Ahsanullah University of Science and Technology (AUST)
Department of Computer Science and Engineering

LABORATORY MANUAL

Course No. : CSE4102
Course Title: Computer Networks Lab

For the students of 4th Year, 1st semester of
B.Sc. in Computer Science and Engineering program

TABLE OF CONTENTS

COURSE OBJECTIVES

This course is designed to provide computer science and engineering undergraduates with basic understanding of the design, troubleshooting modeling and evaluation of computer networks. In this course, students are going to experiment in a real test-bed networking environment, and learn about network design and troubleshooting topics and tools such as: network addressing, basic troubleshooting tools (e.g. ping, ICMP), IP routing, route discovery. Student will also be introduced to the network modeling and simulation, and they will have the opportunity to build some simple networking models using the tool and perform simulations that will help them evaluate their design approaches and expected network performance.

PREFFERED TOOL(S)

- Packet Tracer

TEXT/REFERENCE BOOK(S)

- "Data Communications and Networking**"**, by 'Behrouz A. Forouzan'**,** Published by Mc-Graw Hill, 4th edition.
- "CCNA Study Guide" written by "Todd Lammle", Publisher: BPB Publications.

ADMINISTRATIVE POLICY OF THE LABORATORY

- ✓ Students must be performed class assessment tasks individually without help of others.
- ✓ Students must be prepared for the online prior to the class.
- ✓ Viva for each task will be taken and considered as a performance.
- ✓ Plagiarism is strictly forbidden and will be dealt with punishment.

Session 1: Building a Local Area Network

Objectives

1. To learn basics of Local Area Network (LAN)
2. Understand different types of LAN devices
3. To learn procedure to make Unshielded Twisted-Pair (UTP) cable

Description

What is a LAN?

A LAN is a high-speed data network that covers a relatively small geographic area. It typically connects workstations, personal computers, printers, servers, and other devices. LANs offer computer users many advantages, including shared access to devices and applications, file exchange between connected users, and communication between users via electronic mail and other applications.

LAN Protocols and the OSI Reference Model

LAN protocols function at the lowest two layers of the OSI reference model i.e. between the physical layer and the data link layer. Figure 1 illustrates how several popular LAN protocols map to the OSI reference model.

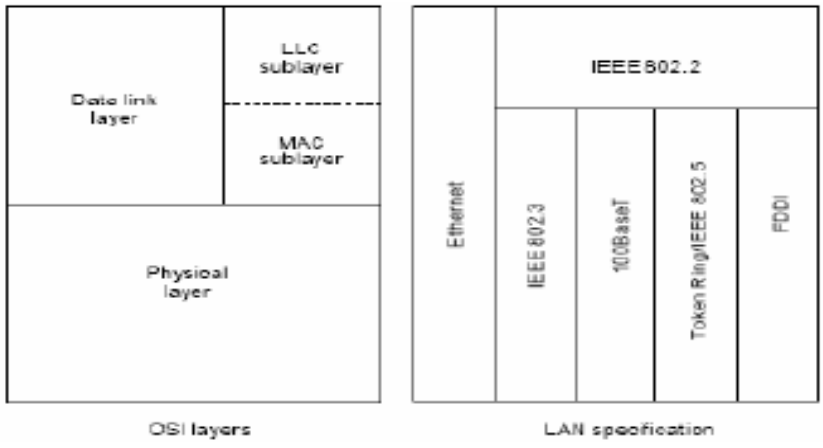


Figure 1*:* Popular LAN Protocols Mapped to the OSI Reference Model

LAN Devices:

1. **NIC (Network Interface Card):** Also called Network Adapter. It connects a host to a network medium. It provides the physical interface between computer and cabling. It prepares data, sends data, and controls the flow of data. It can also receive and translate data into bytes for the CPU to understand. Contain unique MAC Address to control data communication.

2. **Repeater:** Functioning at Physical Layer. A **repeater** is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or on to the other side of an obstruction, so that the signal can cover longer distances. Repeater have two ports, so cannot be use to connect for more than two devices.

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

4. **Switch:** A **network switch** or **switching hub** is a computer networking device that connects network segments. The term commonly refers to a network bridge that processes and routes data at the Data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.

5. **Bridge:** A **network bridge** connects multiple network segments at the data link layer (Layer 2) of the OSI model. In Ethernet networks, the term *bridge* formally means a device that behaves according to the IEEE802.1 standard. A bridge and switch are very much alike; a switch being a bridge with numerous ports. Bridges can analyze incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.

6. **Router:** A **router** is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another. Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.

7. **Gate Way:** A **gateway** is a hardware device that acts as a "gate" between two networks. A gate way may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability.

UTP Cable Construction:

1. **Cross Over Cable:** Diagram shows how to prepare Cross Over Connection.

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

2. **Straight Through Cable:** Diagram shows how to prepare Straight Through Connection.

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #1
1	White/Orange		1	White/Orange	
2	Orange		2	Orange	
3	White/Green		3	White/Green	
4	Blue		4	Blue	
5	White/Blue		5	White/Blue	
6	Green		6	Green	
7	White/Brown		7	White/Brown	
8	Brown		8	Brown	

Session 2: Concept of Network IP Address (Part-1)

Objectives:

1. Study of Class full IP Addressing
2. To learn Classes, Blocks and Masking

Description

IP Addressing v4: The identifier used in network layer to identify each device connected to the Internet is called the Internet address or IP address**.**

Rules for Class full addressing:

1. Format of IP address IPv4 is made up of four parts, in the pattern as w.x.y.z. Each part has 8 binary bits and the values in decimal can range from 0 to 255.
2. IP addresses are divided into different classes. These classes determine the maximum number of hosts per network ID. Only three classes are actually used for network connectivity. The following table lists all of the address class.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved.

3. Grouping of IP addresses into different classes.
   a) Class A, B, C, D, E
   b) Class A: first bit in w is 0 and others can be anything
      i. 0.0.0.0 to 127.255.255.255
      ii. First bits are used for network part and the remaining for host part.
   c) Class B: First bit in w is 1 and second bit is 0.
      i. 128.0.0.0 to 191.255.255.255
      ii. First 16 bits for network part and remaining host part
   d) Class C: first bit in w is 1, second bit in w is 1 and third bit is 0

i. 192.0.0.0 to 223.255.255.255

ii. First 24 bits for network part and last 8 bits for host part.

e) Class D: first, second, third bits in w are 1 and fourth bit is 0; used for multicast.

i. 224.0.0.0 to 247.255.255.255

f) Class E: future use or experimental purposes.

4. Default Subnet mask it is used to identify the network part from the host part. Put binary one for the parts that represent network part and zero for the part that represent host part.

a) Class A: 255.0.0.0

b) Class B: 255.255.0.0

c) Class C: 255.255.255.0

d) We can't have mix of 1s and 0s in subnet mask. Only consecutive 1s is followed by consecutive 0s.

Session 3: Concept of Network IP Address (Part-2)

Objectives

1. Study of Classless IP Addressing
2. To learn the concept of Sub netting and Super netting

Description

Why Class less Addressing?

To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented. In this scheme, there are no classes, but the addresses are still granted in blocks.

Rules for Class less addressing

1. Format of **Class less** is made up of **variable-length block with** the slash notation **A.B.C.D/n.** Slash notation **n** is also called CIDR (Class less Interdomain Routing) notation/prefix length represented using '1', as masking.
2. The addresses in a block must be contiguous, one after another.
3. The number of addresses in a block must be a power of 2 (1, 2, 4, 8, ...).
4. The first address must be evenly divisible by the number of addresses.

Subnetting

A network is divided into several smaller networks. Each smaller network is called a **Subnetwork** or a **Subnet**. The following topics will be discussed:

1. Why we Develop Subnetting?
2. How to calculate Subnet mask?
3. How to identify Subnet address?

Supernetting

In Supernetting, an organisation can combine several class C blocks to create a large range of addresses. The following topics will be discussed:

1. Why we Develop Supernetting?
2. How to calculate Supernet mask?
3. How to identify Supernet address?

Session 4: Introduction to Network Simulator – Packet Tracer

Objectives

1. Introduction to Packet Tracer Interface
2. To learn how to use different components and build a simple network

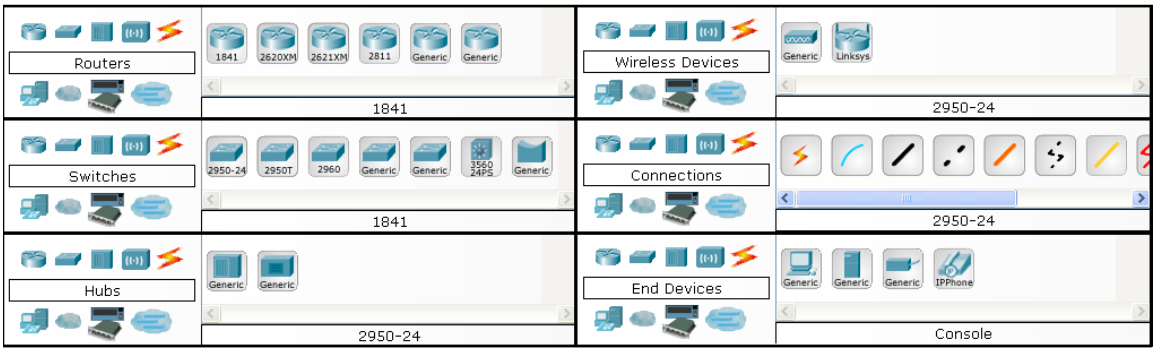
Description

Packet Tracer is a protocol simulator developed by Dennis Frezzo and his team at Cisco Systems. Packet Tracer (PT) is a powerful and dynamic tool that displays the various protocols used in networking, in either Real Time or Simulation mode.

Packet Tracer Interface and how to create a topology

Step 1: Start Packet Tracer and Enter into Simulation Mode

Step 2: Choose Devices and Connections



Step 3: Building the Topology – Adding Hosts in following way:

- Single click on the End Devices.
- Single click on the Generic host.
- Move the cursor into topology area. You will notice it turns into a plus "+" sign. Single click in the topology area and it copies the device.

Step 4: Building the Topology – Connecting the Hosts to Hubs and Switches

- Adding a Hub or Switch: Select a hub or a switch by clicking once on Hubs/Switches and once on a Generic hub/Switch.

- Connect Host to Hub/Switch by first choosing Connections.
- Click once on the Copper Straight-through cable.

Step 5: Configuring IP Addresses and Subnet Masks on the Hosts

- Click once on PC0.
- Choose the Config tab.
- Click on FastEthernet.
- Enter IP address and Subnet Mask.

Exercises

1. Design a topology using 4 PC and a Switch with following IP address:

Host	IP Address	Subnet Mask
PC0	192.68.1.10	255.255.255.0
PC1	192.68.1.11	255.255.255.0
PC2	192.68.1.12	255.255.255.0
PC3	192.68.1.13	255.255.255.0

2. Observe the flow of data from host to host by creating network traffic.

Session 5: Configuration of a Router using Packet Tracer

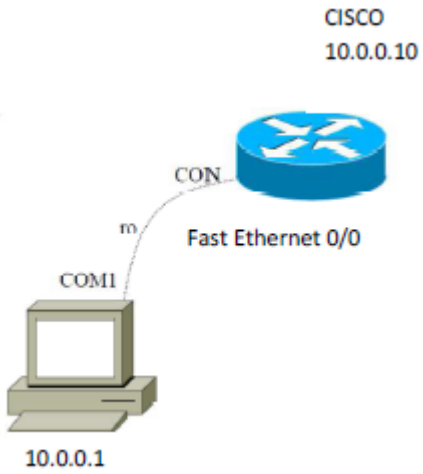
Objectives

1. Understanding basic networking commands
2. Configuring the Router configuration commands

Description

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

Problem 1: Procedure to configure a Router with the PC



1. Get a Consol Cable
2. Plug the serial end into the back of the computer
3. Put the RJ-45 into the consol port of Router.
4. Get a terminal program
    - Hyperterminal
    - Tera term
    - Minicom
    - Securecrt

5. Set it to connect via com port with

    Baud rate=9600

Data bits=8

Parity=None

Stop bits=1

Flow Control:None

Configure IP Address on Fast Ethernet 0/1:..

Router(config)# hostname CISCO

CISCO(config)# int fastEthernet 0/1

CISCO(config-if)# ip address 10.0.0.10 255.0.0.0

CISCO(config-if)# no shutdown

Problem 2: Configure Serial Connectivity between two routers

R1(config)# interface serial 0

R1(config-if)# ip address 15.0.0.1 255.0.0.0

R1(config-if)# no shutdown

R1(config-if)# clock rate 64000 (Clock Rate will set only DCE Interface)

R1(config-if)# end

ping: ***ping dest_ip_address***

ping sends an ICMP ECHO_REQUEST packet to the specified host. If the host responds, you get an ICMP packet back.

Traceroute: ***tracert dest_ip_address***

Tracert is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded.

Session 6: Implementation of a Network using Packet Tracer

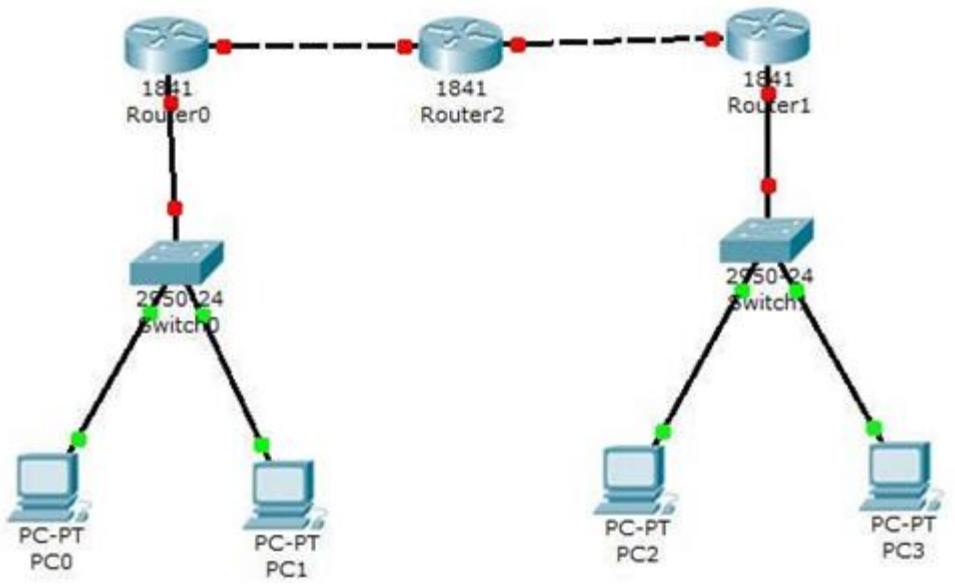
Objectives

1. To learn how to create a network topology in PT
2. To learn how to configure a network topology using command mode

Procedure

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

Topology



Router0 Configuration Command:.....

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

Rout>Enable
Router#config terminal

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

```
Router(config)#hostname router0
router0(config)#interface fastethernet 0/0

router0(config-if)#ip address 192.168.1.1 255.255.255.0
router0(config-if)#description router0 fastethernet 0/0
router0(config-if)#no shutdown
router0(config-if)#exit

router0(config)#interface fastethernet 0/1
router0(config-if)#description router0 fastethernet 0/1
router0(config-if)#no shutdown

router0(config-if)#exit
router0(config)#exit

router0#show running-config

router0#copy running-config startup-config
Destination filename[startup-config]?
Building configuration...[OK]
router0#
```

Exercise

1. Configure PC0 and PC1 with following IP address and Subnet Mask.

Host	IP Address	Subnet Mask
PC0	192.168.1.10	255.255.255.0
PC1	192.168.1.11	255.255.255.0

2. Use ping command to verify the connection from PC0 to PC1.

3. Do the same procedure for Router1, PC2 and PC3 with following IP. Check the connection from PC2 to PC3 using ping command.

Host	IP Address	Subnet Mask
Router1	192.168.2.1	255.255.255.0
PC2	192.168.2.10	255.255.255.0
PC3	192.168.2.11	255.255.255.0

Session 7: Implementation of Static Routing using PT

Objectives

1. To learn how to configure a topology with Static Routing Protocol
2. Test and verify the configuration

Description

Static Routing:
A router can learn about remote networks in one of two ways:

1. Manually, from configured static routes
2. Automatically, from a dynamic routing protocol

Static routes are commonly used when routing from a network to a stub network. A stub network is a network accessed by a single route.

The ip route command:
The command for configuring a static route is ip route. The complete syntax for configuring a static route is:

Router(config)#ip route network-address subnet-mask {ip-address | exit-interface }

The following parameters are used:

- *network-address* - Destination network address of the remote network to be added to the routing table
- *subnet-mask* - Subnet mask of the remote network to be added to the routing table. The subnet mask can be modified to summarize a group of networks.

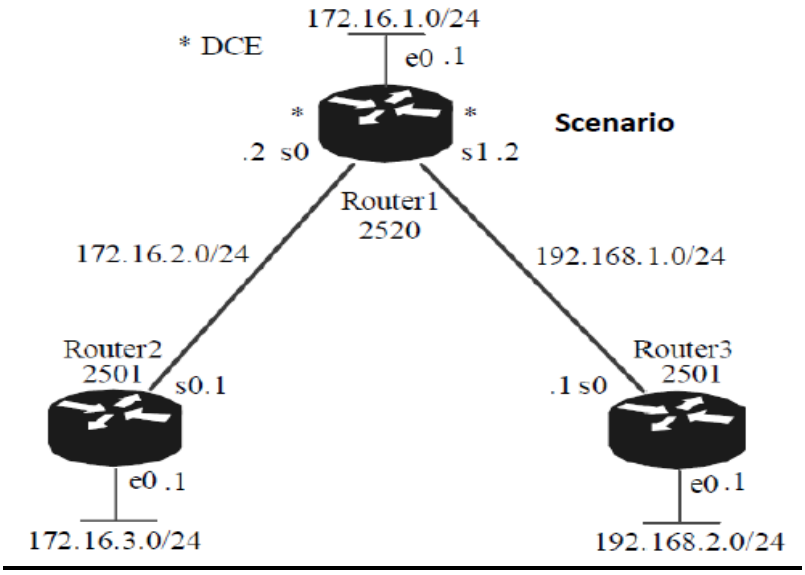
One or both of the following parameters must also be used:

- *ip-address* - Commonly referred to as the next-hop router's IP address
- *Exit-interface* - Outgoing interface that would be used in forwarding packets to the destination network.

Procedure

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

Topology



Router1 Configuration Command

```
Router1>en
Router1#config t
Router1(config)#interface f0/0
Router1(config-if)#ip address 172.16.1.1 255.255.255.0
Router1(config-if)#no shut
Router1(config-if)#interface s2/0
Router1(config-if)#ip address 172.16.2.2 255.255.255.0
Router1(config-if)#no shut
Router1(config-if)#interface s3/0
Router1(config-if)#clock rate 64000
Router1(config-if)#ip address 192.168.1.2 255.255.255.0
Router1(config-if)#no shut
Router1(config-if)#exit
Router1(config)#exit
Router1#copy run start
Router1#config t
Router1(config)#ip route 172.16.3.0 255.255.255.0 172.16.2.1
```

```
Router1(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.1
Router1(config)#exit
Router1#copy run start
```

Verify Router1 configuration command:

Router#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B – BGPD - EIGRP, EX – EIGRP external, O - OSPF, IA – OSPF inter area, N1 – OSPF NSSA external type1, N2 – OSPF NSSA external type2, E1 – OSPF external type1, E2 – OSPF external type2, E – EGP, I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area.
*-candidate default, U - per-user static route, o – ODR, P – periodic downloaded static route

Gateway of last resort is not set

C 172.16.1.1/24 is directly connected, FastEthernet 0/0
C 172.16.2.2/24 is directly connected, Serial 2/0
C 192.168.1.2/24 is directly connected, Serial 3/0
S 172.16.3.0/24 [1/0] via 172.16.2.1
S 192.168.2.0/24 [1/0] via 192.168.1.1

Exercises

1. Configure Router2 and Router3 with their respective IP address and also apply static command.
2. Verify your configuration by using the command – *Router# show ip route*
3. Add a PC with each of the router and configure them with their respective IP.
4. Test the connectivity from any one PC to other by using *ping* command.

Session 8: Implementation of RIP using Packet Tracer

Objectives

1. To learn how to configure a topology with RIP
2. Test and verify the configuration

Description

The Routing Information Protocol (RIP) is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. Originally each RIP router transmitted full updates every 30 seconds.

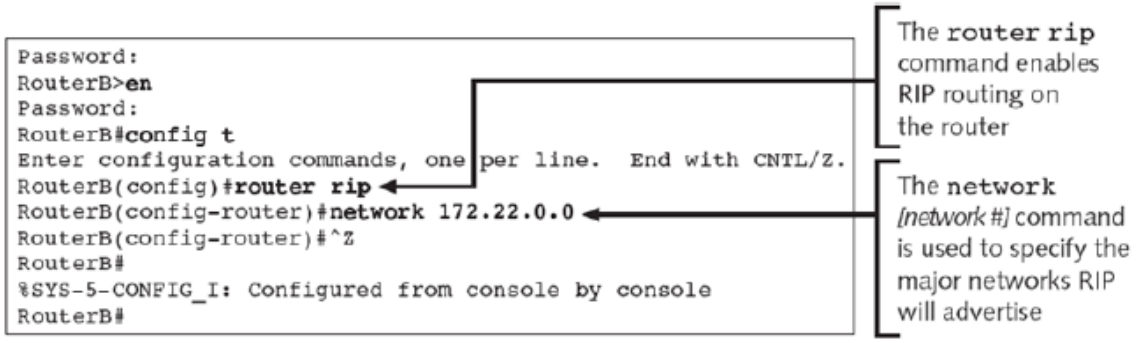
RIP versions:

- RIP version 1
  The original specification of RIP uses Classful routing. The periodic routing updates do not carry subnet information, lacking support for variable length subnet masks (VLSM). In other words, all subnets in a network class must have the same size.

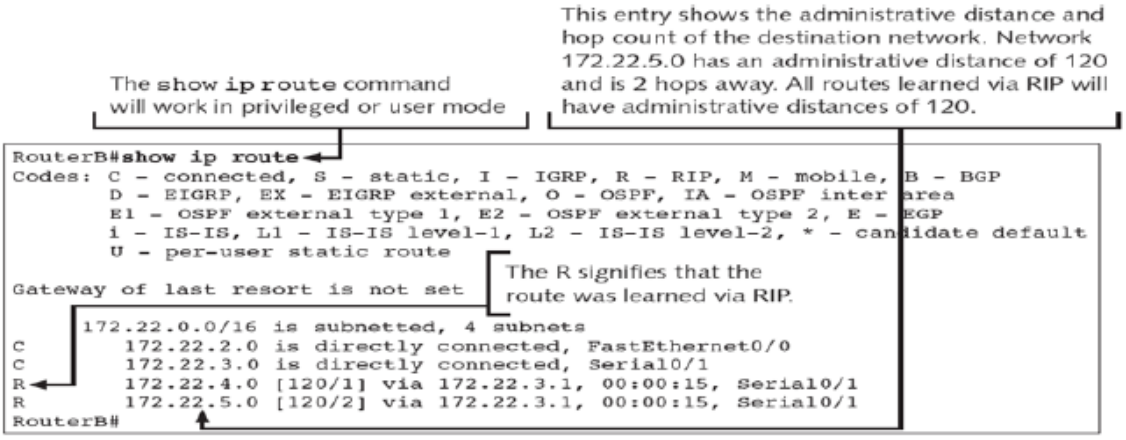
- RIP version 2
  Due to the deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed. It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR).

Enabling RIP on a Cisco router:

RIP can be enabled on a Cisco router by entering router configuration mode from configuration mode. You must be in exec mode to perform the following commands:

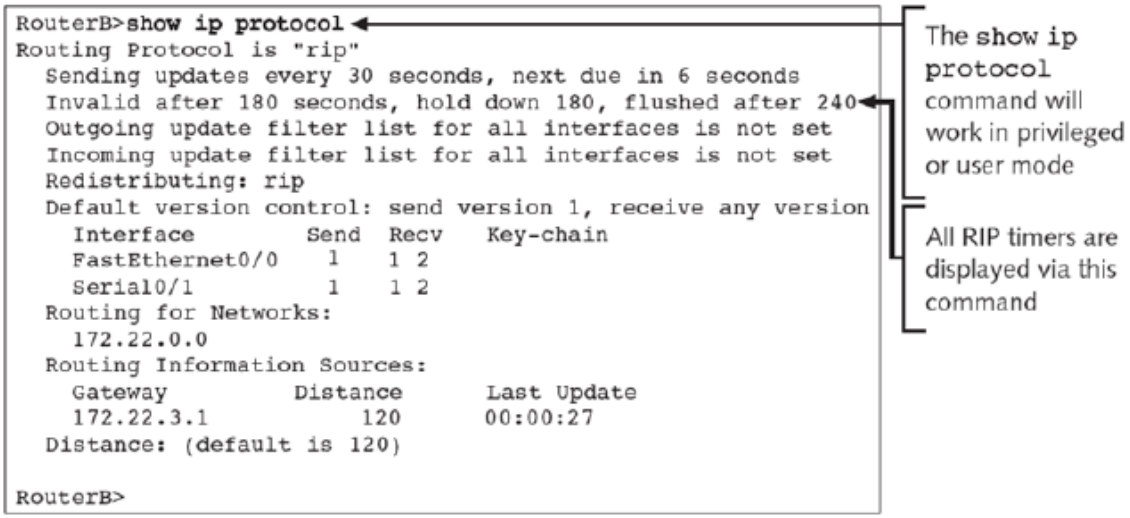


After configuring rip, we can discover routing table by show ip route command:



Commands used to monitor RIP

- Show ip protocol



Exercises

1. Consider the topology of **Lab no 7**, configure RIP on all the Router.
2. Test the connectivity by using *ping* command from any one PC to other.
3. Verify the configuration by using the above mentioned command.

Session 9: Implementation of OSPF using Packet Tracer

Objectives

1. To learn how to configure a topology with OSPF
2. Test and verify the configuration

Description

Open Shortest Path First (OSPF):
OSPF is a link-state routing protocol that was developed as a replacement for the distance vector routing protocol RIP. RIP was an acceptable routing protocol in the early days of networking and the Internet, but its reliance on hop count as the only measure for choosing the best route quickly became unacceptable in larger networks that needed a more robust routing solution. OSPF is a classless routing protocol that uses the concept of areas for scalability.

The router OSPF command:
OSPF is enabled with the following global configuration command.

router ospf process-id

The process-id is a number between 1 and 65535 and is chosen by the network administrator.

The network command:
The OSPF network command uses a combination of network-address and wildcard-mask. The network command is used in router configuration mode.

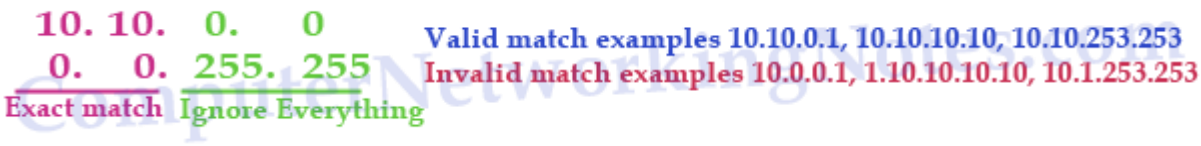
Router(config-router)#network network-address wildcard-mask area area-id

The network address along with the wildcard mask is used to specify the interface or range of interfaces that will be enabled for OSPF using this network command.

The wildcard mask can be configured as the inverse of a subnet mask. Key points:

- 0 (Decimal – octet format) Wildcard mask indicates that corresponding octet in network address must be matched exactly.
- 255 (Decimal – octet format) Wildcard mask indicates that we don't care about corresponding octet in network address.

For example



The area area-id refers to the OSPF area. An OSPF area is a group of routers that share link-state information.

Verifying OSPF configuration

Some powerful OSPF troubleshooting commands include:

#show ip ospf neighbor
#show ip protocols
#show ip ospf
#show ip ospf interface

Exercises

1. Consider the topology of **Lab no 7**, configure OSPF on all the Router.
2. Test the connectivity by using *ping* command from any one PC to other.
3. Verify the configuration by using the above mentioned command.

Session 10: Implementation of EIGRP using Packet Tracer

Objectives

1. To learn how to configure a topology with EIGRP
2. Test and verify the configuration

Description

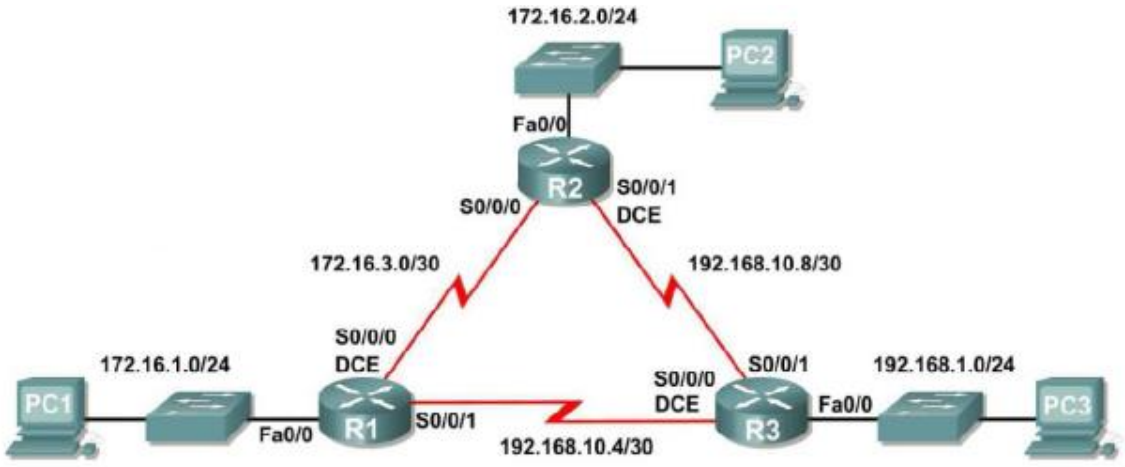
Enhanced Interior Gateway Routing Protocol:

EIGRP is considered an advanced distance-vector routing algorithm, since it uses both the characteristics of distance-vector and link-state, it is really considered a hybrid routing protocol with optimizations to minimize both the routing instability incurred after topology changes, as well as the use of bandwidth and processing power in the router.

Procedure

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

Topology



Configure EIGRP on the R1 Router:

Step 1: Enable EIGRP

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

R1(config)#**router eigrp 1**

Step 2: Configure classful network 172.16.0.0.

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

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

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

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

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

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

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

Exercises:

1. Configure EIGRP on the R2 and R3 Routers.
2. Verify EIGRP operation with the ***show ip eigrp neighbors*** and ***show ip protocols*** commands.
3. Examine EIGRP Routes in the Routing Tables using ***show ip route*** command.

Session 11: Implementation of VLAN using Packet Tracer

Objectives

1. To perform basic configuration tasks on a switch
2. Create VLAN and assign switch ports to a VLAN
3. Test and verify the configuration

Description

Virtual LAN:

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

Procedure

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

Topology

Task 1: Prepare the Network

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

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

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

```
Switch#config term
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range gi0/1-2
Switch(config-if-range)#shutdown
```

Task 2: Perform Basic Switch Configurations

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

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

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

```
S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#switchport mode access
S2(config-if-range)#no shutdown
S3(config)#interface range fa0/6, fa0/11, fa0/18
S3(config-if-range)#switchport mode access
S3(config-if-range)#no shutdown
```

Task 3: Configure and Activate Ethernet Interfaces

Step 1: Configure the PCs.

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

Task 4: Configure VLANs on the Switch

Step 1: Create VLANs on switch S1.

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

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

S1#

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

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

S1#**show vlan brief**

Exercise

1. Create and name VLANs 10, 20, 30, and 99 on S2 and S3 using the commands from Task 4 and Step 1. Verify the correct configuration with the **show vlan brief** command.
2. What ports are currently assigned to the four VLANs you have created?

MID TERM EXAMINATION

There will be a 40-minutes written mid-term examination. Different types of questions will be included such as MCQ, mathematics, writing code fragments etc.

FINAL TERM EXAMINATION

There will be a one-hour written examination. Different types of questions will be included such as MCQ, mathematics, simulate network topology etc.

MID TERM EXAMINATION

There will be a 40-minutes written mid-term examination. Different types of questions will be included such as MCQ, mathematics, writing code fragments etc.

FINAL TERM EXAMINATION

There will be a one-hour written examination. Different types of questions will be included such as MCQ, mathematics, write a program etc.