COMSATS University Islamabad, Lahore Campus
Department of Electrical and Computer Engineering

CPE 314 – Data Communication and Computer Networks

Lab Manual for Spring 2024 & Onwards

Lab Resource Person

Engr. Modassir Ishfaq

Theory Resource Person

Engr. Ahmad Mudassir

Supervised By

Dr. Muhammad Farooq-i-Azam

Name: Abdul Rafay **Registration Number:** *CIIT/* FA21-BCE 050 */LHR*

Program: Data communication **Batch:** FA21

Semester 6th

Revision History

S. No.	Activity	Date	Performed by
1	Lab Manual Preparation	5/Jan/2014	Engr. Mukhtar Hussain
	Lab Manual Review	6/Jan/2014	Dr. Ali Nawaz Khan
2	Layout Modifications	14/Jan/2015	Yasir Jamil Rathore
	Lab Manual Review	15/Jan/2015	Dr. Ali Nawaz Khan
3	Labs Updating/Modifications	4/July/2015	Engr. Arslan Khalid
	Lab Manual Review	5/July/2015	Engr. M. Babar Ali Magsi
4	Layout Modifications	3/Feb/2016	Engr. Ahmed Daud
5	Labs Updating/Modifications	12/Feb/2018	Engr. Fahad Naeem
6	Layout Modifications	15/Sep/2018	Engr. Modassir Ishfaq
7	Lab Manual Modifications	6/Feb/2020	Mayyda Mukhtar
8	Lab Manual Modification	26/Aug/2021	Syed Ahmed Faran
9	Modification of experiments and reducing them to total of 12	11/Feb/2022	Syed Ahmed Faran

Preface

According to the requirement of Bachelors of Electrical (Telecommunication) Engineering and Computer Engineering program, Data Communication and Computer Networks (DCCN) is a core course that provides a comprehensive introduction to fundamental principles and applications in the design of Computer Networks.

It is a four-credit hour course in which one credit hour is reserved for the Lab. This Lab Manual is the reference for the lab part of this course. Over the time, changes have been done and we have tried to synchronize this lab manual with the theory part.

This lab manual comprises of the experiments which can induce learning of multiple software tools enabling the students to better understand the fundamentals of Data Communication and Computer Networks. These tools include:

Wireshark Packet Sniffer

Cisco Packet Tracer

OPNET Simulator

The manual contains sufficient exercises for a typical 14-week course using a three hour practicum period. The topics cover three major portions that are:

Simulation of Media Access Protocols on OPNET simulator, designed to correlate theory with lab. It will also help the students to simulate advance networking protocols in future.

Routing and switching that is covered using Cisco Packet Tracer.

Understanding of network protocols that can be deepened by looking at them in action. Students can initiate any session from their terminal and capture session packets using Wireshark Packet Sniffer. Also analyse captured packets.

We are quite optimistic that this manual will be useful to enhance the skills and expertise of the students in the field of computer networking. Enjoy 'learning by doing'

Books

Text Books

1. Computer Networking: A top-down approach by James Kurose and Keith Ross, 6th ed

Reference Books

1. Data Communication and Networking by Behrouz A. Forouzan, 5th ed
2. Data and Computer Communications by William Stallings, 10th Edition, Prentice Hall

Learning Outcomes

Theory CLOs:

1. CLO1: **Describe** and **identify** data communications and networks based on OSI and TCP/IP models (PLO1-C1)
2. CLO2: **Analyze** the ubiquitous service architectures and important application-level protocols along with their corresponding associated applications in conjunction with transport layer services based on RFC standards (PLO4-C4)
3. CLO3: **Analyze** modern transport, routing, switching, addressing techniques and create small to large enterprise business solutions with higher robustness based on modern networking techniques (PLO4-C4)

Lab CLOs

4. CLO4: To **reproduce** and **show** modern computer networking techniques to examine various Quality of Service parameters with the help of simulators and tools (wireshark, packet tracer, OPNET). (PLO5-P3)

5. CLO5: To be able to **compare**, **contrast** and **analyze** various network algorithms/protocols and propose feasible solutions to computer network problems (PLO2-C4)
6. CLO6: To **form** effective report of complex engineering problem and **justify** the findings in a presentation. (PLO10-A3)

CLOs – PLOs Mapping

PLO / CLO	PLO1	PLO2	PLO3	PLO5	PLO10	Cognitive Domain	Affective Domain	Psychomotor Domain
CLO1	X					C1		
CLO2		X				C4		
CLO3		X				C4		
CLO4				X				P3
CLO5		X				C4		
CLO6					X		A3	

Lab CLOs – Lab Experiment Mapping

CLO \ Lab	Lab 1	Lab 2	Lab 3	Lab 4	Lab 5	Lab 6	Lab 7	Lab 8	Lab 9	Lab 10	Lab 11	Lab 12
CLO4				P3	P3	P3	P3	P3	P3	P3	P3	P3
CLO5	C4	C4	C4									

Grading Policy

The final marks for lab would comprise of Lab Assessment (25%), Lab Midterm (25%) and Lab Terminal (50%).

Lab Assignments: i. Lab Assignment 1 Marks (Lab marks from Labs 1-3) ii. Lab Assignment 2 Marks (Lab marks from Labs 4-6) iii. Lab Assignment 3 Marks (Lab marks from Labs 7-9) iv. Lab Assignment 4 Marks (Lab marks from Labs 10-12)	25%
Lab Midterm = 0.5*(Midterm Lab exam) + 0.5* (average of lab evaluation of Lab 1-8)	25%
Lab Terminal = 0.5*(Complex Engineering Problem) +0.125*(average of lab evaluation of Lab 1-6) + 0.375*(average of lab evaluation of Lab 6-12)	50%
Total (lab)	**100%**

The minimum pass marks for both lab and theory shall be 50%. Students obtaining less than 50% marks (in either theory or lab, or both) shall be deemed to have failed in the course. The final marks would be computed with 75% weight to theory and 25% to lab final marks.

Software Resources

- Wireshark Packet Sniffer
- Cisco Packet Tracewr

Lab Instructions

- All labs comprise of three parts: Pre-Lab, In-Lab and Post-Lab Exercises

- The students should complete and demonstrate each lab task separately for step-wise evaluation (please ensure that course instructor/lab engineer has signed each step after ascertaining its functional verification)
- Only those tasks that completed during the allocated lab time will be credited to the students. Students are however encouraged to practice on their own in spare time for enhancing their skills

Lab Report Instructions

All questions should be answered precisely to get maximum credit. Lab report must ensure following items:

- Lab Objectives
- Configuration Codes
- Results (graphs/tables/observations) duly commented and discussed
- Conclusions

SOP for Lab

- Students should display and must be prepared to show student ID card when requested by lab staff.
- Note the location of the Emergency Disconnect (red button near the door) to shut off power in an emergency.
- Students are allowed in the laboratory only when the instructor is present.
- No edibles are allowed in the Lab.
- Keep the lab clean and tidy.
- This lab is a study and learning environment please be quite.
- University property must not be taken from the laboratory.
- Do not place books or personal belonging on any printer, monitor or computer equipment. This can interfere with hardware operation and/or inhibit proper cooling functions for the equipment.
- NO SMOKING! smoking is not allowed in the lab.
- Do not download software from the internet onto the computer in the lab unless authorized to do so.
- Any kind of chat is strictly banned in the lab.
- Downloading/uploading/viewing any material that might be deemed abusive hateful, degrading, demeaning, or defamatory is strictly prohibited.
- Do not share your account's password with each other.
- Do not Install/configure any programs on the computers unless specifically authorized to do so.
- Once a computer is turned on, leave it on. Never shut down a computer.
- Do not leave important data file on the hard drive of the computer in the lab. We routinely go through the machines and delete files that are not part of the normal software suite.

Laboratory Safety Rules

All students must read and understand the information in this document with regard to laboratory safety and emergency procedures prior to the first laboratory session. **Your personal laboratory safety depends mostly on YOU**. Effort has been made to address situations that may pose a hazard in the lab but the information and instructions provided cannot be considered all-inclusive.

The danger of injury or death from electrical shock, fire, or explosion is present while conducting experiments in this laboratory. To work safely, it is important that you understand the prudent practices necessary to minimize the risks and what to do if there is an accident.

Avoid contact with conductors in energized electrical circuits. Do not touch someone who is being shocked while still in contact with the electrical conductor or you may also be electrocuted. Instead, press the Emergency Disconnect (red button located near the door to the laboratory). This shuts off all power, except the lights.

Make sure your hands are dry. The resistance of dry, unbroken skin is relatively high and thus reduces the risk of shock. Skin that is broken, wet, or damp with sweat has a low resistance. When working with an energized circuit, work with only your right hand, keeping your left hand away from all conductive material. This reduces the likelihood of an accident that results in current passing through your heart.

Be cautious of rings, watches, and necklaces. Skin beneath a ring or watch is damp, lowering the skin resistance. Shoes covering the feet are much safer than sandals.

If the victim isn't breathing, find someone certified in CPR. Be quick! Some of the staff in the Department Office are certified in CPR. If the victim is unconscious or needs an ambulance, contact the Department Office for help or call 1122. If able, the victim should go to the Student Health Services for examination and treatment.

Table of Contents

LAB # 1
To Explain the Basic Idea about OSI Reference Model, Networking Devices and Transmission Media based on Networking Standards

Objectives

- Identify and distinguish multiple transmission media and devices based on IETF & IEEE standards.
- To comprehend the concept of layers using OSI reference model and TCP IP protocol stack.

Pre-Lab Exercise

Read this experiment in its entirety to become familiar with objectives of this lab. Also review the portions of chapter 2 and 4 of your text book and try to understand the OSI Reference Model and transmission media. You may record the terms and sections that require more elaboration for reference. The instructor may provide the class some time to reflect upon these before proceeding with the lab.

The OSI Reference Model

OSI stands for Open Systems Interconnection, it is a logical model, not a physical one. It's essentially a set of guidelines that developers can use to create and implement applications to run on a network. It also provides a framework for creating and implementing networking standards, devices, and internetworking schemes. One of best gifts the OSI specifications gives us is paving the way for the data transfer between disparate hosts running different operating systems, like Unix hosts, Windows machines, Macs, smartphones, and so on. The OSI reference model has the following seven layers:

- Application layer (layer 7)
- Presentation layer (layer 6)
- Session layer (layer 5)
- Transport layer (layer 4)
- Network layer (layer 3)
- Data Link layer (layer 2)
- Physical layer (layer 1)

The OSI seven different layers, divided into two groups. The top three layers define how the applications within the end stations will communicate with each other as well as with users. The bottom four layers define how data is transmitted end to end.

Application	• Provides a user interface
Presentation	• Presents data • Handles processing such as encryption
Session	• Keeps different applications' data separate

Users interact with the computer at the Application layer and also that the upper layers are responsible for applications communicating between hosts. None of the upper layers knows anything about networking or network addresses because that's the responsibility of the four bottom layers.

The bottom four layers are mentioned below, you can see that it's these four bottom layers that define how data is transferred through physical media like wire, cable, fiber optics, switches, and routers. These bottom layers also determine how to rebuild a data stream from a transmitting host to a destination host's application.

Transport

- Provides reliable or unreliable delivery
- Performs error correction before re-transmit

Network

- Provides logical addressing, which routers use for path determination

Data Link

- Combines packets into bytes and bytes into frames
- Provides access to media using MAC address
- Performs error detection not correction

Physical

- Moves bits between devices
- Specifies voltage, wire speed, and pinout of cables

In the upcoming labs we will analyze real time packets transferred from one host to another. Also simulate protocols of network and data link layers.

Internet Protocol (IP)

The Internet Protocol (IP) is one of the most important protocols in the Internet. The IP protocol specifies the format of the packets that are sent and received among routers and end systems.

IP Address

In the Internet, every end system has an address called an IP address. When a source end system wants to send a packet to a destination end system, the source includes the destination's address in the packets.

Network Devices

Hubs

The hub is the active central element of the star layout. Each station is connected to the hub by two lines (transmit and receive).The hub acts as a repeater: When a single station transmits, the hub repeats the signal on the outgoing line to each station.

Switches

In recent years, a new device, the layer 2 switch, has replaced the hub in popularity, particularly for high-speed LANs. The layer 2 switch is also sometimes referred to as a switching hub. To clarify the distinction between hubs and switches, Figure 1 shows a typical bus layout of a traditional 10-Mbps LAN.

We can achieve greater performance with a layer 2 switch. In this case, the central hub acts as a switch, much as a packet switch or circuit switch. With a layer 2 switch, an incoming frame from a particular station is switched to the appropriate output line to be delivered to the intended destination. At the same time, other unused lines can be used for switching other traffic.

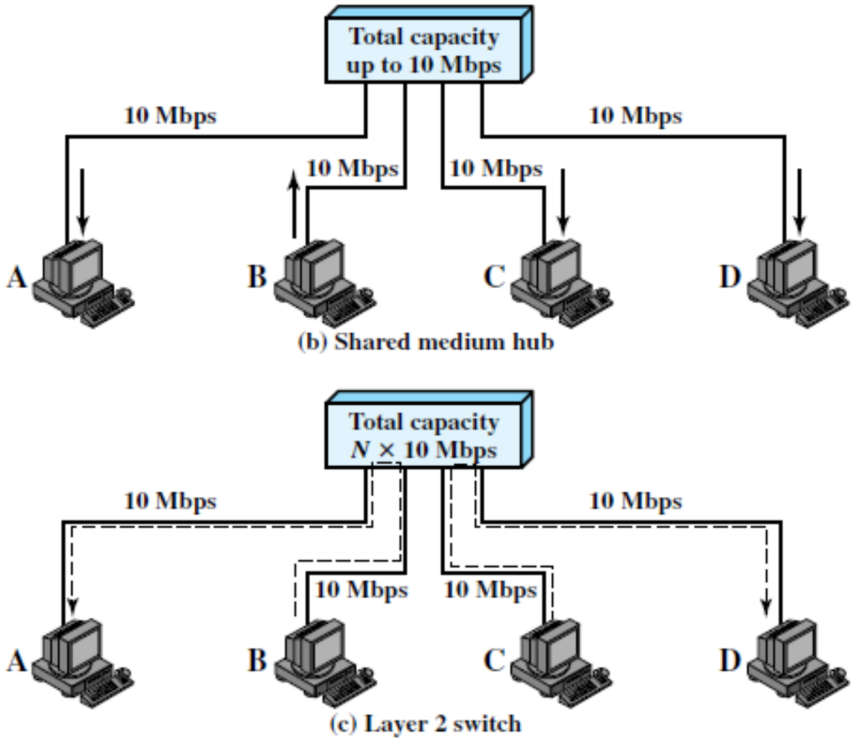

Figure 1: Layer 2 Devices

Two types of layer 2 switches are available as commercial products:

- **Store-and-forward switch:** The layer 2 switch accepts a frame on an input line, buffers it briefly, and then routes it to the appropriate output line.
- **Cut-through switch:** The layer 2 switch takes advantage of the fact that the destination address appears at the beginning of the MAC (medium access control) frame. The layer 2 switch begins repeating the incoming frame onto the appropriate output line as soon as the layer 2 switch recognizes the destination address.

Router

Routers can be considered as layer 3 switches. Unlike layer 2 switches, which forward or filter frames, routers use logical addressing and provide an important capacity called *packet switching*. Router performs following functions in network:

- Packet switching
- Packet filtering
- Internetwork communication
- Path selection

There are two advantages to using routers in your network:

- They don't forward broadcasts by default.
- They can filter the network based on layer 3, Network layer, information such as an IP address.

Cisco's Internetworking Operating System (IOS)

The *Cisco Internetwork Operating System (IOS)* is the kernel of Cisco routers as well as all current Catalyst switches. In case you didn't know, a kernel is the elemental, indispensable part of an operating system that allocates resources and manages tasks like low-level hardware interfaces and security. Cisco IOS is *Command Line Interface (CLI).*

The Cisco IOS is a proprietary kernel that provides routing, switching, internetworking, and telecommunications features. The first IOS was written by William Yeager in 1986 and enabled networked applications. It runs on most Cisco routers as well as a growing number of Cisco Catalyst switches. Cisco router IOS software is responsible for:

- Carrying network protocols and functions
- Connecting high-speed traffic between devices
- Adding security to control access and stop unauthorized network use
- Providing scalability for ease of network growth and redundancy
- Supplying network reliability for connecting to network resources

Transmission Media

Data transmission occurs between transmitter and receiver over some transmission medium. Transmission media may be classified as guided or unguided. In both cases, communication is in the form of electromagnetic waves. With **guided media**, the waves are guided along a physical path; examples of guided media are twisted pair, coaxial cable, and optical fiber. Here we will discuss the transmission medium we will use in for connection between the network devices in Lab.

Twisted Pair

The least expensive and most widely used guided transmission medium is twisted pair. Twisted pair cable has four pairs of wires twisted inside it to eliminate electrical interference. Twisted pair cables are connected using RJ-45 connectors that have eight connector pins to connect through Ethernet port. Twisted pair comes in two varieties: unshielded and shielded. Twisted pair cable is shown in Figure 2:

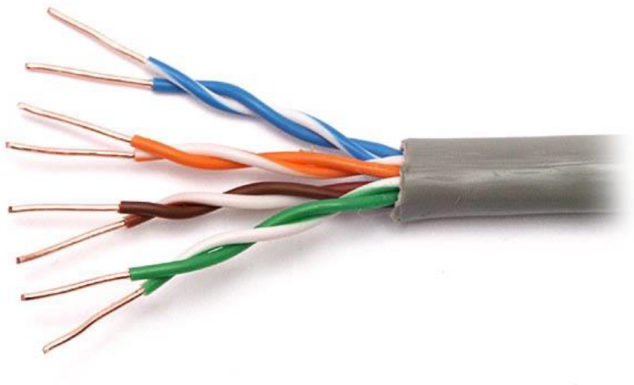

Figure 2: Twisted Pair

Twisted pair cables are used in following configurations and for different purposes, to form an internetwork.

- Straight-through
- Crossover
- Rollover

Straight-through

A straight-through cable is the standard network cable connection and is used to connect the source and destination hosts through an internetworking device. Specifically, you can use it to connect a host to a hub or switch. Configuration of twisted pair cable as straight-through is shown in

Figure 3.

Crossover

A crossover cable is the standard network cable connection and is used to connect same source and destination hosts in a network. Specifically, you can use it to connect a computer to a computer or switch to switch or router to a host (i.e. computer). Configuration of twisted pair cable as crossover is shown in

Figure 3.

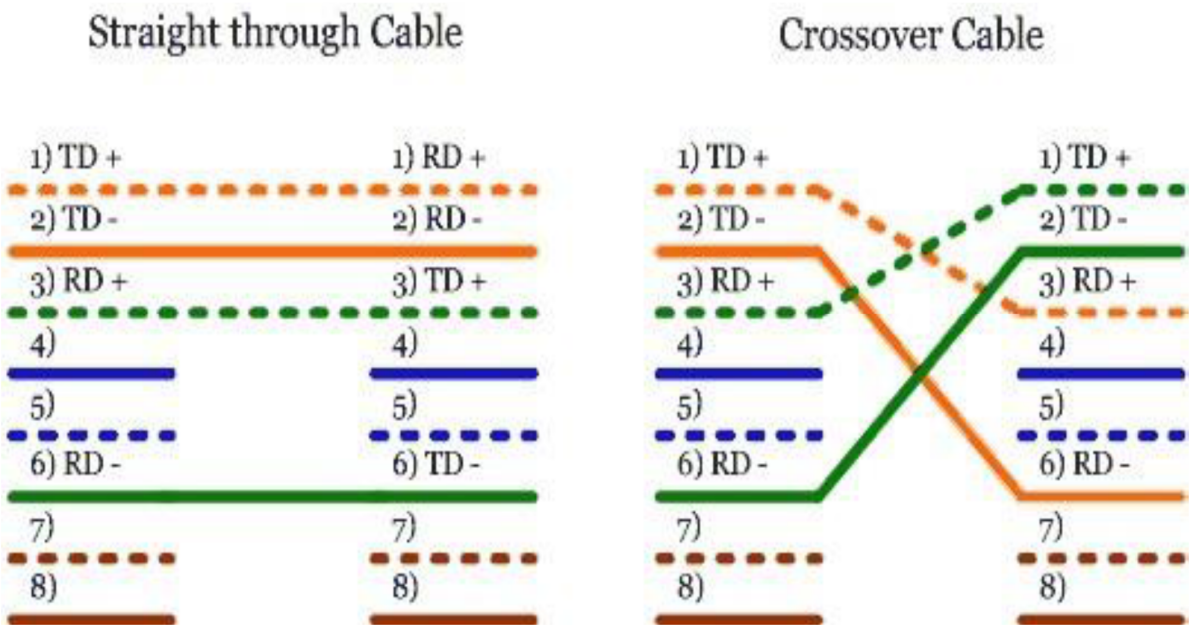

Figure 3: Straight-through and Crossover Cables

Rollover

These Cisco proprietary cables used to connect to a router or switch console port. In a rollover cable (8 pins) RJ-45 connectors are usually present at one ends and DB-9 at other. It is used to configure cisco network devices. A router or a switch connects through RJ-45 connector to a computer COM port through DB-9 connectors. Configuration of twisted pair as rollover is shown in Figure 4.

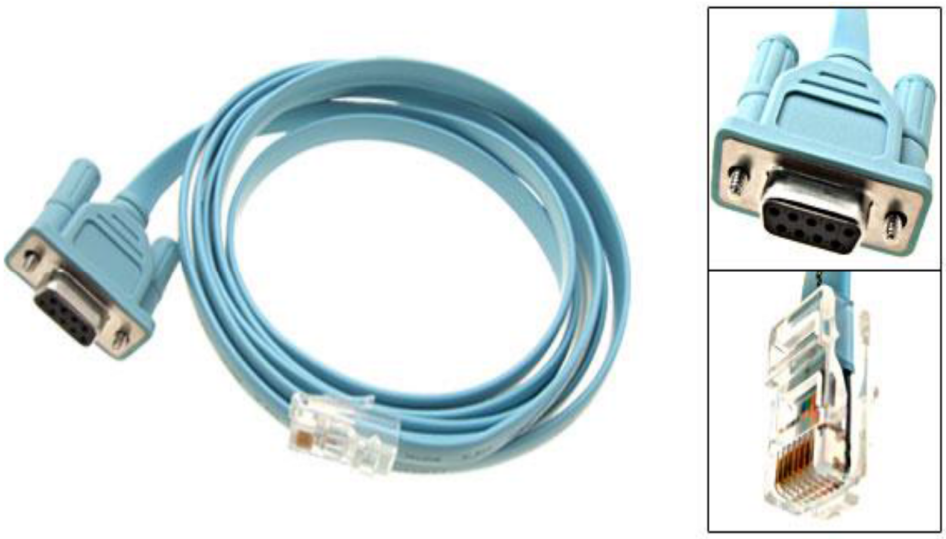

Figure 4: Rollover Cable

Explore different networking devices and make connections between them to make your first small network. Your lab instructor will elaborate further how cables are represented in this simulator. Here you will take a brief introduction. You will explore Cisco Packet Tracer in next lab.

Connecting to a Cisco ISO Device

You can access the *Cisco IOS* through the *console port* of a router or switch, or even through *Telnet* and *Secure Shell (SSH)*. Access to the IOS command line is called an *EXEC session*.

We connect to a Cisco device to configure it, verify its configuration, and check statistics, and although there are different approaches to this, the first place you would usually connect to is the console port. The *console port* is usually an RJ-45, 8-pin modular connection located at the back of the device.

When you first bring up a Cisco IOS device, it will run a power-on self-test—a POST. Upon passing that, the machine will look for and then load the Cisco IOS from flash memory if an IOS file is present, then expand it into RAM. As you probably know, flash memory is electronically erasable programmable read-only memory—an EEPROM. The next step is for the IOS to locate and load a valid configuration known as the startup-configuration that will be stored in *nonvolatile RAM (NVRAM).*

Once the IOS is loaded and up and running, the startup-configuration will be copied from NVRAM into RAM and from then on referred to as the running-configuration.

Rubric for Lab Assessment

The student performance for the assigned task during the lab session was:			
Excellent	The student completed assigned tasks without any help from the instructor and showed the results appropriately.	4	
Good	The student completed assigned tasks with minimal help from the instructor and showed the results appropriately.	3	
Average	The student could not complete all assigned tasks and showed partial results.	2	
Worst	The student did not complete assigned tasks.	1	

Instructor Signature: _____ Date: _____

LAB # 2
To Analyse and Explain the Syntax and Semantics of Application Layer Service and Protocols using Wireshark

Objectives

- To analyse and show the contents captured in Wireshark related to HTTP, SMTP, POP and DNS.
- To show the network transactions between clients and DNS server using Wireshark.

Pre-Lab Exercise

Read this experiment in its entirety to become familiar with objectives of this lab. Study in detail and become familiar with the basics of Hyper Text Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP) and Domain Name Server (DNS) provided with this laboratory experiment and in chapter 2 of the reference book. Have Wireshark Packet Sniffer software program installed on your PC and review how to capture/analyse packets. You may record the terms and sections that require more elaboration for reference. The instructor may provide the class some time to reflect upon these before proceeding with the lab.

Introduction to Packet Sniffer

One's understanding of network protocols can often be greatly deepened by "seeing protocols in action" and by "playing around with protocols" – observing the sequence of messages exchanged between two protocol entities, delving down into the details of protocol operation, and causing protocols to perform certain actions and then observing these actions and their consequences. This can be done in simulated scenarios or in a "real" network environment such as the Internet. In the Wireshark labs you'll be running various network applications in different scenarios using your own computer. You'll observe the network protocols in your computer "in action," interacting and exchanging messages with protocol entities executing elsewhere in the Internet. Thus, you and your computer will be an integral part of these "live" labs. You'll observe, and you'll learn, by doing.

In this first Wireshark lab, you'll get acquainted with Wireshark, and make some simple packet captures and observations.

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 5 shows the structure of a packet sniffer. At the right of Figure 5 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 5 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. Recall from the discussion from the first lab that 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 5 , 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.

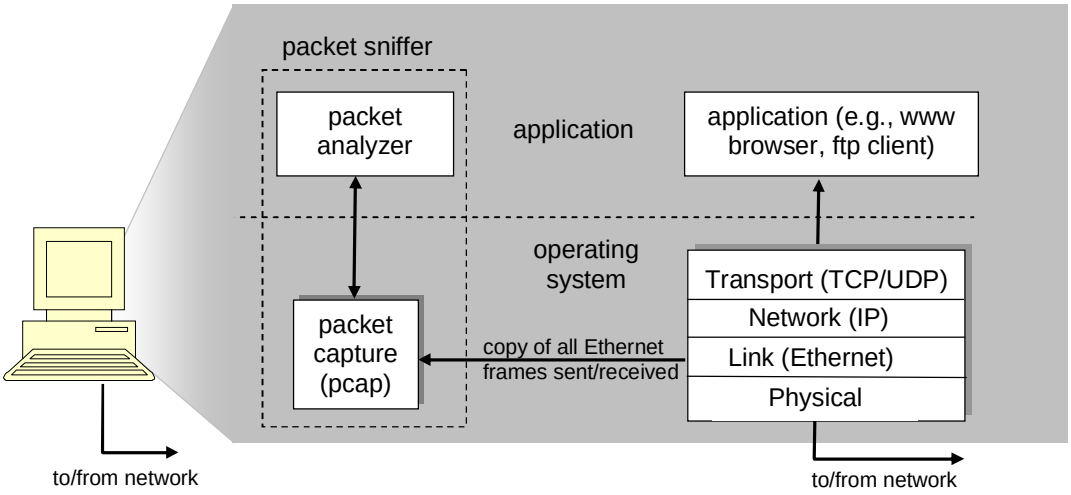

Figure 5: Packet Sniffer Structure

The second component of a packet sniffer is the **packet analyser**, which displays the contents of all fields within a protocol message. In order to do so, the packet analyser must "understand" the structure of all messages exchanged by protocols.

We will be using the Wireshark packet sniffer for these labs, allowing us to display the contents of messages being sent/received from/by protocols at different levels of the protocol stack.

Running Wireshark

When you run the Wireshark program, you'll get a startup screen

Take a look at the upper left hand side of the screen – you'll see an "Interface list". This is the list of network interfaces on your computer. Once you choose an interface, Wireshark will capture all packets on that interface. Start Wireshark on your computer system is there an Ethernet interface?

_____

_____

Click on Ethernet interface and then start. A screen like the one below will be displayed, showing information about the packets being captured. Once you start packet capture, you can stop it by using the Capture pull down menu and selecting Stop.

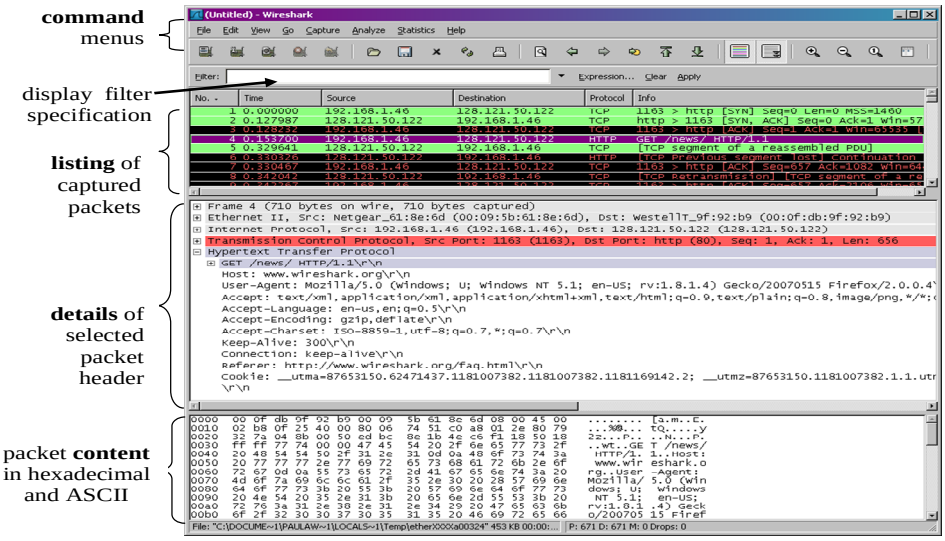

Figure 6: Wireshark GUI, during packet capture and analysis

- 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. The protocol 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 (assuming the packet was sent/received over an Ethernet interface) 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 plus minus boxes to the left of the Ethernet frame or IP datagram line in the packet details window. 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.

Task 1: Starting with Wireshark

Step 1: Check if your computer is connected to the Internet via a wired Ethernet interface? Do the following
Start up your favorite web browser, which will display your selected homepage.
Start up the Wireshark software.
To begin packet capture, select the *Capture* pull down menu and select *Interfaces*. This will cause the "Wireshark: Capture Interfaces" window to be displayed, as shown in Figure 7.

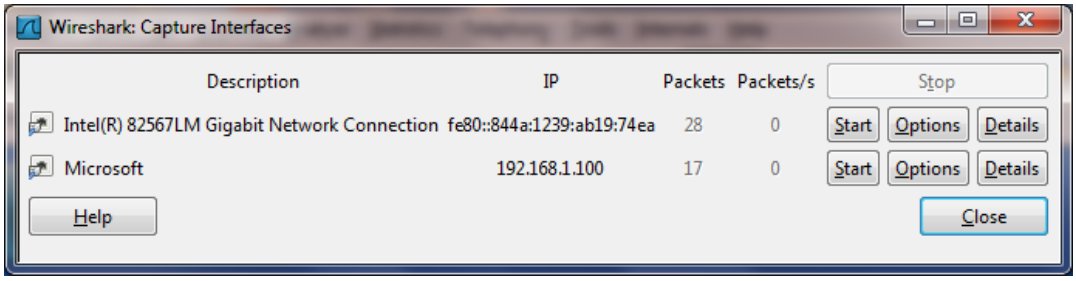

Figure 7: Wireshark Capture Interface Window

Select Ethernet interface.
Once you begin packet capture, a window similar to that shown in Figure 2 will appear. This window shows the packets being captured. By selecting *Capture* pulldown menu and selecting *Stop*, you can stop packet capture.
We will capture some interactive packets and analyse packets in next task.

In-Lab Exercise

Task 1: Capture and Analyse HTTP Trace

Step 1: Let's begin our exploration of HTTP by accessing a website. Do the following:

- Start up your web browser.
- Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.
- Wait a bit more than one minute (we'll see why shortly), and then begin Wireshark packet capture.
- Enter the address to your browserhttps://www.google.com.pk
- As web page appear on browser, go to Wireshark window and stop packet capture.

What do you observe in *packet-listing window*?

Displays all the packet in the current capture space

Step 2: Explore the packets and answer the following questions

What version of HTTP is your browser and google server running?

http 1.1

What languages (if any) does your browser indicate that it can accept to the server?

en-us

What is the IP address of your computer?

192.168.1.187

What is the IP address of google server?

How many bytes of content are being returned to your browser?

128 Bytes

What is the source and destination port number?

source 63673 and destination 80

How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

0.027998

What is date and time of server in HTTP received packets?

Wed, 03 Feb 2021 22:57:36 GMT

Task 2: Analyse SMTP Trace

Step1: Download the following file, and open it up in Wireshark:

http://asecuritysite.com/log/smtp.zip

Step 2: Explore the packets and answer the following questions

The IP address and port used by the host which is sending the Email

ip 192.168.0.12 port 25

The IP address and the port used by the SMTP server

ip 192.168.0.13 port 1713

Who is sending the Email?

martin.tor@4salet.com

Who is receiving the Email?

bert.manly@five8nine.com

When was the Email sent?

Mon, 11 Mar 2013 22:06:28

What was the message, and what was the subject of the Email?

T2theS4gSSB0aGluayBpdC

With SMTP, which character sequence is used to end the message?

quit

Task 3: Analyse POP3 trace

Step 1: Download the following file, and open it up in Wireshark

http://asecuritysite.com/log/pop3.zip

Step 2: Explore the packets and answer the following questions

The IP address and the port used by the host which is sending the email

192.184.0.4 port 26308

The IP address and the port used by the POP-3 server

212.227.15.166 port 110

Whose mail box is being accessed?

digitalinvestigator@networksims.com

How many email messages are in the Inbox?

3 messages

Which command does POP-3 use to get a specific message?

RETR

For Message 1, who sent the message and what is the subject and outline the content of the message?

Subject : A message from 1&1 Internet

Outline: We'd like to take this opportunity to tell you about a feature that is=20 included in 1&1 e-mail services.=20

Which command does POP-3 use to get a specific message?

RETR

DNS

The Domain Name System (DNS) translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we'll take a closer look at the client side of DNS. Client's role in the DNS is relatively simple – a client sends a *query* to its local DNS server, and receives a *response* back.

In this lab we will get DNS record and analyse it. Also trace the packets between your computer and DNS server.

Task 1: Get DNS record

To send query any specified DNS server for a DNS record *nslookup* tool can be used. Your internet browsers already programmed to get DNS records. *nslookup* tool allows user to analyse the DNS records. To run it in Windows, open the Command Prompt and run *nslookup* on the command line.

Step 1: Open Command Prompt and run following command and write down your observations

*nslookup*www.google.com

Received a no authrative answer with name www.google.com and address

2a00:1450:4018:80a::2004
172.217.169.228

Step 2: Run following command and write down your observations

nslookup –type=NS www.google.com

Received the following parameters

primary name server = ns1.google.com
responsible mail addr = dns-admin.google.com
serial = 608928096
refresh = 900 (15 mins)
retry = 900 (15 mins)
expire = 1800 (30 mins)
default TTL = 60 (1 min)

Step 3: Run following command and write down your observations

You can indicate that you want to the query sent to any DNS server rather than to the default DNS server. Like in the following example we send query to google public DNS server. Thus, the query and reply transaction takes place directly between our querying host and 8.8.8.8.

*nslookup*www.hotmail.com8.8.8.8

Received a non authorative answer with the following parameters

Name: a-0010.a-msedge.net
Addresses: 2620:1ec:c11::212
204.79.197.212
Aliases: www.hotmail.com
outlook-fd-0010.live.com

Task 2: Get your system address

ipconfig is among the most useful little utilities in your host, especially for debugging network issues. ipconfig can be used to show your current IP information, including your address, DNS server addresses, adapter type and so on.

Step 1: Run the following command in Command Prompt and write down your observations
ipconfig /all

The following command returned a the windows ip configuration and ethernet adapter setting

Step 2: Run the following command in Command Prompt and write down your observations
ipconfig /displaydns

The command return the following parameters

Windows IP Configuration

array611.prod.do.dsp.mp.microsoft.com

Record Name . . . . . : array611.prod.do.dsp.mp.microsoft.com
Record Type . . . . . : 1
Time To Live . . . . : 732
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 20.54.24.79

Step 2: Run the following command in Command Prompt and write down your observations
ipconfig /flushdns

The command successfully resolved the DNS server Cache

Task 3: Tracing DNS with Wireshark

Step 1: Do the following

Use *ipconfig* to empty the DNS cache in your host.
Open your browser and empty your browser cache.
Open Wireshark and enter "ip.addr == your_IP_address" into the filter, where you obtain your_IP_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.
Start packet capture in Wireshark.
With your browser, visit the Web page: http://www.ietf.org
Stop packet capture.

Step 2: Analyse the DNS packets on Wireshark and answer the following questions

Locate the DNS query and response messages. Are then sent over UDP or TCP?

UDP

What is the destination port for the DNS query message? What is the source port of DNS response message?

source : 56830

Destination: 53

To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Dns 172.168.17.9

Yes they are same

Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

_____

_____

Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

_____

_____

Rubric for Lab Assessment

The student performance for the assigned task during the lab session was:			
Excellent	The student completed assigned tasks without any help from the instructor and showed the results appropriately.	4	
Good	The student completed assigned tasks with minimal help from the instructor and showed the results appropriately.	3	
Average	The student could not complete all assigned tasks and showed partial results.	2	
Worst	The student did not complete assigned tasks.	1	

Instructor Signature: _____ Date: _____

LAB # 3
To Analyse Transport Layer Services and Protocols and Display the Captured Contents using Wireshark

Objectives

- To illustrate and explain hand shaking process in TCP setup and connection termination procedure.
- To explain TCP flow and congestion control mechanism using traces in Wireshark.
- To display and explain the contents in UDP segments captured by using Wireshark.
- To explain ICMP messages generated using trace route program.

Pre-Lab Exercise

Read this experiment in its entirety to become familiar with objectives of this lab. Study in detail and become familiar with the basics of Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) provided with this laboratory experiment and in chapter 3 of the reference book. You may record the terms and sections that require more elaboration for reference. The instructor may provide the class some time to reflect upon these before proceeding with the lab.

In-Lab Exercise

Task 1: Capturing a Bulk TCP Transfer from Your Computer to a Remote Server

Before beginning our exploration of TCP, we'll need to use Wireshark to obtain a packet trace of the TCP transfer of a file from your computer to a remote server. You'll do so by accessing a Web page that will allow you to enter the name of a file stored on your computer (which contains the ASCII text of *Alice in Wonderland*), and then transfer the file to a Web server using the HTTP POST method. We're using the POST method rather than the GET method as we'd like to transfer a large amount of data *from* your computer to another computer. Of course, we'll be running Wireshark during this time to obtain the trace of the TCP segments sent and received from your computer.

Step 1: Start up your web browser. Go the http://gaia.cs.umass.edu/wireshark-labs/alice.txt and retrieve an ASCII copy of *Alice in Wonderland.* Store this file somewhere on your computer.

Step 2: Next go to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html. Use the *Browse* button in this form to enter the name of the file (full path name) on your computer containing *Alice in Wonderland* (or do so manually).Don't yet press the "*Upload alice.txt file*" button.

Step 3: Now start up Wireshark and begin packet capture *(Capture->Start)* and then press *OK* on the Wireshark Packet Capture Options screen (we'll not need to select any options here).

Step 4: Returning to your browser, press the "*Upload alice.txt file*" button to upload the file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short congratulations message will be displayed in your browser window.

Step 5: Stop Wireshark packet capture. Your Wireshark window should look similar to the window shown below.

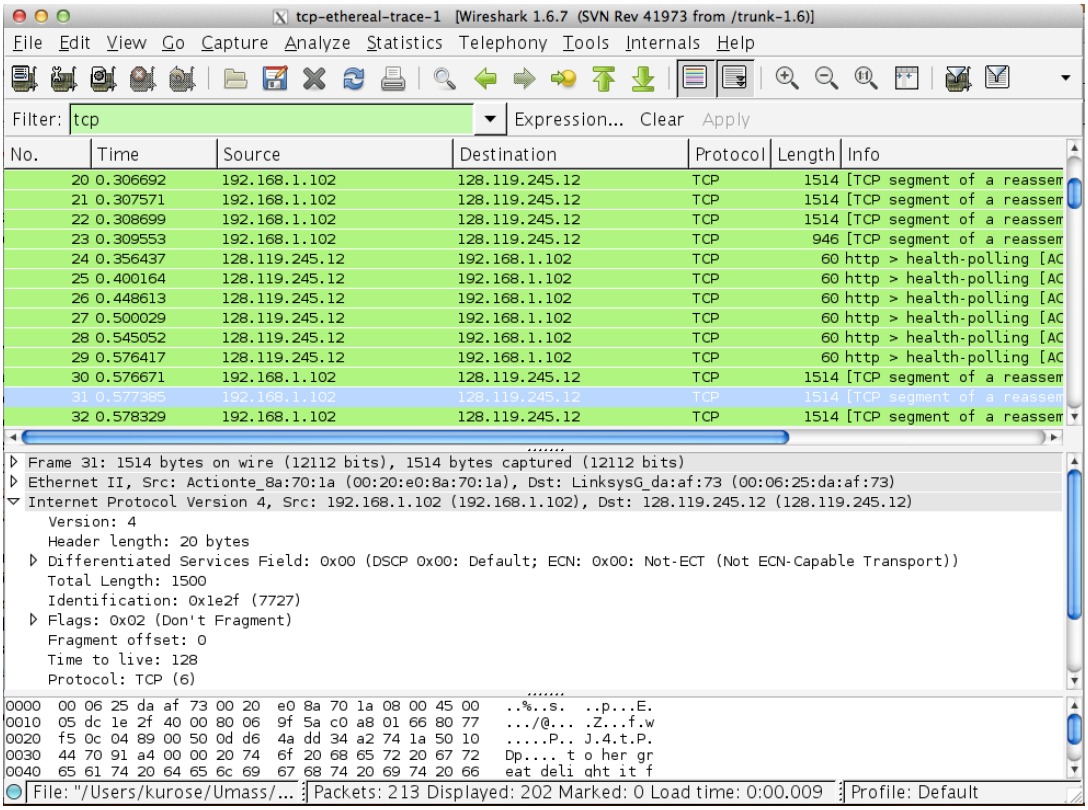

Figure 8: Wireshark Window

Have your packet sniffer captured the packets?

Yes

Task 2: Analyse the Captured Trace

Before analysing the behavior of the TCP connection in detail, let's take a high level view of the trace.

Step 1: First, filter the packets displayed in the Wireshark window by entering "tcp" into the display filter specification window.

What changes have you observed in the captured trace?

The captured traced showed took me to packets having tcp format

Step 2: Answer the following question by analysing the captured trace.

What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?

ip address = 192.168.86.68 Port number = 80

What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

Ip Address = 128.119.245.12 Port Number = 55639

Step 3: This lab is about TCP rather than HTTP, so change Wireshark's "listing of captured packets" window so that it shows information about the TCP segments containing the HTTP messages, rather than about the HTTP messages. To have Wireshark do this, select *Analyse->Enabled Protocols.* Then uncheck the HTTP box and select *OK*.

What changes have you observed in the captured trace now?

Task 3: Analyse TCP Packets

Step 1: Answer the following questions for the TCP segments:

What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu?

0

What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

Sequence number = 0 Acknowledgment Number = 0

What is the sequence number of the TCP segment containing the HTTP POST command?

152041

Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection and fill the following table.

Sr.#	Sequence Number	Sent Time	ACK Received time	Calculated RTT value

What is the length of each of the first six TCP segments?

What is the minimum and maximum amount of available buffer space advertised at the received for the entire trace?

Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

How much data does the receiver typically acknowledge in an ACK?

Step 2: Use Wireshark's TCP graphing utilities to plot out data and examine the amount of data sent per unit time from the client to the server. Select the menu: Statistics->TCP Stream Graph-> Time-Sequence-Graph (Stevens). Your graph will look like Figure 9.

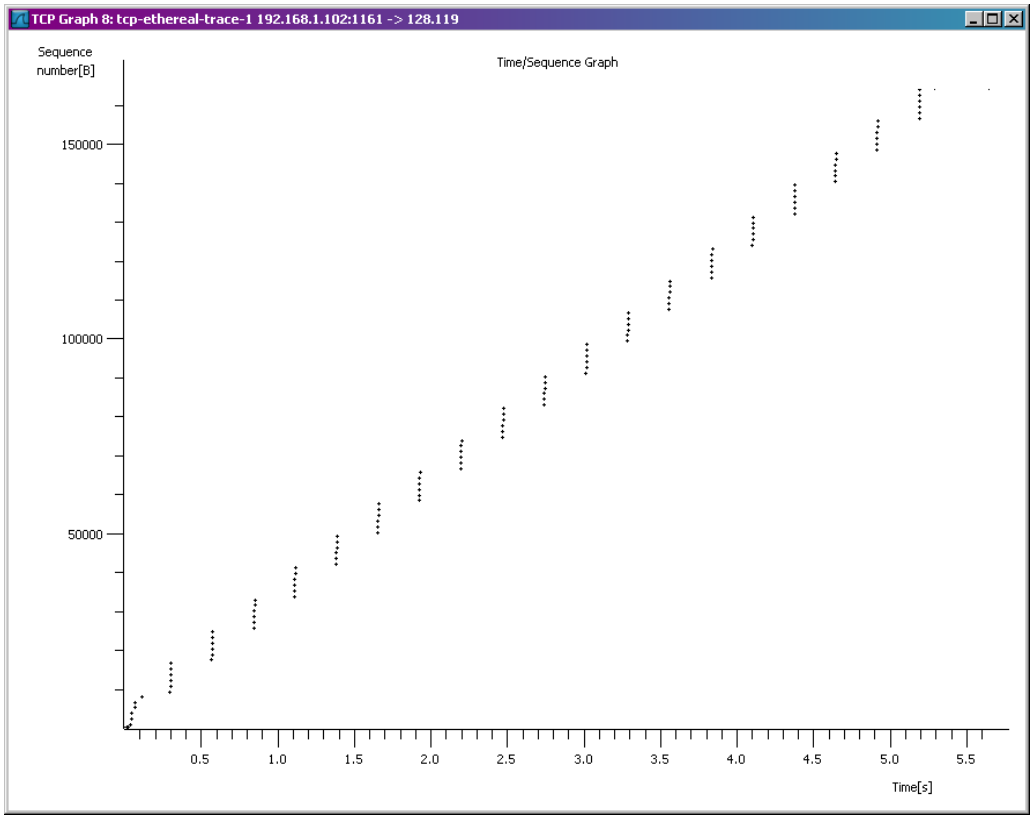

Figure 9: TCP Graph

What does each dot represents and why set of dots stacked above each other?

Segments

Use the *Time-Sequence-Graph(Stevens)* plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behaviour of TCP that we've studied in the text.

What is the throughput (bytes transferred per unit time) for the TCP connection?

1.255*10^6

UDP

TASK 1: Capturing UDP Packets Trace

Before beginning our exploration of UDP, we'll need to use Wireshark to obtain a packet trace of the UDP transfer of domain name resolution from remote server to your computer. You'll do so by using command *nslookup* in command prompt. As you have done in DNS Lab. Set

Step 1: First, filter the packets displayed in the Wireshark window by entering "udp" into the display filter specification window. What do you observe? What is the difference in protocol column of each segment?

Protocol coloumn shows DNS , SSDP and DHCP protocols

Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields.

1; Source Port
2: Destination port

3: Length
4: Checksum

By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

The UDP header has a fixed length of 8 bytes. Each of these 4 header fields is 2 bytes long.

What is the value in the Length field of segment? Verify your claim with your captured UDP packet by reason.

The length field specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next.
The length of UDP payload for selected packet is 32 bytes. 40 bytes - 8 bytes = 32 bytes.

What is the maximum number of bytes that can be included in a UDP payload?

The maximum number of bytes that can be included in a UDP payload is (2^16 – 1) bytes plus the header bytes. This gives 65535 bytes – 8 bytes = 65527 bytes.

What is the largest possible source port number?

The largest possible source port number is (2^16 – 1) = 65535.

What is the protocol number for UDP and TCP? Give your answer in both hexadecimal and decimal notation. (Hint: You'll need to look into the Protocol field of the IP datagram containing this UDP segment)

The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value

The IP protocol number for TCP is 0x06 hex, which is 6 in decimal value

Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. Describe the relationship between the port numbers in the two packets. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet).

The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.

ICMP and Ping

Ping program is simple tool that allows anyone (for example, a network administrator) to verify if a host is live or not. The Ping program in the source host sends a packet to the target IP address; if the target is live, the Ping program in the target host responds by sending a packet back to the source host. Internet Control Message Protocol (ICMP) is a transport layer protocol used to send data for Ping and Traceroute applications.

Task 1: Run Ping Program

Step 1: Open Command Prompt and run following command and write your observations

*ping*www.google.com

_____

_____

_____

_____

Step 2: Enter the ip address obtained in Scenario Task 1, after *ping* command and write your observations

*ping*_____ (IP Address)

_____

_____

_____

_____

Task 2: Capture ICMP packets

Step 1: Do the following

Let's begin this adventure by opening the Windows Command Prompt application

Start up the Wireshark packet sniffer, and begin Wireshark packet capture

Run following command on Command Prompt "*ping* www.google.com" (without quotes)

When the Ping program terminates, stop the packet capture in Wireshark.

Go to Wireshark program and write your observations.

Protocol used is ICMP and the host request"s and the server reply

_____

_____

_____

Step 2: Analyse the packets and answer the following questions

What is the IP address of your host?

172.16.4.33

_____

What is the IP address of the destination host?

142.250.192.100

Why is it that an ICMP packet does not have source and destination port numbers?

The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes.

Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers?

Type= 8 Code =0

What other fields does this ICMP packet have?

Checksum , identifier , sequence Number

How many bytes are the checksum, sequence number and identifier fields?

The checksum, sequence number and identifier fields are two bytes each.

Examine the corresponding ping reply packet. What are the ICMP type and code numbers?

Type 0 , Code 0

What other fields does this ICMP packet have?

Checksum , identifier , sequence Number

How many bytes are the checksum, sequence number and identifier fields?

The checksum, sequence number and identifier fields are two bytes each.

Rubric for Lab Assessment

The student performance for the assigned task during the lab session was:			
Excellent	The student completed assigned tasks without any help from the instructor and showed the results appropriately.	4	
Good	The student completed assigned tasks with minimal help from the instructor and showed the results appropriately.	3	
Average	The student could not complete all assigned tasks and showed partial results.	2	
Worst	The student did not complete assigned tasks.	1	

Instructor Signature: _____ Date: _____

LAB # 4
Reproduce Basic Device Configuration Sequence to Ensure Device Connectivity in Layer 3 Devices using Cisco Packet Tracer Objectives

Objectives

- To trace configuration procedures for basic layer 3 devices using command line interface in Packet Tracer.
- To explain and show network connectivity using Cisco packet tracer.

Pre-Lab Exercise

Read this experiment in its entirety to become familiar with objectives of this lab. Have Cisco Packet Tracer software program installed on your PC and review how to simulate/designs network topologies within it. You may record the terms and sections that require more elaboration for reference. The instructor may provide the class some time to reflect upon these before proceeding with the lab.

Cisco Packet Tracer

Cisco Packet Tracer is a powerful network simulation program that allows students to experiment with network behavior and ask "what if" questions. As an integral part of the Networking Academy comprehensive learning experience, Packet Tracer provides simulation, visualization, authoring, assessment, and collaboration capabilities and facilitates the teaching and learning of complex technology concepts.

Packet Tracer supplements physical equipment in the classroom by allowing students to create a network with an almost unlimited number of devices, encouraging practice, discovery, and troubleshooting. You will simulate network topologies on Cisco Packet Tracer.

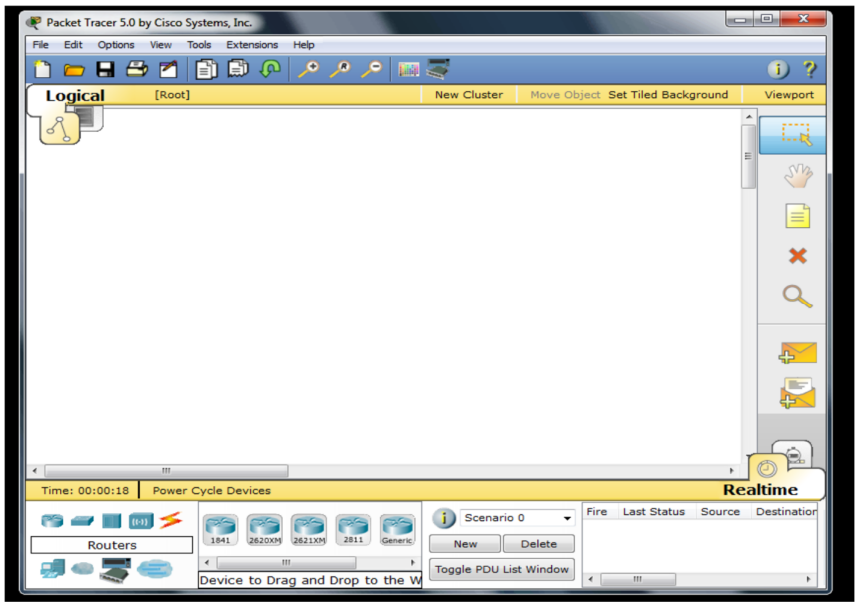

Figure 10: Cisco Packet Tracer

Command Liner Interface (CLI)

After the interface status messages appear and you press Enter, the *Switch>or Router>*prompt will pop up. This is called *user exec mode*, or user mode for short, and although it's mostly used to view statistics. There are three modes each with access to different command sets:

User exec mode—this is the first mode a user has access to after logging into the Switch or Router. This mode allows the user to execute only the basic commands, such as those that show the system's status. The system cannot be configured or restarted from this mode.

Privileged mode—this mode allows users to view the system configuration, restart the system, and enter configuration mode. It also allows all the commands that are available in user mode. You enter it via the enable command like this:

Switch>enable

Switch#

Privileged mode can be identified by the # prompt following the router or switch name. You can go back from privileged mode into user mode by using the **disable** command:

Switch#**disable**

Switch>

Configuration mode— this mode allows users to modify the running system configuration. To enter configuration mode, enter the command **configure terminal** from privileged mode.

Switch#**configure terminal**

Switch(config)#

Configuration mode has various sub modes, starting with global configuration mode, which can be identified by the (config)# prompt following the router name. As the configuration mode submodes change depending on what is being configured, the words inside the parentheses change.

Mode	Definition
User exec mode	Limited to basic monitoring commands
Privileged exec mode	Provides access to all other router commands
Global configuration mode	Commands that affect the entire system
Specific Configuration mode	Commands that affect interfaces/processes only
Setup mode	Interactive configuration dialog

Enhanced Editing Commands

Following commands are very useful while working with CISCO IOS.

Command	Meaning
Ctrl+A	Moves your cursor to the beginning of the line
Ctrl+E	Moves your cursor to the end of the line
Esc+B	Moves back one word
Ctrl+B	Moves back one character
Ctrl+F	Moves forward one character
Esc+F	Moves forward one word
Ctrl+D/ Backspace	Deletes a single character
Ctrl+R	Redisplays a line

Ctrl+U	Erases a line
Ctrl+W	Erases a word
Ctrl+Z	Ends configuration mode and returns EXEC

In-Lab Exercise

Topology Diagram

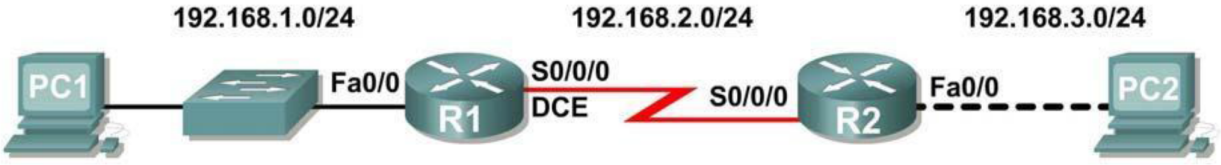

Figure 11: Network Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	NA
	S0/0/0	192.168.2.1	255.255.255.0	NA
R2	Fa0/0	192.168.3.0	255.255.255.0	NA
	S0/0/0	192.168.2.2	255.255.255.0	NA
PC1	NA	192.168.1.10	255.255.255.0	192.168.1.1
PC2	NA	192.168.3.10	255.255.255.0	192.168.3.1

Task 1: Cable the Ethernet and Serial Links of the Network

Step 1: Answer the following questions.

What type of cable is used to connect the Ethernet interface on a host PC to the Ethernet interface on a switch?

straight-through Ethernet cable

What type of cable is used to connect the Ethernet interface on a switch to the Ethernet interface on a router?

straight-through Ethernet cable.

What type of cable is used to connect the Ethernet interface on a router to the Ethernet interface on a host PC?

straight-through Ethernet cable.

What type of cable is used to connect the Serial interface on a router R1 to the Serial interface on a router R2?

DTE (Data Terminal Equipment) to DCE (Data Communications Equipment) connections.

Task 2: Perform basic IOS command line interface operations

Step 1: Establish a terminal session to router R1.

The console port is a management port used to provide out-of-band access to a router. It is used to set up the initial configuration of a router and to monitor it.

A rollover cable and an RJ-45 to DB-9 adapter are used to connect a PC to the console port. As you know from your previous studies, terminal emulation software is used to configure the router over the console connection.

Step 2: Which command is used to enter privileged EXEC mode?

Enable command is used

Step 3: Enter global configuration mode. Run the following command and write your observations.

Router#*configure terminal*

Upon running this command, you will be taken from privileged EXEC mode

This mode allows you to make changes to the router's configuration

Task 3: Perform basic Configuration of Router R1.

Step 1: Configure the router name as R1.

Enter the command at the prompt and write your observations.

Router(config)#*hostname R1*

Upon running this command, the router's hostname will be changed to "R1".

You will see the prompt change accordingly, reflecting the new hostname

Step 2: Disable DNS lookup.

Following command is used to disable DNS lookup.

R1(config)#*no ip domain-lookup*

Why would you want to disable DNS lookup in a lab environment?

Disabling DNS lookup allows you to concentrate on the lab objectives without being

concerned about DNS resolution.

What would happen if you disabled DNS lookup in a production environment?

Disabling DNS lookup in a production environment should be approached with caution, as it can significantly

impact network operations, management, and security

Step 3: Configure the EXEC mode password.

Configure the EXEC mode password using the following command. Use class for the password.

R1(config)#enable secret **class**

OR

R1(config)#enable password **class**

Write difference between setting password using enable secret and enable password?

The main difference between enable secret and enable password lies in

the security level provided. enable secret offers stronger security by

encrypting the password, while enable password stores the password in

plaintext form

Step 4: Configure the console password on the router.

Run following commands to set console password on the router. Use cisco as the password. When you are finished, exit from line configuration mode. Write down your observations.

R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#

line console 0: Enters line configuration mode for the console port.
password cisco: Sets the password for the console port to "cisco".
login: Enables password checking for console access, ensuring that users must enter the password to access the console port.
exit: Exits from line configuration mode and returns to global configuration mode.

Step 5: Configure the password for the virtual terminal lines.

Run following commands to set telnet password on the router. Use cisco as the password. When you are finished, exit from line configuration mode.

R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#

line vty 0 4: Enters line configuration mode for the virtual terminal (telnet) lines.
password cisco: Sets the password for telnet access to "cisco".
login: Enables password checking for telnet access, ensuring that users must enter the password to establish telnet sessions.
exit: Exits from line configuration mode and returns to global configuration mode.

Step 6: Configure the FastEthernet0/0 interface.

Configure the FastEthernet0/0 interface with the IP address 192.168.1.1/24 by using following commands. Write down your observations

R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

interface fastethernet 0/0: Enters interface configuration mode for FastEthernet0/0 interface.
ip address 192.168.1.1 255.255.255.0: Assigns the IP address 192.168.1.1 with a subnet mask of 255.255.255.0 to the interface.
no shutdown: Brings the interface up, enabling it to send and receive traffic.

Step 7: Configure the Serial0/0/0 interface.

Discuss the difference between DCE and DTE.

DTE devices are the endpoints of data communication, while DCE devices facilitate the communication process by providing connectivity and managing the transmission medium.

Why it is necessary to set one device as DCE and other as DTE on serial interface link?

setting one device as DCE and the other as DTE on a serial interface link is necessary to establish proper communication between devices, ensure timing synchronization, maintain interface compatibility, adhere to communication protocol standards, and simplify troubleshooting and maintenance.

Configure the Serial0/0/0 interface with the IP address 192.168.2.1/24. Set the clock rate to 64000.

R1(config-if)#interface serial 0/0/0
R1(config-if)#ip address 192.168.2.1 255.255.255.0

R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
What is the significance of setting clock rate?

setting the clock rate on a serial interface is crucial for establishing proper timing synchronization, controlling transmission speed, ensuring interface functionality, facilitating line speed negotiation, and troubleshooting communication issues.

Step 8: Use the following command to provide a description for this interface.
R1(config-if)#description Link to R2
What is the significance of description for the interface?

Adding descriptions to interfaces enhances network documentation, simplifies troubleshooting, aids in configuration management, improves network visualization, and enhances overall understanding of the network infrastructure

Step 9: Save the R1 configuration.
Save the R1 configuration using the following command and write your observations
R1#**copy running-configstartup-config**

What is a shorter version of this command?
R1# write memory

Task 4: Perform Basic Configuration of Router R2.

Step 1: For R2, repeat Steps 1 through 6 from Task 3
Step 2: Configure the Serial 0/0/0 interface with the IP address 192.168.2.2/24.
Write commands for configuration.

```
R2(config)# interface serial 0/0/0
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
```

Step 3: Configure the FastEthernet0/0 interface with the IP address 192.168.3.1/24. Write commands for configuration.

```
R2(config)# interface FastEthernet0/0
R2(config-if)# ip address 192.168.3.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
```

Step 4: Save the R2 configuration.

Save the R2 configuration as done in Task 3 step 9.

Task 5: Configure IP Addressing on the Host PCs.

Step 1: Configure the host PC1.

Configure the host PC1 that is attached to R1 with an IP address of 192.168.1.10/24 and a default gateway of 192.168.1.1.

Step 2: Configure the host PC2.

Configure the host PC2 that is attached to R2 with an IP address of 192.168.3.10/24 and a default gateway of 192.168.3.1.

Explain the significance of gateway.

the default gateway is essential for enabling communication between devices on different networks,

Task 6:Verify and Test the Configurations.

Step 1: Verify that routing tables have the following routes using the show ip route command.

The show ip route command and output will be thoroughly explored in upcoming labs. For now, you are interested in seeing that both R1 and R2 have two routes. Both routes are designated with a C. These are the directly connected networks that were activated when you configured the interfaces on each router. If you do not see two routes for each router as shown in the following output, proceed to Step 2.

Run the following command on R1 and R2 and write your observations.

R1#show ip route

The output of the show ip route command will display the IP routing table on router R1.
You should see entries in the routing table designated with a "C", indicating directly connected networks.
There should be two entries in the routing table for directly connected networks, corresponding to the IP addresses configured on the interfaces of R1.
Each entry should have a network address and a subnet mask, along with an indication that it is directly connected.

Step 2: Verify interface configurations.

Another common problem is router interfaces that are not configured correctly or not activated. Use the following command to quickly verify the configuration of each router's interfaces. Write your observations

R1#show ip interface brief

The output of the show ip interface brief command will display a summary of all interfaces on router R1.
Each interface will be listed along with its IP address, status, protocol, and other relevant information.
You can quickly verify the configuration and status of each interface on R1 using this command.
The "Status" column indicates whether the interface is up (connected and operational) or down (not connected or disabled).
The "Protocol" column indicates the status of the IP protocol on the interface.
Interfaces with IP addresses configured should show as "up/up" in both the "Status" and "Protocol" columns.
If an interface is not configured or is administratively down, it will show as "down/down" in both columns.

Step 3: Test connectivity using ping.

The ping command is a useful tool for troubleshooting Layers 1 through 3 of the OSI model and diagnosing basic network connectivity. This operation can be performed at either the user or privileged EXEC modes. Using ping sends an Internet Control Message Protocol (ICMP) packet to the specified device and then waits for a reply. Pings can be sent from a router or a host PC. Use the ping command to test connectivity between the R1 router and PC1. Write your observation.

R1#ping 192.168.1.10

After entering the ping command followed by the destination IP address (in this case, 192.168.1.10), the router will start sending ICMP echo requests to the specified IP address.

If there is connectivity between R1 and PC1, you will see a series of messages indicating that the ICMP echo requests are being sent and received successfully.

Test connectivity by pinging from each host to the default gateway that has been configured for that host.
From the host attached to R1, is it possible to ping the default gateway? _____
From the host attached to R2, is it possible to ping the default gateway? _____

Task 7: Reflection

Step 1: Attempt to ping from the host connected to R1 to the host connected to R2.
This ping should be unsuccessful.
Step 2: Attempt to ping from the host connected to R1 to router R2.
This ping should be unsuccessful.
Step 3: Attempt to ping from the host connected to R2 to router R1.
This ping should be unsuccessful.
What is missing from the network that is preventing communication between these devices?

Task 8: Create a startup configuration file

Router configurations can be captured to a text (.txt) file and saved for later use. The configuration can be copied back to the router so that the commands do not have to be entered one at a time.
Step 1: View the running configuration of the router using following command.
R1#***show running-config***

Step 2: Copy the command output.
Select the command output. From the HyperTerminal Edit menu, choose the copy command.
Step 3: Paste output in Notepad.
Open Notepad. Notepad is typically found on the Start menu under Programs > Accessories. From the Notepad Edit menu, click Paste.
Step 4: Edit commands.
Some commands will have to be edited or added before the startup script can be applied to a router. Some of these changes are:
Adding a no shutdown command to FastEthernet and serial interfaces that are being used.
Replacing the encrypted text in the enable secret command with the appropriate password.
Removing the mac-address command from the interfaces.
Removing the ip classless command.

Step 5: Save the open file in Notepad to start.txt.

Task 9: Load the start.txt File onto the R1 Router

Step 1: Erase the current startup configuration of R1.

Use following command and confirm the objective when prompted, and answer no if asked to save changes.

R1#***erase startup-config***

Step 2: When the prompt returns, issue the following command.

R1#***reload***

Confirm the objective when prompted. After the router finishes the boot process, choose not to use the AutoInstall facility.

Step 3: View the running and startup configuration of the router and write your observations.

_____

_____

Step 4: Enter global configuration mode.

Router#***configure terminal***

Step 5: Write the commands to verify the running configuration.

_____

_____

Step 6: Write the commands to save running configurations

_____

_____

Rubric for Lab Assessment

The student performance for the assigned task during the lab session was:			
Excellent	The student completed assigned tasks without any help from the instructor and showed the results appropriately.	4	
Good	The student completed assigned tasks with minimal help from the instructor and showed the results appropriately.	3	
Average	The student could not complete all assigned tasks and showed partial results.	2	
Worst	The student did not complete assigned tasks.	1	

Instructor Signature: _____ Date: _____

LAB # 5
To Reproduce Device Configuration and Show Network Convergence using Static and Default Routing

Objectives

- Preparation of basic configuration on router based on CLI.
- Be able to manipulate configuration sequence in order prepare, configure and activate serial and Ethernet interfaces using Packet Tracer.
- To show connectivity between two devices using static routes.

Pre-Lab Exercise

Read this experiment in its entirety to become familiar with objectives of this lab. Also review the portions of chapter 4 of your reference book and try to understand the Routing algorithms. You may record the terms and sections that require more elaboration for reference. The instructor may provide the class some time to reflect upon these before proceeding with the lab.

Routing Basics

Once you create an internetwork by connecting your WANs and LANs to a router, you'll need to configure logical network addresses, like IP addresses, to all hosts on that internetwork for them to communicate successfully throughout it.

The term *routing* refers to taking a packet from one device and sending it through the network to another device on a different network. Routers don't really care about hosts— they only care about networks and the best path to each one of them. The logical network address of the destination host is key to get packets through a routed network. It's the hardware address of the host that's used to deliver the packet from a router and ensure it arrives at the correct destination host. List of the minimum factors a router must know to be able to affectively route packets is:

- Destination address
- Neighbor routers from which it can learn about remote networks
- Possible routes to all remote networks
- The best route to each remote network
- How to maintain and verify routing information

The router learns about remote networks from neighboring routers or from an administrator. It builds a routing table, which is basically a map of the internetwork, and it describes how to find remote networks. If a network is directly connected, then the router already knows how to get to it. You have observed in previous lab that directly connected networks are already in the routing table using *show iproute* command. The router use one of the following two ways to learn how to get to the remote network.

- Static Routing
- Dynamic Routing

Static Routing

The static routing method requires someone to hand-type all network locations into the routing table, which can be a pretty daunting task when used on all but the smallest of networks!

Dynamic Routing

In dynamic routing, a protocol on one router communicates with the same protocol running on neighboring routers. The routers then update each other about all the networks they know about and place this information into the routing table. If a change occurs in the network, the dynamic routing protocols automatically inform

all routers about the event. If static routing is used, the administrator is responsible for updating all changes by hand onto all routers.

We will discuss dynamic routing in detail in upcoming labs. In this lab we will implement static routing to access remote networks.

There are some important things you should know about routing protocols before we get deeper into them. Being familiar with administrative distances, the three different kinds of routing protocols, and routing loops are three of the most important.

Administrative Distances

The *administrative distance (AD)* is used to rate the trustworthiness of routing information received on a router from a neighbor router. An administrative distance is an integer from 0 to 255, where 0 is the most trusted and 255 means no traffic will be passed via this route.

If a router receives two updates listing the same remote network, the first thing the router checks is the AD. If one of the advertised routes has a lower AD than the other, then the route with the lowest AD will be chosen and placed in the routing table. If both advertised routes to the same network have the same AD, then routing protocol metrics like *hop count* and/or the bandwidth of the lines will be used to find the best path to the remote network. The advertised route with the lowest metric will be placed in the routing table, but if both advertised routes have the same AD as well as the same metrics, then the routing protocol will load-balance to the remote network, meaning the protocol will send data down each link.

Default Administrative Distances

Route Source	Default AD
Connected interface	0
Static route	1
EIGRP	90
OSPF	110
RIP	120

As you will progress to dynamic routing you will understand administrative distance and metrics effectively. For static routing metrics value is 0 as router didn't make any decision for route its administrator who configured the routes manually.

In-Lab Exercise

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 Figure 12. Use any Class C Network ID and fill in the Addressing Table to apply an addressing scheme to the network devices. You will then perform the initial router configurations required for connectivity according to your IP assignment. 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.

Topology Diagram

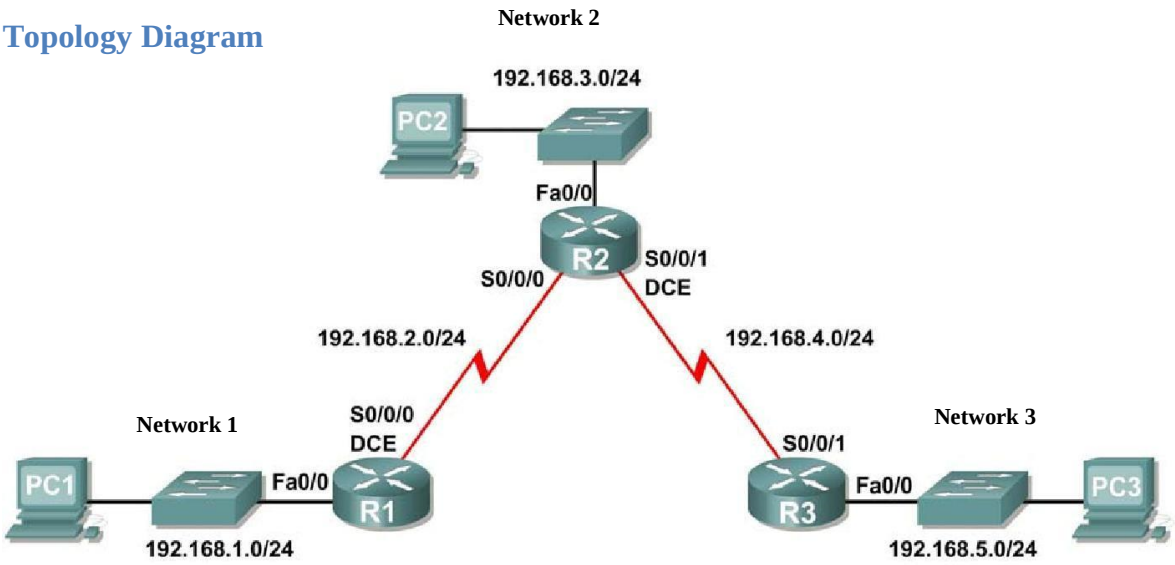

Figure 12: Network Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.2/24	255.255.255.224	NA
	S0/0/0	192.168.30.1/24	255.255.255.224	NA
R2	Fa0/0	192.168.20.2/24	255.255.255.224	NA
	S0/0/0	192.168.30.3/24	255.255.255.224	NA
	S0/0/1	192.168.50.1/24	255.255.255.224	NA
R3	FA0/0	192.168.40.2/24	255.255.255.224	NA
	S0/0/1	192.168.50.3/24	255.255.255.224	NA
PC1	NIC	192.168.50.1/24	255.255.255.224	192.168.50.1/24
PC2	NIC	192.168.50.2/24	255.255.255.224	192.168.50.2/24
PC3	NIC	192.168.50.3/24	255.255.255.224	192.168.50.3/24

Task 1: Perform Basic Router Configuration

Draw the topology diagram on Cisco Packet Tracer. Perform basic configuration on all three routers i.e. assigning IP on LAN and WAN links and other necessary administrative configurations.

Task 2: Configure IP Addressing on the Host PCs

Note: If you have difficulty with any of the commands in task 1 and task 2, see Lab 2

Task 3: Test and Verify the Configurations

Step 1: Test Connectivity of LANs

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?_____yes_____

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

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

Step 2: Test Connectivity of WANs

Check the router interfaces using the ***show ip interface brief*** command. Are all relevant interfaces **up**?_____yes_____

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

_____yes_____

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

_____yes_____

Step 3: Routing Table

Run ***show ip route*** command on each router and answer the following.

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

C 192.168.10.0/24 is directly connected, FastEthernet0/0 C

192.168.30.0/24 is directly connected, Serial0/0/0 S * 0.0.0.0/0 [1/0] via 192.168.30.2

[1/0] via 192.168.30.3

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

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

C 192.168.40.0/24 is directly connected, FastEthernet0/0 C

192.168.50.0/24 is directly connected, Serial0/0/0

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

Routers can be added statically or dynamicaly

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

It can be added statically or dynamically

Task 4: Configure a Static Route Using a Next-Hop Address.

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

Router(config)# **iproute***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.

Step 1: On the R3 router, configure a static route to the network 2 using the Serial 0/0/1 interface of R2 as the next-hop address. Complete the following command and run it on R3.

R3(config)#**ip route** 192.168.50.3/24 255.255.255.224

Step 2: On the R2 router, configure a static route to reach the network 3using the Serial 0/0/1 interface of R3 as the next-hop address. Complete the following command and run it on R2.

R2(config)#**ip route** 192.168.50.1/24 255.255.255.224

Step 3: On the R2 router, configure a static route to reach the network 1 using the Serial 0/0/0 interface of R1 as the next-hop address. Complete the following command and run it on R2.

R2(config)#**ip route** 192.168.30.3/24 255.255.255.224

Step 4: On the R1 router, configure a static route to the network 2using the Serial 0/0/0 interface of R2 as the next-hop address. Complete the following command and run it on R1.

R1(config)#**ip route** 192.168.30.1/24 255.255.255.224

Task 5: Test and Verify the Static Routes

Step 1: View the routing table to verify the new static route entry

Run ***show ip route*** command on each router write down your observations.

Static router have been added to all router

Step 2: Use ping to check connectivity.

Ping to check connectivity between the host PC2 and PC1, is ping successful and why?

Failed , because static connection is not established

Ping to check connectivity between the host PC3 and PC2, is ping successful and why?

Failed , because static connection is not established

Ping to check connectivity between the host PC1 and PC3, is ping successful and why?

Succesful , because static connection is not established

Task 6: 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 Serial 0/0/0 interface of R1 as the next-hop interface. Run the following command on R1

R1(config)#**ip route** 0.0.0.0.0.0.0. 192.168.2.3

View the routing table to verify the new static route entry.

Default static route have been added and represented by s*

Step 2: Remove static route on R1

As we have set the default route on R1 we don't need any static route. Remove the static routes that is currently configured on R1 in Task 4 Step 4 by using the ***no*** form of the command.

Note: *If this route is not to be deleted it cause no problem to routing. It is just done to show you defaultrouting.*

R3(config)#**no ip route** 192.168.2.0 255.255.255.224 192.168.2.3

View the routing table to verify the static route entry is deleted.

Yes it has been deleted

Ping to check connectivity between the host PC2 and PC1, is ping successful and why?

Yes the ping is succesful between pc1 and pc2

Step 3: Configure the R3 router with a default route.

Configure the R3 router with a default route using the Serial 0/0/0 interface of R1 as the next-hop interface. Run the following command on R1

R3(config)#**ip route** 0.0.0.0.0.0.0.0.198.162.2.1

View the routing table to verify the new static route entry.

Default static route has been added and it is represented by s*

Step 4: Use ping to check connectivity.

Ping to check connectivity between the host PC2 and PC1, is ping successful.

Yes ping is succesful between pc1 nd pc2

Ping to check connectivity between the host PC3 and PC2, is ping successful.

Yes ping is succesful between pc3 nd pc2

Ping to check connectivity between the host PC1 and PC3, is ping successful.

No ping is not successful between pc1 and pc3

Task 7: 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 and 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

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**

Rubric for Lab Assessment

The student performance for the assigned task during the lab session was:			
Excellent	The student completed assigned tasks without any help from the instructor and showed the results appropriately.	4	
Good	The student completed assigned tasks with minimal help from the instructor and showed the results appropriately.	3	
Average	The student could not complete all assigned tasks and showed partial results.	2	
Worst	The student did not complete assigned tasks.	1	

Instructor Signature: _____ Date: _____

LAB # 6
To Reproduce a Network and Show Successful Connectivity between Hosts where RIP is Configured in Routers using CISCO Packet Tracer

Objectives

- To construct a network for demonstration of the operation of RIP routing protocol using Cisco Packet Tracer
- To show the connectivity between nodes in a network using RIP on all routers.

Pre-Lab Exercise

Read this experiment in its entirety to become familiar with objectives of this lab. Study in detail and become familiar with the Dynamic Routing basics provided with this laboratory experiment and in the chapter 4 of the reference book. You may record the terms and sections that require more elaboration for reference. The instructor may provide the class some time to reflect upon these before proceeding with the lab.

Dynamic Routing

Dynamic routing is when protocols are used to find networks and update routing tables on routers. This is whole lot easier than using static or default routing, but it will cost you in terms of router CPU processing and bandwidth on network links. A routing protocol defines the set of rules used by a router when it communicates routing information between neighboring routers.

Dynamic routing is further divided into two types as:

- Distance Vector
- Link State

Distance Vector

The distance-vector protocols in use today find the best path to a remote network by judging distance. A distance-vector routing protocol periodically sends out the entire routing table to directly connected neighbors. Example of distance vector protocol is Routing Information Protocol (RIP).

Link State

In link-state protocols, the routers each create three separate tables. One of these tables keeps track of directly attached neighbors, one determines the topology of the entire internetwork, and one is used as the routing table. Link-state routers know more about the internetwork than any distance-vector routing protocol ever could. Link state protocols send updates containing the state of their own links to all other directly connected routers on the network. This is then propagated to their neighbors. Example of link state protocol is OSPF.

In this lab we will learn about distance vector protocol RIP. Link state protocol will be discussed in next lab.

Routing Information Protocol

Routing Information Protocol (RIP) is a true distance-vector routing protocol. RIP sends the complete routing table out of all active interfaces every 30 seconds. It relies on hop count to determine the best way to a remote network, but it has a maximum allowable hop count of 15 by default, so a destination of 16 would be considered unreachable. RIP works okay in very small networks, but it's super inefficient on large networks with slow WAN links or on networks with a large number of routers installed and completely useless on networks that have links with variable bandwidths!

RIP version 1 uses only *classful routing*, which means that all devices in the network must use the same subnet mask. This is because RIP version 1 doesn't send updates with subnet mask information in tow.

RIP version 2 provides something called *prefix routing* and does send subnet mask information with its route updates. This is called *classless routing.* You'll rarely see RIPv1 used in today's networks. Even RIPv2 doesn't get much attention in the objectives. So why am I even telling you about them? Because it helps me explain routing protocols a little better before we get into the much more advanced, and very much focused upon, OSPF protocol.

In-Lab Exercise

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 Figure 13. Assign any Network_ID from Class A and fill in the table. You will then perform the initial router configurations required for connectivity. Use the IP addresses according to your IP assignment. First test the connections between directly connected devices, and then test connectivity between devices that are not directly connected. You will configure the dynamic routing protocol RIP to add remote networks, this will allow communication between the hosts of different networks. View the routing table after each dynamic route is added to observe how the routing table has changed.

Topology Diagram

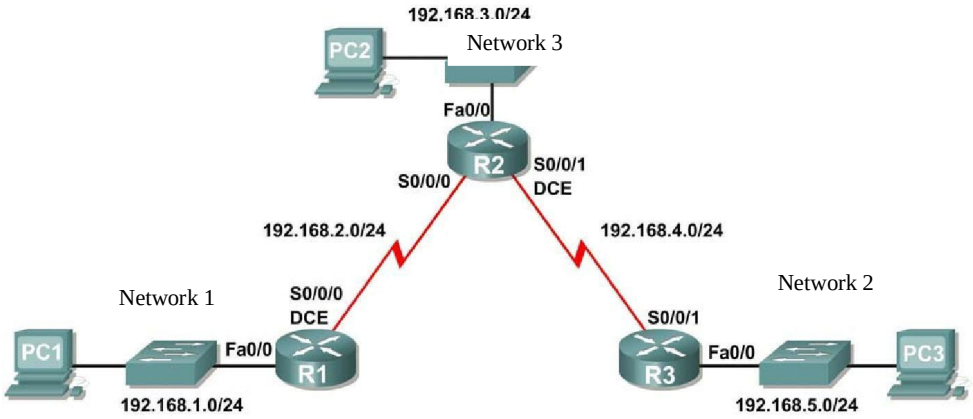

Figure 13: Network Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0			
	S0/0/0			
R2	Fa0/0			
	S0/0/0			
	S0/0/1			
R3	FA0/0			
	S0/0/1			

PC1	**NIC**			
PC2	**NIC**			
PC3	**NIC**			

Task 1: Perform the Basic Router Configuration

Draw the topology diagram on Cisco Packet Tracer. Perform basic configuration on all three routers i.e. assigning IP on LAN and WAN links and other necessary administrative configurations.

Task 2: Configure IP Addressing on the Host PCs

Task 3: Test and Verify the Configurations

Note: If you have difficulty with any of the commands in task 1 to task 3, see Lab 2.

Task 4: Configure RIP v1

To configure RIP, use the following syntax:

Enable the dynamic routing protocol RIP, enter global configuration mode and use the ***router*** command

Router(config)#**router rip**

Router(config-router)#**network***NETWORK 1*

Router(config-router)#**network***NETWORK 2*

Router(config-router)#**network***NETWORK N*

NETWORK –Network that is directly connected with that router. You have to enter each directlyconnected network separately using ***network*** command

Task 5: Enable RIPv1 on Router 1

Step 1: Run following command.

R1(config)#***router rip***

Step 2: Enter network addresses.

R1(config-router)#***network***_____

R1(config-router)#***network***_____

Task 6: Enable RIPv1 on Router 3

Step 1: Run following command.

R3(config)#***router rip***

Step 2: Complete the following commands and run on R2.

R3(config-router)#***network*** _____

R3(config-router)#***network*** _____

Step 3: Use ping to check connectivity.

Ping to check connectivity between the host PC2 and PC1, is ping successful and why?

_____

_____

Ping to check connectivity between the host PC3 and PC2, is ping successful and why?

_____

_____

Ping to check connectivity between the host PC1 and PC3, is ping successful and why?

_____

Task 7: Enable RIPv1 on Router 2

Step 1: Run following command.

R2(config)#***router rip***

Step 2: Complete the following commands and run on R2.

R2(config-router)#***network*** _____

R2(config-router)#***network*** _____

R2(config-router)#***network*** _____

Task 8: Test and verify the routes

Step 1: View the routing table to verify the new route entries

Run ***show ip route*** command on each router write down your observations.

_____

_____

_____

_____

_____

_____

Step 2: What is the value of Administrative Distance for RIP networks?

_____

_____

Step 3: What is the metrics value against each network in R1 routing table? Explain it.

_____

_____

_____

_____

Step 4: Use ping to check connectivity.

Ping to check connectivity between the host PC2 and PC1, is ping successful?

_____

Ping to check connectivity between the host PC3 and PC2, is ping successful?

_____

Ping to check connectivity between the host PC1 and PC3, is ping successful?

Task 9: Summary, Reflection, and Documentation

With the completion of this lab, you have:

- Configured your first network with a dynamic routing protocol RIP to provide full connectivity to all networks
- Observed how a route is installed in the routing table when you correctly configure and activate and interface

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**

Rubric for Lab Assessment

The student performance for the assigned task during the lab session was:			
Excellent	The student completed assigned tasks without any help from the instructor and showed the results appropriately.	4	
Good	The student completed assigned tasks with minimal help from the instructor and showed the results appropriately.	3	
Average	The student could not complete all assigned tasks and showed partial results.	2	
Worst	The student did not complete assigned tasks.	1	

Instructor Signature: _____ Date: _____

LAB # 7
To Reproduce a Network and Show Successful Connectivity between Hosts where OSPF is Configured in Routers using CISCO Packet Tracer

Objectives

- To construct a network for demonstration of the operation of OSPF routing protocol using Cisco Packet Tracer
- To show the connectivity between nodes in a network using OSPF on all routers.

Pre-Lab Exercise

Read this experiment in its entirety to become familiar with objectives of this lab. Study in detail and become familiar with the Link State Routing basics provided with this laboratory experiment and in the chapter 4 of the reference book. You may record the terms and sections that require more elaboration for reference. The instructor may provide the class some time to reflect upon these before proceeding with the lab.

Open Shortest Path First (OSPF) Basics

Open Shortest Path First (OSPF) is an open standard link state routing protocol that's been implemented by a wide variety of network vendors, including Cisco. And it's that open standard characteristic that's the key to OSPF's flexibility and popularity.

OSPF works by using the Dijkstra algorithm to initially construct a shortest path tree and follows that by populating the routing table with the resulting best paths. It is quickly convergent. Another two great advantages OSPF offers are that it supports multiple, equal-cost routes to the same destination, also supports both IP and IPv6 routed protocols. OSPF's best features are:

- Allows for the creation of areas and autonomous systems
- Minimizes routing update traffic
- Is highly flexible, versatile, and scalable
- Supports VLSM/CIDR
- Offers an unlimited hop count
- Is open standard and supports multi-vendor deployment

Here are three of the biggest reasons to implement OSPF in a way that makes full use of its intentional, hierarchical design:

- To decrease routing overhead
- To speed up convergence
- To confine network instability to single areas of the network

OSPF Terminology

Imagine being given a map and compass with no prior concept of east, west, north or south—not even what rivers, mountains, lakes, or deserts are. I'm guessing that without any ability to orient yourself in a basic way, your cool, new tools wouldn't help you get anywhere but completely lost, right? This is exactly why we're going to begin exploring OSPF by getting you solidly acquainted with a fairly long list of terms before setting out from base camp into the great unknown! Here are those vital terms to commit to memory now:

OSPF Metrics

OSPF uses a metric referred to as *cost*. A cost is associated with every outgoing interface included in an SPF tree. The cost of the entire path is the sum of the costs of the outgoing interfaces along the path. Cisco uses a

simple equation of 10^8/*bandwidth*, where *bandwidth* is the configured bandwidth for the interface. Using this rule, a 100 Mbps Fast Ethernet interface would have a default OSPF cost of 1.

Link

A *link* is a network or router interface assigned to any given network. When an interface is added to the OSPF process, it's considered to be a link. This link, or interface, will have up or down state information associated with it as well as one or more IP addresses.

Router ID

The *router ID (RID)* is an IP address used to identify the router. Cisco chooses the router ID by using the highest IP address of all configured loopback interfaces. If no loopback interfaces are configured with addresses, OSPF will choose the highest IP address out of all active physical interfaces. To OSPF, this is basically the "name" of each router.

Neighbor

Neighbors are two or more routers that have an interface on a common network, such as two routers connected on a point-to-point serial link. OSPF neighbors must have a number of common configuration options to be able to successfully establish a neighbor relationship, and all of these options must be configured exactly the same way:

- Area ID
- Stub area flag
- Authentication password (if using one)
- Hello and Dead intervals

Adjacency

An *adjacency* is a relationship between two OSPF routers that permits the direct exchange of route updates. Unlike EIGRP, which directly shares routes with all of its neighbors, OSPF is really picky about sharing routing information and will directly share routes only with neighbors that have also established adjacencies. And not all neighbors will become adjacent—this depends upon both the type of network and the configuration of the routers. In multi-access networks, routers form adjacencies with designated and backup designated routers. In point-to-point and point-to-multipoint networks, routers form adjacencies with the router on the opposite side of the connection.

Designated Router

A *designated router (DR)* is elected whenever OSPF routers are connected to the same broadcast network to minimize the number of adjacencies formed and to publicize received routing information to and from the remaining routers on the broadcast network or link. Elections are won based upon a router's priority level, with the one having the highest priority becoming the winner. If there's a tie, the router ID will be used to break it. All routers on the shared network will establish adjacencies with the DR and the BDR which ensures that all router's topology tables are synchronized.

Backup Designated Router

A *backup designated router (BDR)* is a hot standby for the DR on broadcast, or multi-access, links. The BDR receives all routing updates from OSPF adjacent routers but does not disperse LSA updates.

Hello protocol The OSPF Hello protocol provides dynamic neighbor discovery and maintains neighbor relationships. Hello packets and Link State Advertisements (LSAs) build and maintain the topological database. Hello packets are addressed to multicast address 224.0.0.5.

Neighborship Database

The *neighborship database* is a list of all OSPF routers for which Hello packets have been seen. A variety of details, including the router ID and state, are maintained on each router in the neighborship database.

Topological Database

The *topological database* contains information from all of the Link State Advertisement packets that have been received for an area. The router uses the information from the topology database as input into the Dijkstra algorithm that computes the shortest path to every network.

Link State Advertisement

A *Link State Advertisement (LSA)* is an OSPF data packet containing link-state and routing information that's shared among OSPF routers. An OSPF router will exchange LSA packets only with routers to which it has established adjacencies.

OSPF Areas

An *OSPF area* is a grouping of contiguous networks and routers. All routers in the same area share a common area ID. Because a router can be a member of more than one area at a time, the area ID is associated with specific interfaces on the router. This would allow some interfaces to belong to area 1 while the remaining interfaces can belong to area 0. All of the routers within the same area have the same topology table. When configuring OSPF with multiple areas, you've got to remember that there must be an area 0 and that this is typically considered the backbone area. Areas also play a role in establishing a hierarchical network organization—something that really enhances the scalability of OSPF!

Broadcast (multi-access)

Broadcast (multi-access) networks such as Ethernet allow multiple devices to connect to or access the same network, enabling a *broadcast* ability in which a single packet is delivered to all nodes on the network. In OSPF, a DR and BDR must be elected for each broadcast multi-access network.

Non-Broadcast multi-access

Non-Broadcast multi-access (NBMA) networks are networks such as Frame Relay, X.25, and Asynchronous Transfer Mode (ATM). These types of networks allow for multi-access without broadcast ability like Ethernet. NBMA networks require special OSPF configuration to function properly.

Point-to-Point

Point-to-point refers to a type of network topology made up of a direct connection between two routers that provides a single communication path. The point-to-point connection can be physical—for example, a serial cable that directly connects two routers—or logical, where two routers thousands of miles apart are connected by a circuit in a Frame Relay network. Either way, point-to-point configurations eliminate the need for DRs or BDRs.

Point-to-Multipoint

Point-to-multipoint refers to a type of network topology made up of a series of connections between a single interface on one router and multiple destination routers. All interfaces on all routers share the point-to-multipoint connection and belong to the same network. Point-to-multipoint networks can be further classified according to whether they support broadcasts or not. This is important because it defines the kind of OSPF configurations you can deploy.

In-Lab Exercise

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 Figure 14. Assign Network_ID from Class B i.e. 172.17.0.0/24 and fill in the table. 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. You will then perform the initial router configurations required for connectivity. Use the IP addresses according to your IP assignment. First test the connections between directly connected devices, and then test connectivity between devices that are not directly connected. You will configure the dynamic routing protocol OSPF to add remote networks, this will allow communication between the hosts of different networks. View the routing table after each dynamic route is added to observe how the routing table has changed.

Topology Diagram

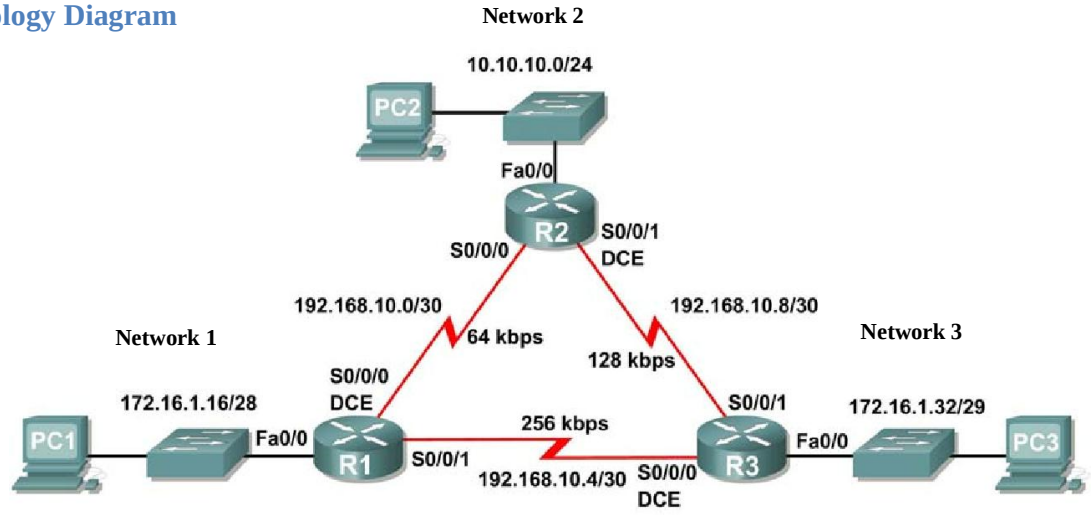

Figure 14: Network Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0			
	S0/0/0			
	S0/0/1			
R2	Fa0/0			
	S0/0/0			
	S0/0/1			
R3	Fa0/0			
	S0/0/0			
	S0/0/1			
PC1	NIC			
PC2	NIC			

PC3	NIC			

Task 1: Prepare the Network

Task 2: Perform Basic Router Configurations.

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

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.

Task 3: Perform IP configuration on host PC's

Task 4: Configure OSPF

Step 1: Learn how to enable OSPF

Router(config)#**router ospf***Process ID*

Router(config-router)#**network** *Network1 Wildcard mask* **area** *OSPF areas*

Router(config-router)#**network***Network2 Wildcard mask* **area** *OSPF areas*

.

.

Router(config-router)#**network***NetworkN Wildcard mask* **area** *OSPF areas*

Process ID: A value in the range from 1 to 65,535 identifies the OSPF process ID. It's a unique number on this router that groups a series of OSPF configuration commands under a specific running process. Different OSPF routers don't have to use the same process ID to communicate. It's a purely local value that doesn't mean a lot, but you still need to remember that it cannot start at 0; it has to start at a minimum of 1.

Network – Network that is directly connected with that router. You have to enter each directly connected network (range from 1 to N) separately using ***network*** command

Wildcard mask – Inverse of a subnet mask. For Example, the inverse of the subnet mask255.255.255.0 is 0.0.0.255. To calculate the inverse of the subnet mask, subtract the subnet mask from 255.255.255.255:

```
  255.255.255.255
– 255.255.255.0          Subtract the subnet mask
-------------------------
  0.  0.  0.  255        Wildcard mask
```

OSPF areas–An *OSPF area* is a grouping of contiguous networks and routers. All routers in the same area share a common area ID. Because a router can be a member of more than one area at a time, the area ID is associated with specific interfaces on the router. This would allow some interfaces to belong to area 1 while the remaining interfaces can belong to area 0. All of the routers within the same area have the same topology table. When configuring OSPF with multiple areas, you've got to remember that there must be an area 0 and that this is typically considered the backbone area. Areas also play a role in establishing a hierarchical network organization—something that really enhances the scalability of OSPF!

Task 5: Configure OSPF on the R1 Router

Step 1: Enable OSPF. 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**

Step 2: Configure the networks

Once you are in the Router OSPF configuration sub-mode, configure the networks to be included in the OSPF updates that are sent out of R1 i.e. networks directly connected with R1.

Step 3: Configure the Network 1

Wildcard mask has been calculated for this network in wildcard mask example i.e. 0.0.0.255. Complete the following command and configure it on Router 1. Enter OSPF area of 0 for the *OSPF areas* parameter. You will use same OSPF area for whole lab.

R1(config-router)#**network** _____

Step 4: Configure the router to advertise the networks attached to the Serial0/0/0 and Serial0/0/1 interface respectively.

Calculate the wildcard mask for the network, complete the following commands and enter in Router OSPF configuration sub-mode.

R1(config-router)#**network** _____ **area** *0*

R1(config-router)#**network** _____ **area** *0*

Step 5: When you are finished with the OSPF configuration for R1, return to privileged EXEC mode and save the current configuration to NVRAM.

R1(config-router)#**end**

Task 6: Configure OSPF on the R2 and R3 Routers

Step 1: Enable OSPF routing on the R2 router. Write the command to enable OSPF.

_____

_____

Step 2: Configure the router R2 to advertise the directly connected networks. Write down the commands and run in Router OSPF configuration sub-mode.

_____

_____

_____

_____

Step 3: Notice that Link State protocol sends a notification message to the console stating that a neighbor relationship with another OSPF router has been established.

What is the IP address of the OSPF neighbor router?

_____

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

_____

Step 4: Enable OSPF routing on the R3 router. Write the command to enable OSPF.

_____

_____

Step 5: Configure the router R3 to advertise the directly connected networks. Write down the commands and run in Router OSPF configuration sub-mode.

_____

_____

_____

Task 7: 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:

- IP address configured with the OSPF *router-id* command.
- Highest IP address of any of the router's loopback addresses.
- 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. Run the following command on each router to check router ID

Router#**showip protocols**

What is the router ID for R1?

_____

What is the router ID for R2?

_____

What is the router ID for 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 *ipospfneighbor*s command to verify that the router IDs have changed.

Task 8: Verify OSPF Operation

Step 1: On the R1 router, Use the *show ipospfneighbor* command and write your observations.

R1#**show ipospfneighbor**

_____

_____

Step 2: On the R1 router, use the *show ip protocols* command and write your observations.

R1#**show ip protocols**

_____

_____

_____

_____

Step 3: Examine OSPF Routes in the Routing Tables

R1#**show ip route**

_____

_____

_____

_____

Step 4: Repeat Step 1 to Step 3 for Router R2 and R3

_____

_____

_____

_____

_____

_____

Step 5: Use ping command to access PC1 to PC2 and PC1 to PC3 verify that OSPF is configured correctly. Is ping successful?

_____

_____

Step 6: Use the show interfaces serial0/0/0 command on the R1 router to view the bandwidth of the Serial 0/0/0 interface. What is the default bandwidth of link?

R1#show interfaces serial0/0/0

_____

_____

Step 7: Calculate the cost of link to find metrics value using the formula 10^8/bandwidth. Is calculate and router measured value same?

_____

Task 9: Configure Additional Features

Step 1: Use the bandwidth command to change the bandwidth of the serial interface serial0/0/0 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**

R2 router:

R2(config)#**interface serial0/0/0**

R2(config-if)#**bandwidth 64**

Step 2: Use the *show ipospf interface* command on the R1 router to verify the cost of the serial links. What is new cost of serial0/0/0 link?

_____

_____

Step 3: Use the *show ipospfneighbor* command on R1 to view the Dead Time counter. What is default dead interval and what do you observe?

_____

_____

Step 4: Configure the OSPF Hello and Dead intervals.

The OSPF Hello and Dead intervals can be modified manually using the*ipospf hello-interval*and*ipospf dead-interval*interface commands. Use these commands to changethe 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)#**ipospf hello-interval 5**

R1(config-if)#**ipospf dead-interval 20**

Step 5: 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)#**ipospf hello-interval 5**

R2(config-if)#**ipospf dead-interval 20**

Rubric for Lab Assessment

The student performance for the assigned task during the lab session was:			
Excellent	The student completed assigned tasks without any help from the instructor and showed the results appropriately.	4	
Good	The student completed assigned tasks with minimal help from the instructor and showed the results appropriately.	3	
Average	The student could not complete all assigned tasks and showed partial results.	2	
Worst	The student did not complete assigned tasks.	1	

Instructor Signature: _____ Date: _____

LAB # 8

To Trace Different Traffic Flows in Computer Networks using Standard ACL

Objectives

- To follow the DHCP protocol configuration for IP address assignment using Packet Tracer
- To identify and understand configurations of standard ACL using Packet Tracer

Pre-Lab Exercise

Read this experiment in its entirety to become familiar with objectives of this lab. Study in detail and become familiar with the basics of Dynamic Host Configuration Protocol and Access Control Lists (ACLs) provided with this laboratory experiment. You may record the terms and sections that require more elaboration for reference. The instructor may provide the class some time to reflect upon these before proceeding with the lab.

Scenario A: Dynamic Host Configuration Protocol

The **Dynamic Host Configuration Protocol** (**DHCP**) is a standardized networking protocol used on IP networks that dynamically configures IP addresses and other information that is needed for Internet communication. DHCP allows computers and other devices to receive an IP address automatically from a central DHCP server, reducing the need for a network administrator or a user from having to configure these settings manually.

There are two methods to implement DHCP.

1. Router act as DHCP server and assign IPs to devices.
2. Router forward the DHCP requests to DHCP server.

Following Commands are used to implement DHCP protocol on Cisco Router.

R1(config)#ipdhcp pool *Pool_Name*

R1(dhcp-config)#network *Network ID Subnet Mask*

R1(dhcp-config)#default-router *Gateway IP*

R1(dhcp-config)#exit

Pool_Nmae: It is the pool name we can use whatever we want. This command gets us into the DHCP Configuration mode.

Network ID: It defines the network to be assigned IP's automatically.

Subnet Mask: It defines the network range to be leased.

Gateway IP: Default gateway for this network

Scenario B: Access Control List

Network security is a huge subject. One of the most important skills a network administrator needs is mastery of access control lists (ACLs). Administrators use ACLs to stop traffic or permit only specified traffic while stopping all other traffic on their networks.

Network designers use firewalls to protect networks from unauthorized use. Firewalls are hardware or software solutions that enforce network security policies. Consider a lock on a door to a room inside a building. The lock only allows authorized users with a key or access card to pass through the door. Similarly, a firewall filters unauthorized or potentially dangerous packets from entering the network. On a Cisco router, you can configure a simple firewall that provides basic traffic filtering capabilities using ACLs.

An ACL is a sequential list of permit or deny statements that apply to addresses or upper-layer protocols. ACLs provide a powerful way to control traffic into and out of your network. You can configure ACLs for all routed network protocols.

What is an ACL?

An ACL is a router configuration script that controls whether a router permits or denies packets to pass based on criteria found in the packet header. ACLs are also used for selecting types of traffic to be analyzed, forwarded, or processed in other ways. You can configure one ACL per protocol, per direction, per interface:

- One ACL per protocol-To control traffic flow on an interface, an ACL must be defined for each protocol enabled on the interface.
- One ACL per direction-ACLs control traffic in one direction at a time on an interface. Two separate ACLs must be created to control inbound and outbound traffic.
- One ACL per interface-ACLs control traffic for an interface, for example, Fast Ethernet 0/0.

ACL Operation

How ACLs Work

ACLs define the set of rules that give added control for packets that enter inbound interfaces, packets that relay through the router and packets that exit outbound interfaces of the router. ACLs do not act on packets that originate from the router itself.

ACLs are configured either to apply to inbound traffic or to apply to outbound traffic.

Inbound ACLs-Incoming packets are processed before they are routed to the outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet is discarded. If the packet is permitted by the tests, it is then processed for routing.

Outbound ACLs-Incoming packets are routed to the outbound interface, and then they are processed through the outbound ACL.

ACL statements operate in sequential order. They evaluate packets against the ACL, from the top down, one statement at a time. If a packet header and an ACL statement match, the rest of the statements in the list are skipped, and the packet is permitted or denied as determined by the matched statement. If a packet header does not match an ACL statement, the packet is tested against the next statement in the list. This matching process continues until the end of the list is reached.

Access List Types

Cisco IOS access lists are divided into two distinct types:

- **Standard ACLs:** This type of ACL is the simplest one since it only filters traffic based on source IP addresses. In other words, this ACL can be used only when you need to permit or deny traffic from a specific host IP address or a specific source network.
- **Extended ACLs:** This type of ACL is the most preferred one and the most advanced as well. Extended ACLs filter IP packets based on several attributes, for example, protocol type, source IP address, destination IP address, source TCP or UDP ports, destination TCP or UDP ports, and optional protocol type information for finer granularity of control.

Numbering and Naming ACLs

Using numbered ACLs is an effective method for determining the ACL type on smaller networks with more homogeneously defined traffic. However, a number does not inform you of the purpose of the ACL. For this reason you can use a name to identify a Cisco ACL.

The rule to designate numbered ACLs and named ACLs is:

Numbered ACL

You assign a number based on which protocol you want to filtered:

- (1 to 99) and (1300 to 1999): Standard IP ACL
- (100 to 199) and (2000 to 2699): Extended IP ACL

In case you are wondering why numbers 200 to 1299 are skipped, it is because those numbers are used by other protocols.

Named ACL

You assign a name by providing the name of the ACL:

- Names can contain alphanumeric characters.
- It is suggested that the name be written in CAPITAL LETTERS.
- Names cannot contain spaces or punctuation and must begin with a letter.
- You can add or delete entries within the ACL.

Where to Place ACLs

The proper placement of an ACL to filter undesirable traffic makes the network operate more efficiently. ACLs can act as firewalls to filter packets and eliminate unwanted traffic. Where you place ACLs can reduce unnecessary traffic. For example, traffic that will be denied at a remote destination should not use network resources along the route to that destination.

Every ACL should be placed where it has the greatest impact on efficiency. The basic rules are:

- Because standard ACLs do not specify destination addresses, place them as close to the destination as possible.
- Locate extended ACLs as close as possible to the source of the traffic denied. This way, undesirable traffic is filtered without crossing the network infrastructure.

In-Lab Exercise

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 Figure 15. Assign Network_ID from Class C as shown in the figure and fill in the table. You will then perform the initial router configurations required for connectivity. Use the IP addresses according to your IP assignment. First test the connections between directly connected devices, and then test connectivity between devices that are not directly connected. You will configure the dynamic routing protocol RIP to add remote networks, this will allow communication between the hosts of different networks. View the routing table after each dynamic route is added to observe how the routing table has changed. After that, configure DHCP protocol on different networks so that all hosts from the network get IP address dynamically. Also create Access Control Lists (ACLs) to block networks from gaining access according to the given scenarios.

Topology Diagram

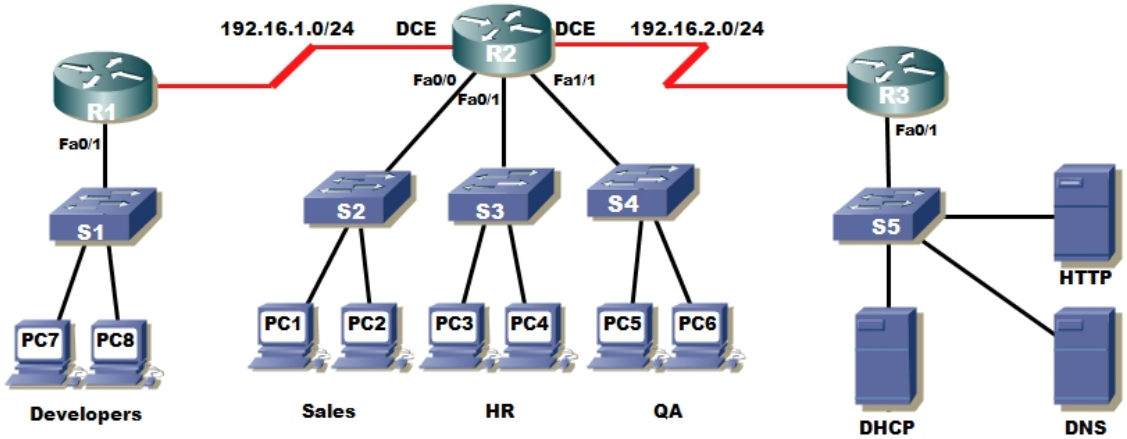

Figure 15: Network Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Gateway
R1	**Se0/1/0**			
	Fa0/0			
R2	**Se0/1/0**			
	Se0/2/0			
	Fa0/0			
	Fa0/1			
	Fa1/0			
R3	**Se0/2/0**			
	Fa0/0			
HTTP Server	**N/A**			
DNS Server	**N/A**			
DHCP Server	**N/A**			
PC1 – PC8	**NIC**	Obtain Automatically	Obtain Automatically	

Task 1: Prepare the Network

Task 2: Perform Basic Router Configurations.

Step 1: Configure Ethernet interfaces on R1.

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.

Task 3: Perform IP configuration on host PC's

Now you don't need to assign IP address on each PC. We will use DHCP to assign to get IP address automatically. Select DHCP on instead of Static on PC IP Configuration.

Step 1: Configure DHCP for Developer's Network

Complete the following commands and run on Router R1.

R1(config)#_____

R1(dhcp-config)#_____

R1(dhcp-config)#_____

R1(dhcp-config)#_____

Step 2: Configure DHCP for Sales Network

Complete the following commands and run on router R2.

R1(config)#_____

R1(dhcp-config)# _____

R1(dhcp-config)# _____

R1(dhcp-config)# _____

Step 3: Configure DHCP for HR Network

Complete the following commands and run on router R2.

R1(config)#_____

R1(dhcp-config)#_____

R1(dhcp-config)#_____

R1(dhcp-config)# _____

Step 4: Configure DHCP for QA Network

Complete the following commands and run on router R2.

R1(config)#_____

R1(dhcp-config)# _____

R1(dhcp-config)# _____

R1(dhcp-config)# _____

Task 4: Verify the Network

Use ping tool to check connectivity between the hosts. Is ping successful?

_____

Task 5: Configuring Standard IP Access Lists

The access list may be created with one or more access-list commands while in global configuration mode. Second, the access list is applied to or referenced by other commands, such as the ip access-group command which applies the ACL to an interface. An example would be the following:

R1#config terminal

R1(config)#access-list *# {permit | deny} ip address wildcard mask*

R1(config)#interface *{serial | Fast Ethernet}*

R1(config-if)#ip access-group *# {in | out}*

***Implicit deny statement*:** Every access list contains a final "deny" statement that matches all packets. This is called the implicit deny. Because the implicit deny statement is not visible in show command output, it is often overlooked, with serious consequences.

At least one permit statement is required: There is no requirement that an ACL contain a deny statement. If nothing else, the implicit deny any statement takes care of that. But if there are no permit statements, the effect will be the same as if there were only a single deny any statement.

Wildcard mask: In identifying IP addresses, ACLs use a wildcard mask instead of a subnet mask. Initially, the masks might look the same, but closer observation reveals that they are very different. Remember that a binary 0 in a wildcard mask instructs the router to match the corresponding bit in the IP address.

In/out: When deciding whether an ACL should be applied to inbound or outbound traffic, always view things from the perspective of the router. In other words, determine whether traffic is coming into the router, inbound, or leaving the router, outbound.

Applying ACLs: Extended ACLs should be applied as close to the source as possible, thereby conserving network resources. Standard ACLs, by necessity, must be applied as close to the destination as possible. This is because the standard ACL can match only at the source address of a packet.

Standard ACLs

Step 1: Your task is to block 192.16.3.3 from gaining access on 192.16.5.0. While 192.16.3.3 must be able to communicate with networks. Other computer from the network of 192.16.3.0 must be able to connect with the network of 192.16.5.0.

Run following commands on router R2.

R2#config terminal

R2(config)#access-list 1 deny host 192.16.3.3

R2(config)#access-list 1 permit any

R2(config)#interface fastEthernet 0/1

R2(config-if)#ip access-group 1 out

Step 2: Verify if the access list is created successfully.

Run following command on router R2 and write down your observations.

R2# *show access-list*

_____

_____

Step 3: Block the network of 192.16.3.0 from gaining access on 192.16.4.0. While 192.16.3.0 must be able to communicate with networks.

Run following commands on router R2.

R2(config)#access-list 2 deny 192.16.3.0 0.0.0.255

R2(config)#access-list 2 permit any

R2(config)#interface fastethernet 0/0

R2(config-if)#ip access-group 2 out

Rubric for Lab Assessment

The student performance for the assigned task during the lab session was:			
Excellent	The student completed assigned tasks without any help from the instructor and showed the results appropriately.	4	
Good	The student completed assigned tasks with minimal help from the instructor and showed the results appropriately.	3	
Average	The student could not complete all assigned tasks and showed partial results.	2	
Worst	The student did not complete assigned tasks.	1	

Instructor Signature: _____ Date: _____

LAB # 9

To Trace Different Traffic Flows in Computer Networks using Extended ACL

Objectives

- To follow the DHCP protocol configuration for IP address assignment using Packet Tracer
- To identify and understand configurations of extended ACL using Packet Tracer

Pre-Lab Exercise

Read this experiment in its entirety to become familiar with objectives of this lab. Study in detail and become familiar with the basics of Dynamic Host Configuration Protocol and Access Control Lists (ACLs) provided with this laboratory experiment. You may record the terms and sections that require more elaboration for reference. The instructor may provide the class some time to reflect upon these before proceeding with the lab.

Scenario A: Dynamic Host Configuration Protocol

The **Dynamic Host Configuration Protocol** (**DHCP**) is a standardized networking protocol used on IP networks that dynamically configures IP addresses and other information that is needed for Internet communication. DHCP allows computers and other devices to receive an IP address automatically from a central DHCP server, reducing the need for a network administrator or a user from having to configure these settings manually.

There are two methods to implement DHCP.

1. Router act as DHCP server and assign IPs to devices.
2. Router forward the DHCP requests to DHCP server.

Following Commands are used to implement DHCP protocol on Cisco Router.

R1(config)#ipdhcp pool *Pool_Name*

R1(dhcp-config)#network *Network ID Subnet Mask*

R1(dhcp-config)#default-router *Gateway IP*

R1(dhcp-config)#exit

Pool_Nmae: It is the pool name we can use whatever we want. This command gets us into the DHCP Configuration mode.

Network ID: It defines the network to be assigned IP's automatically.

Subnet Mask: It defines the network range to be leased.

Gateway IP: Default gateway for this network

Scenario B: Access Control List

Network security is a huge subject. One of the most important skills a network administrator needs is mastery of access control lists (ACLs). Administrators use ACLs to stop traffic or permit only specified traffic while stopping all other traffic on their networks.

Network designers use firewalls to protect networks from unauthorized use. Firewalls are hardware or software solutions that enforce network security policies. Consider a lock on a door to a room inside a building. The lock only allows authorized users with a key or access card to pass through the door. Similarly, a firewall filters unauthorized or potentially dangerous packets from entering the network. On a Cisco router, you can configure a simple firewall that provides basic traffic filtering capabilities using ACLs.

An ACL is a sequential list of permit or deny statements that apply to addresses or upper-layer protocols. ACLs provide a powerful way to control traffic into and out of your network. You can configure ACLs for all routed network protocols.

What is an ACL?

An ACL is a router configuration script that controls whether a router permits or denies packets to pass based on criteria found in the packet header. ACLs are also used for selecting types of traffic to be analyzed, forwarded, or processed in other ways. You can configure one ACL per protocol, per direction, per interface:

- One ACL per protocol-To control traffic flow on an interface, an ACL must be defined for each protocol enabled on the interface.
- One ACL per direction-ACLs control traffic in one direction at a time on an interface. Two separate ACLs must be created to control inbound and outbound traffic.
- One ACL per interface-ACLs control traffic for an interface, for example, Fast Ethernet 0/0.

ACL Operation

How ACLs Work

ACLs define the set of rules that give added control for packets that enter inbound interfaces, packets that relay through the router and packets that exit outbound interfaces of the router. ACLs do not act on packets that originate from the router itself.

ACLs are configured either to apply to inbound traffic or to apply to outbound traffic.

Inbound ACLs-Incoming packets are processed before they are routed to the outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet is discarded. If the packet is permitted by the tests, it is then processed for routing.

Outbound ACLs-Incoming packets are routed to the outbound interface, and then they are processed through the outbound ACL.

ACL statements operate in sequential order. They evaluate packets against the ACL, from the top down, one statement at a time. If a packet header and an ACL statement match, the rest of the statements in the list are skipped, and the packet is permitted or denied as determined by the matched statement. If a packet header does not match an ACL statement, the packet is tested against the next statement in the list. This matching process continues until the end of the list is reached.

Access List Types

Cisco IOS access lists are divided into two distinct types:

- **Standard ACLs:** This type of ACL is the simplest one since it only filters traffic based on source IP addresses. In other words, this ACL can be used only when you need to permit or deny traffic from a specific host IP address or a specific source network.
- **Extended ACLs:** This type of ACL is the most preferred one and the most advanced as well. Extended ACLs filter IP packets based on several attributes, for example, protocol type, source IP address, destination IP address, source TCP or UDP ports, destination TCP or UDP ports, and optional protocol type information for finer granularity of control.

Numbering and Naming ACLs

Using numbered ACLs is an effective method for determining the ACL type on smaller networks with more homogeneously defined traffic. However, a number does not inform you of the purpose of the ACL. For this reason you can use a name to identify a Cisco ACL.

The rule to designate numbered ACLs and named ACLs is:

Numbered ACL

You assign a number based on which protocol you want to filtered:

- (1 to 99) and (1300 to 1999): Standard IP ACL
- (100 to 199) and (2000 to 2699): Extended IP ACL

In case you are wondering why numbers 200 to 1299 are skipped, it is because those numbers are used by other protocols.

Named ACL

You assign a name by providing the name of the ACL:

- Names can contain alphanumeric characters.
- It is suggested that the name be written in CAPITAL LETTERS.
- Names cannot contain spaces or punctuation and must begin with a letter.
- You can add or delete entries within the ACL.

Where to Place ACLs

The proper placement of an ACL to filter undesirable traffic makes the network operate more efficiently. ACLs can act as firewalls to filter packets and eliminate unwanted traffic. Where you place ACLs can reduce unnecessary traffic. For example, traffic that will be denied at a remote destination should not use network resources along the route to that destination.

Every ACL should be placed where it has the greatest impact on efficiency. The basic rules are:

- Because standard ACLs do not specify destination addresses, place them as close to the destination as possible.
- Locate extended ACLs as close as possible to the source of the traffic denied. This way, undesirable traffic is filtered without crossing the network infrastructure.

In-Lab Exercise

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 Figure 15. Assign Network_ID from Class C as shown in the figure and fill in the table. You will then perform the initial router configurations required for connectivity. Use the IP addresses according to your IP assignment. First test the connections between directly connected devices, and then test connectivity between devices that are not directly connected. You will configure the dynamic routing protocol RIP to add remote networks, this will allow communication between the hosts of different networks. View the routing table after each dynamic route is added to observe how the routing table has changed. After that, configure DHCP protocol on different networks so that all hosts from the network get IP address dynamically. Also create Access Control Lists (ACLs) to block networks from gaining access according to the given scenarios.

Topology Diagram

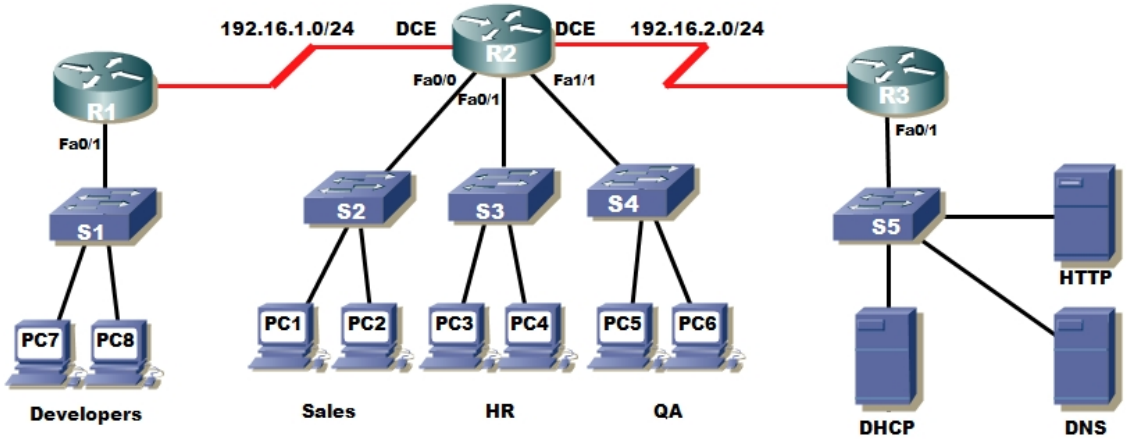

Figure 16: Network Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Gateway
R1	**Se0/1/0**			
	Fa0/0			
R2	**Se0/1/0**			
	Se0/2/0			
	Fa0/0			
	Fa0/1			
	Fa1/0			
R3	**Se0/2/0**			
	Fa0/0			
HTTP Server	**N/A**			
DNS Server	**N/A**			
DHCP Server	**N/A**			
PC1 – PC8	**NIC**	Obtain Automatically	Obtain Automatically	

Task 1: Prepare the Network

Task 2: Perform Basic Router Configurations.

Step 1: Configure Ethernet interfaces on R1.

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.

Task 3: Perform IP configuration on host PC's

Now you don't need to assign IP address on each PC. We will use DHCP to assign to get IP address automatically. Select DHCP on instead of Static on PC IP Configuration.

Step 1: Configure DHCP for Developer's Network

Complete the following commands and run on Router R1.

R1(config)#_____

R1(dhcp-config)#_____

R1(dhcp-config)#_____

R1(dhcp-config)#_____

Step 2: Configure DHCP for Sales Network

Complete the following commands and run on router R2.

R1(config)#_____

R1(dhcp-config)# _____

R1(dhcp-config)# _____

R1(dhcp-config)# _____

Step 3: Configure DHCP for HR Network

Complete the following commands and run on router R2.

R1(config)#_____

R1(dhcp-config)#_____

R1(dhcp-config)#_____

R1(dhcp-config)# _____

Step 4: Configure DHCP for QA Network

Complete the following commands and run on router R2.

R1(config)#_____

R1(dhcp-config)# _____

R1(dhcp-config)# _____

R1(dhcp-config)# _____

Task 4: Verify the Network

Use ping tool to check connectivity between the hosts. Is ping successful?

_____

Task 5: Configuring Extended IP Access Lists

Extended ACLs should be applied as close to the source as possible, thereby conserving network resources. Standard ACLs, by necessity, must be applied as close to the destination as possible. This is because the standard ACL can match only at the source address of a packet.

The steps for configuring an extended IP ACL do not actually differ from those of a standard ACL. More options are available in this case.

The commands to use for creating and applying this type of AL on an interface are the following:

To create extended ACL following command is used:

- **Router(config)#access-list access-list-number** ***{deny | permit} protocol source source-wildcard [source port] destination destination-wildcard [destination port] [log]***
- Keep in mind that the available numbers to use are between 100 and 199 and 2000 to 2699. You can deny or permit a specific protocol (e.g. IP, TCP), traffic coming from a specific host or network destined for a specific host or network and using specific services (identified by application ports for example 23 for telnet, 53 for DNS, etc.).

To apply the access list on an interface use the following command:

- **Router (config-if)#ip access-group** ***access-list-number {in | out}***

Step 1: Create extended ACL such that block the access of 192.16.6.3 from 192.16.3.2. While 192.16.3.2 must be able to connect with other computers of network to perform task.

Run following commands on router R1.

R1(config)#access-list 101 deny ip host 192.16.3.2 192.16.6.3 0.0.0.0

R1(config)#access-list 101 permit ip any any

R1(config)#interface fastEthernet 0/0

R1(config-if)#ip access-group 101 in

R1(config-if)#exit

Step 2: Create extended ACL such that block the access of 192.16.3.0 from 192.16.7.0. While 192.16.3.0 must be able connect with other computers of network to perform task.

Run following commands on router R1.

R1(config)#access-list 102 deny ip 192.16.3.0 0.0.0.255 192.16.7.00.0.0.255

R1(config)#access-list 102 permit ip any any

R1(config)#interface fastethernet 0/0

R1(config-if)#ip access-group 102 in

R1(config-if)#exit

Step 3: Create extended ACL such that block the 192.16.5.2 from gaining access on the network 192.16.7.0.

Run following commands on router R2.

R2(config)#access-list 103 deny ip host 192.16.5.2192.16.7.0 0.0.0.255

R2(config)#access-list 103 permit ip any any

R2(config)#interface fastEthernet 0/1

R2(config-if)#ip access-group 103 in

R2(config-if)#exit

Step 4: Create extended ACL such that block all traffic to 192.16.7.3 from the Network of 192.16.4.0

Run following commands on router R2.

R2(config)#access-list 104 deny ip192.16.4.0 0.0.0.255192.16.7.3 0.0.0.0

R2(config)#access-list 104 permit ip any any

R2(config)#interface fastethernet 0/0

R2(config-if)#ip access-group 104 in

R2(config-if)#exit

Task 7: Application based Extended Access List

In previous examples we filter ip base traffic. Now we will filter application base traffic. To do this practical create a topology as shown in **Error! Reference source not found.**.

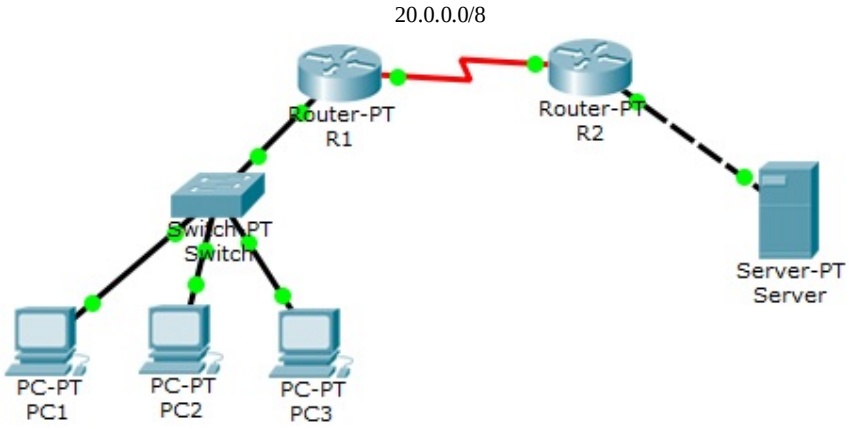

Figure 17: Network Topology

Step 1: Prepare the Network.

Step 2: Perform Basic Router Configurations.

Step 3: Block external user to ping our server as it could be used as denial of services. Create an access list that will filter all ping requests inbound on the serial 0/0/0 interface of R2.

Run following commands on router R2.

R2(config)#access-list 105 deny icmp any any echo

R2(config)#access-list 105 permit ip any any

R2(config)#interface serial 0/0/0

R2(config-if)#ip access-group 105 in

Step 4: Grant FTP access only to 10.0.0.2 while no other user need to provide ftp access on server. So, create a list to prevent FTP traffic that originates from the subnet 10.0.0.0/8, going to the 30.0.0.2 server, from traveling in on Ethernet interface Fa0/0 on R1.

Run following commands on router R1.

R1(config)#access-list 106 permit tcp host 10.0.0.2 30.0.0.2 0.0.0.0 eq 20

R1(config)#access-list 106 permit tcp host 10.0.0.2 30.0.0.2 0.0.0.0 eq 21

R1(config)#access-list 106 deny tcp any anyeq 20

R1(config)#access-list 106 deny tcp any anyeq 21

R1(config)#access-list 106 permit ip any any

R1(config)#interface fastethernet 0/0

R1(config-if)#ip access-group 106 in

Step 5: For security purpose you don't want to provide telnet access on server despite your own system. Your system is 10.0.0.4. Create an extended access list to prevent telnet traffic that originates from the subnet of 10.0.0.0 to server.

Run following commands on router R1.

R1(config)#access-list 107 permit tcp host 10.0.0.4 30.0.0.2 0.0.0.0 eq 23

R1(config)#access-list 107 deny tcp 10.0.0.0 0.255.255.255 30.0.0.2 0.0.0.0 eq 23

R1(config)#access-list 107 permit ip any any

R1(config)#interface fast 0/0

R1(config-if)#ip access-group 104 in

Step 6: Write an extended access list to deny HTTP traffic intended for web server 30.0.0.2, but will permit all other HTTP traffic to reach the only the 30.0.0.0 network.

Run following commands on router R2.

R2(config)#access-list 108 deny tcp any 30.0.0.2 0.0.0.0 eq www

R2(config)#access-list 108 permit tcp any 30.0.0.0 0.255.255.255 eq www

R2(config)#interface fa 0/0

R2(config)#ip access-group 108 in

R2(config)#exit

Step 7: Verify if the access list is created successfully.

Run following command on router R1 and R2. Also write down your observations.

R1# *show access-list*

_____

_____

_____

_____

R2# *show access-list*

_____

_____

_____

_____

Rubric for Lab Assessment

The student performance for the assigned task during the lab session was:			
Excellent	The student completed assigned tasks without any help from the instructor and showed the results appropriately.	4	
Good	The student completed assigned tasks with minimal help from the instructor and showed the results appropriately.	3	
Average	The student could not complete all assigned tasks and showed partial results.	2	
Worst	The student did not complete assigned tasks.	1	

Instructor Signature: _____ Date: _____

LAB # 10
To Show Different Configurations of Layer 2 Devices using Appropriate Command Scripts and Methods in Cisco Packet Tracer

Objectives

- To demonstrate the operation of switch.
- To revise basic configuration on switch.
- To manipulate switch port security using command line interface using packet tracer.

Pre-Lab Exercise

Read this experiment in its entirety to become familiar with objectives of this lab. Study in detail and become familiar with the basics of Switching and Spanning Tree Protocol (STP) provided with this laboratory experiment and in the portion of chapter 5 of the reference book. You may record the terms and sections that require more elaboration for reference. The instructor may provide the class some time to reflect upon these before proceeding with the lab.

Switch

Unlike old bridges, which used software to create and manage a Content Addressable Memory (CAM) filter table, our new, fast switches use application-specific integrated circuits (ASICs) to build and maintain their MAC filter tables.

Layer 2 switches are faster than routers because they don't take up time looking at the Network layer header information. Instead, they look at the frame's hardware addresses before deciding to either forward, flood, or drop the frame.

Functions of Switch

There are three distinct functions of layer 2 switching that are vital for you to remember: *address learning*, *forward/filter decisions*, and *loop avoidance*.

- **Address learning -** Layer 2 switches remember the source hardware address of each frame received on an interface and enter this information into a MAC database called a forward/filter table.
- **Forward/filter decisions -** When a frame is received on an interface, the switch looks at the destination hardware address, and then chooses the appropriate exit interface for it in the MAC database. This way, the frame is only forwarded out of the correct destination port.
- **Loop avoidance -** If multiple connections between switches are created for redundancy purposes, network loops can occur. Editing and Help Features

The Cisco advanced editing features can also help you configure your router. If you type in a question mark (?) at any prompt, you'll be given a list of all the commands available from that prompt:

Run the following command and write down your observation.

Switch#?

_____

_____

_____

_____

_____

_____

_____

_____

In-Lab Exercise

Task 1: Perform basic IOS command line interface operations

Step 1: Set Clock on Switch using Help Features

So with that, let's find the next command in a string by typing the first command and then a question mark and set clock on switch.

Write down your observation.

_____

_____

Task 2: Address Learning

When a switch is first powered on, the MAC forward/filter table (CAM) is empty, as shown in Figure 7.1. When a device transmits and an interface receives a frame, the switch places the frame's source address in the MAC forward/filter table, allowing it to refer to the precise interface the sending device is located on. The switch then has no choice but to flood the network with this frame out of every port except the source port because it has no idea where the destination device is actually located.

If a device answers this flooded frame and sends a frame back, then the switch will take the source address from that frame and place that MAC address in its database as well, associating this address with the interface that received the frame. Because the switch now has both of the relevant MAC addresses in its filtering table, the two devices can now make a point-to-point connection.

Configure the following topology on Cisco Packet Tracer

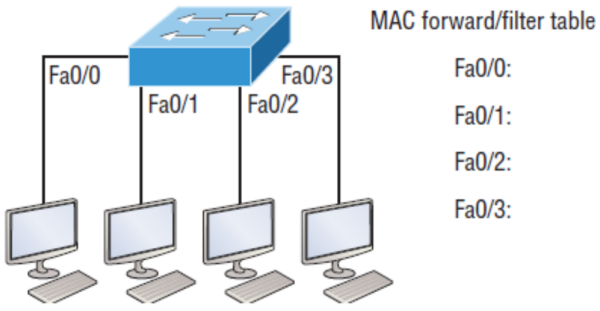

Figure 18: Network Topology

Step 1: Run the following command to see MAC forward/filter table

Switch> show mac-address-table

Step 2: Now access PC at port Fa0/3 from PC Fa0/1 (i.e. Ping from PC1 to PC4)

Switch> show mac-address-table

Discuss the difference in MAC Table in Task 1 and Task 2?

_____

_____

Forward/Filter Decisions

When a frame arrives at a switch interface, the destination hardware address is compared to the forward/filter MAC database. If the destination hardware address is known and listed in the database, the frame is only sent out of the appropriate exit interface. The switch won't transmit the frame out any interface except for the destination interface, which preserves bandwidth on the other network segments. This process is called *frame filtering*.

Task 3: Port Security

It's usually not a good thing to have your switches available for anyone to just plug into and play around with. But just how do we actually prevent someone from simply plugging a host into one of our switch ports. You can limit the number of MAC addresses that can be assigned dynamically to a port, set static MAC addresses so you can set penalties for users who abuse your policy!

Step 1: Find MAC Address of any PC

Run following command on Command Prompt of PC at port Fa0/1 and write down results.

PC>ipconfig /all

_____

_____

_____

_____

Step 2: Following syntax is used to configuring port security on switch.

Enter in port interface submode

Switch(config)#**int fa0/1**

Switch(config-if)#**switchport mode access**

Enable security at switch port

Switch(config-if)#**switchport port-security**

Switch(config-if)#**switchport port-security maximum***max devices*

Allowed mac-address to access through the switch port

Switch(config-if)#**switchport port-security mac-address***MAC-ID*

Switch(config-if)#**switchport port-security violation***mode*

max devices – max devices represents maximum number of system allowed through the switch port.

MAC-ID – MAC-ID represents the mac-address of the system allowed to access through that switch port. If you have set *max devices* more than 1. You have to enter mac-address of each device separately.

mode – mode represents the violation penalty either allow user, block its communication or switch off port.

Step 3: Enable port security on fa0/2

Switch(config)#_____

Switch(config-if)#_____

Switch(config-if)#_____

Switch(config-if)#_____

Switch(config-if)#_____

Switch(config-if)#_____

Step 4: Run the following commands and write down your observations.

Switch# show port-security

Switch# show port-security interface fa0/2

_____

_____

Step 5: Introduce a rogue host.

Attach different PC at that port, ping other hosts in that network through it. Write down your observation.

_____

_____

Step 6: Enable port security on fa0/2 and 0/3. (Hint: Repeat step 3 on interface fa0/2 and fa0/3) Use the different violation modes on fa0/2 and fa0/3 as shown below.

Switch(config-if)#switchport port-security violation ? % to set penalty in case of violation

protect Security violation protect mode

restrict Security violation restrict mode

shutdown Security violation shutdown mode

_____

_____

Step 7: Repeat step 5 and write down your observations.

_____

_____

Step 8: Reactivate the port.

If a security violation occurs and the port is shut down, you can use the no shutdown command to reactivate it. However, as long as the rogue host is attached, any traffic from the host disables the port. Reconnect PC3, and enter the following commands on the switch:

S1(config)#**interface fastethernet 0/3**

S1(config-if)# **no shutdown**

S1(config-if)#**exit**

Task 4: Set Password

Step 1: Set Password on Console Line.

Following are the commands to set password on Console Line limit unauthorized access to Switch. Run the following commands and write what you have observed?

Switch(config)#_____ % Set Password on Console Line

Switch (config-line)#_____ % Here CIIT is password

Switch (config-line)#_____ % Ask for Password every time you access through console line

Switch (config)#**exit**

Switch#**exit**

Step 1: Write the command to check running configurations on switch or router?

Step 2: Examine flash memory.

Issue one of the following commands to examine the contents of the flash directory.

Switch#**dir flash:**

or

Switch#**show flash**

_____

_____

Step 3: Display Cisco IOS information. Examine the following version information that the switch reports.

Switch#**show version**

What is the Cisco IOS version that the switch is running?_____

What is the system image filename? _____

What is the base MAC address of this switch?_____

Loop Avoidance

Redundant links between switches are important to have in place because they help prevent nasty network failures in the event that one link stops working.

But while it's true that redundant links can be extremely helpful, they can also cause more problems than they solve! This is because frames can be flooded down all redundant links simultaneously, creating network loops as well as other evils.

- If no loop avoidance schemes are put in place, the switches will flood broadcasts endlessly throughout the internetwork. This is sometimes referred to as a *broadcast storm*.
- A device can receive multiple copies of the same frame because that frame can arrive from different segments at the same time. Figure 19 demonstrates how a whole bunch of frames can arrive from multiple segments simultaneously.

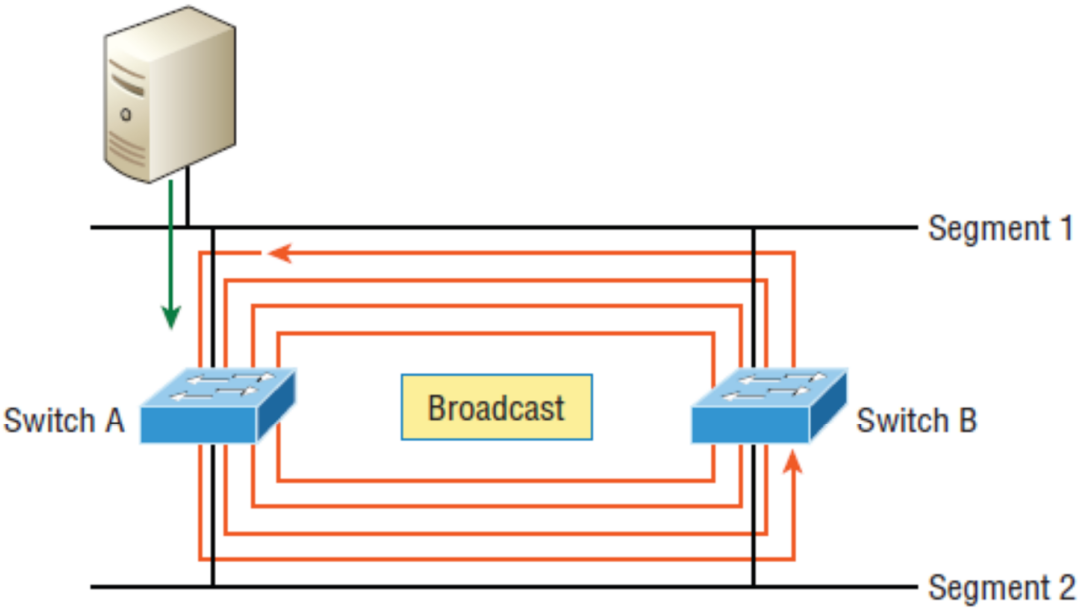

Figure 19: Loop

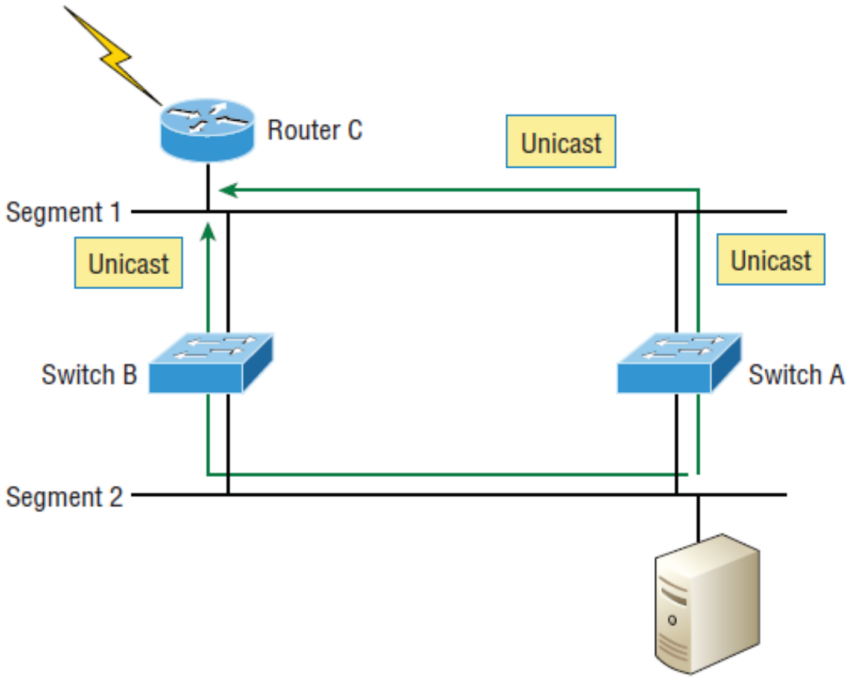

Figure 20: Loop Avoidance

- Spanning Tree Protocol (STP) is used to prevent network loops while still permitting redundancy.

Spanning Tree Protocol

Digital Equipment Corporation (DEC) created the original version of *Spanning Tree Protocol (STP).* The IEEE later created its own version of STP called 802.1D. All Cisco switches run the IEEE 802.1D version of STP.

STP's main task is to stop network loops from occurring on your layer 2 network (bridges or switches). It vigilantly monitors the network to find all links, making sure that no loops occur by shutting down any redundant links. STP uses the spanning-tree algorithm (STA) to first create a topology database, then search out and destroy redundant links. With STP running, frames will be forwarded only on the premium, STP-picked links.

Rules of Operation

- **STP Rule 1**— All ports of the root switch must be in forwarding mode.
- **STP Rule 2** — The root port must be set to forwarding mode.
- **STP Rule 3** — In a single LAN segment, the port of the designated switch that connects to that LAN segment must be placed in forwarding mode.
- **STP Rule 4**— All the other ports in all the switches (VLAN-specific) must be placed in blocking mode. The rule only applies to ports that connect to other bridges or switches. STP does not affect ports that connect to workstations or PCs. These ports remain forwarded.

Above rules can be understand by looking at the following example.

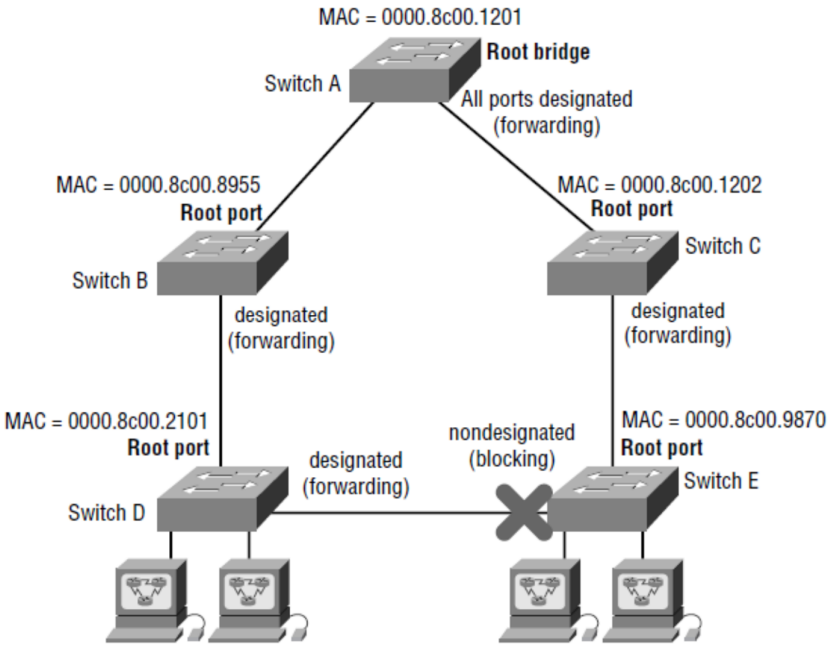

Figure 21

Selecting the Root Port

If more than one link leads to the Root Bridge, then cumulative outbound port costs along the path to the root bridge becomes the factor used to determine which port will be the root port for that device. So, to determine the port that will be used to communicate with the root bridge, you must first figure out the path's cost.

Typical Costs of Different Ethernet Networks

Speed	IEEE Cost
10Gbps	2
1Gbps	4
100Mbps	19
10Mbps	100

Scenario: Basic Spanning Tree Protocol

Topology Diagram

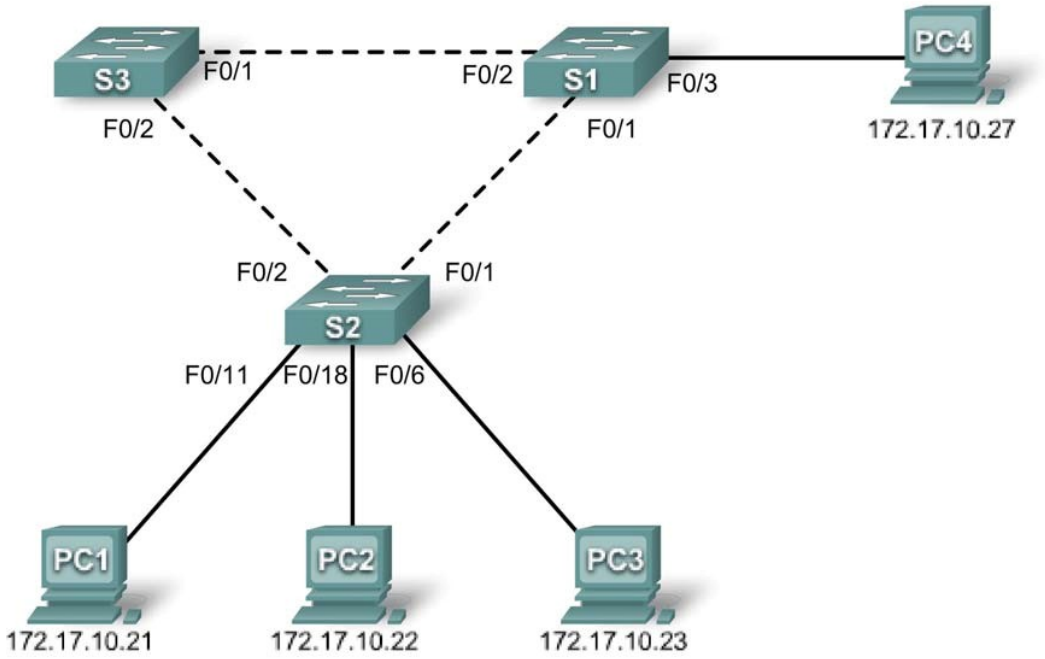

Figure 22: Network Topology

Task 1: Perform Basic Switch Configurations

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the switches.

Task 2: Prepare the Network

Task 3: Configure Host PCs

Configure the Ethernet interfaces of PC1, PC2, PC3, and PC4 with the IP address, subnet mask, and gateway indicated in the Figure 7.5.

Task 4: Examine Spanning Tree

Step 1: Examine the default configuration of 802.1D STP.

On each switch, display the spanning tree table with the **show spanning-tree** command. Root selection varies depending on the BID of each switch in your lab resulting in varying outputs.

S1#**show spanning-tree**

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.964B.9C0E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
    Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
               Address     0001.964B.9C0E
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
               Aging Time  20

    Interface        Role Sts Cost      Prio.Nbr Type
    ---------------- ---- --- --------- -------- --------------------------------
    Fa0/1            Desg FWD 19        128.1    P2p
    Fa1/1            Desg FWD 100       128.2    P2p
    Fa2/1            Desg FWD 19        128.3    P2p
```

S2#**show spanning-tree**

```
 VLAN0001
   Spanning tree enabled protocol ieee
   Root ID     Priority    32769
               Address     0001.964B.9C0E
               Cost        38
               Port        4(FastEthernet3/1)
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

     Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
               Address     00D0.9797.ACD2
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
               Aging Time  20

 Interface        Role Sts Cost      Prio.Nbr Type
 ---------------- ---- --- --------- -------- --------------------------------
 Et6/1            Altn BLK 100       128.7    P2p
 Fa0/1            Desg FWD 19        128.1    P2p
 Fa2/1            Desg FWD 19        128.3    P2p
 Fa3/1            Root FWD 19        128.4    P2p
 Fa1/1            Desg FWD 19        128.2    P2p
```

S3#**show spanning-tree**

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.964B.9C0E
              Cost        19
              Port        2(FastEthernet1/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.C72A.9478
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa1/1            Root FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p
```

Step 2: Examine the output

The bridge identifier (bridge ID), stored in the spanning tree BPDU consists of the bridge priority, the system ID extension, and the MAC address. The combination or addition of the bridge priority and the system ID extension are known as the *bridge ID priority*. The system ID extension is always the number of the VLAN. For example, the system ID extension for VLAN 100 is 100. Using the default bridge priority value of 32768, the *bridge ID priority* for VLAN 100 would be 32868 (32768 + 100).

The show spanning-tree command displays the value of *bridge ID priority*. Note: The "priority" value within the parentheses represents the bridge priority value, which is followed by the value of the system ID extension. Answer the following questions based on the output.

What is the bridge ID priority for switches S1, S2, and S3 on VLAN 1?

S1___ 32769 _____

S2___ 32769 _____

S3___ 32769 _____

Which switch is the root for the VLAN 1 spanning tree? _____

On S1, which spanning tree ports are in the blocking state on the root switch?

_____

_____

On S3, which spanning tree port is in the blocking state?_____

How does STP elect the root switch? _____

Since the bridge priorities are all the same, what else does the switch use to determine the root?

_____

_____

_____

_____

_____

Rubric for Lab Assessment

The student performance for the assigned task during the lab session was:			
Excellent	The student completed assigned tasks without any help from the instructor and showed the results appropriately.	4	
Good	The student completed assigned tasks with minimal help from the instructor and showed the results appropriately.	3	
Average	The student could not complete all assigned tasks and showed partial results.	2	
Worst	The student did not complete assigned tasks.	1	

Instructor Signature: _____ Date: _____

LAB # 11
To Show Different Configurations on Network Switches using VLANs and Inter VLAN Routing in Cisco Packet Tracer

Objectives

- To manipulate router's configuration to support 802.1q trunking on a fast Ethernet interface.
- To demonstrate inter VLAN routing
- Reproduce the network simulation for VLANs and verify device connectivity using Packet Tracer

Pre-Lab Exercise

Read this experiment in its entirety to become familiar with objectives of this lab. Study in detail and become familiar with the basics of Virtual Local Area Networks (VLANs) and VLAN Trunking Protocol (VTP) provided with this laboratory experiment and in the portion of chapter 5 of the reference book. You may record the terms and sections that require more elaboration for reference. The instructor may provide the class some time to reflect upon these before proceeding with the lab.

Virtual Local Area Networks (VLANs)

Virtual local area network (VLAN) is a logical grouping of network users and resources connected to administratively defined ports on a switch. When you create VLANs, you're given the ability to create smaller broadcast domains within a layer 2 switched internetwork by assigning different ports on the switch to service different subnetworks. A VLAN is treated like its own subnet or broadcast domain, meaning that frames broadcast onto the network are only switched between the ports logically grouped within the same VLAN.

Benefits of VLANs are:

- Network adds, moves, and changes are achieved with ease by just configuring a port into the appropriate VLAN.
- A group of users that need an unusually high level of security can be put into its own VLAN so that users outside of that VLAN can't communicate with it.
- As a logical grouping of users by function, VLANs can be considered independent from their physical or geographic locations.
- VLANs greatly enhance network security if implemented correctly.

VLANs increase the number of broadcast domains while decreasing their size

VLAN Identification Methods

VLAN identification is what switches use to keep track of all those frames as they're traversing a switch fabric. It's how switches identify which frames belong to which VLANs, and there's more than one trunking method.

- Inter-Switch Link (ISL)
- IEEE 802.1q

Inter-Switch Link (ISL)

ISL is a way of explicitly tagging VLAN information onto an Ethernet frame. This tagging information allows VLANs to be multiplexed over a trunk link through an external encapsulation method. This allows the switch to identify the VLAN membership of a frame received over the trunked link.

IEEE 802.1q

Created by the IEEE as a standard method of frame tagging, IEEE 802.1q actually inserts a field into the frame to identify the VLAN. If you're trunking between a Cisco switched link and a different brand of switch, you've got to use 802.1q for the trunk to work. Unlike ISL, which encapsulates the frame with control information, 802.1q inserts an 802.1q field along with tag control information, as shown in Figure 23 below.

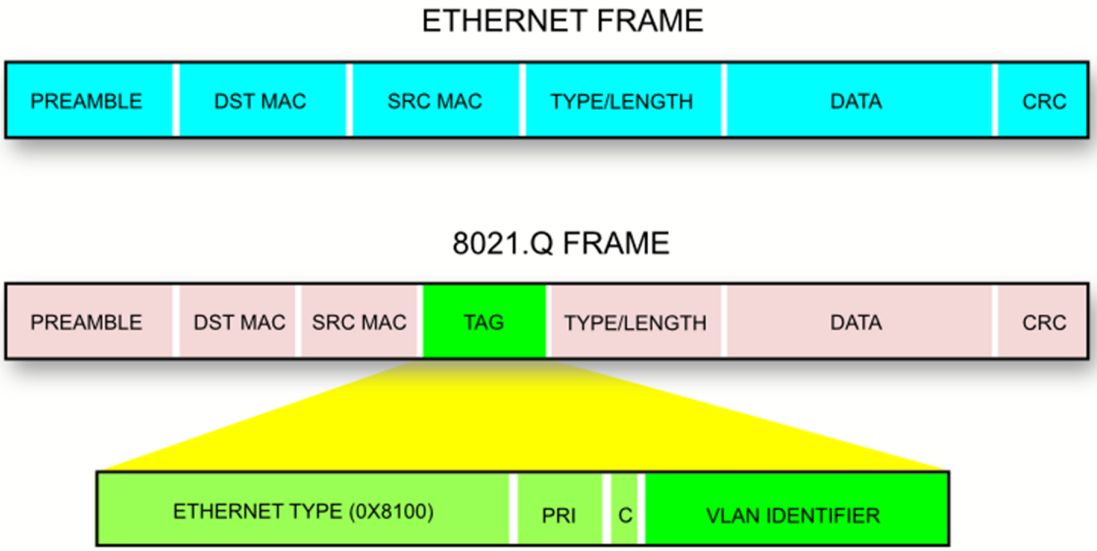

Figure 23: Frames

Trunk Ports

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.

A native VLAN is assigned to an 802.1Q trunk port. 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.

Topology Diagram

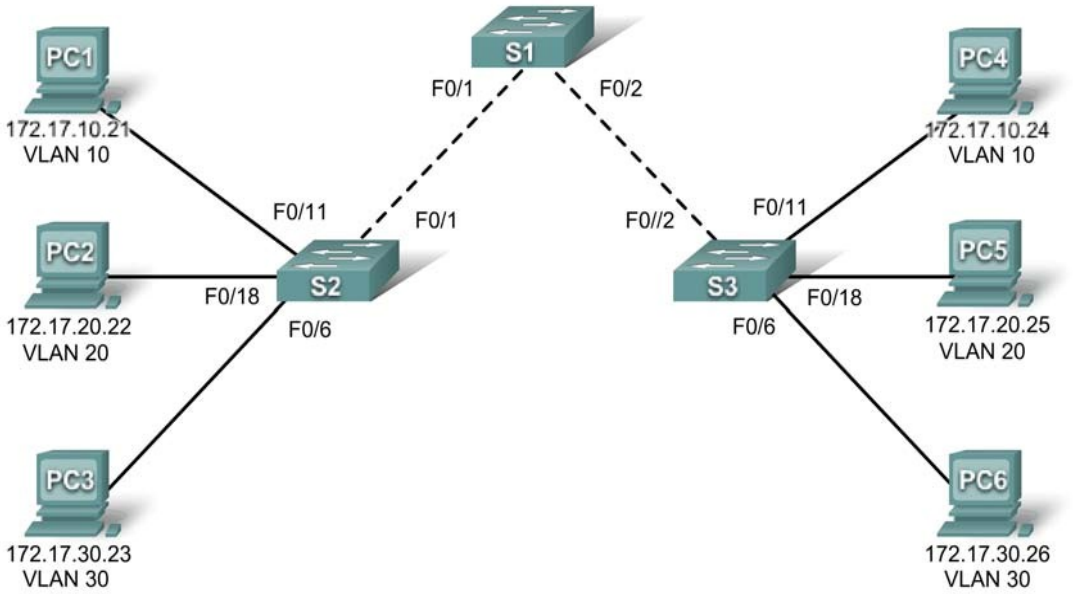

Figure 24: Network Topology

Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
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 1

Initial Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks	N/A
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
Fa0/6 – 0/10	VLAN 30 – Guest	172.17.30.0 /24

Table 2

In-Lab Exercise

Scenario A: Basic VLAN Configuration

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the switches, and initialize all ports in the shutdown state.

Switch#**config term**

Switch(config)#_____int range fa0/2 - fa0/4_____

Switch(config-if-range)#_____switchport mode trunk_____

Switch(config-if-range)#_____descrption 802.1q_____

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 access**

S2(config-if-range)#**no shutdown**

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.

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 three VLANS configured for this lab: VLAN 10 (faculty/staff); VLAN 20 (students); VLAN 30 (guest). 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_____

S1(config-vlan)#_____vlan 20_____

S1(config-vlan)#students

S1(config-vlan)#vlan 30

S1(config-vlan)#guest

S1(config-vlan)#

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. Write your observations.

S1#**show vlan brief**

```
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
                                      Gig0/1, Gig0/2
10   faculty                active
20   students               active
30   guest                  active
1002 fddi-default           active
1003 token-ring-default     active
1004 fddinet-default        active
1005 trnet-default          active
```

Step 3: Configure and name VLANs on switches S2 and S3.

Create and name VLANs 10, 20 and 30 on S2 and S3 using the commands from step 1.

Step 4: Verify the correct configuration with the *show vlan brief* command.

```
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
                                      Gig0/1, Gig0/2
10   faculty                active
20   students               active
30   Guest                  active
```

Step 5: Assign IPs to the VLANs on switch S1.

Use *interface vlan-id* and *ipaddress* commands to configure VLANs**.** The commands are as follows;

S1(config)#

S1(config)#

S1(config)#

S1(config)#

S1(config)#

S1(config)#

Step 6: Assign IPs to the VLANs on switches S2 and S3.

Repeat step 5 on Switches S2 and S3.

Step 7: Assign switch ports to VLANs on S1.

Refer to the port assignment on Table 2. 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.

S1(config)#_____

S1(config-if-range)#_____

S1(config-if-range)#_____

S1(config-if-range)#_____

S1(config-if-range)#_____

S1(config-if-range)#_____

S1(config-if-range)#_____

Step 8: Assign switch ports to VLANs on S2 and S3.

Repeat step 7 on Switches S2 and S3.

Step 9: Determine which ports have been added.

Use the **show vlan id** *vlan-number* command on S1 to see which ports are assigned to VLAN 10.

S1# **show vlan id** *10*

Which ports are assigned to VLAN 10?

_____

_____

Show vlan id *vlan-name* command displays the same output. Which ports are assigned to VLAN **faculty/staff**?

_____

_____

Task 4: Configure Trunking Ports on all Switches

Step 1: 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)#**no shutdown**

S1(config-if-range)#**end**

Similarly on Switch S2 and S3;

S2(config)# _____

S2(config-if-range)#_____

S2(config-if-range)#_____

S2(config-if-range)#_____

S3(config)#_____

S3(config-if-range)#_____

S3(config-if-range)#_____

S3(config-if-range)#_____

Step 3: Verify that the trunks have been configured with the *show interface trunk* command.

_____

_____

Step 4: Verify that the switches can communicate.

Step 5: Ping several hosts from PC2.

Ping from host PC2 to host PC1. Is the ping attempt successful explain your answer?

_____

_____

_____

_____

Ping from host PC2 to host PC5. Is the ping attempt successful explain your answer?

_____

_____

_____

_____

Step 6: 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**

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 explain your answer?

_____

_____

Inter-VLAN Routing

Pre-Lab Exercise

Read this experiment in its entirety to become familiar with objectives of this lab. Study in detail and become familiar with the basics of Inter-VLAN routing provided with this laboratory experiment. You may record the terms and sections that require more elaboration for reference. The instructor may provide the class some time to reflect upon these before proceeding with the lab.

Basic Inter-VLAN Routing

You have demonstrated that connectivity between VLANs requires routing at the network layer, exactly like connectivity between any two remote networks. There are a couple of options for configuring routing between VLANs.

The first is something of a brute force approach. An L3 device, either a router or a Layer 3 capable switch, is connected to a LAN switch with multiple connections—a separate connection for each VLAN that requires inter-VLAN connectivity. Each of the switch ports used by the L3 device are configured in a different VLAN on the switch. After IP addresses are assigned to the interfaces on the L3 device, the routing table has directly connected routes for all VLANS, and inter-VLAN routing is enabled. The limitations to this approach are the lack of sufficient Fast Ethernet ports on routers, under-utilization of ports on L3 switches and routers, and excessive wiring and manual configuration. The topology used in this lab does not use this approach.

An alternative approach is to create one or more Fast Ethernet connections between the L3 device (the router) and the distribution layer switch, and to configure these connections as dot1q trunks. This allows all inter-VLAN traffic to be carried to and from the routing device on a single trunk. However, it requires that the L3 interface be configured with multiple IP addresses. This can be done by creating “virtual” interfaces, called sub-interfaces, on one of the router Fast Ethernet ports and configuring them to dot1q aware.

Using the sub-interface configuration approach requires these steps:

- Enter sub-interface configuration mode
- Establish trunking encapsulation
- Associate a VLAN with the sub-interface
- Assign an IP address from the VLAN to the sub-interface

In-Lab Exercise

Topology Diagram

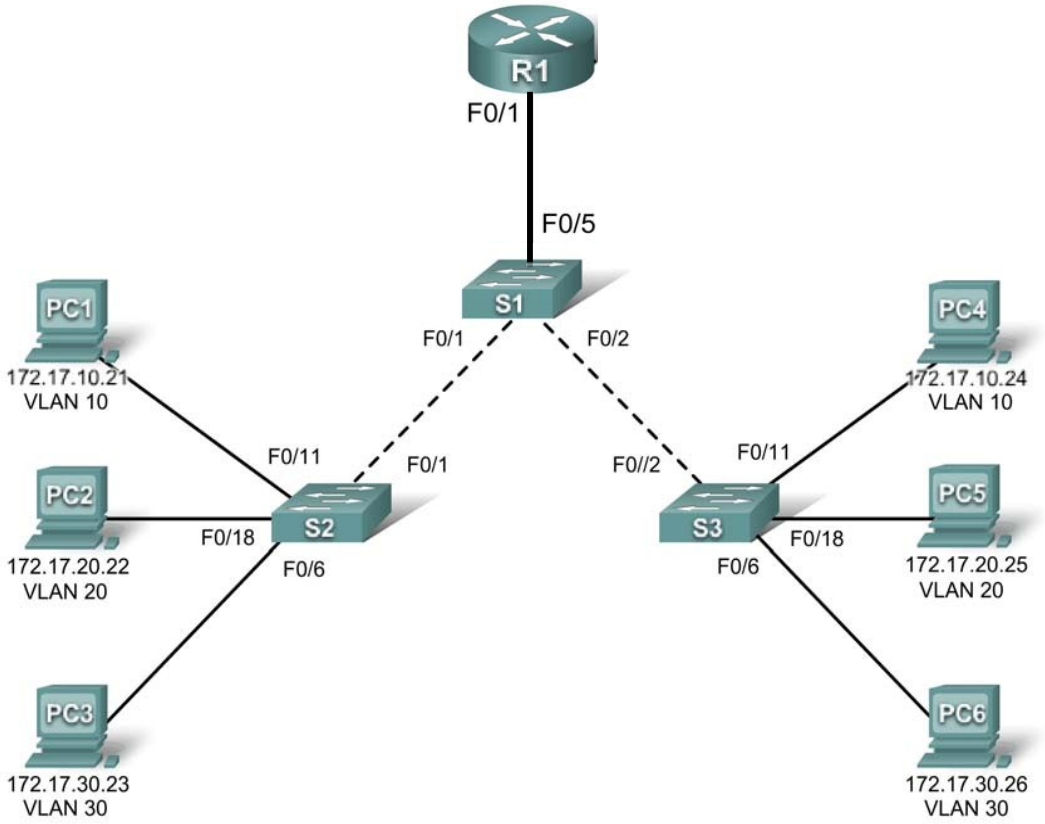

Figure 25: Network Topology

Interface Configuration Table – Router 1

Interface	Assignment	IP Address
Fa0/1.1	VLAN1	172.17.1.1 /24
Fa0/1.10	VLAN 10	172.17.10.1 /24
Fa0/1.20	VLAN 20	172.17.20.1 /24
Fa0/1.30	VLAN 30	172.17.30.1 /24

Table 1

Task 1: Prepare the Network

As you can see that the network is same as in Lab-8 just a router is attached to fast Ethernet interface.

Note: This lab is based on 2960 switches and 2811 router.

Step 1: Prepare the Network

Design topology diagram on Cisco Packet Tracer. Execute basic router and switch configurations as done in previous Lab.

Step 2: VLANs Configuration

Make VLANs on Switch S1, S2 and S3.

Step 3: Check connectivity between VLANs.

To check the connectivity, ping from one host of VLAN to the other host of same VLAN. If packet sent successfully then VLANs are configured.

NOTE: Hosts communicate within same VLAN.

Are the pings successful?

_____

If not, why do these pings fail?

_____

Task 2: Configure the Router

Step 1: Create a basic configuration on the router.

Step 2: Configure the trunking interface on R1.

To configure trunking interface the sample commands are as follows:

R1(config)#**interface fastethernet*port no***

R1(config)#**no shutdown**

R1(config-if)#**interface fastethernet*portno.vlan_id***

R1(config-subif)#**encapsulation dot1q *vlan_id***

R1(config-subif)#**ip address _____**

Note the following points in this configuration:

- The physical interface is enabled using the no shutdown command, because router interfaces are down by default. The virtual interfaces are up by default.
- The sub-interface can use any number that can be described with 32 bits, but it is good practice to assign the number of the VLAN as the interface number, as has been done here.
- The native VLAN, VLAN 1 is specified on the L3 device so that it is consistent with the switches.

Configure trunking interfaces on router using above commands for all three VLANs that you have created. Also configure native VLAN as it has to carry traffic other than the VLAN.

Step 3: There are now four networks configured. Verify that you can route packets to all four by checking the routing table on R1.

R1#**show ip route**

_____

_____

_____

_____

Step 4: Verify Inter-VLAN routing.

Step 5: From PC1, verify that you can ping the other two hosts (172.17.20.22 and 172.17.30.23). It may take a couple of pings before the end-to-end path is established. Are the pings successful?

_____

_____

_____

_____

If not, troubleshoot your configuration. Check to make sure that the default gateways have been set on all PCs and all switches. If any of the hosts have gone into hibernation, the connected interface may go down

Rubric for Lab Assessment

The student performance for the assigned task during the lab session was:			
Excellent	The student completed assigned tasks without any help from the instructor and showed the results appropriately.	4	
Good	The student completed assigned tasks with minimal help from the instructor and showed the results appropriately.	3	
Average	The student could not complete all assigned tasks and showed partial results.	2	
Worst	The student did not complete assigned tasks.	1	

Instructor Signature: _____ Date: _____

LAB # 12
To Show Different Configurations of Network Switches using VLANs and VTP in Cisco Packet Tracer

Objectives

- To demonstrate inter VLAN routing and configure VTP on all switches.
- Manipulate switch configuration for Virtual Tunnelling Protocol as pre network requirements using Command Line Interface (CLI) using Packet Tracer

Pre-Lab Exercise

Read this experiment in its entirety to become familiar with objectives of this lab. Study in detail and become familiar with the basics of Virtual Local Area Networks (VLANs) and VLAN Trunking Protocol (VTP) provided with this laboratory experiment and in the portion of chapter 5 of the reference book. You may record the terms and sections that require more elaboration for reference. The instructor may provide the class some time to reflect upon these before proceeding with the lab.

Virtual Local Area Networks (VLANs)

Virtual local area network (VLAN) is a logical grouping of network users and resources connected to administratively defined ports on a switch. When you create VLANs, you're given the ability to create smaller broadcast domains within a layer 2 switched internetwork by assigning different ports on the switch to service different subnetworks. A VLAN is treated like its own subnet or broadcast domain, meaning that frames broadcast onto the network are only switched between the ports logically grouped within the same VLAN.

Benefits of VLANs are:

- Network adds, moves, and changes are achieved with ease by just configuring a port into the appropriate VLAN.
- A group of users that need an unusually high level of security can be put into its own VLAN so that users outside of that VLAN can't communicate with it.
- As a logical grouping of users by function, VLANs can be considered independent from their physical or geographic locations.
- VLANs greatly enhance network security if implemented correctly.

VLANs increase the number of broadcast domains while decreasing their size

VLAN Identification Methods

VLAN identification is what switches use to keep track of all those frames as they're traversing a switch fabric. It's how switches identify which frames belong to which VLANs, and there's more than one trunking method.

- Inter-Switch Link (ISL)
- IEEE 802.1q

Inter-Switch Link (ISL)

ISL is a way of explicitly tagging VLAN information onto an Ethernet frame. This tagging information allows VLANs to be multiplexed over a trunk link through an external encapsulation method. This allows the switch to identify the VLAN membership of a frame received over the trunked link.

IEEE 802.1q

Created by the IEEE as a standard method of frame tagging, IEEE 802.1q actually inserts a field into the frame to identify the VLAN. If you're trunking between a Cisco switched link and a different brand of switch, you've got to use 802.1q for the trunk to work. Unlike ISL, which encapsulates the frame with control information, 802.1q inserts an 802.1q field along with tag control information, as shown in Figure 23 below.

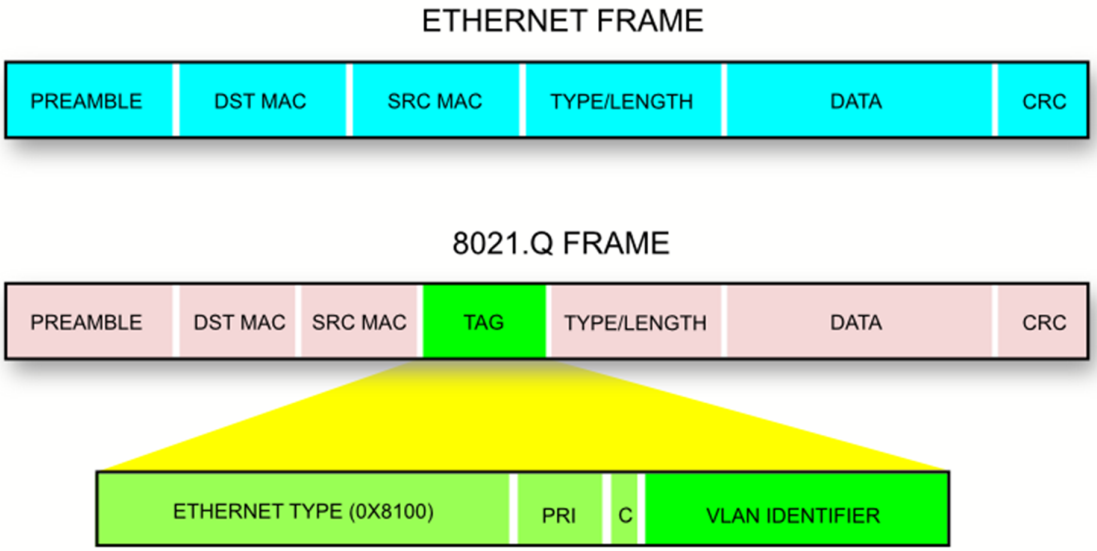

Figure 26: Frames

Trunk Ports

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.

A native VLAN is assigned to an 802.1Q trunk port. 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.

VLAN Trunking Protocol (VTP)

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.

Topology Diagram

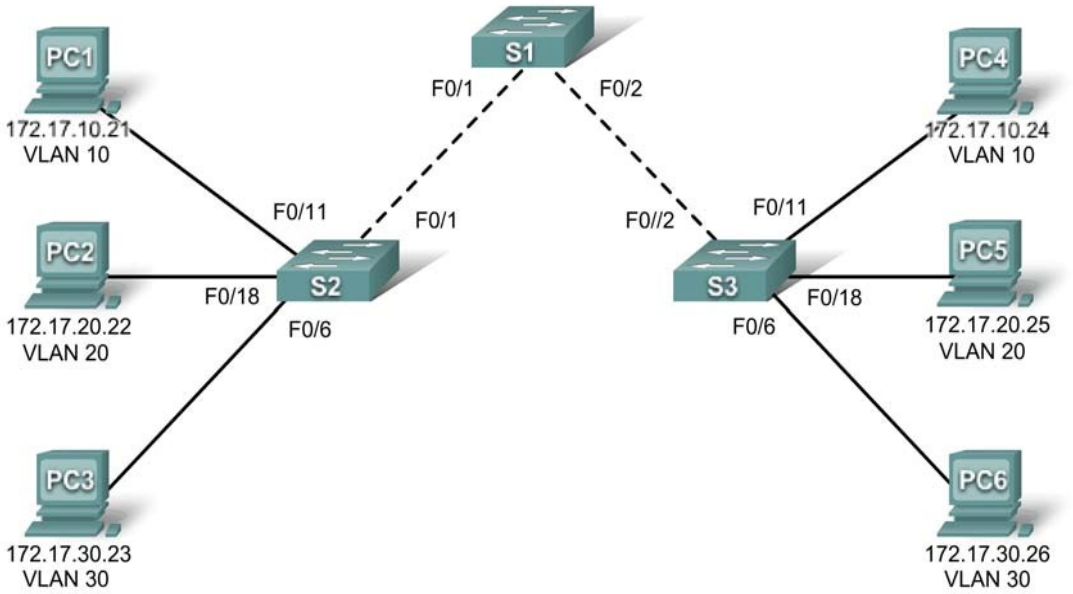

Figure 27: Network Topology

Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
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 3

Initial Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks	N/A
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
Fa0/6 – 0/10	VLAN 30 – Guest	172.17.30.0 /24

Table 4

In-Lab Exercise

Scenario A: Basic VLAN Configuration

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the switches, and initialize all ports in the shutdown state.

Switch#**config term**

Switch(config)#_____

Switch(config-if-range)#_____

Switch(config-if-range)#_____

Switch(config-if-range)#_____

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 access**

S2(config-if-range)#**no shutdown**

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.

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 three VLANS configured for this lab: VLAN 10 (faculty/staff); VLAN 20 (students); VLAN 30 (guest). 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)#_____

S1(config-vlan)#_____

S1(config-vlan)#_____

S1(config-vlan)#_____

S1(config-vlan)#_____

S1(config-vlan)#_____

S1(config-vlan)#_____

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. Write your observations.

S1#**show vlan brief**

_____

_____

_____

_____

Step 3: Configure and name VLANs on switches S2 and S3.

Create and name VLANs 10, 20 and 30 on S2 and S3 using the commands from step 1.

Step 4: Verify the correct configuration with the *show vlan brief* command.

_____

_____

_____

_____

Step 5: Assign IPs to the VLANs on switch S1.

Use *interface vlan-id* and *ipaddress* commands to configure VLANs**.** The commands are as follows;

S1(config)#_____

S1(config)#_____

S1(config)#_____

S1(config)#_____

S1(config)#_____

S1(config)#_____

Step 6: Assign IPs to the VLANs on switches S2 and S3.

Repeat step 5 on Switches S2 and S3.

Step 7: Assign switch ports to VLANs on S1.

Refer to the port assignment on Table 2. 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.

S1(config)#_____

S1(config-if-range)#_____

S1(config-if-range)#_____

S1(config-if-range)#_____

S1(config-if-range)#_____

S1(config-if-range)#_____

S1(config-if-range)#_____

Step 8: Assign switch ports to VLANs on S2 and S3.

Repeat step 7 on Switches S2 and S3.

Step 9: Determine which ports have been added.

Use the **show vlan id** *vlan-number* command on S1 to see which ports are assigned to VLAN 10.

S1# **show vlan id** *10*

Which ports are assigned to VLAN 10?

_____

_____

Show vlan id *vlan-name* command displays the same output. Which ports are assigned to VLAN **faculty/staff**?

_____

_____

Task 4: Configure Trunking Ports on all Switches

Step 1: 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)#**no shutdown**

S1(config-if-range)#**end**

Similarly on Switch S2 and S3;

S2(config)# _____

S2(config-if-range)#_____

S2(config-if-range)#_____

S2(config-if-range)#_____

S3(config)#_____

S3(config-if-range)#_____

S3(config-if-range)#_____

S3(config-if-range)#_____

Step 3: Verify that the trunks have been configured with the *show interface trunk* command.

_____

_____

Step 4: Verify that the switches can communicate.

Step 5: Ping several hosts from PC2.

Ping from host PC2 to host PC1. Is the ping attempt successful explain your answer?

_____

_____

_____

_____

Ping from host PC2 to host PC5. Is the ping attempt successful explain your answer?

_____

_____

_____

_____

Step 6: 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**

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 explain your answer?

_____

_____

_____

_____

Scenario B: VLAN Trunking Protocol (VTP)

Task 1: Clear any existing VLAN configurations on the switches

Step 1: Use the *show vlan* command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

Step 2: Verify that PC1 can ping PC4, PC2 can ping PC5, and that PC3 can ping PC6.

_____

_____

_____

_____

Task 2: Configure VTP on the Switches

Step 1: Check the current VTP settings on the three switches.

Run **show vtpstatus** command on three switches and fill in the Table 3.

	VTP version	VTP Operating mode	VTP domain name
Switch 1			
Switch 2			
Switch 3			

Table 5

Step 2: Configure the operating mode, domain name, and VTP password on all three switches.

Set the VTP domain name to **COMSATS** 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**

S1(config)#**vtp domain COMSATS**

S1(config)#**vtp password cisco**

S1(config)#**end**

S2(config)#**vtp mode client**

S2(config)#**vtp domain COMSATS**

S2(config)#**vtp password cisco**

S2(config)#**end**

S3(config)#**vtp mode transparent**

S3(config)#**vtp domain COMSATS**

S3(config)#**vtp password cisco**

S3(config)#**end**

Why it is necessary that all the switches must be in same VTP domain?

_____

_____

_____

_____

Step 5: Configure VLANs on the VTP server.

- **VLAN 10 (faculty/staff)**
- **VLAN 20 (students)**
- **VLAN 30 (guest)**

Configure these on the VTP server.

S1(config)#_____

S1(config-vlan)#_____

S1(config-vlan)#_____

S1(config)#_____

S1(config-vlan)#_____

S1(config-vlan)#_____

S1(config)#_____

S1(config-vlan)#_____

S1(config-vlan)#_____

Step 6: Verify that the VLANs have been created on S1 with the *show vlan brief* command.

_____

_____

_____

Step 7: Check if the VLANs created on S1 have been distributed to S2 and S3.

S2#**show vlan brief**

_____

_____

S3#**show vlan brief**

Are the same VLANs configured on all switches? Explain why?

Step 8: Create a new VLAN on switch 2 and 3.

S2(config)#**vlan 88**

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?

Step 9: Change Switch S3 mode from transparent to client.

S3(config)#**vtp mode client**

Step 10: Assign ports to specific VLAN as shown in topology diagram.

Step 11: Verify that host in same VLAN can access each other?

Rubric for Lab Assessment

The student performance for the assigned task during the lab session was:			
Excellent	The student completed assigned tasks without any help from the instructor and showed the results appropriately.	4	
Good	The student completed assigned tasks with minimal help from the instructor and showed the results appropriately.	3	
Average	The student could not complete all assigned tasks and showed partial results.	2	
Worst	The student did not complete assigned tasks.	1	

Instructor Signature: _____ Date: _____