Assignment No. B_7

Title: To understand Configure RIP/OSPF/BGP using packet Tracer.

OBJECTIVES:

1.To understand Configure RIP/OSPF/BGP using packet Tracer.

Problem Statement: Configure RIP/OSPF/BGP using packet Tracer.

Theory:

Static Routing:

Typically used in hosts Enter subnet mask, router (gateway), IP address Perfect for cases with few connections, doesn't change much E.g. host with a single router connecting to the rest of the Internet IP: 128.1.1.100

Dynamic Routing:

Most routers use dynamic routing Automatically build the routing tables As we saw previously, there are two major approaches

Link State Algorithms

Distance Vector Algorithms

First some terminology

AS = Autonomous System

Contiguous set of networks under one administrative authority

Common routing protocol

E.g. University of Alaska Statewide, Washington State University

E.g. Intel Corporation

A connected network

There is at least one route between any pair of nodes

RIP (Routing Information Protocol)

Distance vector algorithm

Open Standard Protocol

Classful routing protocol

Administrative Distance is 120

Distance metric: # of hops (max = 15 hops)

Distance vectors: exchanged every 30 sec via Response Message (also called advertisement)

Each advertisement: route to up to 25 destination nets

RIP: Link Failure and Recovery

If no advertisement heard after 180 sec neighbor/link declared dead

routes via neighbor invalidated

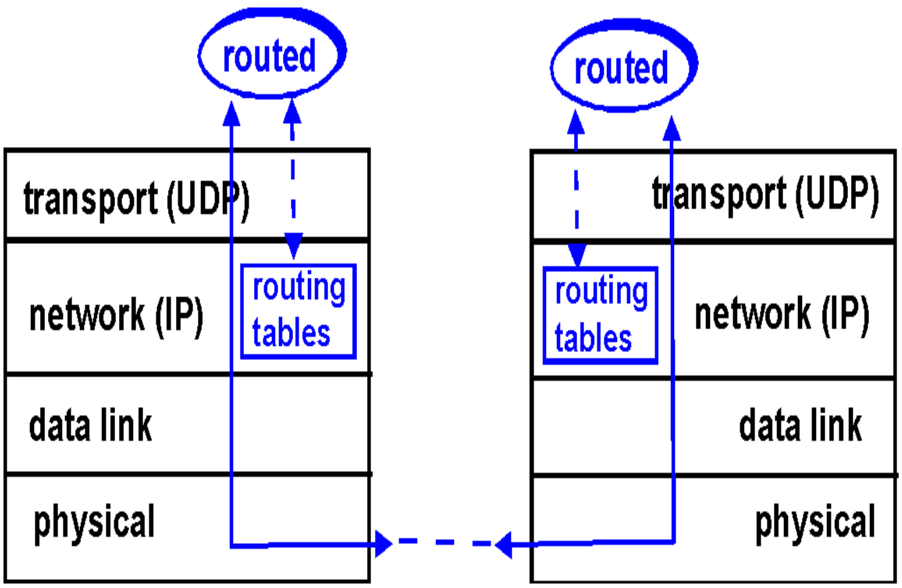
new advertisements sent to neighbors

neighbors in turn send out new advertisements (if tables changed)

link failure info quickly propagates to entire net

RIP Table processing

RIP routing tables managed by application-level process called route-d (daemon) advertisements sent in UDP packets, periodically repeated Why UDP?



RIP:

Advantages

Simplicity ; little to no configuration, just start routed upPassive version for hosts
If a host wants to just listen and update its routing table.

OSPF (Open Shortest Path First)

“Open”: publicly available

RFC 2328

Uses Link State algorithm

LS packet dissemination

Topology map at each node

Route computation using Dijkstra’s algorithm

OSPF advertisement carries one entry per neighbor router Metric is cost

Administrative Distance 110

Conceived as a successor to RIP

OSPF “advanced” features (not in RIP):

Security: all OSPF messages authenticated (to prevent malicious intrusion); TCP connections used Multiple same-cost paths allowed (only one path in RIP) For each link, multiple cost metrics for different Type Of Service (e.g., satellite link cost set “low” for best effort; high for real time) Integrated uni- and multicast support: Multicast OSPF (MOSPF) uses same topology data base as OSPF Hierarchical OSPF in large domains.

BGP Terminology:

Autonomous System :A collection of networks under a single administrative domain

Inter-domain Routing : Routing between the customer and the service provider

Internal Routing: Uses IGP protocol (RIP OSPF) to exchange routing information inside the AS

External Routing: Uses EGP protocol(BGP) to exchange routes between AS

IBGP: When BGP is used inside an AS

EBGP: When BGP is used between AS

Configuring BGP:

The last part of this lab provides some exposure to the inter domain Border Gateway Protocol (BGP), which determines paths between autonomous systems on the Internet. The exercises in this lab cover only the basics of BGP. Essentially, you learn how to set up an autonomous system and observe BGP traffic between autonomous systems. 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 current version of BGP, which is also used in the following exercise, is BGP version 4 (BGP-4).

The network configuration for this part is shown in Figure 4.6, and the IP configuration information is given in table 4.5. 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.

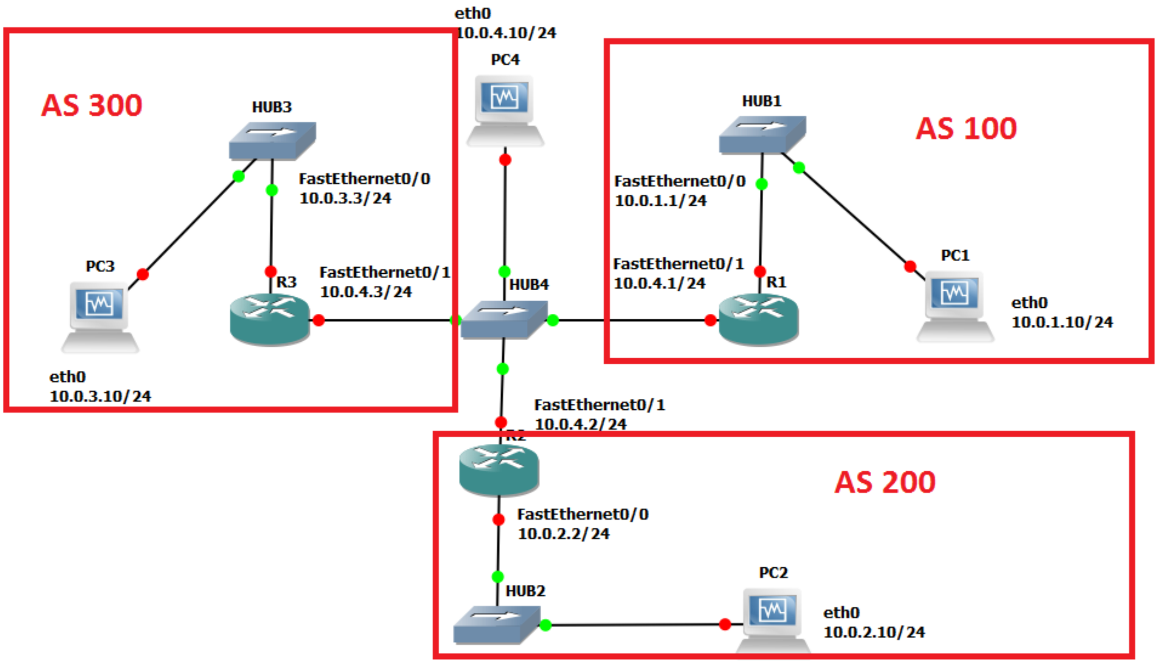


Figure 4.6 Network topology for Part 7.

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 4.5 IP addresses of the routers and PCs for Part 7.

Exercise 7(A). 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 commands:

   Router1# no router ospf 1
   Router1# no router rip

2. 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

3. Assign the IP addresses to Ethernet interface eth0 of each PC as indicated in Table 4.5

4. Disable eth1 on the Linux PCs using the following command as shown in Table 4.5.

For PC1, on the console at the prompt type:

PC1% ifconfig eth1 down

5. Add a default gateway to PC1, 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

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

7. Configure the Cisco routers to run BGP with the autonomous system numbers shown in Figure 4.6. 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.

```
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 *
```

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

9. 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?

10. 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.

Exercise 7(B). BGP convergence

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

1. After completing Exercise 6(A), save the output of the command show ip BGP neighbors on Router2. 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 keepalive timer to 10 seconds and the holdtime 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:

```
Router2# configure terminal
Router2(config)#router bgp 200
Router2(config-router)# timers bgp 10 30
Router2(config-router)#end
Router2#clear ip bgp *
```

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: Thus we have studied Configure RIP/OSPF/BGP using packet Tracer.