LAB MANUAL

COMP 305

Computer Networks

Lab Instructor: Muhammad Waleed

Department of Computer Science

Minhaj University Lahore

Table of Contents

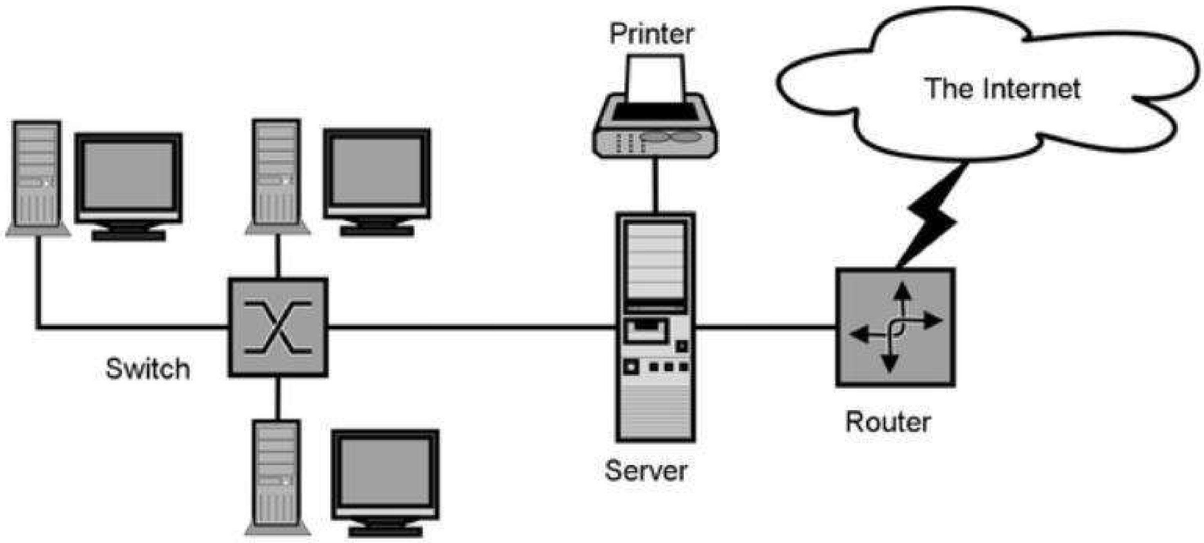
Data: Computer Network	Instructor:
Lab: 1	Max Marks:
Date:	Time Allowed:

1. **Computer Network**

At the end of the session you will be able to become familiar with different types of equipment's and cables used in the networked lab.

1.1 Introduction

Computer network means an interconnected collection of autonomous computers. Two computes said to be connected if they are able to exchange information. The connection needs to be done via some transmission media such as a coaxial cable, twisted pair cable; fiber optics, microwares and communication satellite can also be used. To interconnect the devices in the network requires some networking devices such as a hub, a switch or a router etc. To be autonomous means a device to be able to start or stop of its own.



1.2 Benefits of Computer network:

- Computer networking can help your business grow
- Cost-effective resource sharing
- Improving storage efficiency and volume
- Utilize a Centralized Database
- Securing valuable information
- Access flexibility etc.

1.3 Network Components

Server

Concept of a server is based on one or more personal computers to perform specific tasks for a number of other PCs. The most common function is disk, file and print servers.

A **Disk Server** provides low-level support and performs basic read/write operation to disk sectors.

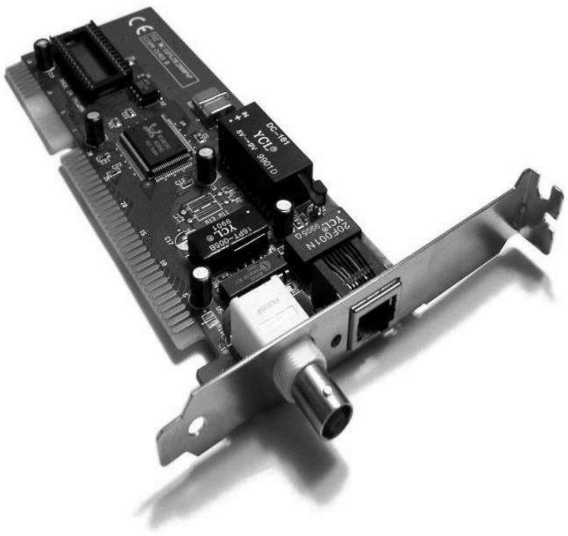
A **File Sever** is a higher-level support mechanism, performing such function as lockout and dynamic allocation of space on disk. In a star topology the server is the principal connection point. All nodes, including the server, are connected to a hub. This enables the server to house and administer software, fie sharing, file saving and to allocate printers or other peripherals. In a bus topology, the server acts like arbitrator, each node talks to the server when requesting information. The server then locates the information on one of the connected clients and sends it to the requesting client. Servers in any network can be an ordinary node but having more capabilities of handling the data and having more speed.

Workstation

A node or stand-alone PC that is connected with network is called Workstation. A workstation is generally a Client.

NIC (Network Interface Card): The network Interface Card (NIC) is the interface between the PC and physical network connection. It is also called as Network Adapter Card. The NIC is responsible for the operation that tasks place in the physical layer of the OSI model. It is only concerned with sending and receiving) 0s and 1s, using the IEEE 802.3 Ethernet standard.
In windows, the NIC card is identified in the network property; to use protocol with NIC you must bind the protocol to the adapter card.

Function of NIC:



- Data Transfer
- Data Buffering
- Frame Construction

- Media Access Control
- Parallel/Serial Conversion
- Data Encoding/Decoding
- Data Transmission/Reception

A network printer: A network printer is a printer that is accessible by network connection, making it usable by other computers connected to the network. The printer may have its own network connection, or use the network connection of a single dedicated computer to which it has a local connection.

Cables

To transmit the data the medium must exist, usually in the form of cables or wireless media. Here are some most commonly used cable types.

Thick Coaxial Cables (thick net) (RG-11)

Thick coaxial cables or thick wire is known as the Ethernet standard RG-11. This cable is mostly used as backbone cable, distributing Ethernet signal throughout a building, an office complex or other large installation. It is used in 10base5 Ethernet standard. The length may be up to 500 meters with a max of five segments connected by repeaters. This gives a total distance of 2500 meters. This is called a network diameter. RG-11 cable is typically orange; with black rings around the cable every 2.5-meter to allow taps into the cable.

Thin coaxial cables (thin net) (RG-58)

RG-58 is typically used for wiring laboratories and offices, or another small group of computers. The maximum length of thin wire Ethernet segment is 185 meters, which is due to the nature of the CSMA/CD method of operation, the cable attenuation, and the speed at which signals propagate inside the coax.

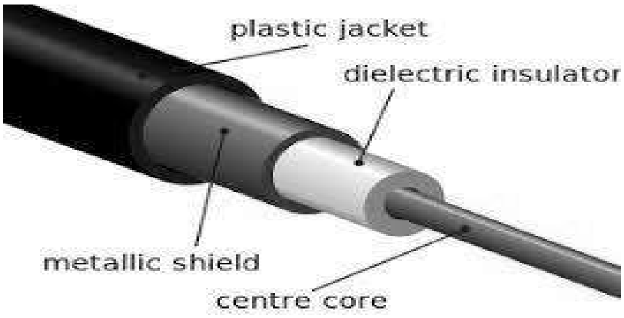


Fig: Thin coaxial cables (thin net) (RG-58)

The length is limited to guarantee that collision is detected when machines that are apart transmit at the same time. BNC connectors are used to terminate each end of the cable. When many machines are connected to the same Ethernet segment, a daisy chain approach is used. The BNC connectors allow the network interface card to the next machine. The machine each end of the cable must use a terminating resistor to eliminate collision-causing reflection in the cable.

Coaxial Cable Connectors

Coaxial connectors are needed to connect coaxial cable to devices. The most common type of connector used today is the Bayone-Neil-Concelman, in short, BNC connector.

Coaxial Cable Connector

The three popular types of connectors are: the BNC connector, the BNC T connector, and the BNC terminator. The BNC connector is used to connect the end of the cable to a device, such as a TV set. The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

1.3 Applications

1. Coaxial cable was widely used in analog telephone networks, and later with digital telephone networks.

2. Cable TV networks use coaxial cables (RG-59) at the network boundaries. However, coaxial cable has largely been replaced today with fiber-optic cable due to its higher attenuation.

3. Traditional Ethernet LAN

– 10Base-2, or thin Ethernet, uses RG-58 coax cable with BNC connectors.

– 10Base-5, or thick Ethernet, uses RG-11 coax cable with specialized connectors.

Twisted pair cables

Twisted pair is probably the most widely used cabling system in Ethernet in networks. Two copper wires twist around each other to form the twisted pair cable. Depending on category several insulated wire strands can reside in the cable.

Twisted pair is available in two basic types

a) Unshielded Twisted Pair (UTP)

b) Shielded Twisted Pair (STP)

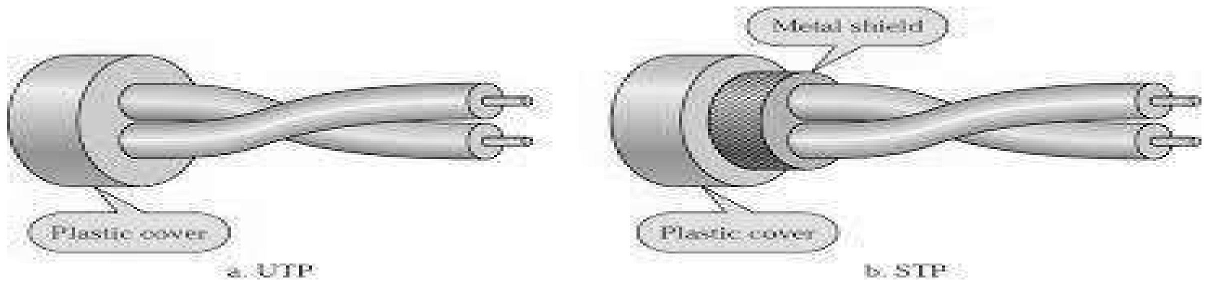


Fig: Twisted pair cables

Unshielded Twisted Pair-Mostly the UTP is used. A twisted pair segment can't exceed 100 meters. This limitation is the only drawback to twisted pair. Twisted pair is used for 10/100 based Ethernet networks. UTP cables are wired as straight through or crossover cables. Straight through cables typically connect the computer's networks interface can't to be a port on the hub. Crossover cables are used for NIC to communication and for hub-to-hub connections when no crossover port is available.

Shielded Twisted Pair -It is 150Ω cable containing additional shielding that protects signals against electromagnetic Interference (EMI) produced by electric motors power lines etc. It is primarily used in Token Ring Network & where UTP cable would provide insufficient protection against interface. Wires within cables are encased in a metallic sheath that is conductive as copper in wires. This sheath when properly grounded converts it ambient noise into current, like antenna. This current is carried to wires within where it creates an equal and opposite current flowing in twisted pair thus getting cancelled and no noise signal is resulted.

Fiber Optic.

Fiber Optic relies on pulsed as light to carry information. Two types of plastic or glass with different physical properties are used (the inner core and the outer cladding) to allow a beam of light to reflect off the boundary between the core and cladding. Some fiber optic cables allow many different paths other to allow one single mode. They are called multimode and single mode fibers. A popular multimode fiber has core/cladding dimensions of 62.5/125 nanometers.

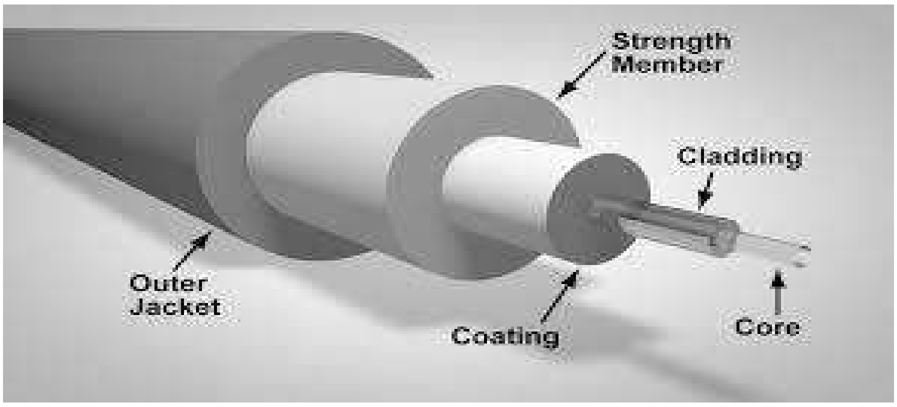


Fig: Fiber Optic cable

Data: Computer Network	Instructor:
Lab: 2	Max Marks:
Date:	Time Allowed:

2. To study different internetworking devices in a computer network.

2.1 Introduction

At the end of the session, you will be able to be familiar with different types of internetworking devices and their functions.

2.2 REPEATER

A Repeater is a purely electrical device that extends maximum distance a LAN cable can span by Amplifying signals passing through it. A Repeater connects two segments and broadcasts packets between them. Since signal loss is a factor in the maximum length of a segment, a Repeater is used to amplify the signal and extend the usable length.

Fig: Repeaters

A common Ethernet rule is that no more than four repeaters may be used to join segments together. This is a physical limitation designed to keep collision detection working properly. Repeaters operate at layer 1 (Physical layer) of the OSI model.

2.3 BRIDGES

The networks bridge provides an inexpensive and easy way to connect network segments. A bridge provides Amplification function of a repeater plus, ability to select filter packets based on their addresses. When network grows in size, it is often necessary to partition it into smaller group of nodes to help isolate traffic and improve performance. One way to do this is to use bridge, the operation of it is to keep one segment traffic to that side and other side will cross the bridge.

The bridge learns which packets should cross it as it is used.

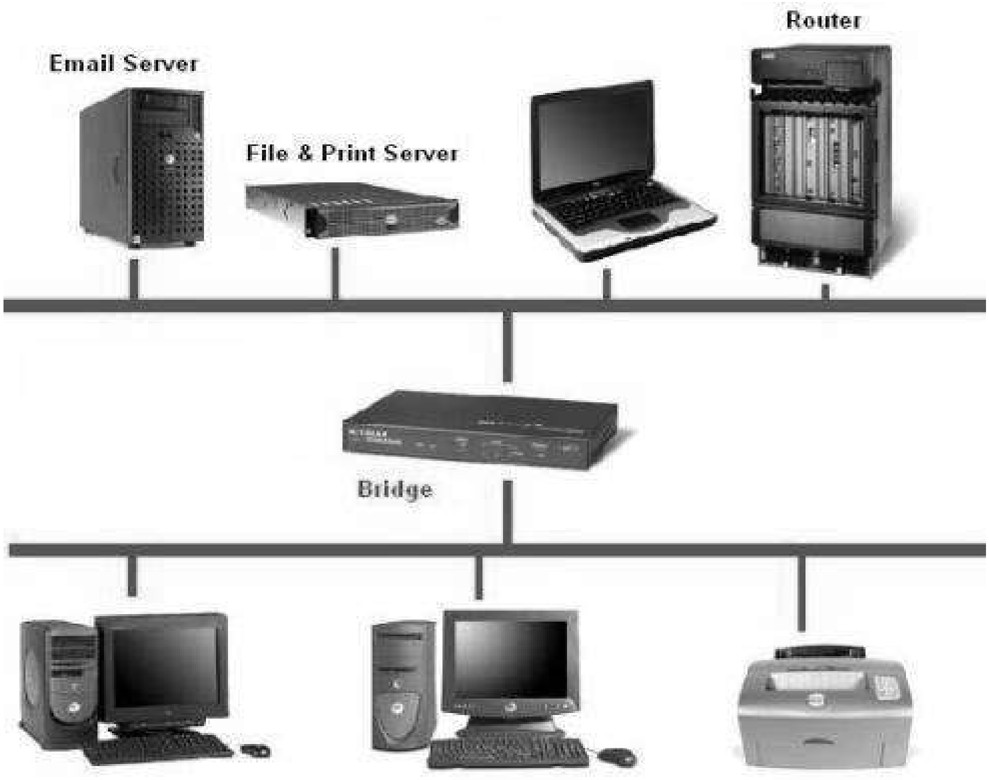


Fig: Bridged network

2.4 ROUTERS

A router is a device that connects two LANs together to form an inter-network. A router is the basic building block of the Internet. Each router connects two or more networks together by providing an interface for an Ethernet network and ring network

Fig:Routers

The router examines each packet of information to detection weather the packet must be translated form on one network to another network performing a function similar to a bridge.

Unlike a ridge, a router can connect network that use different technologies, addressing methods, media type, frame format and speeds. A router is a special purpose device designed to interconnect networks. Such that three networks can be connected using two routers. Routers maintain routing tables in their memories to store information about the physical connection on the network; the router examines each packet of data, checks the routing table and then forwards the packet if necessary. Every other router in the path (between any state destinations) performs a similar procedure. Note that a router does not maintain any state information about the packets; it simply moves them along the network. Routers are operated at layer 3(network) of OSI model.

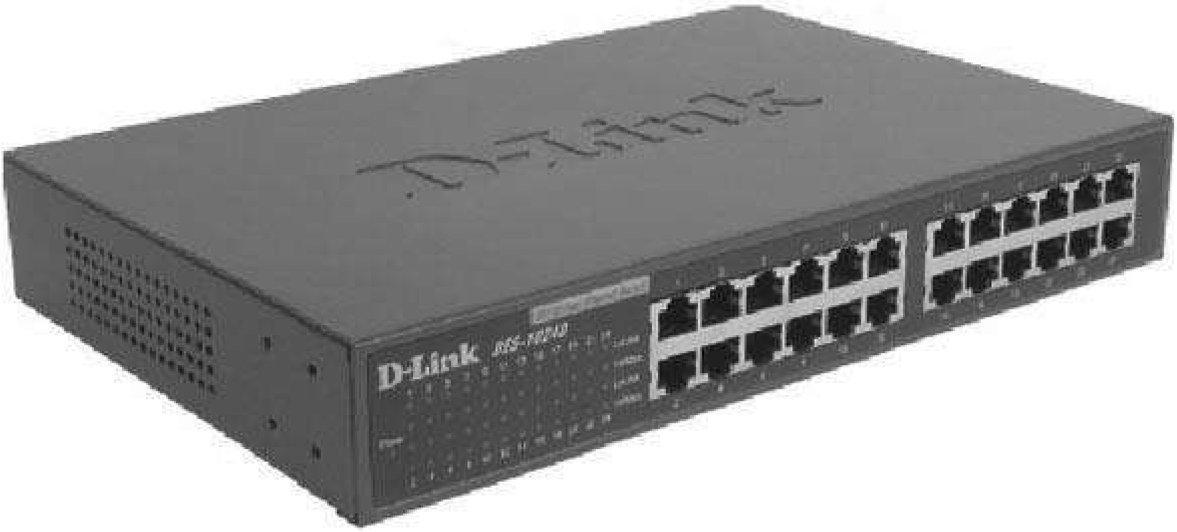
2.5 HUBS

Hubs are also called concentrators; expand one Ethernet connection into many. For example, a four-port hub connects up to four machines via UTP cables. The hub provides a star connection for the four ports. Many hubs contain a single BNC connector as well to connect the hub to existing 10base2 network wiring, the hub can also be connected via one of its ports. One pot is desired to operate in either straight through or crossover mode, selected by a switch on the hub.

Hubs that can connect in this fashion are called stackable hubs. A hub is similar to a repeater, expect it broadcasts data received by any port to all other ports on the hub. Most hubs contain a small amount of intelligence as well. Examining received packets and checking them for integrity. If a bad packet arrives or the hub determines that a port is unreliable. It will shut down the line under the error condition is appears. The hub also acts like a repeater. Because of its slight delay when processing a packet, the numbers of hubs that may be connected in a series are limited.

2.6 SWITCHES

It is similar to a bridge, with some important enhancement. First, a switch may have multiple ports, thus directing packets to several different segments further partitioning and isolating network traffic in as way similar to router. For example, if 8-port n way switch is there it can route packets from any input to any output.



Some or all of incoming packet is called store and forward, which stores the received packet before examining it to for error before retransmitting. Bad packets are not forwarded. A switch typically has auto-sensing 10/100 mbps ports and will just the speed of each port accordingly; furthermore, a managed switch supports SNMP for further control over network traffic. Switches operated at layer 2 (Data Link) of OSI model.

3. Network Layer

3.1 Introduction

In this lab we will learn about:- Computer Networks
Configuration Introduction to IP addressing
Identify tools used for discovering a computer's network configuration with various operating systems.
Gather information, including the connection, host name, MAC(Layer2) address, and TCP/IP

3.2 Network (Layer 3)

Compare the network information to that of other PC's on the network.
Learn to use the TCP/IP packet Internet groper (ping) command from a workstation. Learnt to use the trace route (tracert) command from a workstation.
Observe name-resolution occurrences using WINS and DNS servers Part A:

Background/Preparation

This lab assumes that you are using Windows NT/2000/XP. This is nondestructive lab that you can Perform on any host without changing the system configuration.
Ideally, you perform this lab in a LAN environment that connects to the Internet. You can use a single remote connection via a dial up modem or DSL. You will need the IP address information which the instructor should provide.

3.3 Introduction to IP addressing:

Each Network Interface Card (NIC or Network card) present in a PC is assigned one Net- work address called as IP address [or Network address]. This IP address is assigned by the administrator of the network. No two PCs can have the same IP address. There is a burned- in address on the NIC called as Physical Address [or MAC address or Hardware address]. The MAC address of a network card indicates the vendor of that card and a unique serial number.
PC Network TCP/IP Configuration Rules for IP 4
Addressing

1. Format of IP address IPv4 is made up of four parts, in the pattern as w.x.y.z. Each part has 8 Binary bits and the values in decimal can range from 0 to 255.
2. IP address classes

IP addresses are divided into different classes. These classes determine the maximum num- ber of hosts per network ID. Only three classes are actually used for network connectivity. The following table lists all of the address class.

3. Grouping of IP addresses into different classes.

a) Class A, B, C, D, E

b) Class A: first bit in w is 0 and others can be anything i. 0.0.0.0 to 127.255.255.255

First bits are used for network part and the remaining for host part
. c) Class B: First bit in w is 1 and second bit is
0. i. 128.0.0.0 to 191.255.255.255
ii. First 16 bits for network part and remaining host part
d) Class C: first bit in w is 1, second bit in w is 1 and third
bit is 0 i. 192.0.0.0 to 223.255.255.255
ii. First 24 bits for network part and last 8 bits for host part.
e) Class D: first, second, third bits in w are 1 and fourth bit is 0; used for multicast. i. 224.0.0.0 to 247.255.255.255
f) Class E: future use or experimental purposes.
4. Default Subnet mask it is used to identify the network part from the host part. Put binary one for the parts that represent network part and zero for the part that represent host part. a) Class A: 255.0.0.0
b) Class B: 255.255.0.0
c) Class C: 255.255.255.0
d) We canâA˘ Z´ t have mix of 1s and 0s in subnet mask. Only consecutive 1s is followed by Consecutive 0s
5. Invalid IP address.
a) If the network part is all 0s, the address belongs to class A. But this is an invalid ip address because for an ip address all the network or host part should not be all 1s or all 0s.
i. 0.0.0.0 is not valid. Routers use it internally.
b) If the network part is all 1s, this address belongs to class E. But due to presence of all 1s, it is not valid. This represent broadcast to all networks.
i. 255.255.255.255 is not valid.
c) If the host part is all 0s, this represents network address. This is not a valid ip address.
d) If the host part is all 1s, this represents broadcast address. This is not a valid ip address.
e) We canâA˘ Z´ t use the ip address represented within private address range as part of public ip address.
i. Class A: 10.0.0.0 to 10.255.255.255
ii. Class B: 172.16.0.0 to 172.31.255.255
iii. Class C: 192.168.0.0 to 192.168.255.255
f) 127.0.0.0 network address is used for loop-back testing. This will help you to check the network card of your own PC [localhost].
g) The validity of the IP address is also based on the subnet mask used provided.
6. Default subnet masks for standard IP address classes.
7. Exercise
In this exercise, you will determine the correct class for a given IP address.
1. Write the address class next to each IP address.
2. Which address class (es) will allow you to have more than 1000 hosts per network?
3. Which address (es) will allow only 254 hosts per network?
4. Identify invalid IP address:
Circle the portion of the IP address that would be invalid if it were assigned to a host, and then explain why it is invalid.

a) 131.107.256.80
b) 222.222.255.222
c) 231.200.1.1
d) 126.1.0.0

e) 0.127.4.100
f) 190.7.2.0
g) 127.1.1.1
h) 198.121.254.255
i) 255.255.255.255

3.4 Network Configuration

Step 1. Connect to the Internet.
Establish and verify connectivity to the Internet. This step ensures the computer has an IP address.
Step 2. Gather TCP/IP configuration information.
a. Use the Start menu to open the command prompt (Start>Programs>Accessories>Command Prompt or Start>Programs>Command Prompt).
b. Type ipconfig and press Enter key. The spelling of the ipconfig is critical, but the case is not.

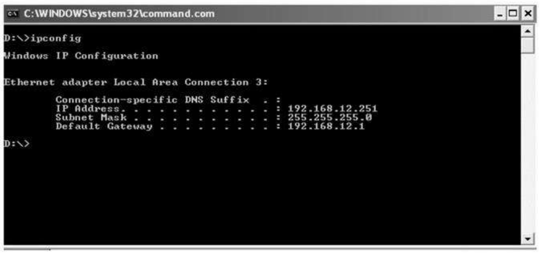


Figure 3.1: IP Configuration

c. The screen shows the IP address, subnet mask and the default gateway. The IP ad- dress and the default gateway should be in the same network or subnet; otherwise this host wouldn't be able to communicate outside the network.
Step 3. Record the following TCP/IP information for this computer. a. IP address:..
b. Subnet mask:...
c. Default gateway:..
Step 4. Compare this computer's TCP/IP configuration to that of others on the LAN. If this computer is on a LAN, compare the information of several machines (Hosts).
a. Are there any similarities? ....
b. What is similar about the IP addresses? ....
c. What is similar about the default gateway? ....
d. Record a couple of the IP addresses (of your nearby hosts)
1..
2..
3..
Step 5. Check additional TCP/IP configuration information.
a. To see more information, type ipconfig/all and press Enter key. The figure shows the detailed IP configuration of this computer on the screen.
b. You should see the following information: the host name (computer name), the Physical address of this machine, IP address, subnet Mask, Default Gateway and DNS Servers.
c. In the LAN, compare your result with a few nearby computers. What similarities do you see inthe physical (MAC) address?
....
d. Write down the computer's host name:

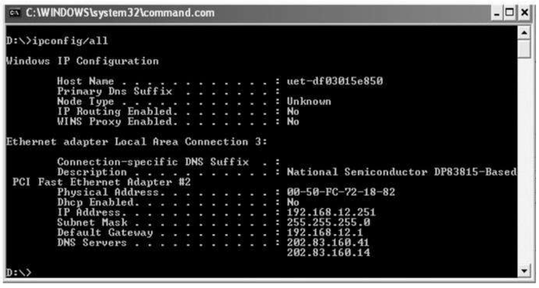


Figure 3.2: Configuration

e. Write down the host names of a couple of other computer:

1..

2..

3..

4..

Step 6. Close the screen when finished.

Part B: Using PING TRACERT from a Workstation

Sept 1. Establish and verify connectivity to the Internet. This step ensures that the computer has an IP address.

Step 2. Open the Command prompt(MS-DOS). Ping the IP address of another computer.

a. In the window, type ping, a space, and the IP address of a computer recorded in the previous lab.

Ping uses the Internet Control Message Protocol(ICMP) echo-request and echo-reply feature to test physical connectivity. Because ping reports on four attempts, it gives an indication the reliability of the connection. Look over the result and verify that the ping was successful. Was the ping successful? If not, report to the instructor.

b. Ask the IP address of the nearby computers and ping. Note the result.

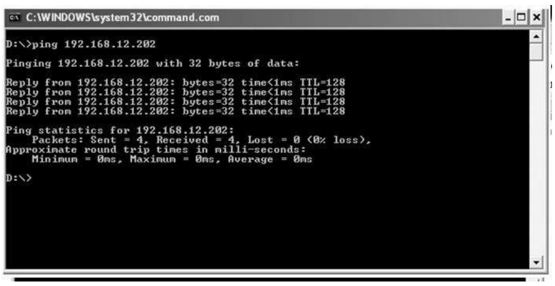


Figure 3.3: Configuration

....

c. Ping the IP address of Default gateway and DNS servers. Was the result successful?

....

d. Ping the computer loopback IP address. Type the following command: ping 127.0.0.1

e. The address 127.0.0.1 is reserved for loopback testing. If the ping is successful, then TCP/IP is properly installed and functioning on this computer.

f. Was the ping successful for e..

g. Ping the hostname of the computer that you recorded in lab 1.1.

h. Ping the Microsoft website (www.microsoft.com)

Step 3. Trace the route to the Umm-alqura university website: type tracert www.uqu.edu.sa and press Enter key.

The result shows the complete route to the site and the number of hops in path. Trace a local host name or IP address in your local area network (LAN).

Record the output and interpret.

Step 4. Close the window. Also see pathing Ip or host command. Which only shows path from source to

Destination\Conclusion:

Summarize, in a paragraph or two, what you conclude from the results of your experiment and whether they are what you expected them to be. Compare the results with theoretical expectations and include percent error when appropriate. Don’t use terms such as "fairly close" and "pretty good;" give explicit quantitative deviations from the expected result. Evaluate whether these deviations fall within your expected errors and state possible explanations for unusual deviations. Discuss and comment on the results and conclusions drawn, including the sources of the errors and the methods used for estimating them.

4. Create a Network Topology in Cisco Packet Tracer

4.1 Introduction

To perform the CN hands- on lab exercises, first, you need to download Cisco Packet Tracer. Once it is downloaded, install it using the default selections. After the installation, you can create a network topology to perform the hands-on lab exercises. In this experiment, we will discuss how to create a network topology using Cisco Packet Tracer.

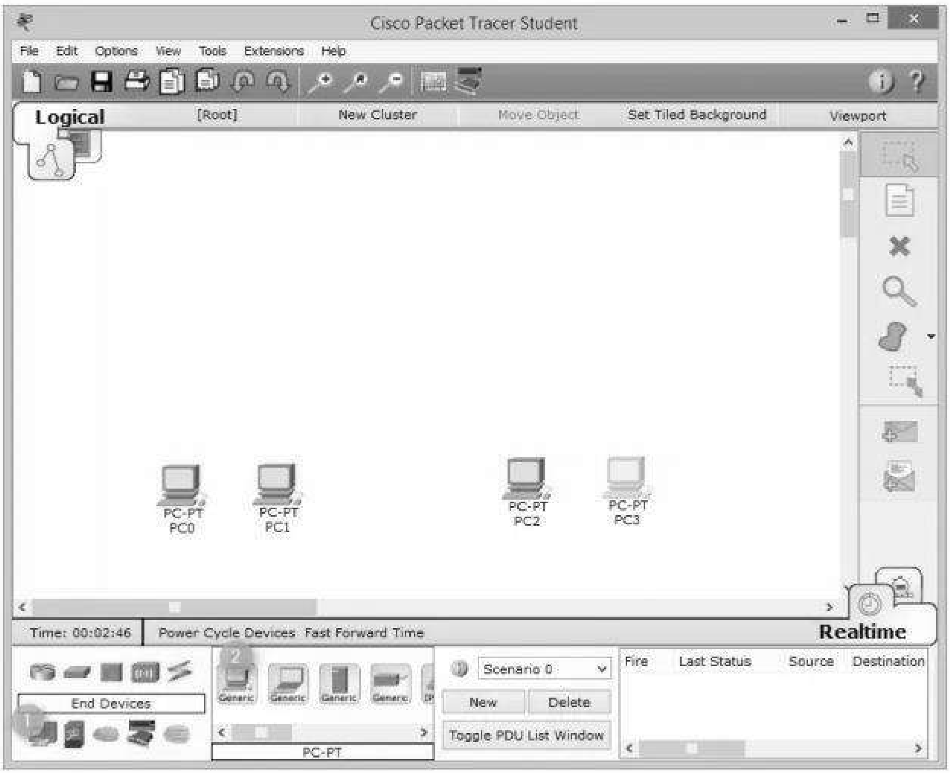
Create a Network Topology

You can easily create a network topology using Cisco Packet Tracer. In the following sections, we are going to explain how to create a network topology that will contain four PCs, two switches, and two routers.

Adding PCs in Cisco Packet Tracer

To add PCs in Cisco Packet Tracer, you need to perform the following steps:

1. In the Cisco Packet Tracer console, click on the **PC** icon, click **Generic**, and then click in the logical view area to add a **Generic** PC.
2. Repeat the same step to add three more Generic PCs in the logical view area, as shown in the following figure.



Adding Switches in Cisco Packet Tracer

1. To add a switch in Cisco Packet Tracer, click the **Switch** icon, select a switch type, such as **2960**, and then add the selected switch in the logical view area.
2. Repeat the same step to add one more switch.

Adding Routers in Cisco Packet Tracer

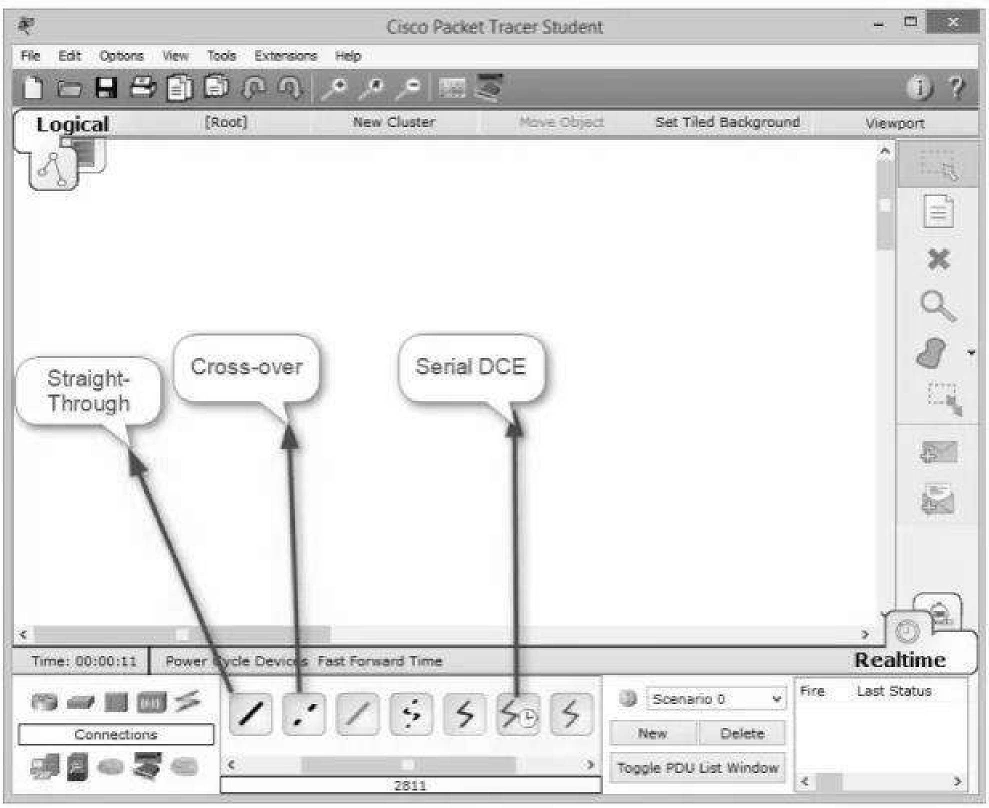
1. To add a router in Cisco Packet Tracer, click the **Router** icon, select a router type, such as **2811**, and then add the selected router in the logical view area.
2. Repeat the same step to add one more router.

Understanding Connection Types in Cisco Packet Tracer

To connect devices in Cisco Packet Tracer, first, you need to understand the various types of cables (connections) used to connect network devices. Some of the common types of cables are:

1. **Straight-through**: Used to connect different types of devices (devices that use different wiring standards), such as Router-to-Switch and Switch-to-PC.
2. **Cross-over**: Used to connect same types of devices, such as router -to-router, PC-to-PC, and switch-to-switch.
3. **Serial DCE**: Used to connect router-to-router in a WAN network.
4. **Console**: Used to take console (using hyper terminal) of a router on a PC.

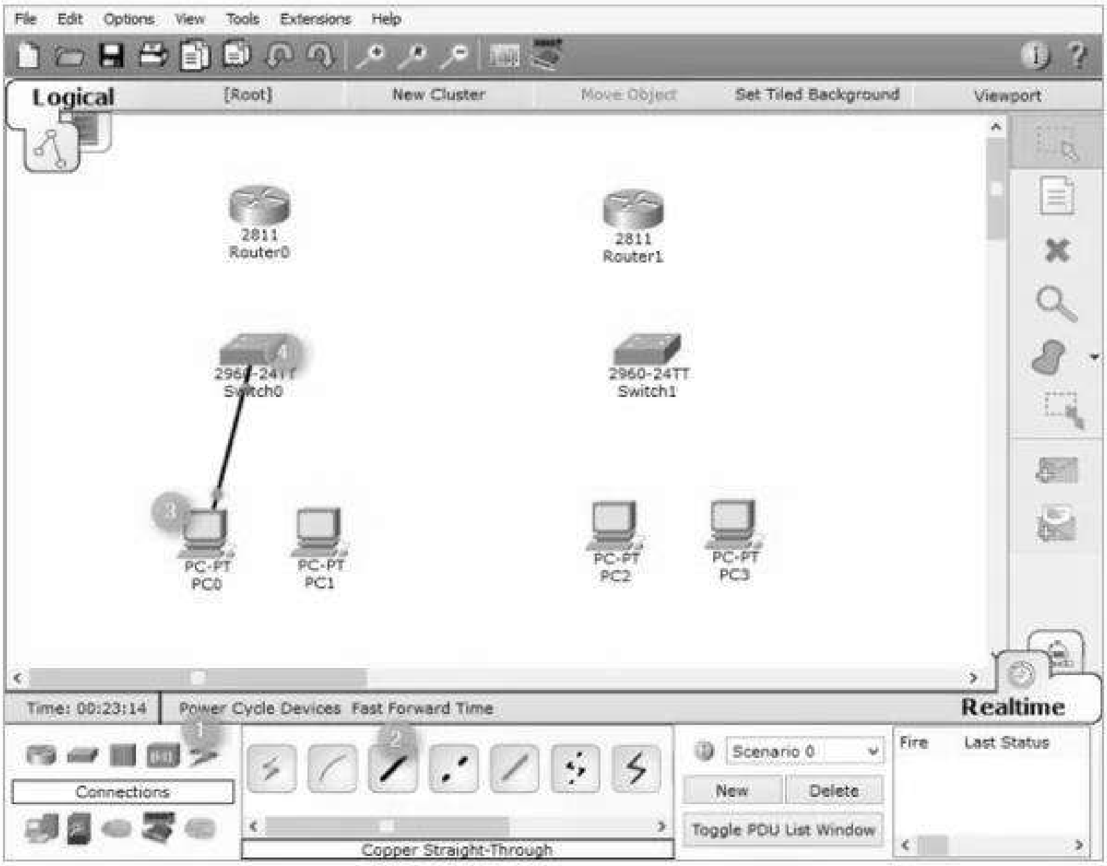
To see the various types of connections, click the **Connection** icon. Spend some time to understand the connections. Once you are familiar with the typ es of connections, connect the devices to create the network topology. The following figure displays the various types of connections used to connect devices.



Connecting Devices in Cisco Packet Tracer

1. To connect devices in Cisco Packet Tracer, click the connection type icon, and select an appropriate cable. For example, to connect **PC0** to **Switch0**, select the straight-through cable, click on **PC0**, select the **FastEthernet0** interface.

2. Next, click on **Switch0**, and then select the **Fast Ethernet0/1** interface. The following figure displays how to connect a PC to a switch in Cisco Packet Tracer.

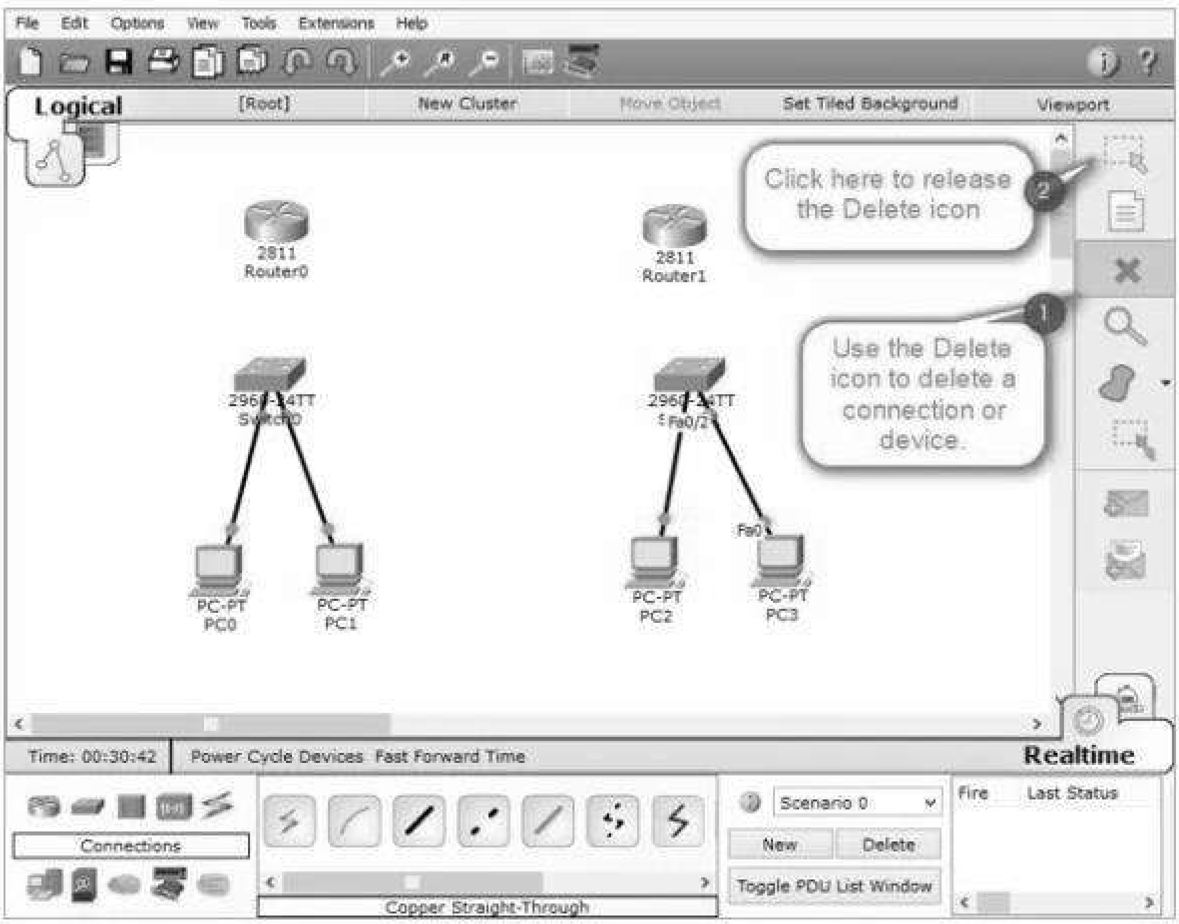


3. Now, add **PC1** to **Switch0** using the **FastEthernet0/2** interface. Also, add **PC2**and **PC3** to the **FastEthernet0/1** and **FastEthernet0/2** interfaces of **Switch1,** respectively.

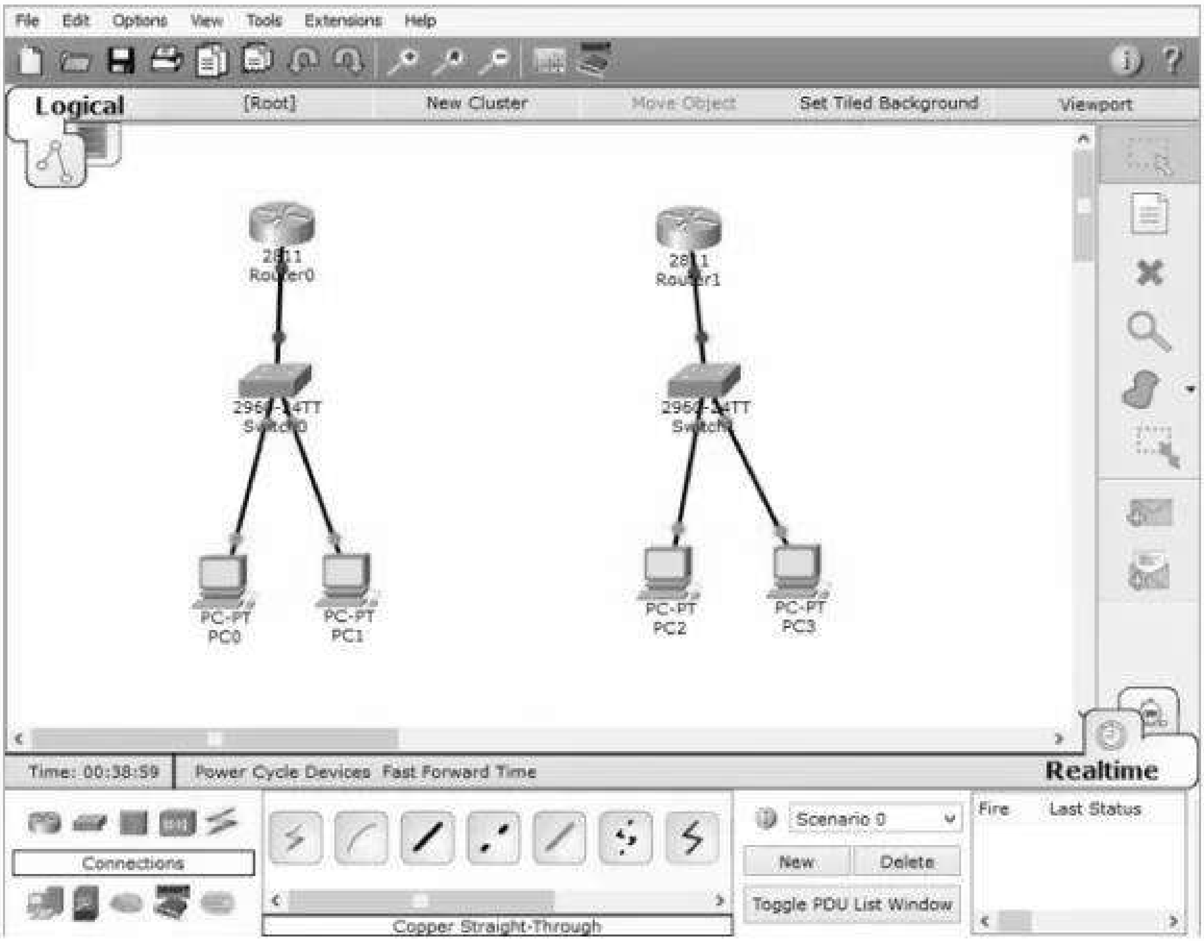
4. If you have connected a wrong device to a wrong interface, you can use the **Delete** option to delete a connection or device. The following figure displays

how to use the **Delete** option to delete a device or connection in Cisco Packet Tracer.

5. Once, you have connected all the PCs to switches, now, connect **Switch0** to **Router0,** and **Switch1** to **Router1** using the straight- through cables.
6. Select the straight-through cable, click on **Switch0**, and then select **FastEthernet0/3** interface.
7. Click **Router0** and select the **FastEthernet0/0** interface.
8. Select again the straight-through cable, click on **Switch1**, and select **FastEthernet0/3** interface.
9. Next, click **Router1** and then select the **FastEthernet0/0** interface.



The following figure displays how to connect routers to switches to create a network topology.



In this experiment, you have learned how to create a network topology in Cisco Packet Tracer. If you wish, you can save the created network topology for the later use. To do this, you need to perform the following steps:

1. In Cisco Packet Tracer, click **File**, and select **Save As**.
2. In the **File name** text box, type a name of the topology, and then click **Save**.

5. Command Prompt and Packet Tracer.

5.1 Introduction

Procedure: To do this EXPERIMENT- follows these steps:

In this EXPERIMENT- students have to understand basic networking commands e.g ping, tracert etc.

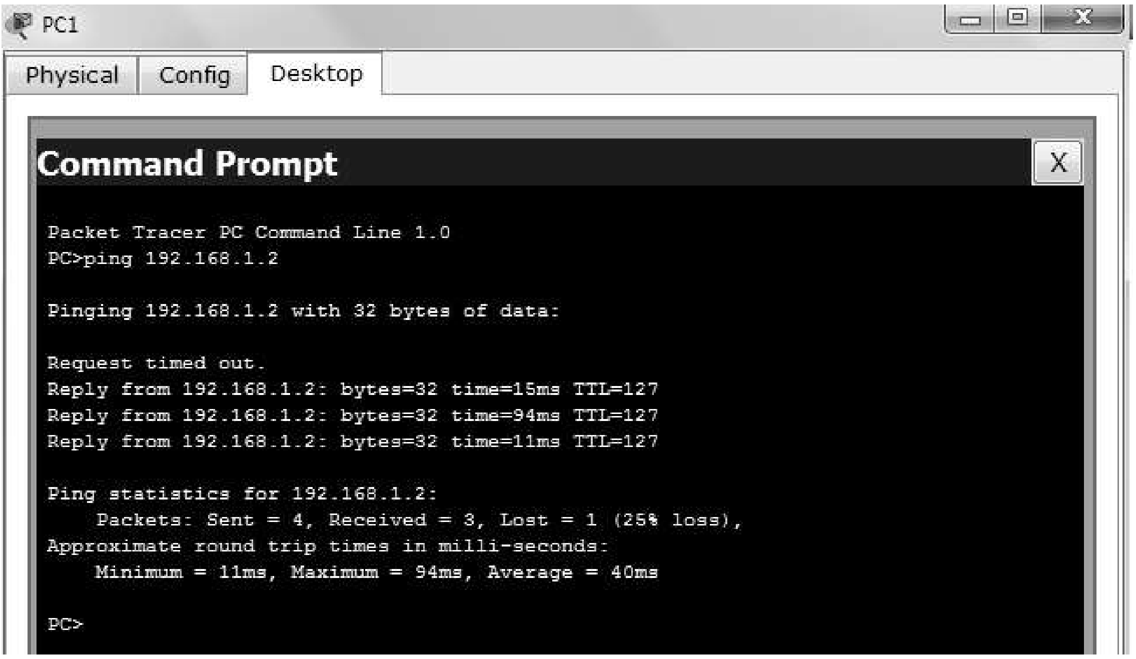
All commands related to Network configuration which includes how to switch to privilege mode and normal mode and how to configure router interface and how to save this configuration to flash memory or permanent memory.

This commands includes

- Configuring the Router commands
- General Commands to configure network
- Privileged Mode commands of a router
- Router Processes & Statistics
- IP Commands
- Other IP Commands e.g. show ip route etc.

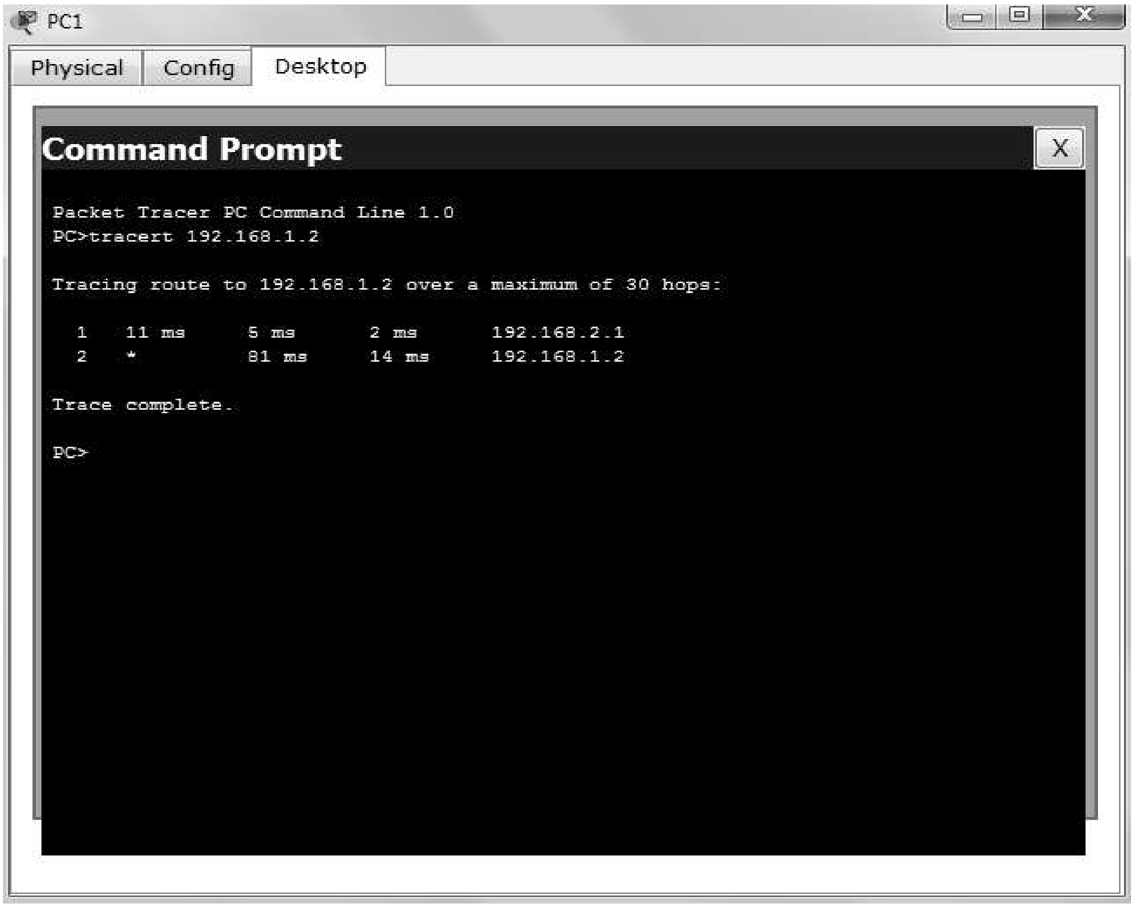
ping:

ping (8) sends an ICMP ECHO_REQUEST packet to the specified host. If the host responds, you get an ICMP packet back. Sound strange? Well, you can "ping" an IP address to see if a machine is alive. If there is no response, you know something is wrong.



Traceroute:

Tracert is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes.

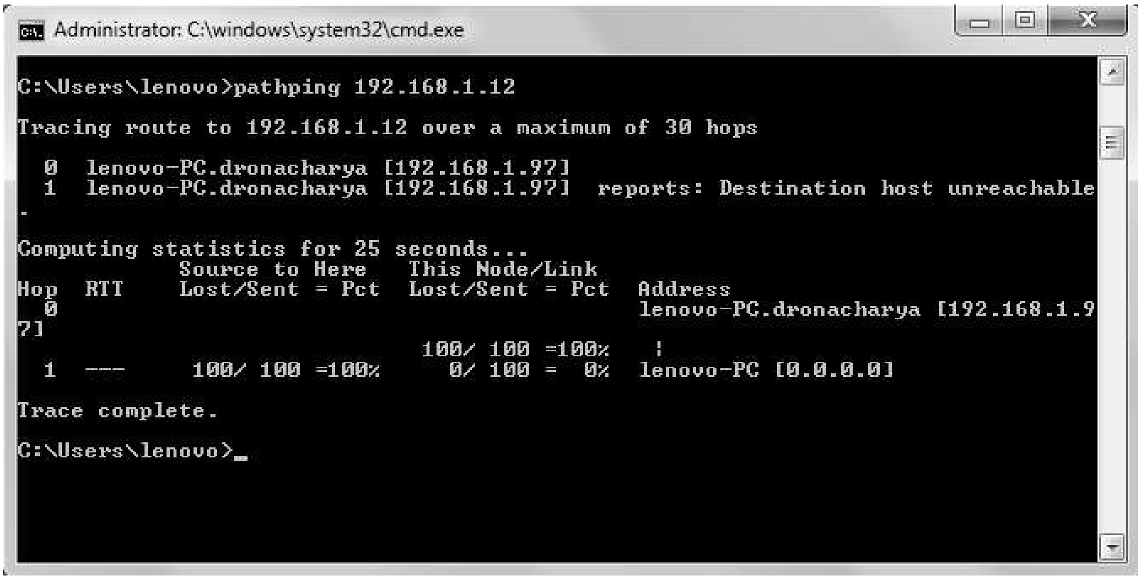


lookup:

Displays information from Domain Name System (DNS) name servers.
NOTE :If you write the command as above it shows as default your pc's server name firstly.

5.2 Path ping:

A better version of tracert that gives you statics about packet lost and latency.



Getting Help

In any command mode, you can get a list of available commands by entering a question mark (?). Router>**?**

To obtain a list of commands that begin with a particular character sequence, type in those haracters followed immediately by the question mark (?).

Router#**co?**

configure connect copy

To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark.

Router#**configure ?**

memory Configure from NV memory network
Configure from a TFTP network host terminal
Configure from the terminal

You can also abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **show** command to **sh**.

5.3 Configuration Files

Any time you make changes to the router configuration, you must save the changes to memory because if you do not they will be lost if there is a system reload or power outage. There are two types of configuration files: the running (current operating) configuration and the startup configuration.

Use the following privileged mode commands to work with configuration files.

- **configure terminal** – modify the running configuration manually from the terminal.
- **show running-config** – display the running configuration.
- **show startup-config** – display the startup configuration.
- **copy running-config startup-config** – copy the running configuration to the startup configuration.
- **copy startup-config running-config** – copy the startup configuration to the running configuration.
- **erase startup-config** – erase the startup-configuration in NVRAM.
- **copy tftp running-config** – load a configuration file stored on a Trivial File Transfer Protocol (TFTP) server into the running configuration.
- **copy running-config tftp** – store the running configuration on a TFTP server.

5.4 IP Address Configuration

Take the following steps to configure the IP address of an interface. Step 1:
Enter privileged EXEC mode:

Router>**enable** password

Step 2: Enter the **configure terminal** command to enter global configuration mode.

Router#**config terminal**

Step 3: Enter the **interface** type slot/port (for Cisco 7000 series) or **interface** type port (for Cisco 2500 series) to enter the interface configuration mode.

Example:

Router (config)#**interface ethernet 0/1**

Step 4: Enter the IP address and subnet mask of the interface using the **ip address** ipaddress subnetmask command.

Example,

Router (config-if)#**ip address 192.168.10.1 255.255.255.0**

Step 5: Exit the configuration mode by pressing Ctrl-Z Router(config-if)#[Ctrl-

6. Create a basic switch setup using Cisco Packet Tracer

6.1 Introduction

Procedure: A new switch just purchased from Cisco contains no default configuration in it. You need to configure the switch with setup mode using the setup mode or from scratch using the command line interface (CLI) before connecting it in your network environment. It is very important to know the basic Cisco switch configuration commands to improve the performances and the security of your internetwork.

Lab instructions

This lab will test your ability to configure basic settings such as hostname, motd banner, encrypted passwords, and terminal options on a Packet Tracer simulated Cisco Catalyst switch.

1. Use the local laptop connect to the switch console and configure the laptop with the right parameters for console access to the Cisco 2960 Catalyst switch

2. Configure Switch hostname as LOCAL-SWITCH

3. Configure the message of the day as "Unauthorized access is forbidden"

4. Configure the password for privileged mode access as "cisco". The password must be md5 encrypted

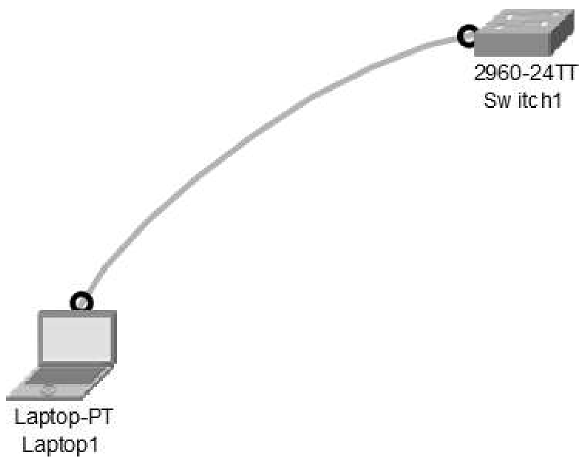
5. Configure password encryption on the switch using the global configuration command

6. Configure CONSOLE access with the following settings :
- Login enabled
- Password : ciscoconsole
- History size : 15 commands
- Timeout : 6'45"
- Synchronous logging

6. Configure TELNET access with the following settings :
- Login enabled
- Password : ciscotelnet
- History size : 15 commands
- Timeout : 8'20"
- Synchronous logging

7. Configure the IP address of the switch as 192.168.1.2/24 and it's default gateway IP (192.168.1.1).
8. Test telnet connectivity from the Remote Laptop using the telnet client.

Network diagram:



Solution**:**

Configure Switch hostname as LOCAL-SWITCH

First connect switch from laptop using console cable (rs232 laptop side and console at switch side)

Then double click on laptop, then goto Terminal press OK.

Switch>enable

Enter configuration commands, one per line. End with CNTL/Z.

Switch#conf t
Switch#hostname LOCAL-SWITCH

Configure the message of the day as "Unauthorized access is forbidden"

banner motd #
Unauthorized access is forbidden#

Configure the password for privileged mode access as "cisco". The password must be md5 encrypted

enable secret cisco

Configure password encryption on the switch using the global configuration command

service password-encryption

Configure CONSOLE access [...]

```
line con 0

password ciscoconsole
logging synchronous
login
history size 15
exec-timeout 6 45
```

Configure TELNET access [...]

```
line vty 0 15

exec-timeout 8 20
password ciscotelnet
logging synchronous
login
history size 15
```

Configure the IP address of the switch as 192.168.1.2/24 and it's default gateway IP (192.168.1.1).

```
interface Vlan1

ip address 192.168.1.2 255.255.255.0

ip default-gateway 192.168.1.1
```

7. Create a basic switch interfaces configuration using Cisco Packet Tracer

7.1 Introduction

Procedure: This lab will test your ability to configure speed, duplex, and vlan settings on Cisco switch network interfaces using Packet Tracer.

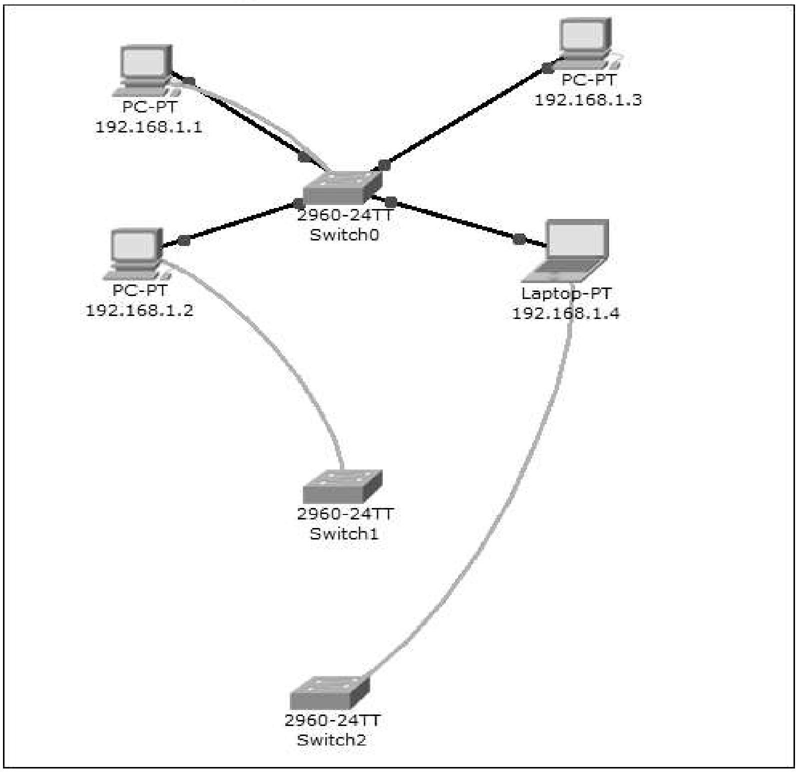
1. Connect to Switch0 using console interface and configure each Switch0 fastethernet switchport for operation. Correct settings are :
- Port type : access port
- Speed : 100 Mbit/s
- Duplex mode : Full Duplex
- Autonegotiation disabled

2. PC "192.168.1.4" seems to be unable to ping other PCs in the network. Check switch configuration.
TIP : How many broadcast domains are there in this network ?

3. Choose the right cable to connect :
- Switch0 gigabitethernet 1/1 to Switch1 gigabitethernet 1/1

- Switch1 gigabitethernet 1/2 to Switch2 gigabitethernet ½

- Network diagram:



Solution:
Connect to Switch0 using console interface and configure each Switch0 fastethernet switchport for operation.

Switch(config)#interface

FastEthernet0/1 switchport

mode access
duplex full
speed 100

Switch(config)#interface FastEthernet0/2 switchport mode access
duplex full speed 100

Switch(config)#interface

FastEthernet0/3 switchport

mode access
duplex full speed
100

Switch(config)#interface

FastEthernet0/4 switchport

mode access
duplex full
speed 100

PC "192.168.1.4" seems to be unable to ping other PCs in the network. Check switch configuration.

Switch(config)#interface

FastEthernet0/4

Switch(config-if)#switchport

mode access Switch(config-

if)#switchport access vlan 1

Choose the right cable to connect :

Switch0 gigabitethernet 1/1 to Switch1 gigabitethernet 1/1

Switch1 gigabitethernet 1/2 to Switch2 gigabitethernet 1/2

Lab 8	Max Marks:
Date:	Time Allowed:

8. Implementation of VLAN Trunk using Packet Tracer

8.1 Introduction

1. To perform basic configuration tasks on a switch

2. Create VLAN and assign switch ports to a VLAN

3. Test and verify the configuration

Description

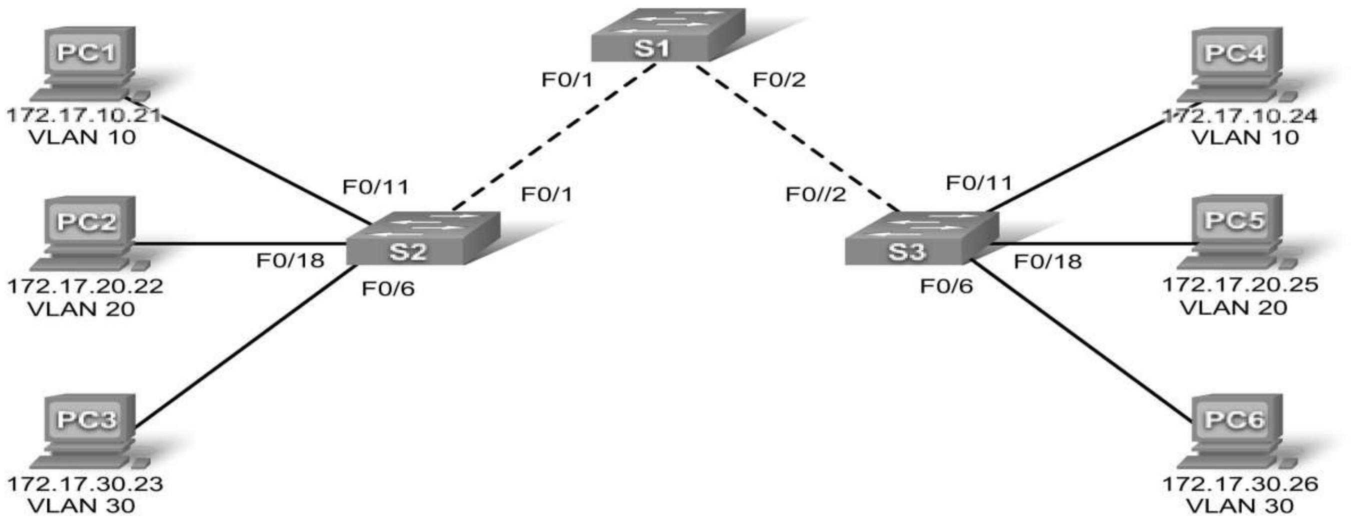
8.2 Virtual LAN:

A Virtual Local Area Network (VLAN) is a logical grouping of network users and resources connected to administratively defined ports on a switch. By creating VLANs, you are able to create smaller broadcast domains within a switch by assigning different ports in the switch to different subnetworks.

8.3 Procedure

To implement this practical following network topology is required to be configured using the VLAN commands. After configuring the given network a packet should be ping from any one machine to another.

8.4 Topology



Task 1: Prepare the Network

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

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

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

```
Switch#config term
Switch(config)#interface range fa0/1-24
```

Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range gi0/1-2
Switch(config-if-range)#shutdown

Task 2: Perform Basic Switch Configurations

Step 1: Configure the switches according to the following guidelines.

· Configure the switch hostname.
· Disable DNS lookup.
· Configure an EXEC mode password of **class**.
· Configure a password of **cisco** for console connections.
· Configure a password of **cisco** for vty connections.

Step 2: Re-enable the user ports on S2 and S3.

S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#switchport mode 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.

You can complete this lab using only two PCs by simply changing the IP addressing for the two PCs specific to a test you want to conduct.

Task 4: Configure VLANs on the Switch

Step 1: Create VLANs on switch S1.

Use the **vlan** *vlan-id* command in global configuration mode to add a VLAN to switch S1. There are four VLANS configured for this lab: VLAN 10 (faculty/staff); VLAN 20 (students); VLAN 30 (guest); and VLAN 99 (management). After you create the VLAN, you will be in vlan configuration mode, where you can assign a name to the VLAN with the **name** *vlan name* command.

S1(config)#vlan 10
S1(config-vlan)#name faculty/staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#end
S1#

Step 2: Verify that the VLANs have been created on S1.

Use the **show vlan brief** command to verify that the VLANs have been created.

S1#**show vlan brief**

Exercise

1. Create and name VLANs 10, 20, 30, and 99 on S2 and S3 using the commands from Task 4 and Step 1. Verify the correct configuration with the **show vlan brief** command.

2. What ports are currently assigned to the four VLANs you have created?

Computer Network	Instructor:
Lab 9	Max Marks:
Date:	Time Allowed:

9. To configure Initial Router Settings

9.1 Introduction

Procedure: In this lab, you will perform basic router configurations. You will secure access to the CLI and console port using encrypted and plain text passwords. You will also configure messages for users **Objectives**

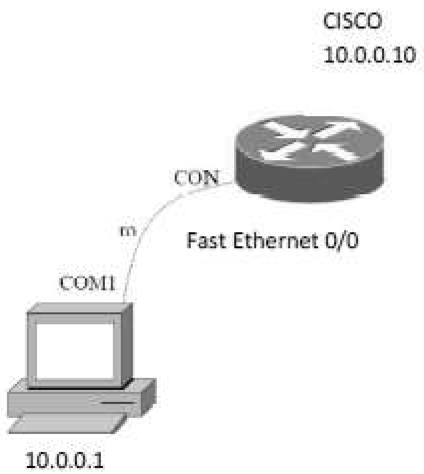
1. Understanding basic networking commands

2. Configuring the Router configuration commands

Description

Cisco uses IOS which stands for Internetwork operating system. IOS is command line interface for configuring switch and router. Following are steps for connecting to router.

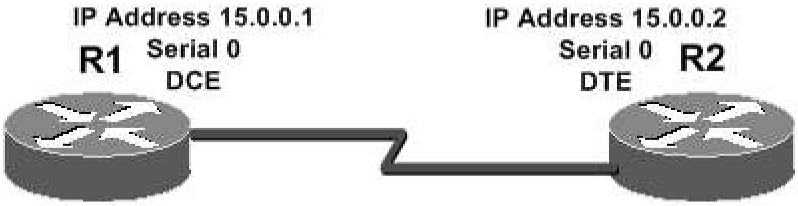
Problem 1: Procedure to configure a Router with the PC



1. Get a Consol Cable
2. Plug the serial end into the back of the computer
3. Put the RJ-45 into the consol port of Router.
4. Get a terminal program
- Hyperterminal
- Tera term
- Minicom
- Securecrt
5. Set it to connect via com port with
Baud rate=9600

Data bits=8
Parity=None
Stop bits=1
Flow Control:None
Configure IP Address on Fast Ethernet 0/1:..
Router(config)# hostname CISCO
CISCO(config)# int fastEthernet 0/1
CISCO(config-if)# ip address 10.0.0.10 255.0.0.0
CISCO(config-if)# no shutdown

Problem 2: Configure Serial Connectivity between two routers

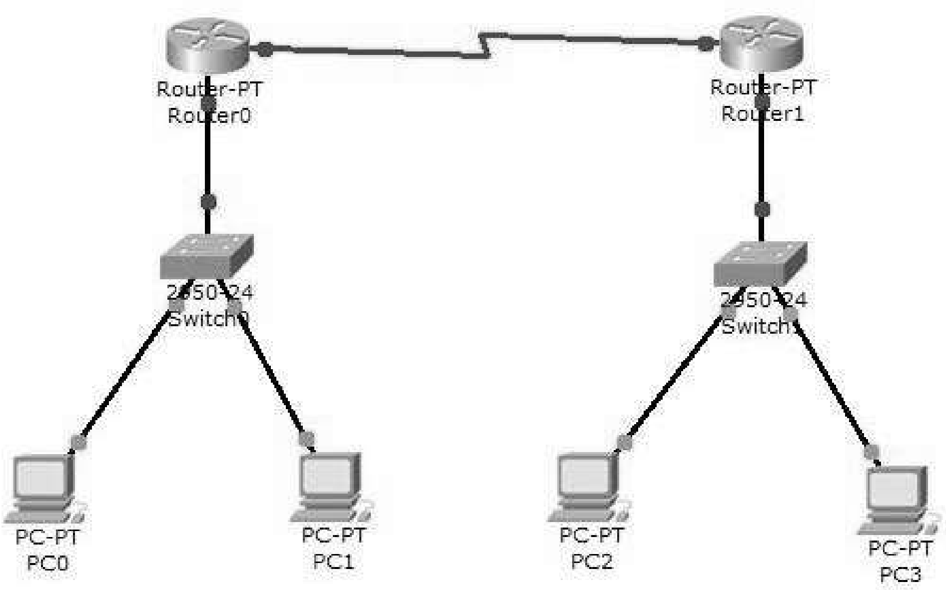


R1(config)# interface serial 0
R1(config-if)# ip address 15.0.0.1 255.0.0.0
R1(config-if)# no shutdown
R1(config-if)# clock rate 64000 (Clock Rate will set only DCE Interface)
R1(config-if)# end
ping: ***ping dest_ip_address***
ping sends an ICMP ECHO_REQUEST packet to the specified host. If the host responds, you get an ICMP packet back.
Traceroute: ***tracert dest_ip_address***
Tracert is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded.

10. Configure a Network topology using packet tracer software.

10.1 Introduction

Procedure: To implement this practical following network topology is required to be configured using the commands learned in previous practical.
After configuring the given network, a packet should be ping from any one machine to another.



Router0 Configuration Command.........

Router>enable
Router#configure
terminal
Enter configuration commands, one per line. End with
CNTL/Z. Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.0.254

255.255.255.0 Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
Router(config-if)#exitRouter(config)#exit
%SYS-5-CONFIG_I: Configured from console by
console Router#
Router#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z. Router(config)#interface FastEthernet0/0
Router(config-
if)#
Router(config-
if)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip address 192.168.1.1
255.255.255.0 Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state
to down Router(config-if)#exit
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by
console Router#wr
Building
configuration...
[OK]
Router#show running-
config Building
configuration...

Current configuration : 542 bytes
!
version 12.2
no service password-encryption
!
hostname Router
!
!
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 192.168.0.254 255.255.255.0
 duplex
 auto speed
 auto
!
interface

```
 FastEthernet1/0 no
 ip address
 duplex
 auto speed
 auto
 shutdown
!
interface Serial2/0
 ip address 192.168.1.1 255.255.255.0
!
nterface Serial3/0 no ip address shutdown
!
interface
 FastEthernet4/0 no
 ip address
 shutdown
!
interface
 FastEthernet5/0 no
 ip address
 shutdown
!
ip classless
!
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end


Router#
```

Router1 Configuration Command.......

```
Continue with configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>ena
ble Router#
```

```
Router#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z. Router(config)#interface Serial2/0
Router(config-if)#ip address 192.168.1.2
255.255.255.0 Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed
state to up Router(config-if)#exit
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by
console Router#config t
Enter configuration commands, one per line. End with
CNTL/Z. Router(config)#
Router(config)#interface
Serial2/0 Router(config-if)#
Router(config-if)#exit
Router(config)#interface
FastEthernet0/0
Router(config-if)#ip address 192.168.2.254
255.255.255.0 Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
Router(config-if)#exit
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by
console Router#wr
Building
configuration...
[OK]
Router#
Router#show running-
config Building
configuration...

Current configuration : 542 bytes
!
version 12.2
no service password-encryption
!
hostname Router
!
!
!
!
!
ip ssh version 1
```

```
!
!
interface FastEthernet0/0
 ip address 192.168.2.254 255.255.255.0
 duplex
 auto speed
 auto
!
interface
 FastEthernet1/0 no
 ip address
 duplex
 auto speed
 auto
 shutdown
!
interface Serial2/0
 ip address 192.168.1.2 255.255.255.0
!
interface
 Serial3/0 no ip
 address
 shutdown
!
interface
 FastEthernet4/0 no
 ip address
 shutdown
!
interface
 FastEthernet5/0 no
 ip address
 shutdown
!
ip classless
!
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end


Router#
```

IP ROUTE Command.....

```
Router#config t
Enter configuration commands, one per line. End with
CNTL/Z. Router(config)#ip route 192.168.2.0
255.255.255.0 192.168.2.2 Router(config)#exit
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
      B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA -
      OSPF inter area N1 - OSPF NSSA external type 1, N2 -
      OSPF NSSA external type 2 E1 - OSPF external type 1, E2
      - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o
      - ODR P - periodic downloaded static route

Gateway of last resort is not set

C   192.168.2.0/24 is directly connected, FastEthernet0/0
C   192.168.1.2/24 is directly connected, Serial2/0
S   192.168.2.0/24 [1/0] via 192.168.1.2
Router#
```

IP ROUTE Command.....

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

Gateway of last resort is not set

S   192.168.0.0/24 [1/0] via 192.168.1.1
C   192.168.0.0/24 is directly connected, FastEthernet0/0
C   192.168.1.1/24 is directly connected, Serial2/0
Router#
```

11. Static Routing

11.1 Introduction

Static routing is a type of network routing technique. Static routing is not a routing protocol; instead, it is the manual configuration and selection of a network route, usually managed by the network administrator. It is employed in scenarios where the network parameters and environment are expected to remain constant.

Static routing is only optimal in a few situations. Network degradation, latency and congestion are inevitable consequences of the non-flexible nature of static routing because there is no adjustment when the primary route is unavailable.

DESCRIPTION:

Figure 8.1: Static Routing

Table: Network addressing for IP network PROCEDURE:

Router	Network Address	Interface	Address
Lab_A	192.168.10.0	fa0/0	192.168.10.1
Lab_A	192.168.20.0	s0/0	192.168.20.1
Lab_B	192.168.20.0	s0/0	192.168.20.2
Lab_B	192.168.40.0	s0/1	192.168.40.1
Lab_B	192.168.30.0	fa0/0	192.168.30.1
Lab_C	192.168.40.0	s0/0	192.168.40.2
Lab_C	192.168.50.0	fa0/0	192.168.50.1

Figure 8.2: Table

Lab_A Configuration
To configure the Lab_A router, you just need to add an IP address to interface FastEthernet 0/0 as well as the serial 0/0. Configuring the hostnames of each router will make identification easier. And why not set the interface descriptions, banner, and router passwords, too? You really should get in the habit of configuring these commands on every router.
Here is how I did all that:

```
Router>en
Router#config t

Router(config)#hostname Lab_A Lab_A(config)#enable secret todd
```

Lab_A(config)#interface fa0/0
Lab_A(config-if)#ip address 192.168.10.1 255.255.255.0 Lab_A(config-if)#description Lab_A LAN Connection Lab_A(config-if)#no shut
Lab_A(config-if)#interface serial 0/0
Lab_A(config-if)#ip address 192.168.20.1 255.255.255.0 Lab_A(config-if)#description WAN Connection to Lab_B Lab_A(config-if)#no shut
Lab_A(config-if)#exit Lab_A(config)#line console 0 Lab_A(config-line)#password ucet Lab_A(config-line)#login Lab_A(config-line)#line aux 0 Lab_A(config-line)#password ucet Lab_A(config-line)#login Lab_A(config-line)#line vty 0 4 Lab_A(config-line)#password ucet Lab_A(config-line)#login Lab_A(config-line)#exit Lab_A(config)#banner motd #
This is the Lab_A router #
Lab_A(config)#ip route 192.168.30.0 255.255.255.0
192.168.20.2
Lab_A(config)#ip route 192.168.40.0 255.255.255.0
192.168.20.2
Lab_A(config)#ip route 192.168.50.0 255.255.255.0
192.168.20.2
Lab_A(config)#ẑ
Lab_A#copy running-config startup-config Destination filename [startup-config]?
[Enter] Lab_A#
Lab_B Configuration
It’s now time to configure the next router. To configure Lab_B, we have three interfaces to deal with: Fast Ethernet 0/0, serial 0/0, and serial 0/1. Both serial interfaces are DCE. What that means to us is that we’ll have to add the clock rate command to each interface.

Router>en Router#config t
Router(config)#hostname Lab_B
Lab_B(config)#enable secret todd Lab_B(config)#interface fa0/0
Lab_B(config-if)#ip address 192.168.30.1 255.255.255.0
Lab_B(config-if)#description Lab_B LAN Connection
Lab_B(config-if)#no shut
Lab_B(config-if)#interface serial 0/0
Lab_B(config-if)#ip address 192.168.20.2 255.255.255.0
Lab_B(config-if)#description WAN Connection to Lab_A

Lab_B(config-if)#clock rate 64000 Lab_B(config-if)#no shut
Lab_B(config-if)#interface serial 0/1
Lab_B(config-if)#ip address 192.168.40.1 255.255.255.0

Lab_B(config-if)#description
WAN Connection to Lab_C
Lab_B(config-if)#clock rate
64000

Lab_B(config-if)#no shut
Lab_B(config-if)#exit
Lab_B(config)#line console 0
Lab_B(config-line)#password
ucet Lab_B(config-line)#login
Lab_B(config-line)#line aux 0
Lab_B(config-line)#password
ucet Lab_B(config-line)#login
Lab_B(config-line)#line vty 0
4 Lab_B(config-
line)#password ucet
Lab_B(config-line)#login
Lab_B(config-line)#exit
Lab_B(config)#banner motd #
This is the Lab_B router #
Lab_B(config)#ip route
192.168.10.0 255.255.255.0
192.168.20.1
Lab_B(config)#ip route
192.168.50.0 255.255.255.0
192.168.40.2
Lab_B(config)#ẑ
Lab_B#copy running-config
startup-config Destination
filename [startup-config]?
[Enter] Lab_B#

Lab_C Configuration

The configuration of Lab_C is
similar to the other two routers
(make sure we remember to
add
passwords, interface
descriptions, and a banner to
the router configuration):
Router>en
Router#config t
Router(config)#hostname
Lab_C Lab_C(config)#enable
secret todd
Lab_C(config)#interface fa0/0
Lab_C(config-if)#ip address
192.168.50.1 255.255.255.0
Lab_C(config-if)#description
Lab_C LAN Connection

Lab_C(config-if)#no shut
Lab_C(config-if)#interface
serial 0/0
Lab_C(config-if)#ip address
192.168.40.2 255.255.255.0
Lab_C(config-if)#description
WAN Connection to Lab_B
Lab_C(config-if)#no shut
Lab_C(config-if)#exit
Lab_C(config)#line console 0
Lab_C(config-line)#password
ucet

Lab_C(config-line)#login
Lab_C(config-line)#line aux 0
Lab_C(config-line)#password
ucet Lab_C(config-line)#login
Lab_C(config-line)#line vty 0
4 Lab_C(config-
line)#password ucet
Lab_C(config-line)#login
Lab_C(config-line)#exit
Lab_C(config)#banner motd #
This is the Lab_C router #
Lab_C(config)#ip route
192.168.30.0 255.255.255.0
192.168.40.1
Lab_C(config)#ip route
192.168.20.0 255.255.255.0
192.16.40.1
Lab_C(config)#ip route
192.168.10.0 255.255.255.0
192.168.40.1
Lab_C(config)# ẑ
Lab_C#copy running-config
startup-config Destination
filename [startup-config]?
[Enter] Lab_C#

11.2 Conclusion:

Summarize, in a paragraph or two, what you conclude from the results of your experiment and whether they are what you expected them to be. Compare the results with theoretical expectations and include percent error when appropriate. Don’t use terms such as "fairly close" and "pretty good;" give explicit quantitative deviations from the expected result. Evaluate whether these deviations fall within your expected errors and state possible explanations for unusual deviations. Discuss and comment on the results and conclusions drawn, including the sources of the errors and the methods used for estimating them.

Computer Network	Instructor:
Lab 12	Max Marks:
Date:	Time Allowed:

12. Dynamic Routing

12.1 Introduction

Dynamic routing is a networking technique that provides optimal data routing. Unlike static routing, dynamic routing enables routers to select paths according to real-time logical network layout changes. In dynamic routing, the routing protocol operating on the router is responsible for the creation, maintenance and updating of the dynamic routing table. In static routing, all these jobs are manually done by the system administrator.

Dynamic routing uses multiple algorithms and protocols. The most popular are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).To accomplish Dynamic routing using Packet Tracer.
PREREQUISITES:
Packet Tracer

software

DESCRIPTION:

Figure 9.1: Dynamic

Routing Table: Network addressing for IP

network

Router	Network Address	Interface	Address
Lab_A	192.168.10.0	fa0/0	192.168.10.1
Lab_A	192.168.20.0	s0/0	192.168.20.1
Lab_B	192.168.20.0	s0/0	192.168.20.2
Lab_B	192.168.40.0	s0/1	192.168.40.1
Lab_B	192.168.30.0	fa0/0	192.168.30.1
Lab_C	192.168.40.0	s0/0	192.168.40.2
Lab_C	192.168.50.0	fa0/0	192.168.50.1

Figure 9.2: Table

PROCEDURE:

Lab_A Configuration To configure the Lab_A router, you just need to add an IP address to interface FastEthernet 0/0 as well as the serial 0/0. Configuring the hostnames of each router will make identification easier. And why not set the interface descriptions, banner, and router passwords, too? You really should get in the habit of configuring these commands on every router.

```
Router>en
Router#config
Router(config)
#hostname
Lab_A
Lab_A(config)
#enable
password ucet
Lab_A(config)
#interface
fa0/0
Lab_A(config-if)#ip address 192.168.10.1
255.255.255.0 Lab_A(config-if)#description
Lab_A LAN Connection Lab_A(config-if)#no
shut
Lab_A(config-if)#interface serial 0/0
Lab_A(config-if)#ip address 192.168.20.1
255.255.255.0 Lab_A(config-if)#description
WAN Connection to Lab_B Lab_B(config-
if)#encapsulation ppp
Lab_A(config-if)#no shut
Lab_A(config-if)#exit
Lab_A(config)#line console
0 Lab_A(config-
line)#password ucet
Lab_A(config-line)#login
Lab_A(config-line)#line
aux 0 Lab_A(config-
line)#password ucet
Lab_A(config-line)#login
Lab_A(config-line)#line vty
0 4 Lab_A(config-
line)#password ucet
Lab_A(config-line)#login
Lab_A(config-line)#exit
Lab_A(config)#banner
motd #
This is the Lab_A
router #
Lab_A(config)#router rip
Lab_A(config-router)#network 192.168.10.0
Lab_A(config-router)#network
192.168.20.0 Lab_A(config-
router)#Ẑ
Lab_A#
Lab_A#copy running-config startup-
config Destination filename [startup-
```

config]? [Enter] Lab_A#
Lab_B Configuration
It’s now time to configure the next router. To configure Lab_B, we have three interfaces to deal with: Fast Ethernet 0/0, serial 0/0, and serial 0/1. Both serial interfaces are DCE. What that means to us is that we’ll have to add the clock rate command to each interface.
Router>en
Router#confi
g t
Router(config)#hostname Lab_B
Lab_B(config)#enable password ucet
Lab_B(config)#interface fa0/0
Lab_B(config-if)#ip address 192.168.30.1
255.255.255.0 Lab_B(config-if)#description
Lab_B LAN Connection Lab_B(config-if)#no
shut
Lab_B(config-if)#interface serial 0/0
Lab_B(config-if)#ip address 192.168.20.2
255.255.255.0 Lab_B(config-if)#description
WAN Connection to Lab_A Lab_B(config-
if)#clock rate 64000
Lab_B(config-if)#no shut
Lab_B(config-
if)#encapsulation
ppp Lab_B(config-
if)#interface serial
0/1
Lab_B(config-if)#ip address
192.168.40.1 255.255.255.0
Lab_B(config-if)#description WAN
Connection to Lab_C Lab_B(config-
if)#clock rate 64000
Lab_B(config-
if)#encapsulation
ppp Lab_B(config-
if)#no shut
Lab_B(config-
if)#exit
Lab_B(config)#line
console 0
Lab_B(config-
line)#password ucet
Lab_B(config-
line)#login
Lab_B(config-
line)#line aux 0
Lab_B(config-
line)#password ucet
Lab_B(config-

line)#login
Lab_B(config-
line)#line vty 0 4
Lab_B(config-
line)#password ucet
Lab_B(config-
line)#login
Lab_B(config-
line)#exit
Lab_B(config)#bann
er motd #
This is the
Lab_B
router #
Lab_B(config)#router rip
Lab_B(config-router)#network 192.168.20.0
Lab_B(config-router)#network 192.168.30.0
Lab_B(config-
router)#network
192.168.40.0
Lab_B(config-router)#Ẑ
Lab_B#
Lab_B#copy running-config
startup-config Destination
filename [startup-config]?
[Enter] Lab_B#
Lab_C Configuration
The configuration of Lab_C is similar to the other two routers (make sure we remember to add passwords, interface descriptions, and a banner to the router configuration):
Route
r>en
Route
r#con
fig t
Router(config)#hostnam
e Lab_C
Lab_C(config)#enable
password ucet
Lab_C(config)#interface
fa0/0
Lab_C(config-if)#ip address
192.168.50.1 255.255.255.0
Lab_C(config-if)#description Lab_C
LAN Connection Lab_C(config-
if)#no shut
Lab_C(config-if)#interface serial 0/0
Lab_C(config-if)#ip address
192.168.40.2 255.255.255.0
Lab_C(config-if)#description WAN

Connection to Lab_B Lab_B(config-
if)#encapsulation ppp
Lab_C(config-if)#no shut Lab_C(config-if)#exit
Lab_C(config)#line console 0 Lab_C(config-
line)#password ucet Lab_C(config-line)#login

Lab_C(config-line)#line
aux 0 Lab_C(config-
line)#password ucet
Lab_C(config-line)#login
Lab_C(config-line)#line
vty 0 4 Lab_C(config-
line)#password ucet
Lab_C(config-line)#login
Lab_C(config-line)#exit
Lab_C(config)#banner
motd #
This is the Lab_C
router #
Lab_C(config)#router rip
Lab_C(config-router)#network 192.168.40.0
Lab_C(config-router)#network
192.168.50.0 Lab_C(config-
router)#Ẑ
Lab_C#
Lab_C#copy running-config startup-
config Destination filename [startup-
config]? [Enter] Lab_C#

12.3 Conclusion:

Summarize, in a paragraph or two, what you conclude from the results of your experiment and whether they are what you expected them to be. Compare the results with theoretical expectations and include percent error when appropriate. Don't use terms such as "fairly close" and "pretty good;" give explicit quantitative deviations from the expected result. Evaluate whether these deviations fall within your expected errors and state possible explanations for unusual deviations. Discuss and comment on the results and conclusions drawn, including the sources of the errors and the methods used for estimating them.

Computer Network	Instructor:
Lab 13	Max Marks:
Date:	Time Allowed:

13. Distance Vector Routing Protocols RIP and IGRP

13.1 Introduction

OBJECTIVES:

To accomplish Dynamic routing using
Packet Tracer. PREREQUISITES:

Packet Tracer software

DESCRIPTION: 

Figure 10.1: Dynamic

Routing Table: Network addressing for IP network

PROCEDURE:

Router	Network Address	Interface	Address
Lab_A	192.168.10.0	fa0/0	192.168.10.1
Lab_A	192.168.20.0	s0/0	192.168.20.1
Lab_B	192.168.20.0	s0/0	192.168.20.2
Lab_B	192.168.40.0	s0/1	192.168.40.1
Lab_B	192.168.30.0	fa0/0	192.168.30.1
Lab_C	192.168.40.0	s0/0	192.168.40.2
Lab_C	192.168.50.0	fa0/0	192.168.50.1

Figure 10.2: Table

Configuring RIP
Routing Lab_A
Lab_A(config)#route
r rip
Lab_A(config-router)#network 192.168.10.0
Lab_A(config-router)#network
192.168.20.0 Lab_A(config-
router)#Ẑ
Lab_A# Lab_B
Lab_B(config)#router rip

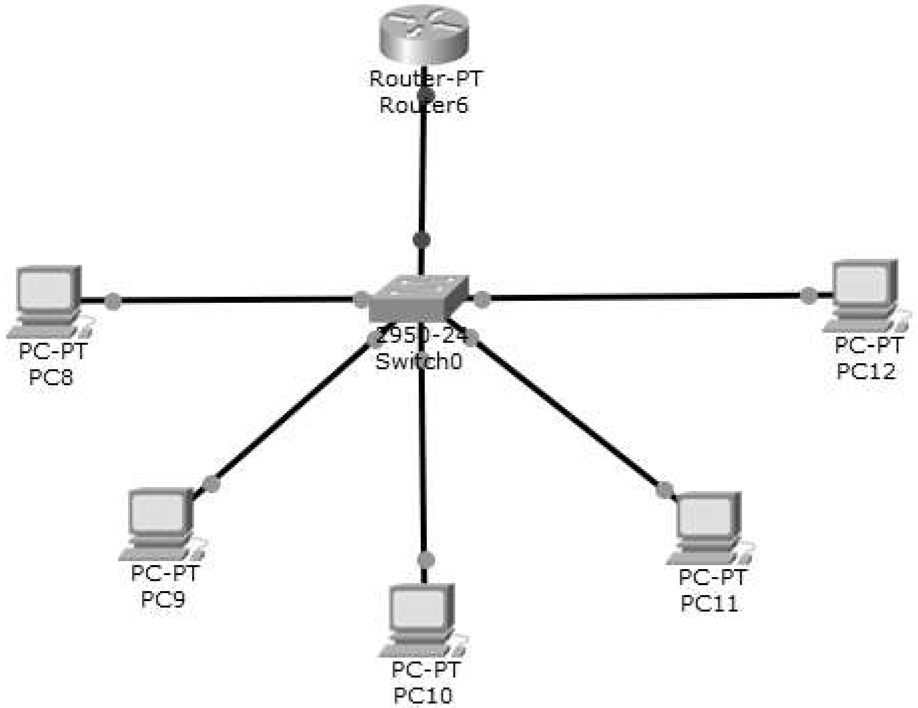
Lab_B(config-router)#network   192.168.20.0
Lab_B(config-router)#network   192.168.30.0
Lab_B(config-router)#network 192.168.40.0
Lab_B(config-router)#Ẑ
Lab_B# Lab_C
Lab_C#config t
Enter configuration commands, one per line. End with CNTL/Z.
Lab_C(config)#no ip route 0.0.0.0 0.0.0.0 192.168.40.1
Lab_C(config)#router rip
Lab_C(config-router)#network 192.168.40.0
Lab_C(config-router)#network 192.168.50.0
Lab_C(config-router)#Ẑ
Lab_C#
Configuring IGRP Routing Lab_A
The AS number, as shown in the router output below, can be any number from 1 to 65,535.
A router can be a member of as many ASes as you need it to be.
Lab_A#config t
Enter configuration commands, one per line. End with CNTL/Z.
Lab_A(config)#router igrp ?
<1-65535> Autonomous system number
Lab_A(config)#router igrp 10
Lab_A(config-router)#netw 192.168.10.0
Lab_A(config-router)#netw 192.168.20.0
Lab_A(config-router)#Ẑ
Lab_A# Lab_B
To configure the Lab_B router, all you need to do is turn on IGRP routing using AS 10 and then
add the network numbers, as shown next:
Lab_B#config t
Enter configuration commands, one per line. End with CNTL/Z.
Lab_B(config)#router igrp 10
Lab_B(config-router)#netw   192.168.20.0
Lab_B(config-router)#netw   192.168.30.0
Lab_B(config-router)#netw 192.168.40.0
Lab_B(config-router)#Ẑ
Lab_B# Lab_C
To configure Lab_C, once again you need to turn on IGRP using AS 10:
Lab_C#config t
Enter configuration commands, one per line. End with CNTL/Z.
Lab_C(config)#router igrp 10
Lab_C(config-router)#netw 192.168.40.0
Lab_C(config-router)#netw 192.168.50.0
Lab_C(config-router)#Ẑ
Lab_C#

13.2 Conclusion:

Summarize, in a paragraph or two, what you conclude from the results of your experiment and whether they are what you expected them to be. Compare the results with theoretical expectations and include percent error when appropriate. Don't use terms such as "fairly close" and "pretty good;" give explicit quantitative deviations from the expected result. Evaluate whether these deviations fall within your expected errors and state possible explanations for unusual deviations. Discuss and comment on the results and conclusions drawn, including the sources of the errors and the methods used for estimating them.

14. Configure DHCP Using Routers.

Diagram:



14.1 Devices:

- *Router (Router PT)*
- *Switch (2950-24)*
- *5 PC's (Generic)*

14.2 Connections:

- *Wire (Copper cross wire)*

14.3 Procedure:

- *open Cisco Packet Tracer from your window menu or shortcut icon displaying on your desktop screen.*
- *Select router from router (Router-PT).*

- *pick the router and put it on the screen.*
- *pick the switch and put it on the screen.*
- *select the end devices from the end devices option and choose generic PC.*
- *pick the end devices and drop them on screen.*
- *now you need a wire to connect these devices, so , pick a wire from connections.*
- *different type of wires found in connections menu. Select the Copper-Cross wire*
- *now connect the end devices with router one by one.*
- *now after connecting the end devices. you just have to configure DHCP on router , IP's to the all PC's will be assigned automatically.*
- *To enable DHCP, router must be configured.*
- *To configure router, click on it.*
- *A menu will appear go to the CLI (Command Line Interface).*
- *Apply the following commands.*

To configure Router PT for Assigning IP to the port fast ethernet 0/0

- *Router>enable*
- *Router#configure terminal*
- *Enter configuration commands, one per line. End with CNTL/Z.*
- *Router(config)#interface fastethernet 0/0*
- *Router(config-if)#ip address 192.168.1.1 255.255.255.0*
- *Router(config-if)#no shutdown*

- *Router(config-if)#*
- *%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up*

- *%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up*

- *To configure Router PT For DHCP*

- *Router>enable*
- *Router#configure terminal*
- *Enter configuration commands, one per line. End with CNTL/Z.*
- *Router(config)#ip dhcp pool 786*
- *Router(dhcp-config)#network 192.168.1.0 255.255.255.0*
- *Router(dhcp-config)#default-router 192.168.1.1*
- *Router(dhcp-config)#end*
- *Router#*
- *%SYS-5-CONFIG_I: Configured from console by console*

- *Now doing all this configuration with router , we just have to configure PC's.*
- *For that purpose, we have to click on PC and have to go to the desktop menu, then to the IP configuration menu and change the static type to the DHCP.*
- *repeat this process for every PC.*
- *you are now done, you have configured DHCP, you can start sending packets from any one PC to the other.*