

**Figure 3. Output of the ping Command to the Default Gateway**

- Use the `ping` command to verify TCP/IP Network layer connectivity to the default gateway. Results should be similar to those shown in Figure 3. Cisco IOS default TTL value is set to 255. Because the router was not crossed, the TTL value returned is 255.
- Fill in the results of the `ping` command to the default Gateway:

Field	Value
Size of packet	
Number of packets sent	
Number of replies	
Number of lost packets	
Minimum delay	
Maximum delay	
Average delay	

What would be the result of a loss of connectivity to the default gateway?

---

**Step 3: Verify TCP/IP Network layer connectivity to a remote network.**

```
C:\> ping 192.168.254.254

Pinging 192.168.254.254 with 32 bytes of data: Reply
from 192.168.254.254: bytes=32 time<1ms TTL=62 Reply
from 192.168.254.254: bytes=32 time<1ms TTL=62 Reply
from 192.168.254.254: bytes=32 time<1ms TTL=62 Reply
from 192.168.254.254: bytes=32 time<1ms TTL=62 Ping
statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average =
0ms C:\>
```

#### Figure 4. Output of the ping Command to Eagle Server

1. Use the **ping** command to verify TCP/IP Network layer connectivity to a device on a remote network. In this case, Eagle Server will be used. Results should be similar to those shown in Figure 4.

Linux default TTL value is set to 64. Two routers were crossed to reach Eagle Server, therefore the returned TTL value is 62.

2. Fill in the results of the **ping** command on your computer:

Field	Value
Size of packet	
Number of packets sent	
Number of replies	
Number of lost packets	
Minimum delay	
Maximum delay	
Average delay	

```
C:\ > ping 192.168.254.254
Pinging 192.168.254.254 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.254.254:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Figure 5. Output of a ping Command with Lost Packets

The **ping** command is extremely useful when troubleshooting network connectivity. However, there are limitations. In Figure 5, the output shows that a user cannot reach Eagle Server. Is the problem with Eagle Server or a device in the path? The **tracert** command, examined next, can display network latency and path information.

#### Task 2: Use the tracert Command to Verify TCP/IP Connectivity.

The **tracert** command is useful for learning about network latency and path information. Instead of using the **ping** command to test connectivity of each device to the destination, one by one, the **tracert** command can be used.

On Linux and Cisco IOS devices, the equivalent command is **traceroute**.

##### Step 1: Verify TCP/IP Network layer connectivity with the tracert command.

1. Open a Windows terminal and issue the following command:

```
C:\> tracert 192.168.254.254
```

```
C:\> tracert 192.168.254.254
Tracing route to 192.168.254.254 over a maximum of 30 hops
  1  <1 ms    <1 ms    <1 ms    172.16.255.254
  2  <1 ms    <1 ms    <1 ms    10.10.10.6
  3  <1 ms    <1 ms    <1 ms    192.168.254.254
Trace complete.
C:\>
```

Figure 6. Output of the tracert command to Eagle Server.



- Output from the `tracert` command should be similar to that shown in Figure 6.
- Record your result in the following table:

Field	Value
Maximum number of hops	
First router IP address	
Second router IP address	
Destination reached?	

**Step 2: Observe `tracert` output to a host that lost network connectivity.**

If there is a loss of connectivity to an end device such as Eagle Server, the `tracert` command can give valuable clues as to the source of the problem. The `ping` command would show the failure but not any other kind of information about the devices in the path. Referring to the Eagle 1 lab Topology Diagram, both R2-Central and R1-ISP are used for connectivity between the pod host computers and Eagle Server.

```
C:\> tracert -w 5 -h 4 192.168.254.254

Tracing route to 192.168.254.254 over a maximum of 4 hops
  0  <1 ms    <1 ms    <1 ms    172.16.255.254
  1  <1 ms    <1 ms    <1 ms    10.10.10.6
  2  *         *         *         Request timed out.
  3  *         *         *         Request timed out.

Trace complete.
C:\>
```

**Figure 7. Output of the `tracert` Command**

Refer to Figure 7. Options are used with the `tracert` command to reduce wait time (in milliseconds), `-w 5`, and maximum hop count, `-h 4`. If Eagle Server was disconnected from the network, the default gateway would respond correctly, as well as R1-ISP. The problem must be on the `192.168.254.0/24` network. In this example, Eagle Server has been turned off.

What would the `tracert` output be if R1-ISP failed?

---

What would the `tracert` output be if R2-Central failed?

---

**Task 3: Challenge**

The default values for the `ping` command normally work for most troubleshooting scenarios. There are times, however, when fine tuning `ping` options may be useful. Issuing the `ping` command without any destination address will display the options shown in Figure 8.

```

C:\> ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-
          list]] [-w timeout] target_name

Options:
  -t          Ping the specified host until stopped.
              To see statistics and continue - type Control-Break;
              To stop - type Control-C.
  -a          Resolve addresses to hostnames.
  -n count    Number of echo requests to send.
  -l size     Send buffer size.
  -f          Set Don't Fragment flag in packet.
  -i TTL      Time To Live.
  -v TOS      Type Of Service.
  -r count    Record route for count hops.
  -s count    Timestamp for count hops.
  -j host-list Loose source route along host-list.
  -k host-list Strict source route along host-list.
  -w timeout  Timeout in milliseconds to wait for each reply.

C:\>

```

**Figure 8. Output of a ping Command with no Destination Address**

The most useful options are highlighted in yellow. Some options do not work together, such as the `-t` and `-n` options. Other options can be used together. Experiment with the following options:

To ping the destination address until stopped, use the `-t` option. To stop, press <CTRL> C:

```

C:\> ping -t 192.168.254.254

Pinging 192.168.254.254 with 32 bytes of data: Reply
from 192.168.254.254: bytes=32 time<1ms TTL=63 Reply
from 192.168.254.254: bytes=32 time<1ms TTL=63 Reply
from 192.168.254.254: bytes=32 time<1ms TTL=63 Reply
from 192.168.254.254: bytes=32 time<1ms TTL=63 Reply
from 192.168.254.254: bytes=32 time<1ms TTL=63 Reply
from 192.168.254.254: bytes=32 time<1ms TTL=63 Ping
statistics for 192.168.254.254:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\>

```

**Figure 9. Output of a ping Command using the -t Option**

To ping the destination once, and record router hops, use the `-n` and `-r` options, as shown in Figure 10. **Note:** Not all devices will honor the `-r` option.

```
C:\> ping -n 1 -r 9 192.168.254.254
Pinging 192.168.254.254 with 32 bytes of data:
Reply from 192.168.254.254: bytes=32 time=1ms TTL=63
    Route:          10.10.10.5 ->
                192.168.254.253 ->
                192.168.254.254 ->
                10.10.10.6 ->
                172.16.255.254
Ping statistics for 192.168.254.254:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average =
1ms C:\>
```

**Figure 10. Output of a ping Command using the -n and -r Options**

#### **Task 4: Reflection**

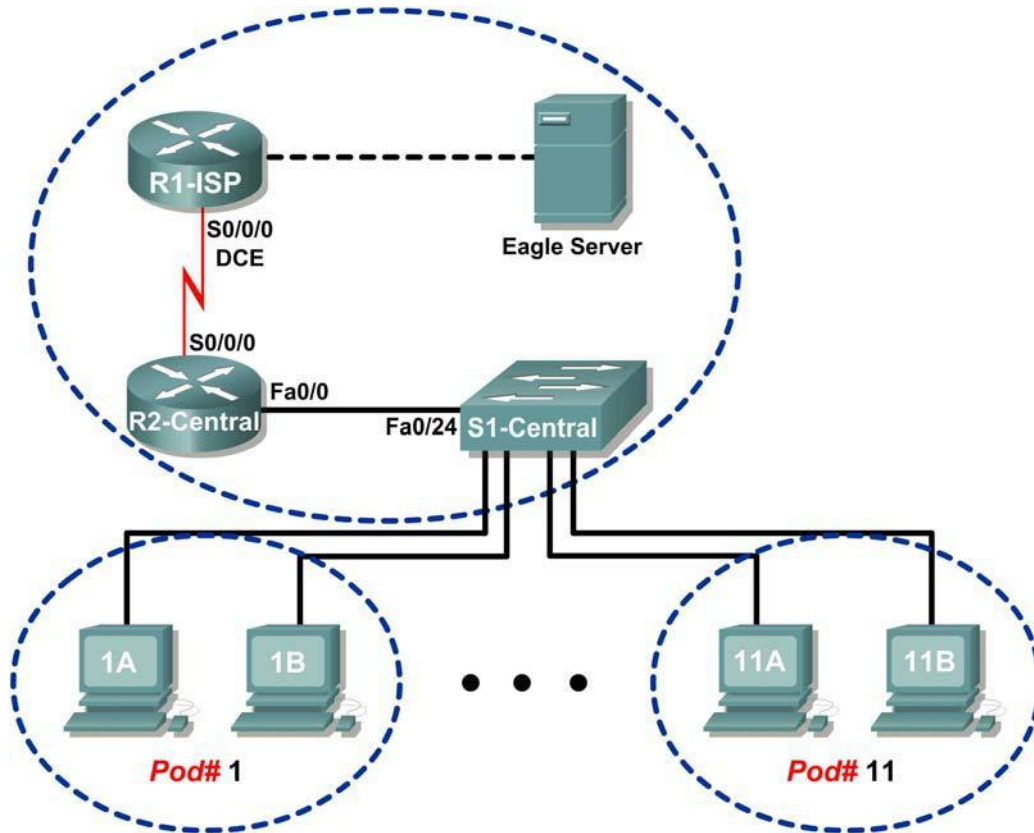
Both **ping** and **tracert** are used by network engineers to test network connectivity. For basic network connectivity, the **ping** command works best. To test latency and the network path, the **tracert** command is preferred. The ability to accurately and quickly diagnose network connectivity issues is a skill expected from a network engineer. Knowledge about the TCP/IP protocols and practice with troubleshooting commands will build that skill.

#### **Task 5: Clean Up**

Unless directed otherwise by the instructor, turn off power to the host computers. Remove anything that was brought into the lab, and leave the room ready for the next class.

## Lab 6: Examining ICMP Packets

### Topology Diagram



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	10.10.10.6
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	N/A	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	N/A
hostPod#A	N/A	172.16.Pod#.1	255.255.0.0	172.16.255.254
hostPod#B	N/A	172.16.Pod#.2	255.255.0.0	172.16.255.254
S1-Central	N/A	172.16.254.1	255.255.0.0	172.16.255.254

## Learning Objectives

Upon completion of this lab, you will be able to:

- Understand the format of ICMP packets.
- Use Wireshark to capture and examine ICMP messages.

## Background

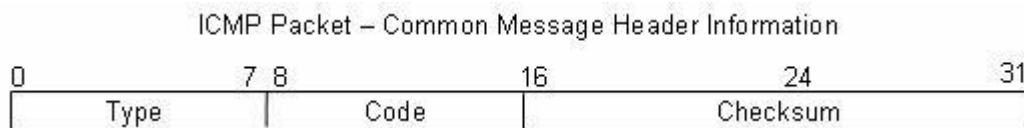
The Internet Control Message Protocol (ICMP) was first defined in RFC 792, September, 1981. ICMP message types were later expanded in RFC 1700. ICMP operates at the TCP/IP Network layer and is used to exchange information between devices.

ICMP packets serve many uses in today's computer network. When a router cannot deliver a packet to a destination network or host, an informational message is returned to the source. Also, the `ping` and `tracert` commands send ICMP messages to destinations, and destinations respond with ICMP messages.

## Scenario

Using the Eagle 1 Lab, Wireshark captures will be made of ICMP packets between network devices.

### Task 1: Understand the Format of ICMP Packets.



**Figure 1. ICMP Message Header**

Refer to Figure 1, the ICMP header fields common to all ICMP message types. Each ICMP message starts with an 8-bit Type field, an 8-bit Code field, and a computed 16-bit Checksum. The ICMP message type describes the remaining ICMP fields. The table in Figure 2 shows ICMP message types from RFC 792:

Value	Meaning
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply

**Figure 2. ICMP Message Types**

Codes provide additional information to the Type field. For example, if the Type field is 3, destination unreachable, additional information about the problem is returned in the Code field.

The table in Figure 3 shows message codes for an ICMP Type 3 message, destination unreachable, from RFC 1700:

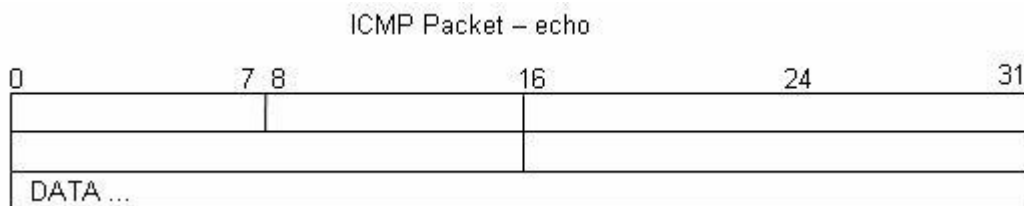
Code Value	Meaning
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation Needed and Don't Fragment was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network is Administratively Prohibited
10	Communication with Destination Host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service

**Figure 3. ICMP Type 3 Message Codes**

Using ICMP message capture shown in Figure 4, fill in the fields for the ICMP packet echo request. Values beginning with 0x are hexadecimal numbers:

```
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x365c [correct]
Identifier: 0x0200
Sequence number: 0x1500
Data (32 bytes)
```

**Figure 4. ICMP Packet Echo Request**



Using the ICMP message capture shown in Figure 5, fill in the fields for the ICMP packet echo reply:

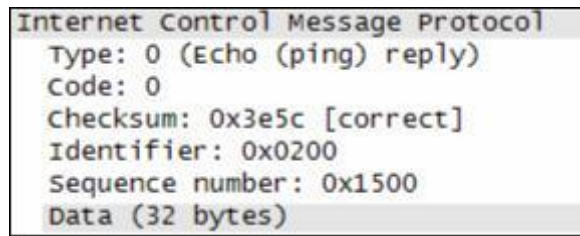
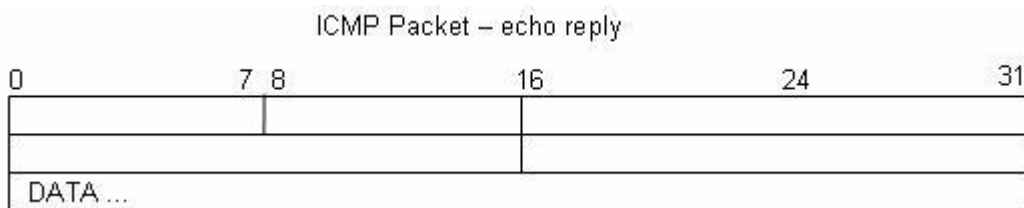


Figure 5. ICMP Packet Echo Reply



At the TCP/IP Network layer, communication between devices is not guaranteed. However, ICMP does provide minimal checks for a reply to match the request. From the information provided in the ICMP messages above, how does the sender know that the reply is to a specific echo?

---



---

**Task 2: Use Wireshark to Capture and Examine ICMP Messages.**

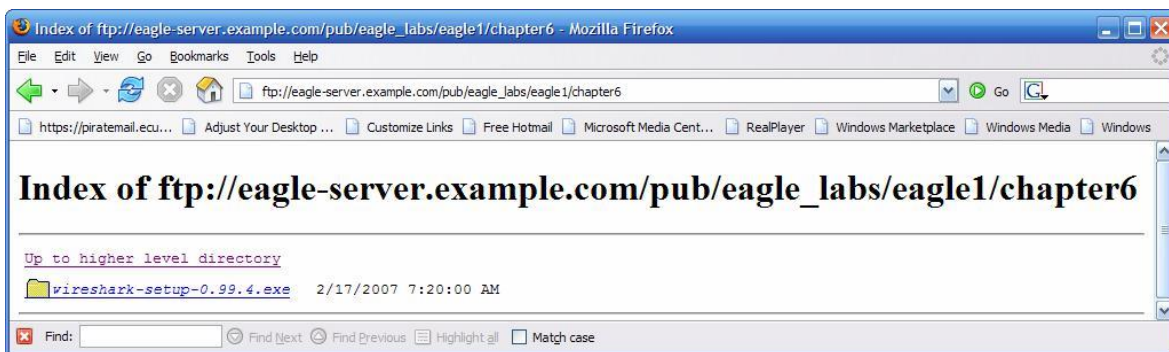


Figure 6. Wireshark Download Site

If Wireshark has not been loaded on the pod host computer, it can be downloaded from Eagle Server.

1. Open a web browser, URL [FTP://eagle-server.example.com/pub/eagle\\_labs/eagle1/chapter6](ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter6), as shown in Figure 6.

2. Right-click the Wireshark filename, click **Save Link As**, and save the file to the pod host computer.
3. When the file has been downloaded, open and install Wireshark.

### Step 1: Capture and evaluate ICMP echo messages to Eagle Server.

In this step, Wireshark will be used to examine ICMP echo messages.

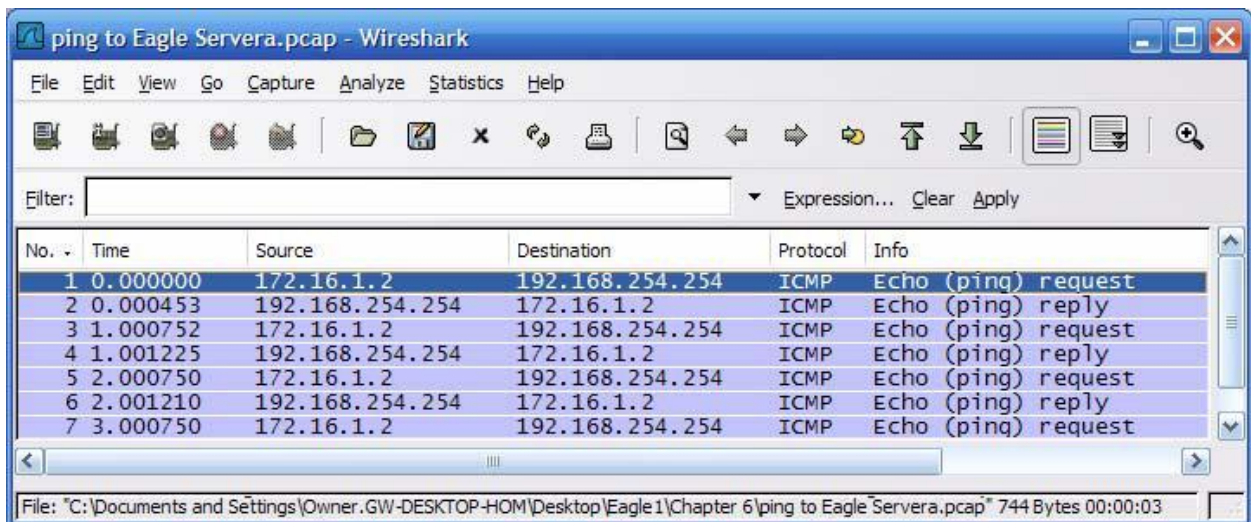
1. Open a Windows terminal on the pod host computer.
2. When ready, start Wireshark capture.

```
C:\> ping eagle-server.example.com

Pinging eagle-server.example.com [192.168.254.254] with 32
bytes of data:
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Ping statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average =
0ms C:\>
```

**Figure 7. Successful ping Replies from Eagle Server**

3. From the Windows terminal, ping Eagle Server. Four successful replies should be received from Eagle Server, as shown in Figure 7.
4. Stop Wireshark capture. There should be a total of four ICMP echo requests and matching echo replies, similar to those shown in Figure 8.



**Figure 8. Wireshark Capture of ping Requests and Replies**

Which network device responds to the ICMP echo request?

---



- Expand the middle window in Wireshark, and expand the Internet Control Message Protocol record until all fields are visible. The bottom window will also be needed to examine the Data field.
- Record information from the *first* echo request packet to Eagle Server:

Field	Value
Type	
Code	
Checksum	
Identifier	
Sequence number	
Data	

Are there 32 bytes of data? \_\_\_\_\_

- Record information from the *first* echo reply packet from Eagle Server:

Field	Value
Type	
Code	
Checksum	
Identifier	
Sequence number	
Data	

Which fields, if any, changed from the echo request?

---

- Continue to evaluate the remaining echo requests and replies. Fill in the following information from each new ping:

Packet	Checksum	Identifier	Sequence number
Request # 2			
Reply # 2			
Request # 3			
Reply # 3			
Request # 4			
Reply # 4			

Why did the Checksum values change with each new request?

---

**Step 2: Capture and evaluate ICMP echo messages to 192.168.253.1.**

In this step, pings will be sent to a fictitious network and host. The results from the Wireshark capture will be evaluated—and may be surprising.

Try to ping IP address 192.168.253.1.

```
C:\> ping 192.168.253.1

C:\> ping 192.168.253.1
Pinging 192.168.253.1 with 32 bytes of data:
Reply from 172.16.255.254: Destination host unreachable.
Reply from 172.16.255.254: Destination host unreachable.
Reply from 172.16.255.254: Destination host unreachable.
Reply from 172.16.255.254: Destination host unreachable.
Ping statistics for 192.168.253.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average =
0ms C:\>
```

**Figure 9. Ping Results from a Fictitious Destination**

See Figure 9. Instead of a request timeout, there is an echo response.

What network device responds to pings to a fictitious destination?

---

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
2	0.000816	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
3	1.000854	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
4	1.001686	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
5	2.001815	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
6	2.002547	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
7	3.002815	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
8	3.003588	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)

**Figure 10. Wireshark Capture from a Fictitious Destination**

Wireshark captures to a fictitious destination are shown in Figure 10. Expand the middle Wireshark window and the Internet Control Message Protocol record.

Which ICMP message type is used to return information to the sender?

---

What is the code associated with the message type?

---

**Step 3: Capture and evaluate ICMP echo messages that exceed the TTL value.**

In this step, pings will be sent with a low TTL value, simulating a destination that is unreachable. Ping Eagle Server, and set the TTL value to 1:

```
C:\> ping -i 1 192.168.254.254
```

```
C:\> ping -i 1 192.168.254.254
Pinging 192.168.254.254 with 32 bytes of data:
Reply from 172.16.255.254: TTL expired in transit.
Reply from 172.16.255.254: TTL expired in transit.
Reply from 172.16.255.254: TTL expired in transit.
Reply from 172.16.255.254: TTL expired in transit.
Ping statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average =
    0ms C:\>
```

**Figure 11. Ping Results for an Exceeded TTL**

See Figure 11, which shows ping replies when the TTL value has been exceeded.

What network device responds to pings that exceed the TTL value?

---

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
2	0.000701	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
3	1.000003	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
4	1.000687	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
5	1.999996	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
6	2.000761	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
7	3.000970	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
8	3.001723	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)

**Figure 12. Wireshark Capture of TTL Value Exceeded**

Wireshark captures to a fictitious destination are shown in Figure 12. Expand the middle Wireshark window and the Internet Control Message Protocol record.

Which ICMP message type is used to return information to the sender?

---

What is the code associated with the message type?

---

Which network device is responsible for decrementing the TTL value?

---

**Task 3: Challenge**

Use Wireshark to capture a `tracert` session to Eagle Server and then to 192.168.254.251. Examine the ICMP TTL exceeded message. This will demonstrate how the `tracert` command traces the network path to the destination.

**Task 4: Reflection**

The ICMP protocol is very useful when troubleshooting network connectivity issues. Without ICMP messages, a sender has no way to tell why a destination connection failed. Using the `ping` command, different ICMP message type values were captured and evaluated.

**Task 5: Clean Up**

Wireshark may have been loaded on the pod host computer. If the program must be removed, click **Start > Control Panel > Add or Remove Programs**, and scroll down to Wireshark. Click the filename, click **Remove**, and follow uninstall instructions.

Remove any Wireshark pcap files that were created on the pod host computer.

Unless directed otherwise by the instructor, turn off power to the host computers. Remove anything that was brought into the lab, and leave the room ready for the next class.

## Lab 7: IPv4 Address Subnetting

### Learning Objectives

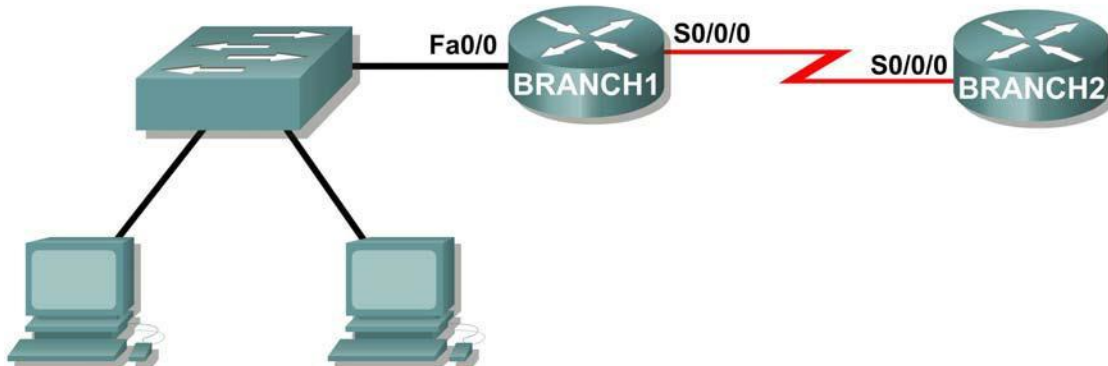
Upon completion of this lab, you will be able to:

- Determine the number of subnets.
- Design an appropriate addressing scheme.
- Assign addresses and subnet mask pairs to device interfaces.
- Examine the use of the available network address space.

### Scenario

In this lab, you have been given the network address 192.168.26.0/24 to subnet and provide the IP addressing for the networks shown in the Topology Diagrams. You must determine the number of networks needed then design an appropriate addressing scheme. Place the correct address and mask in the Addressing Table. In this example, the number of hosts is not important. You are only required to determine the number of subnets per topology example.

### Topology Diagram A



#### Task 1: Determine the Number of Subnets in the Topology Diagram.

**Step 1:** How many networks are there? \_\_\_\_

**Step 2:** How many bits should you borrow to create the required number of subnets? \_\_\_\_

**Step 3:** How many usable host addresses and usable subnets did this give you? \_\_\_\_

**Step 4:** What is the new subnet mask in decimal form? \_\_\_\_\_

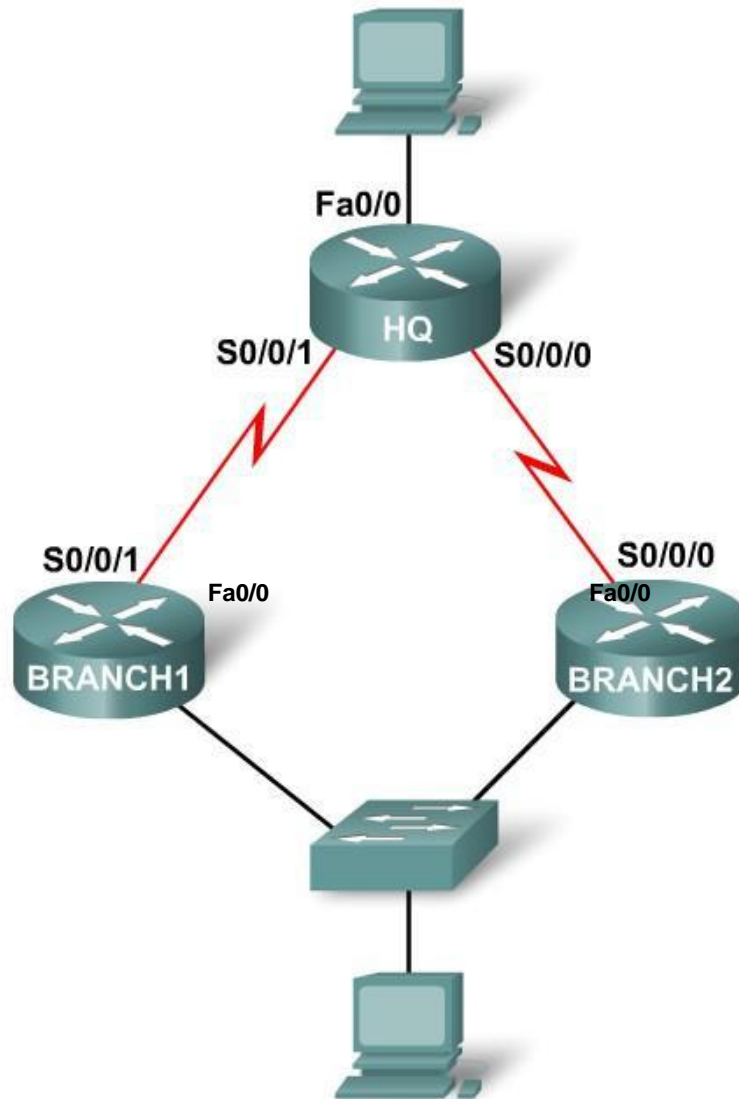
**Step 5:** How many subnets are available for future use? \_\_\_\_

**Task 2: Record Subnet Information.**

Step 1: Fill in the following chart with the subnet information.

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0				
1				
2				
3				
4				
5				
6				
7				

**Topology Diagram B**



**Task 1: Determine the Number of Subnets in the Topology Diagram.**

**Step 1:** How many networks are there? \_\_\_\_

**Step 2:** How many bits should you borrow to create the required number of subnets? \_\_\_\_

**Step 3:** How many usable host addresses and usable subnets did this give you? \_\_\_\_

**Step 4:** What is the new subnet mask in decimal form? \_\_\_\_\_

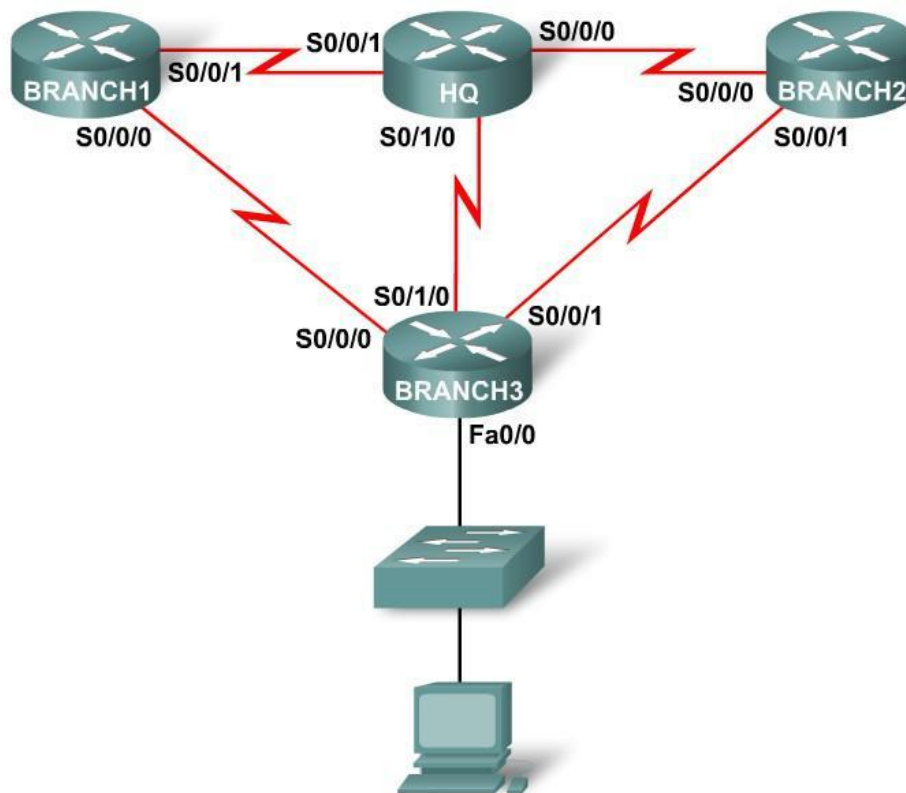
**Step 5:** How many subnets are available for future use? \_\_\_\_

**Task 2: Record Subnet Information.**

**Step 1:** Fill in the following chart with the subnet information.

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0				
1				
2				
3				
4				
5				
6				
7				

**Topology Diagram C**



**Task 1: Determine the Number of Subnets in the Topology Diagram.**

**Step 1:** How many networks are there? \_\_\_\_\_

**Step 2:** How many bits should you borrow to create the required number of subnets? \_\_\_\_\_

**Step 3:** How many usable host addresses and usable subnets did this give you? \_\_\_\_\_

**Step 4:** What is the new subnet mask in decimal form? \_\_\_\_\_

**Step 5:** How many subnets are available for future use? \_\_\_\_\_

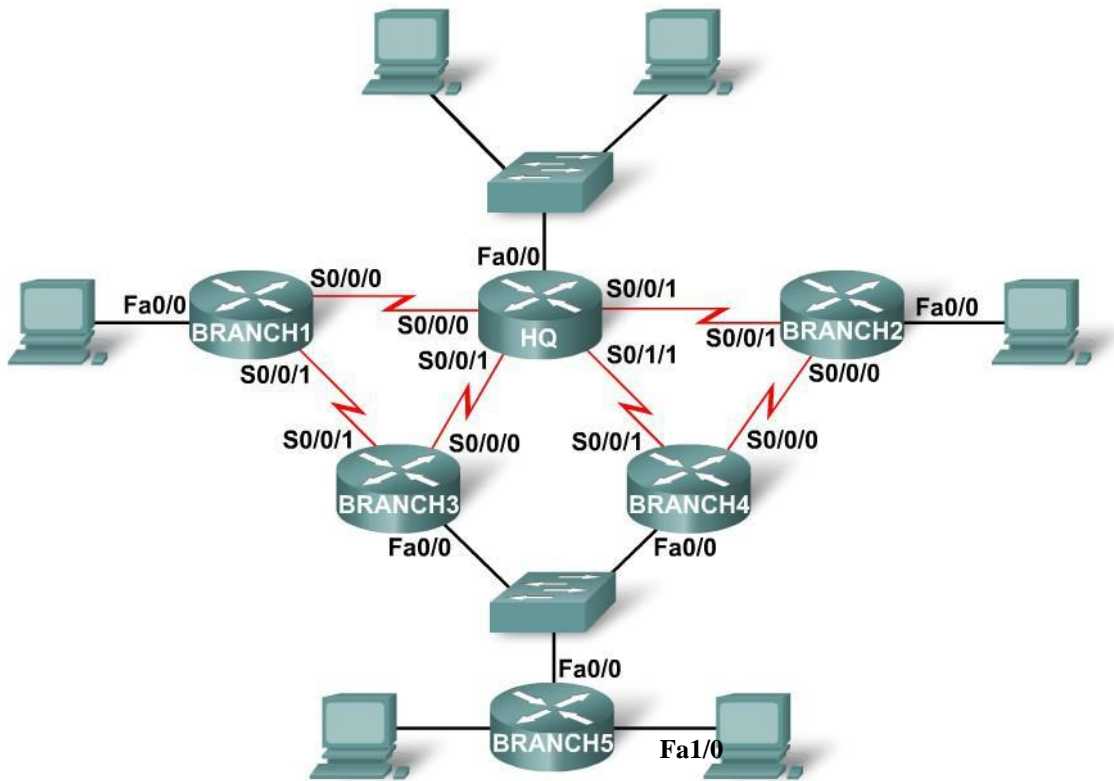
**Task 2: Record Subnet Information.**

**Step 1:** Fill in the following chart with the subnet information.

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				



**Topology Diagram D**



**Task 1: Determine the Number of Subnets in the Topology Diagram.**

**Step 1:** How many networks are there? \_\_\_\_

**Step 2:** How many bits should you borrow to create the required number of subnets? \_\_\_\_

**Step 3:** How many usable host addresses and usable subnets did this give you? \_\_\_\_

**Step 4:** What is the new subnet mask in decimal form? \_\_\_\_\_

**Step 5:** How many subnets are available for future use? \_\_\_\_

**Task 2: Record Subnet Information.**

**Step 1: Fill in the following chart with the subnet information.**

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

**Reflection**

What information is needed when determining an appropriate addressing scheme for a network?

---



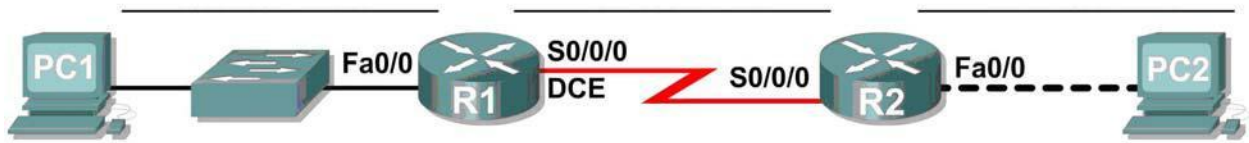
---



---

## Lab 8: Subnet and Router Configuration

### Topology Diagram



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0			N/A
	S0/0/0			N/A
R2	Fa0/0			N/A
	S0/0/0			N/A
PC1	NIC			
PC2	NIC			

### Learning Objectives

Upon completion of this lab, you will be able to:

- Subnet an address space given requirements.
- Assign appropriate addresses to interfaces and document.
- Configure and activate Serial and FastEthernet interfaces.
- Test and verify configurations.
- Reflect upon and document the network implementation.

### Scenario

In this lab activity, you will design and apply an IP addressing scheme for the topology shown in the Topology Diagram. You will be given one address block that you must subnet to provide a logical addressing scheme for the network. The routers will then be ready for interface address configuration according to your IP addressing scheme. When the configuration is complete, verify that the network is working properly.

### Task 1: Subnet the Address Space.

#### Step 1: Examine the network requirements.

You have been given the 192.168.1.0/24 address space to use in your network design. The network consists of the following segments:

- The network connected to router R1 will require enough IP addresses to support 15 hosts.
- The network connected to router R2 will require enough IP addresses to support 30 hosts.
- The link between router R1 and router R2 will require IP addresses at each end of the link.

#### Step 2: Consider the following questions when creating your network design.

How many subnets are needed for this network? \_\_\_\_\_

What is the subnet mask for this network in dotted decimal format? \_\_\_\_\_

What is the subnet mask for the network in slash format? \_\_\_\_\_

How many usable hosts are there per subnet? \_\_\_\_\_

**Step 3: Assign subnetwork addresses to the Topology Diagram.**

1. Assign subnet 1 to the network attached to R1.
2. Assign subnet 2 to the link between R1 and R2.
3. Assign subnet 3 to the network attached to R2.

**Task 2: Determine Interface Addresses.**

**Step 1: Assign appropriate addresses to the device interfaces.**

1. Assign the first valid host address in subnet 1 to the LAN interface on R1.
2. Assign the last valid host address in subnet 1 to PC1.
3. Assign the first valid host address in subnet 2 to the WAN interface on R1.
4. Assign the last valid host address in subnet 2 to the WAN interface on R2.
5. Assign the first valid host address in subnet 3 to the LAN interface of R2.
6. Assign the last valid host address in subnet 3 to PC2.

**Step 2: Document the addresses to be used in the table provide under the Topology Diagram.**

**Task 3: Configure the Serial and FastEthernet Addresses.**

**Step 1: Configure the router interfaces.**

Configure the interfaces on the R1 and R2 routers with the IP addresses from your network design. Please note, to complete the activity in Packet Tracer you will be using the Config Tab. When you have finished, be sure to save the running configuration to the NVRAM of the router.

**Step 2: Configure the PC interfaces.**

Configure the Ethernet interfaces of PC1 and PC2 with the IP addresses and default gateways from your network design.

**Task 4: Verify the Configurations.**

Answer the following questions to verify that the network is operating as expected.

From the host attached to R1, is it possible to ping the default gateway? \_\_\_\_\_

From the host attached to R2, is it possible to ping the default gateway? \_\_\_\_\_

From the router R1, is it possible to ping the Serial 0/0/0 interface of R2? \_\_\_\_\_

From the router R2, is it possible to ping the Serial 0/0/0 interface of R1? \_\_\_\_\_

**Task 5: Reflection**

Are there any devices on the network that cannot ping each other?

---



---

What is missing from the network that is preventing communication between these devices?

---

---

## Lab 9: Media Connectors Lab Activity



**Fluke 620 LAN CableMeter**

### Learning Objectives

Upon completion of this lab, you will be able to:

- Test cables using a Fluke620 LAN CableMeter and a Fluke LinkRunner
- Become familiar with the most common functions of a cable tester.
- Test different cables for type and wiring problems.

### Background

Category (CAT 5) unshielded twisted-pair (UTP) cables are wired according to function. End devices, such as routers and host computers, connect to switches with CAT 5 straight-through cables. When connected together, however, a CAT 5 crossover cable must be used. This is also true of switches. When connecting one switch to another, a CAT 5 crossover cable is used again.

Problems related to cables are one of the most common causes of network failure. Basic cable tests can be very helpful in troubleshooting cabling problems with UTP. The quality of cabling components used, the routing and installation of the cable, and quality of the connector terminations will be the main factors in determining how trouble-free the cabling will be.

The following resources are required:

- Good CAT 5 straight-through and crossover wired cables of different colors.
- Category 5 straight-through and crossover wired cables with open wire connections in the middle or one or more conductors shorted at one end that are different colors and different lengths.
- Fluke 620 LAN CableMeter or equivalent.

- Fluke LinkRunner

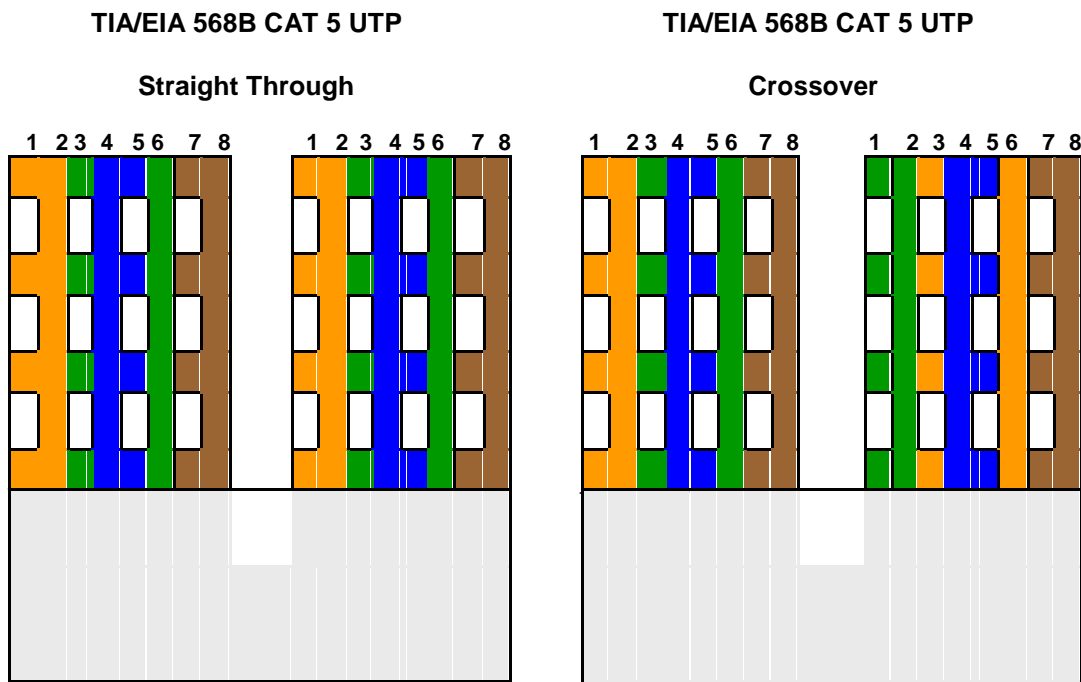
TIA/EIA 568B is different from TIA/EIA 568A wiring. TIA/EIA 568A straight-through cables can be identified by the color coding. Similar to Figure 2, below, the right wiring diagram, starting with the green-white cable, will be identical on both ends.

**Scenario**

First, you will visually determine whether the CAT 5 cable type is crossover or straight-through. Next, you will use the cable tester to verify the cable type, as well as common features available with the tester.

Finally, you will use the cable tester to test for bad cables that cannot be determined with a visual inspection.

**Task 1: Become Familiar with the Most Common Functions of a Cable Tester.**



**Figure 1. Straight-through Wire Location**

**Figure 2. Crossover Wire Location**

Figures 1 and 2 show the TIA/EIA 568B CAT 5 UTP wire positioning for a straight-through and crossover cable, respectively. When CAT 5 connectors are held together, wire color is a quick way to determine the cable type.

**Step 1: Visually determine cable types.**

There should be two numbered cables available. Perform a visual inspection of the cables and then fill out the chart below with the cable color, cable type, and use:

Cable No.	Cable Color	Cable Type (straight-through or crossover)	Cable Use (Circle correct device)
1			Switch to: host / switch
2			Switch to: host / switch

It is now time to verify the cable type and learn about the common features of the cable tester.

**Step 2: Perform initial configuration of the Fluke 620 LAN CableMeter.**

Turn the rotary switch selector on the tester to the WIRE MAP position. The wire map function displays which pins on one end of the cable are connected to which pins on the other end.

Press the **SETUP** button to enter the setup mode, and observe the LCD screen on the tester. The first option should be CABLE. Press the **UP** or **DOWN** arrow buttons until the desired cable type of UTP is selected. Press **ENTER** to accept that setting and go to the next one. Continue pressing the **UP/DOWN** arrows and pressing **ENTER** until the tester is set to the following cabling settings:

Tester Option	Desired Setting – UTP
CABLE:	UTP
WIRING:	10BASE-T or EIA/TIA 4PR
CATEGORY:	CATEGORY 5
WIRE SIZE	AWG 24
CAL to CABLE?	NO
BEEPING:	ON or OFF
LCD CONTRAST	From 1 through 10 (brightest)

When satisfied with the correct settings, press the **SETUP** button to exit setup mode.

**Step 3: Verify cable wire map.**



**Figure 3. Cable Coupler and Cable Identifier**

Use the following procedure to test each cable with the LAN cable coupler and cable identifier, shown in Figure 3. The coupler and the cable identifier are accessories that come with the Fluke 620 LAN CableMeter. Place the near end of the cable into the RJ-45 jack labeled UTP/FTP on the tester. Place the RJ-45-RJ-45 female coupler on the far end of the cable, and then insert the cable identifier into the other side of the coupler. The wiring of both the near and far end of the cable will be displayed. The top set of numbers displayed on the LCD screen refers to the near end, and the bottom set of numbers refers to the far end.

Perform a Wire Map test on each of the cables provided, and fill in the following table based on the results. For each cable, write down the number and color, and whether the cable is straight-through or crossover.

Cable No.	Cable Color	Cable Type (straight-through or crossover)
1		
2		

Note any problems encountered during this test:

**Step 4: Verify cable length.**

Move the rotary switch selector on the tester to the LENGTH position. If power was cycled, repeat the setup steps described in Step 2. The tester LENGTH function displays the length of the cable.

Perform a basic cable test on each of the cables, and complete the following table based on the results. For each cable, write down the number and color, the cable length, the tester screen test results, and what the problem is, if there is a problem.



Cable No.	Cable Color	Cable Length
1		
2		

Note any problems encountered during this test:

Repeat these steps until you are comfortable with the use of the cable tester. In the next task, unknown cables will be tested.

**Task 2: Test Different Cables for Type and Wiring Problems.**

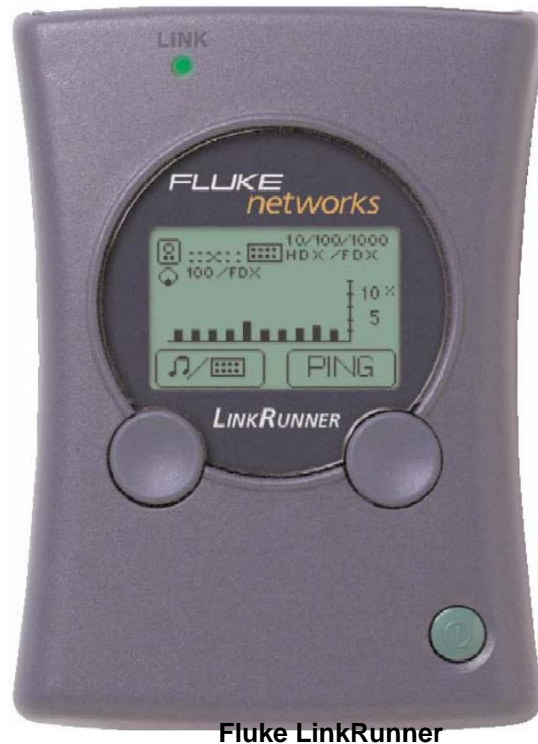
Obtain at least 5 different cables from your instructor. Move the rotary switch selector on the tester to the WIRE MAP position. If power was cycled, repeat the setup steps described in Task 1, Step 2.

Using the cable tester WIRE MAP function, perform a Wire Map test on each of the cables provided. Then fill in the following table based on the result for each Category 5 cable tested. For each cable, write down the number and color, whether the cable is straight-through or crossover, the tester screen test results, and any problem.

Cable No.	Cable Type (Visual inspection)	Cable Color	Cable type (straight-through or crossover)	* Test Results	Problem Description
1					
2					
3					
4					
5					

\* Refer to the Fluke manual for detailed description of test results for wire map.

**Task 3: Perform initial configuration of the Fluke LinkRunner**



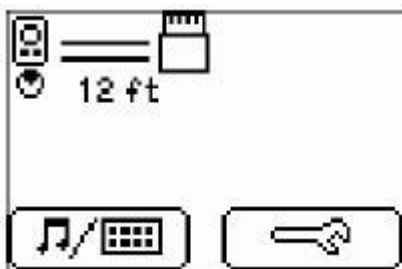
Fluke LinkRunner

**Step 1:** Turn the Fluke LinkRunner on by pressing the green button on the lower right along with the blue button on the right.

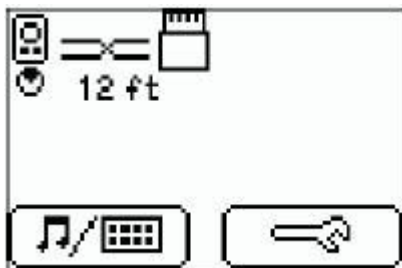
**Step 2:** Press the green button on the lower right to turn it back off.


**Step 3:** Place both ends of the cable into the LAN and MAP ports located on top of the LinkRunner and press the green button on the lower right along with the blue button to the left.

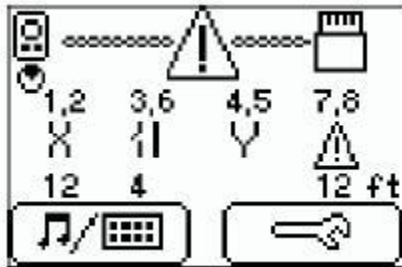
If it is a correct straight-through cable then two parallel lines (as shown below) will appear on the upper left corner on the screen.



If it is a correct crossover cable then two intersecting lines (as shown below) will appear on the upper left corner on the screen.



If it is a bad cable,  will appear and details will be displayed below.



|| Open  
 Y Short  
 X Split  
 X Reversal  
 Δ Unknown

#### Task 4: Verify Cable Length

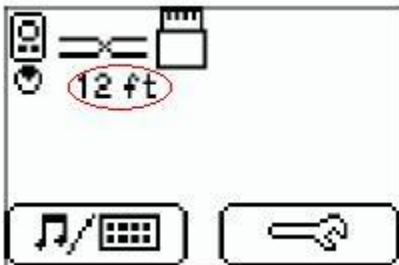
**Note:** The instructions to test a cable are the same as determining cable length.

**Step 1:** Turn the Fluke LinkRunner on by pressing the green button on the lower right along with the blue button on the right.

**Step 2:** Press the green button on the lower right to turn it back off.

**Step 3:** Place both ends of the cable into the LAN and MAP ports located on top of the LinkRunner and press the green button on the lower right along with the blue button to the left.

**Step 4:** Locate the length of the cable below the icon indicating the type of cable (as shown below).



#### Task 5: Reflection

Problems related to cables are one of the most common causes of network failure. Network technicians should be able to determine when to use CAT 5 UTP straight-through and crossover cables.

A cable tester is used to determine cable type, length, and wire map. In a lab environment, cables are constantly moved and reconnected. A properly functioning cable today may be broken tomorrow. This isn't unusual, and is part of the learning process.

#### Task 6: Challenge

Look for opportunities to test other cables with the Fluke 620 LAN CableMeter. Skills learned in this lab will enable you to quickly troubleshoot wrong cable types and broken cables.

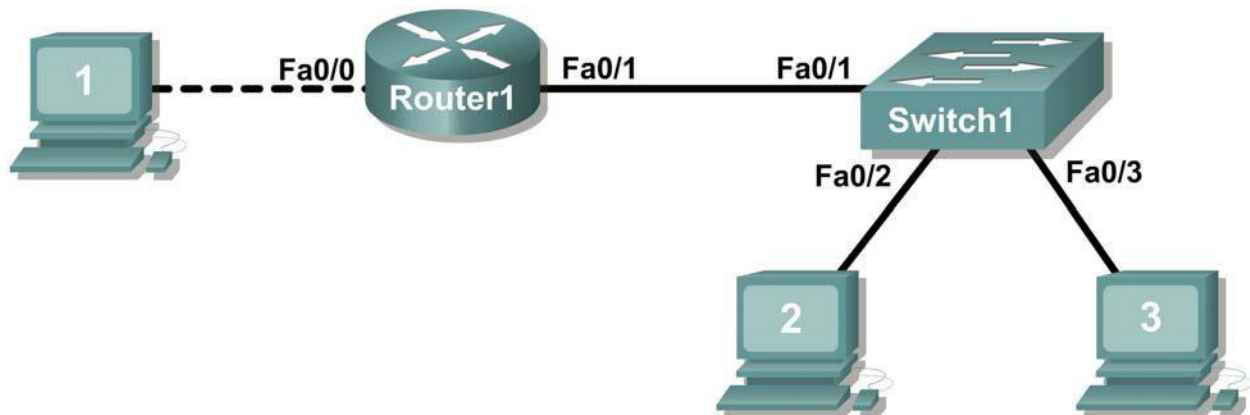
#### Task 7: Clean Up

The cable tester is very expensive and should never be left unattended. Return the cable tester to the instructor when finished.

Ask the instructor where to return used cables. Store the cables neatly for the next class.

## Lab 10: Basic Cisco Device Configuration

### Topology Diagram



### Learning Objectives

- Configure Cisco router global configuration settings.
- Configure Cisco router password access.
- Configure Cisco router interfaces.
- Save the router configuration file.
- Configure a Cisco switch.

### Background

Hardware	Qty	Description
Cisco Router	1	Part of CCNA Lab bundle.
Cisco Switch	1	Part of CCNA Lab bundle.
*Computer (host)	1	Lab computer.
Console (rollover) cable	1	Connects computer host 1 to Router console port.
UTP Cat 5 crossover cable	1	Connects computer host 1 to Router LAN interface Fa0/0
Straight Through Cable	3	Connects computer hosts to Switch and switch to router

Table 1. Equipment and hardware required for this lab.

Gather the necessary equipment and cables. To configure the lab, make sure the equipment listed in Table 1 is available. Common configuration tasks include setting the hostname, access passwords, and MOTD banner. Interface configuration is extremely important. In addition to assigning a Layer 3 IP address, enter a description that describes the destination connection speeds troubleshooting time.

Configuration changes are effective immediately.

Configuration changes must be saved in NVRAM to be persistent across reboot.

Configuration changes may also be saved off-line in a text file for auditing or device replacement.

Cisco IOS switch configuration is similar to Cisco IOS router configuration.

### Scenario

In this lab students will configure common settings on a Cisco Router and Cisco Switch.

Given an IP address of 198.133.219.0/24, with 4 bits borrowed for subnets, fill in the following information in the table below. (Hint: fill in the subnet number, then the host address. Address information will be easy to compute with the subnet number filled in first)

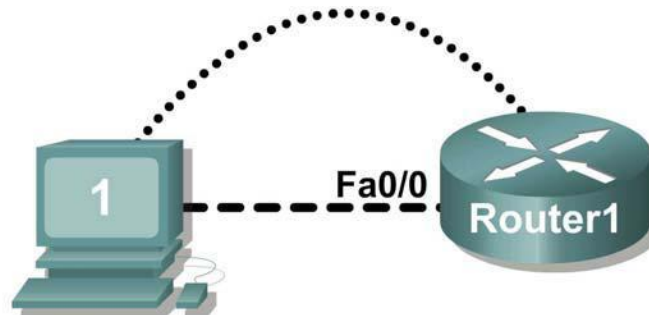
Maximum number of usable subnets (including the 0<sup>th</sup> subnet): \_\_\_\_\_

Number of usable hosts per subnet: \_\_\_\_\_

#	Subnet	IP Address:	Subnet mask:	Broadcast
		First host address	Last host address	

Before proceeding, verify your addresses with the instructor. The instructor will assign subnetworks.

**Task 1: Configure Cisco Router Global Configuration Settings.**



**Straight-through cable**



**Serial cable**



**Console (Rollover)**



**Crossover cable**



Figure 1. Lab cabling.

**Step 1: Physically connect devices.**

Refer to Figure 1. Connect the console or rollover cable to the console port on the router. Connect the other end of the cable to the host computer using a DB-9 or DB-25 adapter to the COM 1 port. Connect the crossover cable between the host computer's network interface card (NIC) and Router interface Fa0/0. Connect a straight-through cable between the Router interface Fa0/1 and any of the switch's interfaces (1-24).

Ensure that power has been applied to the host computer, switch and router.

**Step 2: Connect host computer to router through HyperTerminal.**

From the Windows taskbar, start the HyperTerminal program by clicking on Start | Programs | Accessories | Communications | HyperTerminal.

Configure HyperTerminal with the proper settings:

Connection Description

Name: **Lab 11\_2\_11**

Icon: **Personal choice**

Connect to

Connect Using: **COM1** (or appropriate COM port)

COM1 Properties

Bits per second: **9600**

Data bits: **8**

Parity: **None**

Stop bits: **1**

Flow Control: **None**

When the HyperTerminal session window comes up, press the **Enter** key until there is a response from the router.

If the router terminal is in the configuration mode, exit by typing **no**.

```
Would you like to enter the initial configuration dialog?
```

```
[yes/no]: no
```

```
Press RETURN to get started!
```

```
Router>
```

When in privileged exec command mode, any misspelled or unrecognized commands will attempt to be translated by the router as a domain name. Since there is no domain server configured, there will be a delay while the request times out. This can take between several seconds to several minutes. To terminate the wait, simultaneously hold down the **<CTRL><SHIFT>6** keys then release and press **x**:

```
Router>enabel
```

```
Translating "enabel"...domain server (255.255.255.255) %
```

**Briefly hold down the keys <CTRL><SHIFT>6, release and press x**

```
Name lookup aborted
```

```
Router>
```

From the user exec mode, enter privileged exec mode:

```
Router> enable
```

```
Router#
```

Verify a clean configuration file with the privileged exec command **show running-config**. If a configuration file was previously saved, it will have to be removed. Appendix 1 shows a typical default router's configuration. Depending on router's model and IOS version, your configuration may look slightly different. However, there should be no configured passwords or IP addresses. If your router does not have a default configuration, ask the instructor to remove the configuration.

**Step 3: Configure global configuration hostname setting.**

What two commands may be used to leave the privileged exec mode? \_\_\_\_\_

What shortcut command can be used to enter the privileged exec mode? \_\_\_\_\_

Examine the different configuration modes that can be entered with the command **configure**?

Write down the list of configuration modes and description:

---



---



---



---



---

From the `privileged exec` mode, enter global configuration mode:

```
Router# configuration terminal
```

```
Router(config)#
```

What three commands may be used to leave the global configuration mode and return to the privileged exec mode?

---



---

What shortcut command can be used to enter the global configuration mode?

---

Set the device hostname to Router1:

```
router(config)# hostname Router1
```

```
Router1(config)#
```

How can the hostname be removed?

---



---

**Step 5: Configure the MOTD banner.**

In production networks, banner content may have a significant legal impact on the organization. For example, a friendly "Welcome" message may be interpreted by a court that an attacker has been granted permission to hack into the router. A banner should include information about authorization, penalties for unauthorized access, connection logging, and applicable local laws. The corporate security policy should provide policy on all banner messages.

Create a suitable MOTD banner. Only system administrators of the ABC Company are authorized access, unauthorized access will be prosecuted, and all connection information will be logged.

---



---

---



---



---



---

Examine the different banner modes that can be entered. Write down the list of banner modes and description.

**Router1(config)# banner ?**

---



---



---



---



---

Choose a terminating character that will not be used in the message text. \_\_\_\_\_

Configure the MOTD banner. The MOTD banner is displayed on all connections before the login prompt. Use the terminating character on a blank line to end the MOTD entry:

Router1(config)# **banner motd %**

**Enter TEXT message. End with the character '%'**

\*\*\*You are connected to an ABC network device. Access is granted to only current ABC company system administrators with prior written approval. \*\*\*

\*\*\* Unauthorized access is prohibited, and will be prosecuted. \*\*\*

\*\*\* All connections are continuously logged. \*\*\*

%

Router1(config)#

What is the global configuration command to remove the MOTD banner?

---

## Task 2: Configure Cisco router password access.

Access passwords are set for the privileged exec mode and user entry point such as console, aux, and virtual lines. The privileged exec mode password is the most critical password, since it controls access to the configuration mode.

### Step 1: Configure the privileged exec password.

Cisco IOS supports two commands that set access to the privileged exec mode. One command, **enable password**, contains weak cryptography and should never be used if the **enable secret** command is available. The **enable secret** command uses a very secure MD5 cryptographic hash algorithm. Cisco says "As far as anyone at Cisco knows, it is impossible to recover an enable secret based on the contents of a configuration file (other than by obvious dictionary attacks)." Password security relies on the password algorithm, and the password. . In



production environments, strong passwords should be used at all times. A strong password consists of at least nine characters of upper and lower case letters, numbers, and symbols. In a lab environment, we will use weak passwords.

Set the privileged exec password to **cisco**.

```
Router1(config)# enable secret cisco
Router1(config)#
```

### Step 2: Configure the console password.

Set the console access password to **class**. The console password controls console access to the router.

```
Router1(config)# line console 0
Router1(config-line)# password class
Router1(config-line)# login
```

What is the command to remove the console password? \_\_\_\_\_

### Step 3: Configure the virtual line password.

Set the virtual line access password to **class**. The virtual line password controls Telnet access to the router. In early Cisco IOS versions, only five virtual lines could be set, 0 through 4. In newer Cisco IOS versions, the number has been expanded. Unless a telnet password is set, access on that virtual line is blocked.

```
Router1(config-line)# line vty 0 4
Router1(config-line)# password class
Router1(config-line)# login
```

There are three commands that may be used to exit the line configuration mode:

Command	Effect
	Return to the global configuration mode.
	Exit configuration and return to the privileged exec mode.

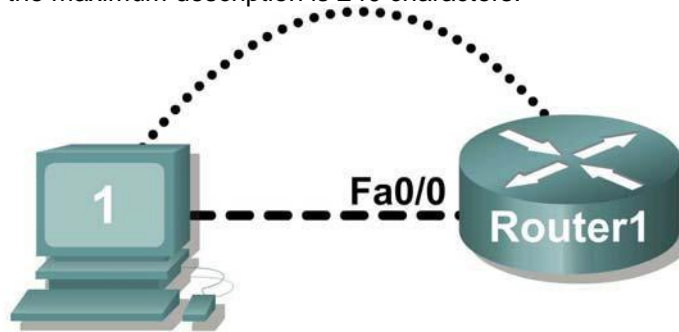
Issue the command **exit**. What is the router prompt? What is the mode?

Router1(config-line)# **exit**

Issue the command **end**. What is the router prompt? What is the mode?

**Task 3: Configure Cisco Router Interfaces.**

All cabled interfaces should contain documentation about the connection. On newer Cisco IOS versions, the maximum description is 240 characters.



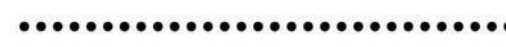
**Straight-through cable**



**Serial cable**



**Console (Rollover)**



**Crossover cable**



Figure 2. Physical lab topology.

Figure 2 shows a network topology where a host computer is connected to Router1, interface Fa0/0.

Write down your subnet number and mask:

---

The first IP address will be used to configure the host computer LAN. Write down the first IP Address:

---

The last IP address will be used to configure the router fa0/0 interface. Write down the last IP Address:

---

**Step 1: Configure the router fa0/0 interface.**

Write a short description for the connections on Router1:

Fa0/0 ->

---

Apply the description on the router interface with the interface configuration command, **description**:

Router1(config)# **interface fa0/0**

```
Router1(config-if)# description Connection to Host1 with
crossover cable
Router1(config-if)# ip address address
mask Router1(config-if)# no shutdown
Router1(config-if)# end Router1#
```

Look for the interface to become active:

```
*Mar 24 19:58:59.602: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/0, changed state to up
```

### Step 2: Configure the router Fa0/1 interface.

Write a short description for the connections on Router1:

Fa0/1 ->

---

Apply the description on the router interface with the interface configuration command, **description**:

```
Router1(config)# interface fa0/1
Router1(config-if)# description Connection to switch with
straight-through cable
Router1(config-if)# ip address address
mask Router1(config-if)# no shutdown
Router1(config-if)# end Router1#
```

Look for the interface to become active:

```
*Mar 24 19:58:59.602: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/1, changed state to up
```

### Step 3: Configure the host computer.

Configure the host computer for LAN connectivity. Recall that the LAN configuration window is accessed through Start | Control Panel | Network Connections. Right-click on the LAN icon, and select Properties. Highlight the Internet Protocol field, and select Properties. Fill in the following fields:

IP Address: The first host address \_\_\_\_\_

Subnet Mask: The subnet mask \_\_\_\_\_

Default Gateway: Router's IP Address \_\_\_\_\_

Click OK, and then Close. Open a terminal window, and verify network settings with the **ipconfig** command.

### Step 4: Verify network connectivity.

Use the **ping** command to verify network connectivity with the router. If ping replies are not successful troubleshoot the connection:

What Cisco IOS command can be used to verify the interface status?

---

What Windows command can be used to verify host computer configuration?

---

What is the correct LAN cable between host1 and Router1?

---

## Task 4: Save the Router Configuration File.

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

### Step 1: Compare router RAM and NVRAM configurations.

Use the Cisco IOS `show` command to view RAM and NVRAM configurations. The configuration is displayed one screen at a time. A line containing “ -- more -- ” indicates that there is additional information to display. The following list describes acceptable key responses:

Key	Description
<SPACE>	Display the next page.
<RETURN>	Display the next line.
Q	Quit
<CTRL> c	Quit

Write down one possible shortcut command that will display the contents of NVRAM.

Display the contents of NVRAM. If the output of NVRAM is missing, it is because there is no saved configuration.:

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

Display the contents of RAM.

```
Router1#show running-config
```

Use the output to answer the following questions:

How large is the configuration file? \_\_\_\_\_

What is the enable secret password? \_\_\_\_\_

Does your MOTD banner contain the information you entered earlier?

\_\_\_\_\_

Do your interface descriptions contain the information you entered earlier?

\_\_\_\_\_

Write down one possible shortcut command that will display the contents of RAM.

\_\_\_\_\_

### Step 2: Save RAM configuration to NVRAM.

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

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

Write down one possible shortcut command that will copy the RAM configuration to NVRAM.

---

Review the contents of NVRAM, and verify that the configuration is the same as the configuration in RAM.

### Task 5: Configure a Cisco Switch.

Cisco IOS switch configuration is (thankfully) similar to configuring a Cisco IOS router. The benefit of learning IOS commands is that they are similar to many different devices and IOS versions.

#### Step 1: Connect the host to the switch.

Move the console, or rollover, cable to the console port on the switch. Ensure power has been applied to the switch. In Hyperterminal, press Enter until the switch responds.

#### Step 2. Configure global configuration hostname setting.

Appendix 2 shows a typical default switch configuration. Depending on router model and IOS version, your configuration may look slightly different. However, there should be no configured passwords. If your router does not have a default configuration, ask the instructor to remove the configuration.

From the user exec mode, enter global configuration mode:

```
Switch> en
Switch# config t
Switch(config)#
```

Set the device hostname to Switch1.

```
Switch(config)# hostname Switch1
Switch1(config)#
```

#### Step 3: Configure the MOTD banner.

Create a suitable MOTD banner. Only system administrators of the ABC company are authorized access, unauthorized access will be prosecuted, and all connection information will be logged.

Configure the MOTD banner. The MOTD banner is displayed on all connections before the login prompt. Use the terminating character on a blank line to end the MOTD entry. For assistance, review the similar step for configuring a router MOTD banner.

```
Switch1(config)# banner motd %
```

#### Step 4: Configure the privileged exec password.

Set the privileged exec password to `cisco`.

```
Switch1(config)# enable secret cisco
Switch1(config)#
```

#### Step 5: Configure the console password.

Set the console access password to `class`.

```
Switch1(config)# line console 0
Switch1(config-line)# password class
Switch1(config-line)# login
```

**Step 6: Configure the virtual line password.**

Set the virtual line access password to `class`. There are 16 virtual lines that can be configured on a Cisco IOS switch, 0 through 15.

```
Switch1(config-line)# line vty 0 15
Switch1(config-line)# password class
Switch1(config-line)# login
```

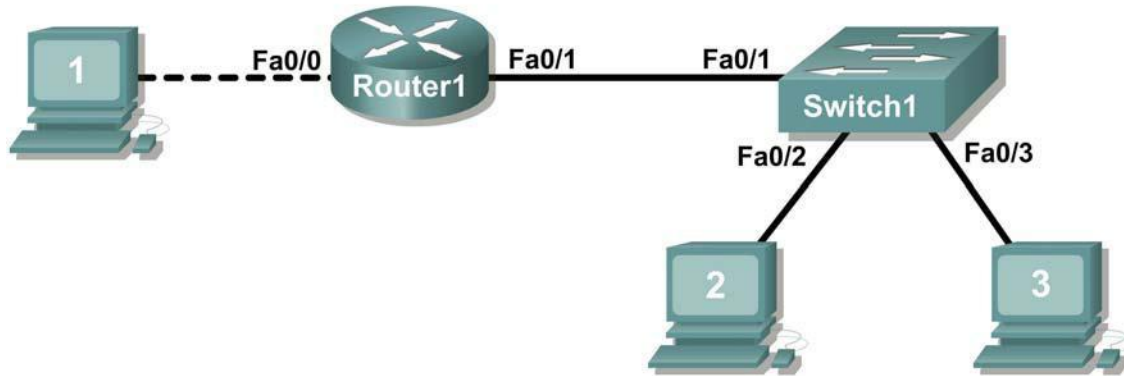


Figure 3. Network topology.

**Step 7: Configure the interface description.**

Figure 3 shows a network topology where Router1 is connected to Switch1, interface Fa0/1. Switch1 interface Fa0/2 is connected to host computer 2, and interface Fa0/3 is connected to host computer 3.

Write a short description for the connections on Switch1:

Router1 Interface	Description
Fa0/1	
Fa0/2	
Fa0/3	

Apply the descriptions on the switch interface with the interface configuration command, **description**:

```
Switch1(config)# interface fa0/1 Switch1(config-if)#
description Connection to Router1 Switch1(config)#
interface fa0/2
Switch1(config-if)# description Connection to host computer
2 Switch1(config)# interface fa0/3
Switch1(config-if)# description Connection to host computer
3 Switch1(config-if)# end
Switch1#
```

**Step 7: Save RAM configuration to NVRAM.**

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

```
Switch1# copy run start
Destination filename [startup-config]?
<ENTER> Building configuration... [OK]

Switch1#
```

Review the contents of NVRAM, and verify that the configuration is the same as the configuration in RAM.

## Task 6: Reflection

The more you practice the commands, the faster you will become in configuring a Cisco IOS router and switch. It is perfectly acceptable to use notes at first to help configure a device, but a professional network engineer does not need a 'cheat sheet' to perform common configuration tasks. The following table lists commands covered in this lab:

Purpose	Command
Enter the global configuration mode.	<b>configure terminal</b> Example: Router> <b>enable</b> Router# configure terminal Router(config)#
Specify the name for the router.	<b>hostname name</b> Example: Router(config)# <b>hostname Router1</b> Router(config)#
Specify an encrypted password to prevent unauthorized access to the privileged exec mode.	<b>enable secret password</b> Example: Router(config)# <b>enable secret cisco</b> Router(config)#
Specify a password to prevent unauthorized access to the console.	<b>password password</b> <b>login</b> Example: Router(config)# <b>line con 0</b> Router(config-line)# <b>password class</b> Router(config-line)# <b>login</b> Router(config)#
Specify a password to prevent unauthorized telnet access. Router vty lines: 0 4 Switch vty lines: 0 15	<b>password password</b> <b>login</b> Example: Router(config)# <b>line vty 0 4</b> Router(config-line)# <b>password class</b> Router(config-line)# <b>login</b> Router(config-line)#
Configure the MOTD banner.	<b>Banner motd %</b> Example: Router(config)# <b>banner motd %</b> Router(config)#
Configure an interface. Router- interface is OFF by default Switch- interface is ON by default	Example: Router(config)# <b>interface fa0/0</b> Router(config-if)# <b>description description</b> Router(config-if)# <b>ip address address mask</b> Router(config-if)# <b>no shutdown</b> Router(config-if)#
Save the configuration to NVRAM.	<b>copy running-config startup-config</b> Example: Router# <b>copy running-config startup-config</b> Router#

## Task 7: Challenge

It is often necessary, and always handy, to save the configuration file to an off-line text file. One way to save the configuration file is to use HyperTerminal Transfer menu option Capture.

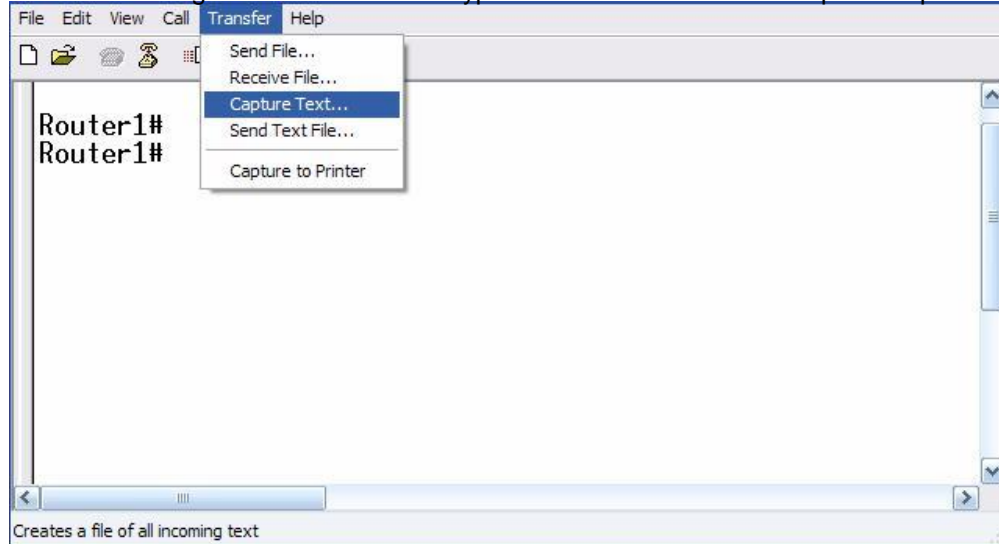


Figure 2. Hyperterminal Capture menu.

Refer to Figure 2. All communication between the host computer and router are saved to a file. The file can be edited, and saved. The file can also be edited, copied, and pasted into a router:

To start a capture, select Hyperterminal menu option Transfer | Capture Text. Enter a path and file name, and select Start.

Issue the privileged exec command **show running-config**, and press the <SPACE> key until all of the configuration has been displayed.

Stop the capture. Select menu option Transfer | Capture Text | Stop.

Open the text file and review the contents. Remove any lines that are not configuration commands, such as the `more` prompt. Manually correct any lines that were scrambled or occupy the same line. After checking the configuration file, highlight the lines and select Notepad menu Edit | Copy. This places the configuration in host computer memory.

To load the configuration file, it is ALWAYS best practice to begin with a clean RAM configuration. Otherwise, stale configuration commands may survive a paste action and have unintended consequences (also known as the Law of Unintended Consequences):

Erase the NVRAM configuration file:

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

Reload the router:

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

When the router reboots, enter the global configuration mode:

```
Router> en
Router# config t
Router(config)#
```



Using the mouse, right-click inside the Hyperterminal window and select Paste To Host. The configuration will be loaded, very quickly, to the router. Watch closely for error messages, each message must be investigated and corrected.

Verify the configuration, and save to NVRAM.

### **Task 6: Cleanup**

Before turning off power to the router and switch, remove the NVRAM configuration file from each device with the privileged exec command **erase startup-config**.

Delete any configuration files saved on the host computers.

Unless directed otherwise by the instructor, restore host computer network connectivity, then turn off power to the host computers. Remove anything that was brought into the lab, and leave the room ready for the next class.

**Appendix 1- default Cisco IOS router configuration**

```
Current configuration : 824 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip cef
!
interface FastEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial0/1/0
  no ip address
  shutdown
  no fair-queue
!
interface Serial0/1/1
  no ip address
  shutdown
  clock rate 2000000
!
interface Vlan1
  no ip address
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
  login
!
scheduler allocate 20000 1000
end
```

**Appendix 2- default Cisco IOS switch configuration**

```
Current configuration : 1519 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
ip subnet-zero
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu
transmission spanning-tree extend system-
id !
!
interface FastEthernet0/1
  no ip address
!
interface FastEthernet0/2
  no ip address
!
interface FastEthernet0/3
  no ip address
!
interface FastEthernet0/4
  no ip address
!
interface FastEthernet0/5
  no ip address
!
interface FastEthernet0/6
  no ip address
!
interface FastEthernet0/7
  no ip address
!
interface FastEthernet0/8
  no ip address
!
interface FastEthernet0/9
  no ip address
!
interface FastEthernet0/10
  no ip address
!
interface FastEthernet0/11
  no ip address
!
interface FastEthernet0/12
```

```
no ip address
!
interface FastEthernet0/13
no ip address
!
interface FastEthernet0/14
no ip address
!
interface FastEthernet0/15
no ip address
!
interface FastEthernet0/16
no ip address
!
interface FastEthernet0/17
no ip address
!
interface FastEthernet0/18
no ip address
!
interface FastEthernet0/19
no ip address
!
interface FastEthernet0/20
no ip address
!
interface FastEthernet0/21
no ip address
!
interface FastEthernet0/22
no ip address
!
interface FastEthernet0/23
no ip address
!
interface FastEthernet0/24
no ip address
!
interface GigabitEthernet0/1
no ip address
!
interface GigabitEthernet0/2
no ip address
!
interface Vlan1
no ip address
no ip route-cache
shutdown
!
ip http server
!
line con 0
line vty 5 15
!
end
```