Data Communication and Computer Networks

EEE314

Lab Manual

Name	
Registration Number	
Class	
Instructor's Name	

Introduction

This is the Lab Manual for EEE – 314 Data Communications and Computer Networks. The labs constitute 25 % of the total marks for this course.

During the labs you will work individually. You are required to complete the 'Pre-Lab' section of the lab before coming to the lab. You will be graded for this and the 'In-Lab' tasks during the in-lab viva. You will complete the 'Post-Lab' section of each lab before coming to the next week's lab.

You are not allowed to wander in the lab or consult other students when performing experiments. Similarly the lab reports must contain original efforts. CIIT has a zero tolerance anti-plagiarism policy.

Apart from these weekly labs you will complete two projects in groups (not more than four students per group). One mini-project that will count towards your Lab Sessional II score and a Final Project which will be graded as Lab Final Exam. The grading policy is already discussed in the Course Description File

Acknowledgement

The labs for EEE-314 Data Communications and Computer Networks were designed by considering CCNA modules of CISCO network academy. The first version of these labs was prepared by Prof. Dr. Shahzad A. Malik and Mr. Atif Shakeel in Spring 2010, that comprises of 14 experiments. In 2013, lab manuals were modified by introducing a semester project along with 12 lab experiments. In 2016, lab manuals were prepared by Mr. Asad Ali Malik, Mr. Obaid-ur-Rehman and Mr. Sajid Ali Gillal under the supervision of Prof. Dr. Shahzad A. Malik. These labs have been remodeled according to new OBE format during Spring 2016. This version is prepared by Asad Ali Malik under the supervision and changes suggested by Dr. Mustafa Shakir during January 2017. Typesetting and formatting of this version was supervised by Dr. Omar Ahmad and was carried out by Mr. Abdul Rehman, Mr Suleman & Mr Baqir Hussain.

History of Revision (Kindly edit according to your course)

Version and Date of Issue	Team	Comments
Version 1. February 2010	Prof. Dr. Shahzad A. Malik Mr.Atif Shakeel	This version comprises of 14 CCNA based lab experiments.
Version 2. February 2013	Prof. Dr. Shahzad A. Malik Dr. Mustafa Shakir Asad Ali Malik Mr. Sajid Ali Gillal	This version comprises of 12 CCNA based labs and a semester project. (Lab manual is available in Networks Lab)

Version 3. September 2016	Prof. Dr. Shahzad A. Malik Mr. Asad Ali Malik Mr. Obaid-ur-Rehman Mr. Sajid Ali Gillal	In the 3rd version, all the labs have been remodeled according to the new OBE format.
Version 4. January 2017	Dr. Mustafa Shakir Mr. Asad Ali Malik Mr. Sajjid Ali Gillal	In 4th version Transport layer related issues are addressed and introduction to Wireshark is included to help the students to observe the messages exchanged between executing protocols entries.
		For comments and suggestions please contact: asadalimalik@comsats.edu.pk

Safety Precautions

- Be calm and relaxed, while working in lab.
- First check your measuring equipment.
- When working with voltages over 40 V or current over 10 A, there must be at least two people in the lab at all time.
- Keep the work area neat and clean.
- Be sure about the locations of fire extinguishers and first aid kit.
- No loose wires or metals pieces should be lying on the table or neat the circuit.
- Avoid using long wires, that may get in your way while making adjustments or changing leads.
- Be aware of bracelets, rings, and metal watch bands (if you are wearing any of them). Do not wear them near an energized circuit.
- When working with energize circuit use only one hand while keeping rest of your body away from conducting surfaces.
- Always check your circuit connections before power it ON.
- Always connect connection from load to power supply.
- Never use any faulty or damage equipment and tools.
- If an individual comes in contact with a live electrical conductor.
    - Do not touch the equipment, the cord, the person.
    - Disconnect the power source from the circuit breaker and pull out the plug using insulated material.

Table of Contents

Lab # 01: Introduction to Networks and Networking Commands in Windows and Introduction to Packet Tracer

1. Objective:

The lab is intended to familiarize the students with the networking commands used in windows environment for debugging network related issues.

At the end of the lab the student must know:

- Local Loop Address and its purpose
- How to find IP address of a machine's NIC
- How to find MAC (Physical) address of machine's NIC
- Name Server lookup
- How to display arp table
- How to display routing table
- How to list the machines on the network
- How to find MAC address of a remote machine IP address
- How to find MAC address of a remote machine from host name

2. PreLab

2.1 OSI Model:

Open Systems Interconnection model (OSI model)l has a layered architecture. Model defines 7 layers. Each layer performs its specific task, hiding the details and complexities of its layer from other layers. Division of the bigger task into smaller subtasks makes it manageable and flexible. Protocol at any layer can be changed without affecting the other layers. Each layer takes and provides services to/from adjacent upper and lower layers.

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	End-to-end connections, reliability and flow control
Media layers	Packet/Datagram	3. Network	Path determination and logical addressing (IP-Address)
	Frame	2. Data link	Physical addressing (MAC-address)
	Bit	1. Physical	Media, signal and binary transmission

Figure 1. 1 OSI Model

2.2. Internet Protocol

The Internet Protocol (IP) is the principal communications protocol used for relaying datagrams (also known as network packets) across an internetwork using the Internet Protocol Suite. Responsible for routing packets across network boundaries, it is the primary protocol that establishes the Internet. It has the task of delivering datagrams from the source host to the destination host solely based on the addresses. For this purpose, IP defines datagram structures that encapsulate the data to be delivered. The first major version of IP, now referred to as Internet Protocol Version 4 (IPv4) is the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6) is in active, growing deployment worldwide.

2.3. IP Address:

An Internet Protocol (IP) address is a numerical identification (logical address) that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. Although IP addresses are stored as binary numbers, they are usually displayed in human-readable notations, such as 208.77.188.166 (for IPv4), and 2001:db8:0:1234:0:567:1:1 (for IPv6). The role of IP address has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates ho to get there."In IPv4 an address consists of 32 bits which limits the address space to 4294967296 (232) possible unique addresses.

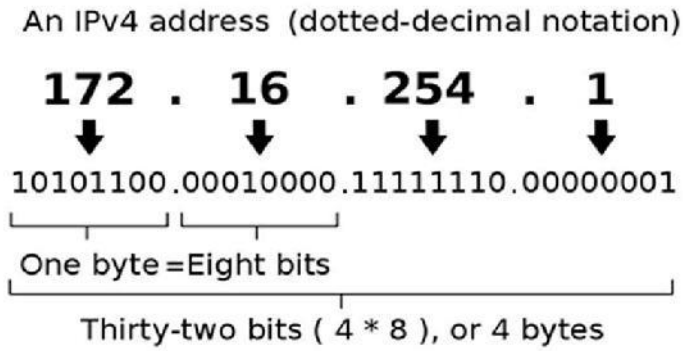


Figure 1. 2

This next generation of the Internet Protocol, intended to replace IPv4 is IPv6 with 128 bits or 16 octets. That is 2128 or about 3.403×1038 unique addresses.

2.4. MAC Address:

A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are most often assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, the card's read-only memory, or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address. It may also be known as an Ethernet hardware address (EHA), hardware address or physical address or adapter address. A network node may have multiple NICs and will then have one unique MAC address per NIC. The standard (IEEE 802) format for printing MAC addresses in human-friendly form is six groups of two hexadecimal digits, separated by hyphens (-) or colons (:), (e.g. 01-23-45-67-89-ab or 01:23:45:67:89:ab). Another convention used by networking equipment uses three groups of four hexadecimal digits separated by dots (.) (e.g. 0123.4567.89ab).

2.5. Routing:

Routing is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks, including the telephone network, electronic data networks (such as the Internet), and transportation (transport) networks in this course we are concerned primarily with routing in electronic data networks. Here routing is the transit of logically addressed packets from their source toward their ultimate destination through intermediate nodes; typically hardware devices called routers, bridges, gateways, or switches. Ordinary computers with multiple network cards can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus constructing routing tables, which are held in the routers' memory, becomes very important for efficient routing.

2.6. Address Resolution Protocol:

In computer networking, the Address Resolution Protocol (ARP) is the method for finding a host's link layer (hardware) address when only its Internet Layer (IP) or some other Network Layer address is known. It is a request and reply protocol. It can be used to resolve many different network layer protocol addresses to interface hardware addresses, although, due to the overwhelming prevalence of IPv4 and Ethernet, ARP is primarily used to translate IP addresses to Ethernet MAC addresses.

2.7. Loop-back Address:

The term loopback (sometimes spelled loop-back) is generally used to describe methods or procedures of routing electronic signals, digital data streams, or other flows of items, from their originating facility quickly back to the same source entity without intentional processing or modification. This is primarily intended as a means of testing the transmission or transportation infrastructure. It is a virtual network interface implemented in software only and not connected to any hardware, but which is fully integrated into the computer system's internal network infrastructure. Any traffic that a computer program sends to the loopback interface is immediately received on the same interface. Correspondingly, the Internet Protocol (IP) specifies a loopback network. The most commonly used IP address on the loopback device is 127.0.0.1 for IPv4, although any address in the range 127.0.0.0 to 127.255.255.255 is mapped to it. IPv6 designates only a single address for this function, 0:0:0:0:0:0:0:1 (also written as ::1). The standard, officially reserved, domain name for these addresses is localhost. On Unix-like systems, the loopback interface usually has the device name lo or lo0.

3. Lab Task

Students are required to explore these commands. Through these commands students can accomplish the goals mentioned in section: “Objective”. Use the command prompt in windows or terminal window in linux.

3.1. Task1:

Run these commands and find out which command performs which of the above listed task

3.2. Task2:

Explore these commands and find out at least 5 new command options (switches)On your PCs open the command prompt (start - - run - and type cmd) and type the commands

1. ipconfig

Purpose: _____

Observation: _____

2. ipconfig / all

Purpose: _____

Observation: _____

3. ping <IP> e.g (C:\>ping 192.168.10.5)

Purpose: _____

Observation: _____

4. arp-a

Purpose: _____

Observation: _____

5. netstat -a

Purpose: _____

Observation: _____

6. net view

Purpose: _____

Observation: _____

7. tracert <hostname> e.g (C:\>tracert www.facefook.com)

Purpose: _____

Observation: _____

8. netstat -r

Purpose: _____

Observation: _____

9. nslookup

Purpose: _____

Observation: _____

10. nbtstat -n

Purpose: _____

Observation: _____

Hints:

- Use Windows Help (Press F1) or search the internet for more info about commands
- Add a question mark (?) after any command to get more info about it.
- If you are stuck in a command either type “exit” or press Ctrl+Break
- Replace <arguments> with actual values.

• Part-2: Introduction to Packet Tracer

Purpose:

The lab is intended to familiarize the students with a network classes and packet tracer simulator used to develop a network

Introduction to Packet Tracer:

Packet Tracer is a self-paced, visual, interactive teaching and learning tool developed by Cisco. Lab activities are an important part of networking education. However, lab equipment can be a scarce resource. Packet Tracer provides a visual simulation of equipment and network processes to offset the challenge of limited equipment. Students can spend as much time as they like completing standard lab exercises through Packet Tracer, and have the option to work from home. Although Packet Tracer is not a substitute for real equipment, it allows students to

practice using a command-line interface. This "e-doing" capability is a fundamental component of learning how to configure routers and switches from the command line.

Steps to use Packet Tracer 5.1

After downloading you can install the software on your PC.

- **Step 1 - Start Packet Tracer And have A Look At The Interface**

The bottom left-hand corner of the Packet Tracer screen displays eight icons that represent device categories or groups, such as Routers, Switches, or End Devices.

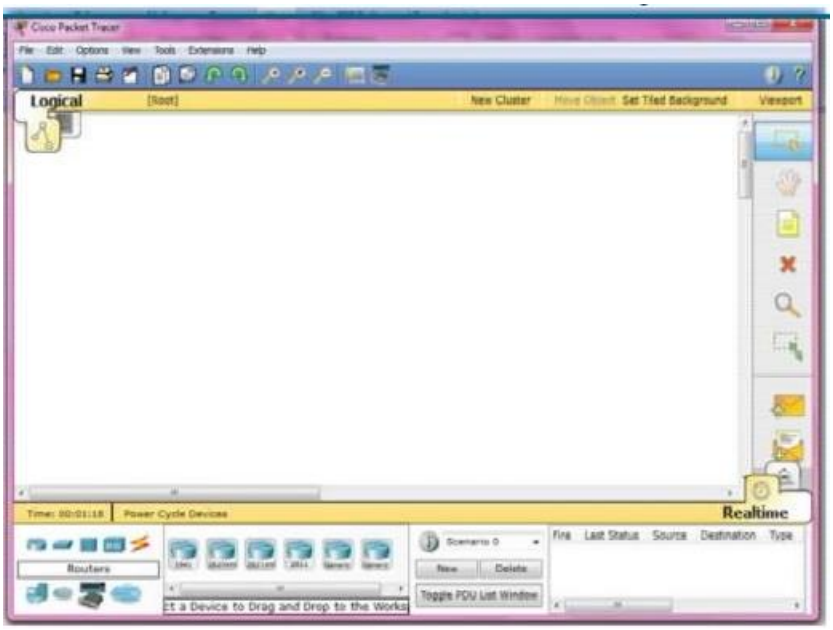


Figure 1. 3

Moving the cursor over the device categories will show the name of the category in the box. To select a device, first select the device category. Once the device category is selected, the options within that category appear in the box next to the category listings. Select the device option that is required. Select End Devices from the options in the bottom left-hand corner. Drag and drop two generic PCs onto the design area.

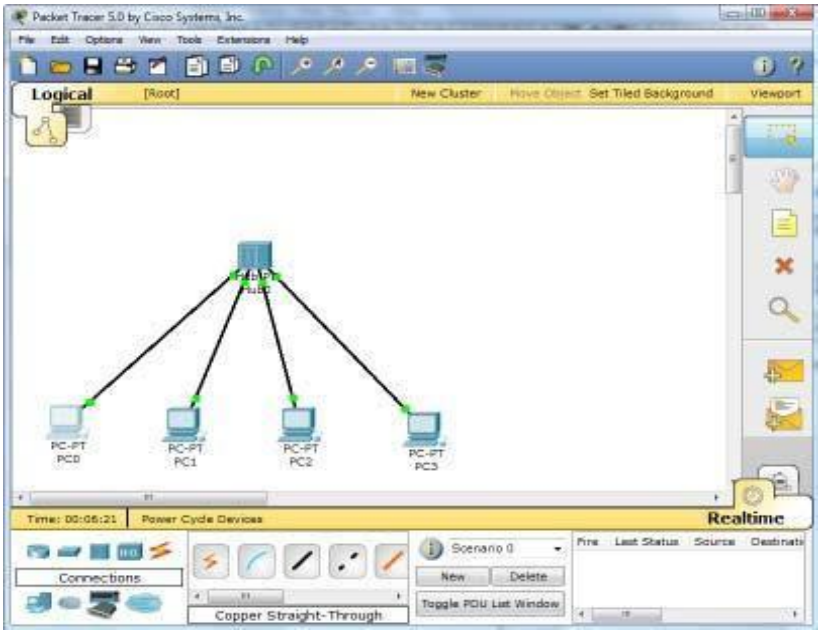


Figure 1. 4

- **Step 2 - Create A Logical Network Diagram With Four PCs And A Hub**

Select Hubs from the options in the bottom left-hand corner. Add a hub to the prototype network by dragging and dropping a generic hub onto the design area.

• Select End Devices from the options in the bottom left-hand corner. Add four PC:s to the prototype network by dragging and dropping them onto the design area.

• Select Connections from the bottom left-hand corner. Choose a Copper Straight-through cable type. Click the first host, PC0, and assign the cable to the FastEthernet connector. Click the hub, Hub0, and select a connection port, Port 0, to connect to PC0.

• Repeat the same steps for the second PC, PC1, to connect the PC to Port 1 on the hub.

• Repeat the same steps for the third PC, PC2, to connect the PC to Port 2 on the hub.

• Repeat the same steps for the last PC, PC3, to connect the PC to Port 3 on the hub.

There should be green dots at both ends of each cable connection. If not, check the cable type selected.

Step 3 - Configure The Hosts Attached To The Hub

• Configure host names and IP addresses on the PCs by clicking the PC0-icon. A PC0 window will appear.

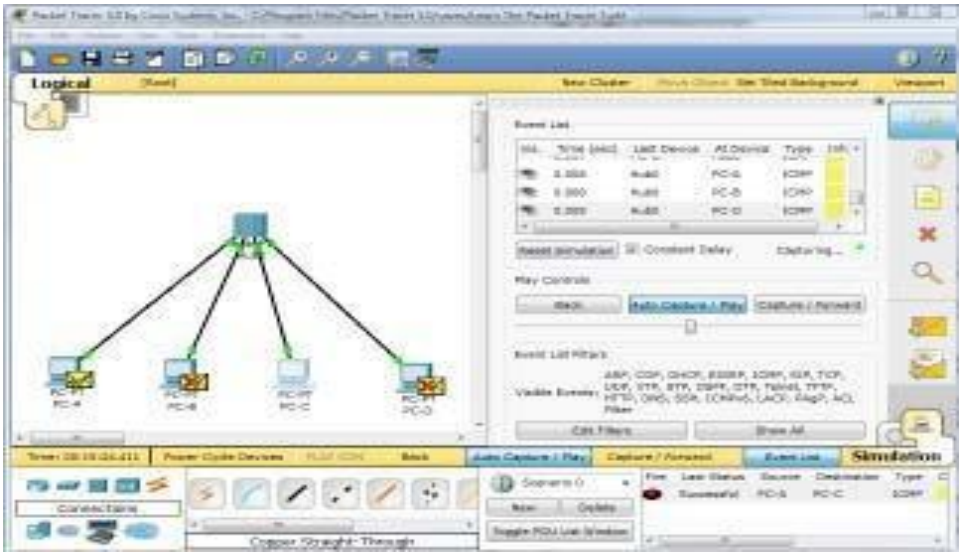


Figure 1

• From the PC0 window, select the Config tab. Change the PC Display Name to PC-A.

• Select the FastEthernet tab on the left and add the IP address of 192.168.1.1 and subnet mask of 255.255.255.0.

• Close the PC-A configuration window by selecting the x in the upper right-hand corner.

• Continue and configure PC1 by clicking on the PC1-icon.

• Select the Config tab. Change the PC Display Name to PC-B.

• Select the FastEthernet tab on the left and add the IP address of 192.168.1.2 and subnet mask of 255.255.255.0.

• Continue and configure PC2 by clicking on the PC2-icon.

• Select the Config tab. Change the PC Display Name to PC-C.

• Select the FastEthernet tab on the left and add the IP address of 192.168.1.3 and subnet mask of 255.255.255.0.

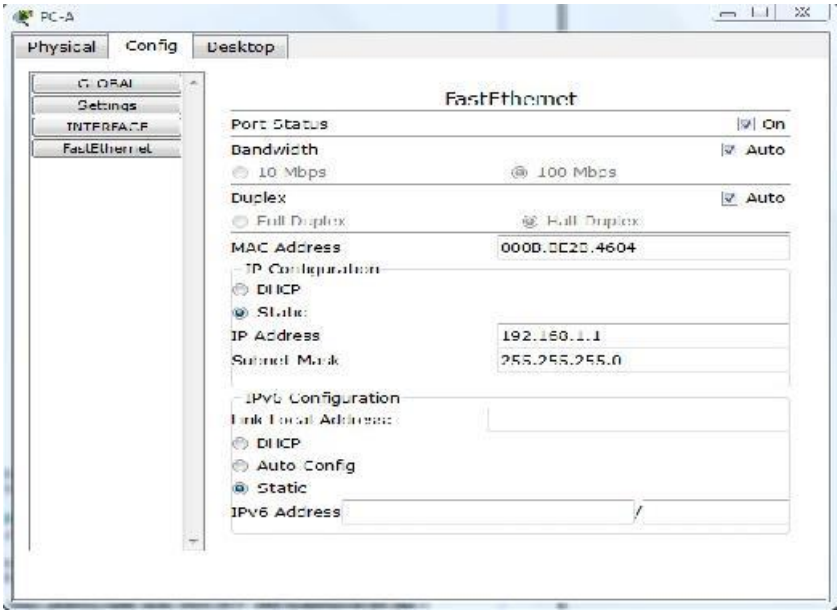
• Continue and configure PC3 by clicking on the PC3-icon.

• Select the Config tab. Change the PC Display Name to PC-D.

• Select the FastEthernet tab on the left and add the IP address of 192.168.1.4 and subnet mask of 255.255.255.0.

Step 4 - Run a Simulation of ICMP (ping)

• Switch to Simulation mode by selecting the tab that is partially hidden behind the Realtime tab in the bottom right-hand corner. The tab has the icon of a stopwatch on it.



• Click the Edit Filters button in the Event List Filters area. Clicking the Edit Filters button will create a popup window.

• In the pop-up window, click the Show All/None box to deselect every filter. Select just the ARP and ICMP filters.

• Select a Simple PDU by clicking the closed envelope on the right vertical toolbar.

• Move your cursor to the display area of your screen. Click PC-A to establish the source.

• Move your cursor to PC-C and click to establish the destination.

Notice that two envelopes are now positioned beside PC-A. One envelope is ICMP, while the other is ARP. The Event List in the Simulation Panel will identify exactly which envelope represents ICMP and which represents ARP.

• Select Auto Capture / Play from the Play Controls area of the Simulation Panel. Below the Auto Capture / Play button is a horizontal bar, with a vertical button that controls the speed of the simulation. Dragging the button to the right will speed up the simulation, while dragging it to the left will slow down the simulation.

• Choose the Reset Simulation button in the Simulation Panel. Notice that the ARP envelope is no longer present. This has reset the simulation but has not cleared any configuration changes or dynamic table entries, such as ARP table entries. The ARP request is not necessary to complete the ping command because PC-A already has the MAC address in the ARP table.

• Choose the Capture / Forward button. The ICMP envelope will move from the source to the hub and stop. The Capture / Forward button allows you to run the simulation one step at a time.

• Continue selecting the Capture / Forward button until you complete the event.

• Choose the Power Cycle Devices button on the bottom left, above the device icons.

An error message might appear asking you to confirm reset. Choose Yes. Now both the ICMP and ARP envelopes are present again. The Reset Network button will clear any configuration changes not saved and will clear all dynamic table entries, such as the ARP and MAC table entries.

Step 5 - View ARP Tables on Each PC

• Choose the Auto Capture / Play button to repopulate the ARP table on the PCs. Click OK when the No More Events message appears.

• Select the magnifying glass on the right vertical tool bar.

• Click PC-A. The ARP table for PC-A will appear. Notice that PC-A does have an ARP entry for PC-c. View the ARP table for PC-C. Close all ARP table windows.

• Click Select Tool on the right vertical tool bar. (This is the first icon present in the toolbar.)

• Click PC-A and select the Desktop tab.

• Select the Command Prompt and type the command arp -a and press enter to view the ARP table from the desktop view. Close the PC-A configuration window.

• Examine the ARP tables for the other PCs.

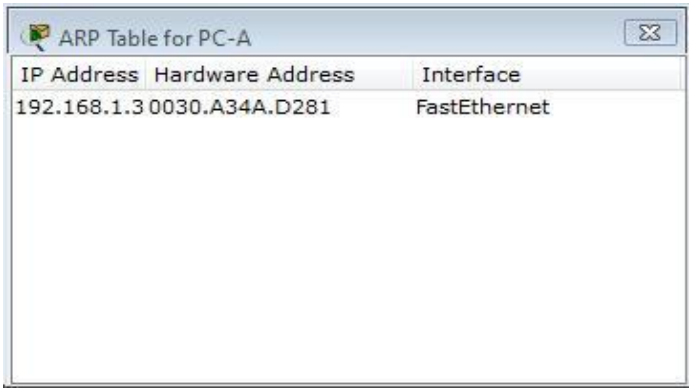


Figure 2

Critical Analysis/Conclusion

Lab Assessment		
Pre Lab	**/5**	**/25**
Performance	**/5**	
Results	**/5**	
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		

Lab #02: IP Addressing Scheme & VLSM

Pre Lab

IP Addressing Scheme & VLSM

Classful network is a term used to describe the network architecture of the Internet until around 1993. It divided the address space for Internet Protocol Version 4 (IPv4) into five address classes.

Each class, coded by the first three bits of the address, defined a different size or type (unicast or multicast) of the network.

All networks in practical use have different sizes.

For example, a company that will have 50 computers, will not need a network of 5000 computers, And on the contrary, a company that needs 5000 computers does not need a network that can only hold 50 computers. This is the main reason that engineers decided that IP address space should be divided in different classes in order to meet different requirements.

This addressing scheme is illustrated below.

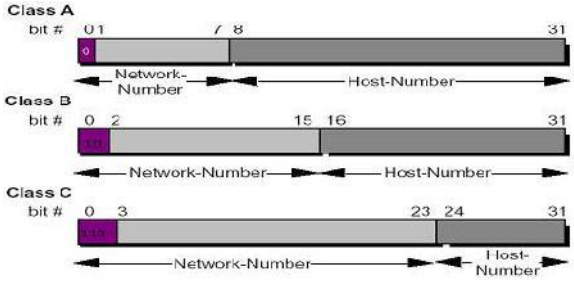


Figure2. 1

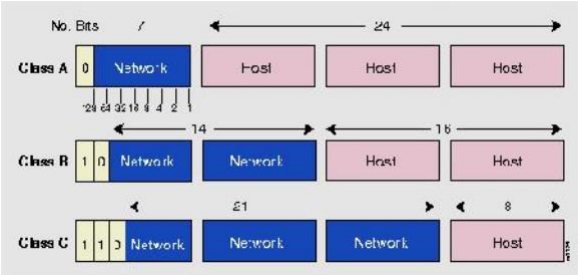


Figure2. 2

Class A Network (/ 8 Prefixes)

This network is 8-bit network prefix. Its highest bit is set to 0, and contains a 7-bit network number and a **24-bit host number**.

A maximum of **126, which is (2 ^{7} -2,) networks can be defined**; two is subtracted because all an (0 and 1) subnet cannot be used in certain routers using RIP-1 Protocol. Each network

supports a maximum of 16,777,214 (2^{24} -2) hosts per network. You must subtract two because the base network represents host "0", and the last host on the network is actually used for 1s ("broadcast") and may not be assigned to any host.

The class **A** network address block contains 2^{31} power (2,147,483,648) individual addresses. The IPv4 address space contains a maximum of 2^{32} power (4,294,967,296) addresses, which mean that a class **A** network address space is 50% of the total IPv4 unicast, address space.

Class B Networks (/16 Prefixes)

This network is a 16-bit network prefix; its highest bit order is set to **1-0**. It is a 14-bit network number with a 16-bit host number.

This class defines 16,384 (2^{14}) /16 networks, and supports a maximum of 65,534 (2^{16} -2) hosts per network. Class B /16 block address is (1,073,741,824) = 2^{30}; therefore it represent 25% of the total IPV4.

Class C Networks (/24 Prefixes)

This is a 24-bit network prefix; it has a 3 bit set to the highest order **1-1-0**. It is a 21-bit network number with 8-bit host number.

This class defines a maximum of 2,097,152 (2^{21}) /24 networks. And each network supports up to 254 (2^{8} -2) hosts. The entire class C network represents 2^{29} (536,870,912) addresses; therefore it is only 12.5 % of the total IPv4.

Other Networks

There are two other networks that are not commonly used, class D and Class E. Class D has its highest bit order set to **1-1-1-0** it is used to support multicasting. Class E has its highest bit order set to **1-1-1-1** which is reserved for experimental use.

Network classes are summarized in following table.

Class	Leading Bits	Size of *Network Number* Bit field	Size of *Rest* Bit field	Number of Networks	Addresses per Network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

Figure2. 3

Pre Lab Task

For The IP address 192.168.0.1 find the network mask, broadcast address number of hosts, IP address of first and last host

Introduction to Subnetting

Purpose:

The lab is intended to familiarize the students with a networking technique of SUBNETTING. At the end of the lab the student must know:

• The Purpose of SUBNETTING.

• Steps of SUBNETTING.

• How to perform SUBNETTING on different IP Classes.

• Calculating the ranges of Hosts in the Subnet.

• Finding the Broadcast address of the Subnet.

• How to make a SUBNET on Linux machines.

• How to Broadcast on that Subnet.

```
prompt> ifconfig <interfaceNo> xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx

prompt> ifconfig eth0 172.20.6.131 netmask 255.255.248.0

prompt> ping -b <broadcast_ip>
```

Subnetting:

In subnetting, a network is divided into smaller subnets with each subnet having its own subnet address.

Reasons for Subnetting

- Imagine a Network Class A with over 16 millions of hosts or a Class B Network with 65 thousand hosts, it is impractical…
- Most IP address assignments were not used very efficiently.
- Broadcast problem.
- Many sites were requesting multiple network numbers due to variable amounts of networks at their sites.

Benefits of subnetting

- Reduced network traffic
- Simplified management
- Smaller broadcast domains

Figure2. 4

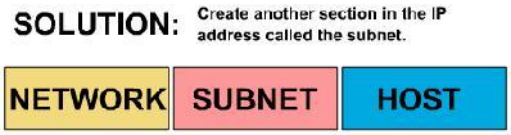


Figure2. 5

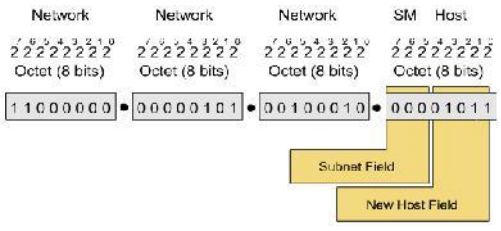


Figure2. 6

Network before Subnetting

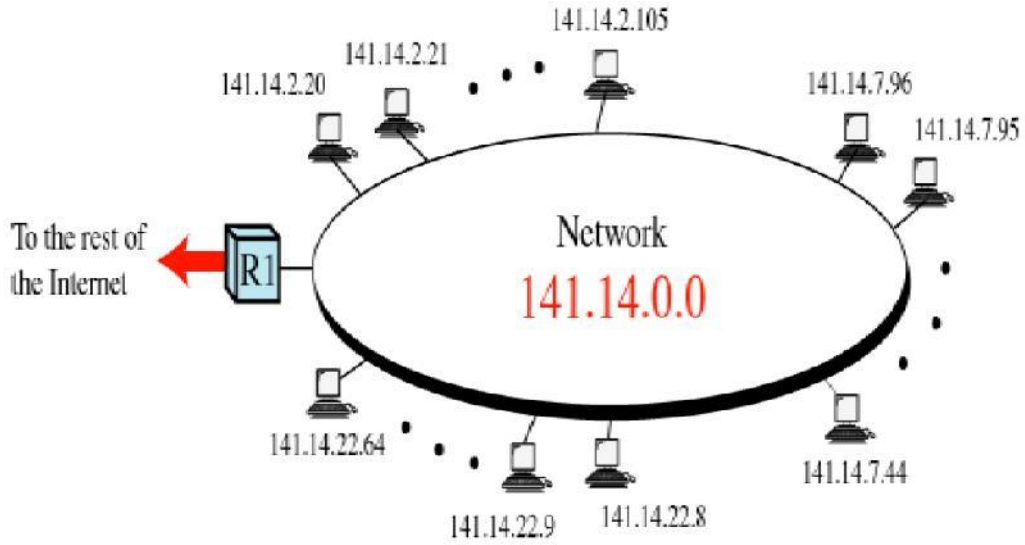


Figure2. 7

Network after Subnetting

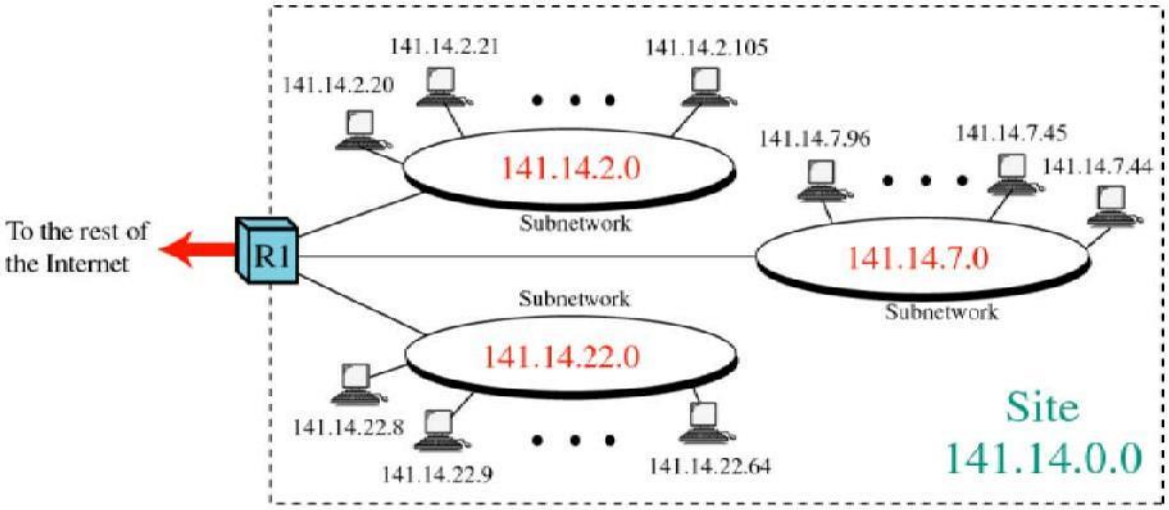


Figure2. 8

SUBNETTING:

The purpose of subnetting is that by using only one given IP we can make different networks.

E.g. If the Given IP is: 172.16.0.0 and we are required to make 169 Subnets, then, by using the following formula for subnets we can find the no. of bits required for the subnets:

$$2^n - 2 >= \text{No. of Subnets.}$$

Where 'n' is No. of Bits further required as network address field in the given IP. Therefore for 169 subnets we get n = 8. So the new mask becomes: 255.255.255.0

First subnet IP address: 172.16.1.0

First PC IP address in this Subnet: 172.16.1.1

Last PC IP address in this Subnet: 172.16.1.254

Broadcast IP address in this Subnet: 172.16.1.255

Last subnet IP address: 172.16.254.0

First PC IP address in this Subnet: 172.16.254.1

Last PC IP address in this Subnet: 172.16.254.254

Broadcast IP address in this Subnet: 172.16.254.255

Default Subnet mask

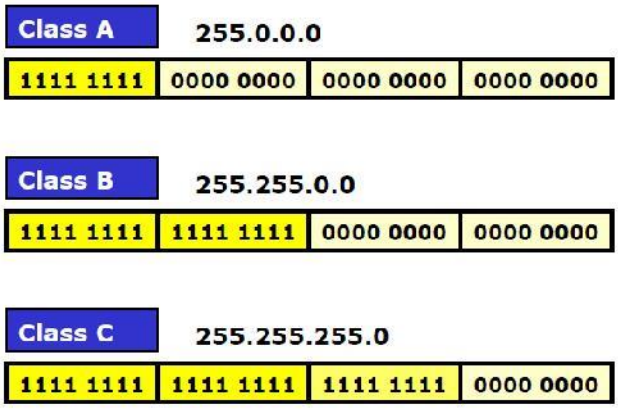


Figure2. 9

Masking

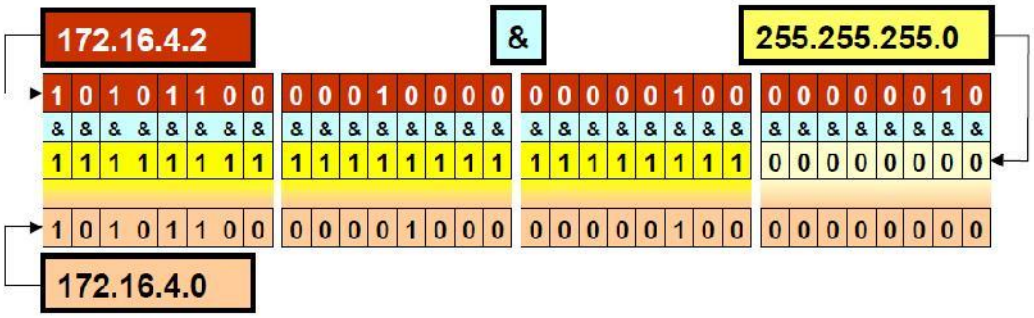


Figure2. 10

Packet Tracer:

Packet Tracer is a self-paced, visual, interactive teaching and learning tool developed by Cisco. Lab activities are an important part of networking education. However, lab equipment can be a scarce resource. Packet Tracer provides a visual simulation of equipment and network processes to offset the challenge of limited equipment. Students can spend as much time as they like completing standard lab exercises through Packet Tracer, and have the option to work from

home. Although Packet Tracer is not a substitute for real equipment, it allows students to practice using a command-line interface. This "e-doing" capability is a fundamental component of learning how to configure routers and switches from the command line.

Steps for First Simulation:

1. Familiarize yourself with the packet tracer. Check all the devices and type of connections available in it.
2. To implement very basic subnetting scenario. Select a switch from switches tab in the bottom right corner of screen.
3. Drag it to the middle of the screen.
4. Then from the end devices tab select desktop PC and drag them to screen. At least 8 of them.
5. Connect these computers to switch using straight-over cable.
6. Next task is to configure all the computers with IP addresses from the subnet they belong.
7. To configure IP address double clicks on any computer. You will see three tabs on top of the window. Go to the Desktop Tab, last one. There you will see different configuration utilities. Use them to assign IP address to computer. Pay special attention to subnet mask.
8. Repeat step 7 for all computers.
9. Now use ping utility to check to communication between computers of same subnet and then among different subnets.

Lab Task 1:

For The following IPs find the first two and last two Subnets and give their Pc range and Broadcast address.

1. 10.0.0.0 for 1025 subnets.

2. 212.31.30.0 for 21 subnets.

3. 190.38.0.0 for 645 subnets.

VLSM

VLSM - Variable Length Subnet Mask

- A technique for conserving Internet Protocol (IP) addresses.
- VLSM reduces the amount of wasted addresses by selecting a subnet mask closest to the needs of each network.
- Variable-length subnet mask (VLSM) was developed in response to shortages in the available pool of IP addresses. Large IP internetworks consisting of multiple subnets typically use assigned IP address blocks inefficiently. This is because although different subnets often have different numbers of hosts, network architects usually design IP internetworks using a single "one size fits all" subnet mask.
- Subnetting is based up HostId portion bits.
- In this case we reserve some bits in hostid portion rest of the bits will be in Netid portion bits.
- Subnet Mask varies for each subnet.
- Actually, you can take a subnetted subnet and subnet it again! With this process, you can come up with a very efficient addressing scheme to accommodate addressing needs in your network.

Principle

- Permit better sized subnetwork
- Permit the waste of less IP addresses
- Variable lenght of subnet mask
- Use classless
- Use of a hierarchical address plan
- Routers must implement the longest match algorithm

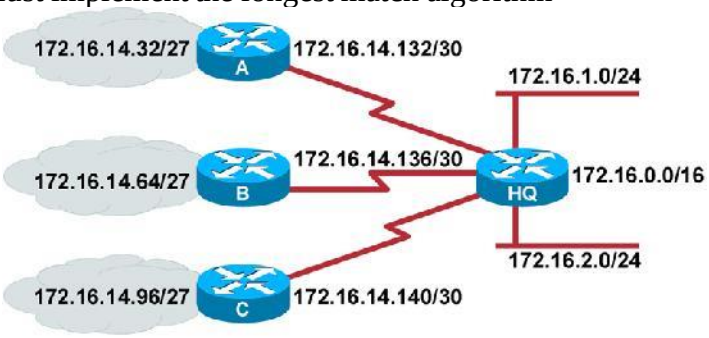


Figure2. 11

- Subnet 172.16.14.0/24 is divided into smaller subnets
- Subnet with one mask (/27)

- Then further subnet one of the unused /27 subnets into multiple /30 subnets

Calculating VLSMs

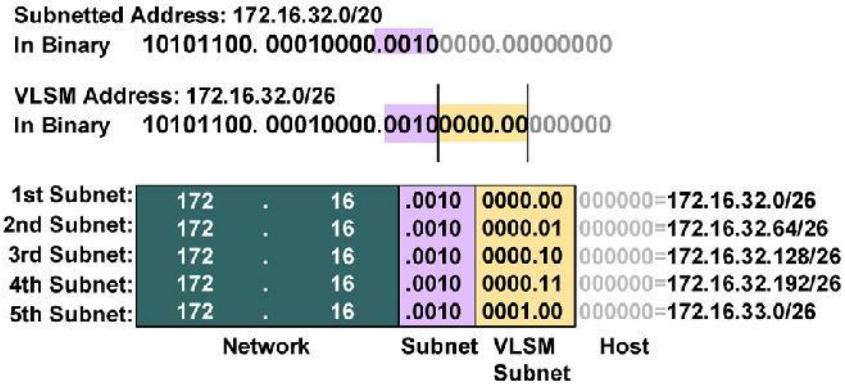


Figure2. 12

A Working VLSM Example

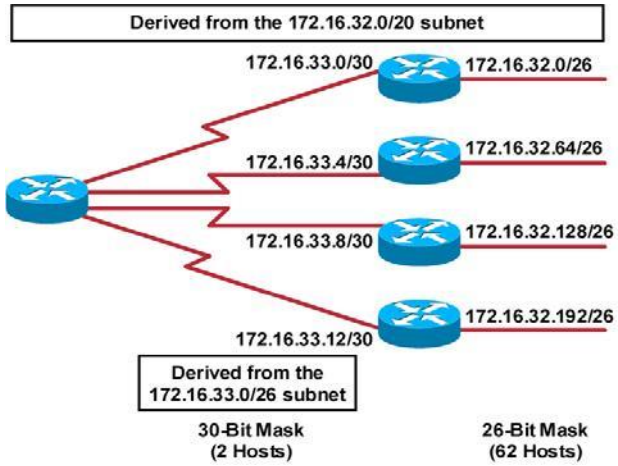


Figure2. 13

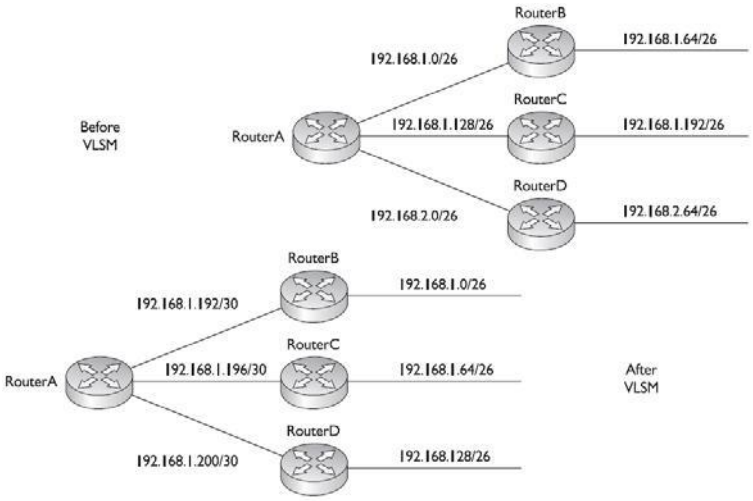


Figure2. 14

Task2:

Implement first two subnets created in Task (1-2) in Packet Tracer.

Addressing with VLSM

To use VLSM, you must be very familiar with IP address and normal subnetting. If you have not yet fully grasped these concepts, VLSM will be out of your reach. VLSM basically means talking a subnet (not a network number) and applying a different subnet mask to this, subnet. This section covers how to create and efficient addressing scheme using VLSM.

Steps of VLSM

- You should follow these steps when performing VLSM:

1. Find the largest segment in the network address apace – the segment with the largest number of advices connected to it.

2. Find the appropriate subnet mask for the largest network segment.

3. Write down your subnet number to fir your subnet mast.

4. For your smaller segments, take one of these newly created subnets and apply a different, more appropriate, subnet mask to it.

5. Write down your newly subnetted subnets.

6. For even smaller segment, go back to step 4 and repeat this process.

- Actually, you can take a subnetted subnet and subnet it again! With this process, you can come up with a very efficient addressing scheme to accommodate addressing needs in your network.

◙VLSM Example

Class “C” network

192.168.2.0/24

You are tasked with using VLSM to accommodate the 30 hosts and this isn't expected to grow in the future.

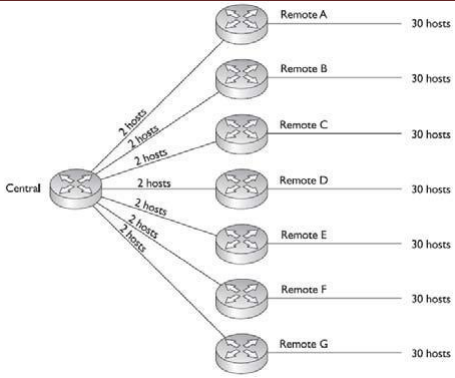


Figure2. 15

VLSM Example Address design

Class "C" network

192.168.2.0/24

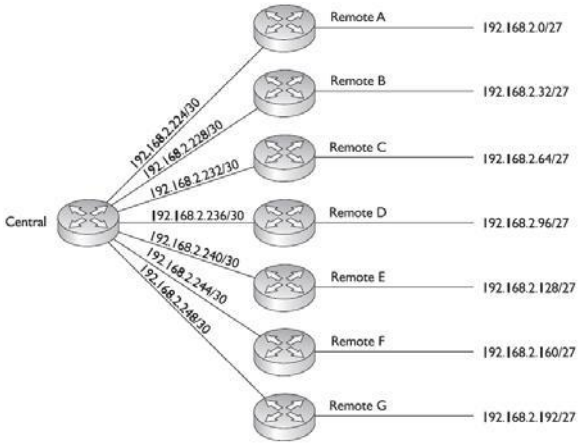


Figure2. 16

Critical Analysis/Conclusion

Lab Assessment		
Pre Lab	**/5**	**/25**
Performance	**/5**	
Results	**/5**	
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		

Lab 3: Network Cabling, Basic CISCO Devices Configuration & Introduction to Wireshark

Pre Lab

Network Cabling & Basic CISCO Devices Configuration

Poor or incorrectly installed network cabling can cause numerous problems with your computer network. Whilst we recommend that you employ a network / cabling specialist to wire and configure your network, we have compiled some important information to help you avoid some of the more common pitfalls.

It is very important to understand that a problem with your network cabling, however small it may appear, can have a catastrophic effect on the operation of your audio network.

WIRING STANDARD

There are two wiring standards for network cabling, T568a and T568b. We will be discussing using the T568b specification.

It is essential that you DO NOT MIX T568a and T568b on the same network.

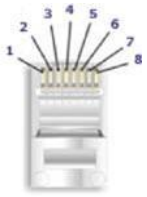


Figure3. 1

USE HIGH QUALITY CAT 5e or CAT 6 cabling

Audio files are generally very large data files and need to be moved around the network as quickly as possible. All the computers sold by BSI are capable of network transfer at 1 Gbps (a Gigabit) full- duplex; however your existing network cabling, switches and routers may not be capable of supporting this speed and may only operate at the more common 100 Mbps,

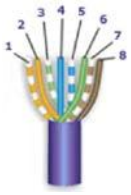


Figure3. 2

Whilst generally it is possible to utilize good quality Cat 5 cabling for Gigabit networks, we highly recommend that you stick to the 'in spec' Cat 5e standard or highly quality Cat 6 cabling and wire for Gigabit connectivity even if your existing network switches and routers only support 100 Mbps. This will then ensure that the cabling infrastructure is in place when the Gigabit routers and switches are more readily available.

Figure3. 3

The rest of the points apply equally to 1Gbps and 100 Mbps connections – each can be affected badly by poor cabling / wrong connections.

In high RF environments, it is also essential to use 'shielded twisted pair' (STP) rather than 'unshielded twisted pair' to prevent interference.

HAVE GOOD CABLES RUNS

Cabling between each of the computers should be in a 'star' configuration with each computer having a separate cable run to the central switch and / or router.

Each cable should be no longer than 265 feet and should be a single piece of cable (there should be no joins). Cabling should NOT be run next to electrical mains cabling (because of the potential for interference); nor should network cabling be suspended on ceiling tiles (this may violate building code and fire regulations).

As typically network cabling uses solid wire, cabling should not be twisted or bent into a tight radius. Do not use metal staples to secure cable runs, nor tightly adjusted cable wraps.

We recommend that you 'flood' wire any new facility with Cat 5e or higher specification wiring, preferably to professional RJ45 patch bays.

This is because as well as network connections; this wiring can also be used for telephone systems and network cabling makes excellent audio cabling runs (the capacitance of the

network cable is such as to allow high- bandwidth, high-speed data to transfer and is perfect for both analog and digital audio).

USE THE RIGHT PLUGS!

Network connections use RJ45 plugs which look similar but are not the same as telephone plugs (which are RJ11). Cables are inserted into the plug and a special tool is used to make the connection between the plug-pins and the cabling – do not try to do this with a screw-driver or pair of pliers!

Typically, cabling will be made up of pairs of 'solid' or 'single-core' wires rather than the more flexible stranded wire often used in patch cables.

RJ45 plugs are designed for either just stranded or just solid cable but usually not both. It's virtually impossible to tell the difference by looking at the plugs themselves – you need to be sure that you specify the correct plugs when ordering them

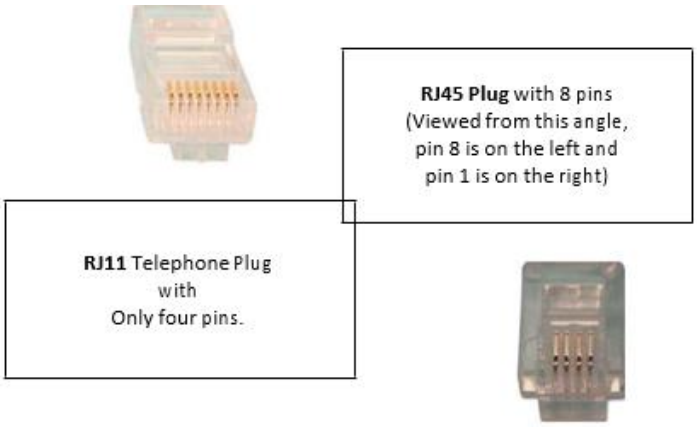


Figure3. 4

DO NOT UNTWIST MORE THAN 0.25" OF CABLE

Network cabling comprises of 4 pairs of twisted wires which are color coded (Orange, Green, Blue and Brown).

The cable specification is such that it has been designed for high-speed data-transfer and very little cross-talk (interference between pairs of wires).

It is very important that no more than about a quarter of an inch of the cable is untwisted at either end as this can lead to problems such as 'near end cross-talk' which will have a detrimental effect on your network.

KEEP THE PAIRS TOGETHER & WIRE CORRECTLY!

As previously mentioned, network cabling comprises of four pairs of wires, although only two pairs are normally used. Despite this, all the pairs should always be wired to maintain the network specification. The cable pair colors, pair numbers and wire descriptions are shown in the table below.

COL	PAI	DESCRIPTION
White / Blue	1	Unused Unused
White / Orange	2	Transmit Data + Transmit Data -
White / Green	3	Receive Data + Receive Data -
White / Brown	4	Unused Unused

Table 3. 1

Confusingly, the 'pairs' in the RJ45 plug run across the following pins. It is essential that you wire the plug correctly and not just from pins 1 through 8 at both ends (note that in this example, the 'hook' on the plug is facing the front):

RJ45	PAI	COL
1 2	2	White / Orange Orange
3	3	White / Green
4 5	1	Blue White / Blue
6	3	Green
7 8	4	White / Brown Brown

Table 3. 2

Figure3. 5

IDENTIFYING PIN NUMBERS

RJ45 plugs have a little ‘hook’ that locks the plug into the socket as can be seen from the enlarged images below. Take time to study the orientation of the plug.

Figure3. 6

Now flip the plug over so that the ‘pins’ are on top, the ‘hook’ underneath and the cable entry towards you and from left to right will be pins 1 to 8…both cable ends are normally wired the same.

Figure3. 7

Now flip the plug over so that the ‘pins’ are on top, the ‘hook’ underneath and the cable entry towards you and from left to right will be pins 1 to 8…both cable ends are normally wired the same.

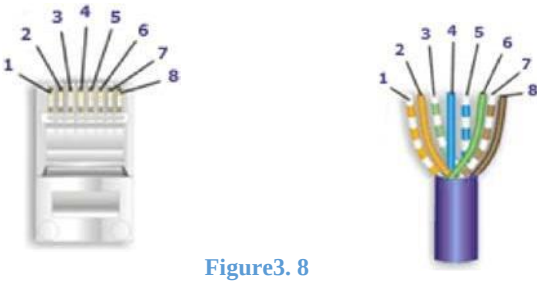


Figure3. 8

The above wiring conforms to the T568b specification and is used for connections between a computer and hub; computer and switch; computer and router; and computer and cable modem.

CROSSOVER CABLE

There are instances where you need to connect two devices such as a switch and a hub together, or a router andcable modem together which involves the Transmit pair of cables on one device talking to the Receive pair of the other device.

Typically, these devices will be fitted with an ‘uplink’ port and you should plug one end of the cable into the uplink port of one device only as the uplink port automatically crosses over the Transmit and Receive pairs in the device itself so that the two devices can ‘talk’ to each other.

If an uplink port is not available, you will have to wire a cross-over cable at one end of a standard RJ45 cable, the diagram below shows first the standard cable end followed by the crossed over cable end.

STANDARD CABLE END

Figure3. 9

One cable end should be wired as above, in the standard configuration. The other end should be wired as cross- over. Note that the Orange and Green Pairs are now crossed over.

CROSSOVER CABLE END

Figure3. 10

USE THE CORRECT TERMINATING TOOL!

As stated before, do not attempt to crimp the RJ45 plug using a screwdriver, metal block or pair of pliers! If you are going to be wiring network cabling, it is worth investing in a high-quality crimping tool.

The better ones will crimp RJ45 and telephone connectors and contain metal blades to cut the network cabling and strip the outer cable cover back and are very easy to use.

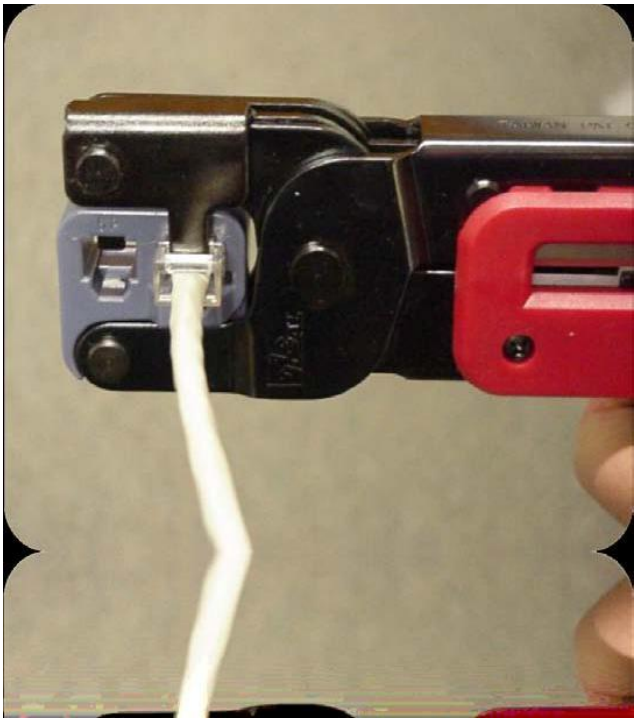


Figure3. 11

CONSIDER USING PATCH PANELS

If you are installing network cabling at a new facility, we strongly suggest that you wire cabling to an RJ45 patch panel. Each room should be 'flood wired' with ample RJ45 sockets that can then be patched as either Network (data), Telephone (voice), or Analog or Digital Audio.

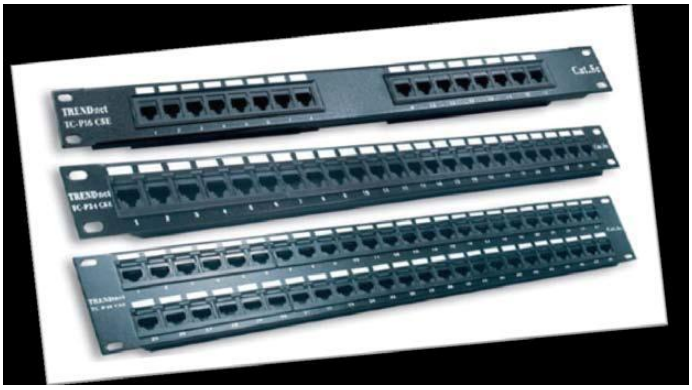


Figure3. 12

Basic Cisco Device Configuration

Topology Diagram

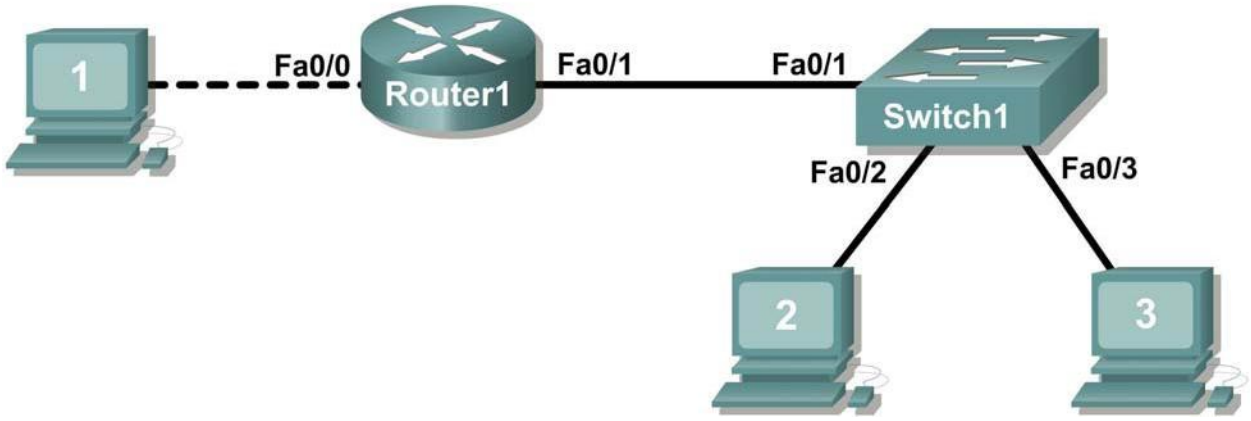


Figure3. 13

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

Hardwar	Qty	Descriptio
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 3. 3 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.

Pre Lab Task

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: _____

Number of usable hosts per subnet: _____

	IP Address:		Subnet mask:	
#	Subnet	First host address	Last host address	Broadcast
0				

Table 3. 4

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

Lab Task

Task 1: Configure Cisco Router Global Configuration Settings.

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).

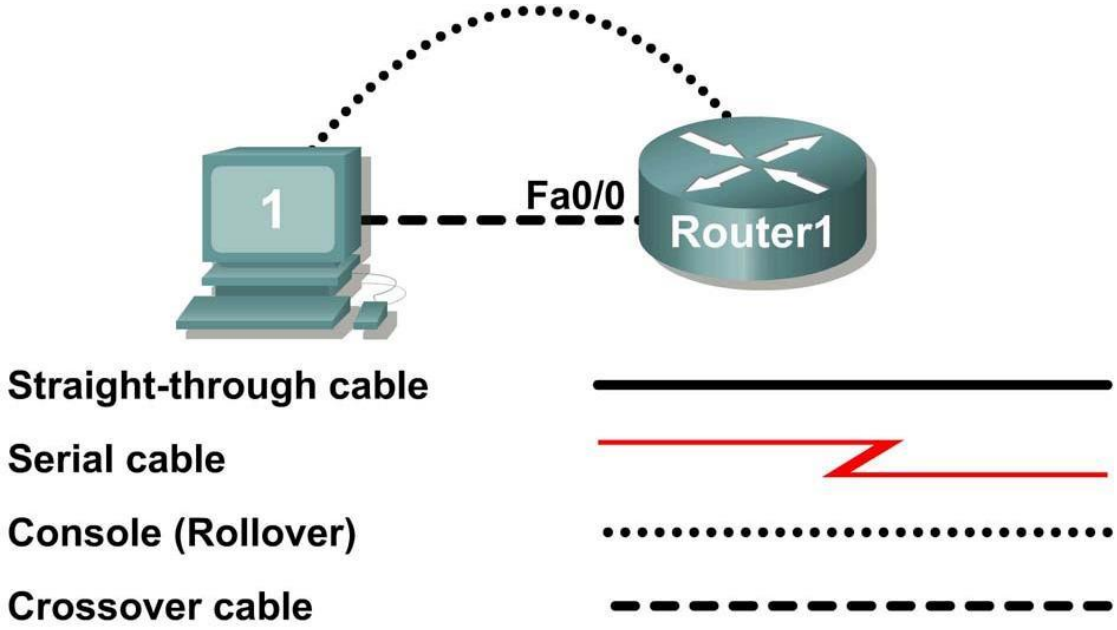


Figure3. 14

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

Step 2: Connect host computer to router through HyperTerminal.

From the Widows 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 4: 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.

Table 3. 5

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.

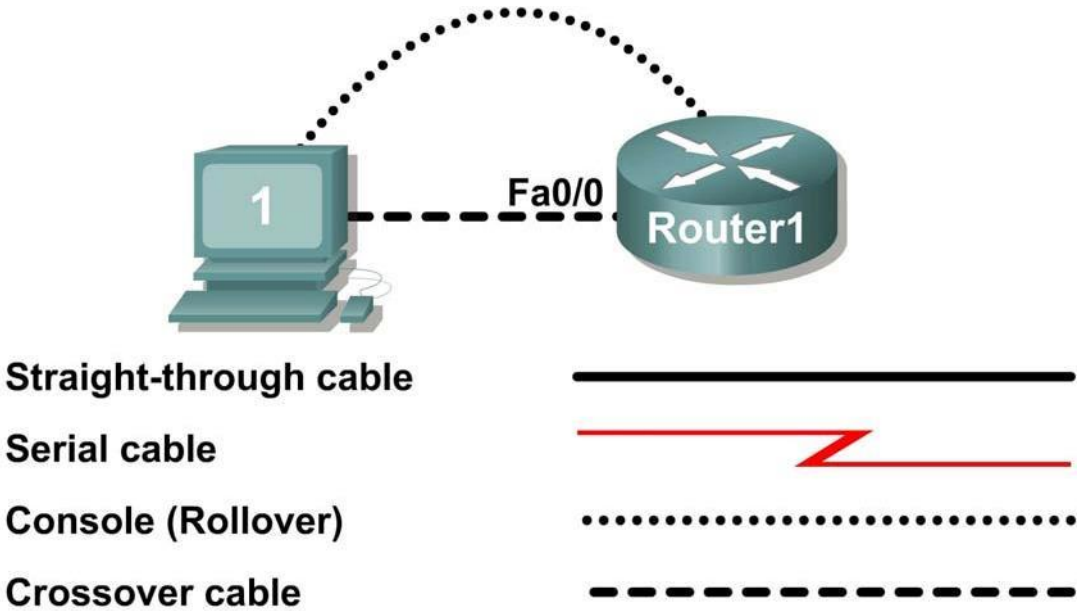


Figure3. 15 Physical lab topology.

Figure 3.15 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:

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

Table 3. 6

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
```

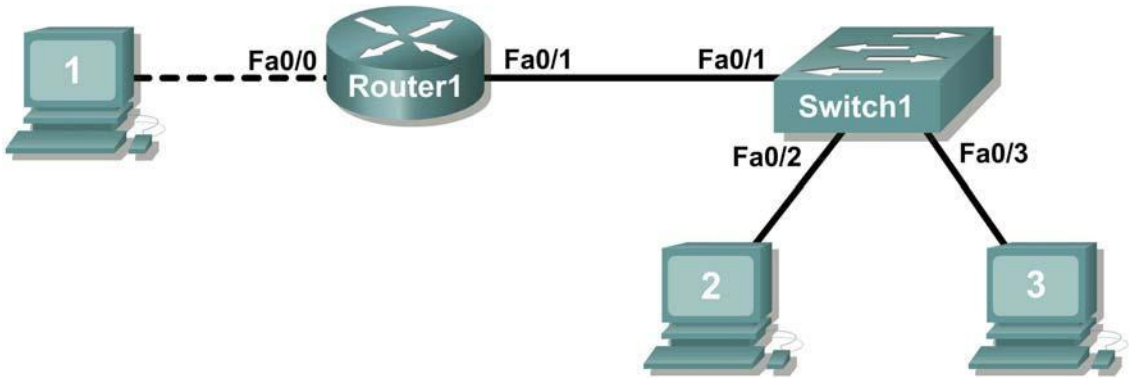


Figure3. 16 Network topology.

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	

Table 3. 7

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 8: 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.	`configure terminal`
	`Example: Router> enable`
	`Router# configure terminal`

Specify the name for the router.	`hostname name`
	`Example:`
	`Router(config)# hostname Router1`

Specify an encrypted password to prevent unauthorized access to the privileged exec mode.	`enable secret password`
	`Example:`
	`Router(config)# enable secret cisco`

Specify a password to prevent unauthorized access to the console.	`password password`
	`login`
	`Example:`
	`Router(config)# line con 0`

Specify a password to prevent unauthorized telnet access. Router vty lines: 0 4 Switch vty lines: 0 15	**password *password*** **login** **Example:** **Router(config)# line vty 0 4**
Configure the MOTD banner.	**Banner motd %** **Example:** **Router(config)# banner motd %** **Router(config)#**
Configure an interface. Router- interface is OFF by default Switch- interface is ON by default	**Example:** **Router(config)# interface fa0/0** **Router(config-if)# description *description*** **Router(config-if)# ip address *address mask*** **Router(config-if)# no shutdown** **Router(config-if)#**
Save the configuration to NVRAM.	**copy running-config startup-config** **Example:** **Router# copy running-config startup-config**

Table 3. 8

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.

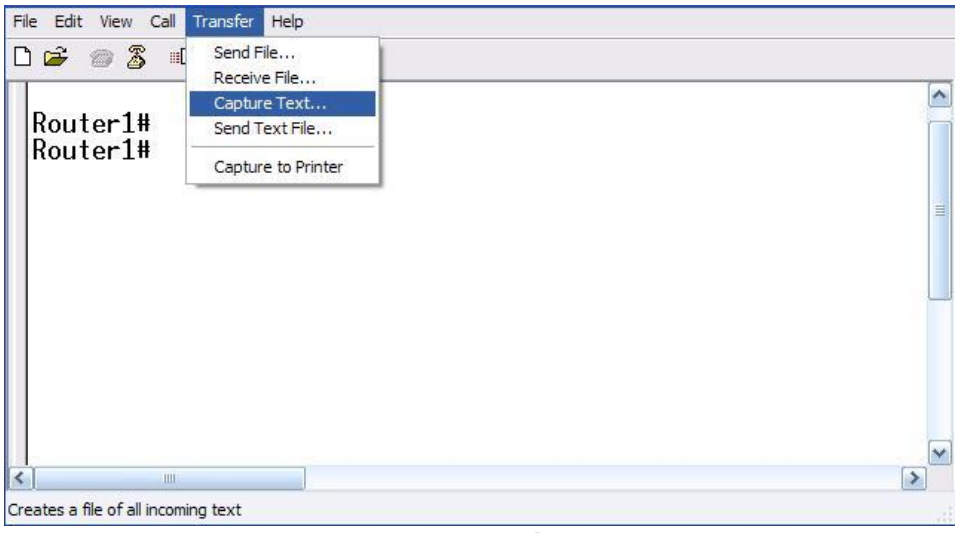


Figure3. 17 Hyperterminal Capture menu.

Refer to Figure 3.17 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 8: Clean Up.

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.

Wireshark Tutorial

INTRODUCTION

The purpose of this document is to introduce the packet sniffer WIRESHARK. This document introduces the basic operation of a packet sniffer, installation, and a test run of WIRESHARK.

PACKER SNIFFER

The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer**. As the name suggests, a packet sniffer captures ("sniffs") messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a *copy* of packets that are sent / received from/by application and protocols executing on your machine.

Figure 1 shows the structure of a packet sniffer. At the right of Figure 1 are the protocols (in this case, Internet protocols) and applications (such as a web browser or ftp client) that normally run on your computer. The packet sniffer, shown within the dashed rectangle in Figure 1 is an addition to the usual software in your computer, and consists of two parts. The **packet capture library** receives a copy of every link-layer frame that is sent from or received by your computer. Messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP all are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable. In Figure 1, the assumed physical media is an Ethernet, and so all upper layer protocols are eventually encapsulated within an Ethernet frame. Capturing all link-layer frames thus gives you all messages sent/received from/by all protocols and applications executing in your computer.

The second component of a packet sniffer is the **packet analyzer**, which displays the contents of all fields within a protocol message. In order to do so, the packet analyzer must "understand" the structure of all messages exchanged by protocols. For example, suppose we are interested in displaying the various fields in messages exchanged by the HTTP protocol in Figure 1. The packet analyzer understands the format of Ethernet frames, and so can identify the IP datagram within an Ethernet frame. It also understands the IP datagram format, so that it can extract the TCP segment within the IP datagram. Finally, it understands the TCP segment structure, so it can extract the HTTP message contained in the TCP segment. Finally, it understands the HTTP protocol and so, for example, knows that the first bytes of an

HTTP message will contain the string “GET,” “POST,” or “HEAD”.

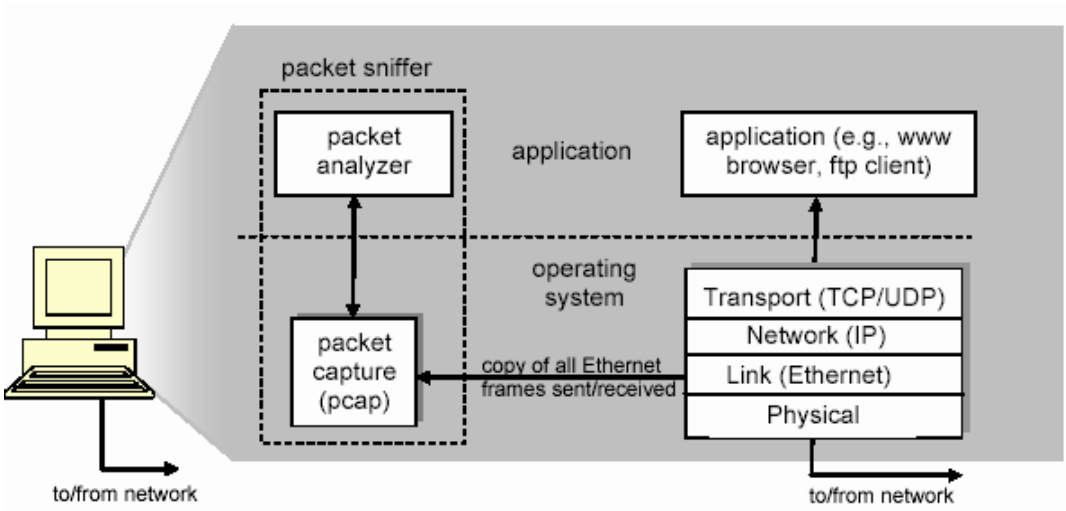


Figure 3.18: Packet sniffer structure

Running Wireshark

When you run the Wireshark program, the Wireshark graphical user interface shown in Figure 2 will de displayed. Initially, no data will be displayed in the various windows.

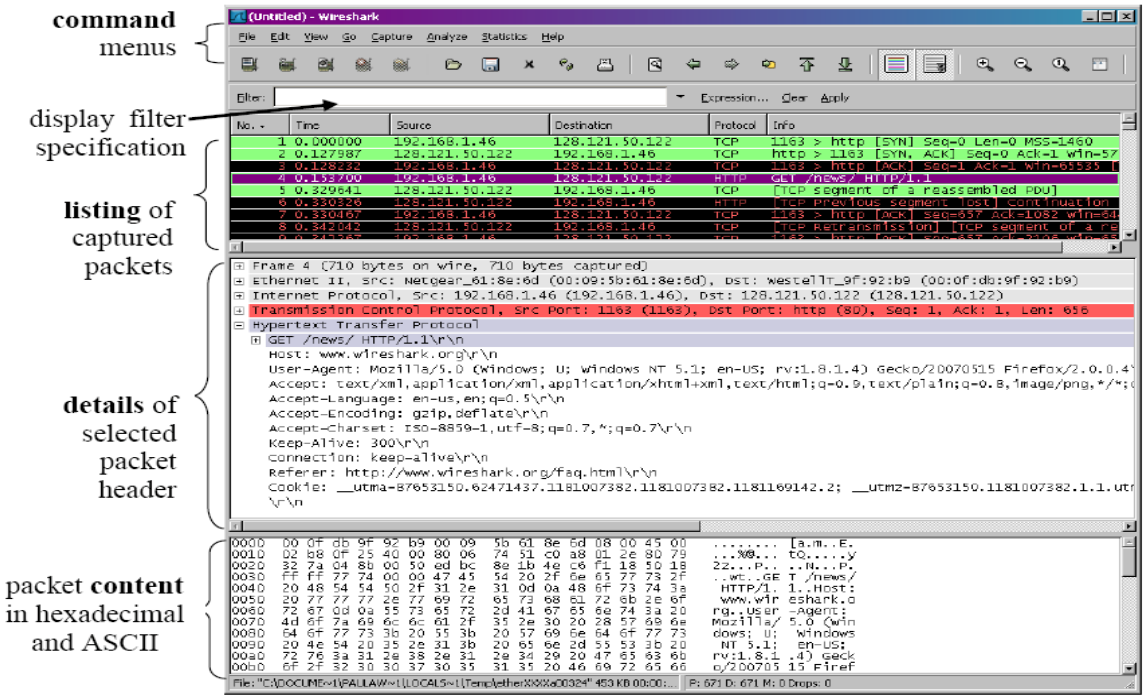


Figure 3.19: Wireshark Graphical User Interface

The Wireshark interface has five major components:

- The **command menus** are standard pulldown menus located at the top of the window. Of interest to us now are the File and Capture menus. The File menu allows you to save captured packet data or open a file containing previously captured packet data, and exit the Wireshark application. The Capture menu allows you to begin packet capture.

- The **packet-listing window** displays a one-line summary for each packet captured, including the packet number (assigned by Wireshark; this is *not* a packet number contained in any protocol's header), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. Theprotocol type field lists the highest level protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet.

- The **packet-header details window** provides details about the packet selected (highlighted) in the packet listing window. (To select a packet in the packet listing window, place the cursor over the packet's one-line summary in the packet listing window and click with the left mouse button.). These details include information about the Ethernet frame and IP datagram that contains this packet. The amount of Ethernet and IP-layer detail displayed can be expanded or minimized by clicking on the right-pointing or down-pointing arrowhead to the left of the Ethernet frame or IP datagram line in the packet details window. If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed, which can similarly be expanded or minimized. Finally, details about the highest level protocol that sent or received this packet are also provided.

- The **packet-contents window** displays the entire contents of the captured frame, in both ASCII and hexadecimal format.

- Towards the top of the Wireshark graphical user interface, is the **packet display filter field,** into which a protocol name or other information can be entered in order to filter the information displayed in the packet-listing window (and hence the packet-header and packet-contents windows). In the example below, we'll use the packet-display filter field to have Wireshark hide (not display) packets except those that correspond to HTTP messages.

Capturing Packets

Click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface. You can configure advanced features by clicking Capture Options, but this isn't necessary for now.

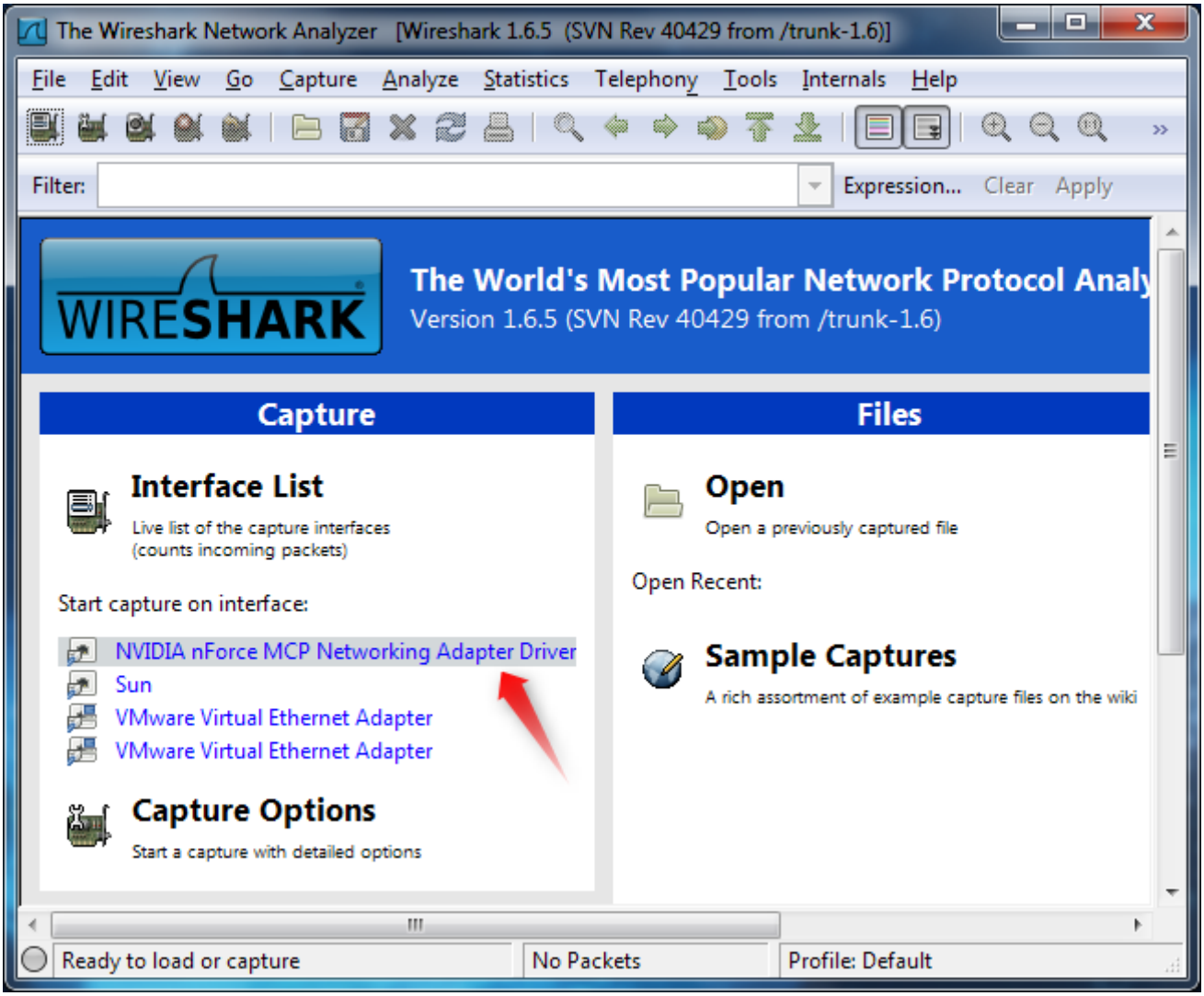


Figure 3.20

As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system. If you're capturing on a wireless interface and have promiscuous mode enabled in your capture options, you'll also see other the other packets on the network.

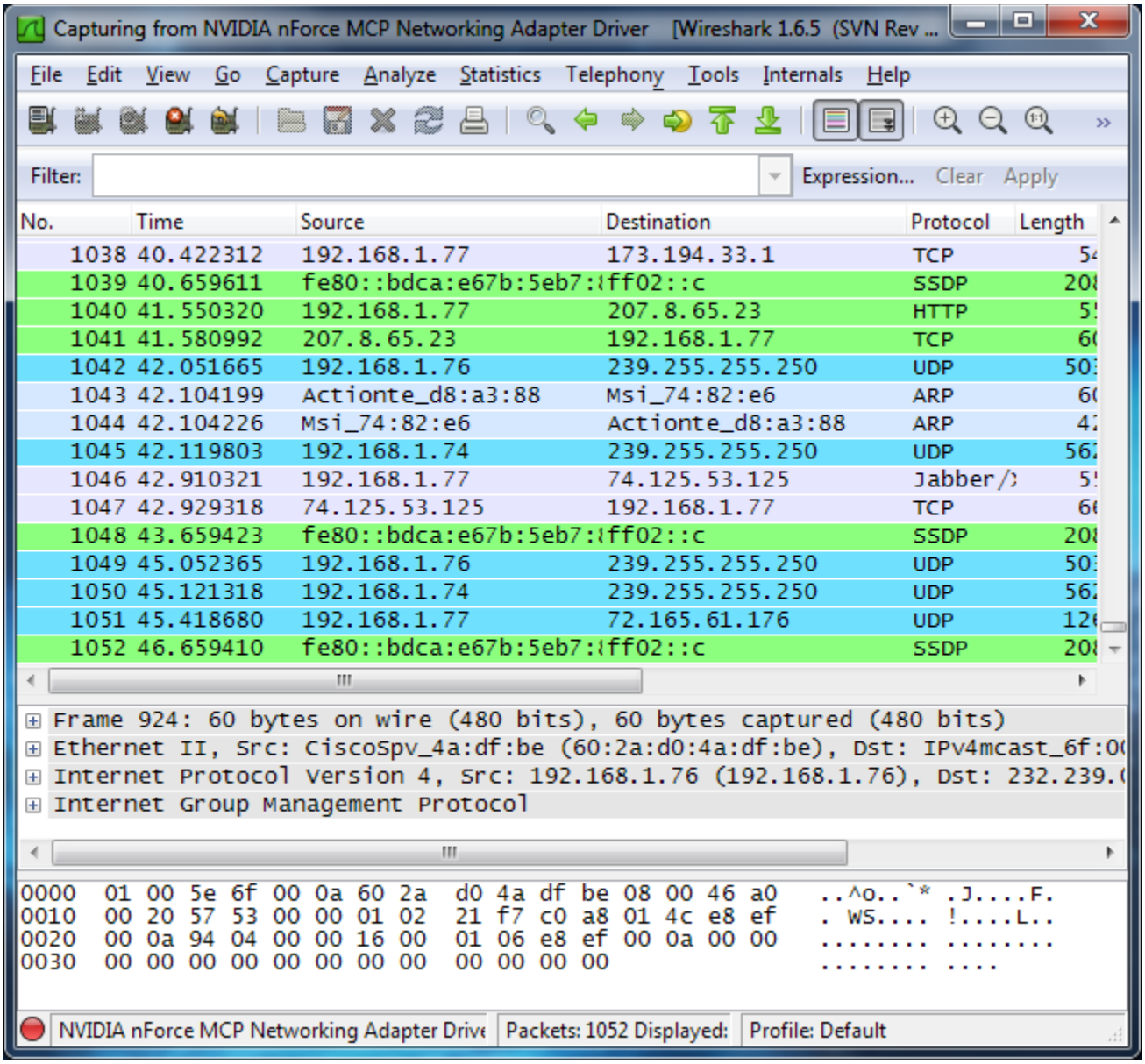


Figure 3.21

Click the stop capture button near the top left corner of the window when you want to stop capturing traffic.

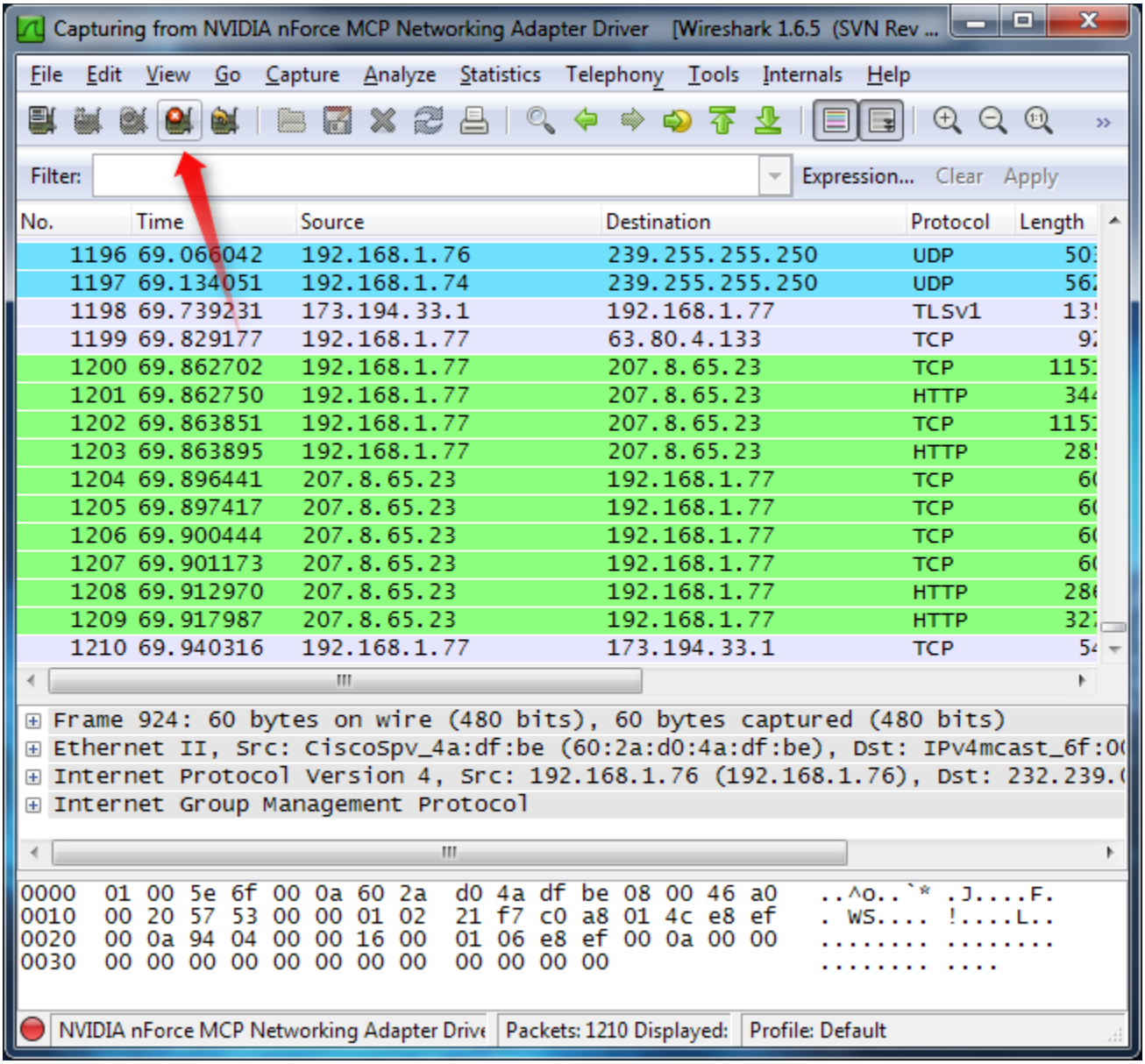


Figure 3.22

Color Coding

You'll probably see packets highlighted in green, blue, and black. Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.

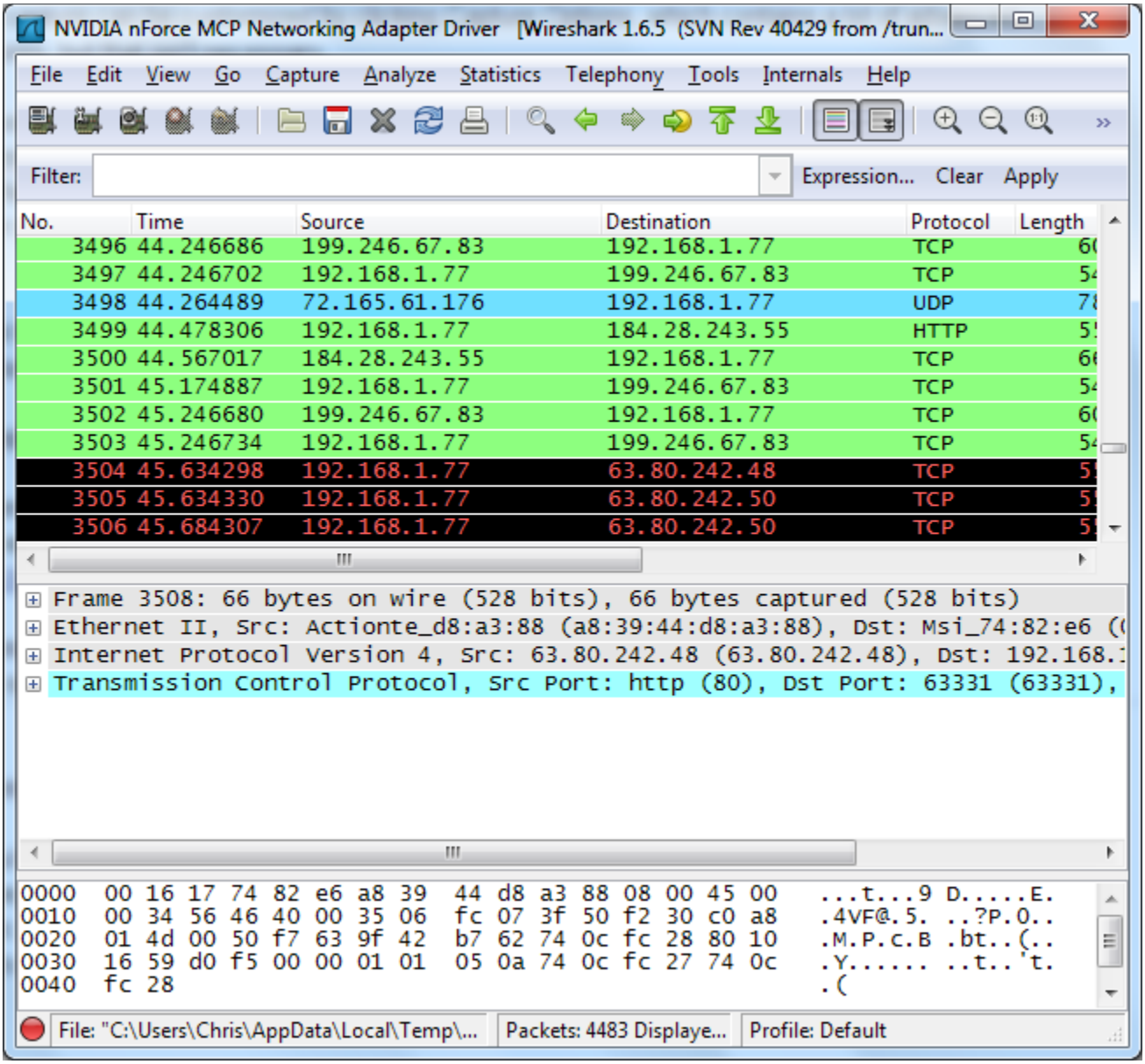


Figure 3.23

Sample Captures

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered. The wiki contains a page of sample capture files that you can load and inspect.

Opening a capture file is easy; just click Open on the main screen and browse for a file. You can also save your own captures in Wireshark and open them later.

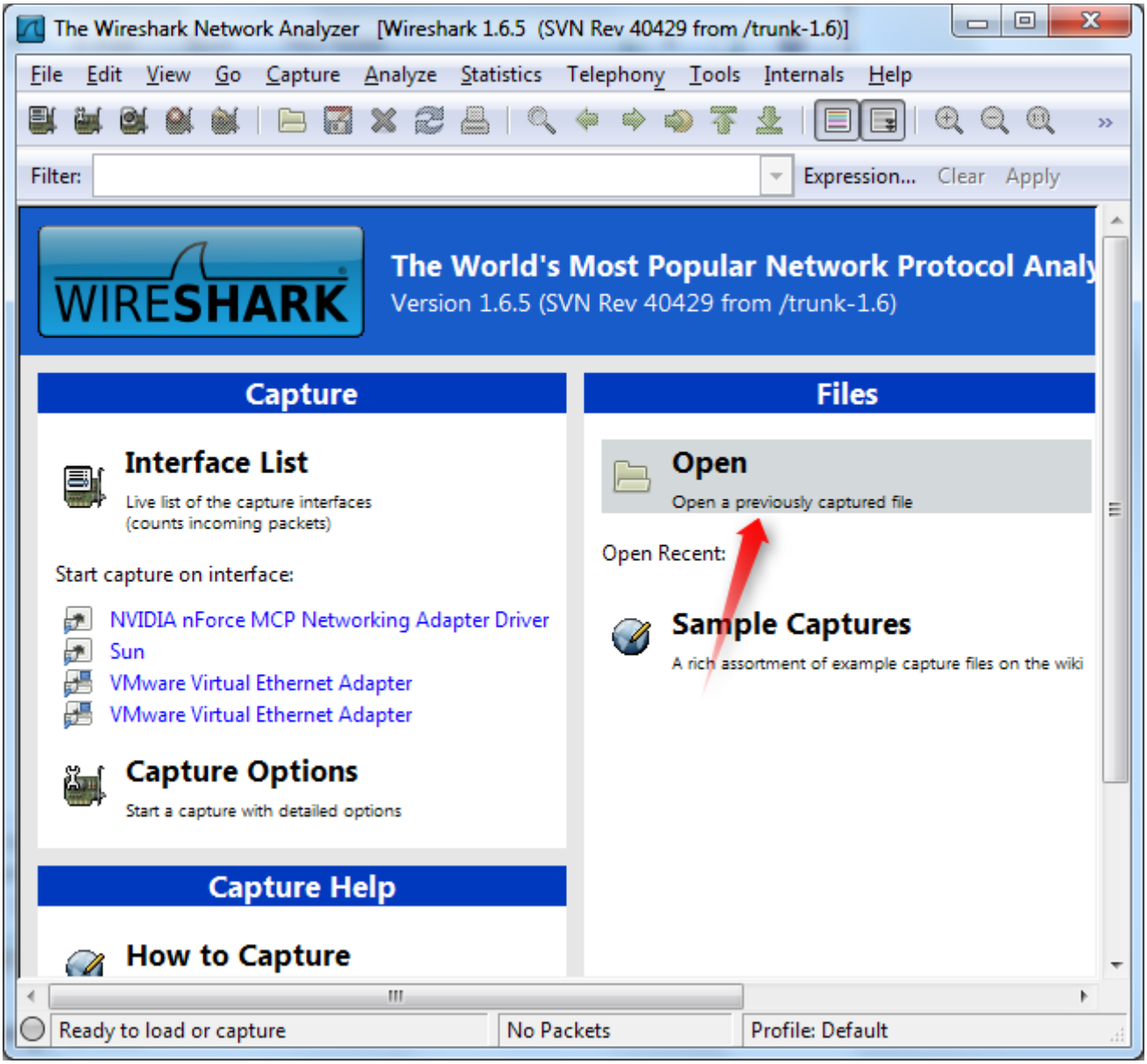


Figure 3.24

Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

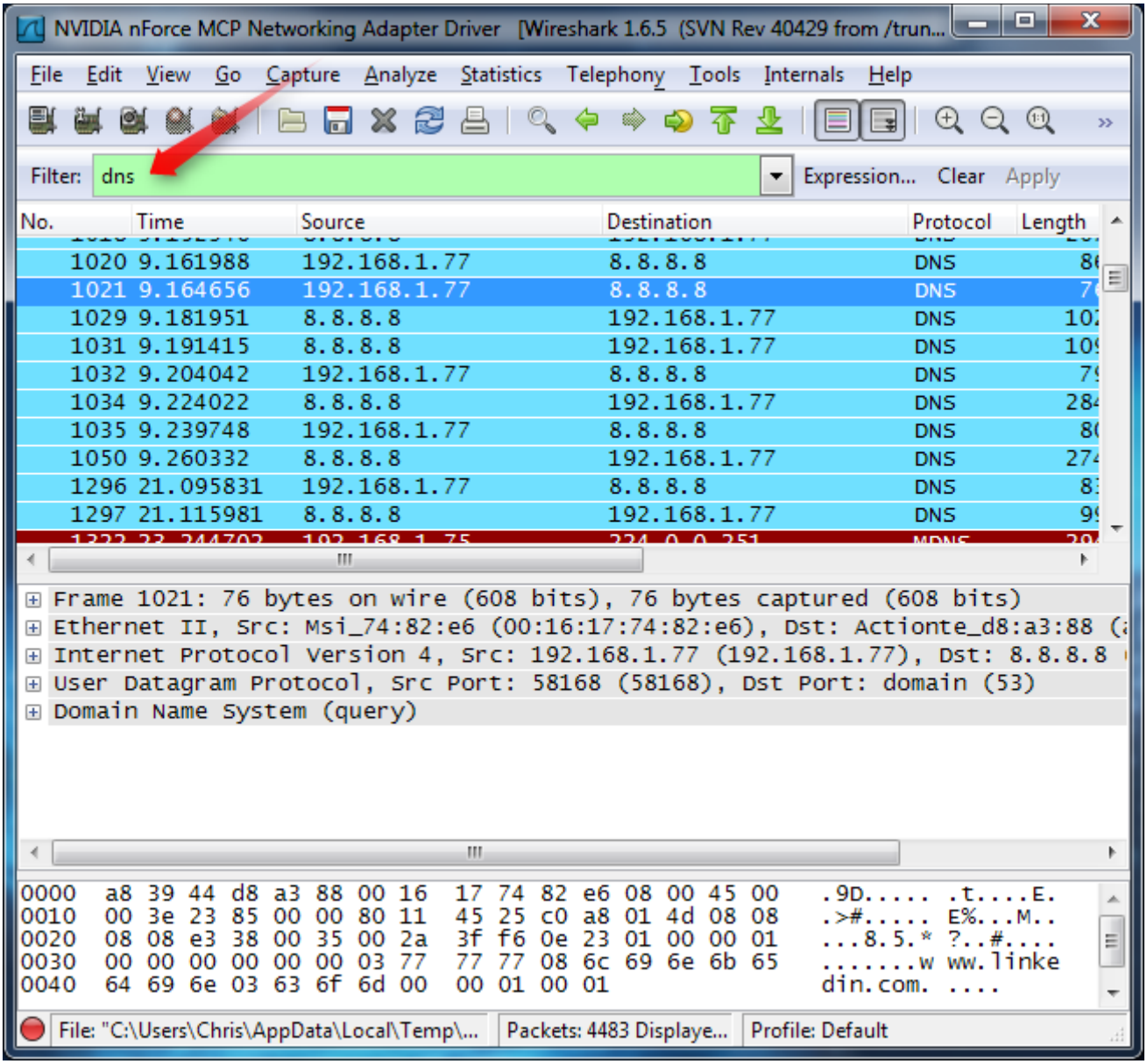

NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trun...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: dns
Expression... Clear Apply
No. Time Source Destination Protocol Length
1020 9.161988 192.168.1.77 8.8.8.8 DNS
1021 9.164656 192.168.1.77 8.8.8.8 DNS
1029 9.181951 8.8.8.8 192.168.1.77 DNS
1031 9.191415 8.8.8.8 192.168.1.77 DNS
1032 9.204042 192.168.1.77 8.8.8.8 DNS
1034 9.224022 8.8.8.8 192.168.1.77 DNS
1035 9.239748 192.168.1.77 8.8.8.8 DNS
1050 9.260332 8.8.8.8 192.168.1.77 DNS
1296 21.095831 192.168.1.77 8.8.8.8 DNS
1297 21.115981 8.8.8.8 192.168.1.77 DNS
Frame 1021: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
Ethernet II, Src: Msi_74:82:e6 (00:16:17:74:82:e6), Dst: Actionte_d8:a3:88
Internet Protocol Version 4, Src: 192.168.1.77 (192.168.1.77), Dst: 8.8.8.8
User Datagram Protocol, Src Port: 58168 (58168), Dst Port: domain (53)
Domain Name System (query)
0000 a8 39 44 d8 a3 88 00 16 17 74 82 e6 08 00 45 00 .9D..... .t....E.
0010 00 3e 23 85 00 00 80 11 45 25 c0 a8 01 4d 08 08 .>#..... E%...M..
0020 08 08 e3 38 00 35 00 2a 3f f6 0e 23 01 00 00 01 ...8.5.* ?..#....
0030 00 00 00 00 00 00 03 77 77 77 08 6c 69 6e 6b 65 ....w ww.linke
0040 64 69 6e 03 63 6f 6d 00 00 01 00 01 din.com. ....
File: "C:\Users\Chris\AppData\Local\Temp\...
Packets: 4483 Displaye...
Profile: Default

Figure 3.25

Another interesting thing you can do is right-click a packet and select Follow TCP Stream.

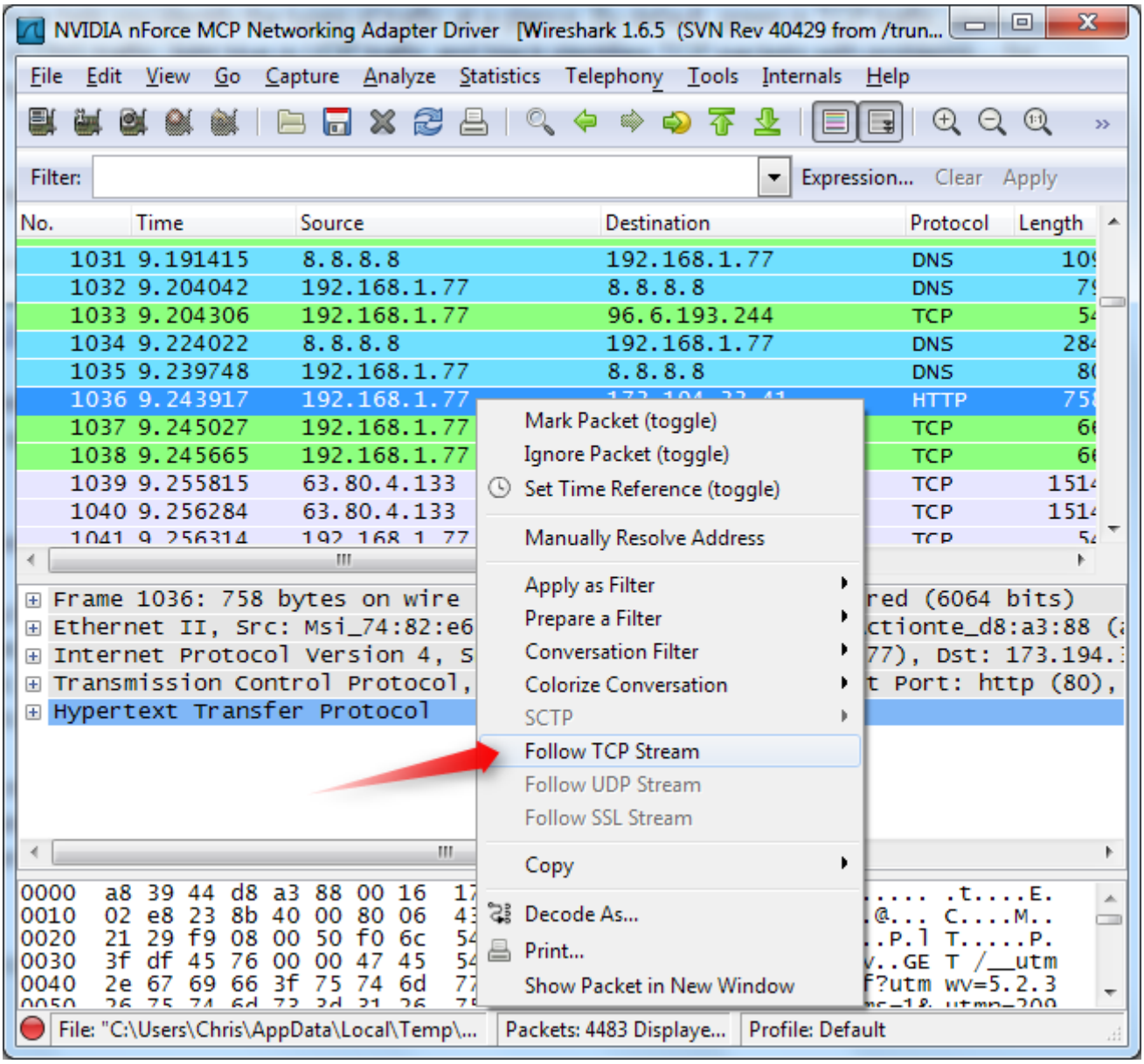


Figure 3.26

You'll see the full conversation between the client and the server.

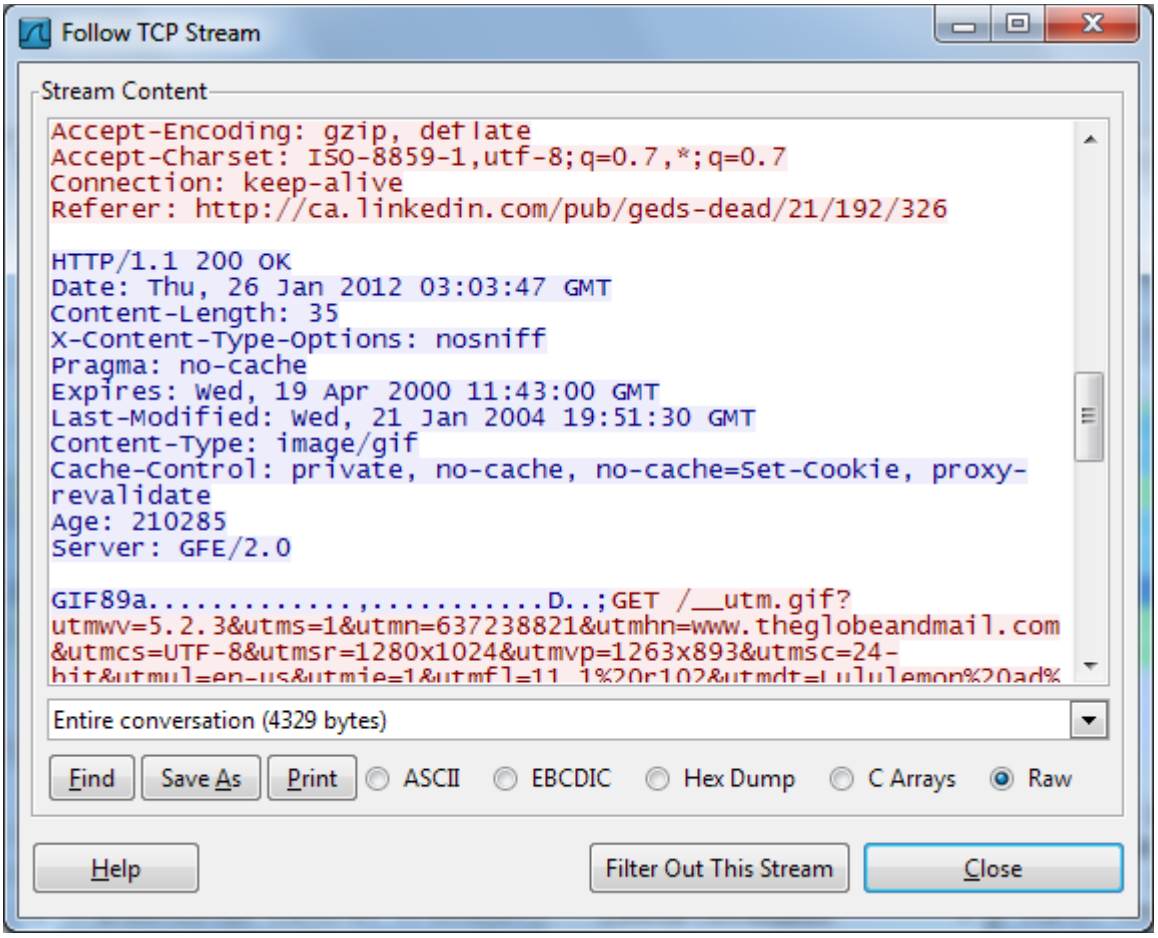


Figure 3.27

Close the window and you'll find a filter has been applied automatically — Wireshark is showing you the packets that make up the conversation.

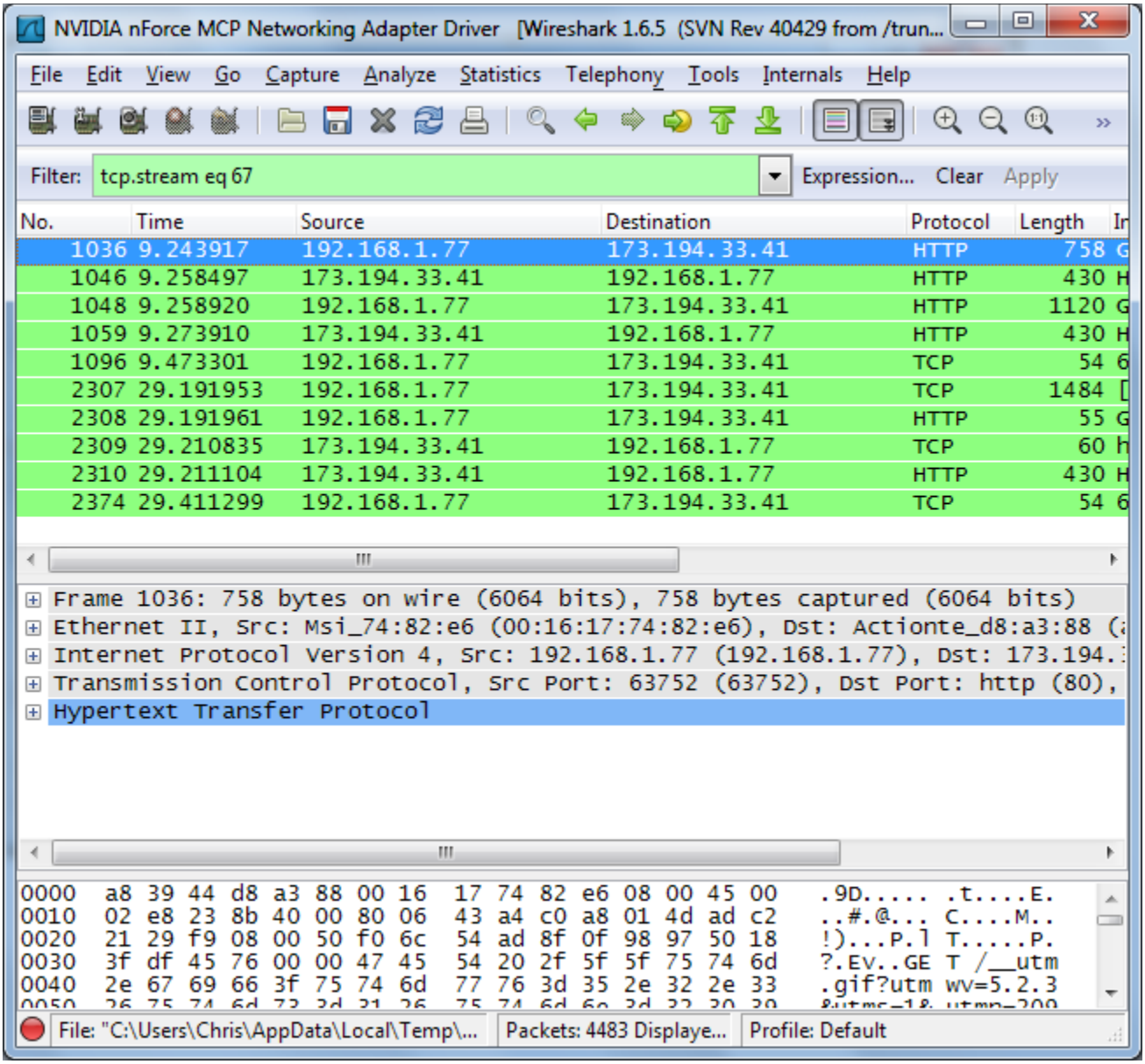


Figure 3.28

Inspecting Packets

Click a packet to select it and you can dig down to view its details.

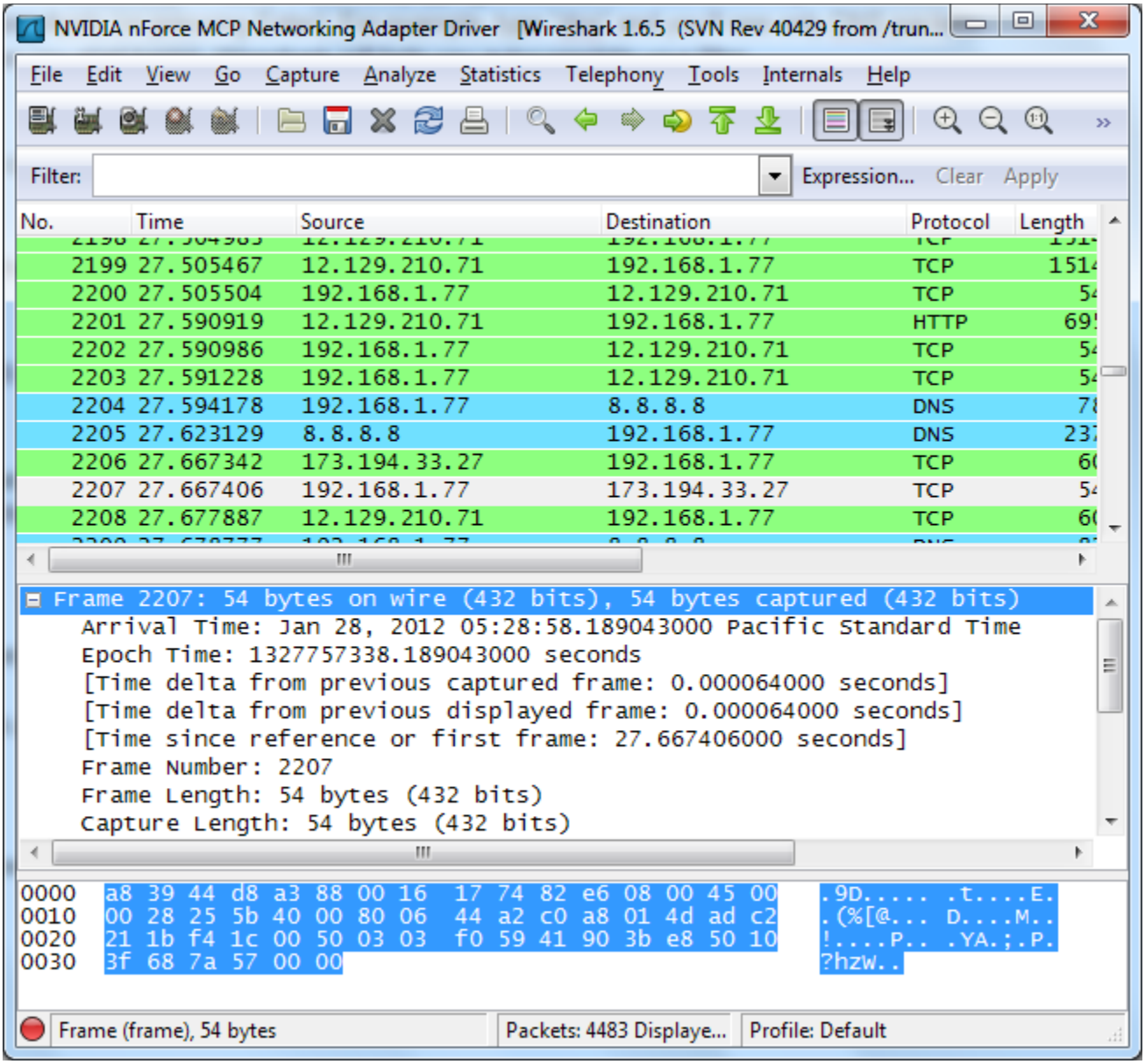


Figure 3.29

You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.

Critical Analysis / Conclusion

Lab Assessment		
Pre Lab	**/5**	**/25**
Performance	**/5**	
Results	**/5**	
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		

Lab 4:Static Route Configuration

Pre Lab

Every TCP/IP packet, whether it's a client request or a server response, contains a source IP address and a destination IP address. Routing is the process of determining the network path a packet should take from the source IP to the destination IP. Most routing is managed automatically by properly configured routing software and hardware.

The process of auto-configuring routes is called *dynamic routing*, and is accomplished through the exchange of routing information packets among systems on the network. The Routing Information Protocol (RIP) and Border Gateway Protocol (BGP) are examples of Internet routing protocols.

In a typical network, each system has at least one interface card installed and sends packets whose destination IPs are on the network segment to which the interface card is bound directly to the destination system.

Each system is also configured with a *default gateway*; the system sends all packets with destination IPs that are *not* directly connected to the local system to the default gateway for forwarding to the final destination IP. The assumption is that the default gateway will know how to reach any network that the system itself cannot reach through one of its own interfaces.

Routing errors can occur for many reasons, but the principal reasons we are concerned with here involve situations where a packet cannot be routed to its destination IP address because the network segment that contains the destination IP is not bound to any of the directly connected network interfaces and the default gateway does not know how to reach the destination. In such cases, we need to define a path through which the packet can be delivered to its destination.

We do this by manually defining *static routes* on one or more systems. Depending on your network configuration and application traffic flow, you may require static routes on Equalizer; on one or more servers, clients, and routers; or, on a combination of these systems.

Basic Routing Behaviour

When a packet leaves any TCP/IP-based system, the next system to send the packet is chosen according to the packet's destination address, an IP address. A packet contains both link layer address and a network layer address. The network layer address is set to the IP address of the final destination host (except in source routing, which is not usually used in Equalizer configurations). How the link layer address is set depends on the route chosen from the routing table.

If the final destination host of the packet is directly connected to the sending system (that is, there are no intelligent routing devices -- such as Equalizer -- between the systems), this is called a *direct*

route and the packet's link layer and network layer addresses will be associated in the ARP table. The packet is forwarded directly to its final destination IP based on the entry in the ARP table.

If the IP destination is not directly connected (an indirect route), then IP routing table uses the best route via a "gateway" to forward the packet to, this IP address is sometimes called the *next hop gateway* in the route for the packet. The next hop gateway may be directly connected to the final destination IP, or it may have to forward the packet to yet another gateway. In this manner, the packet hops from gateway to gateway until it arrives at the final destination IP.

The process that the TCP/IP subsystem uses to determine the link and network layer addresses to specify in an outgoing packet is summarized below. In each step, the *first* entry in the table that matches the destination IP of the packet is used (and any subsequent matching entries are ignored):

1. If the destination IP is bound to one of the system's network interfaces (or is a broadcast packet), the packet is passed to the appropriate protocol handler on the local system for processing.

2.If the destination IP is on one of the subnets bound to one of the system's network interfaces, the packet is sent to the appropriate gateway (indirect route) or network interface (direct route), depending on the flags in the router table

entry. The router table entry chosen in this case may be a *host route*, specifying a single system, or a *network route*,

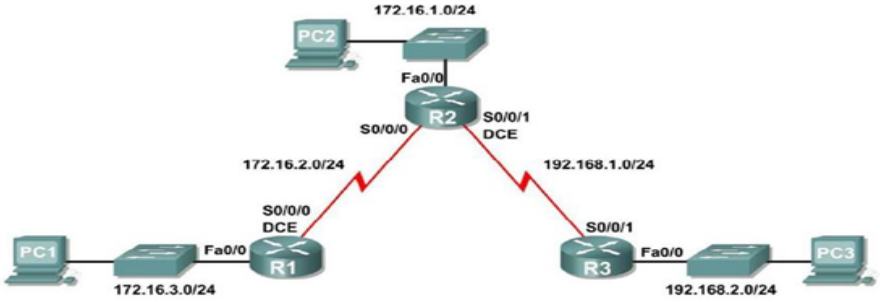
specifying multiple systems.

3.If the routing table contains a *default* entry, send the packet to the default gateway IP address.

4. If all the above fail, the packet is dropped.

Depending on the implementation of the network subsystem and the application being used, an error may be returned indicating that the destination IP or network is unreachable. If no error is returned, usually some sort of timeout occurs that drops the connection attempt.

Static Route configuration



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.3.1	255.255.255.0	N/A
	S0/0/0	172.16.2.1	255.255.255.0	N/A
R2	Fa0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.2.2	255.255.255.0	N/A
	S0/0/1	192.168.1.2	255.255.255.0	N/A
R3	FA0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/1	192.168.1.1	255.255.255.0	N/A
PC1	NIC	172.16.3.10	255.255.255.0	172.16.3.1
PC2	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC3	NIC	192.168.2.10	255.255.255.0	192.168.2.1

Figure 4. 1

Pre Lab Tasks

Task 1:

Cable the network according to the Topology Diagram.

Task 2:

Perform basic Router configuration on the routers, enter the global configuration mode and configure the basic global configuration commands:

- Host Name
- No ip domain
- Enable secret
- Banner

Task 3:

Configure the console and virtual line passwords on each router.

- Password

- Login

Learning Objectives

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

- Cable a network according to the Topology Diagram.
- Erase the startup configuration and reload a router to the default state.
- Perform basic configuration tasks on a router.
- Interpret `debug ip routing` output.
- Configure and activate Serial and Ethernet interfaces.
- Test connectivity.
- Gather information to discover causes for lack of connectivity between devices.
- Configure a static route using an intermediate address.
- Configure a static route using an exit interface.
- Compare a static route with intermediate address to a static route with exit interface.
- Configure a default static route.
- Configure a summary static route.
- Document the network implementation.

Scenario

In this lab activity, you will create a network that is similar to the one shown in the Topology Diagram. Begin by cabling the network as shown in the Topology Diagram. You will then perform the initial router configurations required for connectivity. Use the IP addresses that are provided in the Addressing Table to apply an addressing scheme to the network devices. After completing the basic configuration, test connectivity between the devices on the network. First test the connections between directly connected devices, and then test connectivity between devices that are not directly connected. Static routes must be configured on the routers for end-to-end communication to take place between the network hosts. You will configure the static routes that are needed to allow communication between the hosts. View the routing table after each static route is added to observe how the routing table has changed.

Task 1: Cable, Erase, and Reload the Routers.

Step 1: Cable a network that is similar to the one in the Topology Diagram.

Step 2: Clear the configuration on each router.

Clear the configuration on each of the routers using the `erase startup-config` command and then `reload` the routers. Answer **no** if asked to save changes.

Task 2: Perform Basic Router Configuration.

Note: If you have difficulty with any of the commands in this task, see **Lab 1.5.1: Cabling a Network and Basic Router Configuration**.

Step 1: Use global configuration commands.

On the routers, enter global configuration mode and configure the basic global configuration commands including:

- `hostname`
- `no ip domain-lookup`
- `enable secret`

Step 2: Configure the console and virtual terminal line passwords on each of the routers.

- **password**
- **login**

Step 3: Add the `logging synchronous` command to the console and virtual terminal lines.

This command is very helpful in both lab and production environments and uses the following syntax:

```
Router(config-line)#logging synchronous
```

To synchronize unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or virtual terminal line, we can use the **`logging synchronous`** line configuration command. In other words, the **`logging synchronous`** command prevents IOS messages delivered to the console or Telnet lines from interrupting your keyboard input.

For example, you may have already experienced something similar to the following example:

Note: *Do not* configure R1 interfaces yet.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 172.16.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#descri
*Mar  1 01:16:08.212: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
*Mar  1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to upption
R1(config-if)#
```

The IOS sends unsolicited messages to the console when you activate an interface with the **`no shutdown`** command. However, the next command you enter (in this case, **`description`**) is interrupted by these messages. The **`logging synchronous`** command solves this problem by copying the command entered up to that point down to the next router prompt.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 172.16.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#description
*Mar  1 01:28:04.242: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
*Mar  1 01:28:05.243: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
R1(config-if)#description  <-- Keyboard input copied after message
```

R1 is shown here as an example. Add **`logging synchronous`** to the console and virtual terminal lines on all routers.

```
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#line vty 0 4
R1(config-line)#logging synchronous
```

Step 4: Add the `exec-timeout` command to the console and virtual terminal lines.

To set the interval that the EXEC command interpreter waits until user input is detected, we can use the **`exec-timeout`** line configuration command. If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session. This command allows you to control the amount of time a console or virtual terminal line can be idle before the session is terminated. The syntax follows:

```
Router(config-line)#exec-timeout minutes [seconds]
```

Syntax description:

minutes—Integer that specifies the number of minutes.

seconds—(Optional) Additional time intervals in seconds.

In a lab environment, you can specify "no timeout" by entering the **`exec-timeout 0 0`** command. This command is very helpful because the default timeout for lines is 10 minutes. However, for security purposes, you would not normally set lines to "no timeout" in a production environment.

R1 is shown here as an example.

Add **`exec-timeout 0 0`** to console and virtual terminal lines on all routers.

```
R1(config)#line console 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#line vty 0 4
R1(config-line)#exec-timeout 0 0
```

Task 3: Interpreting Debug Output.

Note: If you already configured IP addressing on R1, please remove all `interface` commands now before proceeding. R1, R2 and R3 should be configured through the end of Task 2 without any interface configurations.

Step 1: On R1 from privileged EXEC mode, enter the `debug ip routing` command.

```
R1#debug ip routing
IP routing debugging is on
```

The **`debug ip routing`** command shows when routes are added, modified, and deleted from the routing table. For example, every time you successfully configure and activate an interface, Cisco IOS adds a route to the routing table. We can verify this by observing output from the **`debug ip routing`** command.

Step 2: Enter interface configuration mode for R1's LAN interface.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fastethernet 0/0
```

Configure the IP address as specified in the Topology Diagram.

```
R1(config-if)#ip address 172.16.3.1 255.255.255.0
is_up: 0 state: 6 sub state: 1 line: 1 has_route: False
```

As soon as you press the **Enter** key, Cisco IOS debug output informs you that there is now a route, but its state is `False`. In other words, the route has not yet been added to the routing table. Why did this occur and what steps should be taken to ensure that the route is entered into the routing table?

_____

_____

LAB Task

Step 3: Enter the command necessary to install the route in the routing table.

If you are not sure what the correct command is, review the discussion in "Examining Router Interfaces" which is discussed in Section 2.2, "Router Configuration Review."

After you enter the correct command, you should see debug output. Your output may be slightly different from the example below.

```
is_up: 1 state: 4 sub state: 1 line: 1 has_route: False
RT: add 172.16.3.0/24 via 0.0.0.0, connected metric [0/0]
RT: NET-RED 172.16.3.0/24
RT: NET-RED queued, Queue size 1
RT: interface FastEthernet0/0 added to routing table
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
is_up: 1 state: 4 sub state: 1 line: 1 has_route: True
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, chan
ged state to up
is_up: 1 state: 4 sub state: 1 line: 1 has_route: True
is_up: 1 state: 4 sub state: 1 line: 1 has_route: True
```

The new network you configured on the LAN interface is now added to the routing table, as shown in the highlighted output.

If you do not see the route added to the routing table, the interface did not come up. Use the following systematic process to troubleshoot your connection:

1. Check your physical connections to the LAN interface.
   Is the correct interface attached? _____
   Your router may have more than one LAN interface. Did you connect the correct LAN interface? _____
   An interface will not come up unless it detects a carrier detect signal at the Physical layer from another device. Is the interface connected to another device such as a hub, switch, or PC? _____
2. Check link lights. Are all link lights blinking? _____
3. Check the cabling. Are the correct cables connected to the devices? _____
4. Has the interface been activated or enabled? _____

If you can answer **yes** to all the proceeding questions, the interface should come up.

Step 4: Enter the command to verify that the new route is now in the routing table.

Your output should look similar to the following output. There should now be one route in the table for R1. What command did you use?

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

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.3.0 is directly connected, FastEthernet0/0
```

Step 5: Enter interface configuration mode for R1's WAN interface connected to R2.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface Serial 0/0/0
```

Configure the IP address as specified in the Topology Diagram.

```
R1(config-if)#ip address 172.16.2.1 255.255.255.0
is_up: 0 state: 0 sub state: 1 line: 0 has_route: False
```

As soon as you press the **Enter** key, Cisco IOS debug output informs you that there is now a route, but its state is `False`. Because R1 is the DCE side of our lab environment, we must specify how fast the bits will be clocked between R1 and R2.

Step 6: Enter the `clock rate` command on R1.

You can specify any valid clocking speed. Use the ? to find the valid rates. Here, we used 64000 bps.

```
R1(config-if)#clock rate 64000
is_up: 0 state: 0 sub state: 1 line: 0 has_route: False
```

Some IOS versions display the output shown above every 30 seconds. Why is the state of the route still `False`? What step must you now take to make sure that the interface is fully configured?

_____

Step 7: Enter the command necessary to ensure that the interface is fully configured.

If you are not sure what the correct command is, review the discussion in "Examining Router Interfaces," which is discussed in Section 2.2, "Router Configuration Review."

```
R1(config-if)#_____________________________
```

After you enter the correct command, you should see debug output similar to the following example:

```
is_up: 0 state: 0 sub state: 1 line: 0 has_route: False
%LINK-3-UPDOWN: Interface Serial0/0/0, changed state to down
```

Unlike configuring the LAN interface, fully configuring the WAN interface does not always guarantee that the route will be entered in the routing table, even if your cable connections are correct. The other side of the WAN link must also be configured.

Step 8: If possible, establish a separate terminal session by consoling into R2 from another workstation. Doing this allows you to observe the debug output on R1 when you make changes on R2. You can also turn on **`debug ip routing`** on R2.

```
R2#debug ip routing
IP routing debugging is on
```

Enter interface configuration mode for R2's WAN interface connected to R1.

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface serial 0/0/0
```

Configure the IP address as specified in the Topology Diagram.

```
R2(config-if)#ip address 172.16.2.2 255.255.255.0
is_up: 0 state: 6 sub state: 1 line: 0
```

Step 9: Enter the command necessary to ensure that the interface is fully configured.

If you are not sure what the correct command is, review the discussion in "Examining Router Interfaces," which is discussed in Section 2.2, "Router Configuration Review."

```
R2(config-if)#_____________________________
```

After you enter the correct command, you should see debug output similar to the following example:

```
is_up: 0 state: 4 sub state: 1 line: 0
%LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
is_up: 1 state: 4 sub state: 1 line: 0
RT: add 172.16.2.0/24 via 0.0.0.0, connected metric [0/0]
RT: interface Serial0/0/0 added to routing table
is_up: 1 state: 4 sub state: 1 line: 0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
up
is_up: 1 state: 4 sub state: 1 line: 0
```

The new network that you configured on the WAN interface is now added to the routing table, as shown in the highlighted output.

If you do not see the route added to the routing table, the interface did not come up. Use the following systematic process to troubleshoot your connection:

1. Check your physical connections between the two WAN interfaces for R1 and R2.
   Is the correct interface attached? _____
   Your router has more than one WAN interface. Did you connect the correct WAN interface? _____
   An interface will not come up unless it detects a link beat at the Physical layer from another device. Is the interface connected to the other router's interface? _____
2. Check link lights. Are all link lights blinking? _____
3. Check the cabling. R1 must have the DCE side of the cable attached and R2 must have the DTE side of the cable attached. Are the correct cables connected to the routers? _____
4. Has the interface been activated or enabled? _____

If you can answer **yes** to all the proceeding questions, the interface should come up.

Step 10: Enter the command to verify that the new route is now in the routing table for R1 and R2.

Your output should look similar to the following output. There should now be two routes in the routing table for R1 and one route in the table for R2. What command did you use?

```
R1#
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 not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0

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

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
```

Step 11: Turn off debugging on both routers using either `no debug ip routing` or simply `undebug all`.

```
R1(config-if)#end
R1#no debug ip routing
IP routing debugging is off
```

Task 4: Finish Configuring Router Interfaces

Step 1: Configure Remaining R2 Interfaces

Finish configuring the remaining interfaces on R2 according to the Topology Diagram and Addressing Table.

Step 2: Configure R3 Interfaces

Console into R3 and configure the necessary interfaces according to the Topology Diagram and Addressing Table.

Task 5: Configure IP Addressing on the Host PCs.

Step 1: Configure the host PC1.

Configure the host PC1 with an IP address of 172.16.3.10/24 and a default gateway of 172.16.3.1.

Step 2: Configure the host PC2.

Configure the host PC2 with an IP address of 172.16.1.10/24 and a default gateway of 172.16.1.1.

Step 3: Configure the host PC3.

Configure the host PC3 with an IP address of 192.168.2.10/24 and a default gateway of 192.168.2.1.

Task 6: Test and Verify the Configurations.

Step 1: Test connectivity.

Test connectivity by pinging from each host to the default gateway that has been configured for that host

From the host PC1, is it possible to ping the default gateway? _____

From the host PC2, is it possible to ping the default gateway? _____

From the host PC3, is it possible to ping the default gateway? _____

If the answer is **no** for any of these questions, troubleshoot the configurations to find the error using the following systematic process:

1. Check the cabling.
   Are the PCs physically connected to the correct router? _____
   (Connection could be through a switch or directly)
   Are link lights blinking on all relevant ports? _____
2. Check the PC configurations. Do they match the Topology Diagram? _____
3. Check the router interfaces using the `show ip interface brief` command.
   Are all relevant interfaces **up** and **up**? _____

If your answer to all three steps is **yes**, you should be able to successfully ping the default gateway.

Step 2: Use the `ping` command to test connectivity between directly connected routers.

From the router R2, is it possible to ping R1 at 172.16.2.1? _____

From the router R2, is it possible to ping R3 at 192.168.1.1? _____

If the answer is **no** for any of these questions, troubleshoot the configurations to find the error using the following systematic process:

1. Check the cabling.
   Are the routers physically connected? _____
   Are link lights blinking on all relevant ports? _____
2. Check the router configurations.
   Do they match the Topology Diagram? _____
   Did you configure the **clock rate** command on the DCE side of the link? _____
3. Has the interface been activated or enabled? _____
4. Check the router interfaces using the **show ip interface brief** command.
   Are the interfaces **up** and **up**? _____

If your answer to all three steps is **yes**, you should be able to successfully ping from R2 to R1 and from R2 to R3.

Step 3: Use ping to check connectivity between devices that are not directly connected.

From the host PC3, is it possible to ping the host PC1? _____

From the host PC3, is it possible to ping the host PC2? _____

From the host PC2, is it possible to ping the host PC1? _____

From the router R1, is it possible to ping router R3? _____

These pings should all fail. Why?

_____

_____

_____

Task 7: Gather Information.

Step 1: Check status of interfaces.

Check the status of the interfaces on each router with the command **show ip interface brief**. The following output is for R2.

```
R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protoc
FastEthernet0/0        172.16.1.1      YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/0            172.16.2.2      YES manual up                    up
Serial0/0/1            192.168.1.2     YES manual up                    up
Vlan1                  unassigned      YES manual administratively down down
```

Are all of the relevant interfaces on each router activated (that is, in the **up** and **up** state)? _____

How many interfaces are activated on R1 and R3? _____

Why are there three activated interfaces on R2? _____

_____

Step 2: View the routing table information for all three routers.

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

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
```

What networks are present in the Topology Diagram but not in the routing table for R1?

_____

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

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
```

What networks are present in the Topology Diagram but not in the routing table for R2?

_____

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

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

What networks are present in the Topology Diagram but not in the routing table for R3?

_____

Why are all the networks not in the routing tables for each of the routers?

_____

_____

What can be added to the network so that devices that are not directly connected can ping each other?

_____

Task 8: Configure a Static Route Using a Next-Hop Address.

Step 1: To configure static routes with a next-hop specified, use the following syntax:

```
Router(config)# ip route network-address subnet-mask ip-address
```

- *network-address*—Destination network address of the remote network to be added to the routing table.
- *subnet-mask*—Subnet mask of the remote network to be added to the routing table. The subnet mask can be modified to summarize a group of networks.
- *ip-address*—Commonly referred to as the next-hop router's IP address.

On the R3 router, configure a static route to the 172.16.1.0 network using the Serial 0/0/1 interface of R2 as the next-hop address.

```
R3(config)#ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)#
```

Step 2: View the routing table to verify the new static route entry.

Notice that the route is coded with an **S**, which means that the route is a static route.

```
R3#_____

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
S       172.16.1.0 [1/0] via 192.168.1.2
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
R3#
```

With this route entered in the routing table, any packet that matches the first 24 left-most bits of 172.16.1.0/24 will be forwarded to the next-hop router at 192.168.1.2.

What interface will R3 use to forward packets to the 172.16.1.0/24 network? _____

Assume that the following packets have arrived at R3 with the indicated destination addresses. Will R3 discard the packet or forward the packet? If R3 forwards the packet, with what interface will R3 send the packet?

Packet	Destination IP	Discard or Forward?	Interface
1	172.16.2.1	_____	_____
2	172.16.1.10	_____	_____
3	192.168.1.2	_____	_____
4	172.16.3.10	_____	_____
5	192.16.2.10	_____	_____

Although R3 will forward packets to destinations for which there is a route, this does not mean that a packet will arrive safely at the final destination.

Step 3: Use `ping` to check connectivity between the host PC3 and the host PC2.

From the host PC3, is it possible to ping the host PC2? _____

These pings should fail. The pings will arrive at PC2 if you have configured and verified all devices through Task 7, "Gather Information." PC2 will send a ping reply back to PC3. However, the ping reply will be discarded at R2 because the R2 does not have a return route to the 192.168.2.0 network in the routing table.

Step 4: On the R2 router, configure a static route to reach the 192.168.2.0 network.

What is the next-hop address to which R2 would send a packet destined for the 192.168.2.0/24 network?

```
R2(config)#ip route 192.168.2.0 255.255.255.0 _____
R2(config)#
```

Step 5: View the routing table to verify the new static route entry.

Notice that the route is coded with an **S**, which means the route is a **static** route.

```
R2#

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 [1/0] via 192.168.1.1
R2#
```

Step 6: Use `ping` to check connectivity between the host PC3 and the host PC2.

From the host PC3, is it possible to ping the host PC2? _____

This ping should be successful.

Task 9: Configure a Static Route Using an Exit Interface.

To configure static routes with an exit interface specified, use the following syntax:

```
Router(config)# ip route network-address subnet-mask exit-interface
```

- *network-address*—Destination network address of the remote network to be added to the routing table.
- *subnet-mask*—Subnet mask of the remote network to be added to the routing table. The subnet mask can be modified to summarize a group of networks.
- *exit-interface*—Outgoing interface that would be used in forwarding packets to the destination network.

Step 1: On the R3 router, configure a static route.

On the R3 router, configure a static route to the 172.16.2.0 network using the Serial 0/0/1 interface of the R3 router as the exit interface.

```
R3(config)# ip route 172.16.2.0 255.255.255.0 Serial0/0/1
R3(config)#
```

Step 2: View the routing table to verify the new static route entry.

```
R3#_____________________________
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
S       172.16.1.0 [1/0] via 192.168.1.2
S       172.16.2.0 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
R3#
```

Use the **show running-config** command to verify the static routes that are currently configured on R3.

```
R3#show running-config
Building configuration...

<output omitted>
!
hostname R3
!
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.0
!
interface Serial0/0/0
 no ip address
 shutdown

!
interface Serial0/0/1
 ip address 192.168.1.1 255.255.255.0
!
ip route 172.16.1.0 255.255.255.0 192.168.1.2
ip route 172.16.2.0 255.255.255.0 Serial0/0/1
!
end
```

How would you remove either of these routes from the configuration?

_____

Step 3: On the R2 router, configure a static route.

On the R2 router, configure a static route to the 172.16.3.0 network using the Serial 0/0/0 interface of the R2 router as the exit interface.

```
R2(config)# ip route 172.16.3.0 255.255.255.0 Serial0/0/0
R2(config)#
```

Step 4: View the routing table to verify the new static route entry.

```
R2#_____________________________________

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate defau
       U - per-user static route, o - ODR

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 [1/0] via 192.168.1.1
R2#
```

At this point, R2 has a complete routing table with valid routes to all five networks shown in the Topology Diagram.

Does this mean that R2 can receive ping replies from all destinations shown in the Topology Diagram?

_____

Why or why not?

_____

_____

Step 5: Use `ping` to check connectivity between the host PC2 and PC1.

This ping should fail because the R1 router does not have a return route to the 172.16.1.0 network in the routing table.

Task 10: Configure a Default Static Route.

In the previous steps, you configured the router for specific destination routes. But could you do this for every route on the Internet? No. The router and you would be overwhelmed. To minimize the size of the routing tables, add a default static route. A router uses the default static route when there is not a better, more specific route to a destination.

Instead of filling the routing table of R1 with static routes, we could assume that R1 is a *stub router*. This means that R2 is the default gateway for R1. If R1 has packets to route that do not belong to any of R1 directly connected networks, R1 should send the packet to R2. However, we must explicitly configure R1 with a default route before it will send packets with unknown destinations to R2. Otherwise, R1 discards packets with unknown destinations.

To configure a default static route, use the following syntax:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 { ip-address | interface }
```

Step 1: Configure the R1 router with a default route.

Configure the R1 router with a default route using the interface option on Serial 0/0/0 of R1 as the next-hop interface.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
R1(config)#
```

Step 2: View the routing table to verify the new static route entry.

```
R1#_____________________________________
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate def
       U - per-user static route, o - ODR

Gateway of last resort is 172.16.2.2 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 172.16.2.2
R1#
```

Note that the R1 router now has a default route, the *gateway of last resort*, and will send all unknown traffic out Serial 0/0/0, which is connected to R2.

Step 3: Use `ping` to check connectivity between the host PC2 and PC1.

From the host PC2, is it possible to ping PC1? _____

This ping should be successful this time because the R1 router can return the packet using the default route.

From the host PC3, is it possible to ping the host PC1? _____

Is there a route to the 172.16.3.0 network in the routing table on the R3 router? _____

Task 11: Configure a Summary Static Route.

We could configure another static route on R3 for the 172.16.3.0 network. However, we already have two static routes to 172.16.2.0/24 and 172.16.1.0/24. Because these networks are so close together, we can summarize them into one route. Again, doing this helps reduce the size of routing tables, which makes the route lookup process more efficient.

Looking at the three networks at the binary level, we can a common boundary at the 22nd bit from the left.

```
172.16.1.0      10101100.00010000.00000001.00000000
172.16.2.0      10101100.00010000.00000010.00000000
172.16.3.0      10101100.00010000.00000011.00000000
```

The prefix portion will include 172.16.0.0, because this would be the prefix if we turned off all the bits to the right of the 22nd bit.

```
Prefix    172.16.0.0
```

To mask the first 22 left-most bits, we use a mask with 22 bits turned on from left to right:

```
Bit Mask 11111111.11111111.11111100.00000000
```

This mask, in dotted-decimal format, is...

```
Mask      255.255.252.0
```

Step 1: Configure the summary static route on the R3 router.

The network to be used in the summary route is 172.16.0.0/22.

```
R3(config)#ip route 172.16.0.0 255.255.252.0 192.168.1.2
```

Step 2: Verify that the summary route is installed in the routing table.

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

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S       172.16.0.0/22 [1/0] via 192.168.1.2
S       172.16.1.0/24 [1/0] via 192.168.1.2
S       172.16.2.0/24 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Configuring a summary route on R3 did not remove the static routes configured earlier because these routes are more specific routes. They both use **/24** mask, whereas the new summary will be using a **/22** mask. To reduce the size of the routing table, we can now remove the more specific **/24** routes.

Step 3: Remove static routes on R3.

Remove the two static routes that are currently configured on R3 by using the **no** form of the command.

```
R3(config)#no ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)#no ip route 172.16.2.0 255.255.255.0 Serial0/0/1
```

Step 4: Verify that the routes are no longer in the routing table.

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

Gateway of last resort is not set

     172.16.0.0/22 is subnetted, 1 subnets
S       172.16.0.0 [1/0] via 192.168.1.2
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

R3 now only has one route to any host belonging to networks 172.16.0.0/24, 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24. Traffic destined for these networks will be sent to R2 at 192.168.1.2.

Step 5: Use `ping` to check connectivity between the host PC3 and PC1.

From the host PC3, is it possible to ping the host PC1? _____

This ping should be successful this time because there is a route to the 172.16.3.0 network on the R3 router, and the R1 router can return the packet using the default route.

Task 12: Summary, Reflection, and Documentation

With the completion of this lab, you have:

- Configured your first network with a combination of static and default routing to provide full connectivity to all networks
- Observed how a route is installed in the routing table when you correctly configure and activate the interface
- Learned how to statically configure routes to destinations that are not directly connected
- Learned how to configure a default route that is used to forward packets to unknown destinations
- Learned how to summarize a group of networks into one static route to reduce the size of a routing table

Along the way, you have also probably encountered some problems either in your physical lab setup or in your configurations. Hopefully, you have learned to systematically troubleshoot such problems. At this point, record any comments or notes that may help you in future labs.

_____

_____

_____

_____

Finally, you should document your network implementation. On each router, capture the following command output to a text (.txt) file and save for future reference.

- `show running-config`
- `show ip route`
- `show ip interface brief`

If you need to review the procedures for capturing command output, see Lab 1.5.1.

Task 13: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Task 14: Challenge

In the following exercise, fill in the blanks to document the process as the ping travels from source to destination. If you need help with this exercise see Section 1.4, "Path Determination and Switching Function."

1. The ICMP process on PC3 formulates a ping request to PC2 and sends the request to the IP process.
2. The IP process on PC3 encapsulates the ping packet with a source IP address of _____ and destination IP address of _____.
3. PC3 then frames the packet with the source MAC address of (indicate device name) ___ _____ and the destination MAC address of (indicate device name) _____ _____.
4. Next, PC3 sends the frame out on the media as an encoded bit stream.
5. R3 receives the bit stream on its _____ interface. Because the destination MAC address matches the receiving interface's MAC address, R3 strips off the Ethernet header.

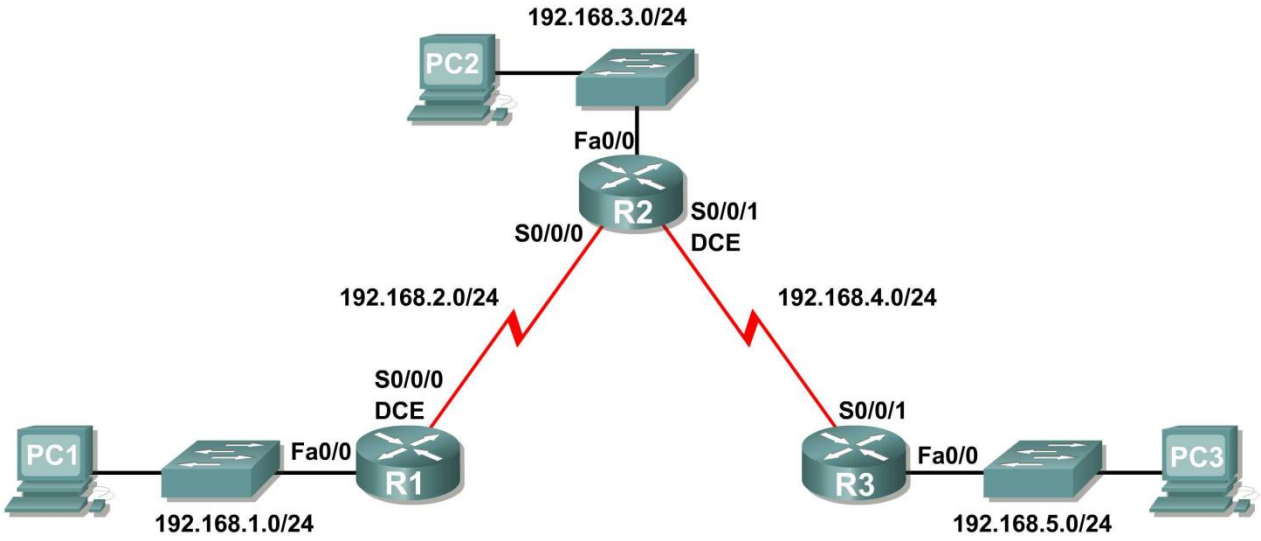
4. Next, PC3 sends the frame out on the media as an encoded bit stream.
5. R3 receives the bit stream on its _____ interface. Because the destination MAC address matches the receiving interface's MAC address, R3 strips off the Ethernet header.
6. R3 looks up the destination network address _____ in its routing table. This destination has a next-hop IP address of _____. The next-hop IP address is reachable out interface _____.
7. R3 encapsulates the packet in an HDLC frame and forwards the frame out the correct interface. (Because this is a point-to-point link, no address is needed. However, the address field in the HDLC packet contains the value 0x8F.)
8. R2 receives the frame on the _____ interface. Because the frame is HDLC, R2 strips off the header and looks up the network address _____ in its routing table. This destination address is directly connected to the _____ interface.
9. R2 encapsulates the ping request in a frame with the source MAC address of (indicated device name) _____ _____ and the destination MAC address of (indicate device name) _____.
10. R2 then sends the frame out on the media as an encoded bit stream.
11. PC2 receives the bit stream on its _____ interface. Because the destination MAC address matches the MAC address of PC2, PC2 strips off the Ethernet header.
12. The IP process on PC2 examines the _____ IP address to make sure that it matches its own IP address. Then PC2 passes the data to the ICMP process.
13. The ICMP process on PC2 formulates a ping reply to PC3 and sends the reply to the IP process.
14. The IP process on PC2 encapsulates the ping packet with a source IP address of _____ and destination IP address of _____.
15. PC2 then frames the packet with the source MAC address of (indicate device name) _____ and the destination MAC address of (indicate device name) _____.
16. PC2 then sends the frame out on the media as an encoded bit stream.
17. R2 receives the bit stream on its _____ interface. Because the destination MAC address matches the receiving interface's MAC address, R2 strips off the Ethernet header.
18. R2 looks up the destination network address _____ in its routing table. This destination has a next-hop IP address of _____. The next-hop IP address is reachable out interface _____.
19. R2 encapsulates the packet in an HDLC frame and forwards the frame out the correct interface. (Because this is a point-to-point link, no address is needed. However, the address field in the HDLC packet contains the value 0x8F.)
20. R3 receives the frame on the _____ interface. Because the frame is HDLC, R3 strips off the header and looks up the destination network address _____ in its routing table. This destination address is directly connected to the _____ interface.
21. R3 encapsulates the ping request in a frame with the source MAC address of (indicated device name) _____ and the destination MAC address of (indicate device name) _____.
22. R3 then sends the frame out on the media as an encoded bit stream.
23. PC3 receives the bit stream on its _____ interface. Because the destination MAC address matches the MAC address of PC3, PC3 strips off the Ethernet header.
24. The IP process on PC3 examines the _____ IP address to make sure that it matches its own IP address. Then PC3 passes the data to the ICMP process.
25. ICMP sends a "success" message to the requesting application.

Critical Analysis / Conclusion

Lab Assessment		
Pre Lab	**/5**	**/25**
Performance	**/5**	
Results	**/5**	
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		

LAB #05 RIP Configuration

Topology Diagram



Learning Objectives

- Cable a network according to the Topology Diagram.
- Erase the startup configuration and reload a router to the default state.
- Perform basic configuration tasks on a router.
- Configure and activate interfaces.
- Configure RIP routing on all routers.
- Verify RIP routing using **show**and **debug**commands.
- Reconfigure the network to make it contiguous.
- Observe automatic summarization at boundary router.
- Gather information about RIP processing using the **debug ip rip**command.
- Configure a static default route.
- Propagate default routes to RIP neighbors.
- Document the RIP configuration.

Scenarios

- Scenario A: Running RIPv1 on Classful Networks
- Scenario B: Running RIPv1 with Subnets and Between Classful Networks
- Scenario C: Running RIPv1 on a Stub Network.

Pre Lab

Perspective and Background of Dynamic Routing:

Dynamic routing protocols have evolved over several years to meet the demands of changing network requirements. Although many organizations have migrated to more recent routing protocols such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), many of the earlier routing protocols, such as Routing Information Protocol (RIP), are still in use today.

One of the earliest routing protocols was RIP. RIP has evolved into a newer version: RIPv2. However, the newer version of RIP still does not ***scale*** to larger network implementations. To address the needs of larger networks, two advanced routing protocols were developed: OSPF and Intermediate System–to–Intermediate System (IS-IS). Cisco developed Interior Gateway Routing Protocol (IGRP) and Enhanced IGRP (EIGRP). EIGRP also scales well in larger network implementations. Additionally, there was the need to interconnect different internetworks and provide routing among them. Border Gateway Protocol (BGP) is now used between Internet service providers (ISP) as well as between ISPs and their larger private clients to exchange routing information.

Role of Dynamic Routing Protocol

What exactly are dynamic routing protocols? Routing protocols are used to facilitate the exchange of routing information between routers. Routing protocols allow routers to dynamically learn information about remote networks and automatically add this information to their own routing tables.

Routing protocols determine the best path to each network, which is then added to the routing table. One of the primary benefits of using a dynamic routing protocol is that routers exchange routing information whenever there is a topology change. This exchange allows routers to automatically learn about new networks and also to find alternate paths if there is a link failure to a current network.

Compared to static routing, dynamic routing protocols require less administrative overhead. However, the expense of using dynamic routing protocols is dedicating part of a router's resources for protocol operation, including CPU time and network link bandwidth. Despite the benefits of dynamic routing, static routing still has its place. There are times when static routing is more appropriate and other times when dynamic routing is the better choice. More often than not, you will find a combination of both types of routing in any network that has a moderate level of complexity.

Purpose of Dynamic Routing Protocols

A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the routing protocol's choice of best paths. The purpose of a routing protocol includes

- Discovering remote networks
- Maintaining up-to-date routing information

■ Choosing the best path to destination networks
■ Having the ability to find a new best path if the current path is no longer available

The components of a routing protocol are as follows:
■ **Data structures:** Some routing protocols use tables or databases for their operations. This information is kept in RAM.

■ **Algorithm:** An ***algorithm*** is a finite list of steps used in accomplishing a task. Routing protocols use algorithms for processing routing information and for best-path determination.
■ **Routing protocol messages:** Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and do other tasks to learn and maintain accurate information about the network

Dynamic Routing Protocol Operation
All routing protocols have the same purpose: to learn about remote networks and to quickly adapt whenever there is a change in the topology. The method that a routing protocol uses to accomplish this depends on the algorithm it uses and the operational characteristics of that protocol. The operations of a dynamic routing protocol vary depending on the type of routing protocol and the specific operations of that routing protocol. The specific operations of RIP, EIGRP, and OSPF are examined in later chapters. In general, the operations of a dynamic routing protocol can be described as follows:

a) The router sends and receives routing messages on its interfaces.
b) The router shares routing messages and routing information with other routers that are
c) using the same routing protocol.
d) Routers exchange routing information to learn about remote networks.
e) When a router detects a topology change, the routing protocol can advertise this change
f) to other routers.

Classifying Dynamic Routing Protocols
Routing protocols can be classified into different groups according to their characteristics:
■ IGP or EGP
■ Distance vector or link-state
■ Classful or classless
The sections that follow discuss these classification schemes in more detail.

IGP and EGP

An ***autonomous system*** (AS)—otherwise known as a ***routing domain***—is a collection of routers under a common administration. Typical examples are a company's internal network and an ISP's

network. Because the Internet is based on the autonomous system concept, two types of routing protocols are required: interior and exterior routing protocols. These protocols are

■ ***Interior gateway protocols (IGP)*:** Used for intra-autonomous system routing, that is, routing inside an autonomous system

■ ***Exterior gateway protocols (EGP)*:** Used for inter-autonomous system routing, that is, routing between autonomous systems.

Distance Vector and Link State Routing

Distance vector means that routes are advertised as ***vectors*** of distance and direction. Distance is defined in terms of a metric such as hop count, and direction is simply the nexthop router or exit interface. Distance vector protocols typically use the Bellman-Ford algorithm for the best-path route determination. In contrast to distance vector routing protocol operation, a router configured with a ***linkstate*** routing protocol can create a "complete view," or topology, of the network by gathering information from all the other routers. Think of using a link-state routing protocol as having a complete map of the network topology. The signposts along the way from source to destination are not necessary, because all link-state routers are using an identical "map" of the network. A ***link-state router*** uses the link-state information to create a topology map and to select the best path to all destination networks in the topology. With some distance vector routing protocols, routers send periodic updates of their routing information to their neighbors. Link-state routing protocols do not use periodic updates. After the network has ***converged***, a link-state update is only sent when there is a change in the topology.

Classful and Classless Routing Protocols

Classful routing protocols do not send subnet mask information in routing updates. The first routing protocols, such as RIP, were classful. This was at a time when network addresses were allocated based on classes: Class A, B, or C. A routing protocol did not need to include the subnet mask in the routing update because the network mask could be determined based on the first octet of the network address. Classless routing protocols include the subnet mask with the network address in routing updates. Today's networks are no longer allocated based on classes, and the subnet mask cannot be determined by the value of the first octet. Classless routing protocols are required in most networks today because of their support for VLSM, discontiguous networks, and other features.

Convergence, Metric and Administrative distance

The process of bringing all routing tables to a state of consistency is called convergence. Convergence is when all the routers in the same routing domain or area have complete and accurate information about the network.

Metrics are used by routing protocols to determine the best path or shortest path to reach a destination network. Different routing protocols can use different metrics. Typically, a lower metric means a better path. Five hops to reach a network is better than ten hops. Routers sometimes learn about multiple routes to the same network from both static routes and dynamic routing protocols. When a Cisco router learns about a destination network from more than one

routing source, it uses the administrative distance value to determine which source to use. Each dynamic routing protocol has a unique administrative value, along with static routes and directly connected networks. The lower the administrative value, the more preferred the route source. A directly connected network is always the preferred source, followed by static routes and then various dynamic routing protocols.

Routing Information Protocol (RIP)

RIP is a standardized Distance Vector protocol, designed for use on smaller networks. RIP was one of the first true Distance Vector routing protocols, and is supported on a wide variety of systems. RIP adheres to the following Distance Vector characteristics:

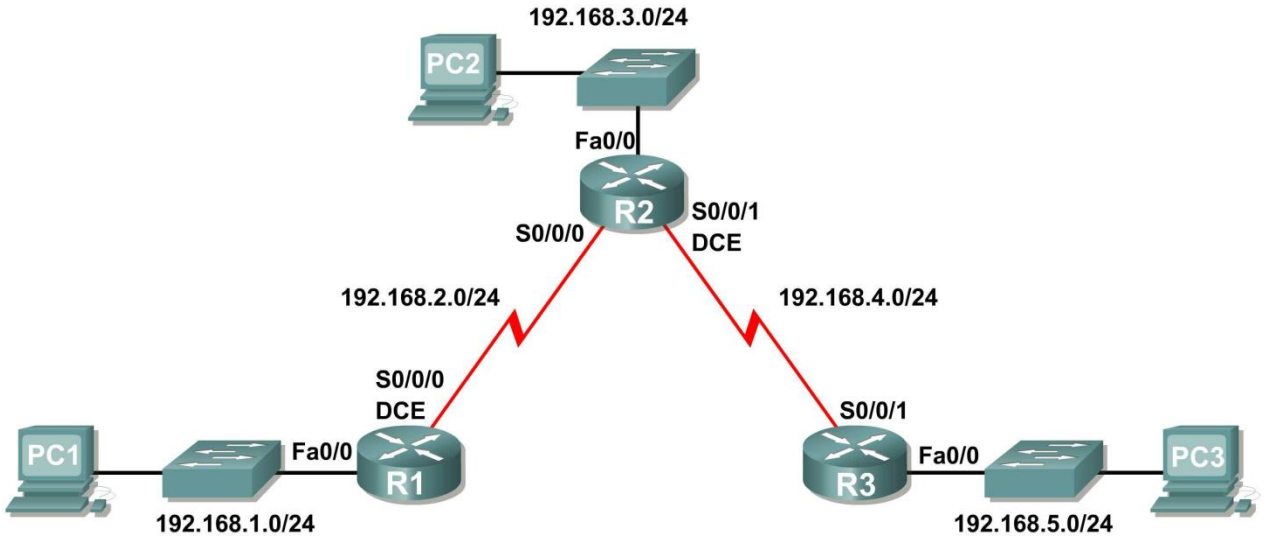
i. RIP sends out periodic routing updates (every **30 seconds**)
ii. RIP sends out the full routing table every periodic update
iii. 3.RIP uses a form of distance as its metric (in this case, **hopcount**)
iv. RIP uses the Bellman-Ford Distance Vector algorithm to determine the best "path" to a particular destination

PRE LAB Questions

Q.1: What are the differences between a distance vector and a link-state routing protocol? What kind of routing protocol is RIP?
Q.2: What is metric and its parameters?
Q.3: What is the purpose of administrative distance?
Q.2: How do RIP routers to exchange routing information?
Q.3: What is the maximum number of routes that can be sent in a RIP update?
Q.4: What is VLSM? Does RIP support it? Justify your answer.
Q.5: What metric does RIP use?
Q.6: What is difference between RIPv1 and RIPv2?

Scenario A: Running RIPv1 on Classful Networks

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/0**	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	**Fa0/0**	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
	S0/0/1	192.168.4.2	255.255.255.0	N/A
R3	**Fa0/0**	192.168.5.1	255.255.255.0	N/A
	S0/0/1	192.168.4.1	255.255.255.0	N/A
PC1	**NIC**	192.168.1.10	255.255.255.0	192.168.1.1
PC2	**NIC**	192.168.3.10	255.255.255.0	192.168.3.1
PC3	**NIC**	192.168.5.10	255.255.255.0	192.168.5.1

Pre Lab Task 1: Prepare the Network.

Step 1: Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations.

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

1. Configure the router hostname.
2. Disable DNS lookup.
3. Configure an EXEC mode password.
4. Configure a message-of-the-day banner.
5. Configure a password for console connections.
6. Configure a password for VTY connections.

Task 3: Configure and Activate Serial and Ethernet Addresses.

Step 1: Configure interfaces on R1, R2, and R3.

Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the table under the
Topology Diagram.

Step 2: Verify IP addressing and interfaces.

Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 3: Configure Ethernet interfaces of PC1, PC2, and PC3.

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from the table under the Topology Diagram.

Step 4: Test the PC configuration by pinging the default gateway from the PC.

Pre Lab Task

Task 4: Configure RIP.

Step 1: Enable dynamic routing.

To enable a dynamic routing protocol, enter global configuration mode and use the **router** command. Enter **router ?** at the global configuration prompt to a see a list of available routing protocols on your
router.

To enable RIP, enter the command **router rip** in global configuration mode.

```
R1(config)#router rip
R1(config-router)#
```

Step 2: Enter classful network addresses.

Once you are in routing configuration mode, enter the classful network address for each directly connected network, using the **network** command.

```
R1(config-router)#network 192.168.1.0

R1(config-router)#network 192.168.2.0
R1(config-router)
```

The **network** command:

- Enables RIP on all interfaces that belong to this network. These interfaces will now both send and receive RIP updates.
- Advertises this network in RIP routing updates sent to other routers every 30 seconds.

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

R1(config-router)#**end**
%SYS-5-CONFIG_I: Configured from console by console
R1#**copy run start**

Step 3: Configure RIP on the R2 router using the router ripand networkcommands.

R2(config)#**router rip**
R2(config-router)#**network 192.168.2.0**
R2(config-router)#**network 192.168.3.0**
R2(config-router)#**network 192.168.4.0**
R2(config-router)#**end**
%SYS-5-CONFIG_I: Configured from console by console
R2#**copy run start**

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Step 4: Configure RIP on the R3 router using the router ripand networkcommands.

R3(config)#**router rip**
R3(config-router)#**network 192.168.4.0**
R3(config-router)#**network 192.168.5.0**
R3(config-router)#**end**
%SYS-5-CONFIG_I: Configured from console by console
R3# **copy run start**

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Task 5: Verify RIP Routing.

Step 1: Use the show ip route command to verify that each router has all of the networks in the topology entered in the routing table.

Routes learned through RIP are coded with an **R** in the routing table. If the tables are not converged as shown here, troubleshoot your configuration. Did you verify that the configured interfaces are active? Did you configure RIP correctly? Return to Task 3 and Task 4 to review the steps necessary to achieve convergence.

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

Gateway of last resort is not set

```
C       192.168.1.0/24 is directly connected, FastEthernet0/0
C       192.168.2.0/24 is directly connected, Serial0/0/0
R       192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:04, Serial0/0/0
R       192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:04, Serial0/0/0
R       192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:04, Serial0/0/0
R1#
```

R2#**show ip route**

<Output omitted>

```
R       192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:22, Serial0/0/0
C       192.168.2.0/24 is directly connected, Serial0/0/0
C       192.168.3.0/24 is directly connected, FastEthernet0/0
C       192.168.4.0/24 is directly connected, Serial0/0/1
R       192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:23, Serial0/0/1
R2#
```

R3#**show ip route**

<Output omitted>

```
R       192.168.1.0/24 [120/2] via 192.168.4.2, 00:00:18, Serial0/0/1
R       192.168.2.0/24 [120/1] via 192.168.4.2, 00:00:18, Serial0/0/1
R       192.168.3.0/24 [120/1] via 192.168.4.2, 00:00:18, Serial0/0/1
C       192.168.4.0/24 is directly connected, Serial0/0/1
C       192.168.5.0/24 is directly connected, FastEthernet0/0
R3#
```

Step 2: Use the show ip protocolscommand to view information about the routing processes.

The **show ip protocols** command can be used to view information about the routing processes that are occurring on the router. This output can be used to verify most RIP parameters to confirm that:

- RIP routing is configured
- The correct interfaces send and receive RIP updates
- The router advertises the correct networks
- RIP neighbors are sending updates

R1#**show ip protocols**

```
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 16 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface              Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0        1     2 1
  Serial0/0/0            1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
```

```
        192.168.1.0
        192.168.2.0
Passive Interface(s):
Routing Information Sources:
        Gateway         Distance      Last Update
        192.168.2.2           120
Distance: (default is 120)
R1#
```

R1 is indeed configured with RIP. R1 is sending and receiving RIP updates on FastEthernet0/0 and Serial0/0/0. R1 is advertising networks 192.168.1.0 and 192.168.2.0. R1 has one routing information source. R2 is sending R1 updates.

Step 3: Use the debug ip ripcommand to view the RIP messages being sent and received.

Rip updates are sent every 30 seconds so you may have to wait for debug information to be displayed.

```
R1#debug ip rip
R1#RIP: received v1 update from 192.168.2.2 on Serial0/0/0
        192.168.3.0 in 1 hops
        192.168.4.0 in 1 hops
        192.168.5.0 in 2 hops
RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (192.168.1.1)
RIP: build update entries
        network 192.168.2.0 metric 1
        network 192.168.3.0 metric 2
        network 192.168.4.0 metric 2
        network 192.168.5.0 metric 3
RIP: sending v1 update to 255.255.255.255 via Serial0/0/0 (192.168.2.1) RIP: build
update entries
        network 192.168.1.0 metric 1
```

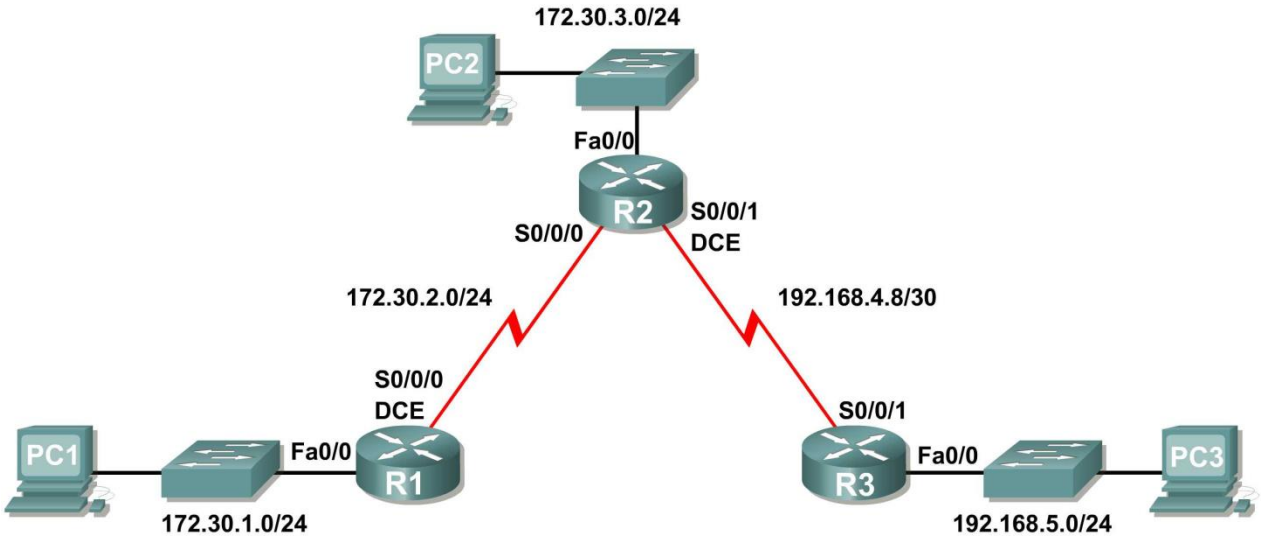
The debug output shows that R1 receives an update from R2. Notice how this update includes all the networks that R1 does not already have in its routing table. Because the FastEthernet0/0 interface belongs to the 192.168.1.0 network configured under RIP, R1 builds an update to send out that interface. The update includes all networks known to R1 except the network of the interface. Finally, R1 builds an update to send to R2. Because of split horizon, R1 only includes the 192.168.1.0 network in the update.

Step 4: Discontinue the debug output with the undebug all command.

```
R1#undebug all
All possible debugging has been turned off
```

Scenario B: Running RIPv1 with Subnets and Between Classful Networks

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/0**	172.30.1.1	255.255.255.0	N/A
	S0/0/0	172.30.2.1	255.255.255.0	N/A
R2	**Fa0/0**	172.30.3.1	255.255.255.0	N/A
	S0/0/0	172.30.2.2	255.255.255.0	N/A
	S0/0/1	192.168.4.9	255.255.255.252	N/A
R3	**Fa0/0**	192.168.5.1	255.255.255.0	N/A
	S0/0/1	192.168.4.10	255.255.255.252	N/A
PC1	**NIC**	172.30.1.10	255.255.255.0	172.30.1.1
PC2	**NIC**	172.30.3.10	255.255.255.0	172.30.3.1
PC3	**NIC**	192.168.5.10	255.255.255.0	192.168.5.1

Task 1: Make Changes between Scenario A and Scenario B

Step 1: Change the IP addressing on the interfaces as shown in the Topology Diagram and the Addressing Table.

Sometimes when changing the IP address on a serial interface, you may need to reset that interface by using the **shutdown** command, waiting for the LINK-5-CHANGED message, and then using the **no shutdown** command. This process will force the IOS to starting using the

new IP address.

R1(config)#**int s0/0/0**
R1(config-if)#**ip add 172.30.2.1 255.255.255.0**
R1(config-if)#**shutdown**

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
R1(config-if)#**no shutdown**

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Step 2: Verify that routers are active.

After reconfiguring all the interfaces on all three routers, verify that all necessary interfaces are active with the **show ip interface brief**command.

Step 3: Remove the RIP configurations from each router.

Although you can remove the old **network**commands with the **no**version of the command, it is more efficient to simply remove RIP and start over. Remove the RIP configurations from each router with the **no router rip**global configuration command. This will remove all the RIP configuration commands including the **network**commands.

R1(config)#**no router rip**

R2(config)#**no router rip**

R3(config)#**no router rip**

Task 2: Configure RIP

Step 1: Configure RIP routing on R1 as shown below.

R1(config)#**router rip**
R1(config-router)#**network 172.30.0.0**

Notice that only a single network statement is needed for R1. This statement includes both interfaces on different subnets of the 172.30.0.0 major network.

Step 2: Configure R1 to stop sending updates out the FastEthernet0/0 interface.

Sending updates out this interface wastes the bandwidth and processing resources of all devices on the LAN. In addition, advertising updates on a broadcast network is a security risk. RIP updates can be intercepted with packet sniffing software. Routing updates can be modified and sent back to the router, corrupting the router table with false metrics that misdirects traffic.

The **passive-interface fastethernet 0/0**command is used to disable sending RIPv1 updates out that interface. When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

```
R1(config-router)#passive-interface fastethernet 0/0
R1(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#copy run start
```

Step 3: Configure RIP routing on R2 as shown below.

```
R2(config)#router rip
R2(config-router)#network 172.30.0.0
R2(config-router)#network 192.168.4.0
R2(config-router)#passive-interface fastethernet 0/0
R2(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R2#copy run start
```

Again notice that only a single network statement is needed for the two subnets of 172.30.0.0. This statement includes both interfaces, on different subnets, of the 172.30.0.0 major network. The network for the WAN link between R2 and R3 is also configured.

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Step 4: Configure RIP routing on R3 as shown below.

```
R3(config)#router rip
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#passive-interface fastethernet 0/0
R3(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R3#copy run start
```

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Task 3: Verify RIPRouting

Step 1: Use the show ip routecommand to verify that each router has all of the networks in the topology in the routing table.

```
R1#show ip route

<Output omitted>

     172.30.0.0/24 is subnetted, 3 subnets
C       172.30.1.0 is directly connected, FastEthernet0/0
C       172.30.2.0 is directly connected, Serial0/0/0
R       172.30.3.0 [120/1] via 172.30.2.2, 00:00:22, Serial0/0/0
R    192.168.4.0/24 [120/1] via 172.30.2.2, 00:00:22, Serial0/0/0
R    192.168.5.0/24 [120/2] via 172.30.2.2, 00:00:22, Serial0/0/0
R1#
```

Note: RIPv1 is a classful routing protocol. Classful routing protocols do not send the subnet mask with network in routing updates. For example, 172.30.1.0 is sent by R2 to R1 without any subnet mask information.

R2#**show ip route**

<Output omitted>

```
     172.30.0.0/24 is subnetted, 3 subnets
R       172.30.1.0      [120/1] via 172.30.2.1, 00:00:04, Serial0/0/0
C       172.30.2.0      is directly connected, Serial0/0/0
C       172.30.3.0      is directly connected, FastEthernet0/0
     192.168.4.0/30      is subnetted, 1 subnets
C       192.168.4.8     is directly connected, Serial0/0/1
R    192.168.5.0/24     [120/1] via 192.168.4.10, 00:00:19, Serial0/0/1
R2#
```

R3#**show ip route**

<Output omitted>

```
R    172.30.0.0/16 [120/1] via 192.168.4.9, 00:00:22, Serial0/0/1
          192.168.4.0/30 is subnetted, 1 subnets
C       192.168.4.8 is directly connected, Serial0/0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
```

Step 2: Verify that all necessary interfaces are active.

If one or more routing tables does not have a converged routing table, first make sure that all necessary interfaces are active with **show ip interface brief**.

Then use **show ip protocols** to verify the RIP configuration. Notice in the output from this command that the FastEthernet0/0 interface is no longer listed under **Interface** but is now listed under a new section of the output: **Passive Interface(s)**.

```
R1#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 20 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface              Send  Recv  Triggered RIP  Key-chain
    Serial0/1/0            2     2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    172.30.0.0
    209.165.200.0
Passive Interface(s):
    FastEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    209.165.200.229         120      00:00:15
  Distance: (default is 120)
```

Step 3: View the RIP messages being sent and received.

To view the RIP messages being sent and received use the **debug ip rip**command. Notice that RIP updates are not sent out of the fa0/0 interface because of the **passive-interface fastethernet 0/0**command.

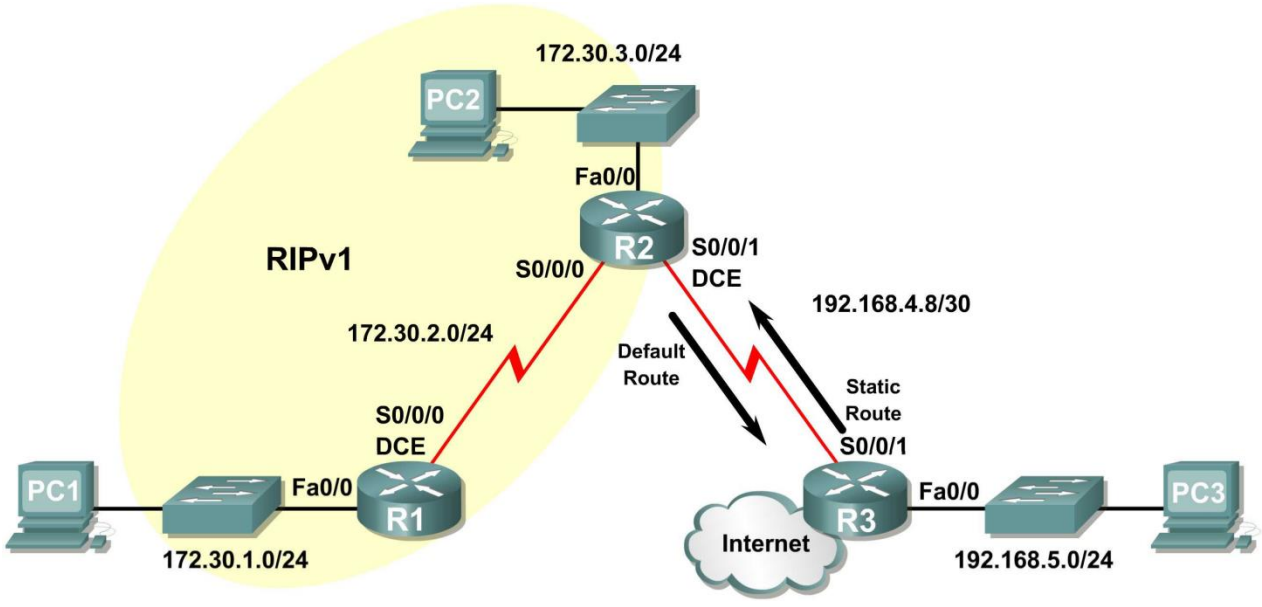
```
R1#debug ip rip
R1#RIP: sending          v1 update to 255.255.255.255 via Serial0/0/0 (172.30.2.1) RIP: build update entries
        network 172.30.1.0 metric 1
RIP: received v1 update from 172.30.2.2 on Serial0/0/0
        172.30.3.0 in 1 hops
```

Step 4: Discontinue the debug output with the undebug allcommand.

```
R1#undebug all
All possible debugging has been turned off
```

Scenario C: Running RIPv1 on a Stub Network

Topology Diagram



Background

In this scenario we will modify Scenario B to only run RIP between R1 and R2. Scenario C is a typical configuration for most companies connecting a stub network to a central headquarters router or an ISP. Typically, a company runs a dynamic routing protocol (RIPv1 in our case) within the local network but finds it unnecessary to run a dynamic routing protocol between the company's gateway router and the ISP. For example, colleges with multiple campuses often run a dynamic routing protocol between campuses but use default routing to the ISP for access to the Internet. In some cases, remote campuses may even use default routing to the main campus, choosing to use dynamic routing only locally.

To keep our example simple, for Scenario C, we left the addressing intact from Scenario B. Let's assume that R3 is the ISP for our Company XYZ, which consists of the R1 and R2 routers using the 172.30.0.0/16 major network, subnetted with a /24 mask. Company XYZ is a stub network, meaning that there is only one way in and one way out of the 172.30.0.0/16 network—in via R2 (the gateway router) and out via R3 (the ISP). It doesn't make sense for R2 to send

Lab#05 RIP Configuration

R3 RIP updates for the 172.30.0.0 network every 30 seconds, because R3 has no other way to get to 172.30.0.0 except through R2. It makes more sense for R3 to have a static route configured for the 172.30.0.0/16 network pointing to R2.

How about traffic from Company XYZ toward the Internet? It makes no sense for R3 to send over 120,000 summarized Internet routes to R2. All R2 needs to know is that if a packet is not destined for a host on the 172.30.0.0 network, then it should send the packet to the ISP, R3. This is the same for all other Company XYZ routers (only R1 in our case). They should send all traffic not destined for the 172.30.0.0 network to R2. R2 would then forward the traffic to R3.

Task 1: Make Changes between Scenario B and Scenario C.

Step 1: Remove network 192.168.4.0 from the RIP configuration for R2.

Remove network 192.168.4.0 from the RIP configuration for R2, because no updates will be sent between R2 and R3 and we don't want to advertise the 192.168.4.0 network to R1.

R2(config)#**router rip**
R2(config-router)#**no network 192.168.4.0**

Step 2: Completely remove RIP routing from R3.

R3(config)#**no router rip**

Task 2: Configure the Static Route on R3 for the 172.30.0.0/16 network.

Because R3 and R2 are not exchanging RIP updates, we need to configure a static route on R3 for the 172.30.0.0/16 network. This will send all 172.30.0.0/16 traffic to R2.

R3(config)#**ip route 172.30.0.0 255.255.252.0 serial0/0/1**

Task 3: Configure a Default Static Route on R2.

Step 1: Configure R2 to send default traffic to R3.

Configure a default static route on R2 that will send all default traffic—packets with destination IP addresses that do not match a specific route in the routing table—to R3.

R2(config)# **ip route 0.0.0.0 0.0.0.0 serial 0/0/1**

Step 2: Configure R2 to send default static route information to R1.

The **default-information originate**command is used to configure R2 to include the default static route with its RIP updates. Configure this command on R2 so that the default static route information is sent to R1.

R2(config)#**router rip**
R2(config-router)#**default-informationoriginate**
R2(config-router)#

Note: Sometimes it is necessary to clear the RIP routing process before the **default-information originate** command will work. First, try the command **clear ip route *** on both R1 and R2. This command will cause the routers to immediately flush routes in the routing table and request updates from each other. Sometimes this does not work with RIP. If the default route information is still not sent to R1, save the configuration on R1 and R2 and then reload both routers. Doing this will reset the hardware and both routers will restart the RIP routing process.

Task 4: Verify RIP Routing.

Step 1: Use the show ip routecommand to view the routing table on R2 and R1.

R2#**show ip route**
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external,
O - OSPF, IA - OSPF inter area

Lab#05 RIP Configuration

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

172.30.0.0/24 is subnetted, 3 subnets
C 172.30.2.0 is directly connected, Serial0/0/0
C 172.30.3.0 is directly connected, FastEthernet0/0
R 172.30.1.0 [120/1] via 172.30.2.1, 00:00:16, Serial0/0/0

```
        192.168.4.0/30 is subnetted, 1 subnets
C       192.168.4.8 is directly connected, Serial0/0/1
S*      0.0.0.0/0 is directly connected, Serial0/0/1
```

Notice that R2 now has a static route tagged as a **candidate default**.

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

Gateway of last resort is 172.30.2.2 to network 0.0.0.0

     172.30.0.0/24 is subnetted, 3 subnets
C       172.30.2.0 is directly connected, Serial0/0/0
R       172.30.3.0 [120/1] via 172.30.2.2, 00:00:05, Serial0/0/0
C       172.30.1.0 is directly connected, FastEthernet0/0
R*      0.0.0.0/0 [120/1] via 172.30.2.2, 00:00:19, Serial0/0/0
```

Notice that R1 now has a RIP route tagged as a **candidate default** route. The route is the "quad-zero" default route sent by R2. R1 will now send default traffic to the **Gateway of last resort** at 172.30.2.2, which is the IP address of R2.

Step 2: View the RIP updates that are sent and received on R1 with the debug ip ripcommand.

```
R1#debug ip rip
RIP protocol debugging is on
R1#RIP: sending      v1 update to 255.255.255.255 via Serial0/0/0 (172.30.2.1)
RIP: build update entries
     network 172.30.1.0 metric 1
RIP: received v1 update from 172.30.2.2 on Serial0/0/0
     0.0.0.0 in 1 hops
     172.30.3.0 in 1 hops
```

Notice that R1 is receiving the default route from R2.

Step 3: Discontinue the debug output with the undebug allcommand.

```
R1#undebug all
All possible debugging has been turned off
```

Step 4: Use the show ip routecommand to view the routing table on R3.

```
R3#show ip route

<Output omitted>

S       172.30.0.0/16 is directly connected, Serial0/0/1
        192.168.4.0/30 is subnetted, 1 subnets
C       192.168.4.8 is directly connected, Serial0/0/1
C       192.168.5.0/24 is directly connected, FastEthernet0/0
```

Notice that RIP is not being used on R3. The only route that is not directly connected is the static route.

Task 5: Document the Router Configurations

On each router, capture the following command output to a text file and save for future reference:

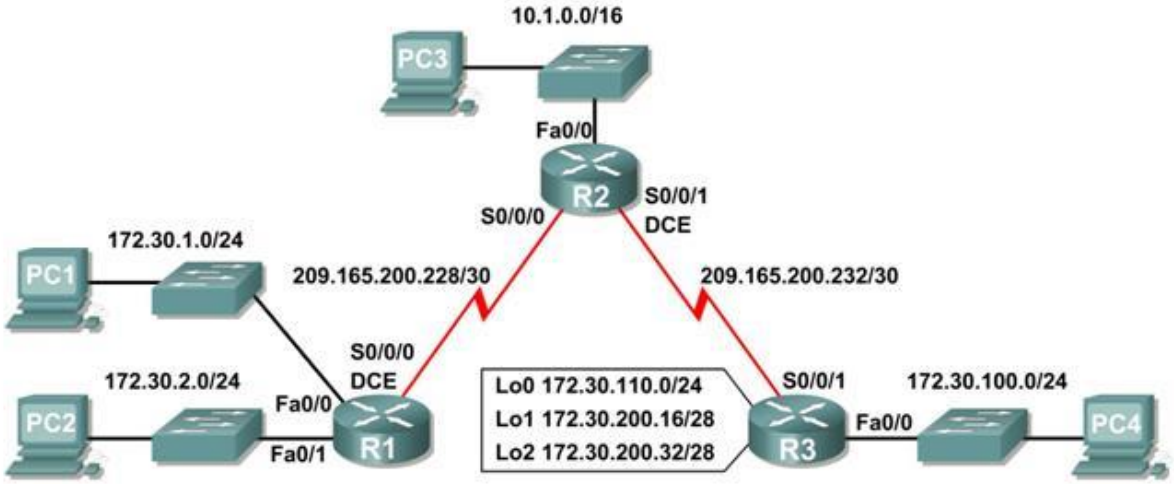
- Running configuration
- Routing table
- Interface summarization
- Output from **show ip protocols**

Task 6: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

RIPv2 Configuration Lab

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/0**	172.30.1.1	255.255.255.0	N/A
	Fa0/1	172.30.2.1	255.255.255.0	N/A
	S0/0/0	209.165.200.230	255.255.255.252	N/A
R2	**Fa0/0**	10.1.0.1	255.255.0.0	N/A
	S0/0/0	209.165.200.229	255.255.255.252	N/A
	S0/0/1	209.165.200.233	255.255.255.252	N/A
R3	**Fa0/0**	172.30.100.1	255.255.255.0	N/A
	S0/0/1	209.165.200.234	255.255.255.252	N/A
	Lo0	172.30.110.1	255.255.255.0	N/A
	Lo1	172.30.200.17	255.255.255.240	N/A

	Lo2	172.30.200.33	255.255.255.240	N/A
PC1	**NIC**	172.30.1.10	255.255.255.0	172.30.1.1
PC2	**NIC**	172.30.2.10	255.255.255.0	172.30.2.1
PC3	**NIC**	10.1.0.10	255.255.0.0	10.1.0.1
PC4	**NIC**	172.30.100.10	255.255.255.0	172.30.100.1

Learning Objectives

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

- Cable a network according to the Topology Diagram.
- Load provided scripts onto the routers.
- Examine the current status of the network.
- Configure RIPv2 on all routers.
- Examine the automatic summarization of routes.
- Examine routing updates with **debug ip rip**.
- Disable automatic summarization.
- Examine the routing tables. Verify
- network connectivity. Document the
- RIPv2 configuration.

Scenari

o

The network shown in the Topology Diagram contains a discontiguous network, 172.30.0.0. This network has been subnetted using VLSM. The 172.30.0.0 subnets are physically and logically divided by at least one other classful or major network, in this case the two serial networks 209.165.200.228/30 and 209.165.200.232/30. This can be an issue when the routing protocol used does not include enough information to distinguish the individual subnets. RIPv2 is a classless routing protocol that can be used to provide subnet mask information in the routing updates. This will allow VLSM subnet information to be propagated throughout the network.

Task 1: Cable, Erase, and Reload the Routers.

Step 1: Cable a network.

Cable a network that is similar to the one in the Topology Diagram.

Step 2: Clear the configuration on each router.

Clear the configuration on each of routers using the **erase startup-config**command and then **reload**the routers. Answer **no** if asked to save changes.

Task 2: Load Routers with the Supplied Scripts.

Step 1: Load the following script onto R1.

```
!
hostname R1
!
!
!
interface FastEthernet0/0
  ip address 172.30.1.1 255.255.255.0 duplex auto
   speed auto
```

```
        no shutdown
       !
       interface FastEthernet0/1
         ip address 172.30.2.1 255.255.255.0
         duplex auto

speed auto no shutdown
      !
      interface Serial0/0/0
        ip address 209.165.200.230 255.255.255.252
        clock rate 64000
        no shutdown
      !
      router rip
        passive-interface FastEthernet0/0
        passive-interface FastEthernet0/1
        network    172.30.0.0    network
        209.165.200.0
      !
      line con 0
      line vty 0 4
        login
      !
      end
```

Step 2: Load the following script onto R2.

```
      hostname R2
      !
      !
      !
      interface FastEthernet0/0
        ip address 10.1.0.1 255.255.0.0 duplex auto
        speed auto
        no shutdown
      !
      interface Serial0/0/0
        ip address 209.165.200.229 255.255.255.252
        no shutdown
      !
      interface Serial0/0/1
        ip address 209.165.200.233 255.255.255.252 clock rate 64000
        no shutdown
      !
      router rip
        passive-interface       FastEthernet0/0       network
        10.0.0.0
        network 209.165.200.0
      !
      line con 0
      line vty 0 4 login
      !
      end
```

Step 3: Load the following script onto R3.

```
hostname R3
!
!
!
interface FastEthernet0/0
  ip address 172.30.100.1 255.255.255.0
  duplex auto
  speed auto no
  shutdown
!
interface Serial0/0/1
  ip address 209.165.200.234 255.255.255.252 no shutdown
!
interface Loopback0
  ip address 172.30.110.1 255.255.255.0
!
interface Loopback1
  ip address 172.30.200.17 255.255.255.240
!
interface Loopback2
  ip address 172.30.200.33 255.255.255.240
!
router rip
  passive-interface FastEthernet0/0
  network 172.30.0.0
  network 209.165.200.0
!
line con 0 line vty
0 4
  login
!
end
```

Task 3: Examine the Current Status of the Network.

Step 1: Verify that both serial links are up.

The two serial links can quickly be verified using the **show ip interface brief**command on R2.

```
R2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.0.1        YES manual up                    up
FastEthernet0/1            unassigned      YES manual administratively down down Serial0/0/0
                           209.165.200.229 YES manual up                    up
Serial0/0/1                209.165.200.233 YES manual up                    up
Vlan1                      unassigned      YES manual administratively down down
```

Step 2: Check the connectivity from R2 to the hosts on the R1 and R3 LANs.

Note: For the 1841 router, you will need to disable IP CEF to obtain the correct output from the **ping** command. Although a discussion of IP CEF is beyond the scope of this course, you may disable IP CEF by using the following command in global configuration mode:

```
R2(config)#no ip cef
```

From the R2 router, how many ICMP messages are successful when pinging PC1?

From the R2 router, how many ICMP messages are successful when pinging PC4?

Step 3: Check the connectivity between the PCs. From the PC1, is it possible to ping PC2? _____ What is the success rate? _____

From the PC1, is it possible to ping PC3? _____

What is the success rate? _____

From the PC1, is it possible to ping PC4? _____

What is the success rate? _____

From the PC4, is it possible to ping PC2? _____

What is the success rate? _____

From the PC4, is it possible to ping PC3? _____

What is the success rate? _____

Step 4: View the routing table on R2.

Both the R1 and R3 are advertising routes to the 172.30.0.0/16 network; therefore, there are two entries for this network in the R2 routing table. The R2 routing table only shows the major classful network address of 172.30.0.0—it does not show any of the subnets for this network that are used on the LANs attached to R1 and R3. Because the routing metric is the same for both entries, the router alternates the routes that are used when forwarding packets that are destined for the 172.30.0.0/16 network.

R2#**show ip route**

Output omitted

```
      10.0.0.0/16 is subnetted, 1 subnets
C        10.1.0.0 is directly connected, FastEthernet0/0
R     172.30.0.0/16 [120/1] via 209.165.200.230, 00:00:24, Serial0/0/0
                            [120/1] via 209.165.200.234, 00:00:15, Serial0/0/1
      209.165.200.0/30 is subnetted, 2 subnets
C        209.165.200.228 is directly connected, Serial0/0/0
C        209.165.200.232 is directly connected, Serial0/0/1
```

Step 5: Examine the routing table on the R1 router.

Both R1 and R3 are configured with interfaces on a discontiguous network, 172.30.0.0. The 172.30.0.0 subnets are physically and logically divided by at least one other classful or major network—in this case, the two serial networks 209.165.200.228/30 and 209.165.200.232/30. Classful routing protocols like RIPv1 summarize networks at major network boundaries. Both R1 and R3 will be summarizing 172.30.0.0/24 subnets to 172.30.0.0/16. Because the route to 172.30.0.0/16 is directly connected, and because R1 does not have any specific routes for the 172.30.0.0 subnets on R3, packets destined for the R3 LANs will not be forwarded properly.

R1#**show ip route**

Output omitted

```
R       10.0.0.0/8 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
        172.30.0.0/24 is subnetted, 2 subnets
C           172.30.1.0 is directly connected, FastEthernet0/0
C           172.30.2.0 is directly connected, FastEthernet0/1
        209.165.200.0/30 is subnetted, 2 subnets
C           209.165.200.228 is directly connected, Serial0/0/0
R           209.165.200.232 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
```

Step 6: Examine the routing table on the R3 router.

R3 only shows its own subnets for 172.30.0.0 network: 172.30.100/24, 172.30.110/24, 172.30.200.16/28, and 172.30.200.32/28. R3 does not have any routes for the 172.30.0.0 subnets on R1.

R3#**show ip route**

Output omitted

```
R       10.0.0.0/8 [120/1] via 209.165.200.233, 00:00:19, Serial0/0/1
        172.30.0.0/16 is variably subnetted, 4 subnets, 2 masks
C           172.30.100.0/24 is directly connected, FastEthernet0/0
C           172.30.110.0/24 is directly connected, Loopback0
C           172.30.200.16/28 is directly connected, Loopback1
C           172.30.200.32/28 is directly connected, Loopback2
        209.165.200.0/30 is subnetted, 2 subnets
R           209.165.200.228 [120/1] via 209.165.200.233, 00:00:19, Serial0/0/1
C           209.165.200.232 is directly connected, Serial0/0/1
```

Step 7: Examine the RIPv1 packets that are being received by R2.

Use the **debug ip rip**command to display RIP routing updates.

R2 is receiving the route 172.30.0.0, with 1 hop, from both R1 and R3. Because these are equal cost metrics, both routes are added to the R2 routing table. Because RIPv1 is a classful routing protocol, no subnet mask information is sent in the update.

```
R2#debug ip rip
RIP protocol debugging is on
RIP: received v1 update from 209.165.200.234 on Serial0/0/1
     172.30.0.0 in 1 hops
RIP: received v1 update from 209.165.200.230 on Serial0/0/0
     172.30.0.0 in 1 hops
```

R2 is sending only the routes for the 10.0.0.0 LAN and the two serial connections to R1 and R3. R1 and R3 are not receiving any information about the 172.30.0.0 subnet routes.

```
RIP: sending v1 update to 255.255.255.255 via Serial0/0/1 (209.165.200.233)
RIP: build update entries network 10.0.0.0
     metric 1
     network 209.165.200.228 metric 1
RIP: sending v1 update to 255.255.255.255 via Serial0/0/0
(209.165.200.229)
```

```
RIP: build update entries network 10.0.0.0
        metric 1
             network 209.165.200.232 metric 1
```

When you are finished, turn off the debugging.

```
R2#undebug all
```

Task 4: Configure RIP Version 2.

Step 1: Use the version 2command to enable RIP version 2 on each of the routers.

```
R2(config)#router rip
R2(config-router)#version 2

R1(config)#router rip
R1(config-router)#version 2

R3(config)#router rip
R3(config-router)#version 2
```

RIPv2 messages include the subnet mask in a field in the routing updates. This allows subnets and their masks to be included in the routing updates. However, by default RIPv2 summarizes networks at major network boundaries, just like RIPv1, except that the subnet mask is included in the update.

Step 2: Verify that RIPv2 is running on the routers.

The **debug ip rip**, **show ip protocols**, and **show run**commands can all be used to confirm that RIPv2 is running. The output of the **show ip protocols**command for R1 is shown below.

```
R1# show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set Incoming update filter list for all
interfaces is not set Redistributing: rip
Default version control: send version 2, receive 2
    Interface              Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0        2     2
    FastEthernet0/1        2     2
    Serial0/0/0            2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
     172.30.0.0
     209.165.200.0
      Passive Interface(s):
        FastEthernet0/0
        FastEthernet0/1
Routing Information Sources:
     Gateway         Distance      Last Update
     209.165.200.229         120
Distance: (default is 120)
```

Task 5: Examine the Automatic Summarization of Routes.

The LANs connected to R1 and R3 are still composed of discontiguous networks. R2 still shows two equal cost paths to the 172.30.0.0/16 network in the routing table. R2 still shows only the major classful network address of 172.30.0.0 and does not show any of the subnets for this network.

R2#**show ip route**

Output omitted

```
     10.0.0.0/16 is subnetted, 1 subnets
C       10.1.0.0 is directly connected, FastEthernet0/0
R    172.30.0.0/16 [120/1] via 209.165.200.230, 00:00:07, Serial0/0/0
                           [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
     209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.228 is directly connected, Serial0/0/0
C       209.165.200.232 is directly connected, Serial0/0/1
```

R1 still shows only its own subnets for the 172.30.0.0 network. R1 still does not have any routes for the 172.30.0.0 subnets on R3.

R1#**show ip route**

Output omitted

```
R    10.0.0.0/8 [120/1] via 209.165.200.229, 00:00:09, Serial0/0/0
     172.30.0.0/24 is subnetted, 2 subnets
C       172.30.1.0 is directly connected, FastEthernet0/0
C       172.30.2.0 is directly connected, FastEthernet0/1
     209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.228 is directly connected, Serial0/0/0
R       209.165.200.232 [120/1] via 209.165.200.229, 00:00:09, Serial0/0/0
```

R3 still only shows its own subnets for the 172.30.0.0 network. R3 still does not have any routes for the 172.30.0.0 subnets on R1.

R3#**show ip route**

Output omitted

```
R    10.0.0.0/8 [120/1] via 209.165.200.233, 00:00:16, Serial0/0/1
     172.30.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.30.100.0/24 is directly connected, FastEthernet0/0
C       172.30.110.0/24 is directly connected, Loopback0
C       172.30.200.16/28 is directly connected, Loopback1
C       172.30.200.32/28 is directly connected, Loopback2
     209.165.200.0/30 is subnetted, 2 subnets
R       209.165.200.228 [120/1] via 209.165.200.233, 00:00:16, Serial0/0/1
C       209.165.200.232 is directly connected, Serial0/0/1
```

Use the output of the **debug ip rip**command to answer the following questions:

What entries are included in the RIP updates sent out from R3?

_____

_____

_____

_____

_____

On R2, what routes are in the RIP updates that are received from R3?

_____

_____

_____

R3 is not sending any of the 172.30.0.0 subnets—only the summarized route of 172.30.0.0/16, including the subnet mask. This is why R2 and R1 are not seeing the 172.30.0.0 subnets on R3.

Task 6: Disable Automatic Summarization.

The **no auto-summary** command is used to turn off automatic summarization in RIPv2. Disable auto summarization on all routers. The routers will no longer summarize routes at major network boundaries.

```
R2(config)#router rip
R2(config-router)#no auto-summary

R1(config)#router rip
R1(config-router)#no auto-summary

R3(config)#router rip
R3(config-router)#no auto-summary
```

The **show ip route**and **ping**commands can be used to verify that automatic summarization is off.

Task 7: Examine the Routing Tables.

The LANs connected to R1 and R3 should now be included in all three routing tables.

```
R2#show ip route

Output omitted

      10.0.0.0/16 is subnetted, 1 subnets
C        10.1.0.0 is directly connected, FastEthernet0/0
     172.30.0.0/16 is variably subnetted, 7 subnets, 3 masks
R        172.30.0.0/16 [120/1] via 209.165.200.230, 00:01:28, Serial0/0/0
                       [120/1] via 209.165.200.234, 00:01:56, Serial0/0/1
R        172.30.1.0/24 [120/1] via 209.165.200.230, 00:00:08, Serial0/0/0
```

```
R       172.30.2.0/24 [120/1] via 209.165.200.230, 00:00:08, Serial0/0/0
R       172.30.100.0/24 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
R       172.30.110.0/24 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
R       172.30.200.16/28 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
R       172.30.200.32/28 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
    209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.228 is directly connected, Serial0/0/0
C       209.165.200.232 is directly connected, Serial0/0/1
```

R1#**show ip route**

Output omitted

```
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R       10.0.0.0/8 [120/1] via 209.165.200.229, 00:02:13, Serial0/0/0
R       10.1.0.0/16 [120/1] via 209.165.200.229, 00:00:21, Serial0/0/0
    172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
C       172.30.1.0/24 is directly connected, FastEthernet0/0
C       172.30.2.0/24 is directly connected, FastEthernet0/1
R       172.30.100.0/24 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
R       172.30.110.0/24 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
R       172.30.200.16/28 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
R       172.30.200.32/28 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
    209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.228 is directly connected, Serial0/0/0
R       209.165.200.232 [120/1] via 209.165.200.229, 00:00:21, Serial0/0/0
```

R3#**show ip route**

Output omitted

```
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R       10.0.0.0/8 [120/1] via 209.165.200.233, 00:02:28, Serial0/0/1
R       10.1.0.0/16 [120/1] via 209.165.200.233, 00:00:08, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
R       172.30.1.0/24 [120/2] via 209.165.200.233, 00:00:08, Serial0/0/1
R       172.30.2.0/24 [120/2] via 209.165.200.233, 00:00:08, Serial0/0/1
C       172.30.100.0/24 is directly connected, FastEthernet0/0
C       172.30.110.0/24 is directly connected, Loopback0
C       172.30.200.16/28 is directly connected, Loopback1
C       172.30.200.32/28 is directly connected, Loopback2
    209.165.200.0/30 is subnetted, 2 subnets
R       209.165.200.228 [120/1] via 209.165.200.233, 00:00:08, Serial0/0/1
C       209.165.200.232 is directly connected, Serial0/0/1
```

Use the output of the **debug ip rip** command to answer the following questions: What entries are included in the RIP updates sent out from R1?

_____

_____

_____

On R2, what routes are in the RIP updates that are received from R1?

_____

_____

_____

Are the subnet masks now included in the routing updates? _____

Task 8: Verify Network Connectivity.

Step 1: Check connectivity between R2 router and PCs.

From R2, how many ICMP messages are successful when pinging PC1?

_____

From R2, how many ICMP messages are successful when pinging PC4?

_____

Step 2: Check the connectivity between the PCs.

From PC1, is it possible to ping PC2? _____

What is the success rate? _____

From PC1, is it possible to ping PC3? _____

What is the success rate? _____

From PC1, is it possible to ping PC4? _____

What is the success rate? _____

From PC4, is it possible to ping PC2? _____

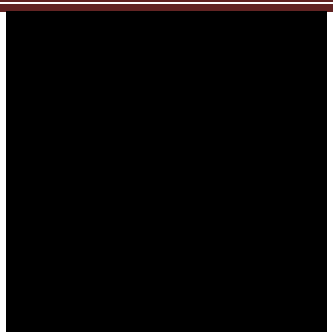
What is the success rate? _____

From PC4, is it possible to ping PC3? _____

What is the success rate? _____

Task 9: Documentation

On each router, capture the following command output to a text (.txt) file and save for future reference.



sho

w running-config

show ip route

show ip interface brief

show ip protocols

Task 10: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Critical Analysis/Conclusion

Lab Assessment		
Pre Lab	**/5**	**/25**
Performance	**/5**	
Results	**/5**	
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		

LAB #06

EIGRP configuration

Introduction

Enhanced Interior Gateway Routing Protocol (EIGRP) is an interior gateway protocol suited for many different topologies and media. In a well designed network, EIGRP scales well and provides extremely quick convergence times with minimal network traffic.

EIGRP Theory of Operation

Some of the many advantages of EIGRP are:

1. Very low usage of network resources during normal operation; only hello packets are transmitted on a stable network.
2. When a change occurs, only routing table changes are propagated, not the entire routing table; this reduces the load the routing protocol itself places on the network
3. Rapid convergence times for changes in the network topology (in some situations convergence can be almost instantaneous)

Neighbor Discovery and Maintenance

To distribute routing information throughout a network, EIGRP uses non-periodic incremental routing updates. That is, EIGRP only sends routing updates about paths that have changed when those paths change.

The basic problem with sending only routing updates is that you may not know when a path through a neighboring router is no longer available. You cannot time out routes, expecting to receive a new routing table from your neighbors. EIGRP relies on neighbor relationships to reliably propagate routing table changes throughout the network; two routers become neighbors when they see each other's hello packets on a common network.

EIGRP sends hello packets every 5 seconds on high bandwidth links and every 60 seconds on low bandwidth multipoint links. The rate at which EIGRP sends hello packets is called the hello interval, and you can adjust it per interface with the **ip hello-interval eigrp** command. The hold time is the amount of time that a router will consider a neighbor alive without receiving a hello packet. The hold time is typically three times the hello interval, by default, 15 seconds and 180 seconds. You can adjust the hold time with the **ip hold-time eigrp** command.

It is possible for two routers to become EIGRP neighbors even though the hello and hold timers do not match. The hold time is included in the hello packets so each neighbor should stay alive even though the hello interval and hold timers do not match.

While there is no direct way of determining what the hello interval is on a router, you can infer it from the output of **show ip eigrp neighbors** on the neighboring router.

There are no limitations on the number of neighbors that EIGRP can support. The actual number of supported neighbors depends on the capability of the device, such as:

1. Memory capacity 2. Processing power 3. Amount of exchanged information, such as the number of routes sent 4. Topology complexity 5.network stability

EIGRP Metrics

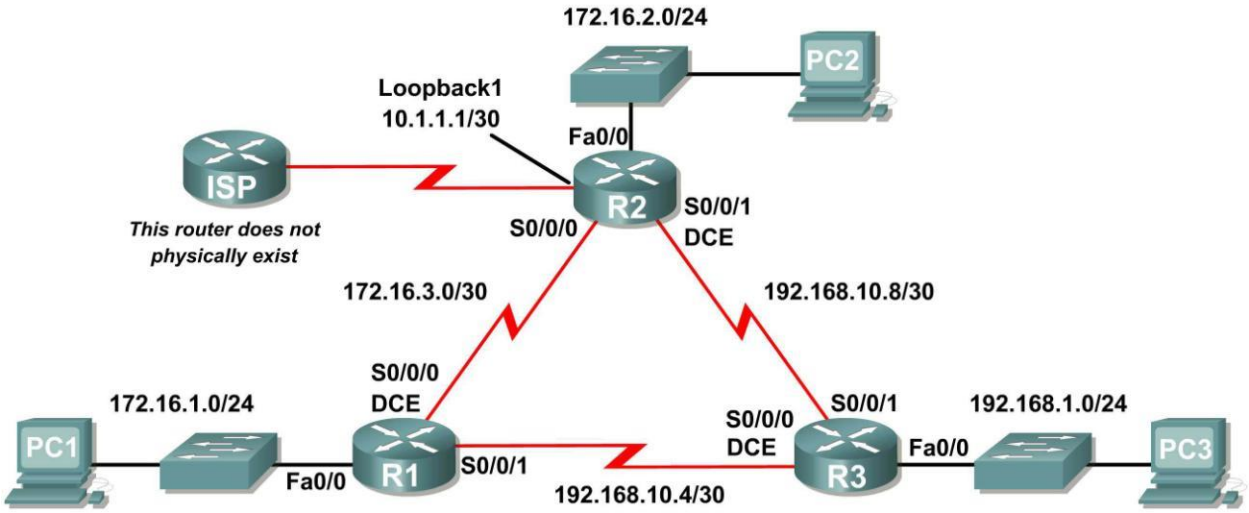
EIGRP uses the minimum bandwidth on the path to a destination network and the total delay to compute routing metrics. Although you can configure other metrics, we do not recommend it, as it can cause routing loops in your network. The bandwidth and delay metrics are determined from values configured on the interfaces of routers in the path to the destination network.

Metric = bandwidth + delay

PreLab Questions:

1.Define successor and feasible distance?
2.How to calculate successor and feasible distance in EGIRP?
3.What is Wildcard Mask?
4.What is metric for EIGRP?
5. Difference Between IGRP and EIGRP?

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	Fa0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
	Lo1	10.1.1.1	255.255.255.252	N/A
R3	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC2	NIC	172.16.2.10	255.255.255.0	172.16.2.1
PC3	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Learning Objectives

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

- Cable a network according to the Topology Diagram.
- Erase the startup configuration and reload a router to the default state.
- Perform basic configuration tasks on a router.
- Configure and activate interfaces.
- Configure EIGRP routing on all routers.
- Verify EIGRP routing using **show** commands.
- Disable automatic summarization.
- Configure manual summarization.
- Configure a static default route.
- Propagate default route to EIGRP neighbors.
- Document the EIGRP configuration.

Scenario

In this lab activity, you will learn how to configure the routing protocol EIGRP using the network shown in the Topology Diagram. A loopback address will be used on the R2 router to simulate a connection to an ISP, where all traffic that is not destined for the local network will be sent. Some segments of the network have been subnetted using VLSM. EIGRP is a classless routing protocol that can be used to provide subnet mask information in the routing updates. This will allow VLSM subnet information to be propagated throughout the network.

Pre Lab Task

Task 1: Prepare the Network.

Step 1: Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations,

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

1. Configure the router hostname.
2. Disable DNS lookup.
3. Configure an EXEC mode password.
4. Configure a message-of-the-day banner.
5. Configure a password for console connections.
6. Configure a password for VTY connections.

Task 3: Configure and Activate Serial and Ethernet Addresses.

Step 1: Configure the interfaces on the R1, R2, and R3 routers.

Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the table under the Topology Diagram.

Step 2: Verify IP addressing and interfaces.

Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 3: Configure Ethernet interfaces of PC1, PC2, and PC3.

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from the table under the Topology Diagram.

Lab Task

Task 4: Configure EIGRP on the R1 Router.

Step 1: Enable EIGRP.

Use the **router eigrp** command in global configuration mode to enable EIGRP on the R1 router. Enter a process ID of 1 for the *autonomous-system* parameter.

```
R1(config)#router eigrp 1
R1(config-router)#
```

Step 2: Configure classful network 172.16.0.0.

Once you are in the Router EIGRP configuration sub-mode, configure the classful network 172.16.0.0 to be included in the EIGRP updates that are sent out of R1.

```
R1(config-router)#network 172.16.0.0
R1(config-router)#
```

The router will begin to send EIGRP update messages out each interface belonging to the 172.16.0.0 network. EIGRP updates will be sent out of the FastEthernet0/0 and Serial0/0/0 interfaces because they are both on subnets of the 172.16.0.0 network.

Step 3: Configure the router to advertise the 192.168.10.4/30 network attached to the Serial0/0/1 interface.

Use the *wildcard-mask* option with the **network** command to advertise only the subnet and not the entire 192.168.10.0 classful network.

Note: Think of a wildcard mask as the inverse of a subnet mask. The inverse of the subnet mask 255.255.255.252 is 0.0.0.3. To calculate the inverse of the subnet mask, subtract the subnet mask from 255.255.255.255:

```
    255.255.255.255
-   255.255.255.252      Subtract the subnet mask
------------------
      0.  0.  0.  3      Wildcard mask
```

```
R1(config-router)# network 192.168.10.4 0.0.0.3
R1(config-router)#
```

When you are finished with the EIGRP configuration for R1, return to privileged EXEC mode and save the current configuration to NVRAM.

```
R1(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#
```

Task 5: Configure EIGRP on the R2 and R3 Routers.

Step 1: Enable EIGRP routing on the R2 router using the `router eigrp` command.

Use a process ID of 1.

```
R2(config)#router eigrp 1
R2(config-router)#
```

Step 2: Use the classful address 172.16.0.0 to include the network for the FastEthernet0/0 interface.

```
R2(config-router)#network 172.16.0.0
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial0/0/0) is up:
new adjacency
```

Notice that DUAL sends a notification message to the console stating that a neighbor relationship with another EIGRP router has been established.

What is the IP address of the EIGRP neighbor router?

_____

What interface on the R2 router is the neighbor adjacent to?

_____

Step 3: Configure the R2 router to advertise the 192.168.10.8/30 network attached to the Serial0/0/1 interface.

1. Use the *wildcard-mask* option with the **network** command to advertise only the subnet and not the entire 192.168.10.0 classful network.
2. When you are finished, return to privileged EXEC mode.

```
R2(config-router)#network 192.168.10.8 0.0.0.3
R2(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

Step 4: Configure EIGRP on the R3 router using the `router eigrp` and `network` commands.

1. Use a process ID of 1.
2. Use the classful network address for the network attached to the FastEthernet0/0 interface.
3. Include the wildcard masks for the subnets attached to the Serial0/0/0 and Serial 0/0/1 interfaces.
4. When you are finished, return to privileged EXEC mode.

```
R3(config)#router eigrp 1
R3(config-router)#network 192.168.1.0
R3(config-router)#network 192.168.10.4 0.0.0.3
R3(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.5 (Serial0/0/0) is up:
new adjacency
R3(config-router)#network 192.168.10.8 0.0.0.3
R3(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.9 (Serial0/0/1) is up:
new adjacency
R3(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
```

Notice that when the networks for the serial links from R3 to R1 and R3 to R2 are added to the EIGRP configuration, DUAL sends a notification message to the console stating that a neighbor relationship with another EIGRP router has been established.

Task 6: Verify EIGRP Operation.

Step 1: View neighbors.

On the R1 router, use the **show ip eigrp neighbors** command to view the neighbor table and verify that EIGRP has established an adjacency with the R2 and R3 routers. You should be able to see the IP address of each adjacent router and the interface that R1 uses to reach that EIGRP neighbor.

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   172.16.3.2      Ser0/0/0        10   00:36:51  40     500   0   13
1   192.168.10.6    Ser0/0/1        11   00:26:51  40     500   0   4
R1#
```

Step 2: View routing protocol information.

On the R1 router, use **the show ip protocols** command to view information about the routing protocol operation. Notice that the information that was configured in Task 5, such as protocol, process ID, and networks, is shown in the output. The IP addresses of the adjacent neighbors are also shown.

```
R1#show ip protocols

Routing Protocol is "eigrp  1 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
  Automatic network summarization is in effect
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
     172.16.0.0
     192.168.10.4/30
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.3.2      90            4811399
    192.168.10.6    90            5411677
  Distance: internal 90 external 170
```

Notice that the output specifies the process ID used by EIGRP. Remember, the process ID must be the same on all routers for EIGRP to establish neighbor adjacencies and share routing information.

Task7: Examine EIGRP Routes in the Routing Tables.

Step1: View the routing table on the R1 router.

EIGRP routes are denoted in the routing table with a **D**, which stands for DUAL (Diffusing Update Algorithm), which is the routing algorithm used by EIGRP.

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

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 01:16:19, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/2172416] via 172.16.3.2, 01:16:20, Serial0/0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/2172416] via 192.168.10.6, 01:06:18, Serial0/0/1
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 01:06:07, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/1
D       192.168.10.8/30 [90/2681856] via 192.168.10.6, 01:06:07, Serial0/0/1
R1#
```

Notice that the 172.16.0.0/16 parent network is variably subnetted with three child routes using either a /24 or /30 mask. Also notice that EIGRP has automatically included a summary route to Null0 for the 172.16.0.0/16 network. The 172.16.0.0/16 route does not actually represent a path to reach the parent network, 172.16.0.0/16. If a packet destined for 172.16.0.0/16 does not match one of the level 2 child routes, it is sent to the Null0 interface.

```
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 01:16:19, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/2172416] via 172.16.3.2, 01:16:20, Serial0/0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
```

The 192.168.10.0/24 Network is also variably subnetted and includes a Null0 route.

```
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 01:06:07, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/1
D       192.168.10.8/30 [90/2681856] via 192.168.10.6, 01:06:07, Serial0/0/1
```

Step 2: View the routing table on the R3 router.

The routing table for R3 shows that both R1 and R2 are automatically summarizing the 172.16.0.0/16 network and sending it as a single routing update. Because of automatic summarization, R1 and R2 are not propagating the individual subnets. Because R3 is getting two equal cost routes for 172.16.0.0/16 from both R1 and R2, both routes are included in the routing table.

```
R3#show ip route

<output omitted>

D    172.16.0.0/16 [90/2172416] via 192.168.10.5, 01:15:35, Serial0/0/0
                   [90/2172416] via 192.168.10.9, 01:15:22, Serial0/0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 01:15:22, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/0
C       192.168.10.8/30 is directly connected, Serial0/0/1
R3#
```

Task 8: Configure EIGRP Metrics.

Step 1: View the EIGRP metric information.

Use the **show interface serial0/0/0** command to view the EIGRP metric information for the Serial0/0/0 interface on the R1 router. Notice the values that are shown for the bandwidth, delay, reliability, and load.

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)

<output omitted>
```

Step 2: Modify the bandwidth of the Serial interfaces.

On most serial links, the bandwidth metric will default to 1544 Kbits. If this is not the actual bandwidth of the serial link, the bandwidth will need to be changed so that the EIGRP metric can be calculated correctly.

For this lab, the link between R1 and R2 will be configured with a bandwidth of 64 kbps, and the link between R2 and R3 will be configured with a bandwidth of 1024 kbps. Use the **bandwidth** command to modify the bandwidth of the Serial interfaces of each router.

R1 router:

```
R1(config)#interface serial0/0/0
R1(config-if)#bandwidth 64
```

R2 router:

```
R2(config)#interface serial0/0/0
R2(config-if)#bandwidth 64
R2(config)#interface serial0/0/1
R2(config-if)#bandwidth 1024
```

R3 router:

```
R3(config)#interface serial0/0/1
R3(config-if)#bandwidth 1024
```

Note: The **bandwidth** command only modifies the bandwidth metric used by routing protocols, not the physical bandwidth of the link.

Step 3: Verify the bandwidth modifications.

Use the **show ip interface** command to verify that the bandwidth value of each link has been changed.

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)

<output omitted>

R2#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 172.16.3.2/30
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)

<output omitted>

R3#show interface serial0/0/1
Serial0/0/1 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 192.168.10.10/30
  MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)

<output omitted>
```

Note: Use the interface configuration command **no bandwidth** to return the bandwidth to its default value.

Task 9: Examine Successors and Feasible Distances.

Step 1: Examine the successors and feasible distances in the routing table on R2.

```
R2#show ip route

<output omitted>

     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:00:52, Null0
D       172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:52, Serial0/0/0
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:11, Serial0/0/1
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:00:11, Null0
D       192.168.10.4/30 [90/3523840] via 192.168.10.10, 00:00:11,
Serial0/0/1
C       192.168.10.8/30 is directly connected, Serial0/0/1
R2#
```

Step 2: Answer the following questions:

What is the best path to PC1?

A successor is a neighboring router that is currently being used for packet forwarding. A successor is the least-cost route to the destination network. The IP address of a successor is shown in a routing table entry right after the word “via”.

What is the IP address and name of the successor router in this route?

Feasible distance (FD) is the lowest calculated metric to reach that destination. FD is the metric listed in the routing table entry as the second number inside the brackets.

What is the feasible distance to the network that PC1 is on?

Task 10: Determine if R1 is a Feasible Successor for the Route from R2 to the 192.168.1.0 Network.

A feasible successor is a neighbor who has a viable backup path to the same network as the successor. In order to be a feasible successor, R1 must satisfy the feasibility condition. The feasibility condition (FC) is met when a neighbor’s reported distance (RD) to a network is less than the local router’s feasible distance to the same destination network.

Step 1: Examine the routing table on R1.

```
R1#show ip route

<output omitted>

     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:42:59, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/40514560] via 172.16.3.2, 00:43:00, Serial0/0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:42:26, Serial0/0/1
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:42:20, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/1
D       192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:42:20,
Serial0/0/1
R1#
```

What is the reported distance to the 192.168.1.0 network?

Step 2: Examine the routing table on R2.

```
R2#show ip route

<output omitted>
```

```
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:00:52, Null0
D       172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:52, Serial0/0/0
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:11, Serial0/0/1
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:00:11, Null0
D       192.168.10.4/30 [90/3523840] via 192.168.10.10, 00:00:11, Serial0/0/1
C       192.168.10.8/30 is directly connected, Serial0/0/1
R2#
```

What is the feasible distance to the 192.168.1.0 network?

_____

Would R2 consider R1 to be a feasible successor to the 192.168.1.0 network? _____

Task 11: Examine the EIGRP Topology Table.

Step 1: View the EIGRP topology table.

Use the **show ip eigrp topology** command to view the EIGRP topology table on R2.

```
R2#show ip eigrp topology
IP-EIGRP Topology Table for AS 1

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 172.16.2.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 172.16.3.0/30, 1 successors, FD is 40512000
         via Connected, Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
         via Connected, Serial0/0/1
P 172.16.0.0/16, 1 successors, FD is 28160
         via Summary (28160/0), Null0
P 192.168.10.0/24, 1 successors, FD is 3011840
         via Summary (3011840/0), Null0
P 172.16.1.0/24, 1 successors, FD is 40514560
         via 172.16.3.1 (40514560/28160), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 3014400
         via 192.168.10.10 (3014400/28160), Serial0/0/1
         via 172.16.3.1 (41026560/2172416), Serial0/0/0
P 192.168.10.4/30, 1 successors, FD is 3523840
         via 192.168.10.10 (3523840/2169856), Serial0/0/1
R2#
```

Step 2: View detailed EIGRP topology information.

Use the [*network*] parameter of the **show ip eigrp topology** command to view detailed EIGRP topology information for the 192.16.0.0 network.

```
R2#show ip eigrp topology 192.168.1.0
IP-EIGRP (AS 1): Topology entry for 192.168.1.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 3014400
  Routing Descriptor Blocks:
  192.168.10.10 (Serial0/0/1), from 192.168.10.10, Send flag is 0x0
      Composite metric is (3014400/28160), Route is Internal
      Vector metric:
        Minimum bandwidth is 1024 Kbit
        Total delay is 20100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
  172.16.3.1 (Serial0/0/0), from 172.16.3.1, Send flag is 0x0
      Composite metric is (41026560/2172416), Route is Internal
      Vector metric:
        Minimum bandwidth is 64 Kbit
        Total delay is 40100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
R2#
```

How many successors are there for this network?

_____

What is the feasible distance to this network?

_____

What is the IP address of the feasible successor?

_____

What is the reported distance for 192.168.1.0 from the feasible successor?

_____

What would be the feasible distance to 192.168.1.0 if R1 became the successor?

_____

Task 12: Disable EIGRP Automatic Summarization.

Step 1: Examine the routing table of the R3 router.

Notice that R3 is not receiving individual routes for the 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24 subnets. Instead, the routing table only has a summary route to the classful network address of 172.16.0.0/16 through the R1 router. This will cause packets that are destined for the 172.16.2.0/24 network to be sent through the R1 router instead of being sent straight to the R2 router.

```
R3#show ip route

<outputomitted>
```

```
D     172.16.0.0/16 [90/2172416] via 192.168.10.5, 01:21:54, Serial0/0/0
C     192.168.1.0/24 is directly connected, FastEthernet0/0
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D        192.168.10.0/24 is a summary, 01:21:47, Null0
C        192.168.10.4/30 is directly connected, Serial0/0/0
C        192.168.10.8/30 is directly connected, Serial0/0/1
R3#
```

Why is the R1 router (192.168.10.5) the only successor for the route to the 172.16.0.0/16 network?

Notice that the reported distance from R2 is higher than the feasible distance from R1.

```
R3#show ip eigrp topology
IP-EIGRP Topology Table for AS 1

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.1.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 192.168.10.4/30, 1 successors, FD is 2169856
         via Connected, Serial0/0/0
P 192.168.10.0/24, 1 successors, FD is 2169856
         via Summary (2169856/0), Null0
P 172.16.0.0/16, 1 successors, FD is 2172416
         via 192.168.10.5 (2172416/28160), Serial0/0/0
         via 192.168.10.9 (3014400/28160), Serial0/0/1
P 192.168.10.8/30, 1 successors, FD is 3011840
         via Connected, Serial0/0/1
```

Step 3: Disable automatic summarization on all three routers with the `no auto-summary` command.

```
R1(config)#router eigrp 1
R1(config-router)#no auto-summary

R2(config)#router eigrp 1
R2(config-router)#no auto-summary

R3(config)#router eigrp 1
R3(config-router)#no auto-summary
```

Step 4: View the routing table on R1 again.

Notice that individual routes for the 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24 subnets are now present and the summary Null route is no longer listed.

```
R3#show ip route

<output omitted>
```

```
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.1.0/24 [90/2172416] via 192.168.10.5, 00:02:37, Serial0/0/0
D       172.16.2.0/24 [90/3014400] via 192.168.10.9, 00:02:39, Serial0/0/1
D       172.16.3.0/30 [90/41024000] via 192.168.10.9, 00:02:39, Serial0/0/1
                      [90/41024000] via 192.168.10.5, 00:02:37, Serial0/0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C       192.168.10.4/30 is directly connected, Serial0/0/0
C       192.168.10.8/30 is directly connected, Serial0/0/1
R3#
```

Task 13: Configure Manual Summarization.

Step 1: Add loopback addresses to R3 router.

Add two loopback addresses, 192.168.2.1/24 and 192.168.3.1/24, to the R3 router. These virtual interfaces will be used to represent networks to be manually summarized along with the 192.168.1.0/24 LAN.

```
R3(config)#interface loopback1

%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state
to upR3(config-if)#ip address 192.168.2.1 255.255.255.0
R3(config-if)#interface loopback2

%LINK-5-CHANGED: Interface Loopback2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2, changed state
to up
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#
```

Step 2: Add the 192.168.2.0 and 192.168.3.0 networks to the EIGRP configuration on R3.

```
R3(config)#router eigrp 1
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
```

Step 3: Verify new routes.

View the routing table on the R1 router to verify that the new routes are being sent out in the EIGRP updates sent by R3.

```
R1#show ip route

<output omitted>

     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/3526400] via 192.168.10.6, 00:15:07, Serial0/0/1
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:15:07, Serial0/0/1
D    192.168.2.0/24 [90/2297856] via 192.168.10.6, 00:01:07, Serial0/0/1
D    192.168.3.0/24 [90/2297856] via 192.168.10.6, 00:00:57, Serial0/0/1
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C       192.168.10.4/30 is directly connected, Serial0/0/1
D       192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:15:07, Serial0/0/1
R1#
```

Step 4: Apply manual summarization to outbound interfaces.

The routes to the 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24 networks can be summarized in the single network 192.168.0.0/22. Use the **ip summary-address eigrp** *as-number network-address subnet-mask* command to configure manual summarization on each of the outbound interfaces connected to EIGRP neighbors.

```
R3(config)#interface serial0/0/0
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
R3(config-if)#interface serial0/0/1
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
R3(config-if)#
```

Step 5: Verify the summary route.

View the routing table on the R1 router to verify that the summary route is being sent out in the EIGRP updates sent by R3.

```
R1#show ip route

<output omitted>

     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/3526400] via 192.168.10.6, 00:15:07, Serial0/0/1
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.0.0/22 [90/2172416] via 192.168.10.6, 00:01:11, Serial0/0/1
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C       192.168.10.4/30 is directly connected, Serial0/0/1
D       192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:15:07, Serial0/0/1
R1#
```

Task 14: Configure and Distribute a Static Default Route.

Step 1: Configure a static default route on the R2 router.

Use the loopback address that has been configured to simulate a link to an ISP as the exit interface.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback1
R2(config)#
```

Step 2: Include the static route in EIGRP updates.

Use the **redistribute static** command to include the static route in the EIGRP updates that are sent from the R2 router.

```
R2(config)#router eigrp 1
R2(config-router)#redistribute static
R2(config-router)#
```

Step 3: Verify the static default route.

View the routing table on the R1 router to verify that the static default route is being redistributed via EIGRP.

```
R1#show ip route

<output omitted>
```

```
Gateway of last resort is 192.168.10.6 to network 0.0.0.0

     192.168.10.0/30 is subnetted, 2 subnets
C       192.168.10.4 is directly connected, Serial0/0/1
D       192.168.10.8 [90/3523840] via 192.168.10.6, 01:06:01, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/3526400] via 192.168.10.6, 01:05:39, Serial0/0/1
C       172.16.3.0/30 is directly connected, Serial0/0/0
D*EX 0.0.0.0/0 [170/3651840] via 192.168.10.6, 00:02:14, Serial0/0/1
D    192.168.0.0/22 [90/2172416] via 192.168.10.6, 01:05:38, Serial0/0/1
```

Task 15: Documentation

On each router, capture the following command output to a text (.txt) file and save for future reference.

- **show running-config**
- **show ip route**
- **show ip interface brief**
- **show ip protocols**

Task 16: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings

Critical Analysis / Conclusion

Lab Assessment		
Pre Lab	**/5**	**/25**
Performance	**/5**	
Results	**/5**	
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		

Lab #07 OSPF Configuration

Learning Objectives

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

- Cable a network according to the Topology Diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure and activate interfaces
- Configure OSPF routing on all routers
- Configure OSPF router IDs
- Verify OSPF routing using show commands
- Configure a static default route
- Propagate default route to OSPF neighbors
- Configure OSPF Hello and Dead Timers
- Configure OSPF on a Multi-access network
- Configure OSPF priority
- Understand the OSPF election process
- Document the OSPF configuration

Scenarios

In this lab activity, there are two separate scenarios. In the first scenario, you will learn how to configure the routing protocol OSPF using the network shown in the Topology Diagram in Scenario A. The segments of the network have been subnetted using VLSM. OSPF is a classless routing protocol that can be used to provide subnet mask information in the routing updates. This will allow VLSM subnet information to be propagated throughout the network.

In the second scenario, you will learn to configure OSPF on a multi-access network. You will also learn to use the OSPF election process to determine the designated router (DR), backup designated router (BDR), and DRother states.

OSPF Concepts and Configuration

Things to Remember about Link State Routing

1. Link state protocols advertise a large amount of topological information about the network

2. Routers must calculate the metric (using shortest path First Algorithm)

3. Routers perform CPU intensive computations on the data.

4. Discover neighbors before exchanging information.

Process of Learning Routes:

1. Each router discovers its neighbors on each interface, list kept in **neighbors table**.

2. Each router uses a reliable protocol to exchange topology information in its **topology database**.

3. Each router places the learned topology information in its topology database.

4. Each router then runs the SPF algorithm against its own topology database to calculate the best routes to each subnet in the database.

5. Each router finally places the best route to each subnet in the IP routing table.

OSPF Topology Database: Consists of lists of subnet numbers (links), list of routers (and links they are connected to). Uniquely identifier each router in this database using OSPF Router ID (RID)

To select the RID. The router **first checks for any loopback** interfaces that are up, and choose the highest numeric IP address of those.

• **If no loopback exists**, router chooses highest IP address from interfaces that are up and up. **Meeting OSPF Neighbors:** Once router has assigned itself a RID, and some of its interfaces are up, the router is ready to meet its neighbors (connected routers).

• Can become neighbors if connected to same subnet

• Router multicasts OSPF Hello packets out each interface

• Hello message follows IP packet header (**port = 89**)

• Hello packets sent to **224.0.0.5** (all OSPF speaking routers)

Routers learn several things from Hello Packets:

RID, Area ID, Hello Interval, Dead Interval, router priority, designated router, backup designated

router, and a list of neighbors sending router already knew about.

To confirm that a Hello Packet was received, next Hello Message will include the sender's RID within the list of neighbors.

Once router sees its RID included, two-way state achieved, and more detailed information can be exchanged.

The following must match before routers become neighbors:

1. Subnet mask

2. Hello Interval

3. OSPF Area ID

4. Dead Interval

5. Subnet number (derived using the mask applied to the IP)

Reducing Overhead Using Designated Routers

Sometimes **Designated Routers** (DR) are required before sending **Database Description** (DD) packets.

• DR's always required on a LAN

• Sometimes required with Frame Relay/ATM (depending on topology/config)

After DR is elected, all updates flow through the Designated Router (DR). This means that the

DR collects and distributes the routing updates to alleviate OSPF update congestion. Router decides if it needs to elect a DR depending on the *network type*.

* **Point-to-point** DOES NOT need a DR

* **Broadcast** (for LANs), always needs a DR

**** Since DR's are so important**, loss of one could cause delay in convergence, so Backup DR (BDR) is also needed. ****

Electing the Designated Router

To elect, neighboring routers hold an election, and look at two fields in the Hello Packet:

* Router that sends the highest OSPF priority becomes DR.

* If there is a tie, the highest RID wins.

* **To elect BDR**, typically the second highest priority is used. *

* Priority setting of 0 means router will never be DR

* Range of valid priority values is 1-255 (to become a DR)

* If DR is elected, then another router comes online with a higher priority, this router will not become DR until both the DR and BDR fail.

Once DR/BDR is elected:

1. Non-DR send updates to 224.0.0.6 (All OSPF DRs)

2. DR relays these messages to 224.0.0.5 (BDR does not forward, only receives)

3. Once router has exchanged its entire link state database, transition to *Full State*

Steady-State Operation: If Hello Interval is not received for [dead interval] amount of time, the router believes the neighbor has failed.

• Default dead timer is 4 times the hello interval

(10 second hello, 40 second dead timer)

• Router marks as "down" in its neighbor table

• Runs the dijkstra algorithm to calculate new routes, floods to inform other routers of failed link **Loop Avoidance:** Link state does not use SPF algorithm, but rather it relies on router broadcasting downed link immediately. This is the main reason for fast convergence time (distance vector uses holdtime, split horizon, etc, while link state does not).

Scaling OSPF: If network has many routers (~50 or more, a few hundred subnets), would result in:

* Slow convergence time

* Memory shortages/processor overloading

Scalability Solutions Include:

* **OSPF Areas:** Break up the network so that routers in one area know less topology information

about the subnets in the other area, and don’t know about other routers at all.

* **Border Router:** OSPF Area Border Router (ABR), border between 2 different areas (sits in both areas).

* **Makes other routers in same area** view network as if it had fewer routers.

* **Area 0 defined as backbone**, OSPF designs hierarchical

Pre-lab questions:

1. What is the main difference between link state and distance vector routing?
2. What is significance of designated router and backup designated router in OSPF?
3. Why OSPF is divided into different areas?
4. Define area boarder router and its functionality?
5. List three types of tables/databases build during OSPF operation.

Scenario A: Basic OSPF Configuration

Topology Diagram

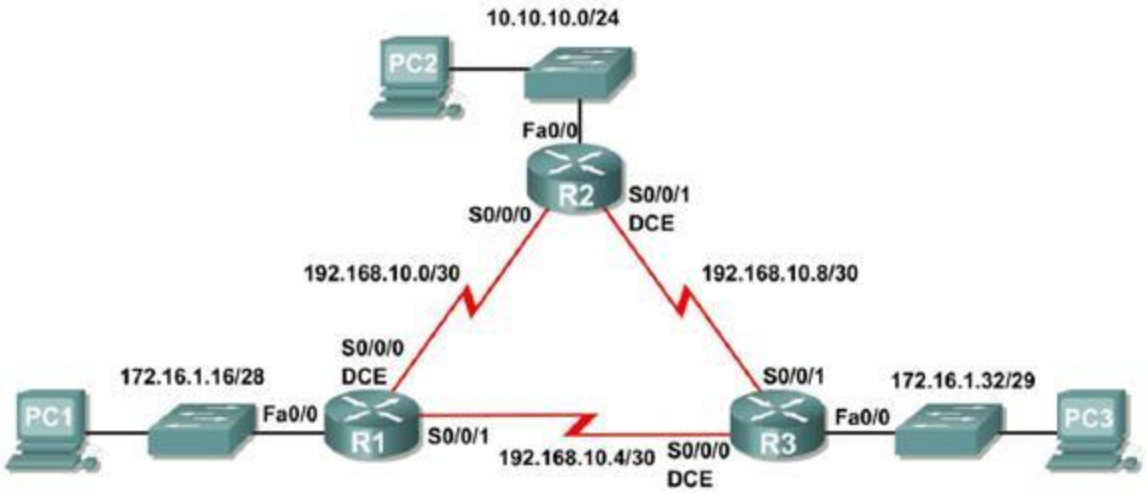


Figure 7. 1

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.1.17	255.255.255.240	N/A
	S0/0/0	192.168.10.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	Fa0/0	10.10.10.1	255.255.255.0	N/A
	S0/0/0	192.168.10.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	Fa0/0	172.16.1.33	255.255.255.248	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.20	255.255.255.240	172.16.1.17
PC2	NIC	10.10.10.10	255.255.255.0	10.10.10.1
PC3	NIC	172.16.1.35	255.255.255.248	172.16.1.33

Table 7. 1 Addressing Table

Lab Task:

Task 1: Prepare the Network.

Step 1: Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations.

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

1. Configure the router hostname.
2. Disable DNS lookup.
3. Configure a privileged EXEC mode password.
4. Configure a message-of-the-day banner.

5. Configure a password for console connections.
6. Configure a password for VTY connections.

Task 3: Configure and Activate Serial and Ethernet Addresses.

Step 1: Configure interfaces on R1, R2, and R3.

Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the table under the Topology Diagram.

Step 2: Verify IP addressing and interfaces.

Use the **`show ip interface brief`** command to verify that the IP addressing is correct and that the interfaces are active.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 3: Configure Ethernet interfaces of PC1, PC2, and PC3.

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from the table under the Topology Diagram.

Step 4: Test the PC configuration by pinging the default gateway from the PC.

Task 4: Configure OSPF on the R1 Router

Step 1: Use the router ospf command in global configuration mode to enable OSPF on the

R1 router.

Enter a process ID of 1 for the *`process-ID`* parameter.

```
R1(config)#router ospf 1

R1(config-router)#
```

Step 2: Configure the `network` statement for the LAN network.

Once you are in the Router OSPF configuration sub-mode, configure the LAN network

172.16.1.16/28 to be included in the OSPF updates that are sent out of R1.

The OSPF **network**command uses a combination of *network-address*and *wildcard-mask* similar to that which can be used by EIGRP. Unlike EIGRP, the wildcard mask in OSPF is required.

Use an area ID of 0 for the OSPF *area-id*parameter. 0 will be used for the OSPF area ID in all of the **network**statements in this topology.

```
R1(config-router)#network 172.16.1.16 0.0.0.15 area 0

R1(config-router)#
```

Step 3: Configure the router to advertise the 192.168.10.0/30 network attached to the

```
Serial0/0/0 interface.

R1(config-router)# network 192.168.10.0 0.0.0.3 area 0

R1(config-router)#
```

Step 4: Configure the router to advertise the 192.168.10.4/30 network attached to the

Serial0/0/1 interface.

```
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0

R1(config-router)#
```

Step 5: When you are finished with the OSPF configuration for R1, return to privileged

```
EXEC mode.

R1(config-router)#end

%SYS-5-CONFIG_I: Configured from console by console

R1#
```

Task 5: Configure OSPF on the R2 and R3 Routers

Step 1: Enable OSPF routing on the R2 router using the router ospf command.

Use a process ID of 1.

```
R2(config)#router ospf 1

R2(config-router)#
```

Step 2: Configure the router to advertise the LAN network 10.10.10.0/24 in the OSPF

updates.

```
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0

R2(config-router)#
```

Step 3: Configure the router to advertise the 192.168.10.0/30 network attached to the Serial0/0/0 interface.

```
R2(config-router)#network 192.168.10.0 0.0.0.3 area 0

R2(config-router)#

00:07:27: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0

from EXCHANGE to FULL, Exchange Done
```

Notice that when the network for the serial link from R1 to R2 is added to the OSPF configuration, the router sends a notification message to the console stating that a neighbor relationship with another OSPF router has been established.

Step 4: Configure the router to advertise the 192.168.10.8/30 network attached to the Serial0/0/1 interface.

When you are finished, return to privileged EXEC mode.

```
R2(config-router)#network 192.168.10.8 0.0.0.3 area 0

R2(config-router)#end

%SYS-5-CONFIG_I: Configured from console by console

R2#
```

Step 5: Configure OSPF on the R3 router using the router ospf and network commands.

Use a process ID of 1. Configure the router to advertise the three directly connected networks. When you are finished, return to privileged EXEC mode.

```
R3(config)#router ospf 1

R3(config-router)#network 172.16.1.32 0.0.0.7 area 0

R3(config-router)#network 192.168.10.4 0.0.0.3 area 0

R3(config-router)#

00:17:46: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0 from
LOADING to FULL, Loading Done

R3(config-router)#network 192.168.10.8 0.0.0.3 area 0

R3(config-router)#

00:18:01: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.9 on Serial0/0/1

from EXCHANGE to FULL, Exchange Done

R3(config-router)#end

%SYS-5-CONFIG_I: Configured from console by console

R3#
```

Notice that when the networks for the serial links from R3 to R1 and R3 to R2 are added to the OSPF configuration, the router sends a notification message to the console stating that a neighbor relationship with another OSPF router has been established.

Task 6: Configure OSPF Router IDs

The OSPF router ID is used to uniquely identify the router in the OSPF routing domain. A router

ID is an IP address. Cisco routers derive the Router ID in one of three ways and with the following precedence:

1. IP address configured with the OSPF **`router-id`** command.
2. Highest IP address of any of the router's loopback addresses.
3. Highest active IP address on any of the router's physical interfaces.

Step 1: Examine the current router IDs in the topology.

Since no router IDs or loopback interfaces have been configured on the three routers, the router

ID for each router is determined by the highest IP address of any active interface.

What is the router ID for R1? _____

What is the router ID for R2? _____

What is the router ID for R3? _____

The router ID can also be seen in the output of the **show ip protocols**, **show ip ospf**, and show ip ospf interfacescommands.

```
R3#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 192.168.10.10

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

<output omitted>

R3#show ip ospf

Routing Process "ospf 1" with ID 192.168.10.10

Supports only single TOS(TOS0) routes

Supports opaque LSA

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

<output omitted>

R3#show ip ospf interface

FastEthernet0/0 is up, line protocol is up

Internet address is 172.16.1.33/29, Area 0

Process ID 1, Router ID 192.168.10.10, Network Type BROADCAST, Cost:

1

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 192.168.10.10, Interface address 172.16.1.33

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
Hello due in 00:00:00

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

<output omitted>

R3#
```

Step 2: Use loopback addresses to change the router IDs of the routers in the topology.

```
R1(config)#interface loopback 0

R1(config-if)#ip address 10.1.1.1 255.255.255.255


R2(config)#interface loopback 0

R2(config-if)#ip address 10.2.2.2 255.255.255.255


R3(config)#interface loopback 0

R3(config-if)#ip address 10.3.3.3 255.255.255.255
```

Step 3: Reload the routers to force the new Router IDs to be used.

When a new Router ID is configured, it will not be used until the OSPF process is restarted. Make sure that the current configuration is saved to NRAM, and then use the **`reload`** command to restart each of the routers.

When the router is reloaded, what is the router ID for R1? _____

When the router is reloaded, what is the router ID for R2? _____

When the router is reloaded, what is the router ID for R3? _____

Step 4: Use the `show ip ospf neighbors` command to verify that the router IDs have changed.

```
R1#show ip ospf neighbor

Neighbor ID Pri   State Dead Time   Address
```

```
Interface

10.3.3.3    0     FULL/ -     00:00:30    192.168.10.6

Serial0/0/1

10.2.2.2    0     FULL/ -     00:00:33    192.168.10.2

Serial0/0/0

R2#show ip ospf neighbor
```

```
Neighbor    IDPri     State   Dead Time            Address
Interface
10.3.3.3        0       FULL/   -       00:00:36        192.168.10.10
Serial0/0/1
10.1.1.1        0       FULL/   -       00:00:37        192.168.10.1
Serial0/0/0
```

```
R3#show ip ospf neighbor
```

```
Neighbor ID    Pri     State   Dead Time            Address
Interface
10.2.2.2        0       FULL/   -       00:00:34        192.168.10.9

Serial0/0/1
Serial0/0/0
```

Step 5: Use the `router-id` command to change the router ID on the R1 router.

Note: Some IOS versions do not support the **`router-id`** command. If this command is not available, continue to Task 7.

```
R1(config)#router ospf 1

R1(config-router)#router-id 10.4.4.4
```

Reload or use "clear ip ospf process" command, for this to take effect

If this command is used on an OSPF router process which is already active (has neighbors), the new router-ID is used at the next reload or at a manual OSPF process restart. To manually restart the OSPF process, use the **`clear ip ospf process`** command.

```
R1#(config-router)#end

R1# clear ip ospf process

Reset ALL OSPF processes? [no]:yes

R1#
```

Step 6: Use the `show ip ospf neighbor` command on router R2 to verify that the router ID of R1 has been changed.

```
R2#show ip ospf neighbor
```

Neighbor ID	Interface	Pri	State	Dead Time	Address
10.3.3.3		0	FULL/	- 00:00:36	192.168.10.10
10.4.4.4		0	FULL/	- 00:00:37	192.168.10.1
	Serial0/0/0				

Step 7: Remove the configured router ID with the `no` form of the `router-id` command.

```
R1(config)#router ospf 1

R1(config-router)#no router-id 10.4.4.4
```

Reload or use "clear ip ospf process" command, for this to take effect

Step 8: Restart the OSPF process using the `clear ip ospf process` command.

Restarting the OSPF process forces the router to use the IP address configured on the Loopback 0 interface as the Router ID.

```
R1(config-router)#end

R1# clear ip ospf process

Reset ALL OSPF processes? [no]:yes

R1#
```

Task 7: Verify OSPF Operation

Step 1: On the R1 router,

Use the `show ip ospf neighbor` command to view the information about the OSPF neighbor routers R2 and R3. You should be able to see the neighbor ID and IP address of each adjacent router, and the interface that R1 uses to reach that OSPF neighbor.

```
R1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address
Interface
10.2.2.2          0   FULL/-          00:00:32    192.168.10.2
Serial0/0/0
10.3.3.3          0   FULL/-          00:00:32    192.168.10.6
Serial0/0/1
R1#
```

Step 2: On the R1 router, use the `show ip protocols` command to view information about the routing protocol operation.

Notice that the information that was configured in the previous Tasks, such as protocol, process ID, neighbor ID, and networks, is shown in the output. The IP addresses of the adjacent neighbors are also shown.

```
R1#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set Incoming update
filter list for all interfaces is not set Router ID 10.1.1.1

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

    172.16.1.16          Area              0
    192.168.10.0         Area              0
    192.168.10.4.0       Area              0
Routing Information Sources:

  Gateway         Distance      Last Update
  10.2.2.2             110      00:11:43
  10.3.3.3             110      00:11:43
Distance: (default is 110) R1#
```

Notice that the output specifies the process ID used by OSPF. Remember, the process ID is local to the router and can be different between routers without affecting neighbor adjacencies and the sharing of routing information.

Task8: Examine OSPF Routes in the Routing Tables

View the routing table on the R1 router. OSPF routes are denoted in the routing table with an “O”.

R1#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS

inter area

* - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.1.1.1/32 is directly connected, Loopback0

O 10.10.10.0/24 [110/65] via 192.168.10.2, 00:01:02, Serial0/0/0

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.1.16/28 is directly connected, FastEthernet0/0

O 172.16.1.32/29 [110/65] via 192.168.10.6, 00:01:12, Serial0/0/1

192.168.10.0/30 is subnetted, 3 subnets

C 192.168.10.0 is directly connected, Serial0/0/0

C 192.168.10.4 is directly connected, Serial0/0/1

O 192.168.10.8 [110/128] via 192.168.10.6, 00:01:12, Serial0/0/1

[110/128] via 192.168.10.2, 00:01:02, Serial0/0/0

R1#

Notice that unlike RIPv2 and EIGRP, OSPF does not automatically summarize at major network boundaries.

Task 9: Configure OSPF Cost

Step 1: Use the `show ip route` command on the R1 router to view the OSPF cost to reach the 10.10.10.0/24 network.

R1#show ip route

<output omitted>

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.1.1.1/32 is directly connected, Loopback0

O 10.10.10.0/24 [110/65] via 192.168.10.2, 00:16:56, Serial0/0/0

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.1.16/28 is directly connected, FastEthernet0/0

O 172.16.1.32/29 [110/65] via 192.168.10.6, 00:17:06, Serial0/0/1

192.168.10.0/30 is subnetted, 3 subnets

C 192.168.10.0 is directly connected, Serial0/0/0

C 192.168.10.4 is directly connected, Serial0/0/1

O 192.168.10.8 [110/128] via 192.168.10.6, 00:17:06, Serial0/0/1 [110/128] via 192.168.10.2, 00:16:56, Serial0/0/0

R1#

Step 2: Use the `show interfaces serial0/0/0` command on the R1 router to view the bandwidth of the Serial 0/0/0 interface.

R1#show interfaces serial0/0/0

Serial0/0/0 is up, line protocol is up (connected) Hardware is HD64570

Internet address is 192.168.10.1/30

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load

1/255

Encapsulation HDLC, loopback not set, keepalive set (10 sec)

Last input never, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0 (size/max/drops); Total output drops: 0

<output omitted>

On most serial links, the bandwidth metric will default to 1544 Kbits. If this is not the actual bandwidth of the serial link, the bandwidth will need to be changed so that the OSPF cost can be calculated correctly.

Step 3: Use the bandwidth command to change the bandwidth of the serial interfaces of the R1 and R2 routers to the actual bandwidth, 64 kbps.

R1 router:

```
R1(config)#interface serial0/0/0
R1(config-if)#bandwidth 64
R1(config-if)#interface serial0/0/1
```

```
R1(config-if)#bandwidth 64
```

R2 router:

```
R2(config)#interface serial0/0/0
R2(config-if)#bandwidth 64
R2(config)#interface serial0/0/1
R2(config-if)#bandwidth 64
```

Step 4: Use the `show ip ospf interface` command on the R1 router to verify the cost of the serial links.

The cost of each of the Serial links is now 1562, the result of the calculation: 10^8/64,000 bps.

```
R1#show ip ospf interface
<output omitted>
Serial0/0/0 is up, line protocol is up
Internet address is 192.168.10.1/30, Area 0
Process ID 1, Router ID 10.1.1.1, Network Type POINT-TO-POINT,
Cost:
1562
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
Hello due in 00:00:05
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 10.2.2.2
Suppress hello for 0 neighbor(s) Serial0/0/1 is up, line protocol
is up
```

```
Internet address is 192.168.10.5/30, Area 0

Process ID 1, Router ID 10.1.1.1, Network Type POINT-TO-POINT, Cost:

1562

Transmit Delay is 1 sec, State POINT-TO-POINT,

<output omitted>
```

Step 5: Use the ip ospf cost command to configure the OSPF cost on the R3 router. An alternative method to using the **bandwidth** command is to use the **ip ospf cost** command, which allows you to directly configure the cost. Use the **ip ospf cost** command to change

the bandwidth of the serial interfaces of the R3 router to 1562.

R3(config)#interface serial0/0/0

R3(config-if)#ip ospf cost 1562

R3(config-if)#interface serial0/0/1

R3(config-if)#ip ospf cost 1562

Step 6: Use the show ip ospf interface command on the R3 router to verify that the cost of the link the cost of each of the Serial links is now 1562.

R3#show ip ospf interface

<output omitted>

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

Internet address is 192.168.10.10/30, Area 0

Process ID 1, Router ID 10.3.3.3, Network Type POINT-TO-POINT, Cost:

1562

Transmit Delay is 1 sec, State POINT-TO-POINT,

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:06

Index 2/2, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec
```

```
Neighbor Count is 1 , Adjacent neighbor count is 1

Adjacent with neighbor 10.2.2.2

Suppress hello for 0 neighbor(s) Serial0/0/0 is up, line protocol is up

Internet address is 192.168.10.6/30, Area 0

Process ID 1, Router ID 10.3.3.3, Network Type POINT-TO-POINT, Cost:

1562

Transmit Delay is 1 sec, State POINT-TO-POINT,

<output omitted>
```

Task 10: Redistribute an OSPF Default Route

Step 1: Configure a loopback address on the R1 router to simulate a link to an ISP.

R1(config)#interface loopback1

%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

R1(config-if)#ip address 172.30.1.1 255.255.255.252

Step 2: Configure a static default route on the R1 router.

Use the loopback address that ha been configured to simulate a link to an ISP as the exit interface.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback1

R1(config)#
```

Step 3: Use the default-information originate command to include the static route in the OSPF updates that are sent from the R1 router.

R1(config)#router ospf 1

R1(config-router)#default-information originate

R1(config-router)#

Step 4: View the routing table on the R2 router to verify that the static default route is being redistributed via OSPF.

R2#show ip route

<output omitted>

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.2.2.2/32 is directly connected, Loopback0

C 10.10.10.0/24 is directly connected, FastEthernet0/0

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

O 172.16.1.16/28 [110/1563] via 192.168.10.1, 00:29:28,

Serial0/0/0

O 172.16.1.32/29 [110/1563] via 192.168.10.10, 00:29:28,

Serial0/0/1

192.168.10.0/30 is subnetted, 3 subnets

C 192.168.10.0 is directly connected, Serial0/0/0

O 192.168.10.4 [110/3124] via 192.168.10.10, 00:25:56, Serial0/0/1

[110/3124] via 192.168.10.1, 00:25:56, Serial0/0/0

C 192.168.10.8 is directly connected, Serial0/0/1

O*E2 0.0.0.0/0 [110/1] via 192.168.10.1, 00:01:11, Serial0/0/0

R2#

Task 11: Configure Additional OSPF Features

Step 1: Use the `auto-cost reference-bandwidth` command to adjust the reference bandwidth value.

Increase the reference bandwidth to 10000 to simulate 10GigE speeds. Configure this command on all routers in the OSPF routing domain.

```
R1(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all
routers.
R2(config-router)#auto-cost reference-bandwidth 10000
```

```
% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all

routers.

R3(config-router)#auto-cost reference-bandwidth 10000

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all
routers.
```

Step 2: Examine the routing table on the R1 router to verify the change in the OSPF cost

metric.

Notice that the values are much larger cost values for OSPF routes.

```
R1#show ip route

<output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C       10.1.1.1/32 is directly connected, Loopback0

O       10.10.10.0/24 [110/65635] via 192.168.10.2, 00:01:01, Serial0/0/0

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C       172.16.1.16/28 is directly connected, FastEthernet0/0

O       172.16.1.32/29 [110/65635] via 192.168.10.6, 00:00:51, Serial0/0/1

172.30.0.0/30 is subnetted, 1 subnets

C       172.30.1.0 is directly connected, Loopback1

192.168.10.0/30 is subnetted, 3 subnets

C       192.168.10.0 is directly connected, Serial0/0/0

C       192.168.10.4 is directly connected, Serial0/0/1

O       192.168.10.8 [110/67097] via 192.168.10.2, 00:01:01, Serial0/0/0

S*      0.0.0.0/0 is directly connected, Loopback1

R1#
```

Step 3: Use the `show ip ospf neighbor` command on R1 to view the Dead Time counter.

The Dead Time counter is counting down from the default interval of 40 seconds.

R1#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.2.2.2	0	FULL/-	00:00:34	192.168.10.2	Serial0/0/0
10.3.3.3	0	FULL/-	00:00:34	192.168.10.6	Serial0/0/1

Step 4: Configure the OSPF Hello and Dead intervals.

The OSPF Hello and Dead intervals can be modified manually using the **`ip ospf hello-interval`** and **`ip ospf dead-interval`** interface commands. Use these commands to change the hello interval to 5 seconds and the dead interval to 20 seconds on the Serial 0/0/0 interface of the R1 router.

R1(config)#interface serial0/0/0

R1(config-if)#ip ospf hello-interval 5

R1(config-if)#ip ospf dead-interval 20

R1(config-if)#

01:09:04: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from

FULL to DOWN, Neighbor Down: Dead timer expired

01:09:04: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from

FULL to Down: Interface down or detached

After 20 seconds the Dead Timer on R1 expires. R1 and R2 loose adjacency because the Dead Timer and Hello Timers must be configured identically on each side of the serial link between R1 and R2.

Step 5: Modify the Dead Timer and Hello Timer intervals.

Modify the Dead Timer and Hello Timer intervals on the Serial 0/0/0 interface in the R2 router to match the intervals configured on the Serial 0/0/0 interface of the R1 router.

```
R2(config)#interface serial0/0/0

R2(config-if)#ip ospf hello-interval 5

R2(config-if)#ip ospf dead-interval 20
```

```
R2(config-if)#

01:12:10: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.1 on Serial0/0/0 from
EXCHANGE to FULL, Exchange Done
```

Notice that the IOS displays a message when adjacency has been established with a state of Full.

Step 5: Use the `show ip ospf interface serial0/0/0` command to verify that the Hello Timer and Dead Timer intervals have been modified.

R2#show ip ospf interface serial0/0/0

Serial0/0/0 is up, line protocol is up

Internet address is 192.168.10.2/30, Area 0

Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost:

1562

Transmit Delay is 1 sec, State POINT-TO-POINT,

Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5

Hello due in 00:00:00

Index 3/3, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1 , Adjacent neighbor count is 1

Adjacent with neighbor 10.1.1.1

Suppress hello for 0 neighbor(s)

R2#

Step 6: Use the `show ip ospf neighbor` command on R1 to verify that the neighbor adjacency with R2 has been restored.

Notice that the Dead Time for Serial 0/0/0 is now much lower since it is counting down from 20 seconds instead of the default 40 seconds. Serial 0/0/1 is still operating with default timers.

R1#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address

Interface

10.2.2.2 0 FULL/- 00:00:19 192.168.10.2

Serial0/0/0

10.3.3.3 0 FULL/- 00:00:34 192.168.10.6

Serial0/0/1

R1#

Task 12: Document the Router Configurations.

On each router, capture the following command output to a text file and save for future reference:

- Running configuration
- Routing table
- Interface summarization
- Output from **`show ip protocols`**

Task 13: Clean Up.

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Critical Analysis/ Conclusion

Lab Assessment		
Pre Lab	**/5**	**/25**
Performance	**/5**	
Results	**/5**	
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		

LAB #08: VLAN Configuration

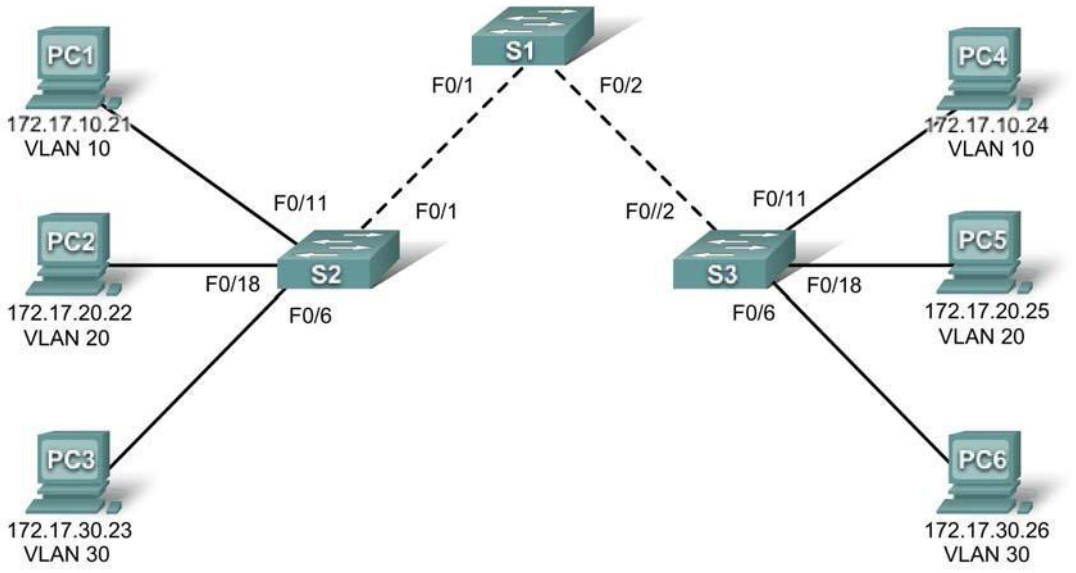


Figure 8. 1 Topology Diagram

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 99**	172.17.99.11	255.255.255.0	N/A
S2	**VLAN 99**	172.17.99.12	255.255.255.0	N/A
S3	**VLAN 99**	172.17.99.13	255.255.255.0	N/A
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.1
PC4	**NIC**	172.17.10.24	255.255.255.0	172.17.10.1
PC5	**NIC**	172.17.20.25	255.255.255.0	172.17.20.1
PC6	**NIC**	172.17.30.26	255.255.255.0	172.17.30.1

Table 8. 1 Addressing Table

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

Table 8. 2 Initial Port Assignments (Switches 2 and 3)

VLAN is a set of workstations within a LAN that can communicate with each other as though they were on a single, isolated LAN. A VLAN acts like an ordinary LAN, but connected devices don't have to be physically connected to the same segment.

In Virtual Local Area Network:-

1. Broadcast packets sent by one of the workstations will reach all the others in the VLAN.

2. Broadcasts sent by one of the workstations in the VLAN will not reach any workstations that are not in the VLAN.

3. Broadcasts sent by workstations that are not in the VLAN will never reach workstations that are in the VLAN.

4. The workstations can all communicate with each other without needing to go through a gateway. For example, IP connections would be established by ARPing for the destination IP and sending packets directly to the destination workstation-there would be no need to send packets to the IP gateway to be forwarded on.

In computer networking, virtual local area network, virtual LAN or VLAN is a concept of partitioning a physical network, so that distinct broadcast domains are created. This is usually achieved on switch or router level. Simpler devices only support partitioning on a port level (if at all), so sharing VLANs across devices requires running dedicated cabling for each VLAN. More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for various VLANs.

Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if not on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections. Most enterprise-level networks today use the concept of virtual LANs (VLAN). Without VLANs, a switch considers all interfaces on the switch to be in the same broadcast domain.

Types of VLANS

The two common approaches to assigning VLAN membership are as follows:

_ Static VLANs

_ Dynamic VLANs

Static VLANs are also referred to as port-based VLANs. Static VLAN assignments are created by assigning ports to a VLAN. As a device enters the network, the device automatically assumes the VLAN of the port. If the user changes ports and needs access to the same VLAN, the network administrator must manually make a port-to-VLAN assignment for the new connection.

Dynamic VLANs are created through the use of software. With a VLAN Management Policy Server (VMPS), an administrator can assign switch ports to VLANs dynamically based on information such as the source MAC address of the device connected to the port or the username

used to log onto that device. As a device enters the network, the switch queries a database for the VLAN membership of the port that device is connected to.

The purpose of VLANs

The basic reason for splitting a network into VLANs is to reduce congestion on a large LAN.

Initially LANs were very at all the workstations were connected to a single piece of coaxial cable, or to sets of chained hubs. In flat LAN, every packet that any device puts onto the wire gets sent to every other device on the LAN. As the number of workstations on the typical LAN gr ew, they started to become hopelessly congested; there were just too many collisions, because most of the time when a workstation tried to send a packet, it would find that the wire was already occupied by a packet sent by some other device.

Advantages of using VLANs

1. Performance:

Routers that forward data in software become a bottleneck as LAN data rates increase. Doing away

with the routers removes this bottleneck.

2. Formation of virtual workgroups:

Because workstations can be moved from one VLAN to another just by changing the configuration on switches, it is relatively easy to put all the people working together on a particular project all into a single VLAN. They can then more easily share files and resources with each other.

3. Greater flexibility:

If users move their desks, or just move around the place with their laptops, then, if the VLANs are

set up the right way, they can plug their PC in at the new location, and still be within the same

VLAN. This is much harder when a network is physically divided up by routers.

4. Ease of partitioning of resources:

If there are servers or other equipment to which the network administrator wishes to limit access,

then they can be put o_ into their own VLAN. Then users in other VLANs can be given access selectively.

5. VLANs help to reduce the cost.

PreLab Questions:

1. What is VLAN?

2. What are the advantages of VLAN over LAN?

3. What are the types of VLAN?

Learning Objectives

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

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a switch to the default state
- Perform basic configuration tasks on a switch
- Create VLANs
- Assign switch ports to a VLAN
- Add, move, and change ports
- Verify VLAN configuration
- Enable trunking on inter-switch connections
- Verify trunk configuration
- Save the VLAN configuration

Lab Task:

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current switch in your lab as long as it has the required interfaces shown in the topology. Note: If you use 2900 or 2950 switches, the outputs may appear different. Also, certain commands may be different or unavailable.

Step 2: Clear any existing configurations on the switches, and initialize all ports in the shutdown state.

If necessary, refer to Lab 2.5.1, Appendix 1, for the procedure to clear switch configurations.

It is a good practice to disable any unused ports on the switches by putting them in shutdown. Disable all ports on the switches:

```
Switch#config term

Switch(config)#interface range fa0/1-24

Switch(config-if-range)#shutdown

Switch(config-if-range)#interface range gi0/1-2

Switch(config-if-range)#shutdown
```

Task 2: Perform Basic Switch Configurations

Step 1: Configure the switches according to the following guidelines.

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 2: Re-enable the user ports on S2 and S3.

```
S2(config)#interface range fa0/6, fa0/11, fa0/18

S2(config-if-range)#switchport mode acces

S3(config)#interface range fa0/6, fa0/11, fa0/18

S3(config-if-range)#switchport mode access

S3(config-if-range)#no shutdown
```

Task 3: Configure and Activate Ethernet Interfaces

Step 1: Configure the PCs.

You can complete this lab using only two PCs by simply changing the IP addressing for the two PCs specific to a test you want to conduct. For example, if you want to test connectivity between PC1 and PC2, then configure the IP addresses for those PCs by referring to the addressing table at the beginning of the lab. Alternatively, you can configure all six PCs with the IP addresses and default gateways.

Task 4: Configure VLANs on the Switch

Step 1: Create VLANs on switch S1.

Use the **vlan** *vlan-id* command in global configuration mode to add a VLAN to switch S1. There are four VLANS configured for this lab: VLAN 10 (faculty/staff); VLAN 20 (students); VLAN 30 (guest); and VLAN 99 (management). After you create the VLAN, you will be in vlan configuration mode, where you can assign a name to the VLAN with the **name** *vlan name* command.

```
S1(config)#vlan 10
S1(config-vlan)#name faculty/staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#end
S1#
```

Step 2: Verify that the VLANs have been created on S1.

Use the **show vlan brief** command to verify that the VLANs have been created.

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
```

```
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
10   faculty/staff                      active
20   students                           active
30   guest                              active
99   management                         active
```

Step 3: Configure and name VLANs on switches S2 and S3.

Create and name VLANs 10, 20, 30, and 99 on S2 and S3 using the commands from Step 1. Verify the correct configuration with the **show vlan brief** command.

What ports are currently assigned to the four VLANs you have created?

_____

Step 4: Assign switch ports to VLANs on S2 and S3.

Refer to the port assignment table on page 1. Ports are assigned to VLANs in interface configuration mode, using the **switchport access vlan** *vlan-id* command. You can assign each port individually or you can use the **interface range** command to simplify this task, as shown here. The commands are shown for S3 only, but you should configure both S2 and S3 similarly. Save your configuration when done.

```
S3(config)#interface range fa0/6-10

S3(config-if-range)#switchport access vlan 30

S3(config-if-range)#interface range fa0/11-17

S3(config-if-range)#switchport access vlan 10

S3(config-if-range)#interface range fa0/18-24

S3(config-if-range)#switchport access vlan 20

S3(config-if-range)#end

S3#copy running-config startup-config

Destination filename [startup-config]? [enter] Building configuration...

[OK]
```

Step 5: Determine which ports have been added.

Use the **show vlan id** *vlan-number* command on S2 to see which ports are assigned to VLAN 10. Which ports are assigned to VLAN 10?

_____

Note: The **show vlan name** *vlan-name* displays the same output.

You can also view VLAN assignment information using the **show interfaces** *interface* **switchport**

command.

Step 6: Assign the management VLAN.

A management VLAN is any VLAN that you configure to access the management capabilities of a switch. VLAN 1 serves as the management VLAN if you did not specifically define another VLAN. You assign the management VLAN an IP address and subnet mask. A switch can be managed via HTTP, Telnet, SSH, or SNMP. Because the out-of-the-box configuration of a Cisco switch has VLAN 1 as the default VLAN, VLAN 1 is a bad choice as the management VLAN. You do not want an arbitrary user who is connecting to a switch to default to the management VLAN. Recall that you configured the management VLAN as VLAN 99 earlier in this lab.

From interface configuration mode, use the **ip address** command to assign the management IP address to the switches.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown
S3(config)#interface vlan 99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

host connected to a port assigned to VLAN 99 to connect to the switches. Because VLAN 99 is configured as the management VLAN, any ports assigned to this VLAN are considered management ports and should be secured to control which devices can connect to these ports.

Step 7: Configure trunking and the native VLAN for the trunking ports on all switches.

Trunks are connections between the switches that allow the switches to exchange information for all VLANS. By default, a trunk port belongs to all VLANs, as opposed to an access port, which can only belong to a single VLAN. If the switch supports both ISL and 802.1Q VLAN encapsulation,

the trunks must specify which method is being used. Because the 2960 switch only supports 802.1Q trunking, it is not specified in this lab.

A native VLAN is assigned to an 802.1Q trunk port. In the topology, the native VLAN is VLAN 99. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic) as well as traffic that does not come from a VLAN (untagged traffic). The 802.1Q trunk port places untagged traffic on the native VLAN. Untagged traffic is generated by a computer attached to a switch port that is configured with the native VLAN. One of the IEEE 802.1Q specifications for Native VLANs is to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. For the purposes of this lab, a native VLAN serves as a common identifier on opposing ends of a trunk link. It is a best practice to use a VLAN other than VLAN 1 as the native VLAN.

Use the **interface range** command in global configuration mode to simplify configuring trunking.

```
S1(config)#interface range fa0/1-5

S1(config-if-range)#switchport mode trunk

S1(config-if-range)#switchport trunk native vlan 99

S1(config-if-range)#no shutdown

S1(config-if-range)#end

S2(config)# interface range fa0/1-5

S2(config-if-range)#switchport mode trunk

S2(config-if-range)#switchport trunk native vlan 99

S2(config-if-range)#no shutdown

S2(config-if-range)#end

S3(config)# interface range fa0/1-5

S3(config-if-range)#switchport mode trunk

S3(config-if-range)#switchport trunk native vlan 99

S3(config-if-range)#no shutdown

S3(config-if-range)#end
```

Verify that the trunks have been configured with the **show interface trunk** command.

```
S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/2       on           802.1q         trunking      99

Port        Vlans allowed on trunk

Fa0/1       1-4094
```

Fa0/2 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1,10,20,30,99

Fa0/2 1,10,20,30,99

```
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,99
Fa0/2       1,10,20,30,99
```

Step 8: Verify that the switches can communicate.

From S1, ping the management address on both S2 and S3.

```
S1#ping 172.17.99.12

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2
seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9
ms

S1#ping 172.17.99.13

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.17.99.13, timeout is 2
seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1
ms
```

Step 9: Ping several hosts from PC2.

Ping from host PC2 to host PC1 (172.17.10.21). Is the ping attempt successful? ___

Ping from host PC2 to the switch VLAN 99 IP address 172.17.99.12. Is the ping attempt successful?

Because these hosts are on different subnets and in different VLANs, they cannot communicate without a Layer 3 device to route between the separate subnetworks.

Ping from host PC2 to host PC5. Is the ping attempt successful? ___

Because PC2 is in the same VLAN and the same subnet as PC5, the ping is successful

Step 10: Move PC1 into the same VLAN as PC2.

The port connected to PC2 (S2 Fa0/18) is assigned to VLAN 20, and the port connected to PC1 (S2 Fa0/11) is assigned to VLAN 10. Reassign the S2 Fa0/11 port to VLAN 20. You do not need to first remove a port from a VLAN to change its VLAN membership. After you reassign a port to a new VLAN, that port is automatically removed from its previous VLAN.

```
S2#configure terminal

Enter configuration commands, one per line.     End     with     CNTL/Z.
S2(config)#interface fastethernet 0/11

S2(config-if)#switchport access vlan 20

S2(config-if)#end
```

Ping from host PC2 to host PC1. Is the ping attempt successful? ___

Even though the ports used by PC1 and PC2 are in the same VLAN, they are still in different subnetworks, so they cannot communicate directly.

Step 11: Change the IP address and network on PC1.

Change the IP address on PC1 to 172.17.20.21. The subnet mask and default gateway can remain the same. Once again, ping from host PC2 to host PC1, using the newly assigned IP address.

Is the ping attempt successful? _____

Why was this attempt successful?_____

Task 5: Document the Switch Configurations

On each switch, capture the running configuration to a text file and save it for future reference.

Task 6: Clean Up

Erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Critical Analysis / Conclusion

Lab Assessment		
Pre Lab	**/5**	**/25**
Performance	**/5**	
Results	**/5**	
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		

Lab # 09:VTP Configuration

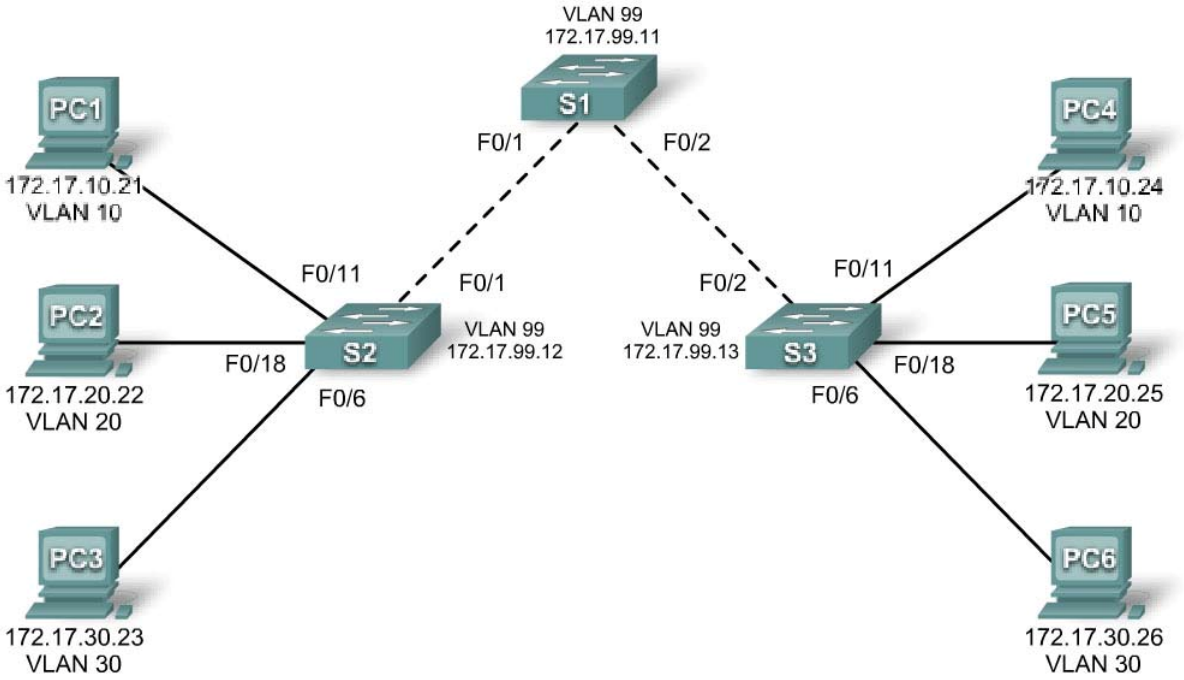


Figure 9. 1 Topology Diagram

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 99**	172.17.99.11	255.255.255.0	N/A
S2	**VLAN 99**	172.17.99.12	255.255.255.0	N/A
S3	**VLAN 99**	172.17.99.13	255.255.255.0	N/A
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.1
PC4	**NIC**	172.17.10.24	255.255.255.0	172.17.10.1
PC5	**NIC**	172.17.20.25	255.255.255.0	172.17.20.1
PC6	**NIC**	172.17.30.26	255.255.255.0	172.17.30.1

Table 9. 1Addressing Table

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

Table 9. 2 Port Assignments (Switches 2 and 3)

Learning Objectives

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

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a switch to the default state
- Perform basic configuration tasks on a switch
- Configure VLAN Trunking Protocol (VTP) on all switches
- Enable trunking on inter-switch connections
- Verify trunk configuration
- Modify VTP modes and observe the impact
- Create VLANs on the VTP server, and distribute this VLAN information to switches in the network
- Explain the differences in operation between VTP transparent mode, server mode, and client

Pre Lab

VLAN Trunking Protocol (VTP) is a Cisco proprietary protocol that propagates the definition of Virtual Local Area Networks (VLAN) on the whole local area network.[1] To do this, VTP carries VLAN information to all the switches in a VTP domain. VTP advertisements can be sent over ISL, 802.1Q, IEEE 802.10 and LANE trunks. VTP is available on most of the Cisco Catalyst Family products. Using VTP, each Catalyst Family Switch advertises the following on its trunk ports:

Management domain

Configuration revision number

Known VLANs and their specific parameters

There are three versions of VTP, namely version 1, version 2, version 3.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current switch in your lab as long as it has the required interfaces shown in the topology. The output shown in this lab is based on 2960 switches. Other switch types may produce

different output. If you are using older switches, then some commands may be different or unavailable.

You will notice in the Addressing Table that the PCs have been configured with a default gateway IP address. This would be the IP address of the local router which is not included in this lab scenario. The default gateway, the router would be needed for PCs in different VLANS to be able to communicate. This is discussed in a later chapter.

Set up console connections to all three switches.

Step 2: Clear any existing configurations on the switches.

If necessary, refer to Lab 2.5.1, Appendix 1, for the procedure to clear switch configurations and VLANs. Use the **show vlan** command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

Switch#show vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15,Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19,Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23,Fa0/24
                                                 Gig1/1, Gig1/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Step 3: Disable all ports by using the shutdown command.

Repeat these commands for each switch in the topology.

```
Switch(config)#interface range fa0/1-24

Switch(config-if-range)#shutdown

Switch(config-if-range)#interface range gi0/1-2

Switch(config-if-range)#shutdown
```

Task 2: Perform Basic Switch Configurations

Step 1: Complete basic configuration of switches S1, S2, and S3.

Configure the S1, S2, and S3 switches according to the following guidelines and save all your configurations:

- Configure the switch hostname as indicated on the topology.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections. (Output for S1 shown)

```
Switch>enable

Switch#configure terminal

Enter configuration commands, one per line.     End      with      CNTL/Z.
Switch(config)#hostname S1

S1(config)#enable    secret    class    S1(config)#no    ip    domain-lookup
S1(config)#line console 0

S1(config-line)#password cisco

S1(config-line)#login

S1(config-line)#line vty 0 15

S1(config-line)#password cisco

S1(config-line)#login

S1(config-line)#end

%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration... [OK]
```

Step 2: Re-enable the user ports on S2 and S3.

Configure the user ports in access mode. Refer to the topology diagram to determine which ports are connected to end-user devices.

```
S2(config)#interface fa0/6
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/11
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S3(config)#interface fa0/6
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
S3(config-if)#interface fa0/11
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
S3(config-if)#interface fa0/18
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
```

Step 3: Re-enable the trunk ports on S1, S2 and S3

```
S1(config)#interface fa0/1
S1(config-if)#no shutdown
S1(config)#interface fa0/2
S1(config-if)#no shutdown
S2(config)#interface fa0/1
S2(config-if)#no shutdown
S3(config)#interface fa0/2
S3(config-if)#no shutdown
```

Task 3: Configure the Ethernet Interfaces on the Host PCs

Configure the Ethernet interfaces of PC1, PC2, PC3, PC4, PC5, and PC6 with the IP addresses and default gateways indicated in the addressing table at the beginning of the lab.

Verify that PC1 can ping PC4, PC2 can ping PC5, and that PC3 can ping PC6.

Task 4: Configure VTP on the Switches

VTP allows the network administrator to control the instances of VLANs on the network by creating VTP domains. Within each VTP domain, one or more switches are configured as VTP servers. VLANs are then created on the VTP server and pushed to the other switches in the domain. Common VTP configuration tasks are setting the operating mode, domain, and password. In this lab, you will be using S1 as the VTP server, with S2 and S3 configured as VTP clients or in VTP transparent mode.

Step 1: Check the current VTP settings on the three switches.

```
S1#show vtp status

VTP Version : 2

Configuration Revision  : 0

Maximum VLANs supported locally : 255

Number of existing VLANs      : 5

VTP Operating Mode      : Server

VTP Domain Name   :

VTP Pruning Mode  : Disabled VTP V2 Mode  : Disabled VTP Traps Generation
      : Disabled

MD5 digest  : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD Configuration last
modified by 0.0.0.0 at 0-0-00 00:00:00

Local updater ID is 0.0.0.0 (no valid interface found)
```

```
S2#show vtp status

VTP Version :
Configuration Revision  :
Maximum VLANs supported
Number of existing VLANs
VTP Operating Mode      : Server

VTP Domain Name   :

VTP Pruning Mode  : Disabled VTP V2 Mode  : Disabled VTP Traps Generation
      : Disabled
```

```
MD5 digest  : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD Configuration last
modified by 0.0.0.0 at 0-0-00 00:00:00

Local updater ID is 0.0.0.0 (no valid interface found)
```

```
S3#show vtp status

VTP Version :
Configuration Revision  :
Maximum  VLANs  supported
Number  of  existing  VLANs
VTP Operating Mode      : Server

VTP Domain Name   :

VTP Pruning Mode  : Disabled VTP V2 Mode  : Disabled VTP Traps Generation
      : Disabled

MD5 digest  : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD Configuration last
modified by 0.0.0.0 at 0-0-00 00:00:00
```

Note that all three switches are in server mode. Server mode is the default VTP mode for most Catalyst switches.

Step 2: Configure the operating mode, domain name, and VTP password on all three switches.

Set the VTP domain name to **Lab4** and the VTP password to **cisco** on all three switches**.** Configure S1 in server mode, S2 in client mode, and S3 in transparent mode.

```
S1(config)#vtp mode server Device mode already VTP SERVER. S1(config)#vtp
domain Lab4

Changing VTP domain name from NULL to Lab4

S1(config)#vtp password cisco
```

Setting device VLAN database password to cisco

```
S1(config)#end

S2(config)#vtp mode client

Setting device to VTP CLIENT mode

S2(config)#vtp domain Lab4

Changing VTP domain name from NULL to Lab4

S2(config)#vtp password cisco

Setting device VLAN database password to cisco

S2(config)#end
```

```
S3(config)#vtp mode transparent

Setting device to VTP TRANSPARENT mode. S3(config)#vtp domain Lab4

Changing VTP domain name from NULL to Lab4

S3(config)#vtp password cisco

Setting device VLAN database password to cisco

S3(config)#end
```

Note: The VTP domain name can be learned by a client switch from a server switch, but only if the client switch domain is in the null state. It does not learn a new name if one has been previously set. For that reason, it is good practice to manually configure the domain name on all switches to ensure that the domain name is configured correctly. Switches in different VTP domains do not exchange VLAN information.

Step 3: Configure trunking and the native VLAN for the trunking ports on all three switches.

Use the **interface range** command in global configuration mode to simplify this task.

```
S1(config)#interface range fa0/1-5

S1(config-if-range)#switchport mode trunk

S1(config-if-range)#switchport trunk native vlan 99

S1(config-if-range)#no shutdown

S1(config-if-range)#end

S2(config)# interface range fa0/1-5

S2(config-if-range)#switchport mode trunk

S2(config-if-range)#switchport trunk native vlan 99

S2(config-if-range)#no shutdown

S2(config-if-range)#end

S3(config)# interface range fa0/1-5

S3(config-if-range)#switchport mode trunk

S3(config-if-range)#switchport trunk native vlan 99

S3(config-if-range)#no shutdown

S3(config-if-range)#end
```

Step 4: Configure port security on the S2 and S3 access layer switches.

Configure ports fa0/6, fa0/11, and fa0/18 so that they allow only a single host and learn the MAC address of the host dynamically.

```
S2(config)#interface fa0/6
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/11
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#end
S3(config)#interface fa0/6
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/11
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/18
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#end
```

Step 5: Configure VLANs on the VTP server.

There are four additional VLANS required in this lab:

- VLAN 99 (management)
- VLAN 10 (faculty/staff)
- VLAN 20 (students)
- VLAN 30 (guest)

Configure these on the VTP server.

```
S1(config)#vlan 99

S1(config-vlan)#name management S1(config-vlan)#exit S1(config)#vlan 10

S1(config-vlan)#name  faculty/staff  S1(config-vlan)#exit  S1(config)#vlan
20

S1(config-vlan)#name students

S1(config-vlan)#exit

S1(config)#vlan 30

S1(config-vlan)#name guest

S1(config-vlan)#exit
```

Verify that the VLANs have been created on S1 with the **show vlan brief** command.

Step 6: Check if the VLANs created on S1 have been distributed to S2 and S3.

Use the **show vlan brief** command on S2 and S3 to determine if the VTP server has pushed its VLAN configuration to all the switches.

```
S2#show vlan brief

VLAN Name   Status      Ports

---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12,Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16,Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20,Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
10   faculty/staff                    active
20   students                         active
30   guest                            active
99   management                       active
```

```
S3#show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12,Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16,Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20,Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Are the same VLANs configured on all switches? _____

Explain why S2 and S3 have different VLAN configurations at this point. _

_____

_____

Step 7: Create a new VLAN on switch 2 and 3.

```
S2(config)#vlan 88

%VTP VLAN configuration not allowed when device is in CLIENT mode.

S3(config)#vlan 88

S3(config-vlan)#name test

S3(config-vlan)#
```

Why are you prevented from creating a new VLAN on S2 but not S3? _____

_____

Delete VLAN 88 from S3.

```
S3(config)#no vlan 88
```

Step 8: Manually configure VLANs.

Configure the four VLANs identified in Step 5 on switch S3.

```
S3(config)#vlan 99

S3(config-vlan)#name management S3(config-vlan)#exit S3(config)#vlan 10

S3(config-vlan)#name  faculty/staff  S3(config-vlan)#exit  S3(config)#vlan
20

S3(config-vlan)#name students S3(config-vlan)#exit S3(config)#vlan 30

S3(config-vlan)#name guest
```

```
S3(config-vlan)#exit
```

Here you see one of the advantages of VTP. Manual configuration is tedious and error prone, and any error introduced here could prevent intra-VLAN communication. In addition, these types of errors can be difficult to troubleshoot.

Step 9: Configure the management interface address on all three switches.

```
S1(config)#interface vlan 99

S1(config-if)#ip address 172.17.99.11 255.255.255.0

S1(config-if)#no shutdown

S2(config)#interface vlan 99

S2(config-if)#ip address 172.17.99.12 255.255.255.0

S2(config-if)#no shutdown

S3(config)#interface vlan 99

S3(config-if)#ip address 172.17.99.13 255.255.255.0

S3(config-if)#no shutdown
```

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Were the pings successful? _____

If not, troubleshoot the switch configurations and try again.

Step 10: Assign switch ports to VLANs.

Refer to the port assignment table at the beginning of the lab to assign ports to the VLANs. Use the **interface range** command to simplify this task. Port assignments are not configured through VTP. Port assignments must be configured on each switch manually or dynamically using a VMPS server. The commands are shown for S3 only, but both S2 and S1 switches should be similarly configured. Save the configuration when you are done.

```
S3(config)#interface range fa0/6-10

S3(config-if-range)#switchport access vlan 30

S3(config-if-range)#interface range fa0/11-17

S3(config-if-range)#switchport access vlan 10

S3(config-if-range)#interface range fa0/18-24
```

```
S3(config-if-range)#switchport access vlan 20

S3(config-if-range)#end

S3#copy running-config startup-config

Destination filename [startup-config]? [enter] Building configuration...

[OK]

S3#
```

Task 5: Configure VTP Pruning on the Switches

VTP pruning allows a VTP server to suppress IP broadcast traffic for specific VLANs to switches that do not have any ports in that VLAN. By default, all unknown unicasts and broadcasts in a VLAN are flooded over the entire VLAN. All switches in the network receive all broadcasts, even in situations in which few users are connected in that VLAN. VTP pruning is used to eliminate or prune this unnecessary traffic. Pruning saves LAN bandwidth because broadcasts do not have to be sent to switches that do not need them.

Pruning is configured on the server switch with the **vtp pruning** command in global configuration mode. The configuration is pushed to client switches.

Confirm VTP pruning configuration on each switch using the **show vtp status** command. VTP pruning mode should be enabled on each switch.

```
S1#show vtp status

VTP Version : 2

Configuration Revision  : 17

Maximum VLANs supported locally : 255

Number of existing VLANs      : 9

VTP Operating Mode      : Server

VTP Domain Name   : Lab4

VTP Pruning Mode  : Enabled

<output omitted>
```

Task 6: Clean Up

Erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Critical Analysis/Conclusion

Lab Assessment		
Pre Lab	**/5**	**/25**
Performance	**/5**	
Results	**/5**	
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		

Lab # 10: DHCP Configuration

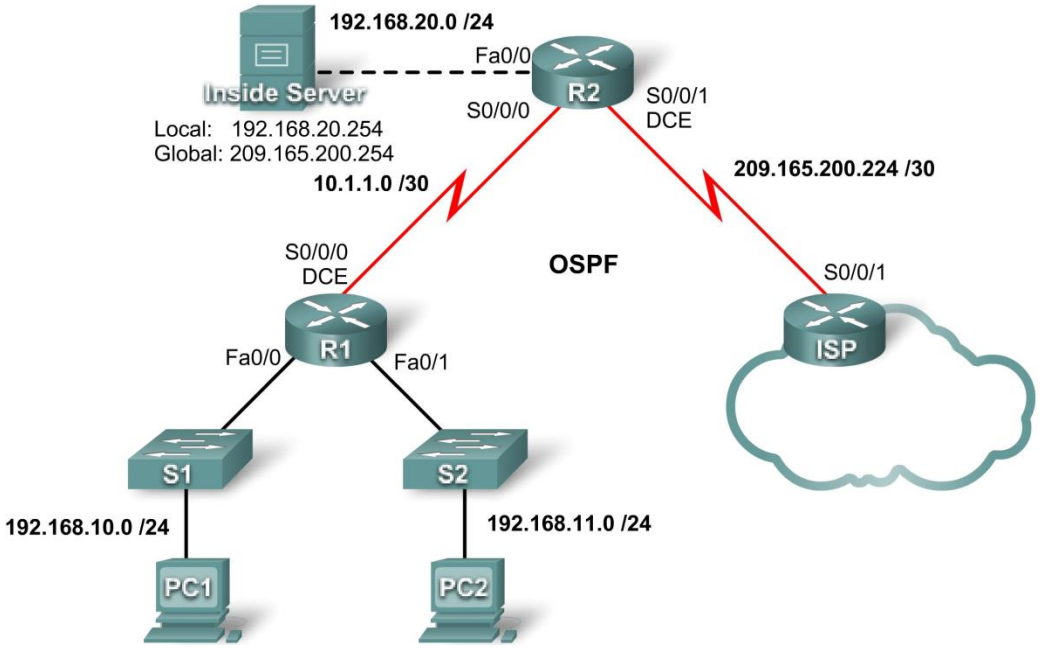


Figure 10. 1 Topology Diagram

Device	Interface	IP Address	Subnet Mask
R1	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	209.165.200.225	255.255.255.252
	Fa0/0	192.168.20.1	255.255.255.0
ISP	S0/0/1	209.165.200.226	255.255.255.252

Table 10. 1 Addressing Table

Learning Objectives

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

- Prepare the network.
- Perform basic router configurations.
- Configure a Cisco IOS DHCP server.
- Configure static and default routing.
- Configure static NAT.

- Configure dynamic NAT with a pool of addresses
- Configure NAT overload.

Scenario

In this lab, you will configure the DHCP and NAT IP services. One router is the DHCP server. The other router forwards DHCP requests to the server. You will also configure both static and dynamic NAT configurations, including NAT overload. When you have completed the configurations, verify the connectivity between the inside and outside addresses.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology. Note: If you use a 1700, 2500, or 2600 series router, the router outputs and interface descriptions may look different. On older routers some commands may be different, or not exist.

Step 2: Clear all existing configurations on the routers.

Task 2: Perform Basic Router Configurations

Configure the R1, R2, and ISP routers according to the following guidelines:

- Configure the device hostname.
- Disable DNS lookup.
- Configure a privileged EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for the console connections.
- Configure a password for all vty connections.
- Configure IP addresses on all routers. The PCs receive IP addressing from DHCP later in the lab.
- Enable OSPF with process ID 1 on R1 and R2. Do not advertise the 209.165.200.224/27 network.

Note: Instead of attaching a server to R2, you can configure a loopback interface on R2 to use the IP address 192.168.20.254/24. If you do this, you do not need to configure the Fast Ethernet interface.

Pre Lab

The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

Task 3: Configure PC1 and PC2 to receive an IP address through DHCP

On a Windows PC go to Start -> Control Panel -> Network Connections -> Local Area Connection. Right mouse click on the Local Area Connection and select Properties.

Figure 10. 2

Scroll down and highlight **Internet Protocol (TCP/IP)**. Click on the **Properties** button.

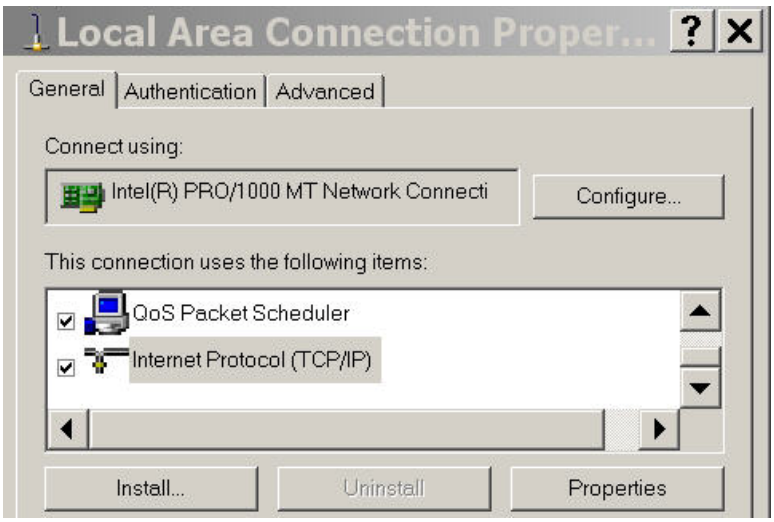


Figure 10. 3

Make sure the button is selected that says **Obtain an IP address automatically**.

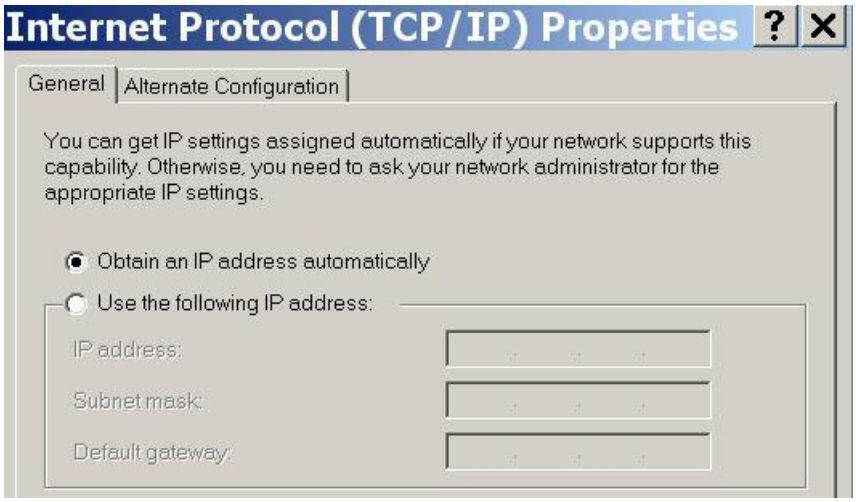


Figure 10. 4

Once this has been done on both PC1 and PC2, they are ready to receive an IP address from a DHCP server.

Task 4: Configure a Cisco IOS DHCP Server

Cisco IOS software supports a DHCP server configuration called Easy IP. The goal for this lab is to have devices on the networks 192.168.10.0/24 and 192.168.11.0/24 request IP addresses via DHCP from R2.

Step 1: Exclude statically assigned addresses.

The DHCP server assumes that all IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients. You must specify the IP addresses that the DHCP server should not assign to clients. These IP addresses are usually static addresses reserved for the router interface, switch management IP address, servers, and local network printer. The **ip dhcp excluded-address** command prevents the router from assigning IP addresses within the configured range. The following commands exclude the first 10 IP addresses from each pool for the LANs attached to R1. These addresses will not be assigned to any DHCP clients.

```
R2(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10

R2(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
```

Step 2: Configure the pool.

Create the DHCP pool using the **ip dhcp pool** command and name it **R1Fa0**.

```
R2(config)#ip dhcp pool R1Fa0
```

Specify the subnet to use when assigning IP addresses. DHCP pools automatically associate with an interface based on the network statement. The router now acts as a DHCP server, handing out addresses in the 192.168.10.0/24 subnet starting with 192.168.10.1.

```
R2(dhcp-config)#network 192.168.10.0 255.255.255.0
```

Configure the default router and domain name server for the network. Clients receive these settings via DHCP, along with an IP address.

```
R2(dhcp-config)#dns-server 192.168.11.5

R2(dhcp-config)#default-router 192.168.10.1
```

Note: There is not a DNS server at 192.168.11.5. You are configuring the command for practice only. Because devices from the network 192.168.11.0/24 also request addresses from R2, a separate pool must be created to serve devices on that network. The commands are similar to the commands shown above:

```
R2(config)#ip dhcp pool R1Fa1

R2(dhcp-config)#network 192.168.11.0 255.255.255.0

R2(dhcp-config)#dns-server 192.168.11.5

R2(dhcp-config)#default-router 192.168.11.1
```

Step 3: Test DHCP

On PC1 and PC2 test whether each has received an IP address automatically. On each PC go to **Start** - > **Run** -> **cmd** -> **ipconfig**

Figure 10. 5

Why are these the results? _____

Step 4: Configure a helper address.

Network services such as DHCP rely on Layer 2 broadcasts to function. When the devices providing these services exist on a different subnet than the clients, they cannot receive the broadcast packets. Because the DHCP server and the DHCP clients are not on the same subnet, configure R1 to forward DHCP broadcasts to R2, which is the DHCP server, using the **ip helper-address** interface configuration command.

Notice that **ip helper-address** must be configured on each interface involved.

```
R1(config)#interface fa0/0

R1(config-if)#ip helper-address 10.1.1.2

R1(config)#interface fa0/1

R1(config-if)#ip helper-address 10.1.1.2
```

Step 5: Release and Renew the IP addresses on PC1 and PC2

Depending upon whether your PCs have been used in a different lab, or connected to the internet, they may already have learned an IP address automatically from a different DHCP server. We need to clear this IP address using the **ipconfig /release** and **ipconfig /renew** commands.

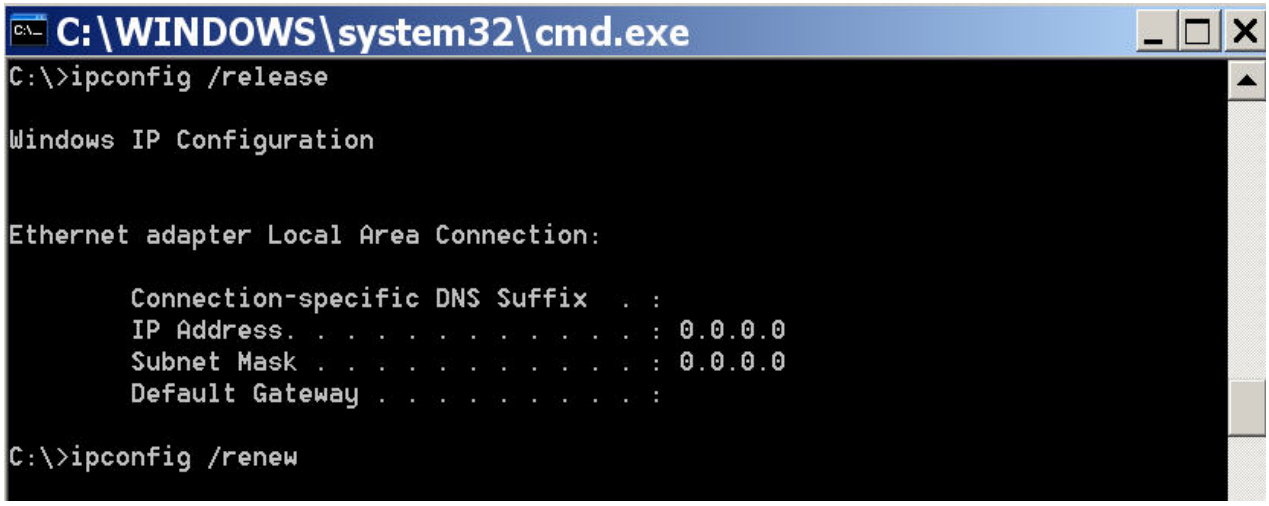


Figure 10. 6

Step 6: Verify the DHCP configuration.

You can verify the DHCP server configuration in several different ways. Issue the command **ipconfig** on PC1 and PC2 to verify that they have now received an IP address dynamically. You can then issue commands on the router to get more information. The **show ip dhcp binding** command provides information on all currently assigned DHCP addresses. For instance, the following output shows that the IP address 192.168.10.11 has been assigned to MAC address 3031.632e.3537.6563. The IP lease expires on September 14, 2007 at 7:33 p.m.

```
R1#show ip dhcp binding

Bindings from all pools not associated with VRF:

IP address  Client-ID/  Lease expiration  Type

Hardware address/ User name

192.168.10.11     0063.6973.636f.2d30.    Sep    14    2007    07:33    PM
      Automatic
```

```
3031.632e.3537.6563.

2e30.3634.302d.566c.
```

The **show ip dhcp pool** command displays information on all currently configured DHCP pools on the router. In this output, the pool **R1Fa0** is configured on R1. One address has been leased from this pool. The next client to request an address will receive 192.168.10.12.

```
R2#show ip dhcp pool

Pool R1Fa0 :

Utilization mark (high/low)    : 100 / 0

Subnet size (first/next)       : 0 / 0

Total addresses    : 254

Leased addresses   : 1

Pending event      : none

1 subnet is currently in the pool :

Current index      IP address range   Leased addresses

192.168.10.12      192.168.10.1       - 192.168.10.254   1
```

The **debug ip dhcp server events** command can be extremely useful when troubleshooting DHCP leases with a Cisco IOS DHCP server. The following is the debug output on R1 after connecting a host. Notice that the highlighted portion shows DHCP giving the client an address of 192.168.10.12 and mask of 255.255.255.0

```
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:

*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640

*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80b01010000000000

*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000

*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified
pool class:

*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640

*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80b01010000000000

*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000

*Sep 13 21:04:18.072: DHCPD: there is no address pool for 192.168.11.1.

*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER: R1#

*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
```

```
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80a01000000000000

*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000

*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified
pool class:

*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640

*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80a01000000000000

*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000

R1#

*Sep 13 21:04:20.072: DHCPD: Adding binding to radix tree (192.168.10.12)

*Sep 13 21:04:20.072: DHCPD: Adding binding to hash tree

*Sep 13 21:04:20.072: DHCPD: assigned IP address 192.168.10.12 to client

0063.6973.636f.2d30.3031.632e.3537.6563.2e30.3634.302d.566c.31.

*Sep 13 21:04:20.072: DHCPD: Sending notification of ASSIGNMENT:

*Sep 13 21:04:20.072:   DHCPD: address 192.168.10.12 mask 255.255.255.0

*Sep 13 21:04:20.072:   DHCPD: htype 1 chaddr 001c.57ec.0640

*Sep 13 21:04:20.072:   DHCPD: lease time remaining (secs) = 86400

*Sep 13 21:04:20.076: DHCPD: Sending notification of ASSIGNMENT:

*Sep 13 21:04:20.076:   DHCPD: address 192.168.10.12 mask 255.255.255.0

R1#

*Sep 13 21:04:20.076:   DHCPD: htype 1 chaddr 001c.57ec.0640

*Sep 13 21:04:20.076:   DHCPD: lease time remaining (secs) = 86400
```

Task 5: Configure Static and Default Routing

ISP uses static routing to reach all networks beyond R2. However, R2 translates private addresses into public addresses before sending traffic to ISP. Therefore, ISP must be configured with the public addresses that are part of the NAT configuration on R2. Enter the following static route on ISP:

```
ISP(config)#ip route 209.165.200.240 255.255.255.240 serial 0/0/1
```

This static route includes all addresses assigned to R2 for public use. Configure a default route on R2 and propagate the route in OSPF.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
```

```
R2(config)#router ospf 1

R2(config-router)#default-information originate
```

Allow a few seconds for R1 to learn the default route from R2 and then check the R1 routing table. Alternatively, you can clear the routing table with the **clear ip route** * command. A default route pointing to R2 should appear in the R1 routing table. Note that the static route that is configured on the ISP only routes to the public addresses that the R1 hosts will use after NAT is configured on R2. Until NAT is configured, the static route will lead to an unknown network, causing the pings from R1 to fail.

Critical Analysis/Conclusion

Lab Assessment		
Pre Lab	**/5**	**/25**
Performance	**/5**	
Results	**/5**	
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		

Lab # 11: NAT Configuration

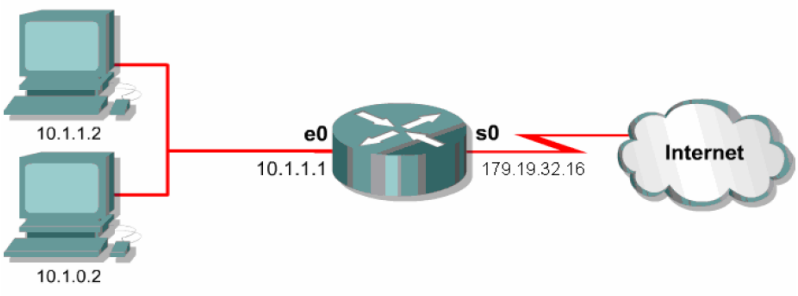


Figure11. 1

Pre Lab

Network address translation (NAT) is a methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. The technique was originally used for ease of rerouting traffic in IP networks without renumbering every host. It has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion by sharing one Internet-routable IP address of a NAT gateway for an entire private network.

Task 1: Configure Static NAT

Step 1: Statically map a public IP address to a private IP address.

The inside server attached to R2 is accessible by outside hosts beyond ISP. Statically assign the public IP address 209.165.200.254 as the address for NAT to use to map packets to the private IP address of the inside server at 192.168.20.254.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
```

Step 2: Specify inside and outside NAT interfaces.

Before NAT can work, you must specify which interfaces are inside and which interfaces are outside.

```
R2(config)#interface serial 0/0/1

R2(config-if)#ip nat outside

R2(config-if)#interface fa0/0

R2(config-if)#ip nat inside
```

Note: If using a simulated inside server, assign the **ip nat inside** command to the loopback interface.

Step 3: Verify the static NAT configuration.

From ISP, ping the public IP address 209.165.200.254.

Task 2: Configure Dynamic NAT with a Pool of Addresses

While static NAT provides a permanent mapping between an internal address and a specific public address, dynamic NAT maps private IP addresses to public addresses. These public IP addresses come from a NAT pool.

Step 1: Define a pool of global addresses.

Create a pool of addresses to which matched source addresses are translated. The following command creates a pool named MY-NAT-POOL that translates matched addresses to an available IP address in the 209.165.200.241–209.165.200.246 range.

```
R2(config)#ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246
netmask 255.255.255.248
```

Step 2: Create an extended access control list to identify which inside addresses are translated.

```
R2(config)#ip access-list extended NAT

R2(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any

R2(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

Step 3: Establish dynamic source translation by binding the pool with the access control list.

A router can have more than one NAT pool and more than one ACL. The following command tells the router which address pool to use to translate hosts that are allowed by the ACL.

```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL
```

Step 4: Specify inside and outside NAT interfaces.

You have already specified the inside and outside interfaces for your static NAT configuration. Now add the serial interface linked to R1 as an inside interface.

```
R2(config)#interface serial 0/0/0

R2(config-if)#ip nat inside
```

Step 5: Verify the configuration.

Ping ISP from PC1 or the Fast Ethernet interface on R1 using extended **ping**. Then use the **show ip nat translations** and **show ip nat statistics** commands on R2 to verify NAT.

```
R2#show ip nat translations
```

Pro Inside global	Inside local	Outside local	Outside global
icmp 209.165.200.	192.168.10.1:4	209.165.200.226:4	209.165.200.226:
--- 209.165.200.2	192.168.10.1	---	---
--- 209.165.200.2	192.168.20.254	---	---

```
R2#show ip nat statistics

Total active translations: 2 (1 static, 1 dynamic; 0 extended) Outside
interfaces:

Serial0/0/1

Inside interfaces:

Serial0/0/0, Loopback0

Hits: 23    Misses: 3

CEF Translated packets: 18, CEF Punted packets: 0

Expired translations: 3

Dynamic mappings:

-- Inside Source

[Id: 1] access-list NAT pool MY-NAT-POOL refcount 1 pool MY-NAT-POOL:
netmask 255.255.255.248

start 209.165.200.241 end 209.165.200.246

type generic, total addresses 6, allocated 1 (16%), misses 0

Queued Packets: 0
```

To troubleshoot issues with NAT, you can use the **debug ip nat** command. Turn on NAT debugging and repeat the ping from PC1.

```
R2#debug ip nat

IP NAT debugging is on

R2#
```

```
*Sep    13    21:15:02.215:    NAT*:    s=192.168.10.11->209.165.200.241,
d=209.165.200.226 [25]

*Sep   13   21:15:02.231:   NAT*:   s=209.165.200.226,   d=209.165.200.241-
>192.168.10.11 [25]

*Sep    13    21:15:02.247:    NAT*:    s=192.168.10.11->209.165.200.241,
d=209.165.200.226 [26]

*Sep   13   21:15:02.263:   NAT*:   s=209.165.200.226,   d=209.165.200.241-
>192.168.10.11 [26]

*Sep    13    21:15:02.275:    NAT*:    s=192.168.10.11->209.165.200.241,
d=209.165.200.226 [27]

*Sep   13   21:15:02.291:   NAT*:   s=209.165.200.226,   d=209.165.200.241-
>192.168.10.11 [27]

*Sep    13    21:15:02.307:    NAT*:    s=192.168.10.11->209.165.200.241,
d=209.165.200.226 [28]

*Sep   13   21:15:02.323:   NAT*:   s=209.165.200.226,   d=209.165.200.241-
>192.168.10.11 [28]

*Sep    13    21:15:02.335:    NAT*:    s=192.168.10.11->209.165.200.241,
d=209.165.200.226 [29]

*Sep   13   21:15:02.351:   NAT*:   s=209.165.200.226,   d=209.165.200.241-
>192.168.10.11 [29] R2#
```

Task 3: Configure NAT Overload

In the previous example, what would happen if you needed more than the six public IP addresses that the pool allows?

_____

By tracking port numbers, NAT overloading allows multiple inside users to reuse a public IP address.

In this task, you will remove the pool and mapping statement configured in the previous task. Then you will configure NAT overload on R2 so that all internal IP addresses are translated to the R2 S0/0/1 address when connecting to any outside device.

Step 1: Remove the NAT pool and mapping statement.

Use the following commands to remove the NAT pool and the map to the NAT ACL.

```
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL

R2(config)#no  ip  nat  pool  MY-NAT-POOL  209.165.200.241  209.165.200.246
netmask 255.255.255.248
```

If you receive the following message, clear your NAT translations.

```
%Pool MY-NAT-POOL in use, cannot destroy

R2#clear ip nat translation *
```

Step 2: Configure PAT on R2 using the serial 0/0/1 interface public IP address.

The configuration is similar to dynamic NAT, except that instead of a pool of addresses, the **interface** keyword is used to identify the outside IP address. Therefore, no NAT pool is defined. The **overload** keyword enables the addition of the port number to the translation.

Because you already configured an ACL to identify which inside IP addresses to translate as well as which interfaces are inside and outside, you only need to configure the following:

```
R2(config)#ip nat inside source list NAT interface S0/0/1 overload
```

Step 3: Verify the configuration.

Ping ISP from PC1 or the Fast Ethernet interface on R1 using extended **ping**. Then use the **show ip nat translations** and **show ip nat statistics** commands on R2 to verify NAT.

```
R2#show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
icmp	192.168.10.11:6	209.165.200.226:6	209.165.200.226:	
---	209.165.200.254	192.168.20.254	---	---

```
R2#show ip nat statistics

Total active translations: 2 (1 static, 1 dynamic; 1 extended) Outside
interfaces:

Serial0/0/1

Inside interfaces:

Serial0/0/0, Loopback0

Hits: 48    Misses: 6

CEF Translated packets: 46, CEF Punted packets: 0

Expired translations: 5

Dynamic mappings:

-- Inside Source

[Id: 2] access-list NAT interface Serial0/0/1 refcount 1

Queued Packets: 0
```

Note: In the previous task, you could have added the keyword **overload** to the **ip nat inside source list NAT pool MY-NAT-POOL** command to allow for more than six concurrent users.

Task 4: Document the Network

```
On each router, issue the show run command and capture the configurations. R1#show run

<output omitted>

!

hostname R1

!

enable secret class

!

no ip domain lookup

!

interface FastEthernet0/0

ip address 192.168.10.1 255.255.255.0 ip helper-address 10.1.1.2

no shutdown

!

interface FastEthernet0/1

ip address 192.168.11.1 255.255.255.0 ip helper-address 10.1.1.2

no shutdown

!

interface Serial0/0/0

ip address 10.1.1.1 255.255.255.252 clock rate 125000

!

interface Serial0/0/1 no ip address shutdown

!

router ospf 1

network 10.1.1.0 0.0.0.3 area 0

network 192.168.10.0 0.0.0.255 area 0 network 192.168.11.0 0.0.0.255 area 0
```

```
!
!
banner motd ^C
**********************************
!!!AUTHORIZED ACCESS ONLY!!!
**********************************
^C
!
line con 0
exec-timeout 0 0 password cisco logging synchronous login
line aux 0
exec-timeout 0 0 password cisco logging synchronous
login
line vty 0 4
exec-timeout 0 0 password cisco logging synchronous login
!
end


R2#show run
!
hostname R2
!
!
enable secret class
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.10.1 192.168.10.10 ip dhcp excluded-
address 192.168.11.1 192.168.11.10
!
ip dhcp pool R1Fa0
```

```
network 192.168.10.0 255.255.255.0 default-router 192.168.10.1
dns-server 192.168.11.5
!
ip dhcp pool R1Fa1
network 192.168.11.0 255.255.255.0 dns-server 192.168.11.5
default-router 192.168.11.1
!
no ip domain lookup
!
interface Loopback0
ip address 192.168.20.254 255.255.255.0 ip nat inside
ip virtual-reassembly
!
!
!
interface Serial0/0/0
ip address 10.1.1.2 255.255.255.252 ip nat inside
ip virtual-reassembly
!
interface Serial0/0/1
ip address 209.165.200.225 255.255.255.252 ip nat outside
ip virtual-reassembly
clock rate 125000
!
router ospf 1
network 10.1.1.0 0.0.0.3 area 0
network 192.168.20.0 0.0.0.255 area 0 default-information originate
!
ip route 0.0.0.0 0.0.0.0 209.165.200.226
```

```
!
!
no ip http server
no ip http secure-server
ip nat inside source list NAT interface Serial0/0/1 overload ip nat
inside source static 192.168.20.254 209.165.200.254
!
ip access-list extended NAT
permit ip 192.168.10.0 0.0.0.255 any permit ip 192.168.11.0 0.0.0.255 any
!
!
banner motd ^C
**********************************
!!!AUTHORIZED ACCESS ONLY!!!
**********************************
^C
!
line con 0
exec-timeout 0 0 password cisco logging synchronous login
line aux 0
exec-timeout 0 0 password cisco logging synchronous login
line vty 0 4
exec-timeout 0 0 password cisco logging synchronous login
!
end
ISP#show run
<output omitted>
!
hostname ISP
!
```

```
enable secret class
!
no ip domain lookup
!
interface Serial0/0/1
ip address 209.165.200.226 255.255.255.252 no shutdown
!
!
!
ip route 209.165.200.240 255.255.255.240 Serial0/0/1
!
banner motd ^C
**********************************
!!!AUTHORIZED ACCESS ONLY!!!
**********************************
^C
!
line con 0
exec-timeout 0 0 password cisco logging synchronous login
line aux 0
exec-timeout 0 0 password cisco logging synchronous
login
line vty 0 4 password cisco logging synchronous login
!
end
```

Task 5: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Critical Analysis / Conclusion

Lab Assessment		
Pre Lab	**/5**	**/25**
Performance	**/5**	
Results	**/5**	
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		

Lab # 12:Access Control List Configuration

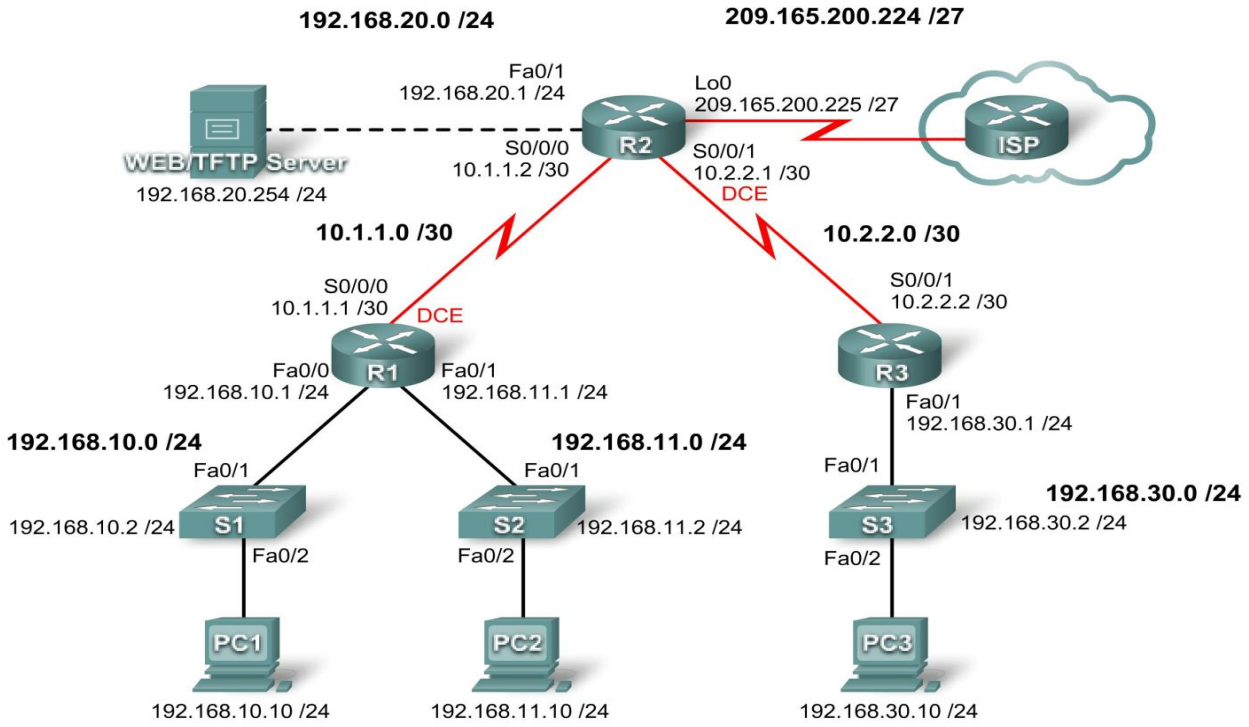


Figure12. 1 Topology Diagram

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.1	255.255.255.0	N/A
	Fa0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	Fa0/1	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	Fa0/1	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
S1	Vlan1	192.168.10.2	255.255.255.0	192.168.10.1
S2	Vlan1	192.168.11.2	255.255.255.0	192.168.11.1
S3	Vlan1	192.168.30.2	255.255.255.0	192.168.30.1
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
Web Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Table 12. 1 Addressing Table

1. Objectives

Scenario

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

- Design named standard and named extended ACLs.
- Apply named standard and named extended ACLs.
- Test named standard and named extended ACLs.
- Troubleshoot named standard and named extended ACLs.

In this lab, you will learn how to configure basic network security using Access Control Lists. You will apply both standard and extended ACLs.

2. Pre Lab

An access control list (ACL): basic traffic filtering capabilities.

Cisco provides basic traffic filtering capabilities with access control lists (also referred to as access lists). Access lists can be configured for all routed network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a router.

You can configure access lists at your router to control access to a network: access lists can prevent certain traffic from entering or exiting a network.

an access control list refers to rules that are applied to port numbers or IP addresses that are available on a host or other layer 3, each with a list of hosts and/or networks permitted to use the service.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology diagram.

Note: This lab was developed and tested using 1841 routers. If you use 1700, 2500, or 2600 series routers, the router outputs and interface descriptions might be different. On older routers, or versions of the IOS before 12.4, some commands may be different or non-existent.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations

Configure the R1, R2, R3, S1, S2, and S3 routers and switches according to the following guidelines:

- Configure the router hostname to match the topology diagram.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a message-of-the-day banner.
- Configure a password of cisco for console connections.
- Configure a password for VTY connections.
- Configure IP addresses and masks on all devices.
- Enable OSPF area 0 with a process ID of 1 on all routers for all networks.
- Configure a loopback interface on R2 to simulate the ISP.
- Configure IP addresses and masks on all devices.
- Enable OSPF area 0 with a process ID of 1 on all routers for all networks.
- Configure a loopback interface on R2 to simulate the ISP.

Task 3: Configuring a Standard ACL

Standard ACLs can filter traffic based on source IP address only. A typical best practice is to configure a standard ACL as close to the destination as possible. In this task, you are configuring a standard ACL. The ACL is designed to block traffic from the 192.168.11.0/24 network located in a student lab from accessing any local networks on R3.

This ACL will be applied inbound on the R3 serial interface. Remember that every ACL has an implicit “deny all” that causes all traffic that has not matched a statement in the ACL to be blocked. For this reason, add the **permit any** statement to the end of the ACL.

Before configuring and applying this ACL, be sure to test connectivity from PC1 (or the Fa0/1 interface on R1) to PC3 (or the Fa0/1 interface on R3). Connectivity tests should be successful before applying the ACL.

Step 1: Create the ACL on router R3.

In global configuration mode, create a standard named ACL called **STND-1**.

```
R3(config)#ip access-list standard STND-1
```

In standard ACL configuration mode, add a statement that denies any packets with a source address of 192.168.11.0/24 and prints a message to the console for each matched packet.

```
R3(config-std-nacl)#deny 192.168.11.0 0.0.0.255 log
```

Permit all other traffic.

```
R3(config-std-nacl)#permit any
```

Step 2: Apply the ACL.

Apply the ACL **STND-1** as a filter on packets entering R3 through Serial interface 0/0/1.

```
R3(config)#interface serial 0/0/1

R3(config-if)#ip access-group STND-1 in

R3(config-if)#end

R3#copy run start
```

Step 3: Test the ACL.

Before testing the ACL, make sure that the console of R3 is visible. This will allow you to see the access list log messages when the packet is denied.

Test the ACL by pinging from PC2 to PC3. Since the ACL is designed to block traffic with source addresses from the 192.168.11.0/24 network, PC2 (192.168.11.10) should not be able to ping PC3.

You can also use an extended ping from the Fa0/1 interface on R1 to the Fa0/1 interface on R3.

```
R1#ping ip

Target IP address: 192.168.30.1

Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended
commands [n]: y

Source address or interface: 192.168.11.1
```

Type of service [0]:

Set DF bit in IP header? [no]: Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds: Packet sent with a source address of 192.168.11.1

U.U.U

Success rate is 0 percent (0/5)

You should see the following message on the R3 console:

```
*Sep  4 03:22:58.935: %SEC-6-IPACCESSLOGNP: list STND-1 denied 0

0.0.0.0 -> 192.168.11.1, 1 packet
```

In privileged EXEC mode on R3, issue the **show access-lists** command. You see output similar to the following. Each line of an ACL has an associated counter showing how many packets have matched the rule.

Standard IP access list STND-1

```
10 deny     192.168.11.0, wildcard bits 0.0.0.255 log (5 matches)

20 permit any (25 matches)
```

The purpose of this ACL was to block hosts from the 192.168.11.0/24 network. Any other hosts, such as those on the 192.168.10.0/24 network should be allowed access to the networks on R3. Conduct another test from PC1 to PC3 to ensure that this traffic is not blocked.

You can also use an extended ping from the Fa0/0 interface on R1 to the Fa0/1 interface on R3.

```
R1#ping ip

Target IP address: 192.168.30.1

Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended
commands [n]: y

Source address or interface: 192.168.10.1

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]: Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes
[n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1

!!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/44 ms

Task 4: Configuring an Extended ACL

When greater granularity is required, you should use an extended ACL. Extended ACLs can filter traffic based on more than just source address. Extended ACLs can filter on protocol, source, and destination IP addresses, and source and destination port numbers.

An additional policy for this network states that devices from the 192.168.10.0/24 LAN are only permitted to reach internal networks. Computers on this LAN are not permitted to access the Internet. Therefore, these users must be blocked from reaching the IP address 209.165.200.225. Because this requirement needs to enforce both source and destination, an extended ACL is needed.

In this task, you are configuring an extended ACL on R1 that blocks traffic originating from any device on the 192.168.10.0/24 network to access the 209.165.200.255 host (the simulated ISP). This ACL will be applied outbound on the R1 Serial 0/0/0 interface. A typical best practice for applying extended ACLs is to place them as close to the source as possible.

Before beginning, verify that you can ping 209.165.200.225 from PC1.

Step 1: Configure a named extended ACL.

In global configuration mode, create a named extended ACL called **EXTEND-1**.

```
R1(config)#ip access-list extended EXTEND-1
```

Notice that the router prompt changes to indicate that you are now in extended ACL configuration mode. From this prompt, add the necessary statements to block traffic from the 192.168.10.0/24 network to the host. Use the **host** keyword when defining the destination.

```
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
```

Recall that the implicit “deny all” blocks all other traffic without the additional **permit** statement. Add the **permit** statement to ensure that other traffic is not blocked.

```
R1(config-ext-nacl)#permit ip any any
```

Step 2: Apply the ACL.

With standard ACLs, the best practice is to place the ACL as close to the destination as possible. Extended ACLs are typically placed close to the source. The **EXTEND-1** ACL will be placed on the Serial interface, and will filter outbound traffic.

```
R1(config)#interface serial 0/0/0

R1(config-if)#ip access-group EXTEND-1 out

R1(config-if)#end
```

```
R1#copy run start
```

Step 3: Test the ACL.

From PC1, ping the loopback interface on R2. These pings should fail, because all traffic from the 192.168.10.0/24 network is filtered when the destination is 209.165.200.225. If the destination is any other address, the pings should succeed. Confirm this by pinging R3 from the 192.168.10.0/24 network device.

Note: The extended ping feature on R1 cannot be used to test this ACL, since the traffic will originate within R1 and will never be tested against the ACL applied to the R1 serial interface.

You can further verify this by issuing the **show ip access-list** on R1 after pinging.

```
R1#show ip access-list

Extended IP access list EXTEND-1

10 deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 matches)

20 permit ip any any
```

Task 5: Control Access to the VTY Lines with a Standard ACL

It is good practice to restrict access to the router VTY lines for remote administration. An ACL can be applied to the VTY lines, allowing you to restrict access to specific hosts or networks. In this task, you will configure a standard ACL to permit hosts from two networks to access the VTY lines. All other hosts are denied.

Verify that you can telnet to R2 from both R1 and R3.

Step 1: Configure the ACL.

Configure a named standard ACL on R2 that permits traffic from 10.2.2.0/30 and 192.168.30.0/24. Deny all other traffic. Call the ACL **TASK-5**.

```
R2(config)#ip access-list standard TASK-5

R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3

R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
```

Step 2: Apply the ACL.

Enter line configuration mode for VTY lines 0–4.

```
R2(config)#line vty 0 4
```

Use the **access-class** command to apply the ACL to the vty lines in the inbound direction. Note that this differs from the command used to apply ACLs to other interfaces.

```
R2(config-line)#access-class TASK-5 in

R2(config-line)#end

R2#copy run start
```

Step 3: Test the ACL

Telnet to R2 from R1. Note that R1 does not have IP addresses in the address range listed in the ACL TASK-5 permit statements. Connection attempts should fail.

```
R1# telnet 10.1.1.2

Trying 10.1.1.2 …

% Connection refused by remote host
```

From R3, telnet to R2. You will be presented with a prompt for the VTY line password.

```
R3# telnet 10.1.1.2

Trying 10.1.1.2 … Open

CUnauthorized access strictly prohibited, violators will be prosecuted to
the full extent of the law.

User Access Verification

Password:
```

Why do connection attempts from other networks fail even though they are not specifically listed in the ACL?

Task 6: Troubleshooting ACLs

When an ACL is improperly configured or applied to the wrong interface or in the wrong direction, network traffic may be affected in an undesirable manner.

Step 1: Remove ACL STND-1 from S0/0/1 of R3.

In an earlier task, you created and applied a named standard ACL on R3. Use the **show running-config** command to view the ACL and its placement. You should see that an ACL named **STND-1** was configured and applied inbound on Serial 0/0/1. Recall that this ACL was designed to block all network traffic with a source address from the 192.168.11.0/24 network from accessing the LAN on R3.

To remove the ACL, go to interface configuration mode for Serial 0/0/1 on R3. Use the **no ip access-group STND-1 in** command to remove the ACL from the interface.

```
R3(config)#interface serial 0/0/1

R3(config-if)#no ip access-group STND-1 in
```

Use the **show running-config** command to confirm that the ACL has been removed from Serial 0/0/1.

Step 2: Apply ACL STND-1 on S0/0/1 outbound.

To test the importance of ACL filtering direction, reapply the **STND-1** ACL to the Serial 0/0/1 interface. This time the ACL will be filtering outbound traffic, rather than inbound traffic. Remember to use the **out** keyword when applying the ACL.

```
R3(config)#interface serial 0/0/1

R3(config-if)#ip access-group STND-1 out
```

Step 3: Test the ACL.

Test the ACL by pinging from PC2 to PC3. As an alternative, use an extended ping from R1. Notice that this time pings succeed, and the ACL counters are not incremented. Confirm this by issuing the **show ip access-list** command on R3.

Step 4: Restore the ACL to its original configuration.

Remove the ACL from the outbound direction and reapply it to the inbound direction.

```
R3(config)#interface serial 0/0/1

R3(config-if)#no ip access-group STND-1 out

R3(config-if)#ip access-group STND-1 in
```

Step 5: Apply TASK-5 to the R2 serial 0/0/0 interface inbound.

```
R2(config)#interface serial 0/0/0

R2(config-if)#ip access-group TASK-5 in
```

Step 6: Test the ACL.

Attempt to communicate to any device connected to R2 or R3 from R1 or its attached networks. Notice that all communication is blocked; however, ACL counters are not incremented. This is because of the implicit “deny all” at the end of every ACL. This deny statement will prevent all inbound traffic to serial

0/0/0 from any source other than R3. Essentially, this will cause routes from R1 to be removed from the routing table.

You should see messages similar to the following printed on the consoles of R1 and R2 (It will take some time for the OSPF neighbor relationship to go down, so be patient):

```
*Sep  4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on

Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

Once you receive this message, issue the command **`show ip route`** on both R1 and R2 to see which routes have been removed from the routing table.

Remove ACL TASK-5 from the interface, and save your configurations.

```
R2(config)#interface serial 0/0/0

R2(config-if)#no ip access-group TASK-5 in

R2(config)#exit

R2#copy run start
```

Task 7: Document the Router Configurations

Configurations Router 1

```
hostname R1

!

enable secret class

!

no ip domain lookup

!

interface FastEthernet0/0

ip address 192.168.10.1 255.255.255.0 no shutdown

!

interface FastEthernet0/1

ip address 192.168.11.1 255.255.255.0 no shutdown

!

interface Serial0/0/0

ip address 10.1.1.1 255.255.255.252
```

```
ip access-group EXTEND-1 out clockrate 64000

no shutdown

!

router ospf 1

network 10.1.1.0 0.0.0.3 area 0 network 192.168.10.0 0.0.0.255 area 0
network 192.168.11.0 0.0.0.255 area 0

!

ip access-list extended EXTEND-1

deny  ip 192.168.10.0 0.0.0.255 host 209.165.200.225 permit ip any any

!

banner motd ^CUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^

!

line con 0 password cisco logging synchronous login

!

line vty 0 4 password cisco login

!
```

Router 2

```
hostname R2

!

enable secret class

!

no ip domain lookup

!

interface Loopback0

ip address 209.165.200.225 255.255.255.224

!

interface FastEthernet0/1

ip address 192.168.20.1 255.255.255.0

no shutdown
```

```
!
interface Serial0/0/0
ip address 10.1.1.2 255.255.255.252 no shutdown
!
interface Serial0/0/1
ip address 10.2.2.1 255.255.255.252 clockrate 125000
no shutdown
!
router ospf 1 no auto-cost
network 10.1.1.0 0.0.0.3 area 0 network 10.2.2.0 0.0.0.3 area 0 network
192.168.20.0 0.0.0.255 area 0
network 209.165.200.224 0.0.0.31 area 0
!
ip access-list standard TASK-5 permit 10.2.2.0 0.0.0.3
permit 192.168.30.0 0.0.0.255
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0 password cisco logging synchronous login
!
line vty 0 4
access-class TASK-5 in password cisco
login
!
```

Router 3

```
hostname R3
!
enable secret class
!
```

```
no ip domain lookup

!

interface FastEthernet0/1

ip address 192.168.30.1 255.255.255.0 no shutdown

!

interface Serial0/0/1

ip address 10.2.2.2 255.255.255.252

ip access-group STND-1 in

no shutdown

!

router ospf 1

network 10.2.2.0 0.0.0.3 area 0 network 192.168.30.0 0.0.0.255 area 0

!

ip access-list standard STND-1

deny  192.168.11.0 0.0.0.255 log permit any

!

banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^

!

line con 0 password cisco logging synchronous login

!

line vty 0 4 password cisco login

!

end
```

Task 8: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Critical Analysis/Conclusion

Lab Assessment		
Pre Lab	**/5**	**/25**
Performance	**/5**	
Results	**/5**	
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		