UNIVERSITY OF SOUTH CAROLINA

BORDER GATEWAY PROTOCOL

Lab 11: Configuring Multiprotocol BGP

Document Version: 03-18-2020

Award 1829698
“CyberTraining CIP: Cyberinfrastructure Expertise on High-throughput Networks for Big Science Data Transfers”

Contents

Overview

This lab introduces Multiprotocol Border Gateway Protocol (MP-BGP). This protocol makes BGP available for other network layer protocols, including Internet Protocol version 6 (IPv6). For Interior Gateway Protocol (IGP), Open Shortest Path First version 2 (OSPFv2) and OSPFv3 will be configured to advertise IPv4 and IPv6 addresses. For Exterior Gateway Protocol (EGP), Internal BGP (IBGP) and External BGP (EBGP) will be configured to advertise IPv4 and IPv6 across Autonomous Systems (ASes).

Objectives

By the end of this lab, students should be able to:

1. Assign IPv6 addresses on hosts.
2. Configure OSPFv2 and OSPFv3.
3. Configure and verify IBGP and EBGP.
4. Use MP-BGP to distribute IPv4 and IPv6 in parallel.

Lab settings

The information in Table 1 provides the credentials to access Client1 machine.

Table 1. Credentials to access Client1 machine.

Device	Account	Password
Client1	admin	password

Lab roadmap

This lab is organized as follows:

1. Section 1: Introduction.
2. Section 2: Lab topology.
3. Section 3: Configure and verify OSPF on router r2 and router r3.
4. Section 4: Configure and verify BGP for IPv4 networks.
5. Section 5: Configure and verify BGP for IPv6 networks.
6. Section 6: Verify BGP configuration.

1 Introduction

1.1 IPv4 and IPv6 addresses

The IP transmits blocks of data called datagrams from the source to the destination that are identified by a fixed length address. IPv4 is the dominant protocol of the Internet that identifies devices on a network. It uses a 32-bit address space which allows to store more than 4 billion addresses[1].

As the Internet evolves, more IP addresses are required than the IPv4 offers. Thus, IPv6 was designed to fulfill the need for more Internet addresses. IPv6 uses a 64-bit address space which allows to store a huge number of addresses (more than 340 undecillion)[2].

IPv6 has multiple address types. The link local address is used on a single link, or within a Local Area Network (LAN). Link local addresses do not have to be globally unique, thus, they are not routable. The prefix of the link local address is fe80::/10. Global unicast address is globally unique, and it is used to identify a single interface on the Internet. The prefix of the global unicast address is 2000::/3 [3].

Consider Figure 1. In IPv6, the link local address is used between routers that are directly connected, whereas the global address is used between routers that do not share a common link.

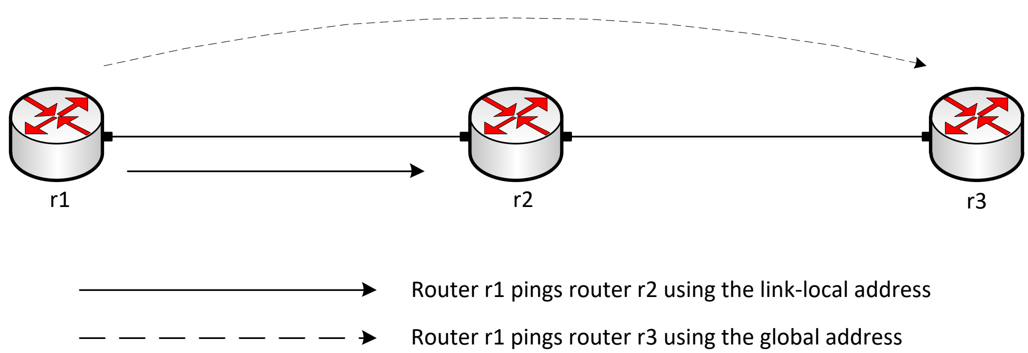

Figure 1. IPv6 link local and global addresses.

1.2 Intradomain and Interdomain routing protocols

The Internet consists of many independent administrative domains, referred to as ASes. ASes are operated by different organizations, which can run their own internal routing protocols. A routing protocol that runs within an AS is referred to as intradomain routing protocol. One of the most widely used intradomain protocols is OSPF. Since an AS may be large and nontrivial to manage, OSPF allows an AS to be divided into numbered areas[4]. An area is a logical collection of networks, routers, and links. All routers in the same area have detailed information of the topology within their area[5]. Traditionally, OSPF only supported IPv4 addresses (OSPFv2); however, it was redesigned to support IPv6 as well (OSPFv3)[6].

A routing protocol that runs between ASes is referred to as interdomain routing protocol. ASes may use different intradomain routing protocols; however, they must use the same interdomain routing protocol, i.e., BGP. BGP allows the enforcement of different routing policies on the traffic from one AS to another. For example, a security policy can prevent the dissemination of routing information from one AS to another[4]. BGP has been extended to carry routing information for multiple protocols, such as IPv6 [7].

BGP is referred to as EBGP when it is running between different ASes, whereas it is referred to as IBGP when it is running within an AS[4]. IBGP is usually used to distribute the EBGP learned routes among the routers within the same AS[4].

Consider Figure 2. The intradomain routing protocol within AS 100 is OSPF, and the interdomain routing protocol between AS 100 and AS 200 is BGP (EBGP). Routers within the same AS advertise their EBGP learned routes among each other through IBGP.

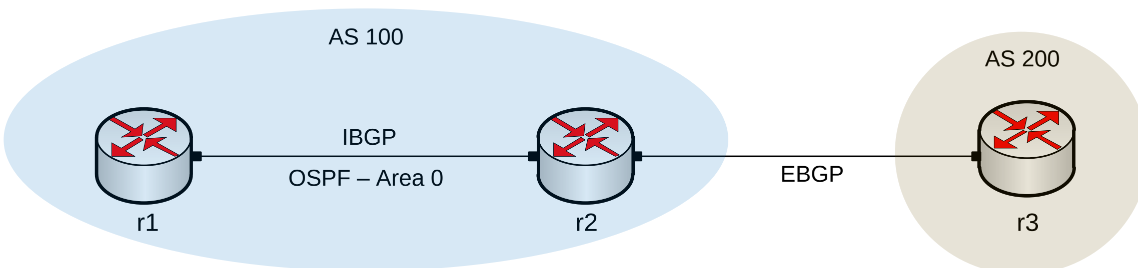

Figure 2. Routers that exchange information within the same AS use OSPF and IBGP, while routers that exchange information between different ASes use EBGP.

1.3 MP-BGP

In an IPv4 environment, BGP establishes sessions using IPv4, i.e., BGP peers are configured with IPv4 addresses. The routes that are advertised by BGP also have IPv4 addresses[8].

MP-BGP was introduced to make BGP available for other network layer protocols, including IPv6. In an environment where IPv4 and IPv6 are both configured, MP-BGP routers can become neighbors using IPv4 addresses and exchange IPv6 prefixes or the other way around[8].

Consider Figure 3. The BGP session established between router r1 and router r2 is done using IPv4. Using MP-BGP, router r1 can advertise the address of the attached IPv6 LAN through the current BGP session.

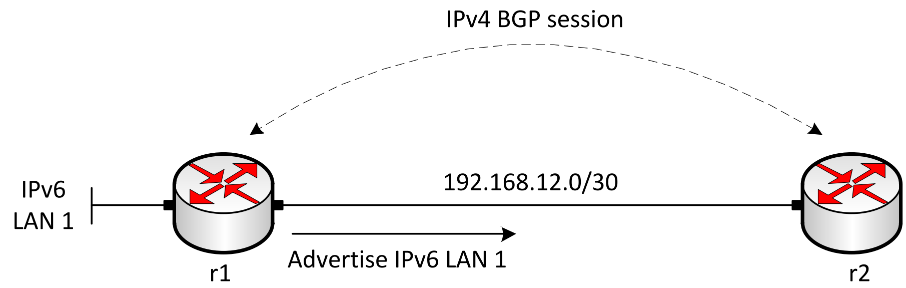

Figure 3. Advertising an IPv6 LAN address through a BGP IPv4 session.

Similarly, consider Figure 4. The BGP session established between router r1 and router r2 is done using IPv6. Using MP-BGP, router r1 can advertise the address of the attached IPv4 LAN through the current BGP session.

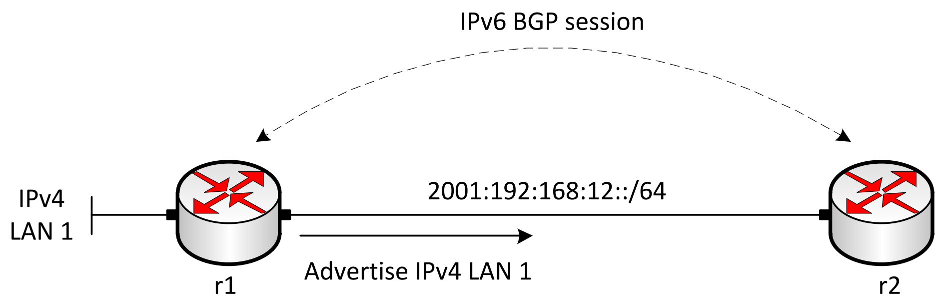

Figure 4. Advertising an IPv4 LAN address through a BGP IPv6 session.

2 Lab topology

Consider Figure 5. The topology consists of two ASes. The Internet Service Provider (ISP), i.e., router r1, provides Internet service to the Campus network (routers r2 and r3). The ASN assigned to the ISP and the Campus network are 100 and 200, respectively. The ISP communicates with the Campus via EBGP routing protocol, and the routers within the Campus network communicate using IBGP and OSPF.

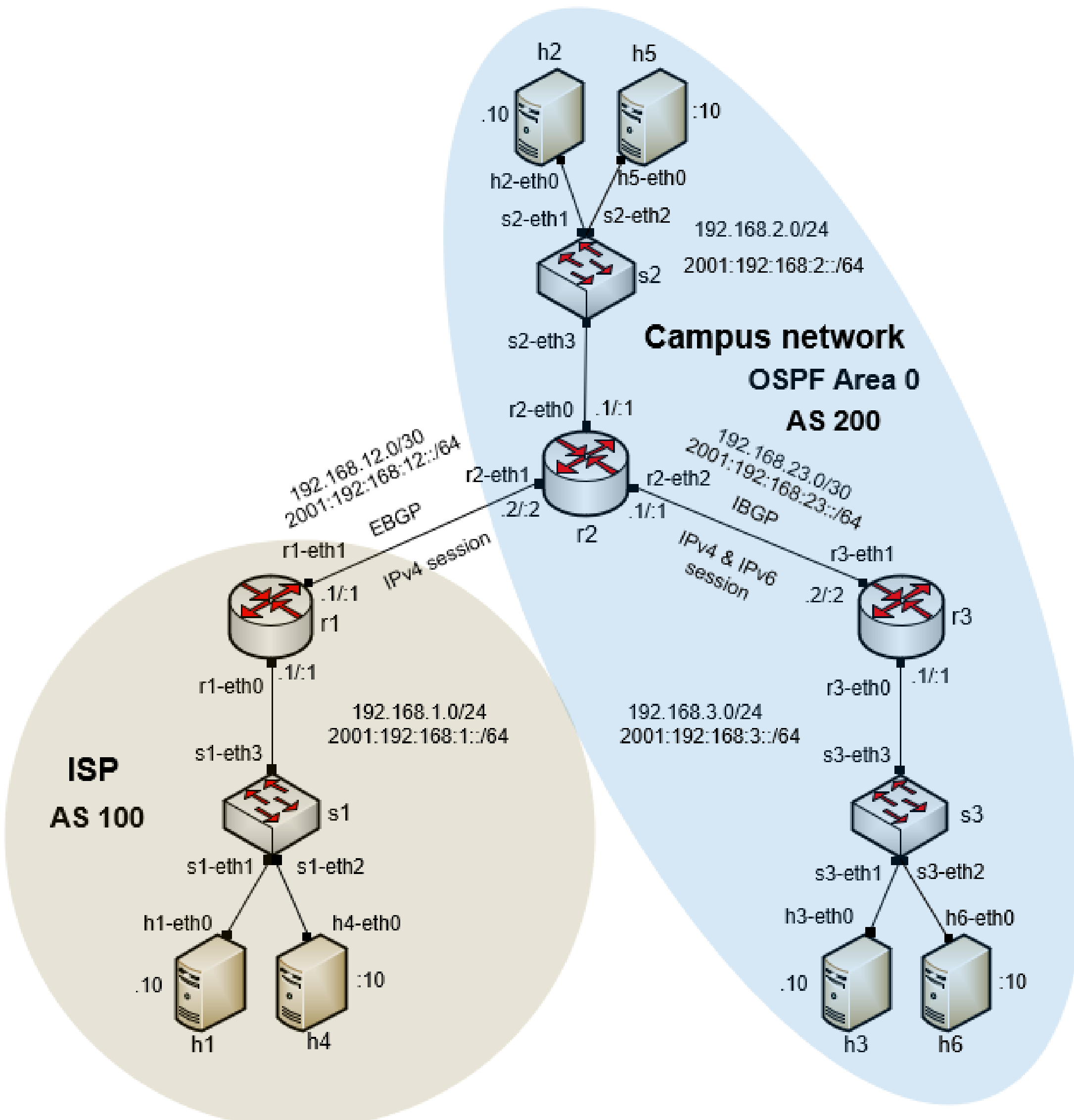

Figure 5. Lab topology.

2.1 Lab settings

Routers and hosts are already configured according to the IP addresses shown in Table 2.

Table 2. Topology information.

Device	Interface	IPV4 Address	IPV6 Address	Default gateway
r1 (ISP)	r1-eth0	192.168.1.1/24	2001:192:168:1::1/64	N/A
	r1-eth1	192.168.12.1/30	2001:192:168:12::1/64	N/A
	lo	192.168.11.1/32	2001:192:168:11::1/64	N/A
	r2-eth0	192.168.2.1/24	2001:192:168:2::1/64	N/A

r2 (Campus network)	r2-eth1	192.168.12.2/30	2001:192:168:12::2/64	N/A
	r2-eth2	192.168.23.1/30	2001:192:168:23::1/64	N/A
	lo	192.168.22.1/32	2001:192:168:22::1/64	N/A
r3 (Campus network)	r3-eth0	192.168.3.1/24	2001:192:168:3::1/64	N/A
	r3-eth1	192.168.23.2/30	2001:192:168:23::2/64	N/A
	lo	192.168.33.1/32	2001:192:168:33::1/64	N/A
h1	h1-eth0	192.168.1.10/24	N/A	192.168.1.1
h2	h2-eth0	192.168.2.10/24	N/A	192.168.2.1
h3	h3-eth0	192.168.3.10/24	N/A	192.168.3.1
h4	h4-eth0	N/A	2001:192:168:1::10/64	2001:192:168:1::1
h5	h5-eth0	N/A	2001:192:168:2::10/64	2001:192:168:1::1
h6	h6-eth0	N/A	2001:192:168:3::10/64	2001:192:168:1::1

2.2 Open topology and load the configuration

Step 1. Start by launching Miniedit by clicking on Desktop's shortcut. When prompted for a password, type `password`.

Figure 6. MiniEdit shortcut.

Step 2. On Miniedit's menu bar, click on *File* then *open* to load the lab's topology. Locate the *Lab11.mn* topology file in the default directory, */home/frr/BGP_Labs/lab11* and click on *Open*.

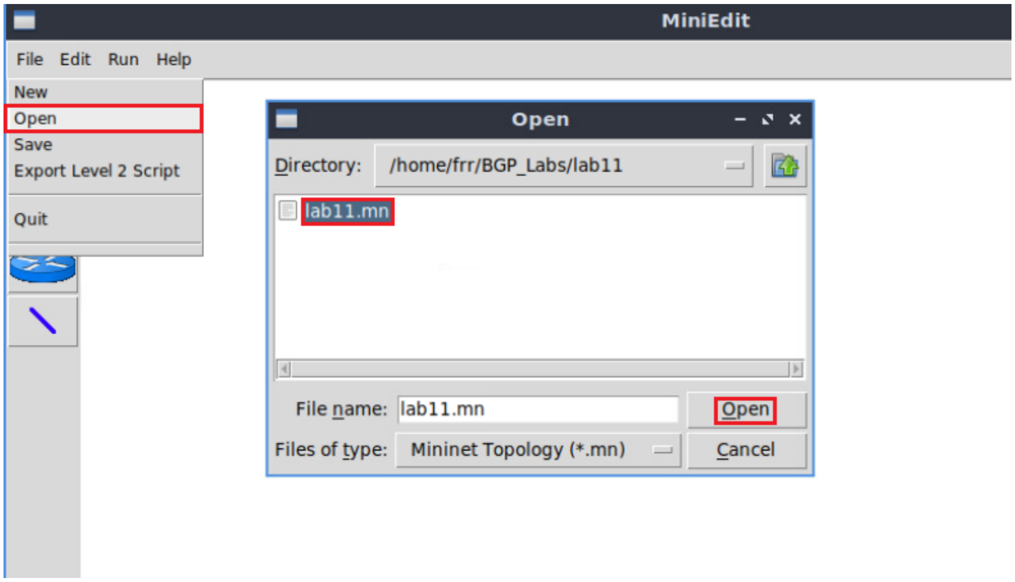

Figure 7. MiniEdit's Open dialog.

At this point the topology is loaded with all the required network components. You will execute a script that will load the configuration of the routers.

Step 3. Open the Linux Terminal.

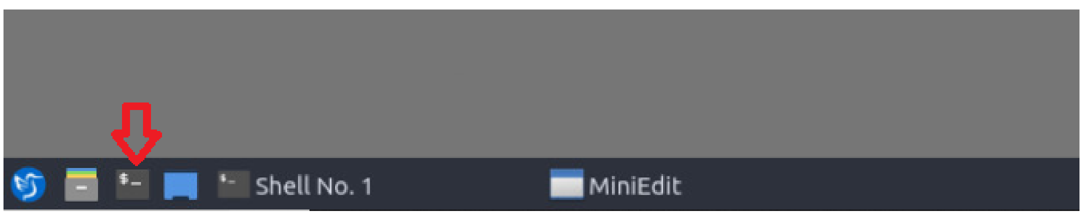

Figure 8. Opening Linux terminal

Step 4. Click on the Linux's terminal and navigate into *BGP_Labs/lab11* directory by issuing the following command. This folder contains a configuration file and the script responsible for loading the configuration. The configuration file will assign the IP addresses to the routers' interfaces. The `cd` command is short for change directory followed by an argument that specifies the destination directory.

```
cd BGP_Labs/lab11
```

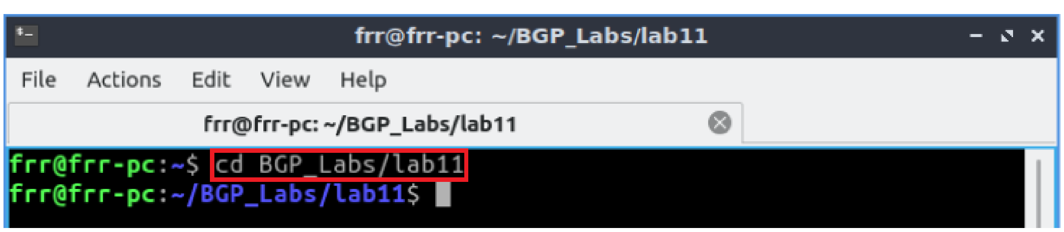

Figure 9. Entering to the *BGP_Labs/lab11* directory.

Step 5. To execute the shell script, type the following command. The argument of the program corresponds to the configuration zip file that will be loaded in all the routers in the topology.

```
./config_loader.sh lab11_conf.zip
```

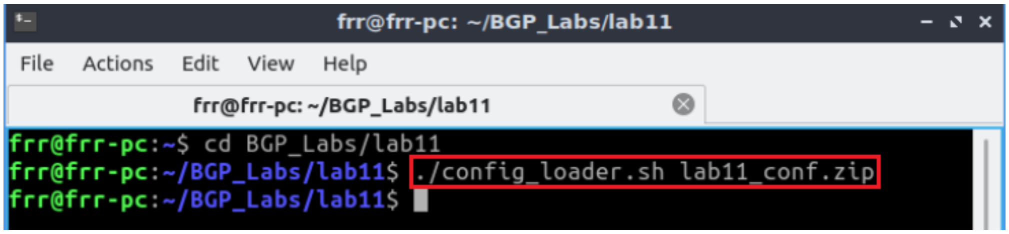

Figure 10. Executing the shell script to load the configuration.

Step 6. Type the following command to exit the Linux terminal.

```
exit
```

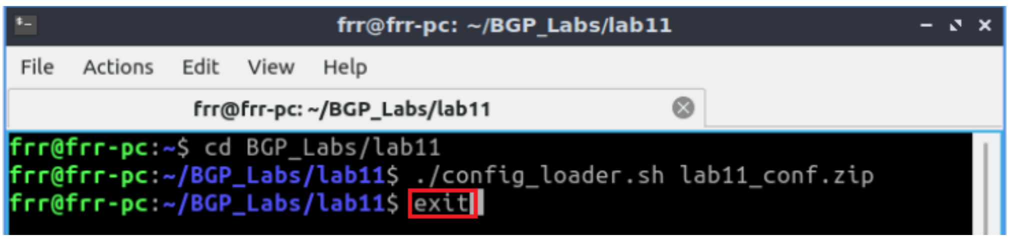

Figure 11. Exiting from the terminal.

Step 7. At this point hosts h1, h2 and h3 interfaces are configured. To proceed with the emulation, click on the *Run* button located in lower left-hand side.

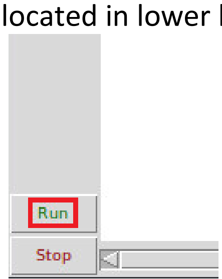

Figure 12. Starting the emulation.

Step 8. Click on Mininet's terminal, i.e., the one launched when MiniEdit was started.

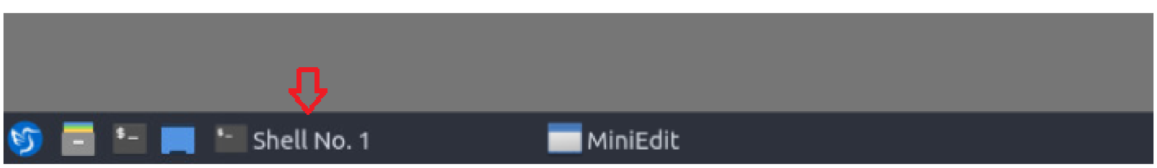

Figure 13. Opening Mininet's terminal.

Step 9. Issue the following command to display the interface names and connections.

```
links
```

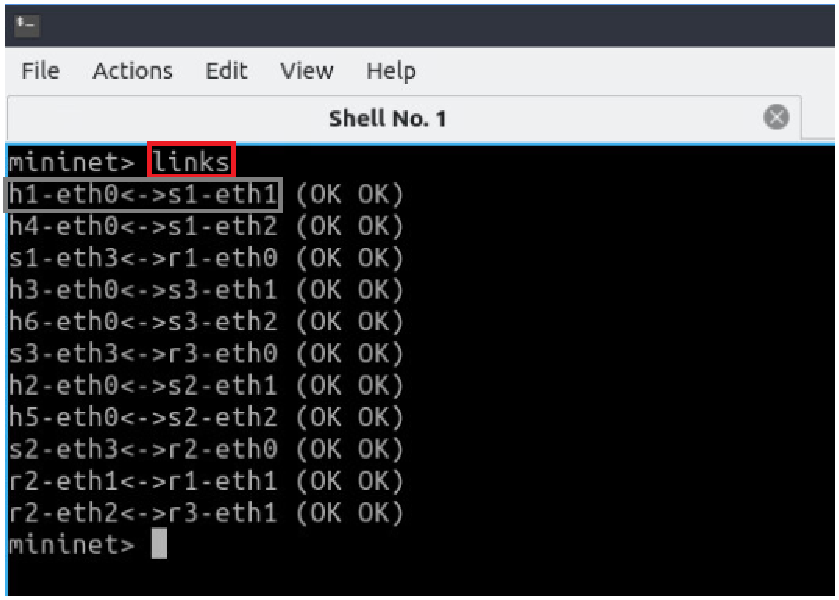

Figure 14. Displaying network interfaces.

In Figure 14, the link displayed within the gray box indicates that interface eth0 of host h1 connects to interface eth1 of switch s1 (i.e., *h1-eth0<->s1-eth1*).

2.3 Configure and verify the hosts

You will verify IPv4 addresses of each host (h1, h2 and h3) following Table 2. Additionally, you will assign the IP addresses and the default gateway to IPv6 hosts (h4, h5 and h6).

Step 1. Hold right-click on host h1 and select *Terminal*. This opens the terminal of host h1 and allows the execution of commands on that host.

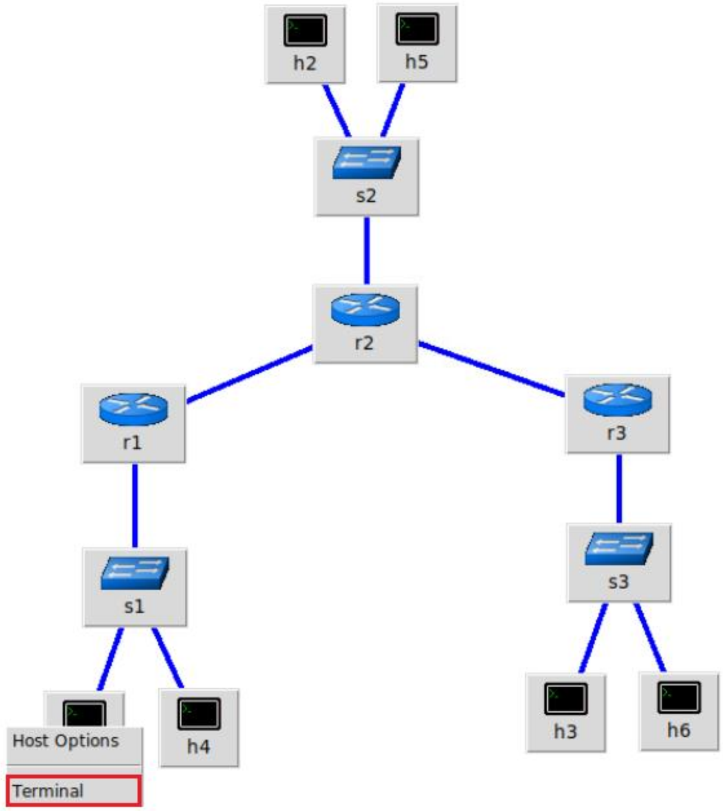

Figure 15. Opening terminal on host h1.

Step 2. On h1 terminal, type the command shown below to verify that the IP address was assigned successfully. You will verify that host h1 has two interfaces, *h1-eth0* configured with the IP address 192.168.1.10 and the subnet mask 255.255.255.0.

```
ifconfig
```

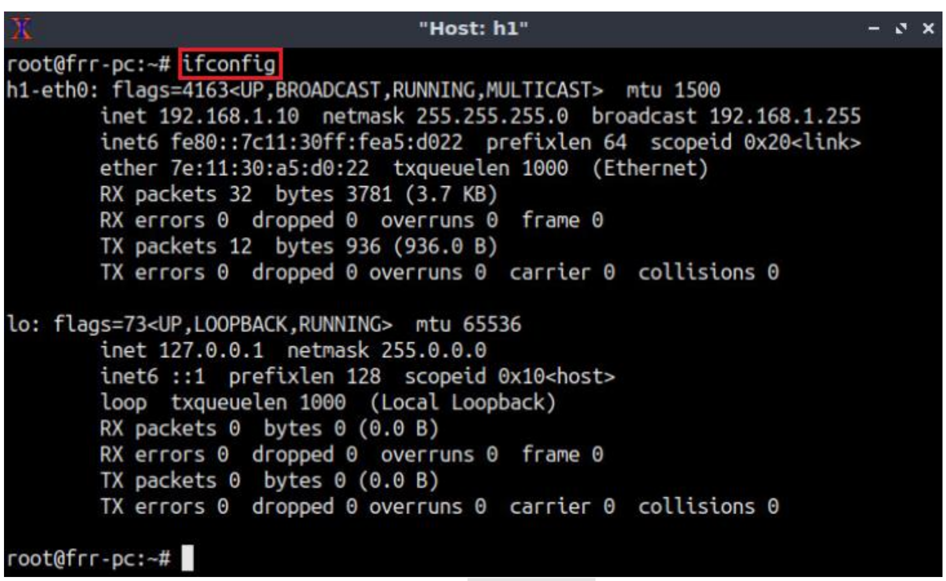

Figure 16. Output of `ifconfig` command.

Step 3. On host h1 terminal, type the command shown below to verify that the default gateway IP address is 192.168.1.1.

```
route
```

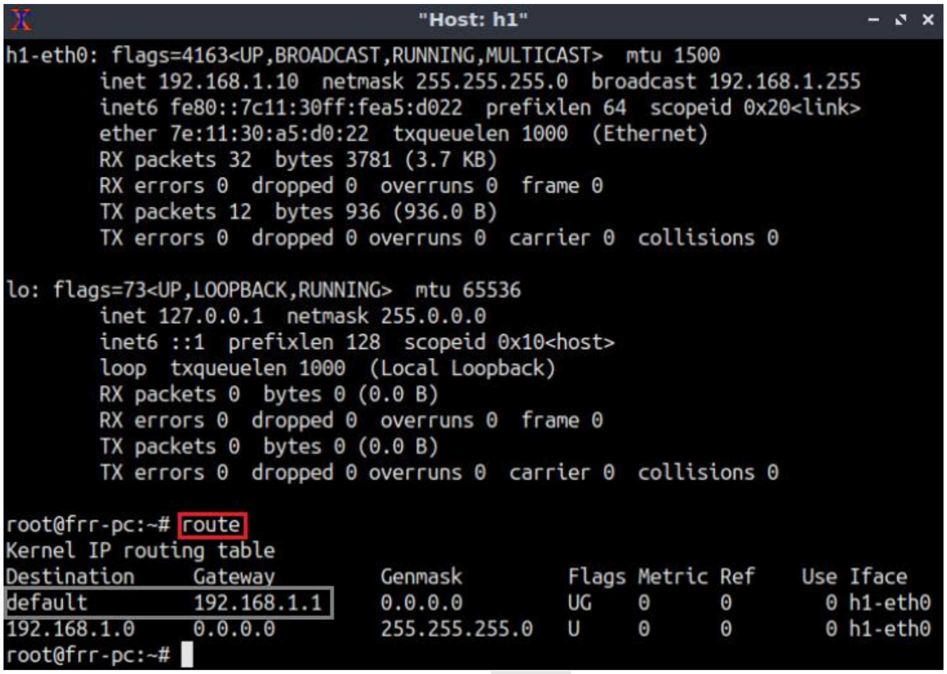

Figure 17. Output of `route` command.

Step 4. In order to verify host 2 and host 3, proceed similarly by repeating from step 1 to step 3 on host h2 and host 3 terminal. Similar results should be observed.

Step 5. On host h4 terminal, type the following command to assign IPv6 address.

```
ifconfig h4-eth0 inet6 add 2001:192:168:1::10/64
```

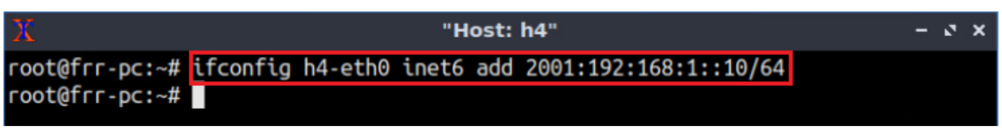

Figure 18. Assigning IPv6 address on host h4.

Step 6. Type the following command to assign IPv6 default gateway on host h4.

```
ip -6 route add default via 2001:192:168:1::1
```

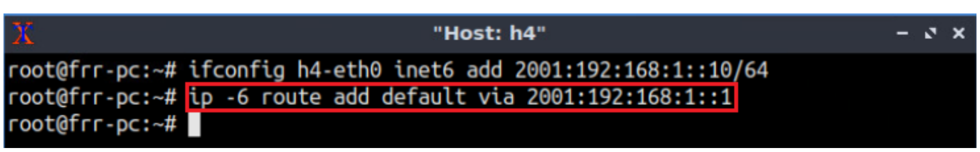

Figure 19. Assigning IPv6 default gateway on host h4.

Step 7. Type the following command to verify IPv6 addresses on host h4. The following figure contains two IPv6 addresses.

```
ifconfig
```

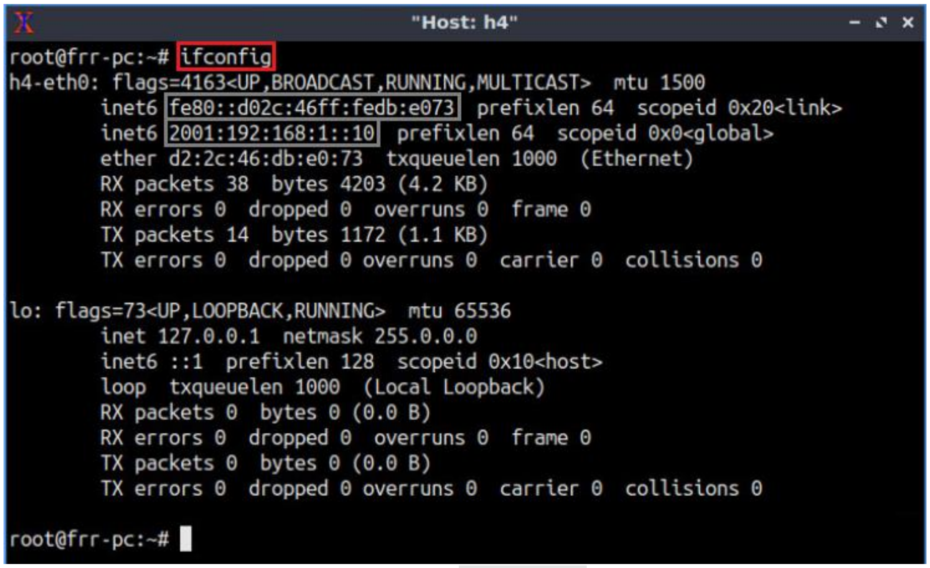

Figure 20. Output of `ifconfig` command.

Consider Figure 20. There are two IPv6 addresses assigned to host h4. IPv6 addresses fe80::d02c:46ff:fedb:e073 and 2001:192:168:1::10 are assigned as link local address and global address, respectively. You may notice a different link local address as they are assigned randomly in FRR. Link local address is used to communicate with directly connected networks. IPv6 global addresses are like IPv4 public addresses which is globally unique.

Step 8. Follow from step 5 to step 6 to assign IPv6 addresses on host h5. These steps are summarized in the figure below.

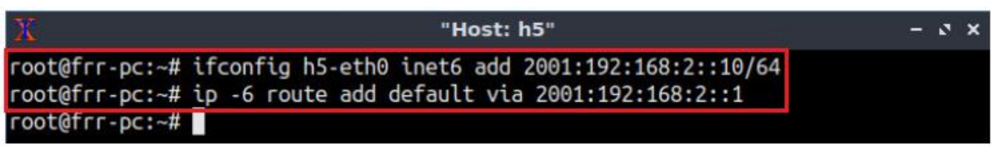

Figure 21. Assigning IPv6 address on host h5.

Step 9. Follow from step 5 to step 6 to assign IPv6 addresses on host h6. These steps are summarized in the figure below.

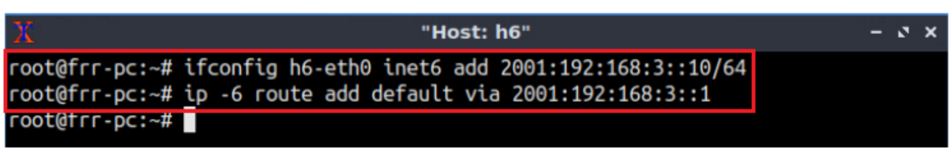

Figure 22. Assigning IPv6 address on host h6.

2.4 Load zebra daemon and verify the Connectivity

In this section, you will verify the routing table of routers r1, r2, and r3.

Step 1. You will validate that the router interfaces are configured correctly according to Table 2. In order to verify router r1, hold right-click on router r1 and select *Terminal*.

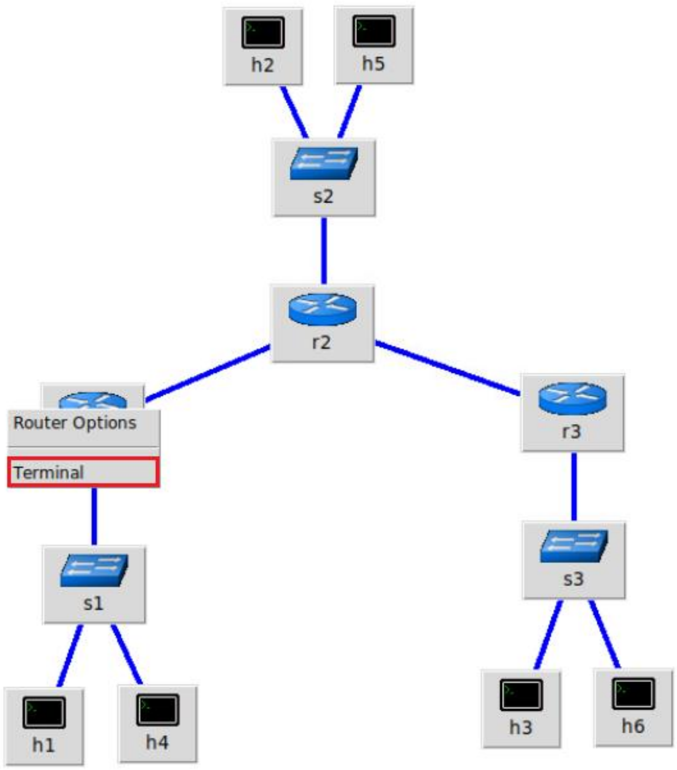

Figure 23. Opening terminal on router r1.

Step 2. In this step, you will start zebra daemon, which is a multi-server routing software that provides TCP/IP based routing protocols. The configuration will not be working if you do not enable zebra daemon initially. In order to start the zebra, type the following command:

```
zebra
```

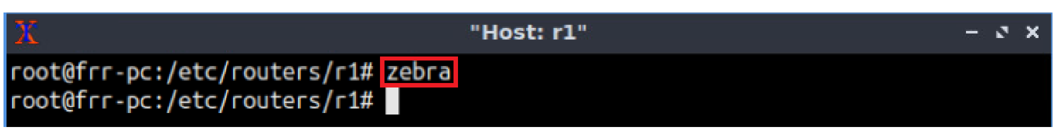

Figure 24. Starting zebra daemon.

Step 3. After initializing zebra, vtysh should be started in order to provide all the CLI commands defined by the daemons. To proceed, issue the following command:

```
vtysh
```

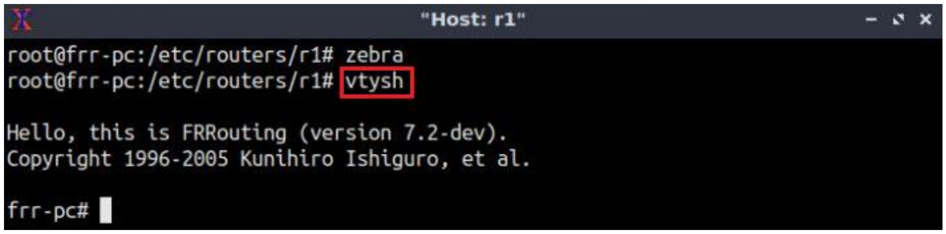

Figure 25. Starting vtysh on router r1.

Step 4. Type the following command on router r1 terminal to verify the routing table of router r1. It will list all the connected IPv4 networks. The routing table of router r1 does not contain any route to the networks attached to router r3 (192.168.23.0/30, 192.168.3.0/24) as there is no routing protocol configured yet.

```
show ip route
```

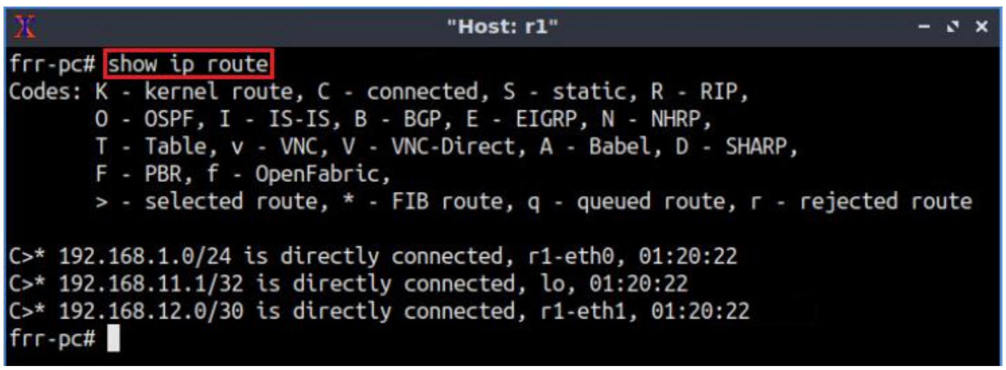

Figure 26. Displaying the routing table for IPv4 routes of router r1.

Step 5. Type the following command on router r1 terminal to verify the routing table for IPv6 routes. You will verify link local addresses (fe80::/64) for each link which is automatically configured in FRR to communicate with directly connected networks. The routing table of router r1 does not contain any route to the networks attached to router r3 (2001:192:168:23::/64, 2001:192:168:3::/64) as there is no routing protocol configured yet.

```
show ipv6 route
```

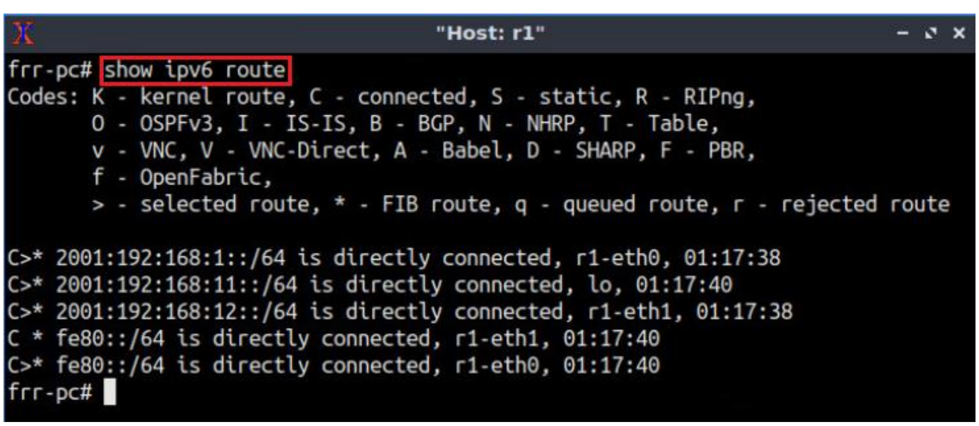

Figure 27. Displaying the routing table for IPv6 routes of router r1.

Step 6. Router r2 is configured similarly to router r1 but, with different IP addresses (see Table 2). Those steps are summarized in the following figure. To proceed, in router r2 terminal, issue the commands depicted below. At the end, you will verify all the directly connected networks of router r2.

```
"Host: r2"
root@frr-pc:/etc/routers/r2# zebra
root@frr-pc:/etc/routers/r2# vtysh

Hello, this is FRRouting (version 7.2-dev).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

frr-pc# show ipv6 route
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

C>* 2001:192:168:2::/64 is directly connected, r2-eth0, 00:05:51
C>* 2001:192:168:12::/64 is directly connected, r2-eth1, 00:05:51
C>* 2001:192:168:22::/64 is directly connected, lo, 00:05:52
C>* 2001:192:168:23::/64 is directly connected, r2-eth2, 00:05:50
C * fe80::/64 is directly connected, r2-eth2, 00:05:52
C * fe80::/64 is directly connected, r2-eth1, 00:05:52
C>* fe80::/64 is directly connected, r2-eth0, 00:05:52
frr-pc#
```

Figure 28. Displaying the routing table for IPv6 routes of router r2.

Step 7. Router r3 is configured similarly to router r1 but, with different IP addresses (see Table 2). Those steps are summarized in the following figure. To proceed, in router r3 terminal, issue the commands depicted below. At the end, you verify all the directly connected networks of router r3.

```
"Host: r3"
root@frr-pc:/etc/routers/r3# zebra
root@frr-pc:/etc/routers/r3# vtysh

Hello, this is FRRouting (version 7.2-dev).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

frr-pc# show ipv6 route
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

C>* 2001:192:168:3::/64 is directly connected, r3-eth0, 00:00:05
C>* 2001:192:168:23::/64 is directly connected, r3-eth1, 00:00:05
C>* 2001:192:168:33::/64 is directly connected, lo, 00:00:06
C * fe80::/64 is directly connected, r3-eth1, 00:00:06
C>* fe80::/64 is directly connected, r3-eth0, 00:00:06
frr-pc#
```

Figure 29. Displaying the routing table for IPv6 routes of router r3.

3 Configure and verify OSPF on router r2 and router r3

In this section, you will configure OSPF routing protocol in router r2 and router r3. First, you will enable the OSPF daemon on the routers. Second, you will establish a single area OSPF, which is classified as area 0 or backbone area. Finally, all the directly connected networks (except 192.168.12.0/30 and 2001:192:168:12::/64) will be advertised in area 0 between routers r2, r3. Networks 192.168.12.0/30 and 2001:192:168:12::/64 will be used to configure EBGP between routers r1 and r2 in the following section.

Step 1. To configure OSPF routing protocol, you need to enable the OSPF daemon first. In router r2, type the following command to exit the vtysh session.

```
exit
```

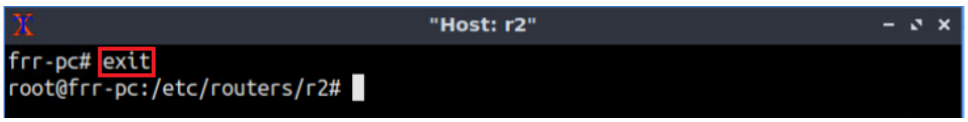

Figure 30. Exiting the vtysh session.

Step 2. Type the following command on router r2 to enable OSPF daemon for IPv4 networks:

```
ospfd
```

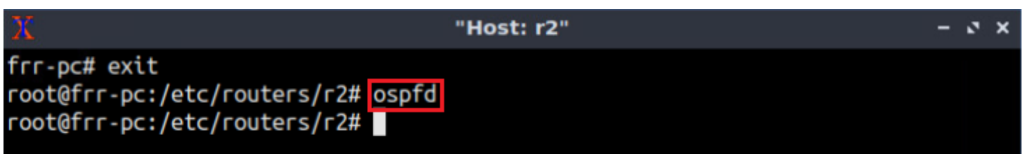

Figure 31. Starting OSPF daemon for IPv4 networks.

Step 3. Type the following command on router r2 to enable OSPF daemon for IPv6 networks:

```
ospf6d
```

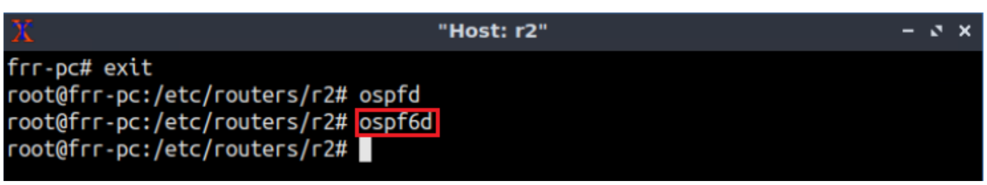

Figure 32. Starting OSPF daemon for IPv6 networks.

Step 4. In order to enter to router r2 terminal, issue the following command:

```
vtysh
```

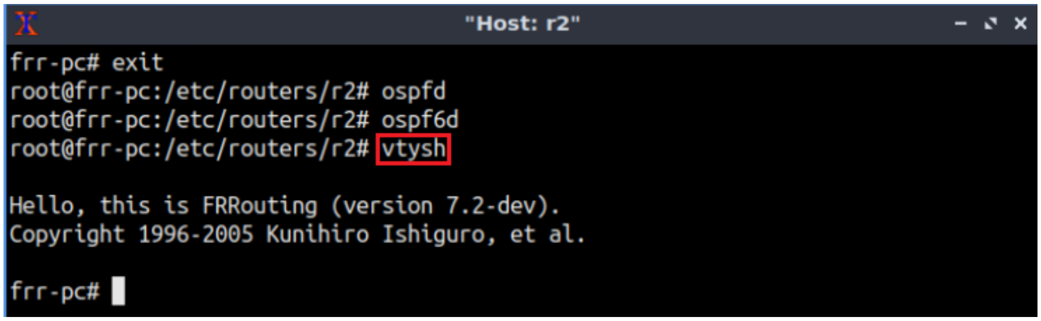

Figure 33. Starting vtysh on router r2.

3.1 Configure OSPFv2 for IPv4 networks

Step 1. To enable router r2 configuration mode, issue the following command:

```
configure terminal
```

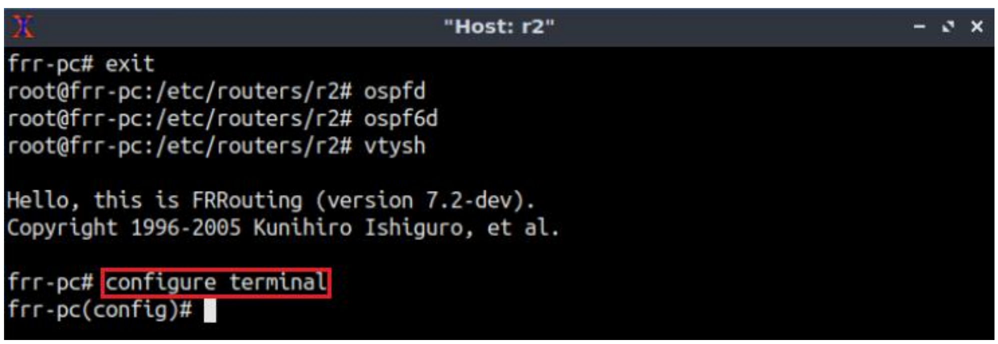

Figure 34. Enabling configuration mode on router r2.

Step 2. In order to configure OSPF routing protocol, type the command shown below. This command will enable OSPF configuration mode where you can advertise the IPv4 networks directly connected to the router r2.

```
router ospf
```

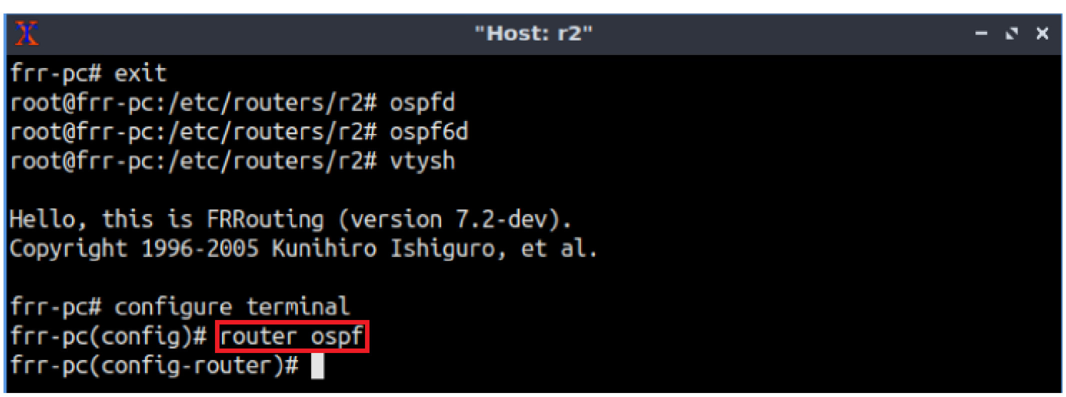

Figure 35. Configuring OSPF for IPv4 networks on router r2.

Step 3. In this step, type the following command to enable the interface *r2-eth2*, corresponding to the network 192.168.23.0/30, to participate in the routing process. This network is associated with area 0.

```
network 192.168.23.0/30 area 0
```

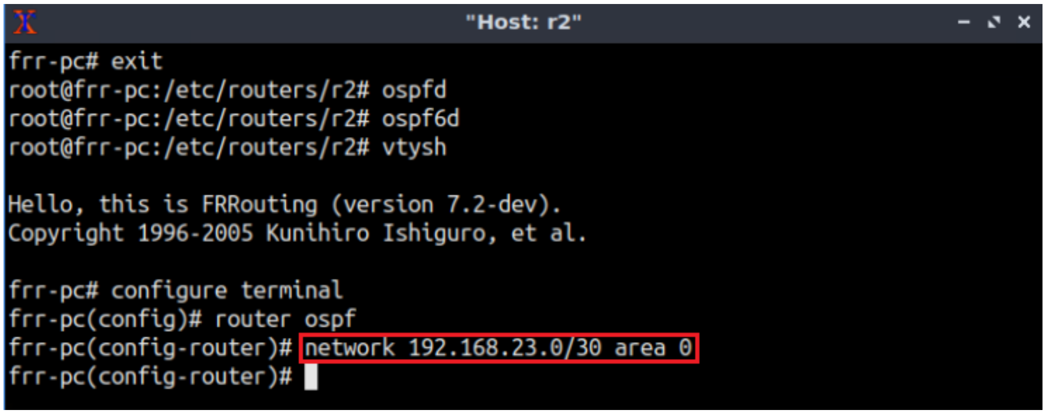

Figure 36. Enabling the interface corresponding to 192.168.23.0/30 to participate in the OSPF routing process.

Step 4. Similarly, type the following command in router r2 terminal to enable the interface r2-eth0 to participate in the OSPF routing process.

```
network 192.168.2.0/24 area 0
```

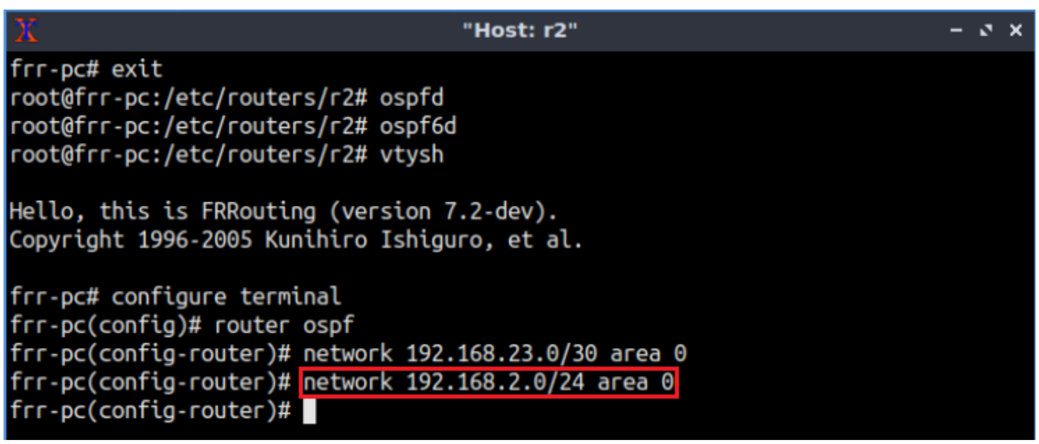

Figure 37. Enabling the interface corresponding to 192.168.2.0/24 to participate in the OSPF routing process.

Step 5. Type the following command to enable the loopback interface 192.168.22.1/32 to participate in the routing process.

```
network 192.168.22.1/32 area 0
```

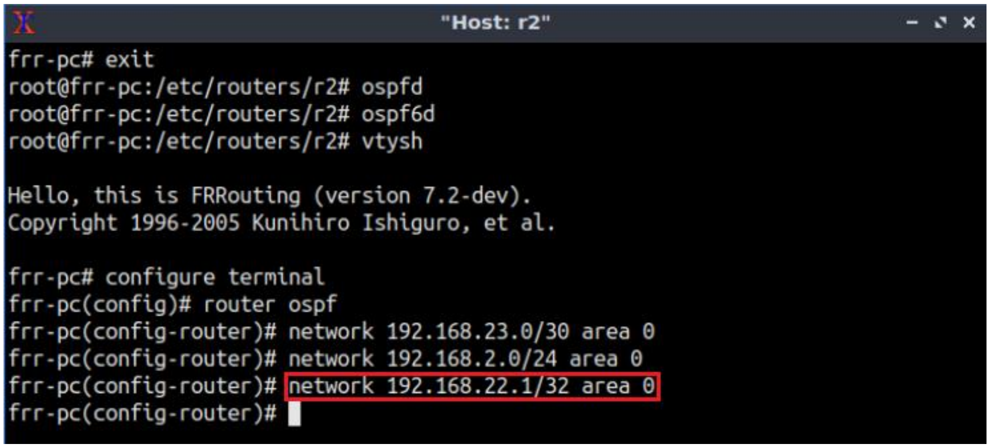

Figure 38. Enabling the interface corresponding to 192.168.22.1/32 to participate in the OSPF routing process.

Step 6. Type the following command to exit from the configuration mode.

```
end
```

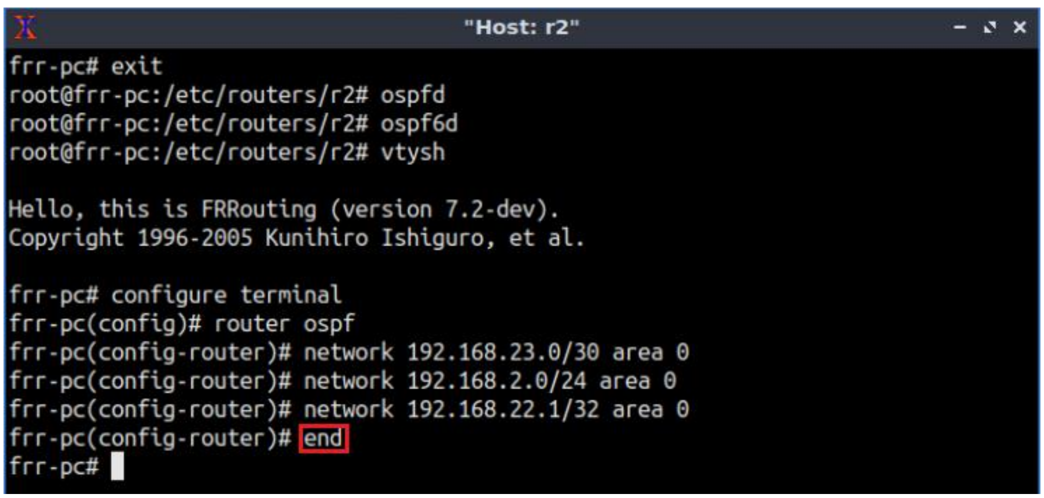

Figure 39. Exiting from configuration mode.

Step 7. Router r3 is configured similarly to router r2 but, with different IP addresses (see Table 2). Those steps are summarized in the following figure. To proceed, on router r3 terminal issue the commands depicted below.

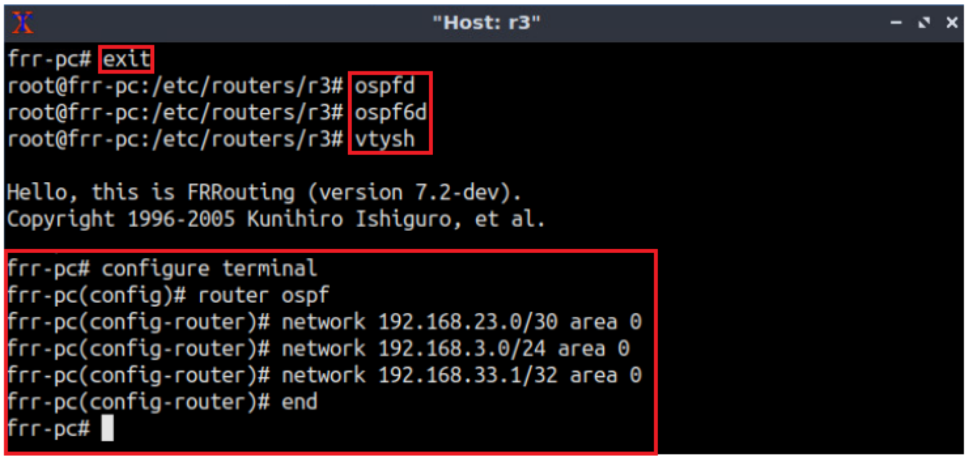

Figure 40. Configuring OSPF for IPv4 networks in router r3.

Step 8. Type the following command to verify the routing table of router r3.

```
show ip route
```

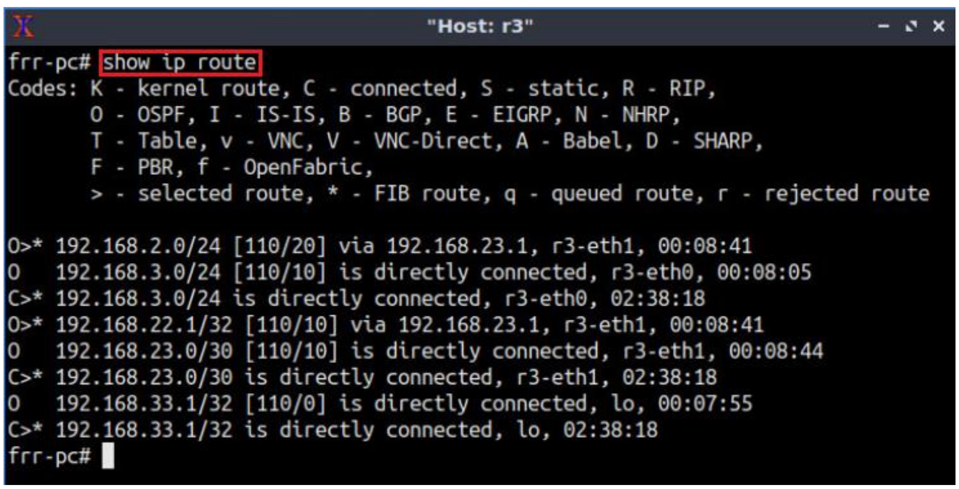

Figure 41. Verifying IPv4 routes on router r3.

Consider Figure 41. Router r3 reaches the network 192.168.2.0/24 via the IP address 192.168.23.1. Networks 192.168.3.0/24 and 192.168.23.0/30 have two available paths from router r3. The administrative distance (AD) of the paths advertised through OSPF is 110. The AD is a value used by routers to select the best path when there are multiple available routes to the same destination. A smaller AD is always preferable to the routers. The characters `>*` indicates that the following path is used to reach a specific network. Router r3 prefers directly connected networks over OSPF since the former has a lower AD than the latter.

3.2 Configure OSPFv3 for IPv6 networks

In this section, you will configure OSPFv3 for IPv6 networks to participate in the OSPF process. To do the configuration, you will enable the interface associated with area ID and specify area range parameters on the router. In this lab, you will use area 0.0.0.0 which is default in FRR.

Step 1. To enable router r2 configuration mode, issue the following command:

```
configure terminal
```

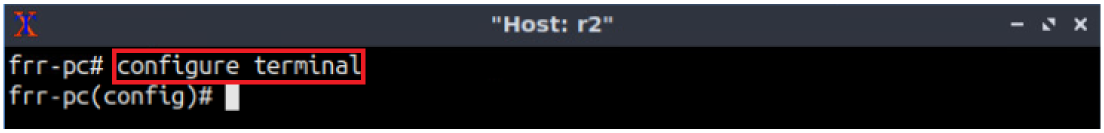

Figure 42. Enabling configuration mode on router r2.

Step 2. In order to configure OSPF routing protocol, type the command shown below. This command will enable OSPF configuration mode where you can advertise the networks directly connected to the router r2.

```
router ospf6
```

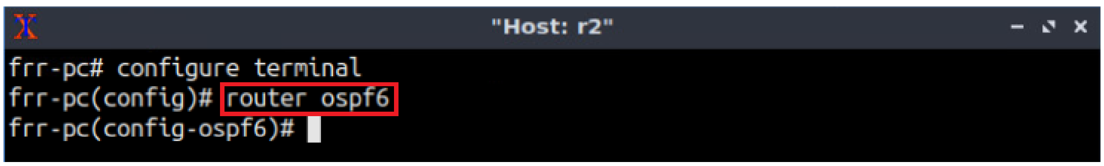

Figure 43. Configuring OSPF for IPv6 networks on router r3.

Step 3. In this step, you will enable the interface of router r2 to participate in the routing process. Type the following command to enable the interface *r2-eth0* along with area 0.0.0.0.

```
interface r2-eth0 area 0.0.0.0
```

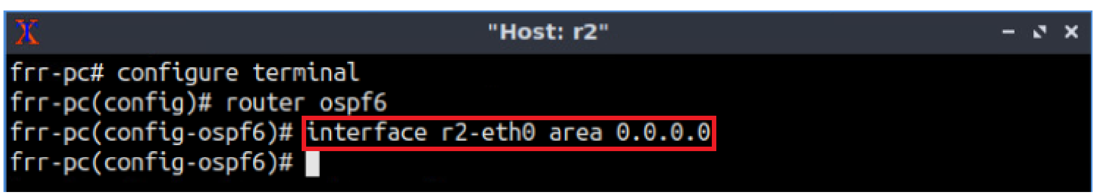

Figure 44. Enabling the interface corresponds to r2-eth0 to participate in the OSPF routing process.

Step 4. In this step, you will specify the area range so that the network 2001:192:168:2::/64 will be advertised through OSPF.

```
area 0.0.0.0 range 2001:192:168:2::/64
```

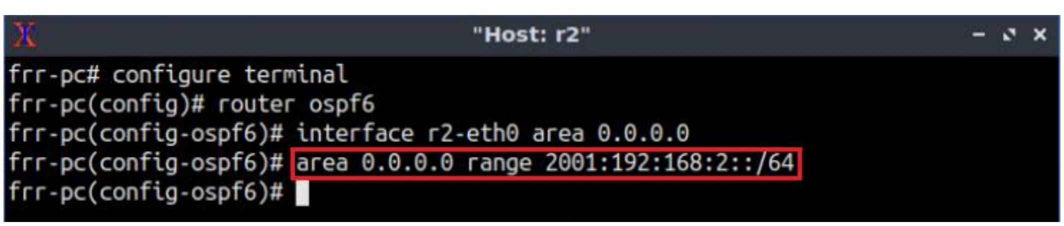

Figure 45. Advertising the network corresponding to r2-eth0 to participate in the OSPF routing process.

Step 5. Type the following command to enable the interface *r2-eth2* along with area 0.0.0.0.

```
interface r2-eth2 area 0.0.0.0
```

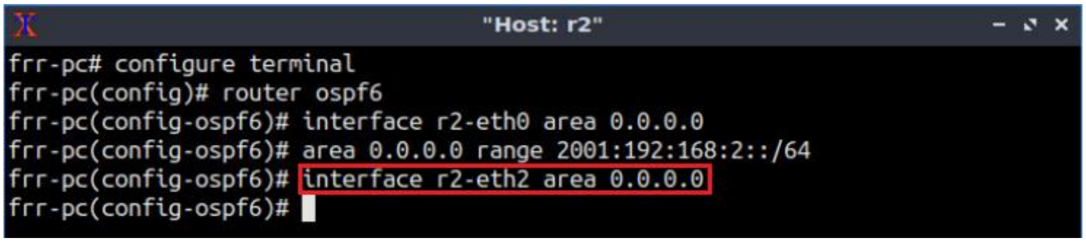

Figure 46. Enabling the interface corresponding to r2-eth2 to participate in the OSPF routing process.

Step 6. Type the following command to advertise the network 2001:192:168:23::/64 through OSPF.

```
area 0.0.0.0 range 2001:192:168:23::/64
```

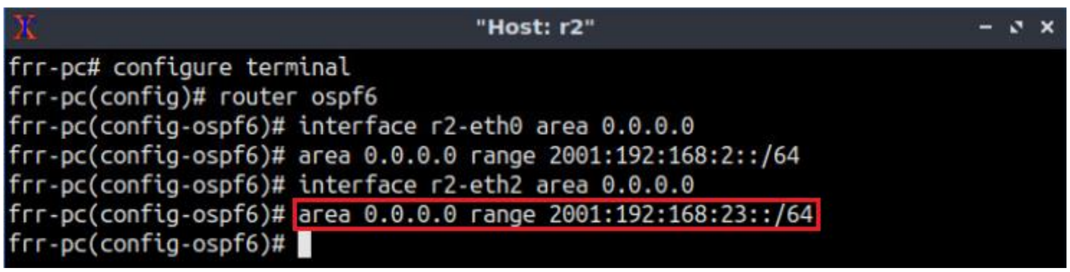

Figure 47. Advertising the network corresponding to r2-eth2 to participate in the OSPF routing process.

Step 7. Type the following command to enable the interface *lo* along with area 0.0.0.0.

```
interface lo area 0.0.0.0
```

Figure 48. Enabling the interface corresponding to lo to participate in the OSPF routing process.

Step 8. Type the following command to advertise the loopback address 2001:192:168:22::1/64 through OSPF.

```
area 0.0.0.0 range 2001:192:168:22::1/64
```

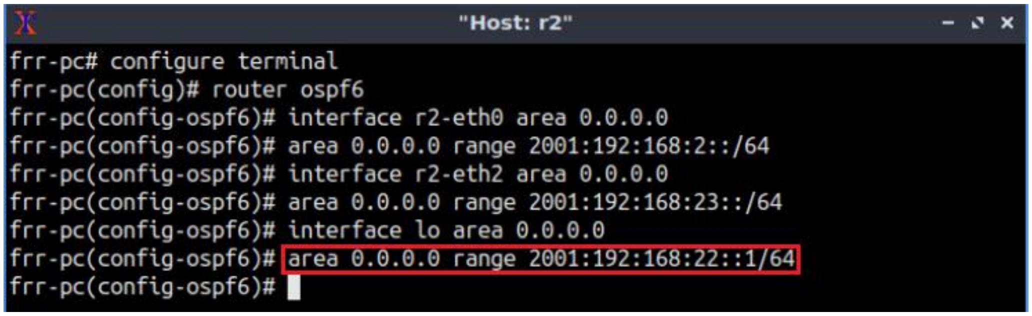

Figure 49. Advertising the loopback address to participate in the OSPF routing process.

Step 9. Type the following command to exit from the configuration mode.

```
end
```

Figure 50. Exiting from configuration mode.

Step 10. Router r3 is configured similarly to router r2 but, with different IP addresses (see Table 2). Those steps are summarized in the following figure. To proceed, on router r3 terminal issue the commands depicted below.

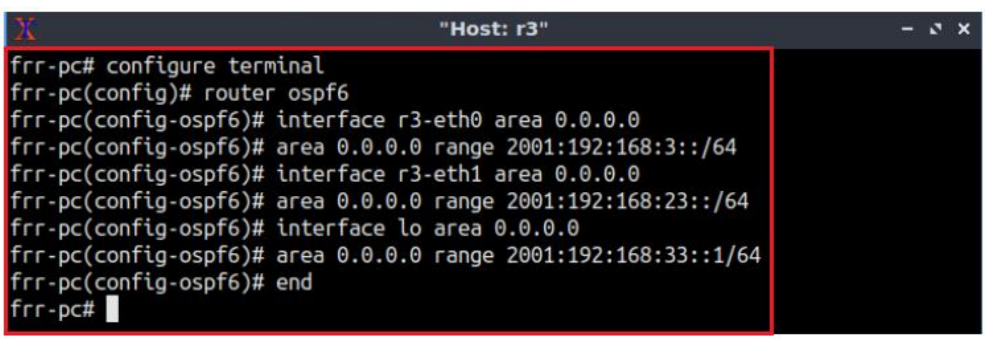

Figure 51. Configuring OSPFv3 on router r3.

3.3 Verify connectivity between router r2 and router r3

Step 1. Type the following command to verify the routing table of router r3. Router r3 will communicate with the networks attached to router r2 (2001:192:168:2::/64 and 2001:192:168:22::1/64) through OSPF.

```
show ipv6 route
```

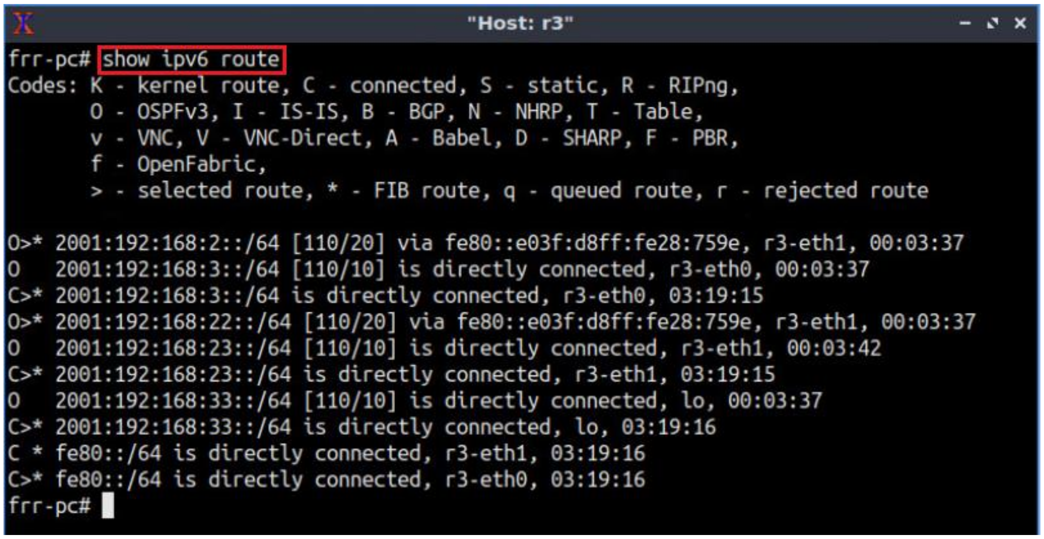

Figure 52. Verifying IPv6 routes on router r3.

Step 2. At this point, router r2 and router r3 will exchange routes. By default, IPv6 forwarding is disabled in FRR. You will enable IPv6 forwarding so that all the IPv6 hosts can participate in the routing process. In order to enable router r3 configuration mode, issue the following command:

```
configure terminal
```

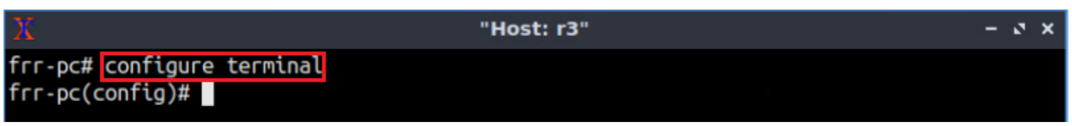

Figure 53. Enabling configuration mode on router r2.

Step 3. Type the following command to enable IPv6 forwarding.

```
ipv6 forwarding
```

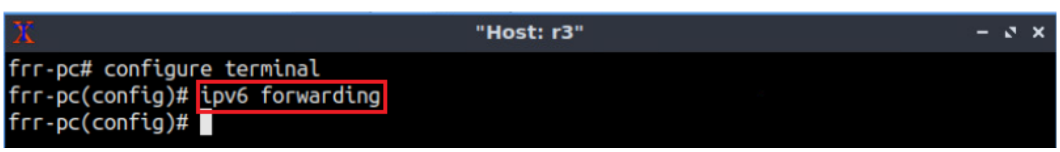

Figure 54. Enabling IPv6 forwarding in router r3.

Step 4. Type the following command to exit from the configuration mode.

```
end
```

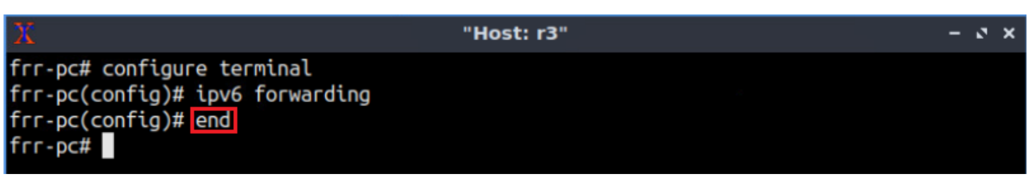

Figure 55. Exiting from configuration mode.

Step 5. Repeat from step 2 to step 4 in order to enable IPv6 forwarding in router r2.

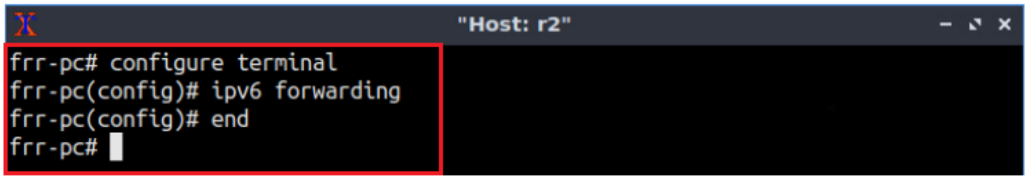

Figure 56. Enabling IPv6 forwarding on router r2.

Step 6. Repeat from step 2 to step 4 in order to enable IPv6 forwarding in router r1.

Figure 57. Enabling IPv6 forwarding on router r1.

Step 7. On host h6 terminal, perform a connectivity between host h6 and host h5 by issuing the command shown below. To stop the test, press `Ctrl+c`. The result will show a successful connectivity test.

```
ping 2001:192:168:2::10
```

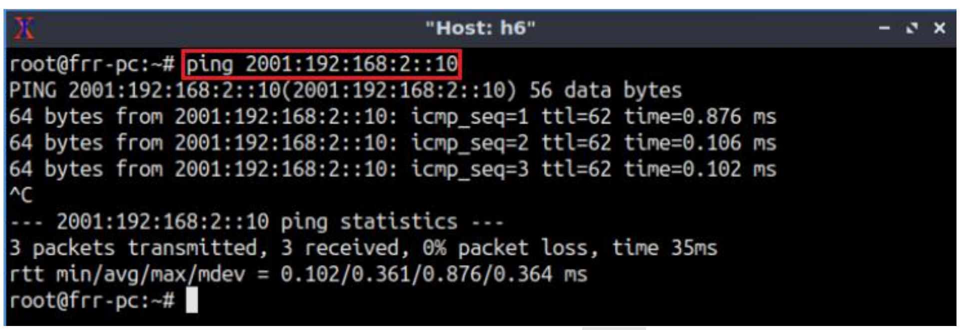

Figure 58. Connectivity test using `ping` command.

4 Configure and verify BGP for IPv4 networks

In this section, you will configure BGP on all routers. Routers r2 and r3 communicate with router r1 through EBGP, while router r2 communicates with router r3 through IBGP. You will assign BGP neighbors to allow the routers to exchange BGP routes. Furthermore, routers r1, r2, and r3 will advertise their LANs via BGP so that the LANs are learned by peer routers.

You will configure EBGP so that router r1 uses IPv4 as the BGP transport for IPv4 sessions. For IBGP, you will configure router r2 so that IPv4 routing information is transported by IPv4 TCP sessions.

4.1 Configure and verify EBGP on router r1

Step 1. To configure BGP routing protocol, you need to enable the BGP daemon first. On router r1 terminal, type the following command to exit the vtysh session:

```
exit
```

Figure 59. Exiting the vtysh session.

Step 2. Type the following command on r1 terminal to enable and start BGP routing protocol.

```
bgpd
```

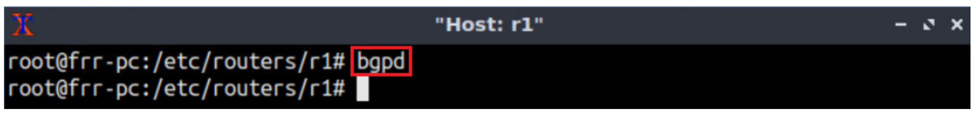

Figure 60. Starting BGP daemon.

Step 3. In order to enter to router r1 terminal, type the following command:

```
vtysh
```

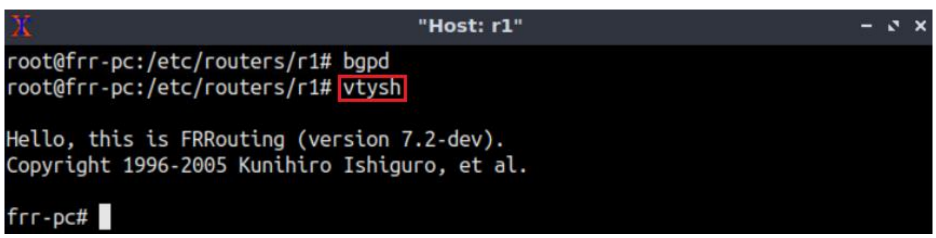

Figure 61. Starting vtysh on router r1.

Step 4. To enable router r1 into configuration mode, issue the following command:

```
configure terminal
```

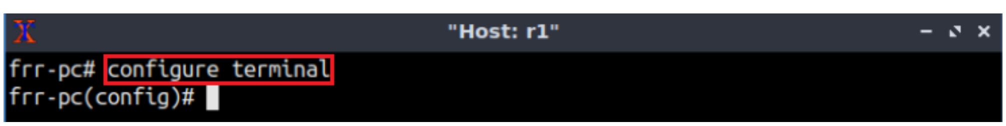

Figure 62. Enabling configuration mode on router r1.

Step 5. The ASN assigned for router r1 is 100. In order to apply the configuration, type the following command:

```
router bgp 100
```

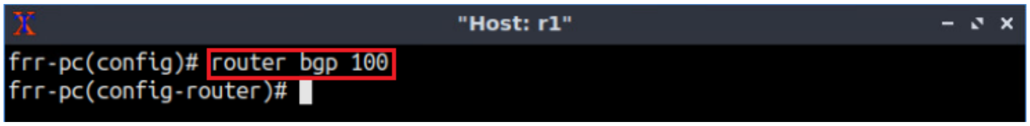

Figure 63. Configuring BGP on router r1.

Step 6. To configure a BGP neighbor to router r1 (AS 100), type the command shown below. This command specifies the neighbor IP address (192.168.12.2) and the ASN of the remote BGP peer (AS 200). This neighbor will act as the BGP transport for both IPv4 and IPv6 networks.

```
neighbor 192.168.12.2 remote-as 200
```

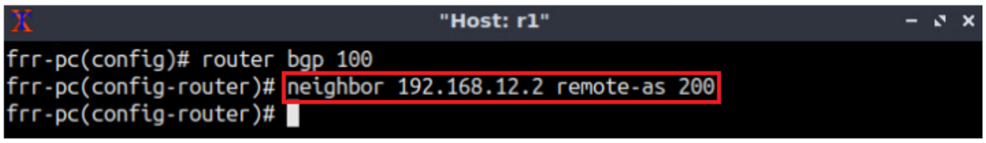

Figure 64. Assigning BGP neighbor to router r1.

Step 7. Type the following command to enter address-family mode where you can configure routing sessions that use standard IPv4 address prefixes.

```
address-family ipv4 unicast
```

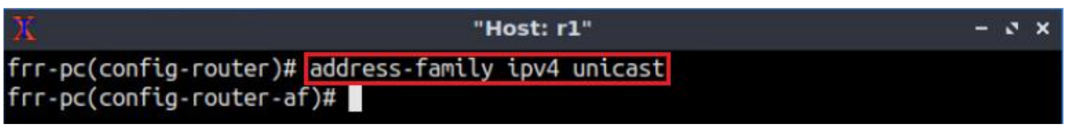

Figure 65. Enabling address-family IPv4 configuration mode on router r1.

Step 8. In this step, router r1 will advertise the LAN 192.168.1.0/24 to its BGP peers. To do so, issue the following command:

```
network 192.168.1.0/24
```

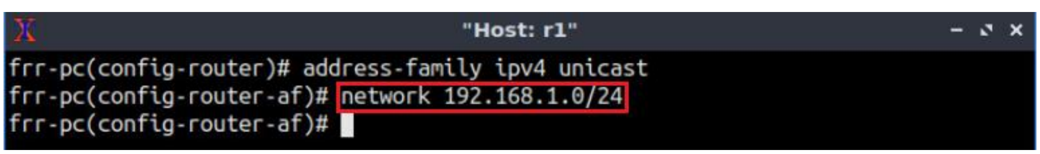

Figure 66. Advertising IPv4 LAN on router r1.

Step 9. Type the following command to activate the neighbor 192.168.12.2 so that router r1 uses this neighbor to advertise the IPv4 LAN.

```
neighbor 192.168.12.2 activate
```

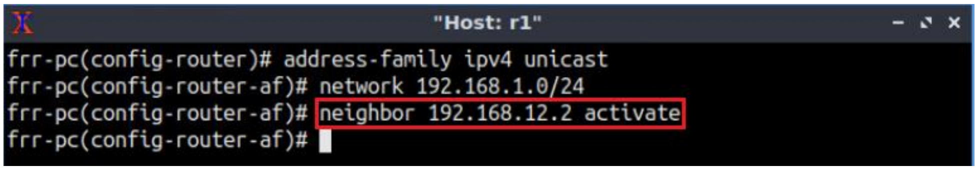

Figure 67. Activating neighbor to advertise IPv4 network.

Step 10. Type the following command to exit from the address-family mode.

```
exit-address-family
```

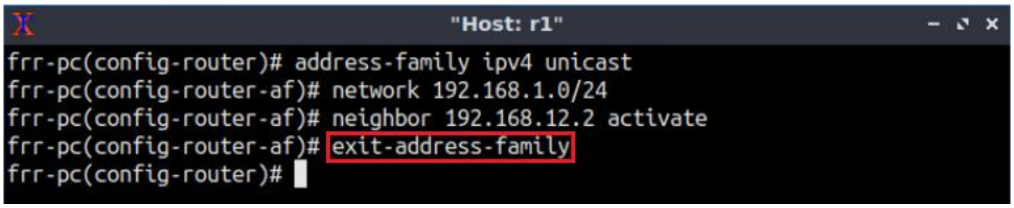

Figure 68. Exiting from address-family mode.

Step 11. Type the following command to exit from configuration mode.

```
end
```

Figure 69. Exiting from configuration mode.

Step 12. Type the following command to verify BGP networks. You will observe the LAN network of router r1.

```
show ip bgp
```

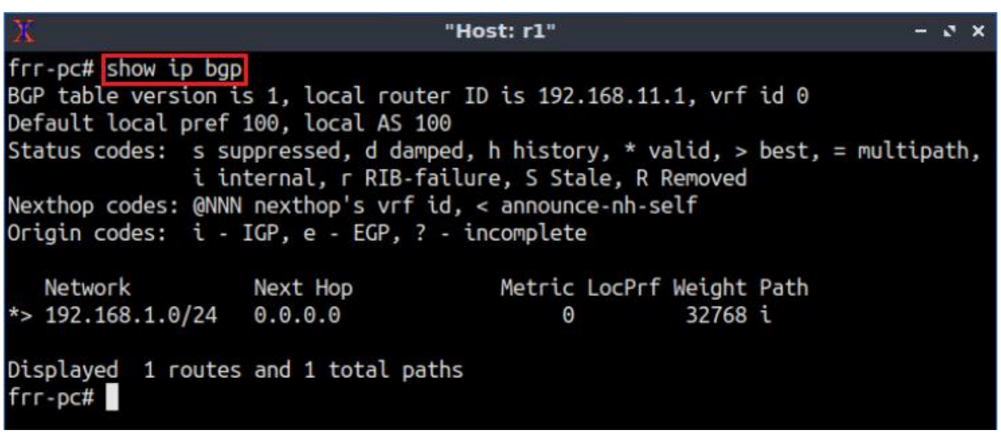

Figure 70. Verifying BGP networks on router r1.

Step 13. Type the following command on router r1 to verify IPv4 peering information with router r2. You will notice that BGP connectivity for IPv4 is over an IPv4 BGP transport session, using the neighbor address 192.168.12.2.

```
show bgp ipv4 summary
```

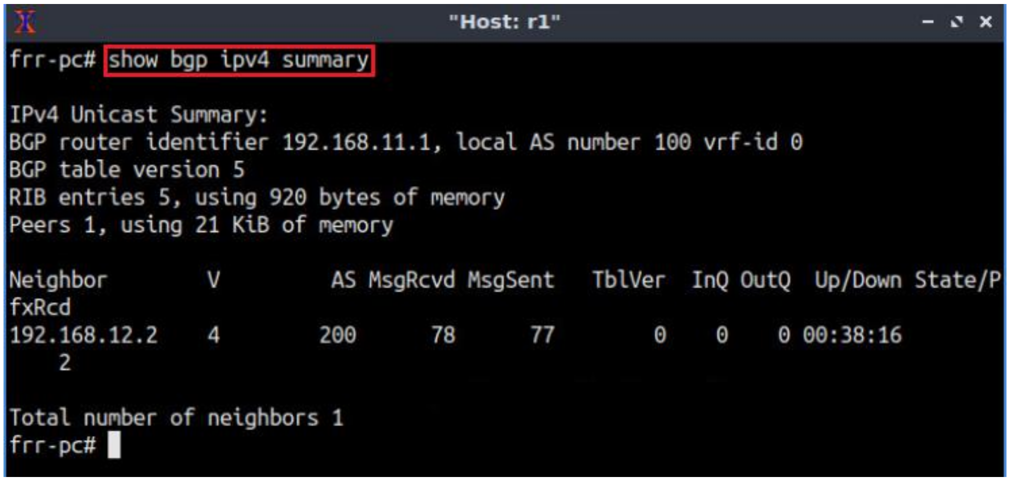

Figure 71. Verifying IPv4 BGP summary on router r1.

4.2 Configure and verify EBGP and IBGP on router r2

Step 1. On router r2, exit vtysh session and enable the BGP daemon. Enable router into configuration mode to configure BGP on router r2. All the steps are summarized in the following figure.

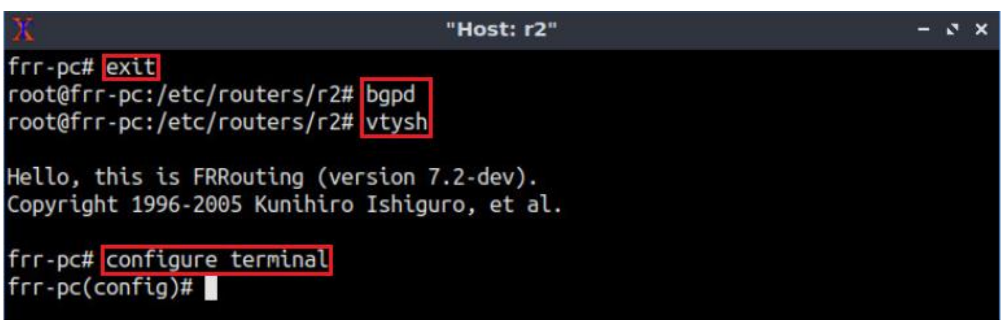

Figure 72. Starting BGP daemon on router r2.

Step 2. The ASN assigned for router r2 is 200. In order to configure BGP, type the following command:

```
router bgp 200
```

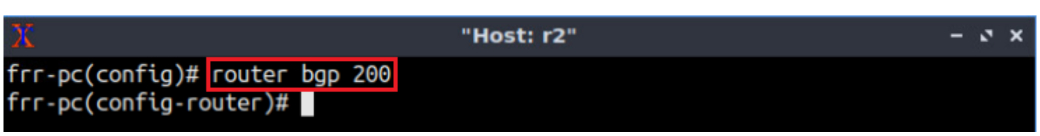

Figure 73. Configuring BGP on router r2.

Step 3. To configure EBGP neighbor to router r2 (AS 200), type the command shown below. This command specifies the neighbor IP address (192.168.12.1) and the ASN of the remote BGP peer (AS 100). This neighbor will act as the BGP transport for both IPv4 and IPv6 networks.

```
neighbor 192.168.12.1 remote-as 100
```

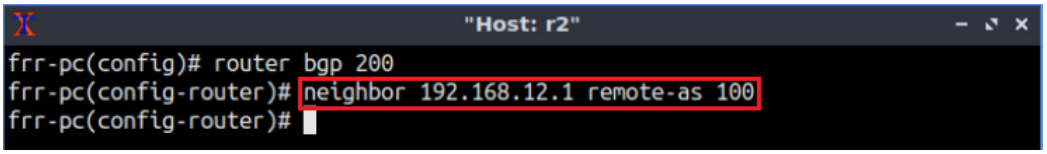

Figure 74. Assigning EBGP neighbor to router r2.

Step 4. Type the following command to assign the IPv4 neighbor so that IPv4 network uses IPv4 BGP transport while communicating with router r3. For IBGP peering between router r2 and router r3, assign the loopback address of router r3 as the neighbor of router r2.

```
neighbor 192.168.33.1 remote-as 200
```

Figure 75. Assigning IBGP neighbor to router r2 for IPv4 network.

Step 5. Type the following command to assign *lo* as the source IP in router r2.

```
neighbor 192.168.33.1 update-source lo
```

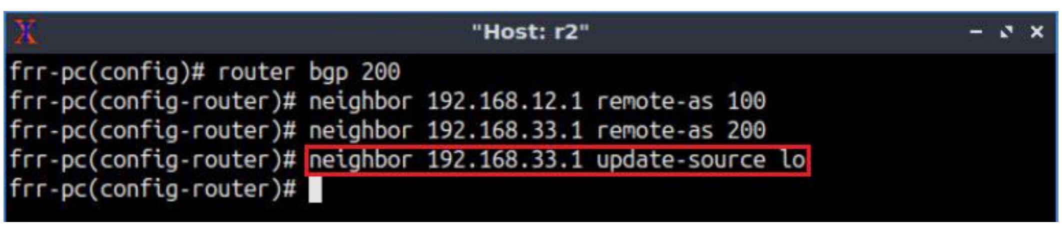

Figure 76.Assigning loopback as source IP for the neighbor 192.168.33.1.

Step 6. Type the following command to enter address-family mode where you can configure routing sessions that use standard IPv4 address prefixes.

```
address-family ipv4 unicast
```

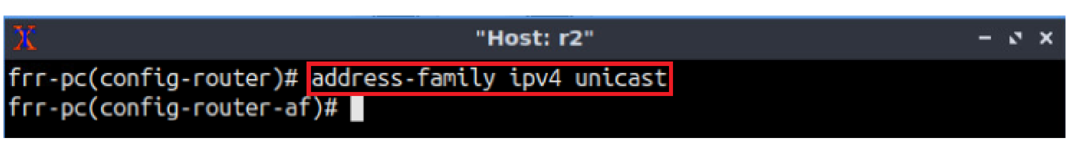

Figure 77. Enabling address-family IPv4 configuration mode on router r2.

Step 7. In this step, router r2 will advertise the LAN 192.168.2.0/24 to its BGP peers. To do so, issue the following command:

```
network 192.168.2.0/24
```

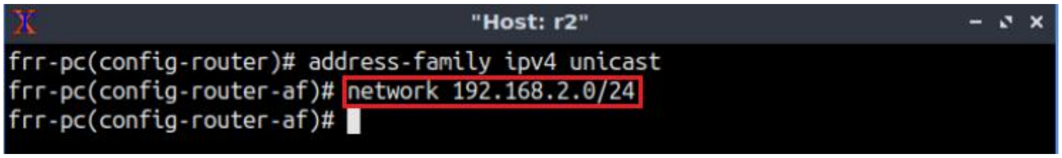

Figure 78. Advertising IPv4 LAN on router r2.

Step 8. Type the following command to activate the neighbor 192.168.12.1 so that this neighbor is used to exchange IPv4 routes with router r1.

```
neighbor 192.168.12.1 activate
```

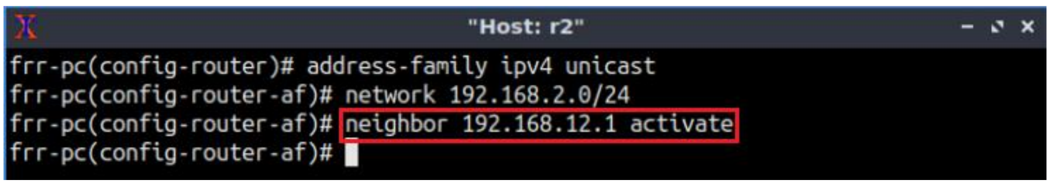

Figure 79. Activating EBGP neighbor to advertise IPv4 network.

Step 9. Type the following command to activate the neighbor 192.168.33.1 so that this neighbor is used to exchange IPv4 routes with router r3.

```
neighbor 192.168.33.1 activate
```

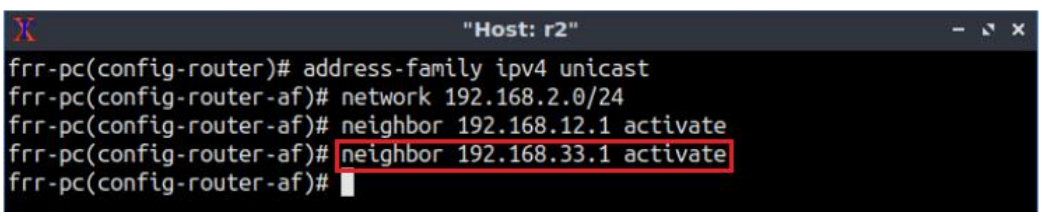

Figure 80. Activating IBGP neighbor to advertise IPv4 network.

Step 10. Type the following command on router r2 so that the interface lo is used as the next hop address of router r2. It will allow router r3 to receive the route to router r1 as the next hop address (192.168.22.1) is known to router r3.

```
neighbor 192.168.33.1 next-hop-self
```

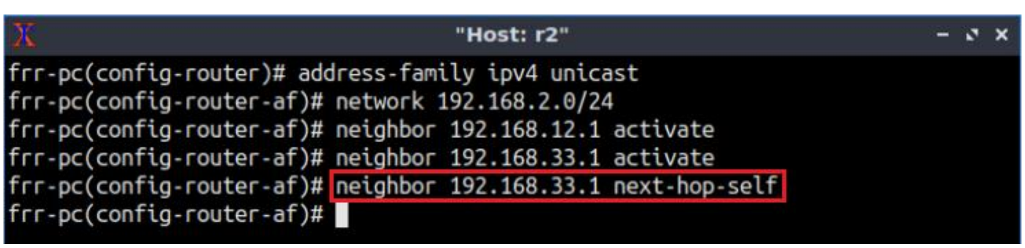

Figure 81. Assigning next hop address on router r2.

Step 11. Type the following command to exit from the address-family mode.

```
exit-address-family
```

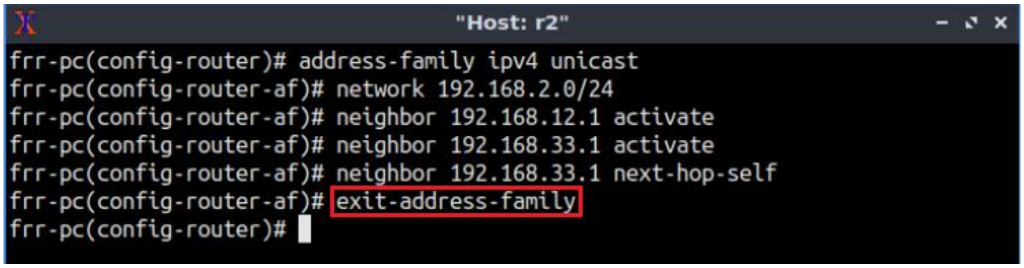

Figure 82. Exiting from address-family mode.

Step 12. Type the following command to exit from configuration mode.

```
end
```

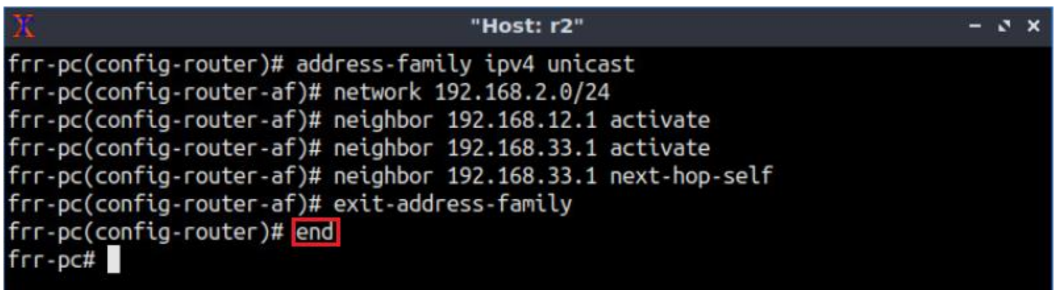

Figure 83. Exiting from configuration mode.

Step 13. Type the following command on router r2 to verify IPv4 peering information with routers r1 and r3. You will notice that BGP connectivity for IPv4 is over IPv4 BGP transport session, using the neighbor address 192.168.12.1 and 192.168.33.1 respectively.

```
show bgp ipv4 summary
```

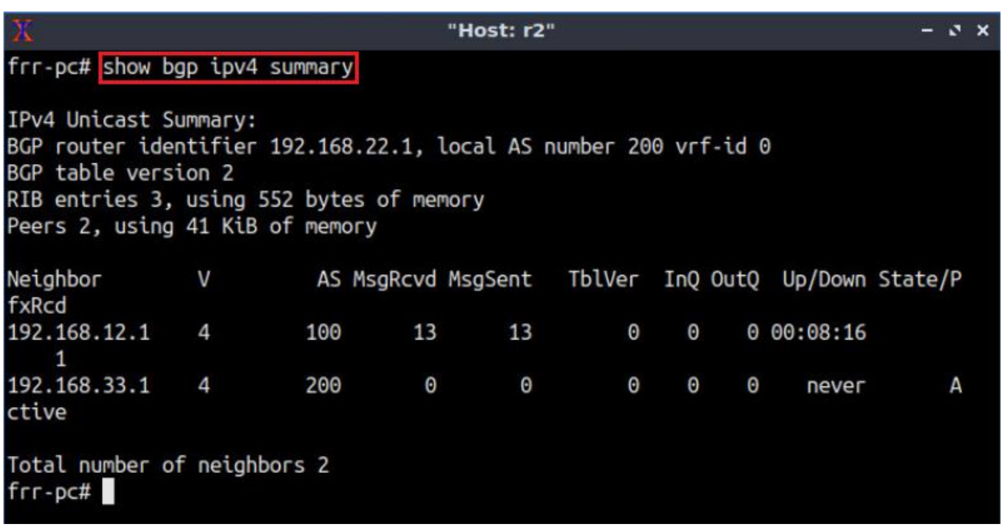

Figure 84. Verifying IPv4 BGP summary on router r2.

4.3 Configure and verify IBGP on router r3

Step 1. Router r3 is configured similarly to router r2 but, with different metrics in order to establish IBGP peering with router r2. All the steps are summarized in the following figure.

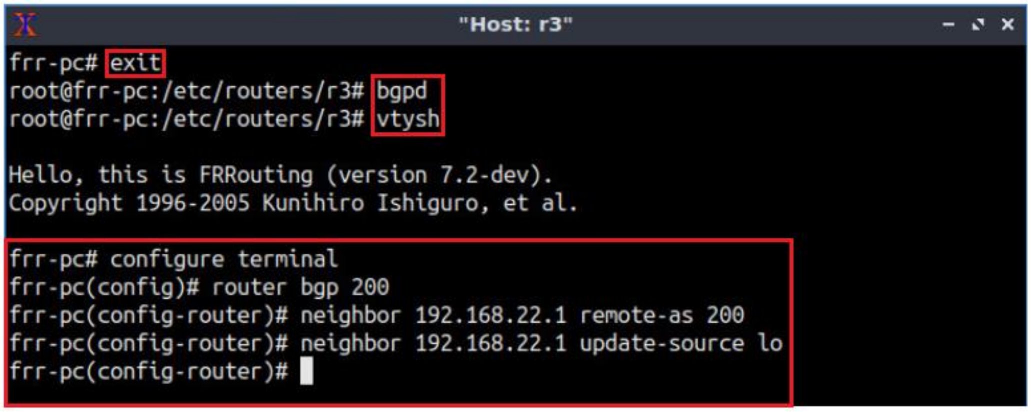

Figure 85. Configuring BGP on router r3.

Step 2. Configure IPv4 address-family on router r3. There is no need to assign the next hop when configuring BGP, since router r3 is not participating in any EBGP session. All the steps are summarized in the following figure.

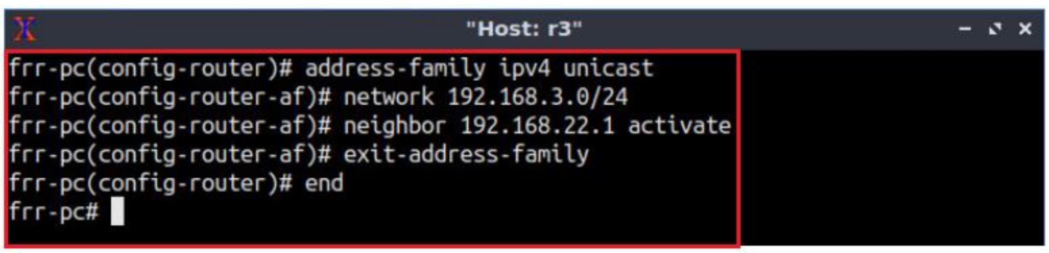

Figure 86. Configuring IPv4 address-family on router r3.

Step 3. Type the following command on router r3 to verify IPv4 peering information with router r2. You will notice that BGP connectivity for IPv4 is over an IPv4 BGP transport session, using the neighbor address 192.168.22.1.

```
show bgp ipv4 summary
```

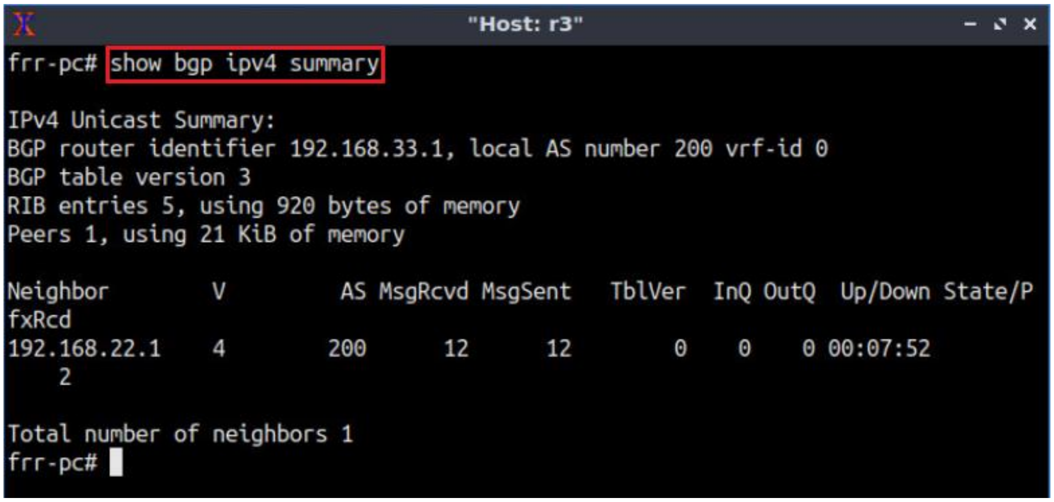

Figure 87. Verifying IPv4 BGP summary on router r3.

5 Configure and verify BGP for IPv6 networks

In this section, you will configure EBGP so that router r1 uses IPv4 as the BGP transport for IPv6 sessions. Create a route-map next-hop-IPv6 to attach to the BGP neighbor in the outbound direction so that the next-hop parameter overwrites with the appropriate IPv6 next-hop address. For IBGP, you will configure router r2 so that IPv6 routing information is transported by IPv6 TCP sessions.

5.1 Configure and verify EBGP on router r1

Step 1. To enable router r1 into configuration mode, issue the following command:

```
configure terminal
```

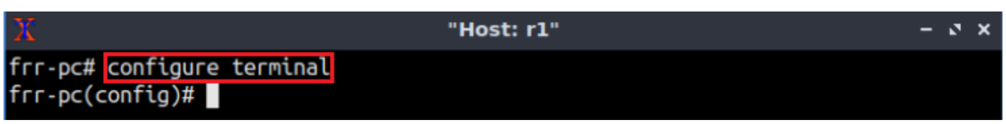

Figure 88. Enabling configuration mode on router r1.

Step 2. Type the following command to create a route-map named next-hop-IPv6 with permit clause. The permit clause will allow BGP to use the route map policy. The sequence number allows the identification and editing of multiple statements. You will use default sequence number which is 10. You will be entering the configuration mode where you can set the route-map policy.

```
route-map next-hop-ipv6 permit 10
```

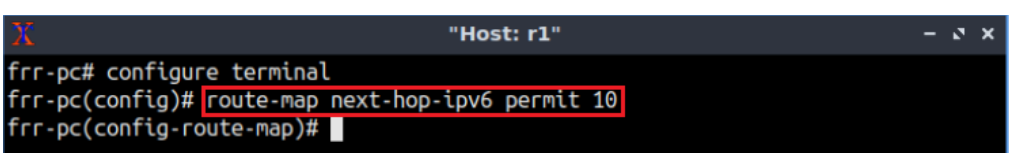

Figure 89. Creating next-hop-IPv6 route-map.

Step 3. Type the following command to set the route-map policy. As the IPv6 address will be transported by IPv4 TCP session, you need an IPv6 address so that the next-hop parameter overwrites with the appropriate IPv6 next-hop address. By the route-map policy, you will set the global IPv6 address 2001:192:168:12::1 for router r1 which will be the next hop address for router r2 and the link local address will appear as the next hop address in the BGP table of router r2.

```
set ipv6 next-hop global 2001:192:168:12::1
```

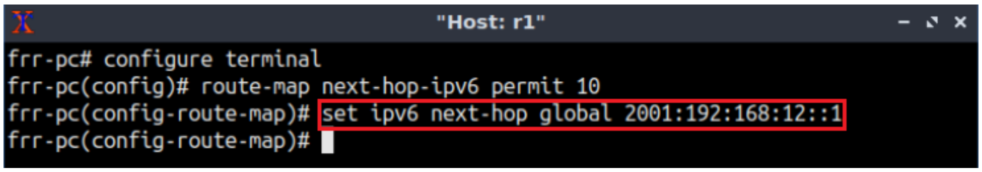

Figure 90. Setting route-map policy in router r1.

Step 4. Type the following command to exit from the configuration mode.

```
exit
```

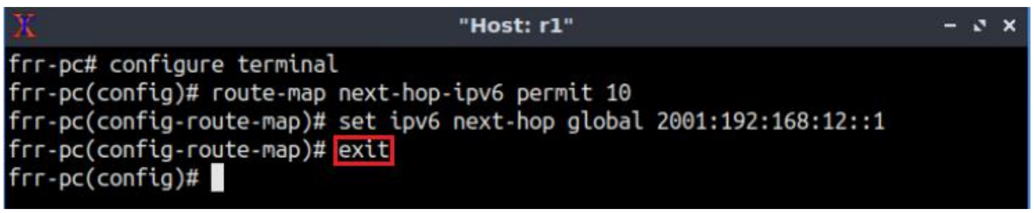

Figure 91. Exiting from route-map mode.

Step 5. The ASN assigned for router r1 is 100. In order to apply the configuration, type the following command:

```
router bgp 100
```

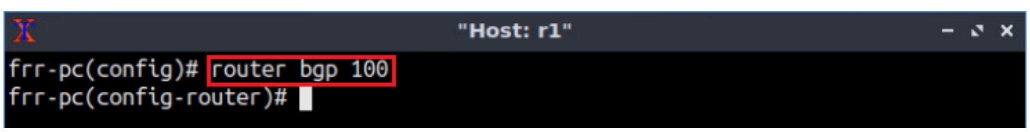

Figure 92. Configuring BGP on router r1.

Step 6. Type the following command to enter address-family mode where you can configure routing sessions that use standard IPv6 address prefixes.

```
address-family ipv6 unicast
```

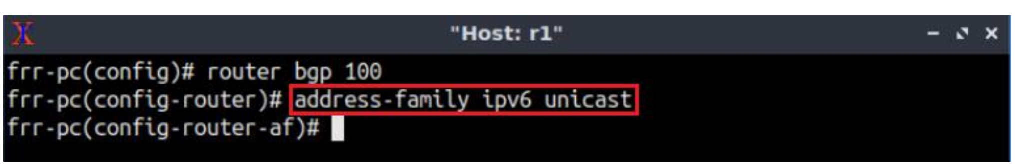

Figure 93. Enabling address-family IPv6 configuration mode on router r1.

Step 7. In this step, router r1 will advertise the IPv6 LAN 2001:192:168:1::/64 to its BGP peers. To do so, issue the following command:

```
network 2001:192:168:1::/64
```

Figure 94. Advertising IPv6 LAN on router r1.

Step 8. Since you are using IPv4 neighbor as BGP transport, you will activate the IPv4 neighbor within the IPv6 address-family. To do so, type the following command.

```
neighbor 192.168.12.2 activate
```

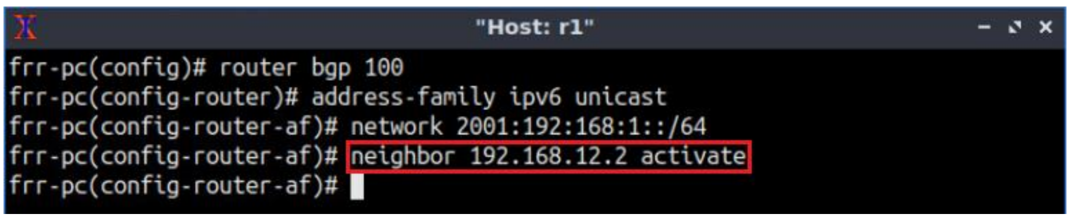

Figure 95. Activating neighbor to advertise IPv6 network.

Step 9. Type the following command to attach the route-map to BGP neighbor in the outbound direction. Outbound direction means that this information in the route-map will be applied to IPv6 BGP updates as they are sent to router r2. In the BGP table of router r2, 2001:192:168:12::1 will be used as next-hop address. The next-hop address will be the link local address of 2001:192:168:12::1 because link local addresses are used as next-hop address in FRR.

```
neighbor 192.168.12.2 route-map next-hop-ipv6 out
```

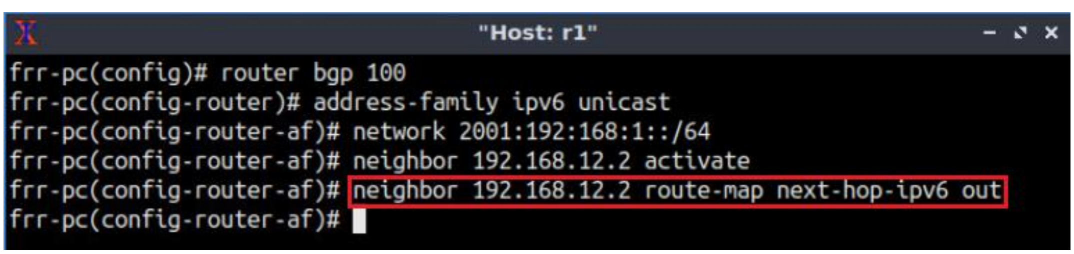

Figure 96. Attaching the route-map to BGP neighbor.

Step 10. Type the following command to exit from the address-family mode.

```
exit-address-family
```

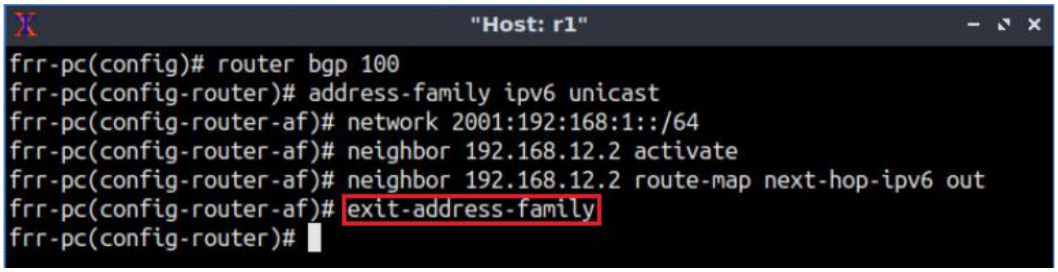

Figure 97. Exiting from address-family mode.

Step 11. Type the following command to exit from configuration mode.

```
end
```

Figure 98. Exiting from configuration mode.

Step 12. Type the following command on router r1 to verify IPv6 peering information with router r2. You will notice that BGP connectivity for IPv6 is over an IPv4 BGP transport session, using the neighbor address 192.168.12.2.

```
show bgp ipv6 summary
```

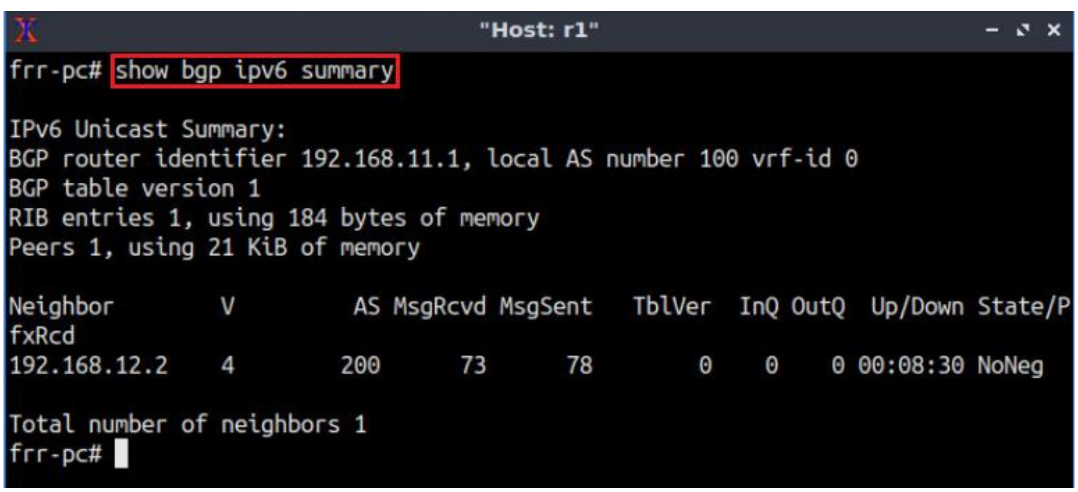

Figure 99. Verifying IPv6 BGP summary on router r1.

5.2 Configure and verify EBGP and IBGP on router r2

Step 1. Enable BGP daemon and create a route-map so that you can attach the route-map to the BGP neighbor of router r2. All the steps are summarized in the figure below.

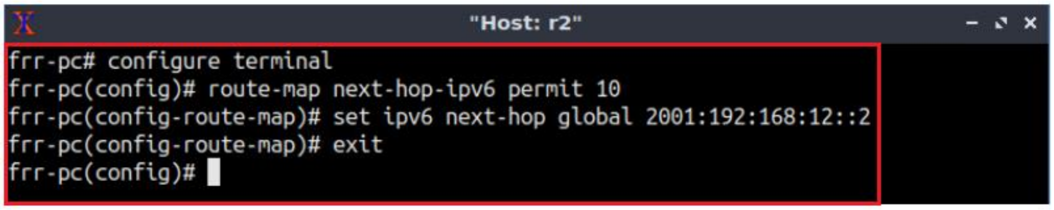

Figure 100. Creating next-hop-IPv6 route-map on router r2.

Step 2. The ASN assigned for router r2 is 200. In order to configure BGP, type the following command:

```
router bgp 200
```

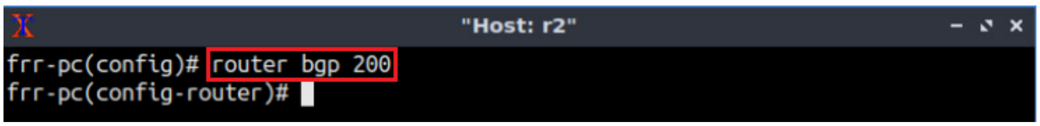

Figure 101. Configuring BGP on router r2.

Step 3. In this step, you will configure IBGP neighbor to router r2. Type the following command to assign the IPv6 neighbor so that IPv6 network uses IPv6 BGP transport. For IBGP peering between router r2 and router r3, assign the loopback address of router r3 as the neighbor of router r2.

```
neighbor 2001:192:168:33::1 remote-as 200
```

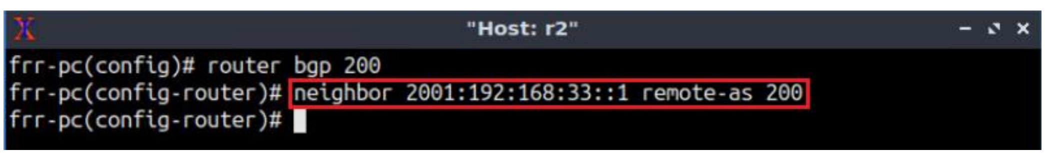

Figure 102. Assigning IBGP neighbor to router r2 for IPv6 network.

Step 4. In BGP, the source IP address of BGP packets sent by the router must be the same as neighbor IP address set on the neighboring router. As you are assigning the loopback as neighbor address, you must use loopback address as the source of BGP packets sent to the neighbor. Type the following command to assign *lo* as source IP in router r2.

```
neighbor 2001:192:168:33::1 update-source lo
```

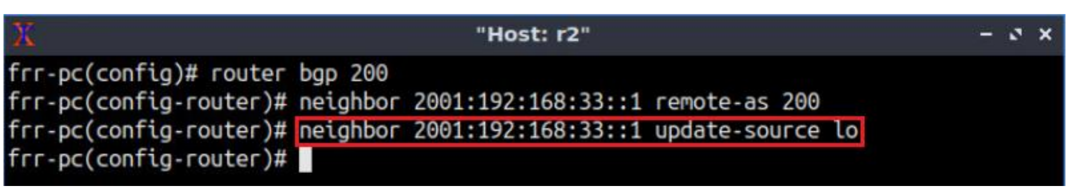

Figure 103.Assigning loopback as source IP for the neighbor 2001:192:168:33::1.

Step 5. Type the following command to enter address-family mode where you can configure routing sessions that use standard IPv6 address prefixes.

```
address-family ipv6 unicast
```

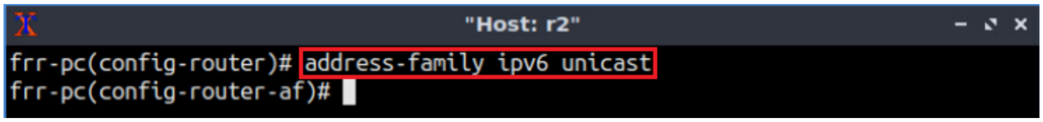

Figure 104. Enabling address-family IPv6 configuration mode on router r2.

Step 6. In this step, router r2 will advertise the LAN 2001:192:168:2::/64 to its BGP peers. To do so, issue the following command:

```
network 2001:192:168:2::/64
```

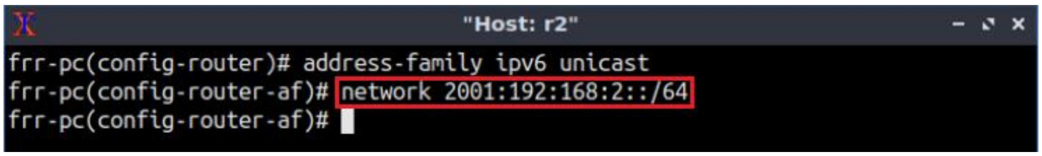

Figure 105. Advertising IPv6 LAN on router r2.

Step 7. Type the following command to activate the neighbor 192.168.12.1 so that router r2 uses this neighbor to exchange IPv6 routes with router r1.

```
neighbor 192.168.12.1 activate
```

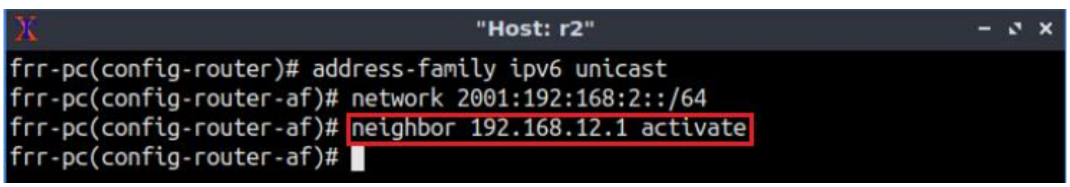

Figure 106. Activating neighbor to advertise IPv6 network.

Step 8. Type the following command to attach the route-map to BGP neighbor in the outbound direction. Outbound direction means that this information in the route-map will be applied to IPv6 BGP updates as they are sent to router r1. In the BGP table of router r1, 2001:192:168:12::2 will be used as next-hop address. The next-hop address will be the link local address of 2001:192:168:12::2 because FRR always uses link local address as next-hop address.

```
neighbor 192.168.12.1 route-map next-hop-ipv6 out
```

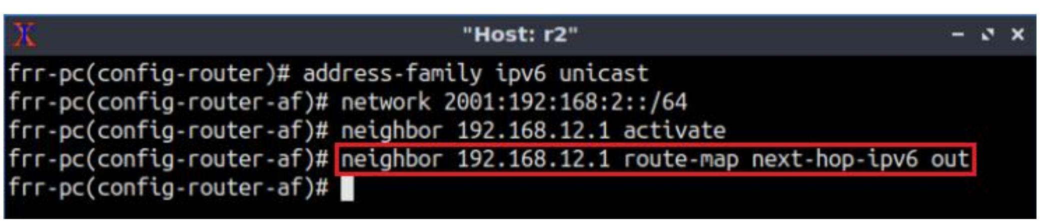

Figure 107. Attaching the route-map to BGP neighbor of router r2.

Step 9. Type the following command to activate the neighbor 2001:192:168:33::1 so that router r2 uses this neighbor to exchange IPv6 routes with router r3.

```
neighbor 2001:192:168:33::1 activate
```

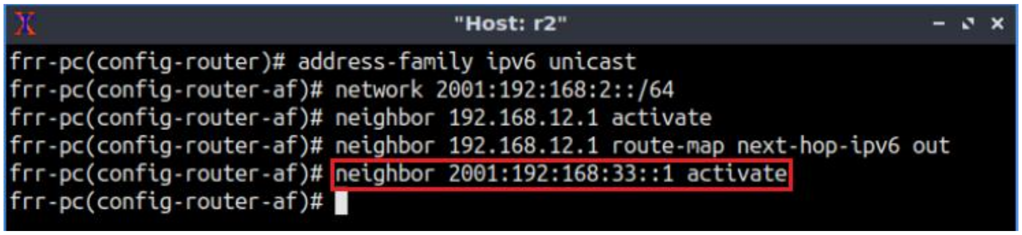

Figure 108. Activating neighbor to advertise IPv6 network.

Step 10. Type the following command on router r2 so that the interface lo is used as the next hop address of router r2. It will allow router r3 to receive the route to router r1 as the next hop address (2001:192:168:22::1) is known to router r3.

```
neighbor 2001:192:168:33::1 next-hop-self
```

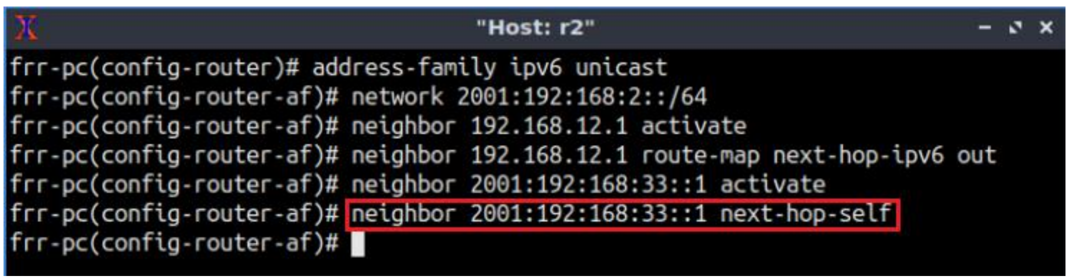

Figure 109. Assigning next hop address on router r2.

Step 11. Type the following command to exit from the address-family mode.

```
exit-address-family
```

Figure 110. Exiting from address-family mode.

Step 12. Type the following command to exit from configuration mode.

```
end
```

Figure 111. Exiting from configuration mode.

Step 13. Type the following command on router r2 to verify IPv6 neighbors. The BGP table shows that router r2 communicates with router r1 through IPv4 neighbor (192.168.12.1) and communicates with router r3 via IPv6 neighbor (2001:192:168:33::1).

```
show bgp ipv6 unicast summary
```

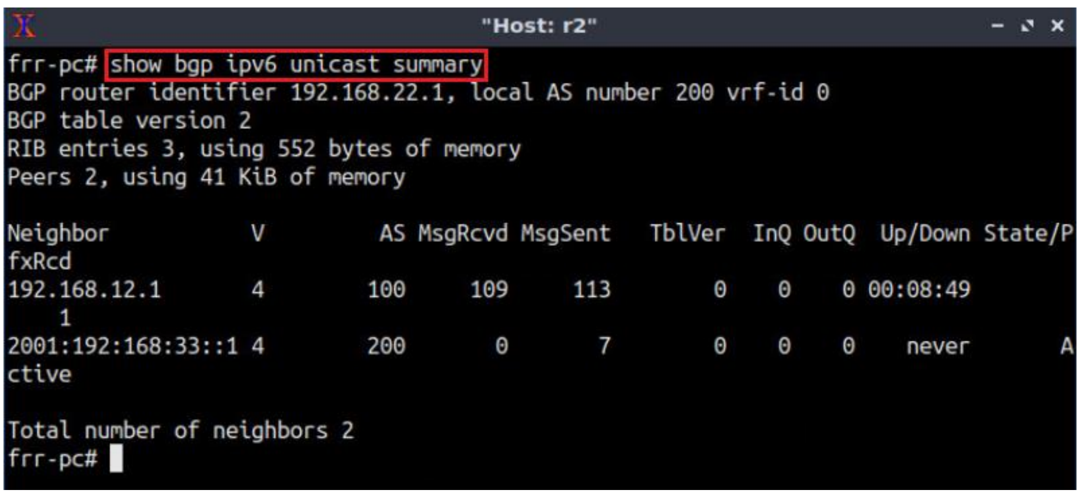

Figure 112. Verifying IPv6 BGP neighbors on router r2.

Step 14. Type the following command on router r2 to verify IPv6 routes. You will notice the link local address of 2001:192:168:12::2 as the next hop address for the network 2001:192:168:1::/64 which was used in the route-map.

```
show bgp ipv6 unicast
```

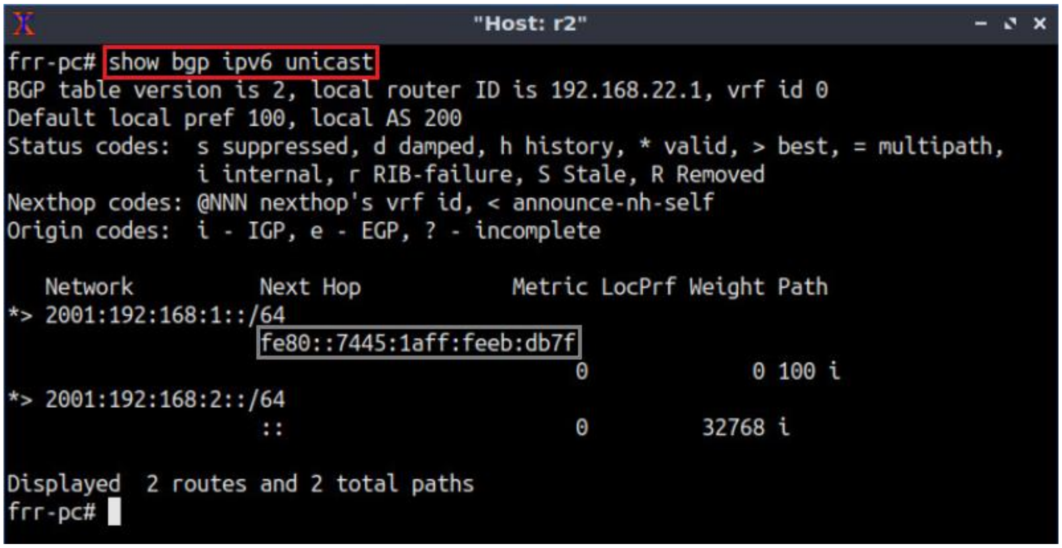

Figure 113. Verifying IPv6 routes on router r2.

5.3 Configure and verify IBGP on router r3

Step 1. Router r3 is configured similarly to router r2 but, with different metrics in order to establish IBGP peering with router r2. All the steps are summarized in the following figure.

Figure 114. Configuring BGP on router r3.

Step 2. Configure IPv6 address-family on router r3. All the steps are summarized in the following figure.

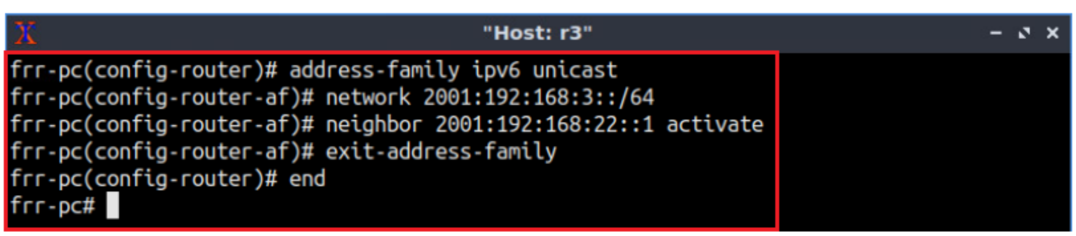

Figure 115. Configuring IPv6 address-family on router r3.

Step 3. Type the following command on router r3 to verify IPv6 neighbors. The BGP table shows that router r3 communicates with router r2 through IPv6 neighbor (2001:192:168:22::1).

```
show bgp ipv6 summary
```

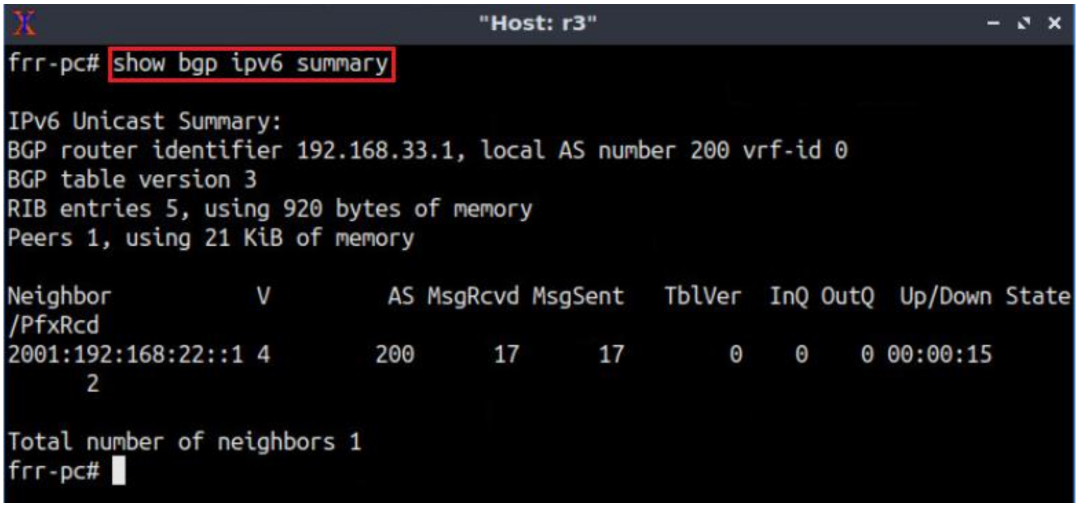

Figure 116. Verifying IPv6 BGP neighbors on router r3.

6 Verify BGP configuration

Step 1. Type the following command to verify the routing table of router r3.

```
show ipv6 route
```

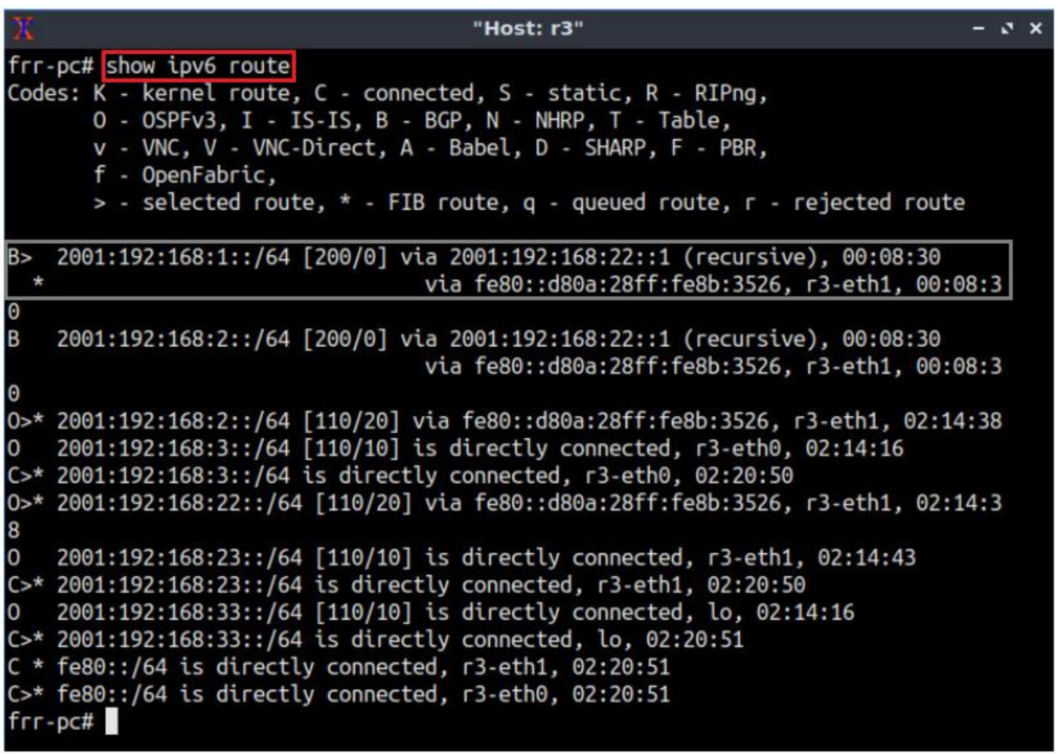

Figure 117. Verifying IPv6 routes on router r3.

Consider Figure 117. To reach the network 2001:192:168:1::/64, router r3 uses the link local address of the interface r3-eth1 to communicate with router r2 since they are directly connected. Then, router r2 (2001:192:168:22::1) uses IPv4 BGP transport to reach the LAN 2001:192:168:1::/64.

Step 2. On host h6 terminal, perform a connectivity between host h6 and host h4 by issuing the command shown below. To stop the test, press `Ctrl+c`. The result will show a successful connectivity test.

```
ping 2001:192:168:1::10
```

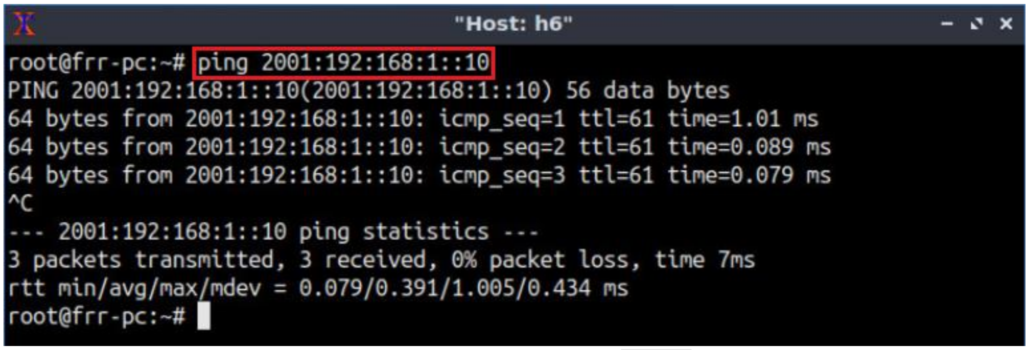

Figure 118. Connectivity test using `ping` command.

This concludes Lab 11. Stop the emulation and then exit out of MiniEdit.

References

1. J. Postelet al., “Internet protocol”, 1981. [Online]. Available: https://tools.ietf.org/html/rfc791
2. S. Deering, R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, 1998. [Online]. Available: https://tools.ietf.org/html/rfc2460
3. Cisco, “IPv6 Addressing and Basic Connectivity Configuration Guide, Cisco IOS Release 15M&T”, 2013. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/15-mt/ip6b-15-mt-book.pdf
4. A. Tanenbaum, D. Wetherall, “Computer networks”, 5th Edition, Pearson, 2012.
5. Cisco, “What Are OSPF Areas and Virtual Links?”, 2016. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13703-8.html
6. R. Coltun, D. Ferguson, J. Moy, A. Lindem, “OSPF for IPv6”, 2008.
7. T. Bates, R. Chandra, D. Katz, Y. Rekhter, “Multiprotocol Extensions for BGP-4”, 1998. [Online]. Available: https://tools.ietf.org/html/rfc2283
8. Cisco, “Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide”, Pearson, 2015.