Department of Computer Science and Engineering
Islamic University of Technology (IUT)
A subsidiary organ of OIC

Laboratory Report

CSE 4412: Data Communication and Networking Lab

Name	**:Nazia Karim Khan Oishee**
Student ID	**:200042137**
Section	**:1A**
Semester	**:Summer**
Academic Year	**:2021-2022**
Date of Submission	**:07.03.2023**
Lab No	**:06**

Title: Configuration of RIP in a network topology.

Objective:

1. Understand distance vector routing
2. Understand RIP
3. Understand the necessity of dynamic routing

Devices/ software Used:

1.Cisco Packet Tracer

Theory:

Distance Vector (DV) Routing

The two major types of Dynamic Routing Protocols are Distance Vector (DV) and Link State routing protocols.

Distance Vector is a type of routing protocol that is used in computer networks to determine the best path for routing data packets from one network node to another. In a DV routing protocol, each node maintains a table that lists the distance to every other node in the network.

These tables periodically exchange information with neighboring nodes to ensure that all nodes have up-to-date information about the network.

Based on this information, each node calculates the best path to reach every other node in the network.

Distance Vector Routing includes Routing Information Protocol (RIP) and Interior Gateway Routing Protocol(IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP).

Count to Infinity problem in DV routing

The Count to Infinity is a problem that can occur in DV routing algorithms. This problem occurs when a network link goes down, and the affected nodes in the network do not receive any updates from their neighboring nodes about the failure.

In this case, the affected nodes being uninformed continue to believe that the link is still operational. So they continue to advertise their connectivity to the rest of the network. As a result, the neighboring nodes continue to send traffic to the affected nodes, which forward it back to the neighboring nodes and results in causing a loop.

To prevent this problem, Distance Vector routing algorithms implement a maximum hop count.

Two node Loop problem in DV routing

The Two Node Loop problem occurs in the Distance Vector routing algorithm. This problem occurs when two network nodes are directly connected to each other.

In this scenario, each node learns from its neighbors that the other node can be reached directly and adds an entry to its routing table for that destination node. However because each node advertises the other node as a valid path to the destination , a loop is created.

For example, if A and B are directly connected to each other, when node A receives a packet destined for node B, it forwards the packet to node B. Node B then forwards it back to node A and thus creates a loop which causes network congestion and leads to packet loss.

Split Horizon (one solution to instability)

Split Horizon is a simple yet effective technique that is used in computer networking to prevent routing loops and to improve the stability of the network.

In a split horizon, a network node that learns a route from a neighboring node will not advertise that route back to the node from which it was learned.

For example, suppose there are three nodes A,B and C in a network. If node A learns from node B that it can reach node C directly, it will not advertise this route back to node B. Similarly, if node A learns from node C that it is connected to node B, it will not advertise this route back to node C.

This helps to prevent creation of network loops and prevents network congestion and packet loss.

Poison Reverse ()

In Poison Reverse, when a network node detects that a route is no longer valid, it advertises the route back to the originating node with an infinite metric. This tells the original node that the route is no longer available. Thus it prevents the node from using the route in its calculations.

For example, suppose there are three nodes A,B and C in a network. Node A is connected to nodes B and C. If node A learns from node B that it can reach node C directly, it will add an entry to its routing table with a metric of two hops. If node B detects that the route to node C is no longer valid, it will advertise the route back to node A with an infinite metric. This tells node A that the route is no longer valid.

Thus, poison reverse ensures that the network nodes do not use the invalid routes. It improves the stability of networks where a split horizon may not be sufficient.

A variation of poison reverse use timer and is known as Poison Reverse with timer. In this technique when a node detects that a route is no longer valid, it advertises the route back to the original node with an infinite metric and starts a timer. After a specified period of time, the timer expires and the router is removed from the routing table.

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a distance vector routing protocol that is used in computer networking to determine the best path for data to travel between nodes in a network. RIP is used by routers to exchange information about the topology of the network.

RIP operates by periodically broadcasting routing updates to other nodes in the network. By analyzing the update information, routers build a map of the network topology and use the information to determine the best path for data to travel between nodes in the network.

RIP uses hop count as the metric for determining the distance between nodes, with a maximum limit of 15 hops.

There are three versions of RIP. They are-

1.**RIPv1:** It is the simplest version of the protocol. It uses a hop count as the metric and its maximum hop count is 15. RIPv1 does not support variable length subnet masking (VLSM), which means all subnets in a network must use the same subnet mask. RIPv1 also doesn’t support authentication.

2. **RIPv2:** RIPv2 supports VLSM which allows more efficient use of IP addresses. It also supports authentication. RIPv2 uses a multicast address to send updates. It has a maximum hop count limit of 15, the same as RIPv1.

3. **RIPng:** ng stands for next generation. RIPng is specifically designed for supporting IPv6 networks, which use 128 bit addresses instead of the 32 bit addresses used in IPv4. RIPng supports VLSM like RIPv2 and also supports authentication. It uses a multicast address to send updates.

RIP uses a number of timers to manage the exchange of information between network devices.. These timers are:

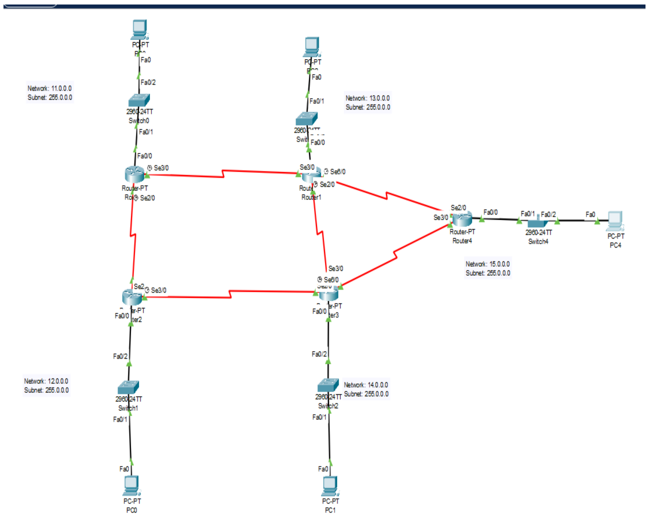
1. **Update Timer:** This timer determines how frequently a router will broadcast its routing table to neighboring routers. By default, the update timer is set to 30 seconds, which means a router will broadcast its routing tables every 30 seconds.

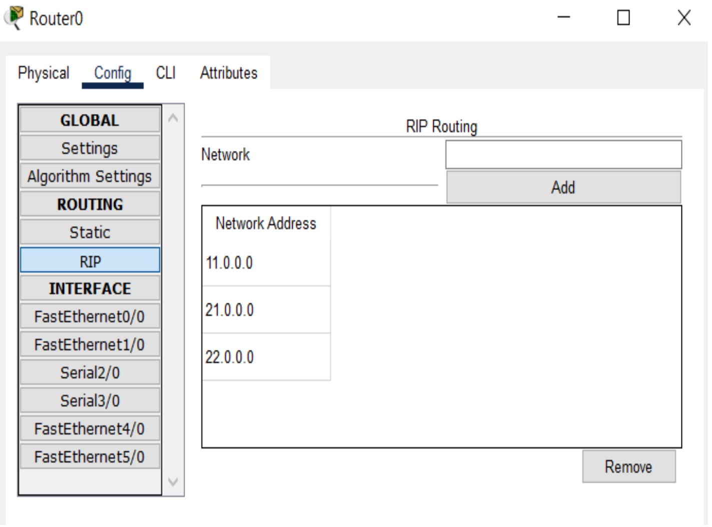
2. **Invalid Timer:** This timer determines how long a router will wait before marking a route invalid. By default, the invalid timer is set to 180 seconds, which means a router will be marked as invalid if the router does not receive an update for that route within 180 seconds.

3. **Hold-Down Timer:** This timer is used to prevent the router from accepting updates for a route that has been marked as invalid. When a route is marked as invalid, it sets the hold-down timer for that route and during this time the router does not accept any updates for that route even if it consists of a lower metric. By default, the hold-down timer is set to 180 seconds.

4.**Flush timer:** This timer determines how long a router will wait before removing a route from its routing table after it has been marked as invalid. By default, the flush timer is set to 240 seconds.

Diagram of the experiment:





RIP Routing

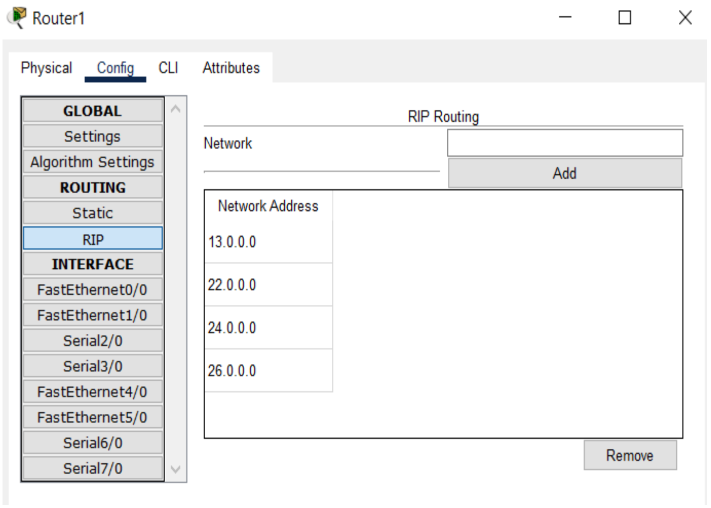
Network

Network Address

11.0.0.0

21.0.0.0

22.0.0.0



RIP Routing

Network

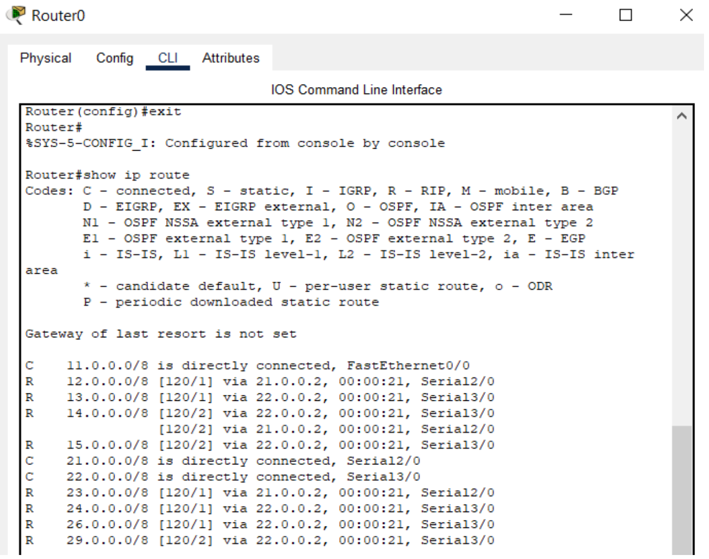
Network Address

13.0.0.0

22.0.0.0

24.0.0.0

26.0.0.0



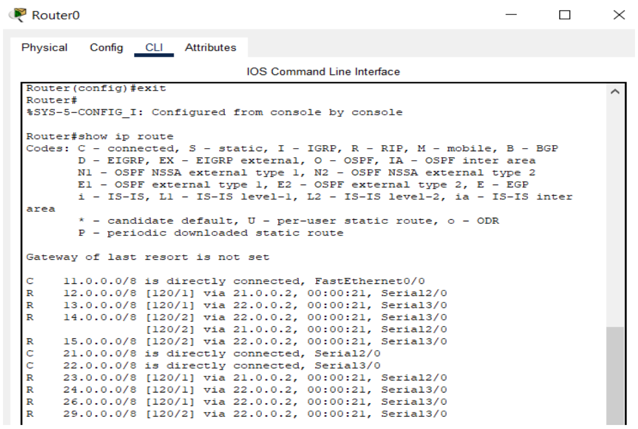
IOS Command Line Interface

```
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

Gateway of last resort is not set

C    11.0.0.0/8 is directly connected, FastEthernet0/0
R    12.0.0.0/8 [120/1] via 21.0.0.2, 00:00:21, Serial2/0
R    13.0.0.0/8 [120/1] via 22.0.0.2, 00:00:21, Serial3/0
R    14.0.0.0/8 [120/2] via 22.0.0.2, 00:00:21, Serial3/0
                [120/2] via 21.0.0.2, 00:00:21, Serial2/0
R    15.0.0.0/8 [120/2] via 22.0.0.2, 00:00:21, Serial3/0
C    21.0.0.0/8 is directly connected, Serial2/0
C    22.0.0.0/8 is directly connected, Serial3/0
R    23.0.0.0/8 [120/1] via 21.0.0.2, 00:00:21, Serial2/0
R    24.0.0.0/8 [120/1] via 22.0.0.2, 00:00:21, Serial3/0
R    26.0.0.0/8 [120/1] via 22.0.0.2, 00:00:21, Serial3/0
R    29.0.0.0/8 [120/2] via 22.0.0.2, 00:00:21, Serial3/0
```



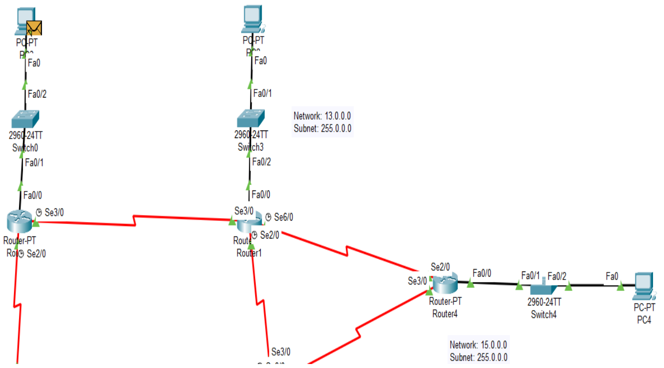
IOS Command Line Interface

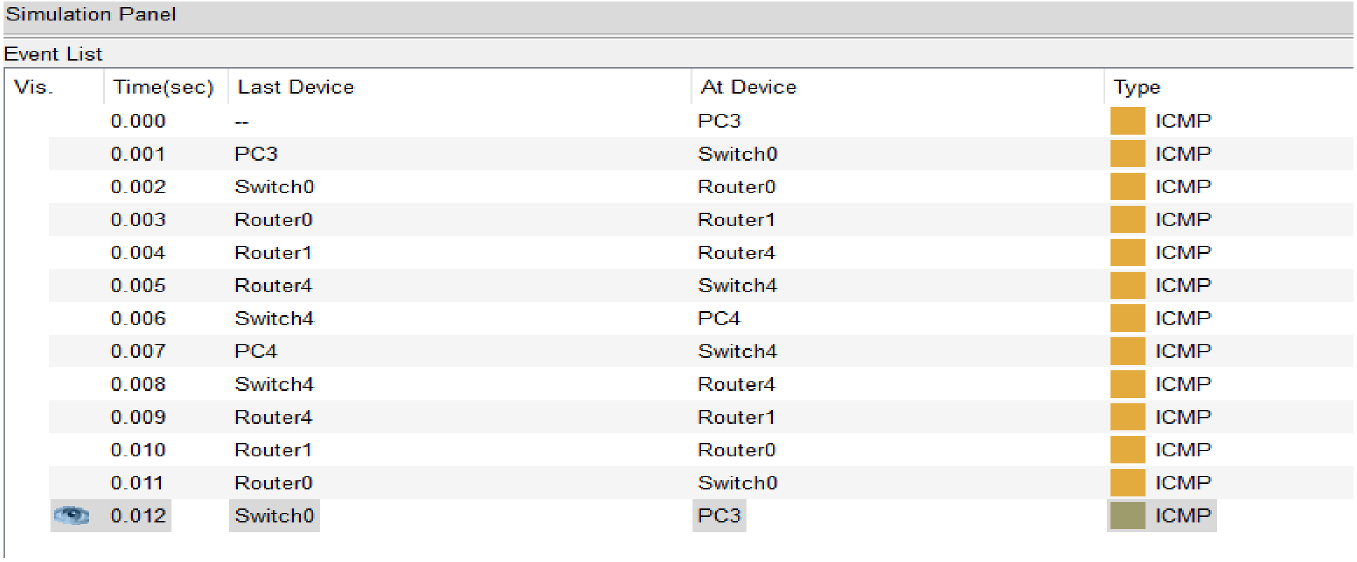
```
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

Gateway of last resort is not set

C    11.0.0.0/8 is directly connected, FastEthernet0/0
R    12.0.0.0/8 [120/1] via 21.0.0.2, 00:00:21, Serial2/0
R    13.0.0.0/8 [120/1] via 22.0.0.2, 00:00:21, Serial3/0
R    14.0.0.0/8 [120/2] via 22.0.0.2, 00:00:21, Serial3/0
                [120/2] via 21.0.0.2, 00:00:21, Serial2/0
R    15.0.0.0/8 [120/2] via 22.0.0.2, 00:00:21, Serial3/0
C    21.0.0.0/8 is directly connected, Serial2/0
C    22.0.0.0/8 is directly connected, Serial3/0
R    23.0.0.0/8 [120/1] via 21.0.0.2, 00:00:21, Serial2/0
R    24.0.0.0/8 [120/1] via 22.0.0.2, 00:00:21, Serial3/0
R    26.0.0.0/8 [120/1] via 22.0.0.2, 00:00:21, Serial3/0
R    29.0.0.0/8 [120/2] via 22.0.0.2, 00:00:21, Serial3/0
```





Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC3	🟧 ICMP
	0.001	PC3	Switch0	🟧 ICMP
	0.002	Switch0	Router0	🟧 ICMP
	0.003	Router0	Router1	🟧 ICMP
	0.004	Router1	Router4	🟧 ICMP
	0.005	Router4	Switch4	🟧 ICMP
	0.006	Switch4	PC4	🟧 ICMP
	0.007	PC4	Switch4	🟧 ICMP
	0.008	Switch4	Router4	🟧 ICMP
	0.009	Router4	Router1	🟧 ICMP
	0.010	Router1	Router0	🟧 ICMP
	0.011	Router0	Switch0	🟧 ICMP
👁	0.012	Switch0	PC3	▨ ICMP

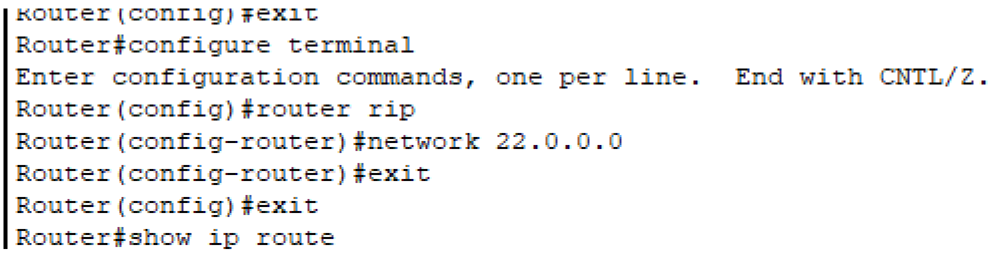
Configuration of Routers

At first I configured the PCs and routers. I assigned the PC an IP address. The default gateway of the PC is the same as the IP address of the connected router.

Next, I assigned IP addresses to the serial ports of the routers. Here the serial port addresses of the router which are connected to each other belong to the same network. For example, Router0 is connected to Router1 via serial port 3. So the addresses of these serial ports are 22.0.0.1 and 22.0.0.2 respectively. Thus they belong to the same network.

After that I enabled the RIP protocol.

Commands for configuring RIP



```
Router(config)#exit
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 22.0.0.0
Router(config-router)#exit
Router(config)#exit
Router#show ip route
```

Router# configure terminal

Router(config)# router rip

Router(config-router)# network <network-address>

Here the network address is the network address of the serial port.

Observation:

After setting up the RIP routing algorithm if Serial port Se3/0 of Router 4 is switched off then what are the changes occurring in Routing information of the routers.

Router4 and Router3 are connected through serial port 3 of Router 4 and serial port 6 of Router 3. If the Se3/0 of Router 4 is switched off, then the packet sent from PC1 goes to PC4 through router3=>Router1=>Router4 path via Se2/0 of Router 4.

Challenges:

In this task, I faced challenges while setting up the serial port of the routers. As there were multiple routers connected to each other, I faced problems connecting them correctly keeping their network id same.