جامعة بيرزيت

BIRZEIT UNIVERSITY

Faculty of Engineering and Technology Electrical and Computer Engineering Department

ENCS4130 || Computer Networks Laboratory

Report 1

Lab 5: Dynamic Routing 3 (Path Vector) BGP

Prepared By: Eman Asfour 1200206

Instructor: Dr. Ismail Khater

T.A: Eng. Burhan Dar Assi

Section: 2

Date of Lab participation: 27/03/2024

Date of submission: 10/4/2024

Place: Masri503

1. *Abstract*:

The objective of this lab is to construct and simulate a particular network topology utilizing Cisco Packet Tracer, incorporating Cisco routers, switches, and PCs. IP routing is configured dynamically, employing OSPF as an internal routing protocol, and BGP as the external routing protocol.

Table of Contents

Tables of Figures

List of Figures

2. Theory:

i. Border Gateway Protocol:

BGP is an interdomain routing protocol utilizing path-vector routing. It serves as a gateway protocol facilitating the exchange of routing information among autonomous systems on the internet. Understanding BGP's history and the various types of autonomous systems it interacts with is crucial, especially given its widespread use across diverse network infrastructures. [1]

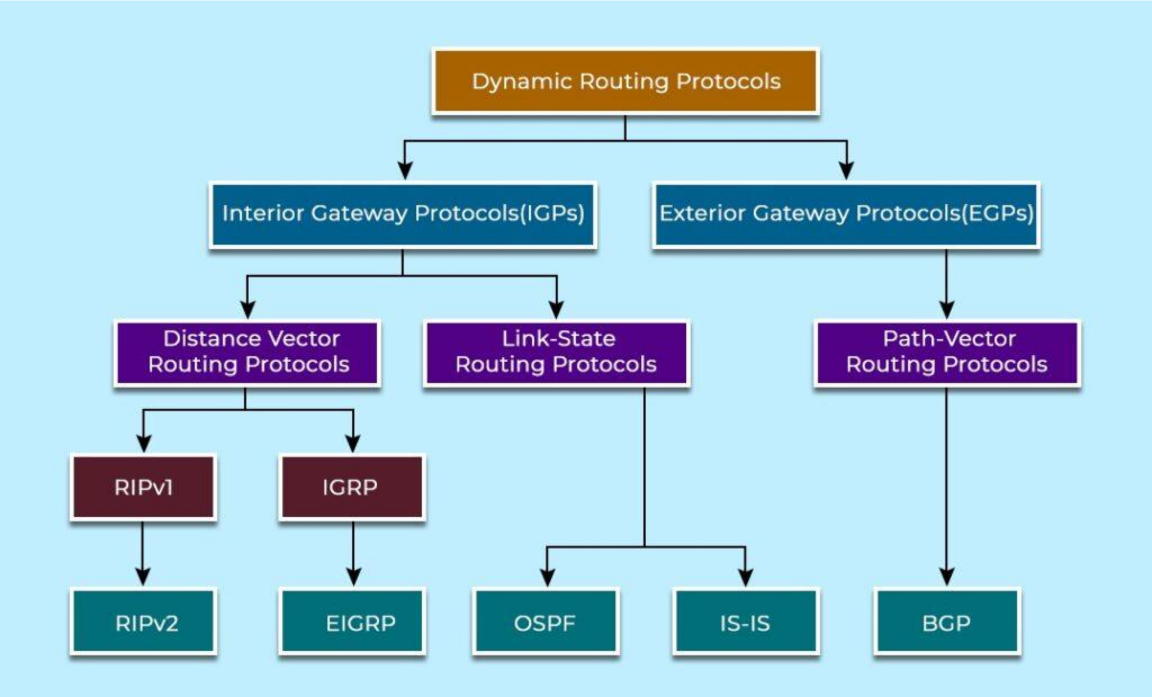

Dynamic Routing Protocols
Interior Gateway Protocols(IGPs)
Exterior Gateway Protocols(EGPs)
Distance Vector Routing Protocols
Link-State Routing Protocols
Path-Vector Routing Protocols
RIPv1
IGRP
RIPv2
EIGRP
OSPF
IS-IS
BGP

Figure 1: computer networks [2]

ii. BGP Autonomous Systems

An autonomous system is essentially a collection of networks administered under a single entity. Whether it's a company with routers spread across various locations or an organization managing a network infrastructure, all routers within the system are recognized by a single autonomous number. Within such systems, Interior Gateway Protocols (IGPs) like RIP, IGRP, EIGRP, and OSPF are commonly deployed for internal routing. However, when it comes to exchanging information between different autonomous systems, Exterior Gateway Protocols (EGPs) come into play. These protocols facilitate communication between distinct autonomous systems, allowing for the exchange of routing information across organizational boundaries. Border Gateway Protocol (BGP) emerges as a critical protocol in this context. It operates at the core of the internet, enabling communication between separate autonomous number systems. BGP serves as the backbone of internet routing, allowing internet service providers to manage and regulate the flow of routing information between independent entities. [3]

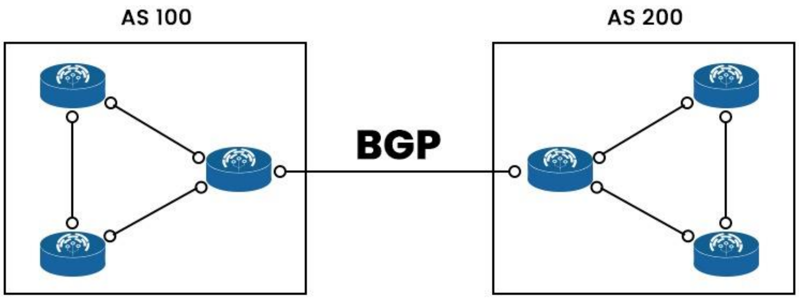


Figure 2: BGP in computer networks [2]

iii. Employing BGP

There's a common misconception that BGP isn't necessary in scenarios requiring multiple internet connections. Some believe that Internal Gateway Protocols (IGPs) like OSPF or EIGRP are sufficient for managing redundancy or fault tolerance in outgoing traffic. Similarly, if there's only one connection to an external Autonomous System (AS), such as the Internet, BGP might seem redundant. However, with the Internet comprising over 100,000 routes, it's crucial to avoid overburdening internal routers. Nevertheless, BGP proves essential in specific situations: when multiple connections to external ASs (e.g., the Internet) exist through various providers; if connections to external ASs via the same provider are through different central offices or routing policies; and when the current routing infrastructure can handle increased traffic effectively. The main advantage of BGP lies in its capability to regulate traffic flow entering and exiting the local AS. To establish a BGP connection, the command "Router (config)# router bgp <AS-Number>" is utilized. [4]

iv. *BGP Neighbors and peers*

In networking, the terms 'neighbor' and 'peer' are often used interchangeably, both referring to routers with established BGP sessions. These sessions allow for the exchange of BGP updates based on administrator-defined routing policies. Peering, derived from peer-to-peer networking, is the process of connecting to another BGP-speaking device. To establish a neighbor relationship with a router in a different AS (eBGP Peer), the command "Router (config-router) # neighbor <IP-Address-Next-Interface> remote-as <AS-REMOTE_NEIGHBOR>" is used. BGP Peer Session Phases: The BGP finite-state machine (FSM) outlines the various phases a BGP peer session undergoes during formation. It starts in the idle state and transitions to the Connect state while awaiting a TCP connection with the remote peer. A successful connection leads to the sending of an OPEN message, whereas an unsuccessful attempt results in the Active state. In the Active state, BGP retries establishing a TCP connection and, upon success, sends an OPEN message; otherwise, it waits for a Connect Retry period before returning to the Connect state. Transitioning to the Open Sent state occurs after establishing a TCP connection and sending an OPEN message. Here, the BGP peer awaits a reply OPEN message and sends a KEEPALIVE message. Upon receiving the reply KEEPALIVE message, the state progresses to Open Confirm, followed by the Established state, where full BGP peer session establishment enables the exchange of UPDATE messages containing routing information. Persistent Active state sessions may indicate issues such as lack of IP connectivity, incorrect neighbor statements, or TCP port 179 access-list filtering.

3. Procedure

a) Build the Topology

The topology was manually constructed, incorporating subnetting for all PCs and routers. OSPF was configured using the commands `` ***Router(config)# router ospf <PROCESS-ID>*` and `*Router(config-router)# network <ID-ADDRESS> <WILDCARD-MASK> area <AREA-ID>*** ``. Validation was performed by sending a packet (message) to ensure correctness. The path between Router 1 and Router 2, or network **192.6.0.4/30**, was intentionally maintained to facilitate the BGP link.

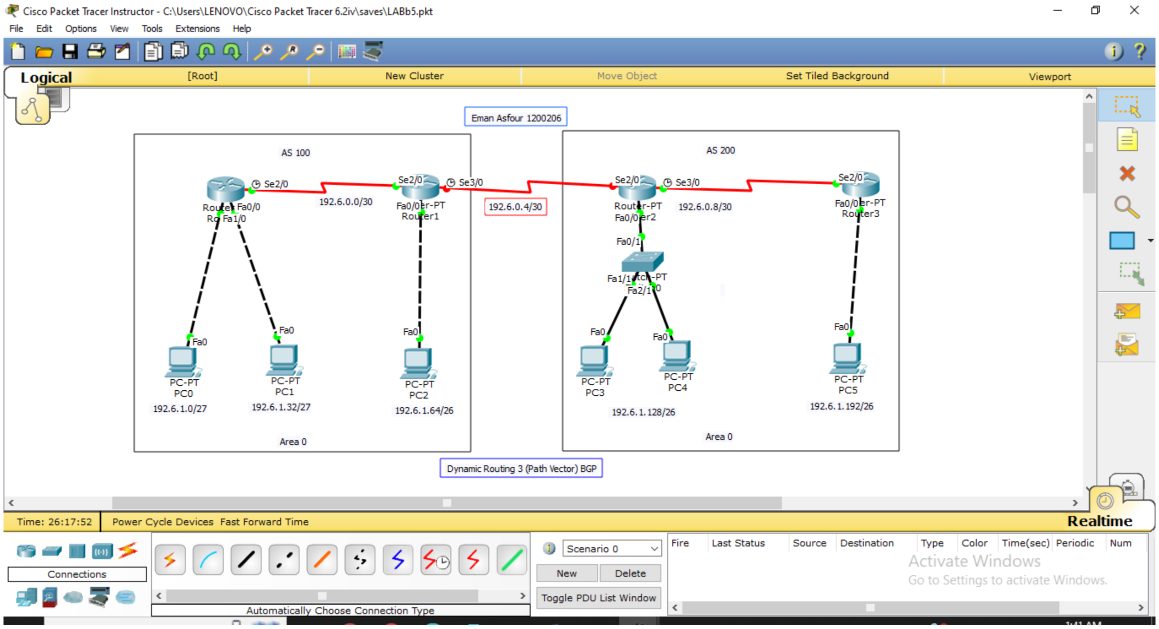


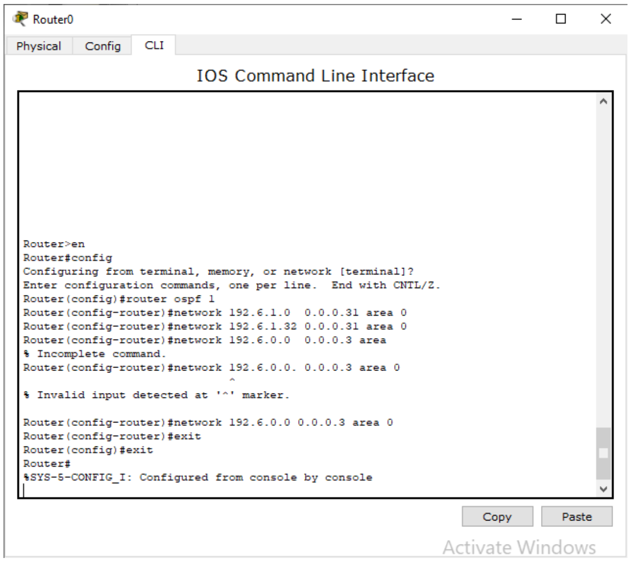
Figure 3: Topology

This network setup consists of two autonomous systems, AS 100 and AS 200. In AS 100, Router 0 and Router 1 are connected via a serial link, while Router 0 is linked to PC0 and PC1 through Fast Ethernet interfaces, and Router 1 is connected to PC2. In AS 200, Router 2 and Router 3 are connected through a serial link, with Router 2 linked to PC3 and PC4, and Router 3 linked to PC5. Additionally, BGP links exist between Router 1 and Router 2, as well as between Router 2 and Router 3. These connections facilitate communication within and between the autonomous systems, forming the network infrastructure.

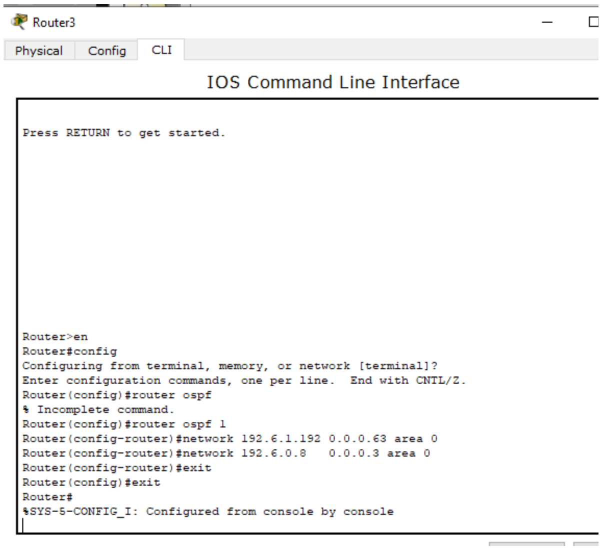
Table 1:Networks IPS

Area/AS & BGP Links	***Network***	***Device***	***Interface***	***IP***	***Subnet Mask***	***Wildcard Mask***
Area 0 / AS 100	192.6.0.0/30	Router 0	Se2/0	192.6.0.1	255.255.255.252	0.0.0.3
		Router 1	Se2/0	192.6.0.2	255.255.255.252	0.0.0.3
	192. 6.1.0/27	Router 0	Fa1/0	192.6.1.1	255.255.255.224	0.0.0.31
		PC0	Fa0	192.6.1.2	255.255.255.224	0.0.0.31
	192. 6.1.32/27	Router 0	Fa0/0	192.6.1.33	255.255.255.224	0.0.0.31
		PC1	Fa0	192.6.1.34	255.255.255.224	0.0.0.31
	192. 6.1.64/26	Router 1	Fa0/0	192.6.1.65	255.255.255.192	0.0.0.63
		PC2	Fa0	192.6.1.66	255.255.255.192	0.0.0.63
Area 0 / AS 200	192.6.0.8/30	Router 2	Se3/0	192.6.0.9	255.255.255.252	0.0.0.3
		Router 3	Se2/0	192.6.0.10	255.255.255.252	0.0.0.3
	192.6.1.128/26	Router 2	Fa0/0	192.6.1.129	255.255.255.192	0.0.0.63
		PC3	Fa0	192.6.1.130	255.255.255.192	0.0.0.63
		PC4	Fa0	192.6.1.131	255.255.255.192	0.0.0.63
	192.6.1.192/26	Router 3	Fa0/0	192.6.1.193	255.255.255.192	0.0.0.63
		PC5	Fa0	192.6.1.194	255.255.255.192	0.0.0.63
BGP Links	192.6.0.4/30	Router 1	Se3/0	192.6.0.5	255.255.255.252	0.0.0.3
		Router 2	Se2/0	192.6.0.6	255.255.255.252	0.0.0.3

b) Configuring OSPF Routing



```
Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.6.1.0  0.0.0.31 area 0
Router(config-router)#network 192.6.1.32 0.0.0.31 area 0
Router(config-router)#network 192.6.0.0  0.0.0.3 area
% Incomplete command.
Router(config-router)#network 192.6.0.0. 0.0.0.3 area 0
                              ^
% Invalid input detected at '^' marker.

Router(config-router)#network 192.6.0.0 0.0.0.3 area 0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```



```
Press RETURN to get started.




Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf
% Incomplete command.
Router(config)#router ospf 1
Router(config-router)#network 192.6.1.192 0.0.0.63 area 0
Router(config-router)#network 192.6.0.8   0.0.0.3 area 0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

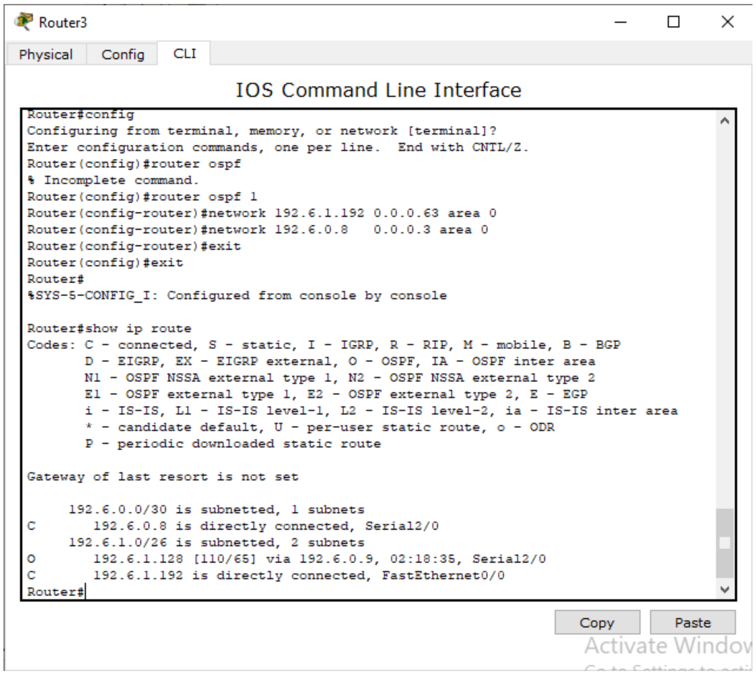
Figure 4: Configuring OSPF of Router 0 & Router 3

The OSPF routing protocol was configured individually for the two Autonomous Systems (AS 100 and 200), with routers 0, 1, 2, and 3 excluding the BGP link from the OSPF configuration. The command used was:

Router (config) # router ospf 1

Router (config-router) # network <ip address> <wildcard mask> <area number>

Establishing the OSPF routing protocol allows communication between two autonomous systems, AS 100 and AS 200. This setup is essential for optimizing routing forms and ensuring data transmission efficiency inside each autonomous system. OSPF, known for its ability to dynamically determine the shortest path between routers, is important for improving network performance. Enhanced reliability and decreased latency can be achieved by implementing OSPF for AS 100 and AS 200, contributing to a more flexible and quick communication building.



```
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf
% Incomplete command.
Router(config)#router ospf 1
Router(config-router)#network 192.6.1.192 0.0.0.63 area 0
Router(config-router)#network 192.6.0.8   0.0.0.3 area 0
Router(config-router)#exit
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

     192.6.0.0/30 is subnetted, 1 subnets
C       192.6.0.8 is directly connected, Serial2/0
     192.6.1.0/26 is subnetted, 2 subnets
O       192.6.1.128 [110/65] via 192.6.0.9, 02:18:35, Serial2/0
C       192.6.1.192 is directly connected, FastEthernet0/0
Router#
```

Figure 5: Testing OSPF

c) Configuring BGP Routing

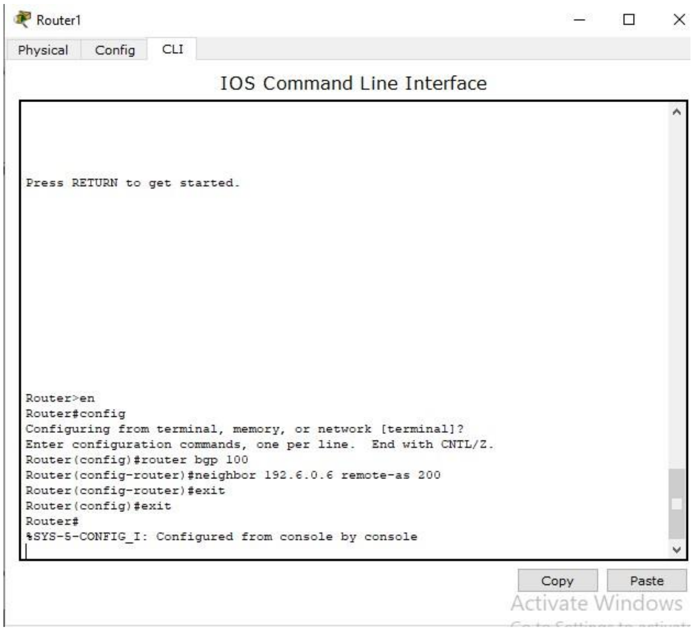
For the BGP setup, the requirement was solely for Routers 1 and 2. Initially, BGP was enabled and the Autonomous System (AS) of the router was specified. BGP was enabled, and the router's Autonomous System (AS) was specified by entering the command:

BGP was enabled, and the Autonomous System (AS) of the router was specified by entering the command:

Router (config) # router bgp <AS-Number>

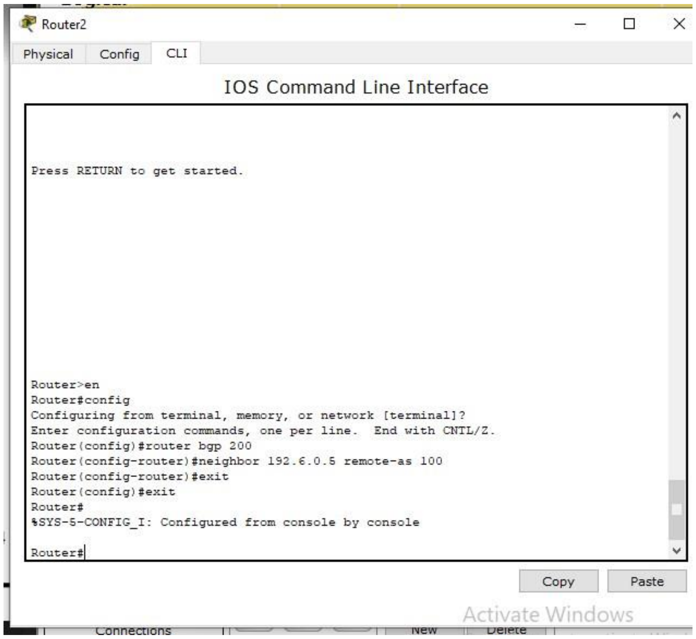
Where the AS number was assigned corresponding to the autonomous system where the router was located. Subsequently, a neighbor relationship with a router in a different AS (eBGP Peer) was established. A neighbor relationship was established with a router in a different AS (eBGP Peer) using the command:

Router (config-router) # neighbor <IP-Address-Next-Interface> remote-as <AS-OF-NEIGHBOR>



```
Press RETURN to get started.




Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 100
Router(config-router)#neighbor 192.6.0.6 remote-as 200
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 6: Configuring BGP of Router 1



```
Press RETURN to get started.








Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 200
Router(config-router)#neighbor 192.6.0.5 remote-as 100
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

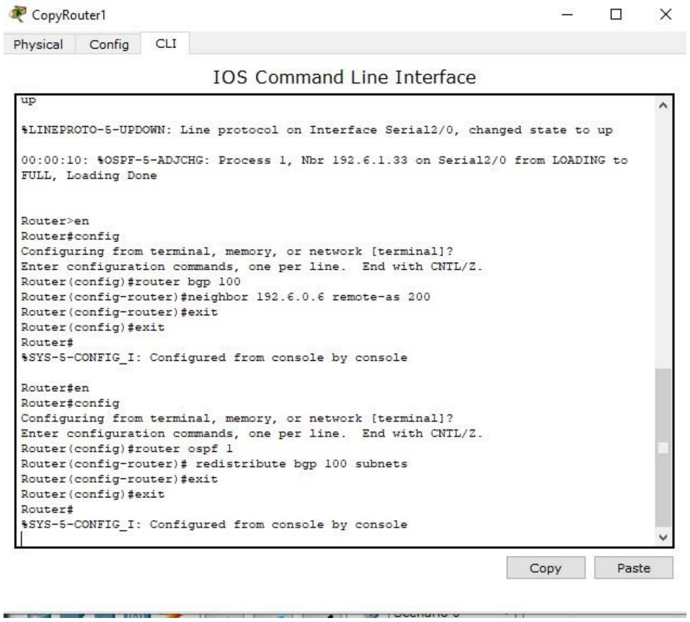
Figure 7: Configuring BGP of Router 2

The spotlight shifts to configuring BGP (Border Gateway Protocol) routing, focusing on Routers 1 and 2. BGP is enabled, and each router is assigned an Autonomous System (AS), representing its location. Next, a neighbor relationship is established with a router in a different AS, termed a BGP Peer. This foundational setup ensures effective BGP routing for Routers 1 and 2, enabling smooth interaction and route exchange between diverse autonomous systems.

d) Define the BGP over the OSPF

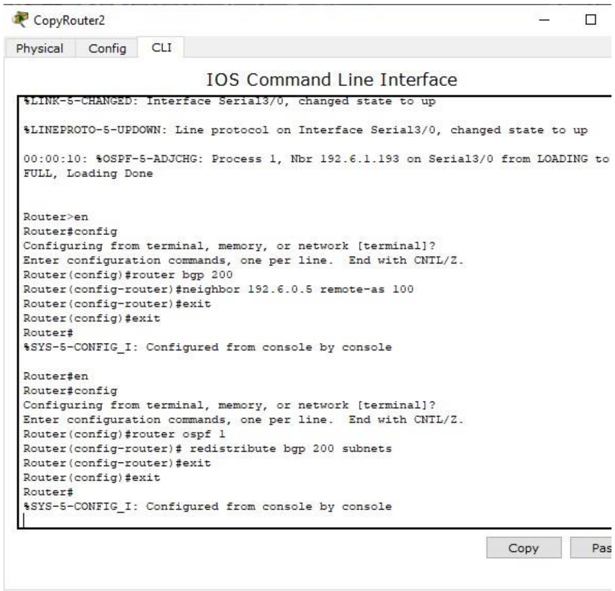
To establish communication between OSPF and BGP, the redistribution command is utilized to integrate the BGP protocol within the OSPF framework. Initially, the OSPF ID is specified with the command "***Router (config)# router ospf <PROCESS-ID***>." Subsequently, the redistribution of BGP routes into OSPF is configured using the command "***Router(config-router) # redistribute bgp <AS-NUMBER> subnets***." This process ensures that OSPF is informed of BGP routes and can incorporate them into its routing table. An example of this configuration involves setting the OSPF ID to 1 with the command "***Router(config)# router ospf 1***" and redistributing BGP routes with autonomous number 100 into OSPF using the command "***Router(config-router) # redistribute bgp 100***

subnets." This integration facilitates seamless communication and route exchange between OSPF and BGP, thereby enhancing network connectivity and efficiency.



```
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.6.1.33 on Serial2/0 from LOADING to
FULL, Loading Done


Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 100
Router(config-router)#neighbor 192.6.0.6 remote-as 200
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)# redistribute bgp 100 subnets
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 8: Define the BGP over the OSPF of router 1

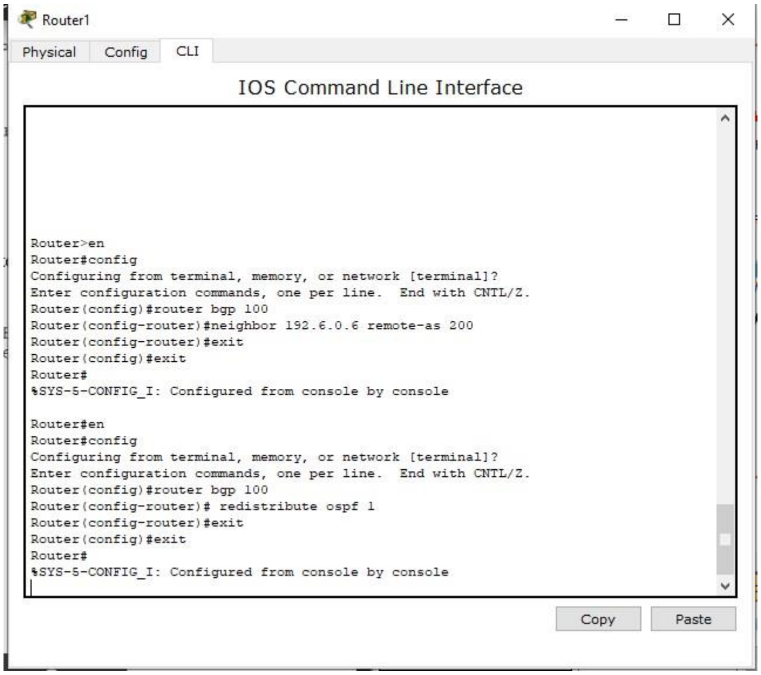


```
%LINK-5-CHANGED: Interface Serial3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.6.1.193 on Serial3/0 from LOADING to
FULL, Loading Done


Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 200
Router(config-router)#neighbor 192.6.0.5 remote-as 100
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)# redistribute bgp 200 subnets
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 9: Define the BGP over the OSPF of router 2

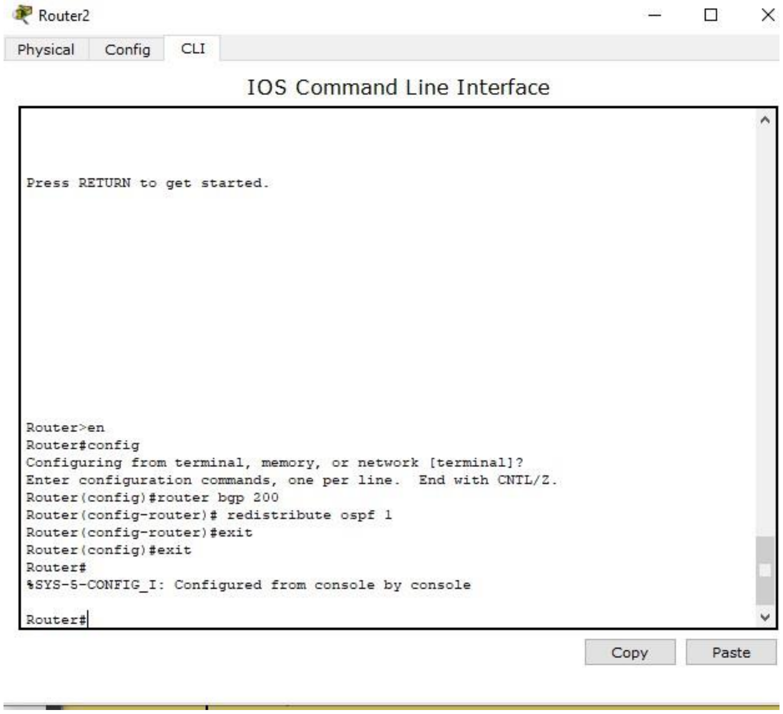
e) Define the OSPF over the BGP

To establish OSPF connectivity with BGP, the OSPF protocol is incorporated within the BGP framework using a redistribute command: Initially, the BGP router's Autonomous System (AS) number is configured, with the command "***Router(config)# router bgp <AS-NUMBER***>."Subsequently, OSPF routes are redistributed into BGP, utilizing the command ***"Router(config-router) # redistribute ospf <PROCESS-ID>."***For example, in this setup's implementation, the BGP router's AS number is configured as 100 via the command "***Router (config) # router bgp 100***," followed by redistributing OSPF routes with process ID 1 using the command "***Router (config-router) # redistribute ospf 1***."This integration ensures seamless communication and route exchange between OSPF and BGP, enhancing network interoperability and efficiency.



```
Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 100
Router(config-router)#neighbor 192.6.0.6 remote-as 200
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 100
Router(config-router)# redistribute ospf 1
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 10: Define the OSPF over the BGP of router 1

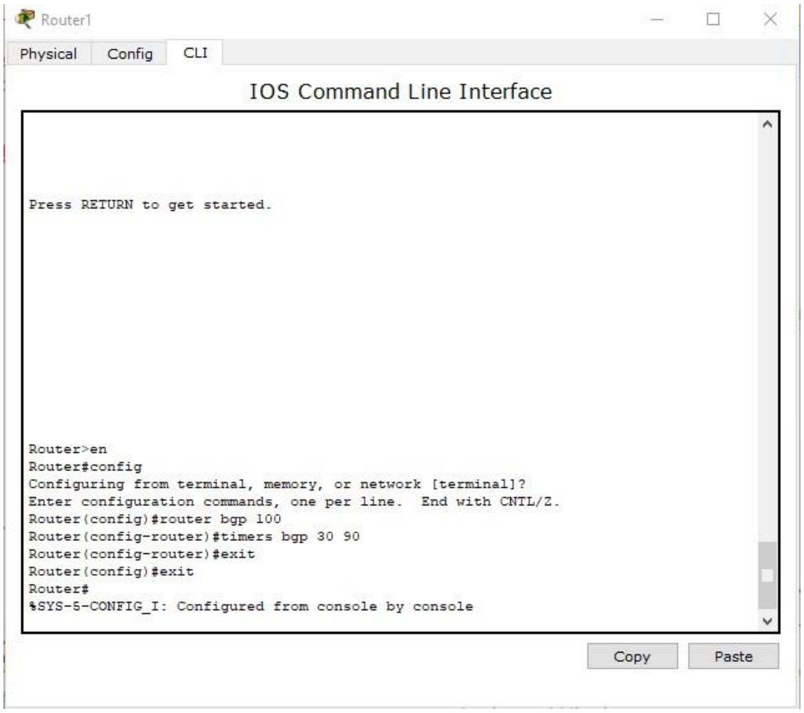


```
Press RETURN to get started.



Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 200
Router(config-router)# redistribute ospf 1
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Figure 11: Define the OSPF over the BGP of router 2

f) Configuring BGP Timers

By default, router timers update automatically. If Hold-time timers between peers differ, the session forms, prioritizing the smaller timer value. To set keep alive and hold times for routers 1 to 30 and 90, respectively: Enter ***"Router (config)# router bgp 100***" to specify the BGP router. Then, use "**Router (config-router) # timers bgp 30 90"** to set a 30-second keep alive timer and a 90-second hold time. These adjustments ensure efficient routing and communication while balancing responsiveness and stability. Automatic timer updates are the default behavior of BGP routers, with preference given to the lesser preset Hold-time timer when timers differ among peers. To specify specific keep alive and hold times for Router 1, the command "router bgp 100" followed by "timers bgp 30 90" is employed, configuring a 30-second keep alive timer and a 90-second hold time. This adjustment is implemented as depicted in Figure 12. When adjusting BGP timers, it's crucial to consider the network's characteristics, size, and stability. In real-world scenarios, these durations often necessitate fine-tuning to achieve a balance between responsiveness and control plane efficiency.



```
Press RETURN to get started.









Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 100
Router(config-router)#timers bgp 30 90
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 12: Configuring BGP Timers on router 1

4. Results

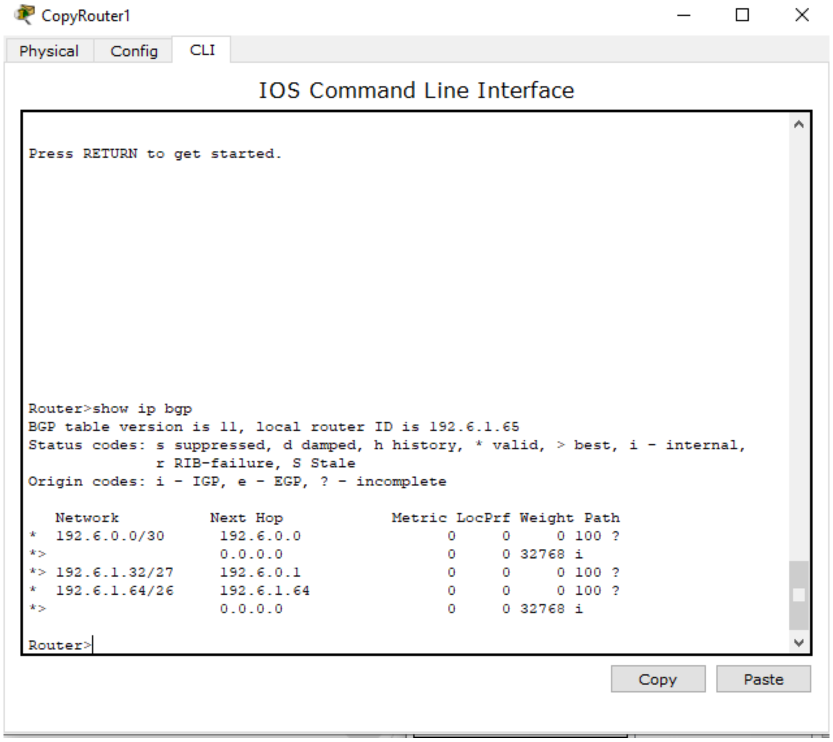
a) Viewing BGP Neighbors

The status of all BGP neighbors was examined using the following commands:

"Router# show ip bgp"

"Router# show ip bgp summary"

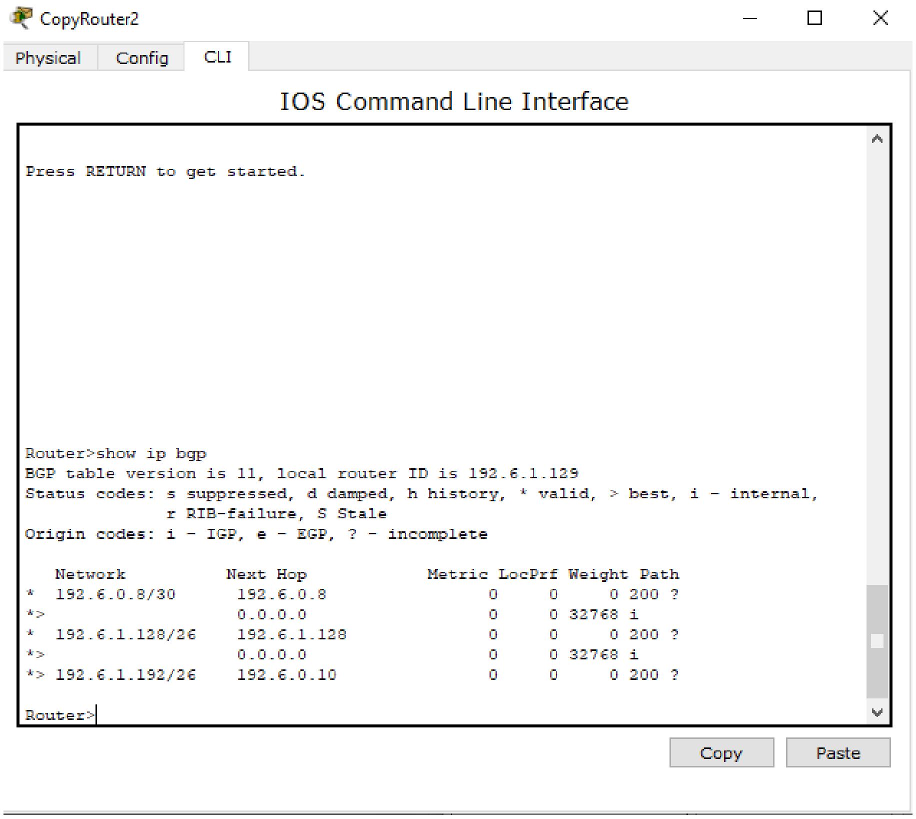
"Router# show IP route"



```
Press RETURN to get started.





Router>show ip bgp
BGP table version is 11, local router ID is 192.6.1.65
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  192.6.0.0/30      192.6.0.0                0      0      0 100 ?
*>                   0.0.0.0                  0      0  32768 i
*> 192.6.1.32/27     192.6.0.1                0      0      0 100 ?
*  192.6.1.64/26     192.6.1.64               0      0      0 100 ?
*>                   0.0.0.0                  0      0  32768 i

Router>
```

Figure 13: Show IP BGP of router1

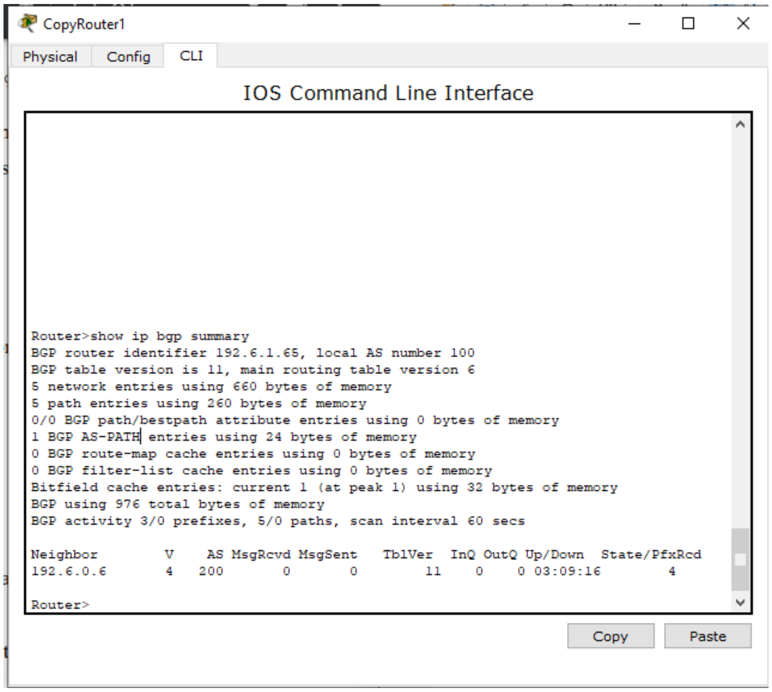
This BGP figure 13 displays the routes learned by the router. Each entry includes information such as the network prefix, next hop IP address, metrics, and path attributes. The ">" symbol indicates the best path to reach a particular network, while "*" denotes a valid route.



```
Press RETURN to get started.








Router>show ip bgp
BGP table version is 11, local router ID is 192.6.1.129
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  192.6.0.8/30      192.6.0.8                0      0      0 200 ?
*>                   0.0.0.0                  0      0 32768 i
*  192.6.1.128/26    192.6.1.128              0      0      0 200 ?
*>                   0.0.0.0                  0      0 32768 i
*> 192.6.1.192/26    192.6.0.10               0      0      0 200 ?

Router>
```

Figure 14: Show IP BGP for router 2

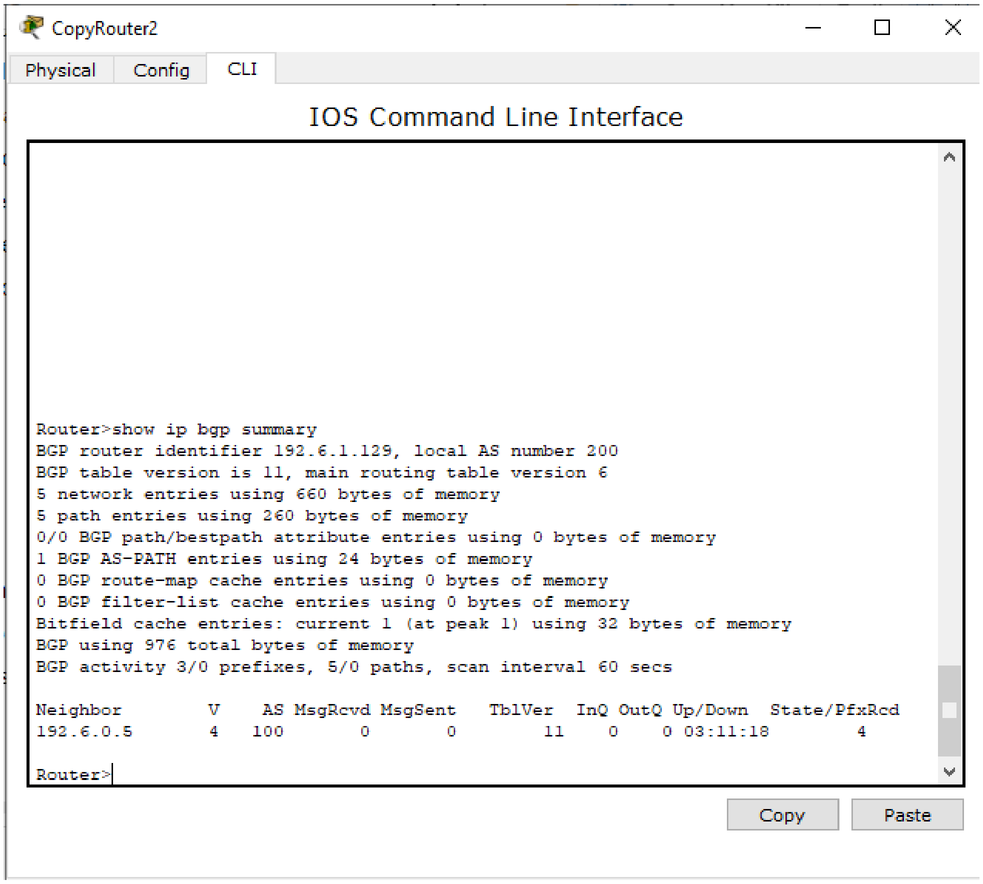
This BGP table output provides a snapshot of the routes learned by the router. Each entry includes details such as the network prefix, next-hop IP address, metrics, and path attributes. The ">" symbol indicates the best path to reach a specific network, while "*" denotes a valid route. In this output, the router has learned routes for networks 192.6.0.8/30, 192.6.1.128/26, and 192.6.1.192/26. These routes are associated with the Autonomous System (AS) number 200. Additionally, the next-hop IP addresses indicate the routers through which these networks are reachable.



```
Router>show ip bgp summary
BGP router identifier 192.6.1.65, local AS number 100
BGP table version is 11, main routing table version 6
5 network entries using 660 bytes of memory
5 path entries using 260 bytes of memory
0/0 BGP path/bestpath attribute entries using 0 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 976 total bytes of memory
BGP activity 3/0 prefixes, 5/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.6.0.6       4   200       0       0       11    0    0 03:09:16        4

Router>
```

Figure 15: Show IP BGP of router 1

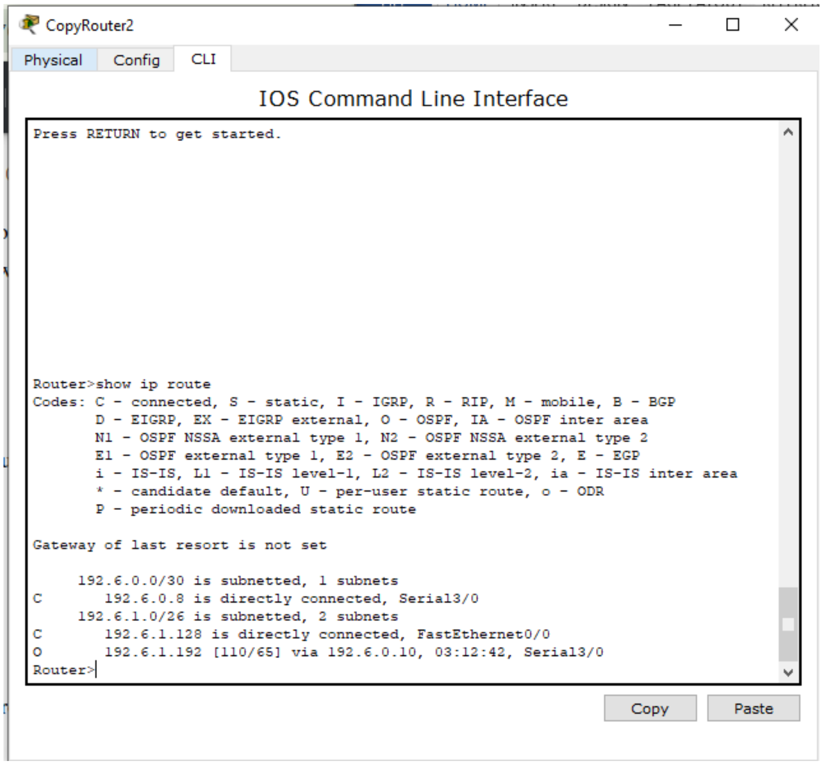
This output from "show ip bgp summary" provides an overview of the BGP status on the router. It indicates that the router's BGP router identifier is 192.6.1.65, with a local AS number of 100. The BGP table version is 11, and the main routing table version is 6. There are 5 network entries in the BGP table, and it's worth noting that the path entries are dependent on the IP addresses. Additionally, the memory usage for various BGP components is provided, with details such as BGP activity and neighbor information. In this case, the router has one neighbor (192.6.0.6) in AS 200, with a stable connection for 03:09:16 and four prefixes received from this neighbor.



```
Router>show ip bgp summary
BGP router identifier 192.6.1.129, local AS number 200
BGP table version is 11, main routing table version 6
5 network entries using 660 bytes of memory
5 path entries using 260 bytes of memory
0/0 BGP path/bestpath attribute entries using 0 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 976 total bytes of memory
BGP activity 3/0 prefixes, 5/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.6.0.5       4   100       0       0       11    0    0 03:11:18        4

Router>
```

Figure 16: Show IP BGP summary of router 2

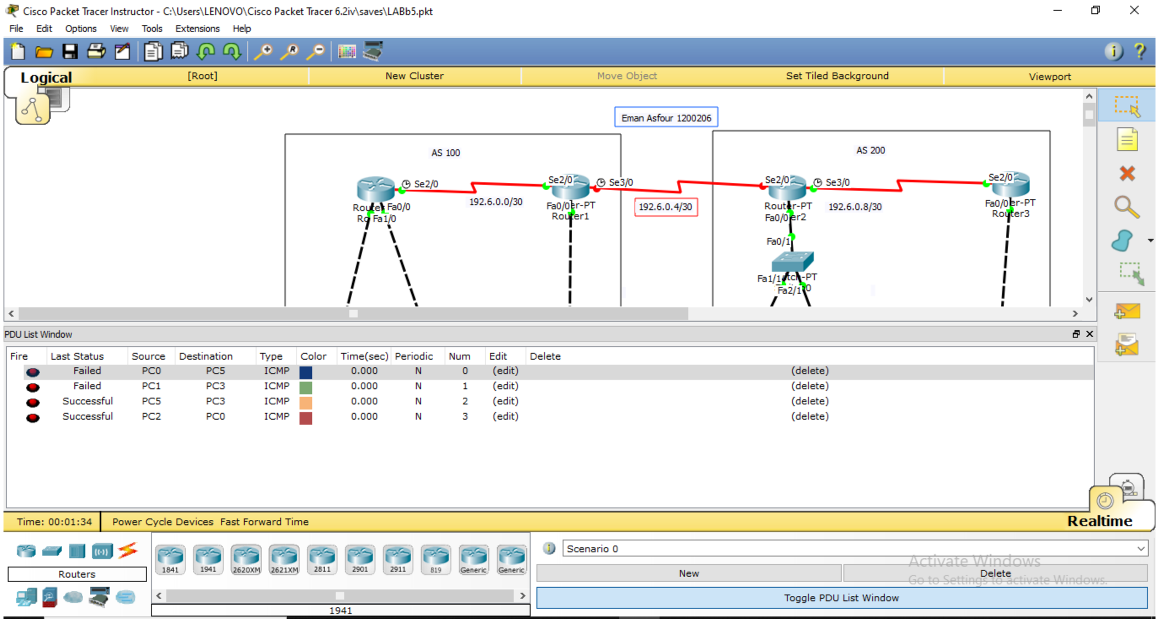
This output from "show ip bgp summary" provides an overview of the BGP status on Router 2. It indicates that the BGP router identifier for Router 2 is 192.6.1.129, with a local AS number of 200. The BGP table version is 11, and the main routing table version is 6. There are 5 network entries in the BGP table, with corresponding path entries. Additionally, the memory usage for various BGP components is provided, with details such as BGP activity and neighbor information. In this case, the neighbor 192.6.0.5 is in AS 100, and the connection has been up for 03:11:18, with four prefixes received from this neighbor.



```
Press RETURN to get started.








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

     192.6.0.0/30 is subnetted, 1 subnets
C       192.6.0.8 is directly connected, Serial3/0
     192.6.1.0/26 is subnetted, 2 subnets
C       192.6.1.128 is directly connected, FastEthernet0/0
O       192.6.1.192 [110/65] via 192.6.0.10, 03:12:42, Serial3/0
Router>
```

Figure 17: Show IP route of router 2

This output from "show ip route" displays the routing table on the router. It provides information about the various routes known to the router, including their network prefixes, route types, and next-hop information. In this case, the router has three routes: The network 192.6.0.0/30 is directly connected via Serial3/0, with a directly connected interface address of 192.6.0.8.The network 192.6.1.0/26 is directly connected via FastEthernet0/0, with a directly connected interface address of 192.6.1.128.The network 192.6.1.192/26 is learned via OSPF (O), with a metric of 110 and a next-hop IP address of 192.6.0.10. This route is reachable via the Serial3/0 interface.

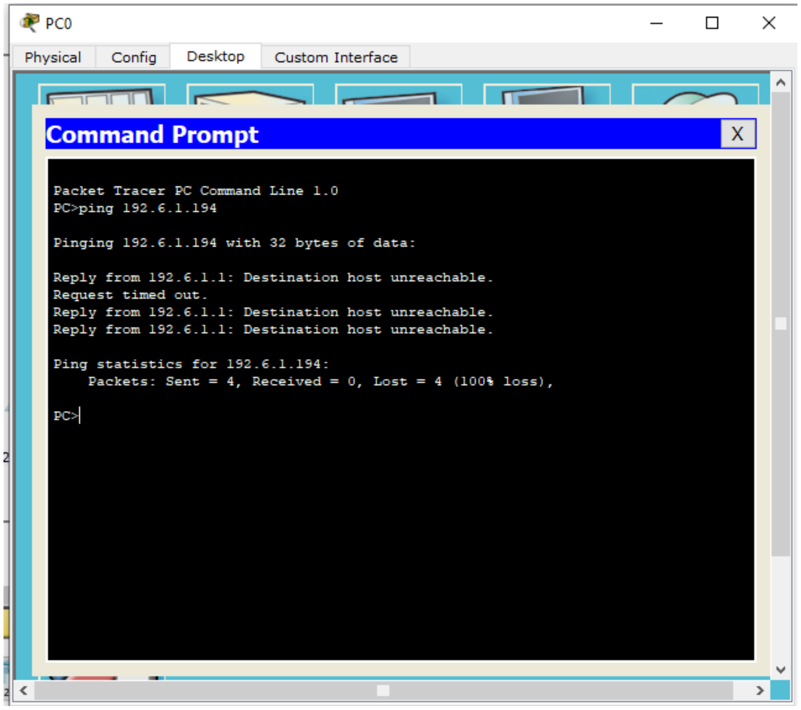


PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Failed	PC0	PC5	ICMP	🟦	0.000	N	0	(edit)	(delete)
●	Failed	PC1	PC3	ICMP	🟩	0.000	N	1	(edit)	(delete)
●	Successful	PC5	PC3	ICMP	🟧	0.000	N	2	(edit)	(delete)
●	Successful	PC2	PC0	ICMP	🟥	0.000	N	3	(edit)	(delete)

Figure 18: Packets Send

g) Test PC BY Ping Command



```
Packet Tracer PC Command Line 1.0
PC>ping 192.6.1.194

Pinging 192.6.1.194 with 32 bytes of data:

Reply from 192.6.1.1: Destination host unreachable.
Request timed out.
Reply from 192.6.1.1: Destination host unreachable.
Reply from 192.6.1.1: Destination host unreachable.

Ping statistics for 192.6.1.194:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Figure 19: Pinging Test on PC0 to PC5

The "Destination host unreachable" message indicates that the router at 192.6.1.1 is unable to forward the ICMP packets to the intended destination host at 192.6.1.194. This issue could stem from several potential factors:

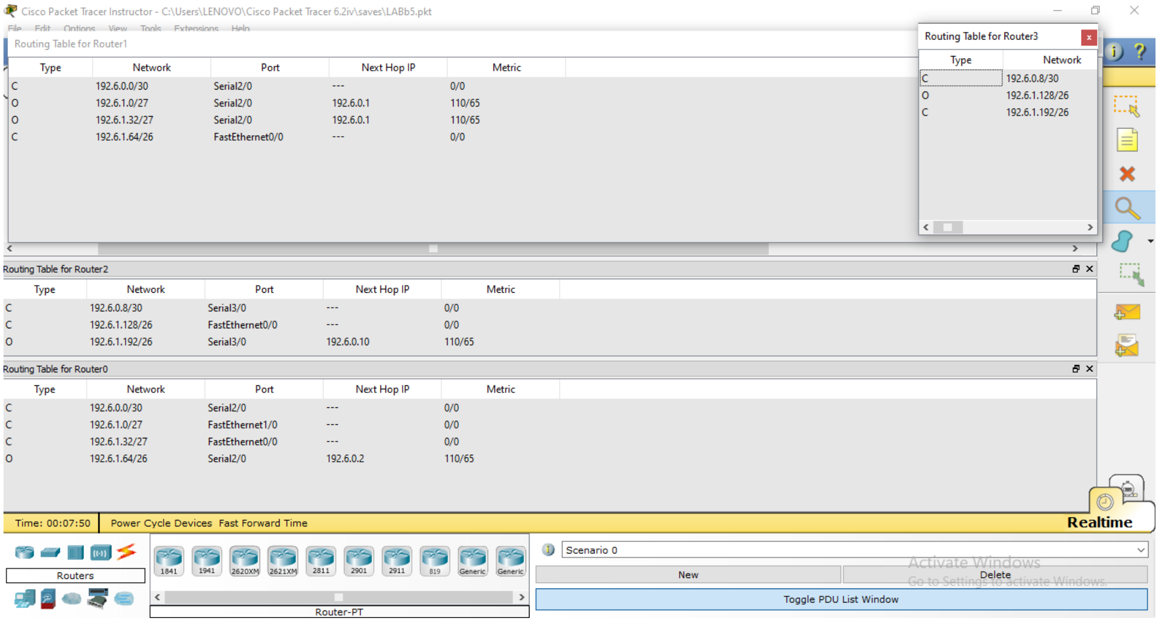
1. Missing Route: The router may lack a proper route to reach the destination network (192.6.1.194) within its routing table. This could be due to configuration errors or incomplete routing information.

2. Access Control Lists (ACLs): An ACL configured on the router could be prohibiting ICMP traffic directed towards 192.6.1.194, effectively blocking the communication attempt.

3. Firewall Configuration: If a firewall is active on the router, it may be configured to deny ICMP traffic destined for the specified host (192.6.1.194), resulting in the "Destination host unreachable" response.

4. Network Connectivity Issues: Physical problems such as faulty cables, interface malfunctions, or other connectivity issues between the router and the destination host may prevent successful communication.

Despite proper BGP configuration, which facilitates routing between autonomous systems, it's important to note that successful BGP configuration does not guarantee end-to-end connectivity. BGP primarily handles routing between autonomous systems, relying on underlying network infrastructure to effectively forward traffic to its intended destination. Thus, while BGP may be correctly configured, it does not inherently ensure reachability to specific hosts within the network.


Cisco Packet Tracer Instructor - C:\Users\LENOVO\Cisco Packet Tracer 6.2iv\saves\LABb5.pkt
File Edit Options View Tools Extensions Help
Time: 00:07:50
Power Cycle Devices Fast Forward Time
Realtime
Routers
1841
1941
2620XM
2621XM
2811
2901
2911
819
Generic
Generic
Router-PT
Scenario 0
New
Delete
Toggle PDU List Window
Activate Windows
Go to Settings to activate Windows.

Routing Table for Router1

Type	Network	Port	Next Hop IP	Metric
C	192.6.0.0/30	Serial2/0	---	0/0
O	192.6.1.0/27	Serial2/0	192.6.0.1	110/65
O	192.6.1.32/27	Serial2/0	192.6.0.1	110/65
C	192.6.1.64/26	FastEthernet0/0	---	0/0

Routing Table for Router3

Type	Network
C	192.6.0.8/30
O	192.6.1.128/26
C	192.6.1.192/26

Routing Table for Router2

Type	Network	Port	Next Hop IP	Metric
C	192.6.0.8/30	Serial3/0	---	0/0
C	192.6.1.128/26	FastEthernet0/0	---	0/0
O	192.6.1.192/26	Serial3/0	192.6.0.10	110/65

Routing Table for Router0

Type	Network	Port	Next Hop IP	Metric
C	192.6.0.0/30	Serial2/0	---	0/0
C	192.6.1.0/27	FastEthernet1/0	---	0/0
C	192.6.1.32/27	FastEthernet0/0	---	0/0
O	192.6.1.64/26	Serial2/0	192.6.0.2	110/65

Figure 20: Routing Table for all routers

5. Conclusion

In summary, the primary focus of the lab was on implementing the Path Vector Border Gateway Protocol (BGP) within the network topology. The setup included a variety of network devices such as routers, switches, and PCs, with dynamic IP routing managed internally by Open Shortest Path First (OSPF) and externally by BGP. Throughout the lab, fundamental BGP concepts were covered, including its role within Autonomous Systems (AS), BGP configuration procedures, and the establishment of interactions between BGP and OSPF. Additionally, adjustments to BGP timers and monitoring of routing tables were explored to ensure efficient network operation. However, it's essential to note that incorrect sequencing of steps or misconfigurations may lead to issues such as failed ping, trace route, or packet transmission tests, indicating potential problems with BGP functionality. These troubleshooting scenarios serve as valuable learning experiences, highlighting the importance of meticulous configuration and careful monitoring to maintain robust network connectivity.

6. References

[1] [Online]. Available: https://www.fortinet.com/resources/cyberglossary/bgp-border-gateway-protocol. [Accessed 10 4 2024].

[2] [Online]. Available: https://www.pynetlabs.com/bgp-in-computer-networks/. [Accessed 10 4 2024].

[3] [Online]. Available: https://www.cloudflare.com/learning/network-layer/what-is-an-autonomous-system/. [Accessed 10 4 2024].

[4] [Online]. Available: https://www.cloudflare.com/learning/security/glossary/what-is-bgp/. [Accessed 10 4 2024].