Ahsanullah University of Science and Technology (AUST)

Department of Computer Science and Engineering

LABORATORY MANUAL

Course No.: CSE3202

Course Title: Introduction to Computer Networks Lab

For the students of 3rd Year, 2nd semester of
B.Sc. in Computer Science and Engineering program

Local Area Network

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.

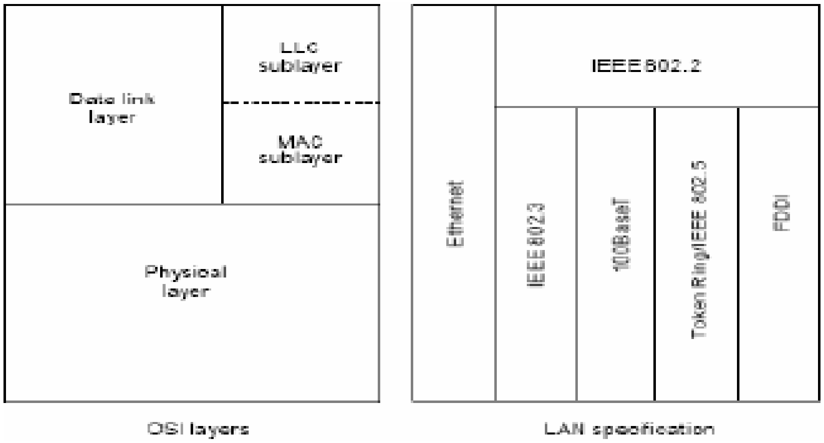


Figure 1: Popular LAN Protocols Mapped to the OSI Reference Model

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.

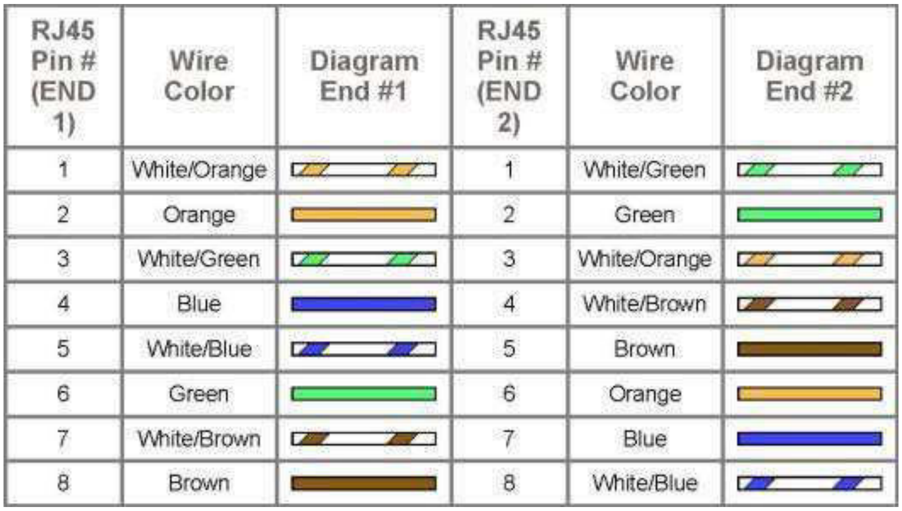
5. **Bridge:** A **network bridge** connects multiple network segments at the data link layer (Layer 2) of the OSI model. In Ethernet networks, the term *bridge* formally means a device that behaves according to the IEEE802.1 standard. A bridge and switch are very much alike; a switch being a bridge 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.

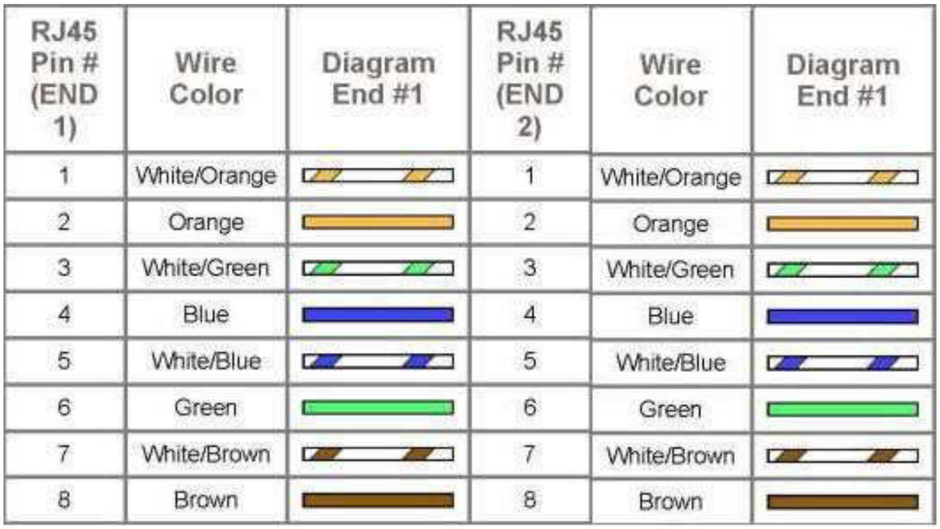
UTP Cable Construction:

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	🟫

Concept of Network 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.

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.

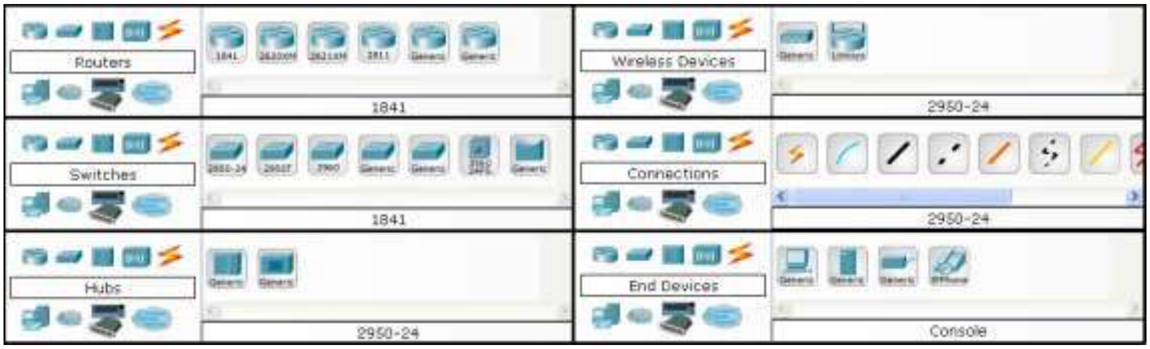
Introduction to Packet Tracer

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.

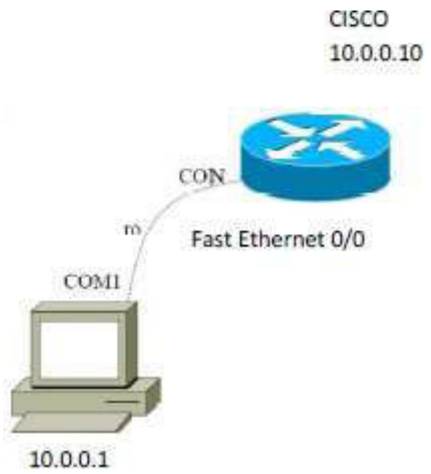
- Connect Host to Hub/Switch by first choosing Connections.
- Click once on the Copper Straight-through cable.

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.

Configuration of a Router using Packet Tracer

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

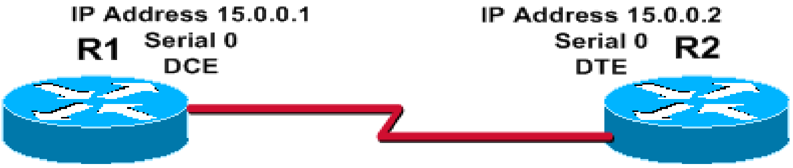
Stop bits=1

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***

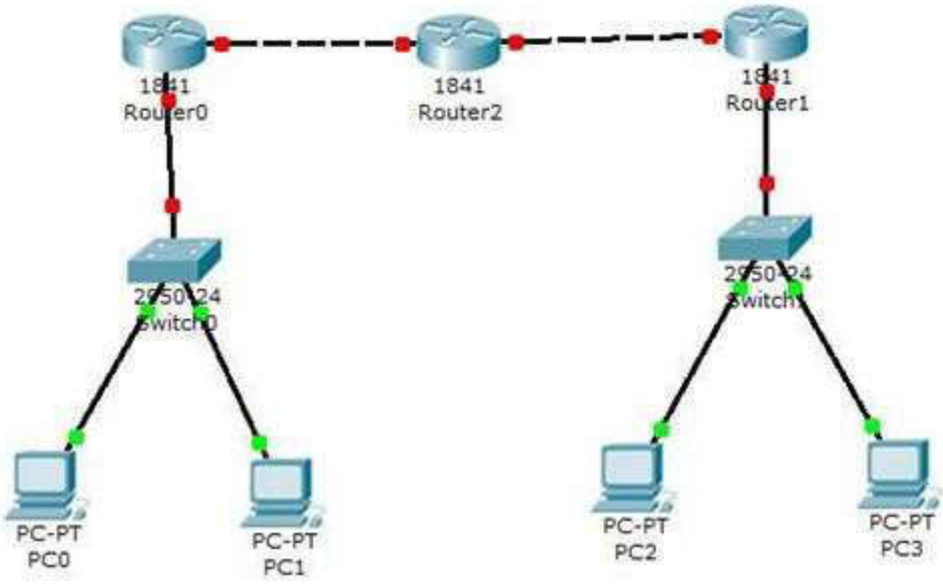
Tracert is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded.

Implementation of a Network using Packet Tracer

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#
```

Implementation of Static Routing using PT

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.

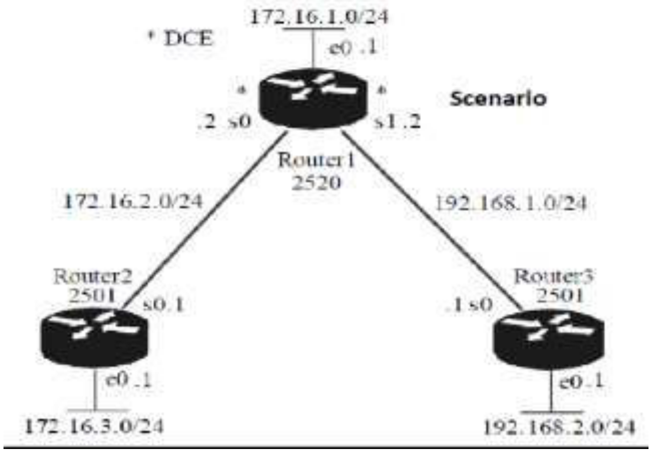
One or both of the following parameters must also be used:

- *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
```

Implementation of RIP using Packet Tracer

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.

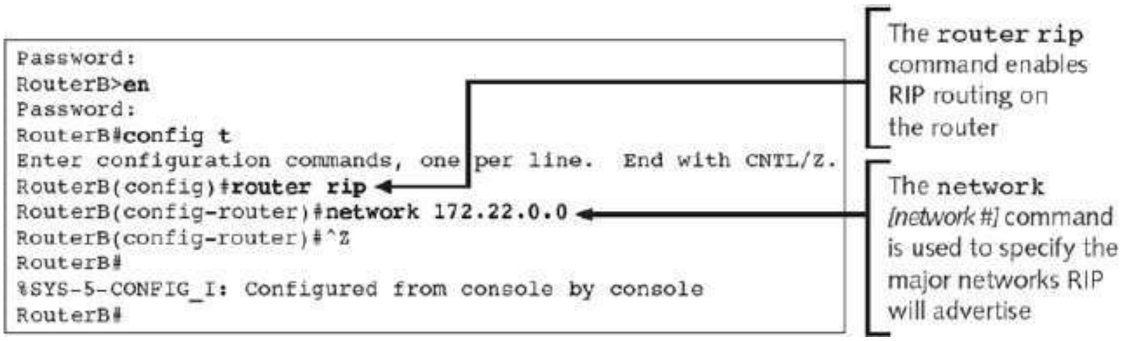
RIP versions:

- 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:

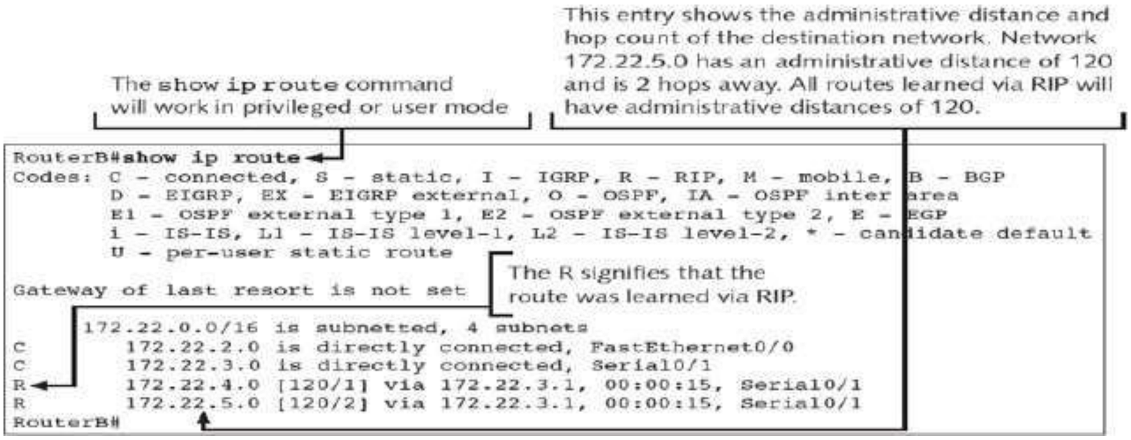


```
Password:
RouterB>en
Password:
RouterB#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RouterB(config)#router rip
RouterB(config-router)#network 172.22.0.0
RouterB(config-router)#^Z
RouterB#
%SYS-5-CONFIG_I: Configured from console by console
RouterB#
```

The **router rip** command enables RIP routing on the router

The **network** *[network #]* command is used to specify the major networks RIP will advertise

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



This entry shows the administrative distance and hop count of the destination network. Network 172.22.5.0 has an administrative distance of 120 and is 2 hops away. All routes learned via RIP will have administrative distances of 120.

The show ip route command will work in privileged or user mode

The R signifies that the route was learned via RIP.

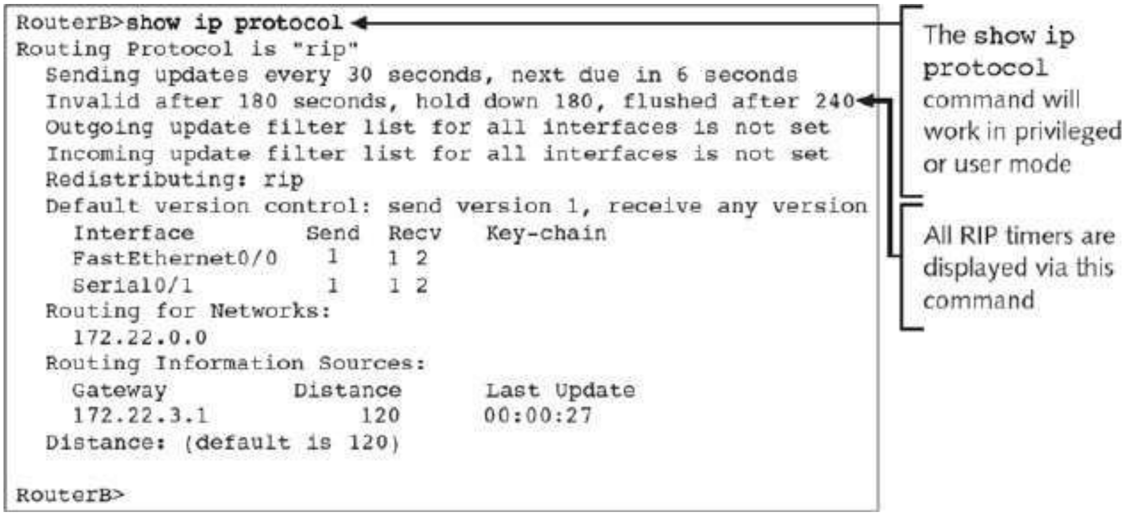
```
RouterB#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate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

Gateway of last resort is not set

     172.22.0.0/16 is subnetted, 4 subnets
C       172.22.2.0 is directly connected, FastEthernet0/0
C       172.22.3.0 is directly connected, Serial0/1
R       172.22.4.0 [120/1] via 172.22.3.1, 00:00:15, Serial0/1
R       172.22.5.0 [120/2] via 172.22.3.1, 00:00:15, Serial0/1
RouterB#
```

Commands used to monitor RIP

- Show ip protocol



```
RouterB>show ip protocol
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 6 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface         Send  Recv   Key-chain
    FastEthernet0/0    1    1 2
    Serial0/1          1    1 2
  Routing for Networks:
    172.22.0.0
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.22.3.1            120      00:00:27
  Distance: (default is 120)

RouterB>
```

The show ip protocol command will work in privileged or user mode

All RIP timers are displayed via this command

Implementation of OSPF using Packet Tracer

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.

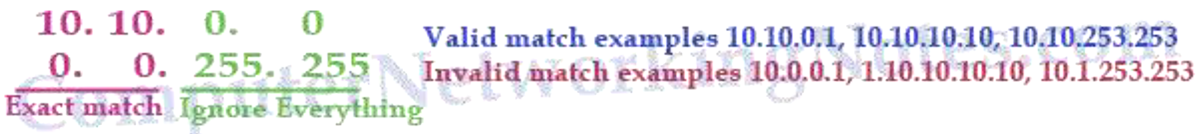
Router(config-router)#network network-address wildcard-mask area area-id

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


10. 10. 0. 0
0. 0. 255. 255
Exact match
Ignore Everything
Valid match examples 10.10.0.1, 10.10.10.10, 10.10.253.253
Invalid match examples 10.0.0.1, 1.10.10.10.10, 10.1.253.253

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

Implementation of EIGRP using Packet Tracer

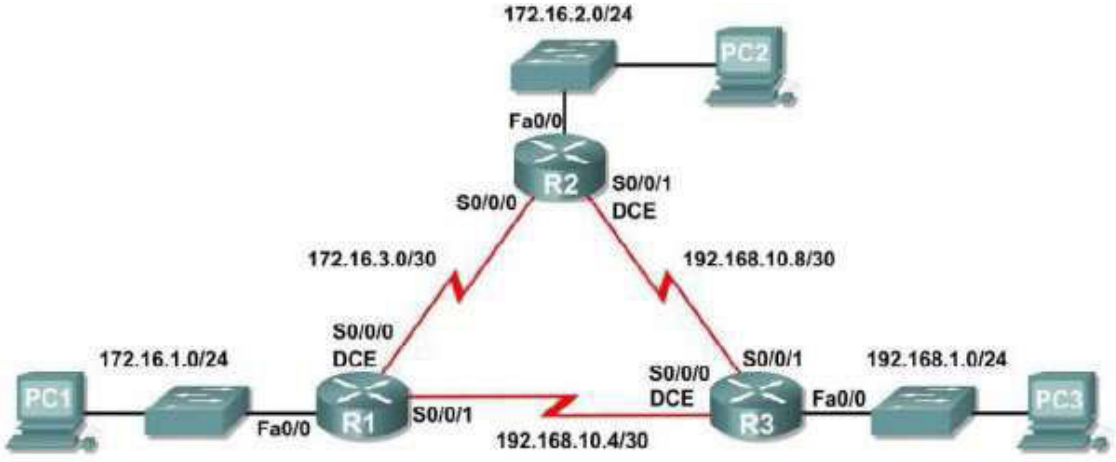
Enhanced Interior Gateway Routing Protocol:

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.