National University of Computer & Emerging Sciences, Karachi
FAST School of Computing
Fall 2021, Lab Manual 10

Course Code: CL-3001	Course: Computer Networks Lab
Instructor(s):	**Amin Sadiq, Muhammad Kariz Kamal**

Contents:

1. Routing Protocol and Routed Protocol

You must understand the difference between a routing protocol and a routed protocol. A routing protocol is used by routers to dynamically find all the networks in the internetwork and to ensure that all routers have the same routing table. Basically, a routing protocol determines the path of a packet through an internetwork.

Examples of routing protocols are RIP, RIPv2, EIGRP, and OSPF.

Once all routers know about all networks, a routed protocol can be used to send user data (packets) through the established enterprise. Routed protocols are assigned to an interface and determine the method of packet delivery.

Examples of routed protocols are IP and IPv6.

2. What is Routing Basis?

The term *routing* is used for taking a packet from one device and sending it through the network to another device on a different network. Routers do not really care about hosts - they only care about networks and the best path to each network.

The logical network address of the destination host is used to get packets to a network through a routed network, and then the hardware address of the host is used to deliver the packet from a router to the correct destination host.

If a network is not directly connected to the router, then the router must use one of two ways to learn how to get to the remote network: **static routing**, meaning that someone must hand-type all network locations into the routing table, or something called **dynamic routing**

3. Introduction to 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 is true for all routing processes. Static routing has the following benefits:

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

Static routing has the following disadvantages:

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

4. 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 should only use default routing on stub networks—those with only one exit path out of the network.

Configuring Routes on Cisco Router

Using Cisco Packet Tracer software, we simulate the following network mentioned in figure 1 which has 4 networks and 10 subnetworks and assign each host an IP. Also we have to assign an IP for each interface on the router. We assign an IP for the Router interface and start it up using the following commands:

Router(config)#interface fa0/0
Router(config-if)#ip address 192.168.1.129 255.255.255.192
Router(config-if)#no shutdown

Where:
fa0/0: is the name of the interface.
192.168.1.129: is the IP address for interface fa0/0.
255.255.255.192: is the subnet mask being used on the network that connected directly to the interface.
no shutdown: to start up the interface.

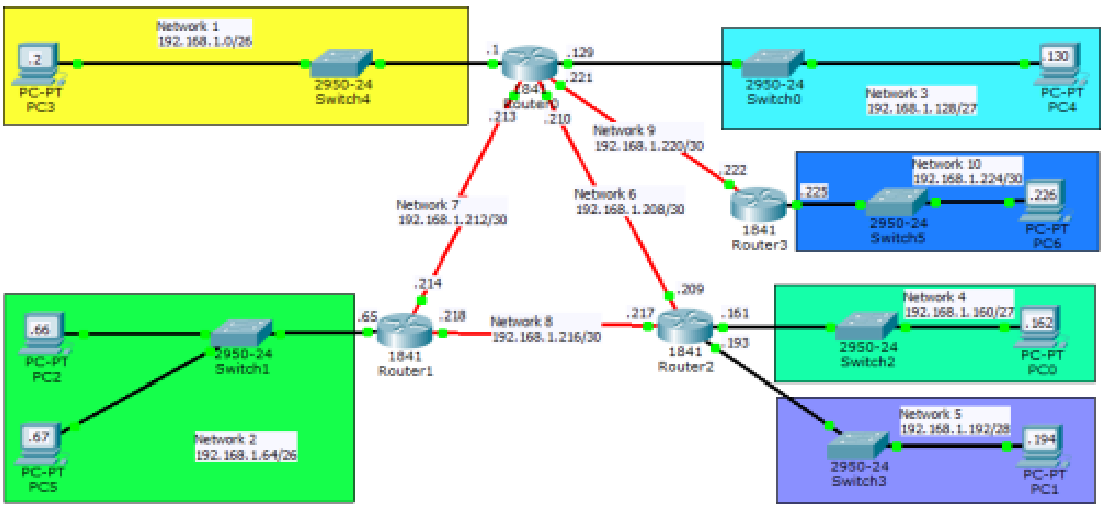

Figure 1 (Network Topology)

Run the same commands for all routers interfaces and assign each interface an appropriate IP/mask pair.

Now we start routing

Network 10 is connected directly to Router 3 and no other subnets is connected to Router 3, so we can configure default route on it using the following command:

Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.221

Where:
0.0.0.0: is the destination network IP [0.0.0.0 in case of default routing]
0.0.0.0: is the subnet mask being used on the destination network.
192.168.1.221: is the address of the next-hop router that will receive the packet and forward it to the destination network.

For the other routers, we cannot implement default routing since each of them is connected to more than one network. In this case, we use static routing. We can configure static route on router0 as follow:

Router(config)#ip route 192.168.1.64 255.255.255.192 192.168.1.214

Where:
192.168.1.64: is the destination network we want to send packets to it.
255.255.255.192: is the subnet mask being used on the destination network.
192.168.1.214: is the address of the next-hop router that will receive the packet and forward it to the destination network.

Configuring all other static routes on router0:

Router(config)#ip route 192.168.1.160 255.255.255.224192.168.1.209
Router(config)#ip route 192.168.1.192 255.255.255.240192.168.1.209
Router(config)#ip route 192.168.1.224 255.255.255.252 192.168.1.222

And do the same thing for the other routers. To review routing table on a router, use command “show ip route” as shown in figure 2

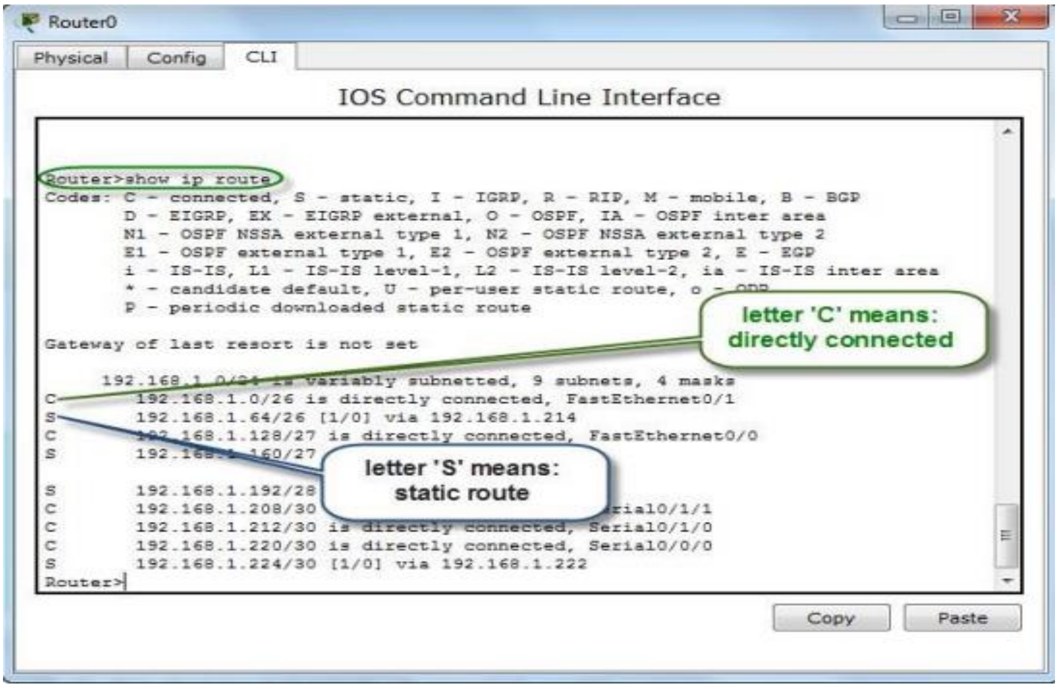

Figure 2(Routing Table)

Alternatively, by using the Inspect tool from the right panel, and select "Routing Table" from the menu:

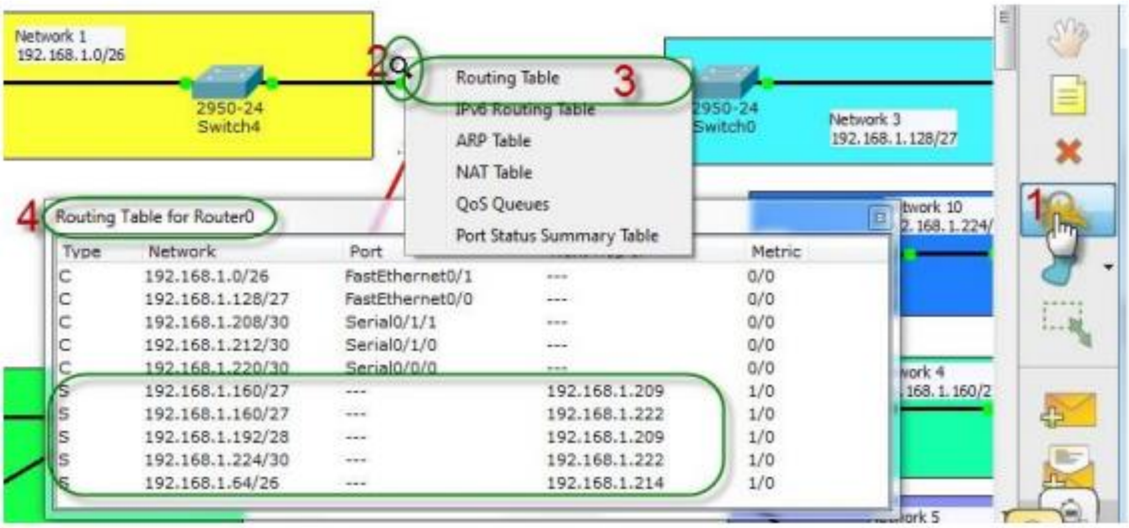

Figure 3 (Alternate way of routing table)

Another quick note: to mention that when (if) the packet is lost on the way back to the originating host, you will typically see a "Request timed out" message because it is an unknown error shown in figure 4. If the error occurs because of a known issue, such as if a route is not in the routing table on the way to the destination device, you will see a "Destination host unreachable" message as shown in figure 5. This should help you determine if the problem occurred on the way to the destination or on the way.

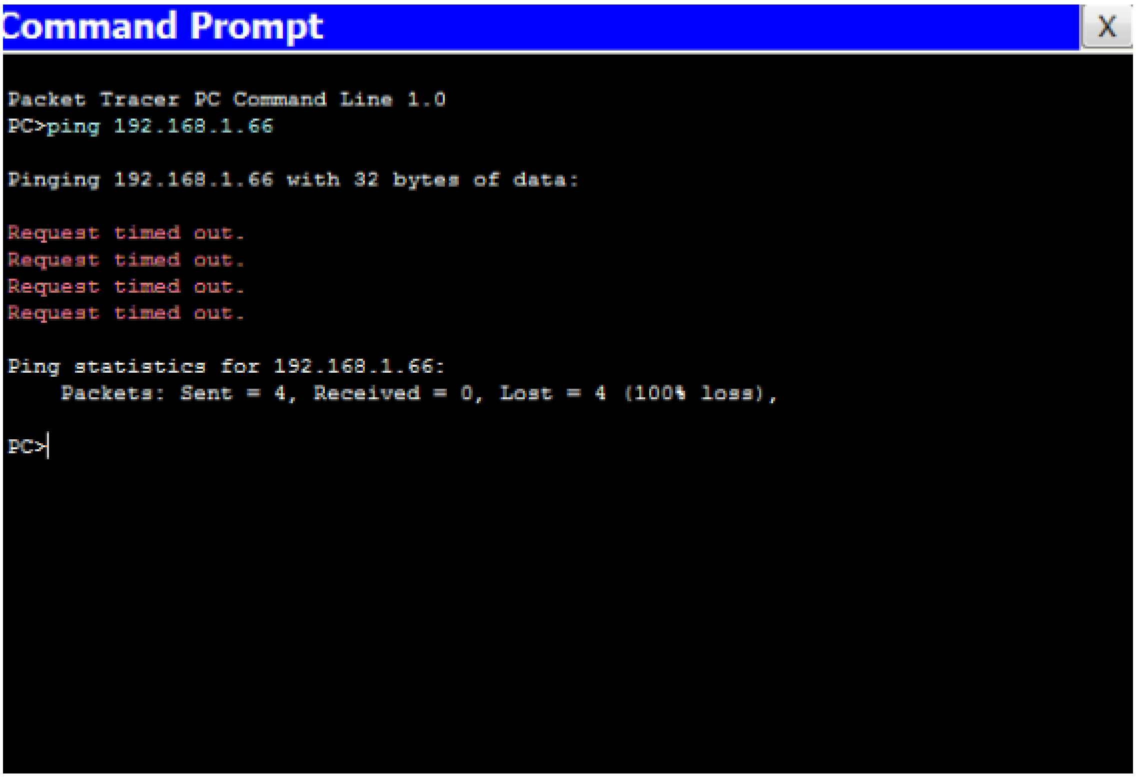

Figure 4 (Request Timed out Error)

Destination host unreachable message:

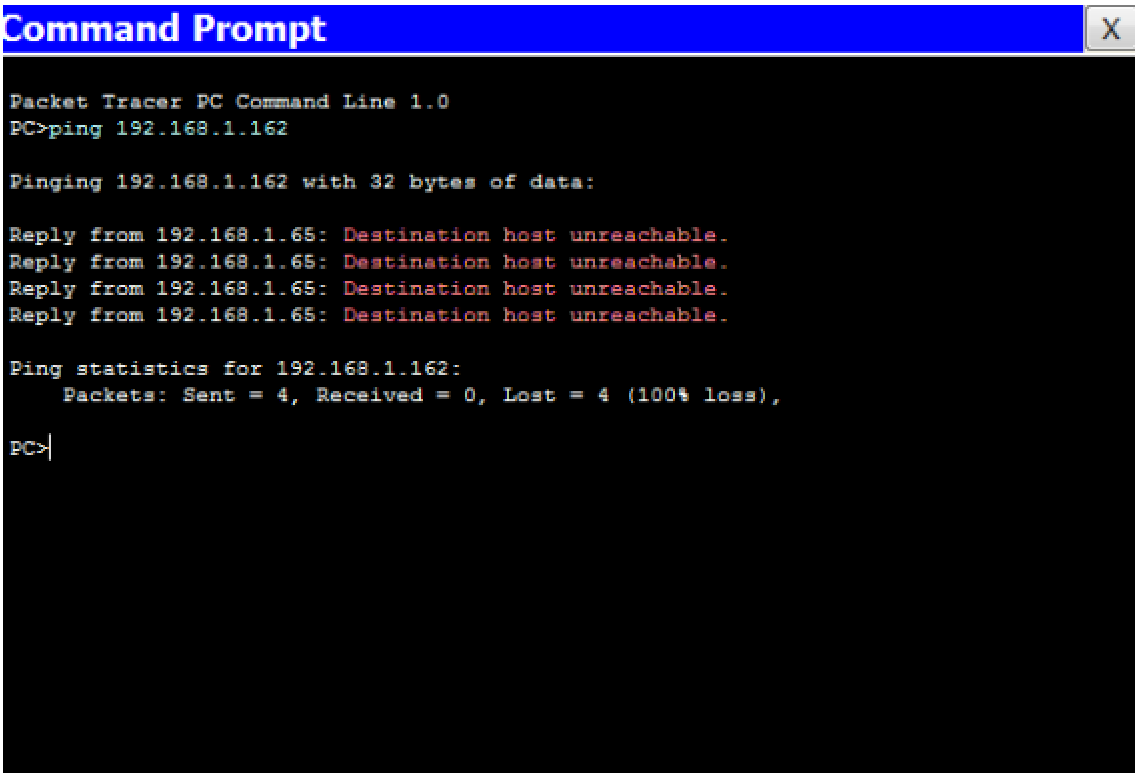

Figure 5 (Destination Host Unreachable Error)

5. Administrative Distances

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

If a router receives two updates listing the same remote network, the first thing the router checks is the AD.

If one of the advertised routes has a lower AD than the other, then the route with the lowest AD will be placed in the routing table. If both advertised routes to the same network have the same AD, then routing protocol metrics (such as hop count or bandwidth of the lines) will be used to find the best path to the remote network. The advertised route with the lowest metric will be placed in the routing table.

But if both advertised routes have the same AD as well as the same metrics, then the routing protocol will load-balance to the remote network (which means that it sends packets down each link).

Table 1 below shows default AD

Route Source	Default AD
Connected interface	0
Static route	1
EIGRP	90
IGRP	100
OSPF	110
RIP 1	120
External EIGRP	170

Table 1(Administrative Distances)

The smaller the AD is, the more preferable to route is.

6. Classes of Routing Protocols

Following are the classes of routing protocols:

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.

Link state

In link-state protocols, also called shortest-path-first protocols. 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.

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.

7. Introduction to Dynamic Routing

Dynamic routing is when protocols are used to find networks and update routing tables on routers. True, this is easier than using static or default routing, but it'll cost you in terms of router CPU processes and bandwidth on the network links.

A routing protocol defines the set of rules used by a router when it communicates routing information between neighbor routers. The routing protocol includes Routing Information Protocol (RIP) versions 1 and 2, with a bit of Interior Gateway Routing Protocol (IGRP) thrown in.

Two types of routing protocols are used in internetworks: interior gateway protocols (IGPs) and exterior gateway protocols (EGPs).

IGPs are used to exchange routing information with routers in the same autonomous system (AS). An AS is a collection of networks under a common administrative domain, which basically means that all routers sharing the same routing table information are in the same AS.

EGPs are used to communicate between ASes. An example of an EGP is Border Gateway Protocol (BGP), which is beyond the scope of our lab.

8. Types of Dynamic Routing and its configuration

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a true distance-vector routing protocol. RIP sends the complete routing table out to all active interfaces every 30 seconds. RIP only uses hop count to determine the best way to a remote network, but it has a maximum allowable hop count of 15 by default, meaning that 16 is deemed unreachable. RIP works well in small networks, but it's inefficient on large networks with slow WAN links or on networks with a large number of routers installed.

What will happen using RIP?

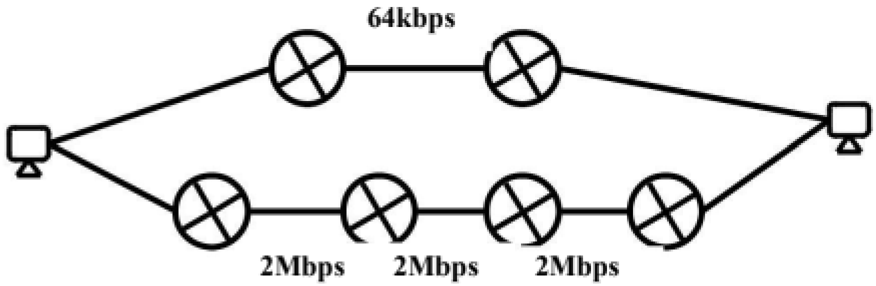

Figure 6 (Topology with RIP)

RIP Versions

	RIP V1	RIP V2
AD	**120**	**120**
Metric	**Hope count**	**Hope count**
Sending update per sec	**30 sec**	**30 sec**
Sending updates using	**Broadcast**	**multicast**
VLSM\CIDR	**Not supported**	**Supported**

RIP practical part

RIPV1

Lab_A#config t
Lab_A(config)#router rip
Lab_A(config-router)#network 192.168.10.0 (only net without mask)

Lab_A(config-router)#passive-interface serial 0/0 (This command prevents RIP update broadcasts from being sent out a specified interface, yet that same interface can still receive RIP updates.)

RIPV2

RIPv2 is considered classless because subnet information is sent with each route update

Lab_C(config)#router rip
Lab_C(config-router)#network 192.168.40.0
Lab_C(config-router)#network 192.168.50.0
Lab_C(config-router)#version 2

Open Shortest Path First (OSPF)

OSPF works by using the Dijkstra algorithm. First, a shortest path tree is constructed, and then the routing table is populated with the resulting best paths. OSPF converges quickly, although perhaps not as quickly as EIGRP, and it supports multiple, equal-cost routes to the same destination. Like EIGRP, it does support both IP and IPv6 routed protocols.

OSPF provides the following features:

- Consists of areas and autonomous systems
- Minimizes routing update traffic
- Allows scalability
- Supports VLSM/CIDR
- Has unlimited hop count
- Allows multi-vendor deployment (open standard)

OSPF Terminology

- Router ID
- Neighbor
- Adjacency
- Hello protocol
- Neighborship database
- Link State Advertisement
- Topological database
- OSPF areas
- Loopback Address
- Link costs

OSPF Practical Part

Lab_A#config t
Lab_A(config)#router ospf 1

1: is OSPF process number: out of scope for CCNA, range: <1-65535>

Lab_A(config-router)#network 10.0.0.0 0.255.255.255 area 0
0.255.255.255 : an example of wildcard

Wildcard

The wildcard mask can be configured as the inverse of a subnet mask. For example, IP 172.16.1.16/28 network. The subnet mask for this interface is /28 or 255.255.255.240. The inverse of the subnet mask results in the wildcard mask.

```
  255.255.255.255
- 255.255.255.240 (Subtract the subnet mask)
-----------------------------
  0. 0. 0. 15          Wildcard mask


  255.255.255.255
- 255.255.255.0 (Subtract the subnet mask)
-----------------------------
   0. 0. 0. 255        Wildcard mask

  255.255.255.255
- 255.255.0.0 (Subtract the subnet mask)
-----------------------------
   0. 0. 255. 255      Wildcard mask
```

9. Lab Exercise

Q1: Implement Subnetting with IP address of XX.XX.0.0/24. where xx is your roll no same are midterm. Then assign ip address in such a way that very less ip address should waste. Last run RIP routing protocol in such a way that all devices can communicate easily. What will be the administrative distance of the routing? Use figure A for your reference

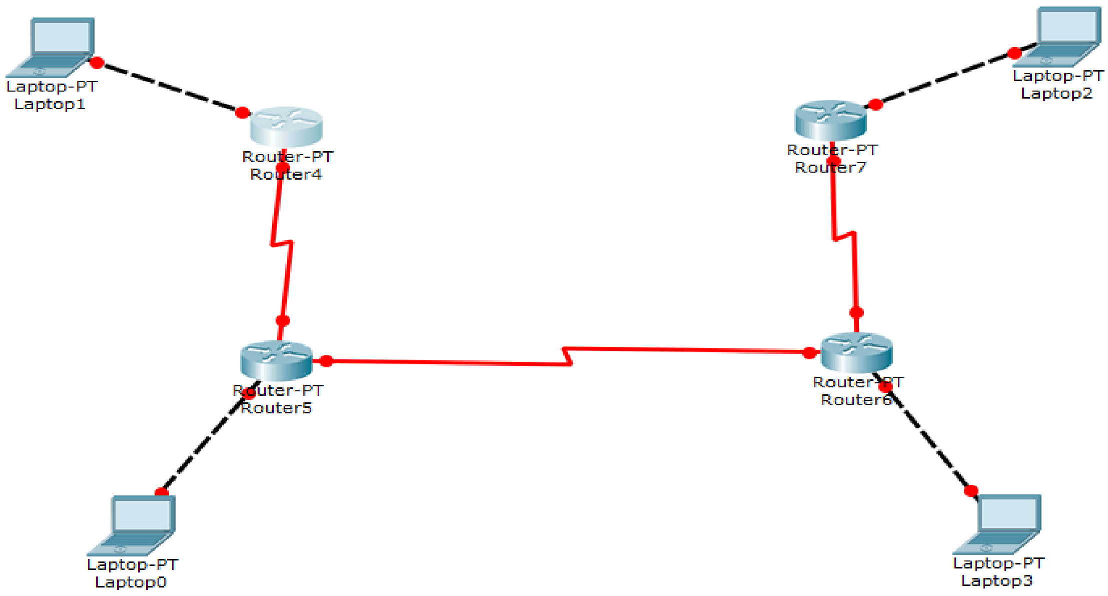

Figure A (Network Topology)

Q2: Implement Subnetting with IP address of 172.168.1.0/24. All the assignment of IP should be done dynamically in such a way that there should be less waste of Ips. Run the dynamic routing protocol will less administrative distance. What will be the administrative distance of the routing? Use Figure B as reference

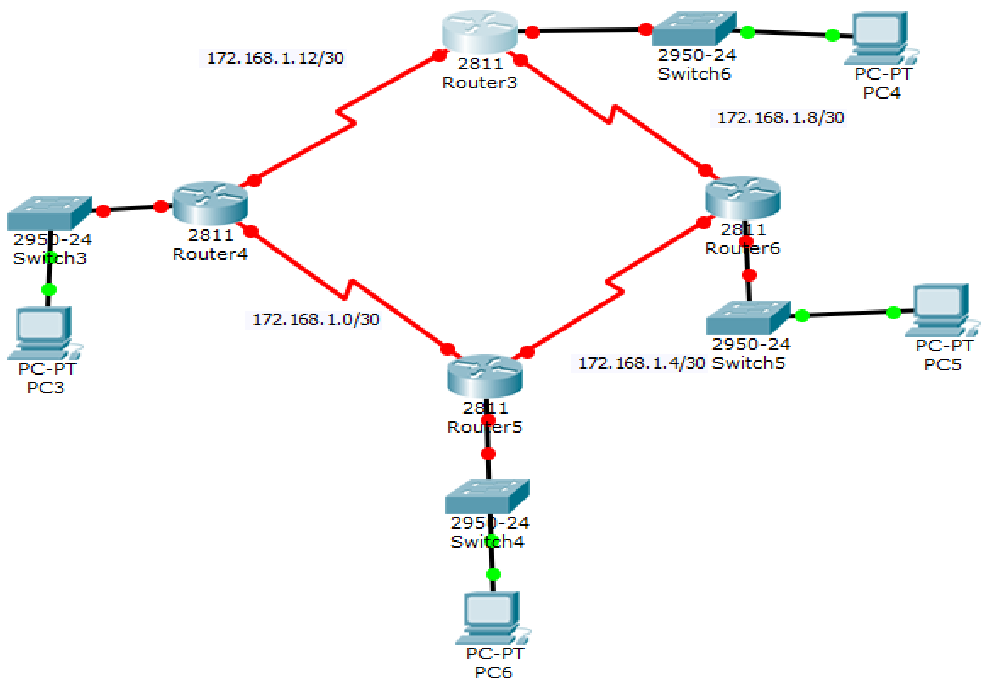

Figure B (Network Topology)

Q3: Implement the subnetting on the given scenario of figure C. You have to implement the static routing on the same. What will be the administrative distance of the routing?

Use Network Address as follows: 192.168.4.0/24.

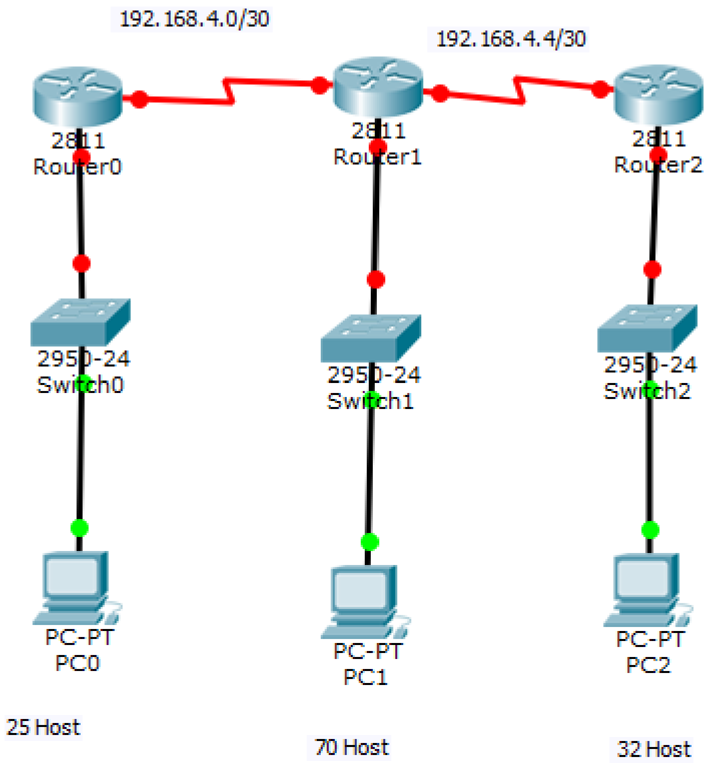

Figure C (Network Topology)

Q4: In what case we use static routing or dynamic routing given a topological reason for this question