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	**: M M Nazmul Hossain**
Student ID	**: 200042118**
Section	**: 1**
Semester	**: 4th**
Academic Year	**: 2021-2022**
Date of Submission	**: 07.03.2023**
Lab No	**: 6**

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: Cisco Packet Tracer, 5 Routers, 5 Switches, 5 PCs

Theory:

Distance Vector (DV) Routing

DV routing is a routing procedure that uses a routing table to store the hop count between routers and find the shortest path possible to transmit data between them.

Count to Infinity problem in DV routing

The Count to Infinity problem occurs when a router advertises an incorrect distance to a destination network, which can occur as a result of link failures or other network issues. When a router receives a higher metric (i.e., a longer path) from a neighbor, it updates its routing table to reflect the higher metric. This process is repeated until all routers in the network agree on a metric.

However, if the network topology contains a cycle and a router receives information about a longer path to a destination network, it may incorrectly believe that the longer path is a shorter path via a different neighbor. As a result, routers may continue to increase the metric to a destination network even though the true metric is much lower.

As a result, routing information "counts" indefinitely, resulting in inefficient and unstable network communication.

Two node Loop problem in DV routing

A loop is formed by two routers that are directly connected to each other. When the routers exchange routing information, they will continue to advertise the same distance to each other, resulting in each router believing that the other router is the best path to the destination network.

As a result, the routers may continue to forward packets to each other in an endless loop, clogging the network and making it unresponsive. This can result in significant delays and packet loss, as well as increased network load.

Split Horizon (one solution to instability)

Split horizon is a mechanism used in Distance Vector Routing protocols such as Distance Velocity Routing to prevent routing loops caused by incorrect routing information.

Split horizon is based on the idea that a router does not advertise a route back to the neighbor from whom it learned the route. This means that if a router learns a route to a destination network from one of its neighbors, it does not advertise it to that same neighbor.

This prevents loop formation because each router only forwards packets to its neighbors if the neighbor is a better path to the destination network than the router itself. The router avoids forwarding packets in a loop between two routers by not advertising routes back to the neighbor from whom the router learned the route.

Split horizon does, however, have some limitations, and other techniques such as route poisoning and hold-down timers may be required to further improve network stability.

Poison Reverse (second solution to instability)

Poison reverse is a technique used to prevent routing loops in Distance Vector Routing protocols such as Distance Velocity Routing.

When a router realizes that a previously advertised route is no longer valid, it immediately informs its neighbors by advertising it with an infinite metric that the route is no longer reachable. This aids in the prevention of loop formation because the router's neighbors are aware that the router is no longer a valid path to the destination network. If the router learned about the invalid route from one of its neighbors, it will use poison reverse to advertise the same unreachable route to that neighbor.

This ensures that the neighbor is aware of the previously advertised route's demise and avoids using it. When combined with other techniques such as split horizon, poison reverse is an effective mechanism. However, it can increase network traffic and may not always be enough to prevent routing loops in some network topologies.

Routing Information Protocol (RIP)

The Routing Information Protocol, or RIP for short, is a type of dynamic routing protocol. In contrast to static routing, which requires the route to the router's terminal to be manually specified, RIP uses its routing table to dynamically select the shortest path to the network.

RIP v1	RIP v2	RIP v3
Broadcast	Multicast	Multicast
No VLSM	VLSM	VLSM
IPv4	IPv4	IPv6
No Authentication	Authentication	Authentication

Hop count: A distance measurement between the source and destination networks calculated by counting the number of routers that a packet passes through on its way to its destination. Each router through which a packet travels counts as one hop, and the hop count is increased by one at each router. RIP uses this metric to choose the path with the fewest hops as the preferred route.

Forwarding Table: A forwarding table is a data structure used by RIP routers to determine the next hop for packets to be forwarded to their destination. It contains information about known networks and the next hop routers associated with them, as well as the cost or distance required to reach those networks.

Routers use the forwarding table to determine how to forward incoming packets based on their destination IP address. The RIP algorithm constructs and updates it by exchanging routing information with neighboring routers to keep the forwarding table up to date with changes in the network topology. As the network evolves, the forwarding table is updated so that the router can make forwarding decisions based on the most up-to-date information.

Timers:

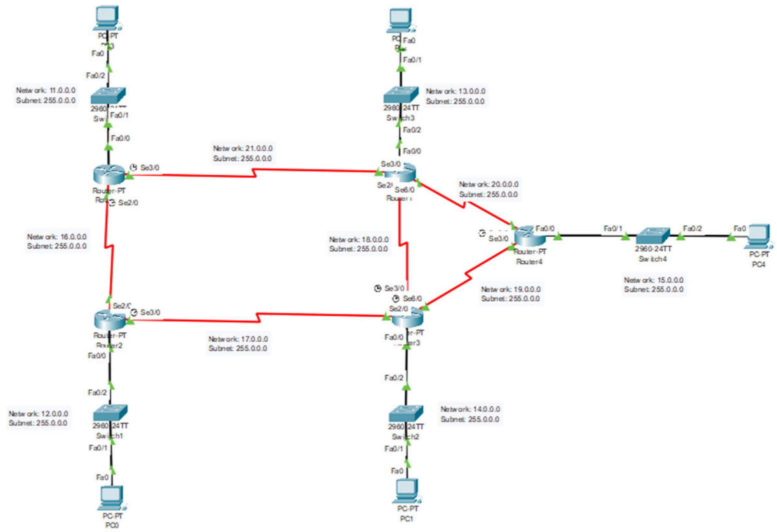
1. Update: The Update timer governs how frequently a router sends updates to its neighbors. The default value is 30 seconds, which means that the router sends an update to its neighboring routers every 30 seconds with information about the state of its routing table.

2. Invalid: The Invalid Timer controls how long a router waits before marking a route as invalid. The default value is 180 seconds, which means that if a router does not receive an update for a route within that time frame, it assumes the route is no longer valid.

3. Hold-Down: The Hold-down Timer is used to prevent the network from rapidly converging. When a router receives notification that a route is no longer valid, the hold-down timer begins. During this time, the router ignores any route updates it receives and does not send any updates of its own. The hold-down timer is set to 180 seconds by default.

4. Flush: The Flush timer controls how long a router waits before removing a route from its routing table. The default value is 240 seconds, which means that if a router does not receive any updates about a route for 240 seconds, the route is removed from its routing table.

Diagram of the experiment:



Configuration of Routers:

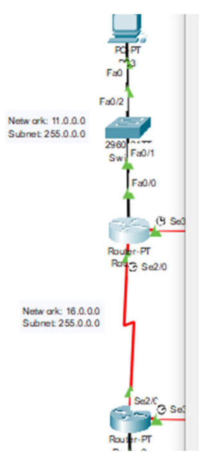
After configuring all the IP addresses and networks to the routing ports and PCs, the Dynamic routing protocol has to be established. To do so, we can use the following commands:

Enable -> configure terminal -> Router RIP -> version 2 -> network <network id>.

In the lab, it was instructed to assign all the network IDs involved in the experiment in the above mentioned <network id> tag. However, we only had to input only the network IDs directly connected to the router. The other network IDs would be dynamically allocated for. But, as instructed, all the network IDs are input at each router.

All the routers are configured similarly. And after using Show IP route command, the following picture can be seen:

Router 0



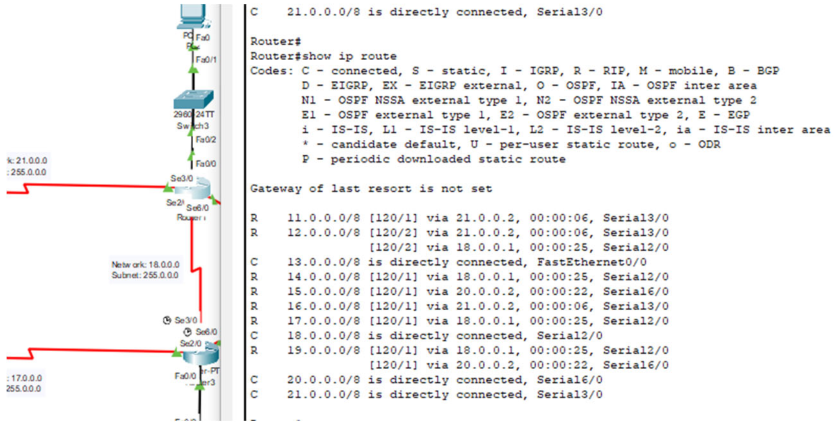

```
Router#
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 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 16.0.0.2, 00:00:29, Serial2/0
R    13.0.0.0/8 [120/1] via 21.0.0.1, 00:00:15, Serial3/0
R    14.0.0.0/8 [120/2] via 16.0.0.2, 00:00:29, Serial2/0
                [120/2] via 21.0.0.1, 00:00:15, Serial3/0
R    15.0.0.0/8 [120/2] via 21.0.0.1, 00:00:15, Serial3/0
C    16.0.0.0/8 is directly connected, Serial2/0
R    17.0.0.0/8 [120/1] via 16.0.0.2, 00:00:29, Serial2/0
R    18.0.0.0/8 [120/1] via 21.0.0.1, 00:00:15, Serial3/0
R    19.0.0.0/8 [120/2] via 21.0.0.1, 00:00:15, Serial3/0
                [120/2] via 16.0.0.2, 00:00:29, Serial2/0
R    20.0.0.0/8 [120/1] via 21.0.0.1, 00:00:15, Serial3/0
C    21.0.0.0/8 is directly connected, Serial3/0
```

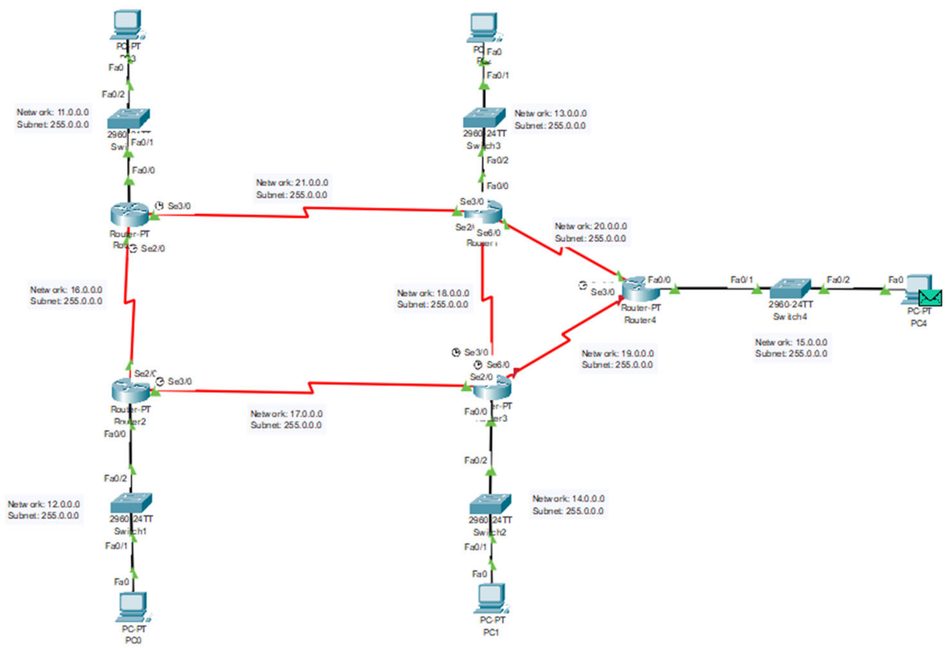
A similar situation can be seen for the rest of the routers, with only the directly connected networks changing.

Router 1



Observation:

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



At first, when the Serial port Se 3/0 is switched off, then, at first, the forwarding tables at all the routers include old data. Attempting to send packets in this state, may result in packet loss. In some cases, the packet will never reach the recipient.

After some time, however, the routers communicate with each other to update their forwarding tables using an appropriate algorithm like the split horizon or poison reverse. This ultimately results in the forwarding tables at all the routers, dynamically updating themselves eventually after the involved timers run out. So, after fast forwarding a few times in the real-time settings, if I attempt to send a packet, the packet route will avoid the turned-off serial port and ultimately reach the recipient destination, if such a route exists. This, however, might result in the packet following a route that is longer than what it was before, but given enough time to build the forwarding tables, it will definitely be the shortest possible route for the provided ports.

Challenges:

- Configuring the routers in the experiment was a bit difficult as everything was too congested.
- Understanding the concepts of RIP took a longer time than intended.
- How the Forwarding Tables at each router is updated was difficult to envision.