Assignment No.7

Title:

Use packet Tracer tool for configuration of 3 router network using one of the following protocol RIP/OSPF/BGP.

Theory

Routing Protocols

Routing protocols maintains routing tables where routing table contains a route to every destination network .

Dynamic Routing Protocols

There are three types of it as follows:

1. Routing Information Protocol (RIP)
2. Open Shortest Path First (OSPF)
3. Border Gateway Protocol (BGP)

RIP and OSPF are Interior Gateway Protocols (IGPs); they are designed to operate in a single autonomous system (AS). (An AS is a group of networks administered by the same authority). BGP is an Exterior Gateway Protocol (EGP), which allows routers in different autonomous systems to exchange routes. Because BGP routers must regulate traffic between networks controlled by organizations with different policies.

How Routing Protocols Work

A router constructs its routing table using the information it receives from other routers. The router changes its routing table in response to routing updates that provide additional information or notification that conditions in the network have changed (for example, a link has failed). This responsiveness explains why using a routing protocol is often called dynamic routing.

The protocol must dictate parameters such as the following:

■ **How routers compute a route's metric and select the best route for their routing table:** Routing protocols can have a relatively complicated system for calculating a route's metric. So that you can select the best routing protocol (or protocols) for your network environment. If necessary, you can change which routes are chosen by altering the default metrics that a protocol assigns certain routes.

■ **What information routers include in routing updates:** With some routing protocols, routers exchange their entire routing tables. With other routing protocols, routers exchange only portions of the routing table.

■ **Which routers and router interfaces send and receive updates:** Most protocols specify that when routers receive an update on an interface, they do not send the same update from that interface. This common sense rule minimizes overhead.

■ **When routers send and receive updates and hellos:** To lower overhead and conserve bandwidth, you can alter how often routers send certain messages.

1. Routing Information Protocol (RIP)

RIP is one of the oldest dynamic routing protocols on the Internet that is still in use.RIP is an intradomain routing protocol that uses a distance vector approach to determine the paths between routers. RIP minimizes the number of hops on each path, where each point-to-point link or LAN constitutes a hop. Each RIP-enabled router periodically sends the content of its routing table to all its neighboring routers in an update message. For each routing table entry, the router sends the destination (host IP address or network IP address and associated prefix) and the distance to the destination measured in hops. When a router receives an update message from a neighboring router, it updates its own routing table

Configuring RIP on CISCO ROUTER

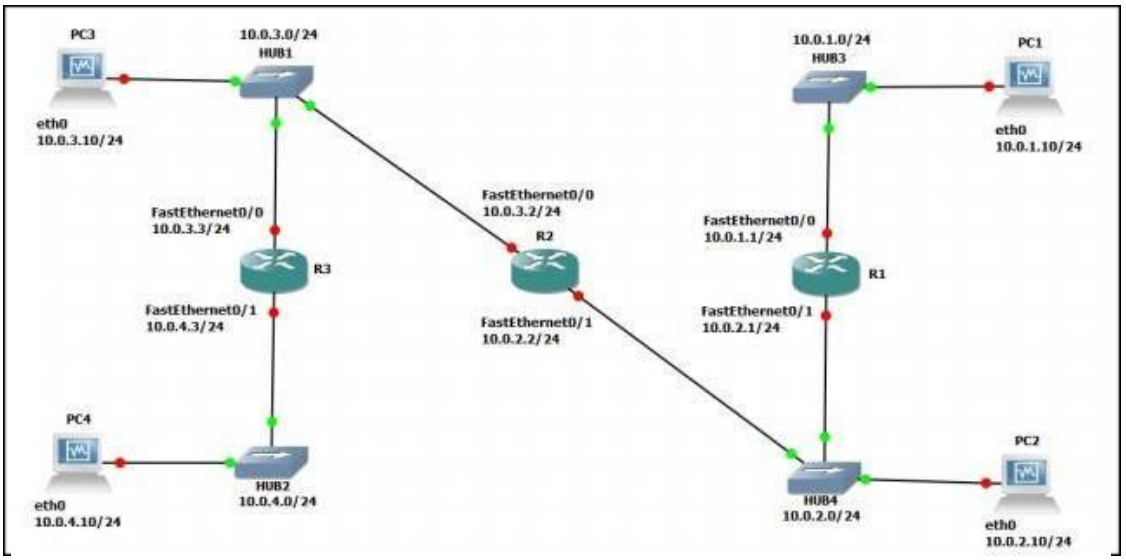

Fig. 1 Network topology

Cisco Routers	Ethernet Interface FastEthernet 0/0	Ethernet Interface FastEthernet 0/1
Router1	10.0.1.1 / 24	10.0.2.1 / 24
Router2	10.0.3.2 / 24	10.0.2.2 / 24
Router3	10.0.3.3 / 24	10.0.4.3 / 24

Linux PC	Ethernet Interface eth0	Ethernet Interface eth1
PC1	10.0.1.10 / 24	Disabled
PC2	10.0.2.10 / 24	Disabled
PC3	10.0.3.10 / 24	Disabled
PC4	10.0.4.10 / 24	Disabled

Table 1: IP addresses of the Cisco routers and Linux PCs

Above Figures describe the network configuration

Exercise 1. Configuring RIP on Cisco routers

In this exercise, you will configure all the routers to run RIP. After the configuration, all the routers should be able to ping all the other routers. Following is a brief overview of the basic commands used to configure RIP on a Cisco router. Make sure you type in the command in the correct command mode (note the prompt).

IOS MODE: GLOBAL CONFIGURATION

`router rip` | `no router rip`

Enables or disables RIP on the local router.

IOS MODE: PRIVILEGED EXEC

`debug ip rip` | `no debug ip rip`

Enables or disables a debugging mode where the router displays a message for each received RIP packet.

IOS MODE: ROUTER CONFIGURATION

`network Netaddr` | `no network Netaddr`

Associates or disables the network IP addresses`Netaddr` with RIP. RIP sends updates only on interfaces on which the network address has been associated with RIP.

`passive-interface Iface` | `no passive-interface Iface`

Sets or disables the interface `Iface` in RIP passive mode. On an interface in passive mode, the router processes incoming RIP packets but does not transmit RIP packages.

`offset-list 0 in valueIface` | `offset-list 0 out valueIface`

Increases the metric (hop count) of incoming RIP packages that arrive or outgoing RIP packets that are sent on interface `Iface` by `value`.

`timers basic update invalid hold-down flush`

update: The time interval between transmissions of RIP update messages (default: 30 seconds).

invalid: The time interval after which a route, which has not been updated, is declared invalid (default: 180 seconds).

hold-down: Determines how long after a route has been updated as unavailable. A router will wait before accepting a new route with a lower metric. This introduces a delay for processing incoming RIP packets with routing updates after a link failure (default: 180 seconds).

flush: The amount of time that must pass before a route that has not been updated is removed from the routing tables (default: 240 seconds).

`flash-update-threshold time`

Sets the router not to perform triggered updates, when the next transmission of routing updates is due in `time`. If `time` is set to the same value as the update timer, then triggered update are disabled. In RIP, a triggered update means that a router sends a RIP packet with a routing update, whenever one of its routing table entries changes.

1. Connect the PCs and the Cisco Routers as shown in Figure1. The PCs and routers are connected with Ethernet hubs.

2. Start Routers by clicking the right button and select Start; then, open a terminal by clicking the right button and select Console.

3. On Router1, Router2, and Router3, configure the IP addresses as shown in Table 1, and enable the routing protocol RIP. The commands to set up Router 1 are as follows:

```
Router1>enable
Router1#configure terminal
Router1(config)#no ip routing
Router1(config)#ip routing
Router1(config)#router rip
Router1(config-router)#version 2
Router1(config-router)#network 10.0.0.0
Router1(config-router)#interface FastEthernet0/0
Router1(config-if)#no shutdown
Router1(config-if)#ip address 10.0.1.1 255.255.255.0
Router1(config-if)#interface FastEthernet0/1
Router1(config-if)#no shutdown
Router1(config-if)#ip address 10.0.2.1 255.255.255.0
Router1(config-if)#end
Router1#clear ip route *
```

4. After you have configured the routers, check the routing table at each router with the show ip route command. Each router should have four entries in the routing table: two entries for directly connected networks and two other entries for remote networks that were added by RIP.

5. From each router, issue a ping command to the IP address of interfaces FastEthernet0/0 and FastEthernet0/1 on all remote routers.

2. Open Shortest Path First (OSPF)

OSPF is a link state routing protocol, in which each router sends information on the cost metric of its network interfaces to all other routers in the network, The information about the interfaces is sent in messages that are called link state advertisements (LSAs). LSAs are disseminated using flooding; that is, a router sends its LSAs to all its neighbors, which, in turn, forward the LSAs to their neighbors and so on. However, each LSA is forwarded only once. Each router maintains a link state database of all received LSAs, which provides the router with complete information about the topology of the network, Routers use their link state databases to run a shortest-path algorithm that computes the shortest paths in the network.

The network configuration is shown in Figure 2 and Table 2. Note that PC1-4 are set up as routers.

PCs	Interface eth0	Interface eth1
PC1	10.0.1.1 / 24	10.0.2.1 / 24
PC2	10.0.1.2 / 24	10.0.5.2 / 24
PC3	10.0.3.4 / 24	10.0.4.4 / 24
PC4	10.0.6.7 / 24	10.0.7.7 / 24

Figure 4.4 Network topology for Part 5

Cisco Routers	Ethernet Interface FastEthernet 0/0	Ethernet Interface FastEthernet 0/1
Router1	10.0.3.3 / 24	10.0.2.3 / 24
Router2	10.0.4.5 / 24	10.0.2.5 / 24
Router3	10.0.5.6 / 24	10.0.6.6 / 24
Router4	10.0.5.8 / 24	10.0.7.8 / 24

Configuring OSPF on Cisco routers

In this exercise, you configure OSPF on the Cisco routers. A brief description of the basic IOS commands used to configure OSPF on a Cisco router follows. As usual, each command must be issued in a particular IOS command mode.

IOS MODE: GLOBAL CONFIGURATION

`router ospf process-id`

Enables an OSPF routing process. Each router can execute multiple OSPF processes. process-id is a number that identifies the process. In this lab, only one OSPF process is started per router, and the process-id value is always set to 1. (The process-id of a router does not need to be the same on all routers). The command enters the router configuration mode, which has the following command prompt:

Router1(config-router)#

`no router ospf process-id`

Disables the specified OSPF process.

IOS MODE: PREVILEGED EXEC

`show ipospf`

Displays general information about the OSPF configuration

`show ipospf database`

Displays the link state database.

`show ipospf border-routers`

Displays the Area Border Router (ABR) and Autonomous System Boundary Router (ASBR).

`clear ipospf process-id process`

Resets the specified OSPF process.

1. Connect the routers as shown in Figure 2.

2. Configure the Cisco routers to run OSPF.

The following commands are used to configure Router1:

IOS MODE: ROUTER CONFIGURATION

`network NetaddrInvNetmask area AreaID`

Associates a network prefix with OSPF and associates an OSPF area to the network address. The prefix is specified with an IP address (Netaddr) and an inverse net mask (InvNetmask). For example, Netaddr=10.0.0.0 and InvNetmask=0.255.255.255 specify the network prefix 10.0.0.0/8 and the broadcast area AreaID is a number that associates an area with the address range. *Area 0* is reserved to specify the backbone area.

Example: To run OSPF on Router 1 for the address range 10.0.0.0/8 and assign it to Area 1, type

Router1(config-router)# network 10.0.0.0 0.255.255.255 area 1

`no network Netaddr InvNetmask area AreaID`

Disables OSPF for the specified network area.

`passive-interface Iface`

Sets interface Iface into passive mode. In passive mode, the router only receives and OSPF messages.

`router-id IPaddress`

Assigns the IP address IPaddress as the router identifier (router-id) of the local OSPF router. In OSPF, the router-id is used in LSA messages to identify a router. In IOS, by default, a router selects the highest IP address as the router-id. This commands can be used to set the value explicitly.

```
Router1> enable
Router1#configure terminal
Router1(config)#interface FastEthernet0/0
Router1(config-if)# no shutdown
Router1(config-if)#ip address 10.0.3.3 255.255.255.0
Router1(config-if)#interface FastEthernet0/1
Router1(config-if)# no shutdown
Router1(config-if)#ip address 10.0.2.3 255.255.255.0
Router1(config-if)#exit
Router1(config)# no ip routing
Router1(config)#ip routing
Router1(config)#no router rip
Router1(config)#router ospf 1
Router1(config-router)#network 10.0.0.0 0.255.255.255 area 1
Router1(config-if)#end
Router1#clear ip route *
```

These commands configure the IP addresses of the routers, disable RIP, and enable OSPF for Area 1 and network 10.0.0.0/8. Since no router-id is specified, the highest IP address of Router1, 10.0.3.3, is used as the router-id. The router-id can be verified by issuing the command show ip OSPF.

3. Set up the PCs as OSPF routers. Refer to Figure 2 for the connections and to Table 2 for the IP addresses. Use the following set of commands.

4. Now configure the PC's similar to the way you configured the routers

```
PC1% telnet localhost 2604
Password:zebra
ospfd>enable
ospfd#configure terminal
ospfd(config)#no router rip
ospfd(config)#router ospf
ospfd(config-router)#network 10.0.0.0/8 area 1
ospfd(config-router)#router-id 10.0.1.1
ospfd(config-router)#no passive-interface eth0
ospfd(config-router)#no passive-interface eth1
ospfd(config-router)#end
ospfd#exit
```

5. Enable ip_forwarding on all the PCs.

Observing convergence of OSPF

In comparison to the distance vector protocol RIP, the link state routing protocol OSPF

quickly adapts to changes in the network topology. In this exercise, you observe the interactions of OSPF after a change to the network topology.

1. On PC1, start to capture traffic with Wireshark on interface FastEthernet0/0. Set a filter to display only OSPF packets.

2. From PC3, run a trace command to PC4. Confirm from the output and Figure 2 whether the path from PC3 to PC4 includes Router3 or Router4.

3. Issue a ping command from PC3 to PC4 (10.0.7.7). Do not terminate the ping command until this exercise is completed.

4. If the path from PC3 to IP address 10.0.7.7 from Step 2 included Router3, then disconnect the Ethernet cable of FastEthernet0/1 interface of Router3. Otherwise, disconnect the Ethernet cable of FastEthernet0/1 interface of Router4. When the Ethernet cable is disconnected, the ping command on PC3 will show that IP address 10.0.7.7 is not reachable.

5. Now OSPF updates the routing tables. Use the Wireshark window on PC1 to observe the transmitted OSPF messages:

• How quickly are OSPF messages sent after the cable is disconnected?

• How many OSPF messages are sent?

• Which type of OSPF packet is used for flooding link state information?

• Describe the flooding of LSAs to all routers.

• Which type of encapsulation is used for OSPF packets (TCP, UDP, or other)?

• What is the destination address of OSPF packets?

6. Wait until the ping command is successful again, that is, ICMP Echo Reply messages arrive at PC3. This happens when the routing tables have been updated.

7. Stop the ping command and save the ping statics output.

• Count the number of lost packets and calculate the time it took OSPF to update the routing tables. (The ping command issues an ICMP Echo Request message approximately once every second.)

8. Issue another trace command from PC3 to IP address 10.0.7.7 By now, the output should show the new route to PC4.

9. Save the link state database on all Cisco routers to a file, and verify that all routers indeed have the same link state database.

• Compare the output of the command “show ip OSPF database” from the Cisco routers

10. Stop Wireshark on PC1, and save the different types of OSPF packets captured by

Wireshark. Save one copy of each type of OSPF packet that you observed. a) Pick a single link state advertisement packet captured by Wireshark, and describe how to interpret the information contained in the link state advertisement.

3. Border Gateway Protocol (BGP)

This provides some exposure to the inter domain Border Gateway Protocol (BGP), which determines paths between autonomous systems on the Internet.

BGP uses a path vector algorithm, where routers exchange full path information of a route. An important feature of BGP is that it can define routing policies, which can be used by a network to specify which type of traffic it is willing to process. The network configuration for this part is shown in Figure 3, and the IP configuration information is given in table 3. the network has three autonomous systems with AS numbers 100, 200 and 300. PC4, is used to capture the BGP packets transmitted between the ASs.

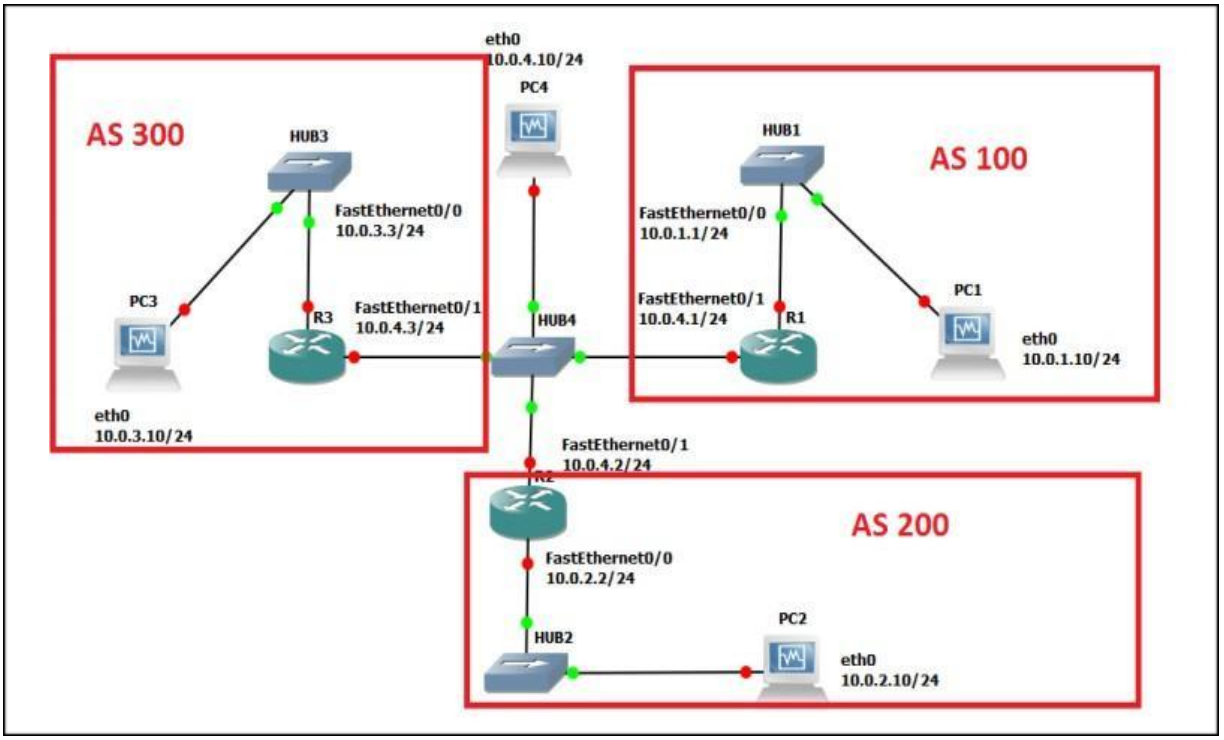

Figure 3 Network topology

VPCS	Ethernet Interface eth0	Ethernet Interface eth1
PC1	10.0.1.10 / 24	Disabled
PC2	10.0.2.10 / 24	Disabled
PC3	10.0.3.10 / 24	Disabled
PC4	10.0.4.10 / 24	Disabled

Cisco Routers	Ethernet Interface FastEthernet 0/0	Ethernet Interface FastEthernet 0/1
Router1	10.0.1.1 / 24	10.0.4.1 / 24
Router2	10.0.2.2 / 24	10.0.4.2 / 24
Router3	10.0.3.3 / 24	10.0.4.3 / 24

Table 3 IP addresses of the routers and PCs

Basic BGP configuration

Here, you configure the Cisco routers as BGP routers and you assign routers to autonomous systems. The configuration is completed when you can issue ping commands between any two PCs Next we summarize the Cisco IOS commands that are used to enable BGP.

IOS MODE: GLOBAL CONFIGURATION

`router bgp ASnumber`

Enables the BGP routing protocol and sets the autonomous system number to ASnumber.

The command enters the router configuration mode with the following prompt:

Router1(config-router)#

`no router bgp ASnumber`

Disables the BGP routing process.

IOS MODE: PREVILEGED EXEC

`show ipbgp`

Displays the BGP routing table.

`show ipbgp neighbors`

Displays the neighbors, also called peers, of this BGP router.

`show ipbgp paths`

Displays the BGP path information in the local database.

`clear ipbgp *`

Deletes BGP routing information

IOS MODE: ROUTER CONFIGURATION

`network Netaddr`

`network Netaddr mask netmask`

Specifies a network address that will be advertised by the local BGP process. A network mask maybe added to denote the length of the network prefix.

`neighbor IPaddress remote-as ASnumber`

Adds a neighbor to the BGP neighbor table. IPaddress is the IP address and ASnumber is the AS number of the neighbor.

`timers bgp keepalive holdtime`

Sets the values of the keep alive and hold time timers of the BGP process. BGP routers exchange periodic messages to confirm that the connection between the routers is maintained. The interval between these messages is keep alive seconds (default: 60 seconds). The number of seconds that a BGP router waits for any BGP message before it decides that a connection is down is specified by the hold time (default: 180 seconds).

1. Disable all RIP or OSPF processes that are running on the Cisco routers. Use the following command

2. Router1# no router ospf 1

   Router1# no router rip

3. Disable all RIP or OSPF processes running on the Linux PCs using the following command.

   For PC1, on the console at the prompt type:

   PC1% /etc/init.d/quagga stop

4. Assign the IP addresses to Ethernet interface eth0 of each PC as indicated in Table 3

5. Disable eth1 on the Linux PCs using the following command as shown in Table 3. For

6. PC1, on the console at the prompt type:

   PC1% ifconfig eth1 downPC1, PC2, and PC3 as follows: PC1% route add default gw 10.0.1.1/24

   PC2% route add default gw 10.0.2.2/24

   PC3% route add default gw 10.0.3.3/24

7. Start Wireshark on PC4 and set a display filter to capture only BGP packets.

8. Configure the Cisco routers to run BGP with the autonomous system numbers shown in Figure 3. The routers must know the AS number of their neighbors. Following is the configuration for Router2. Router 2 is in AS 200 and neighbors are AS 100 and AS 300.

9.

```
Router2> enable
Router2# configure terminal
Router2(config)#no ip routing
Router2(config)# ip routing
Router2(config)# interface FastEthernet0/0
Router2(config-if)# no shutdown
Router2(config-if)# ip address 10.2.2 255.255.255.0
Router2(config-if)# interface FastEthernet0/1
Router2(config-if)# no shutdown
Router2(config-if)# ip address 10.0.4.2 255.255.255.240
Router2(config-if)#router bgp 200
Router2(config-router)# neighbor 10.0.4.1 remote-as 100
Router2(config-router)# neighbor 10.0.4.3 remote-as 300
Router2(config-router)# network 10.0.2.0 mask 255.255.255.0
Router2(config-router)# end
Router2# clear ip bgp *
```

10. On PC1, issue a ping command to PC3. The command succeeds when BGP has converged.

11. Once the routing tables have converged, you see all the other AS entries in the BGP routing table. On each Cisco router, save the output of the following commands:

Router1# show ip route
Router1# show ip bgp

Router1# show ip bgp paths

• Describe the different types of BGP messages that you observe in the Wireshark window on PC4.

• Notice that BGP transmits messages over TCP connections. What is a reason that BGP uses TCP to transmit its messages?

• What is the IP address of the next-hop attribute for AS 100 on Router 2?

• What are the BGP peers in this topology?

12. Stop the Wireshark traffic capture on PC4 and save the BGP packets captured by Wireshark.

a) Use the output to provide answers to the questions in Step 7.

b) Which BGP message(s) contain(s) the AS-PATH information? Use a BGP message to illustrate your answer.

c) Use the saved output to provide a brief explanation of how the routers find the proper path between the autonomous systems.

BGP convergence

Disconnect one of the links between two BGP peers and observe how the BGP protocol reconfigures the paths.

1. After previous Exercise, save the output of the command show ip BGP neighbors on Router.2. Pay attention to the neighbor AS information.

2. On PC4, run Wireshark and set a display filter for BGP. Observe the flow of BGP packets between the autonomous systems.

3. On all routers, change the keep alive timer to 10 seconds and the hold time timer to 30 seconds. This speeds up the convergence time by a factor of 6 as compared to the default values. The following are the commands for Router2:

4. Disconnect the cable of interface FastEthernet0/1 on Router1.

- From the output you saved, describe how the BGP routers learn that a link is down. (Hint: Look at the BGP State field)

- Which BGP messages indicate that there is a link problem? Use a BGP message to answer the question.

5. Use the command show ip BGP neighbors on Router2 and Router3 to obtain the neighbor information. Save the output.

6. Wait until BGP converges. Save the routing tables on Router2 and Router3. What can you say?

7. Stop the Wireshark traffic captured on PC4 and save the Wireshark BGP packets.

a) From the output you saved, describe how the BGP routers learn that a link is down. (Hint: Look at the BGP State field)

b) Which BGP messages indicate that there is a link problem? Use a BGP message to answer the question.

Conclusion:

Hence we have configured RIP, OSPF and BGP using packet tracer.