International Islamic University, Islamabad
Computer Networks LAB

EXPERIMENT # 01: Ethernet Cabling

Name of Student: ……..

Roll No.: ……

Date of Experiment: ……..

Report submitted on: ……..

Marks obtained: ……

Remarks: ……

Instructor's Signature: ……...

Ethernet Cabling

1. Objective

This lab exercise is designed to give students hands on experience of building CAT-5 UTP Ethernet patch cables.

2. Resources Required

- CAT 5 Cable - bulk Category 5, 5e or 6 cable
- RJ45 Ends
- Crimper for RJ45
- Wire Cutters - to cut and strip the cable if necessary
- Wire Stripper
- Cable Tester

3. Introduction

Network media is the actual path over which an electrical signal travels as it moves from one component to another. There are different types of network cables such as **twisted-pair cable** (electric)**, coaxial cable** (electric), and **fiber optic cable** (light). This section, however, describes only twisted pair and coaxial cables.

3.1 Twisted Pair Cable

Twisted-pair cable is a type of cabling that is used for telephone communications and most modern Ethernet networks. A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk, the noise generated by adjacent pairs. When electrical current flows through a wire, it creates a small, circular magnetic field around the wire. When two wires in an electrical circuit are placed close together, their magnetic fields are the exact opposite of each other. Thus, the two magnetic fields cancel each other out. They also cancel out any outside magnetic fields. Twisting the wires can enhance this cancellation effect. Using cancellation together with twisting the wires, cable designers can effectively provide self-shielding for wire pairs within the network media. Two basic types of twisted-pair cable exist: unshielded twisted pair (UTP) and shielded twisted pair (STP). The following sections discuss UTP and STP cable in more detail.

3.2 UTP Cable

UTP cable is a medium that is composed of pairs of wires (see Figure 1-1). UTP cable is used in a variety of networks. Each of the eight individual copper wires in UTP cable is covered by an insulating material. In addition, the wires in each pair are twisted around each other.

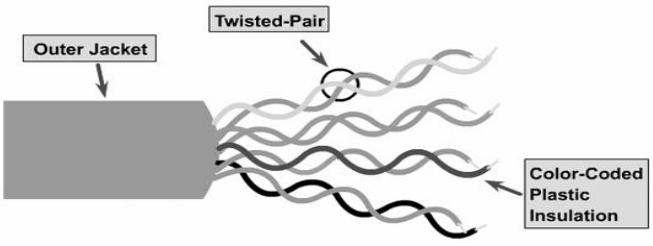


Figure 1-1 Unshielded Twisted-Pair Cable

UTP cable relies solely on the cancellation effect produced by the twisted wire pairs to limit signal degradation caused by electromagnetic interference (EMI) and radio frequency interference (RFI). To further reduce crosstalk between the pairs in UTP cable, the number of twists in the wire pairs varies. UTP cable must follow precise specifications governing how many twists or braids are permitted per meter (3.28 feet) of cable.

UTP cable often is installed using a Registered Jack 45 (RJ-45) connector (see Figure 1-2). The RJ-45 is an eight-wire connector used commonly to connect computers onto a local-area network (LAN), especially Ethernets.

Figure 1-2 RJ-45 Connectors

Although UTP was once considered to be slower at transmitting data than other types of cable, this is no longer true. In fact, UTP is considered the fastest copper-based medium today.

The following summarizes the features of UTP cable:

- Speed and throughput—10 to 1000 Mbps
- Average cost per node—Least expensive
- Media and connector size—Small
- Maximum cable length—100 m (short)

3.3 Shielded Twisted-Pair Cable

Shielded twisted-pair (STP) cable combines the techniques of shielding, cancellation, and wire twisting. Each pair of wires is wrapped in a metallic foil (see Figure 1-3). The four pairs of wires then are wrapped in an overall metallic braid or foil, usually 150-ohm cable. As specified for use in Ethernet network installations, STP reduces electrical noise both within the cable (pair-to-pair coupling, or crosstalk) and from outside the cable (EMI and RFI). STP usually is installed with STP data connector, which is created especially for the STP cable. However, STP cabling also can use the same RJ connectors that UTP uses.

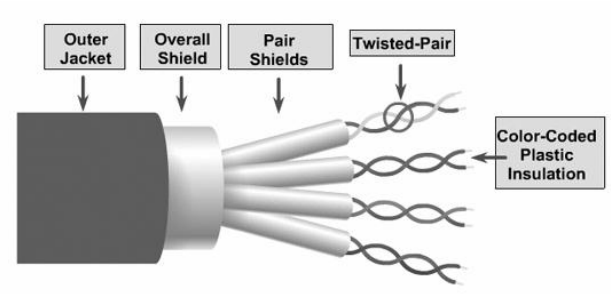


Figure 1-3 Shielded Twisted-Pair Cable

Although STP prevents interference better than UTP, it is more expensive and difficult to install. In addition, the metallic shielding must be grounded at both ends. If it is improperly grounded, the shield acts like an antenna and picks up unwanted signals. Because of its cost and

difficulty with termination, STP is rarely used in Ethernet networks. STP is primarily used in Europe.
The following summarizes the features of STP cable:

- Speed and throughput—10 to 100 Mbps
- Average cost per node—Moderately expensive
- Media and connector size—Medium to large
- Maximum cable length—100 m (short)

When comparing UTP and STP, keep the following points in mind:

- The speed of both types of cable is usually satisfactory for local-area distances.
- These are the least-expensive media for data communication. UTP is less expensive than STP.
- Because most buildings are already wired with UTP, many transmission standards are adapted to use it, to avoid costly rewiring with an alternative cable type.

3.4 Coaxial Cable

Coaxial cable consists of a hollow outer cylindrical conductor that surrounds a single inner wire made of two conducting elements. One of these elements, located in the center of the cable, is a copper conductor. Surrounding the copper conductor is a layer of flexible insulation. Over this insulating material is a woven copper braid or metallic foil that acts both as the second wire in the circuit and as a shield for the inner conductor. This second layer, or shield, can help reduce the amount of outside interference. Covering this shield is the cable jacket.

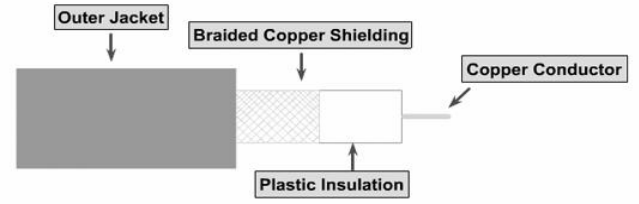


Figure 1-4 Coaxial Cable

Coaxial cable supports 10 to 100 Mbps and is relatively inexpensive, although it is more costly than UTP on a per-unit length. However, coaxial cable can be cheaper for a physical bus topology because less cable will be needed. Coaxial cable can be cabled over longer distances than twisted-pair cable. For example, Ethernet can run approximately 100 meters (328 feet) using twisted-pair cabling. Using coaxial cable increases this distance to 500m (1640.4 feet).

For LANs, coaxial cable offers several advantages. It can be run with fewer boosts from repeaters for longer distances between network nodes than either STP or UTP cable. Repeaters regenerate the signals in a network so that they can cover greater distances. Coaxial cable is less expensive than fiber-optic cable, and the technology is well known; it has been used for many years for all types of data communication.

Figure 1-5 Thinnet and BNC Connector

The following summarizes the features of coaxial cables:

- Speed and throughput—10 to 100 Mbps
- Average cost per node—Inexpensive
- Media and connector size—Medium
- Maximum cable length—500 m (medium)

4. Internal Structure of the UTP Cable

Here is what the internals of the cable look like:

Figure 1-6 Internal Cable Structure and Color Coding

Inside the cable, there are 8 color coded wires. These wires are twisted into 4 pairs of wires; each pair has a common color theme. One wire in the pair being a solid or primarily solid colored wire and the other being a primarily white wire with a colored stripe (Sometimes cable doesn't have any color on the striped cable, the only way to tell is to check which other wire it is twisted around). Examples of the naming schemes used are: Orange (alternatively Orange/White) for the solid colored wire and White/Orange for the striped cable. The twists are extremely important. They are there to counteract noise and interference. It is important to wire according to a standard to get proper performance from the cable. The TIA/EIA-568-A specifies two wiring standards for a 8-position modular connector such as RJ45. The two wiring standards, T568A and T568B vary only in the arrangement of the colored pairs.

5. RJ45 Ends

The RJ45 end is an 8-position modular connector that looks like a large phone plug. There are a couple variations available. The primary variation you need to pay attention to is whether the connector is intended for braided or solid wire. For braided/stranded wires, the connector has contacts that actually pierce the wire. For solid wires, the connector has fingers which pierce the insulation and make contact with the wire by grasping it from both sides. Here is a diagram and pinout:

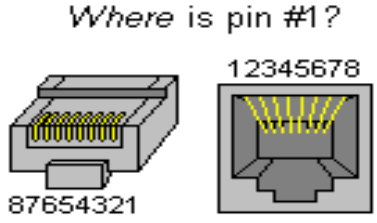
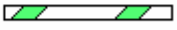
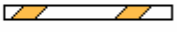
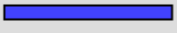
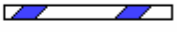
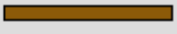


Figure 1-7 RJ45 Jack and Plug Pinout

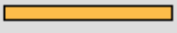
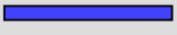
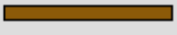
6. Ethernet Cable Pinouts

There are two basic cables. A straight through cable, which is used to connect to a hub or switch, and a cross over cable used to operate in a peer-to-peer fashion without a hub/switch. Some interfaces can cross and un-cross a cable automatically as needed, really quite nice.

Standard, Straight-Through Wiring (both ends are the same)

RJ45 Pin #	Wire Color (T568A)	Wire Diagram (T568A)	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	White/Green		Transmit+	Bl_DA+
2	Green		Transmit-	Bl_DA-
3	White/Orange		Receive+	Bl_DB+
4	Blue		Unused	Bl_DC+
5	White/Blue		Unused	Bl_DC-
6	Orange		Receive-	Bl_DB-
7	White/Brown		Unused	Bl_DD+
8	Brown		Unused	Bl_DD-

Straight-Through Cable Pinout for T568A

RJ45 Pin #	Wire Color (T568B)	Wire Diagram (T568B)	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	White/Orange		Transmit+	Bl_DA+
2	Orange		Transmit-	Bl_DA-
3	White/Green		Receive+	Bl_DB+
4	Blue		Unused	Bl_DC+
5	White/Blue		Unused	Bl_DC-
6	Green		Receive-	Bl_DB-
7	White/Brown		Unused	Bl_DD+
8	Brown		Unused	Bl_DD-

Straight-Through Cable Pinout for T568B

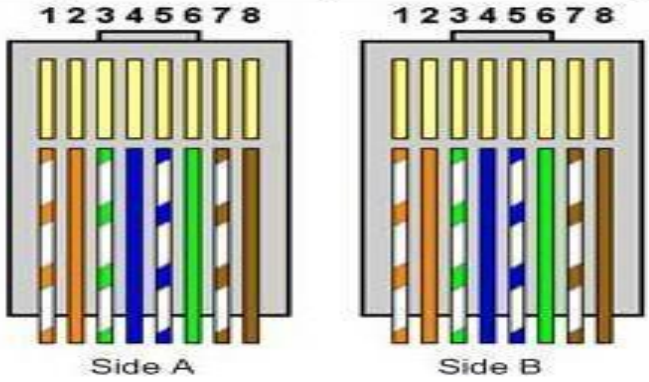
6.1 Straight Cable

You usually use straight cable to **connect different type of devices**. This type of cable will be used most of the time and can be used to:

1) Connect a computer to a switch/hub's normal port.
2) Connect a computer to a cable/DSL modem's LAN port.
3) Connect a router's WAN port to a cable/DSL modem's LAN port.
4) Connect a router's LAN port to a switch/hub's uplink port (normally used for expanding network).
5) Connect 2 switches/hubs with one of the switch/hub using an uplink port and the other one using normal port.

If you need to check how straight cable looks like, it's easy. **Both sides (side A and side B) of cable have wire arrangement with same color**.

Pin ID	Side A	Side B
1	Orange-white	Orange-white
2	Orange	Orange
3	Green-white	Green-white
4	Blue	Blue
5	Blue-white	Blue-white
6	Green	Green
7	Brown-white	Brown-white
8	Brown	Brown



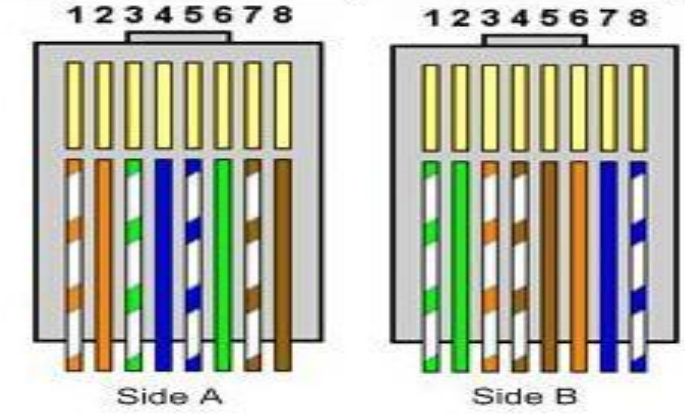
6.2 Crossover Cable

Sometimes you will use crossover cable, it's usually used to **connect same type of devices**. A crossover cable can be used to:

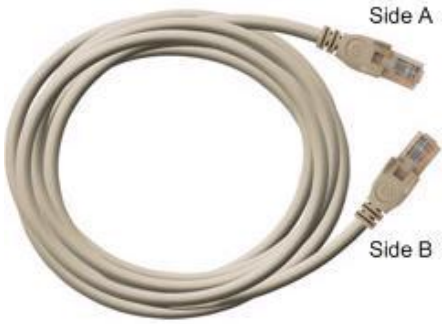
1) Connect 2 computers directly.
2) Connect a router's LAN port to a switch/hub's normal port. (normally used for expanding network)
3) Connect 2 switches/hubs by using normal port in both switches/hubs.

In you need to check how crossover cable looks like; **both sides (side A and side B) of cable have wire arrangement with following different color**.

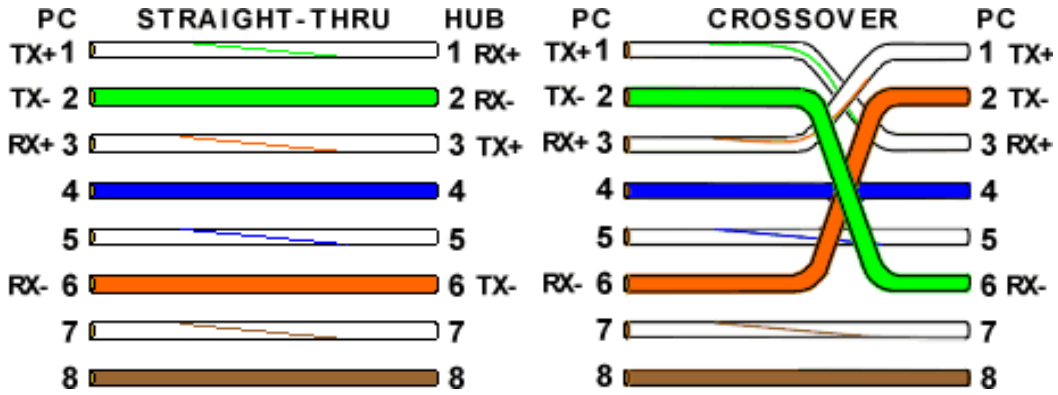
Pin ID	side A	side B
1	Orange-white	green-white
2	Orange	green
3	green-white	orange-white
4	blue	brown-white
5	blue-white	Brown
6	green	orange
7	brown-white	Blue
8	brown	blue-white



Note: If there is **auto MDI/MDI-X** feature support on the switch, hub, network card or other network devices, you don't have to use crossover cable in the situation which is mentioned above. This is because crossover function would be enabled automatically when it's needed.



A simple UTP cable



Commonly used types of UTP cabling are as follows
Category 1—Used for telephone communications. Not suitable for transmitting data.
Category 2—Capable of transmitting data at speeds up to 4 megabits per second (Mbps).
Category 3—Used in 10BASE-T networks. Can transmit data at speeds up to 10 Mbps.
Category 4—Used in Token Ring networks. Can transmit data at speeds up to 16 Mbps.
Category 5—Can transmit data at speeds up to 100 Mbps.
Category 5e—Used in networks running at speeds up to 1000 Mbps (1 gigabit per second [Gbps]).
Category 6—Typically, Category 6 cable consists of four pairs of 24 American Wire Gauge (AWG) copper wires. Category 6 cable is currently the fastest standard for UTP.

7. Procedure to make Ethernet Cables

1. Strip off about 2 inches of the cable sheath.
2. Untwist the pairs - don't untwist them beyond what you have exposed, the more untwisted cable you have the worse the problems you can run into.
3. Align the colored wires according to the diagrams above.
4. Trim all the wires to the same length, about 1/2" to 3/4" left exposed from the sheath.
5. Insert the wires into the RJ45 end - make sure each wire is fully inserted to the front of the RJ45 end and in the correct order. The sheath of the cable should extend into the RJ45 end by about 1/2" and will be held in place by the crimp.
6. Crimp the RJ45 end with the crimper tool

Crimper tool

7. Verify the wires ended up the right order and that the wires extend to the front of the RJ45 end and make good contact with the metal contacts in the RJ45 end.
8. Cut the cable to length - make sure it is more than long enough for your needs. Remember, an end to end connection should not extend more than 100m (~328ft). Try to keep cables short, the longer the cable becomes the more it may affect performance, usually noticeable as a gradual decrease in speed and increase in latency.
9. Repeat the above steps for the second RJ45 end.
10. If a cable tester is available, use it to verify the proper connectivity of the cable.

International Islamic University, Islamabad
Computer Networks Lab

LAB WORKSHEET (Lab # 1)

Q.1 What is the advantage of having twists in a twisted pair cable?

_____
_____
_____
_____
_____

Q.2 Identify the differences between twisted pair and coaxial cables.

_____
_____
_____
_____
_____

Q.3 Which type twisted pair cable will you use to connect?
Router to Hub, Router to Router, PC to HUB, PC to PC

_____
_____
_____
_____
_____

Q.4 Can you connect a hub to another hub or a switch to another switch to another switch using a straight-through cable? Explain your answer.

_____
_____
_____
_____
_____

International Islamic University, Islamabad
Computer Networks LAB

EXPERIMENT # 02: Setting up a small Network

Name of Student: ……..

Roll No.: ……

Date of Experiment: ……..

Report submitted on: ……..

Marks obtained: ……

Remarks: ……

Instructor's Signature: ……...

Setting up a small Network

1. Objective

This lab exercise is designed to demonstrate and help in learning & understanding of the procedure of setting up a small network (that can be used in homes too).

2. Resources Required

- Straight & Cross Cat5 UTP cables – (made in last lab)
- Computers
- A Switch/Hub (if network size is to be increased)
- A Router (if communication is to be done with WAN/Internet)

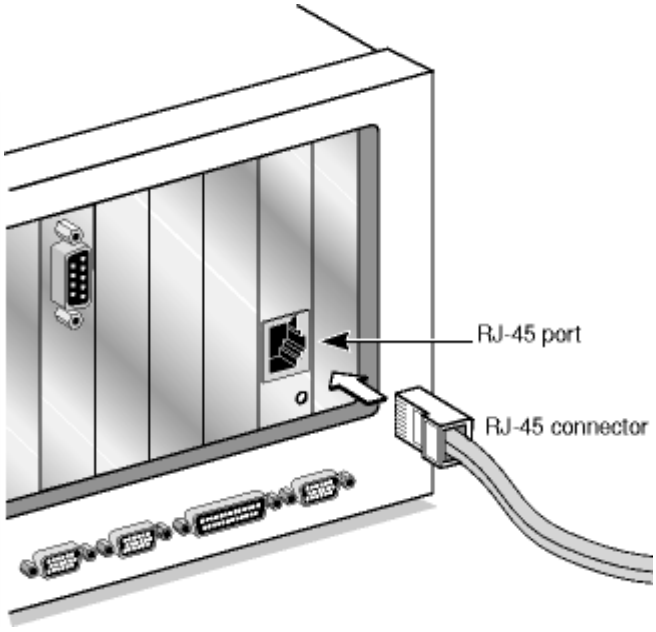
3. Introduction

This lab introduces **NIC** (**N**etwork **I**nterface **C**ontroller/**C**ard), **Switch/Hub** & **Router**. Before going to the procedure, firstly a small introduction of the devices is given.

3.1 NIC (Network Interface Card)

A network interface controller is a computer hardware component that connects a computer to a computer network. The controller may also be referred to as a network adapter, or a LAN adapter. Also known as a network interface card, network card or LAN card.

It is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.



3.1 Hub

An Ethernet hub, active hub, network hub, repeater hub or hub is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. **Hub works at the physical layer (layer 1) of the OSI model**. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

A network hub is a fairly unsophisticated broadcast device. Hubs do not manage any of the traffic that comes through them, and any packet entering any port is regenerated and broadcast out on all other ports.

3.3 Switch (LAN Switch)

Switches are devices capable of creating temporary connections between two or more devices linked to the switch. It acts just like hub but has advanced features for network optimization & better security. **Switch works at the Data Link layer (layer 2) of the OSI model**. The work a switch does is called **switching**.

Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.

The main purpose of both Switch & Hub is to extend the size of network.

3.4 Router

A router is a device in computer networking that forwards data packets to their destinations, based on their addresses. The work a router does is called routing, which is somewhat like switching, but a router is different from a switch. The latter is simply a device to connect machines to form a LAN.

Routers work at the Network layer (layer 3) of the OSI model. Their main purpose is to allow communication between different network.

4. Network Commands (Testing)

The widely used commands for testing network connectivity are PING, TRACERT & TELNET. (Just remember these commands are not case sensitive so PING is same as ping or PinG)

4.1 PING

Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

ping target_name/target_IP

4.2 TRACERT

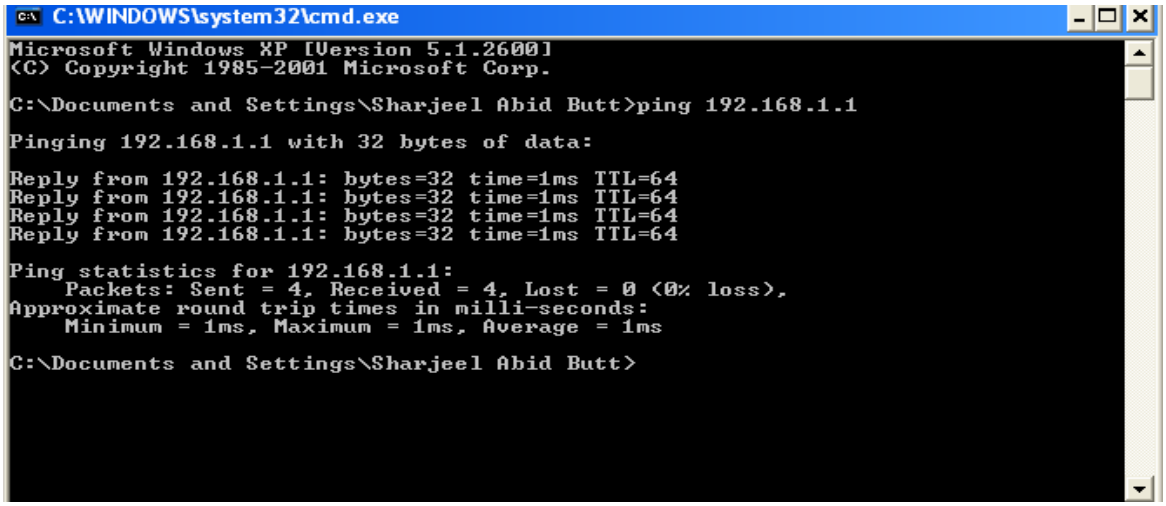
Tracert determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination with incrementally increasing Time to Live (TTL) field values. The path displayed is the list of near-side router interfaces of the routers in the path between a source host and a destination. The near-side interface is the interface of the router that is closest to the sending host in the path.
This utilty is available as **traceroute** in some operating systems.

tracert target_name/target_IP

4.3 TELNET

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection. Historically, Telnet provided access to a command-line interface (usually, of an operating system) on a remote host. Most network equipment and operating systems with a TCP/IP stack support a Telnet service for remote configuration (including systems based on Windows NT). Because of security issues with Telnet, its use for this purpose has waned in favor of SSH (**S**ecure **SH**ell).

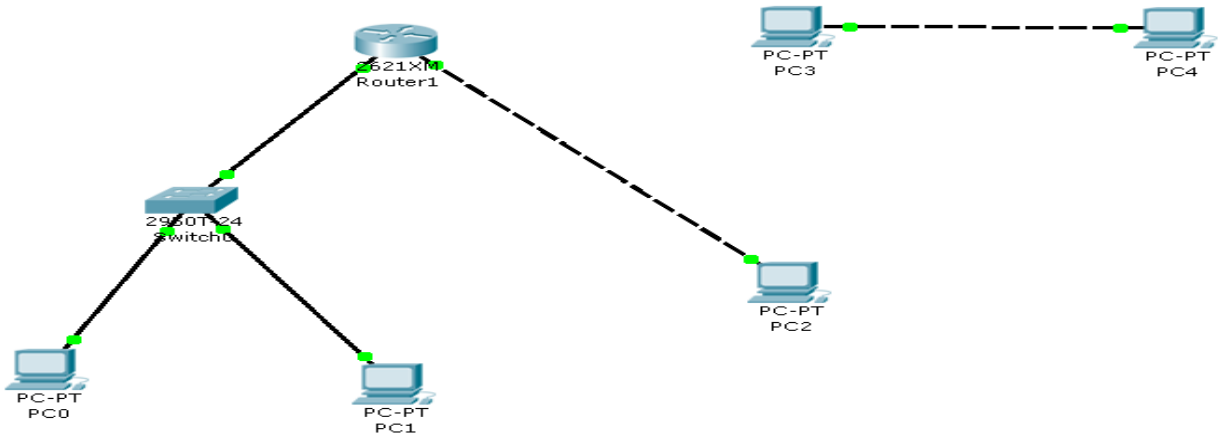
telnet target_name/target_IP



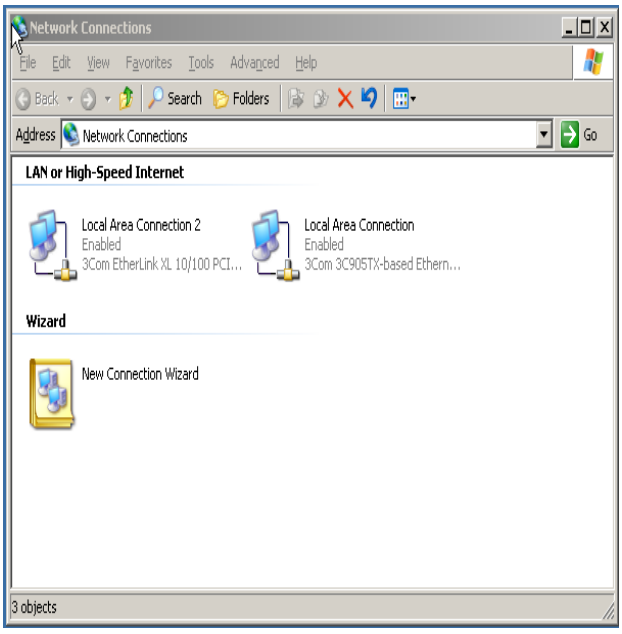
MS DOS command window showing use of ping

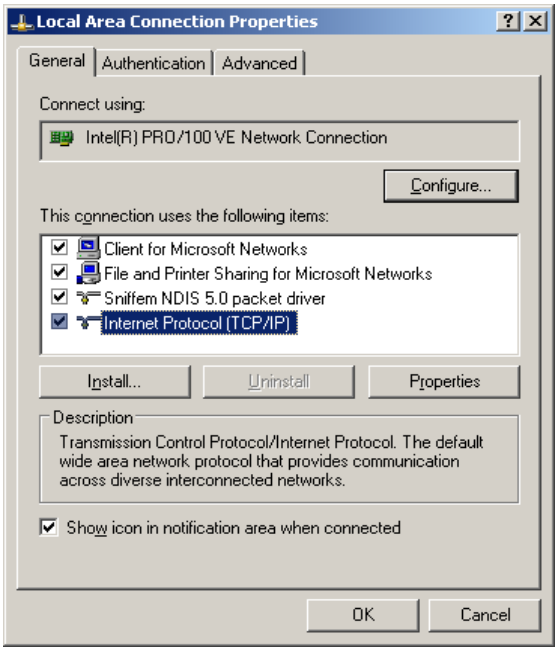
5. Procedure to setup Network

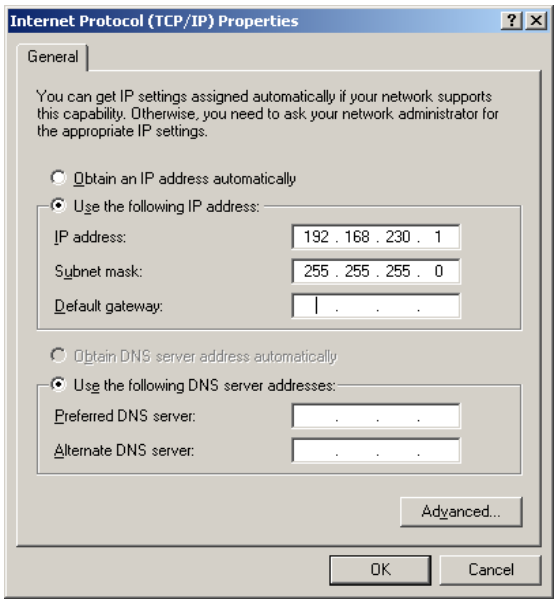
(For this lab only - consider the switch & router automatically configured)



1. Connect devices to each other with the correct UTP (straight/cross) cables and power them ON.
2. Use the Control Panel/Network Connections (or Properties in Context Menu of My Network Places) to display Network Connections Window. Then use Properties in Context Menu of Local Area Connection to display Local Area Connection Properties Window. Select the TCP/IP protocol from the Configuration Tab and click on properties. Check the IP Address and Subnet mask for both workstations on the IP Address Tab.







3. Set **IP address** of PC0 to 192.168.1.2, PC1 to 192.168.1.3 & PC2 to 192.168.3.2 .
4. Set **default gateway** of PC0 & PC1 to 192.168.1.1 and PC2 to 192.168.3.1 . These are actually the addresses of the router interfaces.
5. For PC4 & PC5 set any **IP address** and ignore the **default gateway** as they are not connected to any router.
6. Test the connectivity by using the commands mentioned in **section 4**.
7. If everything is ok then play the multiplayer games installed on the PC.

International Islamic University, Islamabad
Computer Networks Lab

LAB WORKSHEET (Lab # 2)

Q.1 What is the purpose of Switch in a network?

_____
_____
_____
_____
_____

Q.2 Identify the differences between Switch and Hub.

_____
_____
_____
_____
_____

Q.3 Which OSI layer device is the following?
Router, Hub, Switch

_____
_____
_____
_____
_____

Q.4 What are the differences between tracert & ping?

_____
_____
_____
_____
_____

International Islamic University, Islamabad
Computer Networks LAB

EXPERIMENT # 03: Network Emulators & Simulators

Name of Student: ……..

Roll No.: ……

Date of Experiment: ……..

Report submitted on: ……..

Marks obtained: ……

Remarks: ……

Instructor's Signature: ……...

Network Emulators & Simulators

1. Objective

This lab exercise is designed to understand the difference and working of network emulators and simulators.

2. Resources Required

- Computer
- Packet Tracer (version 5 or higher)

3. Introduction

This lab introduces Packet Tracer 5 which is a network simulator provided by Cisco. Before using it we'll learn about network emulators and simulators.

3.1 Network Emulator

Network Emulator creates virtual hardware that allows software, intended to run on real devices, to be run on our general purpose PCs. The process done by it is called **Emulation**. Most widely used network emulator for Cisco devices is **Dynamips.** The two popular front ends for Dynamips are **Dynagen** (CLI based) and **GNS3** (GUI based). Using emulator allows you utilize nearly all the functionalities of original hardware allowing usage in real networks.

The purpose of emulator is to duplicate the hardware functionality of a device.

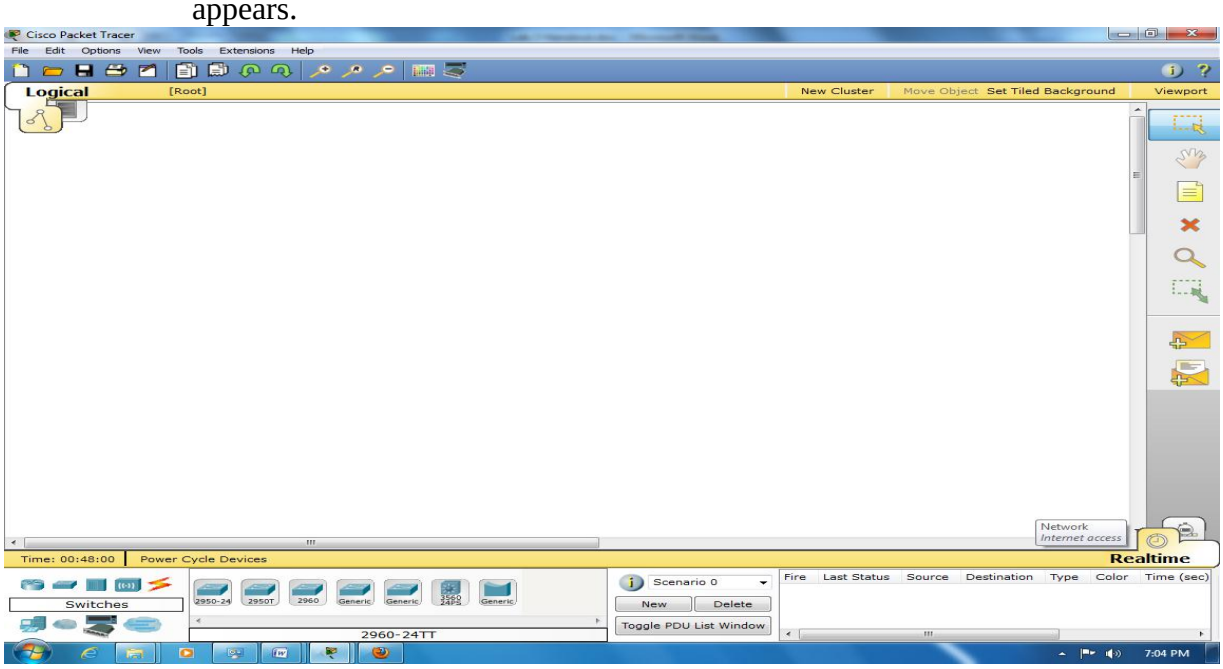
3.2 Network Simulator

Network Simulator creates the software portion of the hardware only so you can't use them with real networks. The process done by it is called **Simulation**. Most widely used network simulators are OPNET, NS (both are general-purpose) and Packet Tracer (for Cisco devices). Using Simulator allows us to (**only**) test networks before deploying in the real world. Also they usually don't have all the functionalities available in real-life devices.

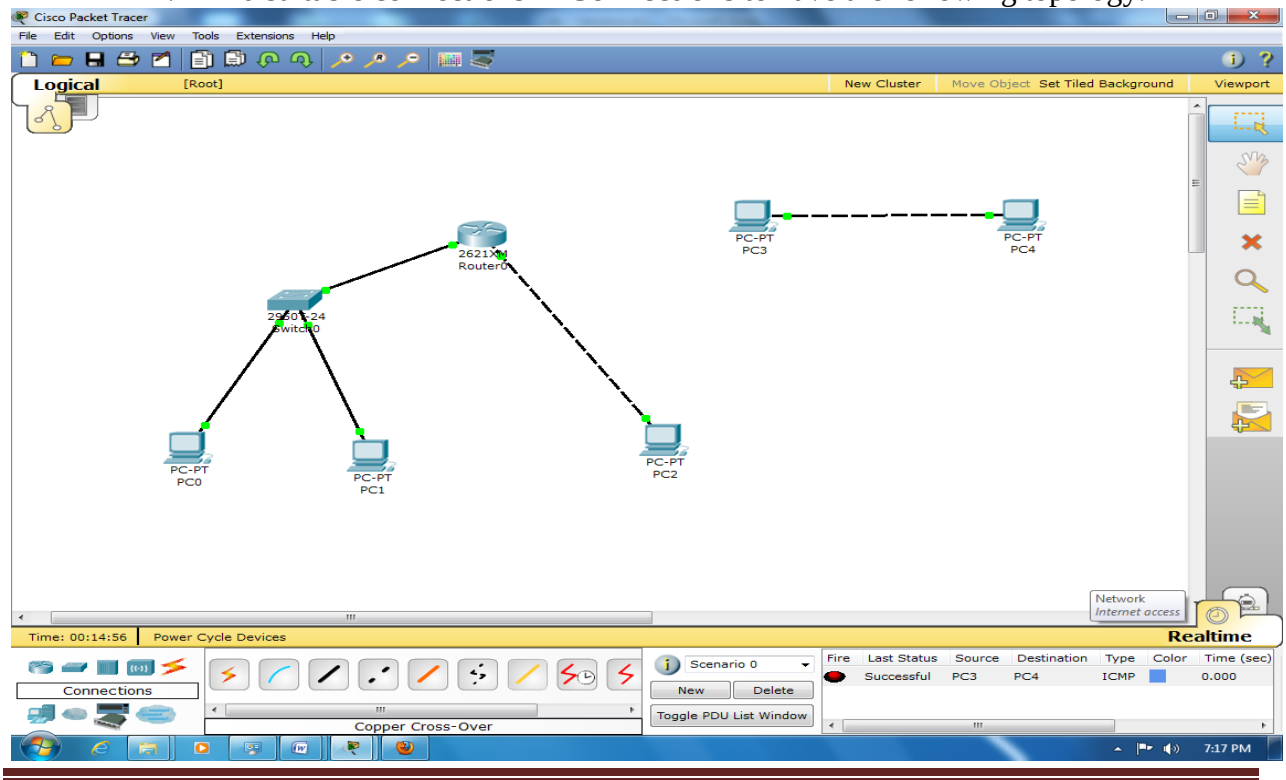
The purpose of simulator is to duplicate the software functionality of a device.

4. Procedure

1. Open Packet Tracer 5 from Desktop or Start Menu. The following window appears.



2. Click on **Routers** in lower left part, click on **2621XM** and then again click in the main window. The router will appear in the main window.
3. Do the same process to have switch **2950T (in Switches)** and five PCs **Generic (in End Devices)** in the main window.
4. Find suitable connections in **Connections** to have the following topology.



5. Double-click on the router and goto **Config** tab. Choose the **FastEthernet 0/0**, check the **On** box and enter **192.168.1.1** as the IP address and **255.255.255.0** as subnet mask. Then choose **FastEthernet 0/1**, check the **On** box an enter **192.168.3.1** as the IP address and **255.255.255.0** as subnet mask.
6. Double-click on PC0 and goto **Dektop** tab. Click on **IP Configuration** and enter **192.168.1.2** as the IP address and **255.255.255.0** as subnet mask. **192.168.1.3** for PC1 and **192.168.3.2** for PC2. Enter any IP address for PC3 and PC4 (in same network).
7. To check communication, goto **Desktop** tab of any PC, click on the **Command Prompt** and use any networking command (ping,tracert etc).
8. You can also use the closed envelope with a plus sign (**Add Simple PDU**) in the right menu of the Packet Tracer window. Click on it, then the two nodes to be checked. **This a much better way. To check it benefits, goto Simulations mode using Shift +S**

or by clicking 

in the lower right corner of window.

International Islamic University, Islamabad
Computer Networks Lab

LAB WORKSHEET (Lab # 3)

Q.1 What is difference between IP address & MAC address?

_____
_____
_____
_____
_____

Q.2 Identify the differences between Network Emulator and Simulator.

_____
_____
_____
_____
_____

Q.3 Can Layer2 Switch be used to connect two LANs? Give reasons for your answer.

_____
_____
_____
_____
_____

Q.4 What are the advantages of using **Add Simple PDU** in place of ping from C**ommand Prompt** in Packet Tracer?

_____
_____
_____
_____
_____

International Islamic University, Islamabad
Computer Networks LAB

EXPERIMENT # 04: Basic Switch Configuration

Name of Student: ……..

Roll No.: ……

Date of Experiment: ……..

Report submitted on: ……..

Marks obtained: ……

Remarks: ……

Instructor's Signature: ……...

Basic Switch Configuration

1. Objective

This lab exercise is designed for understanding and using basic configuration commands on a Cisco Switch interacting through Cisco IOS.

2. Resources Required

- Computer
- Packet Tracer (version 5 or higher)

3. Introduction

This lab introduces Cisco IOS (Internetwork Operating System) which is the proprietary CLI (command line interface) based software empowering nearly all the Cisco devices. IOS is a package of routing, switching, internetworking and telecommunications functions tightly integrated with a multitasking operating system.

The loading process is Cisco IOS is as follows:

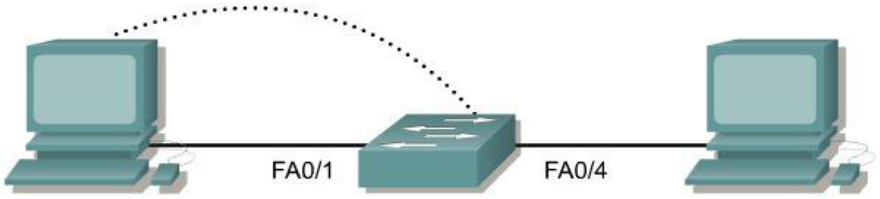
a) Bootstrap is loaded from ROM which starts up POST (Power On Self Test).
b) Valid image file is searched from flash memory, if found is loaded into the RAM, otherwise ROMMON is loaded from ROM.
c) Valid startup-config is searched from NV-RAM, if found is loaded into the RAM as running-config, otherwise the device just starts without any previous configurations.

From this we conclude that Cisco devices have 4 types of memories present:

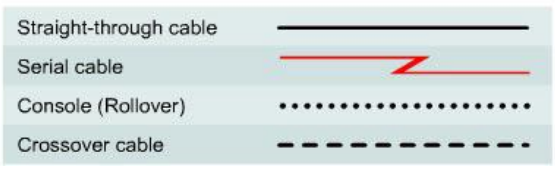
a) ROM b) Flash c) NV-RAM d) RAM

4. Procedure

1. Open Packet Tracer 5 and setup a network similar to the following network. Use Cisco 2950T switch.



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords
Switch 1	AL Switch	class	cisco



2. Double click the switch and goto CLI tab. Follow the steps below to complete the lab. You can do the same using a PC if you use a **console (one side is RS 232, other is RJ45—blue colored in Packet Tracer)** cable for connection between PC and Switch. Goto PC's desktop then Terminal (equivalent of HyperTerminal), accept the default settings and login to the Switch.

Step 1 Enter privileged mode

a. Privileged mode gives access to all the switch commands. Many of the privileged commands configure operating parameters. Therefore, privileged access should be password-protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes is gained.

Switch>**enable**
Switch#
b. Notice the prompt changed in the configuration to reflect privileged EXEC mode.

Step 2 Examine the current switch configuration

a. Examine the following current running configuration file:
Switch#**show running-config**

b. How many Ethernet or Fast Ethernet interfaces does the switch have? _____

c. What is the range of values shown for the VTY lines? _____

d. Examine the current contents of NVRAM as follows:
Switch#**show startup-config**
%% Non-volatile configuration memory is not present

e. Why does the switch give this response?
_____

Step 3 Assign a name to the switch

a. Enter **enable** and then the configuration mode. The configuration mode allows the management of the switch. Enter **ALSwitch**, the name this switch will be referred to in the following:

Switch#**configure terminal**
Enter the configuration commands, one for each line. End by pressing **Ctrl-Z**.
Switch(config)#**hostname ALSwitch**
ALSwitch(config)#**exit**

b. Notice the prompt changed in the configuration to reflect its new name. Type **exit** or press **Ctrl-Z** to go back into privileged mode.

Step 4 Examine the current running configuration

a. Examine the current configuration that follows to verify that there is no configuration except for the hostname:
ALSwitch#**show running-config**

b. Are there any passwords set on the lines? _____

c. What does the configuration show as the hostname of this switch? _____

Step 5 Set the access passwords

Enter config-line mode for the console. Set the password on this line as **cisco** for login. Configure the vty lines 0 to 15 with the password cisco as follows:

ALSwitch#**configure terminal**
Enter the configuration commands, one for each line. End by pressing **Ctrl-Z**.
ALSwitch(config)#**line con 0**
ALSwitch(config-line)#**password cisco**
ALSwitch(config-line)#**login**
ALSwitch(config-line)#**line vty 0 15**
ALSwitch(config-line)#**password cisco**
ALSwitch(config-line)#**login**
ALSwitch(config-line)#**exit**

Step 6 Set the command mode passwords

a. Set the **enable password** to cisco and the **enable secret password** to **class** as follows:
ALSwitch(config)#**enable password cisco**
ALSwitch(config)#**enable secret class**

b. Which password takes precedence, the enable password or enable secret password? _____

Step 7 Configure the layer 3 access to the switch

a. Set the IP address of the switch to 192.168.1.2 with a subnet mask of 255.255.255.0 as follows:
Note: This is done on the internal virtual interface VLAN 1.

ALSwitch(config)#**interface VLAN 1**
ALSwitch(config-if)#**ip address 192.168.1.2 255.255.255.0**
ALSwitch(config-if)#**exit**
b. Set the default gateway for the switch and the default management VLAN to 192.168.1.1 as follows:
ALSwitch(config)#**ip default-gateway 192.168.1.1**
ALSwitch(config)#**exit**

Step 8 Verify the management LANs settings

a. Verify the interface settings on VLAN 1 as follows:

ALSwitch#**show interface VLAN 1**

b. What is the bandwidth on this interface? _____

c. What are the VLAN states: VLAN1 is _____, Line protocol is _____

d. Enable the virtual interface using the **no shutdown** command

ALSwitch(config)#**interface VLAN 1**
ALSwitch(config-if)#**no shutdown**
ALSwitch(config-if)#**exit**

e. What is the queuing strategy? _____

Step 9 Save the configuration

a. The basic configuration of the switch has just been completed. Back up the running configuration file to NVRAM as follows:
Note: This will ensure that the changes made will not be lost if the system is rebooted or loses power.

ALSwitch#**copy running-config startup-config**
Destination filename [startup-config]?[**Enter**]
Building configuration...
[OK]
ALSwitch#

Step 10 Examine the startup configuration file

a. To see the configuration that is stored in NVRAM, type **show startup-config** from the privileged EXEC (enable mode)

ALSwitch#**show startup-config**

b. What is displayed? _____

c. Are all the changes that were entered recorded in the file? _____

Step 11 Configure the hosts attached to the switch

Configure the hosts to use the same IP subnet for the address, mask, and default gateway as on the switch.

Step 12 Verify connectivity

a. To verify that hosts and switch are correctly configured, ping the switch IP address from the hosts.
b. Were the pings successful? _____
c. If the answer is no, troubleshoot the hosts and switch configurations.

Step 13 Record the MAC addresses of the host

a. Determine and record the layer 2 addresses of the PC network interface cards. Check by using command **ipconfig /all** in command prompt of the Packet Tracer PC (in Desktop tab).

b. PC1: _____

c. PC4: _____

Step 14 Determine the MAC addresses that the switch has learned

a. To determine the what MAC addresses the switch has learned use the **show mac-address-table** command as follows at the privileged EXEC mode prompt:
ALSwitch#**show mac-address-table**

b. How many dynamic addresses are there? _____

c. How many total MAC addresses are there? _____

d. How many addresses have been user defined? _____

e. Do the MAC addresses match the host MAC addresses? _____

Step 15 Determine the show MAC table options

a. To determine the options the **show mac-address-table** command has use the **?** option as follows:

ALSwitch#**show mac-address-table ?**

b. How many options are available for the **show mac-address-table** command? _____

c. Show only the mac-address-tables that were learned dynamically.

d. How many are there? _____

Step 16 Clear the MAC address table

To remove the existing MAC addresses use the **clear mac-address-table** command from the privileged EXEC mode prompt as follows:
ALSwitch#**clear mac-address-table dynamic**

Step 17 Verify the results

a. Verify that the **mac-address-table** was cleared as follows:

ALSwitch#**show mac-address-table**

b. How many total MAC addresses are there now? _____

c. Why are there so many? _____

d. How many dynamic addresses are there? _____

Step 18 Determine the clear MAC table options

a. To determine the options available use the command **clear mac-address-table ?** at the privileged EXEC mode prompt as follows:

ALSwitch#**clear mac-address-table ?**

b. How many options are there? _____

c. In what circumstances would these options be used? _____

Step 19 Examine the MAC table again

a. Look at the MAC address table again using the **show mac-address-table** command at the privileged EXEC mode prompt as follows:

ALSwitch#**show mac-address-table**

b. How many dynamic addresses are there? _____

c. Why did this change from the last display? _____

d. The table has not changed yet, ping the switch IP address from the hosts two times each and repeat Step 19.

Step 20 Exit the switch

Leave the switch welcome screen by typing **exit** as follows:

ALSwitch#**exit**

International Islamic University, Islamabad
Computer Networks Lab

LAB WORKSHEET (Lab # 4)

Q.1 What is Cisco IOS and what are its functions?

_____
_____
_____
_____
_____

Q.2 Identify the differences between **line** and **interface** of a Cisco device.

_____
_____
_____
_____
_____

Q.3 If switch doesn't know the destination address, what will it do? If it does then what action is taken?

_____
_____
_____
_____
_____

Q.4 What are the differences between **running-config** and **startup-config**?

_____
_____
_____
_____
_____

International Islamic University, Islamabad
Computer Networks LAB

EXPERIMENT # 05: Configuring Port Security

Name of Student: ……..

Roll No.: ……

Date of Experiment: ……..

Report submitted on: ……..

Marks obtained: ……

Remarks: ……

Instructor's Signature: ……...

Configuring Port Security

1. Objective

This lab exercise is designed for modifying MAC Address Table and configuring port security.

2. Resources Required

- Computer
- Packet Tracer (version 5 or higher)

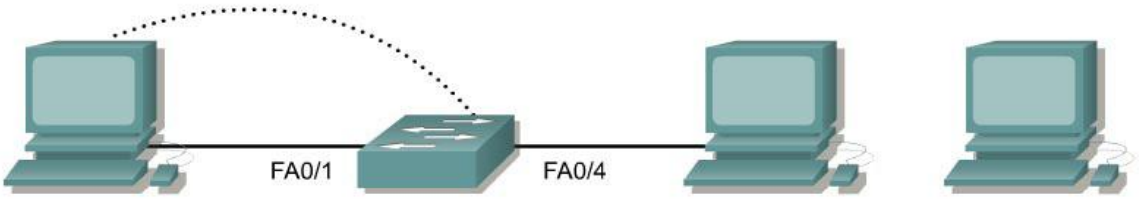
3. Introduction

This lab introduces Cisco IOS (Internetwork Operating System) which is the proprietary CLI (command line interface) based software empowering nearly all the Cisco devices. IOS is a package of routing, switching, internetworking and telecommunications functions tightly integrated with a multitasking operating system.

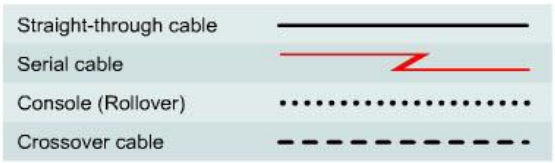
Cisco Switches also have the ability to prevent unauthorized access to a network on the basis of MAC addresses. The process of securing ports is discussed in this lab.

4. Procedure

1. Open Packet Tracer 5 and setup a network similar to the following network. Use Cisco 2950T switch.



Switch Designation	Switch Name	Enable Secret Password	Enable,VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	AL Switch	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0



2. Double click the switch and goto CLI tab. Follow the steps below to complete the lab. You can do the same using a PC if you use a **console (one side is RS 232, other is RJ45—blue colored in Packet Tracer)** cable for connection between PC and Switch. Goto PC's desktop then Terminal (equivalent of HyperTerminal), accept the default settings and login to the Switch.

Step 1 Configure the switch

Configure the hostname, access and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switch

a. Configure the hosts to use the same IP subnet for the address, mask, and default gateway as on the switch.
b. There is a third host needed for this lab. It needs to be configured with the address 192.168.1.7. The subnet mask is 255.255.255.0 and the default gateway is 192.168.1.1.

Note: Do not connect this PC to the switch yet.

Step 3 Verify connectivity

a. To verify that hosts and switch are correctly configured, ping the switch IP address from the hosts.
b. Were the pings successful? _____
c. If the answer is no, troubleshoot the hosts and switch configurations.

Step 4 Record the host MAC addresses

a. Determine and record the layer 2 addresses of the PC network interface cards. Check by using command **ipconfig /all** in command prompt of the Packet Tracer PC (in Desktop tab).

b.PC1_____

c.PC2_____

Step 5 Determine what MAC addresses that the switch has learned

a. Determine what MAC addresses the switch has learned by using the **show mac-addresstable** command, as follows, at the privileged exec mode prompt:

ALSwitch#**show mac-address-table**

b. How many dynamic addresses are there? _____

c. How many total MAC addresses are there? _____

d. Do the MAC addresses match the host MAC addresses? _____

Step 6 Determine the show MAC table options

a. Enter the following to determine the options the **mac-address-table** command has use the **?** option:

ALSwitch(config)#**mac-address-table ?**

Step 7 Setup a static MAC address

Setup a static MAC address on FastEthernet interface 0/4 as follows:

Note: Use the address that was recorded for PC4 in Step 4. The MAC address 00e0.2917.1884 is used in the example statement only.

ALSwitch(config)#**mac-address-table static 00e0.2917.1884 vlan 1 interface fastethernet 0/4**

Step 8 Verify the results

a. Enter the following to verify the **mac–address table** entries.

ALSwitch#**show mac-address-table**

b. How many total MAC addresses are there now? _____

Step 9 Delete the static MAC address

Delete the static MAC address setup on FastEthernet interface 0/4 as follows:

ALSwitch(config)#**no mac-address-table static 00e0.2917.1884 vlan 1 interface fastethernet 0/4**

Step 10 List port security options

a. Determine the options for setting port security on interface FastEthernet 0/4.
Type **port security ?** from the interface configuration prompt for FastEthernet port 0/4 as follows:

ALSwitch(config)#**interface fastethernet 0/4**
ALSwitch(config-if)#**switchport port-security ?**
aging Port-security aging commands
mac-address Secure mac address
maximum Max secure addresses
violation Security Violation Mode
<cr>

b. To allow the switchport FastEthernet 0/4 to accept only one device enter **port security** as follows:

ALSwitch(config-if)#**switchport mode access**
ALSwitch(config-if)#**switchport port-security**
ALSwitch(config-if)#**switchport port-security mac-address sticky**

Step 11 Verify the results

a. Enter the following to verify the mac –address table entries:

ALSwitch#**show mac-address-table**

b. How are the address types listed for the two MAC addresses? _____

c. Show port security settings

ALSwitch#**show port-security**

Step 12 Show the running configuration file

a. Are there statements that directly reflect the security implementation in the listing of the running configuration?

_____

b. What do those statements mean?

_____

Step 13 Limit the number of hosts per port

a. On interface FastEthernet 0/4 set the port security maximum MAC count to 1 as follows:

ALSwitch(config)#**interface fastethernet 0/4**
ALSwitch(config-if)#**switchport port-security maximum 1**

Step 14 Configure the port to shut down if there is a security violation

a. It has been decided that in the event of a security violation the interface should be shut down. Enter the following to make the port security action to shutdown:

ALSwitch(config-if)#**switchport port-security violation shutdown**

b. What other action options are available with port security? _____

c. Disconnect the PC attached to FastEthernet 0/4. Connect to the port on the PC that has been given the IP address 192.168.1.7. This PC has not yet been attached to the switch. It may be necessary to ping the switch address 192.168.1.2 to generate some traffic.

d. Record any observations.

_____
_____

Step 15 Show port 0/4 configuration information

a. To see the configuration information for just FastEthernet port 0/4, type **show interface fastethernet 0/4, as follows,** at the privileged exec mode prompt:

ALSwitch#**show interface fastethernet 0/4**

b. What is the state of this interface?

FastEthernet0/4 is _____, line protocol is _____

Step 15 Reactivate the port

If a security violation occurs and the port is shut down, use firstly **shutdown** then **no shutdown** command in the **interface** mode to reactivate it.

Step 16 Move host

a. Take the PC that had previously been connected to Fast Ethernet 0/4 and reconnect it to Fast Ethernet 0/8. The PC has been moved to a new location. This could be to another VLAN but in this instance all switch ports are in VLAN 1 and network 192.168.1.0.
b. From this PC on Fast Ethernet 0/8, **ping 192.168.1.2 –n 50**

c. Was the ping successful? _____

d. Why or why not? _____

e. Enter the following to show the **mac-address-table**.

ALSwitch#**show mac-address-table**

f. Record observations about the show output.

_____
_____

Step 17 Clear MAC table

a. Enter the following to clear the **mac-address-table**:
Note: This will unlock the MAC addresses from security and allow a new address to be registered.

ALSwitch#**clear mac-address-table dynamic**

b. From the PC on the Fast Ethernet 0/8, **ping 192.168.1.2 –n 50**.

c. Was the ping successful? _____

d. If not troubleshoot as necessary.

Step 18 Change security settings

a. Enter the following to show the **mac-address-table**:

ALSwitch#**show mac-address-table**

b. Notice that Fast Ethernet 0/4 is secure. However, that security should be applied to the machine on port 0/8, as this is the machine that was moved from port 0/4. Remove port security from interface Fast Ethernet 0/4 as follows:

ALSwitch(config)#**interface fastethernet 0/4**
ALSwitch(config-if)#**no switchport port-security**
ALSwitch(config-if)#**no switchport port-security mac-address sticky**
ALSwitch(config-if)#**no switchport port-security mac-address sticky 0008.744d.8ee2**
ALSwitch(config-if)#**shutdown**
ALSwitch(config-if)#**no shutdown**

c. Apply security settings to FastEthernet 0/8 using step 10-14.

Step 19 Exit the switch

Type **exit**, as follows, to leave the switch welcome screen:
Switch#**exit**
Once the steps are completed, logoff by typing **exit**, and turn all the devices off. Then remove and store the cables and adapter.

International Islamic University, Islamabad
Computer Networks Lab

LAB WORKSHEET (Lab # 5)

Q.1 Write any two differences between MAC address and IP address.

_____
_____
_____
_____
_____

Q.2 Identify the differences between **protect** and **restrict** mode of port-security violation.

_____
_____
_____
_____
_____

Q.3 Can port security be done on the basis of IP addresses? Give reasons.

_____
_____
_____
_____
_____

Q.4 Identify the difference between **static** and **dynamic** MAC addresses.

_____
_____
_____
_____
_____

International Islamic University, Islamabad
Computer Networks LAB

EXPERIMENT # 06: VLANs & Inter-VLAN Routing

Name of Student: ……..

Roll No.: ……

Date of Experiment: ……..

Report submitted on: ……..

Marks obtained: ……

Remarks: ……

Instructor's Signature: ……...

VLANs & Inter-VLAN Routing

1. Objective

This lab exercise is designed for understanding VLAN creation and Inter-VLAN routing.

2. Resources Required

- Computer
- Packet Tracer (version 5 or higher)

3. Introduction

This lab introduces Cisco IOS (Internetwork Operating System) which is the proprietary CLI (command line interface) based software empowering nearly all the Cisco devices. IOS is a package of routing, switching, internetworking and telecommunications functions tightly integrated with a multitasking operating system.

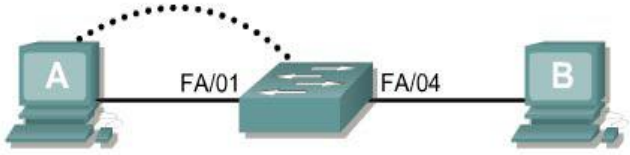
A **broadcast domain** is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer. A simple LAN is a single broadcast domain. To reduce the numbers of devices in a broadcast domain, we have to divide broadcast domain. VLAN serve for this purpose. The whole idea of VLAN technology is to divide LAN into logical, instead of physical, segments. VLANs are created at the Data Link layer so switches apply them to a network. Computers in different VLANs can't communicate with each other so Inter-VLAN routing is required for this purpose.

VLANs create broadcast domains.

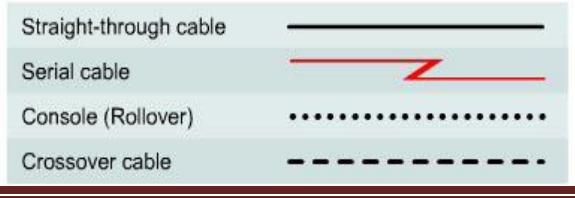
4. Procedure

4.1 Configuring Static VLANs

1. Open Packet Tracer 5 and setup a network similar to the following network. Use Cisco 2950T switch.



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	Switch_A	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0



2. Double click the switch and goto CLI tab. Follow the steps below to complete the lab. You can do the same using a PC if you use a **console (one side is RS 232, other is RJ45—blue colored in Packet Tracer)** cable for connection between PC and Switch. Goto PC's desktop then Terminal (equivalent of HyperTerminal), accept the default settings and login to the Switch.

When managing a switch, the Management Domain is always VLAN 1. The Network Administrator's workstation must have access to a port in the VLAN 1 Management Domain. All ports are assigned to VLAN 1 by default.

Step 1 Configure the switch

Configure the hostname, access and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switch

Configure the host to use the same subnet for the address, mask, and default gateway as on the switch.

Step 3 Verify connectivity

a. To verify that the host and switch are correctly configured, ping the switch from the host.
b. Was the ping successful? _____
c. If the answer is no, troubleshoot the host and switch configurations.

Step 4 Show the IOS version

a. It is very important to know the version of the operating system. Differences between versions may change how commands are entered. Type the **show version** command at the user EXEC or privileged EXEC mode prompt as follows:

Switch_A#**show version**

b. What version of the switch IOS is displayed? _____

c. Does this switch have standard edition or Enterprise edition software? _____

d. What is the Firmware version of the switch? _____

Step 5 Display the VLAN interface information

a. On Switch_A, type the command **show vlan** at the privileged EXEC prompt as follows:

Switch_A#**show vlan**

b. Which ports belong to the default VLAN? _____

c. How many VLANs are set up by default on the switch? _____

d. What does the VLAN 1003 represent? _____

e. How many ports are in the 1003 VLAN? _____

Step 6 Create and name two VLANs

Enter the following commands to create and name two VLANs:

Switch_A#**vlan database**
Switch_A(vlan)#**vlan 2 name VLAN2**
Switch_A(vlan)#**vlan 3 name VLAN3**
Switch_A(vlan)#**exit**

Another (newer) way of doing the same is by entering the following commands:
Switch_A(config)#**vlan 10**
Switch_A(config-vlan)#**name Sales**
Switch_A(config-vlan)#**vlan 20**
Switch_A(config-vlan)# **name Support**

Step 7 Display the VLAN interface information

a. On Switch_A, type the command **show vlan** at the privileged EXEC prompt as follows:

Switch_A#**show vlan**

b. Are there new VLANs in the listing? _____

c. Do they have any ports assigned to them yet? _____

Step 8 Assign ports to VLAN 2

Assigning ports to VLANs must be done from the interface mode. Enter the following commands to add port 2 to VLAN 2:

Switch_A#**configure terminal**
Switch_A(config)#**interface fastethernet 0/2**
Switch_A(config-if)#**switchport mode access**
Switch_A(config-if)#**switchport access vlan 2**
Switch_A(config-if)#**end**

Step 9 Display the VLAN interface information

a. On Switch_A, type the command **show vlan** at the privileged EXEC prompt as follows:

Switch_A#**show vlan**

b. Is port 2 assigned to VLAN 2? _____

c. Is the port still listed in the default VLAN? _____

Step 10 Assign a port to VLAN 3

Assigning ports to VLANs must be done from the interface mode. Enter the following commands to add port 3 to VLAN3

Switch_A#**configure terminal**
Switch_A(config)#**interface fastethernet 0/3**
Switch_A(config-if)#**switchport mode access**
Switch_A(config-if)#**switchport access vlan 3**
Switch_A(config-if)#**end**

Step 11 Look at the VLAN interface information

a. On Switch_A, type the command **show vlan** at the privileged EXEC prompt as follows:

Switch_A#**show vlan**

b. Is port 3 assigned to VLAN 3? _____

c. Is the port still listed in the default VLAN? _____

Step 12 Look at only VLAN2 information

a. Instead of displaying all of the VLANs type the **show vlan id 2** command at the privileged EXEC mode prompt as follows:

Switch_A#**show vlan id 2**

b. Does this command supply any more information than the show VLAN command? _____

Step 13 Look at only VLAN2 information with a different command

a. Instead of displaying all of the VLANs type the **show vlan name VLAN2** command at the privileged EXEC mode prompt.

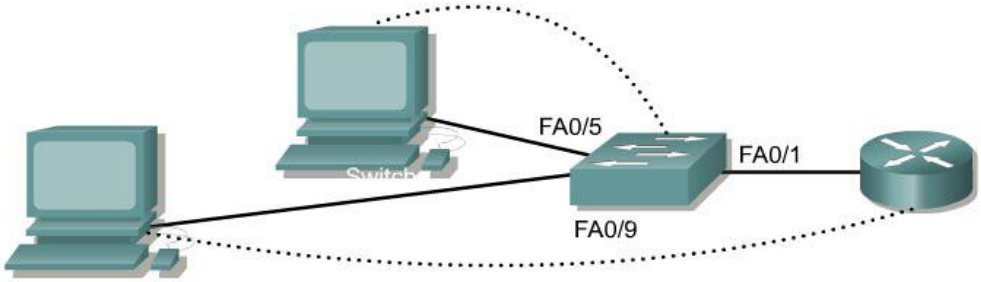
Switch_A#**show vlan name VLAN2**

b. Does this command supply any more information than the show VLAN command? _____

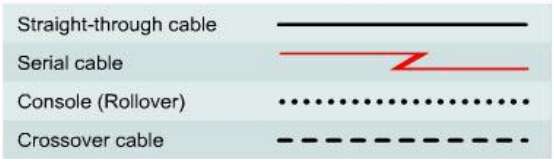
Note:
This configuration is much secure as VLANs can't communicate with each other but if it is a requirement, we can enable Inter-VLAN routing which is discussed in next section.

4.2 Configuring Inter-VLAN Routing

1. Open Packet Tracer 5 and setup a network similar to the following network. Use Cisco 2950T switch & Cisco 2621XM router.



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords	VLAN 1 IP Address	Subnet Mask	VLAN Names and Numbers	Switch Port Assignments
Switch 1	Switch A	class	cisco	192.168.1.2	255.255.255.0	VLAN 1 Native VLAN 10 Sales VLAN 20 Support	fa0/1 - 0/4 fa0/5 - 0/8 fa0/9 - 0/12



2. Double click the switch and goto CLI tab. Follow the steps below to complete the lab. You can do the same using a PC if you use a **console (one side is RS 232, other is RJ45—blue colored in Packet Tracer)** cable for connection between PC and Switch. Goto PC's desktop then Terminal (equivalent of HyperTerminal), accept the default settings and login to the Switch.

This part also involves a router (Layer 3 device) but no major configurations are being done on it. It also uses **trunk link** whose main purpose is multiplexing.

Step 1 Configure the switch

Configure the hostname, access, and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switch

Configure the hosts using the following information.

a. For the host in port 0/5:
IP address 192.168.5.2
Subnet mask 255.255.255.0
Default gateway 192.168.5.1

b. For the host in port 0/9:
IP address 192.168.7.2
Subnet mask 255.255.255.0
Default gateway 192.168.7.1

Step 3 Verify connectivity

a. To verify that the host and switch are correctly configured, ping the switch from the hosts.

b. Ping the switch IP address from the hosts.

c. Were the pings successful? _____

d. Why or why not? _____

Step 4 Create and name two VLANs

Enter the following commands to create and name two VLANs:

Switch_A#**vlan database**
Switch_A(vlan)#**vlan 10 name Sales**
Switch_A(vlan)#**vlan 20 name Support**
Switch_A(vlan)#**exit**

Another (newer) way of doing the same is by entering the following commands:
Switch_A(config)#**vlan 10**
Switch_A(config-vlan)#**name Sales**
Switch_A(config-vlan)#**vlan 20**
Switch_A(config-vlan)# **name Support**

Step 5 Configure VTP protocol

Assigning ports to VLANs must be done from the interface mode. Enter the following commands to add ports 0/5 to 0/8 to VLAN 10:

Switch_A#**configure terminal**
Switch_A(config)#**interface fastethernet 0/5**
Switch_A(config-if)#**switchport mode access**
Switch_A(config-if)#**switchport access vlan 10**
Switch_A(config-if)#**interface fastethernet 0/6**
Switch_A(config-if)#**switchport mode access**
Switch_A(config-if)#**switchport access vlan 10**
Switch_A(config-if)#**interface fastethernet 0/7**
Switch_A(config-if)#**switchport mode access**
Switch_A(config-if)#**switchport access vlan 10**
Switch_A(config-if)#**interface fastethernet 0/8**
Switch_A(config-if)#**switchport mode access**
Switch_A(config-if)#**switchport access vlan 10**
Switch_A(config-if)#**end**

Step 6 Assign ports to VLAN 20

Enter the following commands to add ports 0/9 to 0/12 to VLAN 20:

Switch_A#**configure terminal**
Switch_A(config)#**interface fastethernet 0/9**
Switch_A(config-if)#**switchport mode access**
Switch_A(config-if)#**switchport access vlan 20**
Switch_A(config-if)#**interface fastethernet 0/10**
Switch_A(config-if)#**switchport mode access**
Switch_A(config-if)#**switchport access vlan 20**
Switch_A(config-if)#**interface fastethernet 0/11**
Switch_A(config-if)#**switchport mode acce**ss
Switch_A(config-if)#**switchport access vlan 20**
Switch_A(config-if)#**interface fastethernet0/12**
Switch_A(config-if)#**switchport mode access**
Switch_A(config-if)#**switchport access vlan 20**
Switch_A(config-if)#**end**

Step 7 Display the VLAN interface information

a. On Switch_A, type the command **show vlan** at the privileged EXEC prompt as follows:

Switch_A#**show vlan**

b. Are ports assigned correctly? _____

Step 8 Create the trunk

On Switch_A, type the following commands at the Fast Ethernet 0/1 interface command prompt.

Switch_A(config)#**interface fastethernet0/1**
Switch_A(config-if)#**switchport mode trunk**
Switch_A(config-if)#**end**

Step 9 Configure the router

a. Configure the router with the following data. Note that, in order to support trunking and inter-VLAN routing, the router must have a Fast Ethernet interface.

Hostname is **Router_A**

Console, VTY, and enable passwords are **cisco**.

Enable secret password is **class**.

b. Then configure the Fast Ethernet interface using the following commands:

Router_A(config)#**interface fastethernet 0/0**
Router_A(config-if)#**no shutdown**
Router_A(config-if)#**interface fastethernet 0/0.1**
Router_A(config-subif)#**encapsulation dot1q 1**
Router_A(config-subif)#**ip address 192.168.1.1 255.255.255.0**
Router_A(config-if)#**interface fastethernet 0/0.2**
Router_A(config-subif)#**encapsulation dot1q 10**
Router_A(config-subif)#**ip address 192.168.5.1 255.255.255.0**
Router_A(config-if)#**interface fastethernet 0/0.3**
Router_A(config-subif)#**encapsulation dot1q 20**
Router_A(config-subif)#**ip address 192.168.7.1 255.255.255.0**
Router_A(config-subif)#**end**

Step 10 Display the router routing table

a. Type **show ip route** at the privileged EXEC mode prompt.

b. Are there entries in the routing table? _____

c. What interface are they all pointing to? _____

d. Why is there not a need to run a routing protocol? _____

Step 11 Test the VLANS and the trunk

Ping from the host in Switch_A port 0/9 to the host in port 0/5.

a. Was the ping successful? _____
b. Why? _____

Ping from the host in Switch_A port 0/5 to the switch IP 192.168.1.2.

c. Was the ping successful? _____

Step 12 Move the hosts

a. Move the hosts to other VLANs and try pinging the management VLAN 1.
b. Note the results of the pinging.

_____
_____

Step 13 Exit the switch

Type **exit**, as follows, to leave the switch welcome screen:
Switch#**exit**
Once the steps are completed, logoff by typing **exit**, and turn all the devices off. Then remove and store the cables and adapter.

International Islamic University, Islamabad
Computer Networks Lab

LAB WORKSHEET (Lab # 6)

Q.1 What is VLAN and what is its purpose?

Q.2 Identify the advantages **VLAN** has over **physical LAN**.

Q.3 What is **broadcast domain?**

Q.4 Identify the difference between **access** and **trunk** link.

International Islamic University, Islamabad
Computer Networks LAB

EXPERIMENT # 07: The Cisco Router User Interface

Name of Student: ……..

Roll No.: ……

Date of Experiment: ……..

Report submitted on: ……..

Marks obtained: ……

Remarks: ……

Instructor's Signature: ……...

The Cisco Router User Interface

1. Objective

This lab exercise is designed for understanding cisco router user interface before moving on to advanced configurations. Use the commands mentioned in the following sections on CLI mode of cisco router 2621XM in Packet Tracer.

2. Resources Required

- Computer
- Packet Tracer (version 5 or higher)

3. Introduction

The Cisco IOS was created to deliver network services and enable networked applications. It runs on most Cisco routers and, on an ever-increasing number of Cisco Catalyst switches, such as the Catalyst 2950. Some of the important things that the Cisco router IOS software is responsible for include

- 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

You can access the Cisco IOS through the console port of a router, from a modem into the auxiliary (or Aux) port, or even through Telnet. Access to the IOS command line is called an EXEC session.

Remember: Even though Cisco switches & routers share the same IOS (Router's IOS is more advanced due to layer 3 operation), switch can be added to a network with little configurations or no configuration at all but you can't use a router in a network without configuring it first!

3.1 Connecting to a Cisco Router

You can connect to a Cisco router to configure it, verify its configuration, and check statistics. There are different ways to do this, but most often, the first place you would connect to is the console port. The console port is usually an RJ-45 (8-pin modular) connection located at the back of the router—by default, there's no password set.

You can also connect to a Cisco router through an auxiliary port —which is really the same thing as a console port, so it follows that you can use it as one. But this auxiliary port also allows you to configure modem commands so that a modem can be connected to the router. This is a cool feature—it lets you dial up a remote router and attach to the auxiliary port if the router is down and you need to configure it "out-of-band" (meaning "out-of-the-network"). "In-band" means the opposite—configuring the router through the network. The third way to connect to a Cisco router is in-band, through the program Telnet. Telnet is a terminal emulation program that acts as though it's a dumb terminal. You can use Telnet to connect to any active interface on a router, such as an Ethernet or serial port.

The loading process of router is same as of switch (Refer to Lab 4). Once the IOS is loaded, and up and running, a valid configuration will be loaded from NVRAM. If there isn't a configuration

in NVRAM, the router will go into setup mode —a step-by-step process to help you configure the router. **This doesn't happen in a switch.**

3.2 Logging into the Router

After the interface status messages appear and you press Enter, the Router> prompt will appear. This is called *user exec mode* (user mode) and it's mostly used to view statistics, but it's also a stepping-stone to logging into privileged mode. You can only view and change the configuration of a Cisco router in *privileged exec mode* (privileged mode), which you get into with the enable command. Here's how:

```
Router>
Router>enable
Router#
```

You now end up with a Router# prompt, which indicates that you're in *privileged mode*, where you can both view and change the router's configuration. You can go back from privileged mode into user mode by using the disable command, as seen here:

```
Router#disable
Router>
```

At this point, you can type **logout** to exit the console:

```
Router>logout
Router con0 is now available
Press RETURN to get started.
```

Or you could just type **logout** or **exit** from the privileged-mode prompt to log out:

```
Router>en
Router#logout
Router con0 is now available
Press RETURN to get started.
```

3.4 Overview of Router Modes

To configure from a CLI, you can make global changes to the router by typing **configure terminal** (or **config t** for short), which puts you in global configuration mode and changes what's known as the running-config. A global command (a command run from global config) is set only once and affects the entire router.

You can type **config** from the privileged-mode prompt and then just press Enter to take the default of terminal, as seen here:

```
Router#config
Configuring from terminal, memory, or network [terminal]? [Enter]
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

At this point, you make changes that affect the router as a whole (globally), hence the term global configuration mode.
To change the running-config—the current configuration running in dynamic RAM (DRAM)—you use the configure terminal. To change the startup-config—the configuration stored in NVRAM—you use the configure memory command (or config mem for short). If you want to change a router configuration stored on a TFTP host, you use the configure network command (or config net for short).

3.5 CLI Prompts

It's really important that you understand the different prompts you can find when configuring a router. Knowing these well will help you navigate and recognize where you are at any time within configuration mode. In this section, I'm going to demonstrate the prompts that are used on a Cisco router. (Always check your prompts before making any changes to a router's configuration!). These command prompts really are the ones you'll use most in real life.

3.5.1 Interfaces

To make changes to an interface, you use the interface command from global configuration mode:

```
Router(config)#interface ?
Ethernet            IEEE 802.3
FastEthernet        FastEthernet IEEE 802.3
[output cut]
Router(config)#interface fastethernet 0/0
Router(config-if)#
```

Did you notice that the prompt changed to Router(config-if)#? This tells you that you're in *interface configuration mode*. And wouldn't it be nice if the prompt also gave you an indication of what interface you were configuring? Well, at least for now we'll have to live without the prompt information, because it doesn't. One thing is for sure: You really have to pay attention when configuring a router!

3.5.2 Subinterfaces

Subinterfaces allow you to create logical interfaces within the router. The prompt then changes to Router(config-subif)#, as shown below:

```
Router(config)#int fastethernet0/0.?
<0-4294967295> FastEthernet interface number
Router(config)#int fastethernet0/0.1
Router(config-subif)#
```

3.5.3 Line Commands

To configure user-mode passwords, use the line command. The prompt then becomes Router(config-line)# as shown below:

Router#**config t**
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#**line ?**
<0-0> First Line number
aux Auxiliary line
console Primary terminal line
vty Virtual terminal

Router(config)#**line console 0**
Router(config-line)#

The line console 0 command is known as a major command (also called a *global command*), and any command typed from the (config-line) prompt is known as a subcommand.

3.5.4 Routing Protocol Configurations

To configure routing protocols such as RIP and IGRP, use the prompt (config-router)#:

Router#**config t**
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#**router rip**
Router(config-router)#

3.6 Editing and Help Features

You can use the Cisco advanced editing features to 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:

Router#**?**
Exec commands: *[output cut]*
access-enable Create a temporary Access-List entry
--More—

Plus, at this point you can press the spacebar to get another page of information, or you can press Enter to go one command at a time. You can also press Q (or any other key, for that matter) to quit and return to the prompt.
Here's a shortcut: To find commands that start with a certain letter, use the letter and the question mark with no space between them:

Router#**c?**
clear clock configure connect copy
Router#**c**
By typing **c?**, we received a response listing all the commands that start with *c*. Also notice that the Router# prompt reappears after the list of commands is displayed. This can be helpful when you have long commands and need the next possible command. It would be pretty lame if you had to retype the entire command every time you used a question mark!

To find the next command in a string, type the first command and then a question mark:

Router#**clock ?**
set Set the time and date
Router#**clock set ?**
hh:mm:ss Current Time
Router#**clock set 10:30:10 ?**
<1-31> Day of the month
MONTH Month of the year
Router#**clock set 10:30:10 28 ?**
MONTH Month of the year
Router#**clock set 10:30:10 28 august ?**
<1993-2035> Year
Router#**clock set 10:30:10 28 august 2003 ?**
<cr>
Router#

By typing the **clock ?** command, you'll get a list of the next possible parameters and what they do. Notice that you should just keep typing a command, a space, and then a question mark until <cr> (carriage return) is your only option.
If you're typing commands and receive the following:

Router#**clock set 10:30:10**
% Incomplete command.

you'll know that the command string isn't done yet. Just press the Up arrow key to redisplay the last command entered, then continue with the command by using your question mark.
And if you receive the following error:

Router(config)#**access-list 110 permit host 1.1.1.1**
^
% Invalid input detected at '^' marker.

you've entered a command incorrectly. See that little caret—the ^? It's a very helpful tool that marks the exact point where you blew it and entered the command wrong.
Now if you receive this error:

Router#**sh te**
% Ambiguous command: "sh te"

it means there are multiple commands that begin with the string you entered and it's not unique. Use the question mark to find the command you need:

Router#**sh te?**
tech-support template terminal

4. Router and Switch Administrative Functions

Even though this section isn't critical to making a router or switch work on a network, it's still really important; in it, I'm going to lead you through configuring commands that will help you administrate your network.

The administrative functions that you can configure on a router and switch are

- Hostnames
- Banners
- Password
- Interface descriptions

4.1 Hostnames

You can set the identity of the router with the hostname command. This is only locally significant, which means that it has no bearing on how the router performs name lookups or how the router works on the internetwork.

Here's an example:

```
Router#config t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#hostname Todd
Todd(config)#hostname Atlanta
Atlanta(config)#
```

Even though it's pretty tempting to configure the hostname after your own name, it's definitely a better idea to name the router something pertinent to the location. This is because giving it a hostname that's somehow relevant to where the device actually lives will make finding it a whole lot easier. And it also helps you confirm that you are, indeed, configuring the right device.

4.2 Banners

A *banner* is more than just a little cool—one very good reason for having a banner is to give any and all who dare attempt to telnet or dial into your internetwork a little security notice. And you can create a banner to give anyone who shows up on the router exactly the information you want them to have. Make sure you're familiar with these four available banner types: exec process creation banner, incoming terminal line banner, login banner, and message of the day banner (all illustrated in the code below):

```
Router(config)#banner ?
LINE c banner-text c, where 'c' is a delimiting
character
exec Set EXEC process creation banner
incoming Set incoming terminal line banner
login Set login banner
motd Set Message of the Day banner
```

Message of the day (MOTD) is the most extensively used banner. It gives a message to every person dialing into or connecting to the router via Telnet or auxiliary port, or even through a console port as seen here:

Router(config)#**banner motd ?**
LINE c banner-text c, where 'c' is a delimiting character
Router(config)#**banner motd #**
Enter TEXT message. End with the character '#'.
$ Acme.com network, then you must disconnect immediately.
#
Router(config)#^**Z**
Router#
00:25:12: %SYS-5-CONFIG_I: Configured from console by
console
Router#**exit**
Router con0 is now available
Press RETURN to get started.
If you are not authorized to be in Acme.com network, then
you must disconnect immediately.
Router>

The preceding MOTD banner essentially tells anyone connecting to the router that if they're not on the guest list, get lost! The part to understand is the delimiting character—the thing that's used to tell the router when the message is done. You can use any character you want for it, but (I hope this is obvious) you can't use the delimiting character in the message itself. Also, once the message is complete, press Enter, then the delimiting character, then Enter again. It'll still work if you don't do that, but if you have more than one banner, they'll be combined as one message and put on a single line.

For example, you can set a banner on one line as shown:

Router(config)#**banner motd x Unauthorized access prohibited! x**

This example will work just fine, but if you add another MOTD banner message they would end up on a single line.
Below are some details of the other banners I mentioned:

Exec banner You can configure a line-activation (exec) banner to be displayed when an EXEC process (such as a line-activation or incoming connection to a VTY line) is created. By simply starting a user exec session through a console port, you'll activate the exec banner.

Login banner You can configure a login banner to be displayed on all connected terminals.
This banner is displayed after the MOTD banner, but before the login prompts. The login banner can't be disabled on a per-line basis, so to globally disable it, you've got to delete it with the no banner login command.

4.3 Setting Passwords

There are five passwords used to secure your Cisco routers: console, auxiliary (not available in Packet Tracer), telnet (VTY), enable password, and enable secret. Just as you learned earlier, the first two passwords are used to set your enable password that's used to secure privileged mode. This will prompt a user for a password when the enable command is used. The other three are used to configure a password when user mode is accessed either through the console port, through the auxiliary port, or via Telnet.
Let's take a look at each of these now.

4.3.1 Enable Passwords

You set the enable passwords from global configuration mode like this:

Router(config)#**enable ?**
password Assign the privileged level password
secret Assign the privileged level secret

The following points describe the enable password parameters:

Password Sets the enable password on older, pre-10.3 systems, and isn't ever used if an enable secret is set.

Secret Is the newer, encrypted password that overrides the enable password if it's set.

Here's an example of setting the enable passwords:

Router(config)#**enable secret todd**
Router(config)#**enable password todd**
The enable password you have chosen is the same as your enable secret. This is not recommended. Re-enter the enable password.

If you try to set the enable secret and enable passwords the same, the router will give you a nice, polite warning to change the second password. If you don't have older legacy routers, don't even bother to use the enable password.
User-mode passwords are assigned by using the line command:

Router(config)#**line ?**
<0-70> First Line number
aux Auxiliary line
console Primary terminal line
vty Virtual terminal

Here are the lines to be concerned with:
console Sets a console user-mode password.
vty Sets a Telnet password on the router. If this password isn't set, then Telnet can't be used by default.

To configure the user-mode passwords, you configure the line you want and use either the login or no login command to tell the router to prompt for authentication. The next section will provide a line-by-line example of each line configuration. Cisco has begun this process of not letting you set the "login" command before a password is set on a line because if you set the login command under a line, and then don't set a password, the line won't be usable. And it will prompt for a password that doesn't exist. So this is a good thing— a feature, not a hassle!

4.3.2 Console Password

To set the console password, use the line console 0 command. But look at what happened when I tried to type line console 0 ? from the aux line configuration—I received an error.
You can still type line console 0 and it will accept it, but the help screens just don't work from that prompt. Type **exit** to get back one level and you'll find that your help screens now work. This is a "feature." Really.
Here's the example:

```
Router(config-line)#line console ?
% Unrecognized command
Router(config-line)#exit
Router(config)#line console ?
<0-0> First Line number
Router(config)#line console 0
Router(config-line)# password todd1
Router(config-line)# login
```

Since there's only one console port, I can only choose line console 0. You can set all your line passwords to the same password, but for security reasons, I'd recommend that you make them different.
There are a few other important commands to know for the console port. For one, the **exec-timeout 0 0** command sets the timeout for the console EXEC session to zero, which basically means to never time out. The default timeout is 10 minutes. (If you're feeling mischievous, try this on people at work: Set it to 0 1. That will make the console time out in 1 second! And to fix it, you have to continually press the Down arrow key while changing the timeout time with your free hand!). **logging synchronous** is a very cool command, and it should be a default command, but it's not. It stops annoying console messages from popping up and disrupting the input you're trying to type. The messages still pop up, but you are returned to your router prompt without your input interrupted. This makes your input messages oh-so-much easier to read. Here's an example of how to configure both commands:

```
Router(config)#line con 0
Router(config-line)#exec-timeout ?
<0-35791> Timeout in minutes
Router(config-line)#exec-timeout 0 ?
<0-2147483> Timeout in seconds
<cr>
Router(config-line)#exec-timeout 0 0
Router(config-line)#logging synchronous
```

4.3.3 Telnet Password

To set the user-mode password for Telnet access into the router, use the line vty command. Routers that aren't running the Enterprise edition of the Cisco IOS default to five VTY lines, 0 through 4. But if you have the Enterprise edition, you'll have significantly more. The best way to find out how many lines you have is to use that question mark:

```
Router(config-line)#line vty 0 ?
<1-15> Last Line Number
<cr>
Router(config-line)#line vty 0 4
Router(config-line)# password todd2
Router(config-line)# login
```

So what will happen if you try to telnet into a router that doesn't have a VTY password set? You'll receive an error stating that the connection is refused because, well, the password isn't set. So, if you telnet into a router and receive this message:

```
Router#telnet SFRouter
Trying SFRouter (10.0.0.1)...Open
Password required, but none set
[Connection to SFRouter closed by foreign host]
Router#
```

then the remote router (SFRouter in this example) does not have the VTY (telnet) password set. But you can get around this and tell the router to allow Telnet connections without a password by using the no login command:

```
Router(config-line)#line vty 0 4
Router(config-line)#no login
```

After your routers are configured with an IP address, you can use the Telnet program to configure and check your routers instead of having to use a console cable. You can use the Telnet program by typing **telnet** from any command prompt (DOS or Cisco).

If you can ping a router but are unable to telnet into it, the likely problem is that you didn't set the password on the VTY lines.

4.3.4 Encrypting Your Passwords

Because only the enable secret password is encrypted by default, you'll need to manually configure the user-mode and enable passwords for encryption.
Notice that you can see all the passwords except the enable secret when performing a show running-config on a router:

```
Router#sh running-config
[output cut]
!
enable secret 5 $1$rFbM$8.aXocHg6yHrM/zzeNkAT.
enable password todd1
!
[output cut]
line con 0
password todd1
login
line aux 0
password todd
login
line vty 0 4
password todd2
login
!
end
Router#
```

To manually encrypt your passwords, use the service password-encryption command.
Here's an example of how to do it:

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#service password-encryption
Router(config)#^Z
Router#sh run
Building configuration...
[output cut]
!
enable secret 5 $1$rFbM$8.aXocHg6yHrM/zzeNkAT.
enable password 7 0835434A0D
!
[output cut]
Router and Switch Administrative Functions 187
!
line con 0
password 7 111D160113
login
```

line aux 0
password 7 071B2E484A
login
line vty 0 4
password 7 0835434A0D
login
line vty 5 197
password 7 09463724B
login
!
end
Router#**config t**
Router(config)#**no service password-encryption**
Router(config)#^**Z**

There you have it! The passwords will now be encrypted. You just encrypt the passwords, perform a show run, and then turn off the command. You can see that the enable password and the line passwords are all encrypted.
If you set your passwords and then turn on the service password-encryption command, you've got to perform a show running-config before you turn off the encryption service, or your passwords will not be encrypted.
Here is an example of how you might set and encrypt your Telnet password:
1. Enter the mode to configure telnet access: **line vty 0 4**
2. Enable Telnet login: **login**
3. Set the password to cisco: **password cisco**
4. Return to global configuration mode: **exit**
5. Encrypt password in show run/start output: **service password-encryption**
This is a tad different from what I showed you in the Telnet and encryption sections earlier, but you should know this way as well. Here are the commands in order:

Router(config)#**line vty 0 4**
Router(config-line)#**login**
Router(config-line)#**password cisco**
Router(config)#**exit**
Router(config)#**service password-encryption**

4.4 Descriptions
Setting descriptions on an interface is helpful to the administrator and, like the hostname, only locally significant. The description command is a helpful one because you can, for instance, use it to keep track of circuit numbers.
Here's an example:

Atlanta(config)#**int e0**
Atlanta(config-if)#**description Sales Lan**
Atlanta(config-if)#**int s0**
Atlanta(config-if)#**desc Wan to Miami circuit:6fdda4321**

You can view the description of an interface either with the show running-config command or the show interface command:

Atlanta#**sh run**
[cut]
interface Ethernet0
description Sales Lan
ip address 172.16.10.30 255.255.255.0
no ip directed-broadcast
!
interface Serial0
description Wan to Miami circuit:6fdda4321
no ip address
no ip directed-broadcast
no ip mroute-cache
Atlanta#**sh int e0**
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 0010.7be8.25db (bia
0010.7be8.25db)
Description: Sales Lan
[output cut]
Atlanta#**sh int s0**
Serial0 is up, line protocol is up
Hardware is HD64570
Description: Wan to Miami circuit:6fdda4321
[output cut]

(All the outputs shown above are for example only so your outputs may not match!!)

International Islamic University, Islamabad
Computer Networks Lab

LAB WORKSHEET (Lab # 7)

Q.1 Identify different ways of connecting to the router for configuration.

Q.2 How would you differentiate between user & privileged mode?

Q.3 Which access passwords are not encrypted by default?

Q.4 What is the advantage of **logging synchronous** command?

International Islamic University, Islamabad
Computer Networks LAB

EXPERIMENT # 08: Configuring IP Routing

Name of Student: ……..

Roll No.: ……

Date of Experiment: ……..

Report submitted on: ……..

Marks obtained: ……

Remarks: ……

Instructor's Signature: ……...

Configuring IP Routing

1. Objective

This lab exercise is designed to understand routing and procedure to setup static routes on routers.

2. Resources Required

- Computer
- Packet Tracer (version 5 or higher)

3. Introduction

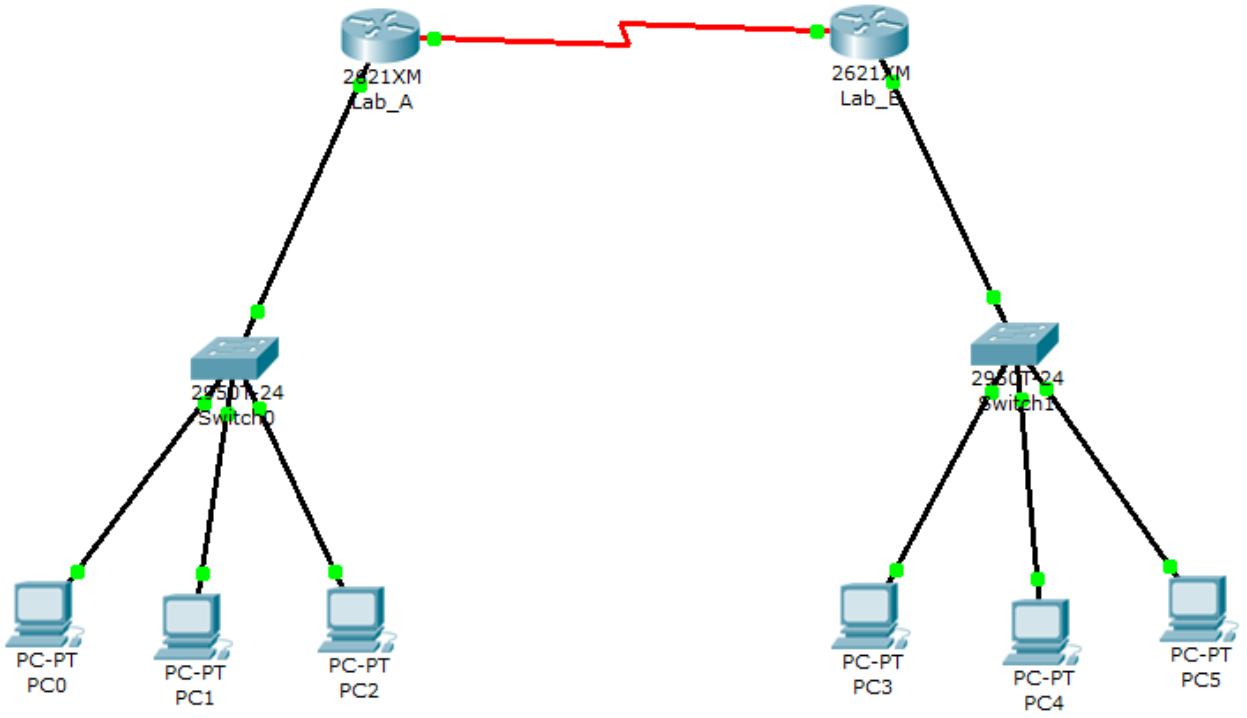
The Cisco IOS was created to deliver network services and enable networked applications. It runs on most Cisco routers and, on an ever-increasing number of Cisco Catalyst switches, such as the Catalyst 2950. Some of the important things that the Cisco router IOS software is responsible for include

- 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

You can access the Cisco IOS through the console port of a router, from a modem into the auxiliary (or Aux) port, or even through Telnet. Access to the IOS command line is called an EXEC session.

4. Procedure

1. Open Packet Tracer 5 and setup a network similar to the following network. Use Cisco 2950T switch & Cisco 2621XM router.



2. The different thing is the red link which is serial link (used for WAN). By default, it is not available so we have to add the modules to the router. Double click on any router. Turn it off by using power button on the router figure in **Physical** tab. On left side modules bar is present. Drag two **WIC-2T** to smaller blank space and one **NM-8A/S** to larger blank space. Now, turn on the router using power switch. Do the same on second router. Then use **Serial DTE** or **Serial DCE** link from **Connections**. The router interface that is chosen first becomes that of that type while the second one becomes the other e.g if you choose DTE and click first router, it becomes DTE while the second one becomes DCE and vice versa. Just remember that by default all serial interfaces are DTE so we have to provide clocking on the DCE one!

3. Use the following values to setup IP addresses on respective interfaces.

Router	Network Address	Interface	Address
Lab_A	192.168.10.0	fa0/0	192.168.10.1
Lab_A	192.168.20.0	s1/0	192.168.20.1
Lab_A	192.168.50.0	s1/1	192.168.50.1
Lab_B	192.168.30.0	fa0/0	192.168.30.1
Lab_B	192.168.20.0	s1/0	192.168.20.2
Lab_B	192.168.40.0	s1/1	192.168.40.1

A sample configuration is given as under

Router>**en**
Router#**config t**
Router(config)#**hostname Lab_A**
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 1/0**
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)#**interface serial 1/1**
Lab_A(config-if)#**ip address 192.168.50.1 255.255.255.0**
Lab_A(config-if)#**no shut**
Lab_A(config-if)#**exit**
Lab_A(config)#**banner motd #**
This is the Lab_A router
#
Lab_A(config)#**^z**
Lab_A#**copy running-config startup-config**
Destination filename [startup-config]? ***[Enter]***
Lab_A#

Before you jump in and configure a serial interface, there are a couple of things you need to know. First, the interface will usually be attached to a CSU/DSU type of device that provides clocking for the line to the router. But if you have a back-to-back configuration (for example, one that's used in a lab environment), one end—the data communication equipment (DCE) end of the cable—must provide clocking. By default, Cisco routers are all data terminal equipment (DTE) devices, so you must tell an interface to provide clocking if you need it to act like a DCE device.
To check the DCE interface, just bring your mouse over serial link, the interface with whose name you see a  (clock symbol) is the DCE one. You configure a DCE serial interface with the clock rate command:

Lab_B(config)#**interface serial 1/0**
Lab_B(config-if)#**clock rate ?**
<300-4000000> Choose clockrate from list above
Router(config-if)#**clock rate 64000**

Notice that the clock rate command is in bits per second.

Configure the PCs and Switches too. Make sure all devices are communicating with each other (use **ping** to verify).

Now you must have noticed that routers can communicate with devices directly connected to them. PC0-PC2 and Switch0 can communicate with Lab_A router & in between themselves but can't with Lab_B router and Switch1 & PC2-PC5 and vice versa.

4.1 Configuring Static Routing

Static routing occurs when you manually add routes in each router's routing table. There are pros and cons to static routing, but that's true for all routing processes. Static routing has the following benefits:

- There is no overhead on the router CPU, which means you could possibly buy a cheaper router than if you were using dynamic routing.
- There is no bandwidth usage between routers, which means you could possibly save money on WAN links.
- It adds security, because the administrator can choose to allow routing access to certain networks only.

Static routing has the following disadvantages:

- The administrator must really understand the internetwork and how each router is connected in order to configure routes correctly.
- If a network is added to the internetwork, the administrator has to add a route to it on all routers—by hand.
- It's not feasible in large networks because maintaining it would be a full-time job in itself.

The command syntax to add a static route to a routing table is as following:

ip route [*destination_network*] [*mask*] [*next-hop_address or exitinterface*] *administrative_distance*] [permanent]

This list describes each command in the string:

ip route The command used to create the static route.

destination_network The network you're placing in the routing table.

mask The subnet mask being used on the network.

next-hop_address The address of the next-hop router that will receive the packet and forward it to the remote network. This is a router interface that's on a directly connected network. You must be able to ping the router interface before you add the route. If you type in the wrong next-hop address, or the interface to that router is down, the static route will show up in the router's configuration, but not in the routing table.

exitinterface You can use it in place of the next-hop address if you want, but it's got to be on a point-to-point link, such as a WAN. This command won't work on a LAN such as Ethernet.

administrative_distance By default, static routes have an administrative distance of 1 (or even 0 if you use an exit interface instead of a next-hop address). You can change the default value by adding an administrative weight at the end of the command.

permanent If the interface is shut down, or the router can't communicate to the next-hop router, the route will automatically be discarded from the routing table. Choosing the permanent option keeps the entry in the routing table no matter what happens.

Configuration of Lab_A

Each routing table automatically includes directly connected networks. To be able to route to all networks in the internetwork, the routing table must include information that describes where these other networks are located and how to get there.

The Lab_A router is connected to networks 192.168.10.0, 192.168.50.0 and 192.168.20.0. For the Lab_A router to be able to route to all networks, the following networks have to be configured in its routing table:
_ 192.168.30.0
_ 192.168.40.0
The following router output shows the configuration of static routes on the Lab_A router and the routing table after the configuration. For the Lab_A router to find the remote networks, an entry is placed in the routing table describing the network, the mask, and where to send the packets. Notice that each static route sends the packets to 192.168.20.2, which is the Lab_A router's next hop.
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** (or serial 1/0)

After the router is configured, you can type **show running-config** and **show ip route** to see the static routes:

Lab_A#**sh ip route**
[output cut]
S 192.168.40.0 [1/0] via 192.168.20.2
S 192.168.30.0 [1/0] via 192.168.20.2
C 192.168.10.0/24 is directly connected, FastEthernet0/0
C 192.168.20.0/24 is directly connected, Serial 1/0
C 192.168.50.0/24 is directly connected, Serial 1/1
Lab_A#

Do the same on Lab_B router. For the Lab_B router to be able to route to all networks, the following networks have to be configured in its routing table:
_ 192.168.10.0
_ 192.168.50.0

After doing this ping the devices to check that they are communicating with each other. Try this step two to three times if unsuccessful for the first time. If still unsuccessful check the configuration.

4.2 Configuring Default Routing

We use *default routing* to send packets with a remote destination network not in the routing table to the next-hop router. You can only use default routing on stub networks—those with only one exit path out of the network.

In the internetworking example used in the previous section, the router that is considered to be in a stub network is Lab_A if its s1/1 is not connected to any other router. If you tried to put a default route on a router with two connected networks, packets wouldn't be forwarded to the correct networks because they have more than one interface routing to other routers. And even though router Lab_A has two connections, it doesn't have another router on the 192.168.50.0 network that needs packets sent to it. Router Lab_A will only send packets to the 192.168.20.1 interface of Lab_A.

To configure a default route, you use wildcards in the network address and mask locations of a static route. In fact, you can just think of a default route as a static route that uses wildcards instead of network and mask information. In this section, you'll create a default route on the Lab_A router.

Router Lab_A is directly connected to networks 192.168.10.0, 192.168.20.0 and 192.168.50.0. The routing table needs to know about networks 192.168.30.0, and 192.168.40.0.

To configure the router to route to the other three networks, we placed three static routes in the routing table. By using a default route, you can just create one static route entry instead. You must first delete the existing static routes from the router and then add the default route.

Lab_A(config)#**no ip route 192.168.30.0 255.255.255.0 192.168.20.2**
Lab_A(config)#**no ip route 192.168.40.0 255.255.255.0 192.168.20.2**
Lab_A(config)#**ip route 0.0.0.0 0.0.0.0 192.168.20.2**

If you look at the routing table now, you'll see only the two directly connected networks plus an S*, which indicates that this entry is a candidate for a default route.

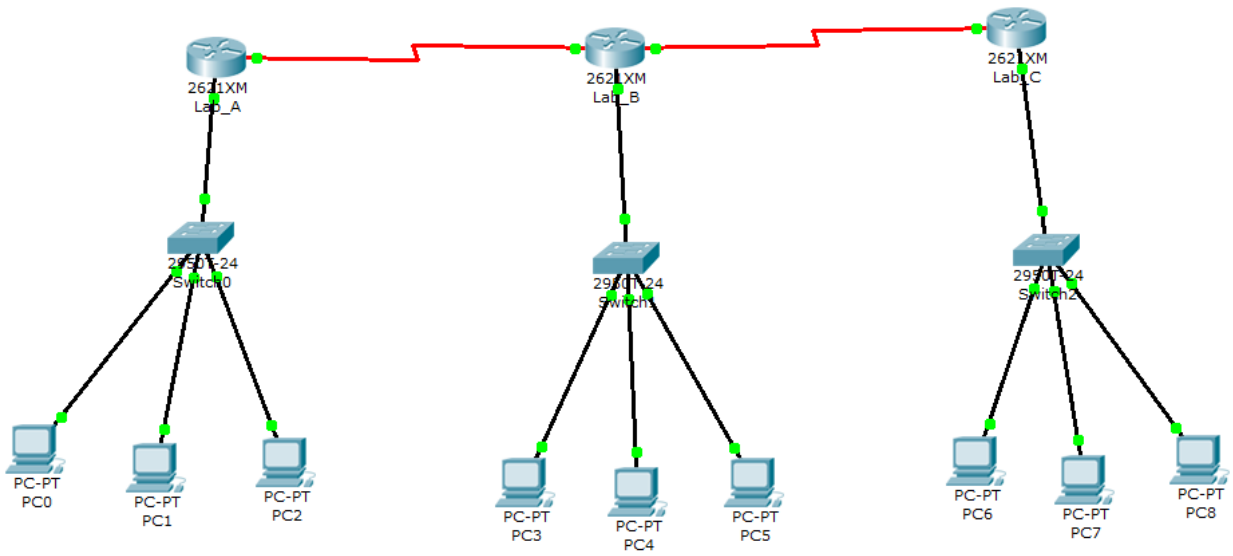
Lab_A#**sh ip route**
[output cut]
Gateway of last resort is 192.168.20.2 to network 0.0.0.0
C 192.168.10.0/24 is directly connected, FastEthernet0/0
C 192.168.20.0/24 is directly connected, Serial 1/0
C 192.168.50.0/24 is directly connected, Serial 1/1
S* 0.0.0.0/0 [1/0] via 192.168.20.2
Lab_A#

We could have completed the default route command another way:

Lab_A(config)#**ip route 0.0.0.0 0.0.0.0 s1/0**

This says that if you don't have an entry for a network in the routing table, just forward it out serial 0/0. You can choose the IP address of the next-hop router or the exit interface—either way, it will work the same. After doing this ping the devices to check that they are communicating with each other. Try this step two to three times if unsuccessful for the first time. If still unsuccessful check the configuration.

To check what happens if default routing is applied on routers other than stub networks, setup the following network in Packet Tracer.



Router	Network Address	Interface	Address
Lab_A	192.168.10.0	fa0/0	192.168.10.1
Lab_A	192.168.20.0	s1/0	192.168.20.1
Lab_A	192.168.50.0	s1/1	192.168.50.1
Lab_B	192.168.30.0	fa0/0	192.168.30.1
Lab_B	192.168.20.0	s1/0	192.168.20.2
Lab_B	192.168.40.0	s1/1	192.168.40.1
Lab_C	192.168.60.0	fa0/0	192.168.60.1
Lab_C	192.168.40.0	s1/0	192.168.40.2
Lab_C	192.168.70.0	s1/1	192.168.70.1

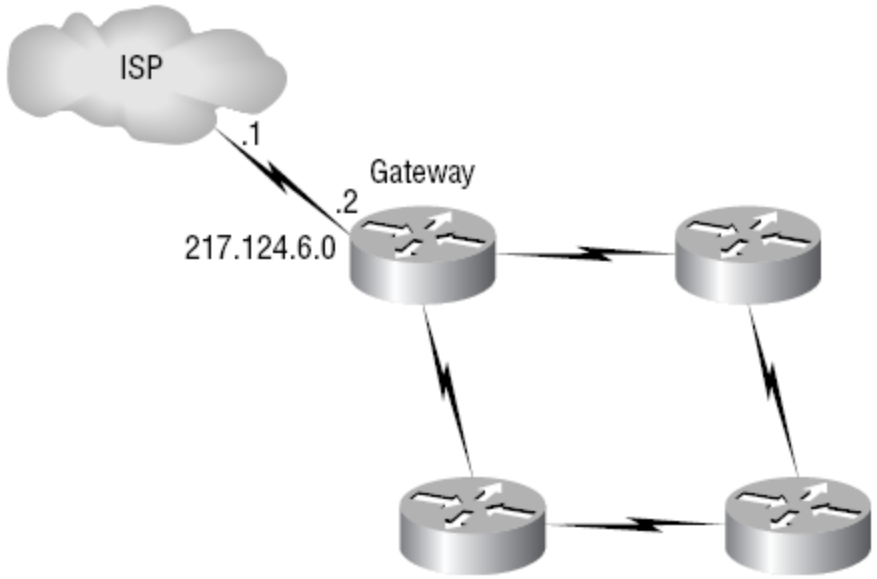
For better understanding, use the simulation mode of Packet tracer.

There's another command you can use to configure a gateway of last resort—the ip default-network command. Figure below shows a network that needs to have a gateway of last resort statement configured.

Here are three solutions (all providing the same solution) for adding a gateway of last resort on the gateway router to the ISP.

Gateway(config)#**ip route 0.0.0.0 0.0.0.0 217.124.6.1**
Gateway(config)#**ip route 0.0.0.0 0.0.0.0 s0/0**
Gateway(config)#**ip default-network 217.124.6.0**

All three of these commands would accomplish the goal of setting the gateway of last resort, but there are some small differences between them.



International Islamic University, Islamabad
Computer Networks Lab

LAB WORKSHEET (Lab # 8)

Q.1 What is Routing and on which OSI layer it happens?

_____
_____
_____
_____
_____

Q.2 Write any two advantages of static routing.

_____
_____
_____
_____
_____

Q.3 What happens when default routing is applied in networks other than stub networks?

_____
_____
_____
_____
_____

Q.4 What **DCE** & **DTE** stand for?

_____
_____
_____
_____
_____

International Islamic University, Islamabad
Computer Networks LAB

EXPERIMENT # 09: Dynamic Routing (Distance Vector)

Name of Student: ……..

Roll No.: ……

Date of Experiment: ……..

Report submitted on: ……..

Marks obtained: ……

Remarks: ……

Instructor's Signature: ……...

Dynamic Routing (Distance Vector)

1. Objective

This lab exercise is designed to understand routing and procedure to setup RIP on routers.

2. Resources Required

- Computer
- Packet Tracer (version 5 or higher)

3. Introduction

A routing protocol is a protocol that specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network, the choice of the route being done by routing algorithms. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network.

3.1 Types of Routing Protocols

There are two main types of routing protocols:

a) **Interior Gateway Protocol (IGP)** is a routing protocol that is used to exchange routing information within an autonomous system (AS). Examples are RIP, OSPF
b) **Exterior Gateway Protocol (EGP)** is for determining network reachability between autonomous systems and makes use of IGPs to resolve routes within an AS. Examples are BGP & EGP.

3.2 Types of Interior Gateway Routing Protocols

IGPs can be divided into following three types:

a) **Distance vector:** The distance-vector protocols find the best path to a remote network by judging distance. Each time a packet goes through a router, that's called a hop. The route with the least number of hops to the network is determined to be the best route. The vector indicates the direction to the remote network. Both RIP and IGRP are distance-vector routing protocols. They send the entire routing table to directly connected neighbors.
b) **Link state:** In link-state protocols, also called shortest-path-first 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. OSPF is an IP routing protocol that is completely link state. Link state protocols send updates containing the state of their own links to all other routers on the network.
c) **Hybrid:** Hybrid protocols use aspects of both distance vector and link state—for example, EIGRP.

There's no set way of configuring routing protocols for use with every business. This is something you really have to do on a case-by-case basis. If you understand how the different routing protocols work, you can make good, solid decisions that truly meet the individual needs of any business.

3.3 Administrative Distance & Metric

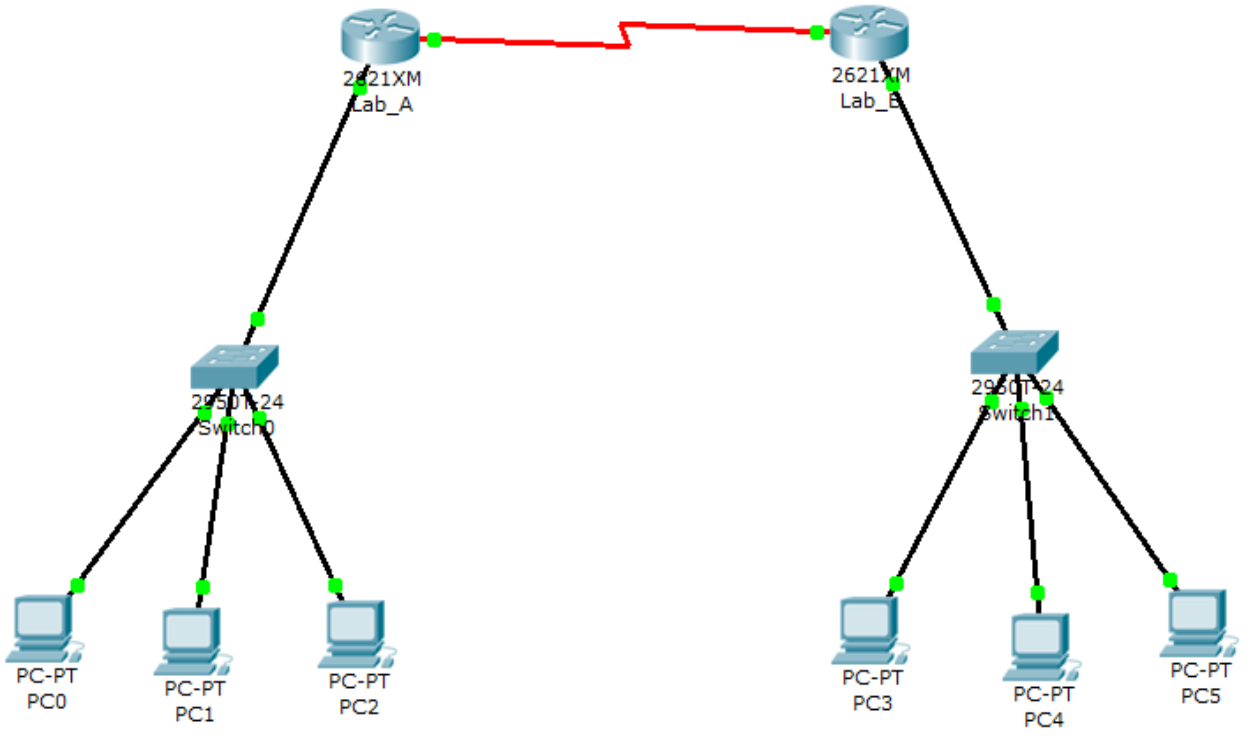
Metric is a property of a route in computer networking, consisting of any value used by routing algorithms to determine whether one route should perform better than another. It is used to choose the best route among the routes found by **same routing protocol**.

Administrative distance is the measure used by Cisco routers to select the best path when there are two or more different routes to the same destination from **two different routing protocols**. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) using an administrative distance value.

Remember! Smaller value (metric or administrative distance) means better route and Administrative Distance has preference over Metric.

4. Procedure

1. Open Packet Tracer 5 and setup a network similar to the following network. Use Cisco 2950T switch & Cisco 2621XM router.



2. The different thing is the red link which is serial link (used for WAN). By default, it is not available so we have to add the modules to the router. Double click on any router. Turn it off by using power button on the router figure in **Physical** tab. On left side modules bar is present. Drag two **WIC-2T** to smaller blank space and one **NM-8A/S** to larger blank space. Now, turn on the router using power switch. Do the same on second router. Then use **Serial DTE** or **Serial DCE** link from **Connections**. The router interface that is chosen first becomes that of that type while the second one becomes the other e.g if you choose DTE and click first router, it becomes DTE while the second one becomes DCE and vice versa. Just

remember that by default all serial interfaces are DTE so we have to provide clocking on the DCE one!

3. Use the following values to setup IP addresses on respective interfaces.

Router	Network Address	Interface	Address
Lab_A	192.168.10.0	fa0/0	192.168.10.1
Lab_A	192.168.20.0	s1/0	192.168.20.1
Lab_A	192.168.50.0	s1/1	192.168.50.1
Lab_B	192.168.30.0	fa0/0	192.168.30.1
Lab_B	192.168.20.0	s1/0	192.168.20.2
Lab_B	192.168.40.0	s1/1	192.168.40.1

A sample configuration is given as under

Router>**en**
Router#**config t**
Router(config)#**hostname Lab_A**
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 1/0**
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)#**interface serial 1/1**
Lab_A(config-if)#**ip address 192.168.50.1 255.255.255.0**
Lab_A(config-if)#**no shut**
Lab_A(config-if)#**exit**
Lab_A(config)#**banner motd #**
This is the Lab_A router
#

Lab_A(config)#**^z**
Lab_A#**copy running-config startup-config**
Destination filename [startup-config]? ***[Enter]***
Lab_A#

Before you jump in and configure a serial interface, there are a couple of things you need to know. First, the interface will usually be attached to a CSU/DSU type of device that provides clocking for the line to the router. But if you have a back-to-back configuration (for example, one that's used in a lab environment), one end—the data communication equipment (DCE) end of the cable—must provide clocking. By default, Cisco routers are all data terminal equipment (DTE) devices, so you must tell an interface to provide clocking if you need it to act like a DCE device.
To check the DCE interface, just bring your mouse over serial link, the interface with whose name you see a  (clock symbol) is the DCE one. You configure a DCE serial interface with the clock rate command:

Lab_B(config)#**interface serial 1/0**
Lab_B(config-if)#**clock rate ?**
<300-4000000> Choose clockrate from list above
Router(config-if)#**clock rate 64000**

Notice that the clock rate command is in bits per second.

Configure the PCs and Switches too. Make sure all devices are communicating with each other (use **ping** to verify).

Now you must have noticed that routers can communicate with devices directly connected to them. PC0-PC2 and Switch0 can communicate with Lab_A router & in between themselves but can't with Lab_B router and Switch1 & PC2-PC5 and vice versa.

4.1 Configuring RIP (Routing Information Protocol)

The network command tells the routing protocol which network to advertise. Look at the next router configuration:

```
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)#network 192.168.50.0
Lab_A(config-router)#^Z
Lab_A#
```

Note the fact that you need to type in every directly connected network that you want RIP to advertise. But because they're not directly connected we're going to leave out networks 192.168.30.0 and 192.168.40.0—it's RIP's job to find them and populate the routing table.
That's it. Dynamic routing makes your job a lot easier than when using static routes, doesn't it? However, keep in mind the extra router CPU process and bandwidth that you're consuming.

The Lab_B router has three directly connected networks and we want RIP to advertise them all, so we will add three network statements. Here are steps to configure RIP on the Lab_B:

```
Lab_B#config t
Enter configuration commands, one per line. End with CNTL/Z.
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)#^Z
Lab_B#
```

Each routing table should now have the routers' directly connected routes as well as RIP injected routes received from neighboring routers.
This output shows us the contents of the Lab_A routing table (your output may differ):

```
Lab_A#sh ip route
[output cut]
R 192.168.40.0 [120/1] via 192.168.20.2, 00:00:23, Serial1/0
R 192.168.30.0 [120/1] via 192.168.20.2, 00:00:23, Serial1/0
C 192.168.50.0 is directly connected, Serial1/1
C 192.168.20.0 is directly connected, Serial1/0
C 192.168.10.0 is directly connected, FastEthernet0/0
Lab_A#
```

Looking at this, you can see that the routing table has the same entries that they had when we were using static routes, except for that R. The R means that the networks were added dynamically using the RIP routing protocol. The [120/1] is the administrative distance of the route (120) along with the number of hops to that remote network (1).

The following output displays Lab_B's routing table.

Lab_B#**sh ip route**
[output cut]
R 192.168.50.0 [120/1] via 192.168.20.1, 00:00:11, Serial1/0
C 192.168.40.0 is directly connected, Serial1/1
C 192.168.30.0.0 is directly connected, FastEthernet0/0
C 192.168.20.0 is directly connected, Serial1/0
R 192.168.10.0 [120/1] via 192.168.20.1, 00:00:21, Serial1/0
Lab_B#

So while yes, it's true that RIP has worked really well in our little internetwork, it's not the solution for every enterprise. That's because this technique has a maximum hop count of only 15 (16 is deemed unreachable) and it performs full routing-table updates every 30 seconds, both things that can wreak havoc in a larger internetwork.

You probably don't want your RIP network advertised everywhere on your LAN and WAN. There's not a whole lot to be gained by advertising your RIP network to the Internet.
There are a few different ways to stop unwanted RIP updates from propagating across your LANs and WANs. The easiest one is through the passive-interface command. This command prevents RIP update broadcasts from being sent out a defined interface, but that same interface can still receive RIP updates.
Here's an example of how to configure a passive-interface on a router:

Lab_A#**config t**
Lab_A(config)#**router rip**
Lab_A(config-router)#**network 192.168.10.0**
Lab_A(config-router)#**passive-interface serial 1/0**

This command will stop RIP updates from being propagated out serial interface 1/0, but serial interface 1/0 can still receive RIP updates.

4.2 RIP Version 2 (RIPv2)
RIP version 2 is mostly the same as RIP version 1. Both RIPv1 and RIPv2 are distance-vector protocols, which means that each router running RIP sends its complete routing tables out all active interfaces at periodic time intervals. Also, the timers and loop-avoidance schemes are the same in both RIP versions—i.e., holddown timers and split horizon rule. Both RIPv1 and RIPv2 are configured as classful addressing, (but RIPv2 is considered classless because subnet information is sent with each route update), and both have the same administrative distance (120).
But there are some important differences that make RIPv2 more scalable than RIPv1. Since RIP is an open standard, you can use RIP with any brand of router. You can also use OSPF, since OSPF is an open standard as well. RIP just requires too much bandwidth, making it pretty intensive to use in your network.
RIPv2, unlike RIPv1, is a classless routing protocol (even though it is configured as classful, like RIPv1), which means that it sends subnet mask information along with the route updates.

By sending the subnet mask information with the updates, RIPv2 can support Variable Length Subnet Masks (VLSMs) as well as the summarization of network boundaries. In addition, RIPv2 can support discontiguous networking.

Configuring RIPv2 is pretty straightforward. Here's an example:

Lab_A(config)#**router rip**
Lab_A(config-router)#**network 192.168.10.0**
Lab_A(config-router)#**network 192.168.50.0**
Lab_A(config-router)#**version 2**

That's it; just add the command **version 2** under the (config-router)# prompt and you are now running RIPv2.

4.3 The *debug ip rip* Command

The debug ip rip command sends routing updates as they are sent and received on the router to the console session. If you are telnetted into the router, you'll need to use the terminal monitor command to be able to receive the output from the debug commands.
Below is an example of how debug output looks, your output may differ according to your configurations. We can see in this output that RIP is both sent and received on serial 0/0 and serial 0/1 interfaces (the metric is the hop count):

Lab_B#**debug ip rip**
RIP protocol debugging is on
Lab_B#
RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (192.168.30.1)
RIP: build update entries
network 192.168.10.0 metric 2
network 192.168.20.0 metric 1

RIP: sending v1 update to 255.255.255.255 via Serial1/0 (192.168.20.2)
RIP: build update entries
network 192.168.30.0 metric 1

RIP: received v1 update from 192.168.20.1 on Serial1/0
192.168.10.0 in 1 hops

To turn off debugging, use the undebug all or the no debug all command. Here is an example of using the undebug all command:

Lab_B#**undebug all**
All possible debugging has been turned off
Lab_B#

International Islamic University, Islamabad
Computer Networks Lab

LAB WORKSHEET (Lab # 9)

Q.1 What is the advantage of Dynamic routing?

Q.2 What are the different types of IGPs?

Q.3 What is the metric of **RIP**?

Q.4 Why **Administrative Distance** is used?

International Islamic University, Islamabad
Computer Networks LAB

EXPERIMENT # 10: Dynamic Routing (Link State)

Name of Student: ……..

Roll No.: ……

Date of Experiment: ……..

Report submitted on: ……..

Marks obtained: ……

Remarks: ……

Instructor's Signature: ……...

Dynamic Routing (Link State)

1. Objective

This lab exercise is designed to understand routing and procedure to setup OSPF on routers.

2. Resources Required

- Computer
- Packet Tracer (version 5 or higher)

3. Introduction

A routing protocol is a protocol that specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network, the choice of the route being done by routing algorithms. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network.

3.1 Types of Routing Protocols

There are two main types of routing protocols:

a) **Interior Gateway Protocol (IGP)** is a routing protocol that is used to exchange routing information within an autonomous system (AS). Examples are RIP, OSPF
b) **Exterior Gateway Protocol (EGP)** is for determining network reachability between autonomous systems and makes use of IGPs to resolve routes within an AS. Examples are BGP & EGP.

3.2 Types of Interior Gateway Routing Protocols

IGPs can be divided into following three types:

a) **Distance vector:** The distance-vector protocols find the best path to a remote network by judging distance. Each time a packet goes through a router, that's called a hop. The route with the least number of hops to the network is determined to be the best route. The vector indicates the direction to the remote network. Both RIP and IGRP are distance-vector routing protocols. They send the entire routing table to directly connected neighbors.
b) **Link state:** In link-state protocols, also called shortest-path-first 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. OSPF is an IP routing protocol that is completely link state. Link state protocols send updates containing the state of their own links to all other routers on the network.
c) **Hybrid:** Hybrid protocols use aspects of both distance vector and link state—for example, EIGRP.

There's no set way of configuring routing protocols for use with every business. This is something you really have to do on a case-by-case basis. If you understand how the different routing protocols work, you can make good, solid decisions that truly meet the individual needs of any business.

3.3 Administrative Distance & Metric

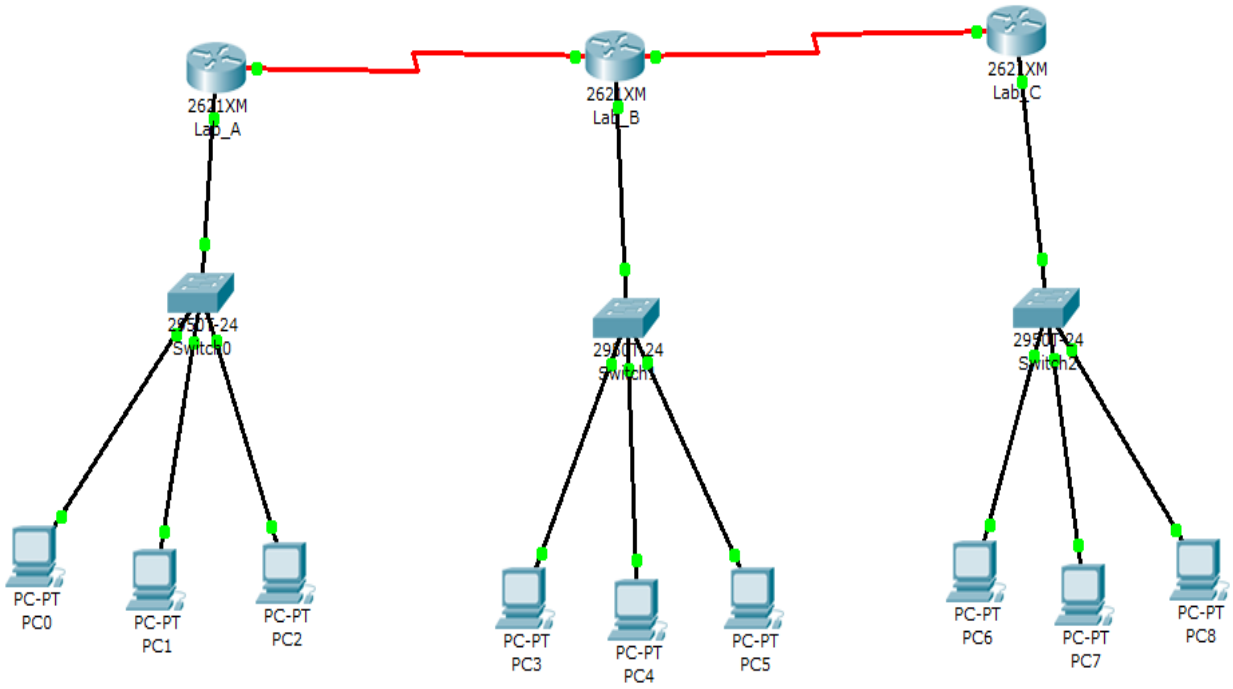
Metric is a property of a route in computer networking, consisting of any value used by routing algorithms to determine whether one route should perform better than another. It is used to choose the best route among the routes found by **same routing protocol**.

Administrative distance is the measure used by Cisco routers to select the best path when there are two or more different routes to the same destination from **two different routing protocols**. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) using an administrative distance value.

Remember! Smaller value (metric or administrative distance) means better route and Administrative Distance has preference over Metric.

4. Procedure

1. Open Packet Tracer 5 and setup a network similar to the following network. Use Cisco 2950T switch & Cisco 2621XM router.



2. The different thing is the red link which is serial link (used for WAN). By default, it is not available so we have to add the modules to the router. Double click on any router. Turn it off by using power button on the router figure in **Physical** tab. On left side modules bar is present. Drag two **WIC-2T** to smaller blank space and one **NM-8A/S** to larger blank space. Now, turn on the router using power switch. Do the same on second router. Then use **Serial DTE** or **Serial DCE** link from **Connections**. The router interface that is chosen first becomes that of that type while the second one becomes the other e.g if you choose DTE and click first router, it becomes DTE while the second one becomes DCE and vice versa. Just

remember that by default all serial interfaces are DTE so we have to provide clocking on the DCE one!

3. Use the following values to setup IP addresses on respective interfaces.

Router	Network Address	Interface	Address
Lab_A	192.168.10.0	fa0/0	192.168.10.1
Lab_A	192.168.20.0	s1/0	192.168.20.1
Lab_A	192.168.50.0	s1/1	192.168.50.1
Lab_B	192.168.30.0	fa0/0	192.168.30.1
Lab_B	192.168.20.0	s1/0	192.168.20.2
Lab_B	192.168.40.0	s1/1	192.168.40.1
Lab_C	192.168.60.0	fa0/0	192.168.60.1
Lab_C	192.168.40.0	s1/0	192.168.40.2
Lab_C	192.168.70.0	s1/1	192.168.70.1

A sample configuration is given as under

Router>**en**
Router#**config t**
Router(config)#**hostname Lab_A**
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 1/0**
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)#**interface serial 1/1**
Lab_A(config-if)#**ip address 192.168.50.1 255.255.255.0**
Lab_A(config-if)#**no shut**

Lab_A(config-if)#**exit**
Lab_A(config)#**banner motd #**
This is the Lab_A router
#
Lab_A(config)#**^z**
Lab_A#**copy running-config startup-config**
Destination filename [startup-config]? ***[Enter]***
Lab_A#

Before you jump in and configure a serial interface, there are a couple of things you need to know. First, the interface will usually be attached to a CSU/DSU type of device that provides clocking for the line to the router. But if you have a back-to-back configuration (for example, one that's used in a lab environment), one end—the data communication equipment (DCE) end of the cable—must provide clocking. By default, Cisco routers are all data terminal equipment (DTE) devices, so you must tell an interface to provide clocking if you need it to act like a DCE device.
To check the DCE interface, just bring your mouse over serial link, the interface with whose name you see a  (clock symbol) is the DCE one. You configure a DCE serial interface with the clock rate command:

Lab_B(config)#**interface serial 1/0**
Lab_B(config-if)#**clock rate ?**
<300-4000000> Choose clockrate from list above
Router(config-if)#**clock rate 64000**

Notice that the clock rate command is in bits per second.

Configure the PCs and Switches too. Make sure all devices are communicating with each other (use **ping** to verify).

Now you must have noticed that routers can communicate with devices directly connected to them. PC0-PC2 and Switch0 can communicate with Lab_A router & in between themselves but can't with Lab_B router and Switch1 & PC2-PC5 and vice versa.

4.1 Configuring OSPF (Open Shortest Path First)

Configuring basic OSPF isn't as simple as RIP, IGRP, and EIGRP, and it can get really complex once the many options that are allowed within OSPF are factored in. The following sections describe how to configure single area OSPF.
These two elements are the basic elements of OSPF configuration:

- Enabling OSPF
- Configuring OSPF areas

4.1.1 Enabling OSPF

The easiest and also least scalable way to configure OSPF is to just use a single area. Doing this requires a minimum of two commands.
The command you use to activate the OSPF routing process is:

Lab_A(config)#**router ospf ?**
<1-65535>

A value in the range 1–65,535 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 in order to communicate. It's purely a local value that essentially has little meaning, but it cannot start at 0, it has to start at a minimum of 1.
You can have more than one OSPF process running simultaneously on the same router if you want, but this isn't the same as running multi-area OSPF. The second process will maintain an entirely separate copy of its topology table and manage its communications independently of the first process. Objectives of this lab only cover single-area OSPF with each router running a single OSPF process.

4.1.2 Configuring OSPF Areas

After identifying the OSPF process, you need to identify the interfaces that you want to activate OSPF communications on, as well as the area in which each resides. This will also configure the networks you're going to advertise to others. OSPF uses wildcards in the configuration.
Here's an OSPF basic configuration example for you:

Lab_A#**config t**
Lab_A(config)#**router ospf 1**
Lab_A(config-router)#**network 10.0.0.0 0.255.255.255 area ?**
<0-4294967295> OSPF area ID as a decimal value
A.B.C.D OSPF area ID in IP address format
Lab_A(config-router)#**network 10.0.0.0 0.255.255.255 area 0**

Remember, the OSPF Process ID number is irrelevant. It can be the same on every router on the network, or it can be different—doesn't matter. It's locally significant and just enables the OSPF routing on the router.
The arguments of the network command are the network number (10.0.0.0) and the wildcard mask (0.255.255.255). The combination of these two numbers identifies the interfaces that OSPF

will operate on, and will also be included in its OSPF LSA advertisements. OSPF will use this command to find any interface on the router configured in the 10.0.0.0 network, and it will place any interface it finds into area 0. You can also label an area using an IP address format.
A quick review of **wildcards**, a 0 octet in the wildcard mask indicates that the corresponding octet in the network must match exactly. On the other hand, a 255 indicates that you don't care what the corresponding octet is in the network number. A network and wildcard mask combination of 1.1.1.1 0.0.0.0 would match 1.1.1.1 only, and nothing else. This is really useful if you want to activate OSPF on a specific interface in a very clear and simple way. If you insist on matching a range of networks, the network and wildcard mask combination of 1.1.0.0 0.0.255.255 would match anything in the range 1.1.0.0–1.1.255.255. Because of this, it's simpler and safer to stick to using wildcard masks of 0.0.0.0 and identify each OSPF interface individually.
The final argument is the **area number**. It indicates the area to which the interfaces identified in the network and wildcard mask portion belong. Remember that OSPF routers will only become neighbors if their interfaces share a network that's configured to belong to the same area number. The format of the area number is either a decimal value from the range 1–4,294,967,295 or a value represented in standard dotted-decimal notation. For example, area 0.0.0.0 is a legitimate area, and is identical to area 0.

Let's configure our network with OSPF using just area 0. The simplest and easiest way to configure OSPF is to use the wildcard mask of 0.0.0.0. We can configure each router differently with OSPF and still come up with the exact same result.

Lab_A
So here's the Lab_A router's configuration:

Lab_A#**config t**
Enter configuration commands, one per line. End with CNTL/Z.
Lab_A(config)#**router ospf 1**
Lab_A(config-router)#**network 192.168.10.1 0.0.0.0 area 0**
Lab_A(config-router)#**network 192.168.20.1 0.0.0.0 area 0**
Lab_A(config-router)#**network 192.168.50.1 0.0.0.0 area 0**
Lab_A(config-router)#**^Z**
Lab_A#

So why did we use OSPF 1? It really doesn't matter—the number is irrelevant!
The two network commands are pretty straightforward. We typed in the IP address of each interface and used the wildcard mask of 0.0.0.0, which means that the IP address must match each octet exactly. Now, let's go on to Lab_B. We're going to use a different configuration.

Lab_B
The Lab_B router is directly connected to networks 20, 30 and 40. Instead of typing in each interface, we can use one network command and still make it work:

Lab_B#**config t**
Enter configuration commands, one per line. End with CNTL/Z.

Lab_B(config)#**router ospf 132**
Lab_B(config-router)#**network 192.168.0.0 0.0.255.255 area 0**
Lab_B(config-router)#**^Z**
Lab_B#

This is a fast and efficient configuration. We turned on OSPF routing process 1 and added the network command 192.168.0.0 with a wildcard of 0.0.255.255. What this said is just, "Find any interface that starts with 192.168, and place those interfaces into area 0." Quick and easy!

Lab_C
Let's give the Lab_C router that's directly connected to networks 40, 60 and 70 some attention:

Lab_C#**config t**
Enter configuration commands, one per line. End with CNTL/Z.
Lab_C(config)#**router ospf 100**
Lab_C(config-router)#**network 192.168.40.0 0.0.0.255 area 0**
Lab_C(config-router)#**network 192.168.60.0 0.0.0.255 area 0**
Lab_C(config-router)#**network 192.168.70.0 0.0.0.255 area 0**
Lab_C(config-router)#**^Z**
Lab_C#

Now that we've configured all the routers with OSPF, what do we do next? We still have to make sure that OSPF is really working! We will do that in the next section.

4.1.3 Verifying OSPF Configuration

There are several ways to verify proper OSPF configuration and operation, and in the following sections I'll show you the OSPF show commands you need to know in order to do this. We're going to start by taking a quick look at the routing table of each router.
So, let's issue a show ip route command on the Lab_A router:

Lab_A#**sh ip route**
Gateway of last resort is not set
C 192.168.10.0/24 is directly connected, FastEthernet0/0
C 192.168.20.0/24 is directly connected, Serial1/0
O 192.168.30.0/24 [110/65] via 192.168.20.2, 00:00:30, Serial1/0
O 192.168.40.0/24 [110/128] via 192.168.20.2, 00:00:30, Serial1/0
O 192.168.60.0/24 [110/129] via 192.168.20.2, 00:00:30, Serial1/0
Lab_A#

The Lab_A router shows the OSPF found routes for networks 30, 40, and 50, with the *O* representing OSPF internet routes.

Now let's see what the Lab_B router found:

```
Lab_B#sh ip route
Gateway of last resort is not set
O    192.168.10.0/24 [110/65] via 192.168.20.1, 00:07:02, Serial1/0
C    192.168.20.0/24 is directly connected, Serial1/0
C    192.168.30.0/24 is directly connected, FastEthernet0/0
C    192.168.40.0/24 is directly connected, Serial1/1
O    192.168.60.0/24 [110/65] via 192.168.40.2, 00:07:02, Serial1/1
Lab_B#
```

The Lab_B router shows the OSPF found routes for 10 and 60—nice!
One more router to verify—Lab C:

```
Lab_C#sh ip route
Gateway of last resort is not set
O    192.168.10.0/24 [110/129] via 192.168.40.1, 00:02:14, Serial1/0
O    192.168.20.0/24 [110/128] via 192.168.40.1, 00:02:14, Serial1/0
O    192.168.30.0/24 [110/65] via 192.168.40.1, 00:02:14, Serial1/0
C    192.168.40.0/24 is directly connected, Serial1/0
C    192.168.60.0/24 is directly connected, FastEthernet0/0
Lab_C#
```

The Lab_C router shows all the routes in the network, so even though each router was configured differently with OSPF, notice that everything is working great.

a) The *show ip ospf* Command

The show ip ospf command is used to display OSPF information for one or all OSPF processes running on the router. Information contained therein includes the Router ID, area information, SPF statistics, and LSA timer information. Let's check out the output from the Lab_A router:

```
Lab_A#sho ip ospf
Routing Process "ospf 1" with ID 192.168.50.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        Area has no authentication
```

SPF algorithm executed 3 times
Area ranges are
Number of LSA 3. Checksum Sum 0x017ee0
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

Notice the Router ID (RID) of 192.168.50.1, which is the highest IP address in the router.

b) The *show ip ospf database* Command

The information displayed by the show ip ospf database command indicates the number of links and the neighboring router's ID and is the topology database mentioned earlier. The output is broken down by area. Here's a sample output, again from Lab A:

Lab_A#**sh ip ospf database**
OSPF Router with ID (192.168.50.1) (Process ID 1)
Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
192.168.50.1	192.168.50.1	1728	0x80000005	0x0078fb	3
192.168.40.1	192.168.40.1	1728	0x80000005	0x009067	5
192.168.70.1	192.168.70.1	1728	0x80000004	0x00757e	3

Lab_A#

The router output shows the link ID (remember that an interface is also a link) and the RID of the router on that link under the ADV router (advertising router).

c) The *show ip ospf interface* Command

The show ip ospf interface command displays all interface-related OSPF information. Data is displayed about OSPF information for all interfaces or for specified interfaces. The information displayed by this command includes:

- Interface IP address
- Area assignment
- Process ID
- Router ID
- Network type
- Cost
- Priority
- DR/BDR election information (if applicable)
- Hello and Dead timer intervals
- Adjacent neighbor information

Here's the output from the Lab_A router:

```
Lab_A#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24, Area 0
  Process ID 1, Router ID 192.168.50.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.50.1, Interface address 192.168.10.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial1/0 is up, line protocol is up
  Internet address is 192.168.20.1/24, Area 0
  Process ID 1, Router ID 192.168.50.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.40.1
  Suppress hello for 0 neighbor(s)
```

d) The *show ip ospf neighbor* Command

The show ip ospf neighbor command is super-useful because it summarizes the pertinent OSPF information regarding neighbors and the adjacency state. If a DR or BDR exists, that information will also be displayed. Here's a sample:

```
Lab_A#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.40.1      0   FULL/  -        00:00:39    192.168.20.2    Serial1/0
Lab_A#
```

e) The *show ip protocols* Command

The show ip protocols command is also useful whether you're running OSPF, EIGRP, IGRP, RIP, BGP, IS-IS, or any other routing protocol that can be configured on your router. It provides an excellent overview of the actual operation of all currently running protocols.

Check out the output from the Lab_A router:

```
Lab_A#sh ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.50.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.10.1 0.0.0.0 area 0
    192.168.20.1 0.0.0.0 area 0
    192.168.50.1 0.0.0.0 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.40.1         110      00:03:29
    192.168.50.1         110      00:03:28
    192.168.70.1         110      00:03:29
  Distance: (default is 110)
Lab_A#
```

Based upon this output, you can determine the OSPF Process ID, OSPF Router ID, type of OSPF area, networks and areas configured for OSPF, and OSPF Router IDs of neighbors— that's a lot.

4.2 OSPF and Loopback Interfaces

Configuring loopback interfaces when using the OSPF routing protocol is important, and Cisco suggests using them whenever you configure OSPF on a router. *Loopback interfaces* are logical interfaces, which are virtual, software-only interfaces; they are not real router interfaces. Using loopback interfaces with your OSPF configuration ensures that an interface is always active for OSPF processes.

They can be used for diagnostic purposes as well as OSPF configuration. The reason you want to configure a loopback interface on a router is because if you don't, the highest IP address on a router will become that router's RID. The RID is used to advertise the routes as well as elect the DR and BDR.

Let's say that you are not using loopback interfaces and the serial interface of your router is the RID of the router because it has the highest IP address of active interfaces. If this interface goes down, then a re-election must occur on who is going to be the DR and BDR on the network. What happens if this is a flapping link (going up/down)?

The routers will not converge because the election is never completed. This is obviously a problem with OSPF. In the following sections, you will see how to configure loopback interfaces, and how to verify loopback addresses and RIDs.

4.2.1 Configuring Loopback Interfaces

Configuring loopback interfaces is the easiest part of OSPF configuration. From previous lab first, let's see what the RID is on the Lab_A router with the show ip ospf command:

```
Lab_A#sh ip ospf
Routing Process "ospf 1" with ID 192.168.50.1
[output cut]
```

We can see that the RID is 192.168.50.1, or the serial 1/1 interface of the router. So let's configure a loopback interface using a completely different IP addressing scheme:

```
Lab_A#config t
Enter configuration commands, one per line. End with CNTL/Z.
Lab_A(config)#int loopback 0
Lab_A(config-if)#ip address 172.16.10.1 255.255.255.255
Lab_A(config-if)#no shut
Lab_A(config-if)#^Z
Lab_A#
```

The IP scheme really doesn't matter here, but each router has to be in a separate subnet. Let's configure lab_B now:

```
Lab_B#config t
Enter configuration commands, one per line. End with CNTL/Z.
Lab_B(config)#int lo0
Lab_B(config-if)#ip address 172.16.20.1 255.255.255.255
Lab_B(config-if)#no shut
Lab_B(config-if)#^Z
Lab_B#
```

Here is the configuration of the loopback interface on Lab_C:

```
Lab_C#config t
Enter configuration commands, one per line. End with CNTL/Z.
Lab_C(config)#int lo0
Lab_C(config-if)#ip address 172.16.30.1 255.255.255.255
Lab_C(config-if)#no shut
Lab_C(config-if)#^Z
Lab_C#
```

You may be wondering what the IP address mask of 255.255.255.255 (/32) means and why we don't just use 255.255.255.0 instead. Well, either mask works, but the /32 mask is called a host mask and works fine for loopback interfaces.

The only question left to answer is whether you want to advertise the loopback interfaces under OSPF. There are pros and cons to using an address that won't be advertised, versus using an address that will be. Using an unadvertised address saves on real IP address space, but the

address won't appear in the OSPF table, so you can't ping it. So basically, what you're faced with here is a choice that equals a trade-off between the ease of debugging the network and conservation of address space—what to do? A really tight strategy is to use a private IP address scheme as we did here in configuration.

4.2.2 Verifying Loopbacks and RIDs

To verify your loopback addresses, use show running-config—it's the easiest way to do it:

```
Lab_C#show running-config
!
hostname Lab_C
!
interface Loopback0
ip address 172.16.30.1 255.255.255.255
```

And to verify the new RIDs of each router, you can use the show ip ospf interface command, the show ip ospf database, or just the show ip ospf command. All three are shown below:

```
Lab_C#show ip ospf database
OSPF Router with ID (172.16.30.1) (Process ID 100)
Router Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.30.1     172.16.30.1     206         0x80000003 0x004d72 3
172.16.10.1     172.16.10.1     208         0x80000003 0x004cf6 3
172.16.20.1     172.16.20.1     203         0x80000005 0x009f44 5
```

The show ip ospf database shows the RID in the first line of output. The show ip ospf interface also displays this information, but you have to dig for it a little more:

```
Lab_C#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
Internet Address 172.16.60.1/24, Area 0
Process ID 100, Router ID 172.16.30.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 172.16.30.1, Interface address 172.16.60.1
No backup designated router on this network
[output cut]
```

The show ip ospf command shows the RID in the first line of output:

```
Lab_C#show ip ospf
Routing Process "ospf 100" with ID 172.16.30.1
[output cut]
```

An important thing to keep in mind is that for some models the new RIDs didn't show up after setting the loopback interface on each router until routers are rebooted.

International Islamic University, Islamabad
Computer Networks Lab

LAB WORKSHEET (Lab # 10)

Q.1 Write one example each of Distance Vector, Link State & Hybrid IGPs.

Q.2 What **OSPF** stands for and what is its **Administrative Distance**?

Q.3 What is the difference between **subnet mask** and **wildcard mask?**

Q.4 Differentiate **Distance Vector** and **Link State** routing protocols.

International Islamic University, Islamabad
Computer Networks LAB

EXPERIMENT # 11: Access Control Lists (ACLs)

Name of Student: ……..

Roll No.: ……

Date of Experiment: ……..

Report submitted on: ……..

Marks obtained: ……

Remarks: ……

Instructor's Signature: ……...

Access Control Lists (ACLs)

1. Objective

This lab exercise is designed to understand creating and applying ACLs on Cisco routers.

2. Resources Required

- Computer
- Packet Tracer (version 5 or higher)

3. Introduction

Cisco routers can be used as part of a good overall security strategy. One of the most important tools in Cisco IOS software used as a part of that strategy are Access Control Lists (ACLs—also called Access Lists). ACLs define rules that can be used to prevent some packets from flowing through the network. The access list is a group of statements. Each statement defines a pattern that would be found in an IP packet. As each packet comes through an interface with an associated access list, the list is scanned from top to bottom--in the exact order that it was entered--for a pattern that matches the incoming packet. A permit or deny rule associated with the pattern determines that packet's fate. You also can use a mask, which is like a wild card, to determine how much of an IP source or destination address to apply to the pattern match. The pattern statement also can include a TCP or UDP (User Datagram Protocol) port number.

3.1 Types of Access Lists

Access lists are generally broken into 2 major groups:

a) **Standard ACLs** only operate on the Network layer of the OSI model. These are used to block or permit networks from reaching other networks.
b) **Extended ACLs** Extended access lists function on both Network and Transport layers of the OSI model. That is, they allow you to filter not only by network address but also by the type of traffic that is being sent or received. Extended access lists are much more flexible and allow for much greater control of traffic into and out of your network than standard access lists.

3.2 Named Access Control Lists

The ACLs introduced in the beginning by Cisco IOS were distinguished by a special number e.g. 1-99 for Standard ACLs and 100-199 for Extended ACLs. The named ACLs (introduced with IOS version 11.2) do the same as standard and extended ACLs but they are not represented by a number but by a name that is given by the user to easily remember.

In addition to using more memorable names, the other major advantage of named ACLs over numbered ACLs, at the time they were introduced into IOS, was that you could delete individual lines in named IP access list.

Remember! With IOS 12.3, Cisco expanded IOS to be able to delete individual lines in numbered ACL, making IOS support for editing both named and numbered ACLs equivalent.

3.3 In, Out, Inbound, Outbound, Source, and Destination

The router uses the terms in, out, source, and destination as references. Traffic on the router can be compared to traffic on the highway. If you were a law enforcement officer in Pennsylvania

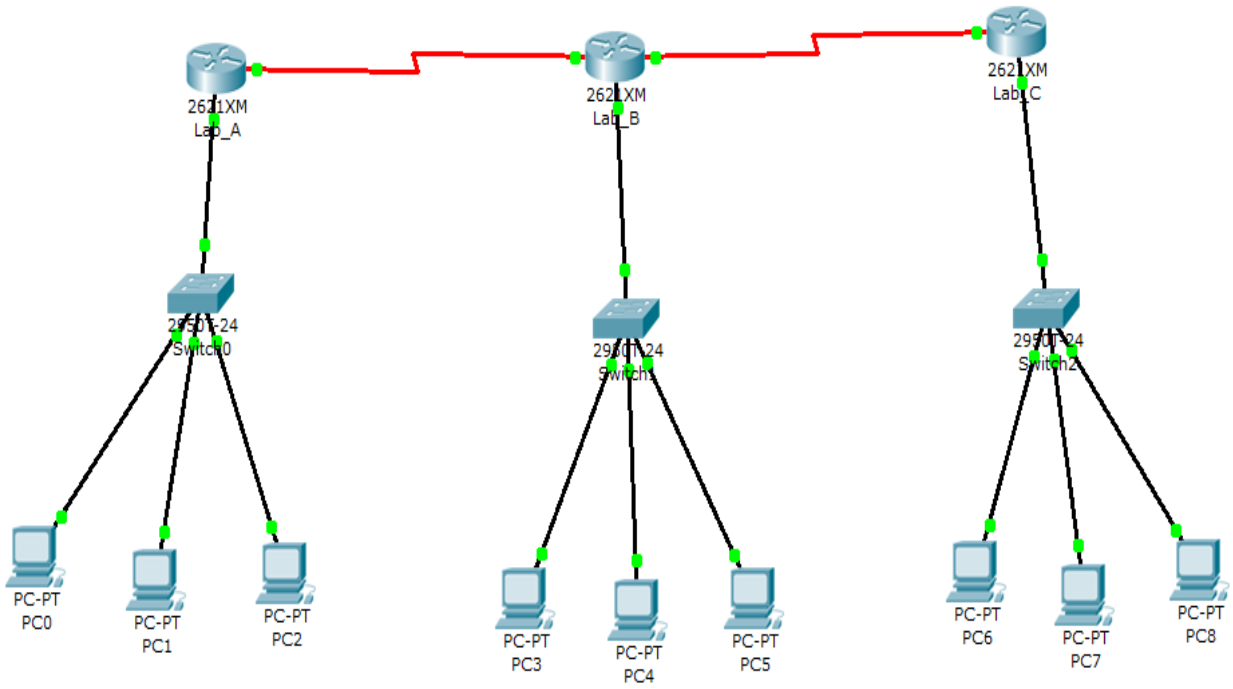
and wanted to stop a truck going from Maryland to New York, the source of the truck is Maryland and the destination of the truck is New York. The roadblock could be applied at the Pennsylvania–New York border (out) or the Maryland–Pennsylvania border (in).
When you refer to a router, these terms have these meanings.

a) Out—Traffic that has already been through the router and leaves the interface. The source is where it has been, on the other side of the router, and the destination is where it goes.
b) In—Traffic that arrives on the interface and then goes through the router. The source is where it has been and the destination is where it goes, on the other side of the router.
c) Inbound —If the access list is inbound, when the router receives a packet, the Cisco IOS software checks the criteria statements of the access list for a match. If the packet is permitted, the software continues to process the packet. If the packet is denied, the software discards the packet.
d) Outbound—If the access list is outbound, after the software receives and routes a packet to the outbound interface, the software checks the criteria statements of the access list for a match. If the packet is permitted, the software transmits the packet. If the packet is denied, the software discards the packet.

The **in** ACL has a source on a segment of the interface to which it is applied and a destination off of any other interface. The **out** ACL has a source on a segment of any interface other than the interface to which it is applied and a destination off of the interface to which it is applied.

4. Procedure

1. Open Packet Tracer 5 and setup a network similar to the following network. Use Cisco 2950T switch & Cisco 2621XM router.



2. The different thing is the red link which is serial link (used for WAN). By default, it is not available so we have to add the modules to the router. Double click on any router. Turn it off by using power button on the router figure in **Physical** tab. On left side modules bar is present. Drag two **WIC-2T** to smaller blank space and one **NM-8A/S** to larger blank space. Now, turn on the router using power switch. Do the same on second router. Then use **Serial DTE** or **Serial DCE** link from **Connections**. The router interface that is chosen first becomes that of that type while the second one becomes the other e.g if you choose DTE and click first router, it becomes DTE while the second one becomes DCE and vice versa. Just remember that by default all serial interfaces are DTE so we have to provide clocking on the DCE one!

3. Use the following values to setup IP addresses on respective interfaces.

Router	Network Address	Interface	Address
Lab_A	192.168.10.0	fa0/0	192.168.10.1
Lab_A	192.168.20.0	s1/0	192.168.20.1
Lab_A	192.168.50.0	s1/1	192.168.50.1
Lab_B	192.168.30.0	fa0/0	192.168.30.1
Lab_B	192.168.20.0	s1/0	192.168.20.2
Lab_B	192.168.40.0	s1/1	192.168.40.1
Lab_C	192.168.60.0	fa0/0	192.168.60.1
Lab_C	192.168.40.0	s1/0	192.168.40.2
Lab_C	192.168.70.0	s1/1	192.168.70.1

A sample configuration is given as under

Router>**en**
Router#**config t**
Router(config)#**hostname Lab_A**
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 1/0**
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)#**interface serial 1/1**
Lab_A(config-if)#**ip address 192.168.50.1 255.255.255.0**
Lab_A(config-if)#**no shut**
Lab_A(config-if)#**exit**
Lab_A(config)#**banner motd #**
This is the Lab_A router
#
Lab_A(config)#**^z**
Lab_A#**copy running-config startup-config**
Destination filename [startup-config]? ***[Enter]***
Lab_A#

Before you jump in and configure a serial interface, there are a couple of things you need to know. First, the interface will usually be attached to a CSU/DSU type of device that provides clocking for the line to the router. But if you have a back-to-back configuration (for example, one that's used in a lab environment), one end—the data communication equipment (DCE) end of the cable—must provide clocking. By default, Cisco routers are all data terminal equipment (DTE) devices, so you must tell an interface to provide clocking if you need it to act like a DCE device.
To check the DCE interface, just bring your mouse over serial link, the interface with whose name you see a  (clock symbol) is the DCE one. You configure a DCE serial interface with the clock rate command:

Lab_B(config)#**interface serial 1/0**
Lab_B(config-if)#**clock rate ?**
<300-4000000> Choose clockrate from list above
Router(config-if)#**clock rate 64000**

Notice that the clock rate command is in bits per second.

Configure the PCs and Switches too. Make sure all devices are communicating with each other (use **ping** to verify).

Now you must have noticed that routers can communicate with devices directly connected to them. PC0-PC2 and Switch0 can communicate with Lab_A router & in between themselves but can't with Lab_B router and Switch1 & PC2-PC5 and vice versa.

Configure **Static** routing (see Lab 8) or **Dynamic** routing via RIP or OSPF (See Lab 9 or 10) so that all the nodes are communicating with each other.

4.1 Configuring Standard ACLs

Standard IP access lists filter network traffic by examining the source IP address in a packet.
You create a standard IP access list by using the access-list numbers 1–99 Access-list types are generally differentiated using a number. Based on the number used when the access list is created, the router knows which type of syntax to expect as the list is entered. By using numbers 1–99, you're telling the router that you want to create a standard IP access list, so the router will expect syntax specifying only the source IP address in the test lines.
Below is an example of the many access-list number ranges that you can use to filter traffic on your network (the protocols for which you can specify access lists depend on your IOS version):

```
Lab_A(config)#access-list ?
<1-99>      IP standard access list
<100-199> IP extended access list
```

Let's take a look at the syntax used when creating a standard access list:

```
Lab_A(config)#access-list 10 ?
deny    Specify packets to reject
permit  Specify packets to forward
remark  Access list entry comment
```

By using the access-list numbers between 1–99, you're telling the router that you want to create a standard IP access list. After you choose the access-list number, you need to decide whether you're creating a permit or deny statement. For this example, you will create a deny statement:

```
Lab_A(config)#access-list 10 deny ?
A.B.C.D  Address to match
any      Any source host
host     A single host address
```

The next step requires a more detailed explanation. There are three options available. You can use the **any** parameter to permit or deny any host or network; you can use an **IP address** to specify either a single host or a range of them; or you can use the **host** command to specify a specific host only. The **any** command is pretty obvious—any source address matches the statement, so every packet compared against this line will match. The host command is relatively simple. Here's an example using it:

```
Lab_A(config)#access-list 10 deny host 192.168.30.3
```

This tells the list to deny any packets from host 192.168.30.3. The default parameter is host. In other words, if you type **access-list 10 deny 192.168.30.3**, the router assumes you mean host 192.168.30.3. But there's another way to specify either a particular host or a range of hosts—you can use wildcard masking. In fact, to specify any range of hosts, you have to use wildcard masking in the access list.

4.1.1 Wildcard Masking

Wildcards are used with access lists to specify an individual host, a network, or a certain range of a network or networks. To understand a wildcard, you need to understand what a block size is; it's used to specify a range of addresses. Some of the different block sizes available are 64, 32, 16, 8, and 4.

When you need to specify a range of addresses, you choose the next-largest block size for your needs. For example, if you need to specify 34 networks, you need a block size of 64. If you want to specify 18 hosts, you need a block size of 32. If you only specify two networks, then a block size of 4 would work.

Wildcards are used with the host or network address to tell the router a range of available addresses to filter. To specify a host, the address would look like this:

192.168.30.3 0.0.0.0

The four zeros represent each octet of the address. Whenever a zero is present, it means that octet in the address must match exactly. To specify that an octet can be any value, the value of 255 is used. As an example, here's how a /24 subnet is specified with a wildcard:

192.168.30.0 0.0.0.255

This tells the router to match up the first three octets exactly, but the fourth octet can be any value.

4.1.2 A simple Example (Standard ACLs)

Consider you want to deny the whole **192.168.60.0** network and the host **192.168.30.3** to communicate with **192.168.10.0** network. You only need to use the following statements on **Lab_A** router.

Lab_A(config)#**access-list 10 deny 192.168.60.0 0.0.0.255**
Lab_A(config)#**access-list 10 deny 192.168.30.3**
Lab_A(config)#**access-list 10 permit any**

The last statement is used to prevent any other packet drop as default action of access lists is **deny.** Now you have to choose the outbound interface (i.e. **FastEthernet 0/0**) which is directly connected to **192.168.10.0** network or inbound interface (i.e. **Serial 1/0)** from which the packet has to enter the router **Lab_A**. (Any one would suffice)

Lab_A(config)#**interface serial 1/0**
Lab_A(config-if)# **ip access-group 10 in**

Or

Lab_A(config)#**interface fastEthernet 0/0**
Lab_A(config-if)# **ip access-group 10 out**

Now check using **Simulation** mode to see the result of your access list in a better way!

4.2 Configuring Extended ACLs

Standard ACLs allow us to make decisions based on source addresses but what if we want to a access a small part of the destination network e.g. Assume that **192.168.10.4** is a DNS server that is required by the source IPs that have been blocked. In this case, Standard ACLs will fail us so we use Extended ACLs which allow us to make decisions based on source and destination addresses. To use Extended ACLs, use access list numbers 100-199. The Extended ACLs also allow us to block any protocol's (Layer 3 and 4) traffic.

Now consider we want to allow our **192.168.60.0** network to access host **192.168.10.3** and deny all other host in the **192.168.10.0** network. Also we want our host **192.168.30.3** to access Switch0 (192.168.10.2) while not allowing it to access any other host in the **192.168.10.0** network. The following commands do the said task:

Lab_A(config)#**access-list 100 permit ip 192.168.60.0 0.0.0.255 host 192.168.10.3**
Lab_A(config)#**access-list 100 permit ip host 192.168.30.3 host 192.168.10.2**
Lab_A(config)#**access-list 100 deny ip 192.168.60.0 0.0.0.255 any**
Lab_A(config)#**access-list 100 deny ip host 192.168.30.3 any**
Lab_A(config)#**access-list 100 permit ip any any**

The last statement just changes the default action of access list from **deny** to **permit.** Now you have to choose the outbound interface (i.e. **FastEthernet 0/0**) which is directly connected to **192.168.10.0** network or inbound interface (i.e. **Serial 1/0)** from which the packet has to enter the router **Lab_A**. (Any one would suffice)

Lab_A(config)#**interface serial 1/0**
Lab_A(config-if)# **ip access-group 100 in**

Or

Lab_A(config)#**interface fastEthernet 0/0**
Lab_A(config-if)# **ip access-group 100 out**

Now check using **Simulation** mode to see the result of your access list in a better way!

Always remember that the ACLs run sequentially so order is very important so if you write in order other than mentioned above then the results would be different!

4.3 Configuring Named ACLs

The named ACLs are not represented by a number but by a name that is given by the user. They behave the same way as standard or extended ACLs but have a name instead of a number.

Lab_A(config)#**ip access-list ?**
extended Extended Access List
standard Standard Access List

The difference is obvious; we have used **ip access-list** instead of **access-list**.

To do the task done in **4.1 (Standard ACLs)** using named ACLs, we use the following commands:

Lab_A(config)#**ip access-list standard Part_4.1**
Lab_A(config-std-nacl)#**deny 192.168.60.0 0.0.0.255**
Lab_A(config-std-nacl)#**deny 192.168.30.3**
Lab_A(config-std-nacl)#**permit any**

Lab_A(config)#**interface serial 1/0**
Lab_A(config-if)# **ip access-group Part_4.1 in**

Or

Lab_A(config)#**interface fastEthernet 0/0**
Lab_A(config-if)# **ip access-group Part_4.1 out**

To do the task done in **4.2 (Extended ACLs)** using named ACLs, we use the following commands:

Lab_A(config)#**ip access-list extended Part_4.2**
Lab_A(config-ext-nacl)#**permit ip 192.168.60.0 0.0.0.255 host 192.168.10.3**
Lab_A(config-ext-nacl)#**permit ip host 192.168.30.3 host 192.168.10.2**
Lab_A(config-ext-nacl)#**deny ip 192.168.60.0 0.0.0.255 any**
Lab_A(config-ext-nacl)#**deny ip host 192.168.30.3 any**
Lab_A(config-ext-nacl)#**permit ip any any**

Lab_A(config)#**interface serial 1/0**
Lab_A(config-if)# **ip access-group Part_4.2 in**

Or

Lab_A(config)#**interface fastEthernet 0/0**
Lab_A(config-if)# **ip access-group Part_4.2 out**

Now check using **Simulation** mode to see the result of your access list in a better way!

4.4 Verifying the Access List Configurations
Use the command **show access-lists** to see the access list configurations.
Lab_A#**show access-lists**
Standard IP access list 10
    deny 192.168.60.0 0.0.0.255
    deny host 192.168.30.3
    permit any (12 match(es))

International Islamic University, Islamabad
Computer Networks Lab

LAB WORKSHEET (Lab # 11)

Q.1 What is an **ACL** and what are its advantages?

Q.2 What is the main difference between **Standard** ACLs & **Extended** ACLs?

Q.3 What is the advantage of using **Named ACLs**?

Q.4 Which command is used to see **ACL** configurations?