# 300-135.exam.71q

Number: 300-135
Passing Score: 800
Time Limit: 120 min
File Version: 1

**Cisco 300-135**


https://www.gratisexam.com/

**Troubleshooting and Maintaining Cisco IP Networks**

**Exam A**

**QUESTION 1**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

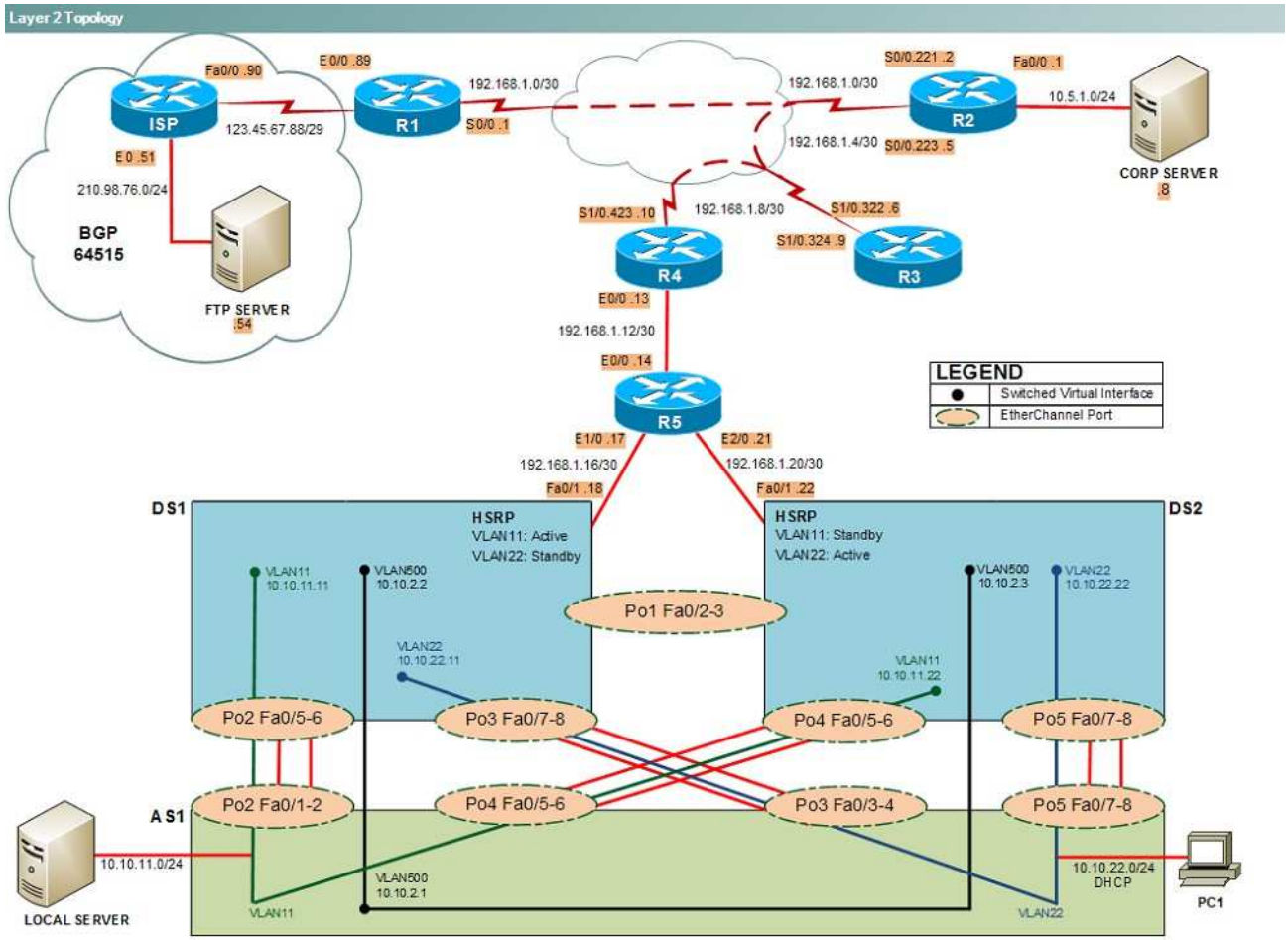
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

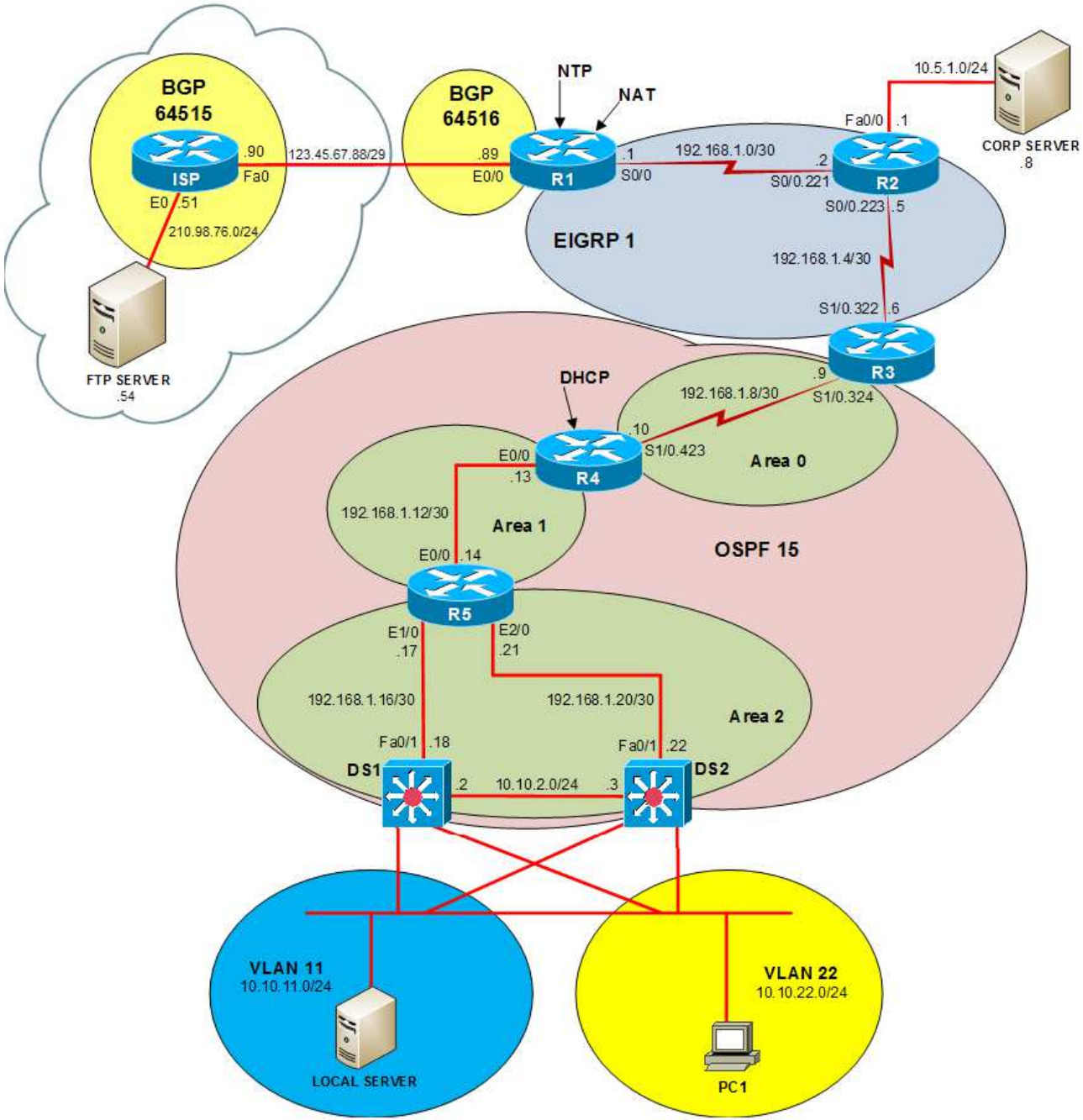
GRATIS EXAM
Free Practice Exams

https://www.gratisexam.com/

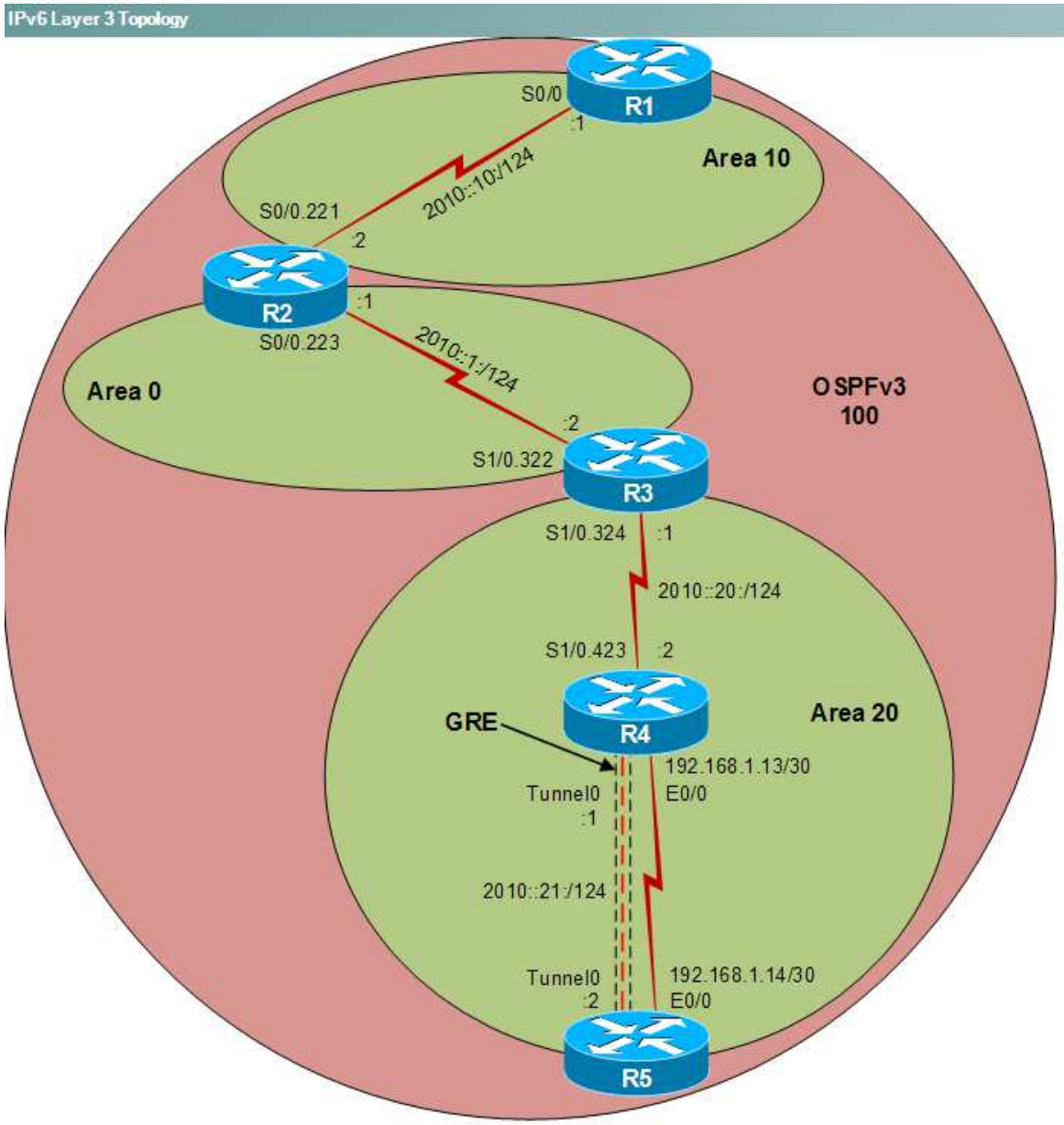
**Layer 2 Topology**




IPv4 layer 3 Topology

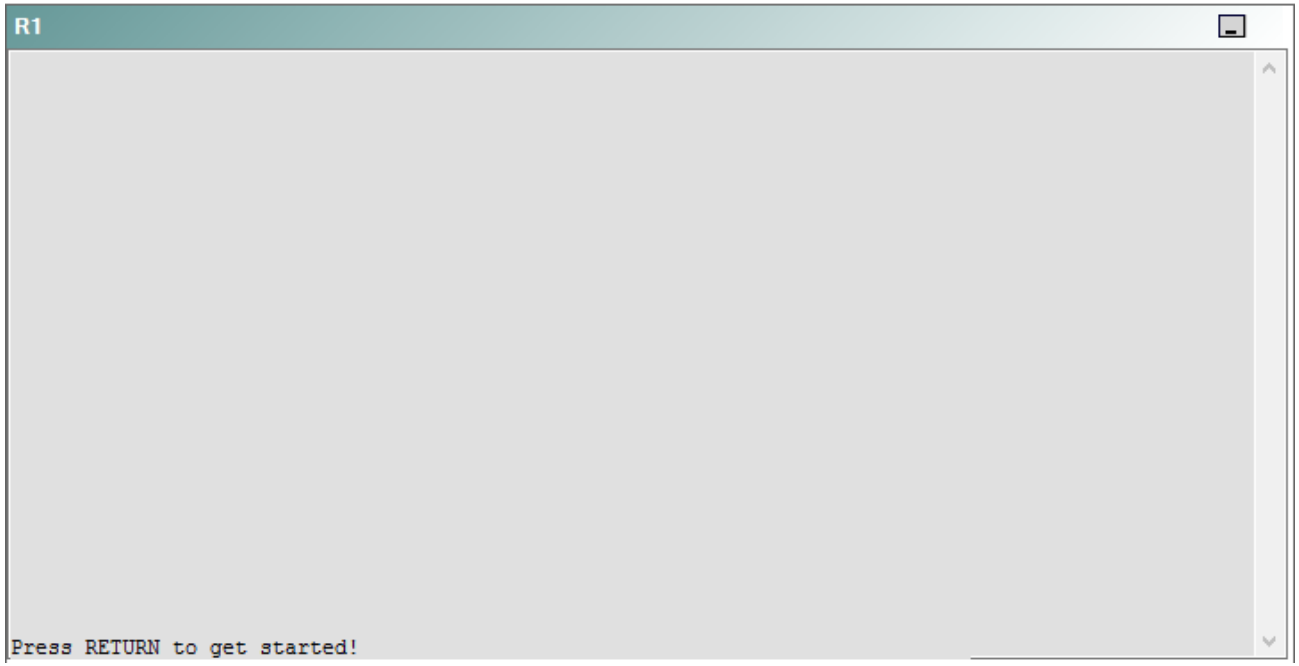

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

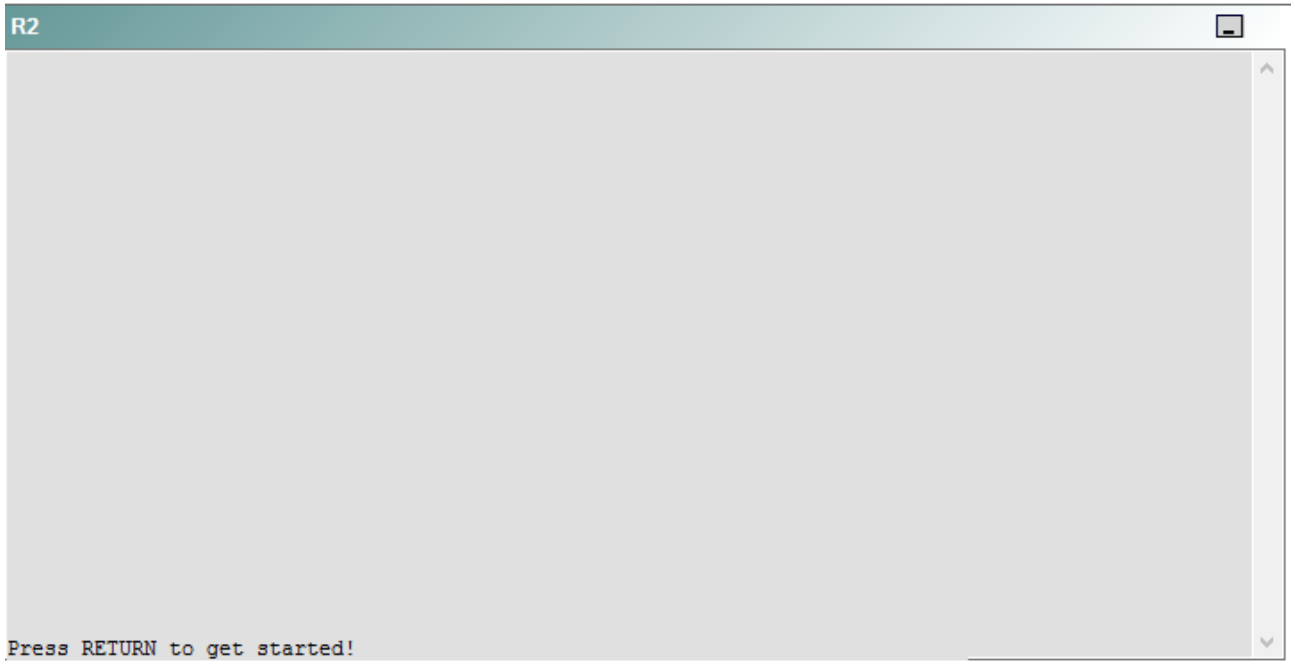



https://www.gratisexam.com/

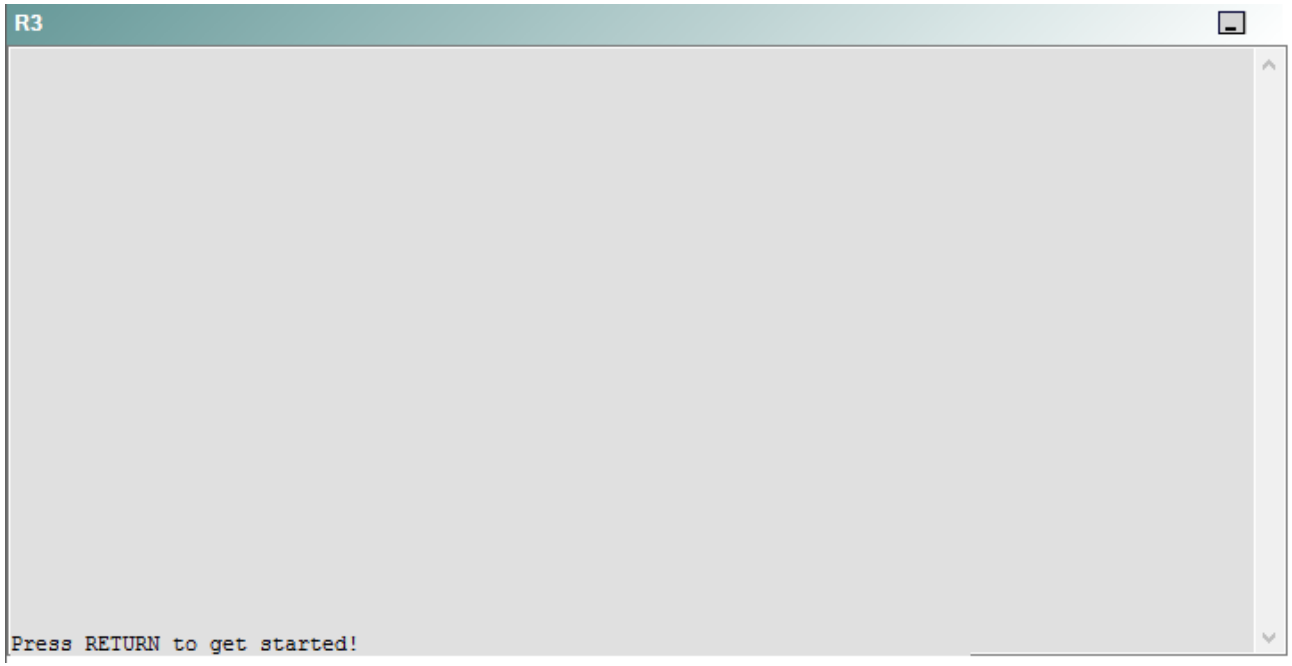
R1



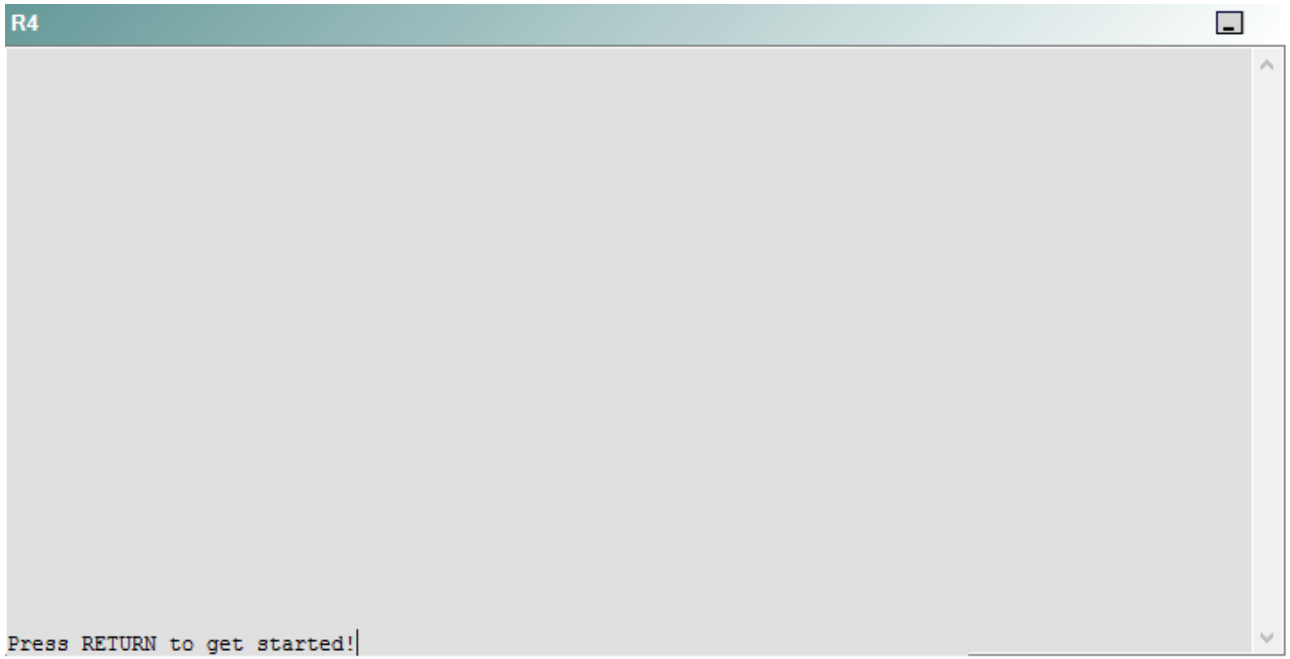

R2



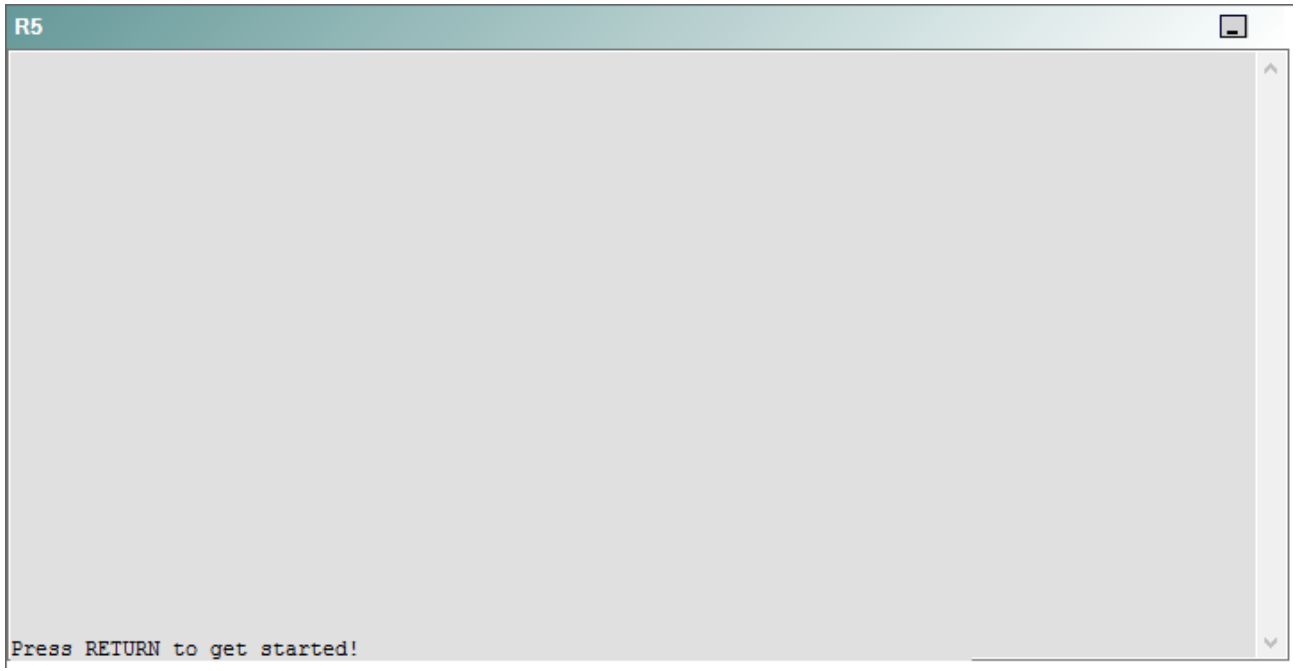

R3



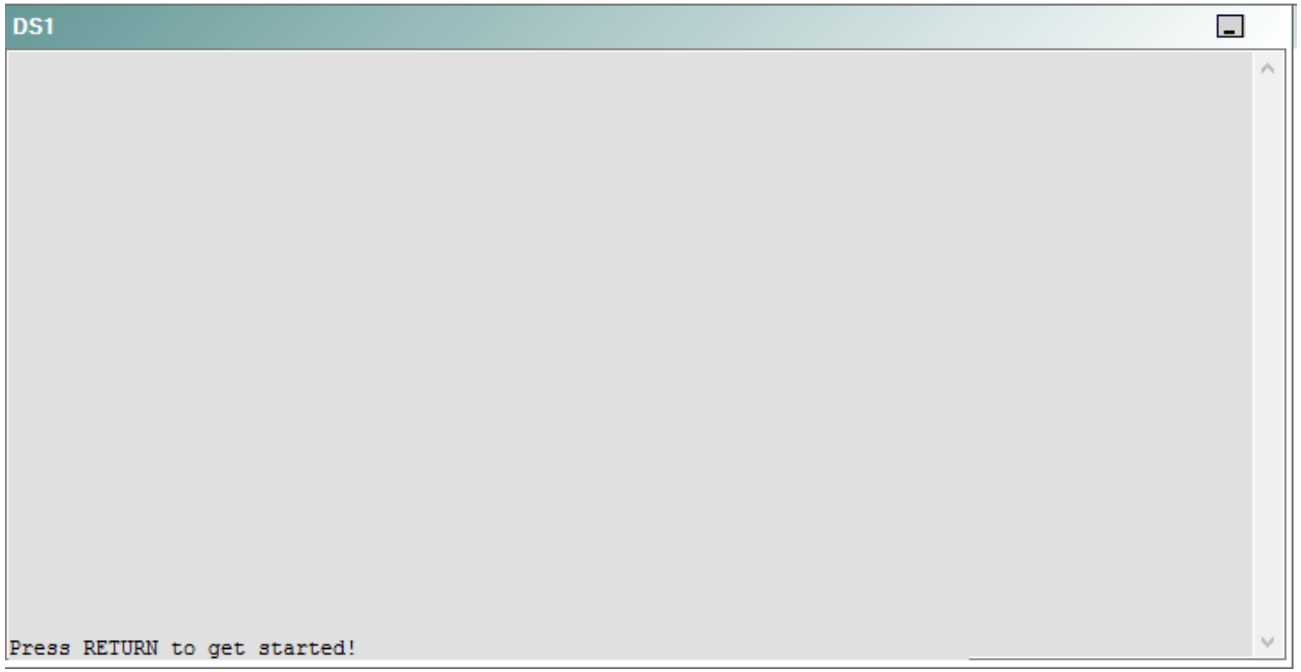

R4



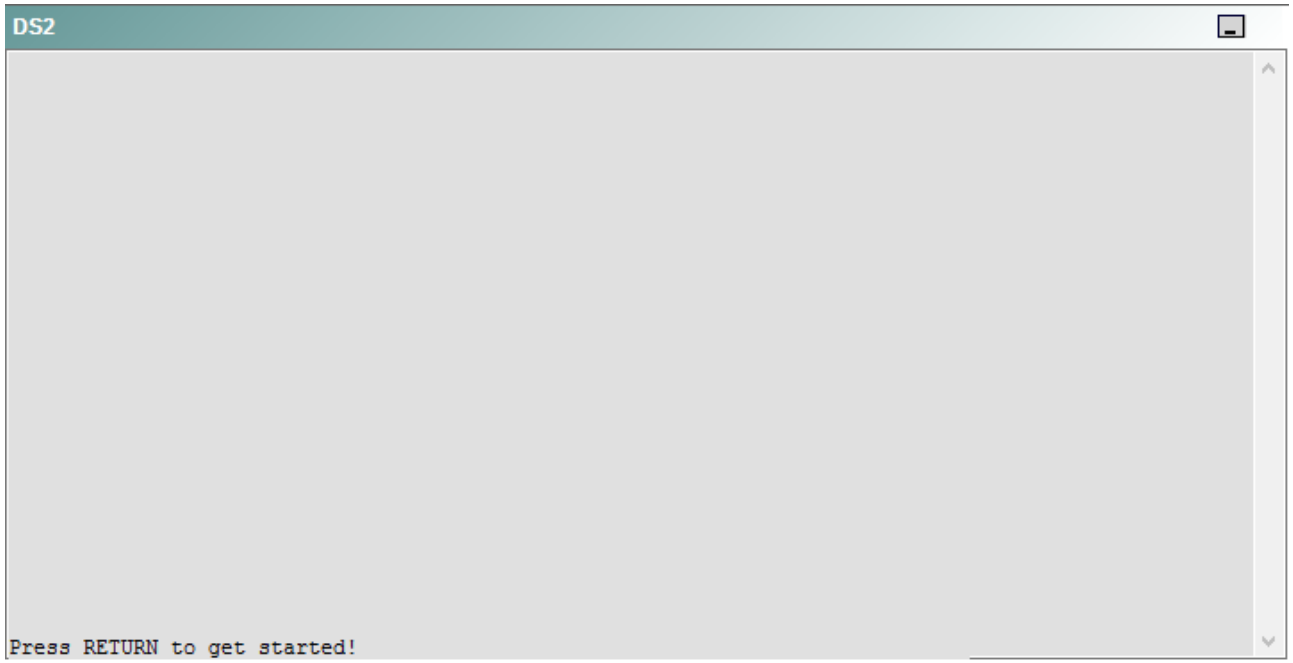

R5



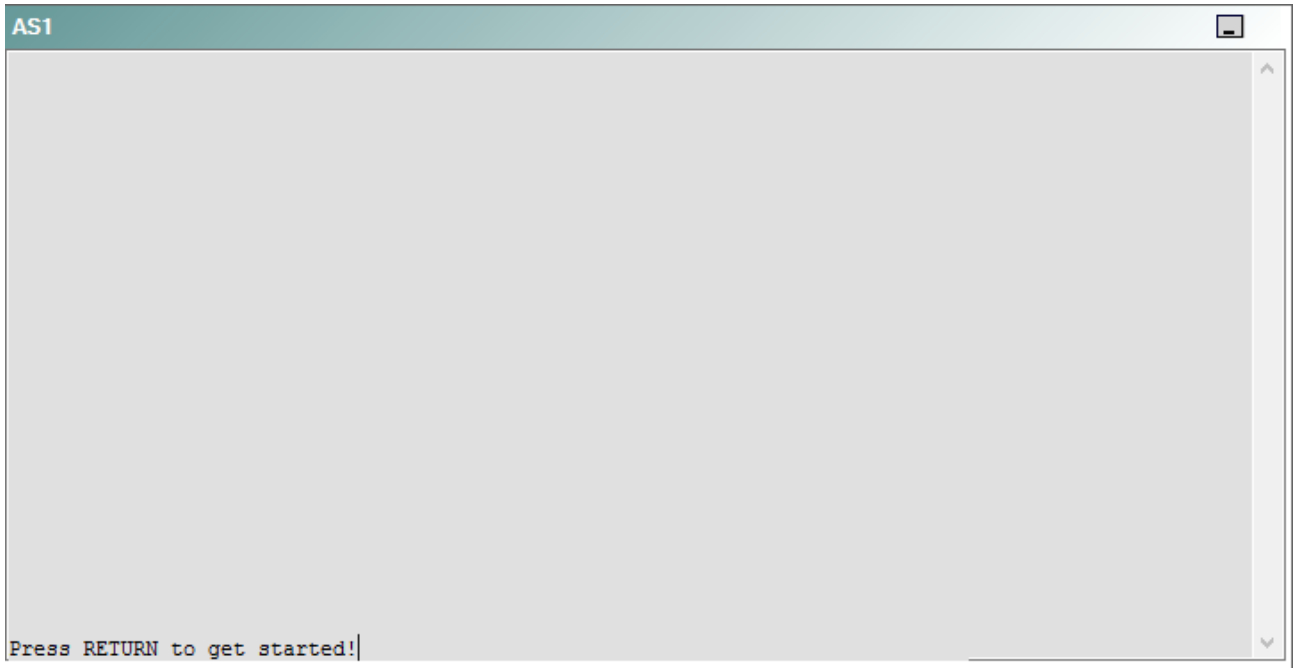

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. OSPFv2
C. OSPFv3
D. EIGRP
E. redistribution
F. Layer 3 addressing
G. interface

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 2**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

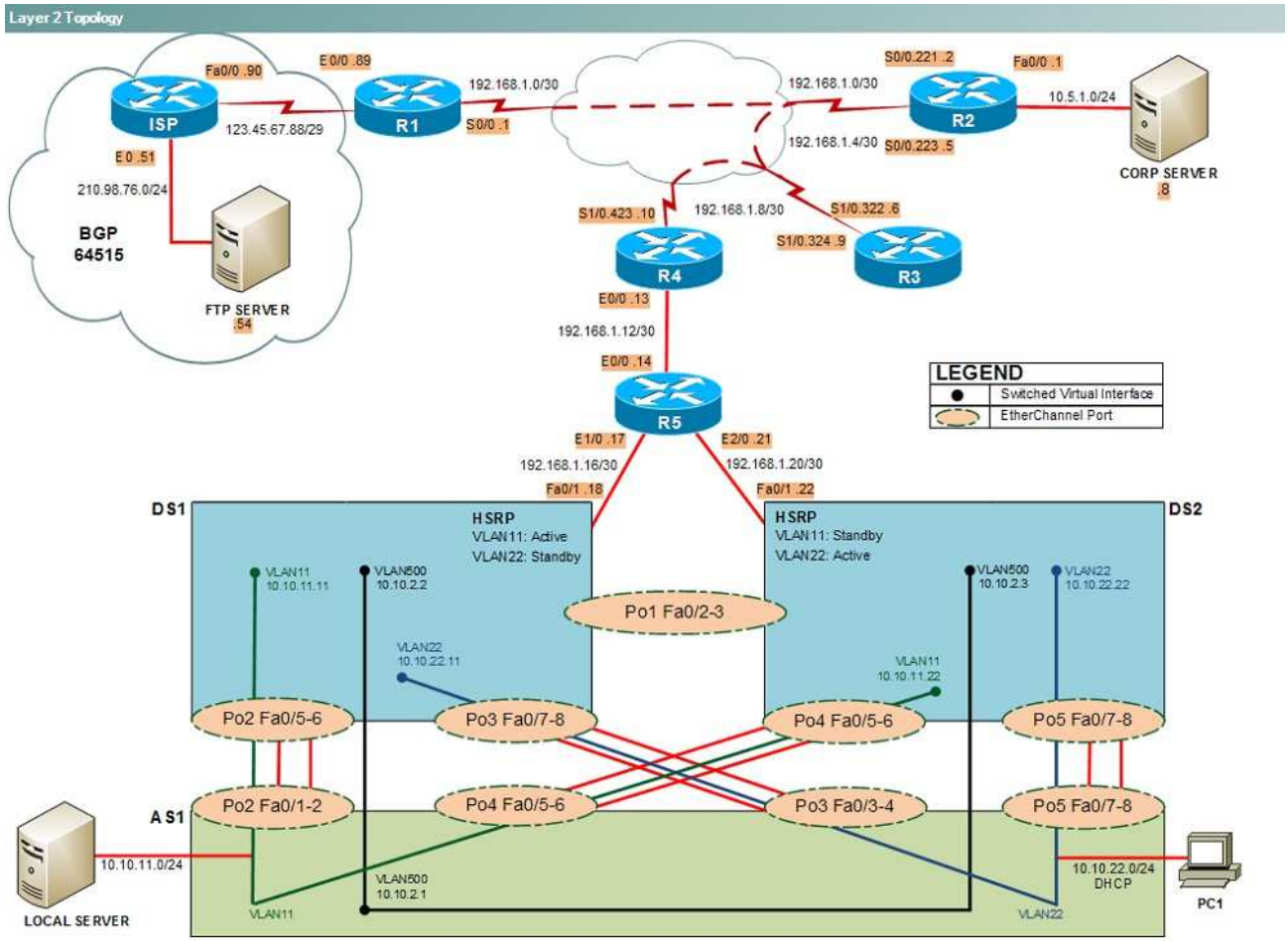
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

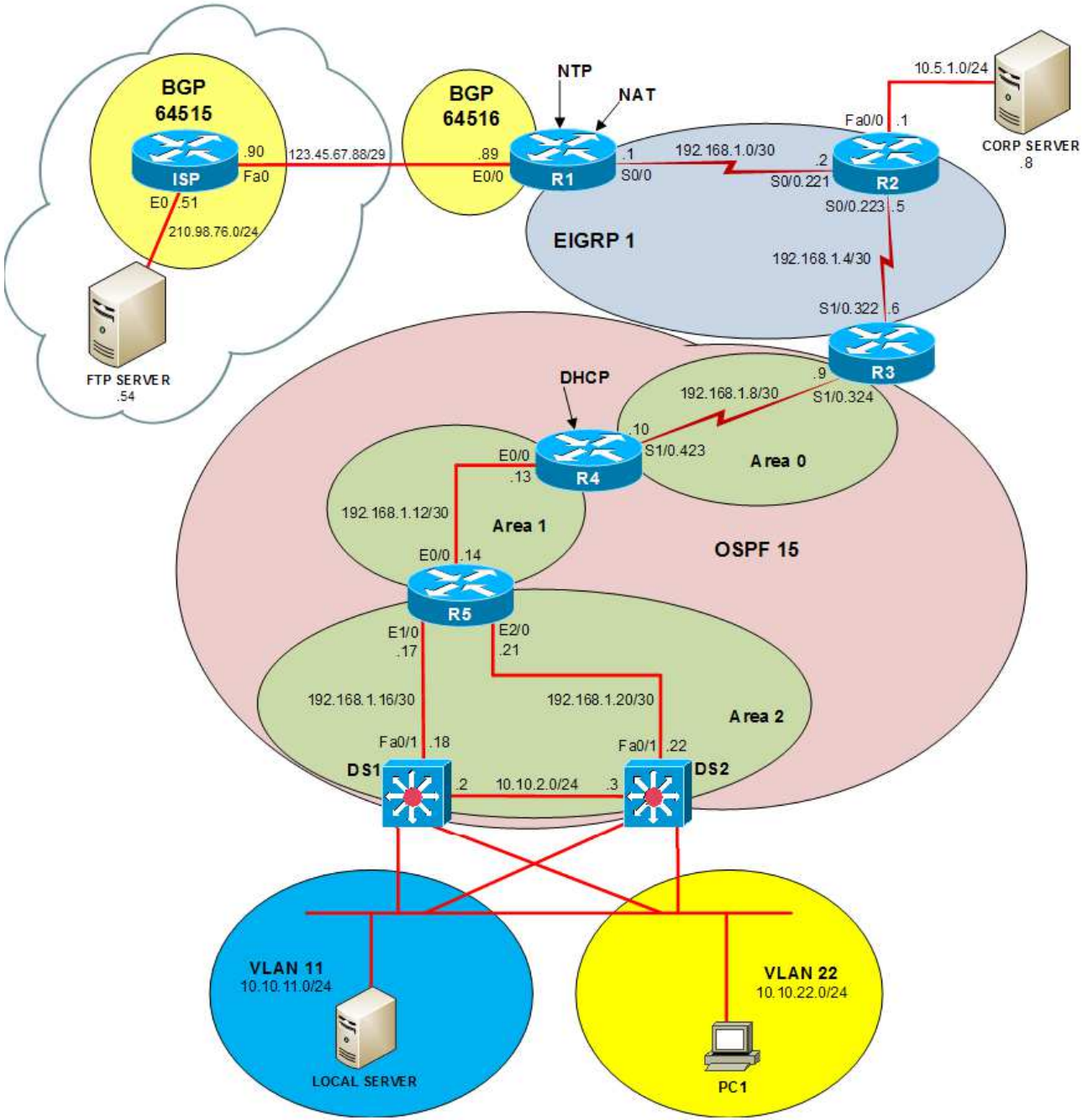
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

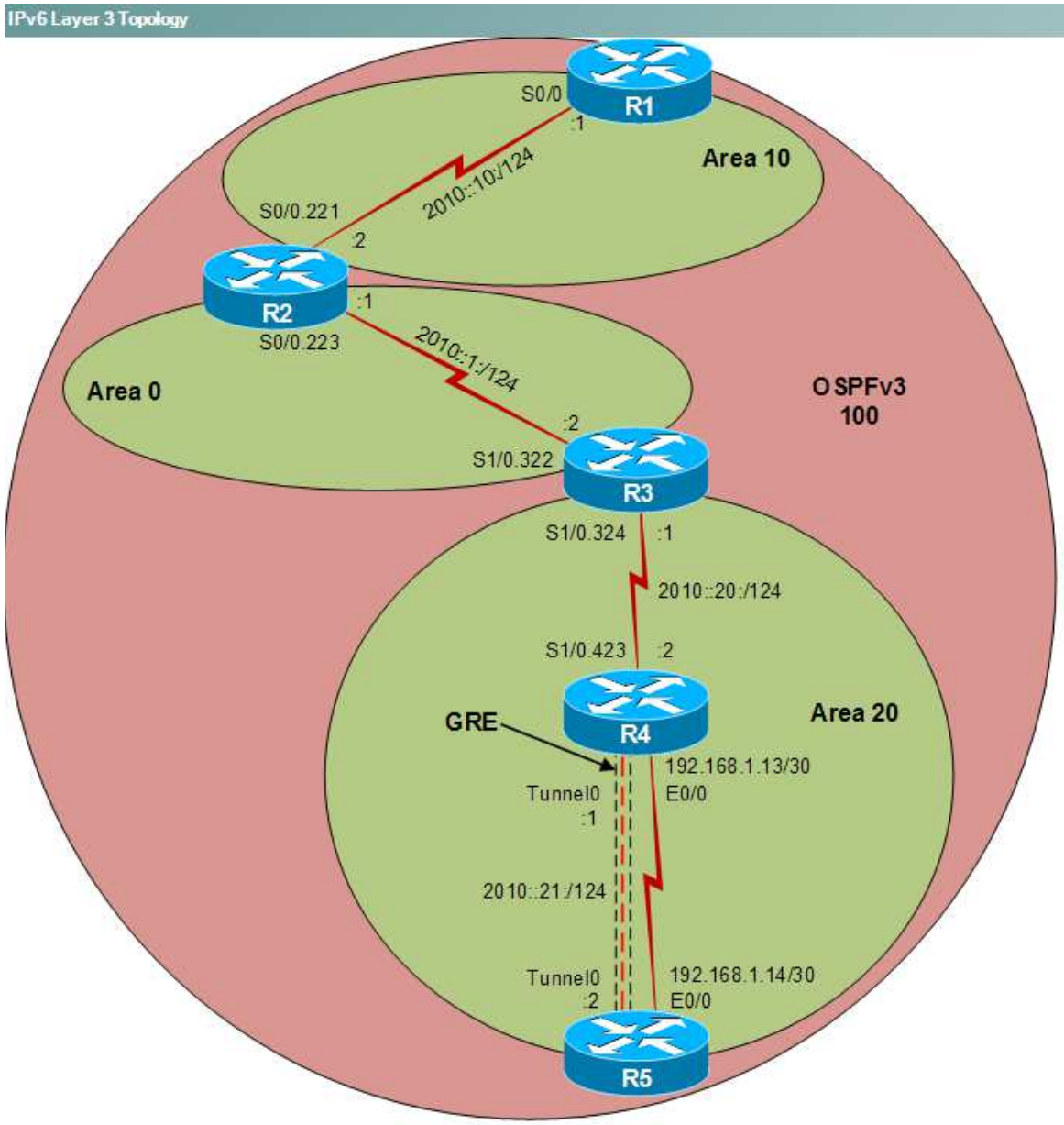
**Layer 2 Topology**




IPv4 layer 3 Topology

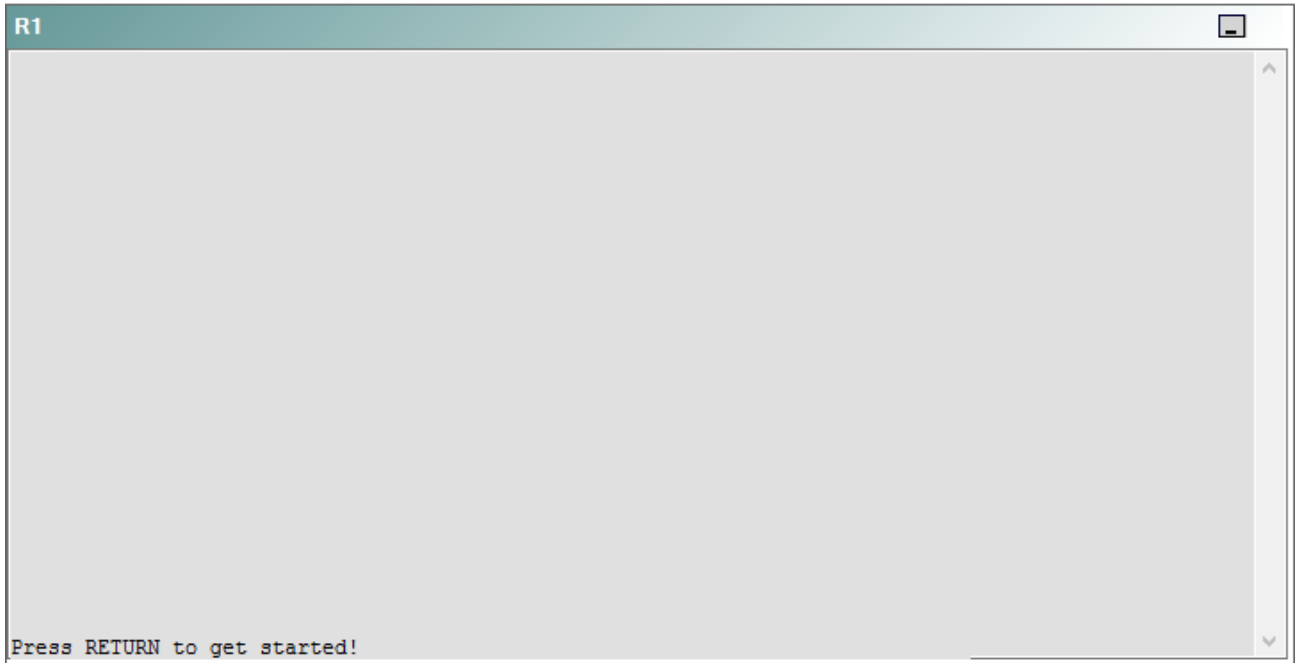

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

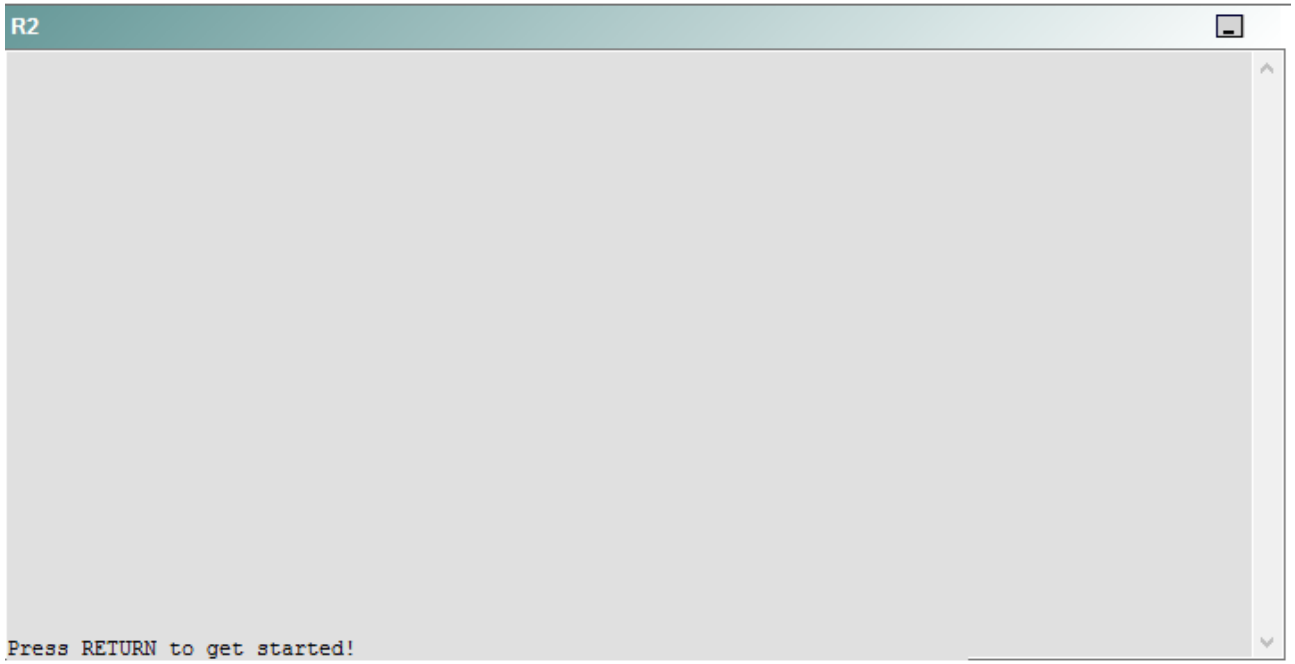



https://www.gratisexam.com/

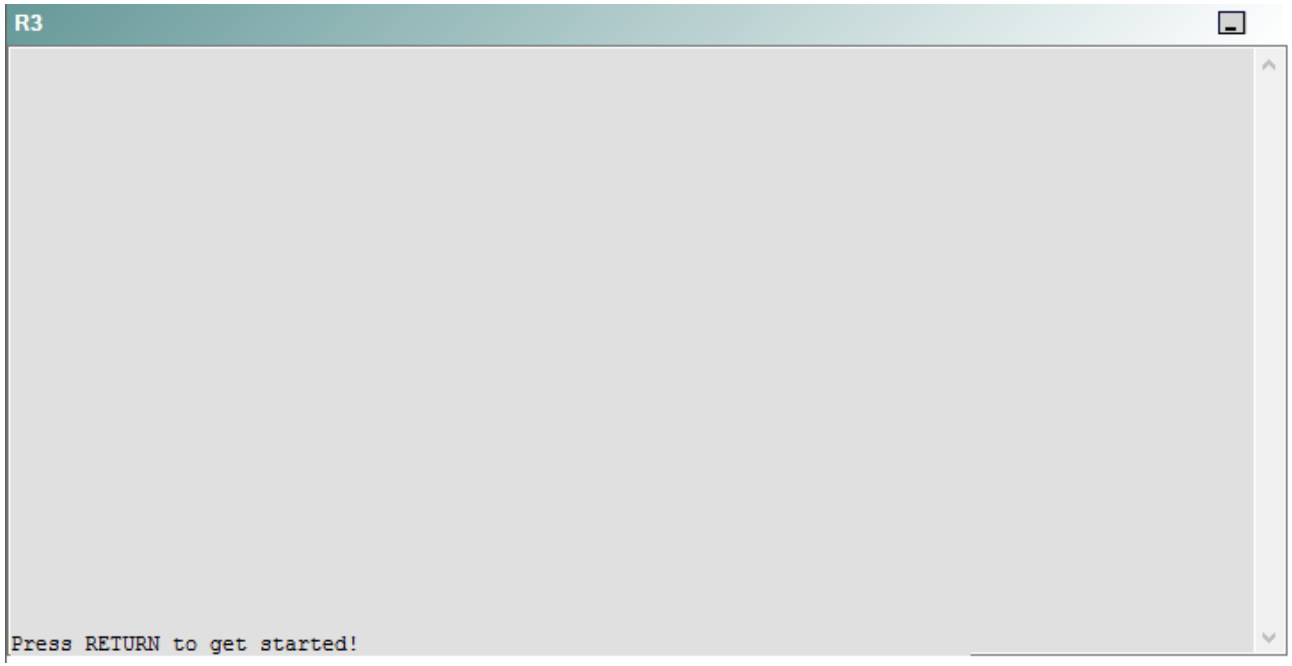
R1



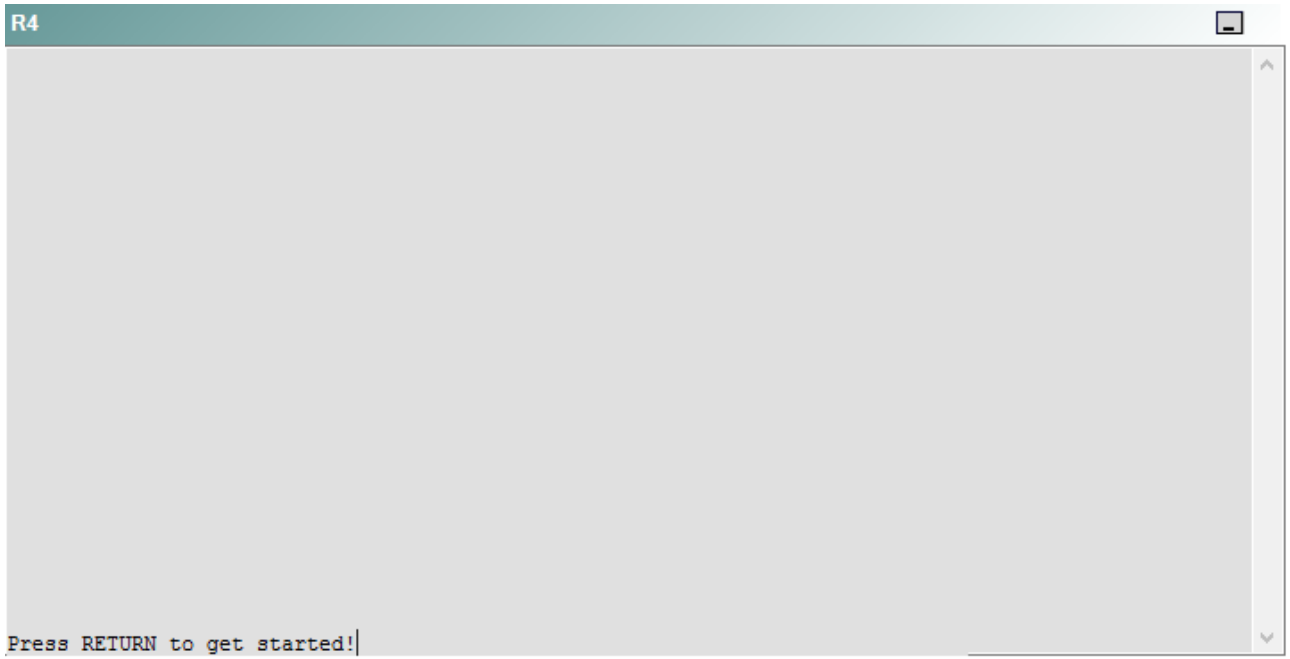

R2



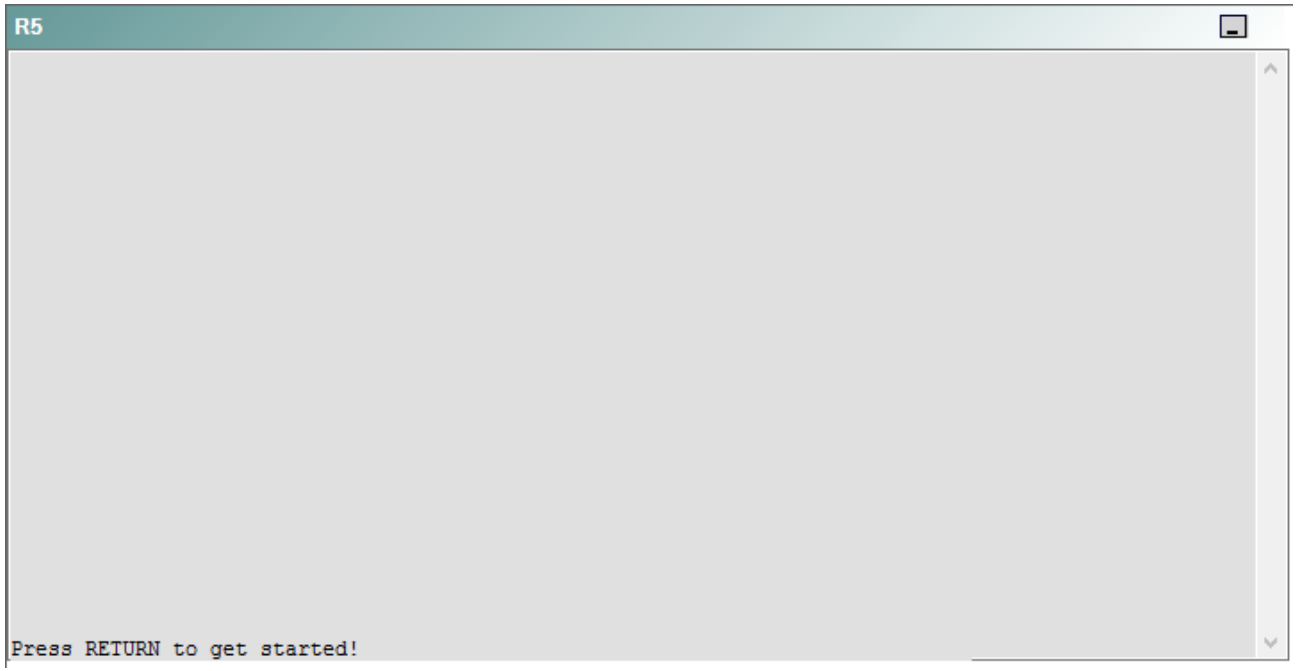

R3



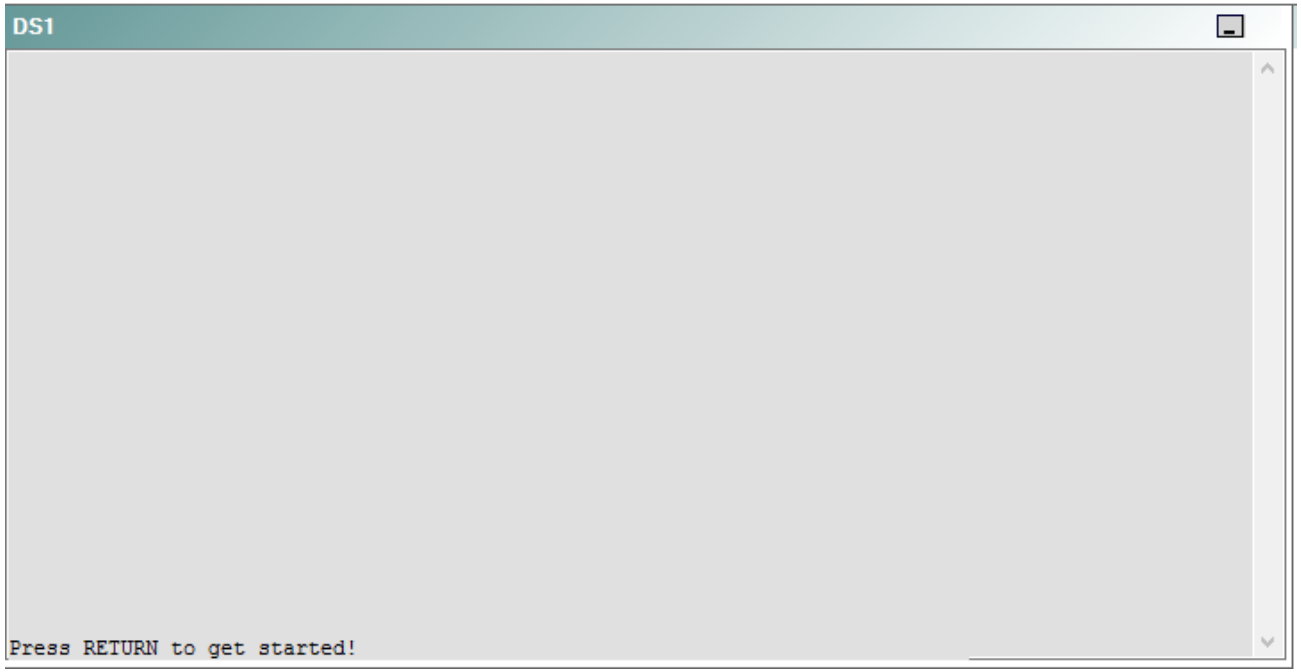

R4



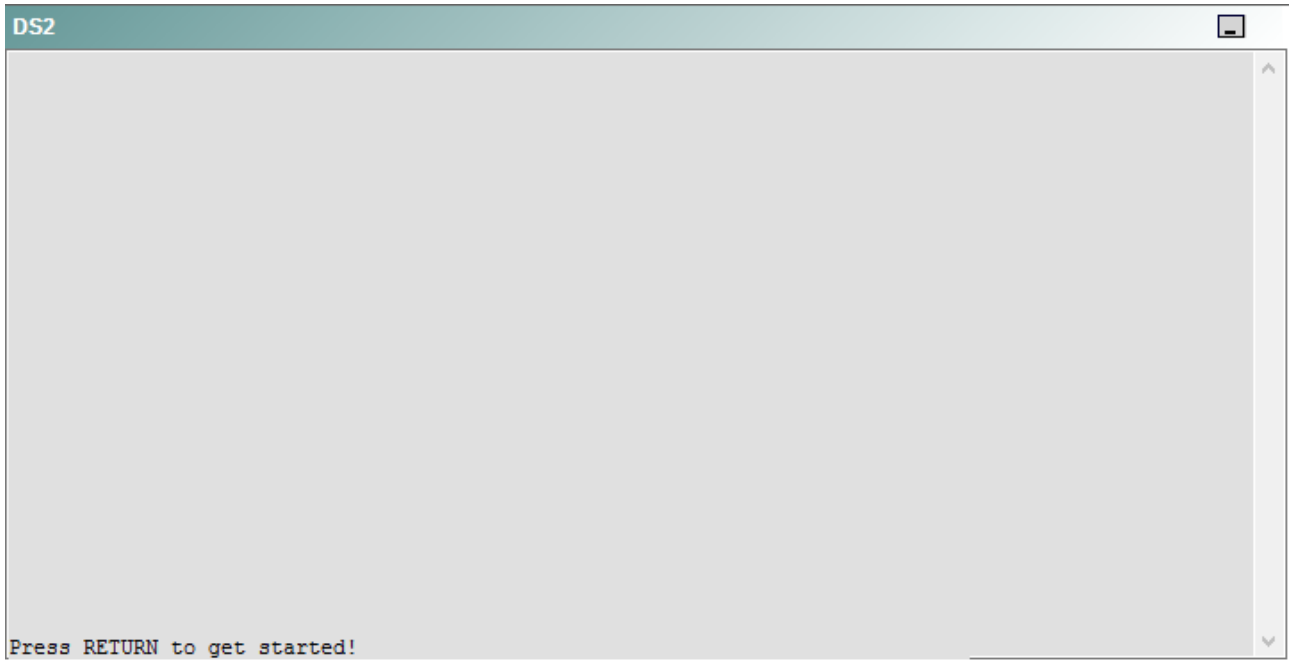

R5



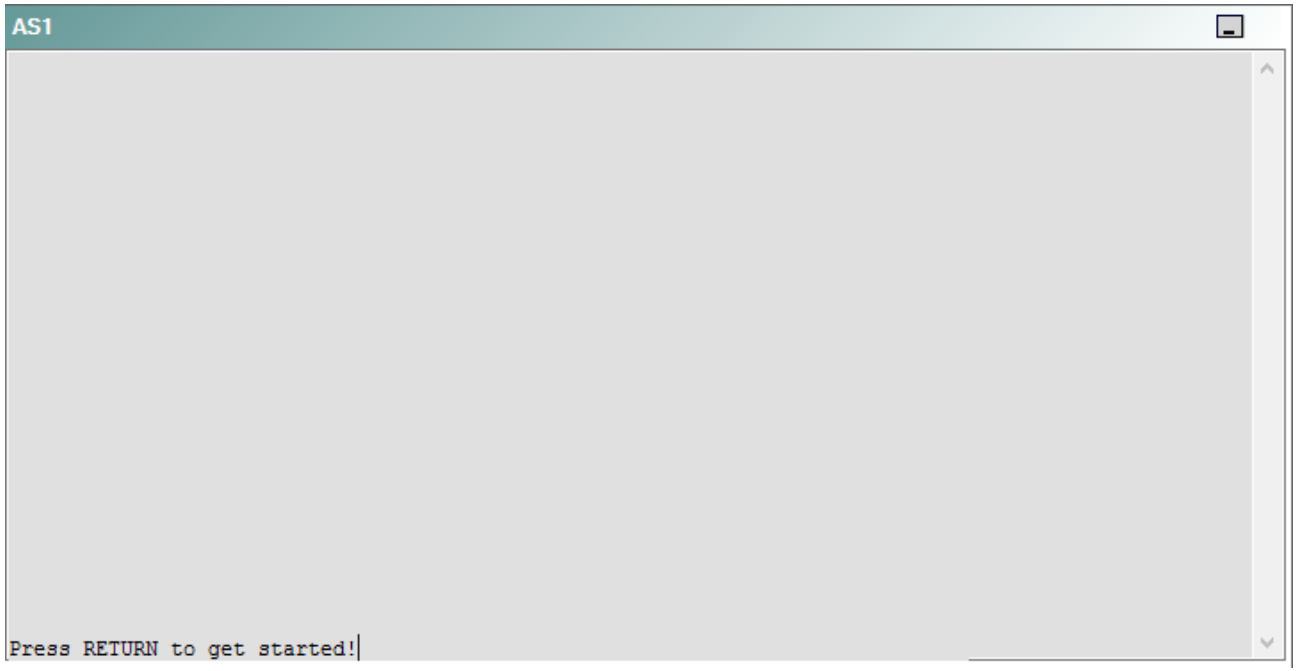

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. issuing the **network 192.168.1.4 0.0.0.3 area 0** command
B. issuing the **network 192.168.1.8 0.0.0.3 area 0** command
C. issuing the **area 2 virtual-link 192.168.99.5** command
D. enabling OSPF MD5 authentication on the S1.0.324 interface
E. changing the OSPF network type on the S1.0.324 interface
F. changing the OSPF area type
G. changing the masks on the OSPF **network** statement
H. issuing the **no ip ospf hello-interval** command on the S1.0.324 interface
I. changing the OSPF router ID

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

You should enable Open Shortest Path First version 2 (OSPFv2) Message Digest 5 (MD5) authentication on the S1/0.324 interface of R3. To determine which device is the source of the problem, you can issue the **ping and traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from PC1 to the farthest device and work your way back to PC1 until pings are successful.

Pings from PC1 to the S1/0.423 interface of R4 are successful. However, pings from PC1 to the S1/1.324 interface of R3 time out and fail. Pings from R1 to R3 are successful, but pings from R1 to R4 are not. Therefore, the problem likely exists on R3 or R4.

Once you have determined where connectivity is lost, you can begin to troubleshoot what is causing the problem. Issuing the **show running-config** command on R4 indicates that OSPF MD5 authentication is enabled on the S1/0.423 interface of R4, as shown in the following partial output:

```
interface Serial1/0.423 point-to-point
 description Link to R3
 ip address 192.168.1.10 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 boson
 frame-relay interface-dlci 423
```

However, OSPF MD5 authentication is not enabled on the S1/0.324 interface of R3. An OSPF adjacency will not be established unless neither side or both sides of the link are configured with authentication; if authentication is configured, then the authentication key must match.

OSPF authentication can be enabled for an interface or for an area. To configure OSPF MD5 authentication for an interface, you should issue the **ip osp authentication message-digest** command in interface configuration mode. To configure OSPF MD5 authentication for an entire area, you would issue the **area** *area-id* **authentication message-digest** command in router configuration mode. To configure the key that should be used for MD5 authentication, you should issue the **ip** ospf **message-digest-key** *key-id* **md5** *key* command in interface configuration mode.

You should not change the OSPF area type on any of the routers, because the area types already match between the devices. The following parameters must match for devices to establish on OSPF adjacency:

- Hello timer
- Dead timer
- Area number and type
- Network type
- Subnet
- Authentication type and password

In addition, OSPF cannot establish an adjacency over a secondary IP address.

You need not change the router ID on R3. As long as the router ID is unique, OSPF routers will from an adjacency. The first line in the output of the **show ip ospf** command displays the router ID. To change the router ID on a router, you would issue the **router-id** *A.B.C.D* command from OSPF router configuration mode, where *A.B.C.D* is a 32-bit router ID in dotted decimal notation.

You need not change the OSPF network type on any of the devices on the network. The OSPF network type must match so that connected interfaces can form an adjacency. The S1/0.324 interface on R3 and the S1/0.423 interface on R4 are both set to the point-to-point OSPF network type. You can determine the OSPF network type by issuing the **show ip ospf interface** command, as shown in the following partial output:

```
R4#show ip ospf interface
Serial1/0.423 is up, line protocol is up
  Internet Address 192.168.1.10/30, Area 0
  Process ID 15, Router ID 192.168.99.4, Network Type POINT_TO_POINT, Cost: 781
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:08
```

To change the OSPF network type for an interface, you would issue the **ip ospf network {broadcast | non-broadcast | point-to-multipoint | point-to-point}** command from interface configuration mode.

You need not issue the **no ip ospf hello-interval** command on any of the devices on the network, because they are all using the default hello timer settings. By default, the hello timer is set to 10 seconds on point-to-point and broadcast links and 30 seconds on nonbroadcast multiaccess (NBMA) links. You can verify the hello timer settings by issuing the **show ip ospf interface** command.

You need not to issue the **network 192.168.1.4  0.0.0.3 area 0** command or the **network 192.168.1.8  0.0.0.3 area 0** command on R3, because these commands have already been issued. Additionally, you should not change the masks on the **network** statements, because the **network** command uses wildcard masks, not subnet masks. A wildcard mask is basically an inverse subnet mask. To calculate the appropriate wildcard mask, you should subtract the subnet mask from 255.255.255.255. For example, the 192.168.1.8 network has a /30 subnet mask, which is 255.255.255.252. Subtracting 255.255.255.252 from 255.255.255.255 yields a wildcard mask of 0.0.0.3.

You need not change the OSPF routing process on R5 to 15, nor do you need to change the OSPF routing process on the other devices to 10. The OSPF routing process number is locally significant, so two OSPF routers with different routing process numbers can still form an adjacency.

All areas in an OSPF internetwork must be connected to the backbone area, Area 0. A virtual link must be created between two area border routers (ABRs) to connect a remote area to the backbone area through a transit area. Only the ABRs that connect to the transit area must be configured with a virtual link; therefore, you should not issue the **area 1 virtual-link 192.168.1.13** command or the **area 2 virtual-link 192.168.99.4** command on DS2.

R4 and R5 are already configured with the proper **area virtual-link** commands. The syntax of the **area virtual-link** command is area *area-id* **virtual-link** *router-id*, where *area-id* is the transit area ID and *router-id* of the router at the other end of the virtual link. You should not issue the **area 2 virtual-link 192.168.99.5** command on R4 or the **area 2 virtual-link 192.168.99.4** command on R5, because Area 1, not Area 2, is the transit area. You should not issue the **area 1 virtual-link 192.168.1.14** command on R4 or the **area 1 virtual-link 192.168.1.13** command on R5, because you should use the router ID of the router at the other end of the virtual link for the *router-id* parameter; you should not use the router's interface IP address. You should not issue the **area 2 virtual-link 192.168.99.5** command on R3, because R3 is not connected to the transit area.

**Reference:**
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13697-25.html
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13699-29.html#seventh
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/47866-ospfdb7.html

**QUESTION 3**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

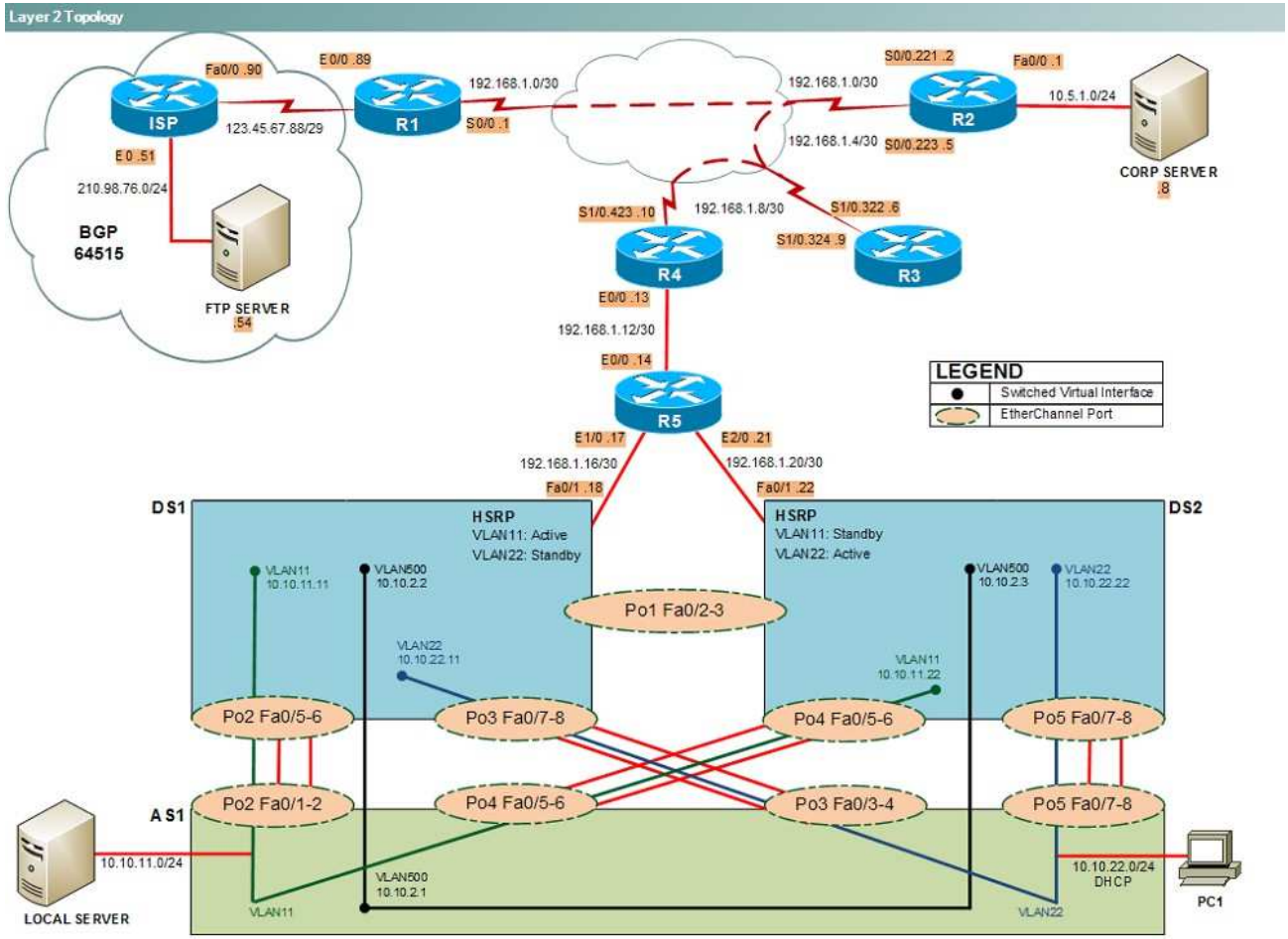
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

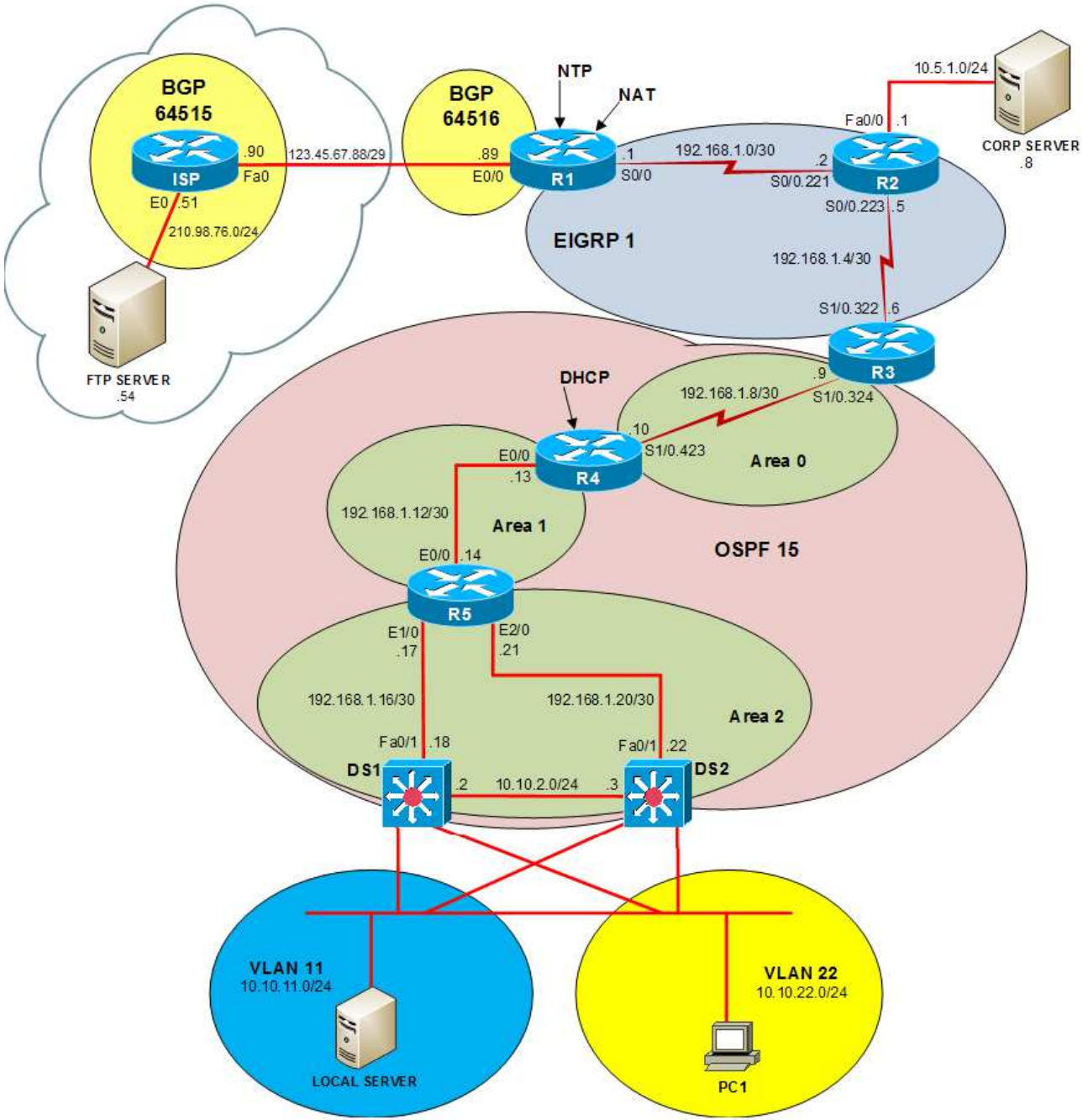
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

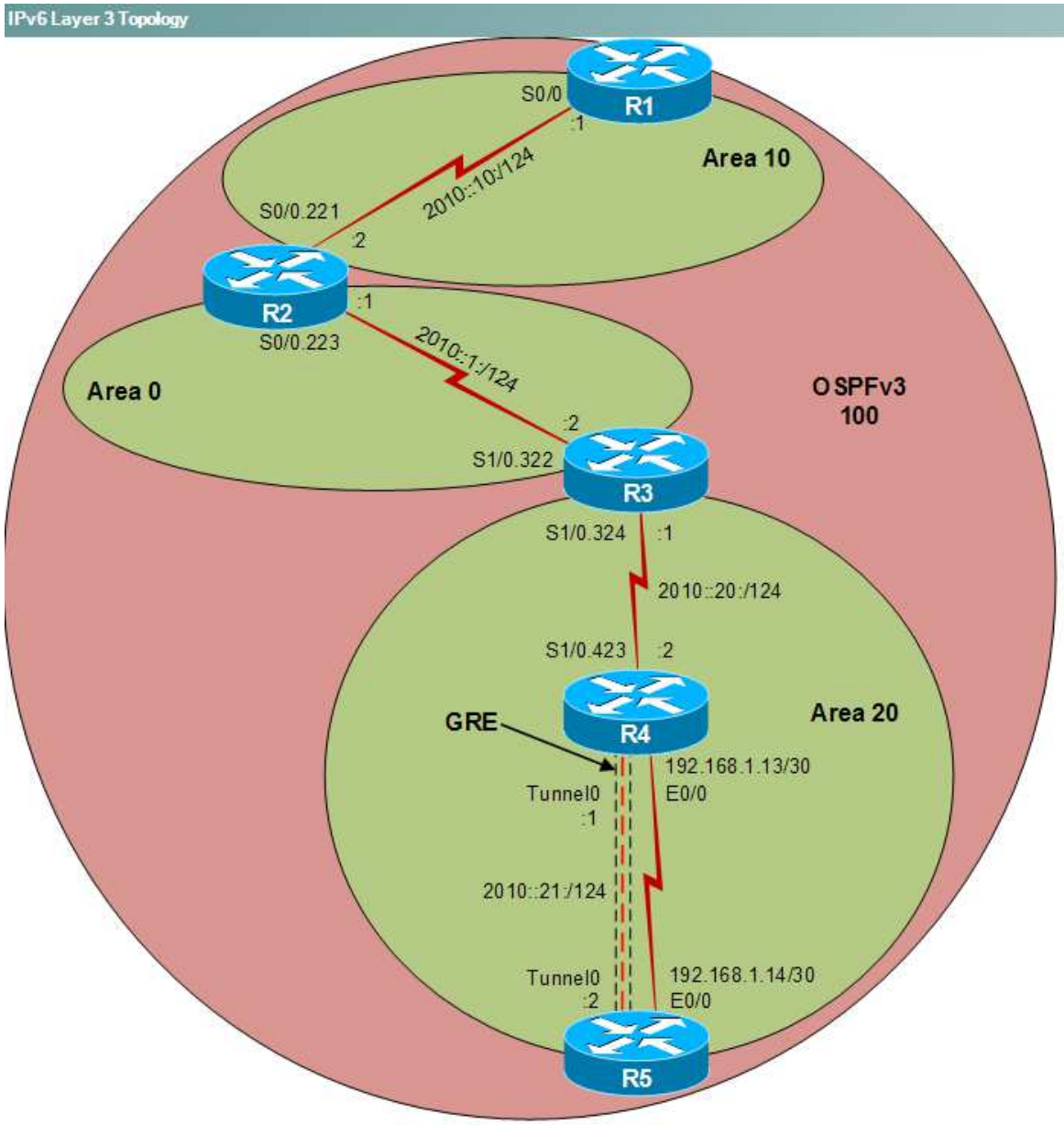
**Layer 2 Topology**




IPv4 layer 3 Topology

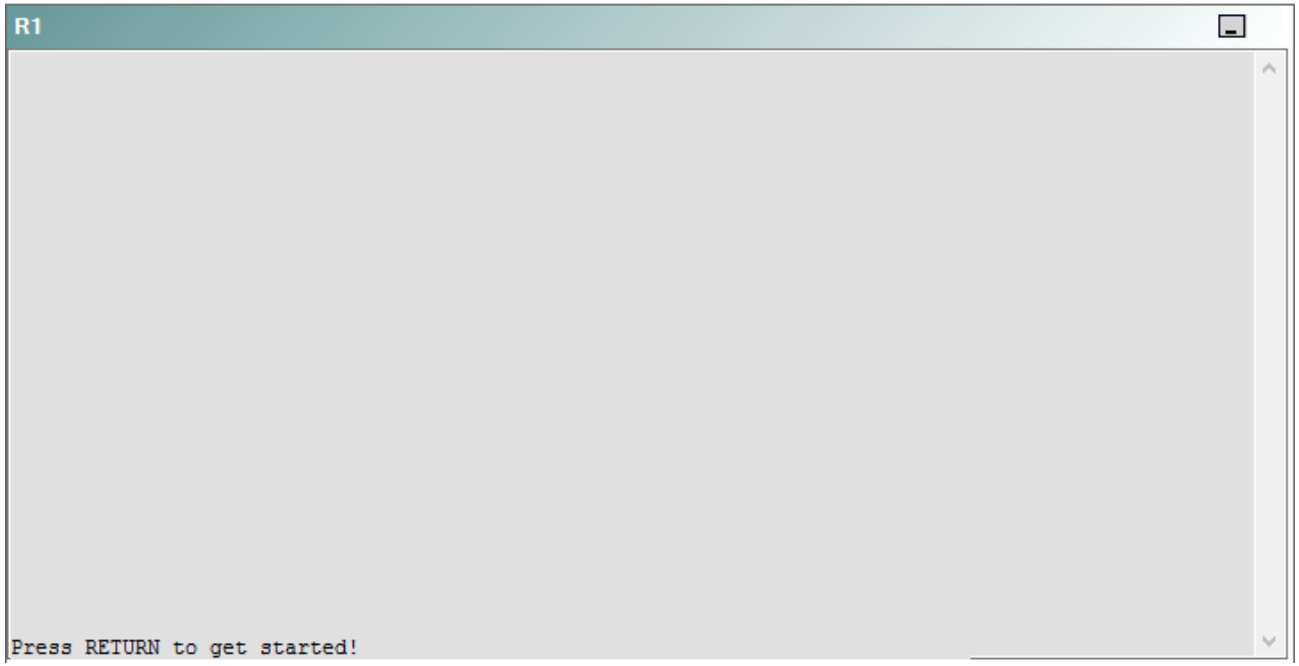

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

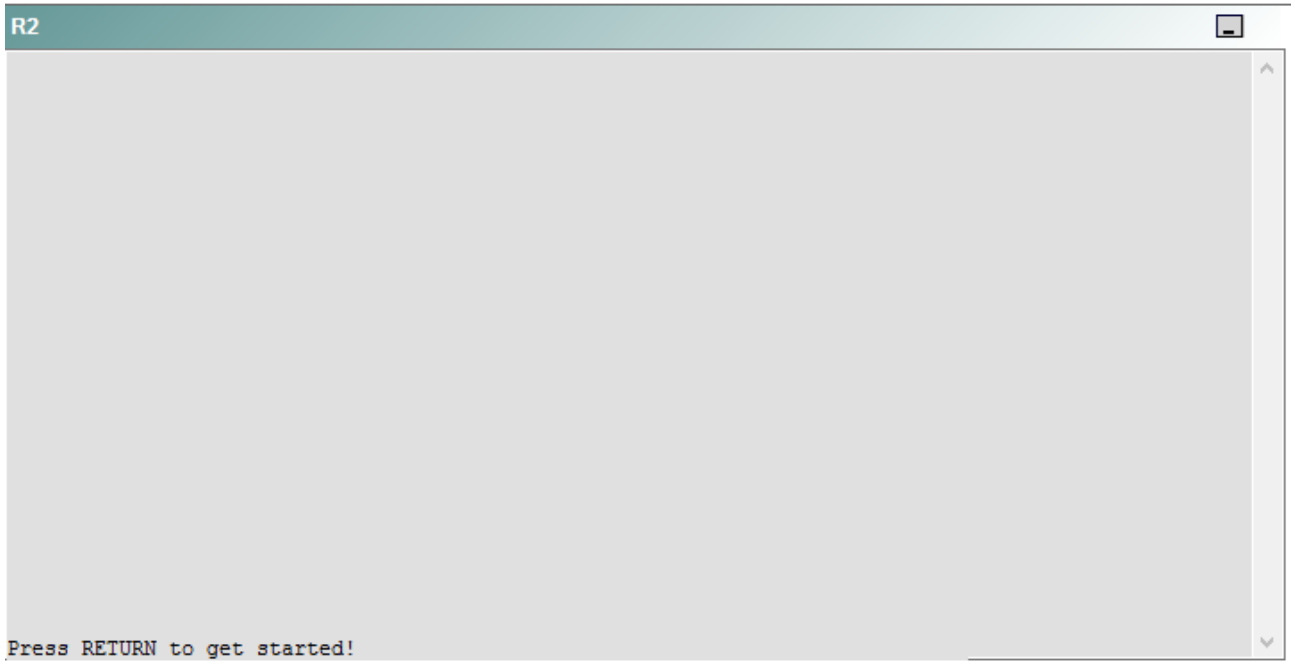



https://www.gratisexam.com/

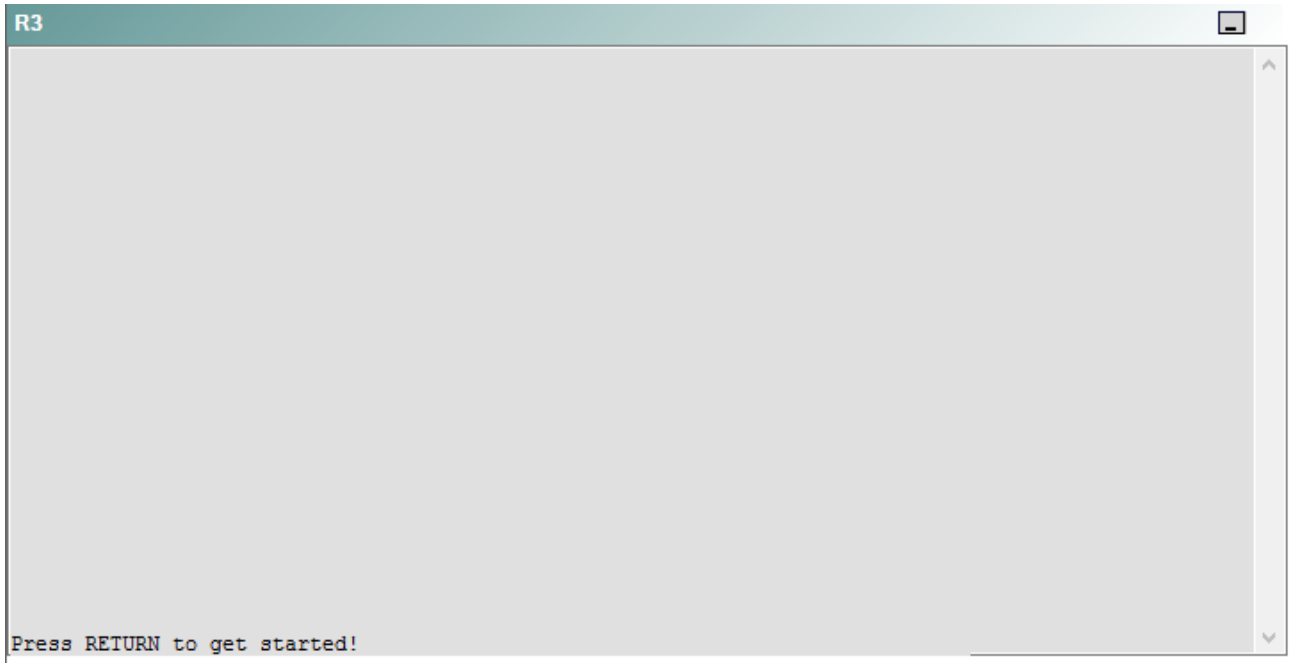
R1



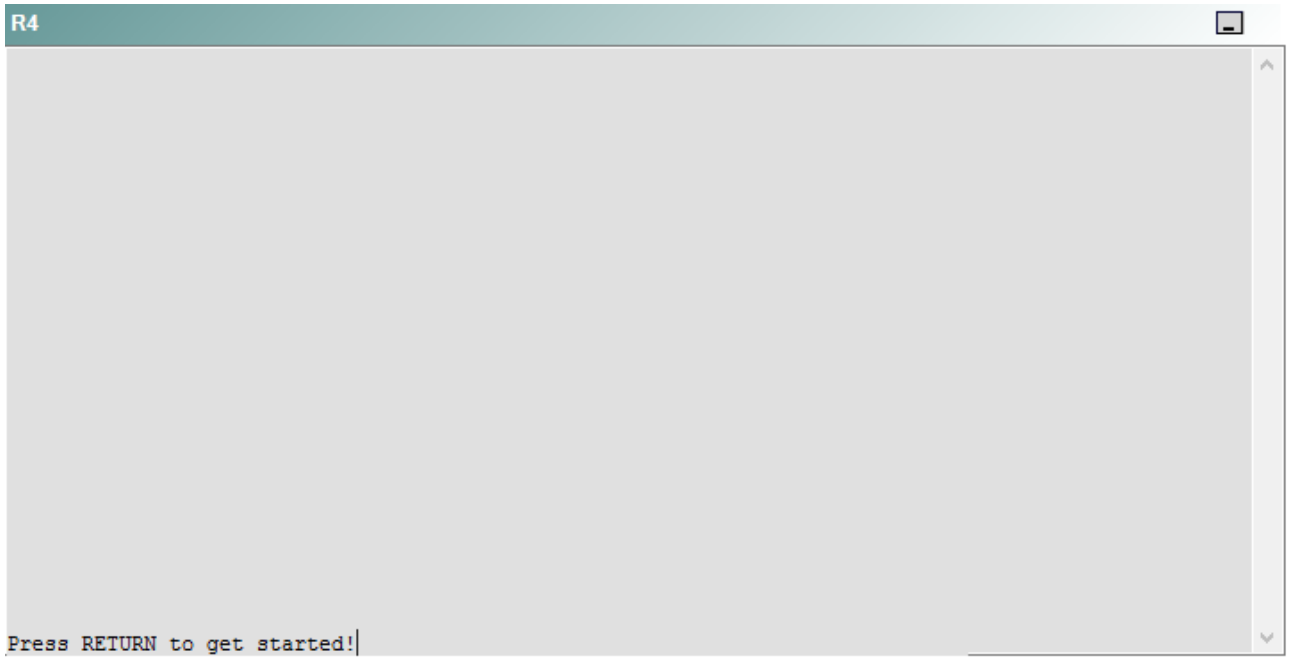

R2



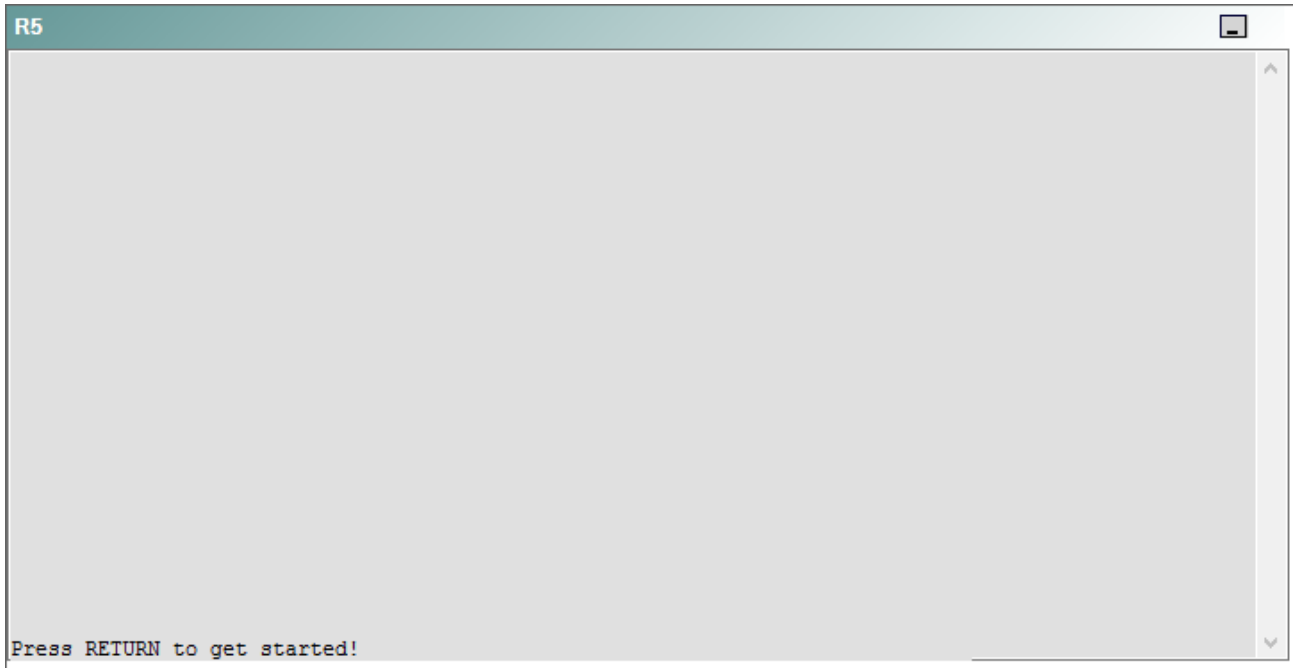

R3



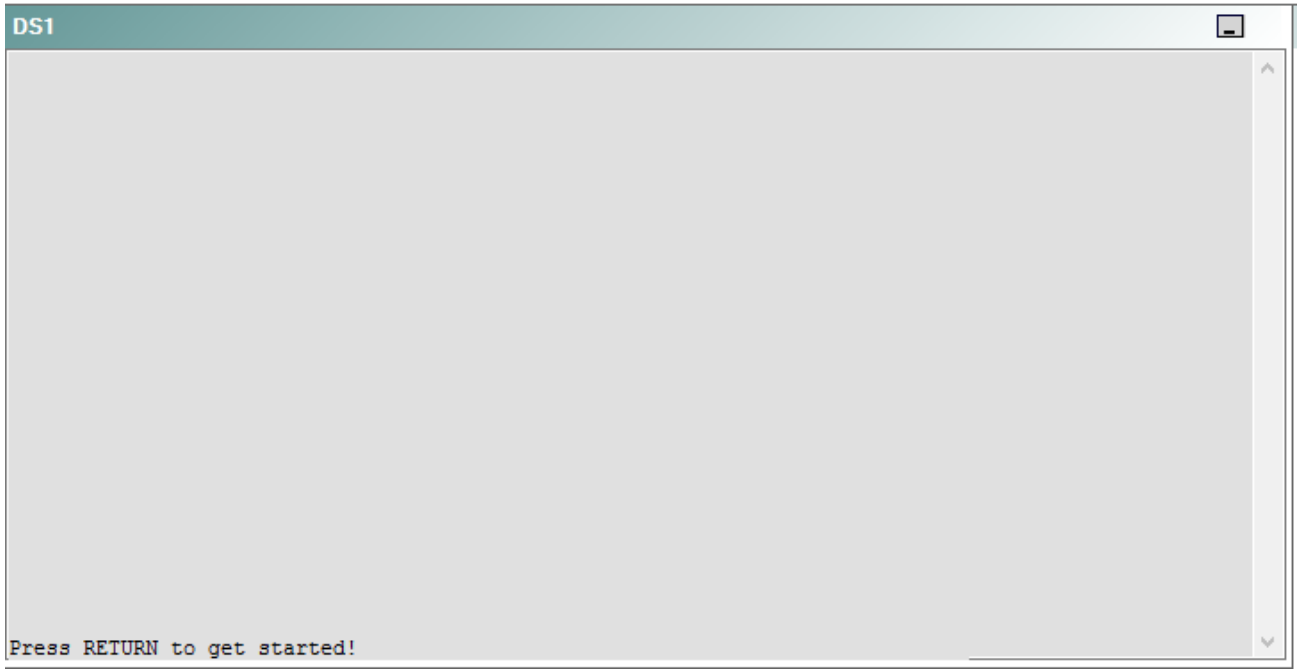

R4



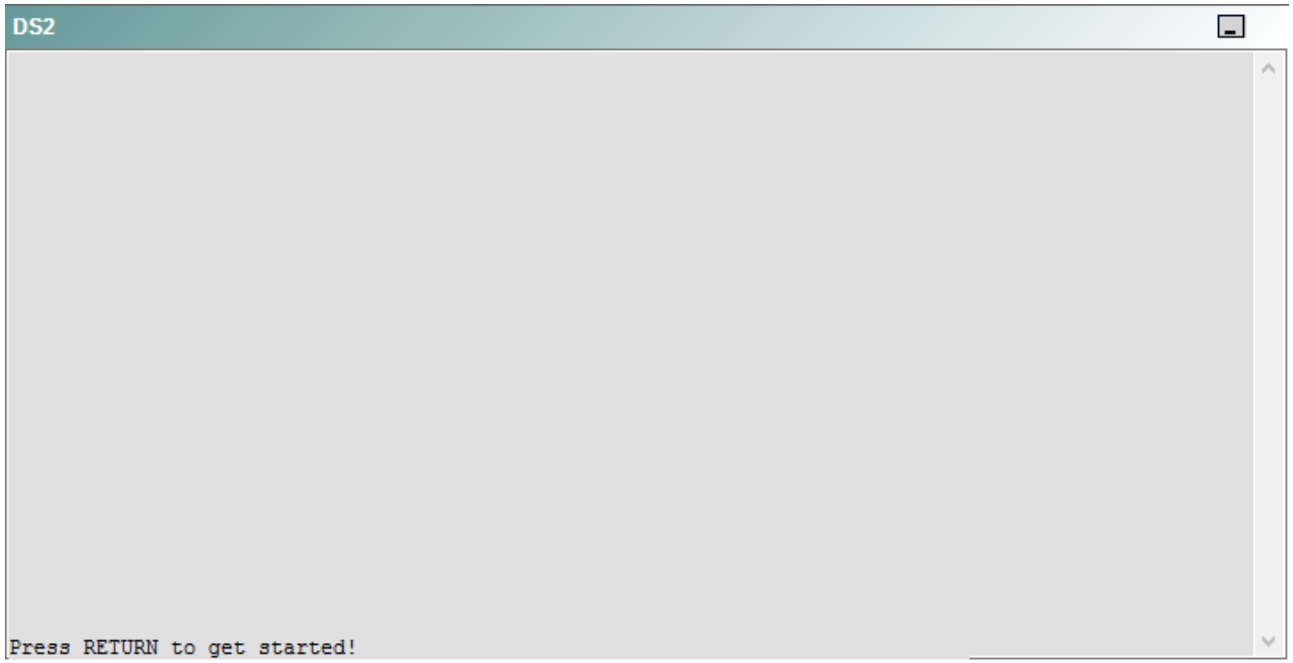

R5



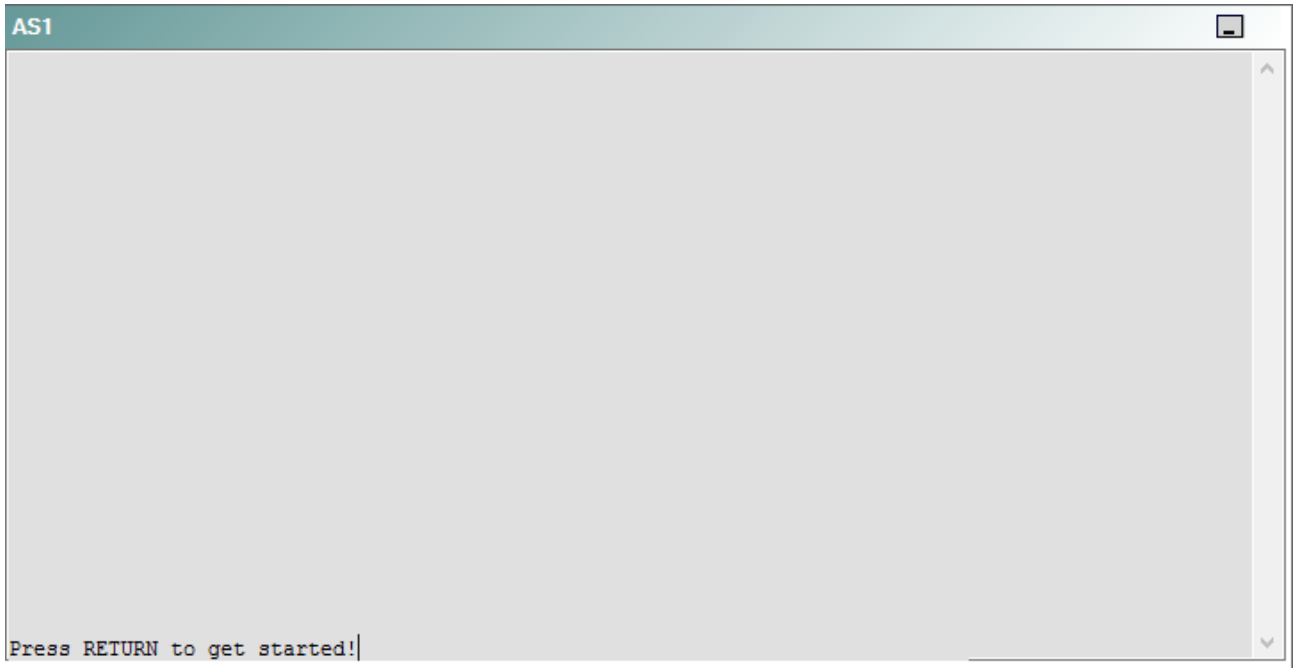

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 4**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

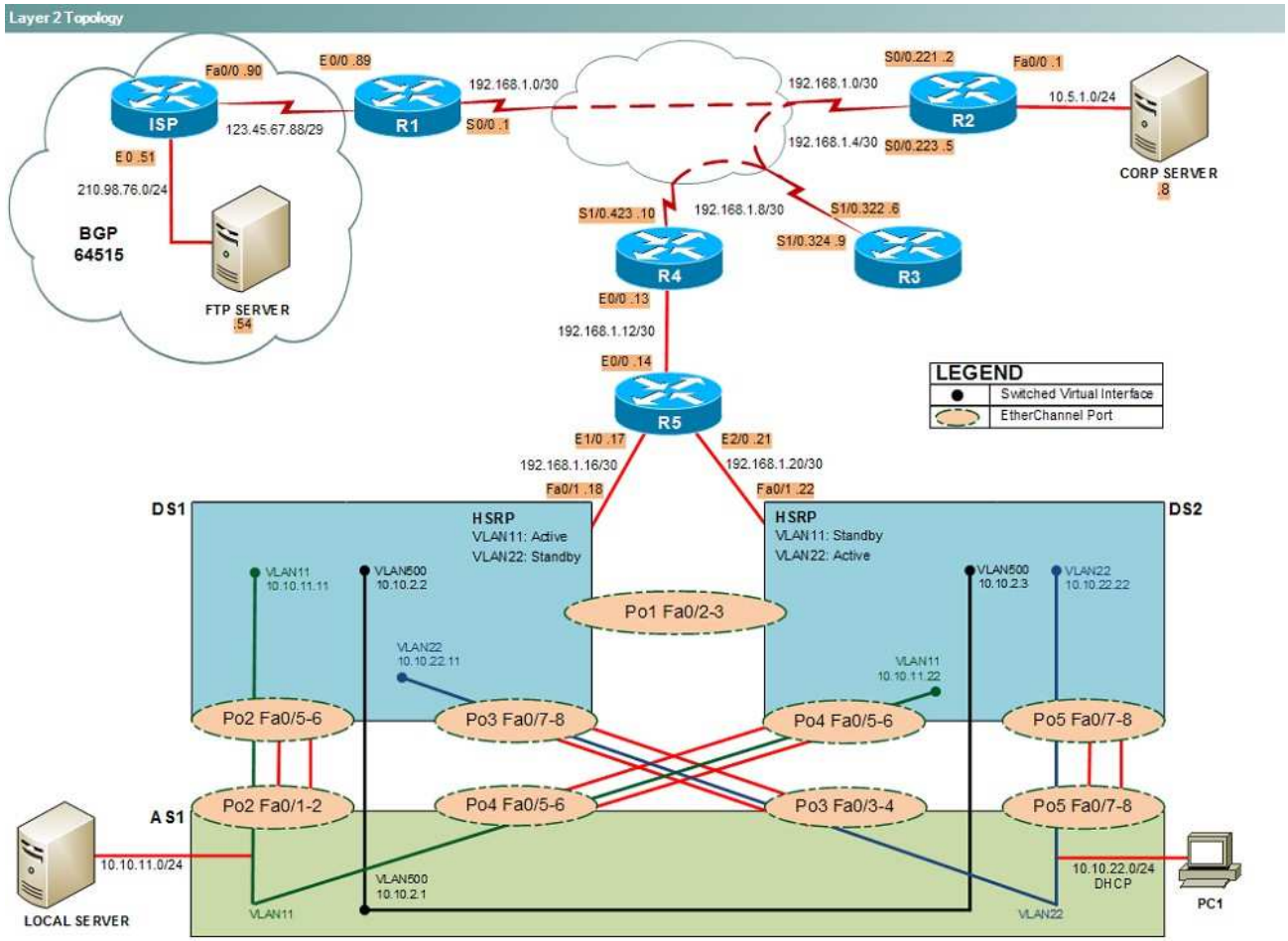
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

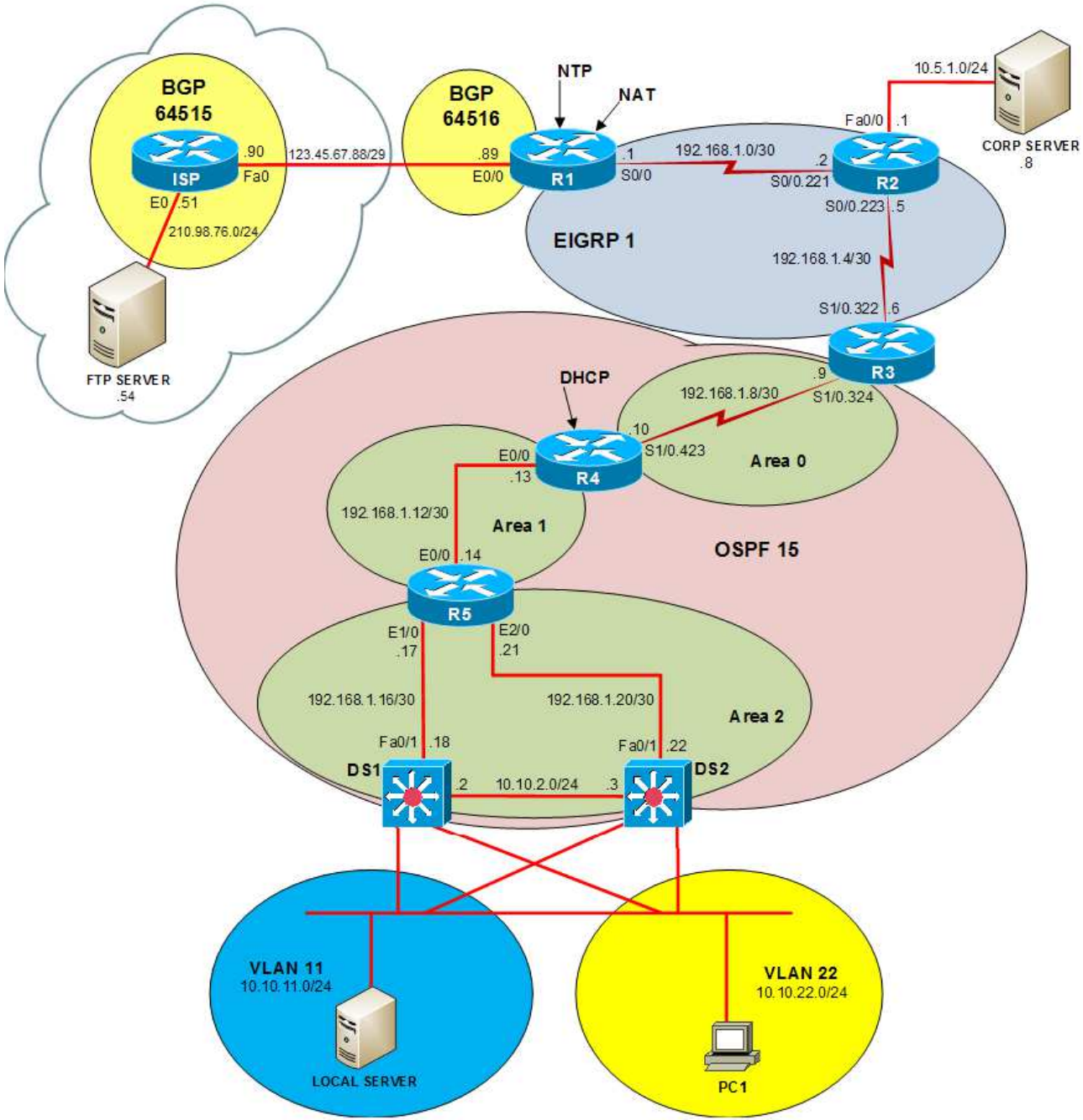
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

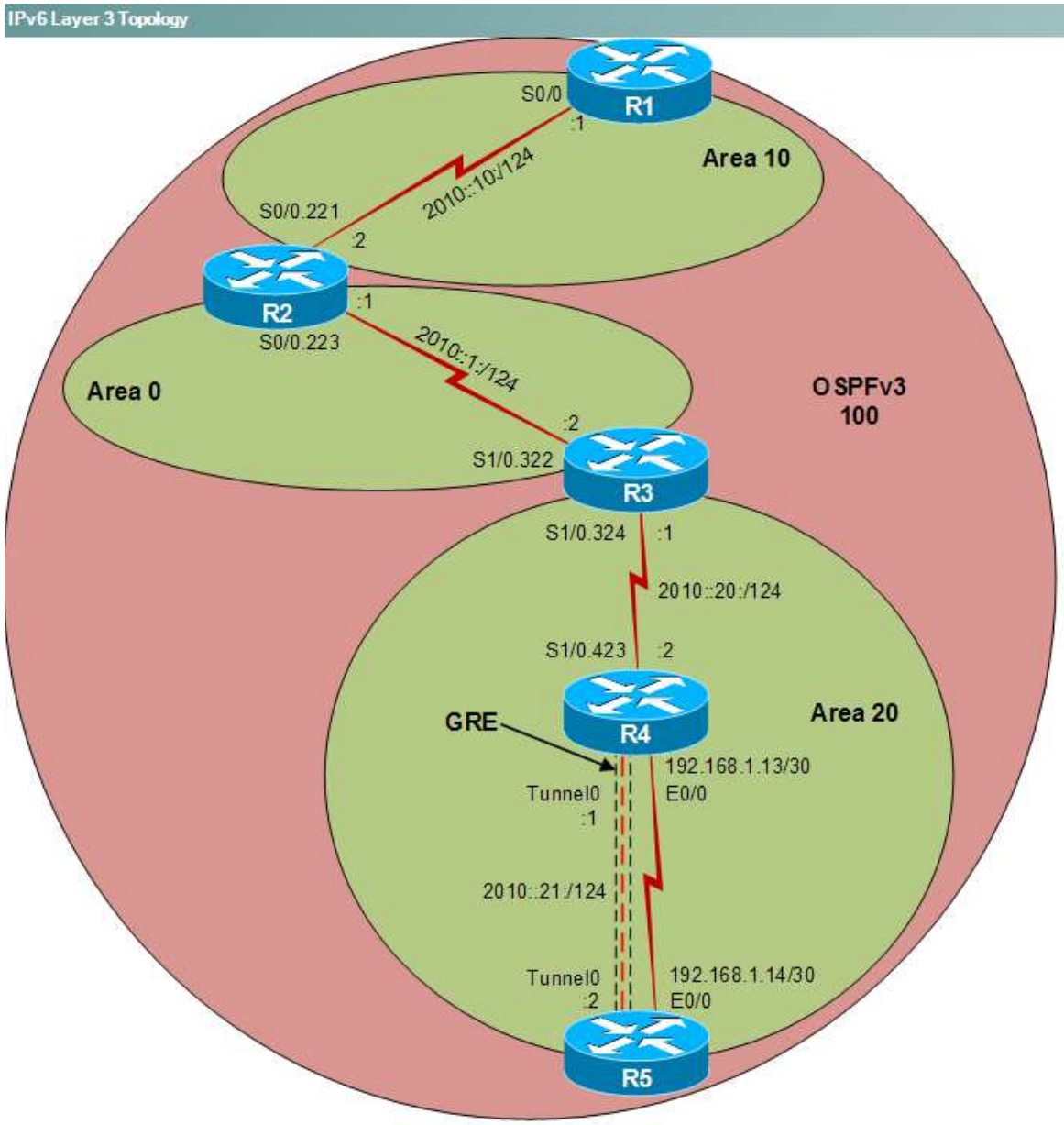
**Layer 2 Topology**




IPv4 layer 3 Topology

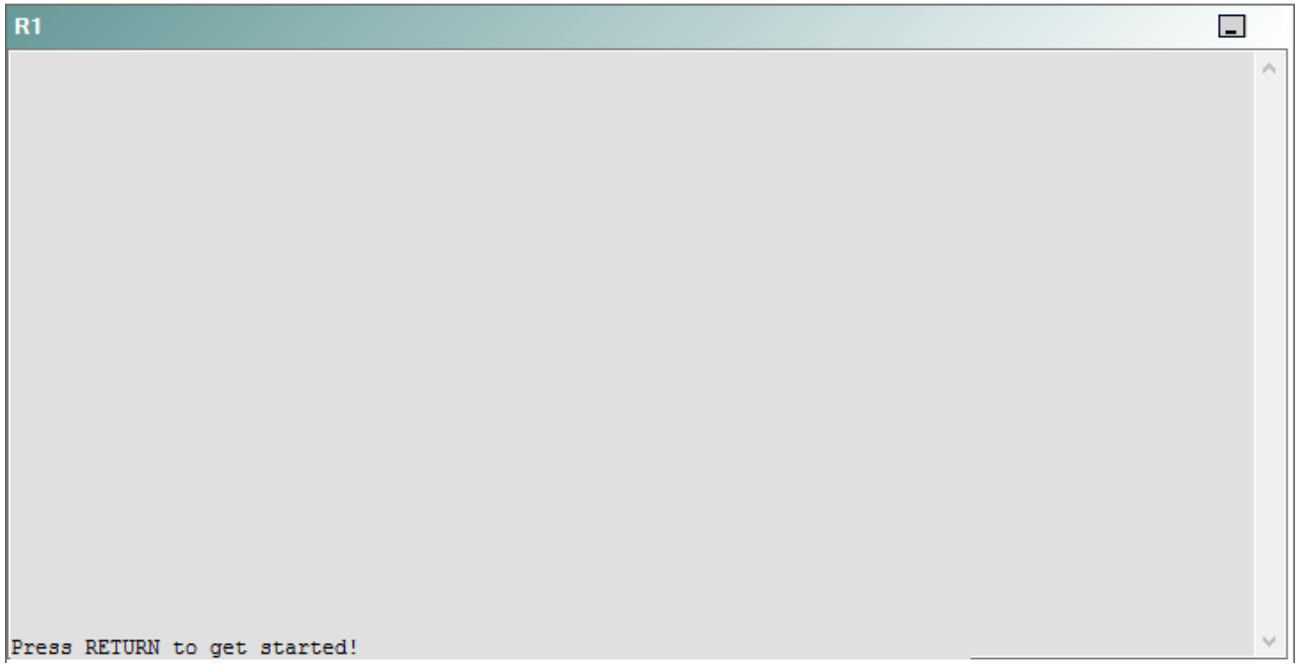

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

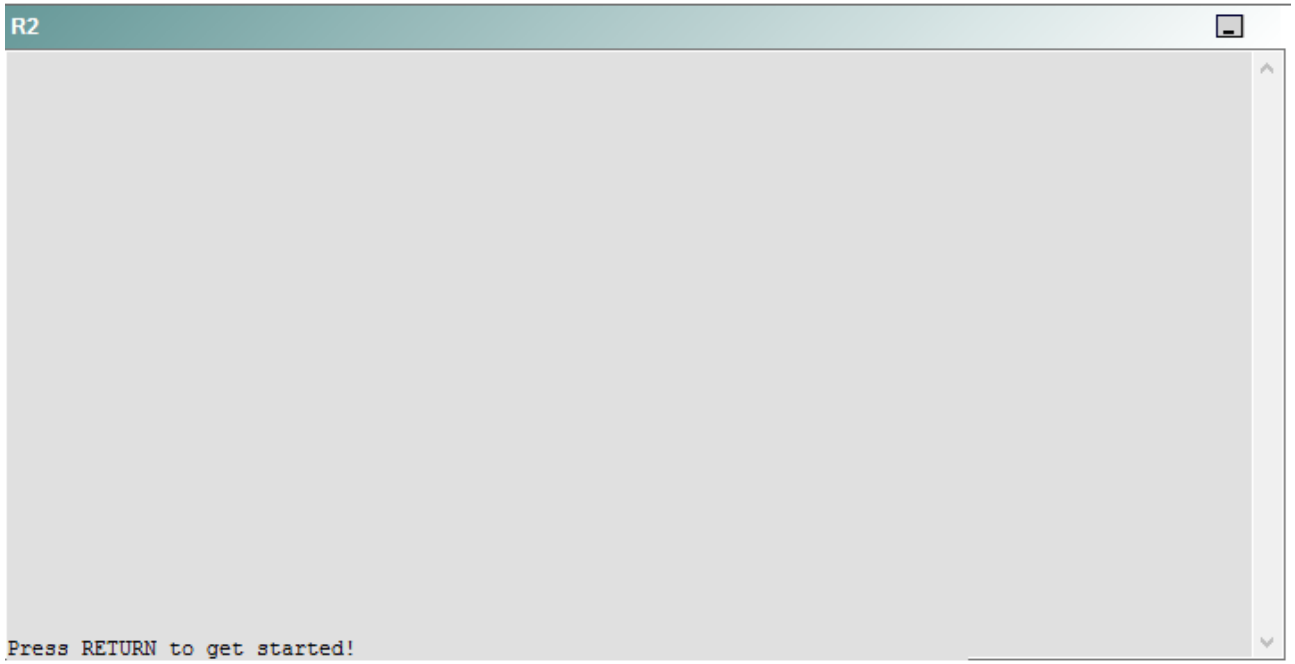



https://www.gratisexam.com/

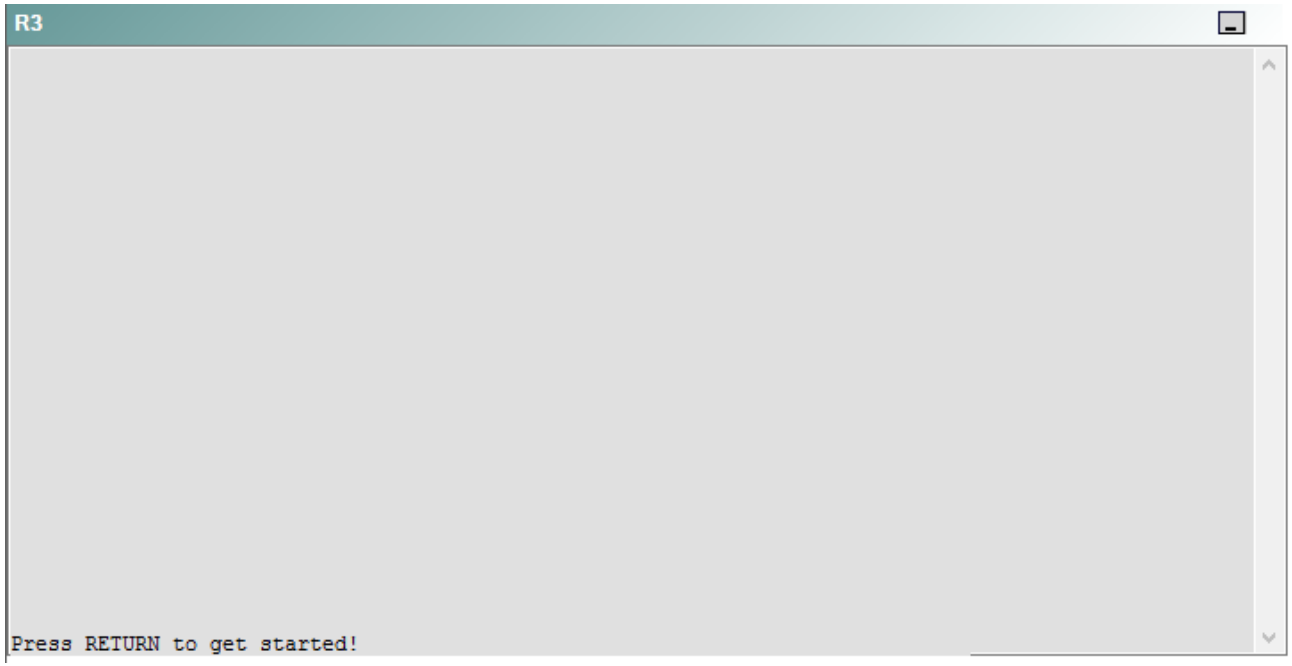
R1



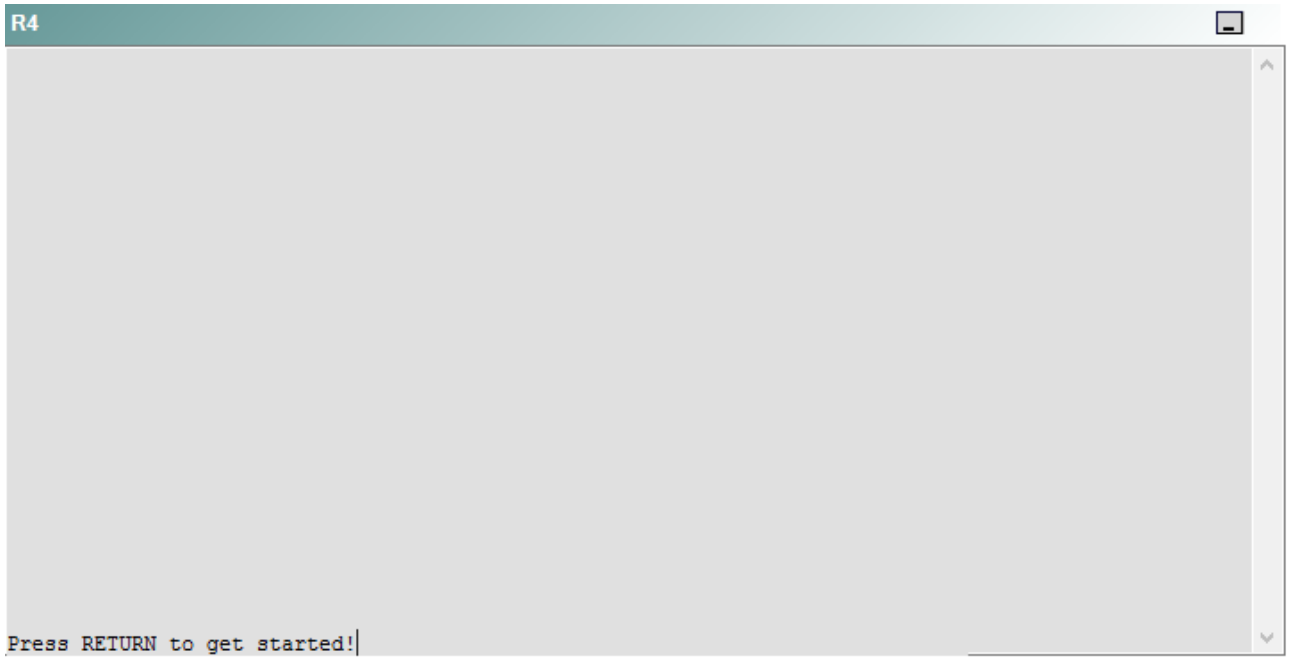

R2



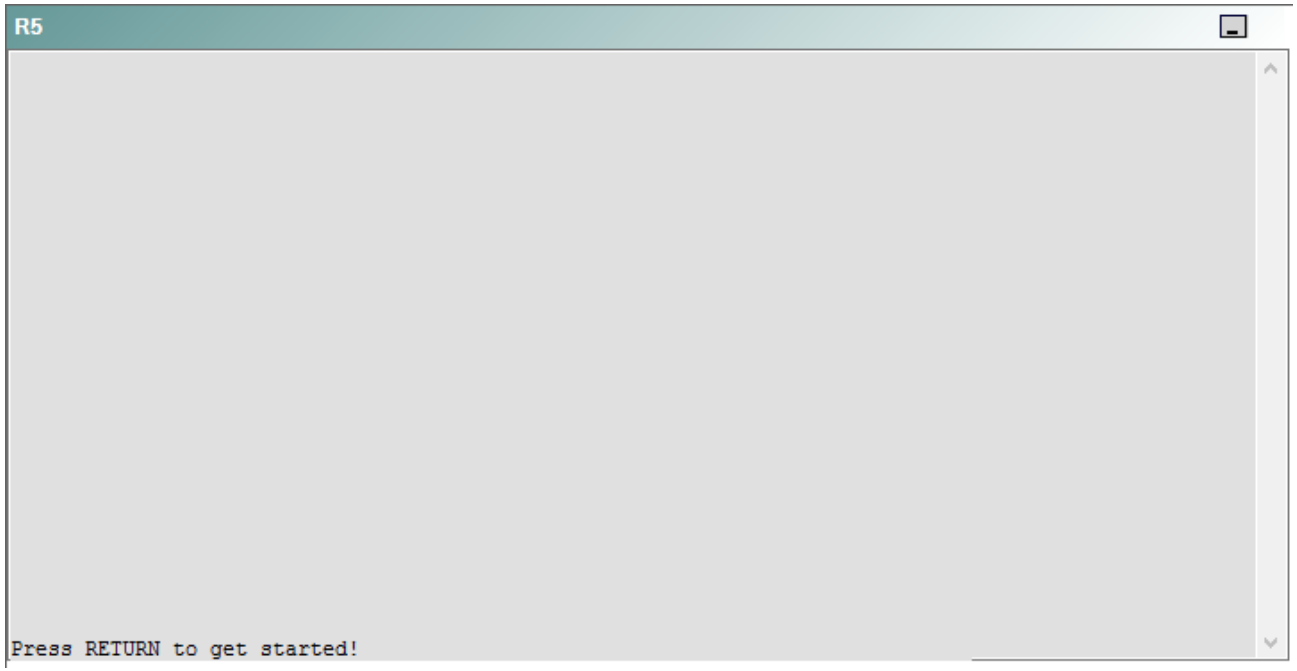

R3



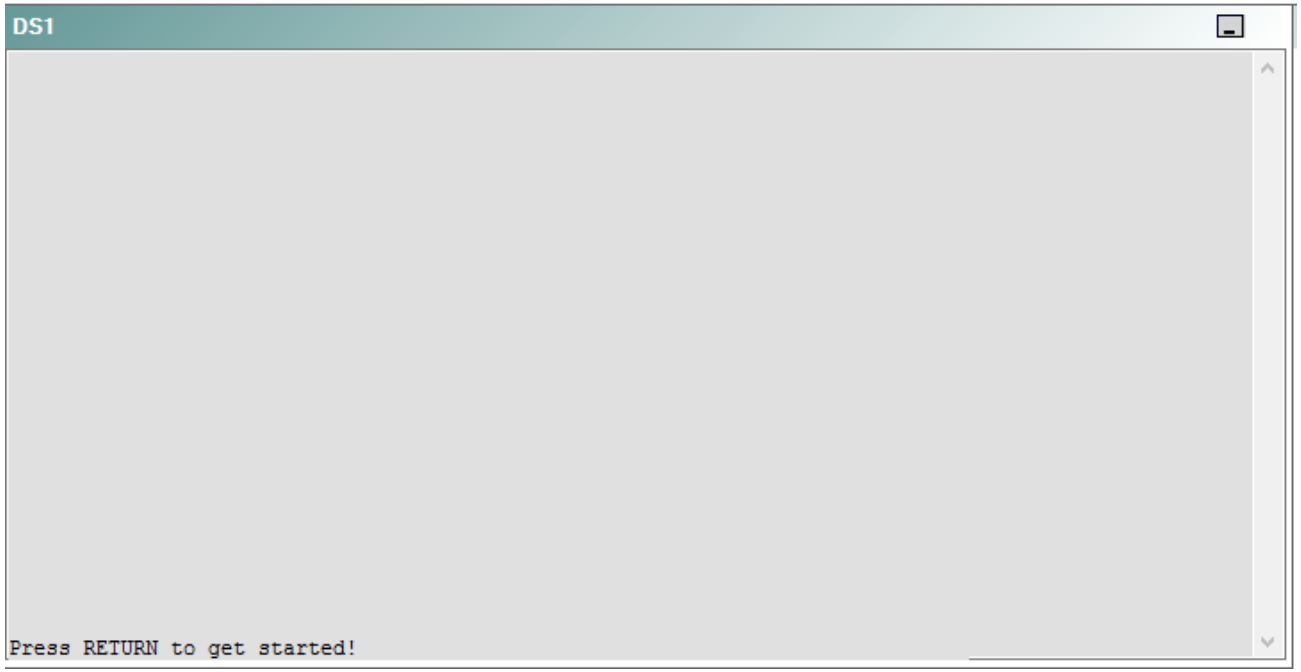

R4



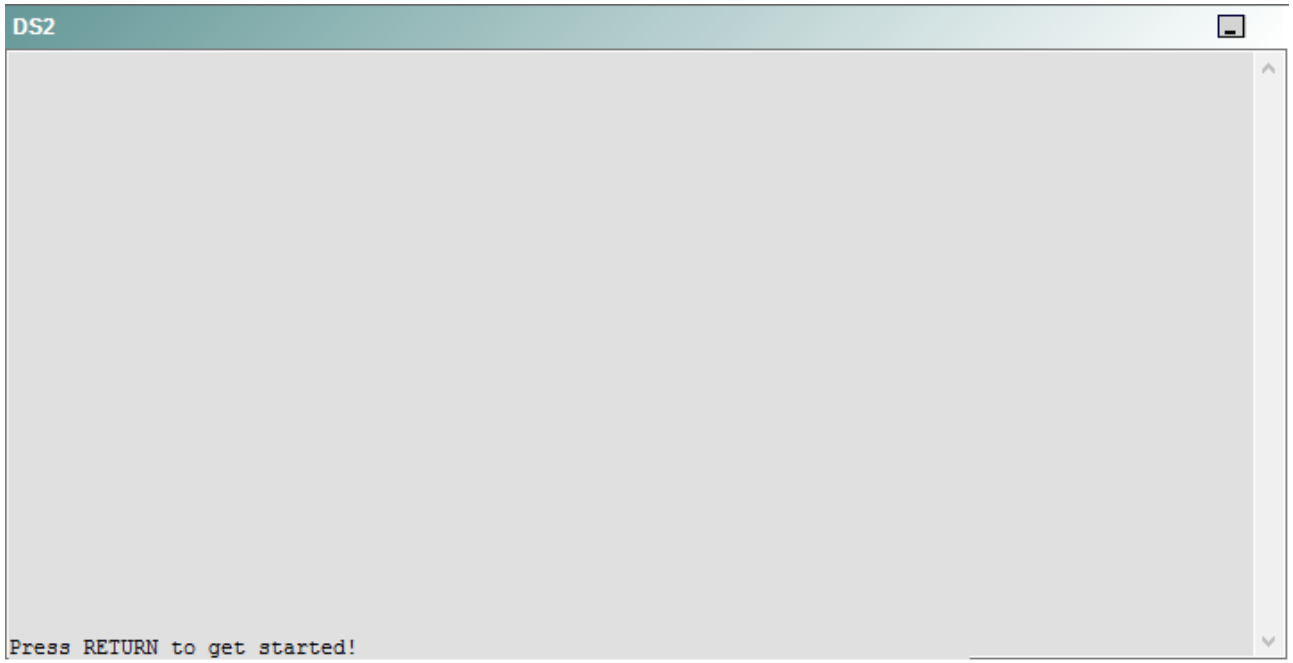

R5



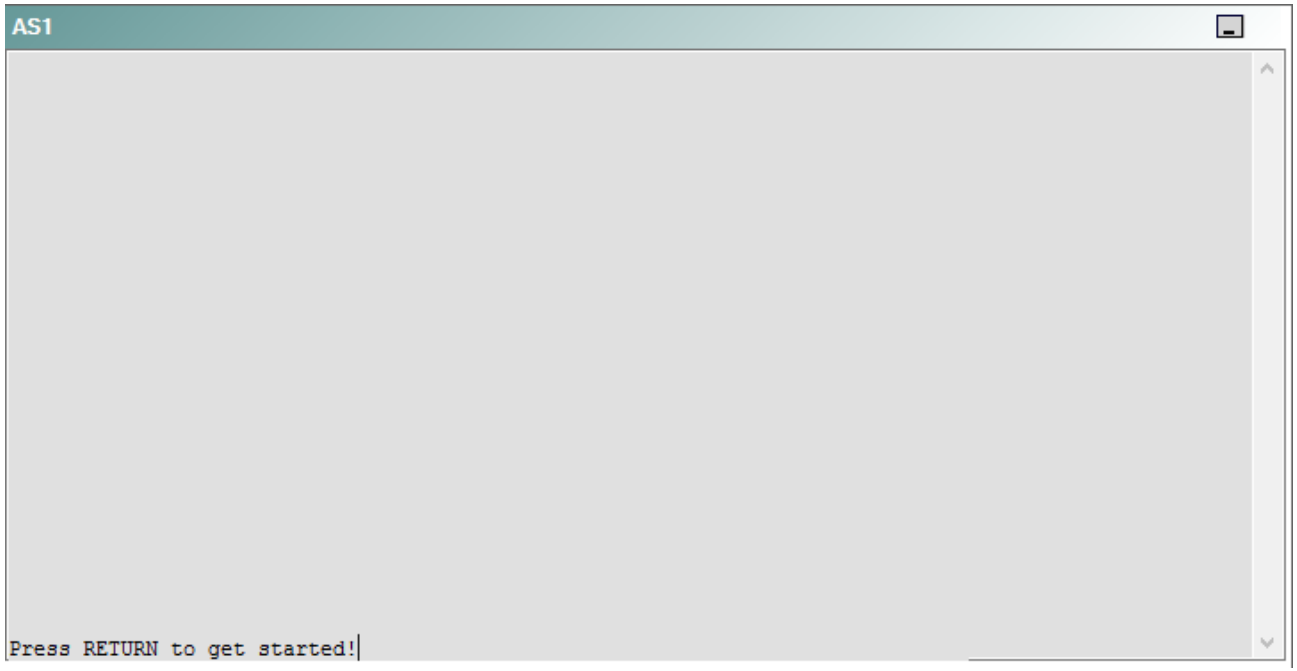

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. GRE
C. OSPFv2
D. OSPFv3
E. redistribution
F. DHCP
G. Layer 3 addressing
H. interface

**Correct Answer:** F
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

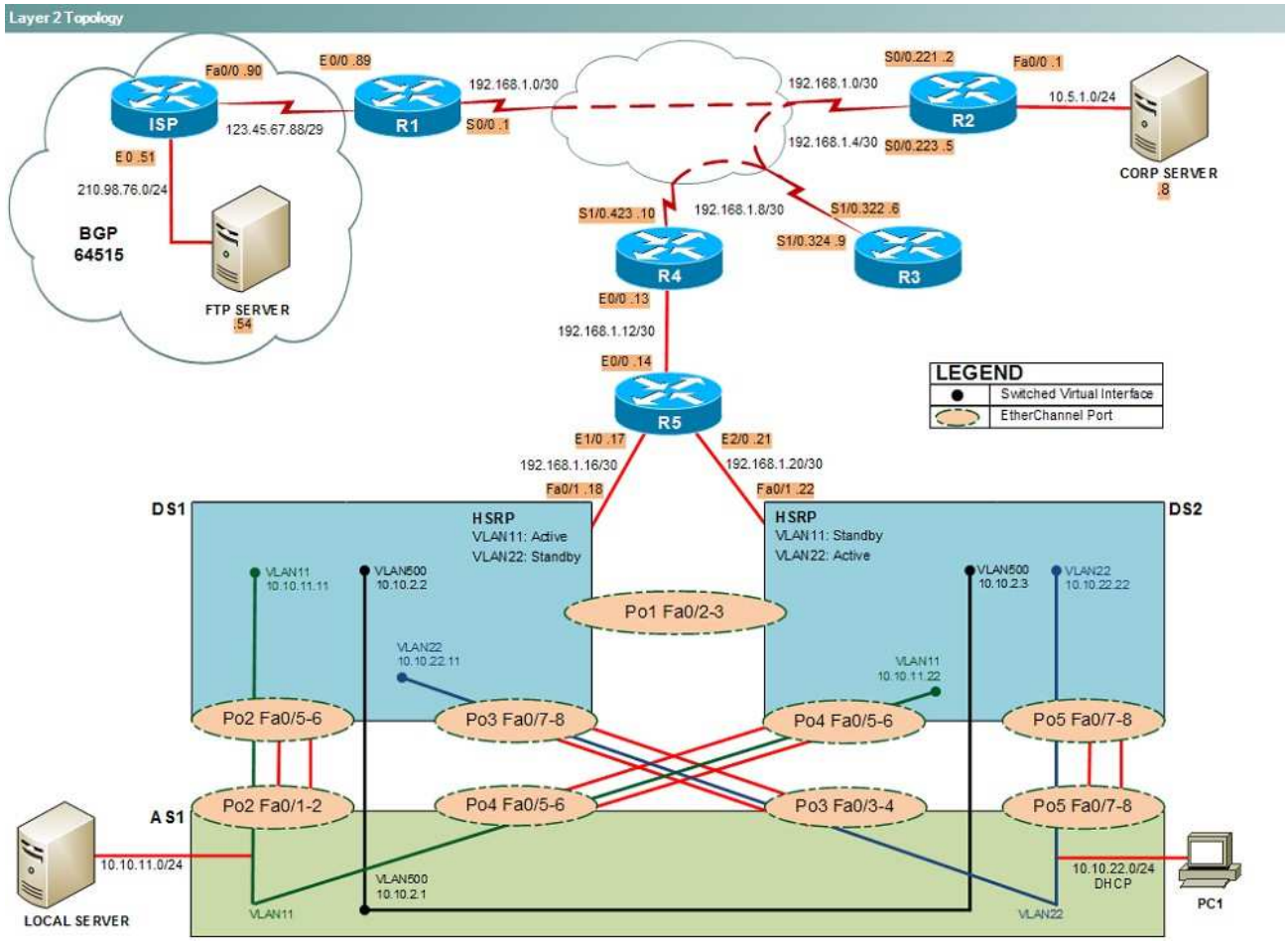
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

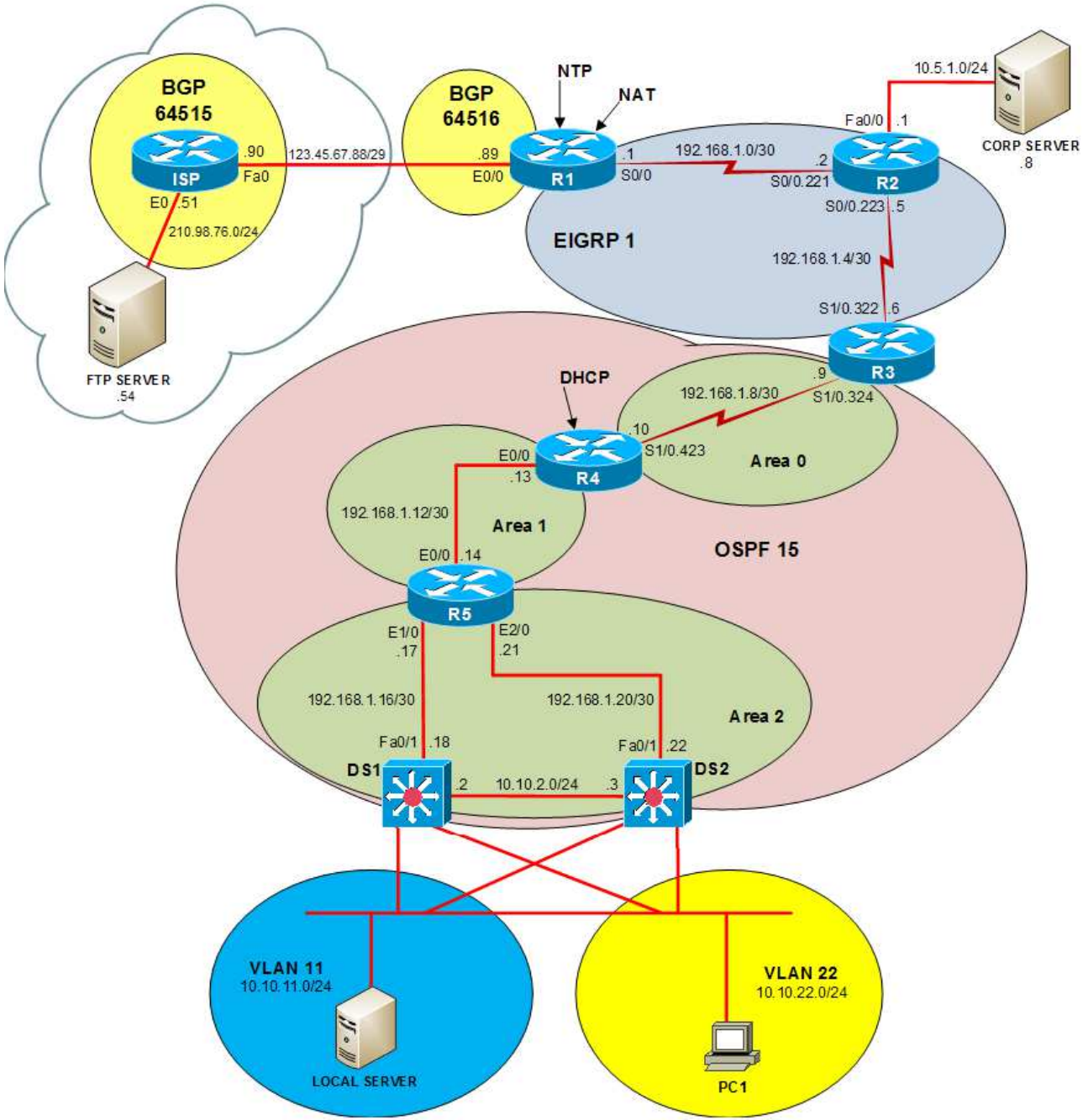
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

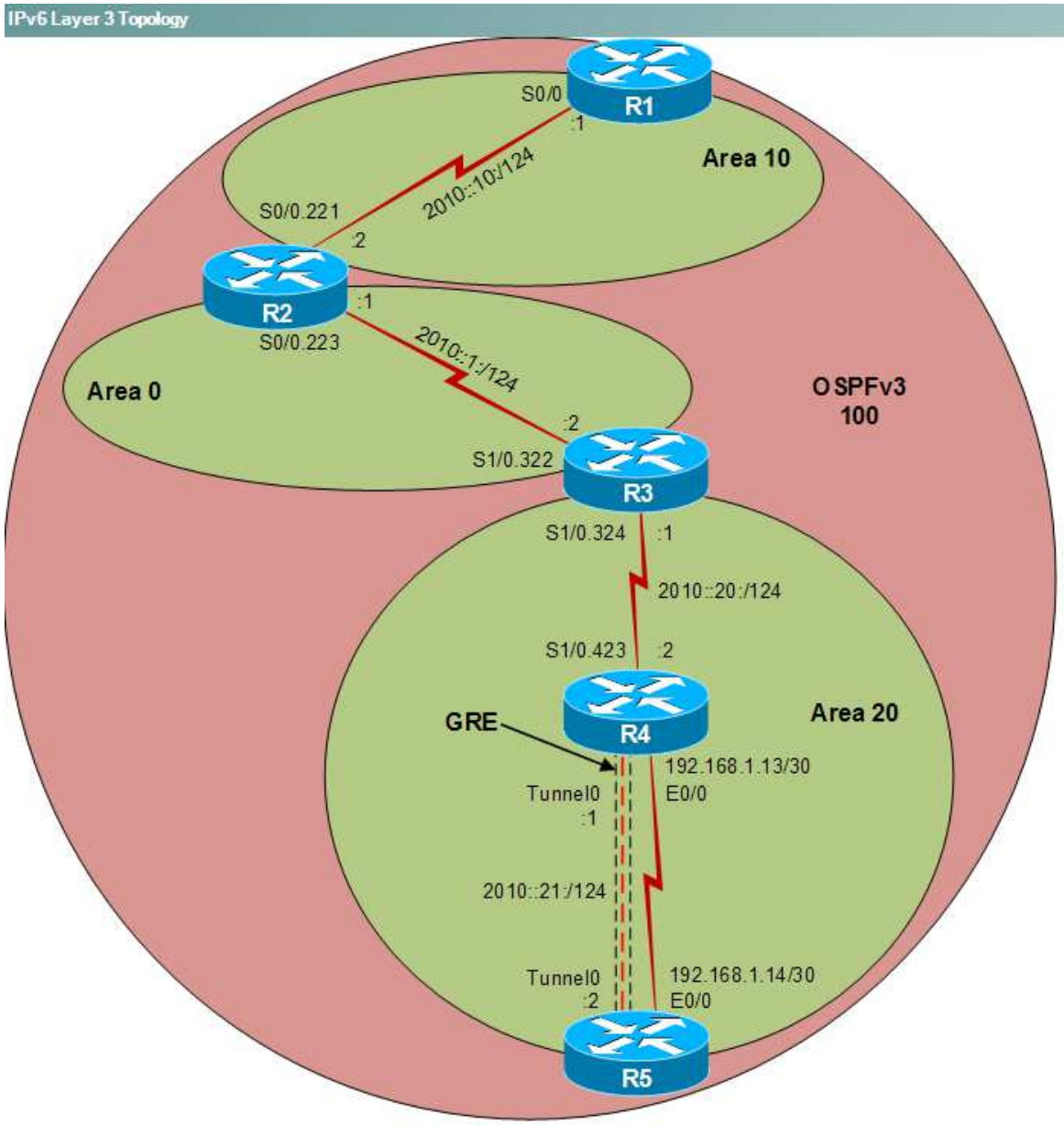
**Layer 2 Topology**




IPv4 layer 3 Topology

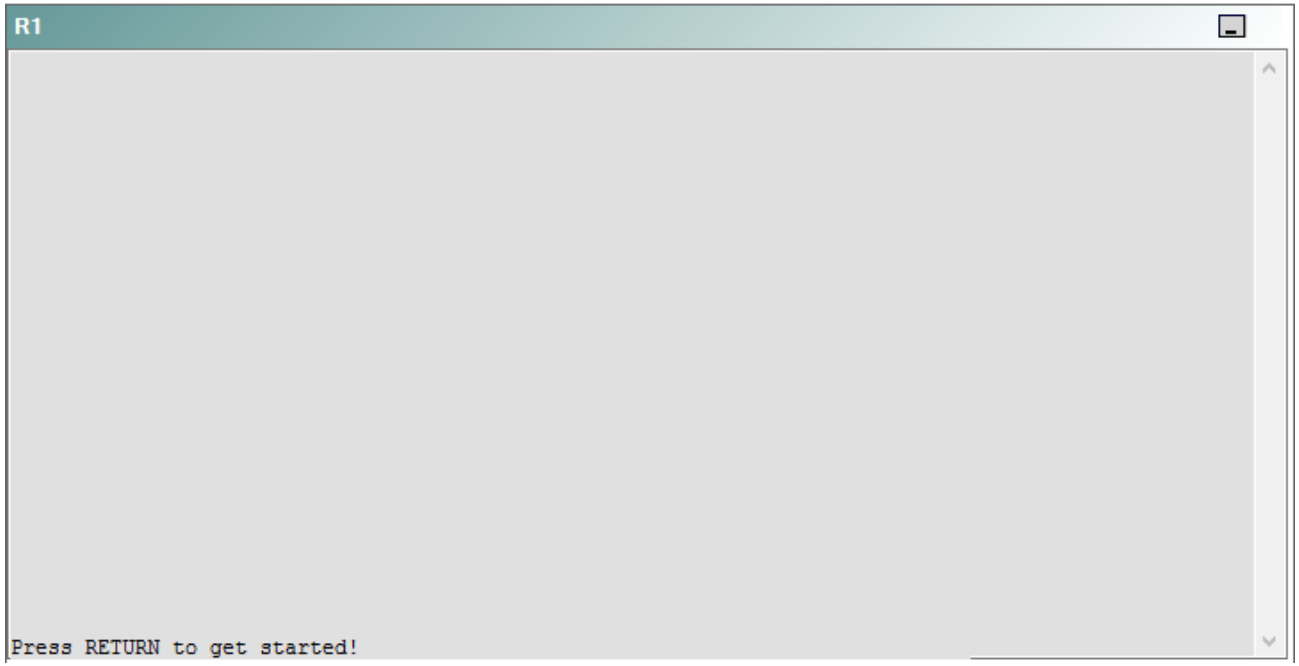

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

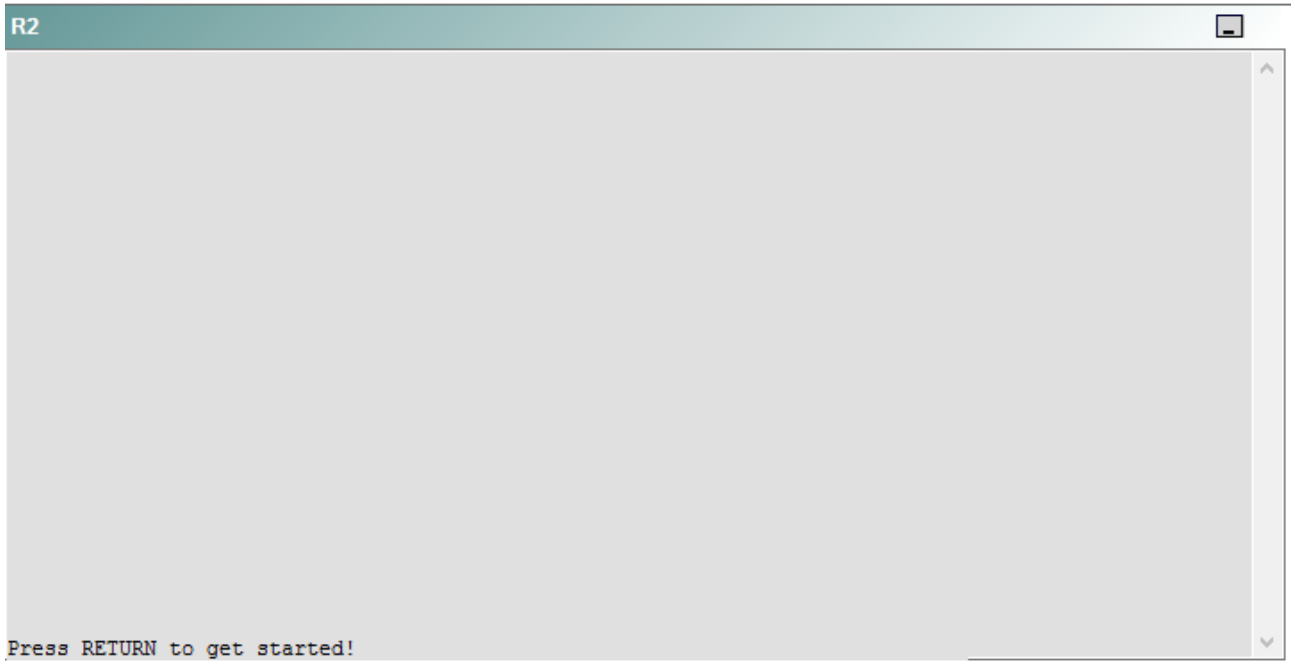



https://www.gratisexam.com/

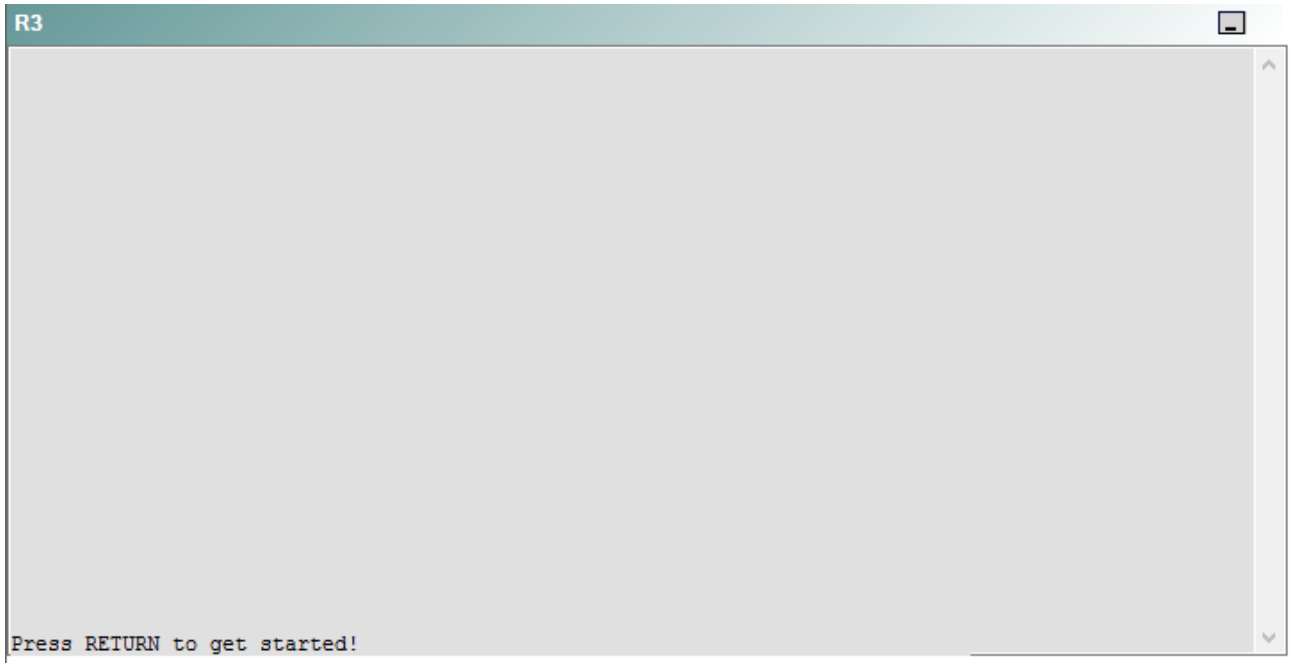
R1



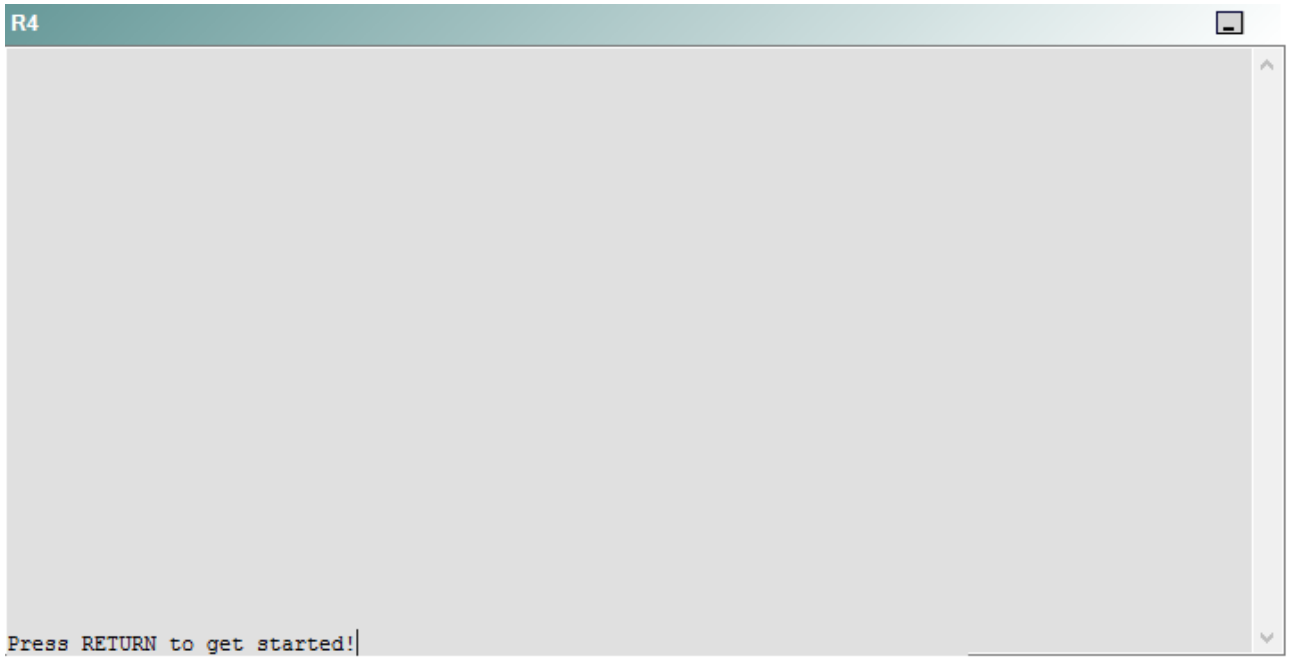

R2



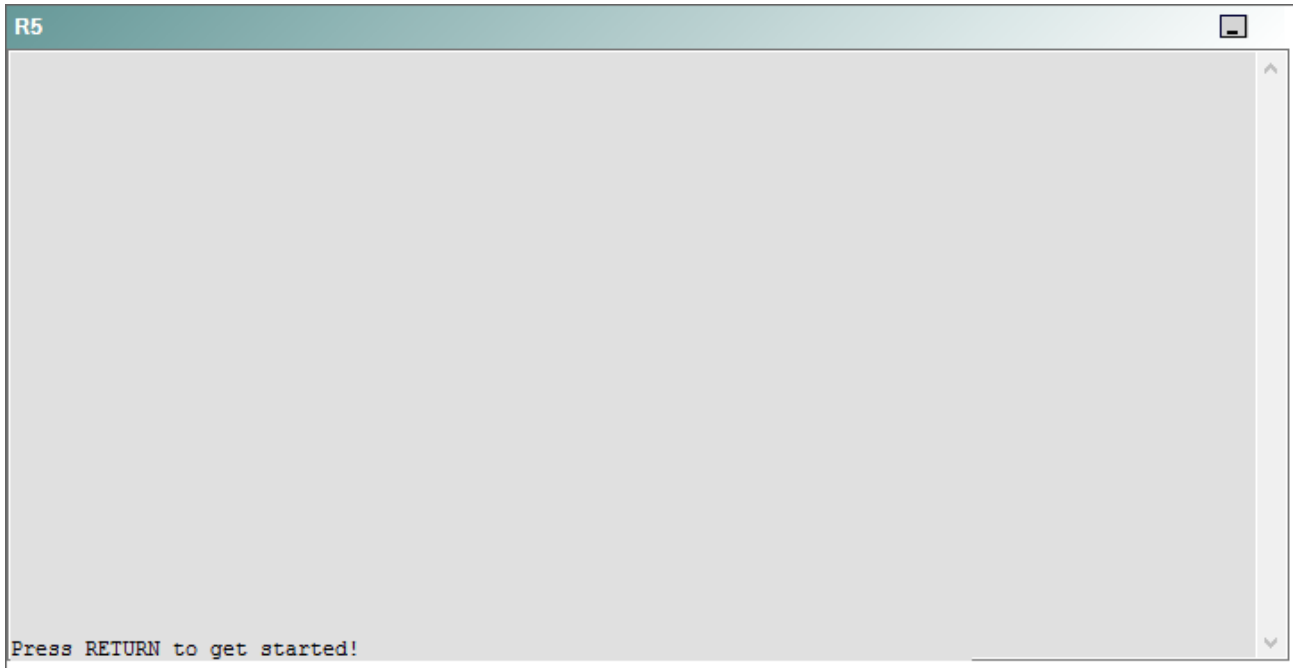

R3



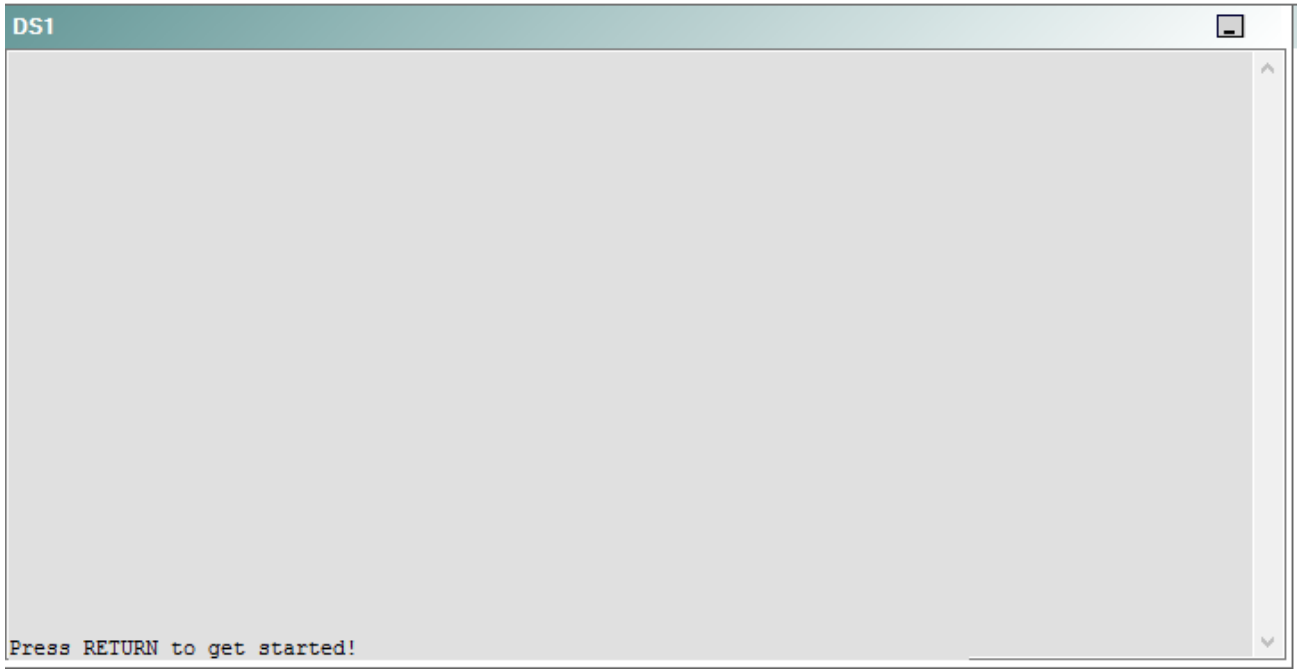

R4



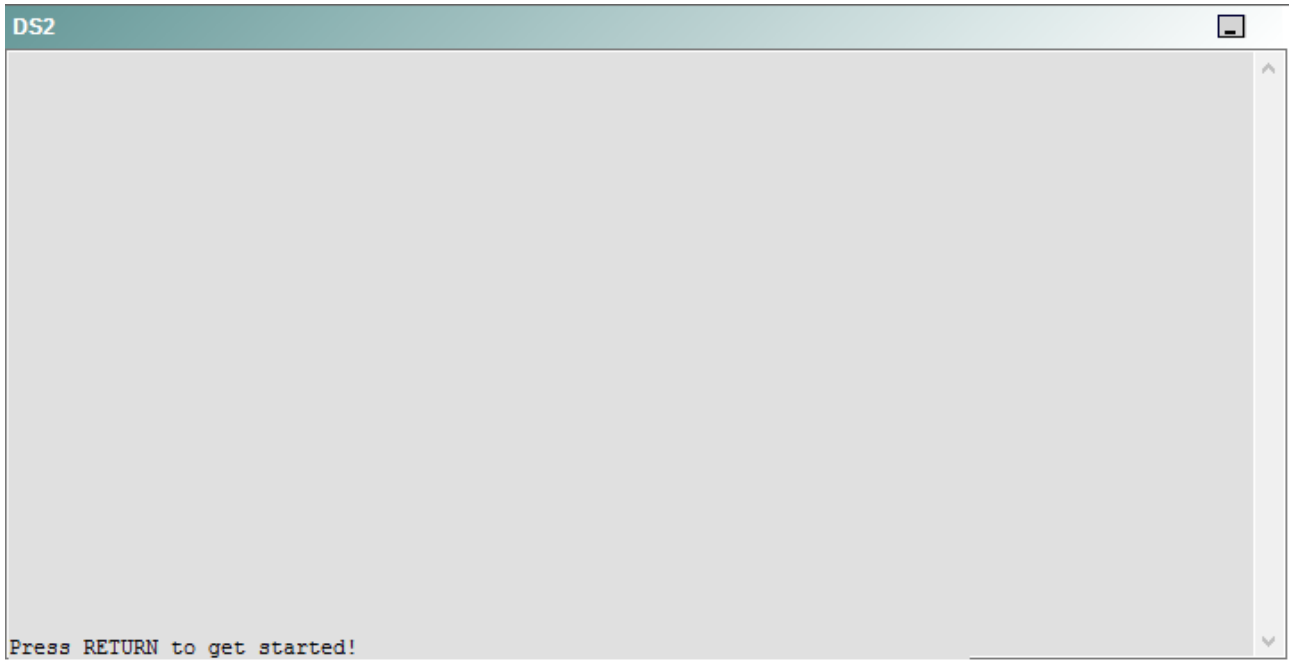

R5



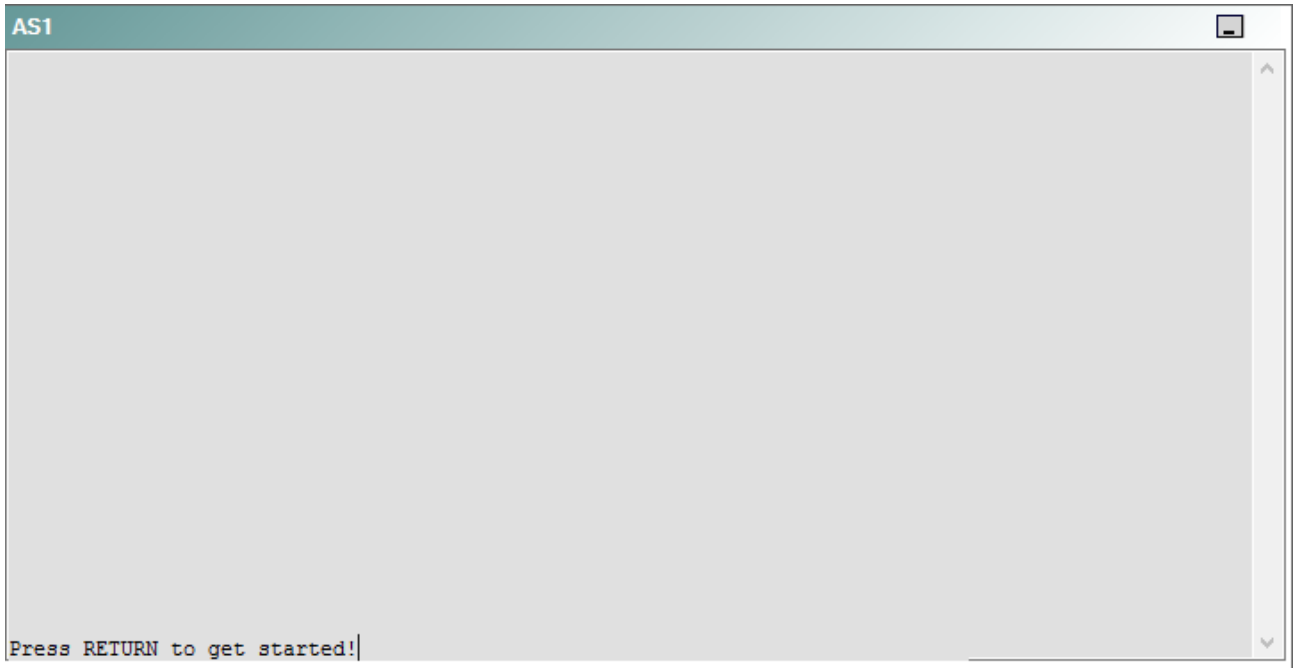

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. creating a new DHCP pool
B. modifying the DHCP exclusion range
C. modifying the IP address range assigned by the DHCP pool
D. changing the default router assigned by the DHCP pool
E. adding a default DNS server to the DHCP pool
F. creating an IP helper address
G. issuing the **ip forward-protocol udp 68** command.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

You should modify the Dynamic Host Configuration Protocol (DHCP) exclusion range on R4. To determine which device is the source of the problem, you can issue the **ping and traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from PC1 to the closest device and work your way up the network until communication is lost, or you can ping from PC1 to the farthest device and work your way back to PC1 until pings are successful.

In this scenario, PC1 is unable to ping any device on the network except 10.10.22.11. Issuing the **ipconfig** command on PC1 will display the following output:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.10.22.11
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.10.22.25
```

Issuing the **show running-config** command on DS1 will reveal that 10.10.22.11 is assigned to the virtual LAN (VLAN) 22 interface of DS1:

```
interface Vlan22
 description Address for VLAN 22
 ip address 10.10.22.11 255.255.255.0
 ip helper-address 192.168.99.4
 standby 2 ip 10.10.22.25
 standby 2 preempt
 standby 2 authentication Secret
```

Therefore, the DHCP server, R4, has assigned PC1 the same IP address as the one configured on the Fa0/1 interface of DS1. Issuing the **show ip dhcp binding** command on R4 confirms that R4 assigned the IP address to PC1, as shown in the following output:

```
R4#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address    Client-ID/          Lease expiration      Type
              Hardware address/
              User name
10.10.22.11   0100.1143.6254.2c   Jun 08 2010 01:21 AM  Automatic
```

R4 should be configured with an exclusion range so that DHCP clients are not assigned IP addresses to servers and static network devices. The **ip dhcp excluded-address** *start-address* end-address command is used to exclude from DHCP the range of addresses from *start-address* through end-address. Issuing the **show running-config** command on R4 displays the following partial output:

```
ip dhcp excluded-address 10.10.22.1 10.10.22.10
```

Issuing the **ip dhcp excluded-address 10.10.22.1 10.10.22.30** command on R4 is sufficient to exclude the statically assigned devices on the network.

You need not create a new DHCP pool on any of the devices on the network. Creating a new DHCP pool on another device with the same address range can cause IP address conflicts to arise if both DHCP servers assign the same IP address to two different devices. The **ip dhcp pool** *pool-name* command creates a DHCP pool and enters DHCP configuration mode, in which you can configure various DHCP client options.

You should not modify the IP address range assigned by the DHCP pool. The DHCP pool must assign addresses from the 10.10.22.0/24 network so that DHCP clients in VLAN 22 can receive IP addresses. The **network** *address subnet* command specifies the range of IP addresses that will be issued by DHCP.

You should not change the default router assigned by the DHCP pool. Clients in VLAN 22 should use the default gateway at 10.10.22.25, which is the shared gateway used by the Hot Standby Router Protocol (HSRP) switches, DS1 and DS2. The **default-router** *address* command specifies the default gateway that is assigned to clients by the DHCP server.

You need not add a Domain Name System (DNS) server to the DHCP pool. DNS servers are used for domain name-to-IP address resolution. PC1 cannot ping the server 210.98.76.54 by its IP address, so a DNS server is unnecessary. The **dns-server** *address* command specifies the DNS server address that is assigned to clients by the DHCP server.

You need not create an IP helper address. DS1 and DS2 are already configured with an IP helper address so that DHCP requests from VLAN 22 can reach R4. The **ip helper-address** command is used to forward User Datagram Protocol (UDP) broadcasts to a remote server or device. DHCP requests use UDP broadcasts, so a device configured as an IP helper can intercept a DHCP request and forward it to a DHCP server on a remote subnet. The address lease process and other communications are then returned to the originating subnet.

You need not issue the **ip forward-protocol udp 68** command. The **ip forward-protocol** command is used to specify the UDP port numbers that should be forwarded by the **ip helper-address** commands. By default, the **ip helper-address** command forwards broadcasts to the following UDP ports:

- 37 - Time Protocol
- 49 - Terminal Access Controller Access Control System (TACACS)
- 53 - DNS
- 67 - Bootstrap Protocol (BOOTP) and DHCP Server
- 68 - BOOTP and DHCP Client
- 69 - Trivial File Transfer Protocol (TFTP)
- 137 - Network Basic Input/Output System (NetBIOS) Name Service
- 138 - NetBIOS Datagram

Because DHCP client requests are already being sent by the **ip helper-address** command, the **ip forward-protocol udp 68** command is unnecessary.

**Reference:** https://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfdhcp.html

**QUESTION 6**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

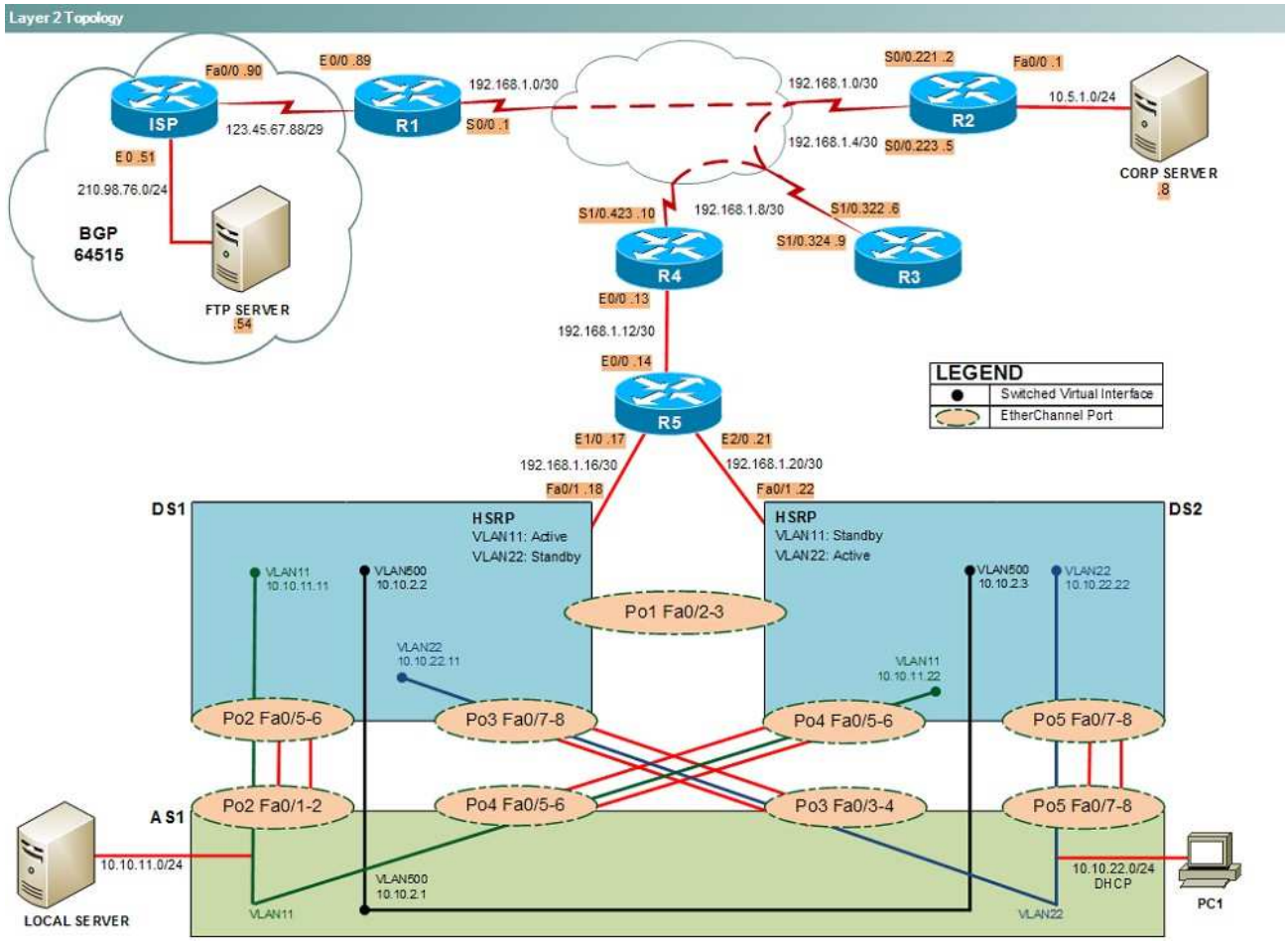
Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**.

However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

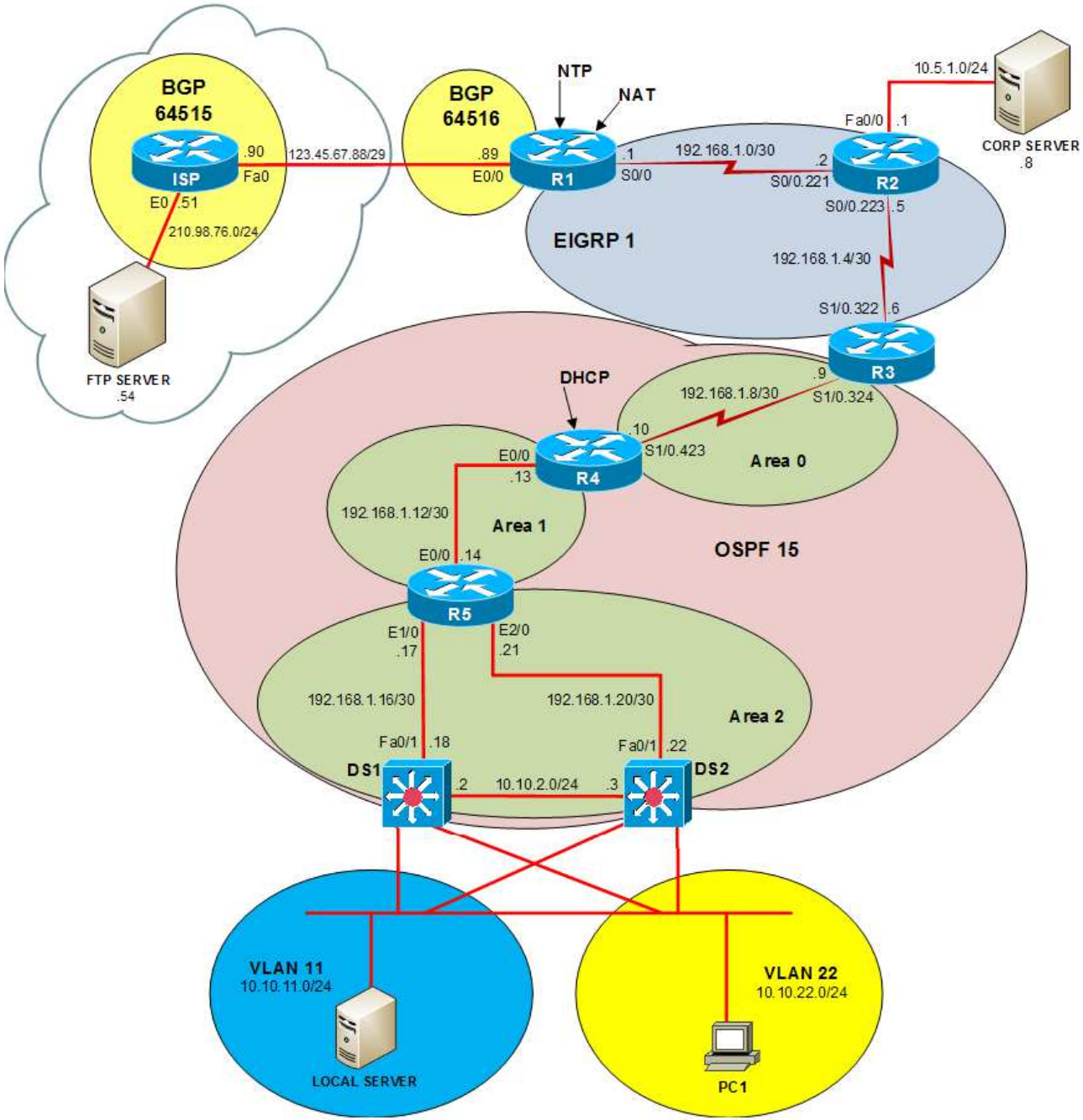
Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

**Layer 2 Topology**

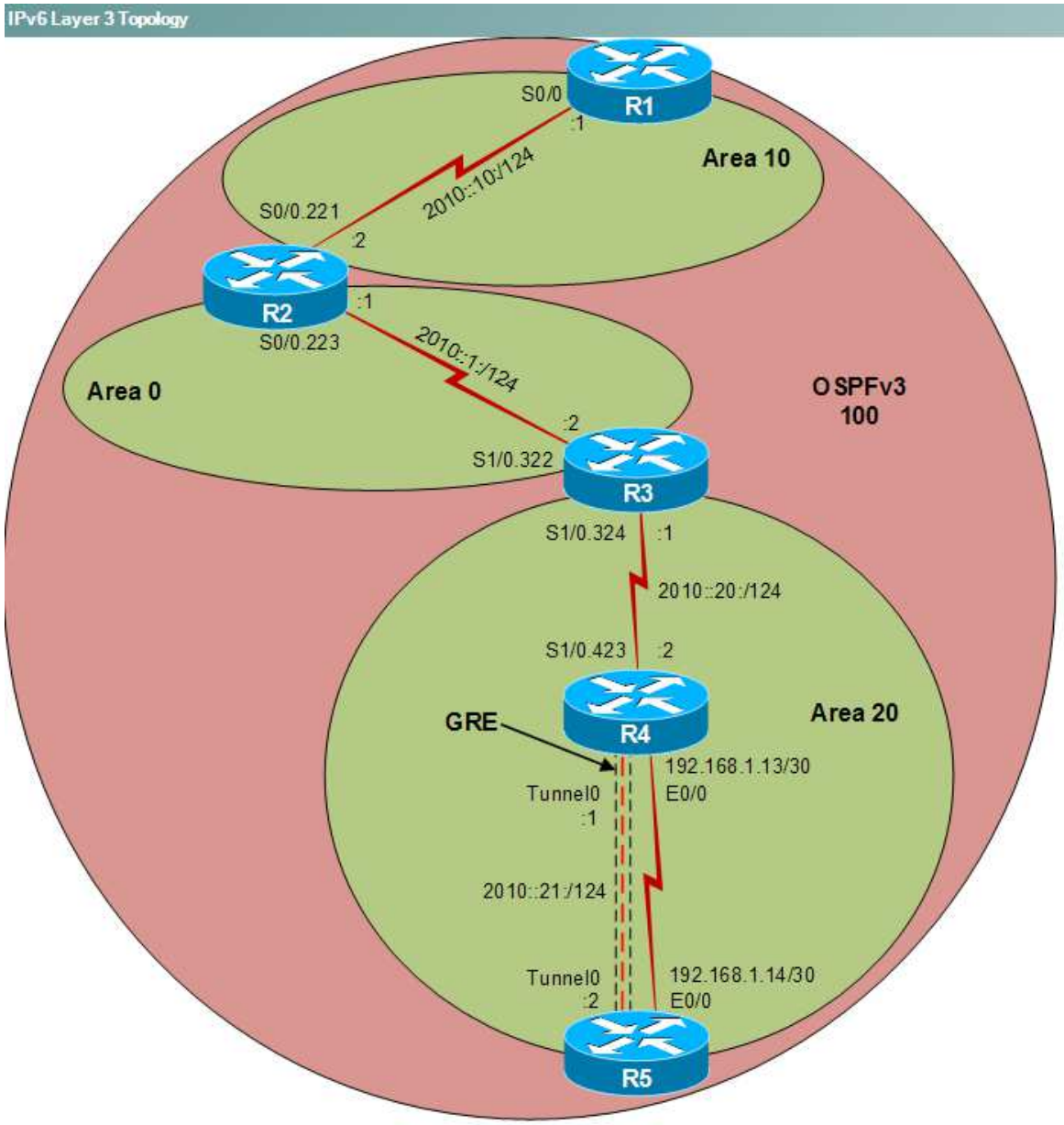



IPv4 layer 3 Topology

https://www.gratisexam.com/

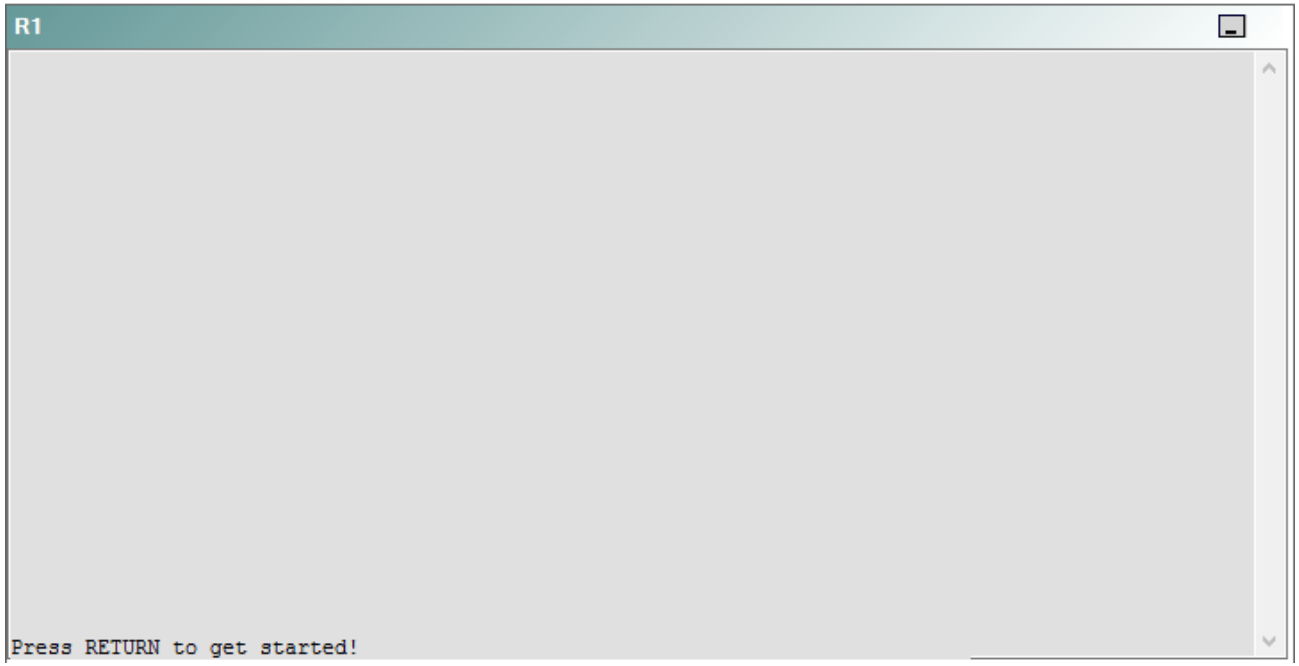

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

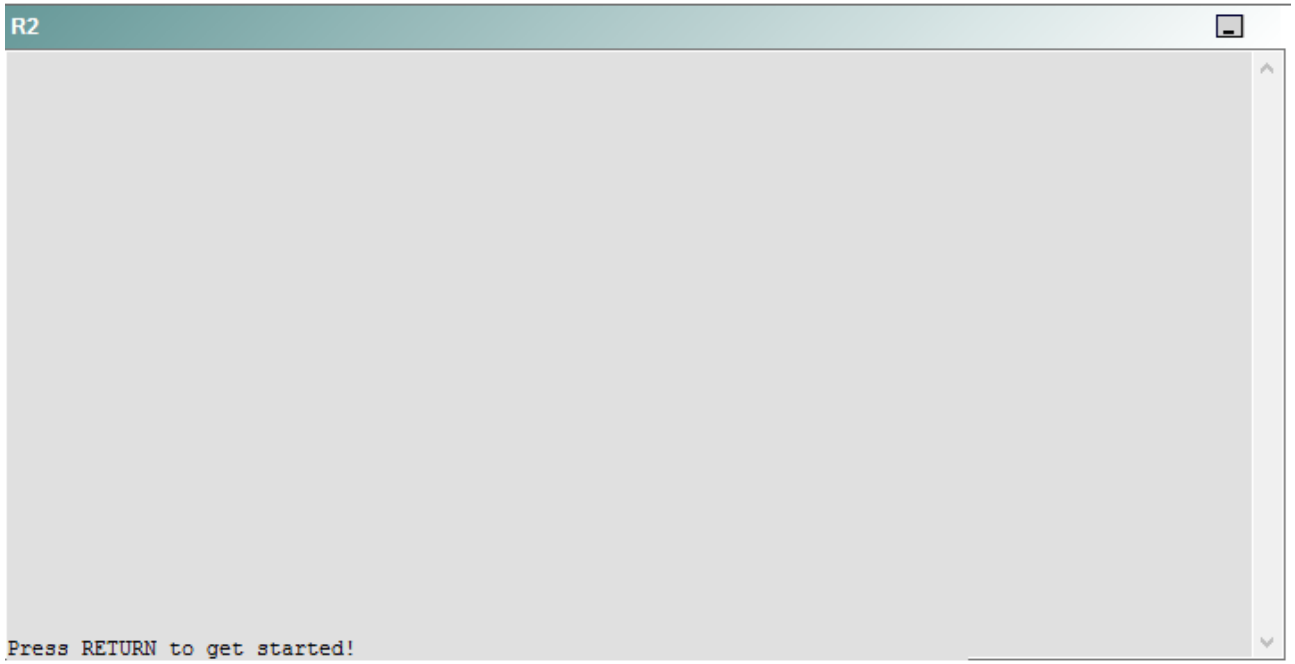



https://www.gratisexam.com/

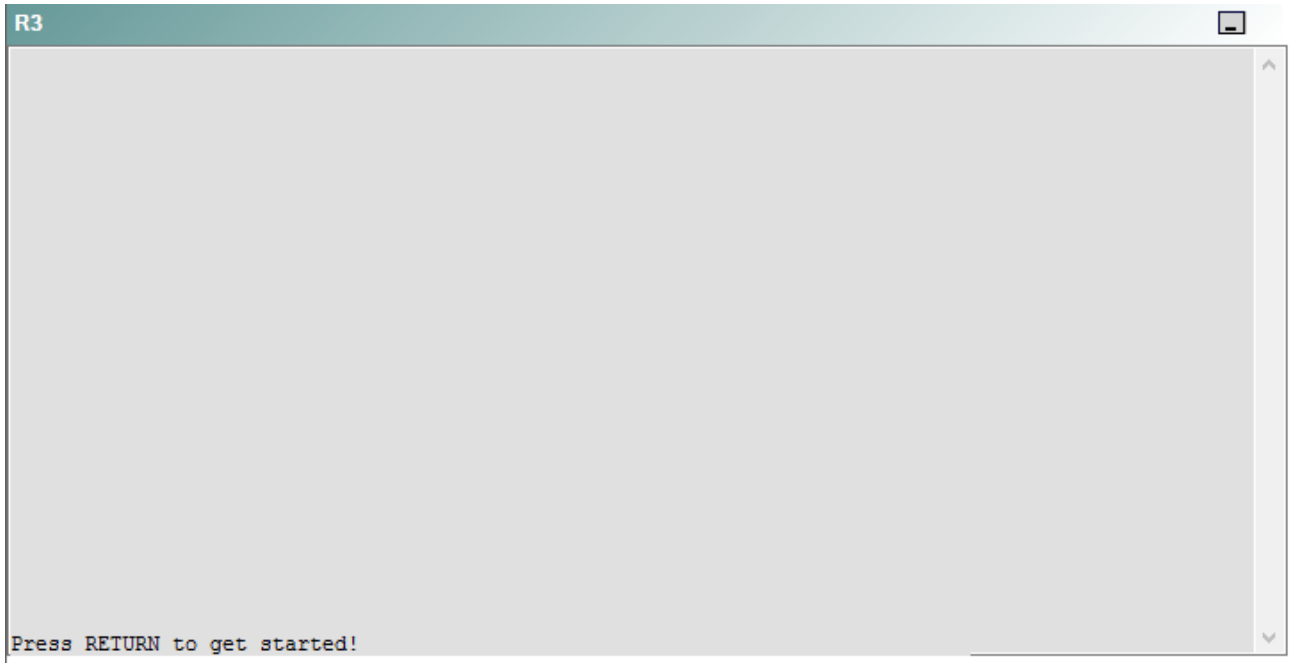
R1



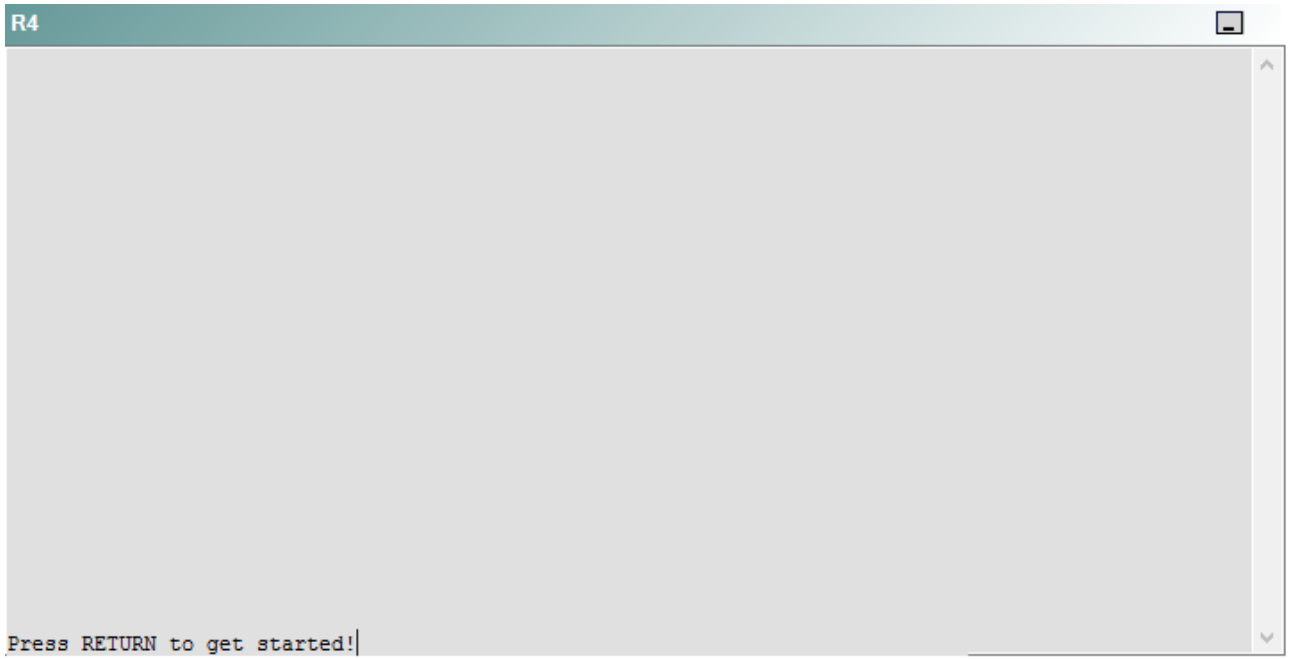

R2



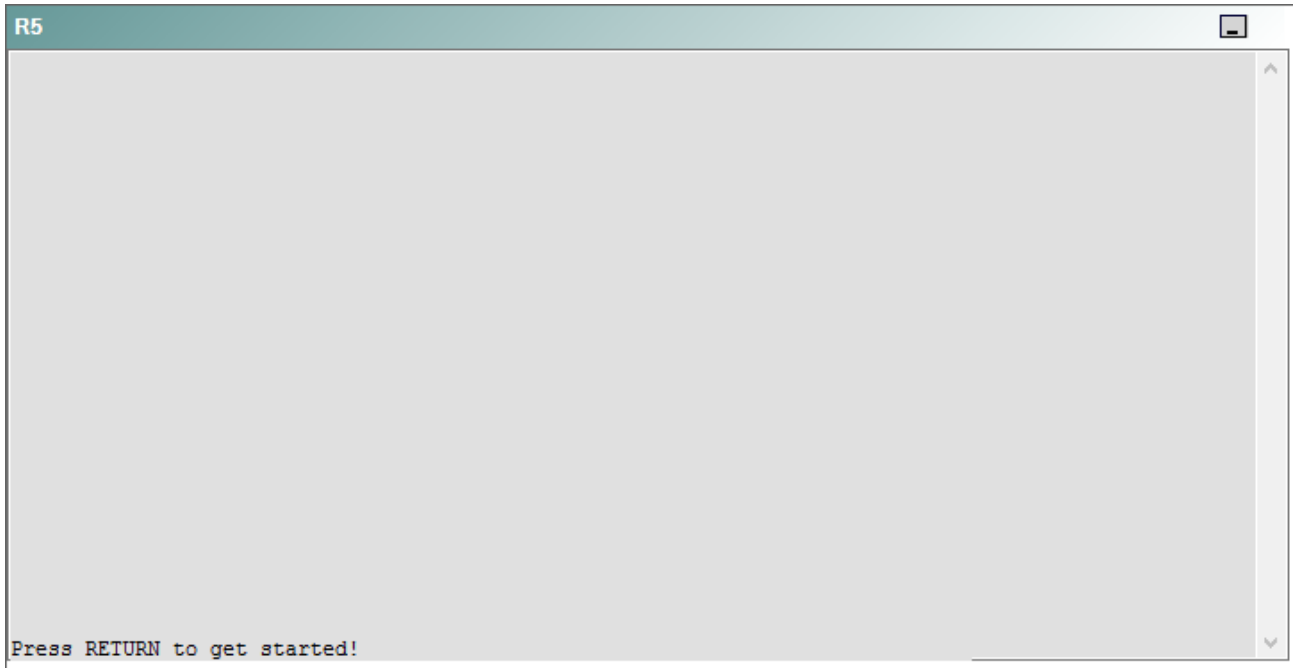

R3



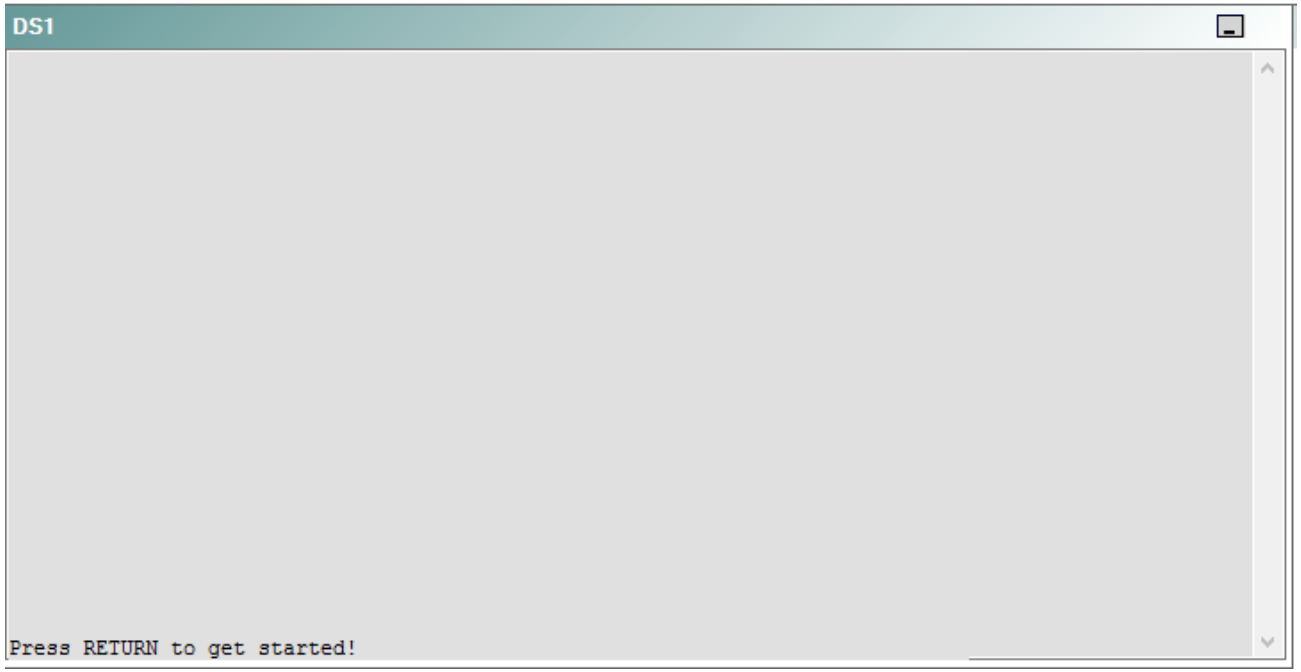

R4



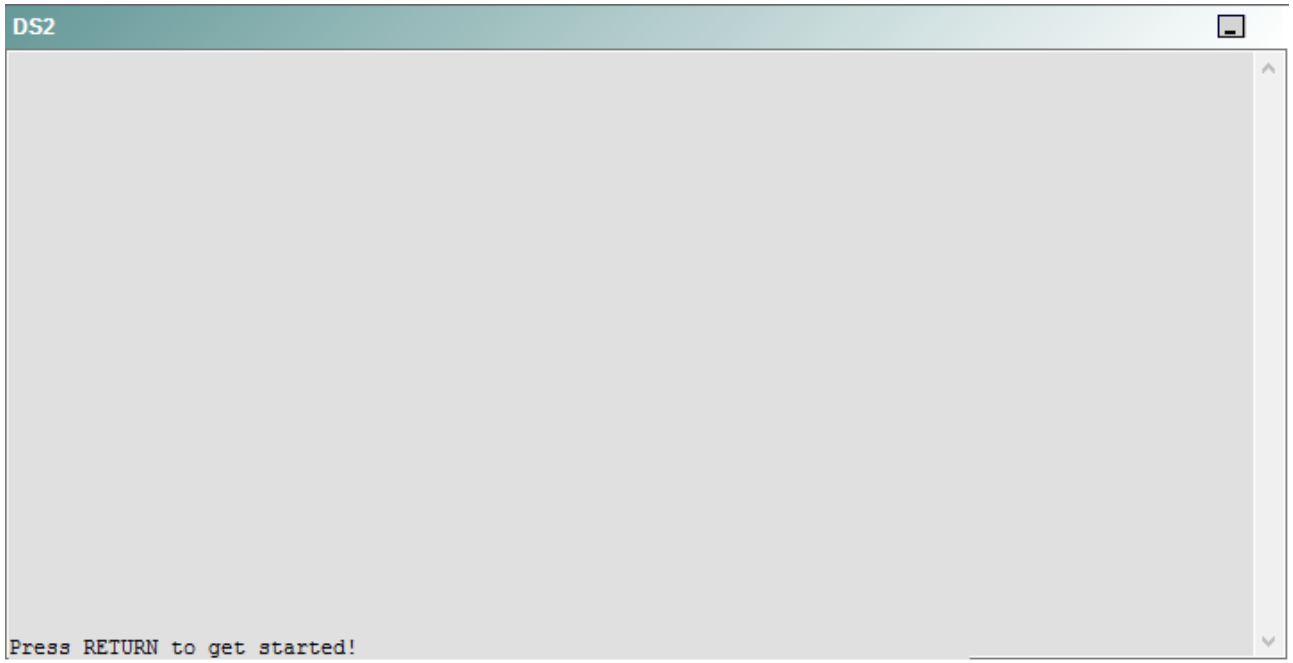

R5



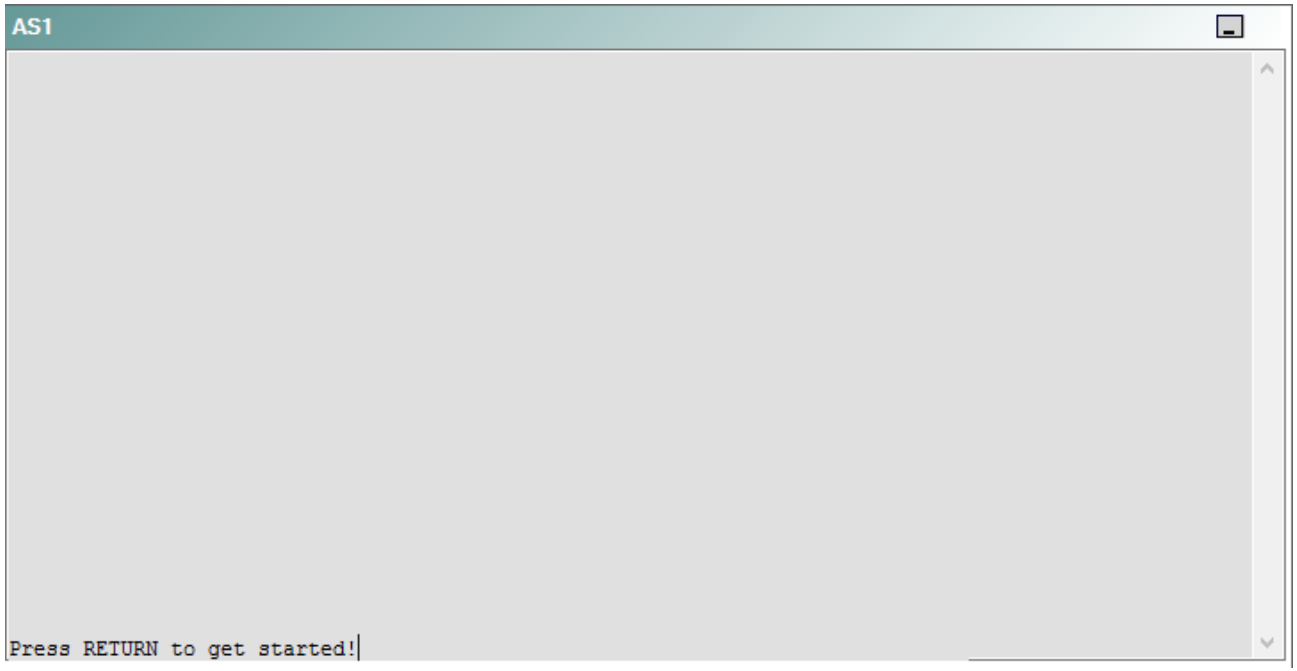

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 7**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

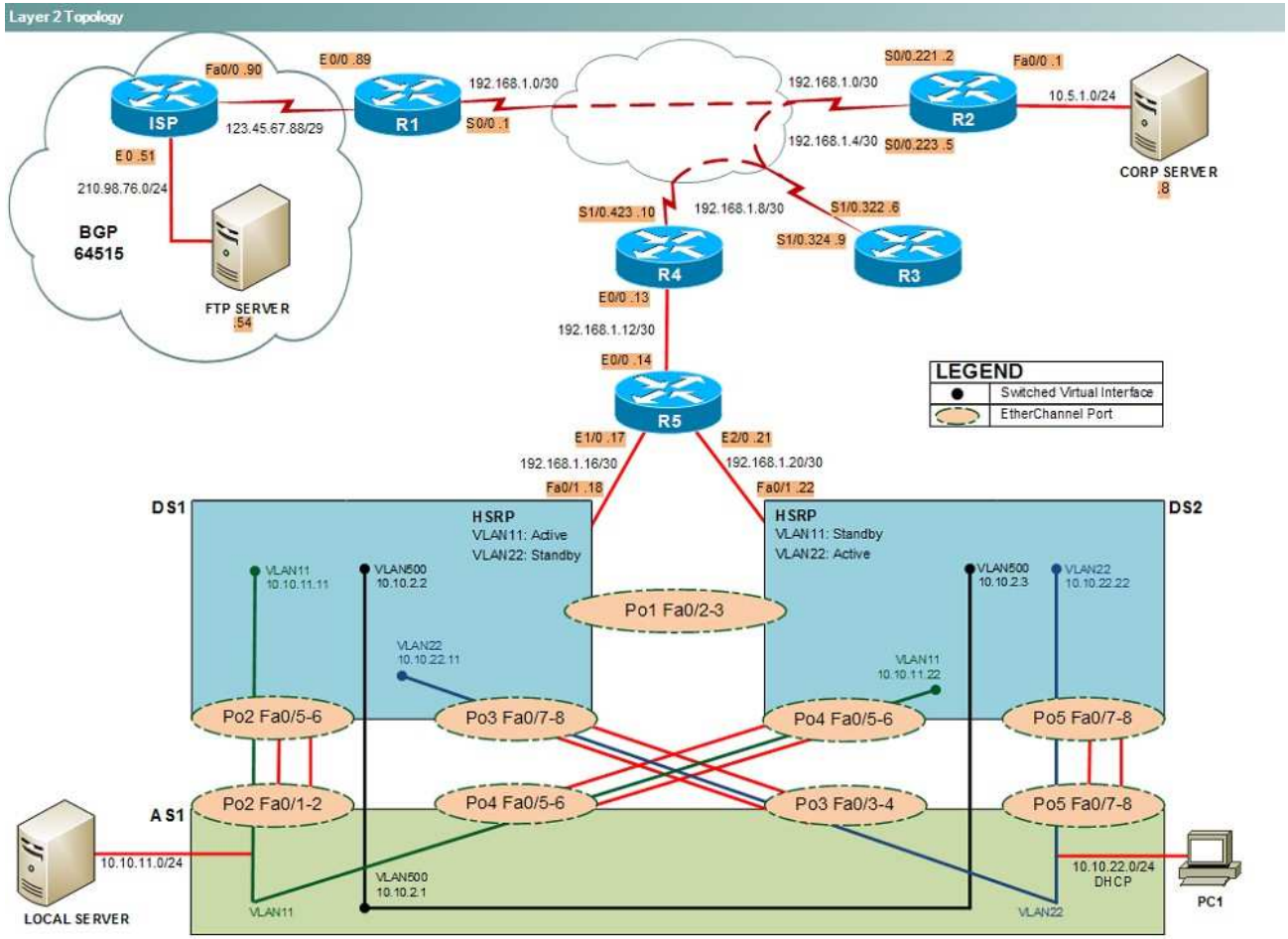
Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

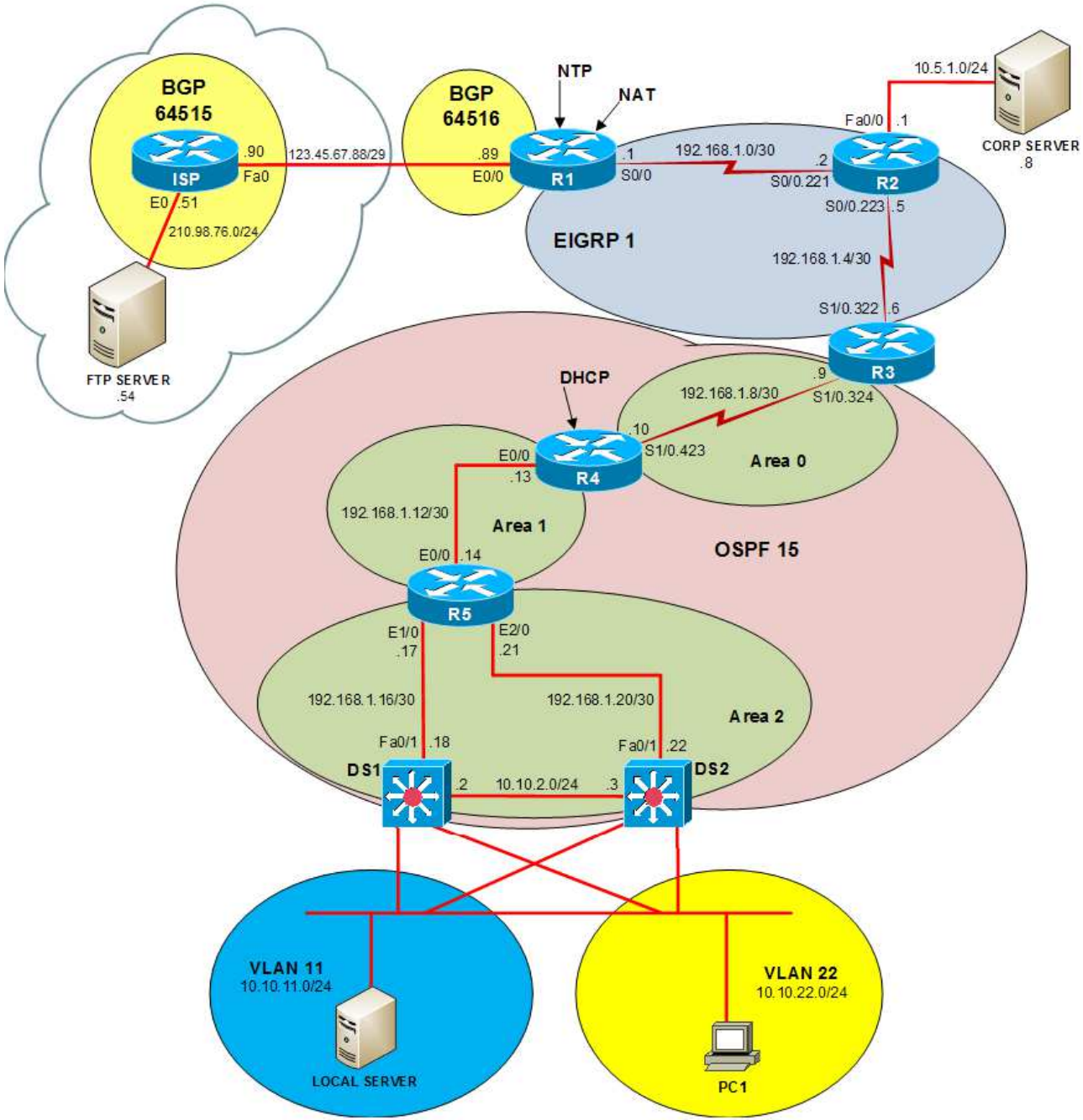
Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

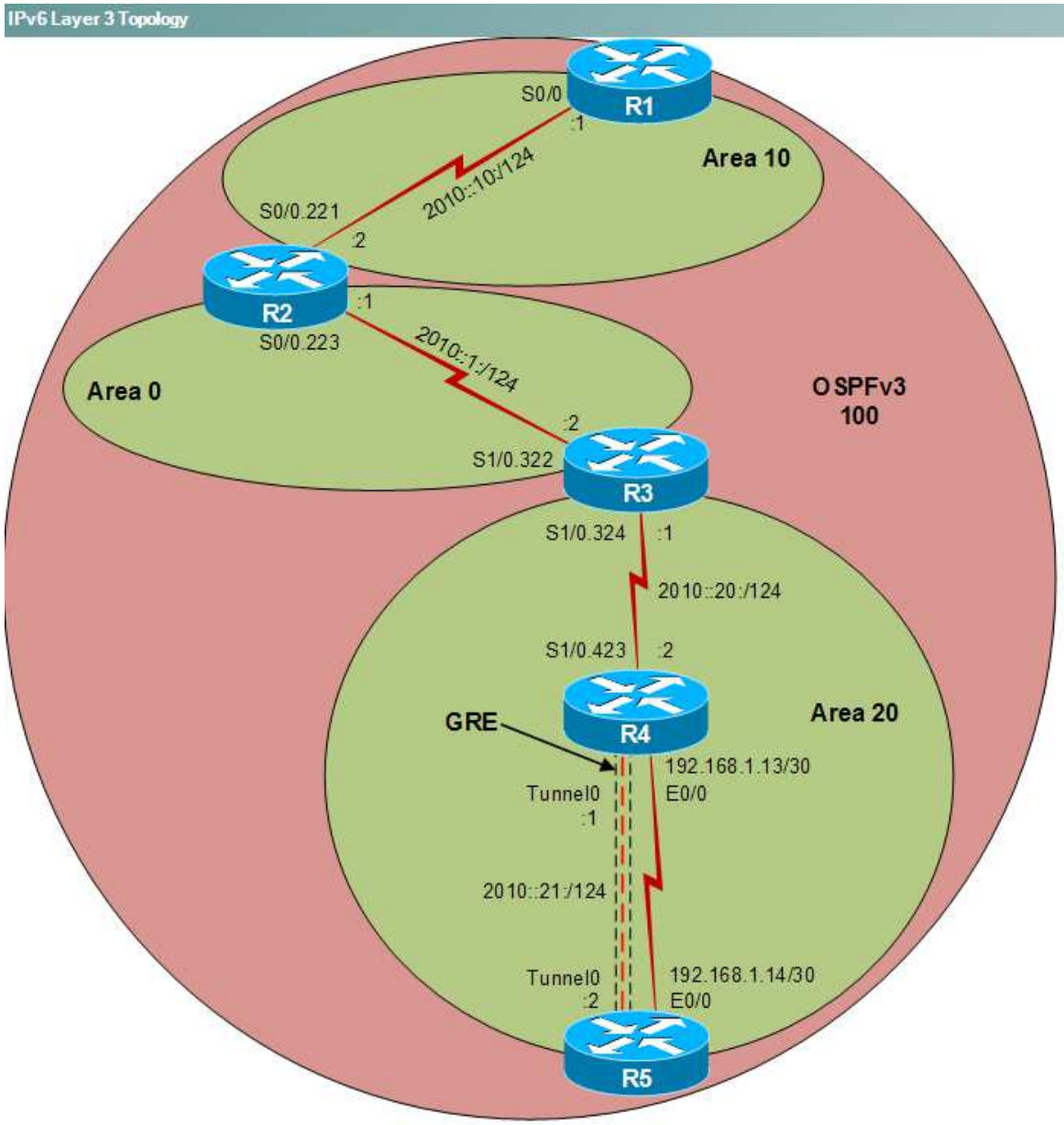
**Layer 2 Topology**



IPv4 layer 3 Topology

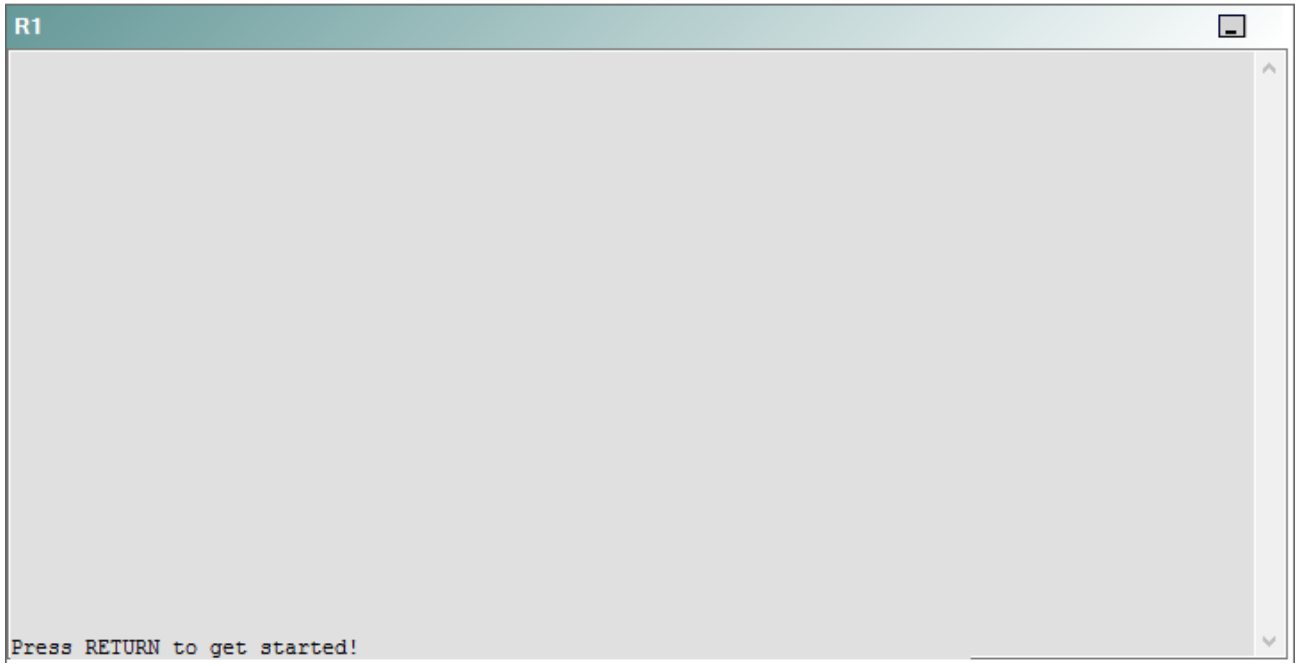

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

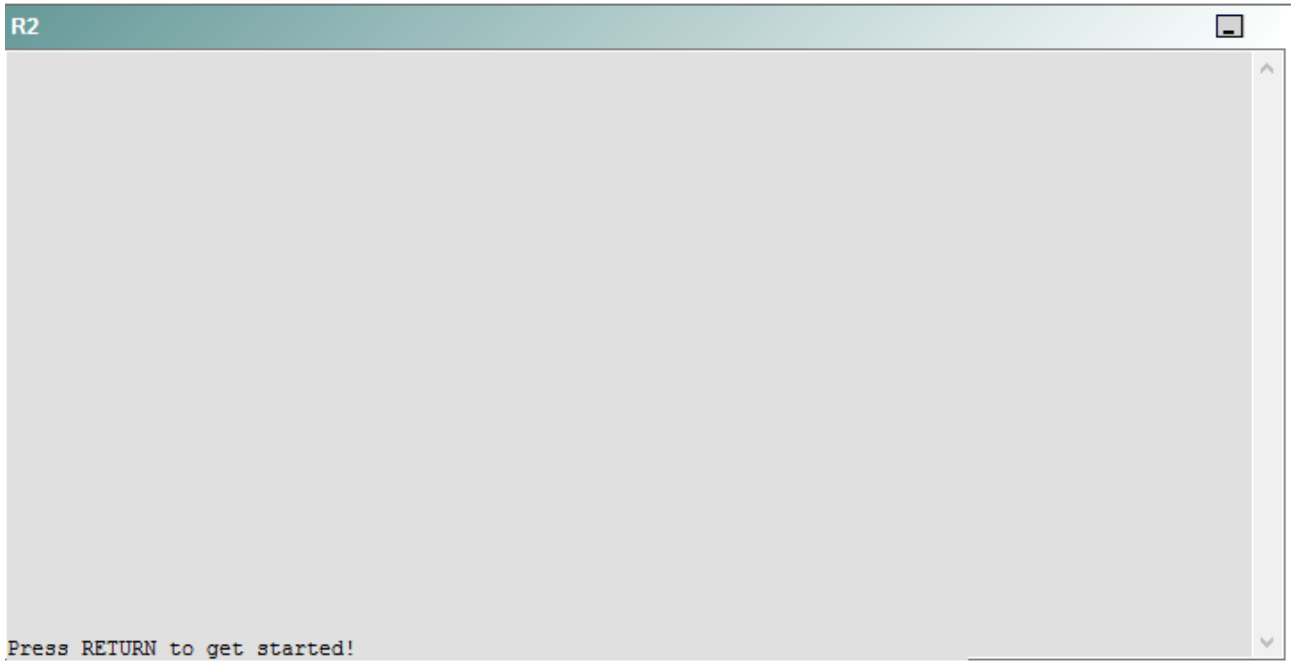



https://www.gratisexam.com/

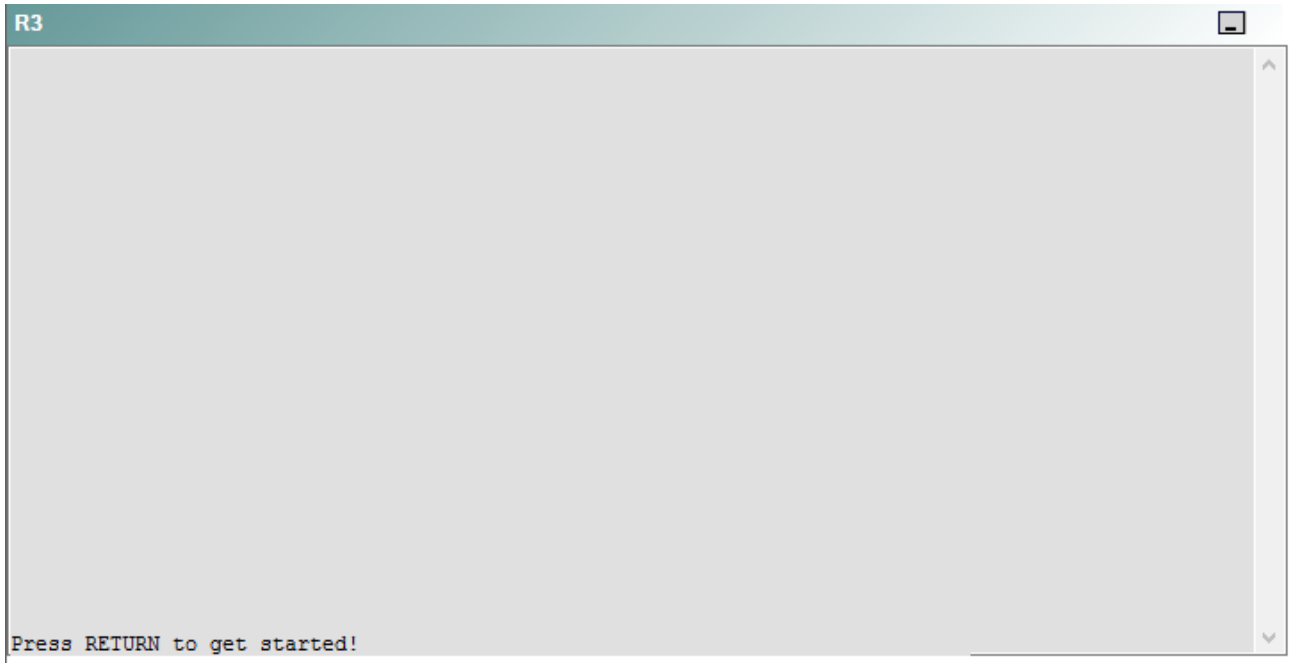
R1



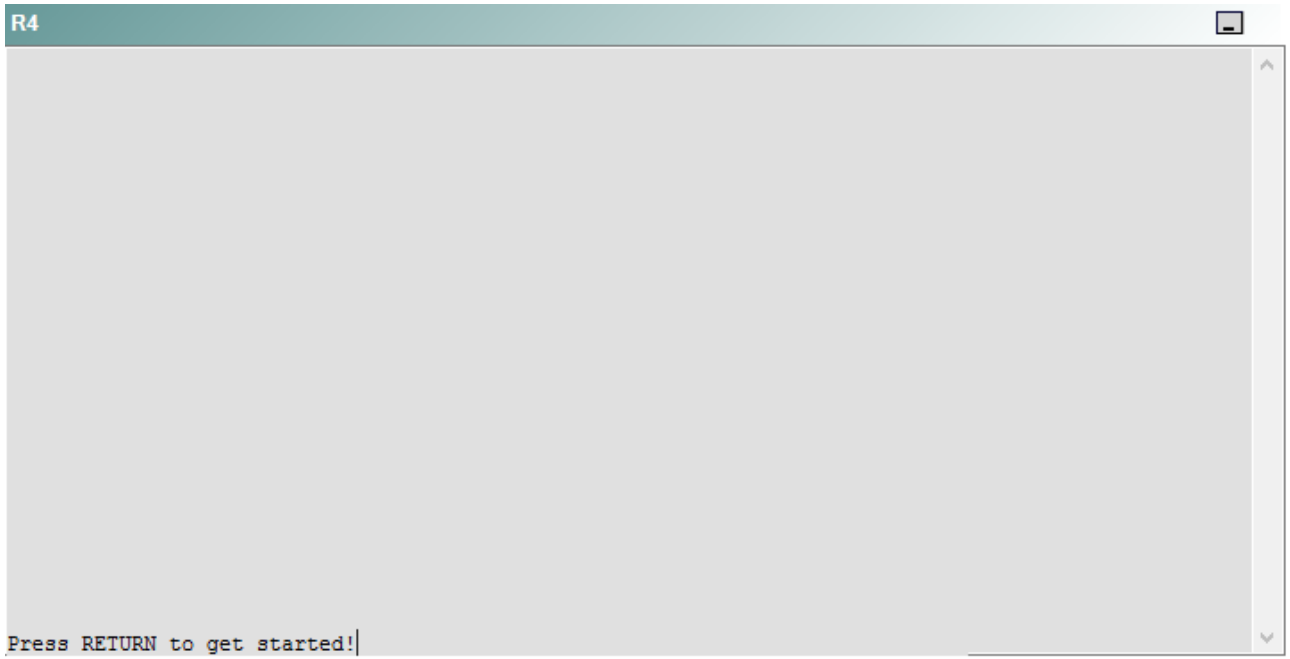

R2



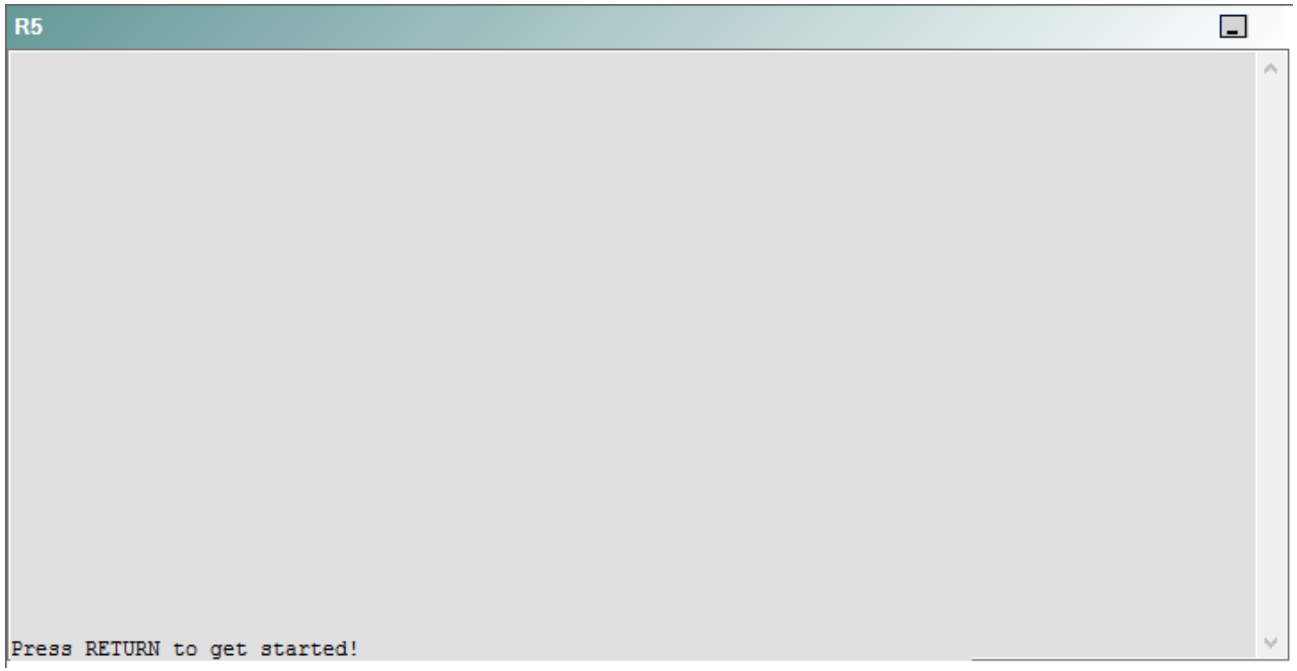

R3



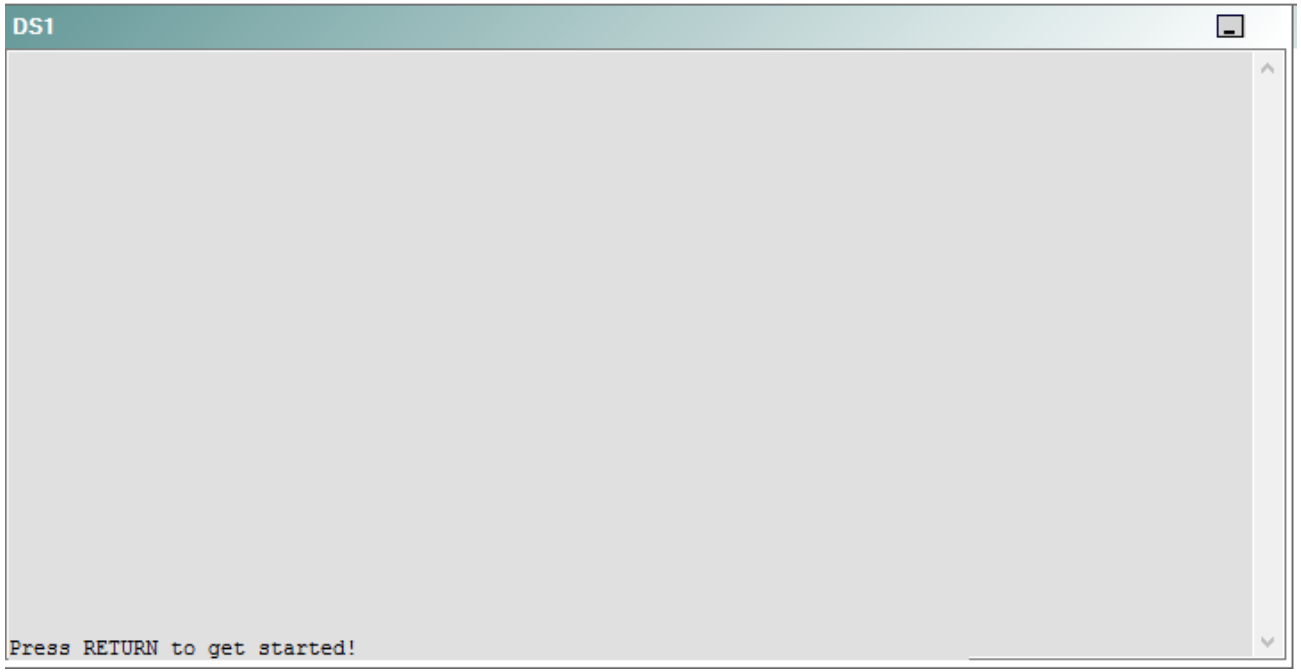

R4



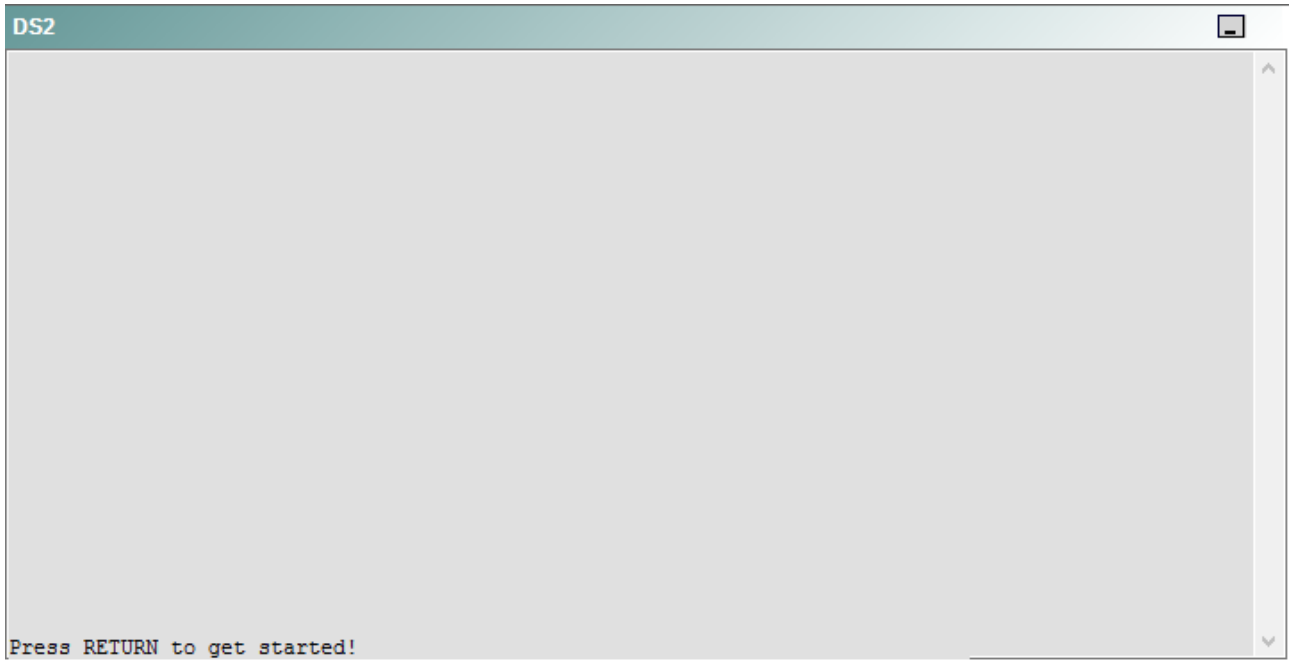

R5



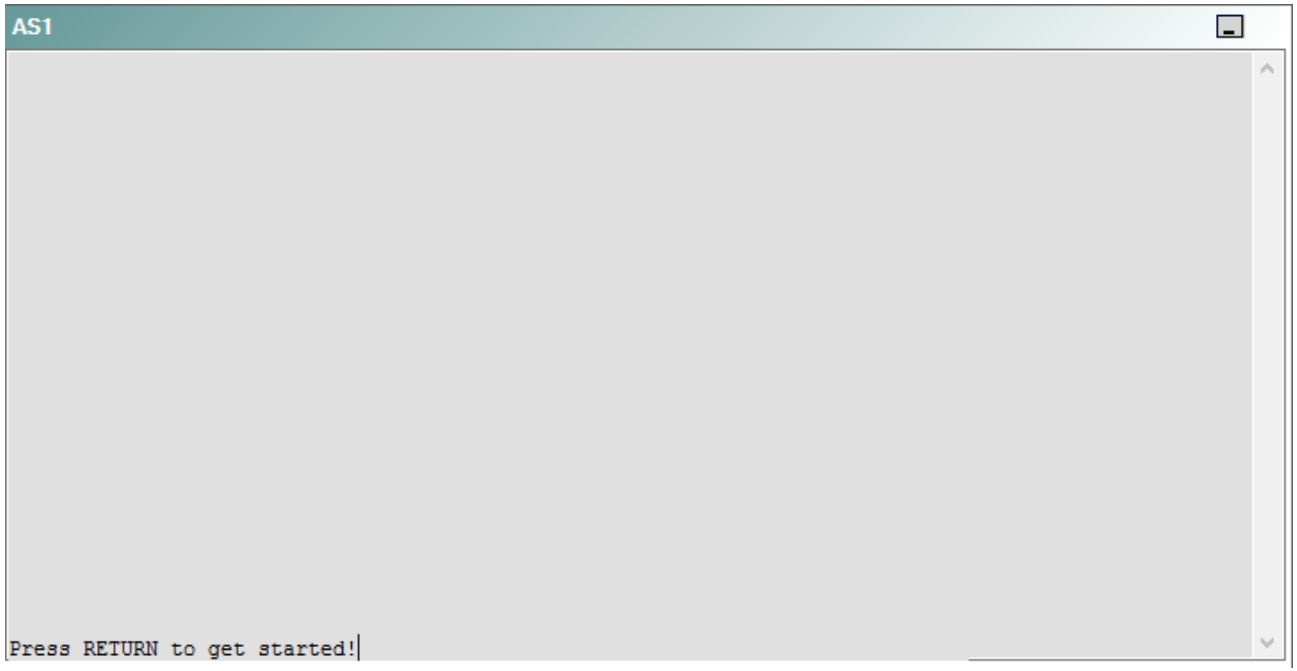

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. DHCP
C. Layer 3 addressing
D. Layer 3 security
E. Layer 2 security
F. STP
G. Etherchannel
H. VLAN configuration
I. interface

**Correct Answer:** I

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

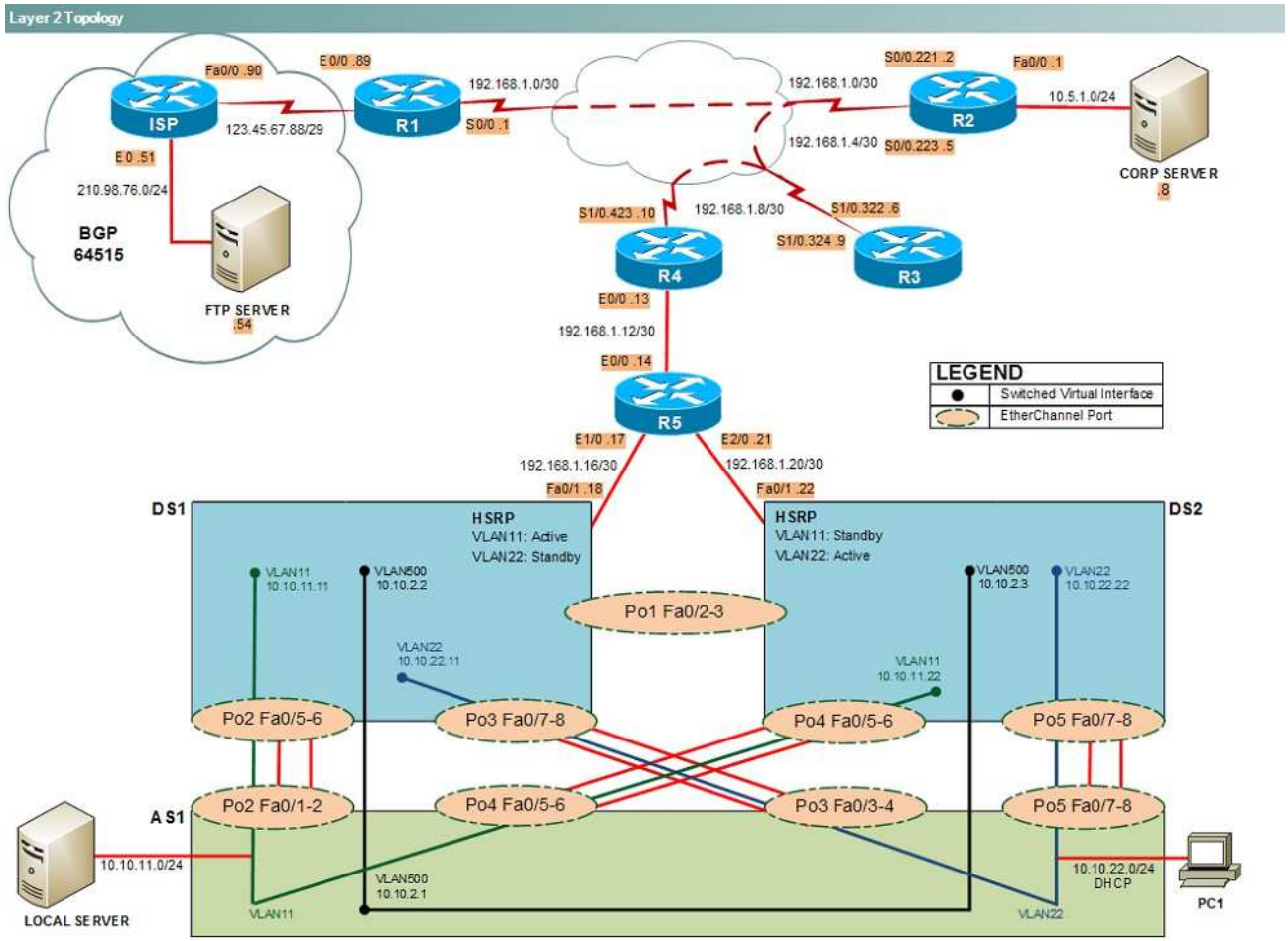
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

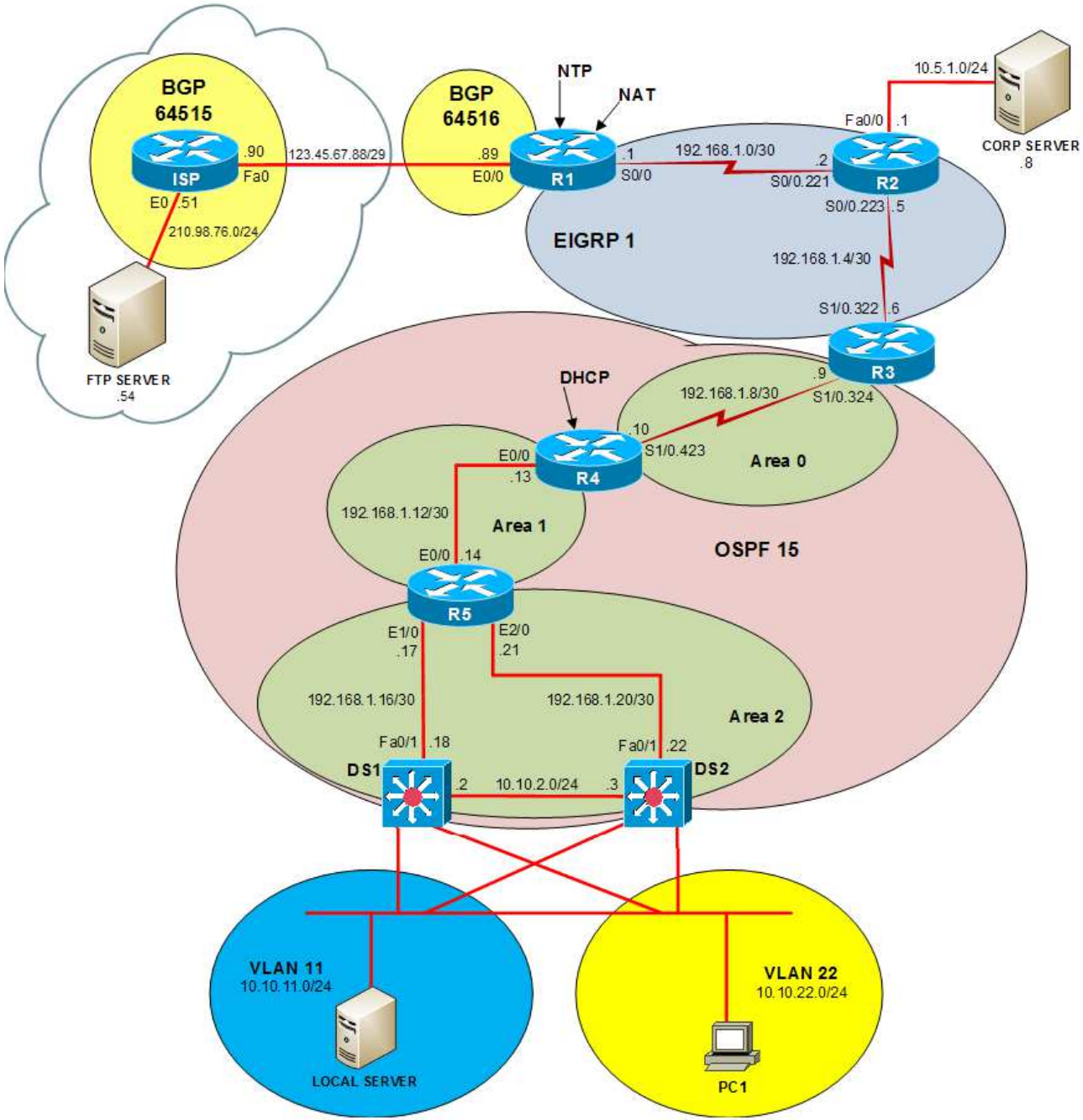
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

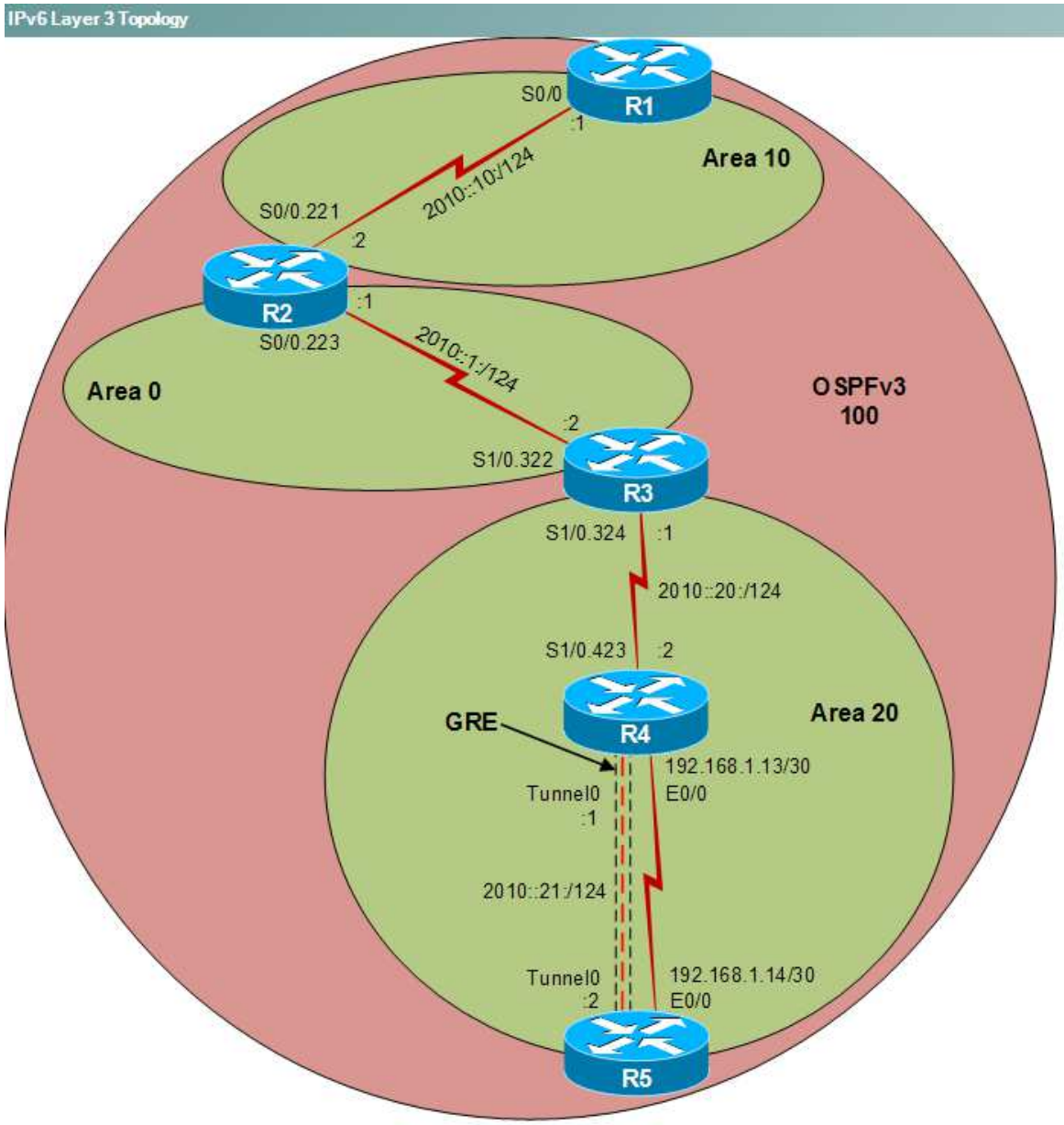
**Layer 2 Topology**




IPv4 layer 3 Topology

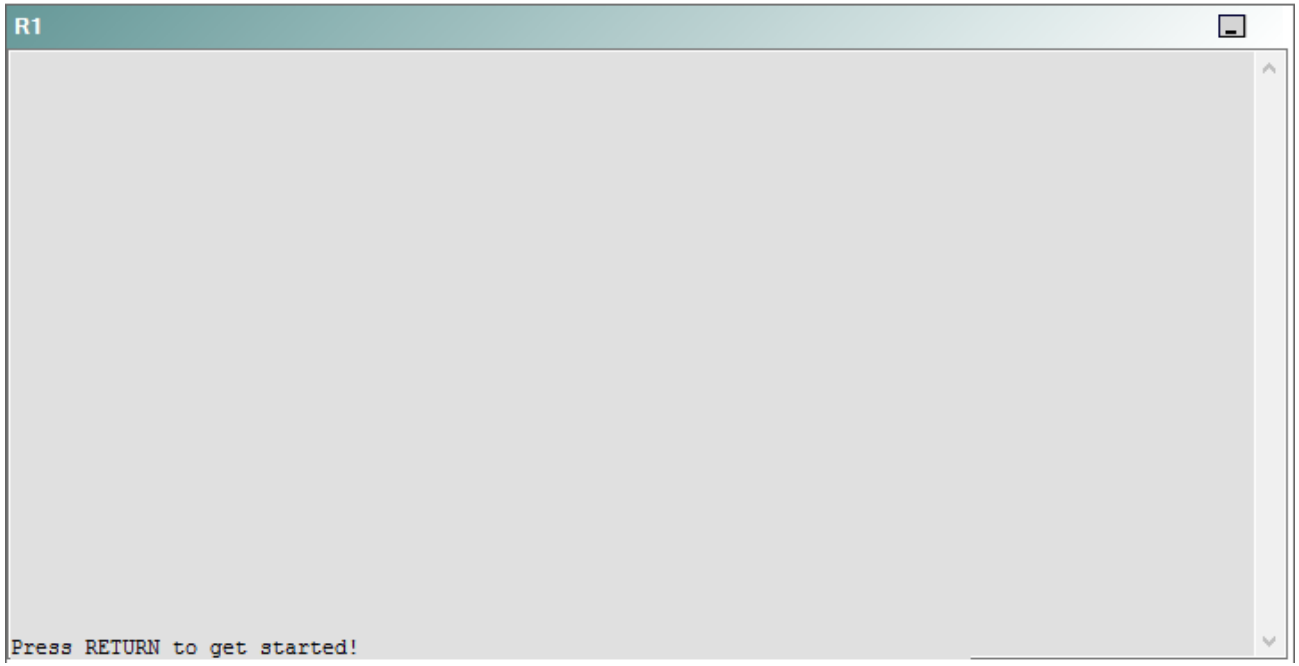

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

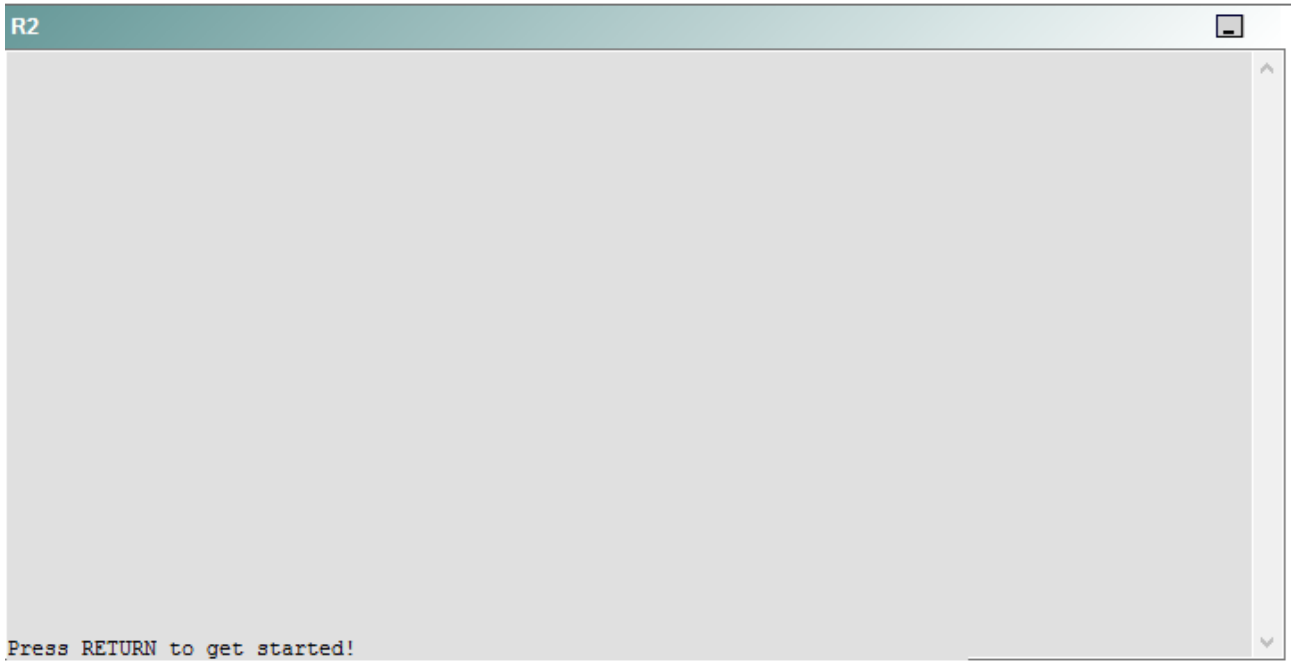



https://www.gratisexam.com/

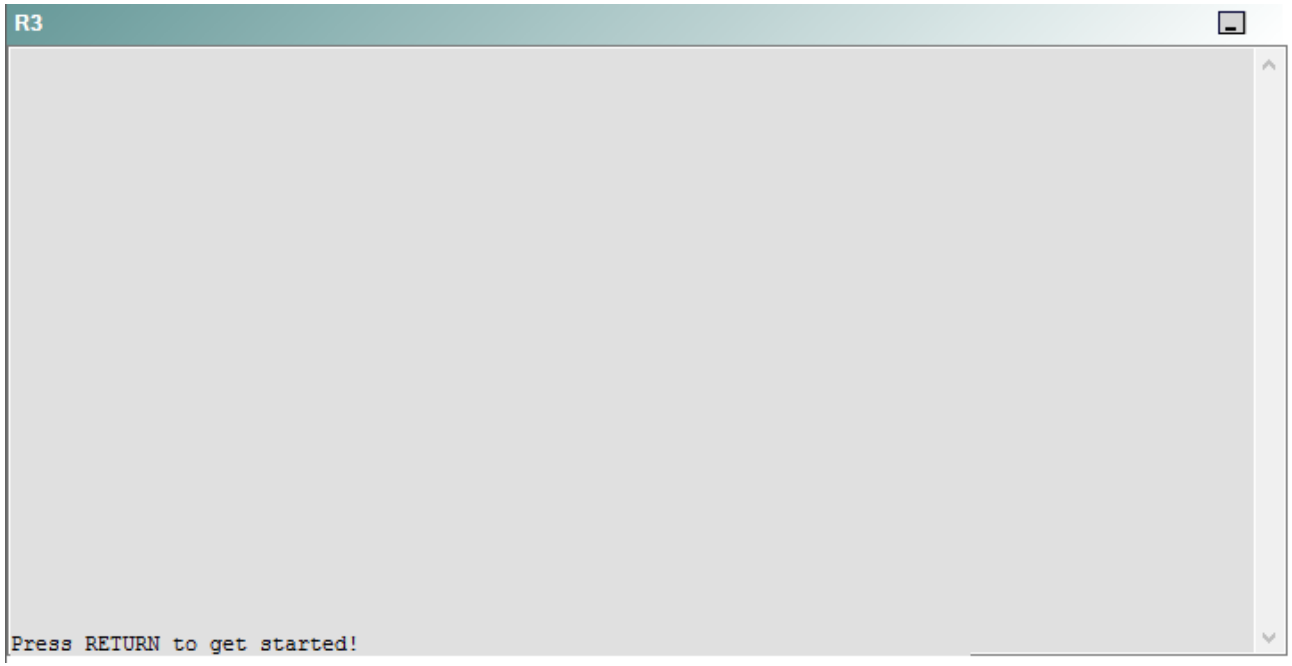
R1



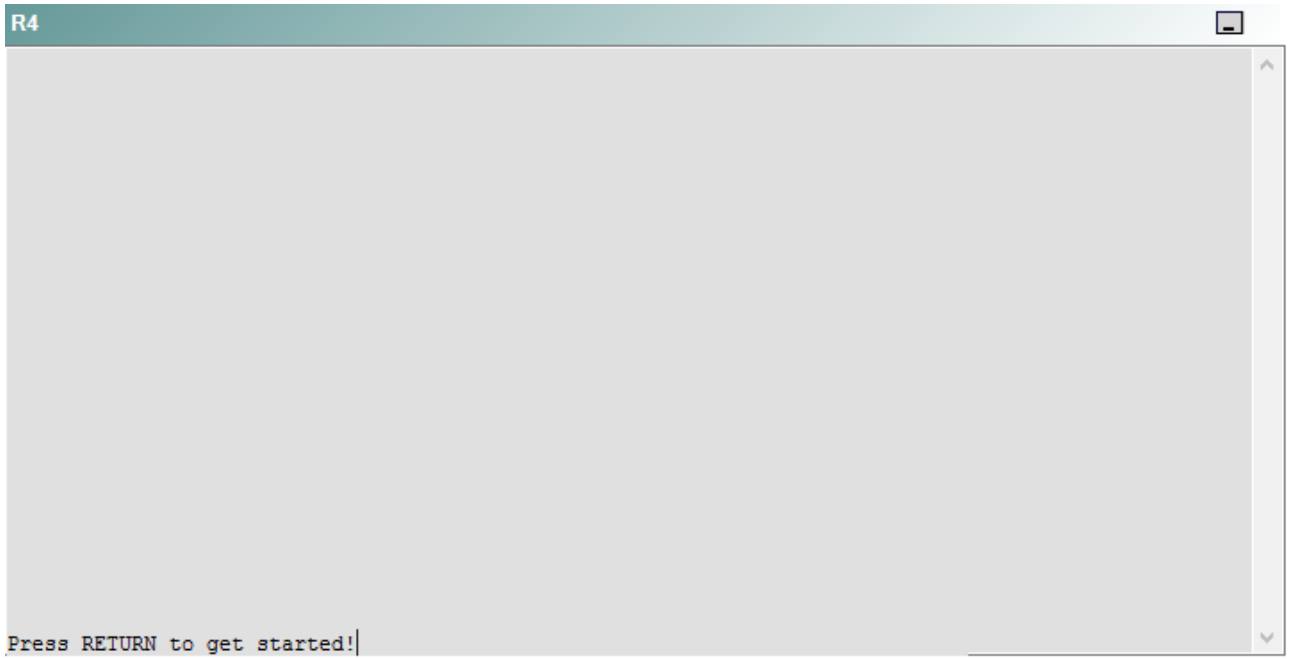

R2



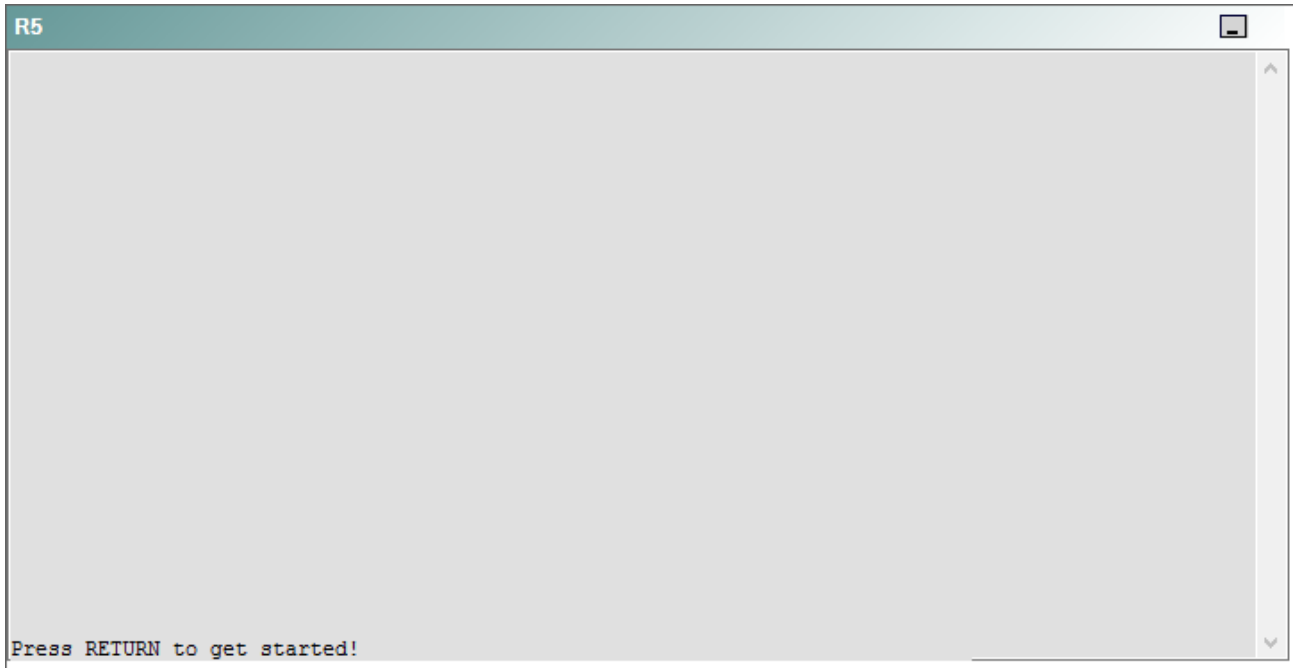

R3



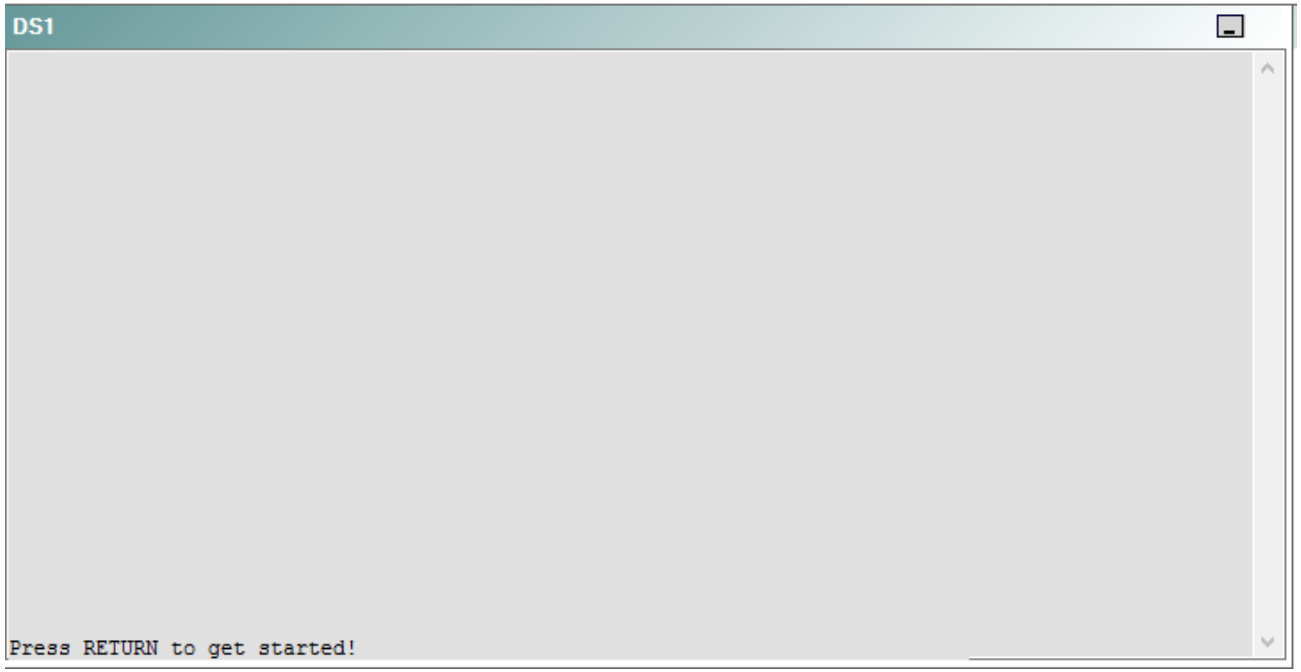

R4



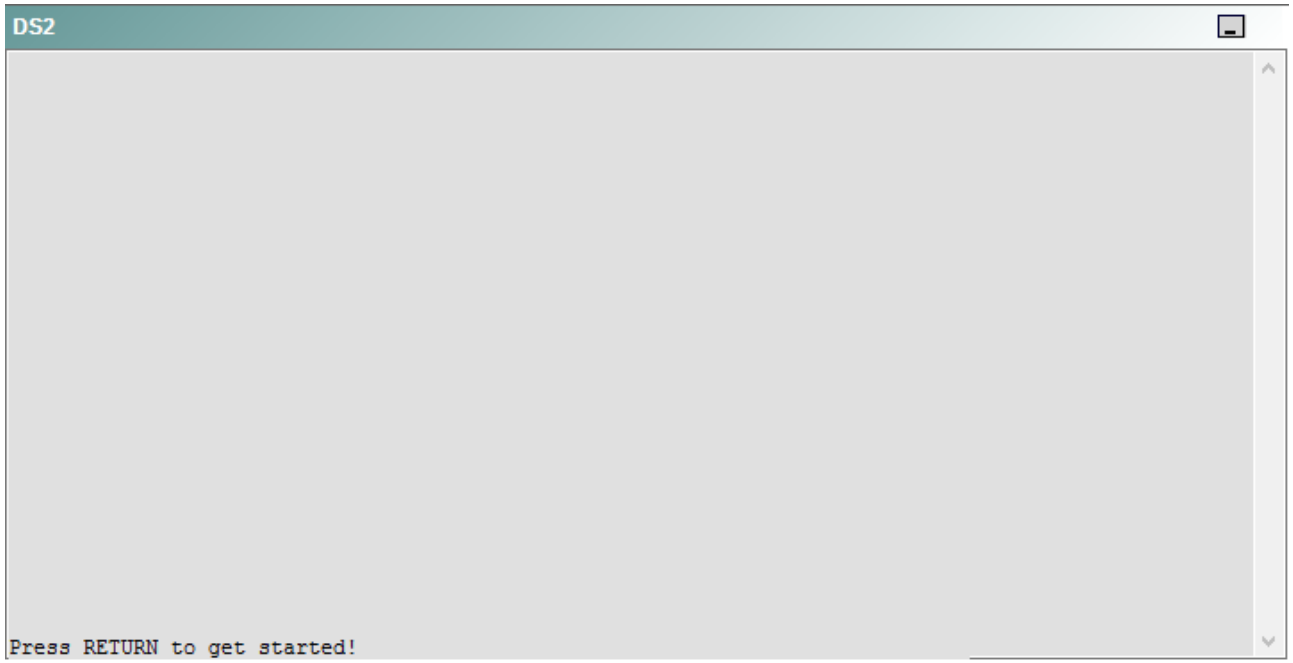

R5



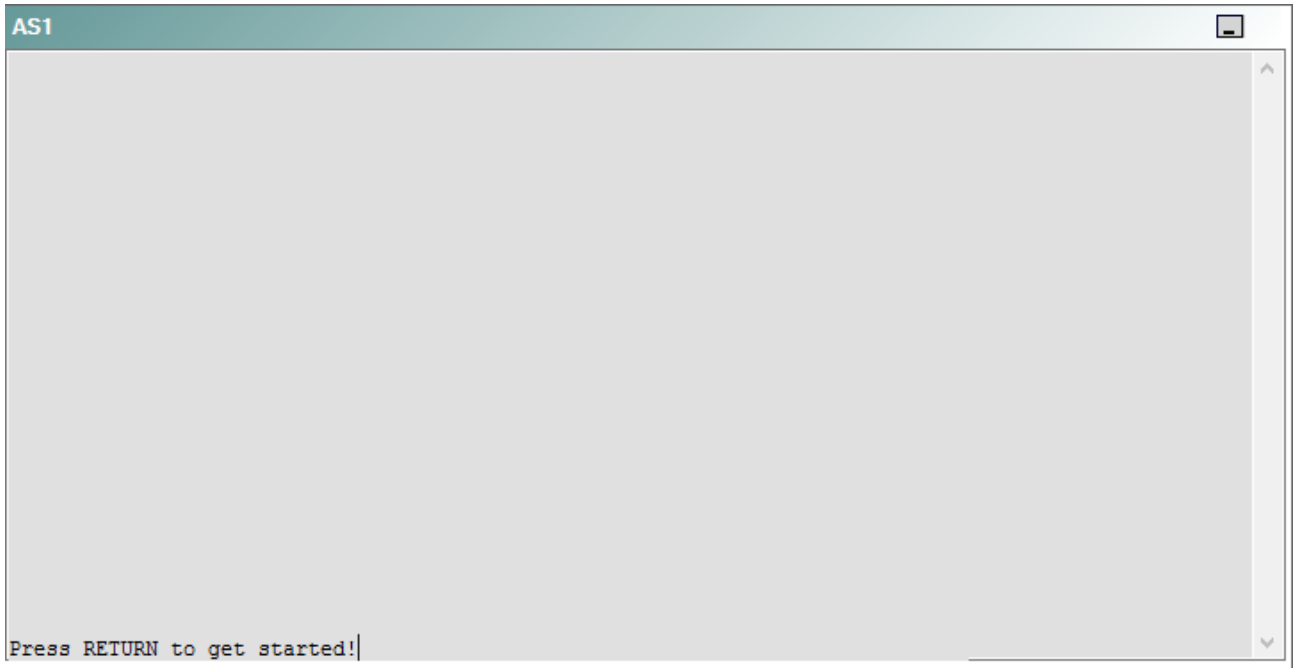

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. reconnecting the cable to the S1/0 interface
B. issuing the **no shutdown** command on the S1/0 interface
C. issuing the **no shutdown** command on the S1/0.322 and S1/0.324 subinterfaces
D. issuing the **clock rate 115200** command on the S1/0 interface
E. issuing the **encapsulation frame-relay** command on the S1/0.322 and S1/0.324 subinterfaces
F. creating Frame Relay maps on the S1/0.322 and S1/0.324 subinterfaces.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

You should issue the **clock rate 115200** command on the S1/0 interface of R3. To determine which device is the source of the problem, you can issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from PC1 to the closest device and work your way up the network until communication is lost, or you can ping from PC1 to the farthest device and work your way back to PC1 until pings are successful.

In this scenario, if you were to ping the E0/0 interface of R4 from PC1, the pings would be successful, as shown in the following output:

```
C:\>ping 192.168.1.13

Pinging 192.168.1.13 with 32 bytes of data:

Reply from 192.168.1.13: bytes=32 time=3ms TTL=253
Reply from 192.168.1.13: bytes=32 time=3ms TTL=253
Reply from 192.168.1.13: bytes=32 time=3ms TTL=253
Reply from 192.168.1.13: bytes=32 time=3ms TTL=253

Ping statistics for 192.168.1.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

However, if you were to ping the S1/0 interface of R4 from PC1, you would receive the following output:

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 10.10.22.22: Destination host unreachable.
Reply from 10.10.22.22: Destination host unreachable.
Reply from 10.10.22.22: Destination host unreachable.
Reply from 10.10.22.22: Destination host unreachable.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Therefore, the problem likely exists on R4 or beyond.

Once you have determined where connectively is lost, you can begin to troubleshoot what is causing the problem. Issuing the **show interfaces Serial 1/0** command on R4 reveals that the interface is up and the line protocol is up. However, issuing **the show interfaces Serial 1/0.423** command on R4 reveals that the subinterface is down and the line protocol is down, as shown in the following partial output:

```
R4#show interfaces Serial 1/0.423
Serial1/0.423 is down, line protocol is down
```

The interface status message `Serial1/0 is down, line protocol is down` often indicates that there is a problem at Layer 1 of the Open Systems Interconnection (OSI) model, which is the Physical layer. When you receive this interface status message, you should check both ends of the physical cable to see if they are securely connected to the proper interfaces. You can check whether the cable is disconnected from the S1/0 interface by issuing the **show controllers Serial 1/0** command. If no cable is connected to the interface, you will receive the following partial output:

```
R4#show controllers Serial 1/0
CD2430 Slot 1, Port 0, Controller 0, Channel 0, Revision 19
Channel mode is synchronous serial
idb 0x82B9EBC0, buffer size 1524, No cable
```

However, in this scenario, the data terminal equipment (DTE) end of the serial cable is connected to R4, as shown by the following partial output from the **show controllers Serial 1/0** command.

```
R4#show controllers Serial 1/0
CD2430 Slot 1, Port 0, Controller 0, Channel 0, Revision 19
Channel mode is synchronous serial
idb 0x82B9EBC0, buffer size 1524, V.35 DTE cable
```

Issuing the **show interfaces Serial 1/0** command on R3 reveals that the interface is up and the line protocol is down, as shown in the following partial output:

```
R3#show interfaces Serial 1/0
Serial1/0 is up, line protocol is down
```

The interface status message Serial1/0 is up, line protocol is down indicates that there is a problem at Layer 2 of the OSI model, which is the Data Link layer. If you receive this interface status message, you should check the encapsulation methods on the connected routers to ensure that they match. If the encapsulation methods match, you should check to ensure that the router connected to the data circuit-terminating equipment (DCE) end of the cable is providing clocking. To determine which end of the cable is connected to the router, you should issue the **show controllers Serial 1/0** command. If you were to issue the **show controllers Serial 1/0** command on R3, you would receive the following partial output:

```
R3#show controllers Serial 1/0
CD2430 Slot 1, Port 0, Controller 0, Channel 0, Revision 19
Channel mode is synchronous serial
idb 0x82BA5FF4, buffer size 1524, V.35 DCE cable
```

The DCE end of the serial cable typically provides clocking, and the DTE end of the serial cable does not. Issuing the **show running-config** command on R3 reveals that the **clock rate** command is missing on the S1/0 interface. To enable clocking on the interface, you should issue the clock rate bps command in interface configuration mode, where *bps* is the **clock rate** in bits per second. After you issue the **clock rate 115200** command on R3, the output from the **show interfaces Serial1/0** command on R3 and R4 will display the interface status message *Serial1/0 is up, line protocol is up.*

You should not enable clocking on the S1/0 interface of R4. The output of **the show controllers Serial 1/0** command on R4 indicates that the DTE end of the cable is connected to R4. Therefore, R4 does not need to provide clocking.

You do not need to issue the **no shutdown** command on the S1/0 interface of R3. The **no shutdown** command is used to enable an interface that has been administratively shut down by the **shutdown** command. If the interface had been administratively shut down, you would have seen the following partial output from the **show interfaces Serial 1/0** command:

```
R3#show interfaces Serial 1/0
Serial1/0 is administratively down, line protocol is down
```

You cannot issue the **encapsulation frame-relay** command on the subinterfaces of R3. The **encapsulation frame-relay** command can be issued only on the S1/0

interface.

You should not create Frame Relay maps on the subinterfaces. Frame Relay maps cannot be created on point-to-point subinterfaces. To create a Frame Relay map, you would issue the **frame-relay map ip** *ip-address dlci* [**broadcast**] [ **ietf** | **cisco**] command.

You need not change the data link connection identifier (DLCI) on the subinterfaces. A DLCI is an address that uniquely identifies a permanent virtual circuit (PVC) connection in a Frame Relay circuit. Each DLCI is locally significant, which means that the routers at each end of the PVC can use different DLCIs to identify the same circuit.

You need no change the interface type to point-to-multipoint on the subinterfaces. The S1/0 interface on R3 is currently configured so that it can communicate only with its upstream and downstream routers, not with all the routers attached to the Frame Relay cloud. If you were to change the interface type to point-to-multipoint, you would also have to configure Frame Relay maps. To configure the interface type for a subinterface, you would issue the **interface** *type slot/ port.subinterface* [**multipoint** | **point-to-point**] command.

Reference:
https://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1915.html#wp1020558

**QUESTION 9**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

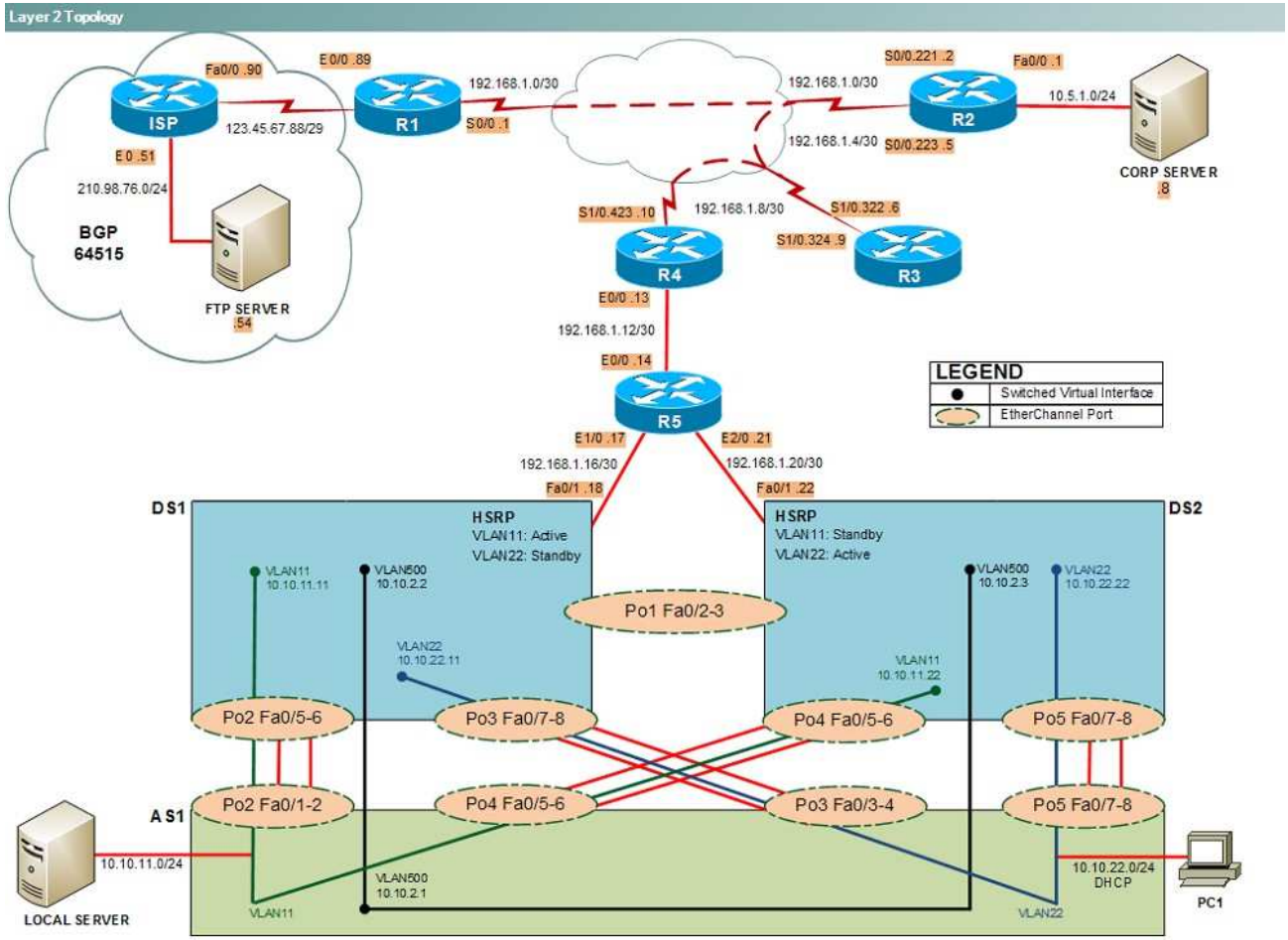
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

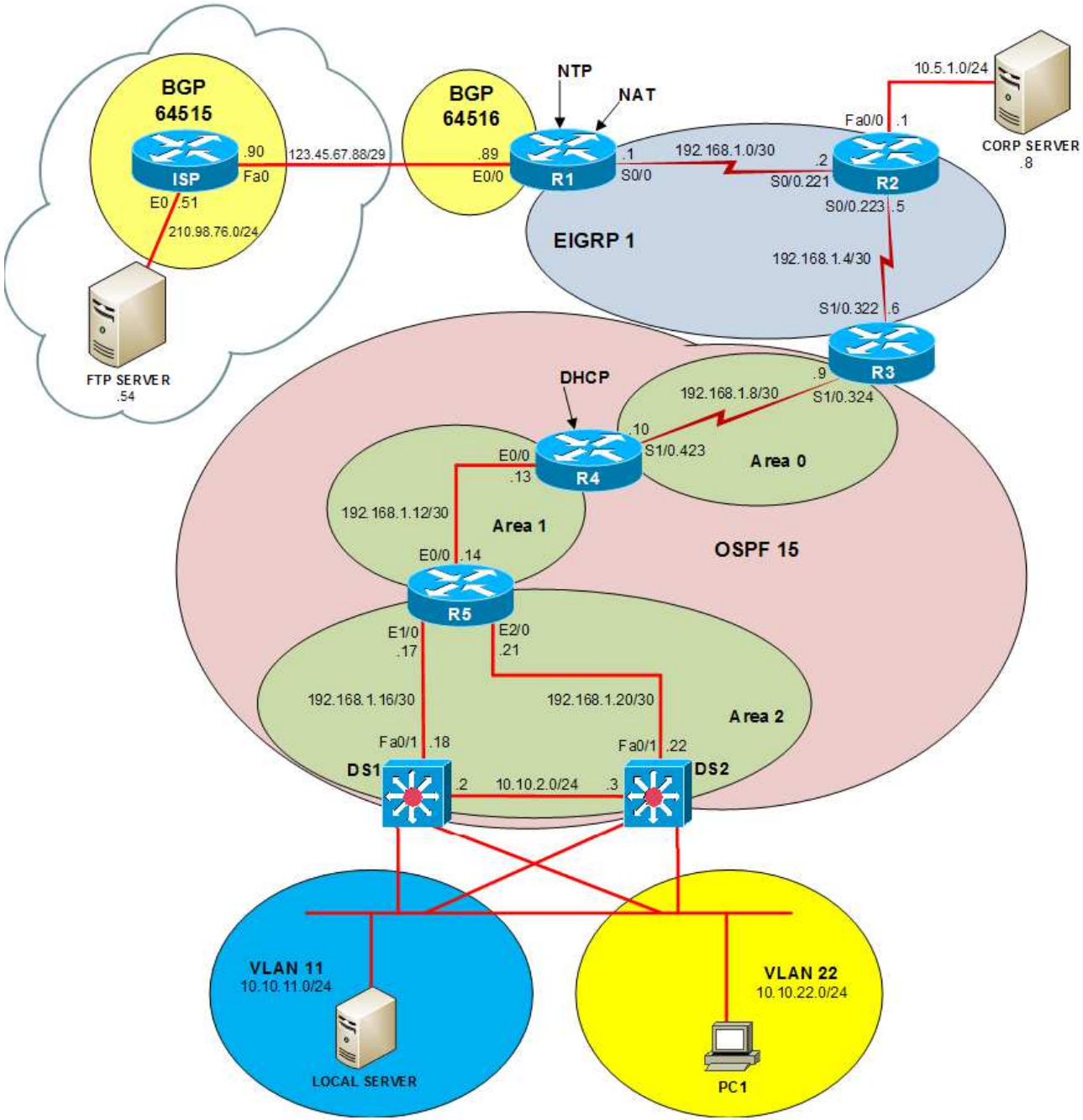
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

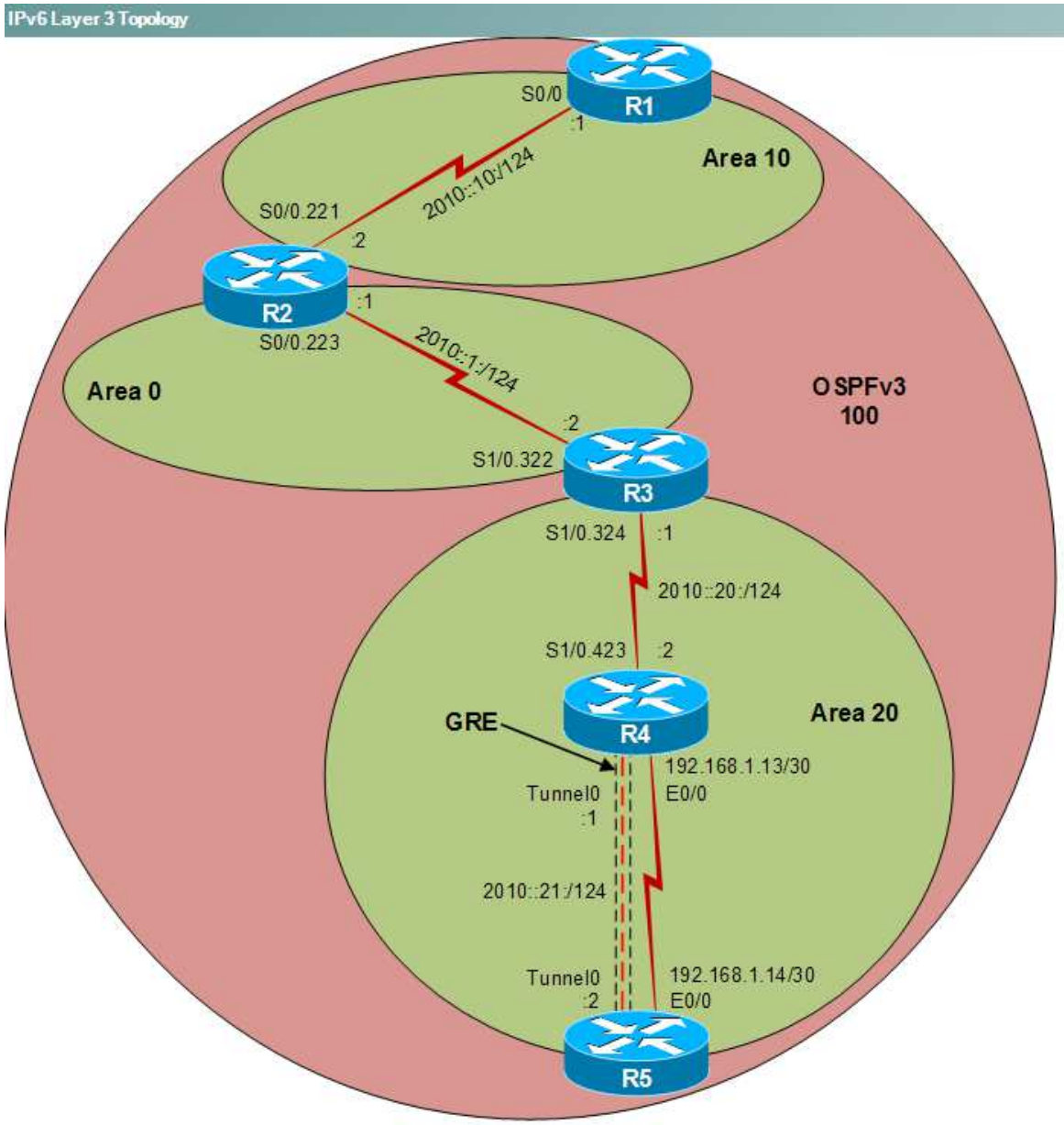
**Layer 2 Topology**



IPv4 layer 3 Topology

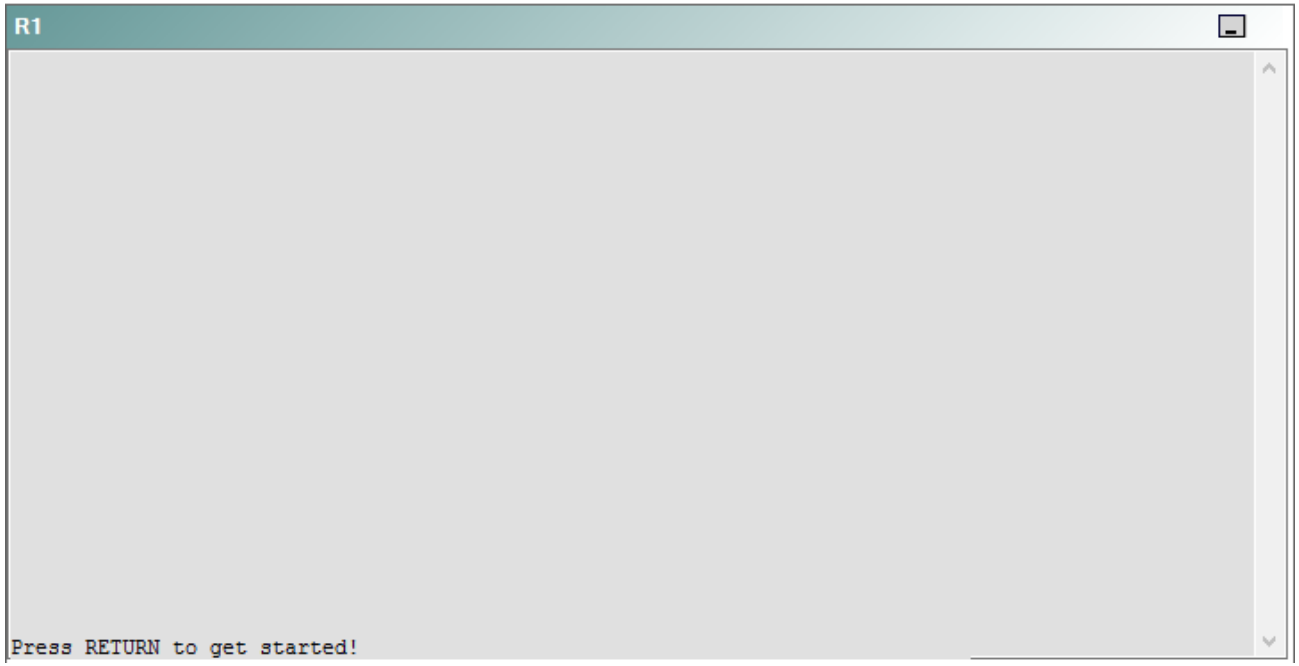

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

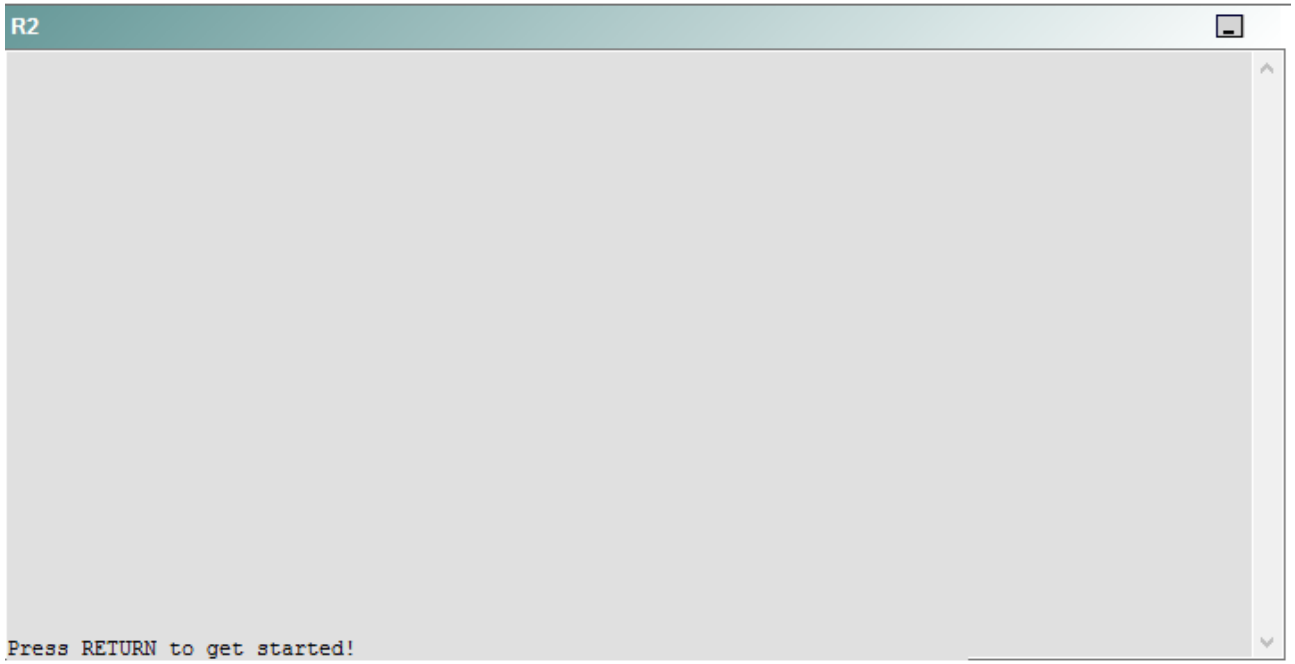



https://www.gratisexam.com/

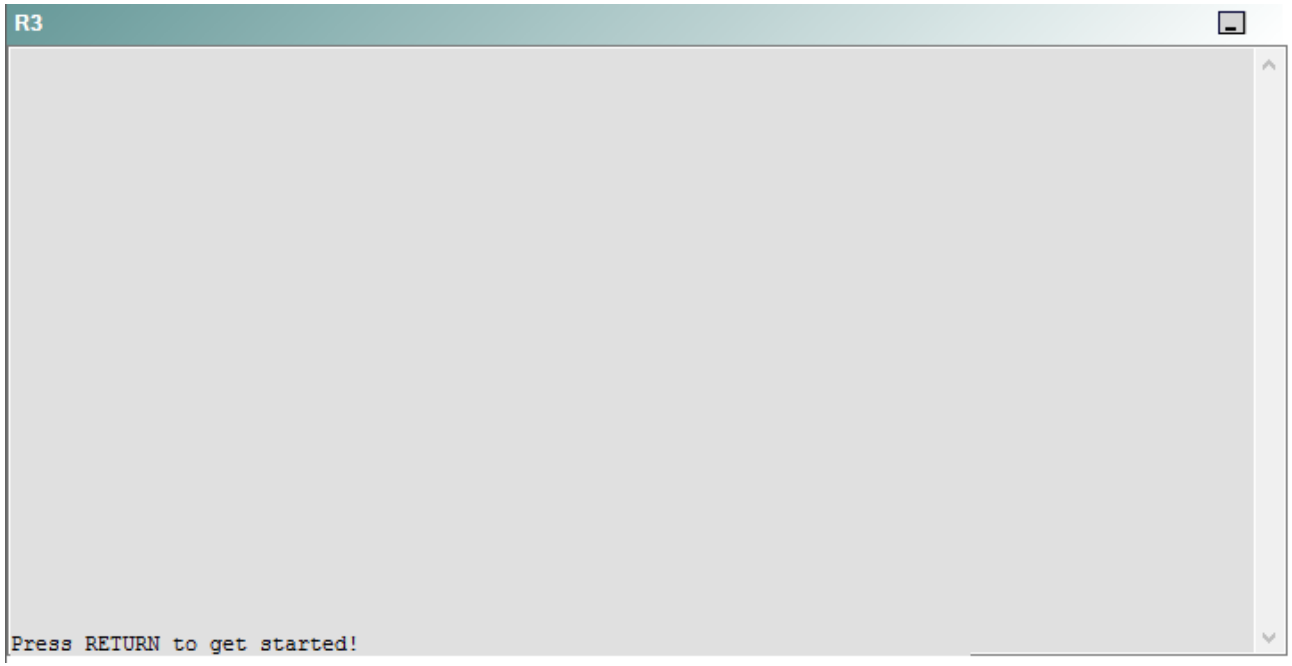
R1



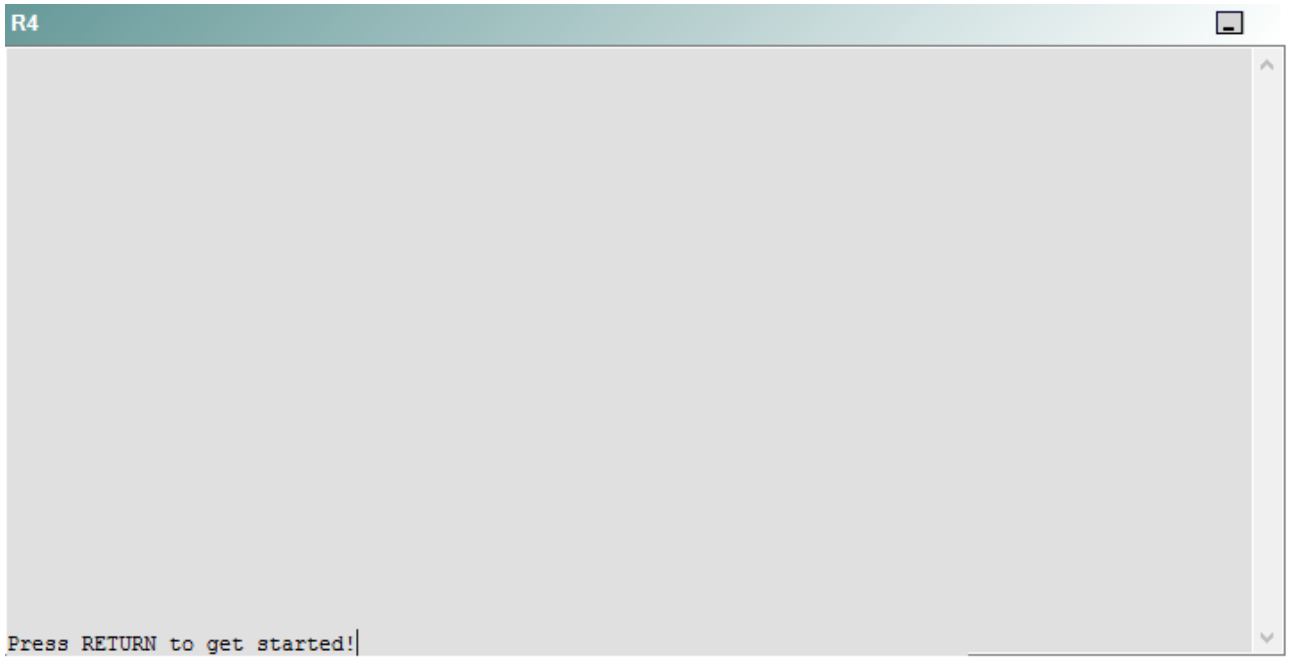

R2



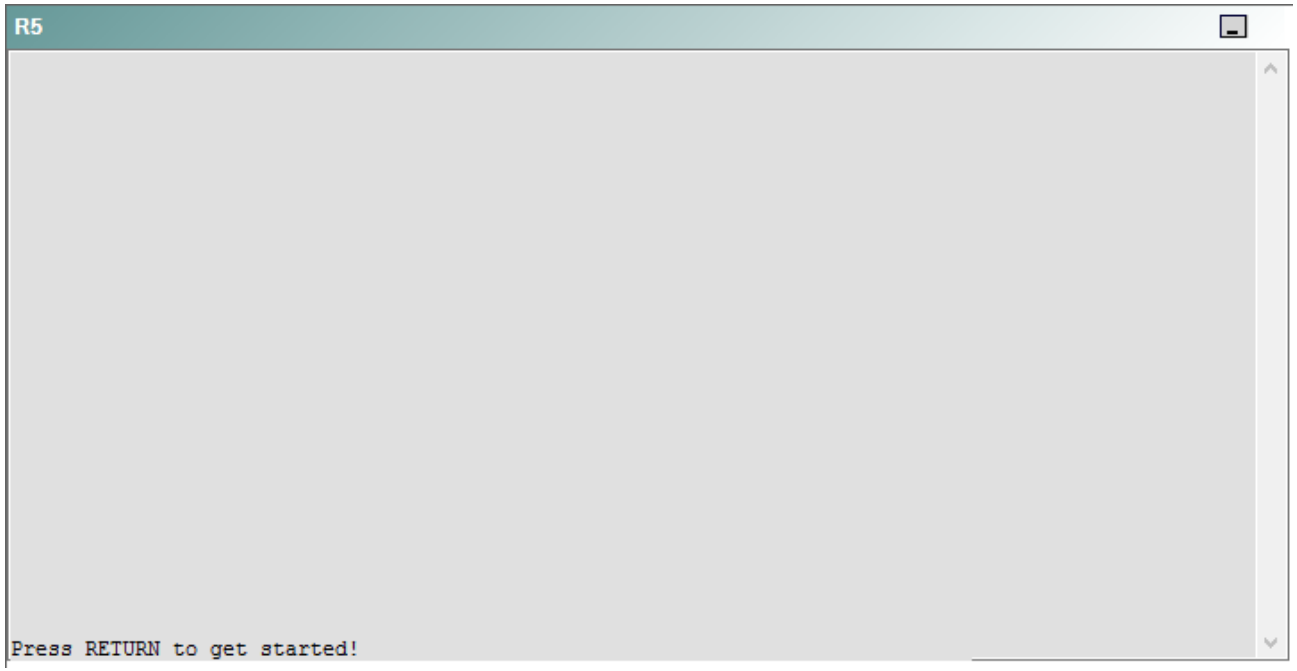

R3



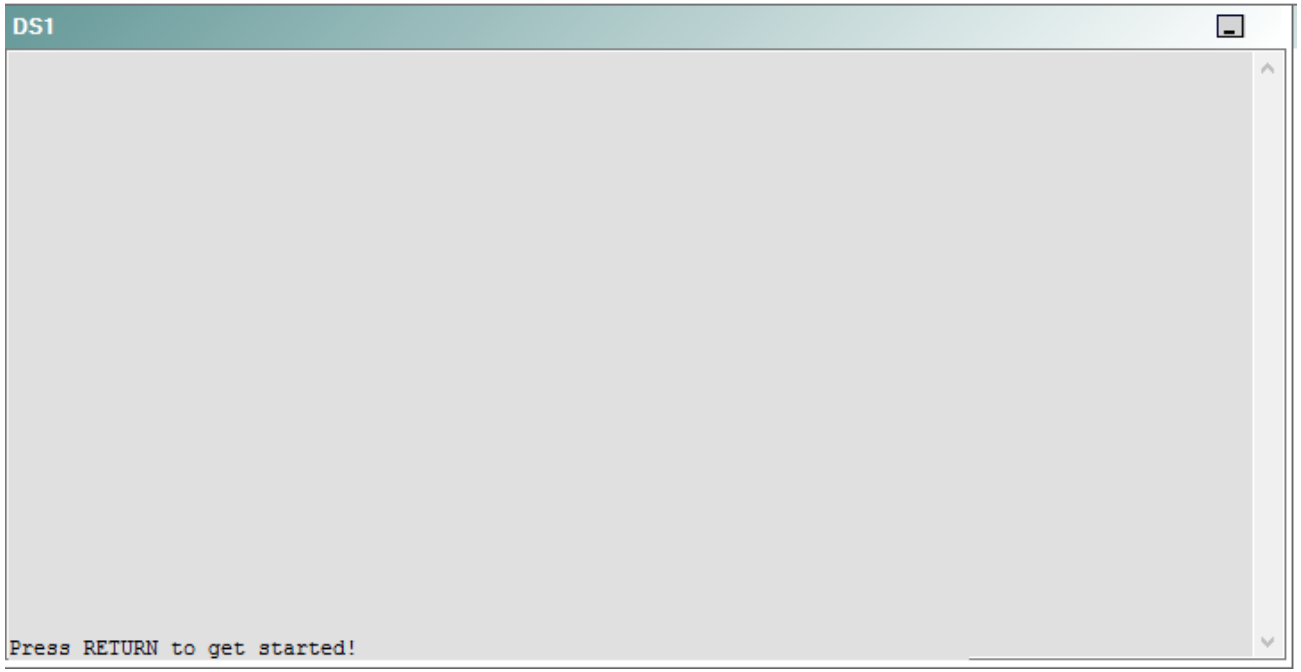

R4



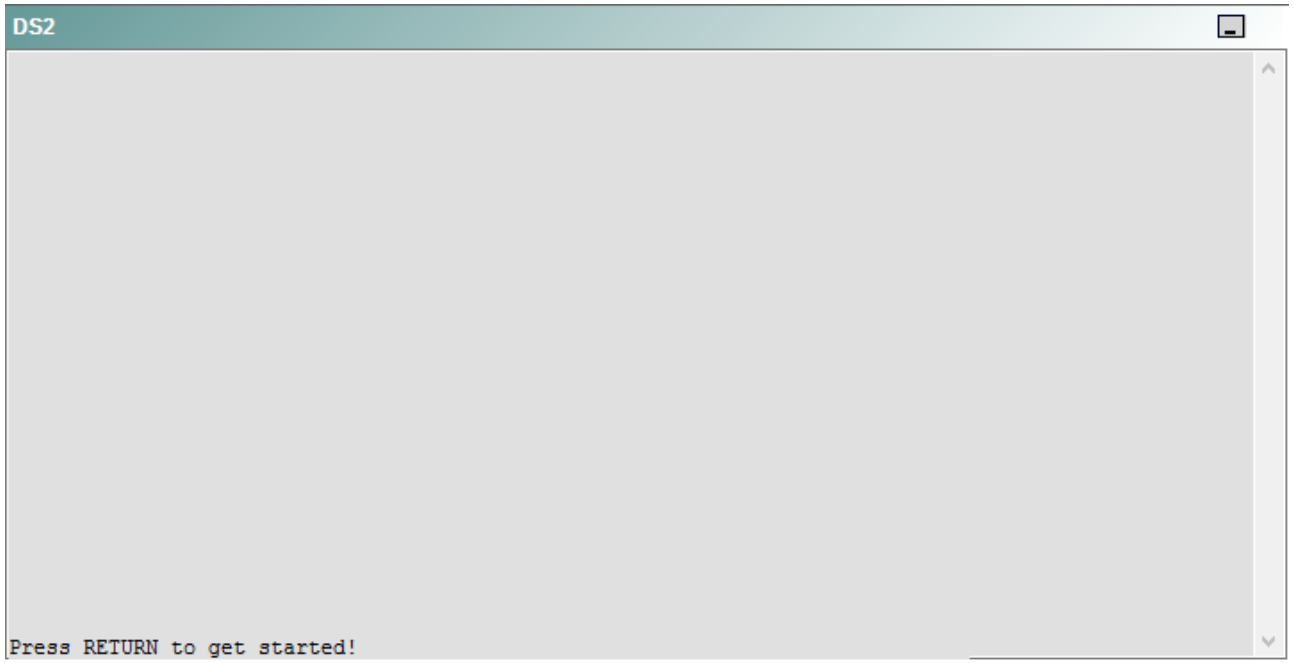

R5



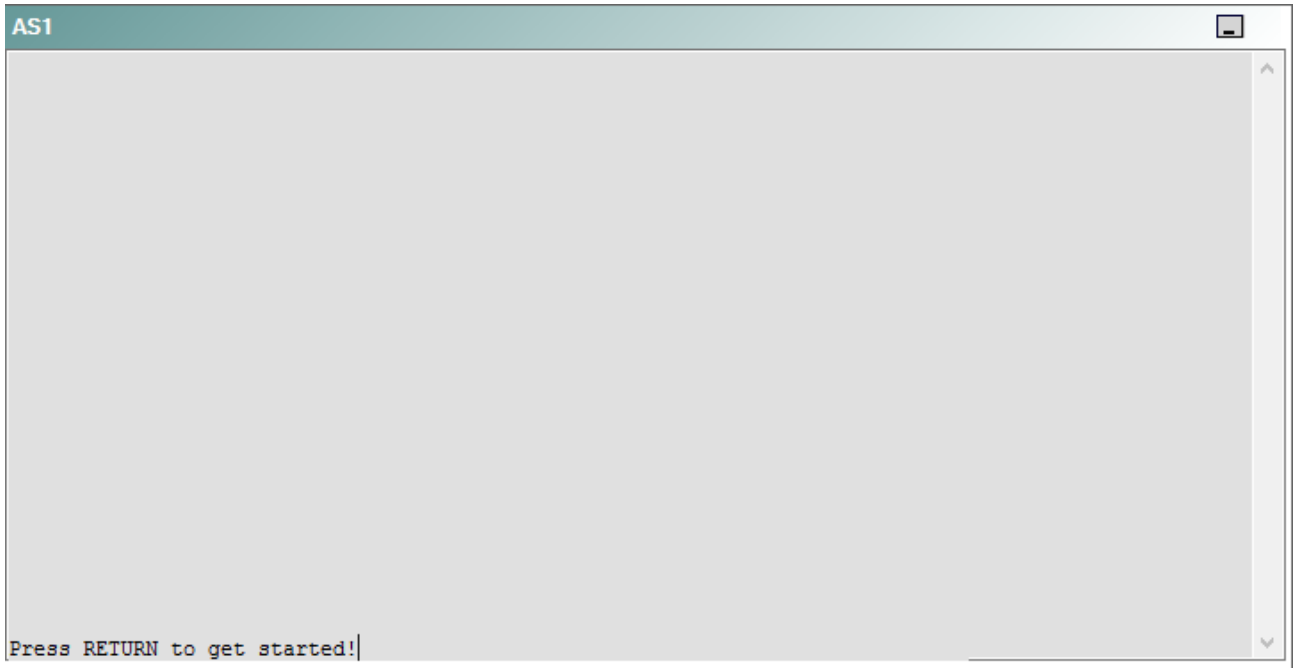

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. issuing the **redistribute eigrp 1 metric 64 subnets route-map eigrp-to-ospf** command in OSPF
B. issuing the **redistribute eigrp 1 metric 64 subnets route-map ospf-to-eigrp** command in OSPF
C. issuing the **default-metric 1000 100 255 1 1500** command in EIGRP
D. issuing the **no redistribute static** command in the OSPF 15 process
E. issuing the **redistribute ospf 15 route-map eigrp-to-ospf** command in EIGRP
F. issuing the **redistribute ospf 15 route-map ospf-to-eigrp** command in EIGRP

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

You should issue the **default-metric 1000 100 255 1 1500** command in Enhanced Interior Gateway Routing Protocol (EIGRP) on R3. To determine which device is the source of the problem, you should issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from R5 to the closest device and work your way up the network until communication is lost, or you can ping from R5 to the farthest device and work your way back to R5 until pings are successful. Alternatively, you can trace from R5 to R1 and see where communication is lost along the path to the destination device.

In this scenario, if you were to issue the **traceroute 210.98.76.74** command from R5, you would receive the following partial output:

```
Type escape sequence to abort.
Tracing the route to 210.98.76.54

  1 192.168.1.13 4 msec 0 msec 4 msec
  2 192.168.1.9 16 msec 20 msec 16 msec
  3  *  *  *
  4  *  *  *
```

The *** in the output indicates that the attempt to trace the IP address 210.98.76,54 timed out after the hop at IP address 192.168.1.9, which is the IP address assigned to the Serial1/0.324 subinterface on R3. All routers above R3 are able to ping and trace to 210.98.76.54. Additionally, if you were to issue the **traceroute 10.10.22.31** command from R2, you would receive the following partial output:

```
Type escape sequence to abort.
Tracing the route to 10.10.22.31

  1 192.168.1.1 16 msec 20 msec 16 msec
  2 123.45.67.90 24 msec 20 msec 20 msec
  3 123.45.67.90 !H  !H  !H
```

The `!H !H !H` in the output above indicates that the host at IP address 10.10.22.31, which is the IP address assigned to PC1 by the Dynamic Host Configuration Protocol (DHCP) server on R5, is unreachable, although there is a route available to that host. The trace reports that the host is unreachable after the IP address 123.45.67.90, which indicates that R2 is attempting to access 10.10.22.31 by a route out R1 and through the public network rather than through R3, which is the correct route to PC1. Because R2 cannot ping or trace below R3 and because R5 cannot ping and trace above R3, the most likely point of connectivity loss in the network is R3, even though R3 can ping and trace to both sides of the network.

Once you have determined where connectivity is lost, you can begin to troubleshoot the cause of the problem. There are two routing protocols that are operating at the Network layer of the OSI model on R3: EIGRP and Open Shortest Path First (OSPF). To determine which protocol is most likely causing the problem, you should verify the configuration and operation of each protocol. If you were to issue the **show ip route** command on R3, you would receive the following output:

```
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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 192.168.1.5 to network 0.0.0.0

     192.168.99.0/32 is subnetted, 7 subnets
C       192.168.99.3 is directly connected, Loopback0
D       192.168.99.2 [90/20640000] via 192.168.1.5, 00:14:49, Serial1/0.322
D       192.168.99.1 [90/21152000] via 192.168.1.5, 00:14:49, Serial1/0.322
O IA    192.168.99.7 [110/802] via 192.168.1.10, 00:14:38, Serial1/0.324
O IA    192.168.99.6 [110/803] via 192.168.1.10, 00:14:38, Serial1/0.324
O IA    192.168.99.5 [110/792] via 192.168.1.10, 00:14:38, Serial1/0.324
O IA    192.168.99.4 [110/782] via 192.168.1.10, 00:14:38, Serial1/0.324
     10.0.0.0/24 is subnetted, 3 subnets
O IA    10.10.11.0 [110/802] via 192.168.1.10, 00:14:38, Serial1/0.324
D       10.5.1.0 [90/20514560] via 192.168.1.5, 00:14:49, Serial1/0.322
O IA    10.10.22.0 [110/802] via 192.168.1.10, 00:14:38, Serial1/0.324
     192.168.1.0/30 is subnetted, 6 subnets
C       192.168.1.8 is directly connected, Serial1/0.324
O IA    192.168.1.12 [110/791] via 192.168.1.10, 00:14:38, Serial1/0.324
D       192.168.1.0 [90/21024000] via 192.168.1.5, 00:14:50, Serial1/0.322
C       192.168.1.4 is directly connected, Serial1/0.322
O IA    192.168.1.16 [110/801] via 192.168.1.10, 00:14:39, Serial1/0.324
O IA    192.168.1.20 [110/801] via 192.168.1.10, 00:14:39, Serial1/0.324
D*EX 0.0.0.0/0 [170/21049600] via 192.168.1.5, 00:14:50, Serial1/0.322
```

The output above indicates that all subnets in the network are accounted for on R3. Two subnets are directly connected routes. Three subnets above R3, including the default 0.0.0.0/0 route, are routed by EIGRP process 1. Nine subnets below R3 are routed by OSPF process 15. Because all of the networks connected to R3 are accounted for in the routing table and are segregated by the EIGRP and OSF boundaries on R3, you should ensure that routing redistribution between EIGRP process 1 and OSPF process 15 is correctly configured.

If you were to issue the **show running-config** command on R3, you would receive the following partial output:

```
router eigrp 1
 redistribute ospf 15 route-map ospf-to-eigrp
 network 192.168.1.4 0.0.0.3
 network 192.168.99.3 0.0.0.0
 no auto-summary
!
router ospf 15
 router-id 1.2.3.4
 log-adjacency-changes
 redistribute static
 redistribute eigrp 1 metric 64 subnets route-map eigrp-to-ospf
 network 192.168.1.8 0.0.0.3 area 0
 default-information originate always
!
route-map ospf-to-eigrp deny 10
 match tag 20
 match route-type external type-2
!
route-map ospf-to-eigrp permit 20
 match ip address prefix-list intpfxs
!
route-map ospf-to-eigrp permit 30
 set tag 8
!
route-map eigrp-to-ospf deny 10
 match tag 8
!
route-map eigrp-to-ospf permit 20
 match ip address prefix-list intpfxs
!
route-map eigrp-to-ospf permit 30
 set tag 20
```

In the output above, the EIGRP 1 routing proves has been configured to redistribute routes from the OSPF 15 process based on permit and deny rules found in a route map named ospf-to-eigrp. Similarly, the OSPF 15 routing process has been configured to redistribute routed from the EIGRP 1 process based on information in a route map named eigrp-to-ospf. The difference between two configurations is that the OSPF process has defined a seed metric of 64 in the **redistribute eigrp** command and the EIGRP process has no seed metric. Routing protocols differ in the types of metrics they use to route traffic. As a result, a seed metric is required in order to inform one protocol of the metric necessary to redistribute routing information from the other protocol. Seed metrics can be defined by issuing the **default-metric** command in the routing process configuration, by issuing the **metric** keyword in the **redistribution** command, or by configuring a route map. The route map in this scenario do not provide seed metrics, and no **metric** keyword has been issued for the **redistribute eigrp** command. Therefore, issuing the **default-metric 1000 100 255 1 1500** command in the EIGRP 1 routing process configuration would solve the problem.

You should not issue the **redistribute eigrp 1 metric 64 subnets route-map eigrp-to-ospf** command or the **redistribute eigrp 1 metric 64 subnets route-map ospf-to-eigrp** command in OSPF on R3. There are two route maps configured on R3, eigrp-to-ospf and ospf-to-eigrp. The eigrp-to-ospf route map applies to routes from EIGRP process 1 that are redistributed into OSPF process 15. The ospf-to-eigrp route map applies to routes from OSPF process 15 that are redistributed into EIGRP process 1. In this scenario, the route maps are already correctly assigned to the appropriate **redistribute** command.

You need not issue the **no redistribute static** command on any device. Although the **redistribute static** command is not necessary on R3, because there are no static routes defined on R3, issuing the **no redistribute static** command would not fix the redistribution problem between EIGRP and OSPF on R3.

You should not issue the **redistribute ospf 15 route-map eigrp-to-ospf** command or the **redistribute ospf 15 route-map ospf-to-eigrp** command in EIGRP on R3. Modifying the route map assignments in this scenario would not fix redistribution between EIGRP and OSPF, because the route maps are already correctly assigned to the appropriate **redistribute** command.

Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/command/ire-cr-book/ire-a1.html#wp3025014087

**QUESTION 10**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s

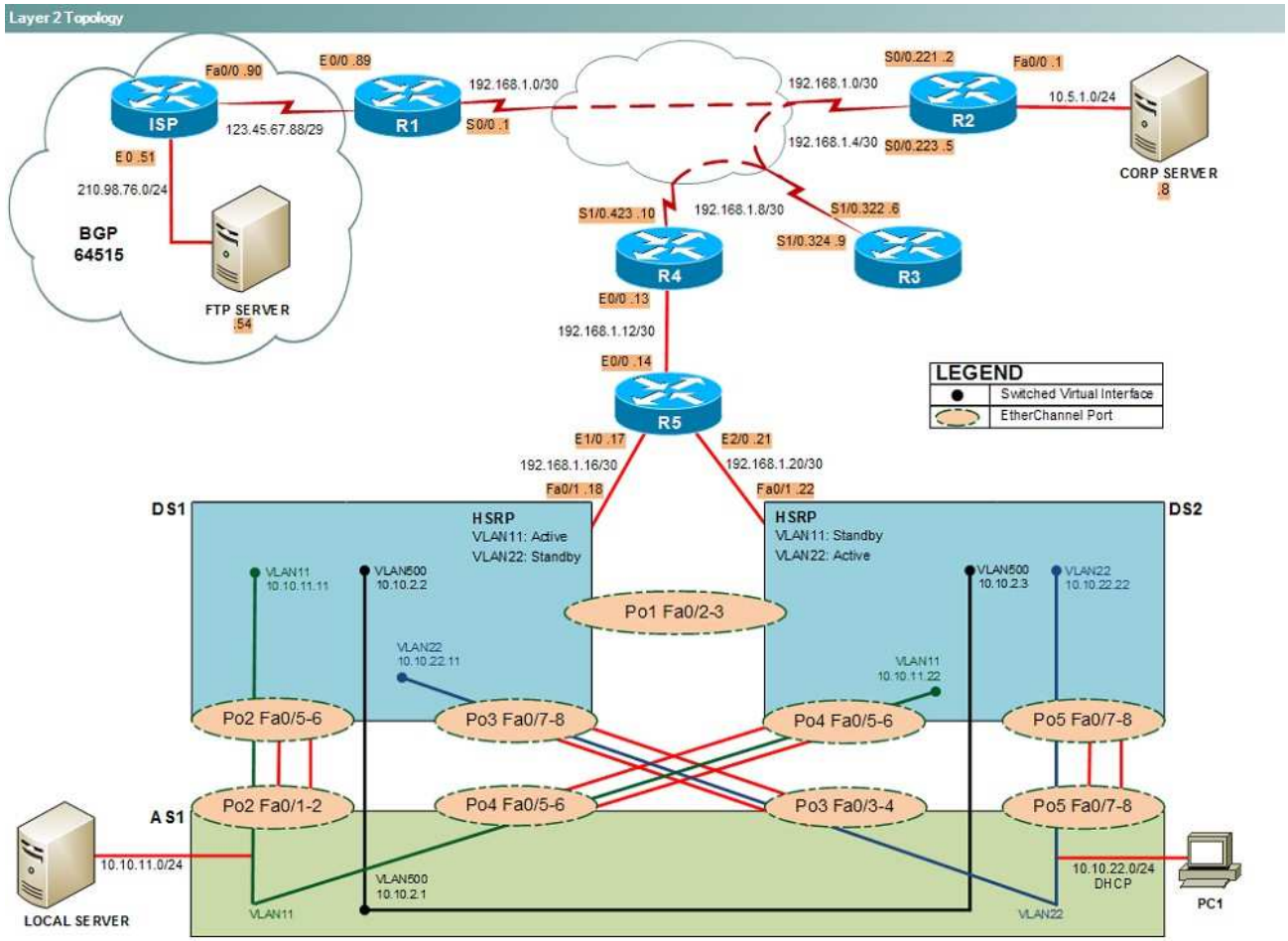
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

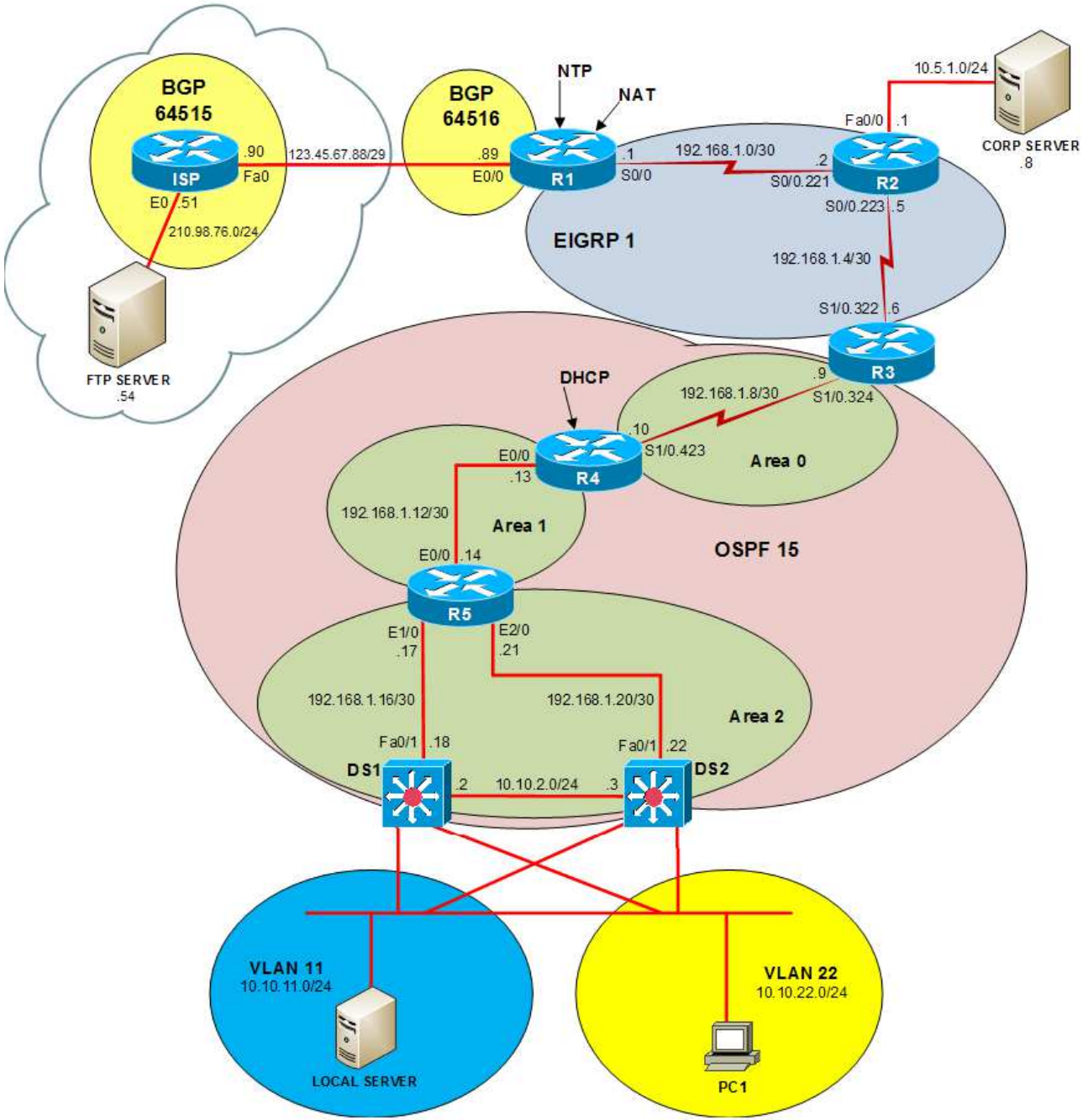
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

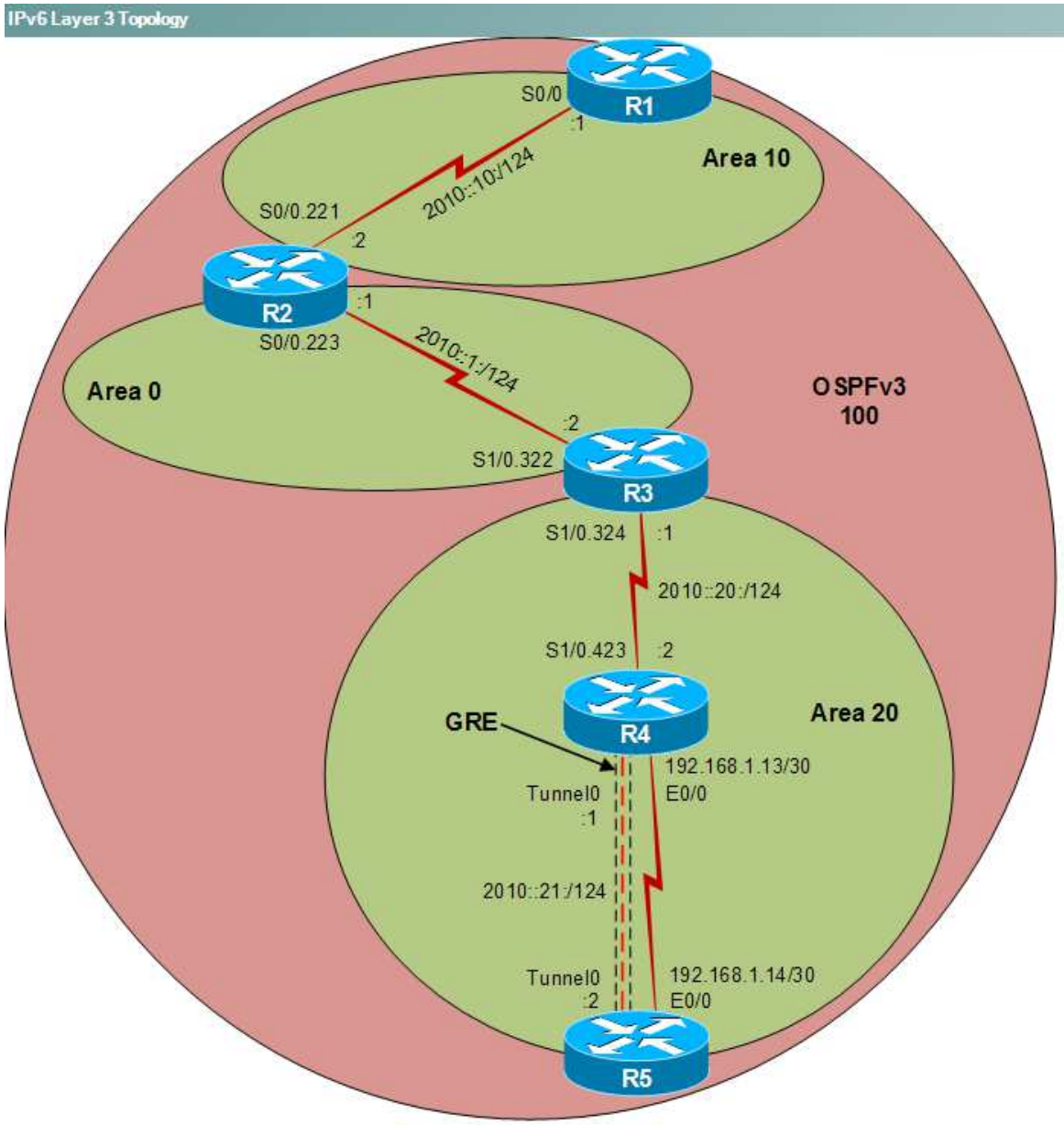
**Layer 2 Topology**




IPv4 layer 3 Topology

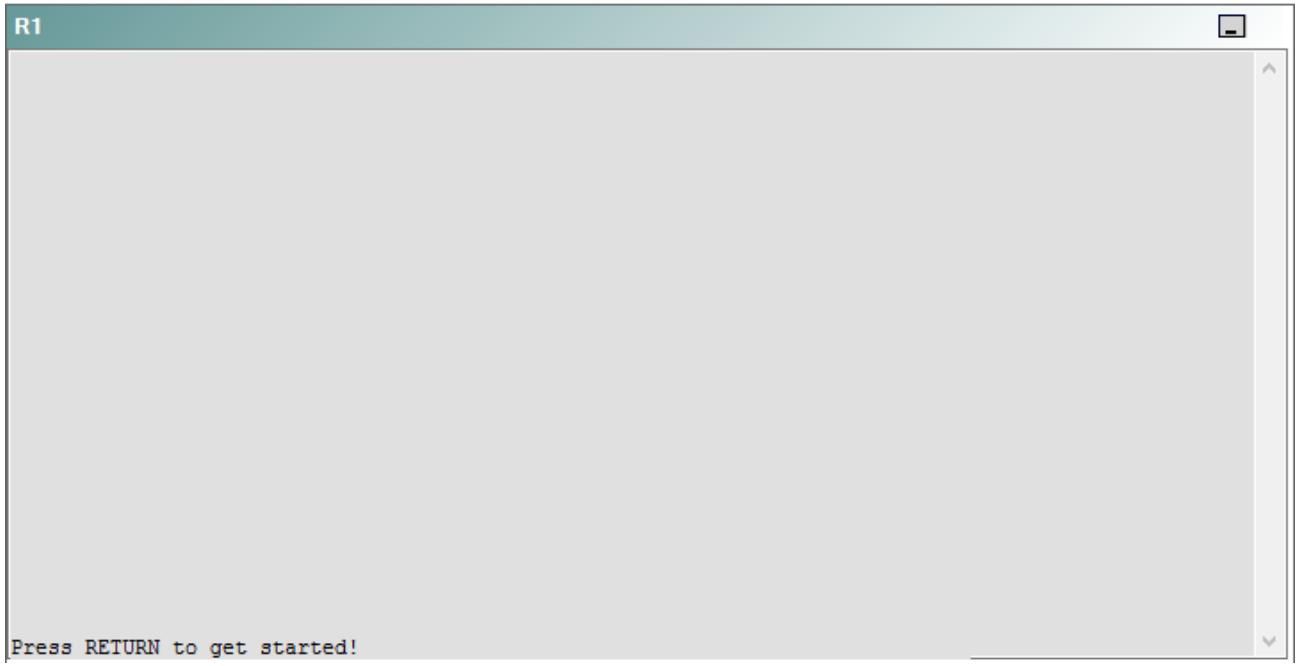

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

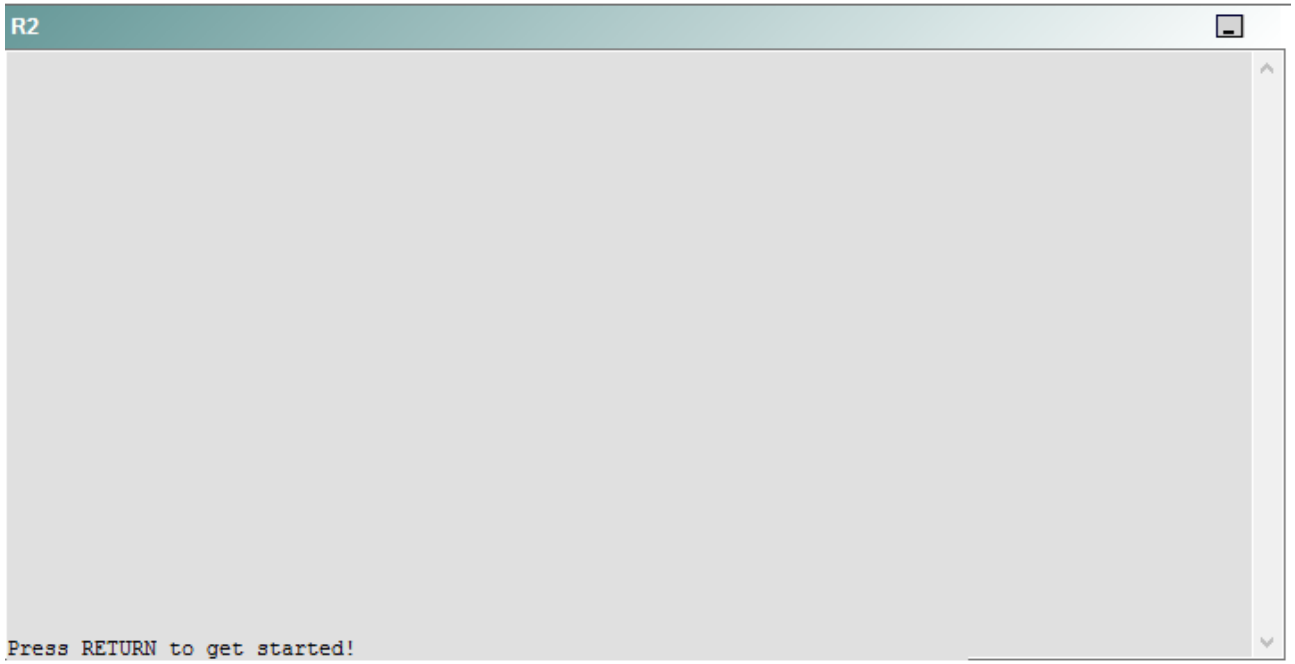



https://www.gratisexam.com/

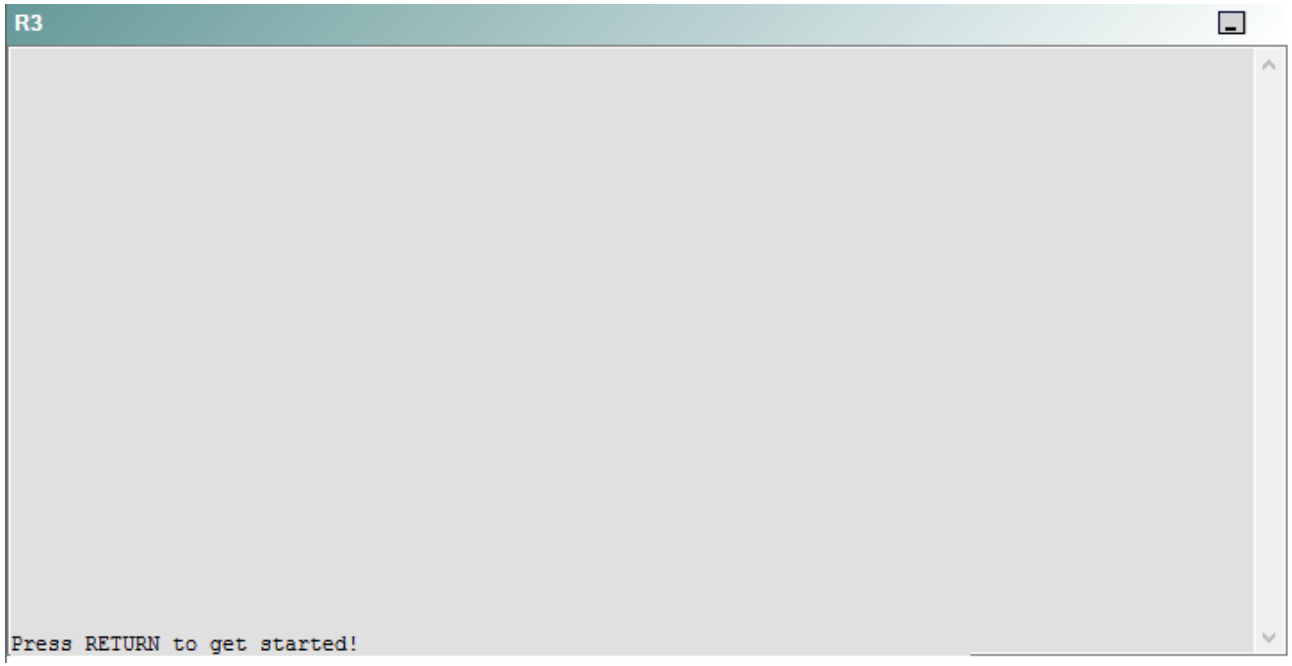
R1



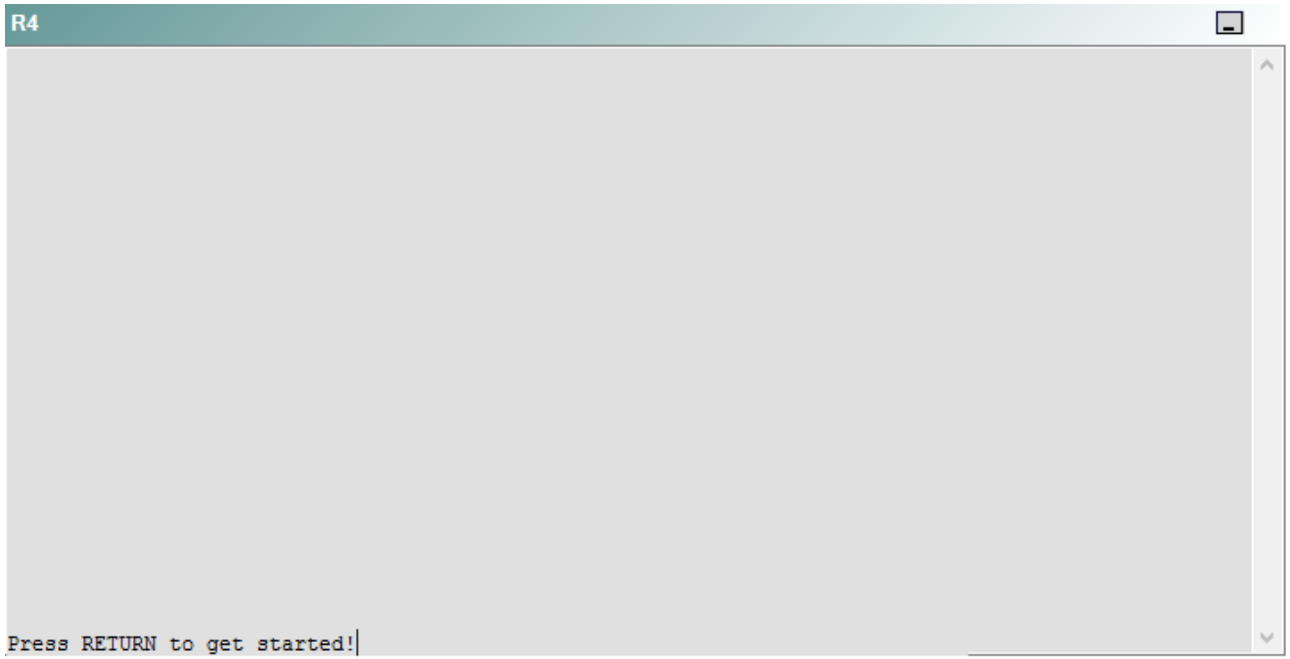

R2



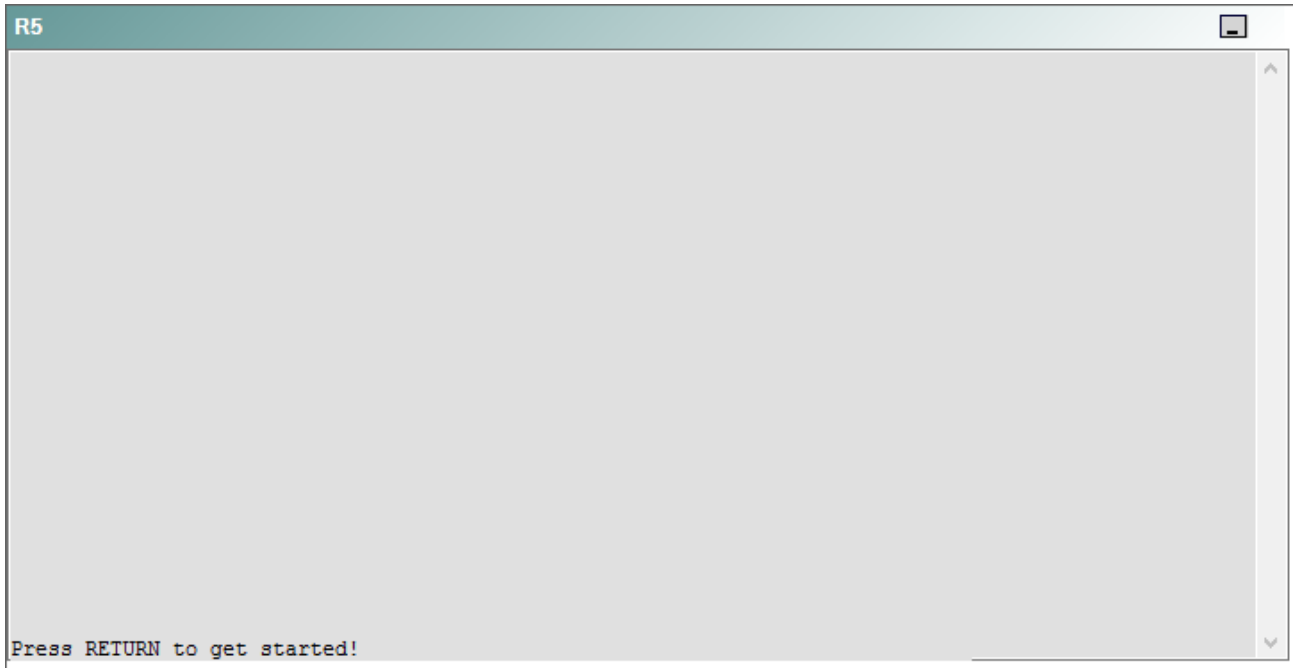

R3



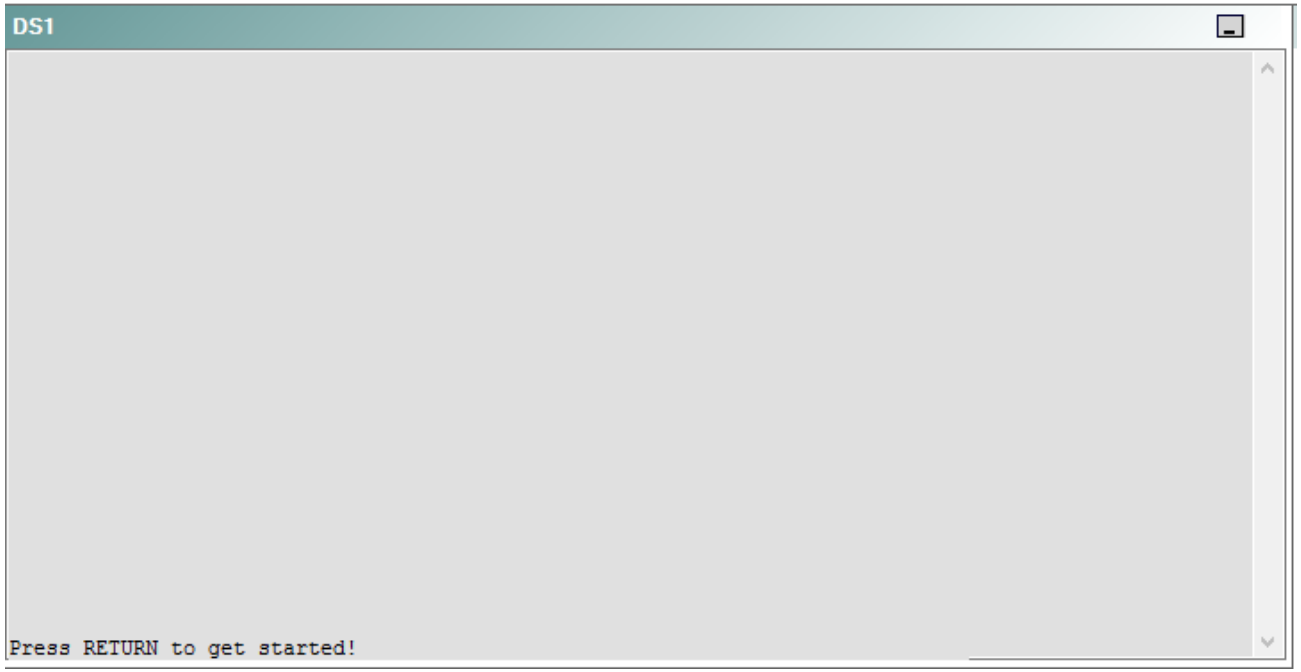

R4



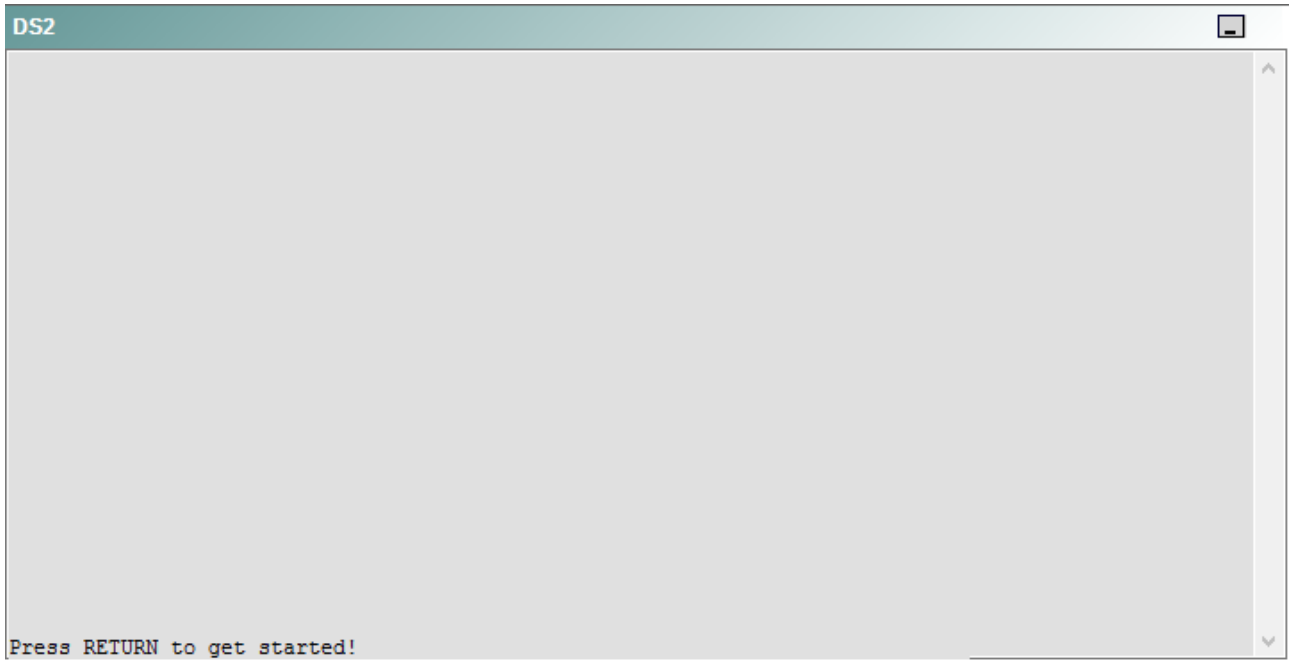

R5



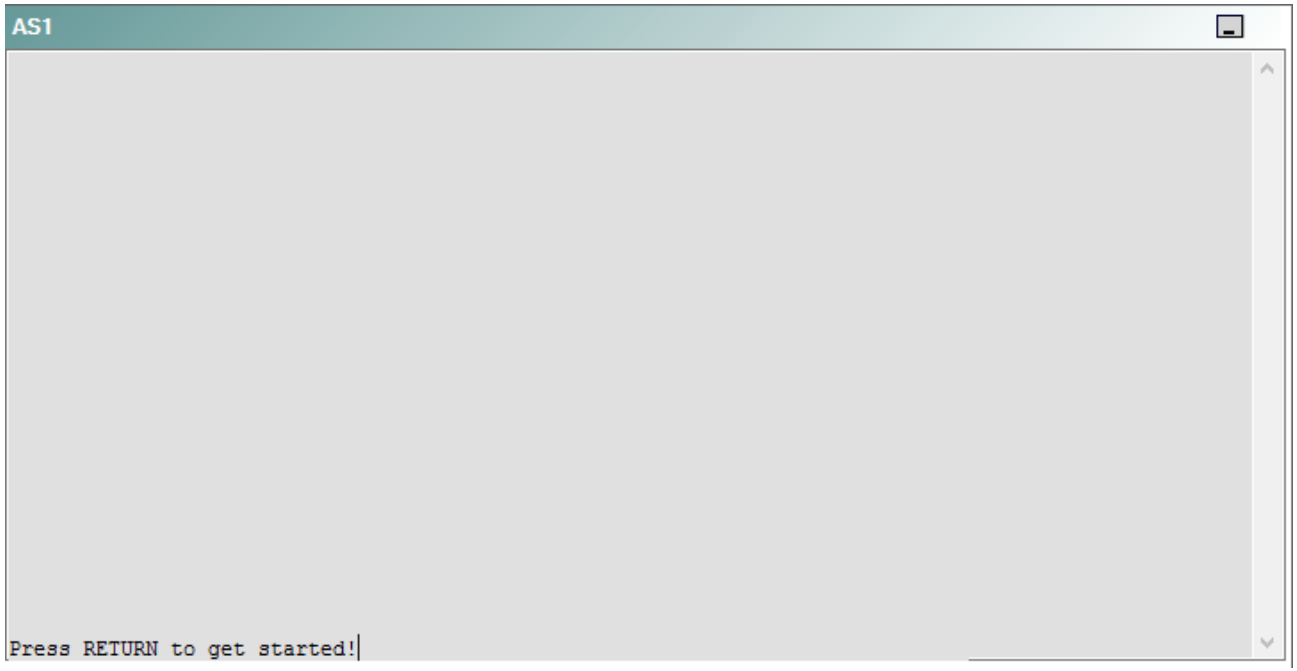

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** E
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

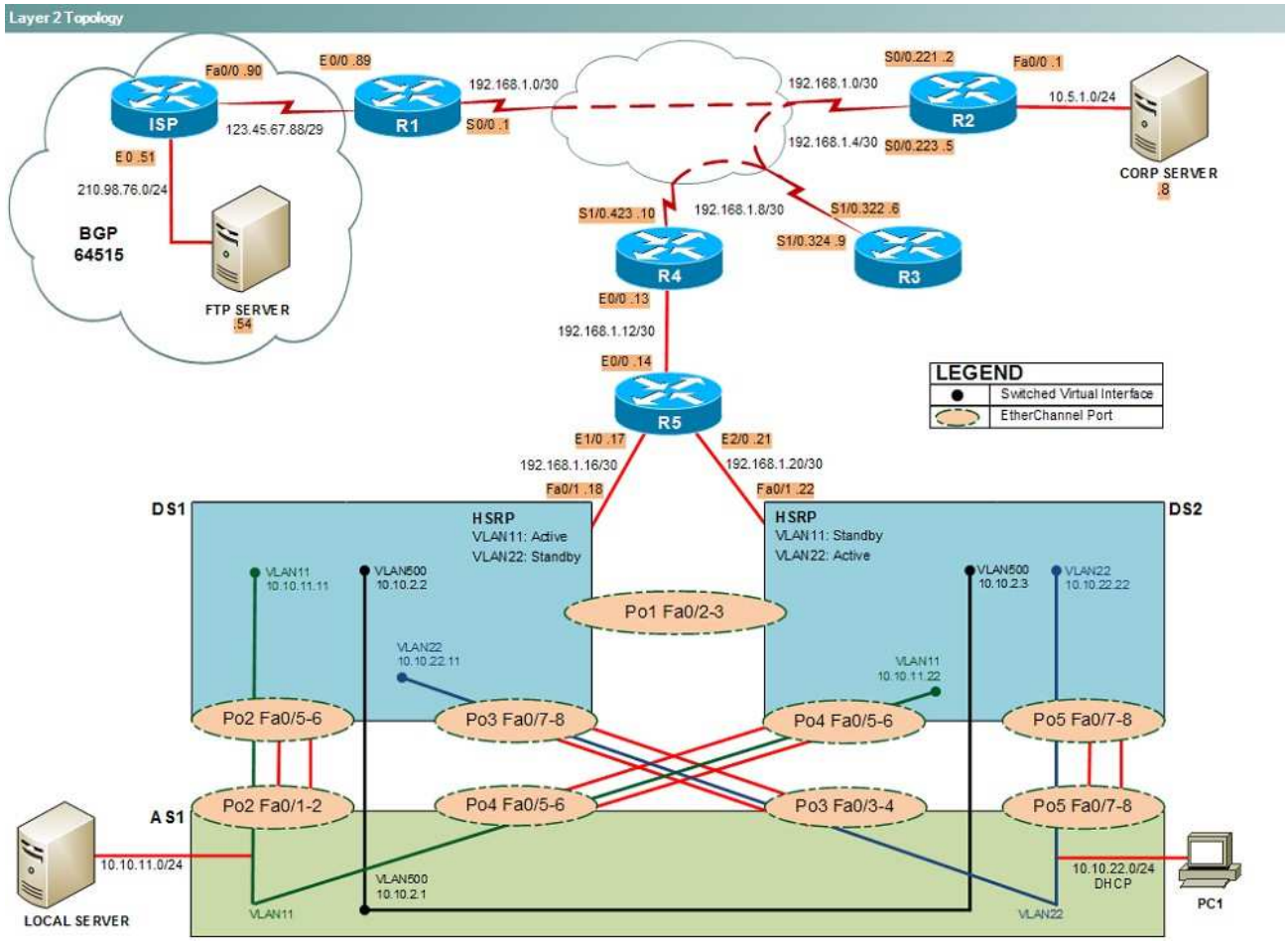
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

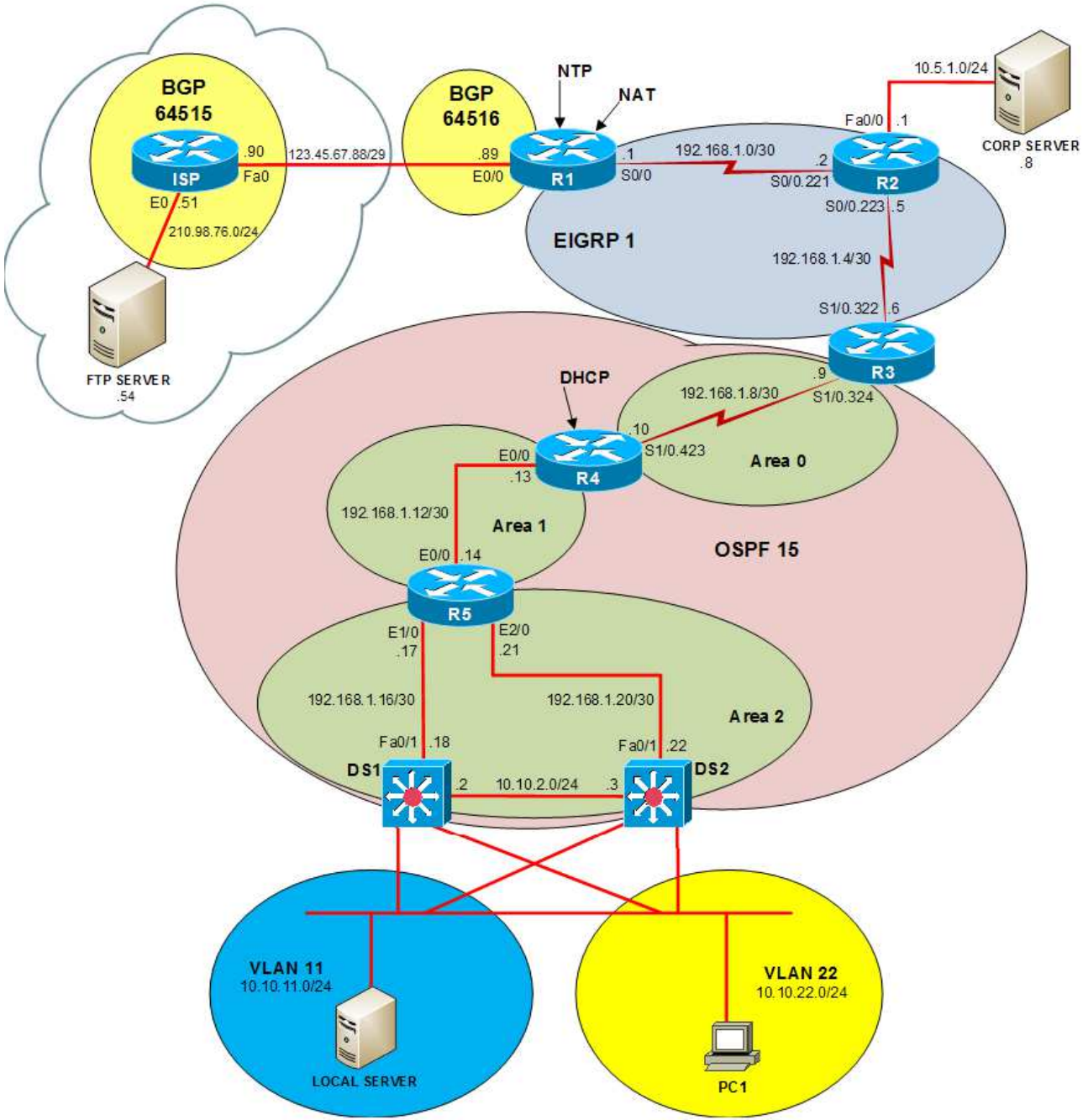
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

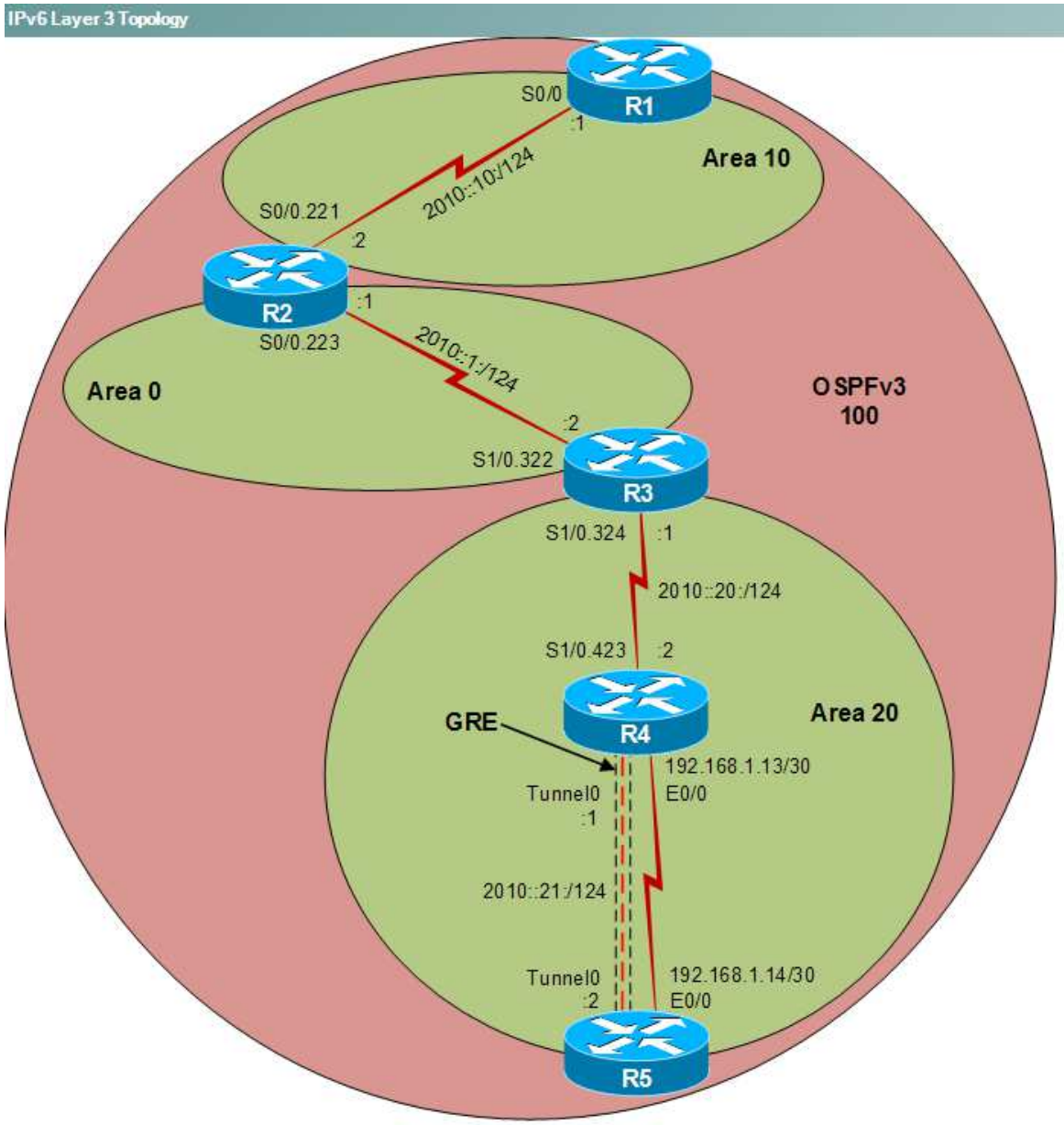
**Layer 2 Topology**




IPv4 layer 3 Topology

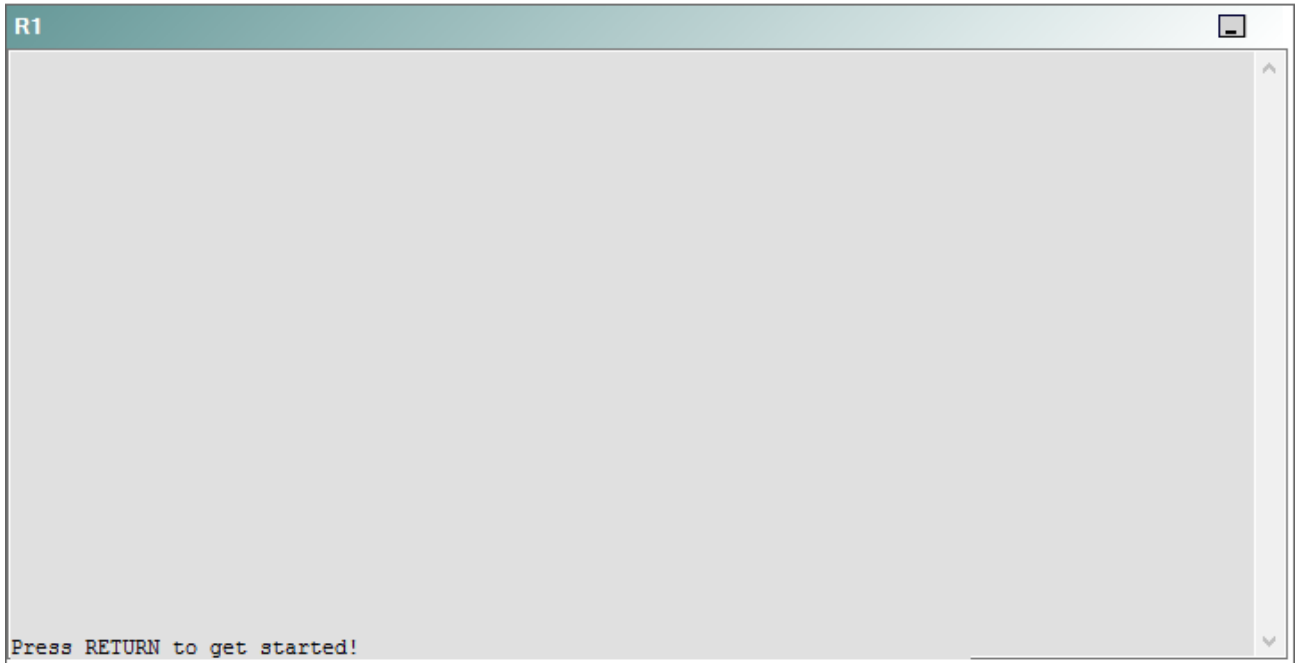

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

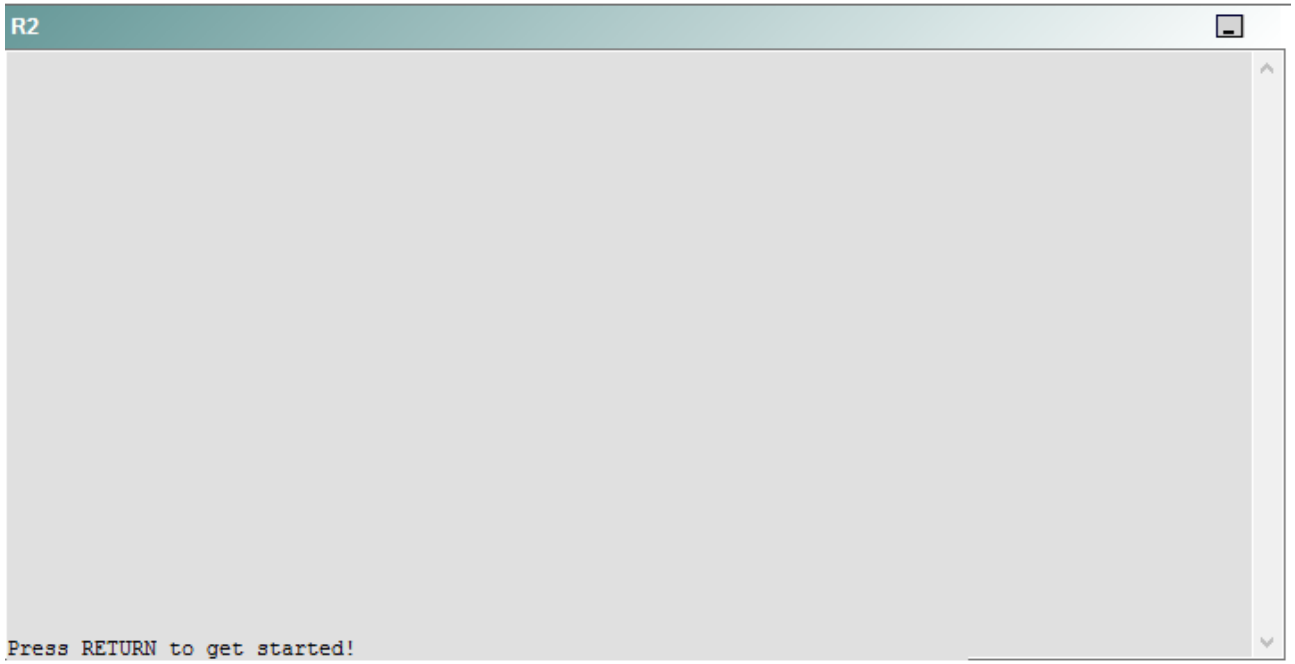



https://www.gratisexam.com/

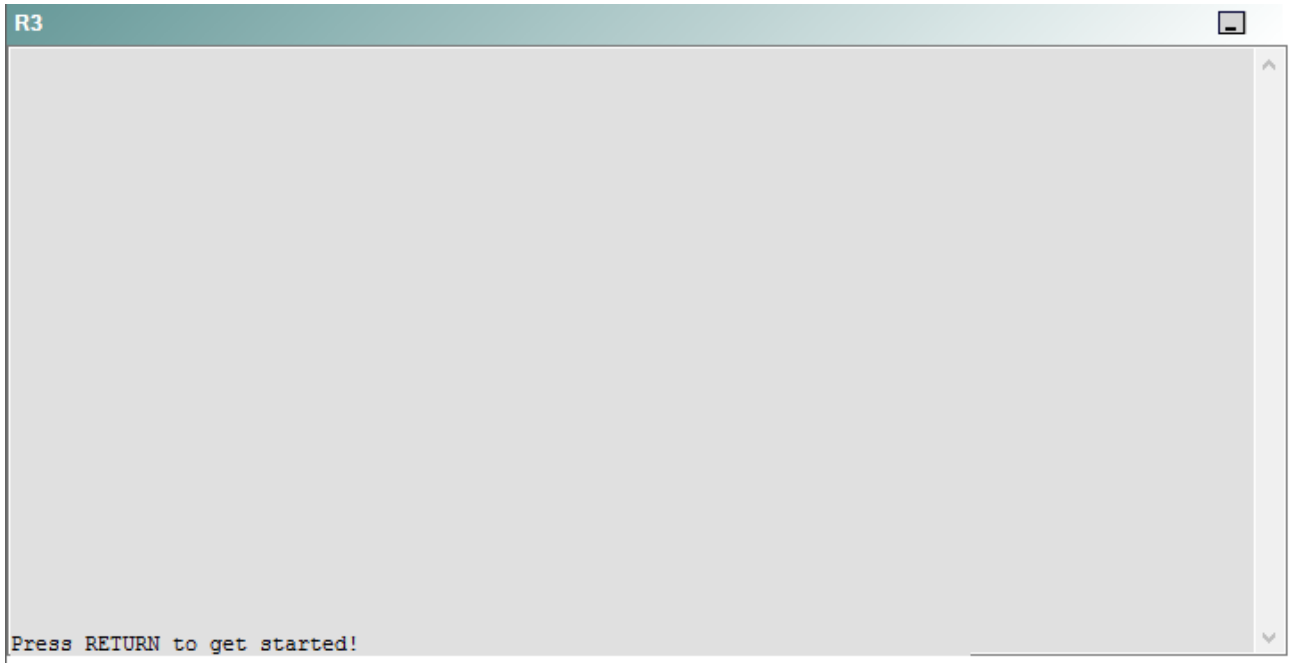
R1



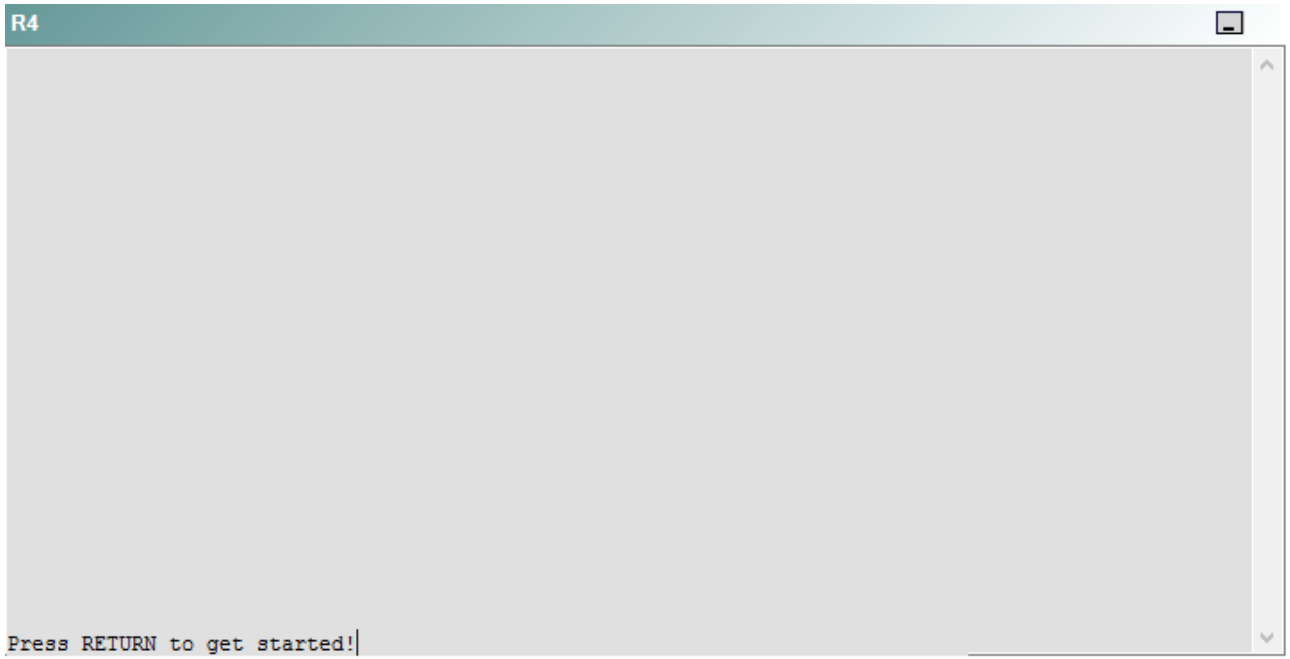

R2



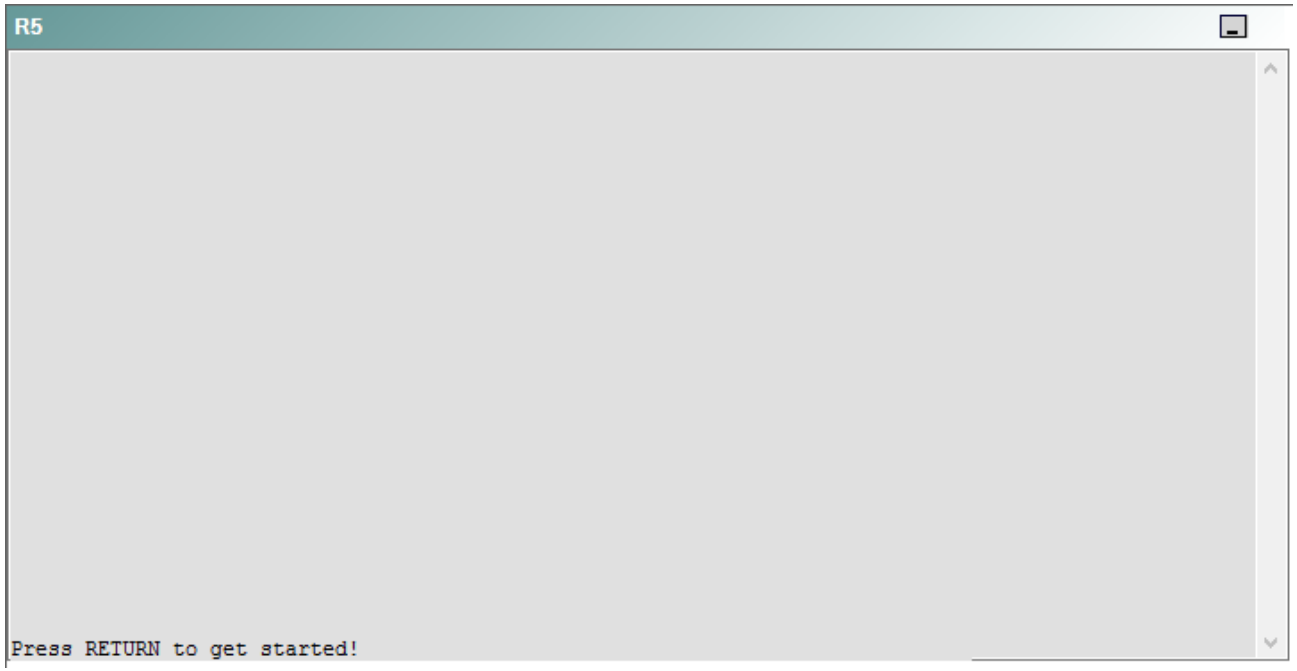

R3



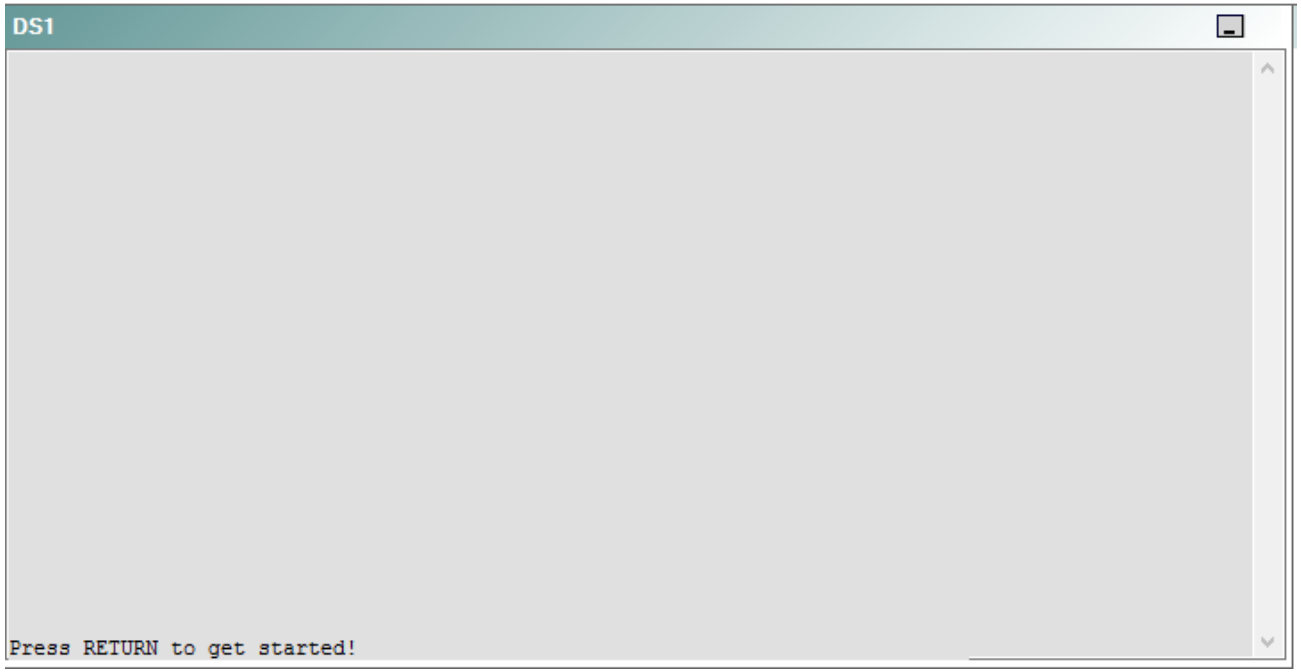

R4



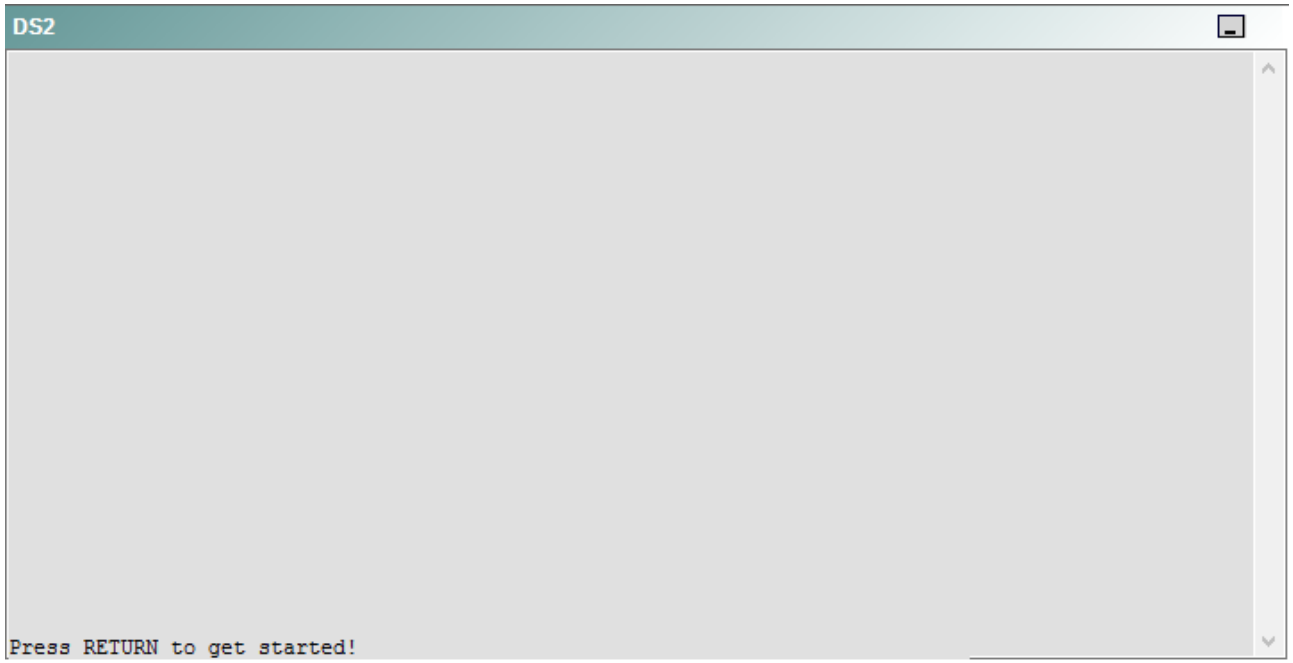

R5



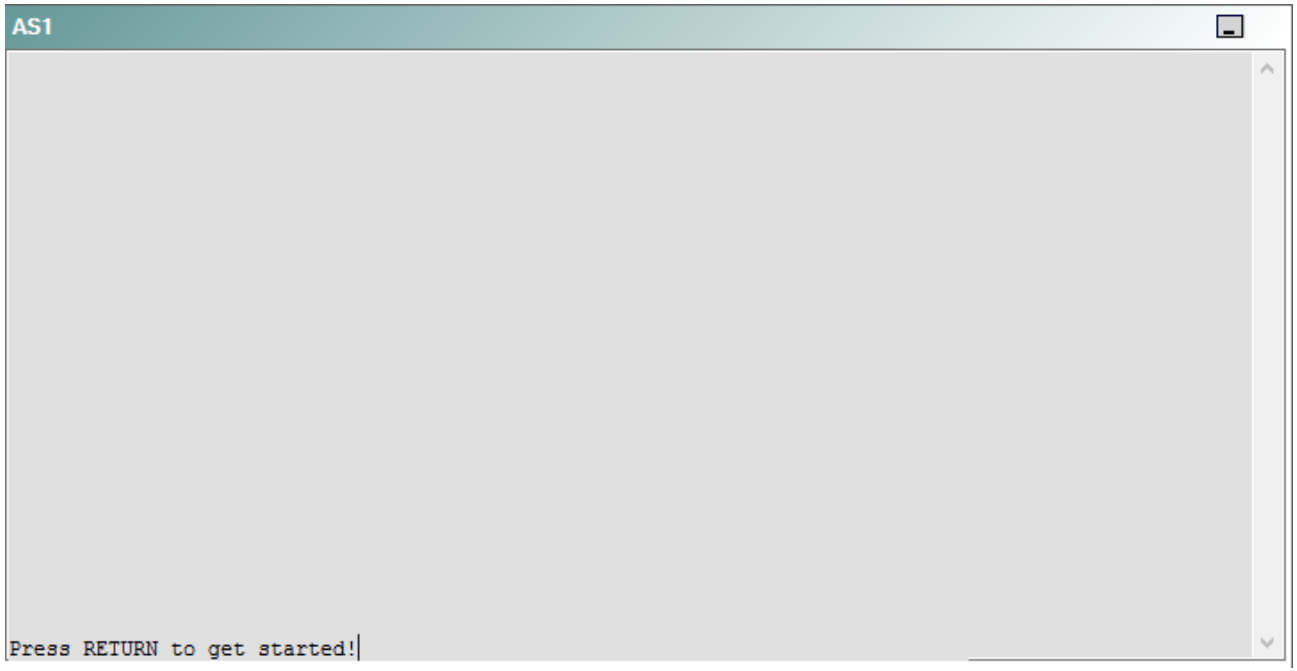

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. GRE
C. OSPFv2
D. Layer 3 security
E. Layer 3 addressing
F. DHCP
G. Etherchannel
H. VLAN configuration
I. interface

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

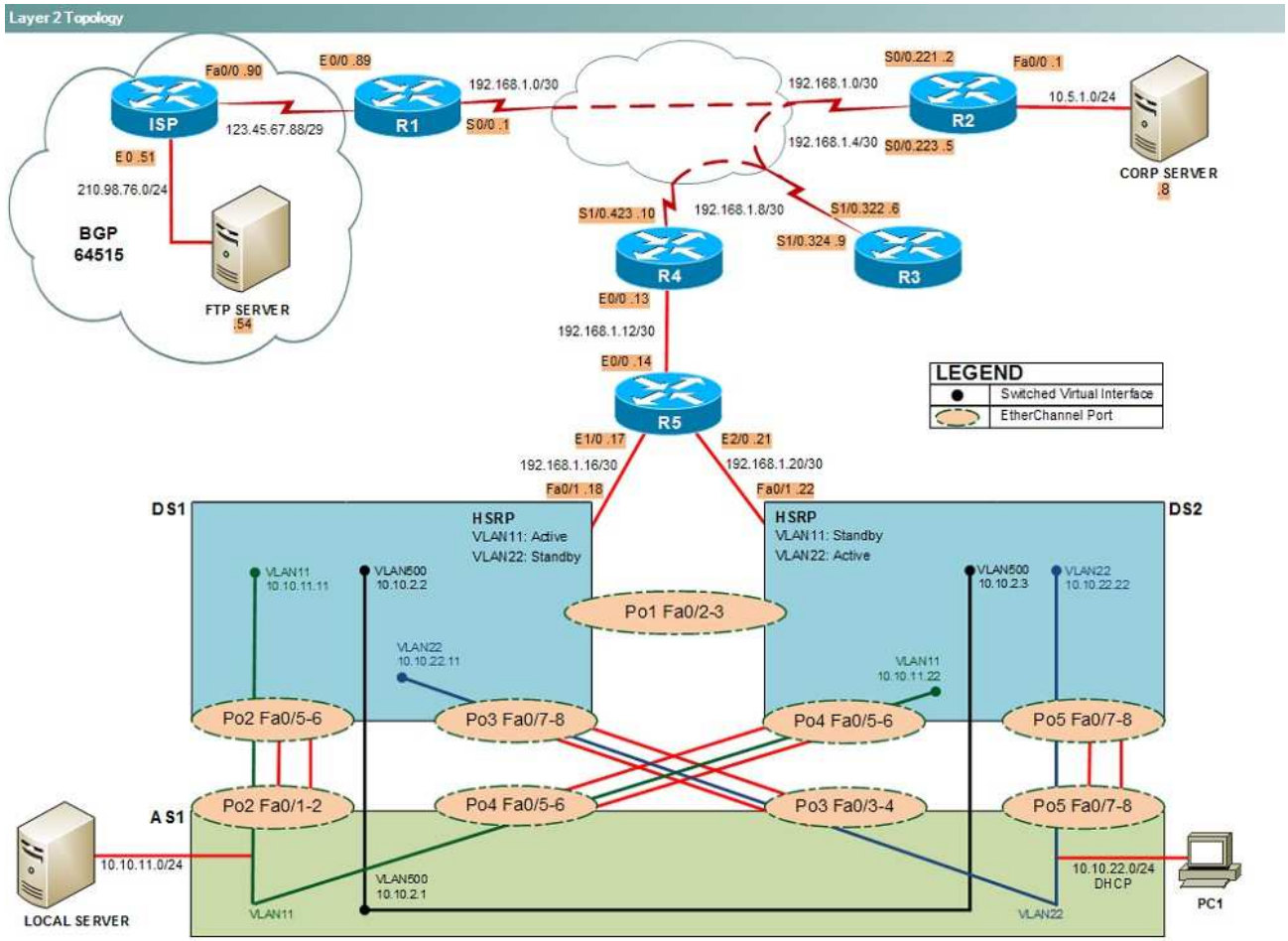
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

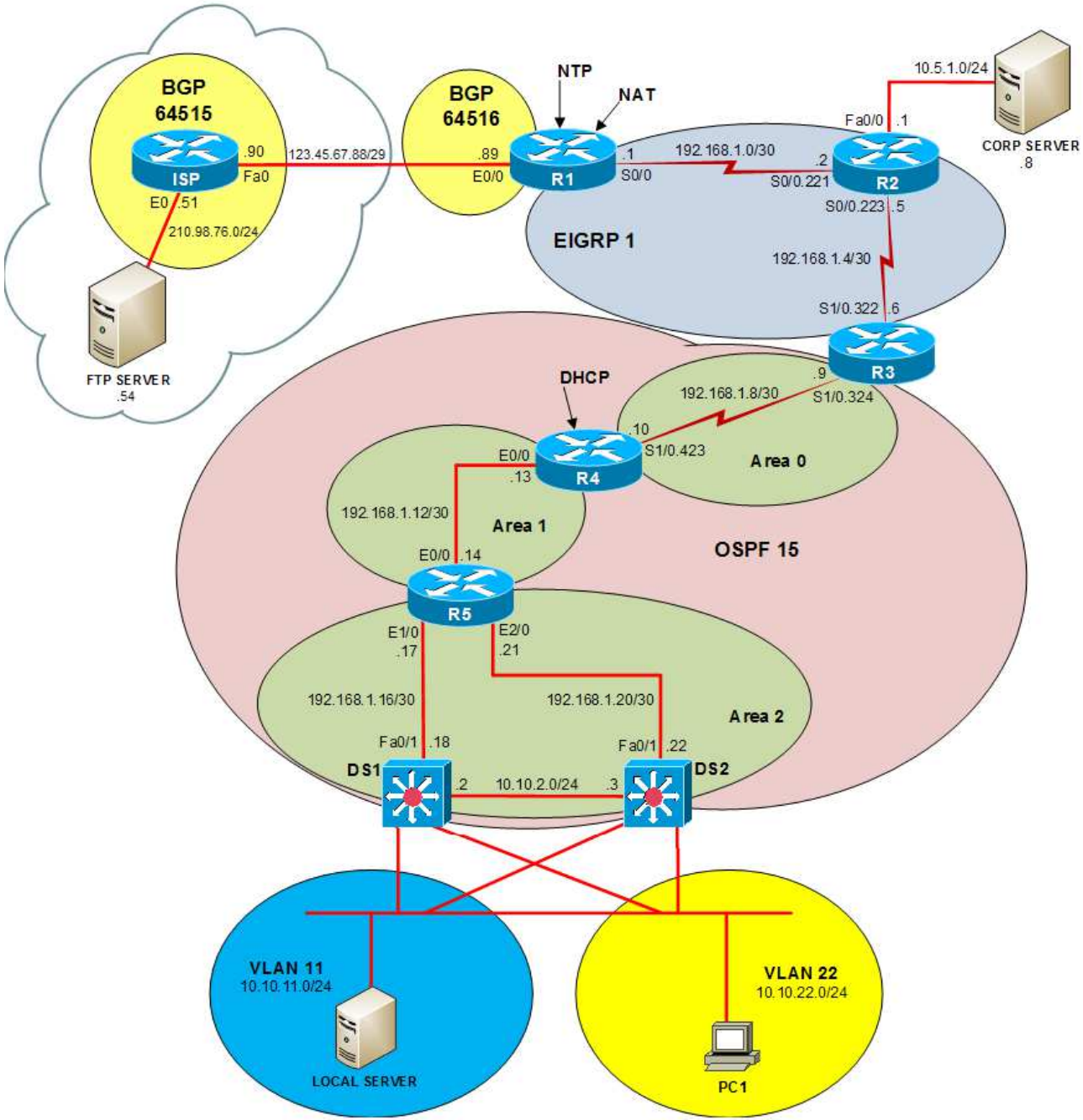
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

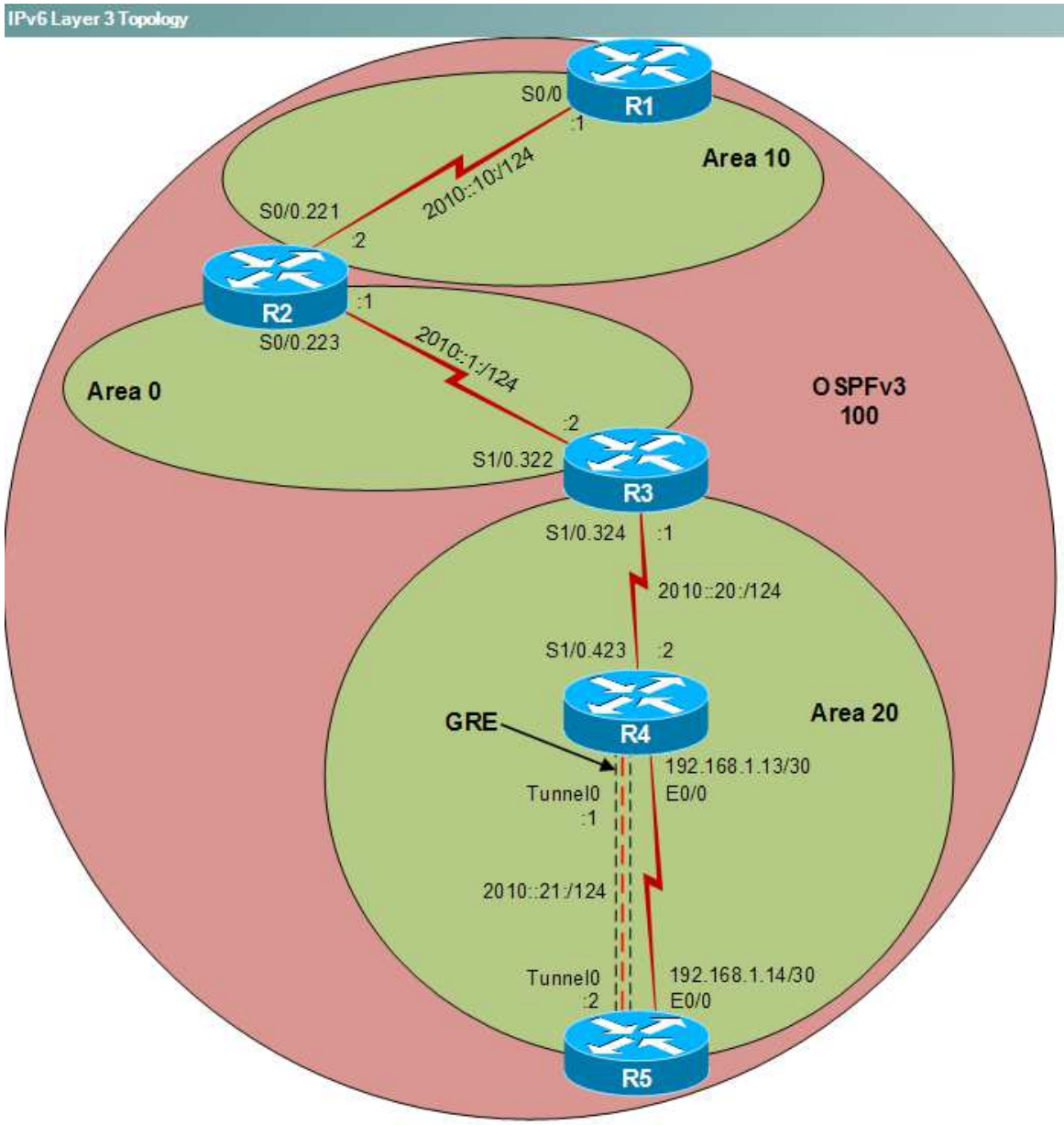
**Layer 2 Topology**




IPv4 layer 3 Topology

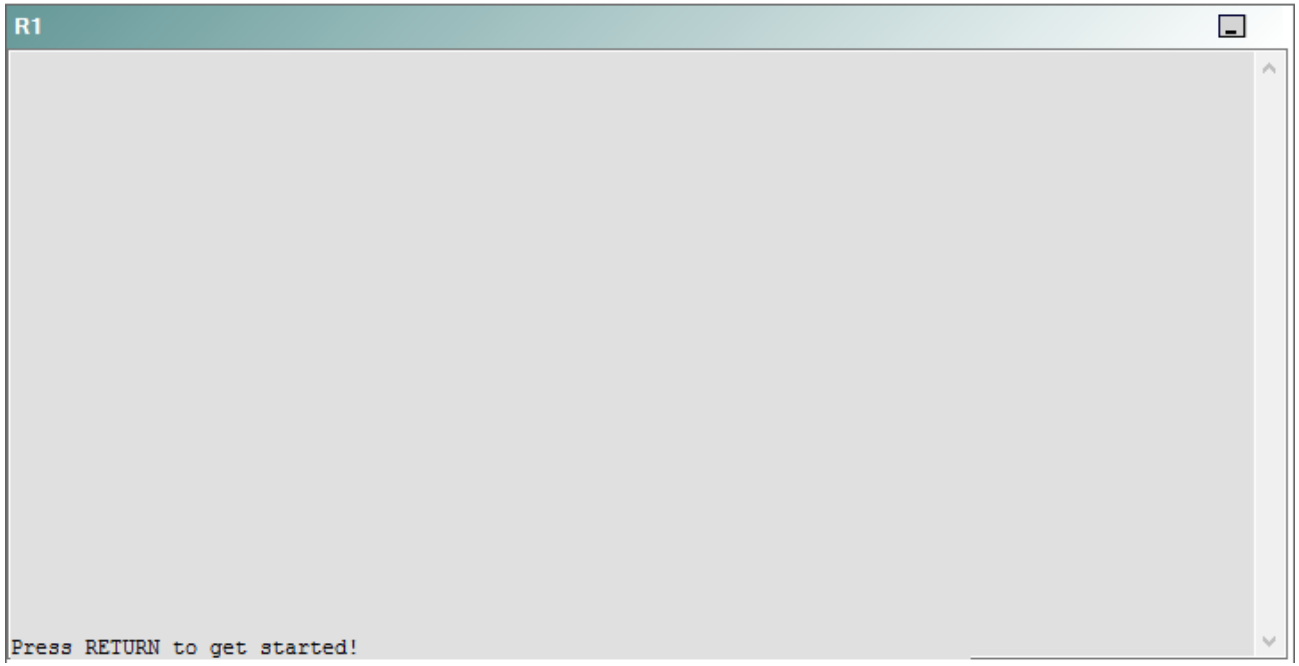

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

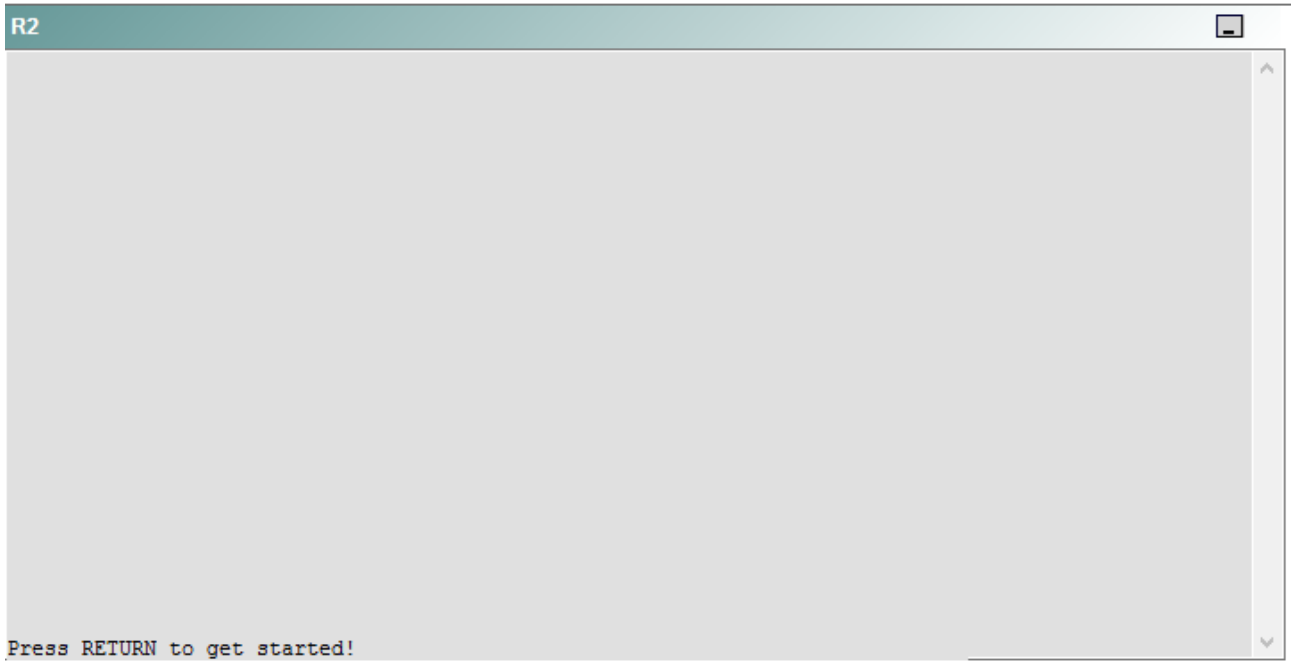



https://www.gratisexam.com/

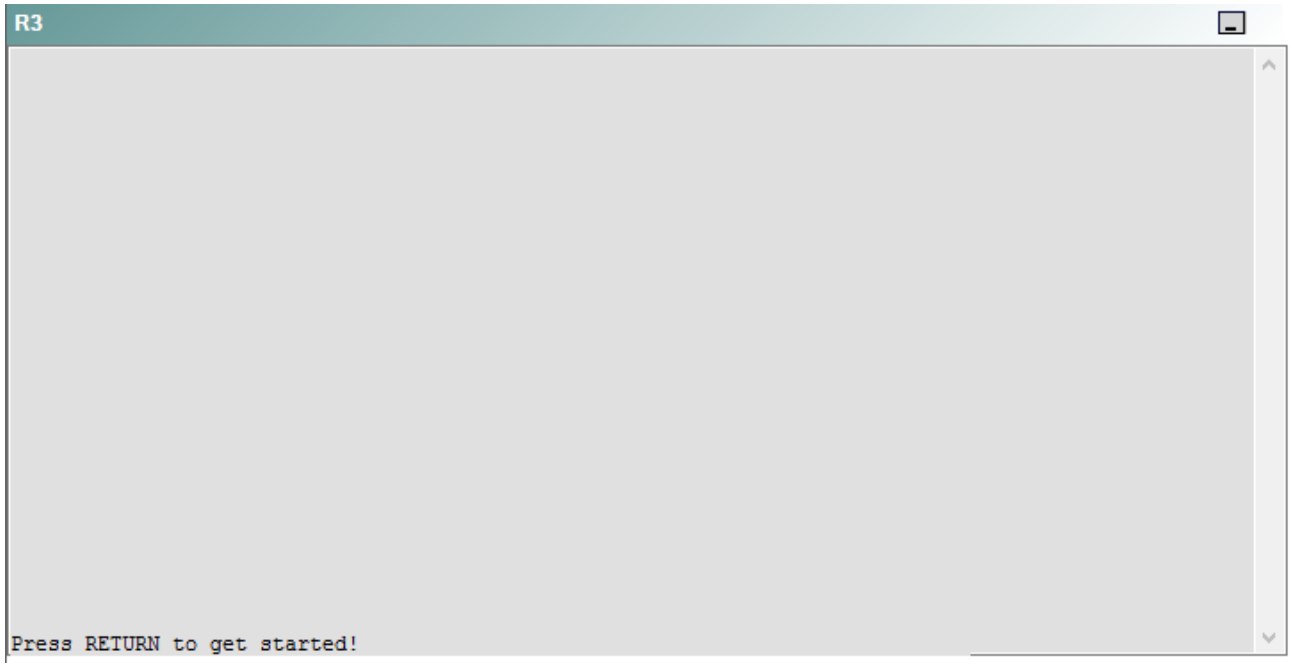
R1



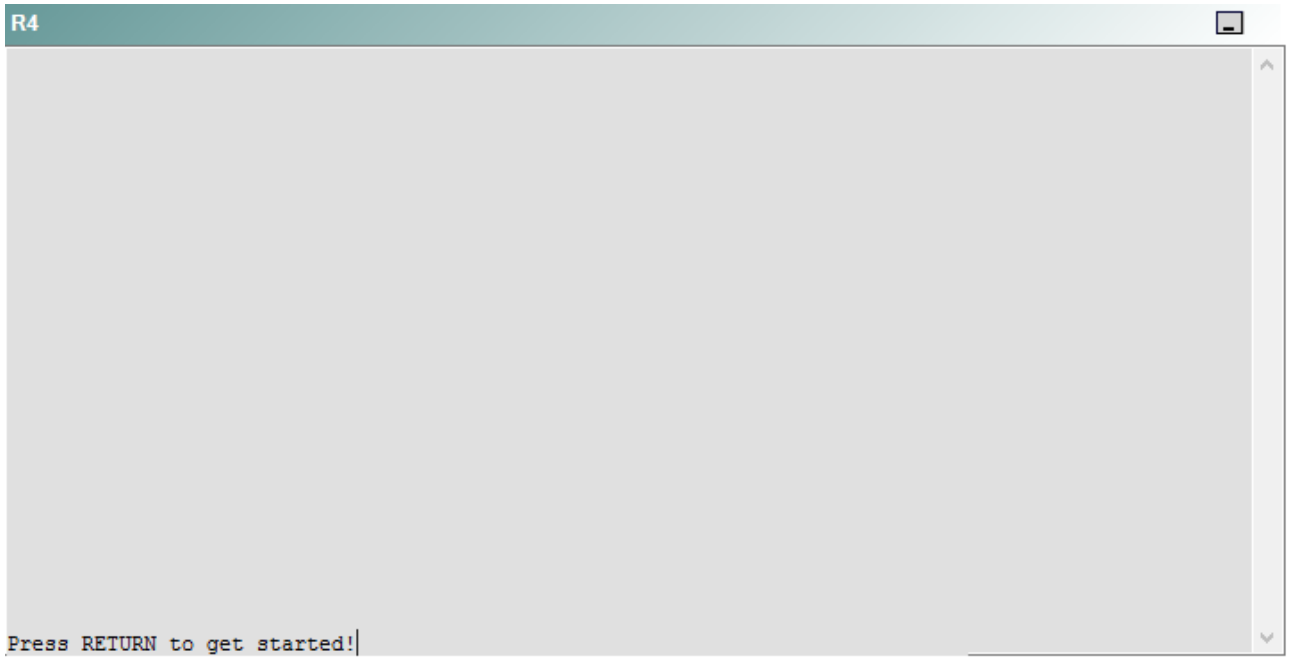

R2



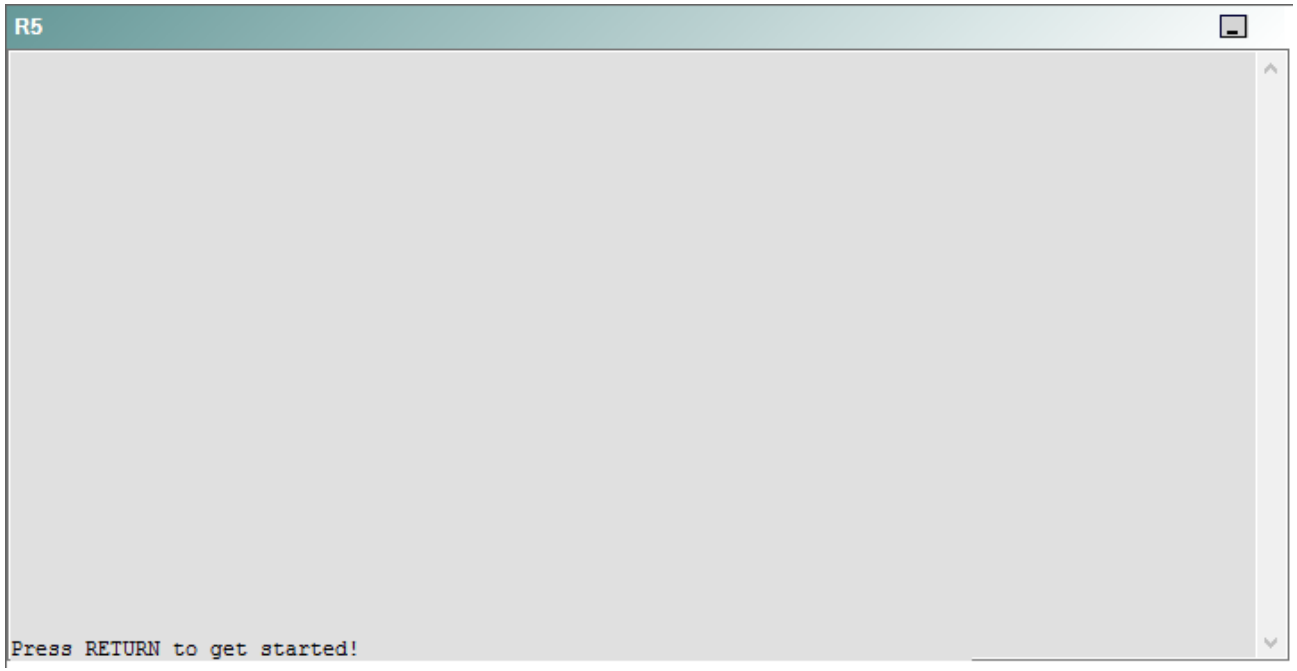

R3



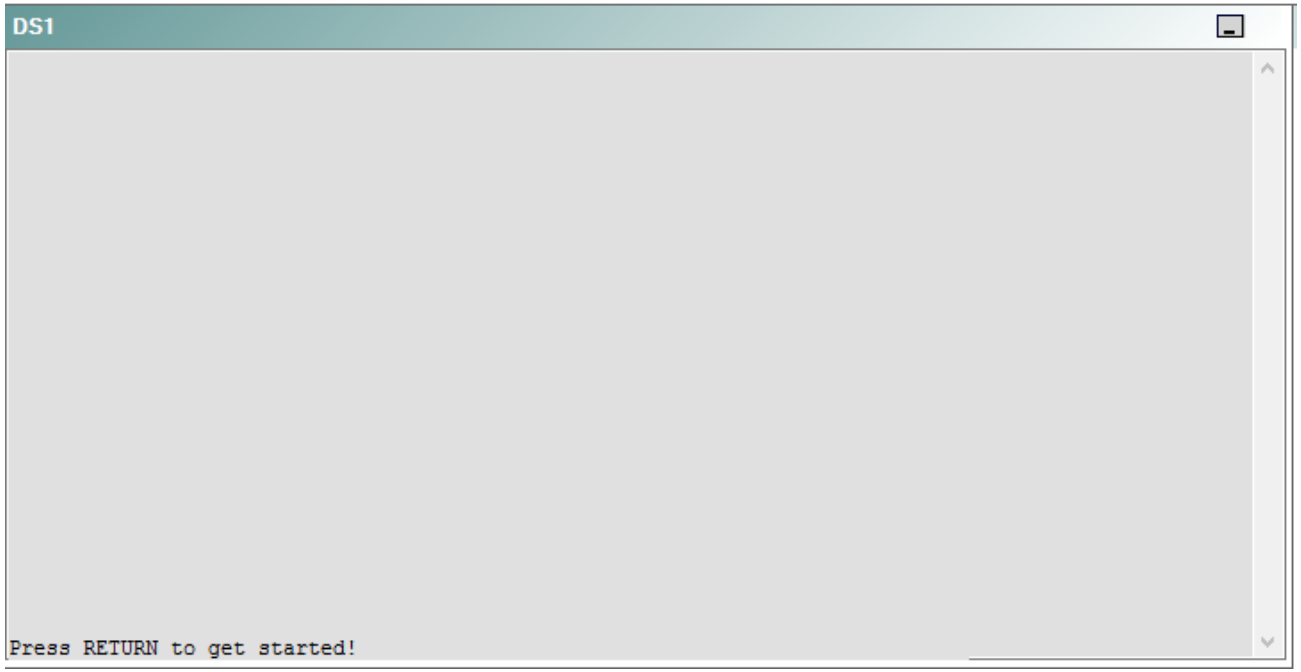

R4



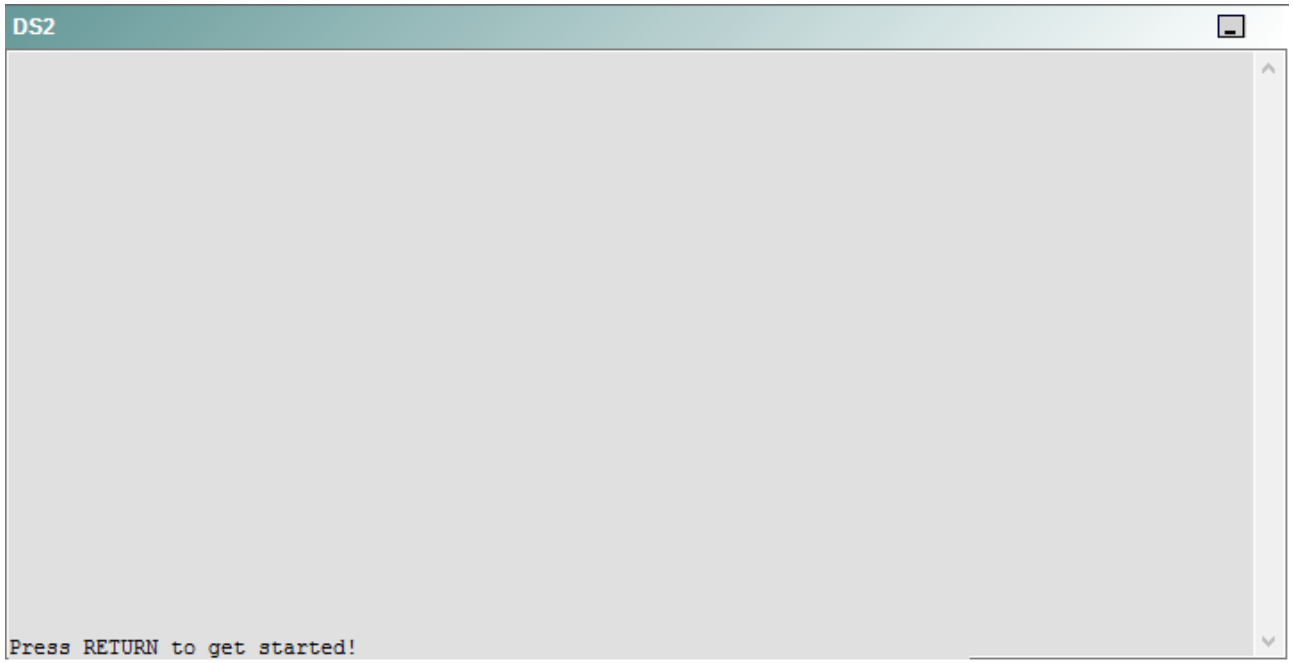

R5



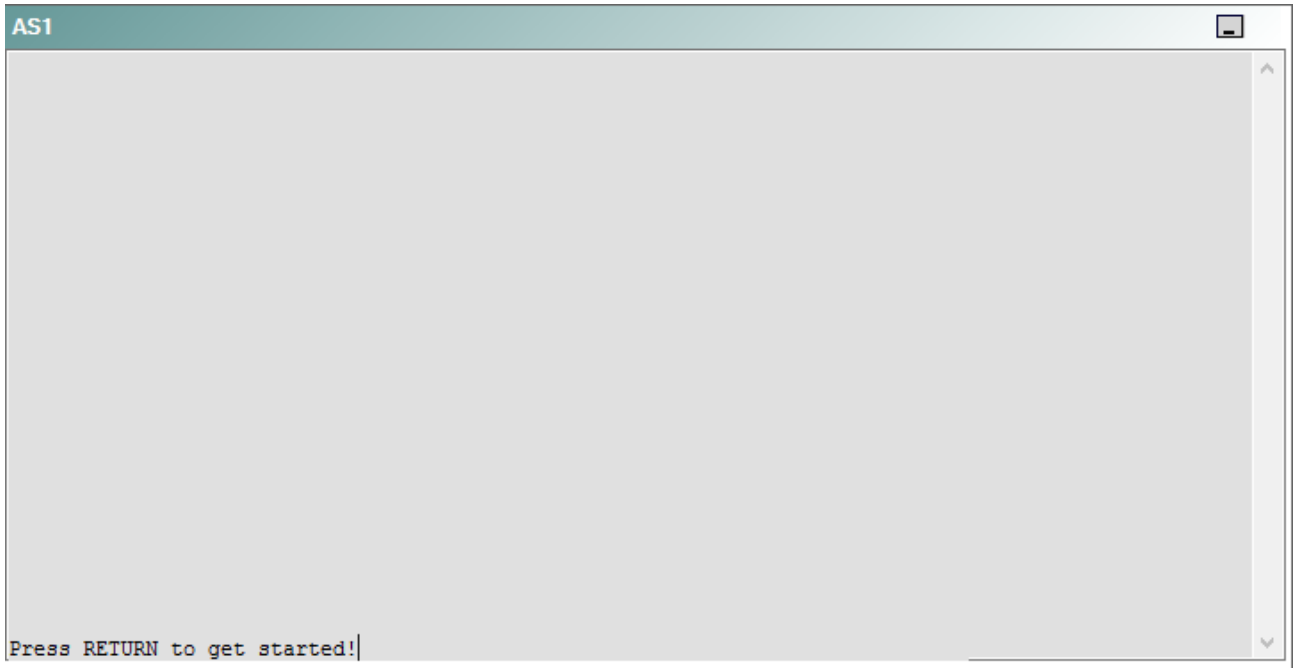

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. issuing the **network 192.168.1.12 0.0.0.3 area 1** command
B. issuing the **network 192.168.1.12 0.0.0.3 area 2** command
C. issuing the **area 1 virtual-link 192.168.1.13** command
D. issuing the **area 2 virtual-link 192.168.99.4** command
E. changing the OSPF routing process to 15
F. changing the OSPF network type on the E0/0 interface
G. changing the masks on the OSPF network statements
H. issuing the **no ip ospf hello-interval** command on the E0/0 interface
I. enabling OSPF MD5 authentication on the E0/0 interface

**Correct Answer:** H

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

You should issue the **no ip ospf hello-interval** command on the E0/0 interface of R5. To determine which device is the source of the problem, you can issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from PC1 to the closest device and work your way up the network until communication is lost, or you can ping from PC1 to the farthest device and work your way back to PC1 until pings are successful.

In this scenario, PC1 is unable to ping any device on the network. Issuing the **ipconfig** command on PC1 will display the following output:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Autoconfiguration IP Address. . . : 169.254.133.250
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :
```

An address that begins with 169.254 indicates that the computer is using an Automatic Private IP Addressing (APIPA) address. A computer will assign itself an APIPA address if it fails to receive an IP address from a Dynamic Host Configuration Protocol (DHCP) server. Therefore, PC1 is unable to communicate with the DHCP server on R4, and the problem must exist somewhere between them.

If you were to ping the loopback interface of R5 from DS2, the pings would be successful, as shown in the following output:

```
DS2#ping 192.168.99.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
```

However, if you were to ping the loopback interface of R4 from DS2, the pings would fail, as shown in the following output:

```
DS2#ping 192.168.99.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Therefore, the problem likely exists between R5 and R4.

Once you have determined where connectivity is lost, you can begin to troubleshoot what is causing the problem. Issuing the **show ip ospf neighbor** command on R4 and R5 indicates that no Open Shortest Path First version 2 (OSPFv2) neighbor relationship exists between the two routers.

Issuing the **show ip ospf interface** command on R5 reveals that the OSPF hello timer on the Ethernet 0/0 interface is misconfigured, as shown in the following partial output:

```
R5#show ip ospf interface
Ethernet0/0 is up, line protocol is up
  Internet Address 192.168.1.14/30, Area 1
  Process ID 10, Router ID 192.168.99.5, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.99.5, Interface address 192.168.1.14
  No backup designated router on this network
  Timer intervals configured, Hello 20, Dead 80, Wait 80, Retransmit 5
    Hello due in 00:00:05
```

By default, the hello timer is set to 10 seconds on point-to-point and broadcast links and 30 seconds on nonbroadcast multiaccess (NBMA) links. Issuing the no **ip ospf hello-interval** command in the E0/0 interface of R5 will set the hello timer back to the default value of 10 seconds.

You should not issue the **no ip ospf hello-interval** command on the E0/0 interface on R4. Issuing the **show ip ospf interface** command will reveal that the E0/0 interface of R4 is already configured with the default OSPF hello timer value of 10 seconds, as shown by the following output:

```
Ethernet0/0 is up, line protocol is up
  Internet Address 192.168.1.13/30, Area 1
  Process ID 15, Router ID 192.168.99.4, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.99.4, Interface address 192.168.1.13
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

You need not change the OSPF routing process on R5 to 15, nor do you need to change the OSPF routing process on the other devices to 10. The OSPF routing process number is locally significant, so two OSPF routers with different routing process numbers can still form an adjacency, as long as the following parameters match:

- Hello timer
- Dead timer
- Area number and type
- Network type
- Subnet
- Authentication type and password

In addition, OSPF cannot establish an adjacency over a secondary IP address.

You need not change the OSPF network type on the E0/0 interface of R4 or R5. The OSPF network type must match so that connected interfaces can form an adjacency. The E0/0 interfaces on R4 and R5 are both set to the broadcast OSPF network type. You can determine the OSPF network type by issuing the **show ip ospf interface** command. To change the OSPF network type for an interface, you would issue the **ip ospf network {broadcast** | **non-broadcast** | **point-to-multipoint** | **point-to-point}** command from interface configuration mode.

You need not change the masks on the OSPF **network** statements. The **network** command uses wildcard masks, which are basically inverse subnet masks. To calculate the appropriate wildcard mask, you should subtract the subnet mask from 255.255.255.255. For example, the 192.168.1.12 network has a /30 subnet mask, which is 255.255.255.252. Subtracting 255.255.255.252 from 255.255.255.255 yields a wildcard mask of 0.0.0.3.

You need not change the router ID on any of the routers. A long as the router ID is unique, OSPF routers will form an adjacency. The first line in the output of the **show ip ospf** command displays the router ID. To change the router ID on a router, you would issue the **router-id** *A.B.C.D* command from OSPF router configuration mode, where *A.B.C.D* is a 32-bit router ID in dotted decimal notation.

You need not enable OSPF Message Digest 5 (MD5) authentication, because OSPF MD5 authentication is not enabled on any of the routers on the network. OSPF authentication can be enabled for an interface or for an area. To configure OSPF MD5 authentication for an interface, you would issue the **ip ospf authentication message-digest** command in interface configuration mode. To configure OSPF MD5 authentication for an area, you would issue the **area** *area-id* **authentication message-digest** command in router configuration mode. To configure the key that should be used for MD5 authentication, you would issue the **ip ospf message-digest-key** *key-id* **md5** *key* command in interface configuration mode.

You need not issue the **network 192.168.1.12 0.0.0.3 area** 1 command on R4 or R5, because the **network 192.168.1.12 0.0.0.3 area 1** command has already been issued on both routers. You should not issue the **network 192.168.1.12 0.0.0.3 area 2** command on R4 or R5, because the 192.168.1.12/30 network should exist in Area 1, not Area 2.

All areas in an OSPF internetwork must be connected to the backbone area, Area 0. A virtual link must be created between two are border routers (ABRs) to connect a remote area to the backbone area through a transit area. The following restrictions apply to virtual links:

- The routers at each end of the virtual link must share a common area.
- The transit area cannot be a stub area.
- One router must connect to the backbone area.

The **area virtual-link** command is used to create a virtual link. The syntax of the **area virtual-link** command is **area** *area-id* **virtual-link** *router-id*, where *area-id* is the transit area ID and *router-id* is the router at the other end of the virtual link. You should not issue the **area 2 virtual-link 192.168.99.5** command on R4 or the **area 2 virtual-link 192.168.99.4** command on R5, because Area 1, not Area 2, is the transit area. You should not issue the **area 1 virtual-link 192.168.1.14** command on R4 or the **area 1 virtual-link 192.168.1.13** command on R5, because you should use the router ID of the router at the other end of the virtual link for the *router-id* parameter; you should not use the router's interface IP address. You should not issue the **area 2 virtual-link 192.168.99.5** command on R3, because R3 is not connected to the transit area.

Reference:

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13699-29.html#seventh
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/47866-ospfdb7.html

**QUESTION 13**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s

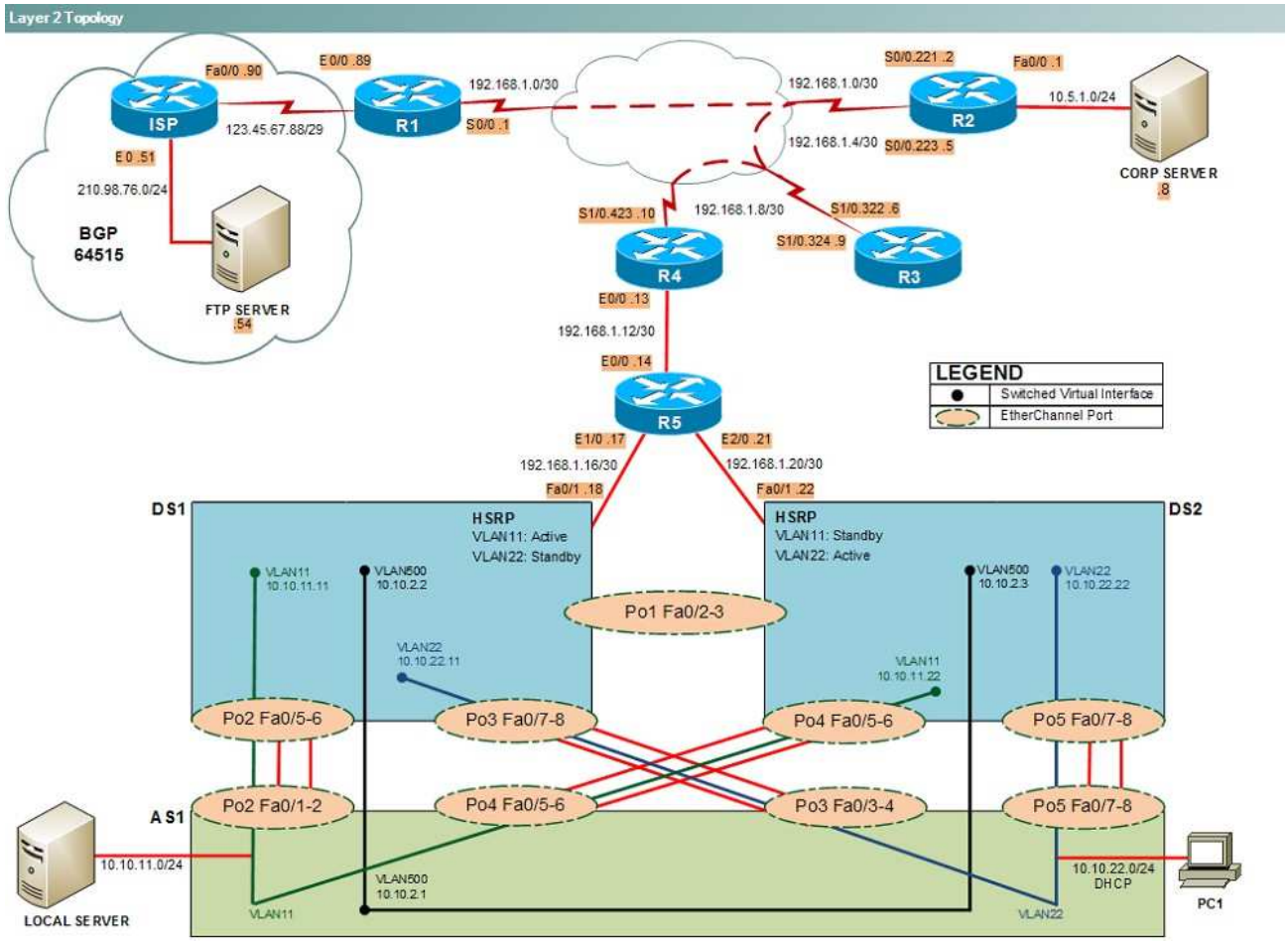
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

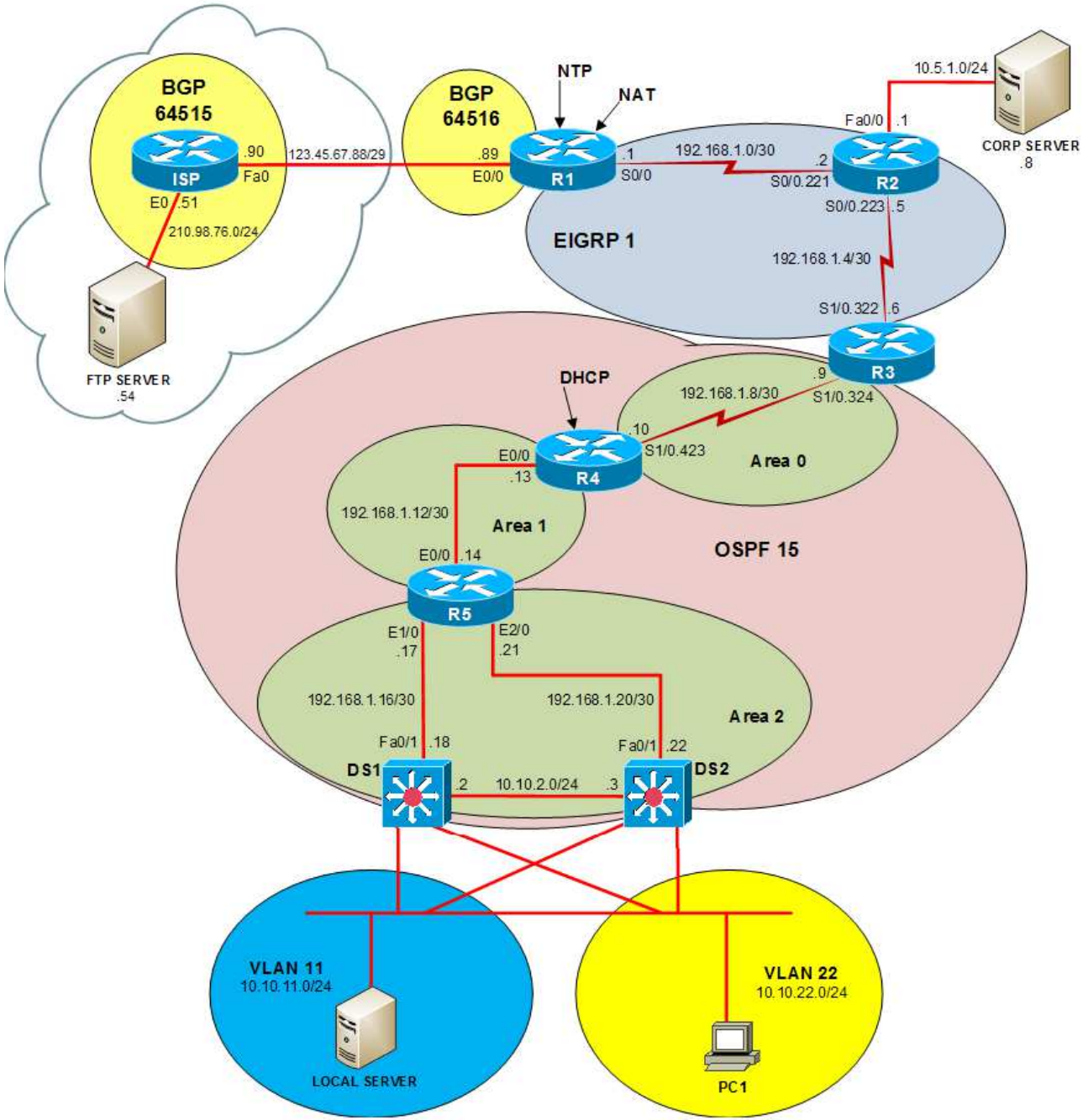
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

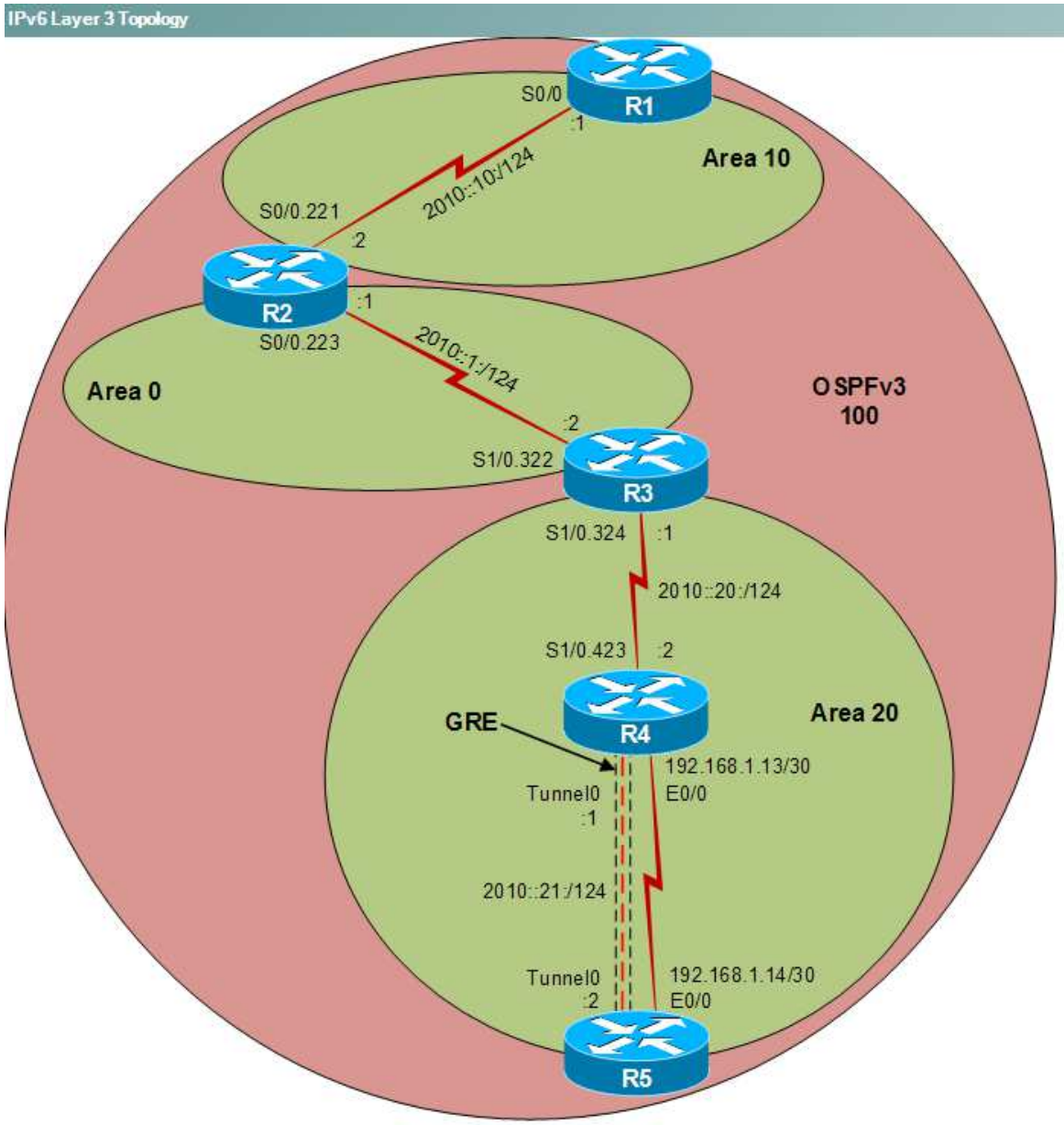
**Layer 2 Topology**




IPv4 layer 3 Topology

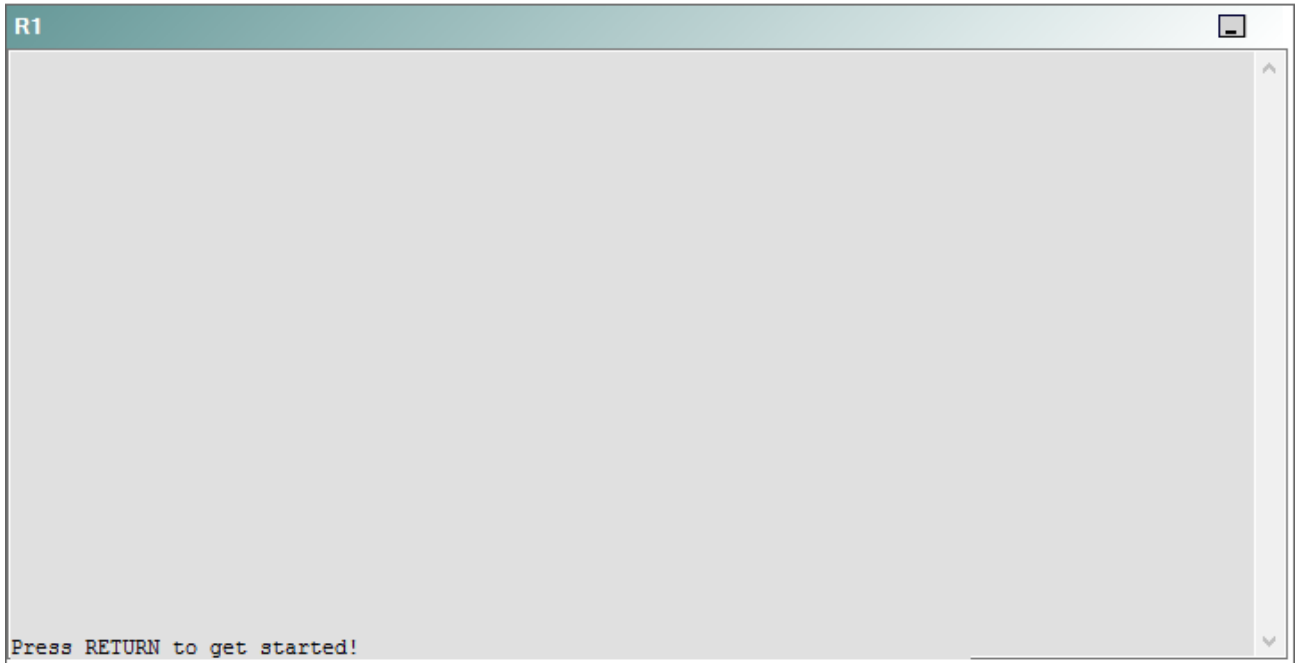

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

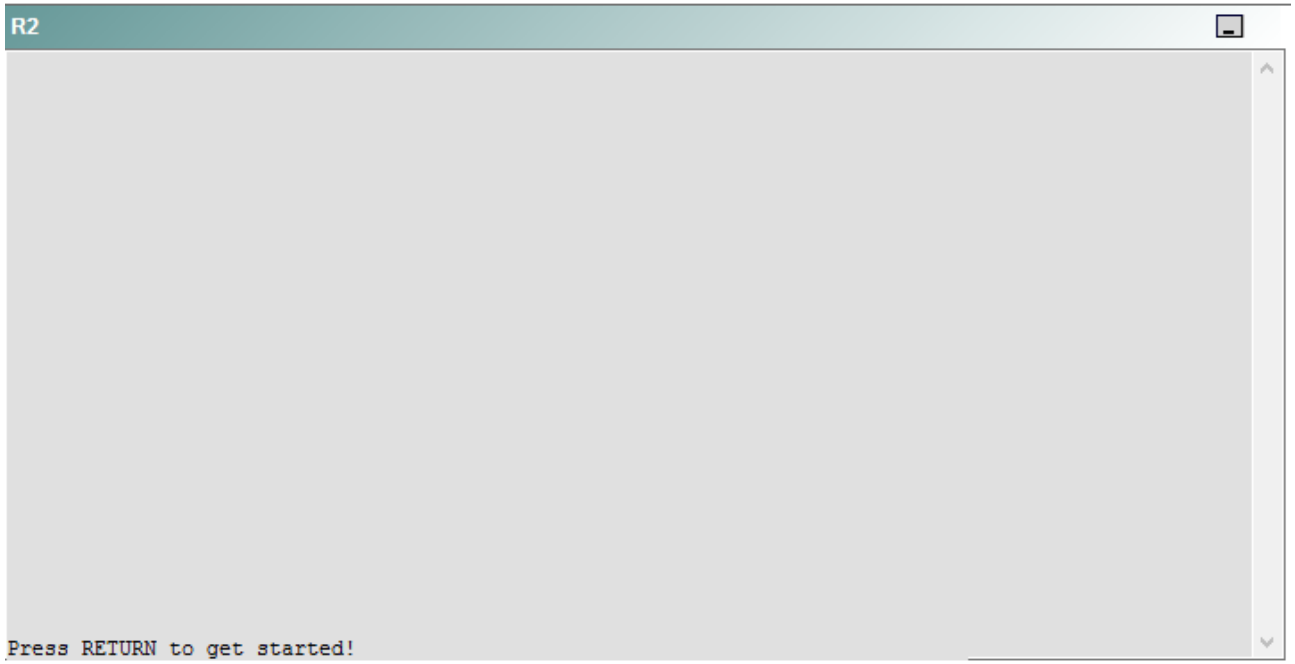



https://www.gratisexam.com/

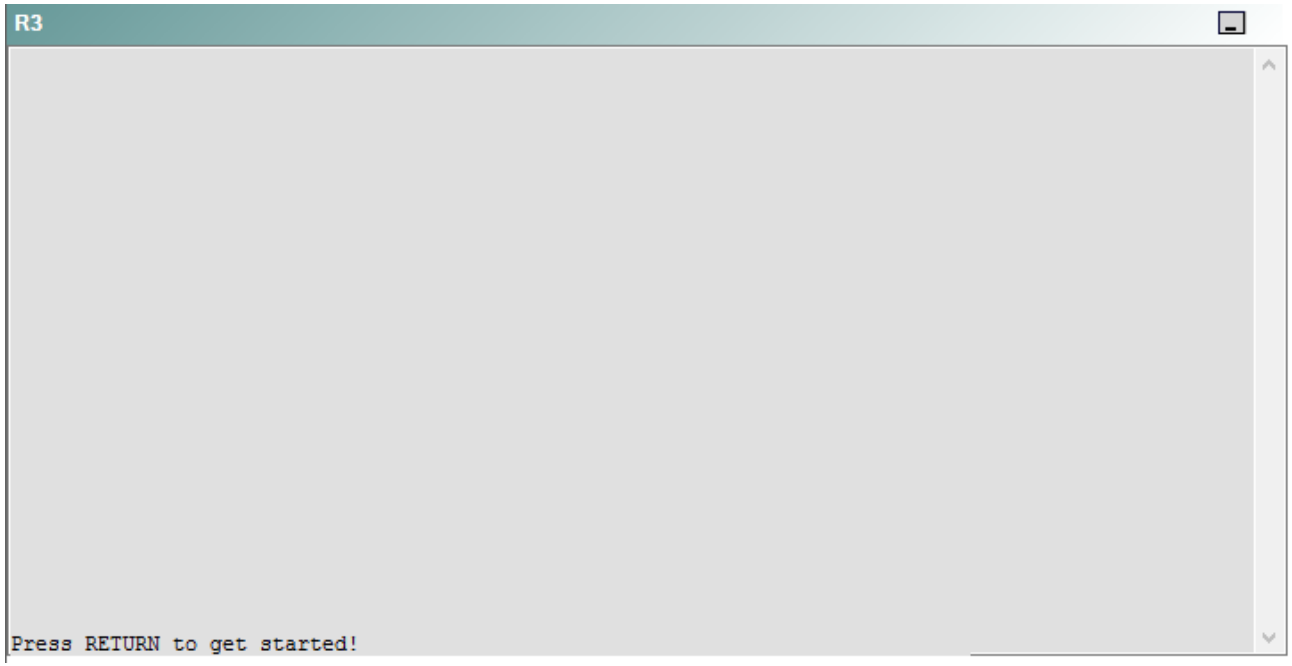
R1



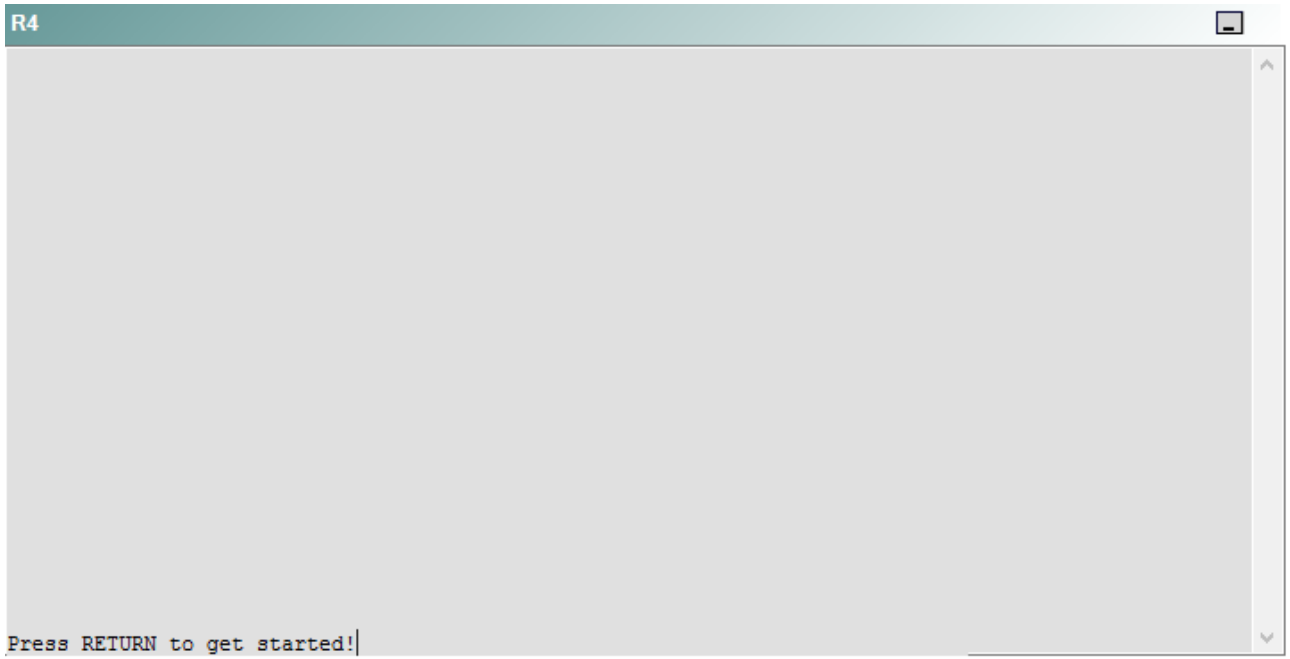

R2



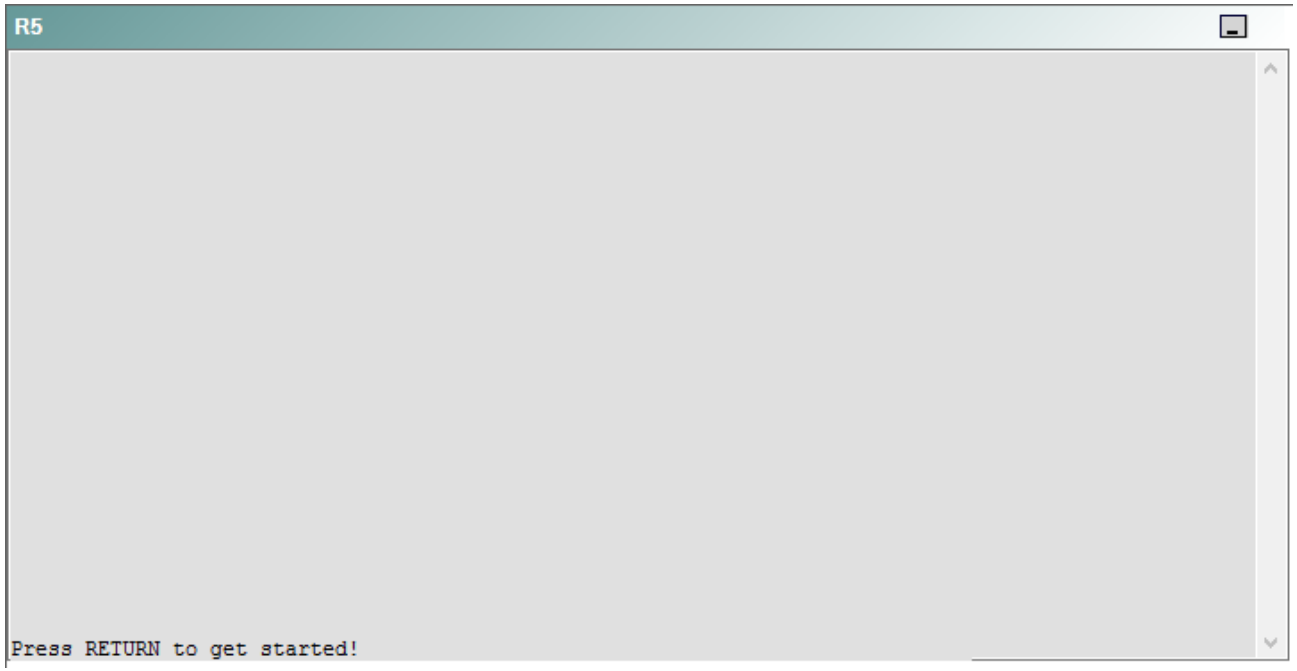

R3



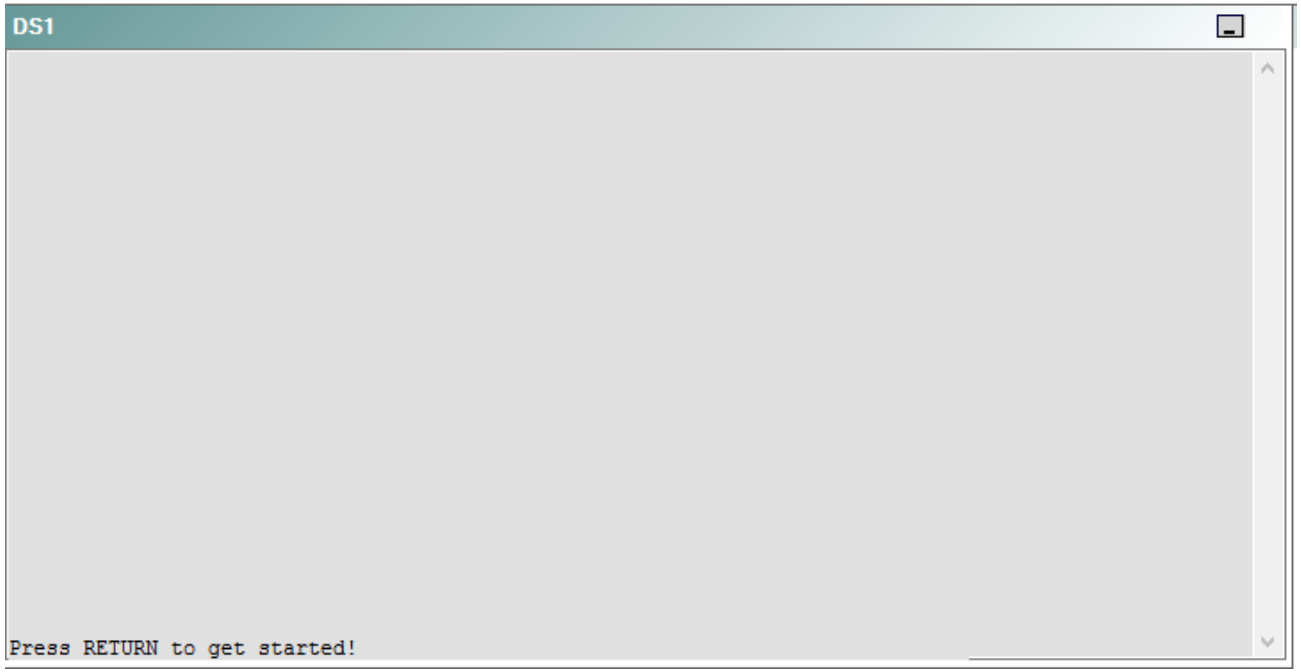

R4



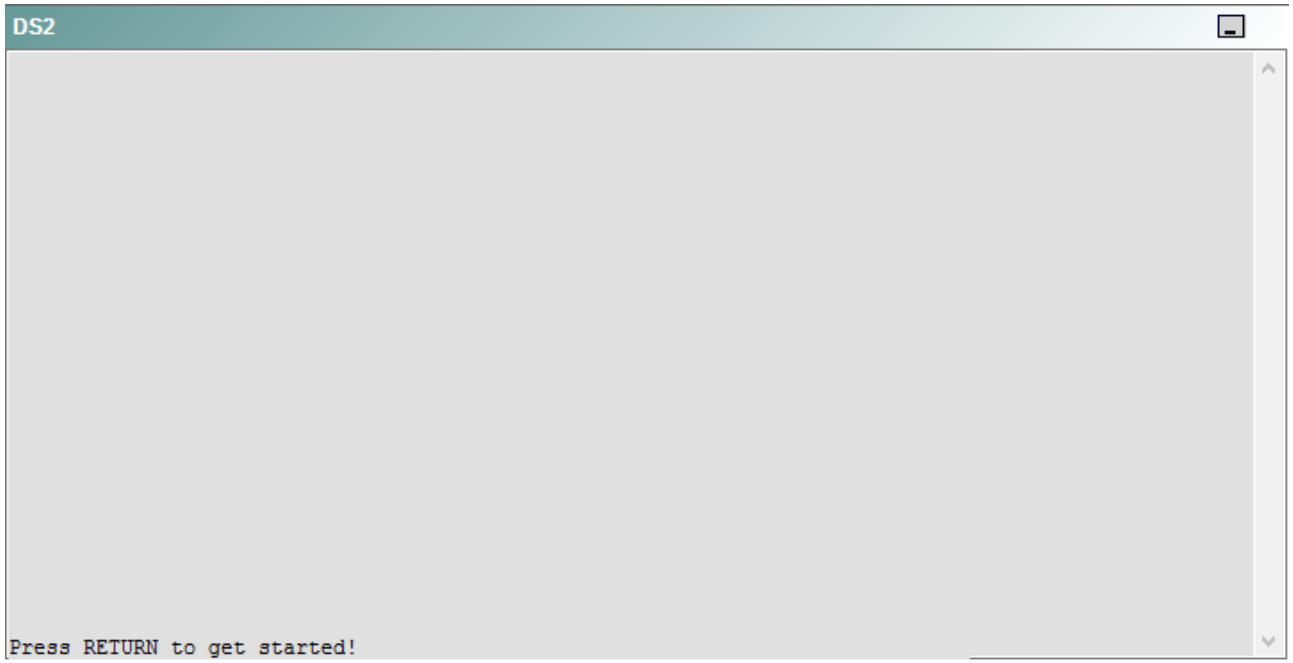

R5



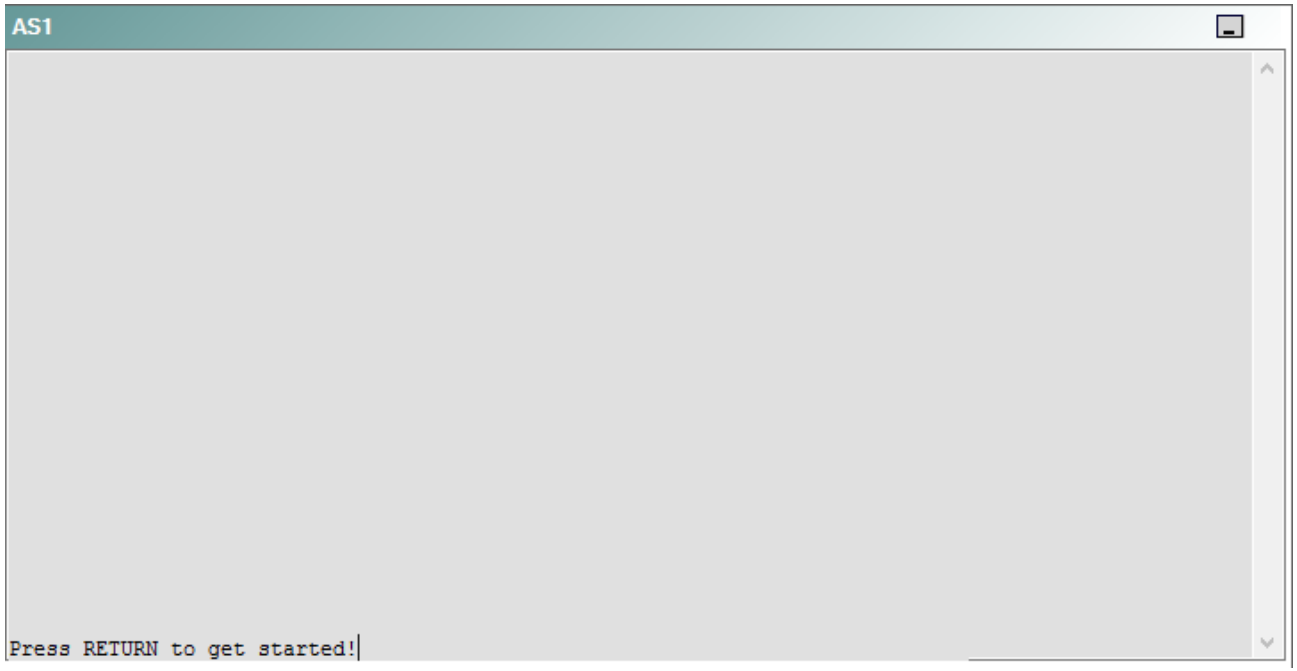

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** H
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

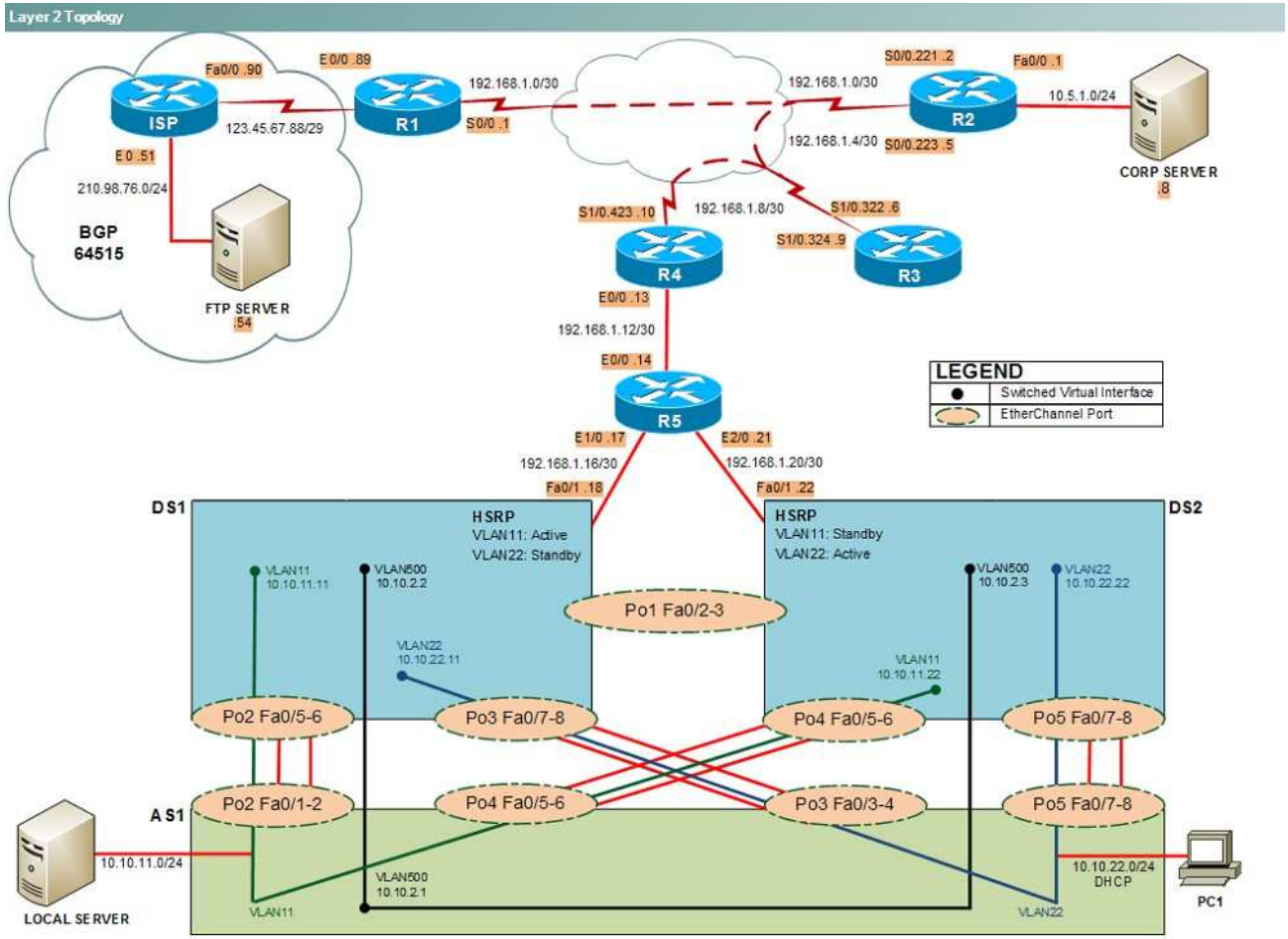
Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

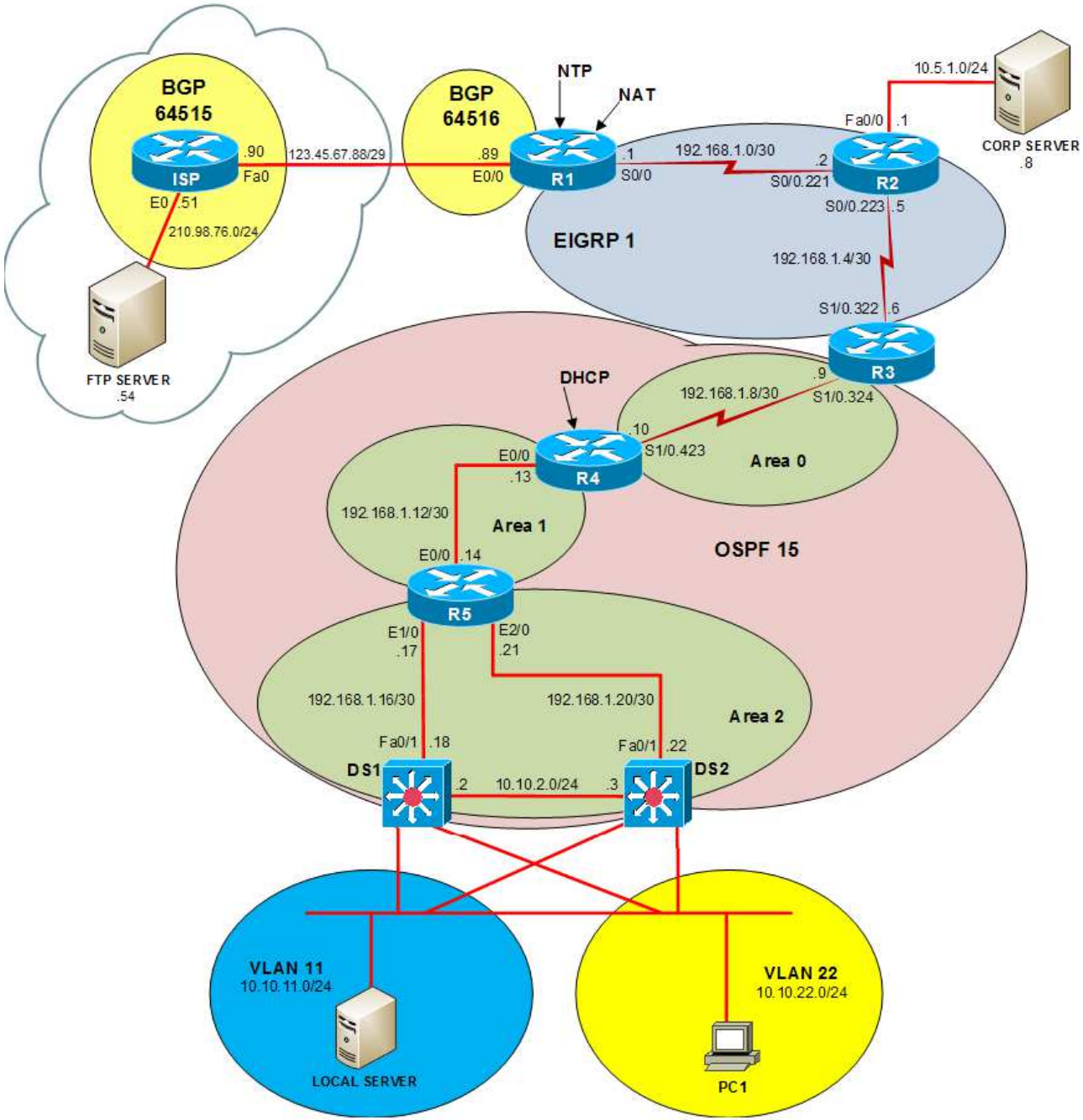
https://www.gratisexam.com/

**Layer 2 Topology**

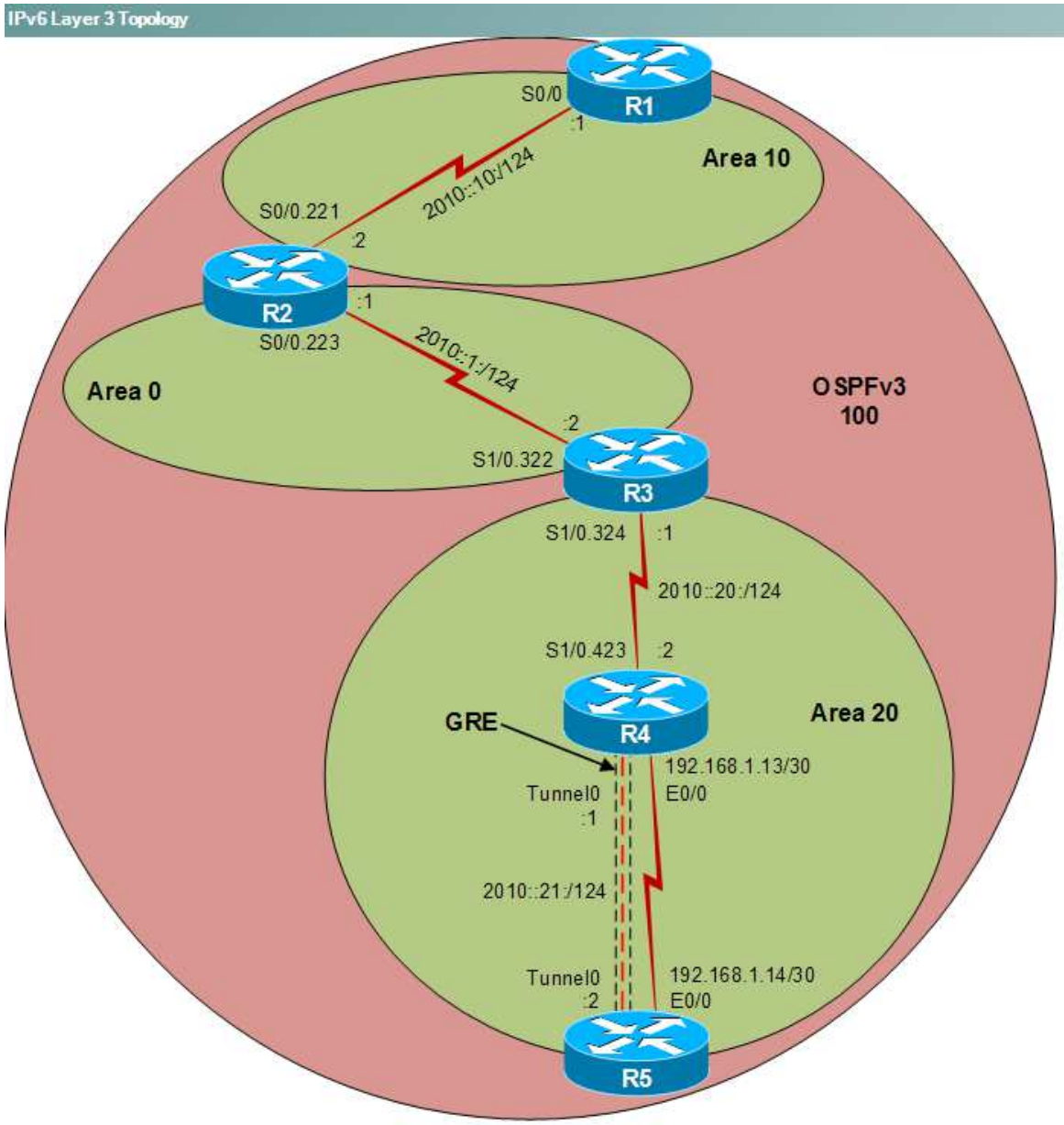



https://www.gratisexam.com/

IPv4 layer 3 Topology

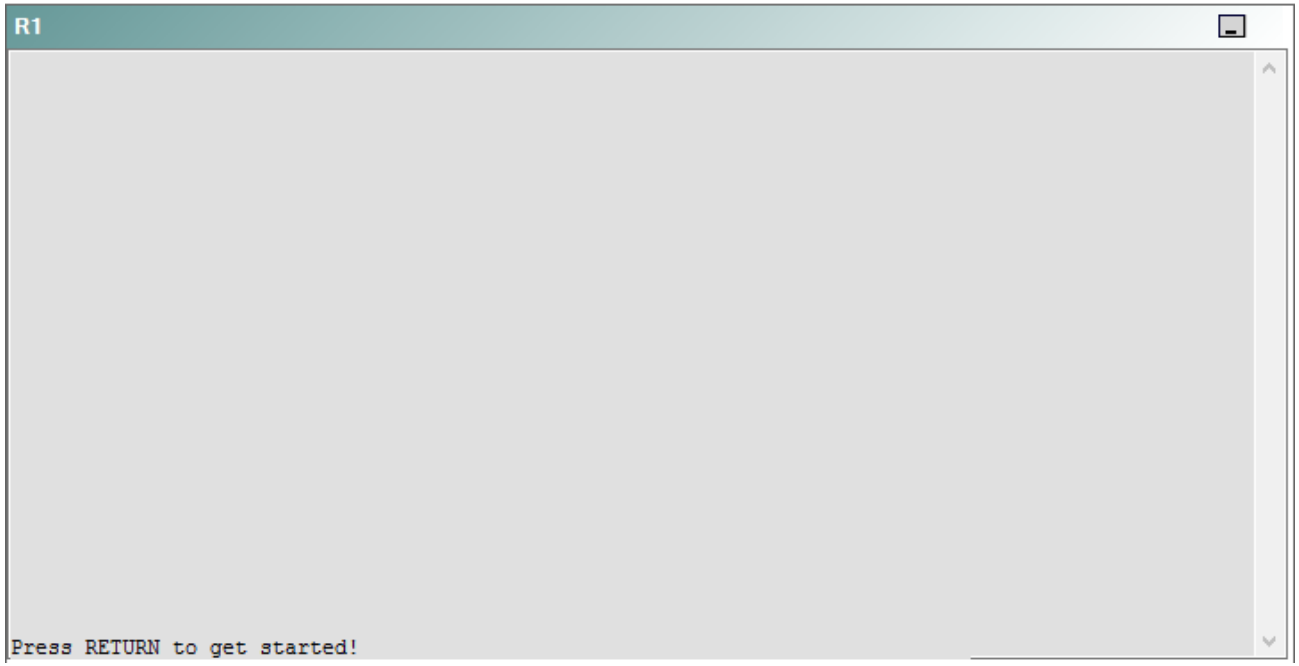

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

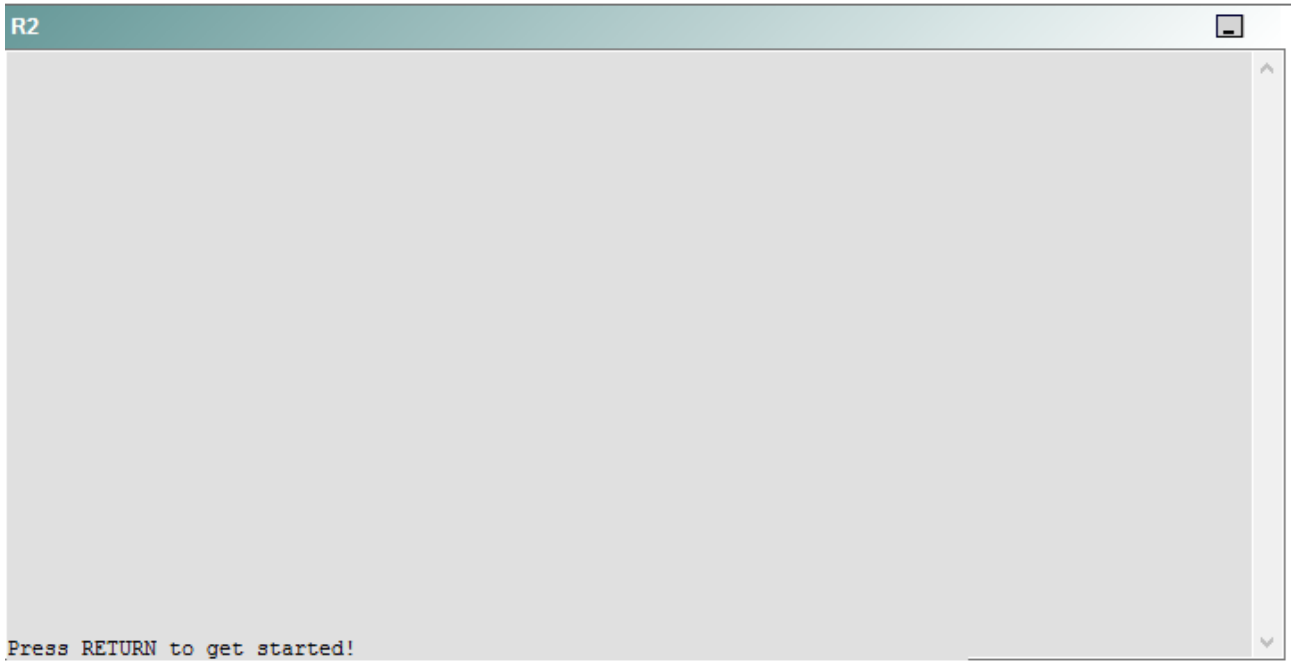



https://www.gratisexam.com/

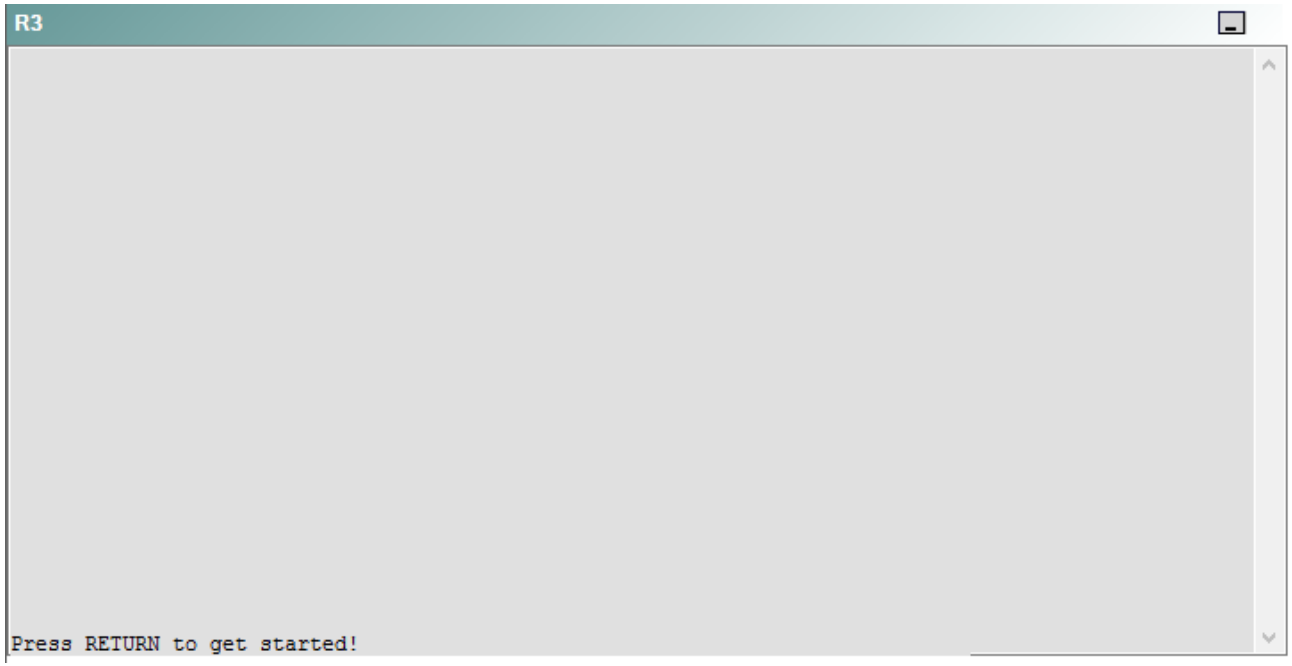
R1



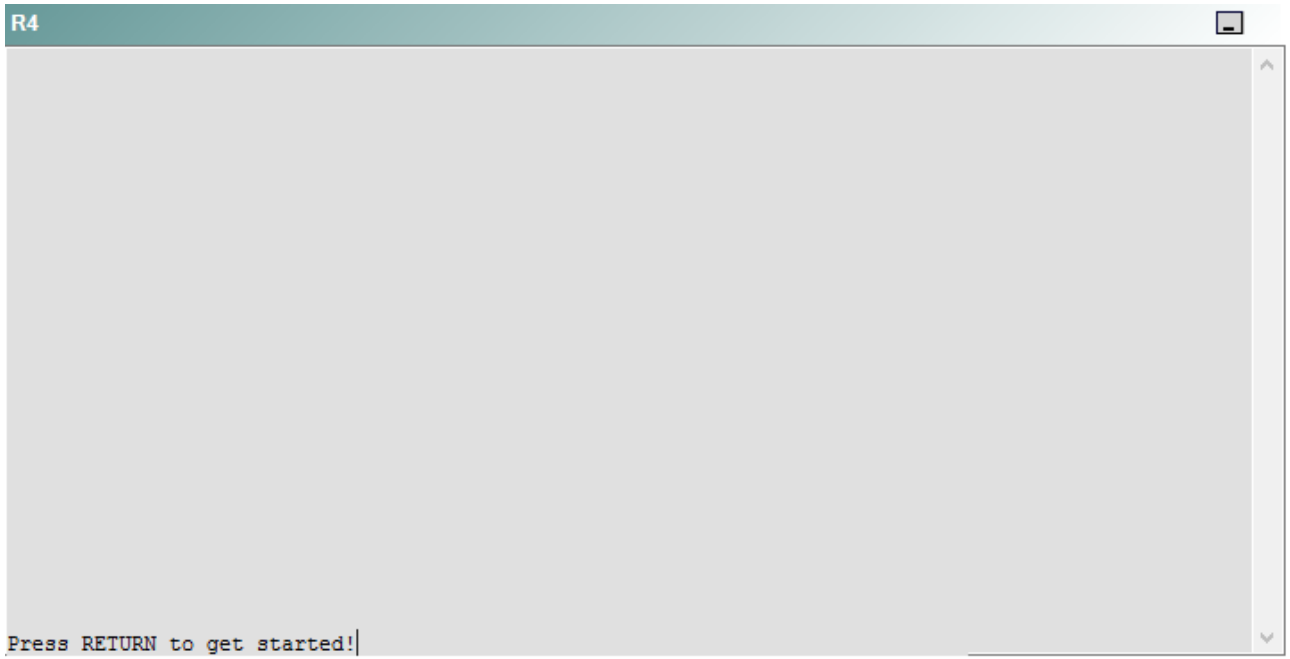

R2



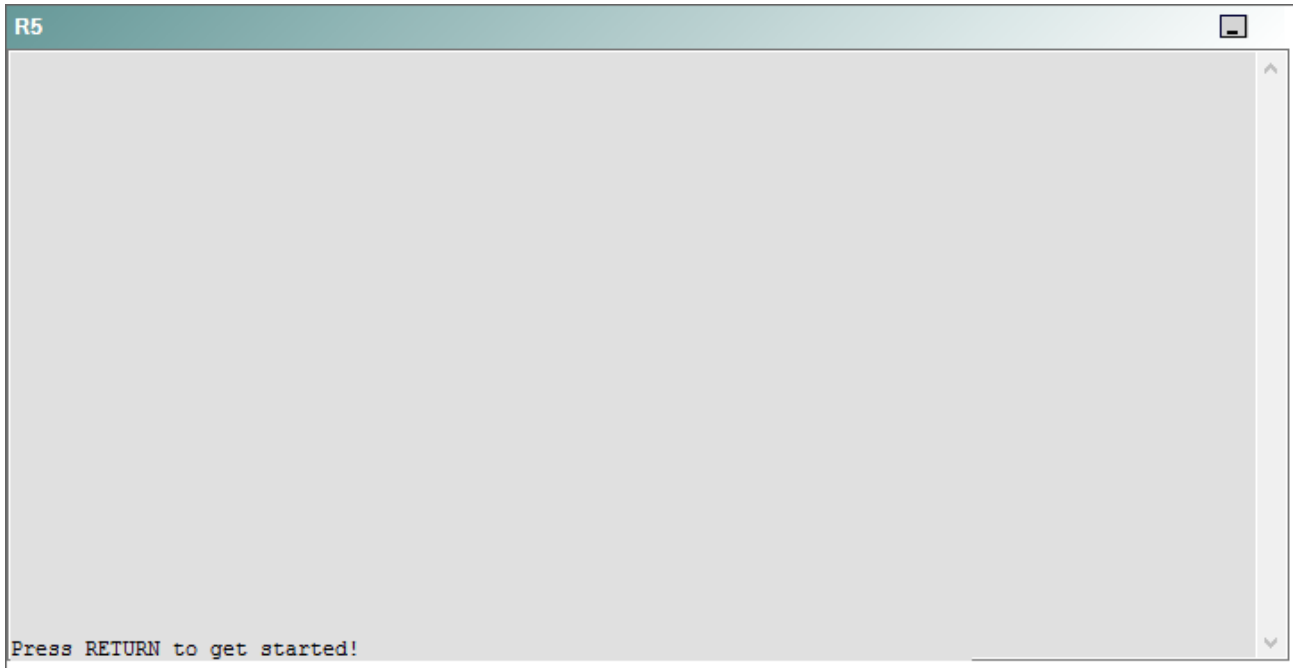

R3



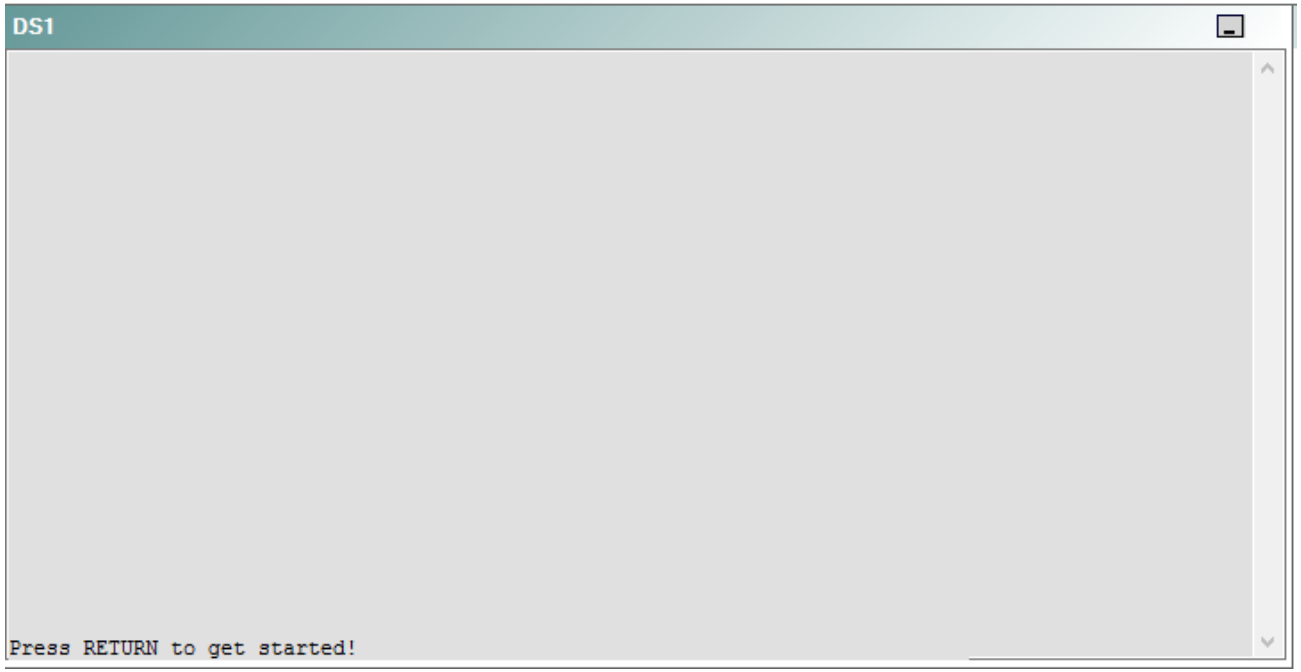

R4



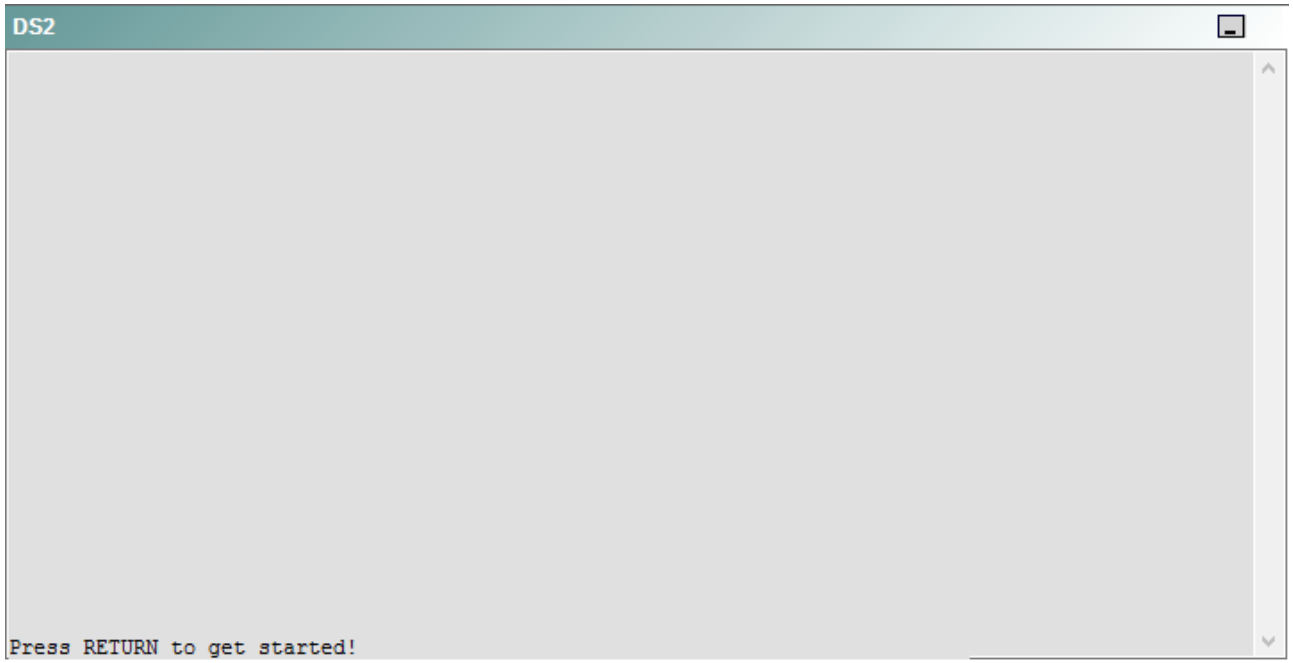

R5



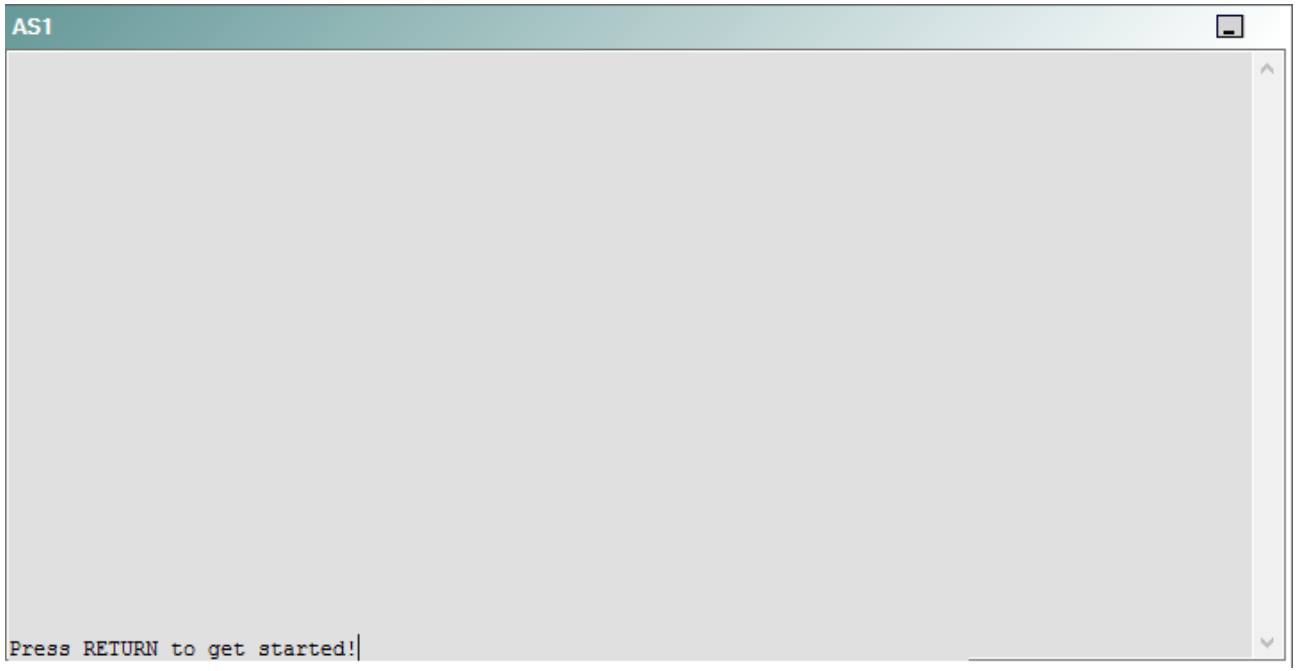

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. DHCP
C. Layer 3 addressing
D. Layer 3 security
E. Layer 2 security
F. STP
G. Etherchannel
H. VLAN configuration
I. interface

**Correct Answer:** E

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

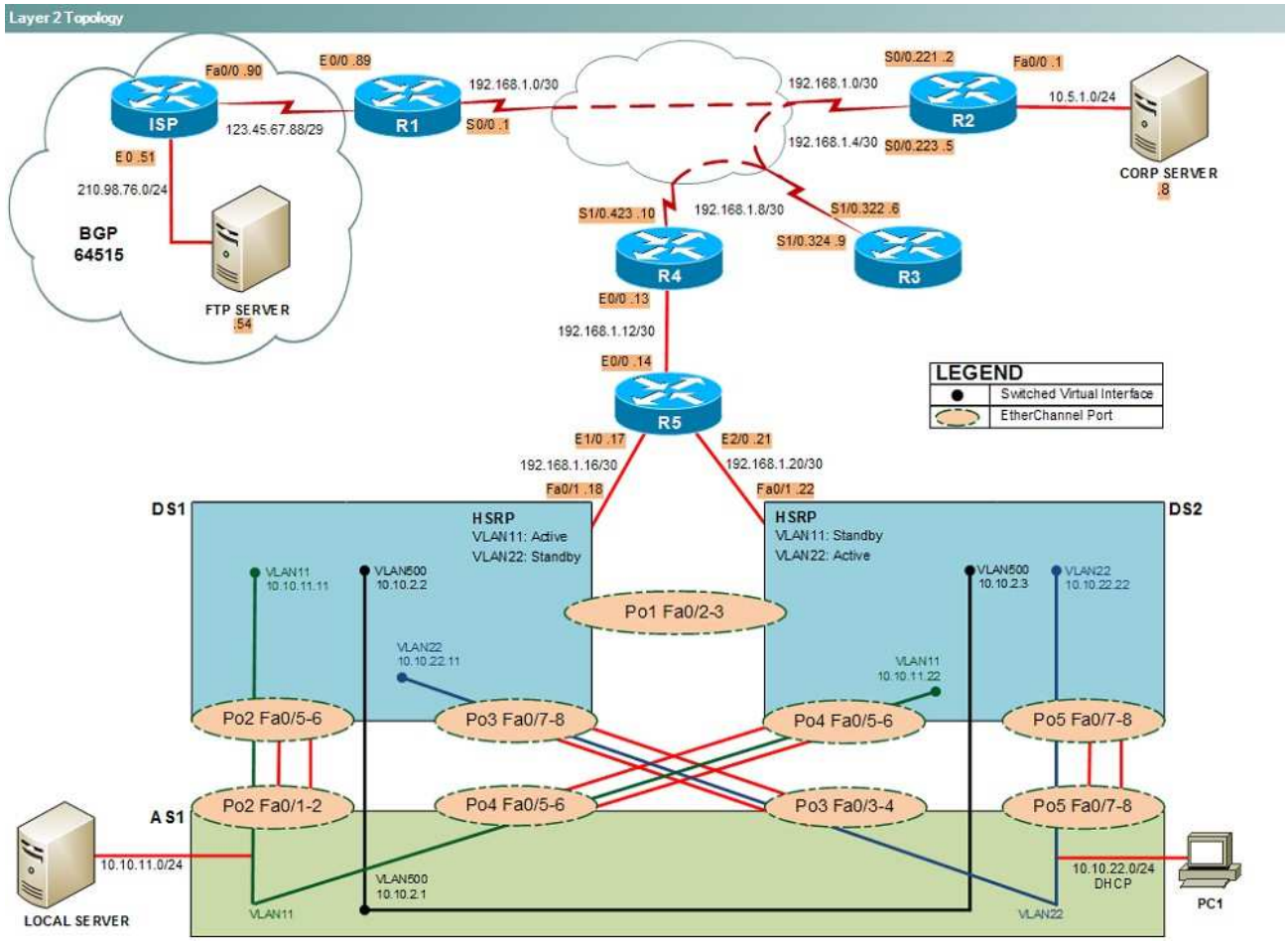
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

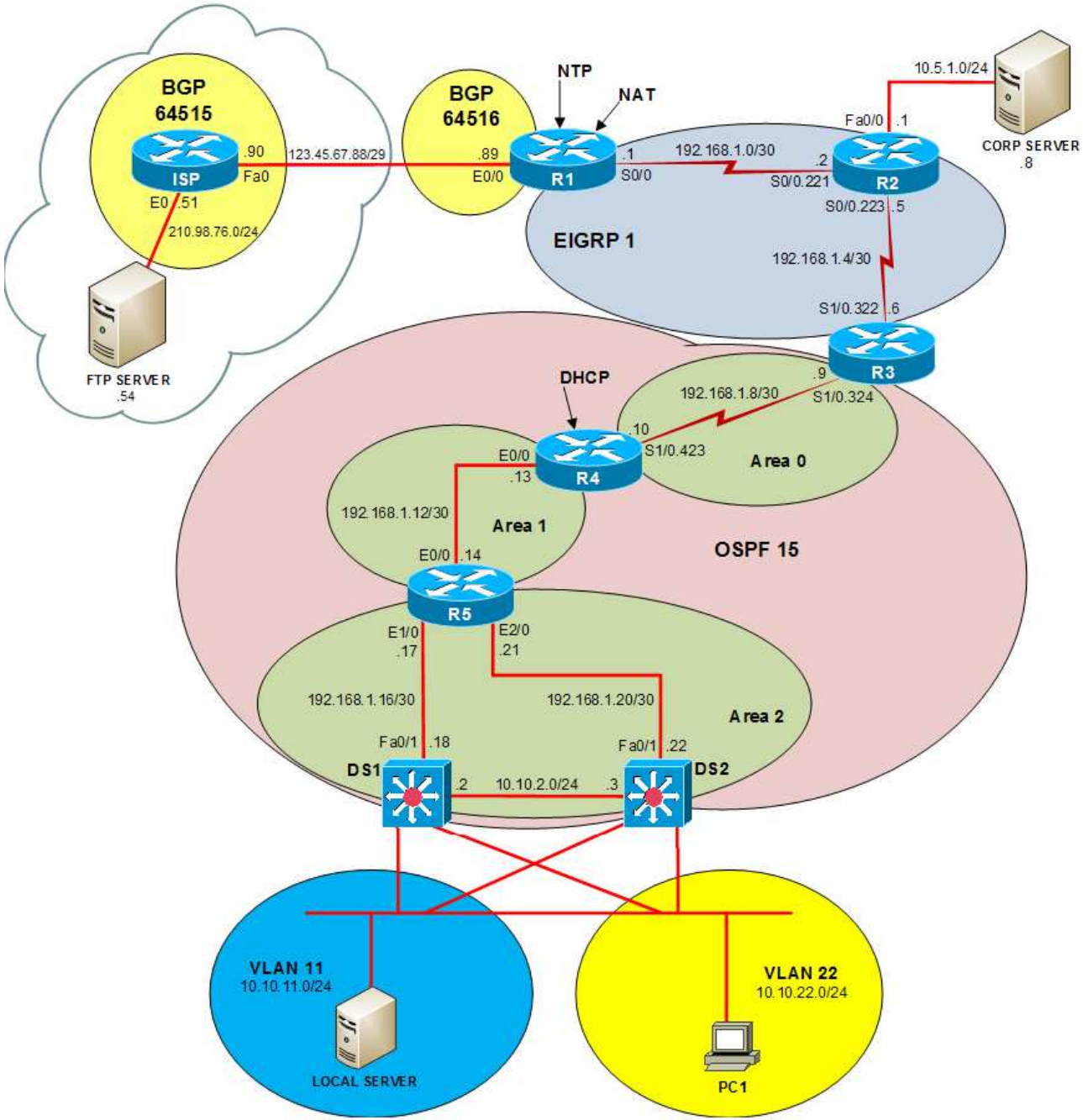
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

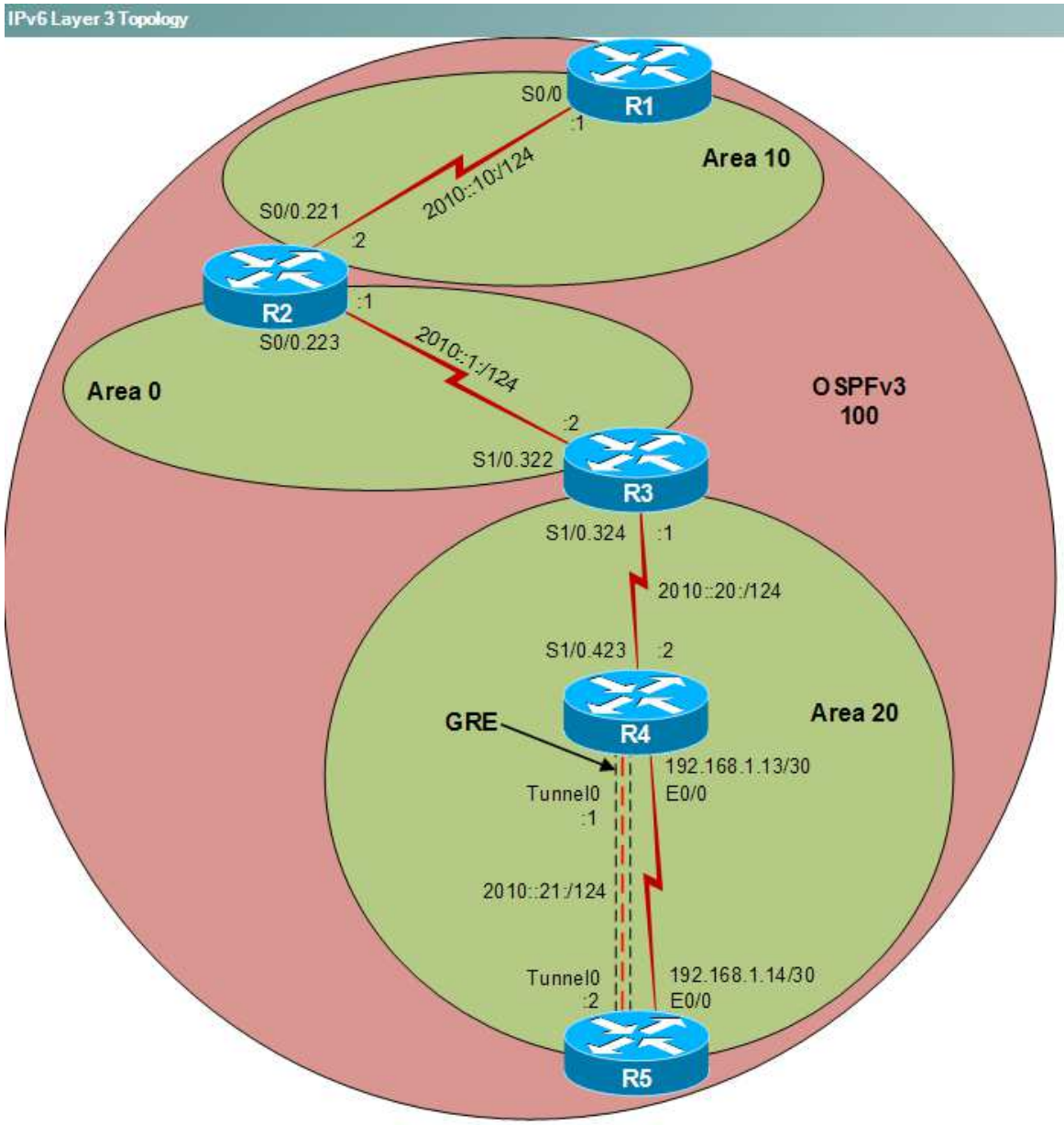
**Layer 2 Topology**




IPv4 layer 3 Topology

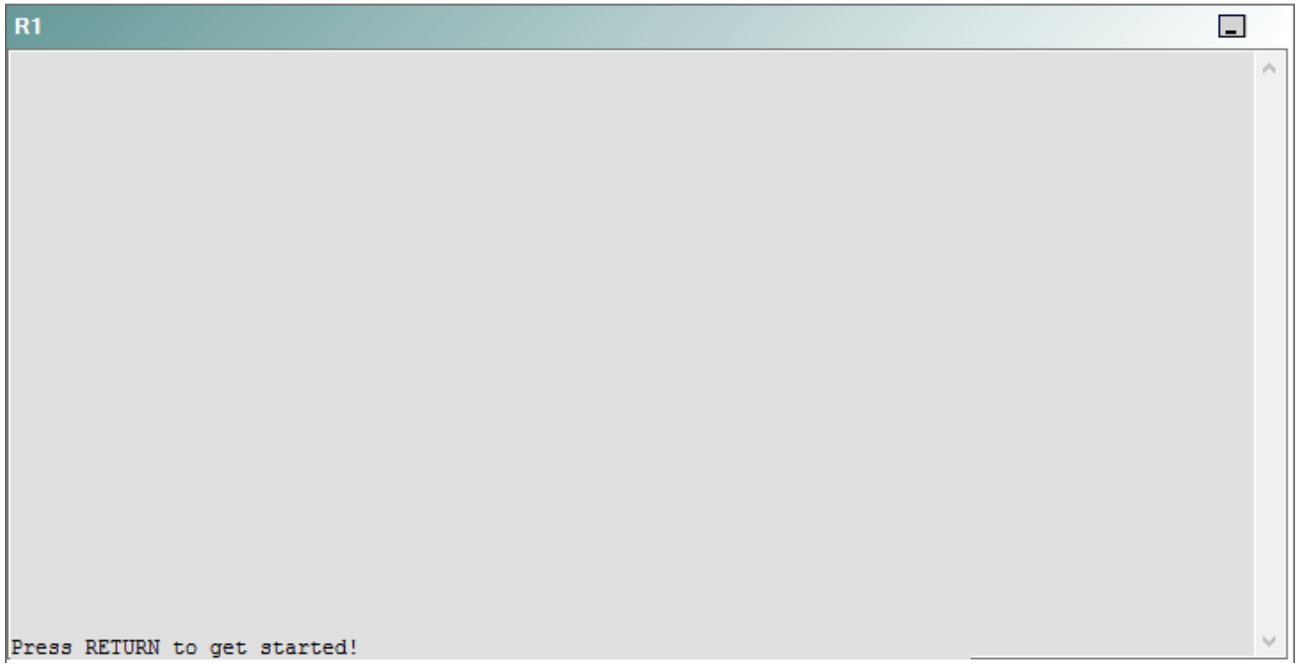

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

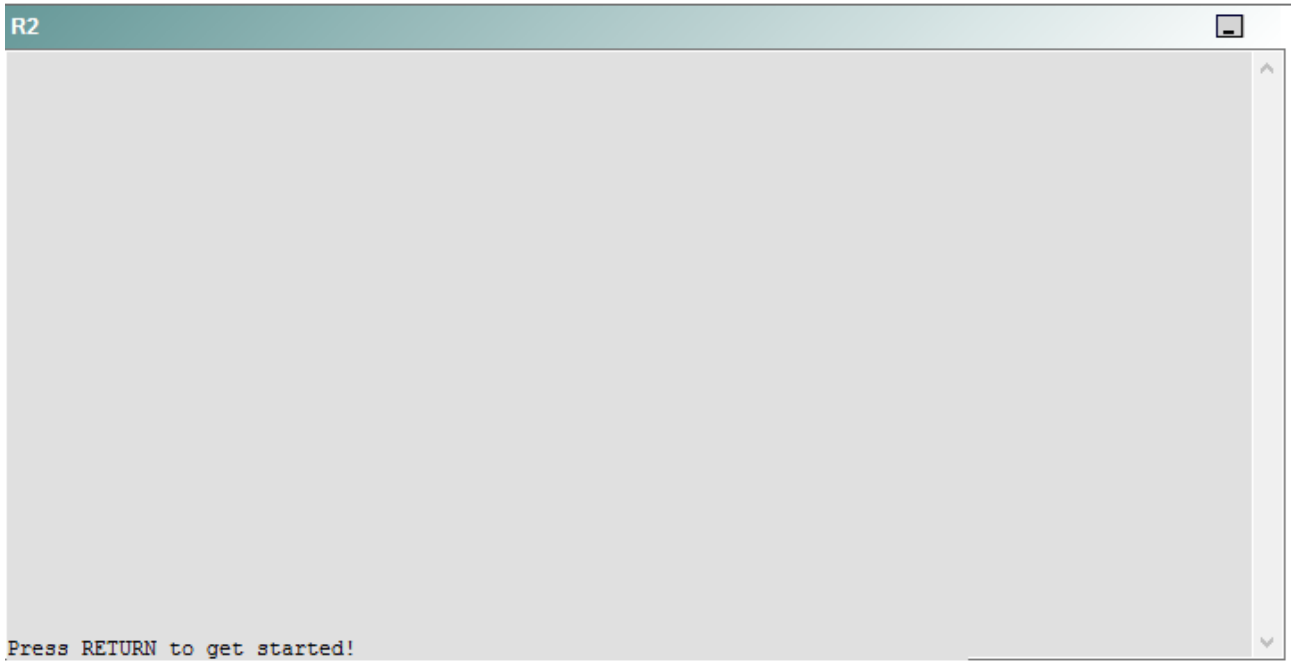



https://www.gratisexam.com/

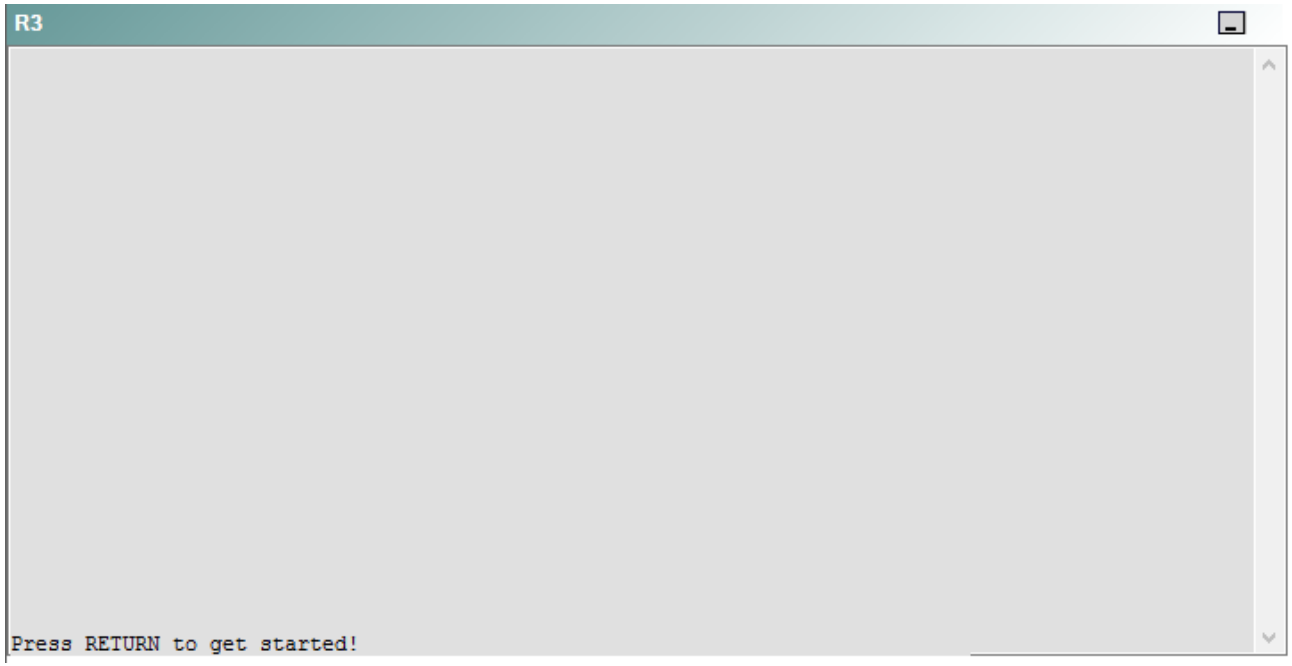
R1



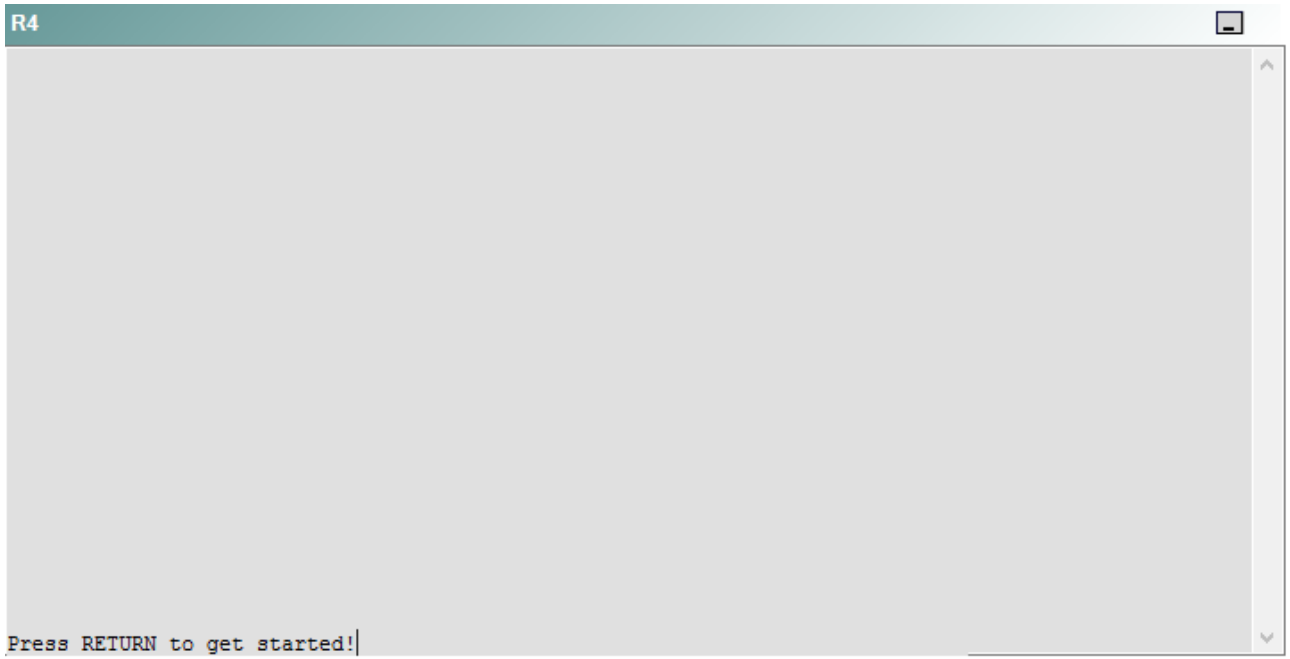

R2



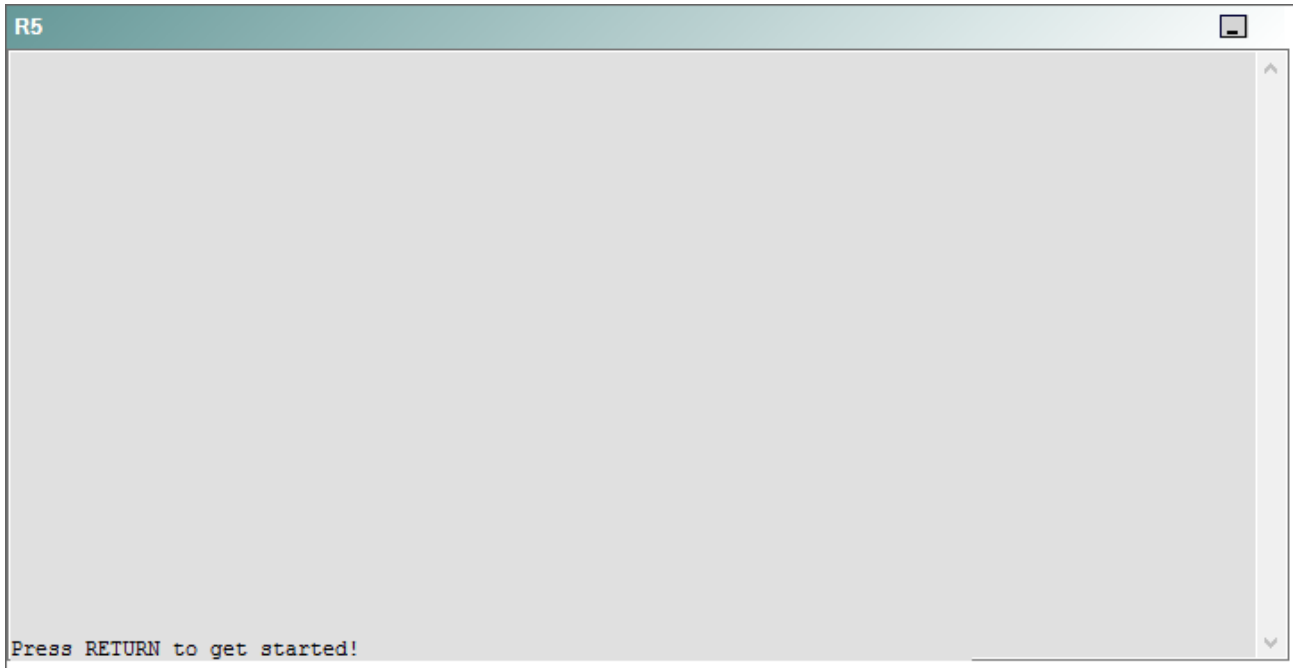

R3



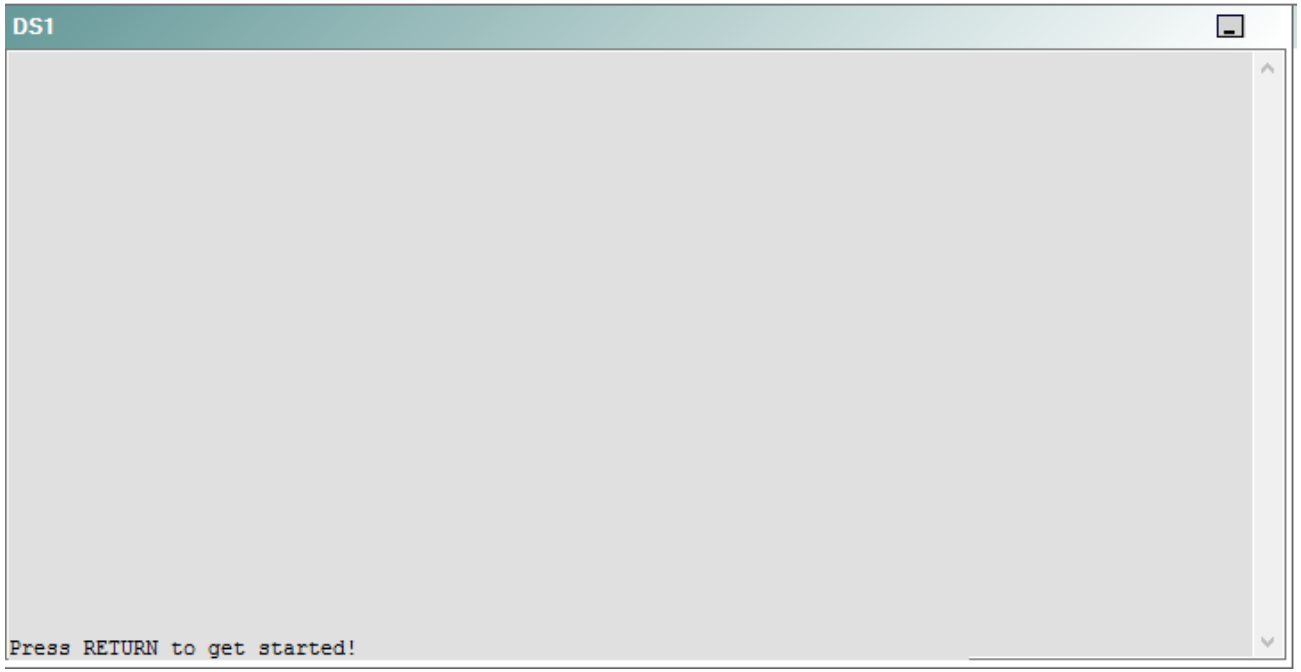

R4



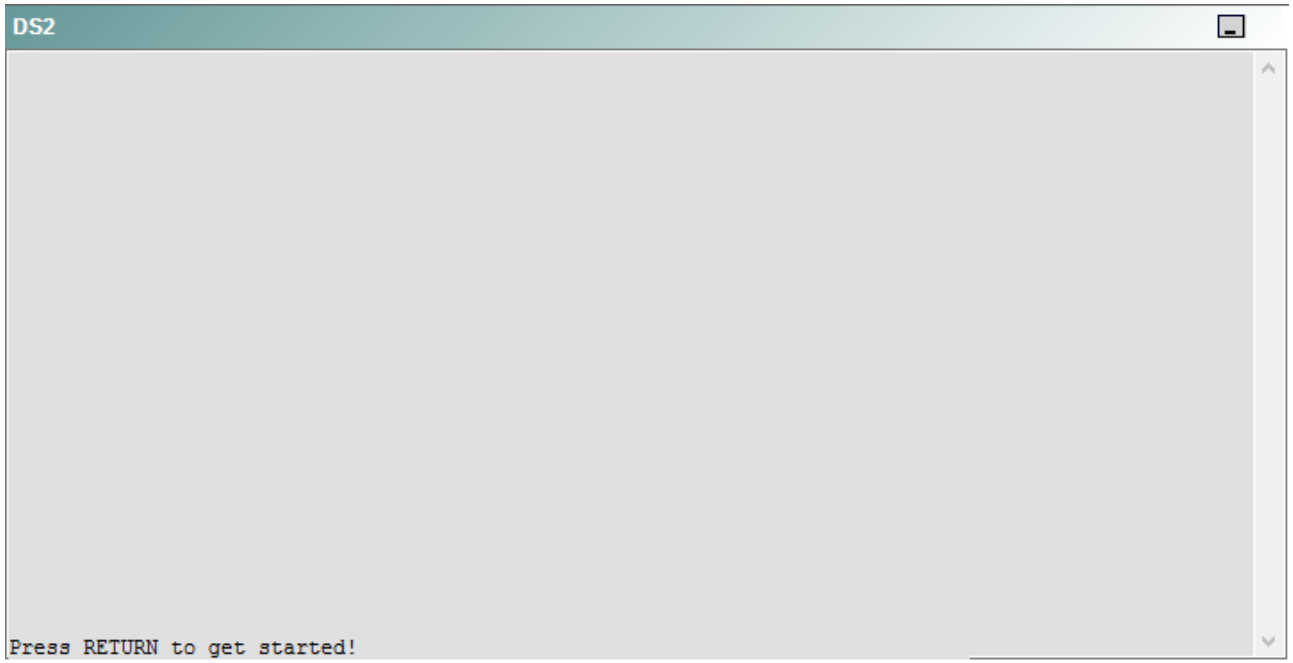

R5



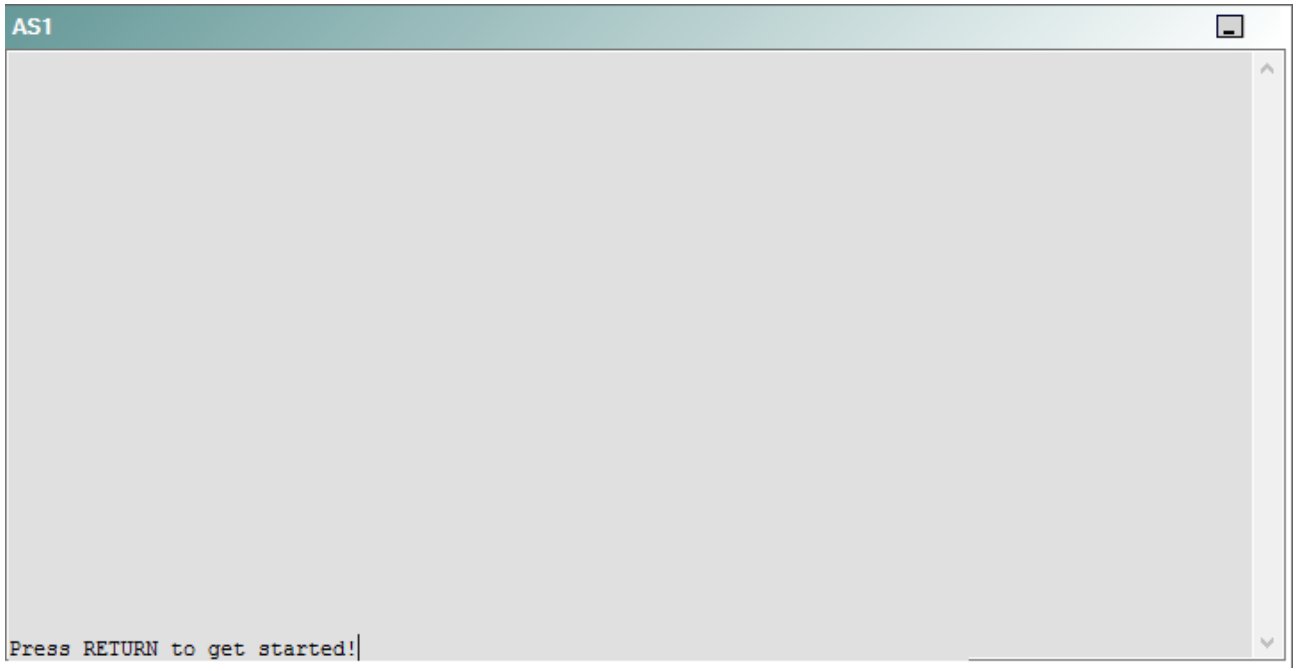

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. issuing the **no port security** command and the **no shutdown** command on Fa0/1 through Fa0/4
B. issuing the **no port security** command and the **no shutdown** command on Fa0/5 through Fa0/8
C. issuing the **no port security** command and the **no shutdown** command on Fa0/11
D. issuing the **no port protected** command on Fa0/11
E. issuing the **port security max-mac-count 0** command on Fa0/1 through Fa0/8
F. issuing the **port security max-mac-count 0** command on Fa0/1 through Fa0/11

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

You should issue the **no port protected** command on the FastEthernet0/11 interface on AS1. To determine which device is the source of the problem, you should issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from R5 to the closest device and work your way up until communication is lost, or you can ping from R5 to the farthest device and work your wat back to R5 until pings are successful. Alternatively, you can trace from R5 to R1 and see where communication is lost along the path to the destination device.

In this scenario, if you were to issue the **ping 210.98.76.54** command from PC1, you would receive the following output:

```
Pinging 210.98.76.54 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
```

The `Destination host unreachable` message in the output above indicates that there is no route from PC1 to the IP address 210.98.76.54, which is the IP address assigned to the external server. You would receive similar output if you were to issue the **ping 10.10.22.25** command from PC1. The IP address 10.10.22.25 is the virtual IP address assigned to the Hot Standby Router Protocol (HSRP) configuration on DS1 and DS2.

Additionally, if you were to issue the **ipconfig** command on PC1, you would receive the following partial output:

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Autoconfiguration IP Address. . . : 169.254.181.239
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :
```

The output above indicates that an Open Systems Interconnection (OSI) Data Link layer problem exists between PC1 and AS1, the device to which PC1 is directly connected. The 169.254.181.239 IP address is an Automatic Private IP Addressing (APIPA) address. A host that is configured as a Dynamic Host Configuration Protocol (DHCP) client will be assigned an APIPA address if something interferes with communication between the host and the DHCP server that is responsible for assigning IP addresses. Therefore, the problem most likely lies between PC1 and R4.

If you were to issue the **show running-config** command on AS1, you would receive the following partial output:

```
interface FastEthernet0/5
 description Link to DS2
 port group 4
 port protected
 switchport access vlan 22
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 500
 switchport trunk allowed vlan 1,11,500,1002-1005
 switchport mode trunk
!
interface FastEthernet0/6
 description Link to DS2
 port group 4
 port protected
 switchport access vlan 22
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 500
 switchport trunk allowed vlan 1,11,500,1002-1005
 switchport mode trunk
!
interface FastEthernet0/7
 description Link to DS2
 port group 5
 port protected
 switchport access vlan 22
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 500
 switchport trunk allowed vlan 1,22,500,1002-1005
 switchport mode trunk
!
```

https://www.gratisexam.com/

```
interface FastEthernet0/8
 description Link to DS2
 port group 5
 port protected
 switchport access vlan 22
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 500
 switchport trunk allowed vlan 1,22,500,1002-1005
 switchport mode trunk

. . .

interface FastEthernet0/11
 description Link to Client
 port security
 port security max-mac-count 1
 port security action shutdown
 port protected
 switchport access vlan 22
 switchport trunk native vlan 500
 spanning-tree portfast
```

The output above indicates that the FastEthernet0/11 interface has been configured with port security and with the **port protected** command. The **port security max-mac-count 1** command configures a switch port to only allow a single Media Access Control (MAC) address to connect to the configured port. If a device with a different MAC address connects to the port that is configured with port security, the port security configuration will either send a Simple Network Messaging Protocol (SNMP) trap message or shut down the port, depending on the configuration of the **port security action** command. In this scenario, the **port security action shutdown** command has been issued for the FastEthernet0/11 interface. The FastEthernet0/11 interface on AS1 has not been placed in the administratively down state and no security violation has occurred, as shown in the following output from the **show port security** command on AS1:

```
Secure Port          Secure Addr    Secure Addr  Security   Security Action
                     Cnt (Current)  Cnt (Max)    Reject Cnt
-------------------  -------------  -----------  ---------- ------------------
FastEthernet0/11     1               1           0          Send Trap/Shut Down
```

The output above indicates that the maximum number of MAC address that can connect to the FastEthernet0/11 interface has been configured to 1. Additionally,

the `Security Reject Cnt` field in the output above indicates that no security incidents have occurred on the FastEthernet0/11 interface. However, the **port protected** command has also been issued for interfaces FastEthernet0/1 through FastEthernet0/8 and for FastEthernet0/11. When **port protected** has been configured on an interface, no Layer 2 traffic from that interface can be forwarded through another interface that is configured with the port protected command. Therefore, the FastEthernet0/11 interface cannot forward Layer 2 traffic to any of the other connected interfaces on AS1. To solve the problem, you should issue the **no port protected** command on the FastEthernet0/11 interface on AS1 so that the FastEthernet0/11 interface can forward Later 2 traffic to any other interface on AS1.

You need to issue the **no port security** command or the **no shutdown** command on any interfaces on AS1. Port security commands have not been issued on interfaces FastEthernet0/1 through FastEthernet0/8. Additionally, the **show port security** command does not indicate that any port security violations have occurred on the FastEthernet0/11 interface. Therefore, the **port security** command is not causing a problem on the interfaces from FastEthernet0/1 through FastEthernet0/11.

You should not issue the **port security max-mac-count 0** command on any interfaces on AS1, DS1, or DS2. The **port security max-mac-count** *number* command indicates the number of MAC address that can communicate through the port. The *number* parameter can be set to a value from 1 through 132. Therefore, the **port security max-mac-count 0** command contains invalid syntax.

Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1_11_yj/command/reference/cr/intro.html#wp1033345

**QUESTION 16**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

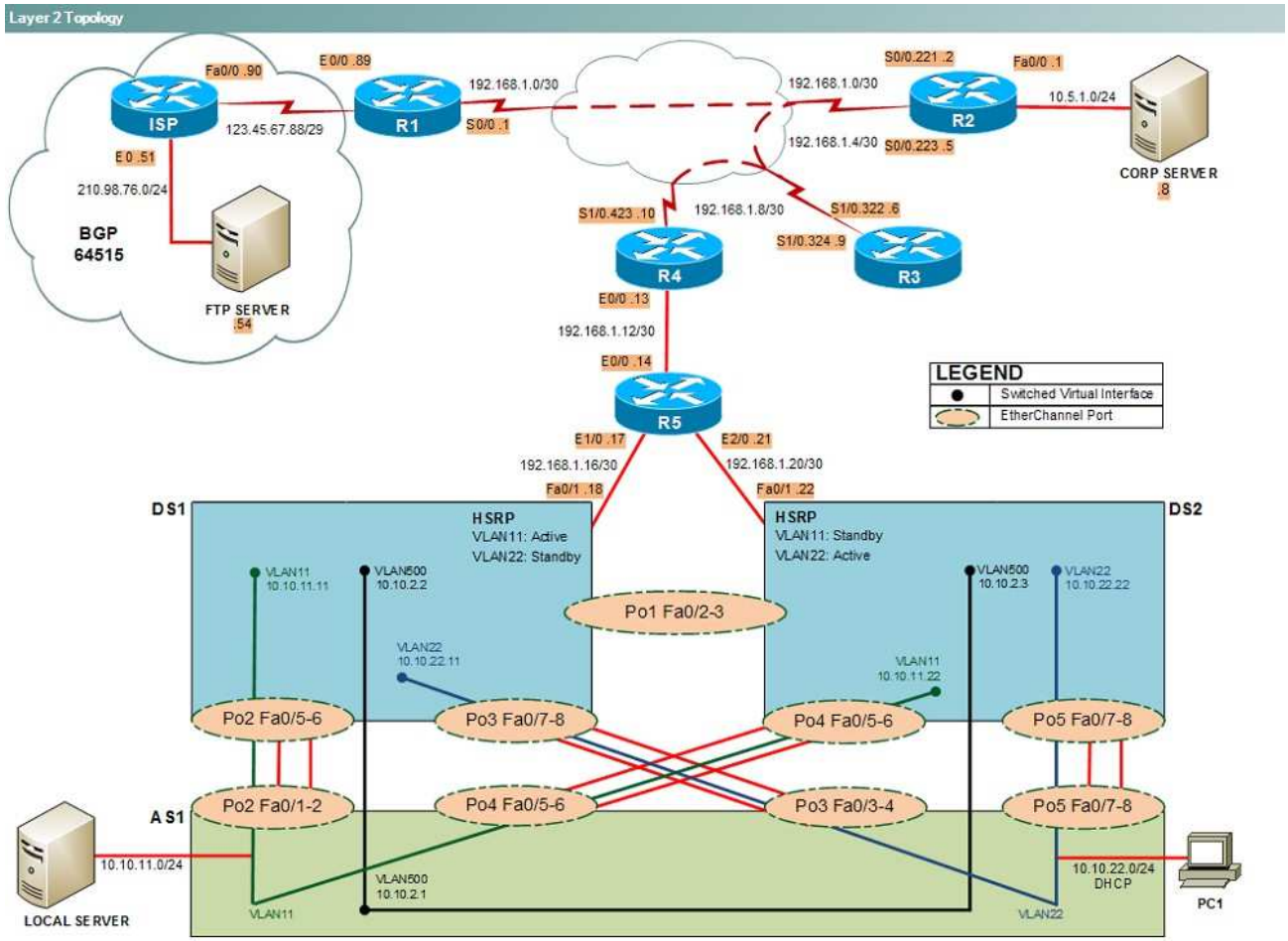
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

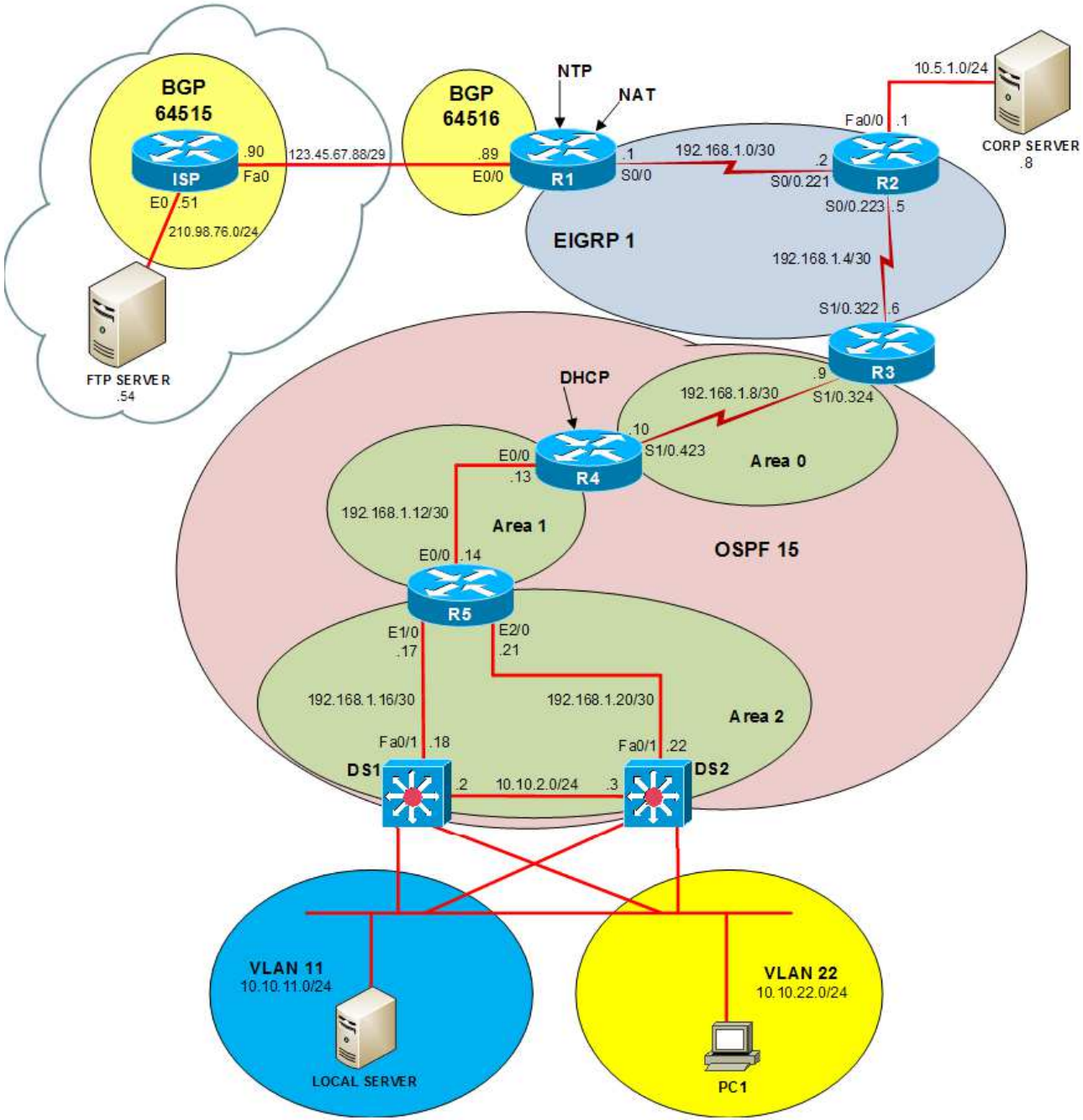
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

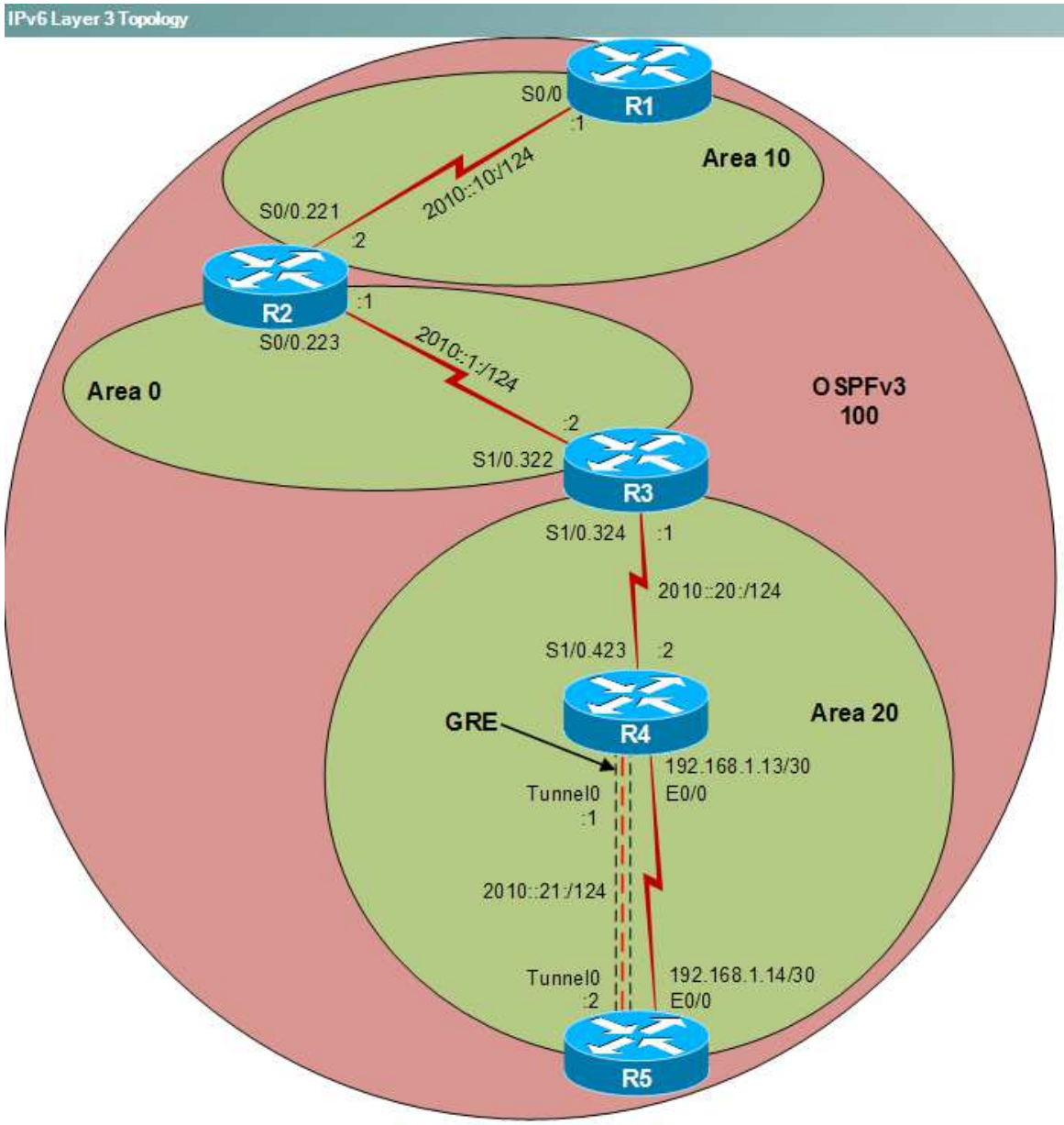
**Layer 2 Topology**




IPv4 layer 3 Topology

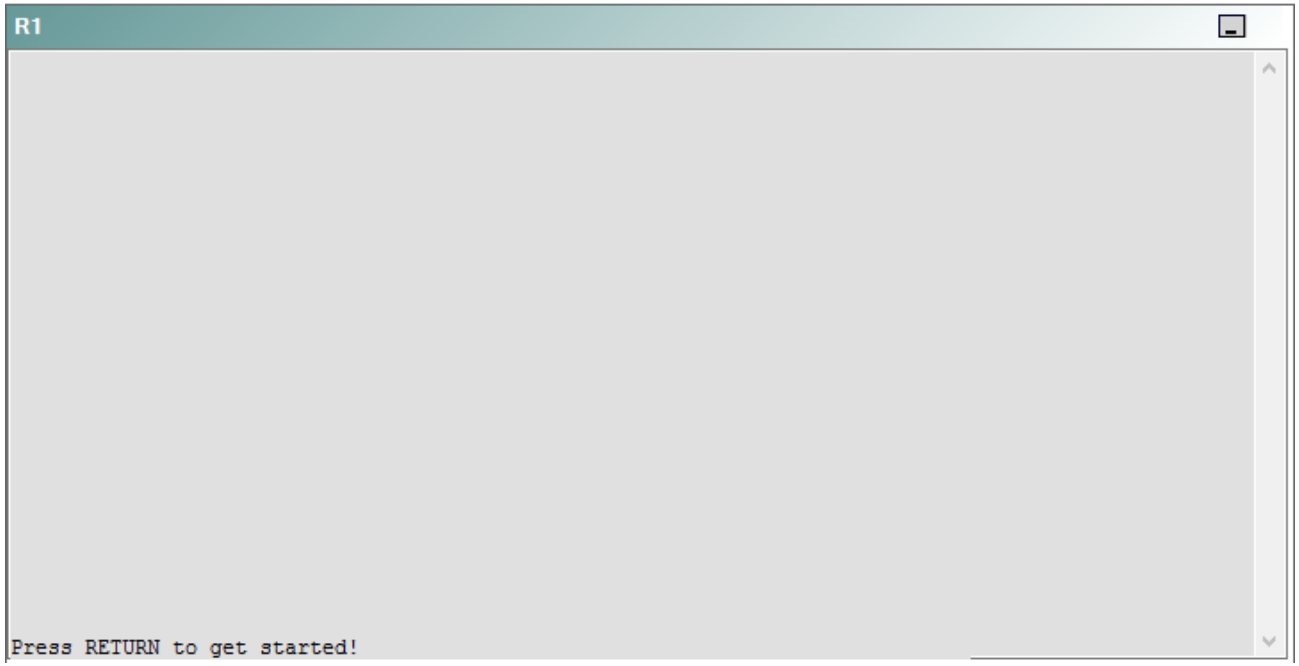

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

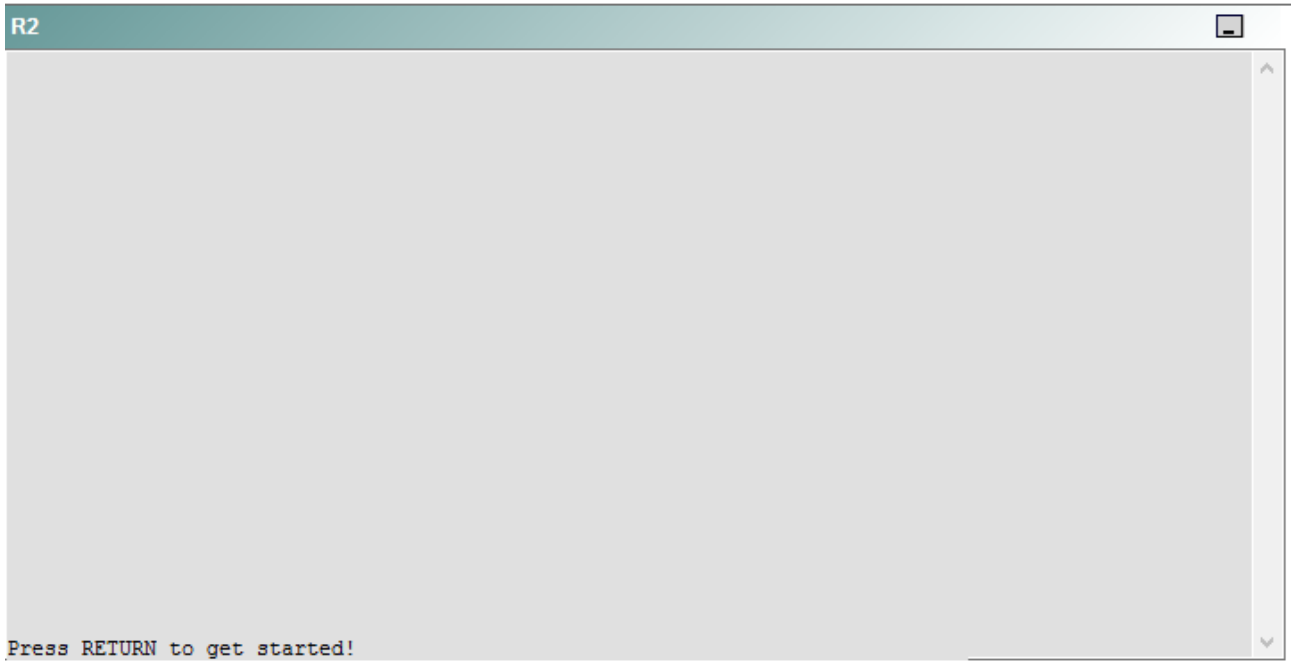



https://www.gratisexam.com/

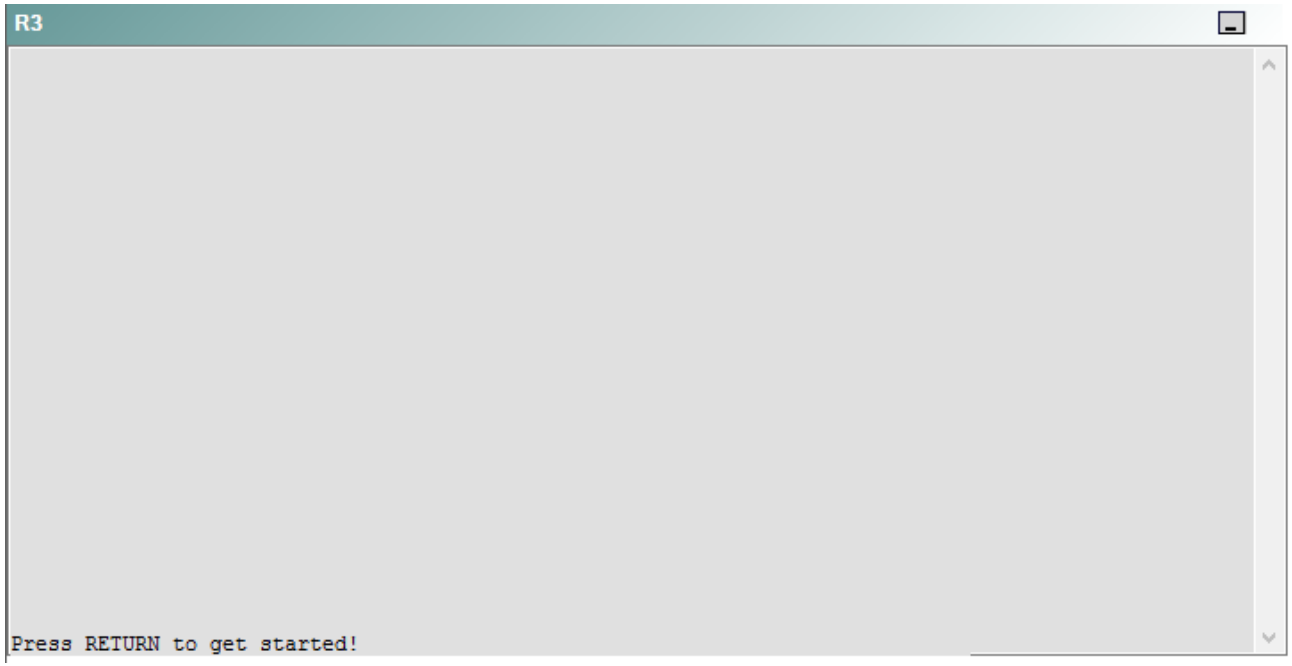
R1



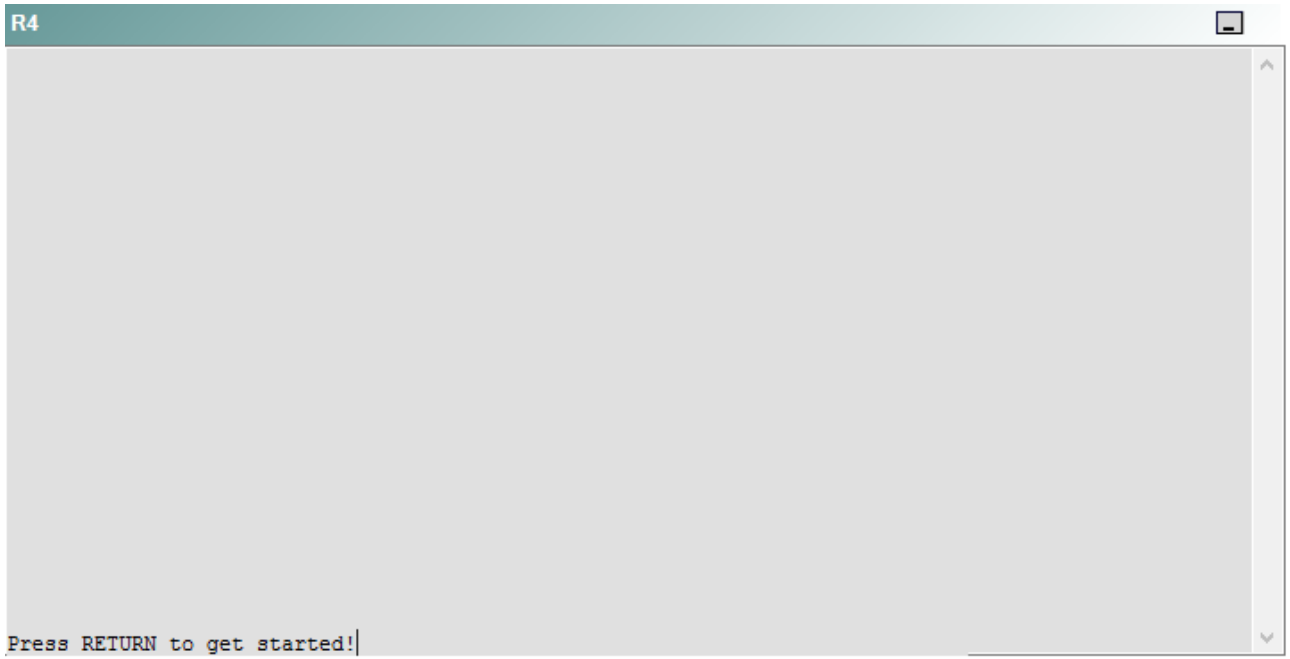

R2



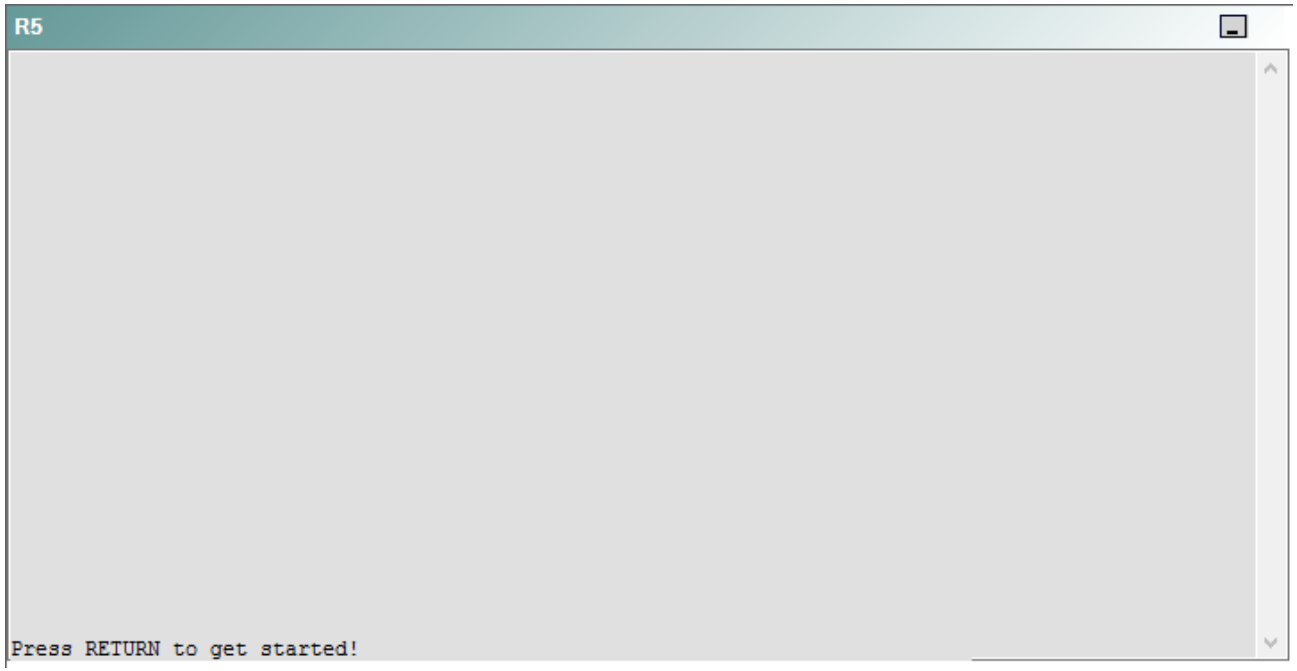

R3



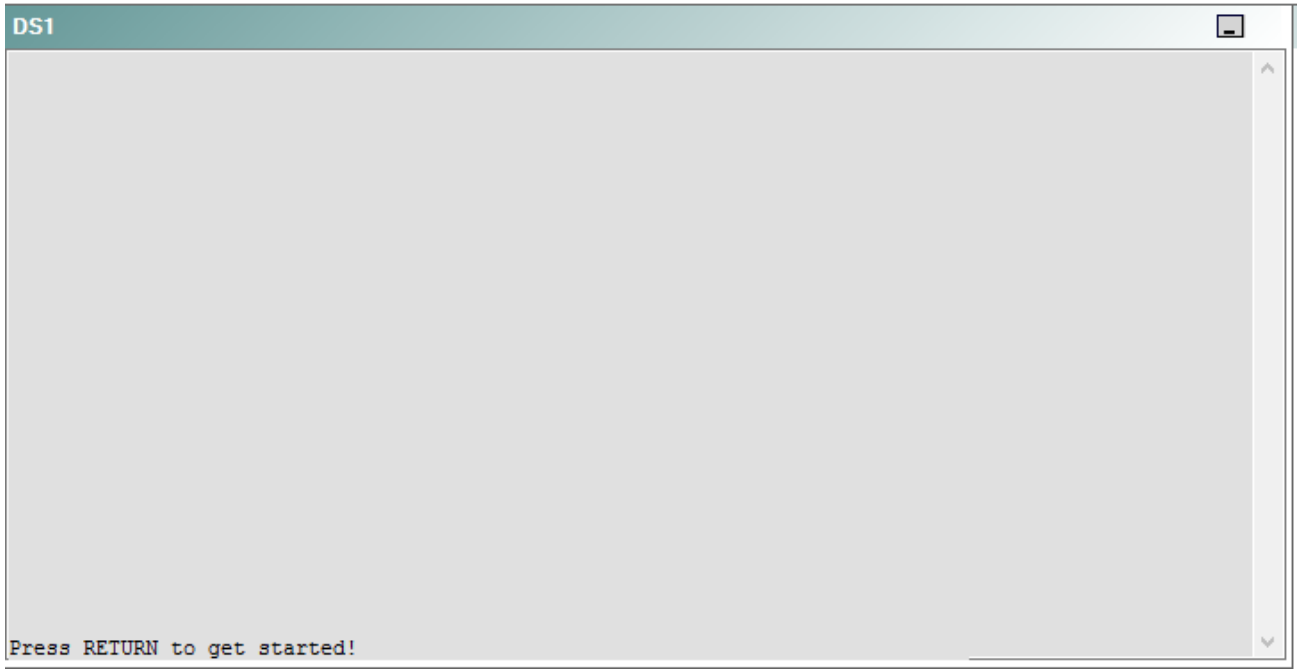

R4



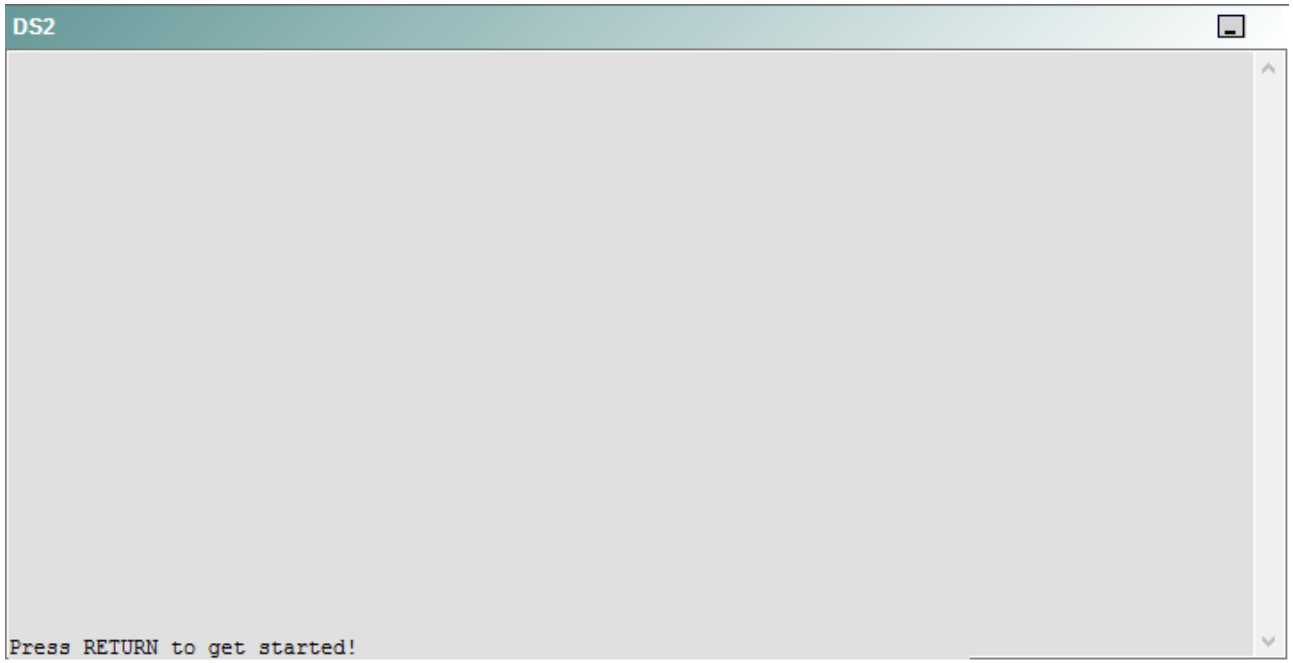

R5



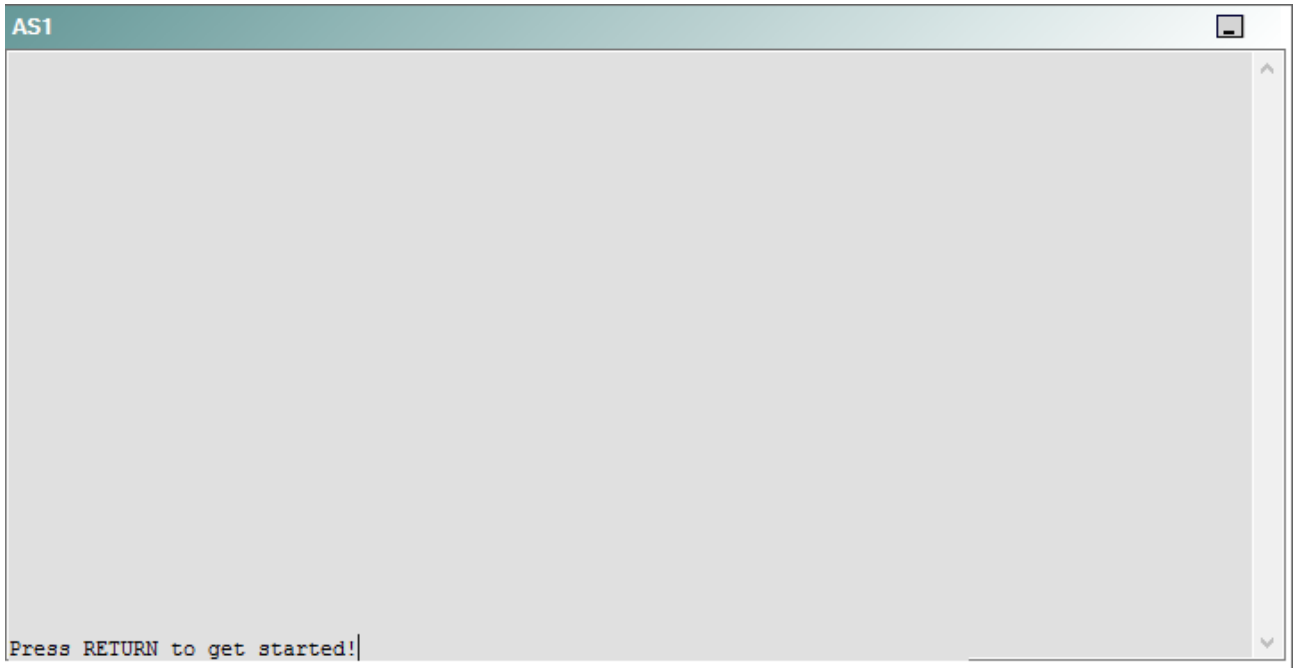

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that the clock on AS1 is not synchronized with the clock on R1.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 17**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

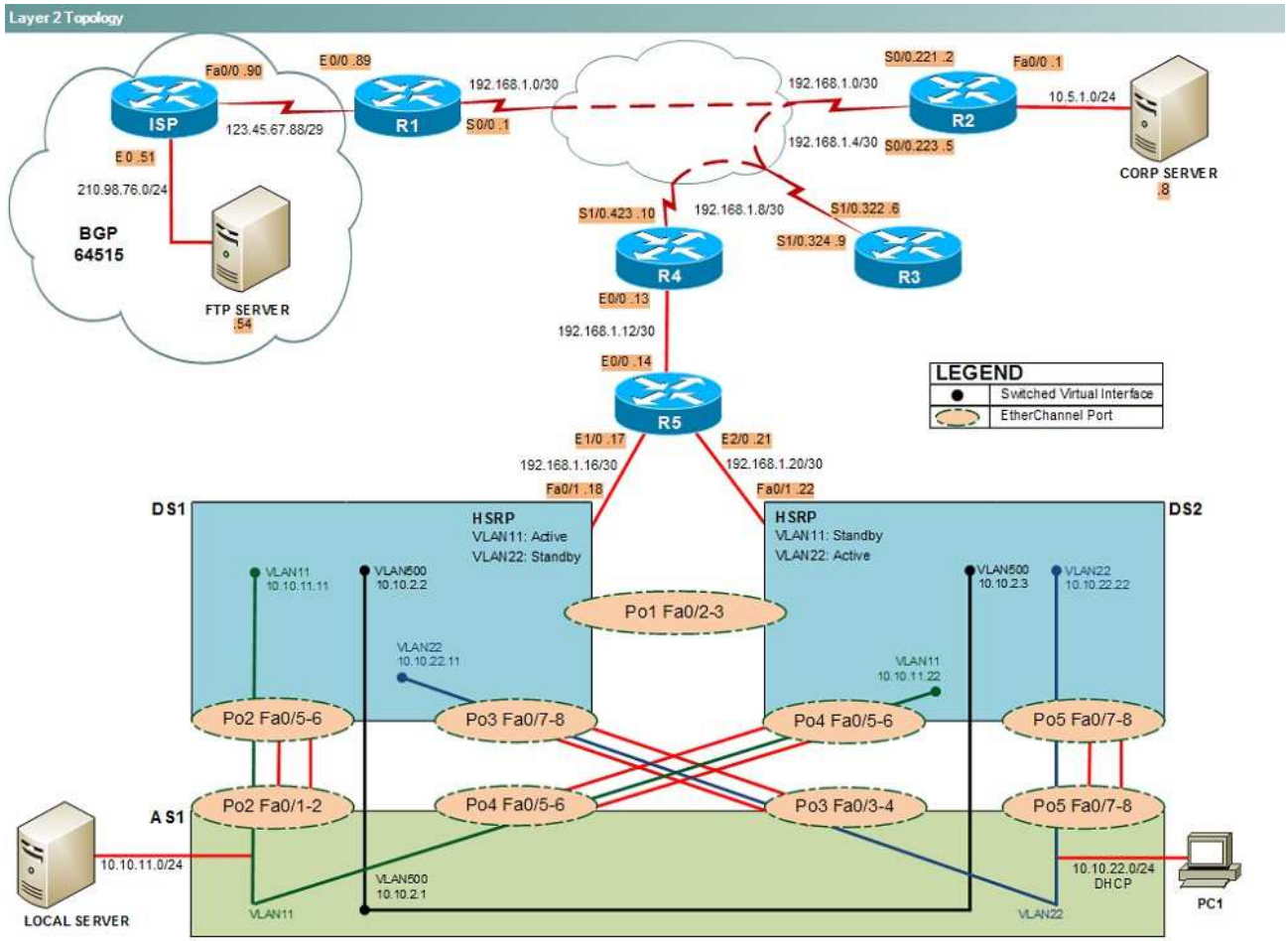
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

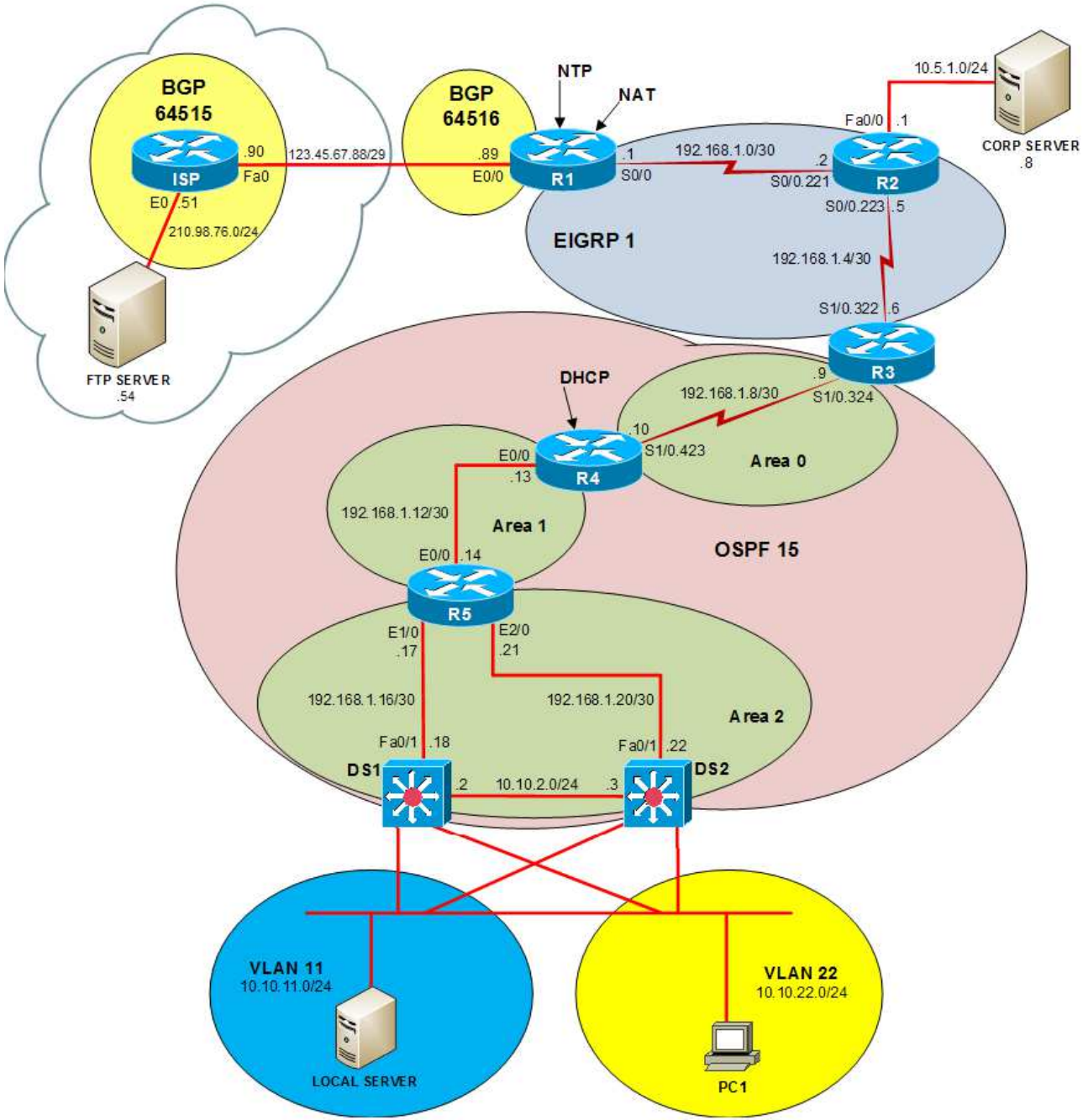
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

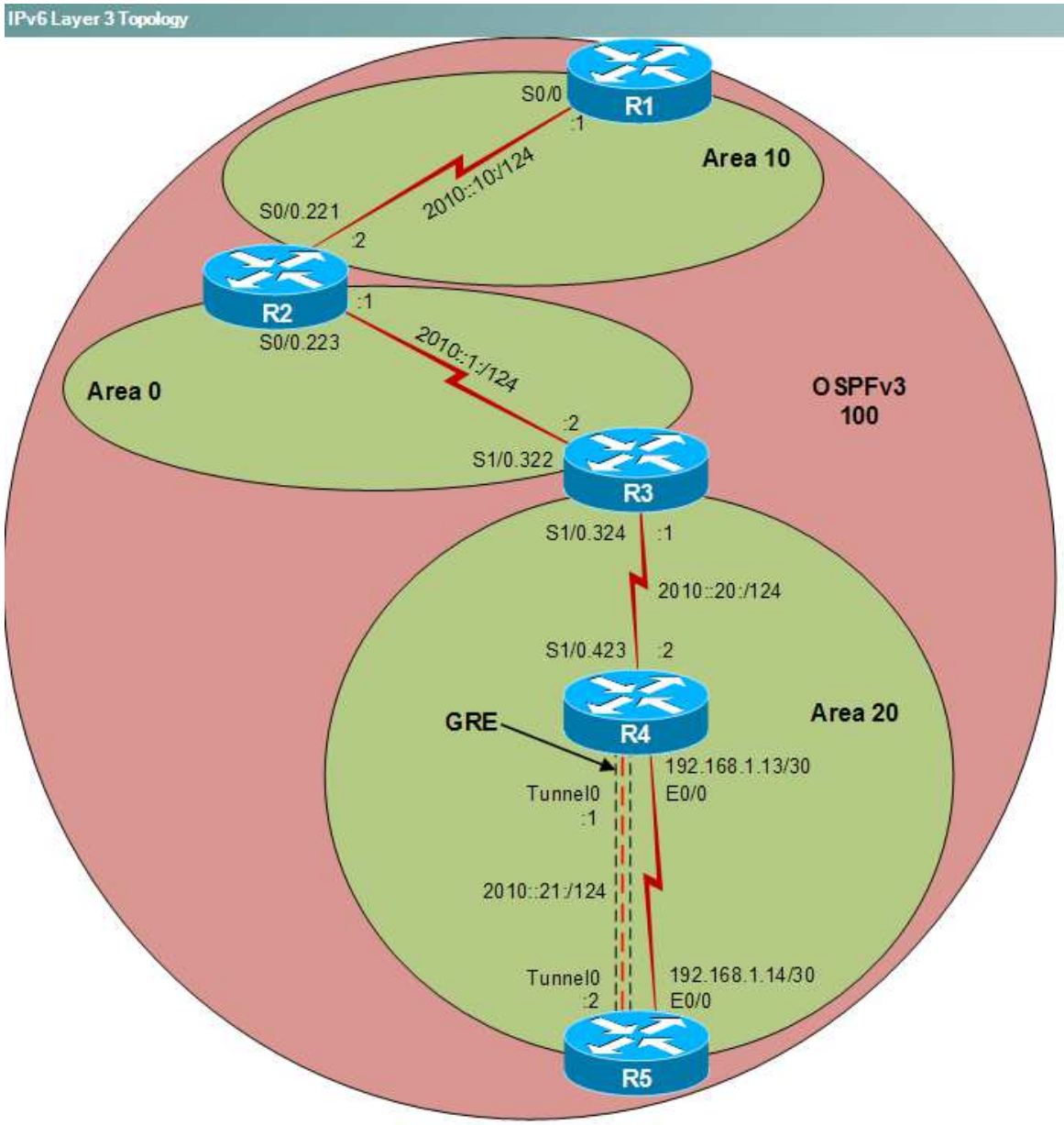
**Layer 2 Topology**




IPv4 layer 3 Topology

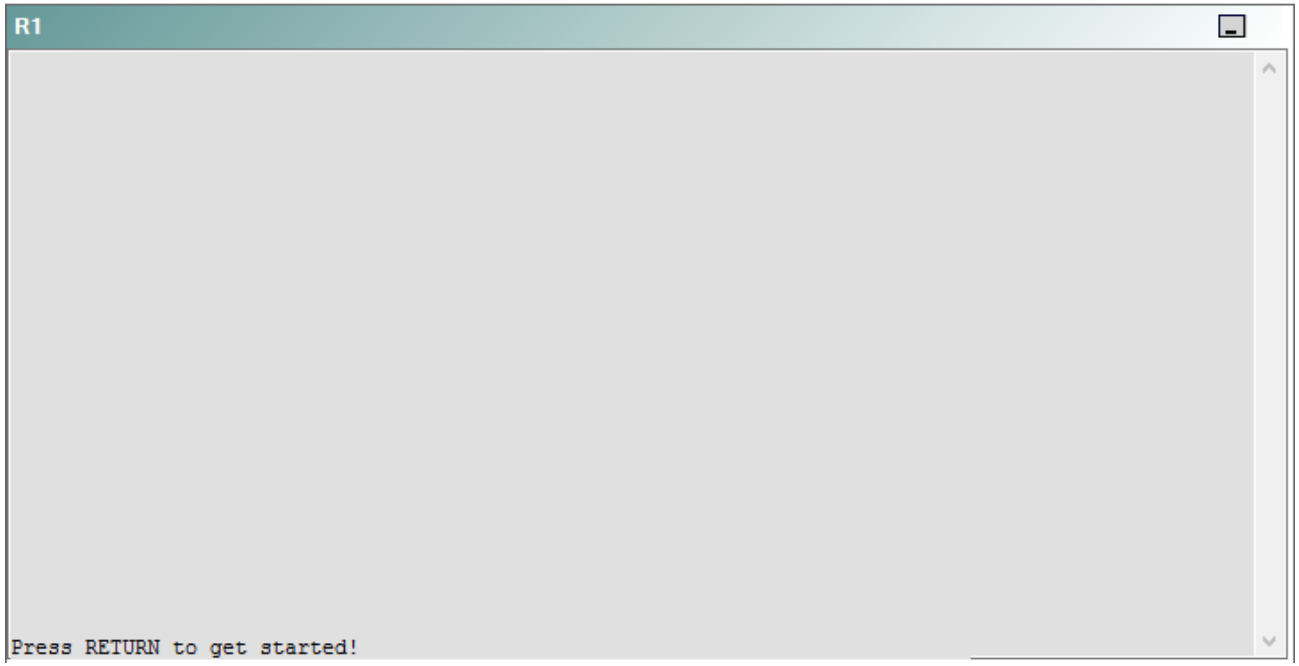

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

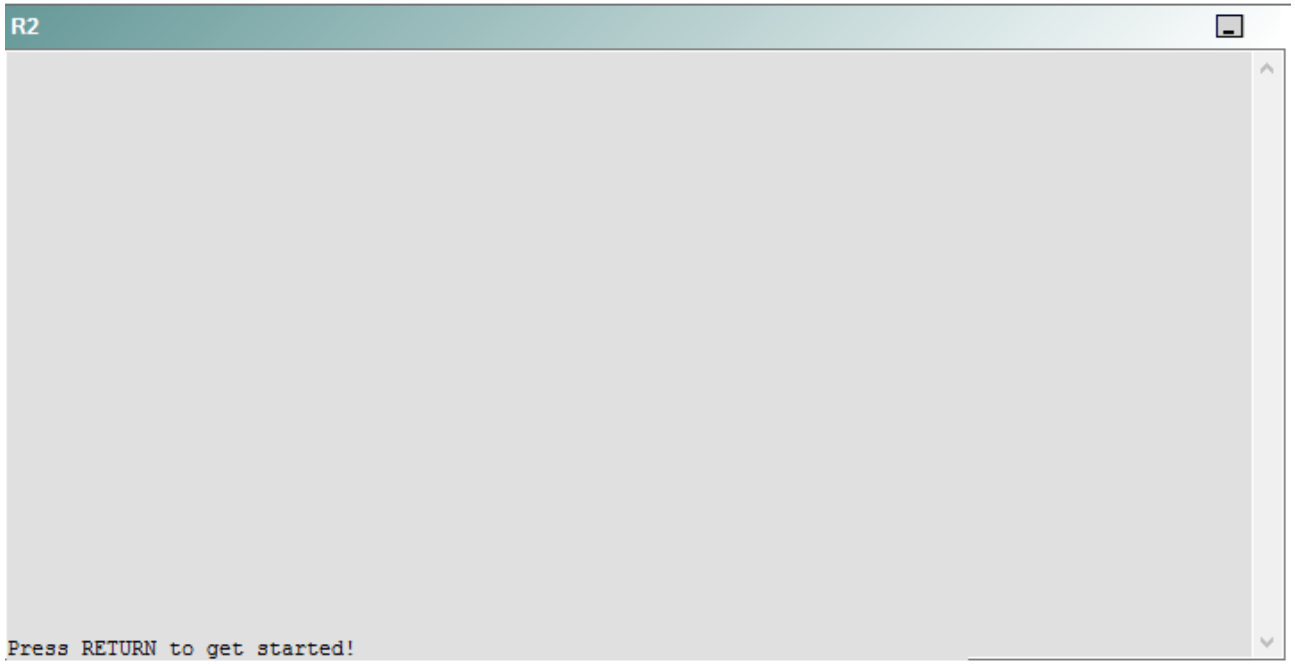



https://www.gratisexam.com/

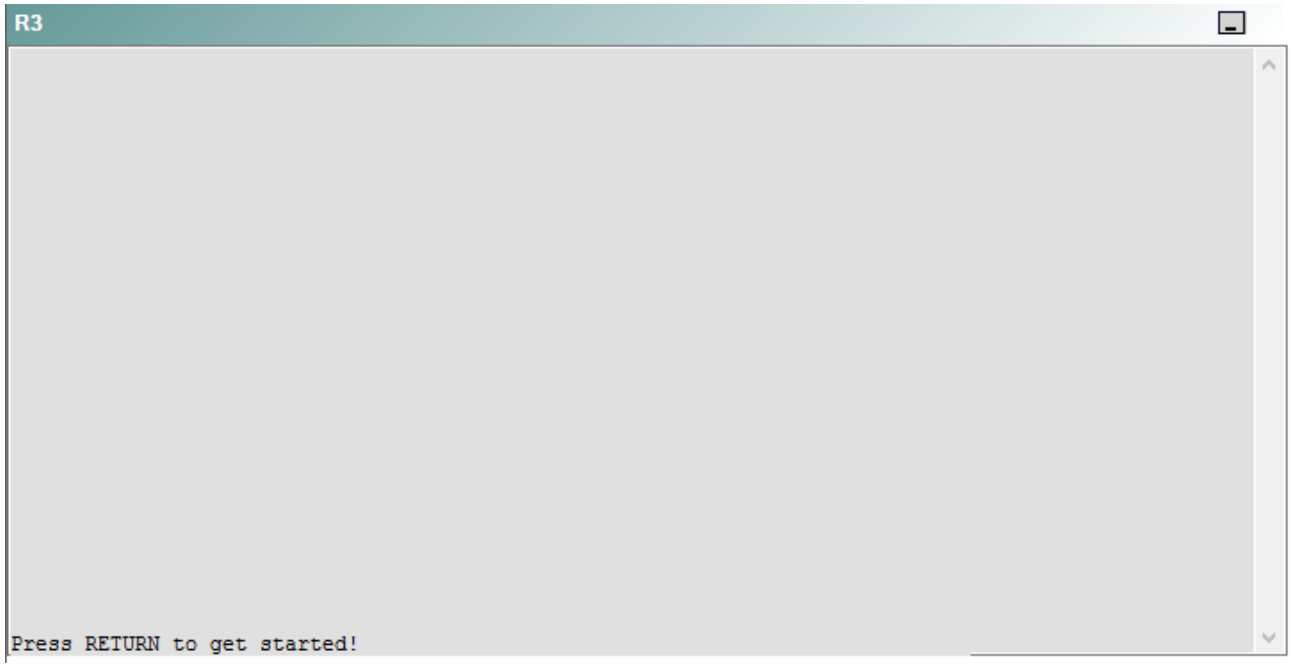
R1



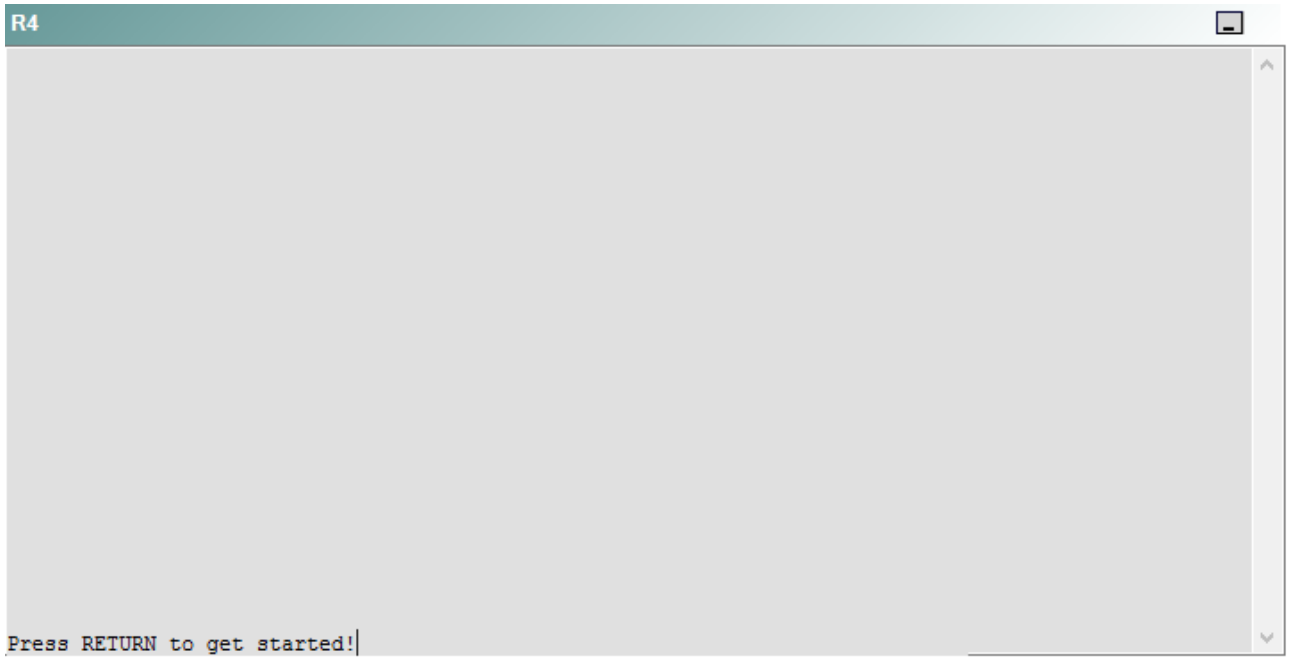

R2



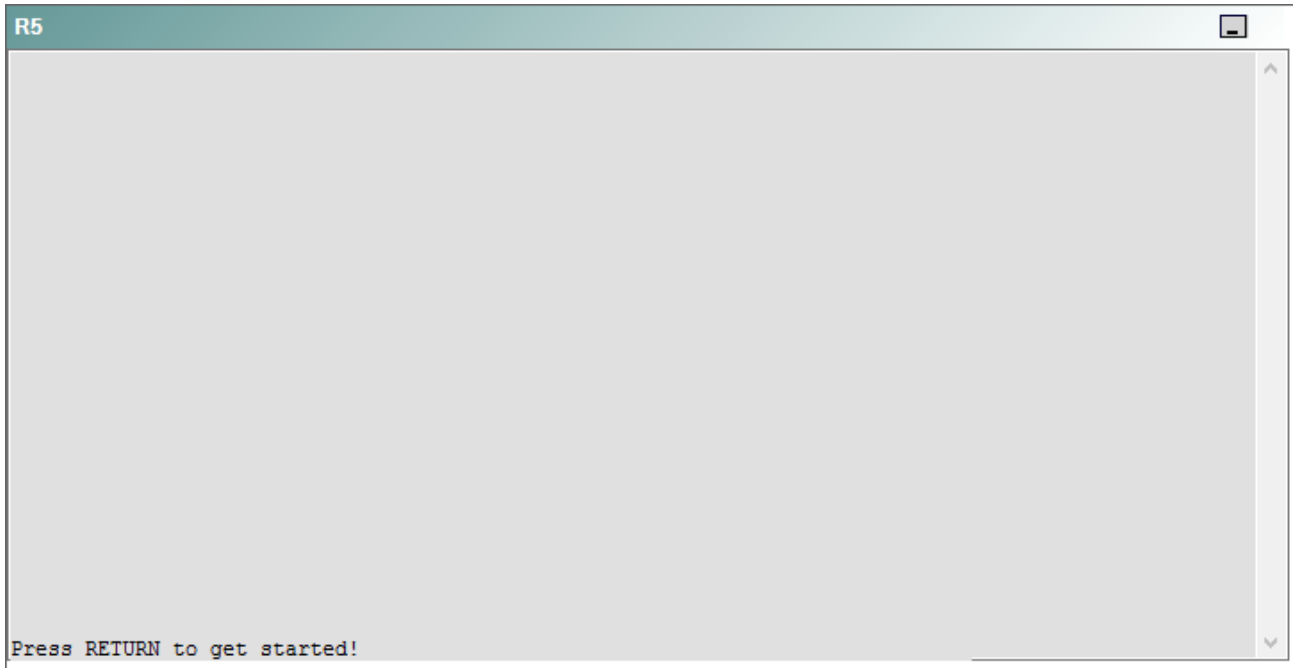

R3



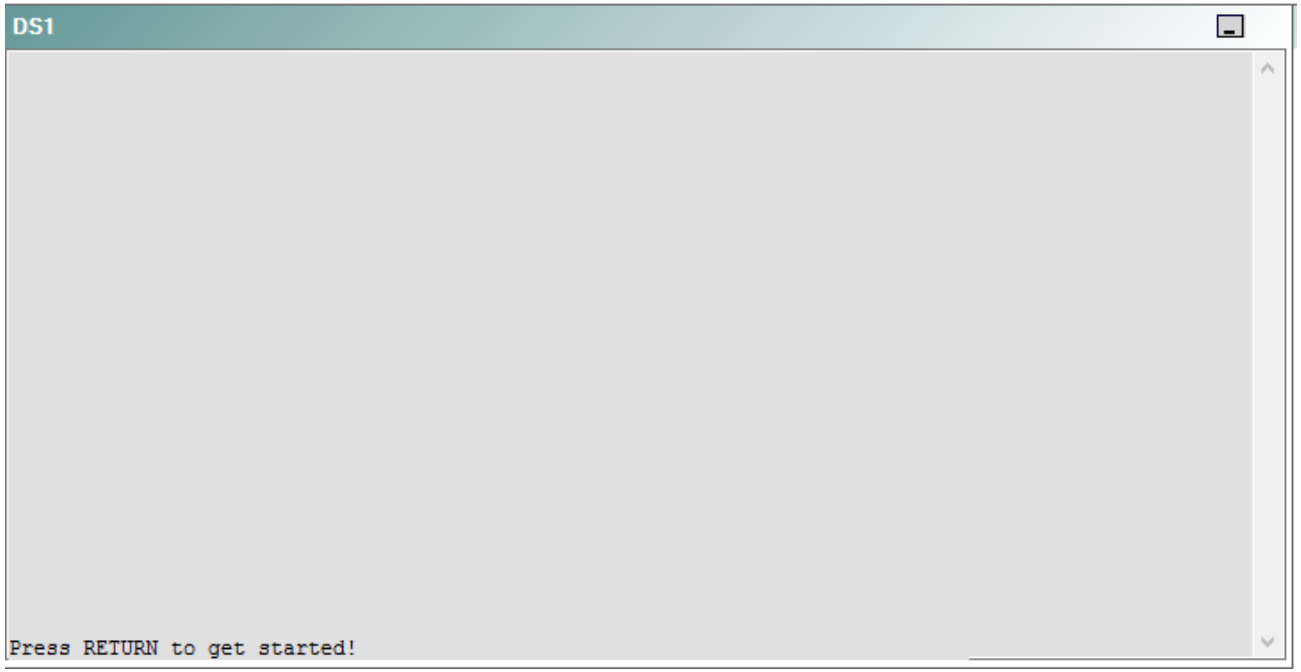

R4



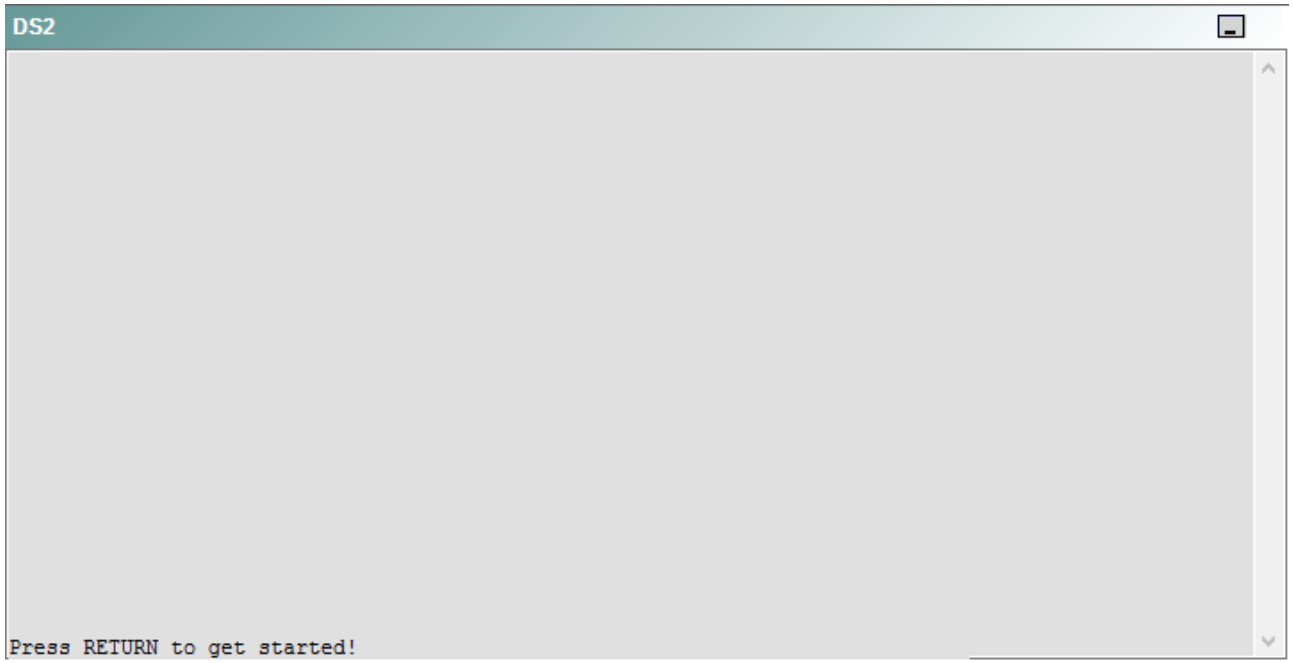

R5



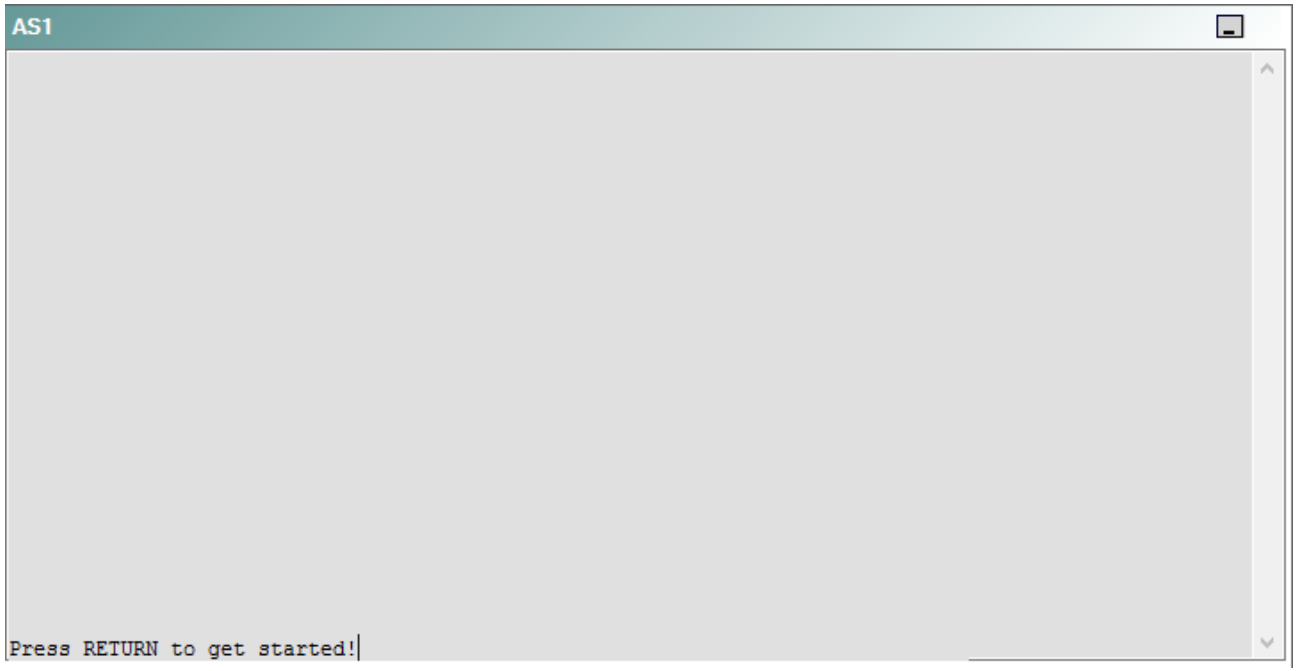

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that the clock on AS1 in not synchronized with the clock on R1.

Which of the following technologies is the source of the problem?

A. NTP
B. OSPFv2
C. OSPFv3
D. EIGRP
E. redistribution
F. Layer 3 addresing
G. interface

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

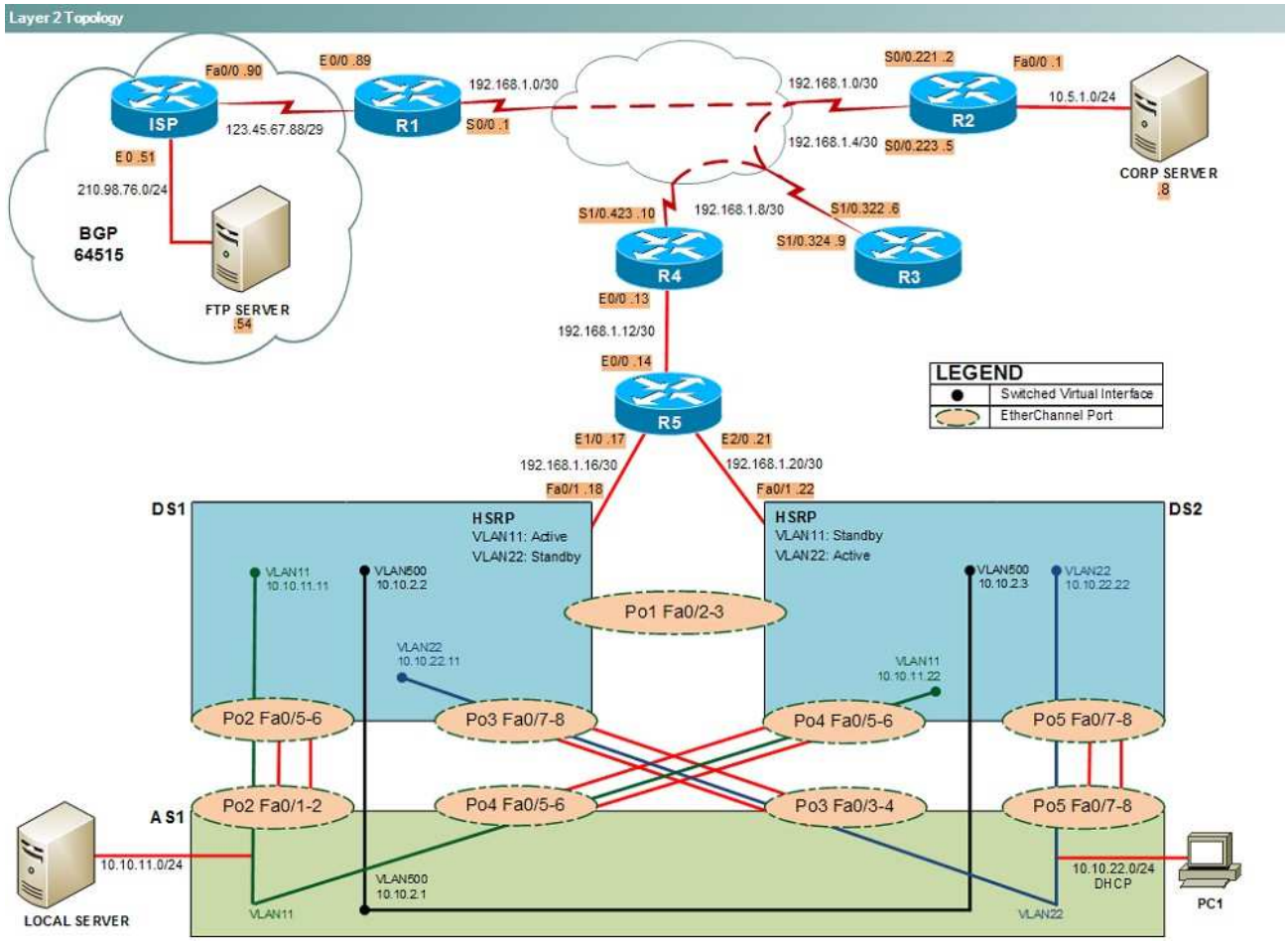
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

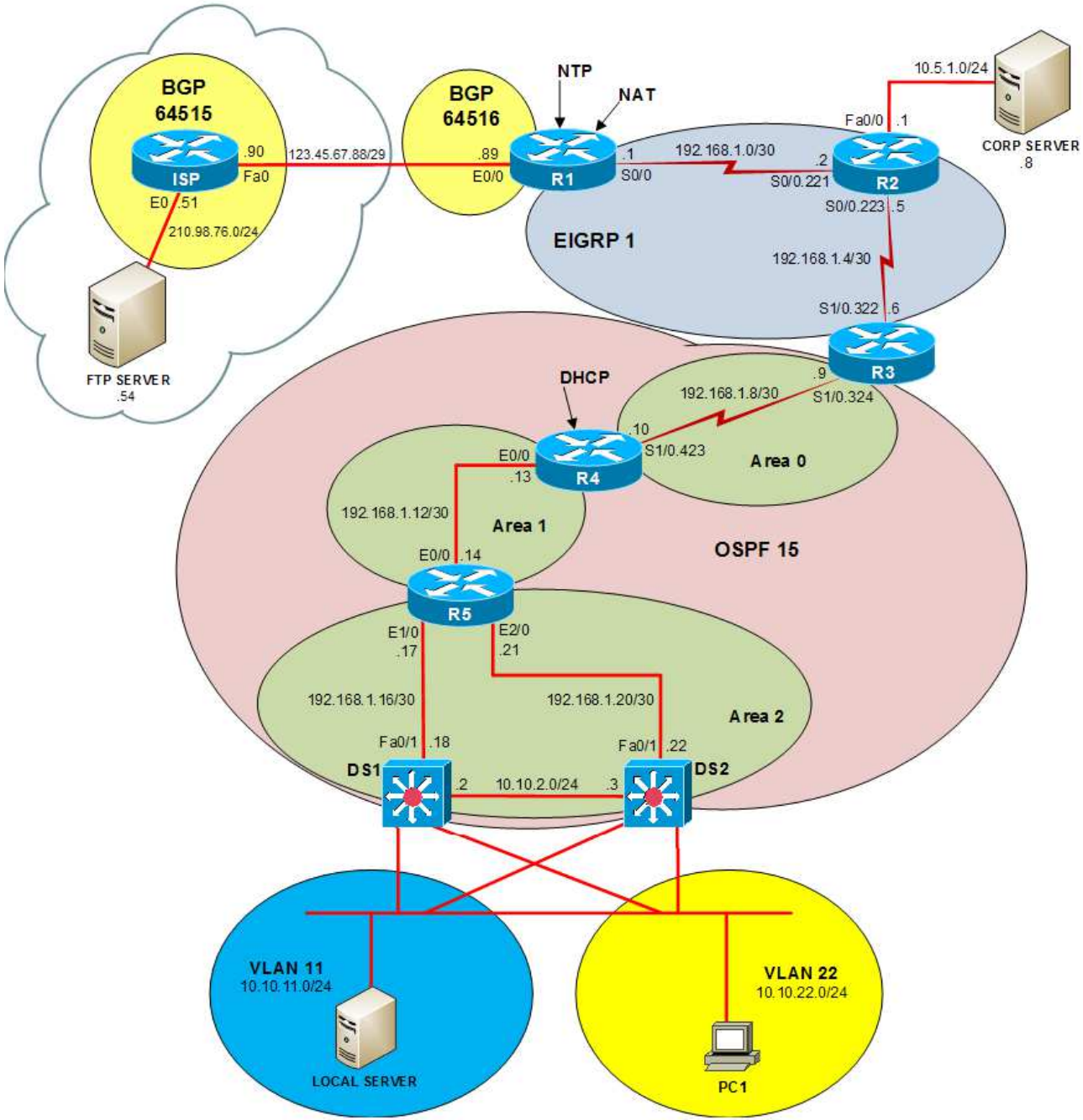
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

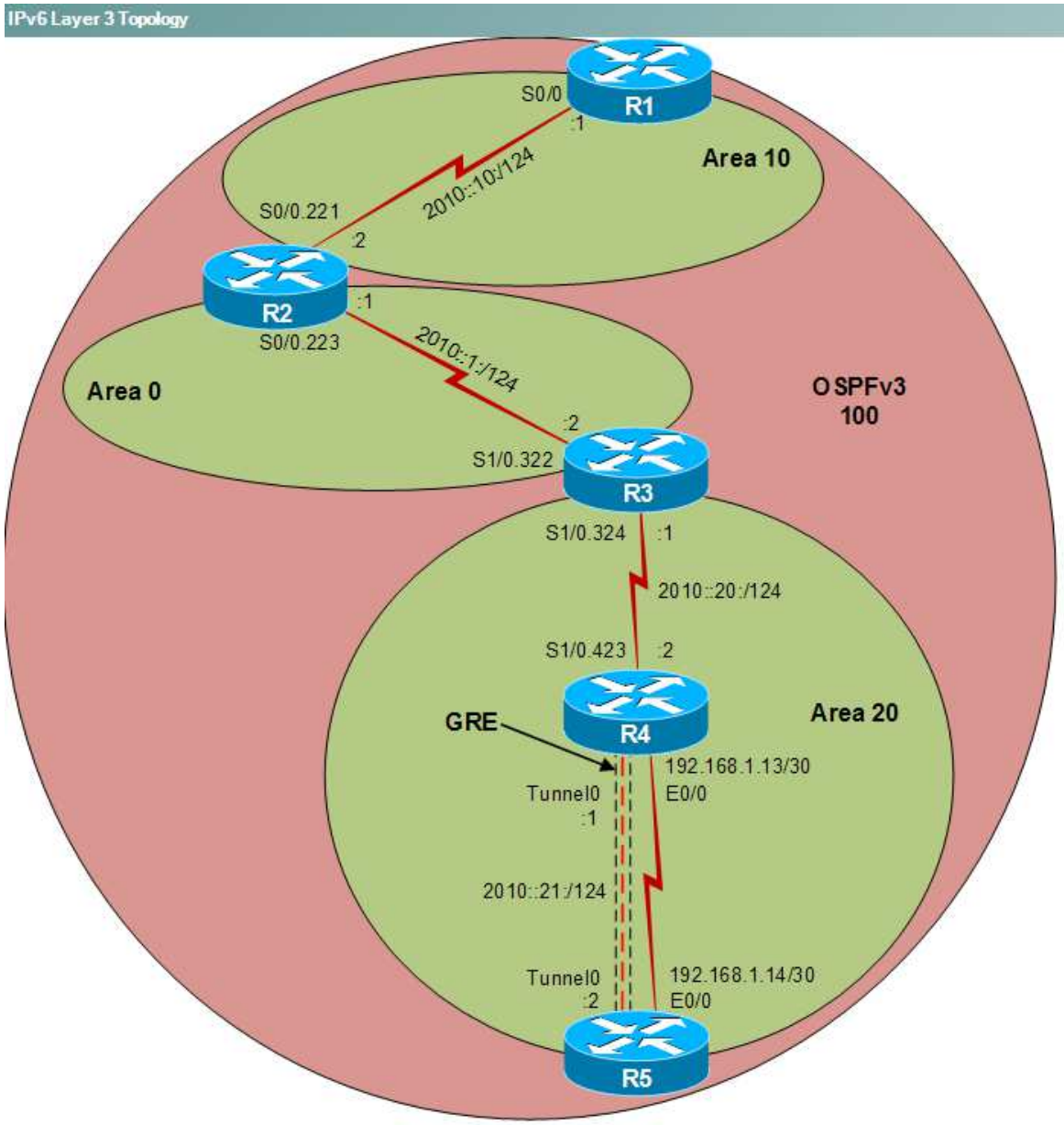
**Layer 2 Topology**




IPv4 layer 3 Topology

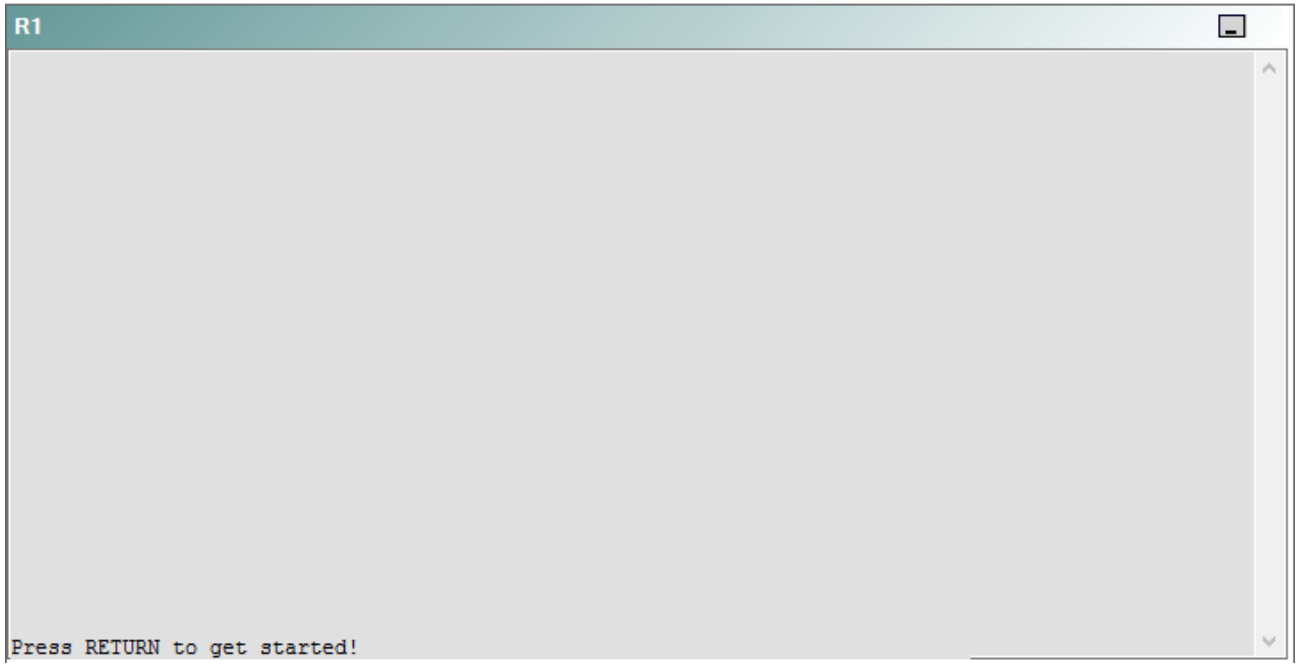

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

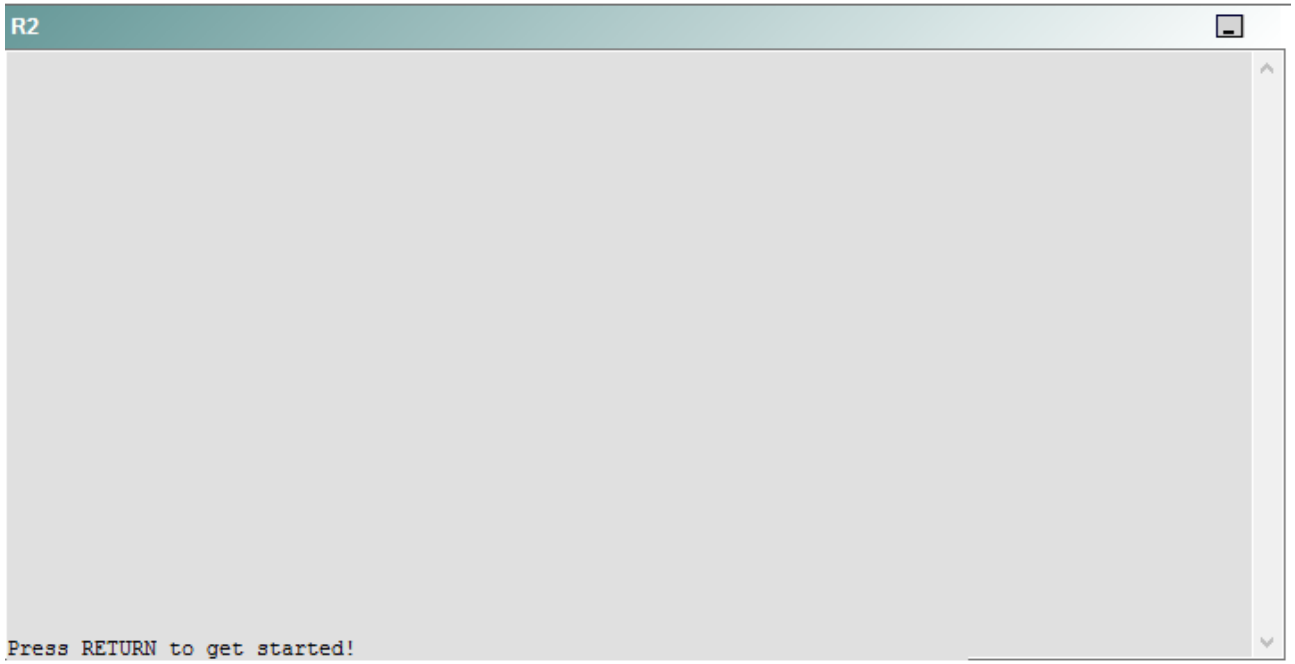



https://www.gratisexam.com/

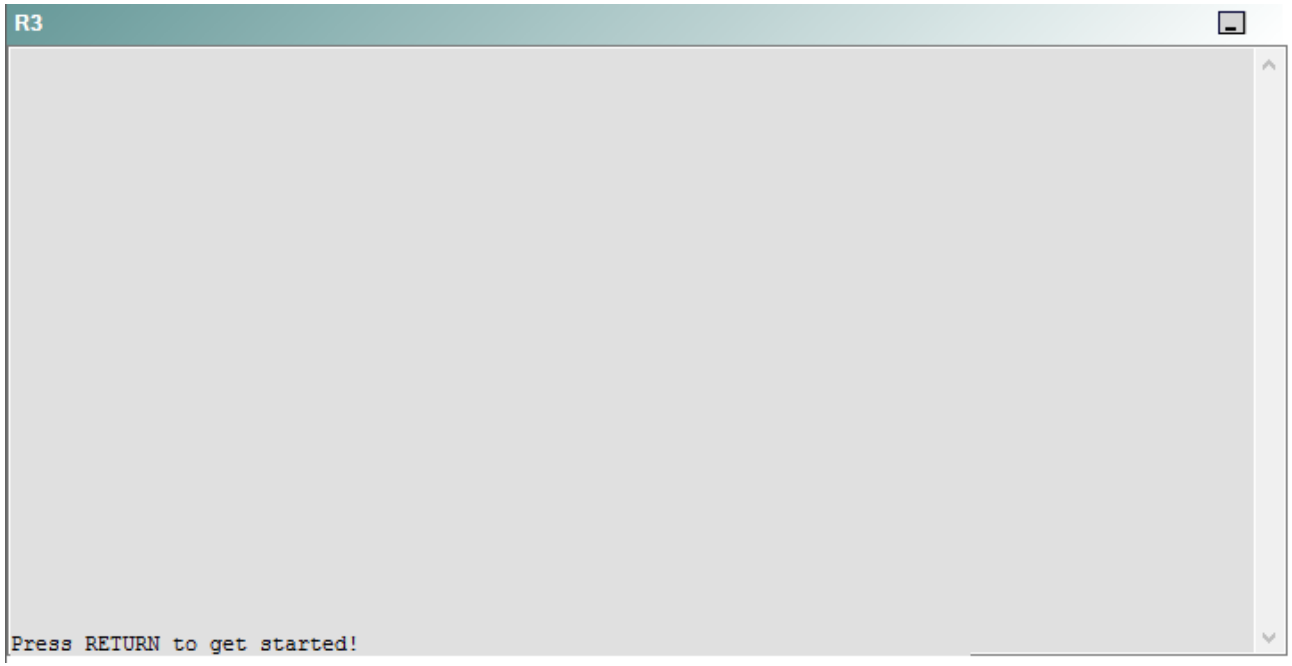
R1



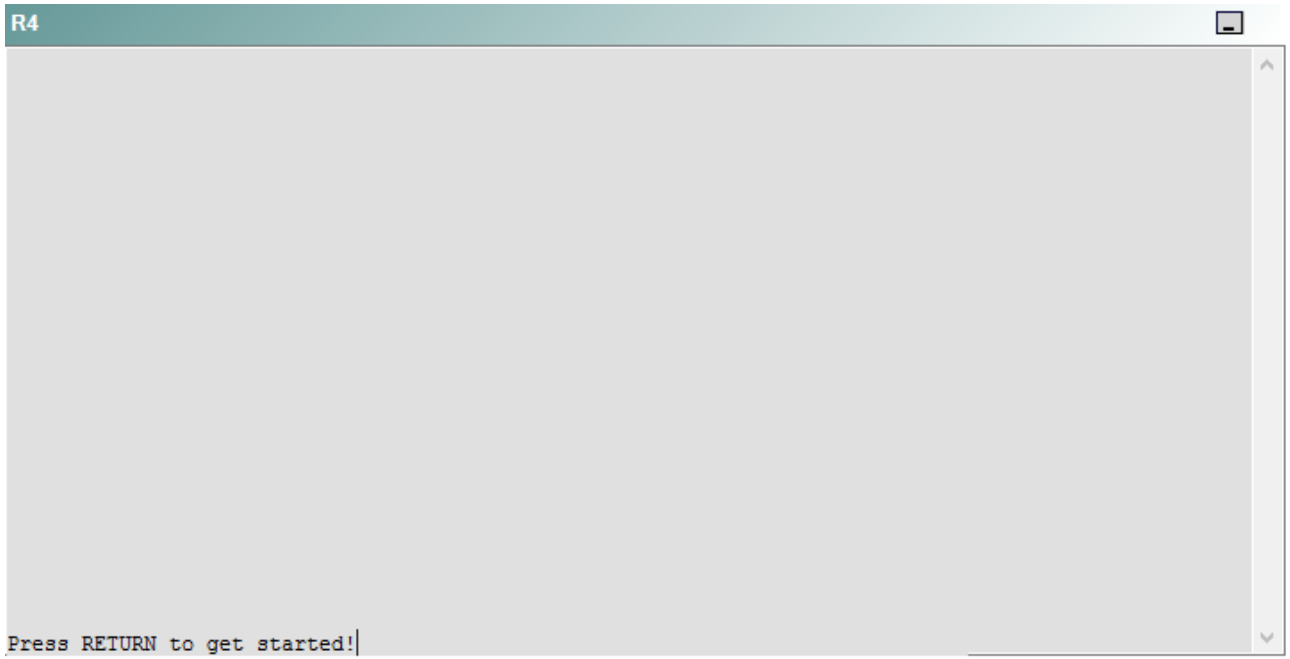

R2



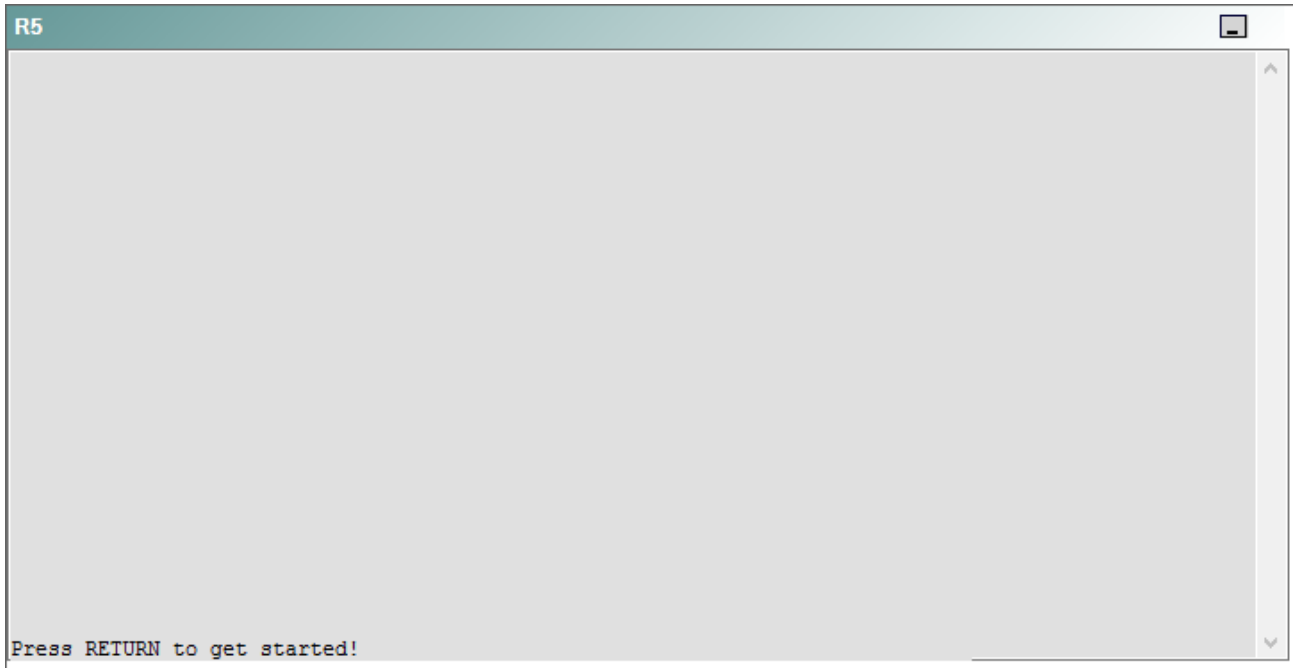

R3



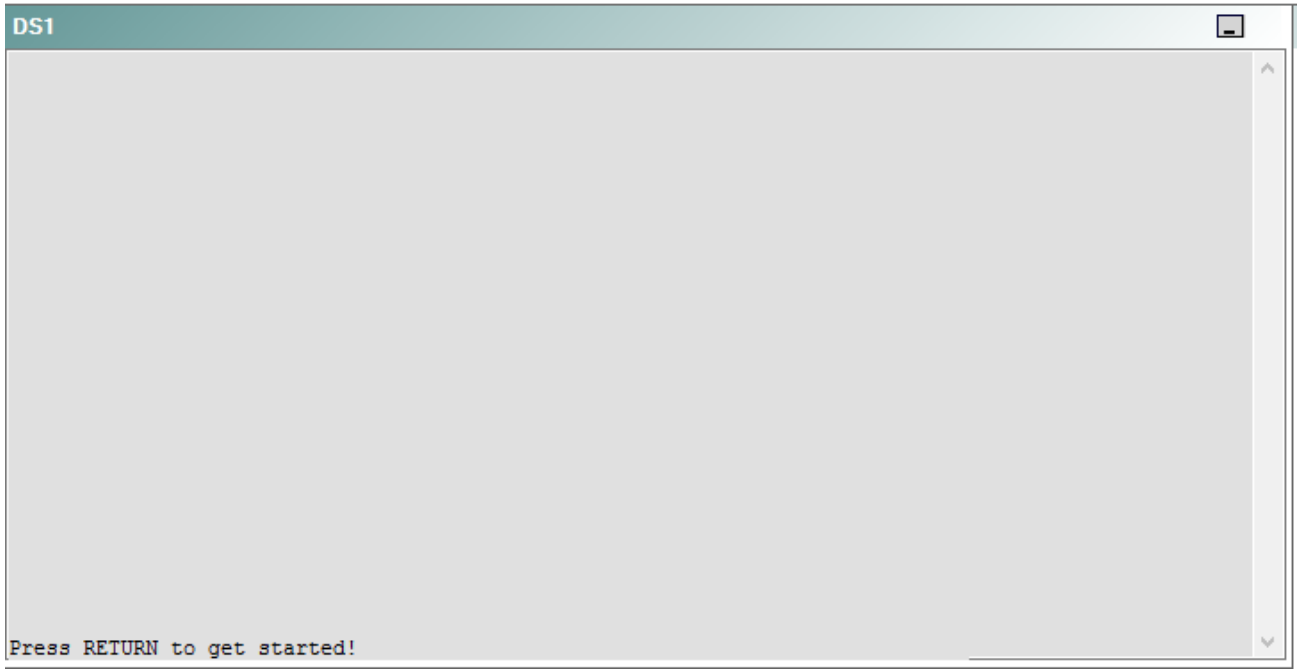

R4



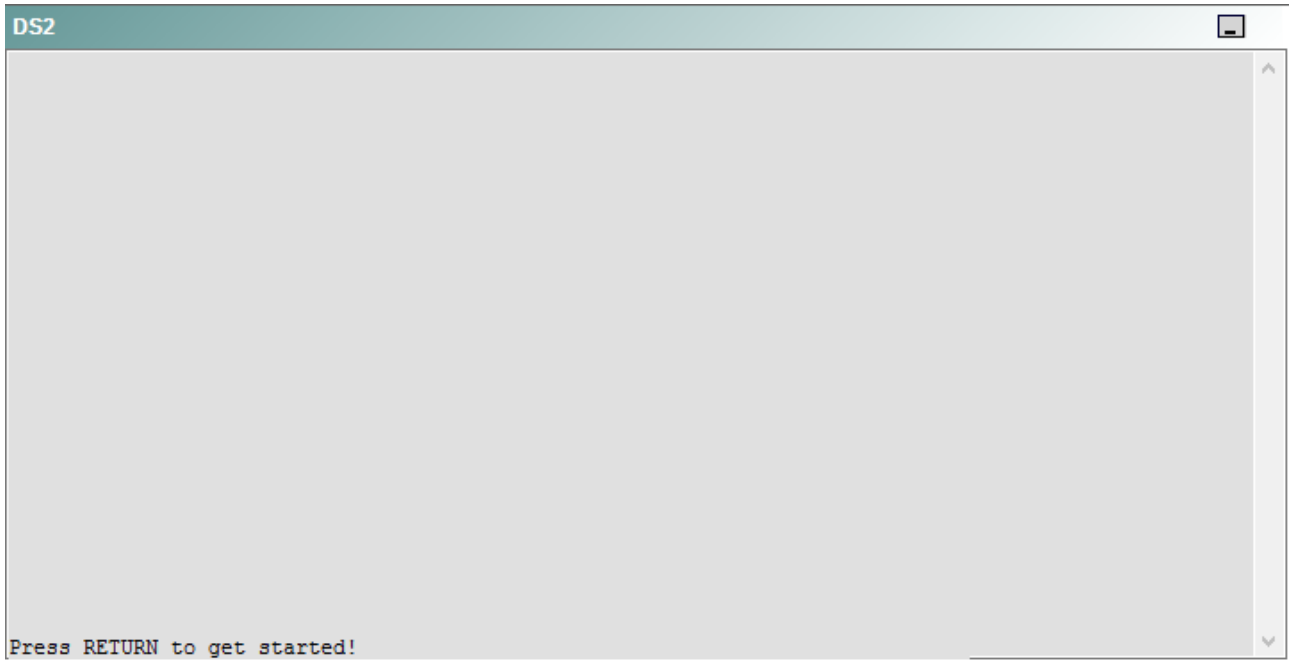

R5



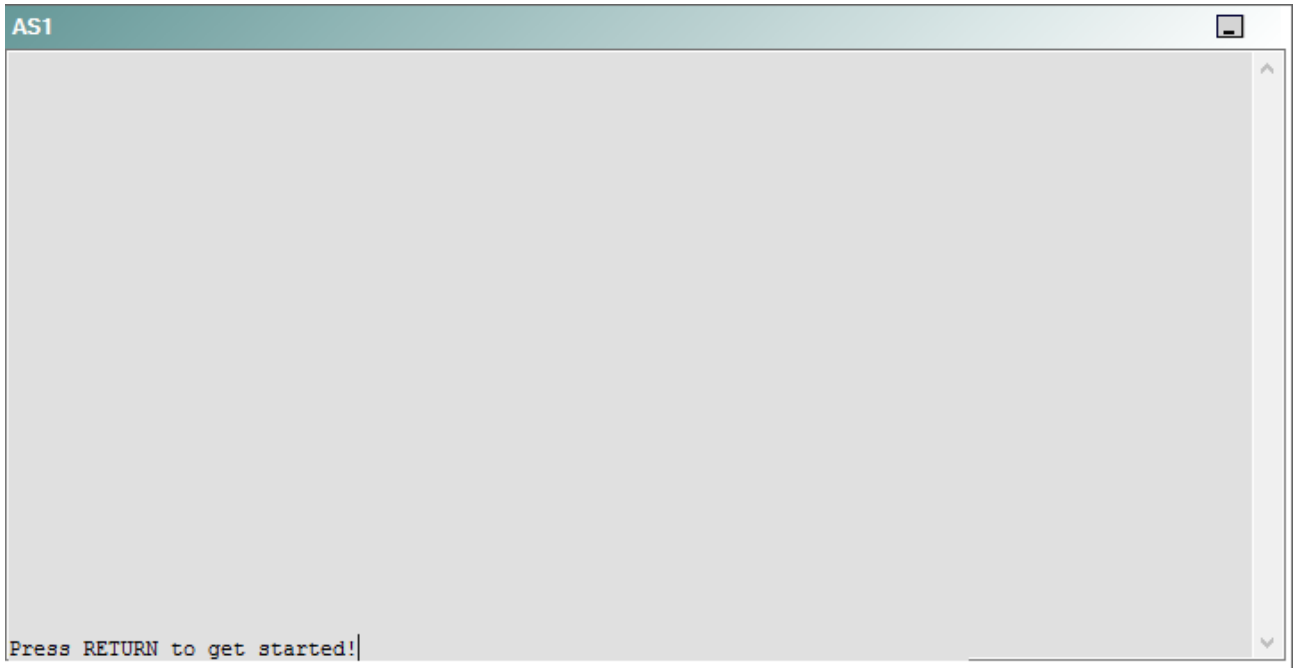

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that the clock on AS1 is not synchronized with the clock on R1.

Which of the following is most likely to solve the problem?

A. issuing the **no ntp master** command in global configuration mode
B. issuing the **ntp master 1** command in global configuration mode
C. issuing the **ntp master 192.168.1.1** command in global configuration mode
D. issuing the **ntp server 192.168.1.5** command in global configuration mode
E. removing the current **NTP server** command, and issuing the ntp server 192.168.1.5 command in global configuration mode
F. issuing the **clock set** command

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

You should issue the **no ntp master** command in global configuration mode on R3. To determine which device is the source of the problem, you can issue the **show running-config** command on each device to view the Network Time Protocol (NTP) configuration. In addition, you can issue the **show ntp associations** command to list the time sources that are configured for the device, and you can issue the **show ntp status** command to display detailed synchronization information. However, one of the simplest methods you can use to determine the synchronization status of a device is to issue the **show clock** command. If the clock is synchronized or has been set manually, no symbol will appear before the time, as shown in the following output:

```
00:20:14.301 CST Wed Apr 1 2009
```

If the clock has never been synchronized or has never been set, an asterisk will appear before the time, as shown in the following output:

```
*00:20:14.301 CST Wed Apr 1 2009
```

If the clock is not currently synchronized but had been synchronized in the past, a dot will appear before the time, as shown the following output:

```
.00:20:14.301 CST Wed Apr 1 2009
```

Issuing the **show running-config** command on all of the devise will show that each of the devices from AS1 to R2 is receiving time from a directly connected upstream device. However, R3 is also configured with the **ntp master 1** command. The **ntp master** command configures a device to act as a master clock source. The syntax of the **ntp master** command is **ntp master** *stratum*, where *stratum* is a value from 1 through 15. A click source with a lower stratum number is preferred over a clock source with a higher stratum number.

In this scenario, R3 prefers its own clock time. Thus, when R4 synchronizes its clock with R3, R3 uses its own clock time instead of the time it has received from R2. R4 then passes this time to R5, which passes it to the two distribution layer switches, and so on. To configure R3 to prefer the time it receives from R2, you should remove the **ntp master 1** command from R3 by issuing the **no ntp master** command in global configuration mode.

You cannot issue the **ntp master 192.168.1.1** command, because it contains invalid syntax. The **ntp master** command accepts a stratum number as a keyword; it cannot accept an IP address.

You need not issue an **ntp server** command on any of the routers on the network. Issuing the **ntp server** command from global configuration mode configures a Cisco router to be an NTP static client that is synchronized by an NTP server. The syntax of the **ntp server** command is **ntp server** *ip-address,* where *ip-address* id the IP address of the NTP server that the client will use to receive its time. Each router in this scenario is correctly configures to receive tome from its directly connected upstream device.

You should not issue the **ntp authentication-key** command or the **ntp-trusted-key** command, because none of the Cisco devices are configured to use NTP authentication. To configure a Message Digest 5 (MD5) authentication key for a Cisco device, you would issue the **ntp authentication-key** *number* **md5** *value* command, where *number* is a number from 1 through 4294967295 and *value* is an eight-character string that represents the value of the MD5 key. Only MD5 keys are supported by NTP authentication. After defining an authentication key, you would issue the **ntp trusted-key** *key-number* command, where *key-number* is the number of the key defined in the **ntp authentication-key** command.

You should not issue the **clock set** command. The **clock set** command is used to manually configure the time on a Cisco device.

**Reference:**

https://www.cisco.com/c/en/us/td/docs/ios/ipv6/command/reference/ipv6_book/ipv6_10.html#wp2650678

**QUESTION 19**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

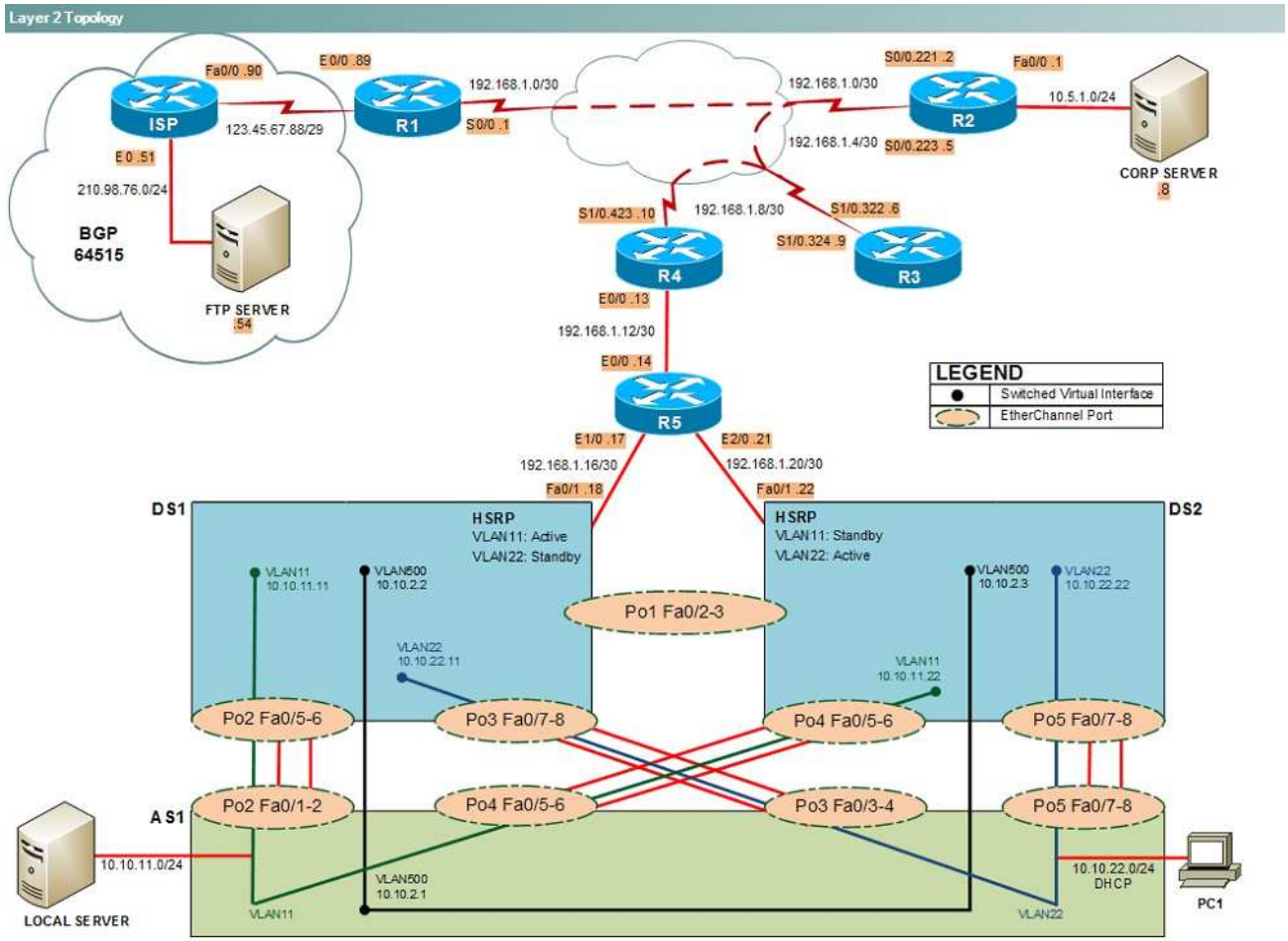
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

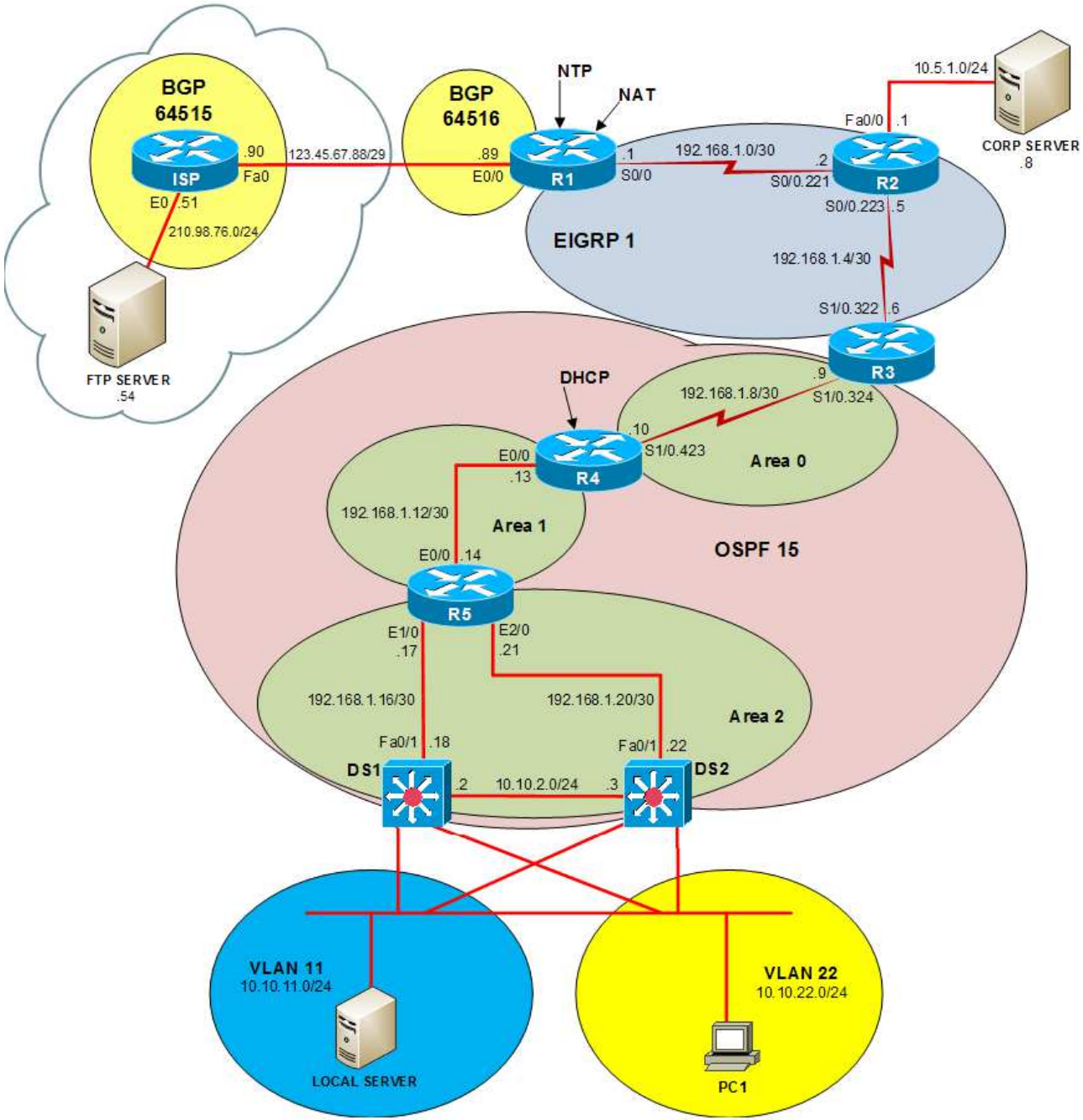
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

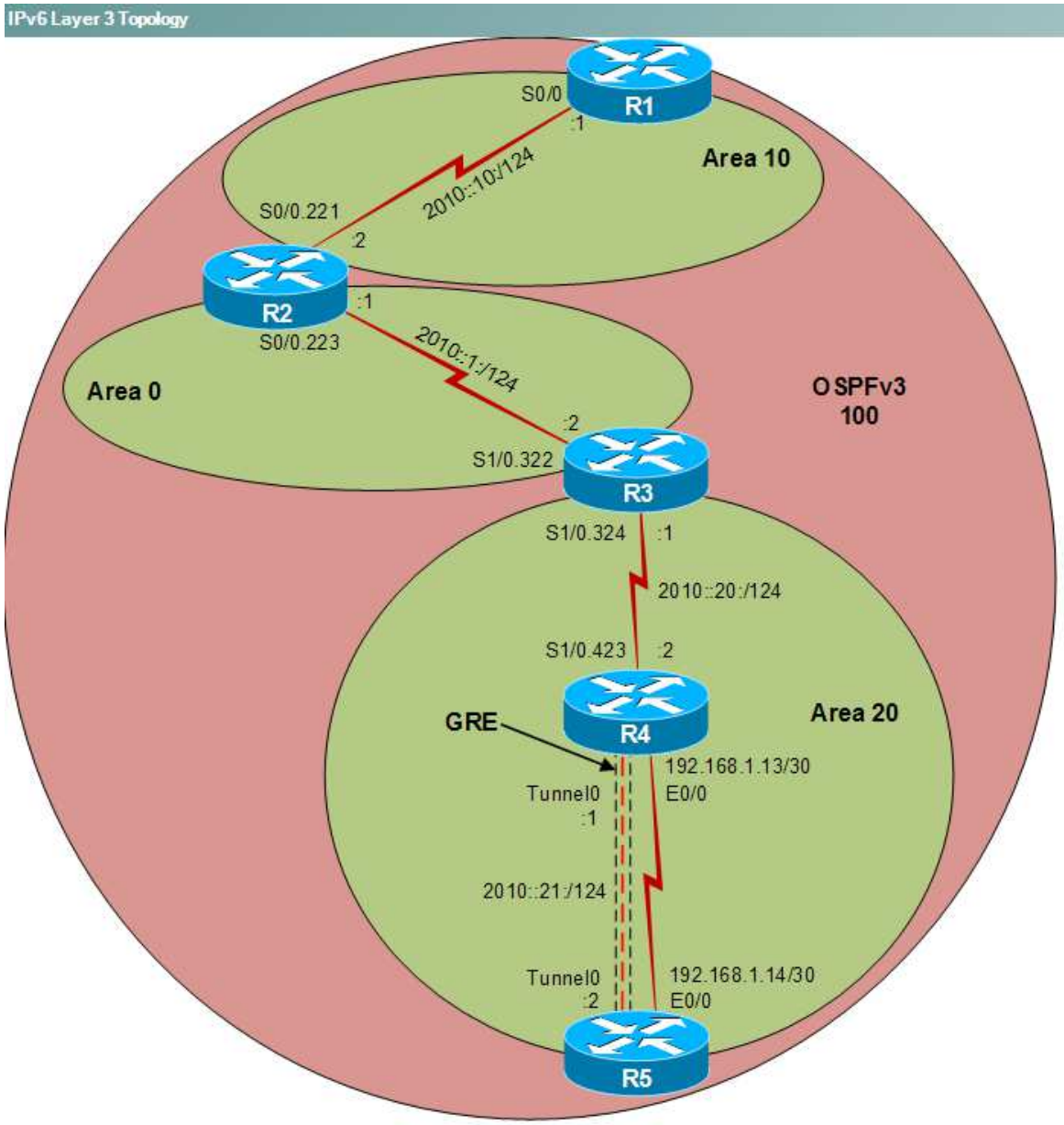
**Layer 2 Topology**




IPv4 layer 3 Topology

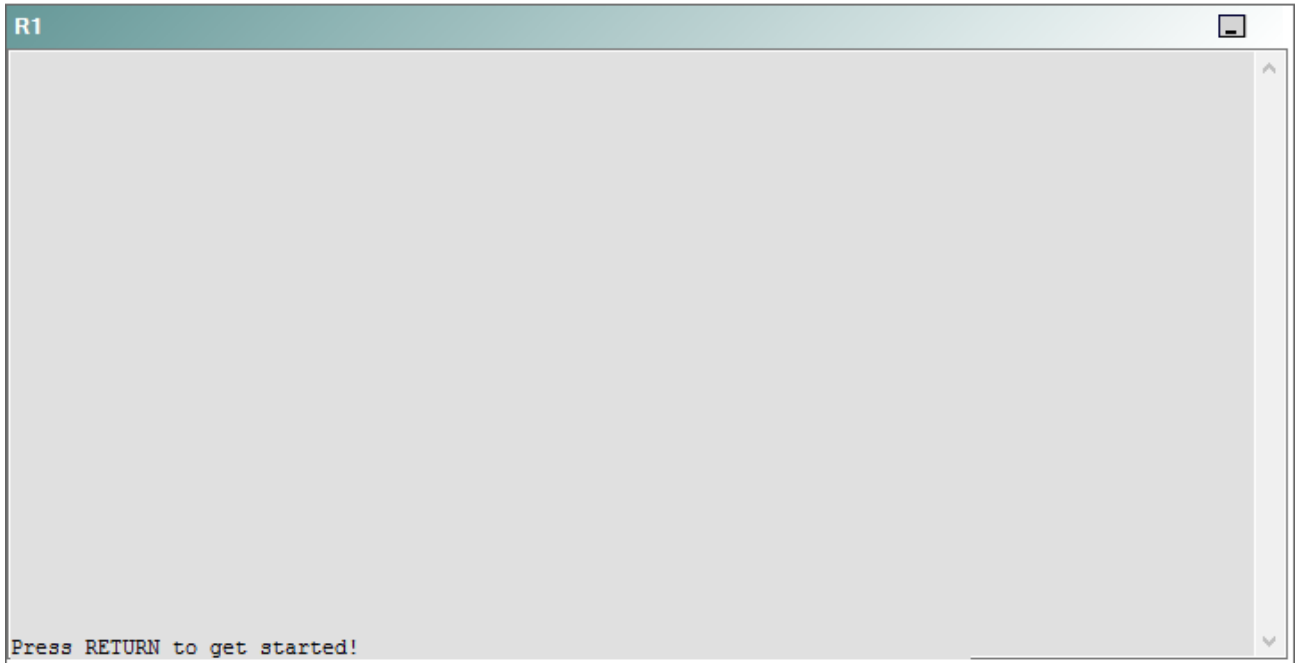

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

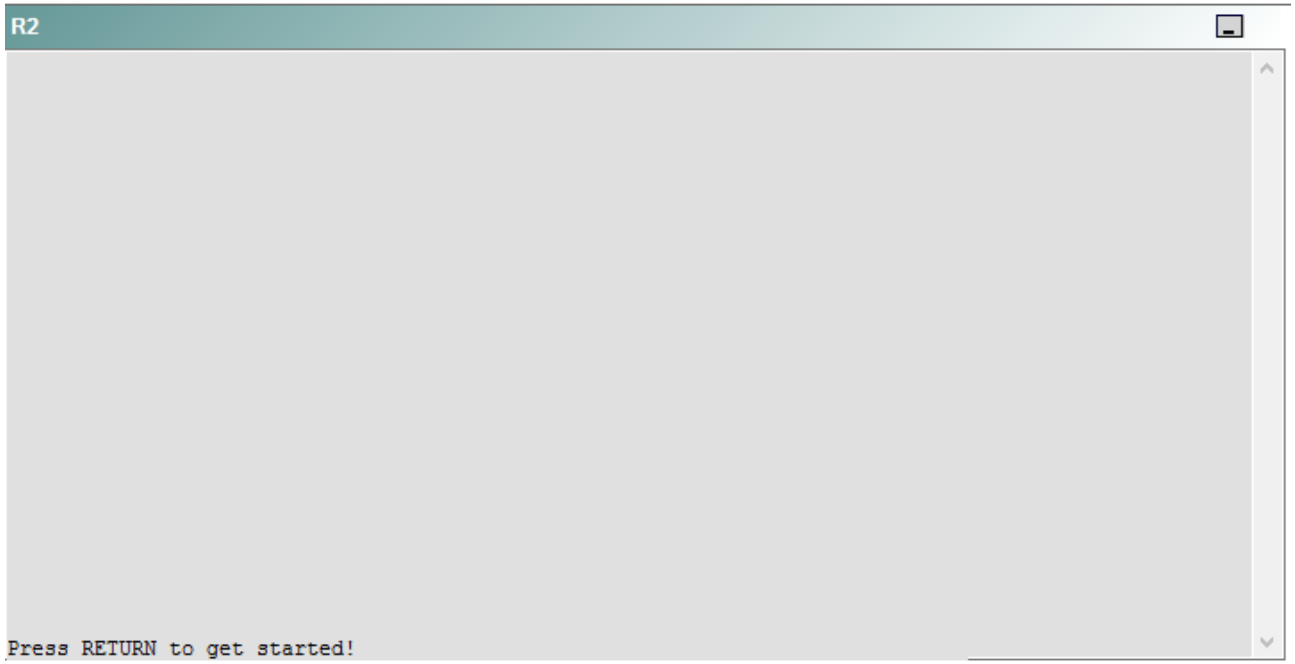



https://www.gratisexam.com/

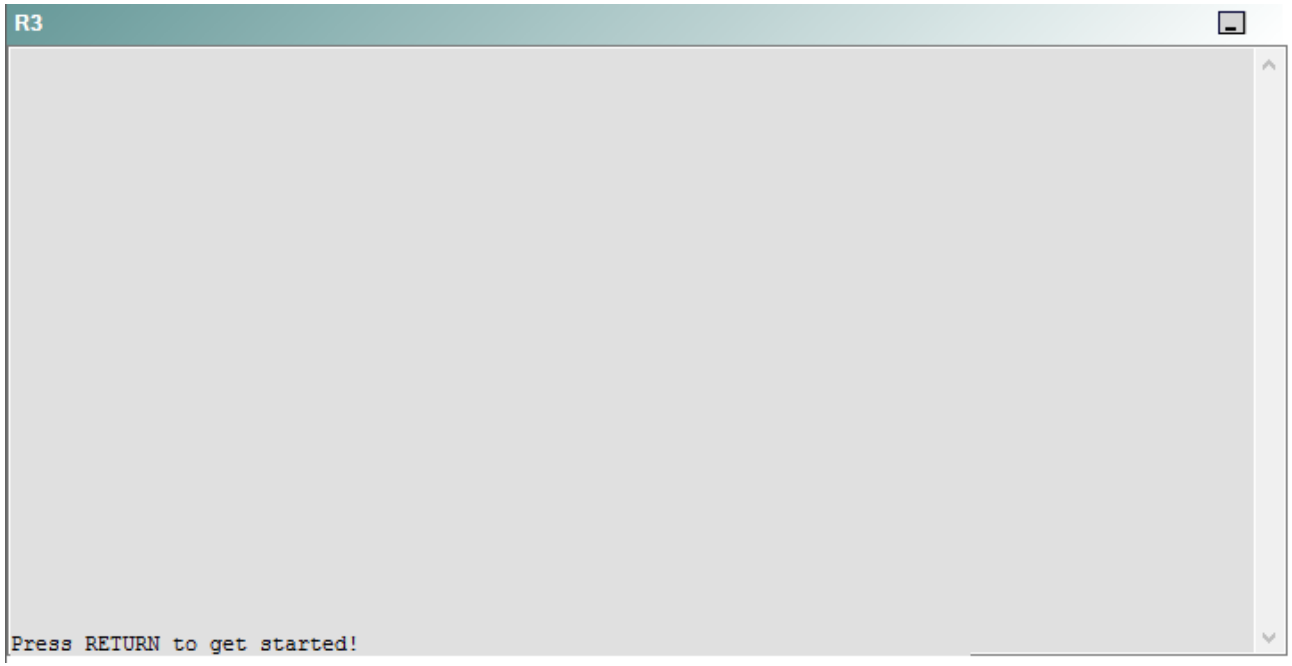
R1



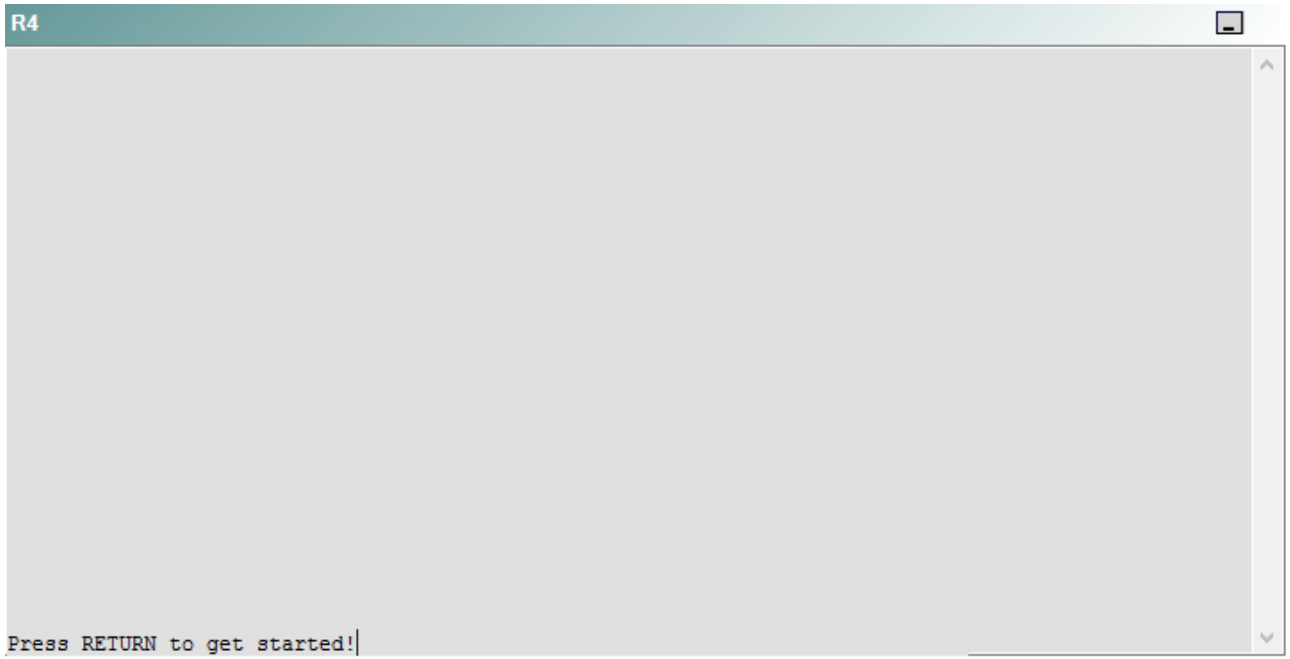

R2



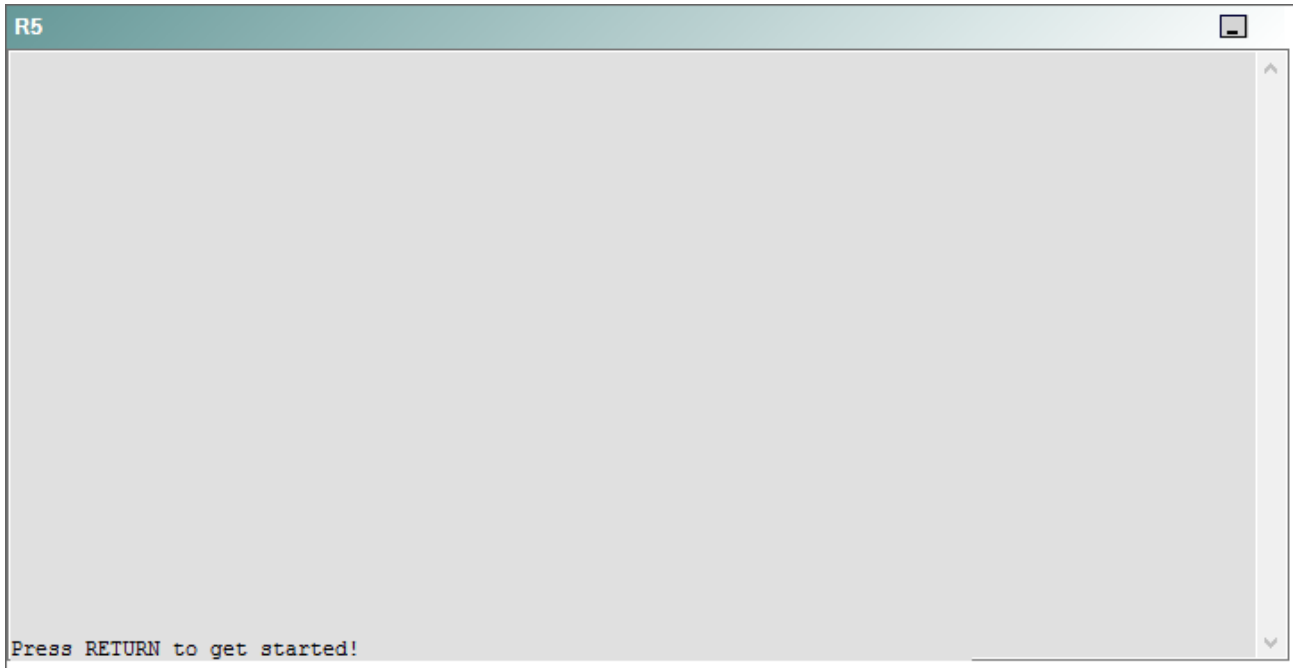

R3



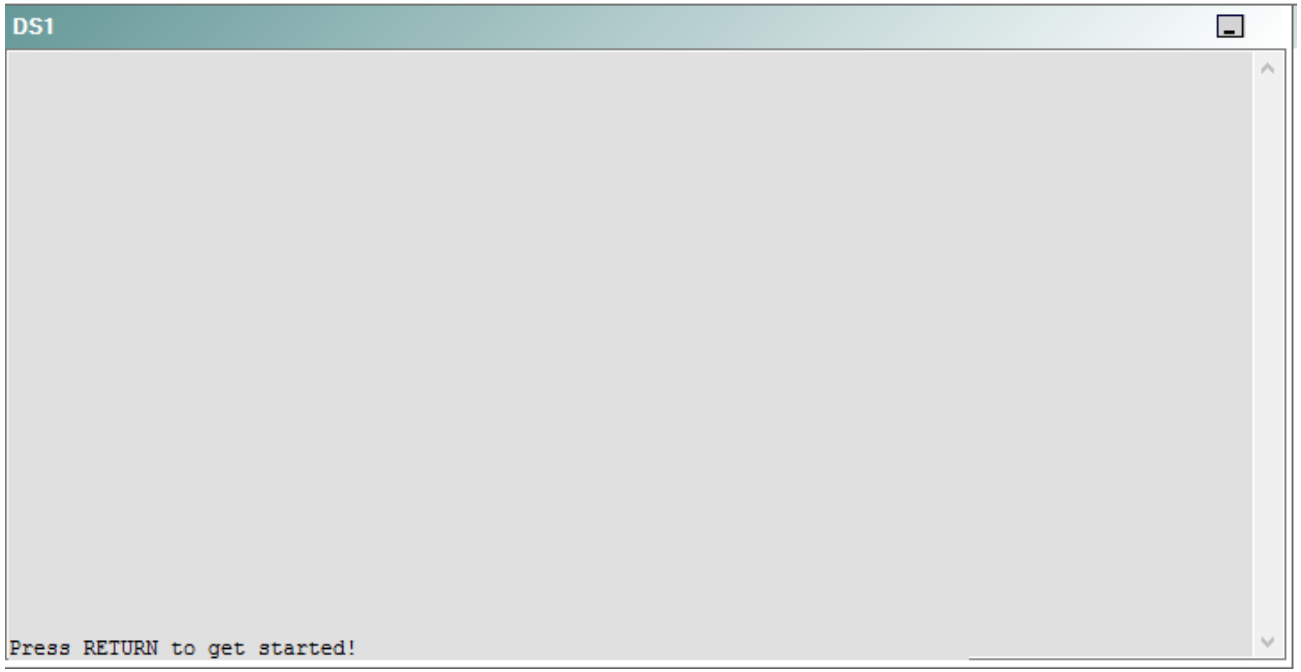

R4



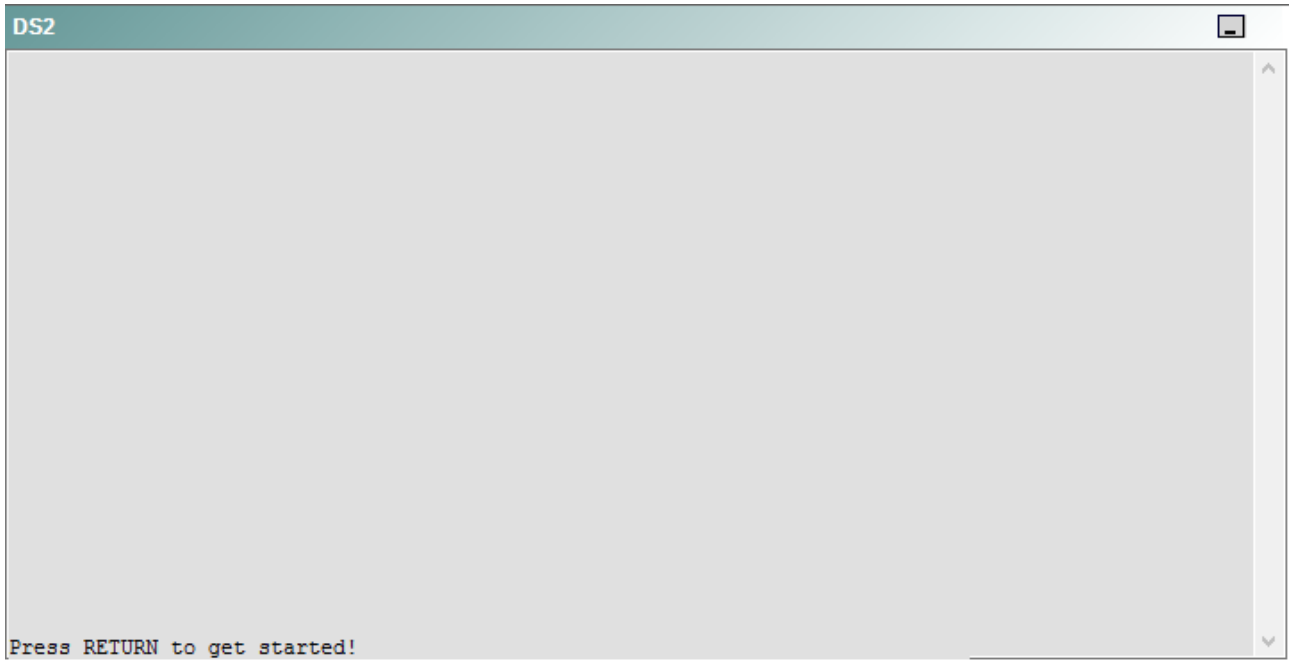

R5



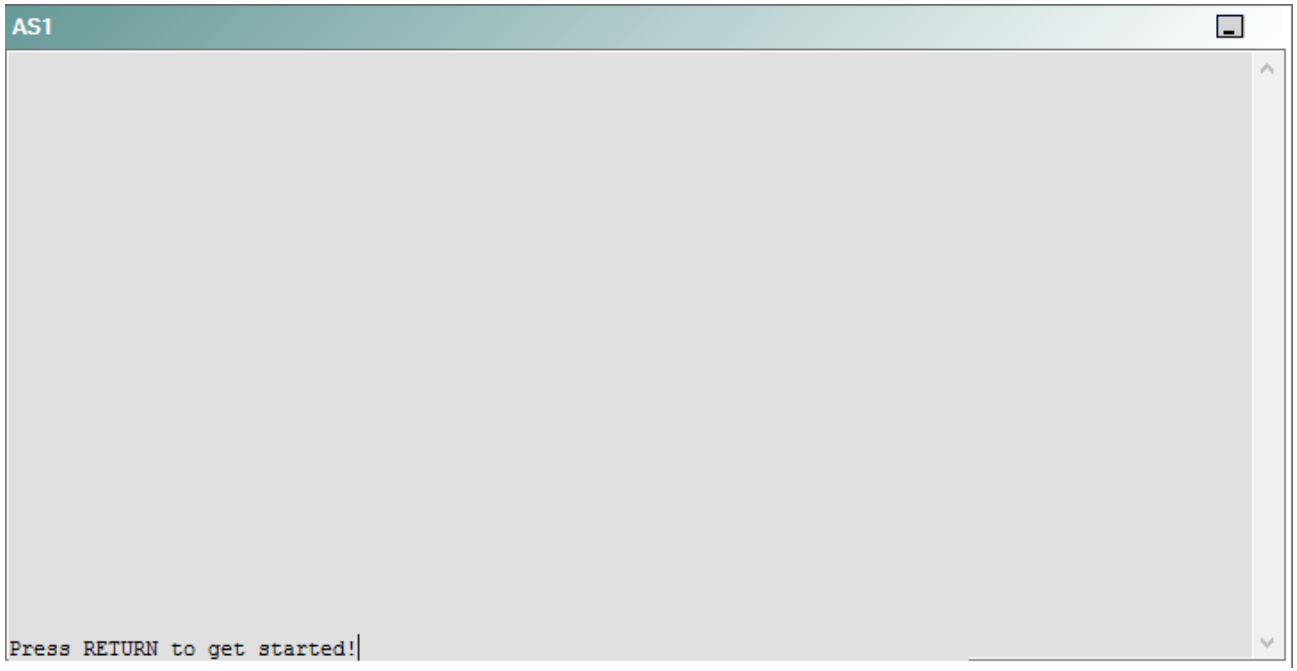

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that, upon reboot, DS1 is not becoming the active router for devices on VLAN 11. DS1 should be the active router for devices on VLAN 11 when DS1 is up, but DS2 should become the active router when DS1 is down.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** F
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 20**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

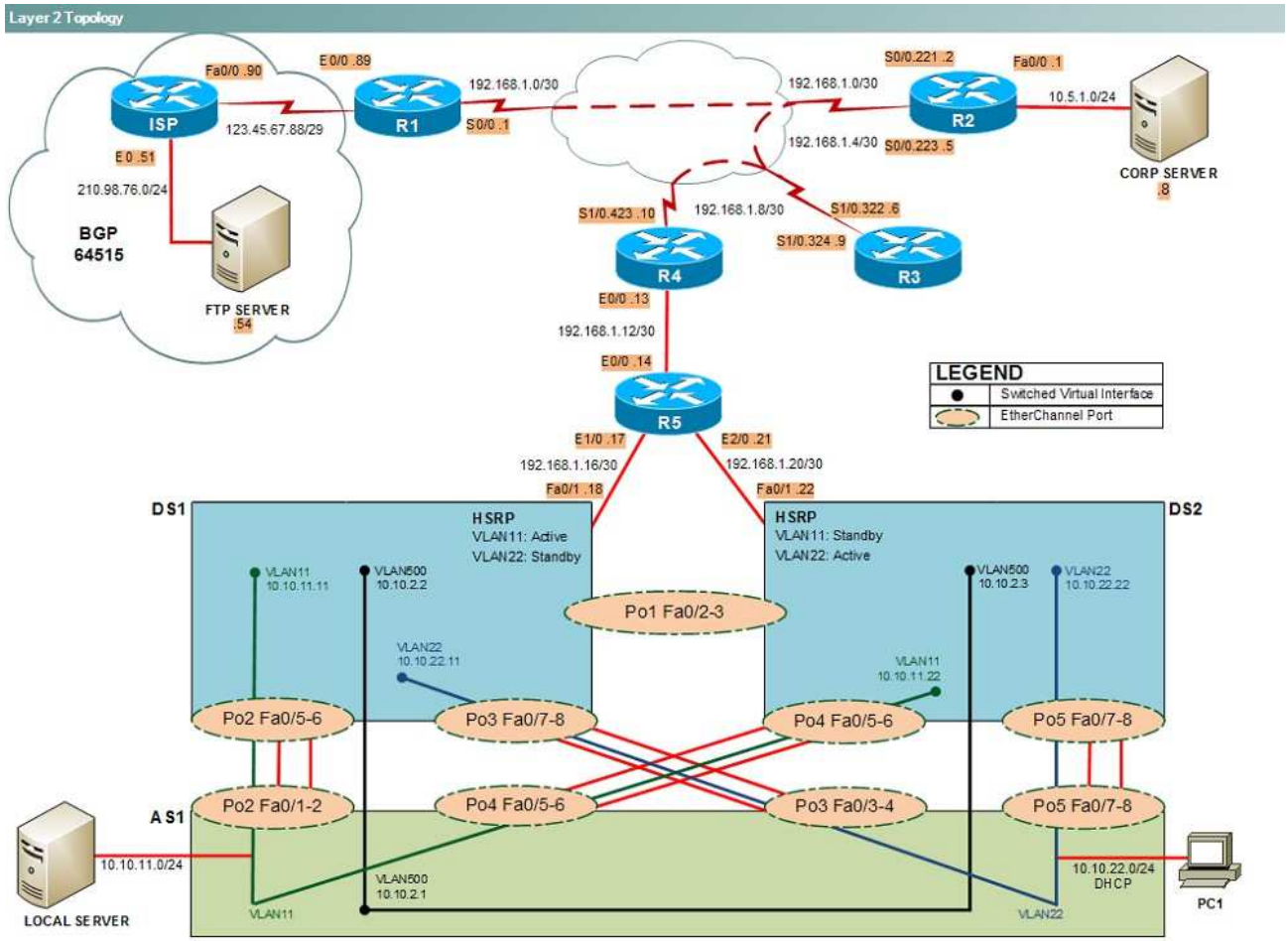
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

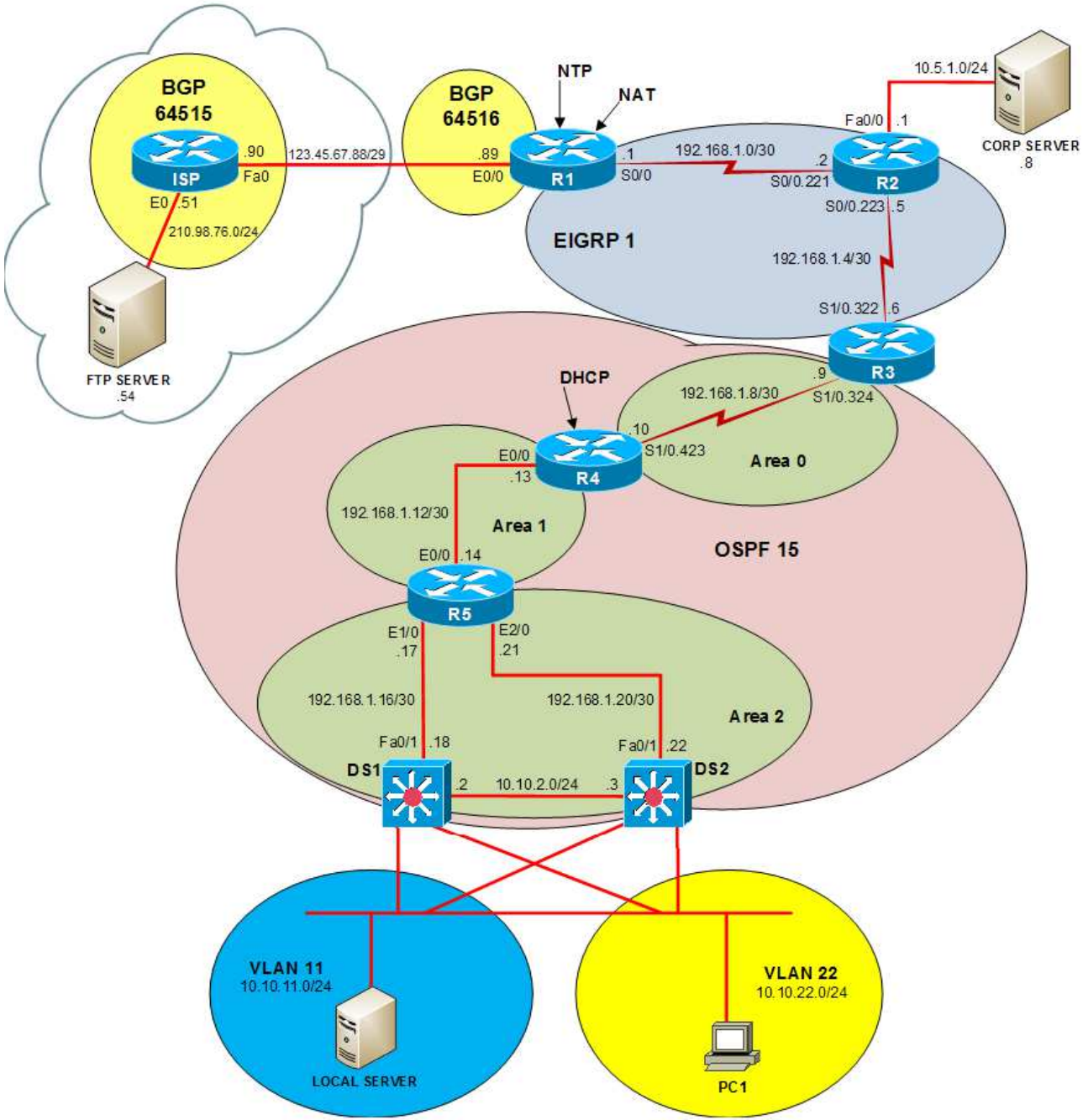
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

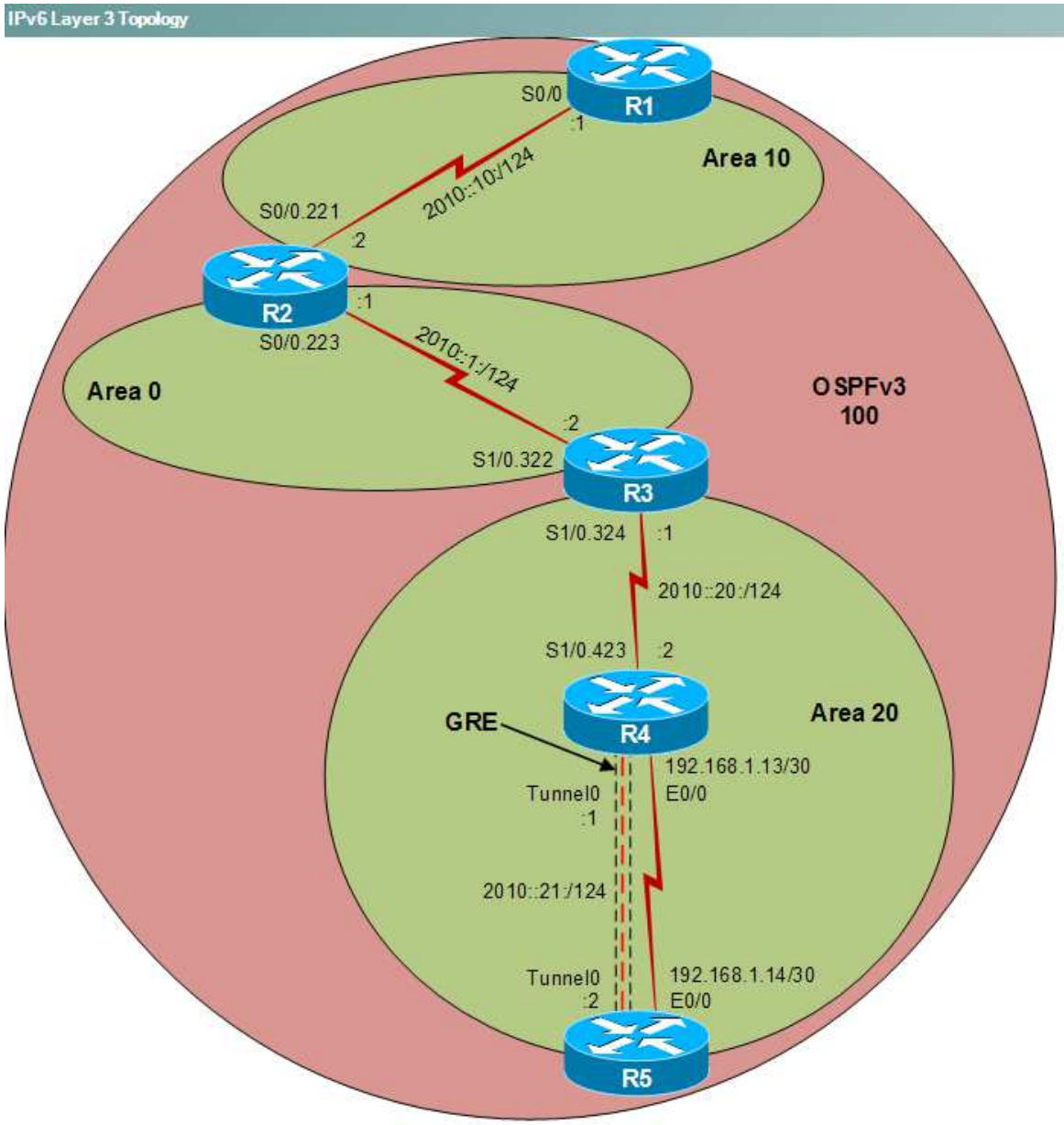
**Layer 2 Topology**




IPv4 layer 3 Topology

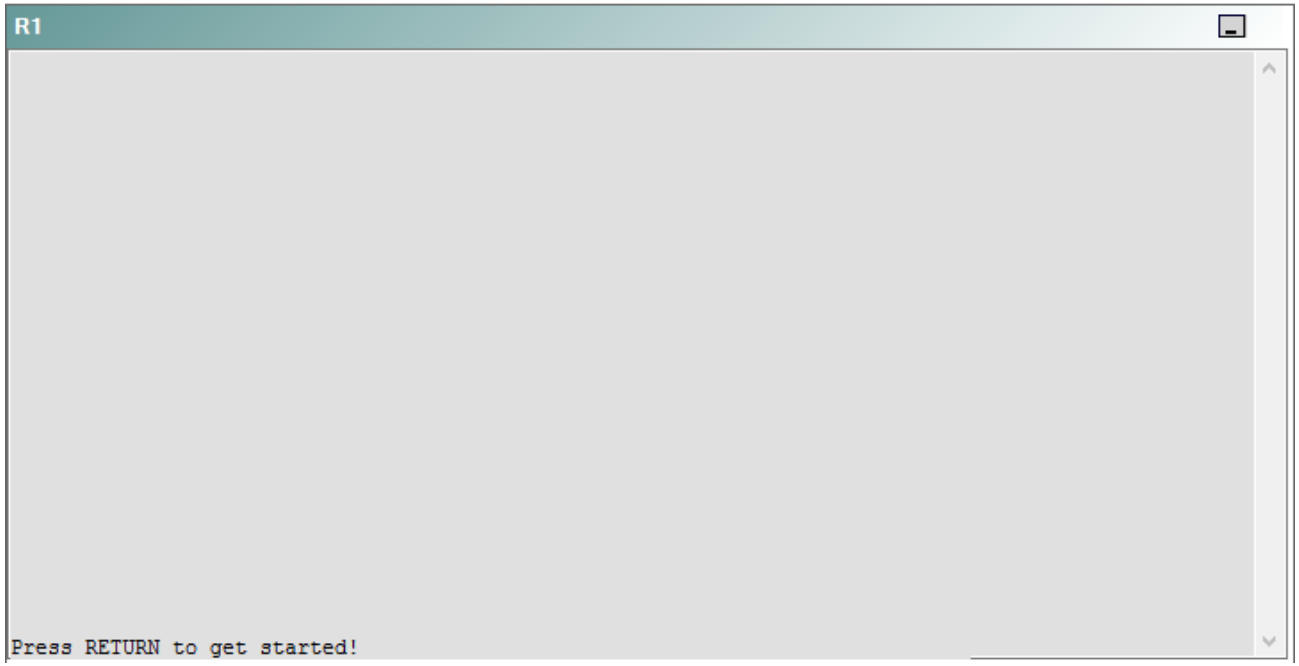

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

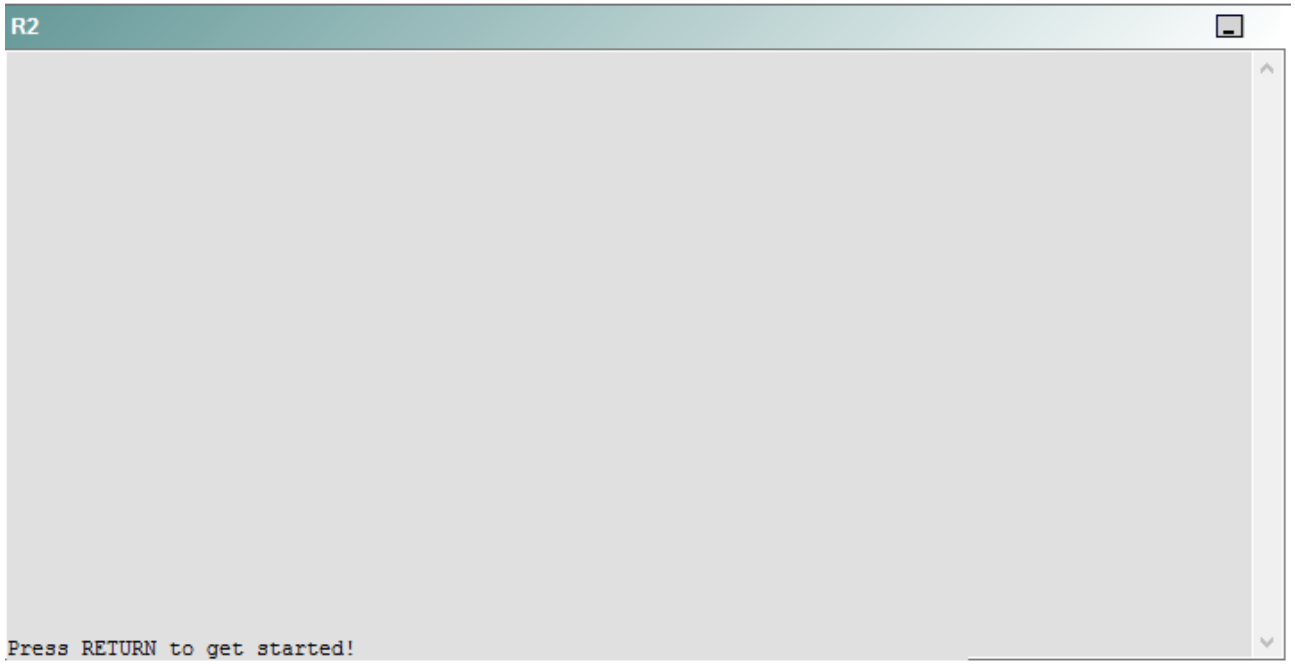



https://www.gratisexam.com/

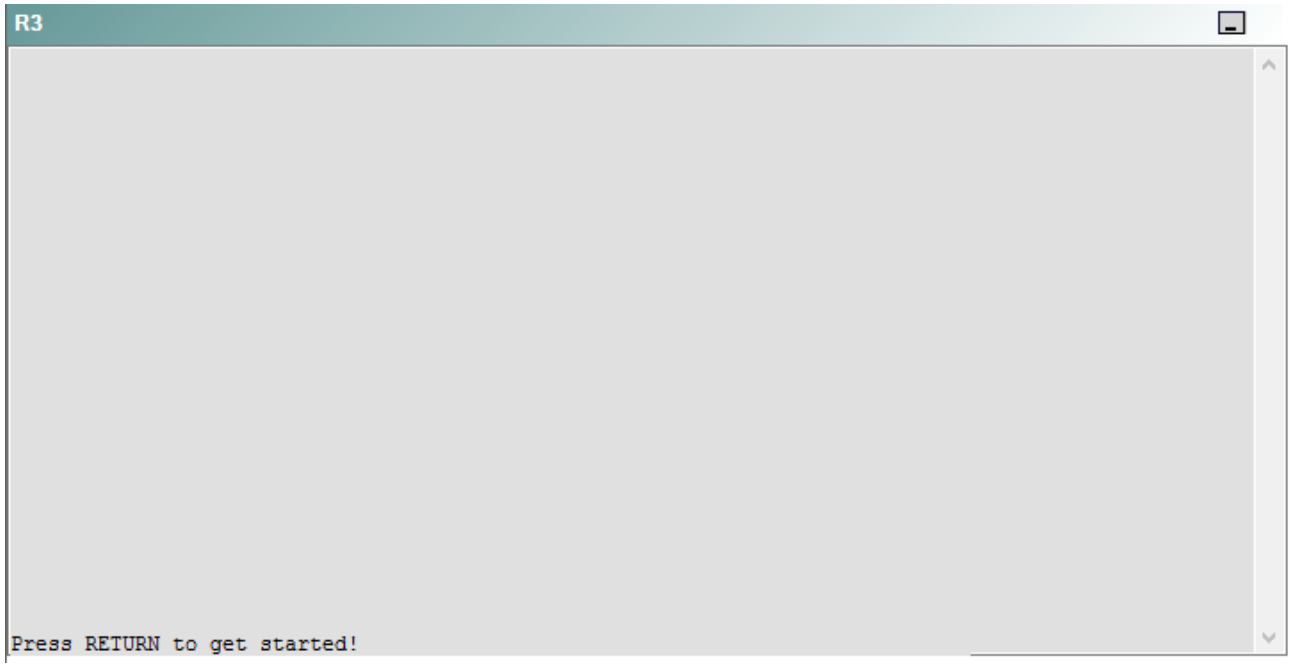
R1



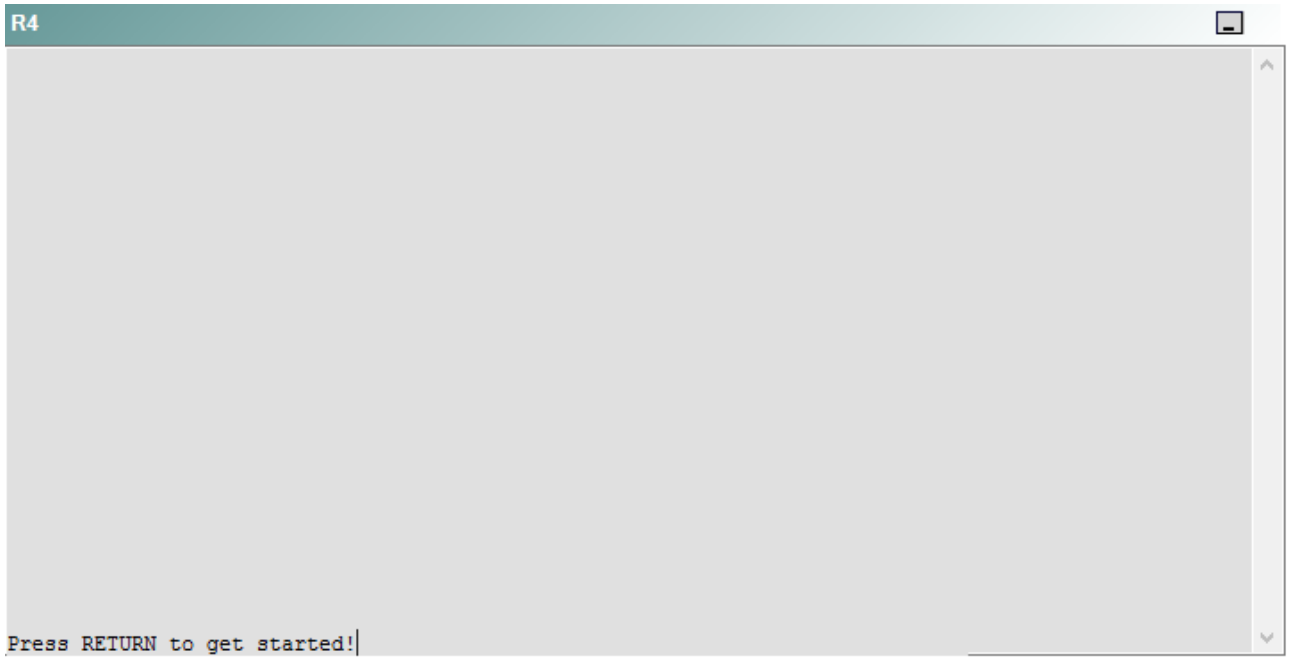

R2



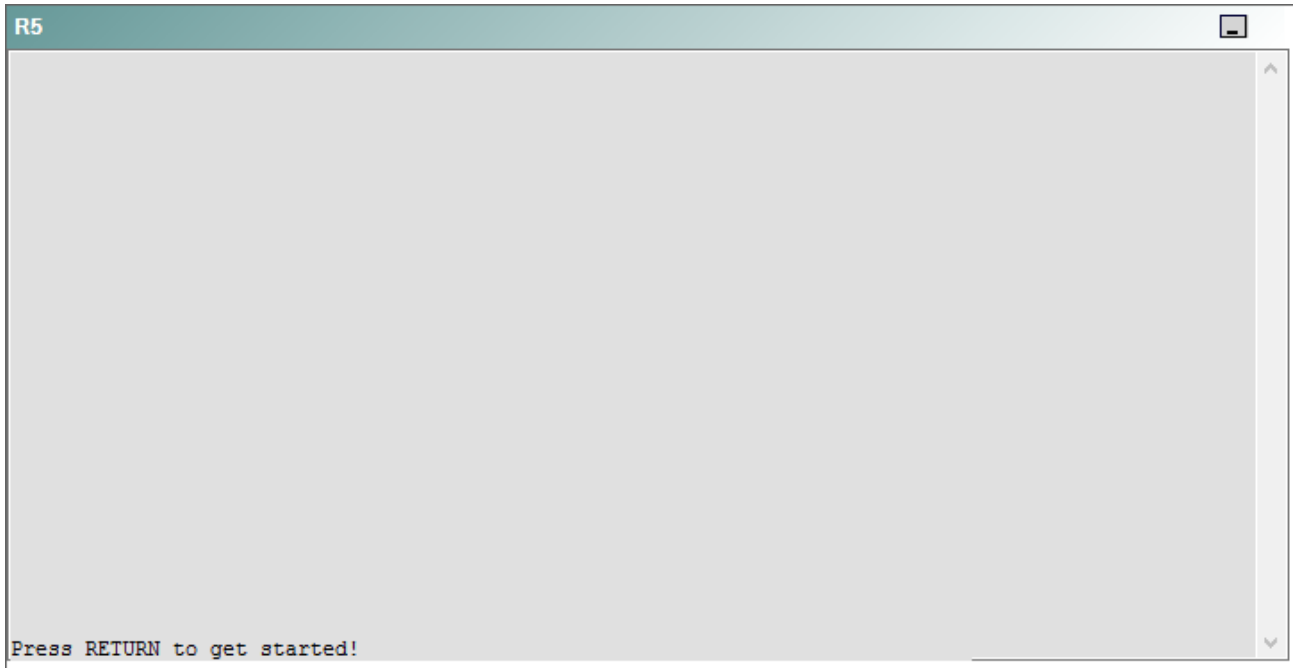

R3



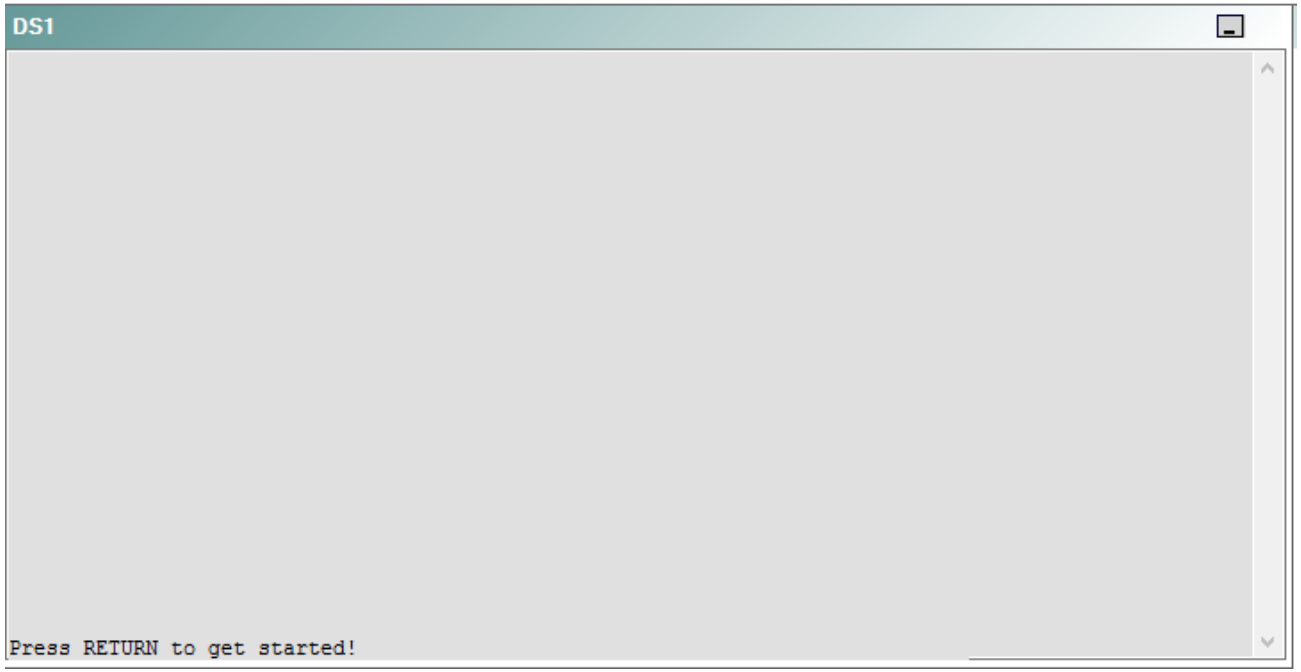

R4



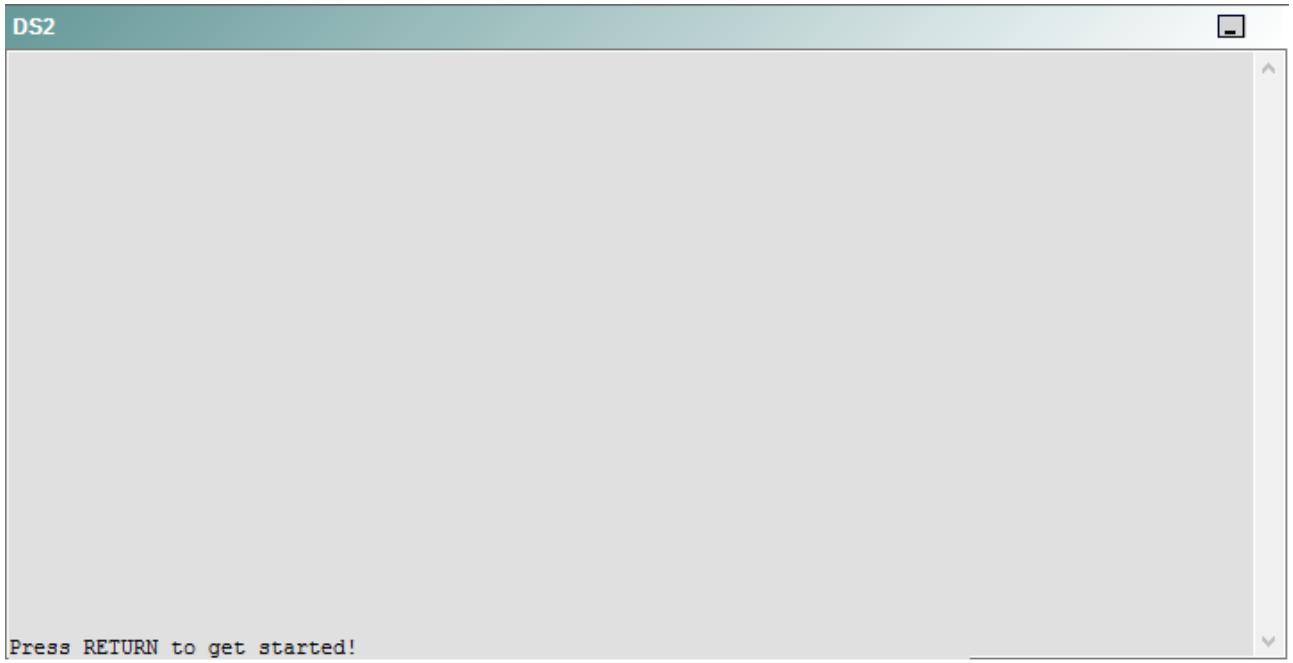

R5



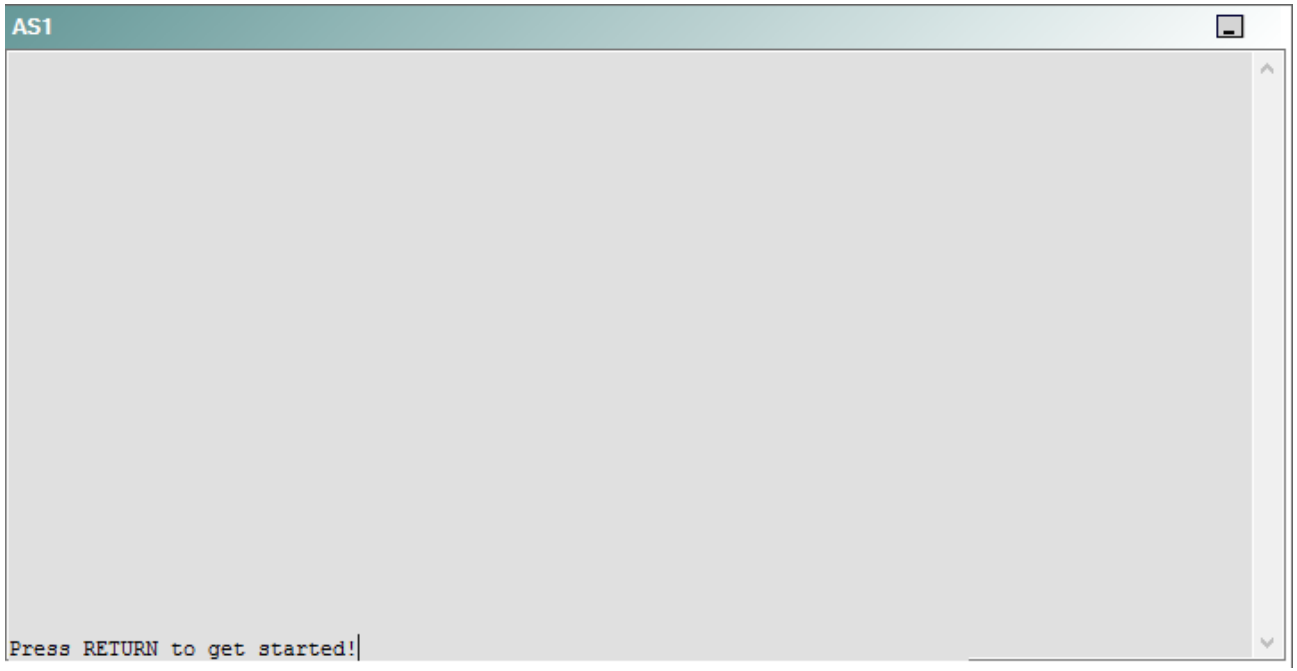

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that, upon reboot, DS1 is not becoming the active router for devices on VLAN 11. DS1 should be the active router for devices on VLAN 11 when DS1 is up, but DS2 should become the active router when DS1 is down.

Which of the following technologies is the source of the problem?

A. NTP
B. HSRP
C. OSPFv2
D. DHCP
E. Layer 3 addressing
F. STP
G. Etherchannel
H. VLAN configuration
I. interface

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

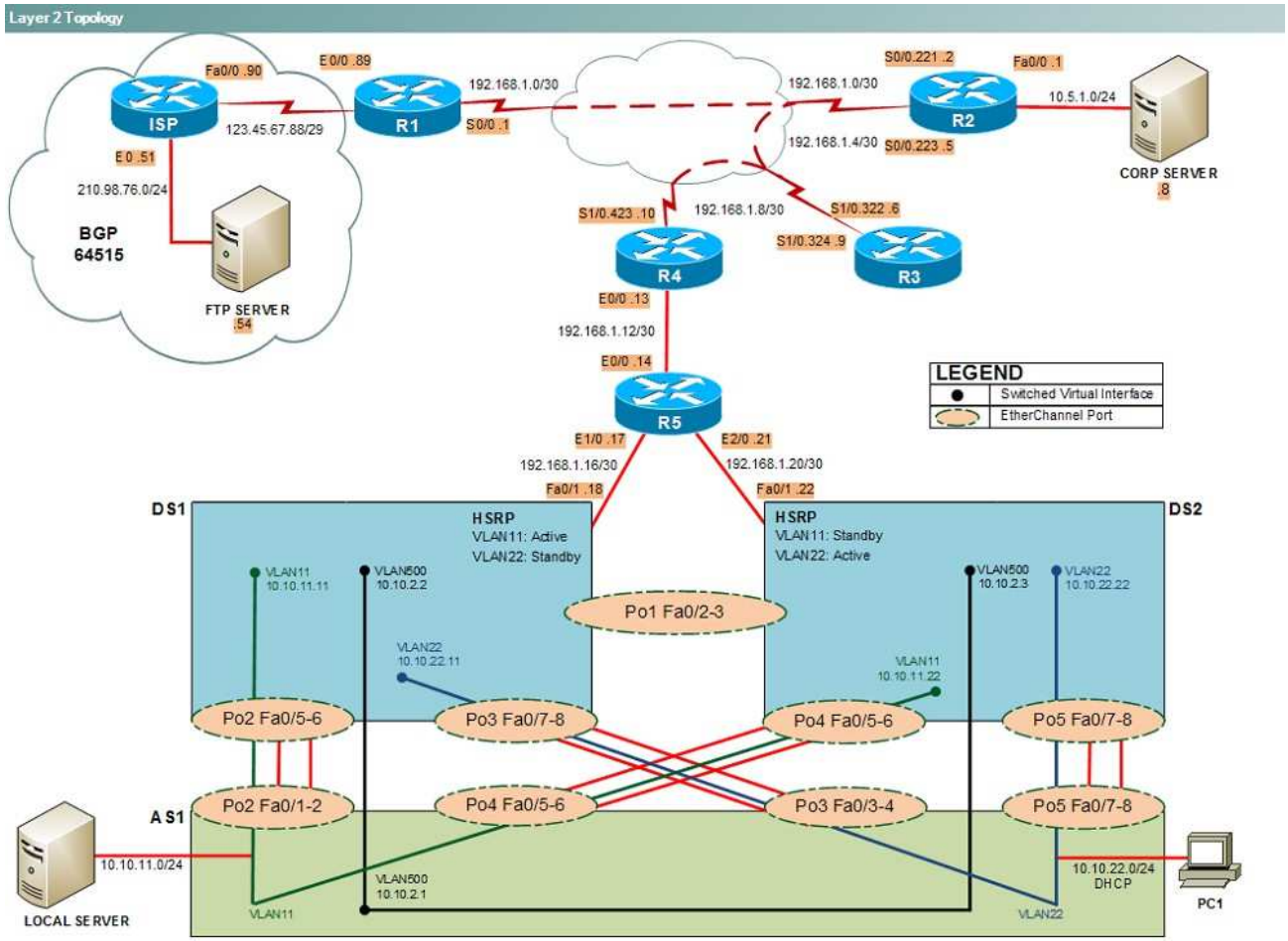
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

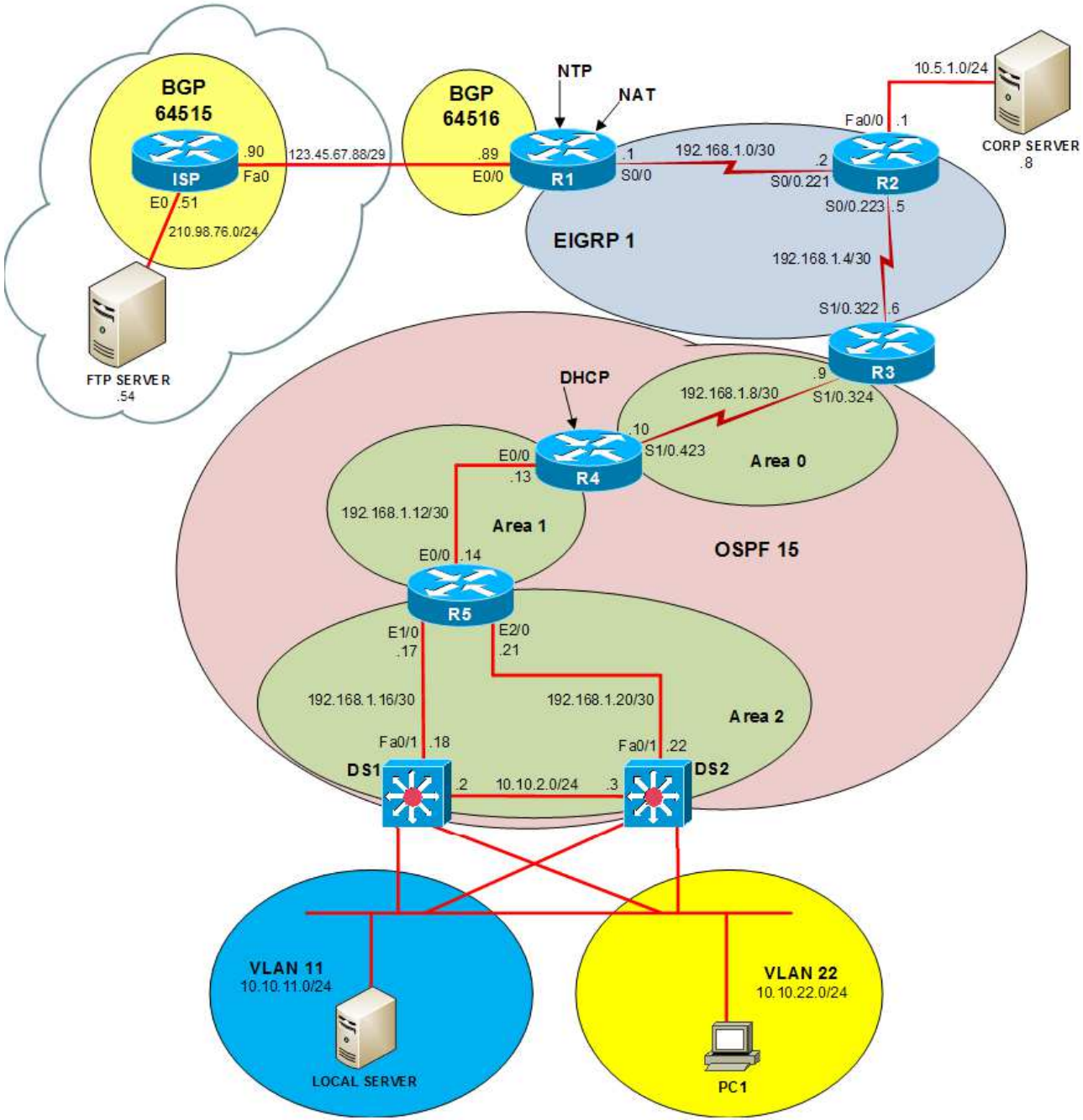
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

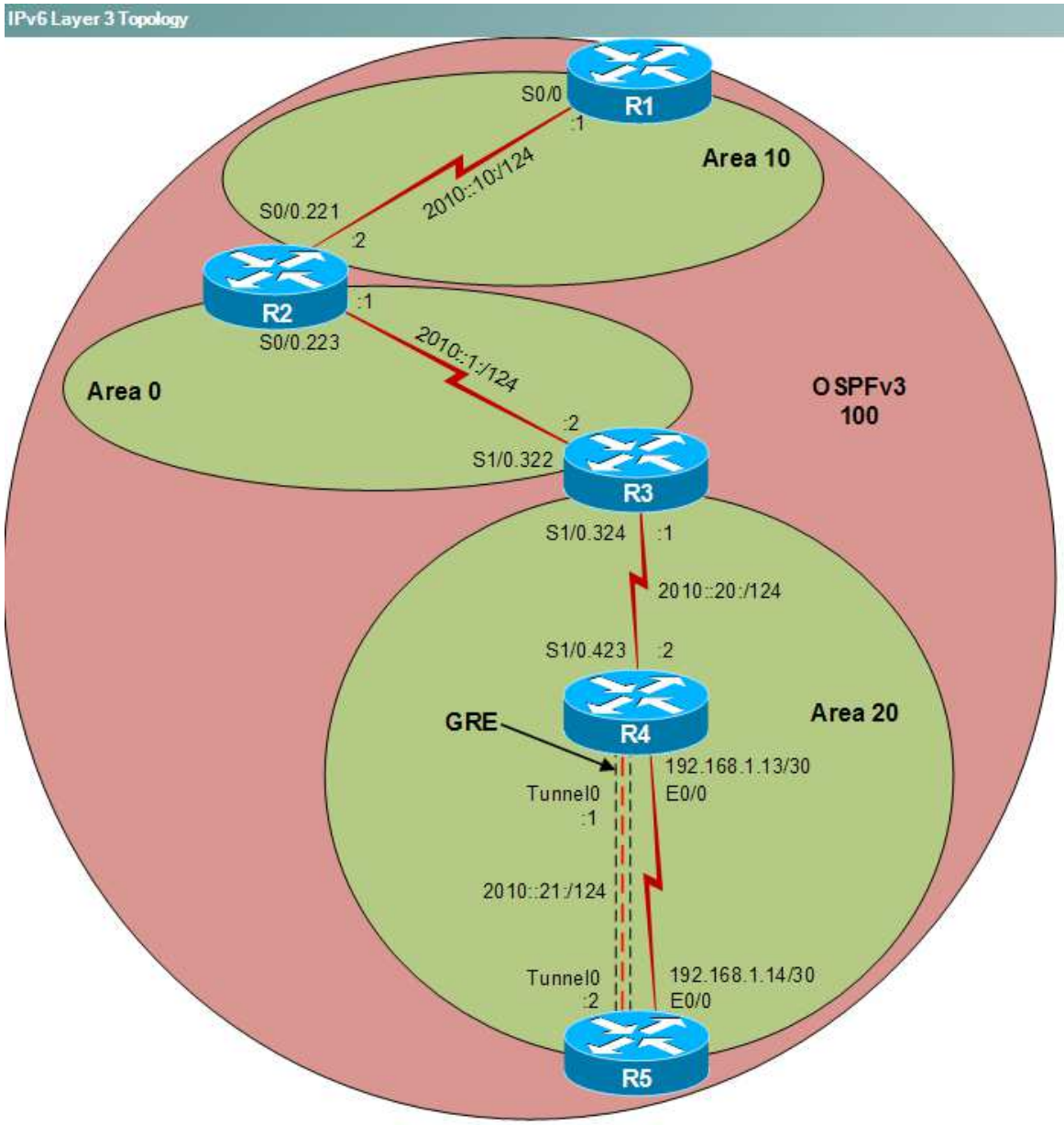
**Layer 2 Topology**




IPv4 layer 3 Topology

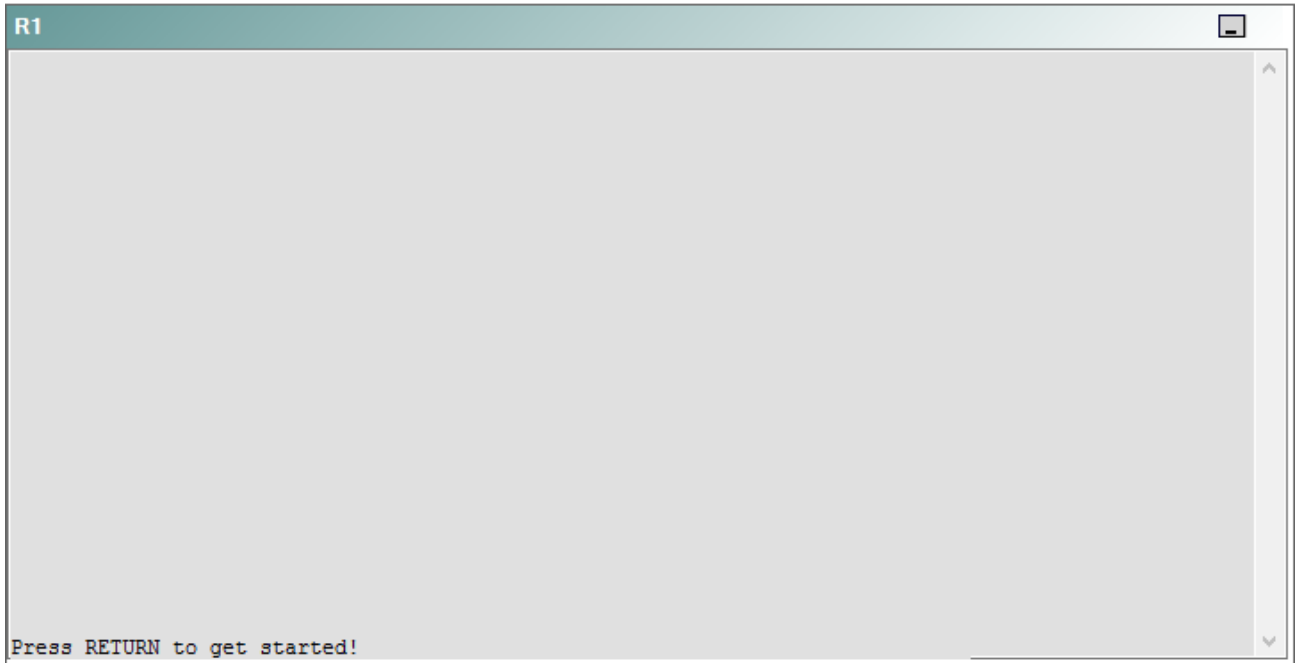

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

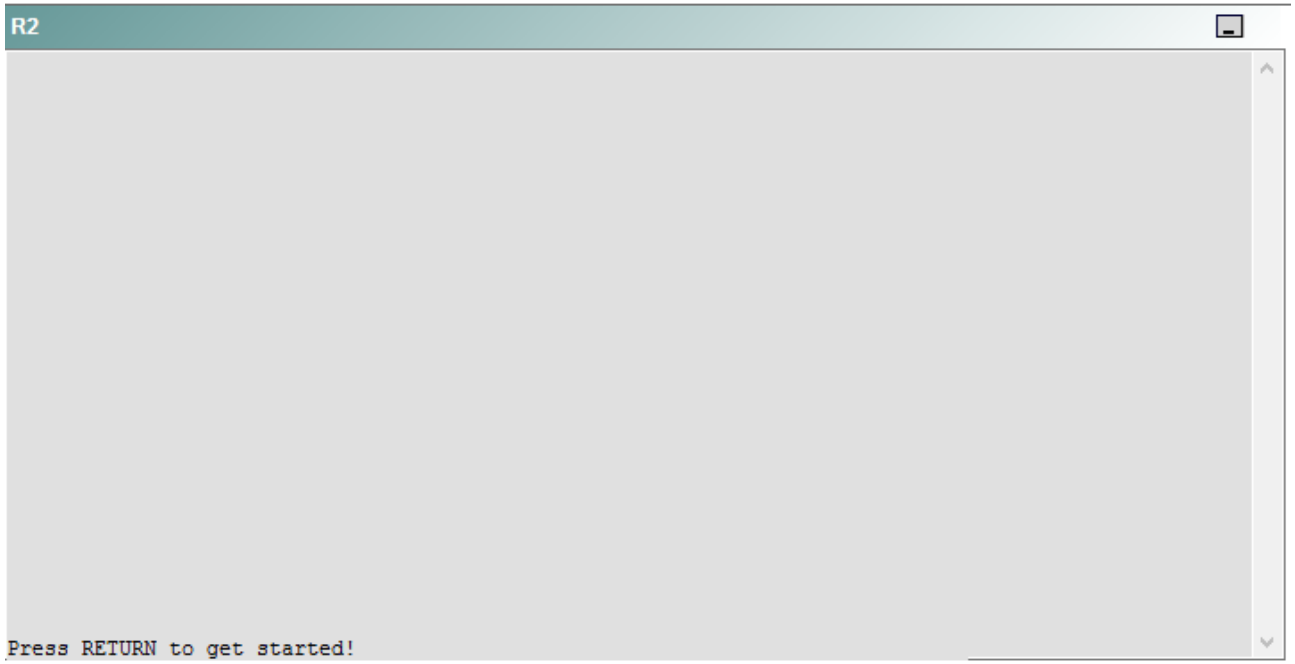



https://www.gratisexam.com/

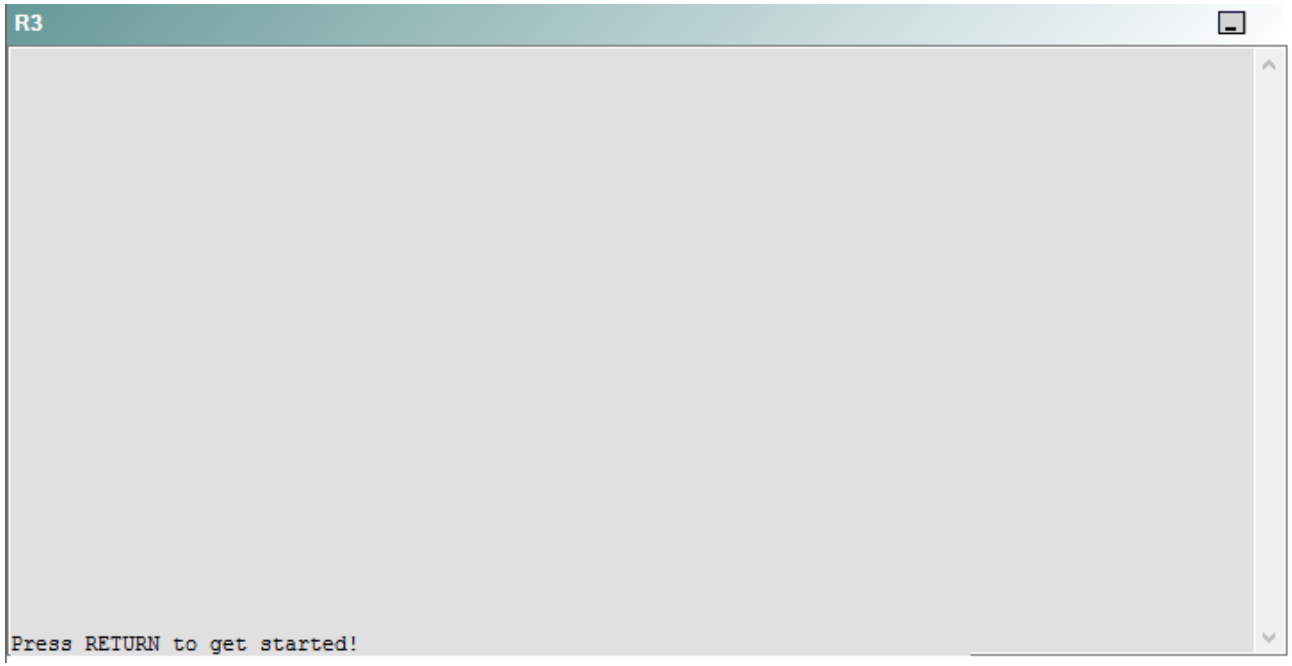
R1



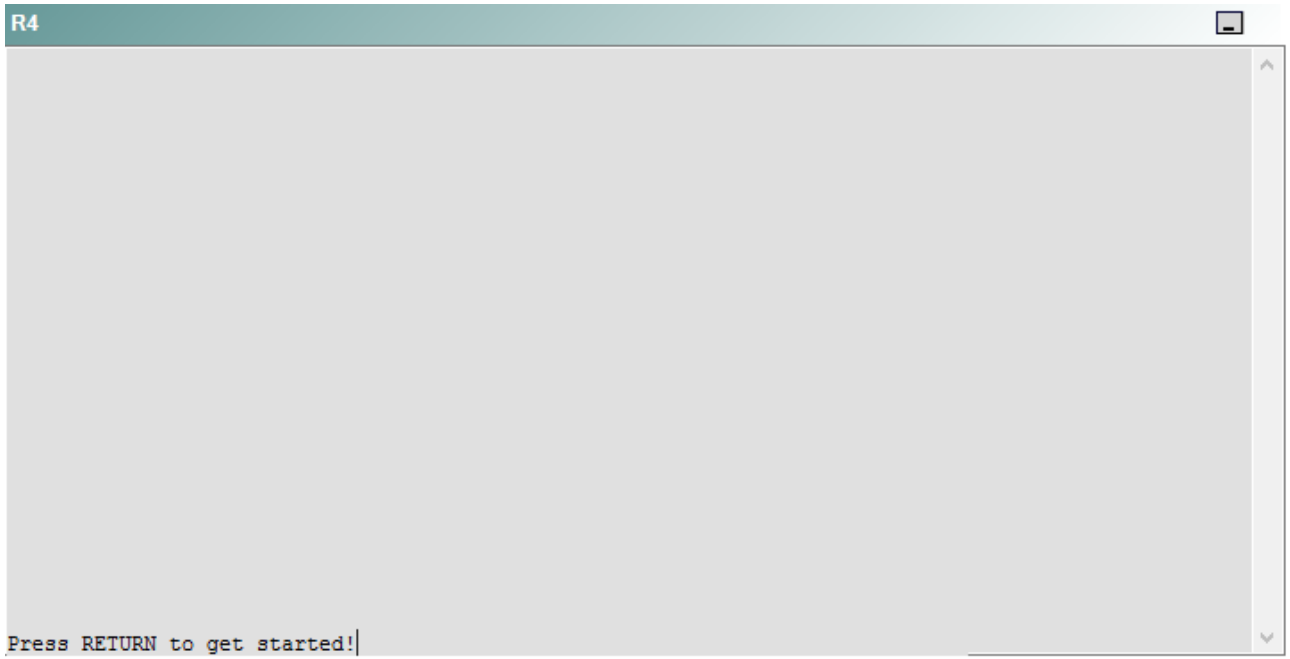

R2



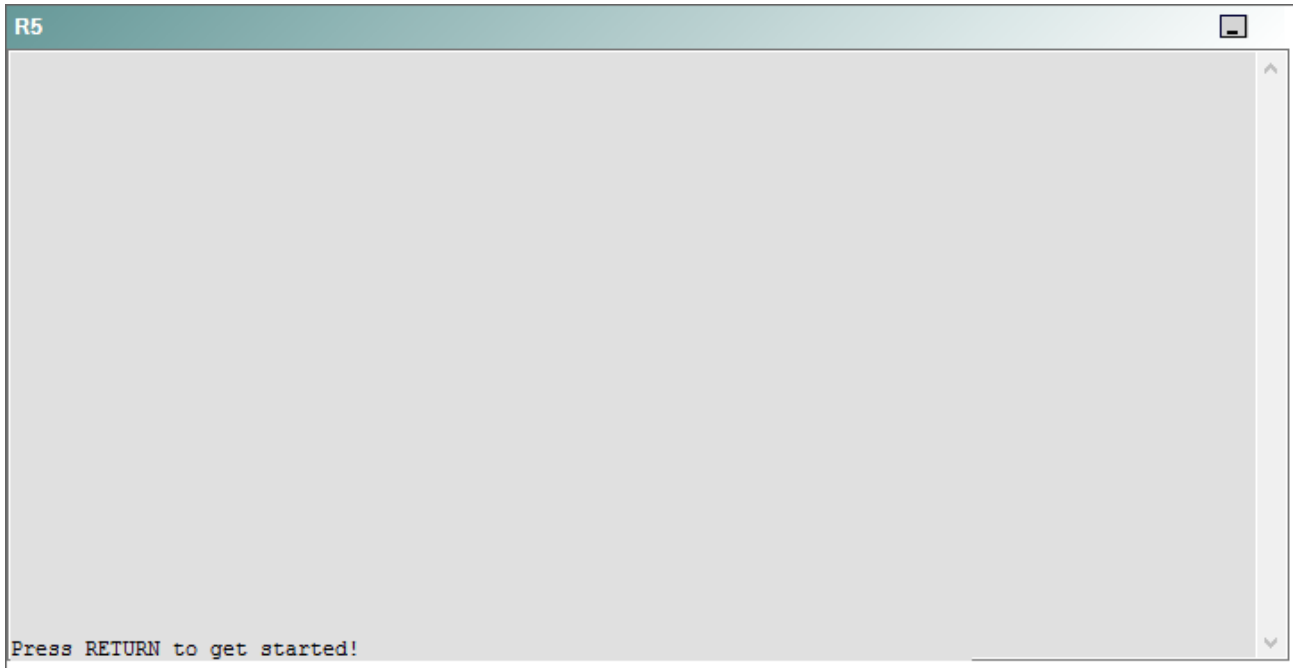

R3



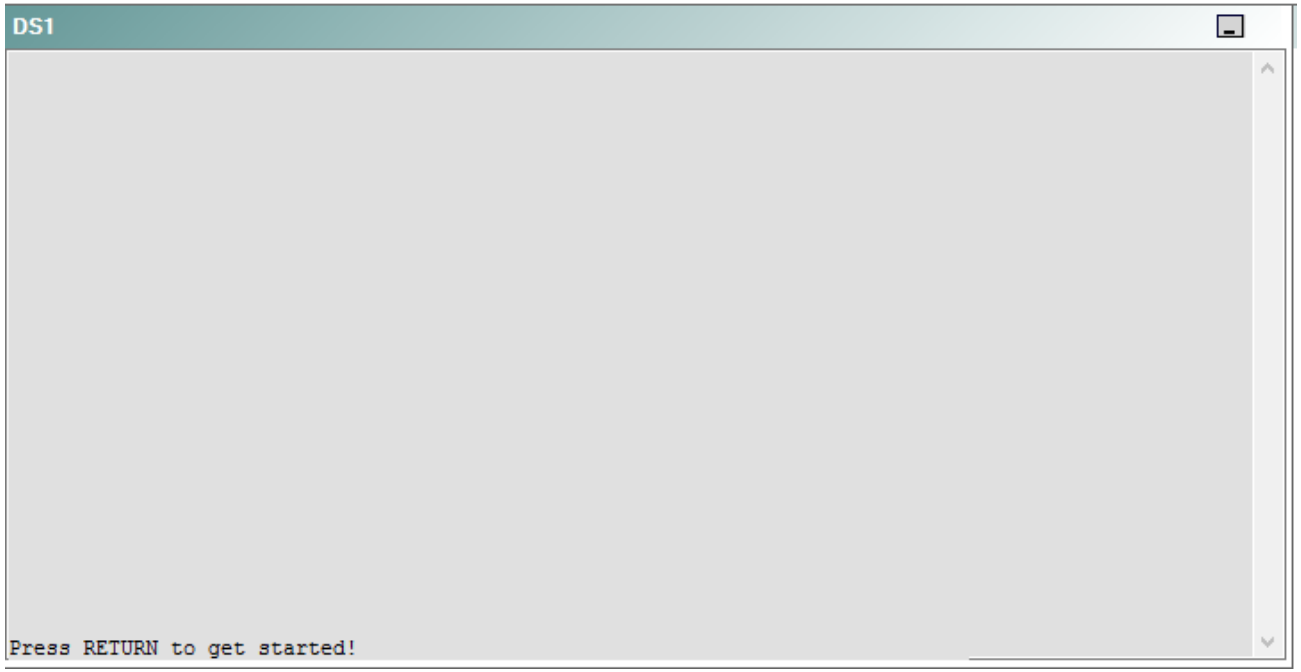

R4



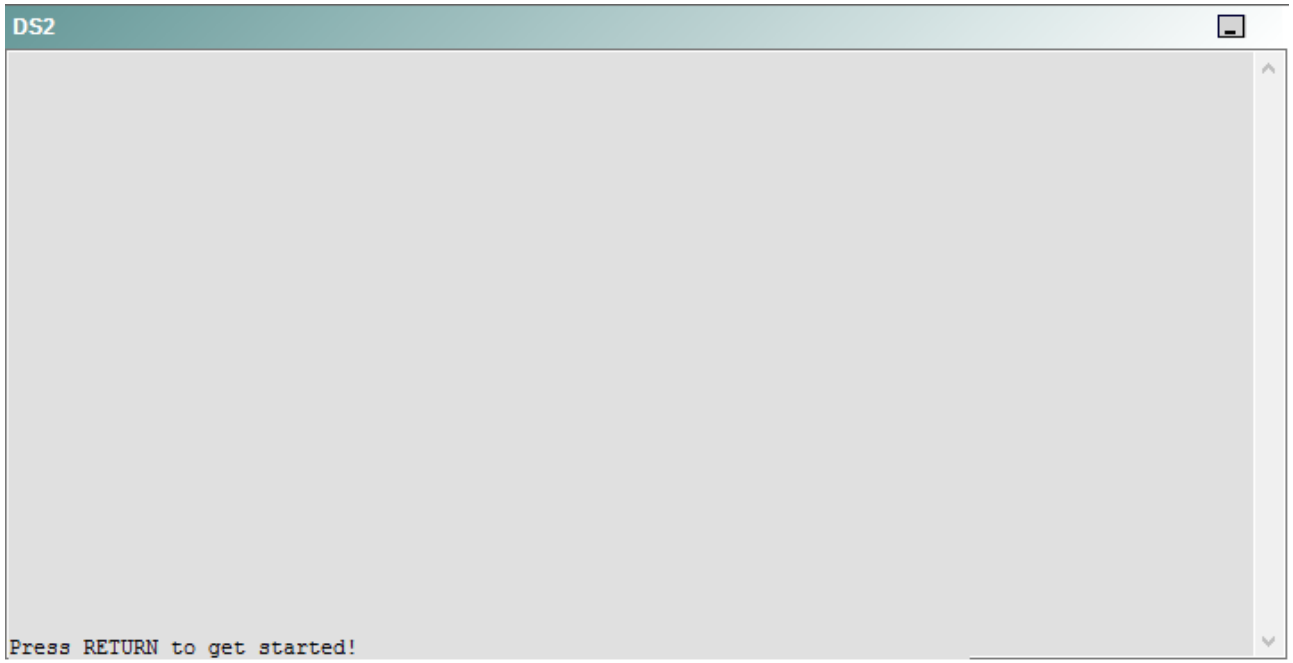

R5



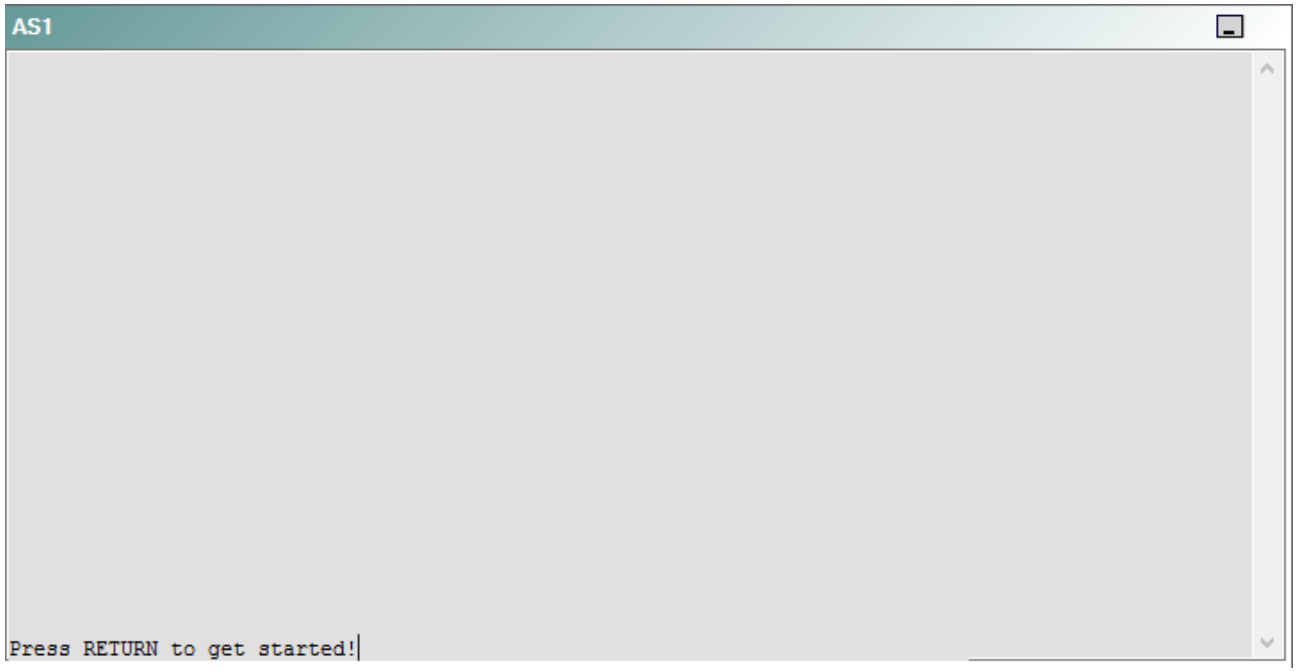

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that, upon reboot, DS1 is not becoming the active router for devices on VLAN 11. DS1 should be the active router for devices on VLAN 11 when DS1 is up, but DS2 should become the active router when DS1 is down.

Which of the following is most likely to solve the problem?

A. issuing the **standby 2 ip 10.10.22.22** command on the VLAN22 interface
B. issuing the **standby 2 ip 10.10.22.25** command on the VLAN22 interface
C. issuing the **standby 1 authentication Secret** command on the Vlan22 interface
D. issuing the **standby 1 authentication Secret** command on the Vlan1 interface
E. issuing the **standby 2 preempt** command on the VLAN11 interface
F. issuing the **standby 1 priority 110** command on the Vlan11 interface
G. issuing the no standby 2 priority 110 on the Vlan22 interface

**Correct Answer:** F
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

You should issue the **standby 1 priority 110** command on the Vlan11 interface DS1. Because there is no connectivity loss on the network, issuing the **ping** and **traceroute** command to test connectivity between devices will not necessary yield the cause of the problem in this scenario. However, you can use the **ping** and **traceroute** commands to verify that DS1 is up and functioning. For example, if you were to issue the **ping 10.10.11.11** command from PC1, you would receive the following partial output:

```
Reply from 10.10.11.11: bytes=32 time=1ms TTL=255
Reply from 10.10.11.11: bytes=32 time=1ms TTL=255
Reply from 10.10.11.11: bytes=32 time=1ms TTL=255
Reply from 10.10.11.11: bytes=32 time=1ms TTL=255
```

The output above indicates that the Vlan11 interface IP address on DS1 is up and reachable from PC1. Additionally, if you were to issue the **ping 210.98.76.54** command from DS1, you would receive the following output:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 210.98.76.54, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 93/99/101 ms
```

The output above indicates that DS1 is able to connect to and communicate with the external server on the public side of the network. Therefore, DS1 does not have a connectivity problem. To determine the source of the problem, you should verify that the Hot Standby Router Protocol (HSRP) configuration is correct on DS1 and DS2, which are the two Layer 3 switches that act as HSRP devices in this scenario.

If you were to issue the **show standby** command on DS1 and on DS2, you would receive the following partial output:

```
DS1#show standby
Vlan11 - Group 1
  State is Standby
    1 state change, last state change 00:18:25
  Virtual IP address is 10.10.11.25
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.647 secs
  Authentication text "Secret"
  Preemption enabled
  Active router is 10.10.11.22, priority 100 (expires in 8.272 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Vl11-1" (default)

DS2#show standby
Vlan11 - Group 1
  State is Active
    5 state changes, last state change 00:18:58
  Virtual IP address is 10.10.11.25
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.690 secs
  Authentication text "Secret"
  Preemption enabled
  Active router is local
  Standby router is 10.10.11.11, priority 100 (expires in 7.475 sec)
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Vl11-1" (default)
```

The output above indicates that HSRP Group 1 has been configured on DS1 and DS2 with a default HSRP priority value of 100. Additionally, both DS1 and DS2 have HSRP preemption enabled. Preemption allows one HSRP device to take over the active router role from another HSRP device, depending on the HSRP priority values that have been configured for the devices. For example, DS2 has been configured with an HSRP propriety value of 110 for HSRP Group 2. Because

**the standby 2 priority 110** command has not been issued on DS1, the default HSRP priority value of 100 will be used for HSRP Group 2 on DS1. When DS2 goes down, DS1 will automatically take over the active router role for virtual LAN (VLAN) 22. When DS2 becomes available again, DS2 will preempt DS1 and assume the active router role because it has been configured with a higher priority for HSRP Group 2.

In this scenario, both DS1 and DS2 have been configured with the same priority value for HSRP Group 1. Therefore, the device that first assumes the active router role for VLAN 11 will maintain that role until that device either goes down or is rebooted. If the original active router goes down or is rebooted, the backup HSRP device will assume the active router role and maintain that role even when the original active router becomes available again, because the priority values are the same.

To enable DS1 to assume the active router role for HSRP Group 1 after DS1 is rebooted, you should issue the **standby 1 priority 110** command on interface Vlan11 of DS1. The **standby 1 priority 110** command configures HSRP Group 1 on the Vlan11 interface with a higher priority than the default value of 100. As long as DS1 is configured with a higher HSRP priority than DS2, it will retake the active router role for HSRP Group 1 from DS2.

You need not issue the **standby 2 preempt** command on the Vlan22 interface on DS1 or DS2. HSRP Group 2 is configured correctly in this scenario, and the **standby 2 preempt** command has already been issued on the Vlan22 interface on DS1 and DS2.

You should not issue the **standby 2 ip 10.10.22.22** command on the Vlan22 interface DS1 or DS2. The **standby 2 ip 10.10.22.22** command would configure the HSRP virtual IP address on DS1 or DS2 to the same IP address as the Vlan22 interface on DS2, which would result in an IP conflict.

You need not issue the **standby 2 ip 10.10.22.25** command on the Vlan22 interface on DS1 or DS2. The **standby 2 ip 10.10.22.25** command has already been issued on the Vlan22 interface on DS1 and DS2 in this scenario.

You need not issue the **standby 1 authentication Secret** command on the Vlan22 interface on DS1 or DS2. Additionally, you need not issue the **standby 2 authentication Secret** command on the Vlan 11 interface on DS1 or DS2. The **standby 1 authentication Secret** command configures HSRP authentication on HSRP Group 1, which is configured on the Vlan11 interface of DS1 and DS2. Similarly, the **standby 2 authentication Secret** command configures HSRP authentication on HSRP Group 2, which is configured on the Vlan22 interface of DS1 and DS2. HSRP authentication is already configured correctly on interface Vlan11 and interface Vlan22 on DS1 and DS2 in this scenario.

You should not issue the no **standby 2 priority 110** command on the Vlan22 interface on DS2. Issuing the **no standby 2 priority 110** command would set the HSRP priority for Group 2 to the default value of 100 on DS2. DS2 should have a higher HSRP priority than DS1 for HSRP Group 2 so that DS2 will always assume the role of active router for VLAN 22 when DS2 is up and functioning properly.

You should not issue the **standby 1 track Fa0/1 20** command on the Vlan11 interface on DS1. The **standby 1 track Fa0/1 20** command would configure DS1 to decrement the HSRP priority on HSRP Group 1 from 100 to 80 when the line protocol on the Fa0/1 interface is in the down state; this would ensure that DS2 would have a higher HSRP priority than DS1 on HSRP Group 1 when the Fa0/1 interface on DS1 is down. In this scenario, the Fa0/1 interface on DS1 is up and functional.

**QUESTION 22**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

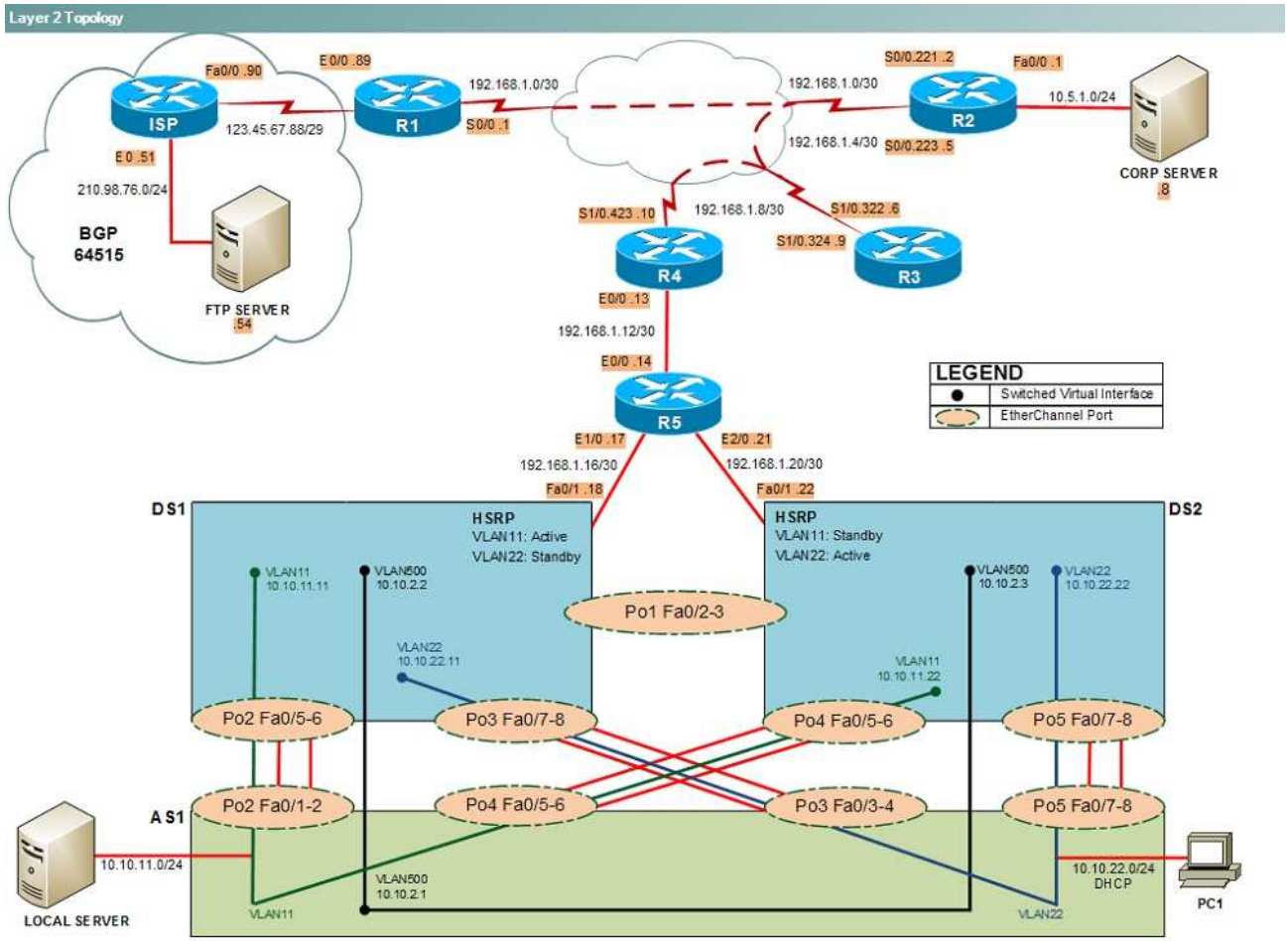
Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

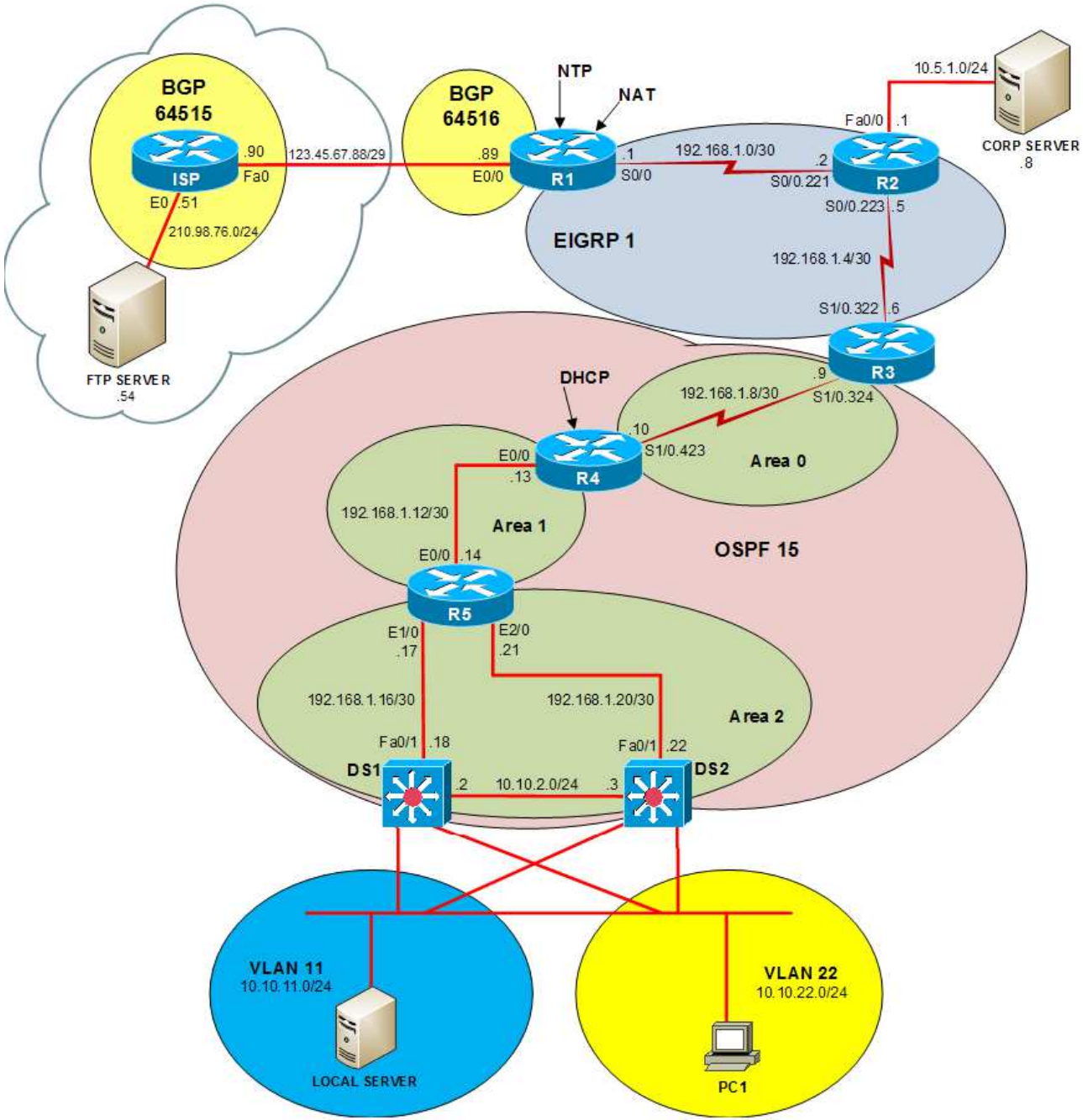
Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

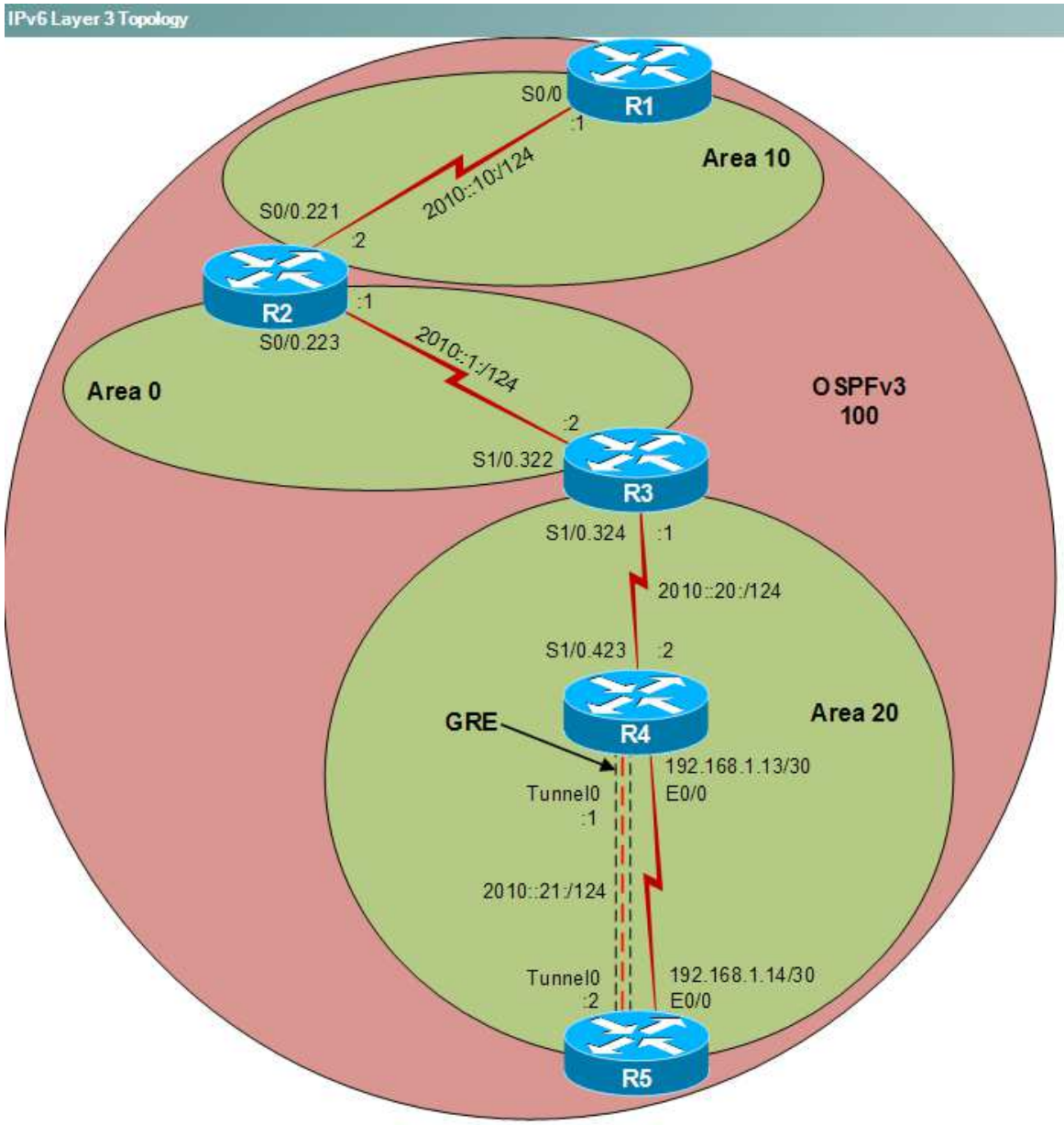
**Layer 2 Topology**




IPv4 layer 3 Topology

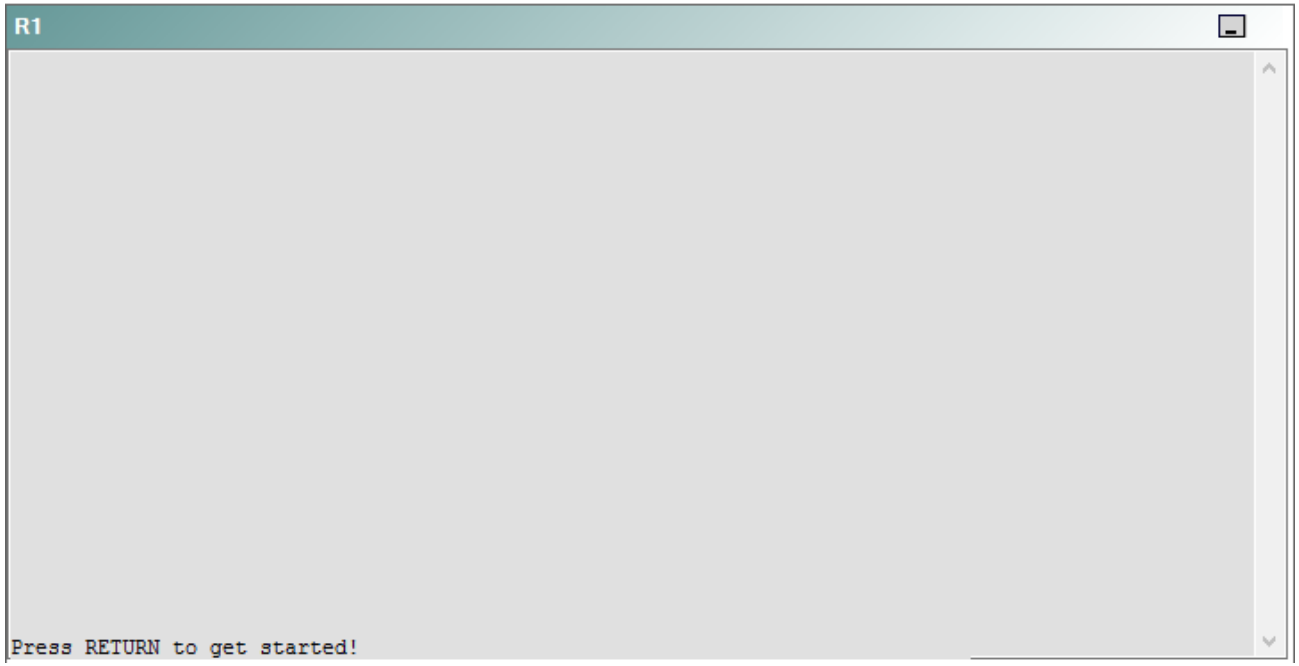

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

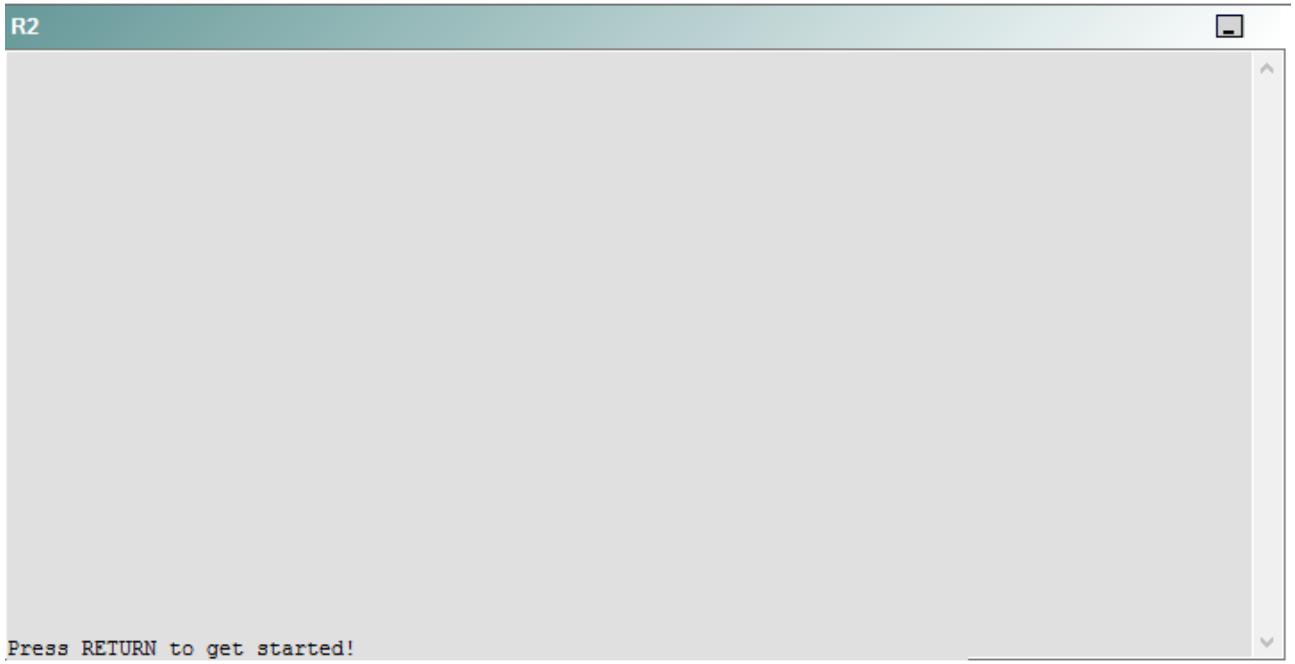



https://www.gratisexam.com/

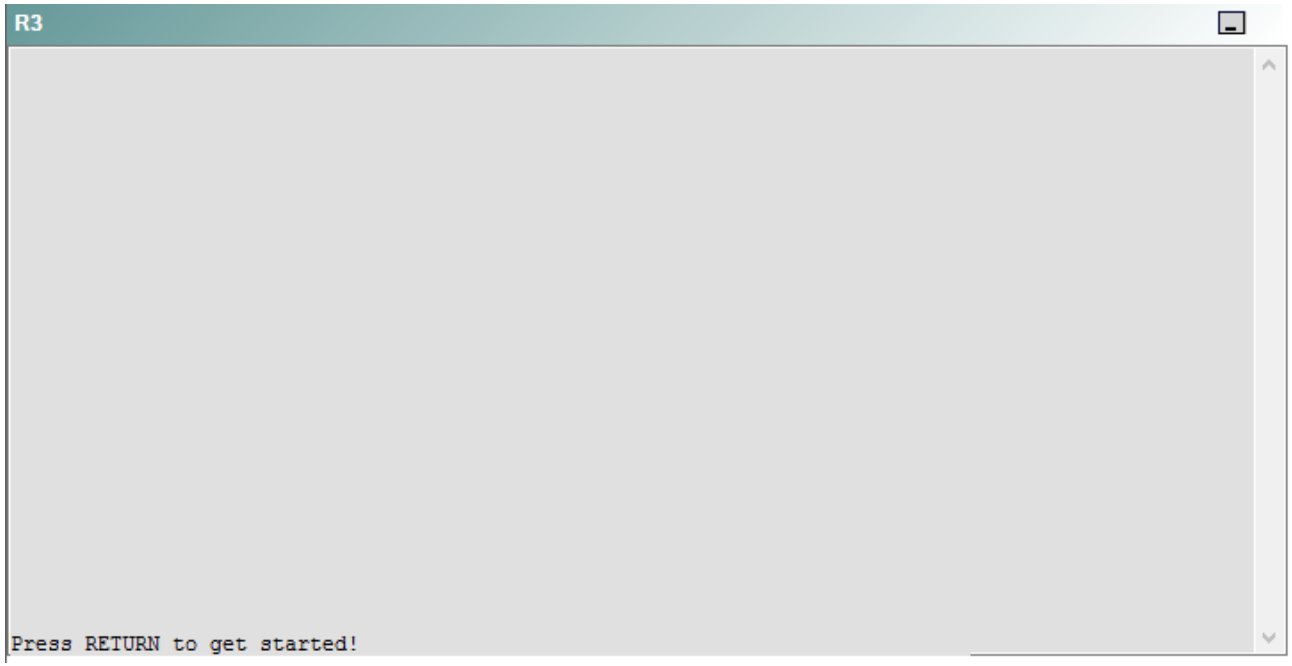
R1



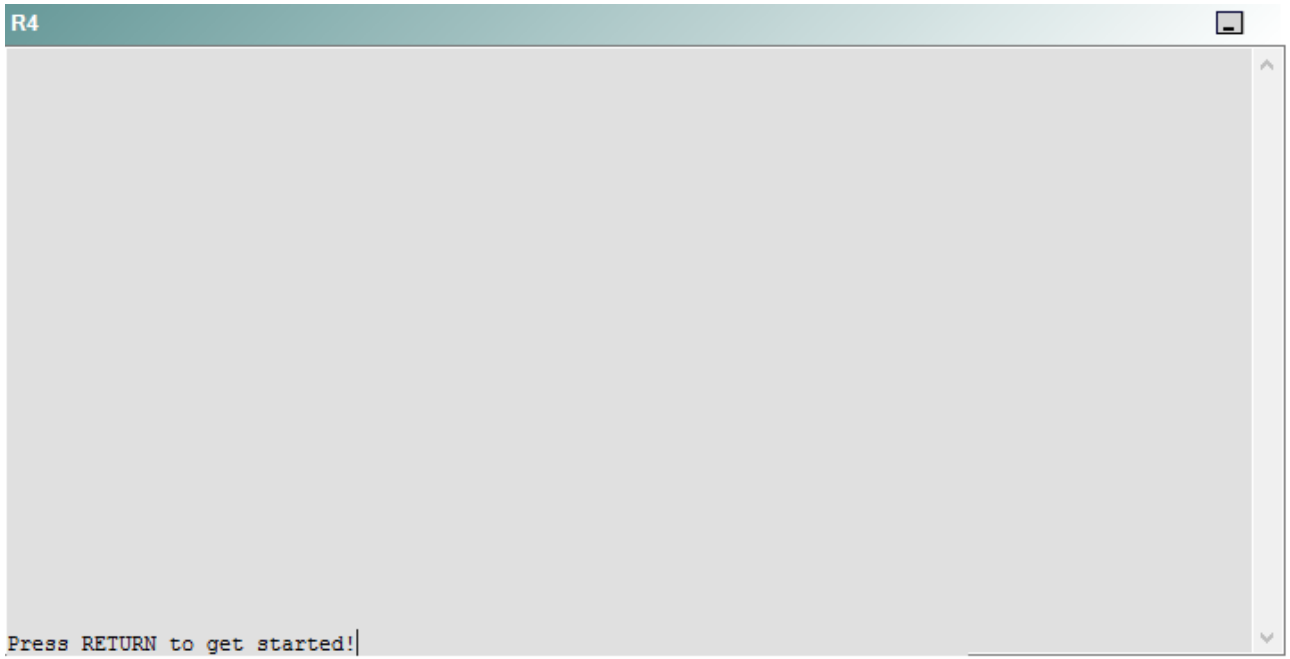

R2



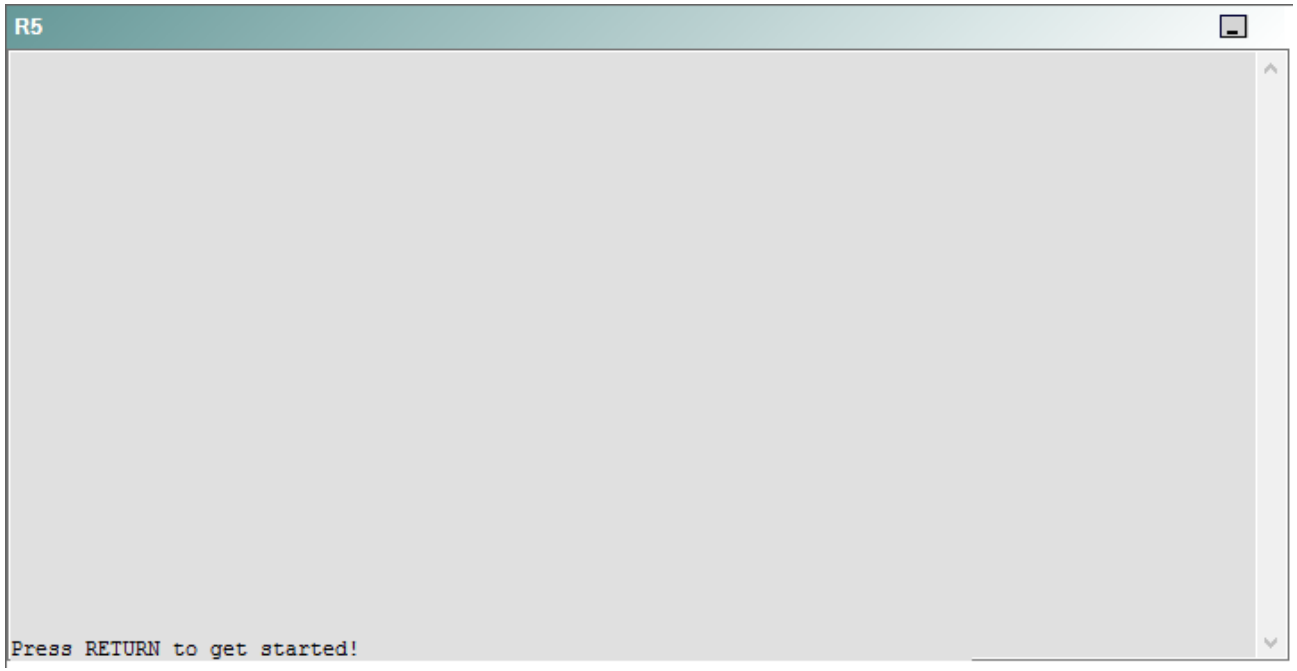

R3



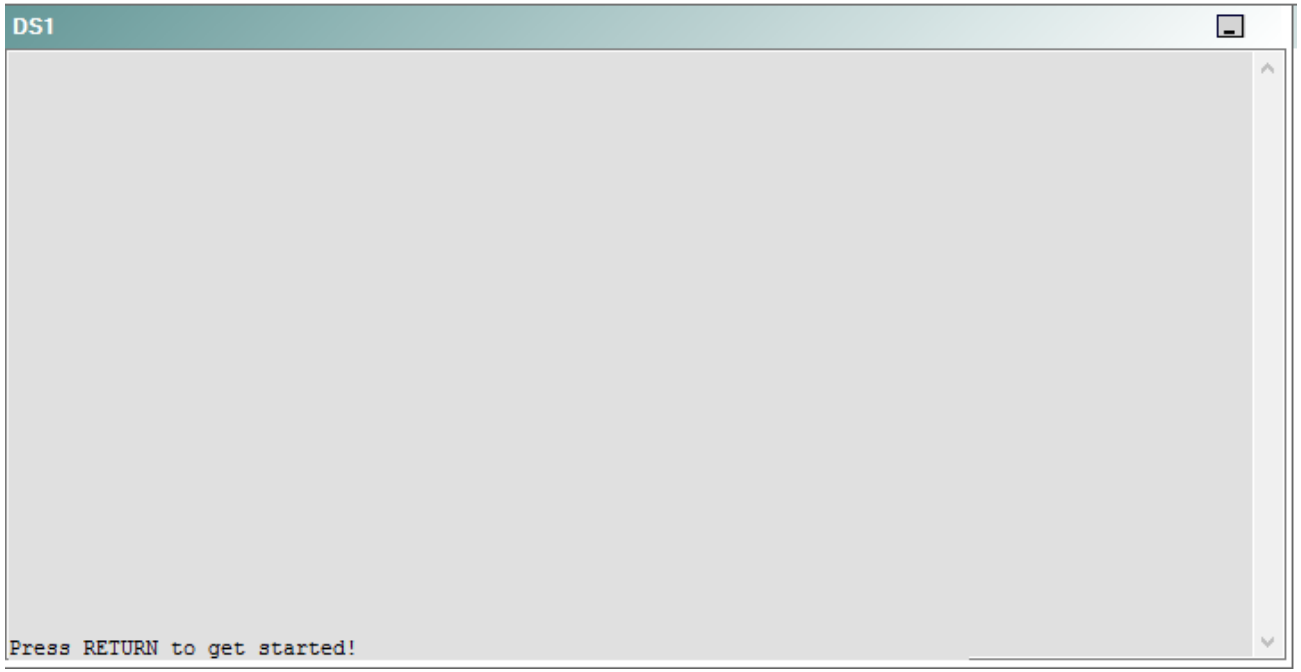

R4



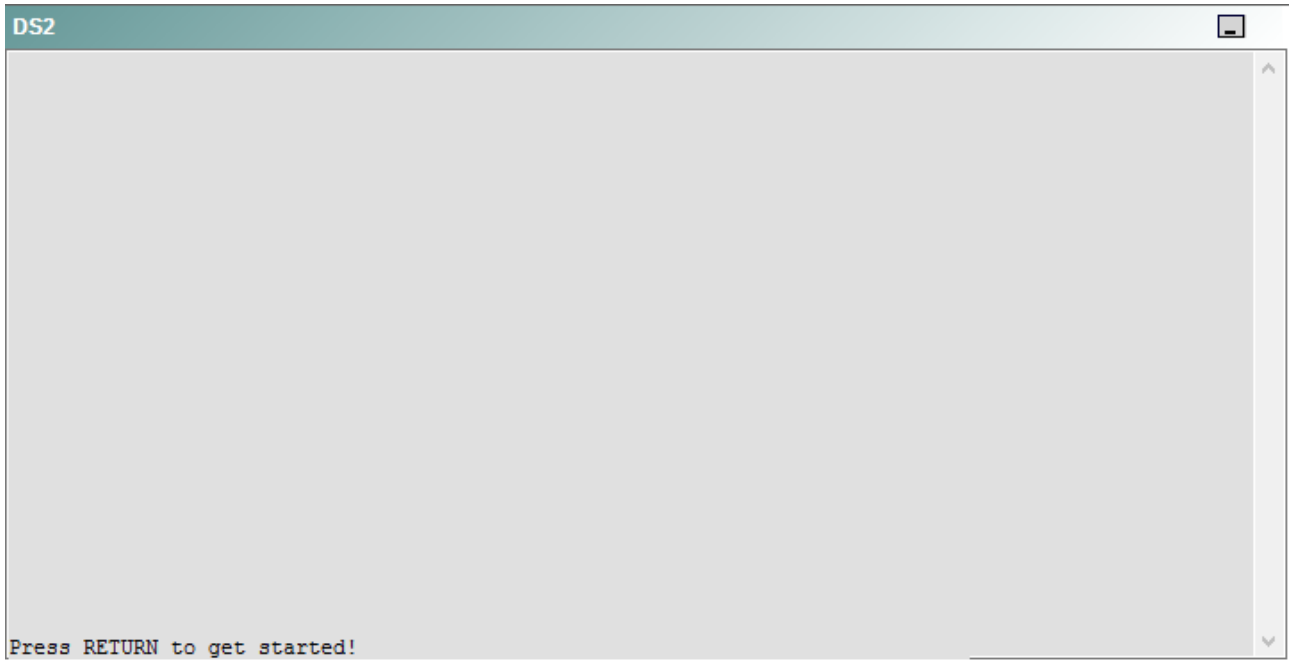

R5



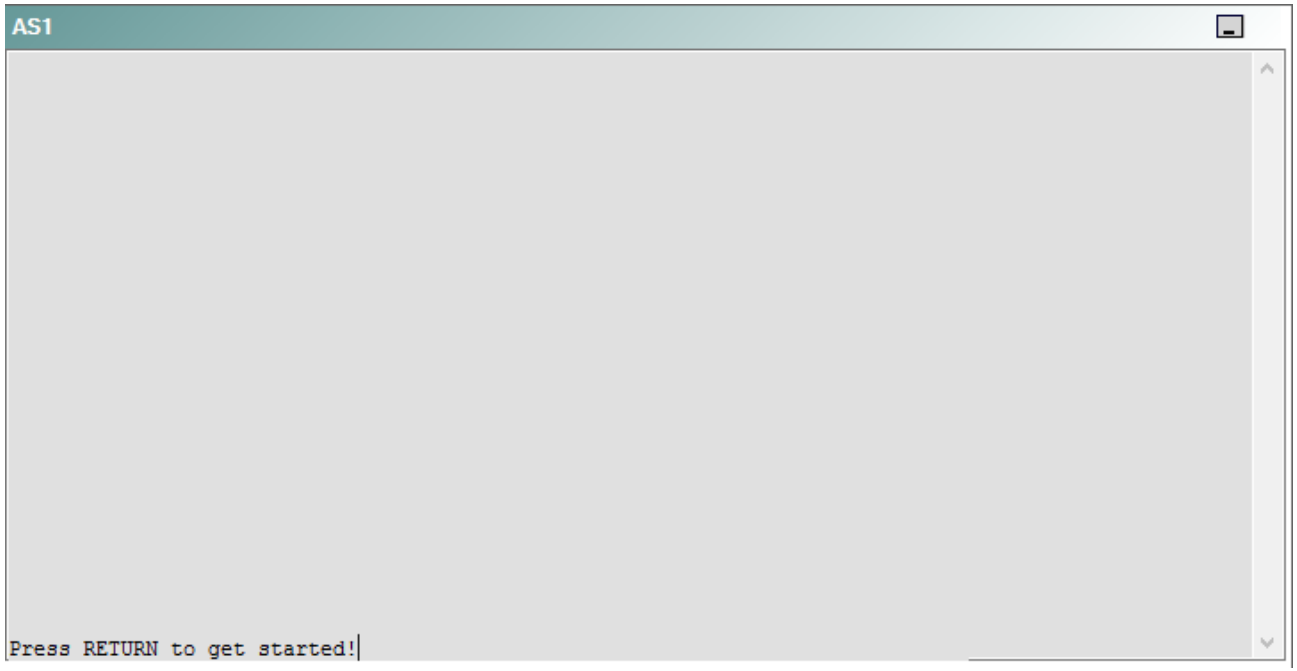

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that R5 is no longer able to ping the IPv6 address 2010::10:1 on R1.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** E
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

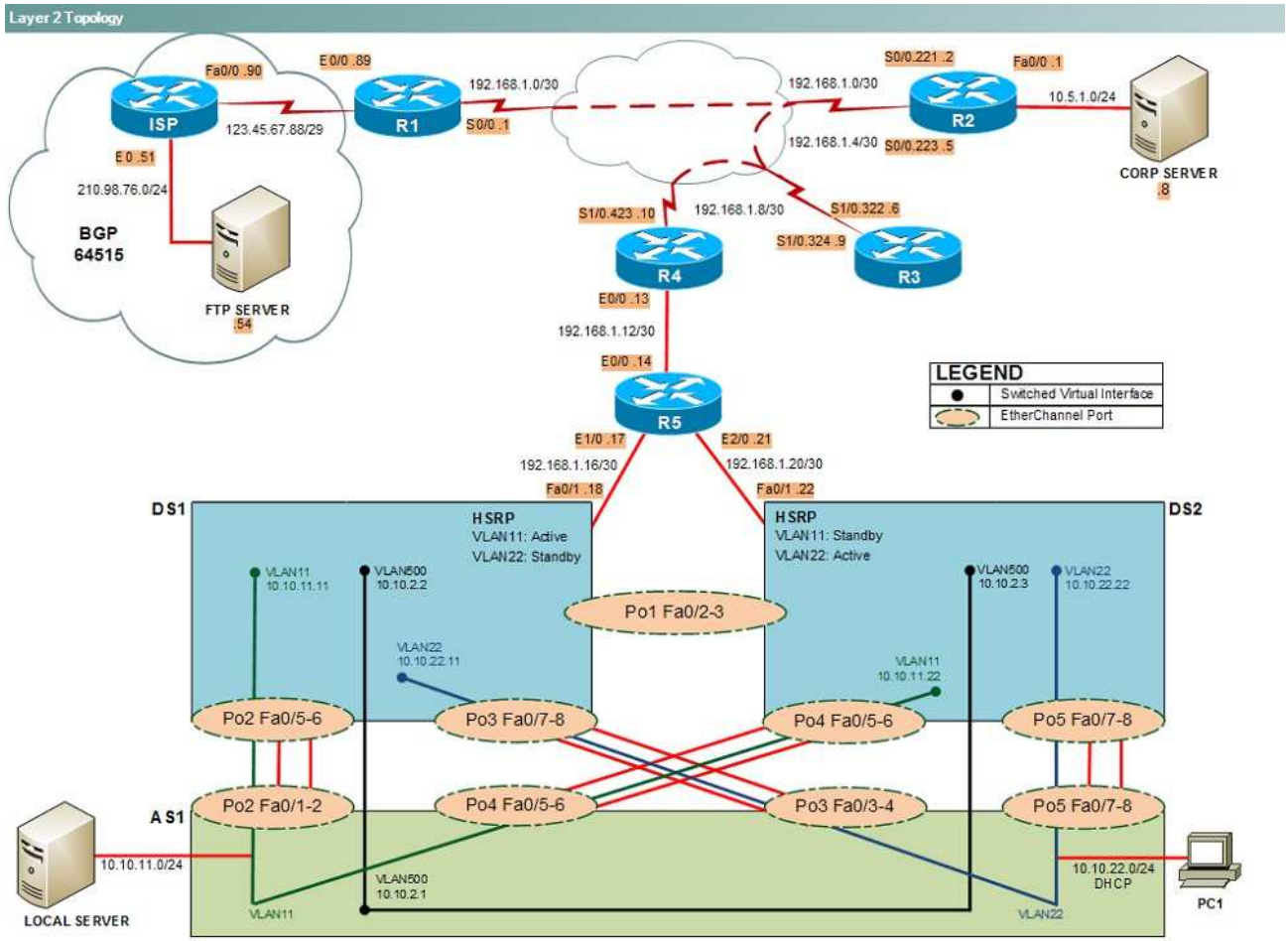
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

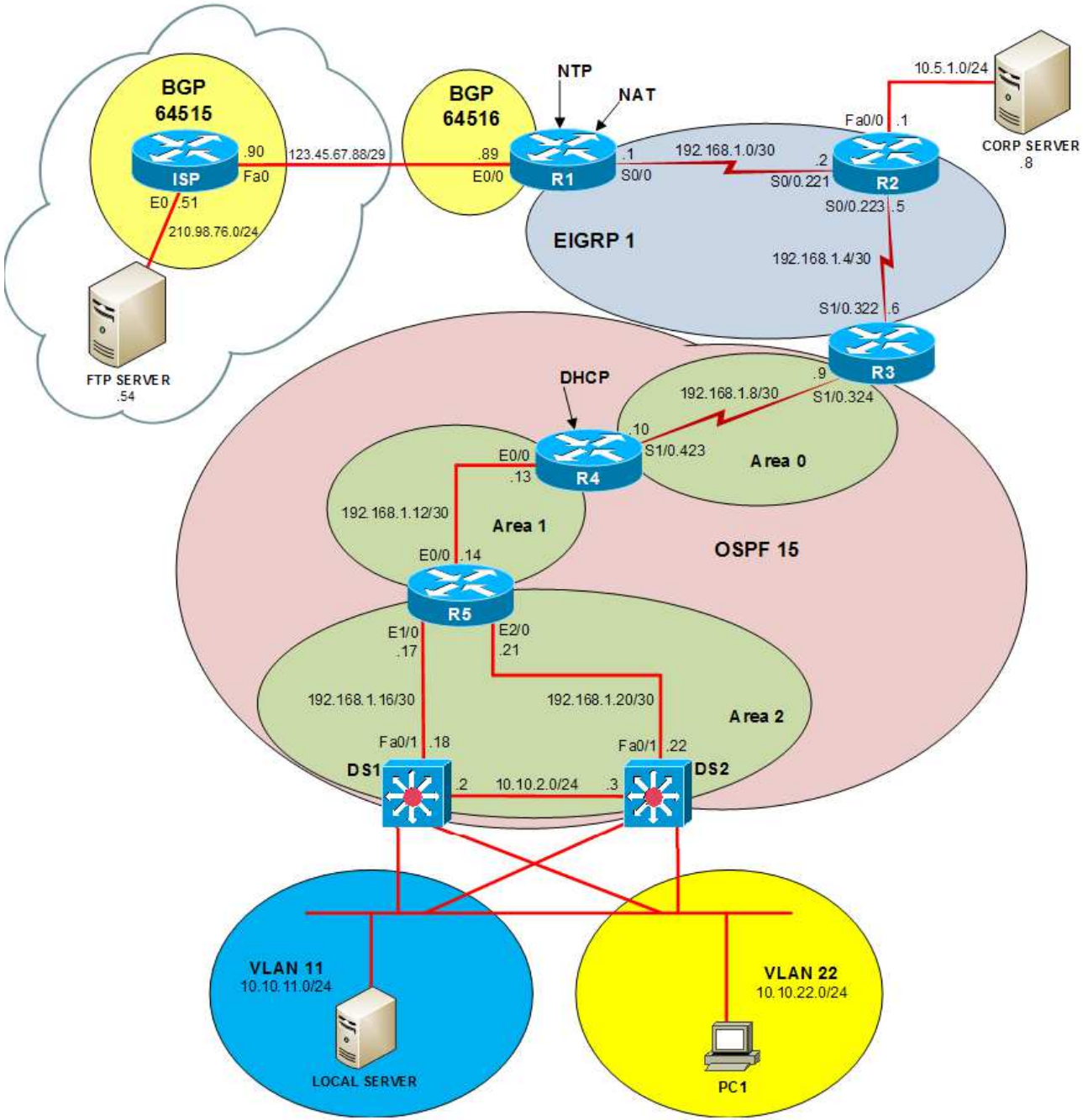
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

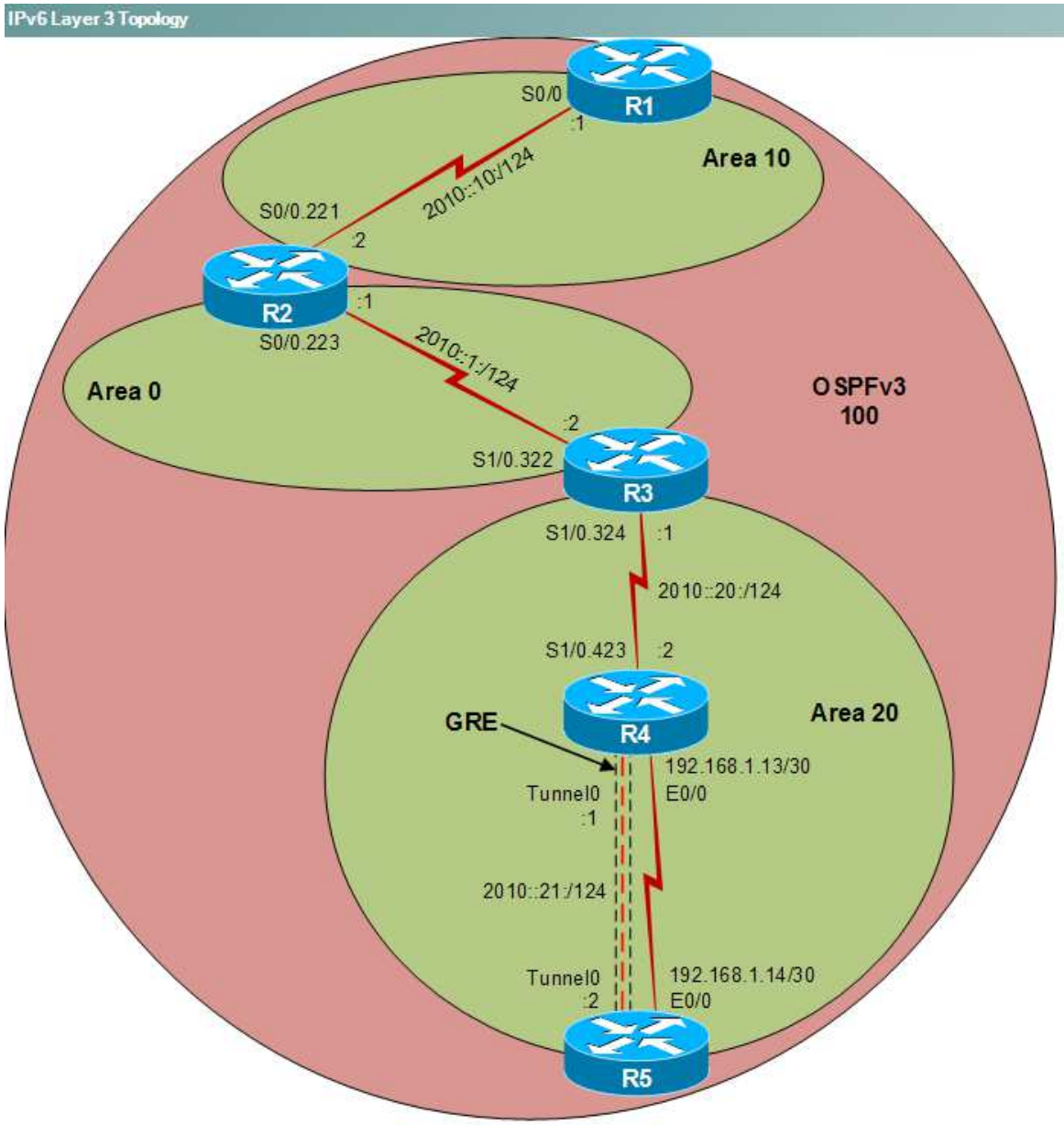
**Layer 2 Topology**




IPv4 layer 3 Topology

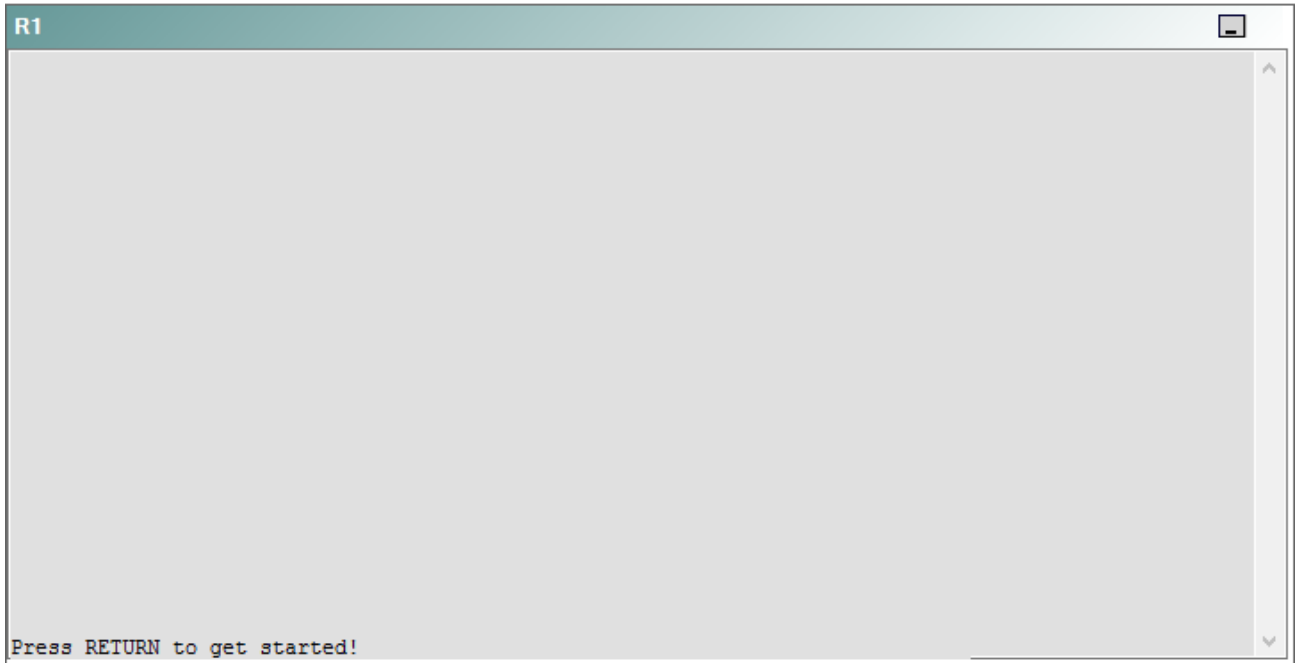

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

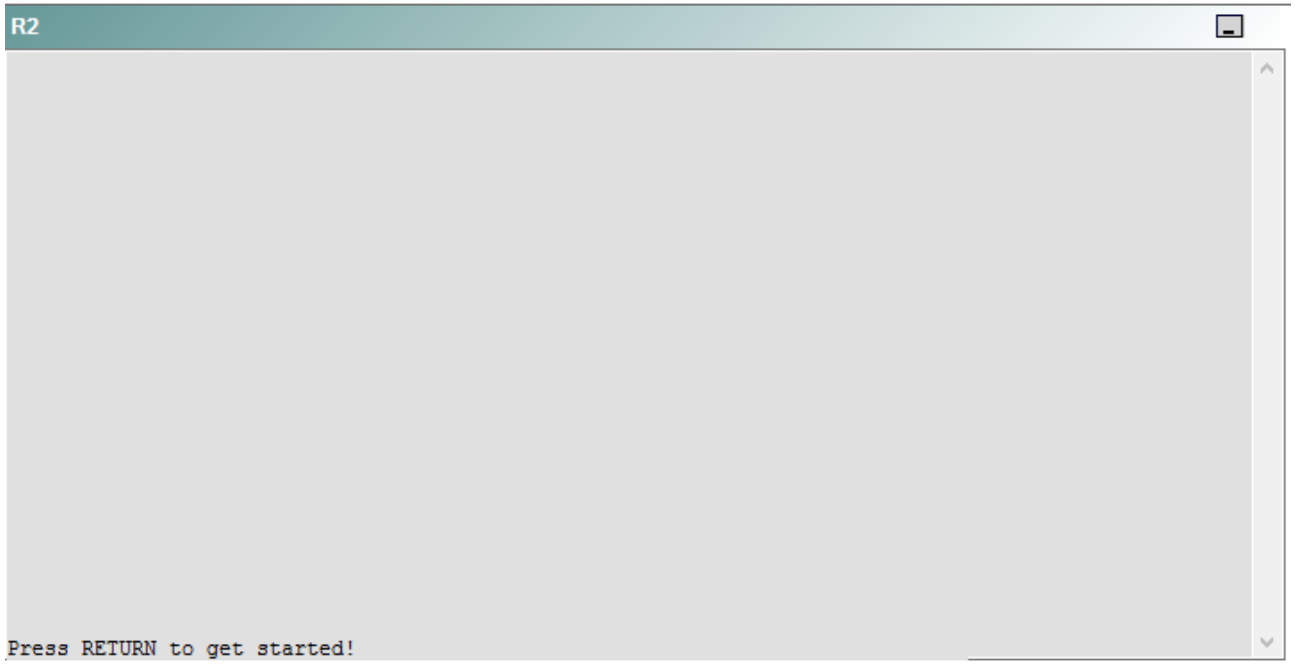



https://www.gratisexam.com/

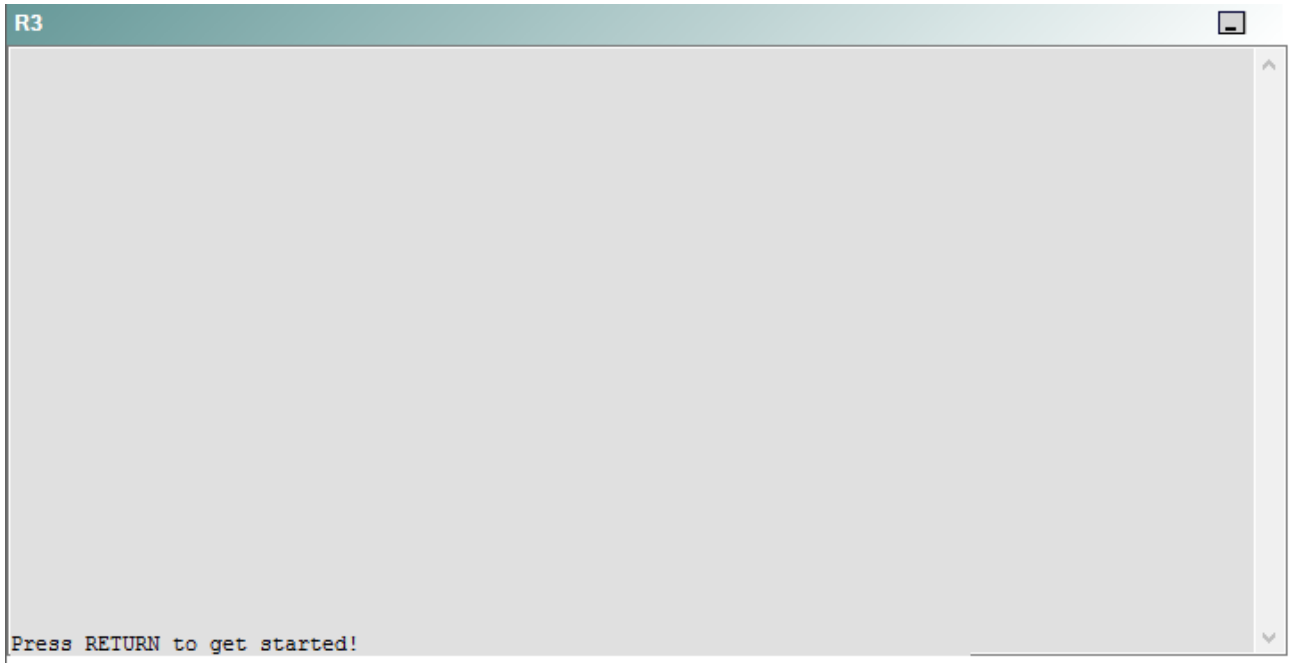
R1



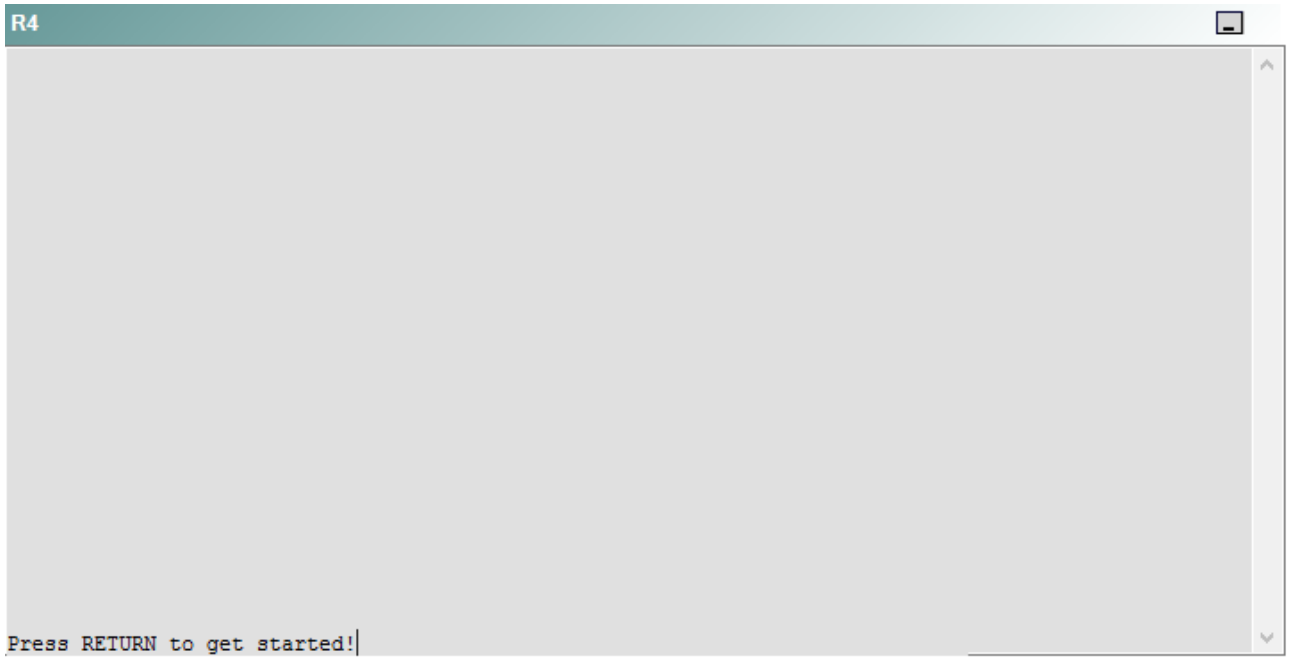

R2



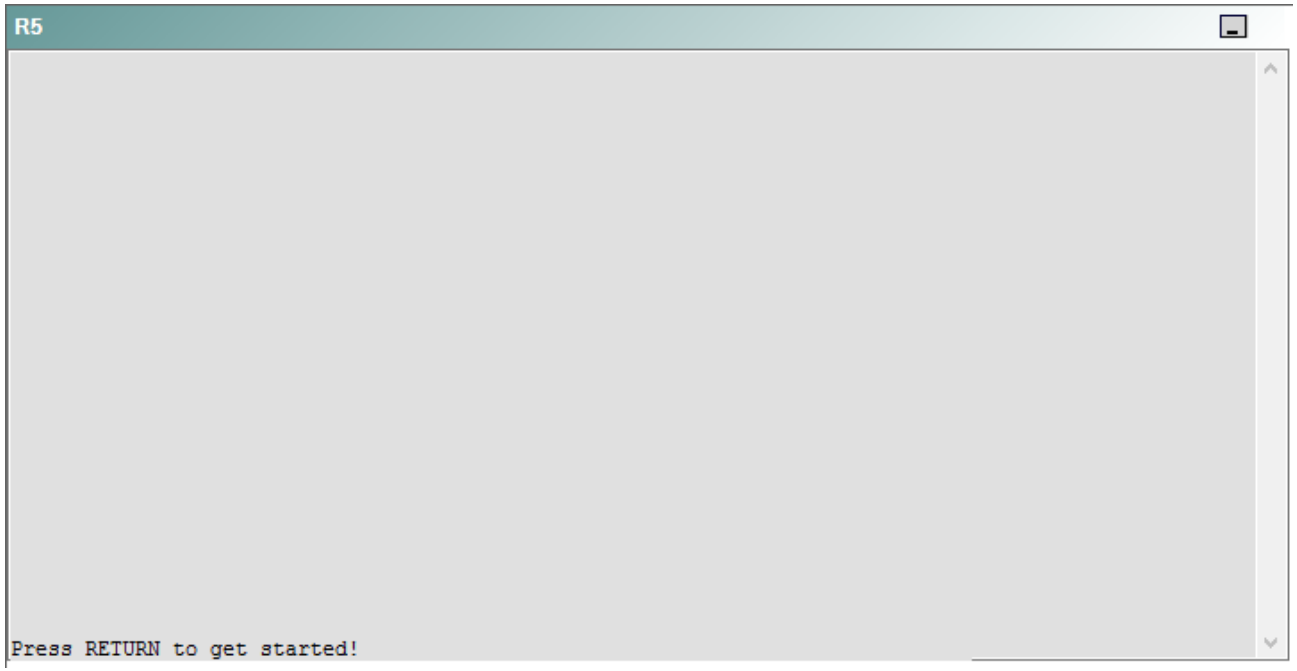

R3



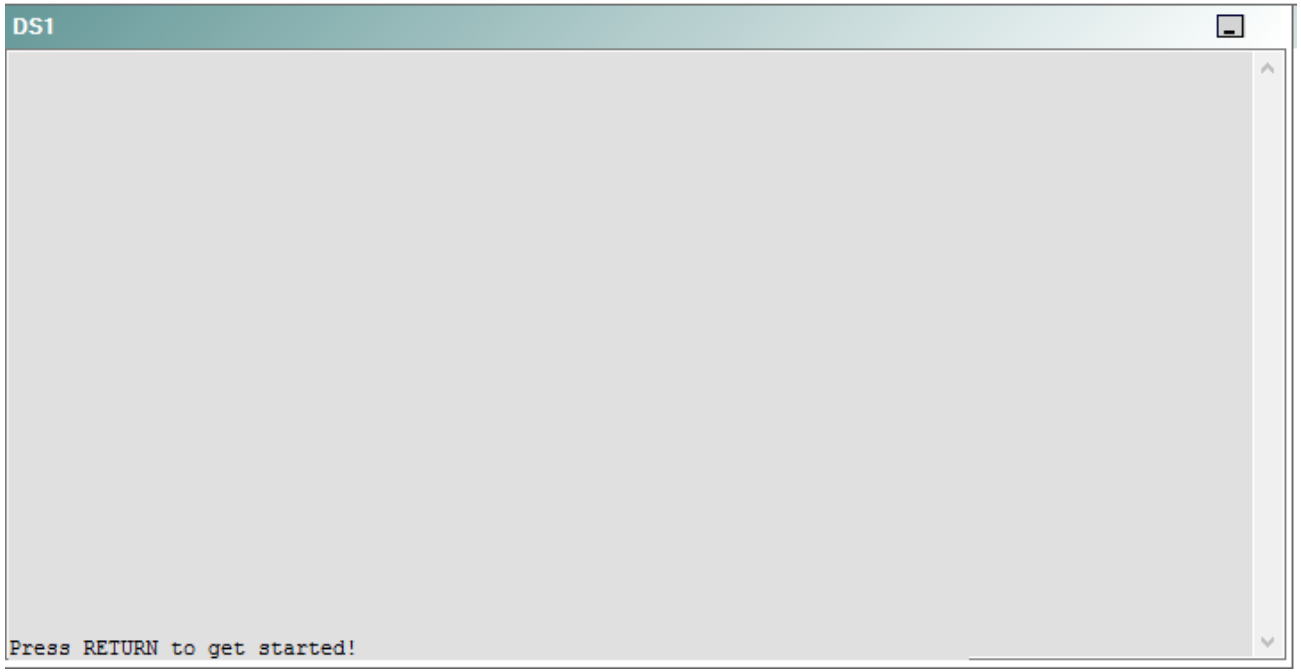

R4



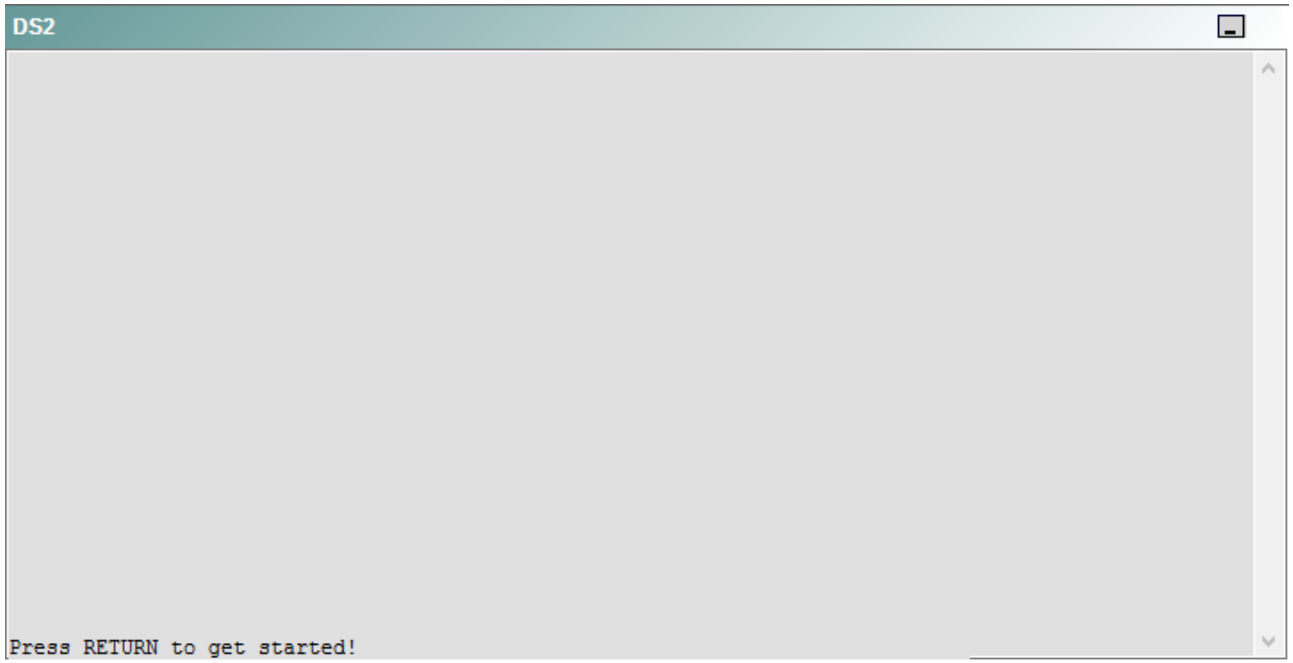

R5



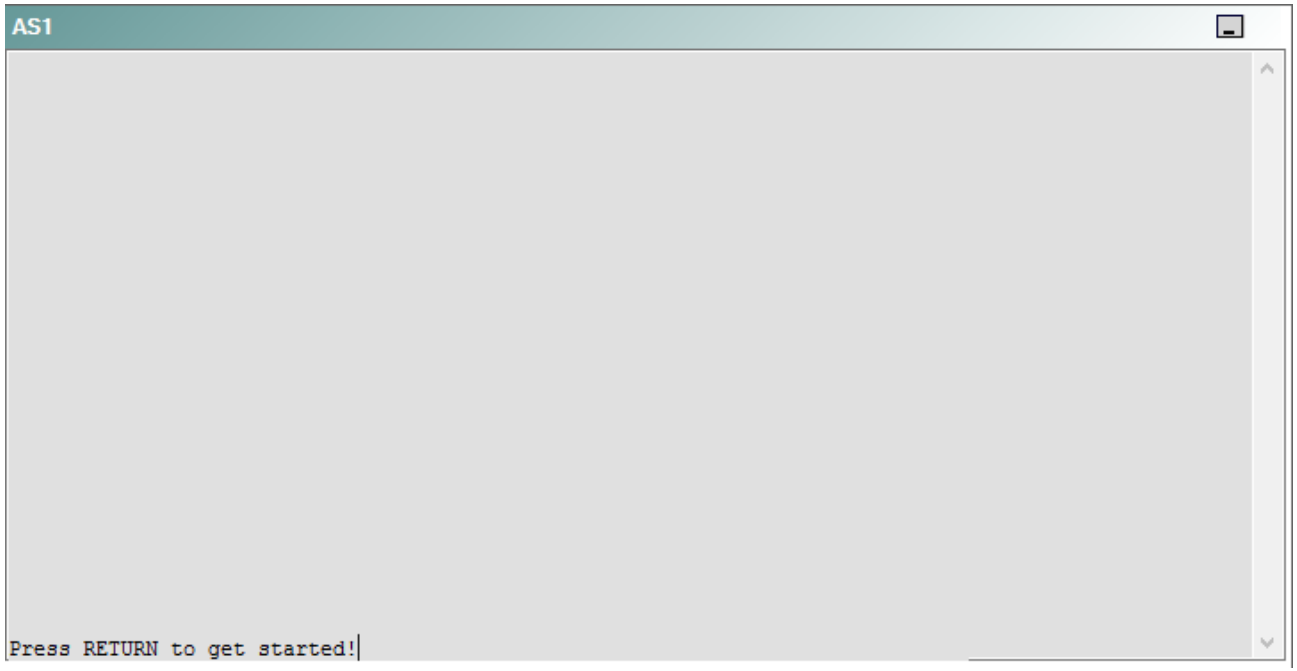

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that R5 is no longer able to ping the IPv6 address 2010::10:1 on R1.

Which of the following technologies is the source of the problem?

A. NTP
B. GRE
C. OSPFv2
D. OSPFv3
E. redistribution
F. DHCP
G. Layer 3 addressing
H. VLAN configuration
I. interface

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 24**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

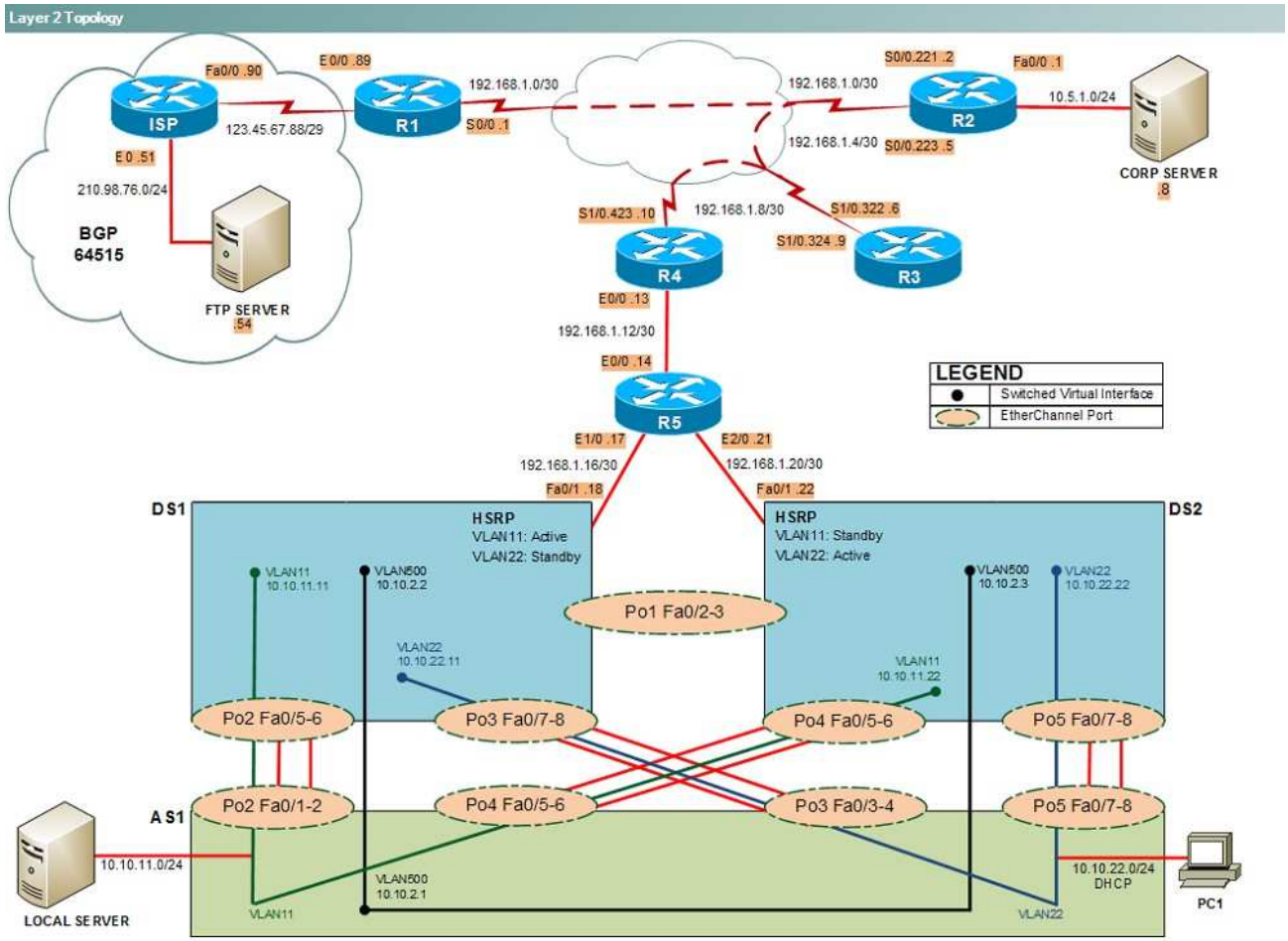
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

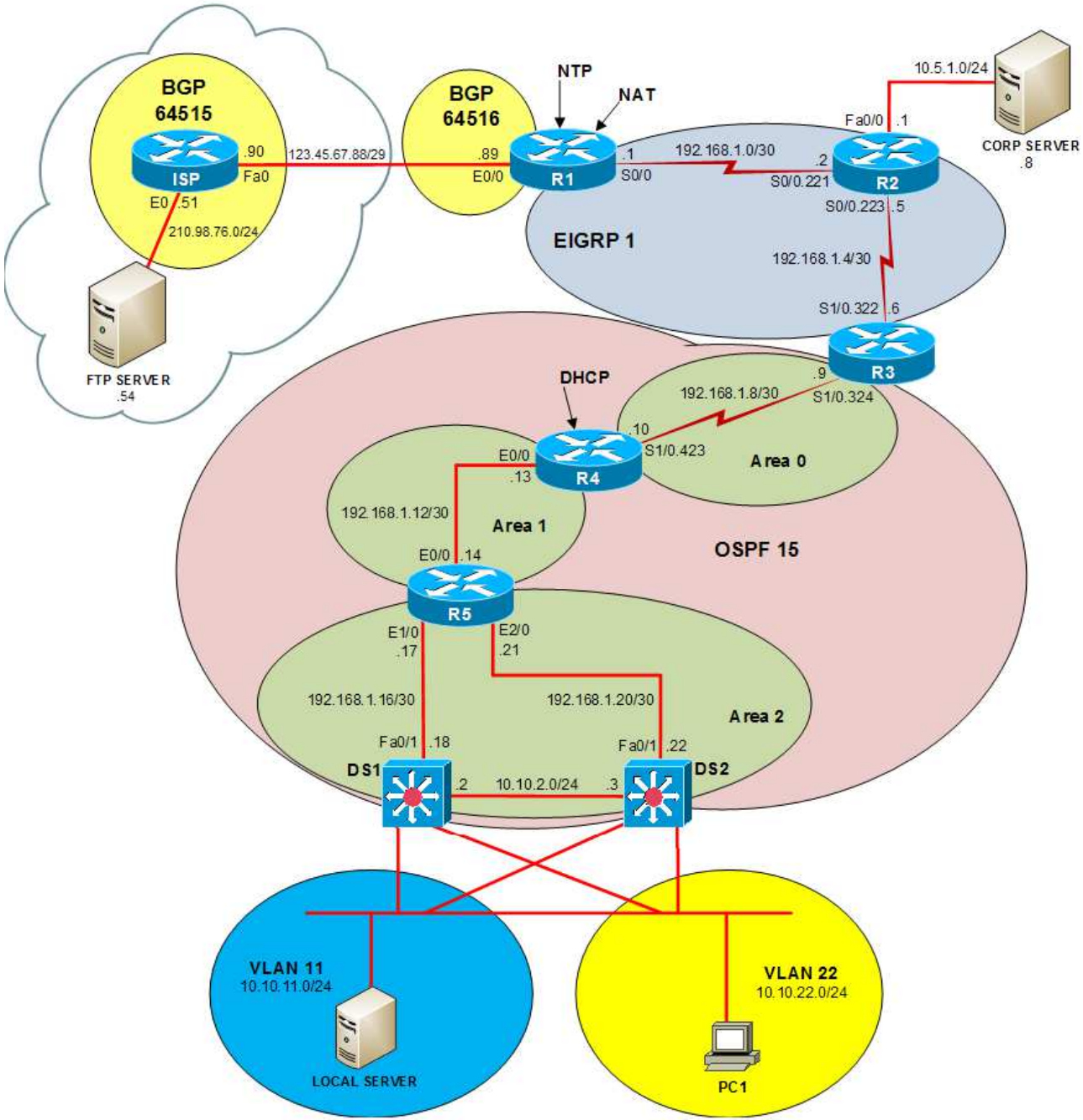
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

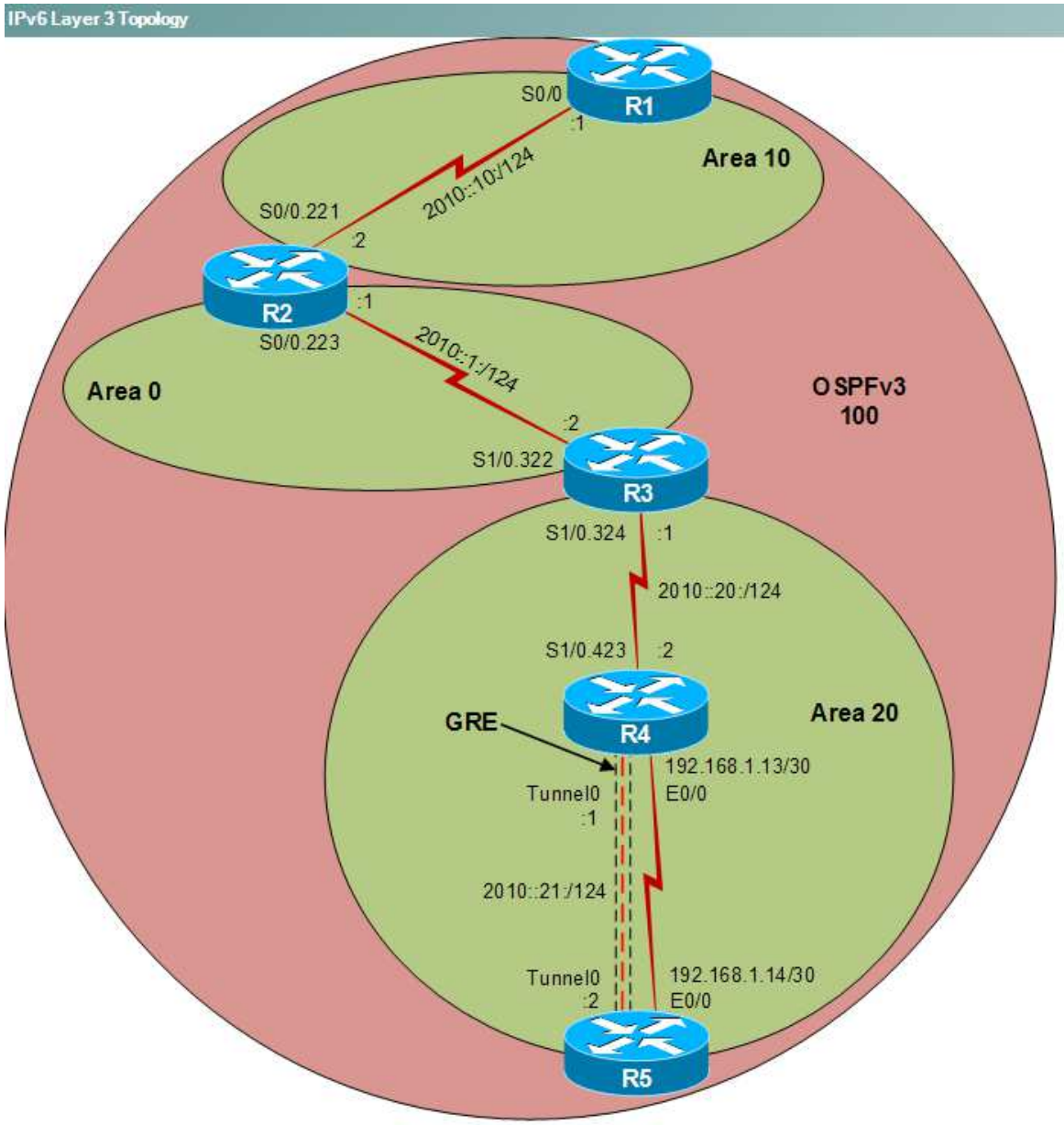
**Layer 2 Topology**




IPv4 layer 3 Topology

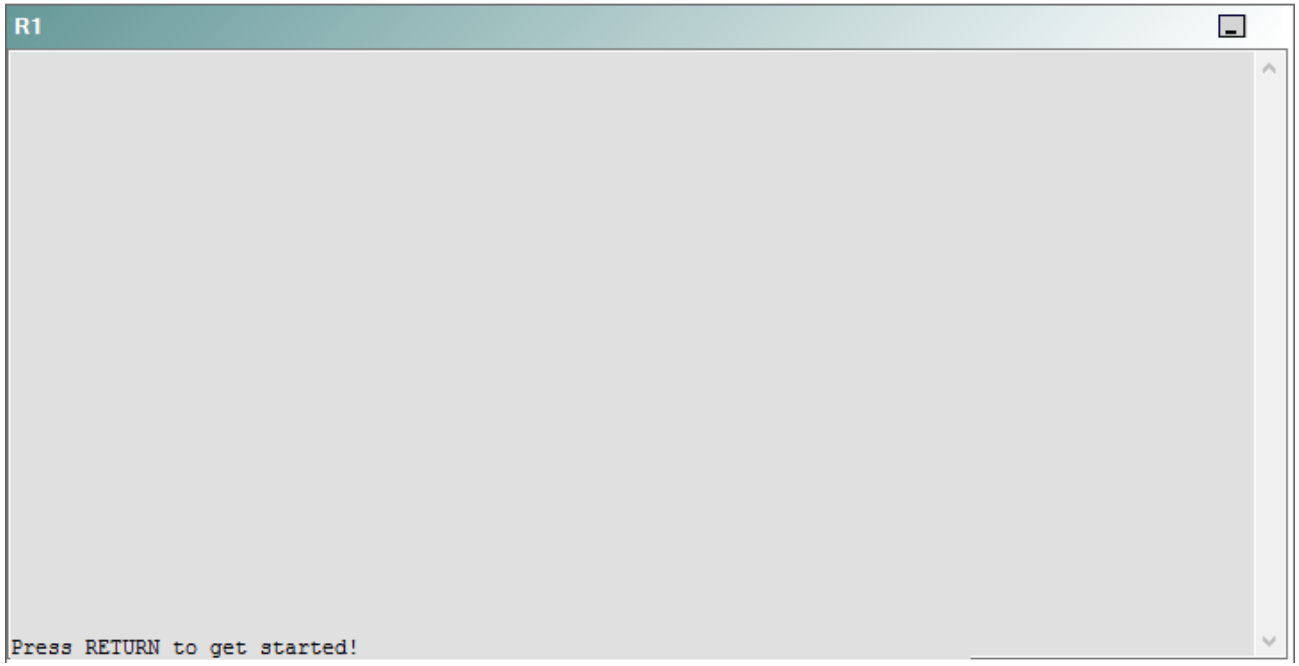

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

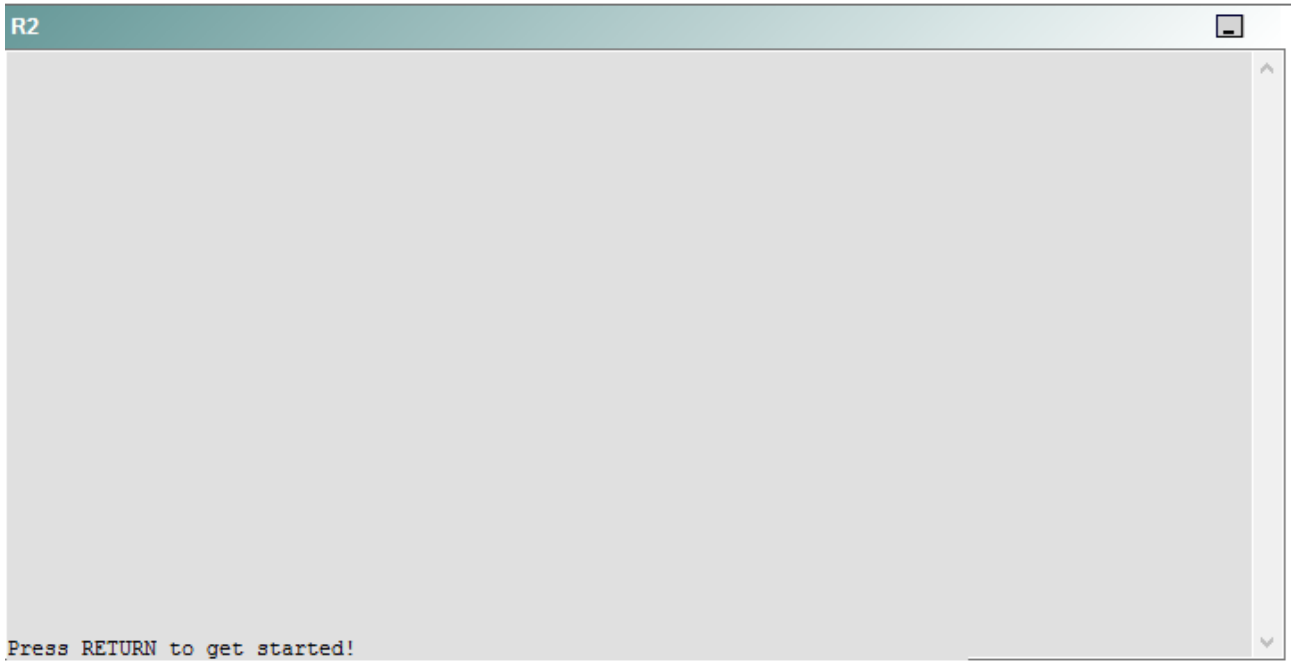



https://www.gratisexam.com/

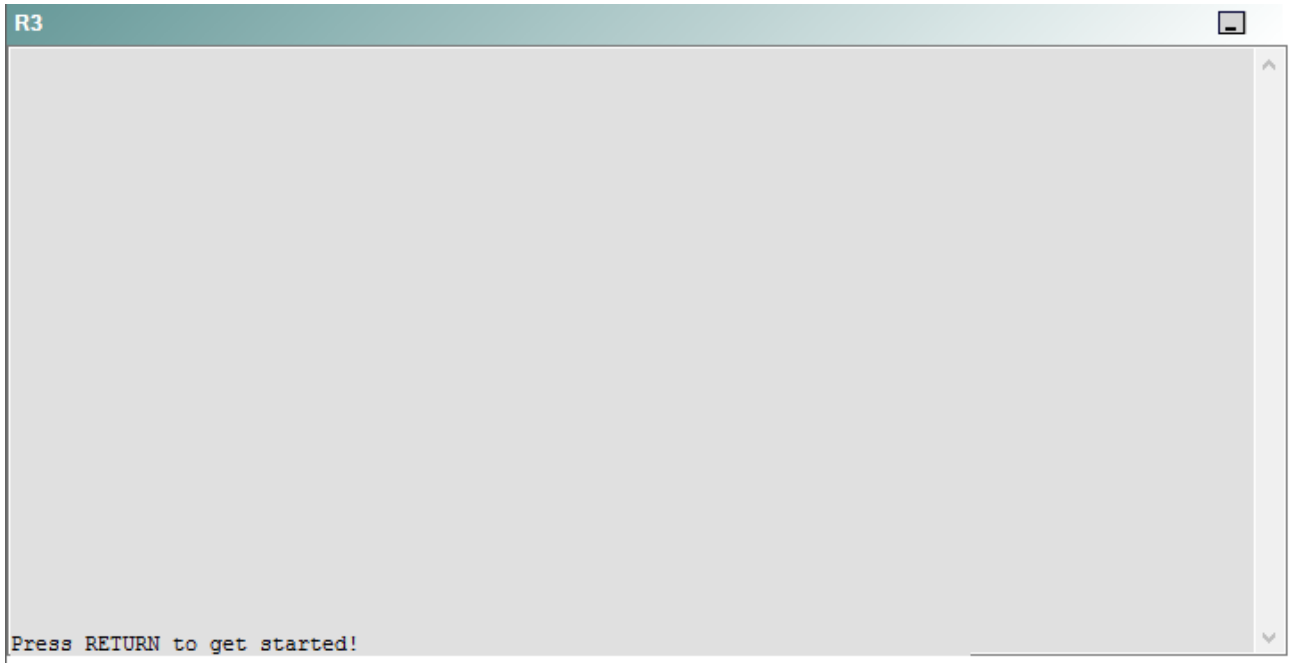
R1



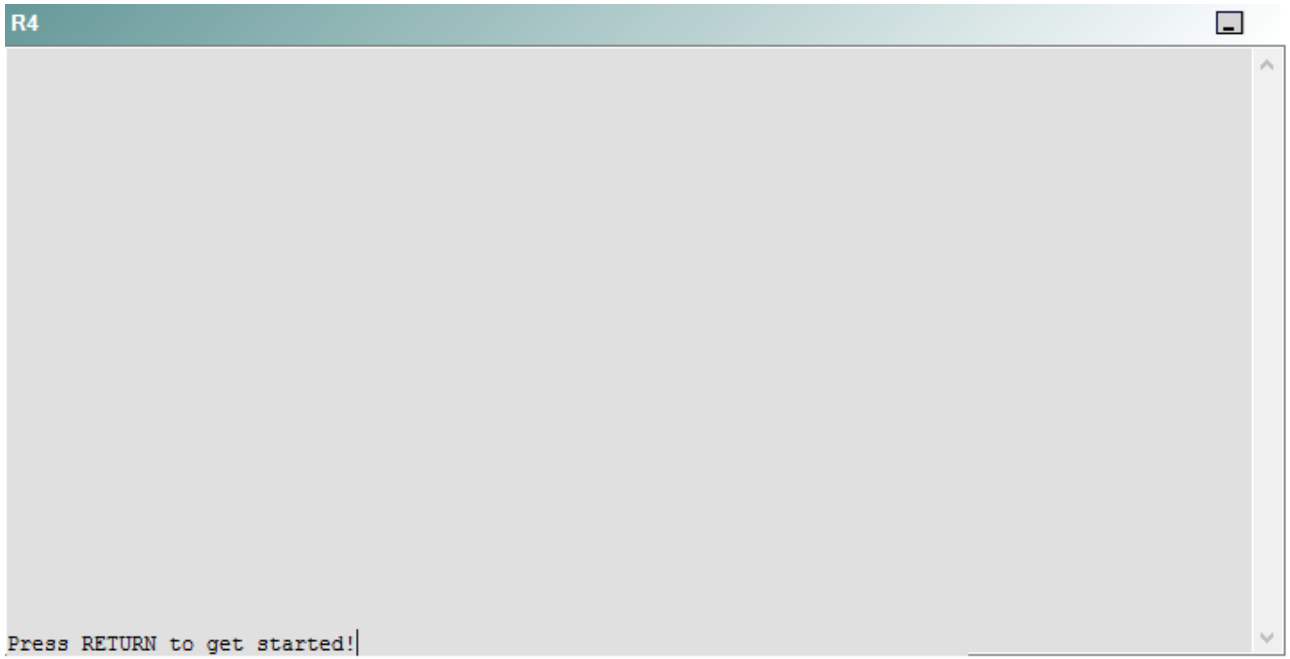

R2



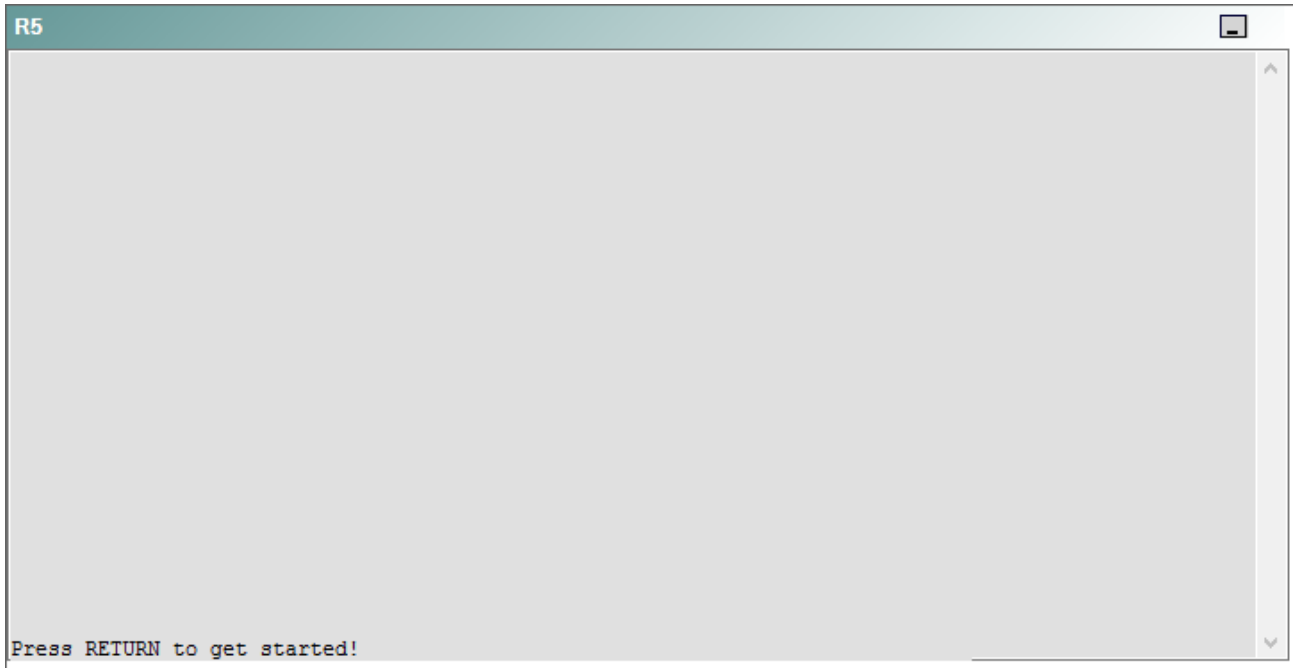

R3



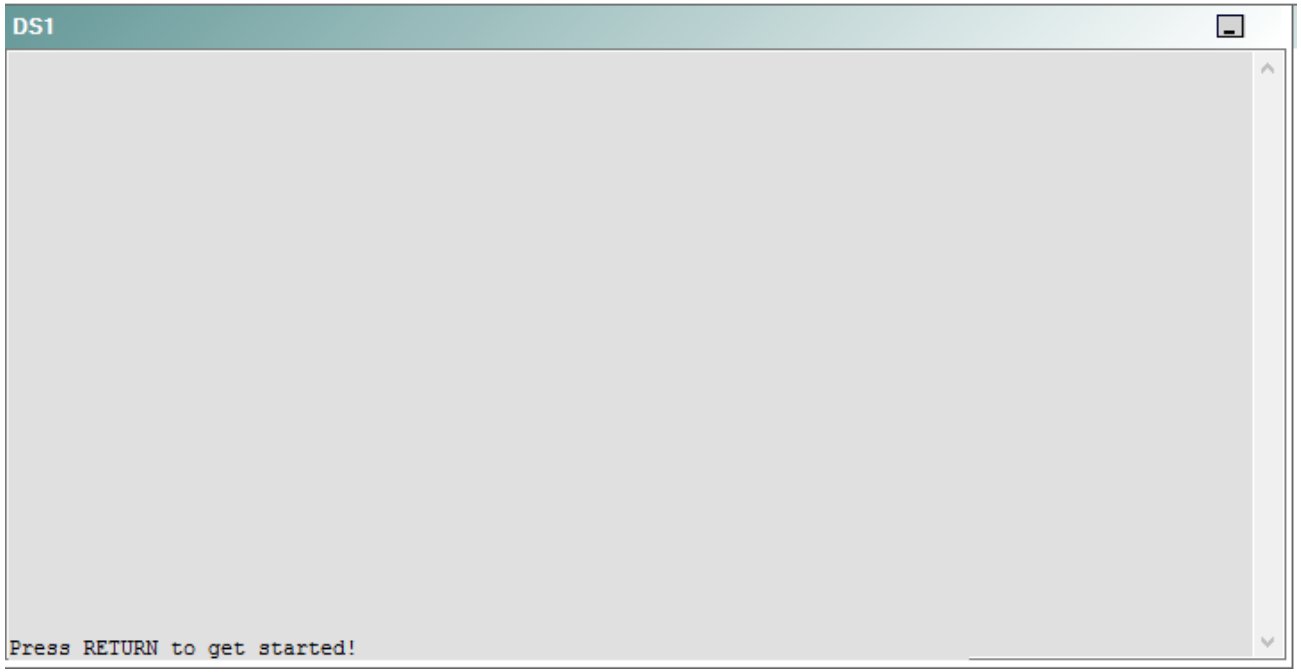

R4



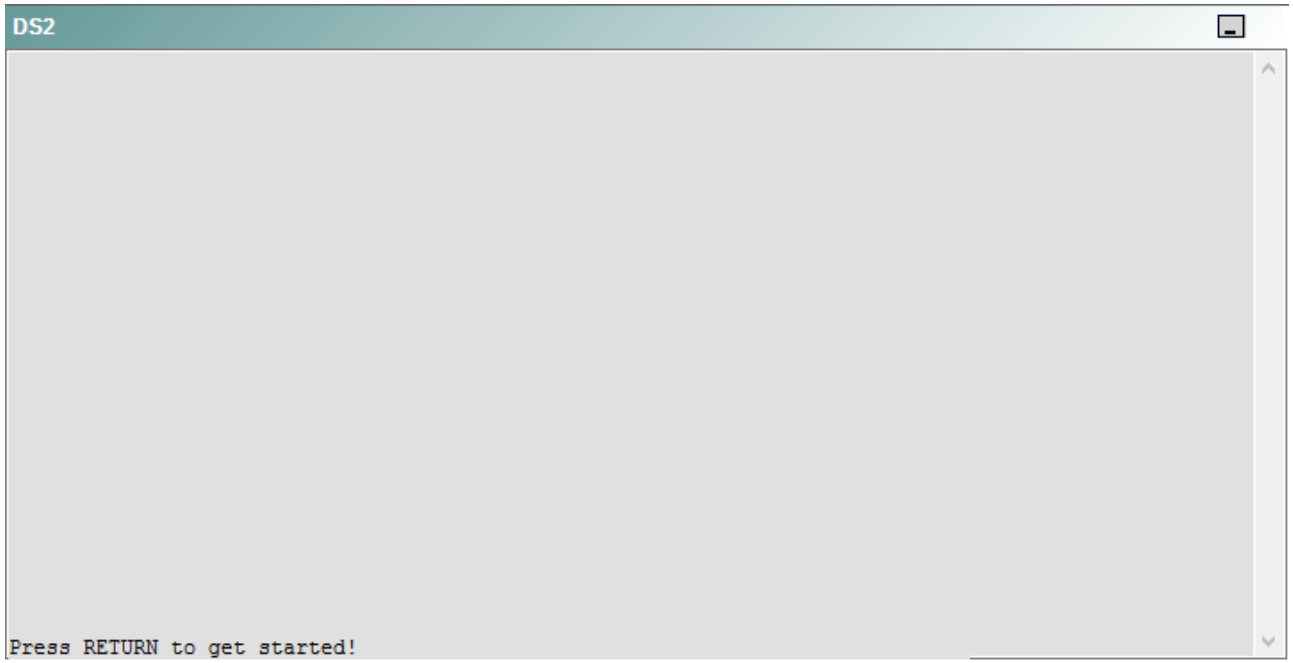

R5



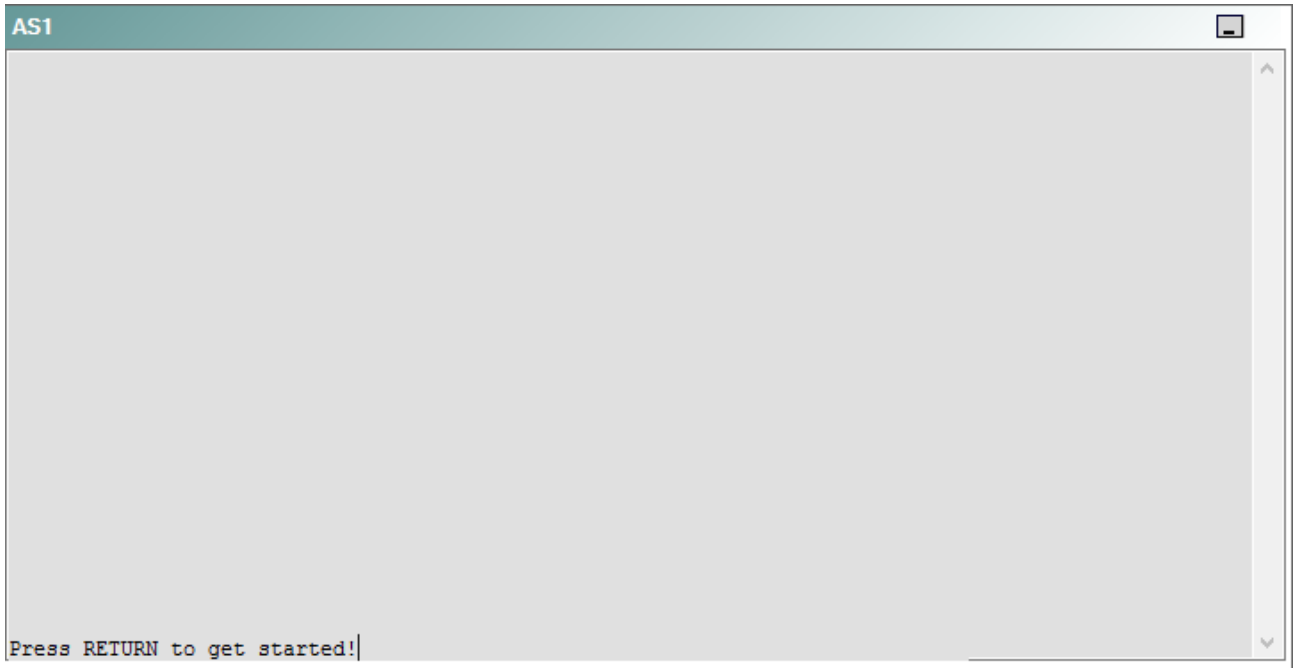

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that R5 is no longer able to ping the IPv6 address 2010::10:1 on R1.

Which of the following is most likely to solve the problem?

A. issuing the **tunnel mode gre ipv6** command on the Tunnel0 interface
B. issuing the **tunnel mode gre ip** command on the Tunnel0 interface
C. issuing the **ipv6 address 2010::21:1** command on the Tunnel0 interface
D. issuing the **ipv6 address 2010::21:2** command on the Tunnel0 interface
E. issuing the **tunnel source Ethernet0/0** command on the Tunnel 0 interface
F. issuing the **tunnel source Serial0/1** command on the Tunnel 0 interface
G. issuing the **tunnel destination 192.168.1.13** command on the Tunnel 0 interface
H. issuing the **tunnel destination 192.168.1.14** command on the Tunnel 0 interface

**Correct Answer:** B
**Section: (none)**

**Explanation**

**Explanation/Reference:**
Explanation:

You should issue the **tunnel mode gre ip** command on R5. To determine which device is the source of the problem, you should issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from R5 to the closest device and work your way up the network until communication is lost, or you can ping from R5 to the farthest device and work your way back to R5 until pings are successful. Alternatively, you can trace from R5 to R1 and see where communication is lost along the path to the destination device.

If you were to issue the **ping 2010::21:1** command on R5 in this scenario, you would receive the following output:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010::21:1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

The . . . . in the output indicates that the attempt to ping the IP version 6 (IPv6) address 2010::21:1 timed out. Internet Control Message Protocol (ICMP) packets from R5, which has been assigned the IPv6 address 2010::21:2, cannot reach 2010::21:1, which has been assigned to R4. However, if you were to issue the **ping 192.168.1.13** command on R5, you would receive the following output:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.13, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

The ! ! ! ! ! in the output above indicates that R5 is able to ping the Internet Protocol version 4 (IPv4) address 192.168.1.13, which has been assigned to the Ethernet0/0 interface on R4. The successful IPv4 ping indicates that the connectivity problem is limited to the IPv6 tunnel configured between R4 and R5. The tunnel0 interfaces on R4 and R5 form a Generic Routing Encapsulation (GRE) overlay tunnel between the two routers. An overlay tunnel encapsulates IPv6 traffic into IPv4 traffic and can be used as an intermediate migration tool from IPv4-based networks to IPv6-based networks.

Once you have determined where connectivity is lost, you can begin to troubleshoot the cause of the problem. If you were to issue the **show interface Tunnel0** command on R4, the output would reveal that the interface is up and the line protocol is up on the Tunnel 0 interface. However, issuing the **show interface Tunnel0** command on R5 reveals that the interface is up and that the line protocol is down, as shown in the following partial output from R5.

```
Tunnel0 is up, line protocol is down
  IPv6 is enabled, link-local address is FE80::CE05:4FF:FE28:0 [TEN]
  Global unicast address(es):
    2010::21:2, subnet is 2010::21:0/124 [TEN]
```

Therefore, the problem most likely exists at the Data Link layer of the Open Systems Interconnection (OSI) model on the Tunnel0 interface on R5. If you were to issue the **show running-config** command on R4 and R5, you would receive the following partial output:

```
R4#show running-config
...
interface Tunnel0
 no ip address
 ipv6 address 2010::21:1/124
 ipv6 ospf 100 area 20
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.14
!

R5#show running-config
...
interface Tunnel0
 no ip address
 ipv6 address 2010::21:2/124
 ipv6 ospf 100 area 20
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.13
 tunnel mode gre ipv6
!
```

The output above indicates that interface Tunnel0 on R5 is configured with a correct tunnel of Ethernet0/0 and a correct tunnel destination of 192.168.1.13. Ethernet0/0 is the internet on R5 that is directly connected to R4, which is the remote end of the GRE overlay tunnel. Likewise, the tunnel source on R4 is configured to use the Ethernet0/0 interface on R4 and the tunnel destination on R4 is configured as the IPv4 address assigned to the Ethernet0/0 on R5. However, the **tunnel mode gre ipv6** command on the output above indicates that the R5 side of the GRE tunnel is configured as a GRE IPv6 tunnel rather than an overlay tunnel. A GRE IPv6 tunnel transports IPv6 and IPv4 packets. Conversely, R4 is configured with the default GRE overlay tunnel configuration. If you were to issue the **tunnel mode gre ip** command or the **no tunnel mode gre ipv6** command on R5, the Tunnel0 interface on R5 would return to the default GRE overlay tunnel configuration, as shown in the following partial output:

```
R5#show running-config
...
interface Tunnel0
 no ip address
 ipv6 address 2010::21:2/124
 ipv6 ospf 100 area 20
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.13
!
```

You should not issue the **tunnel mode gre ipv6** command on the Tunnel0 interface on R4 or R5. You would issue the **tunnel mode gre ipv6** command on the Tunnel0 interface of R4 and R5 to encapsulate IPv4 traffic over an IPv6 network. In this scenario, the GRE tunnel between R4 and R5 is an IPv6 overlay tunnel, which encapsulates IPv6 traffic over an IPv4 network. If you were to issue **the tunnel mode gre ipv6** command on the Tunnel0 interface on R5 so that it matches the encapsulation mode on R4, the tunnel source addresses would be incorrectly configured.

You need not issue the **tunnel source Ethernet0/0** command on the Tunnel0 interface on R4 or R5. The **tunnel source Ethernet0/0** command configures the virtual Tunnel0 interface to use the physical Ethernet0/0 interface as the outgoing interface for the GRE tunnel. In this scenario, the Tunnel0 interface on R4 and the Tunnel0 interface on R5 are correctly configured with Ethernet0/0 as the tunnel source.

You should not issue the **tunnel source Serial0/1** command on the Tunnel0 interface on either R4 or R5, because the Ethernet0/0 interface on each device is the direct physical connection between R4 and R5. If you were to issue the **tunnel source Serial0/1** command in this scenario, the line protocol on the Tunnel0 interface would transition to the down state because the router would be attempting to send tunnel traffic out of the wrong physical interface, as shown in the following partial output from the **show interfaces Tunnel0** command:

```
Tunnel0 is up, line protocol is down
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 0.0.0.0 (Serial0/1), destination 192.168.1.13
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
```

You need not issue the **ipv6 address 2010::21:1** command or the **ipv6 address 2010::21:2** command on the tunnel0 interface on R4 or R5. If you were to issue the **show ipv6 interface Tunnel0** command on R4 and R5 in this scenario, the output would reveal that the Tunnel0 interface on R4 has already been assigned the IPv6 address 2010::21:1 and that the Tunnel0 interface on R5 has already been assigned the IPv6 address 2010::21:2, as shown in the following partial output:

```
R4#show ipv6 interface Tunnel 0
Tunnel0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::CE0B:8FF:FE84:0 [TEN]
  Global unicast address(es):
    2010::21:1, subnet is 2010::21:0/124 [TEN]

R5#show ipv6 interface Tunnel 0
Tunnel0 is up, line protocol is down
  IPv6 is enabled, link-local address is FE80::CE0C:8FF:FE84:0
  Global unicast address(es):
    2010::21:2, subnet is 2010::21:0/124
```

You should not issue the **tunnel destination 192.168.1.13** command or the **tunnel destination 192.168.1.14** command on either R4 or R5, because the destination for each Tunnel0 interface is already configured correctly. The tunnel destination for the Tunnel0 interface on R4 should be configured to the IPv4 address of the Ethernet0/0 interface on R5 because 192.168.1.14 is the IPv4 address of the device to which the Ethernet0/0 interface on R4 is connected. The tunnel destination for the Tunnel0 interface on R5 should be configured to the IPv4 address of the Ethernet0/0 interface on R4 because 192.168.1.13 is the IPv4 address of the device to which the Ethernet0/0 interface on R5 is connected.

**QUESTION 25**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s

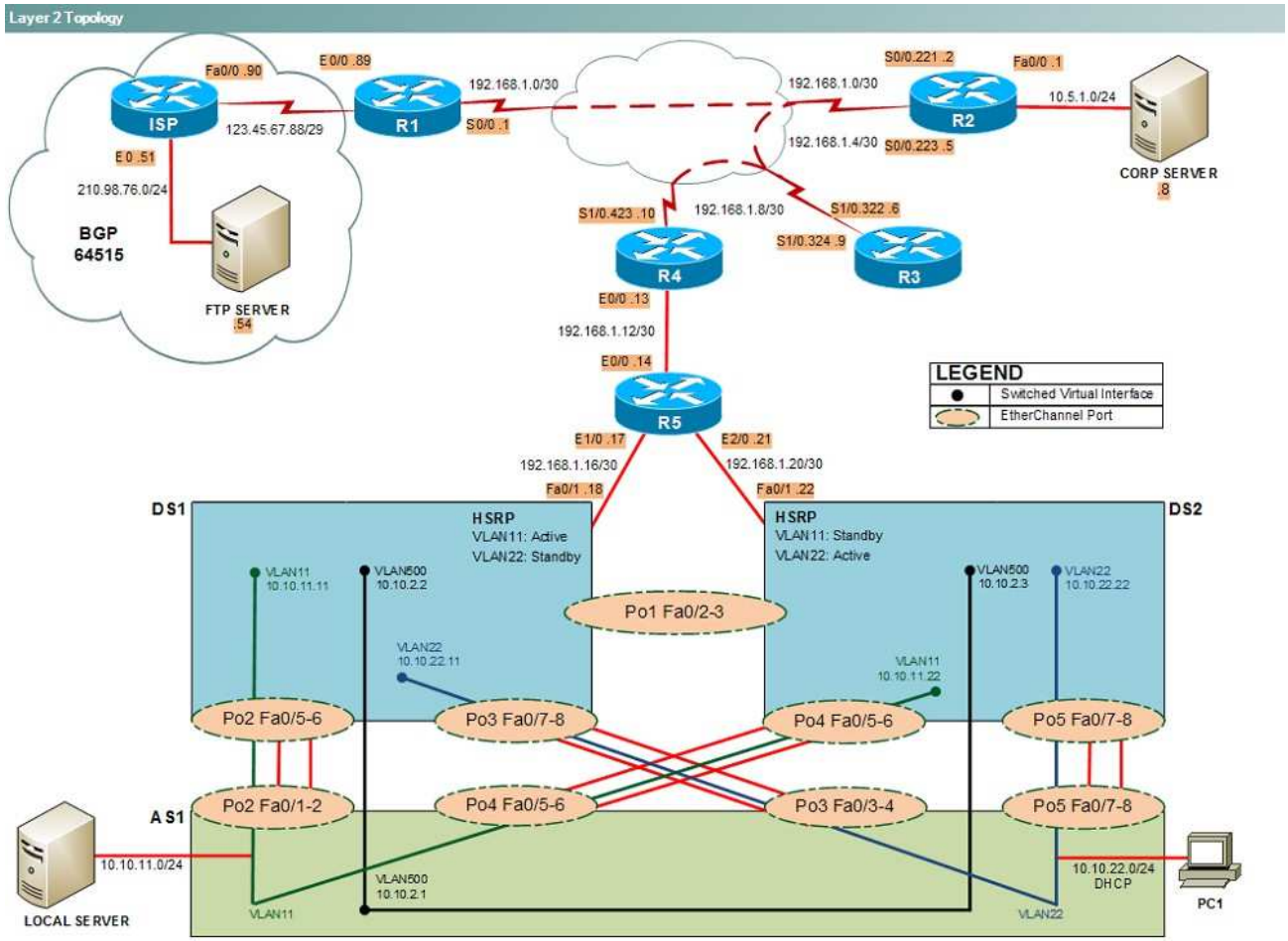
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

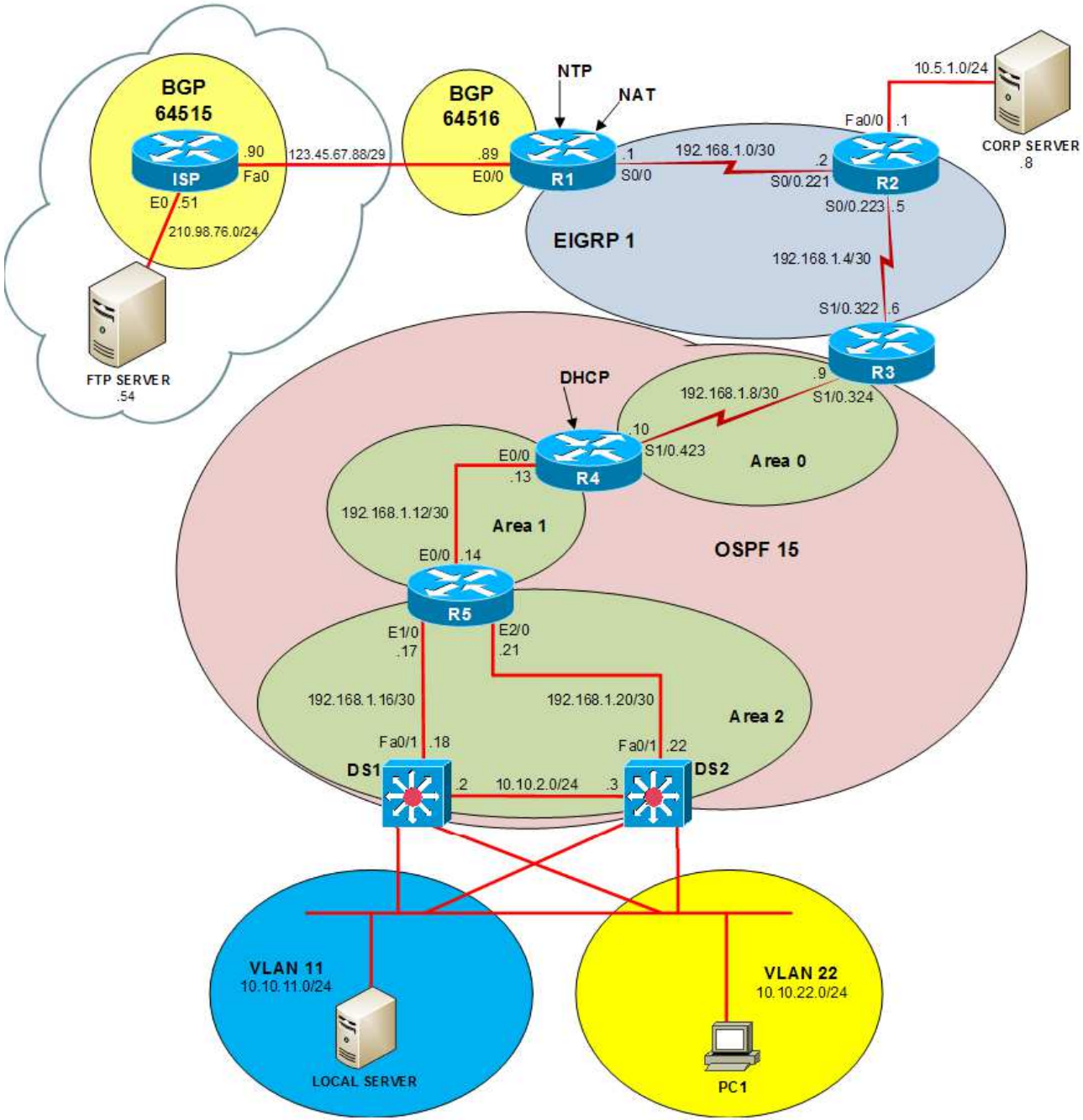
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

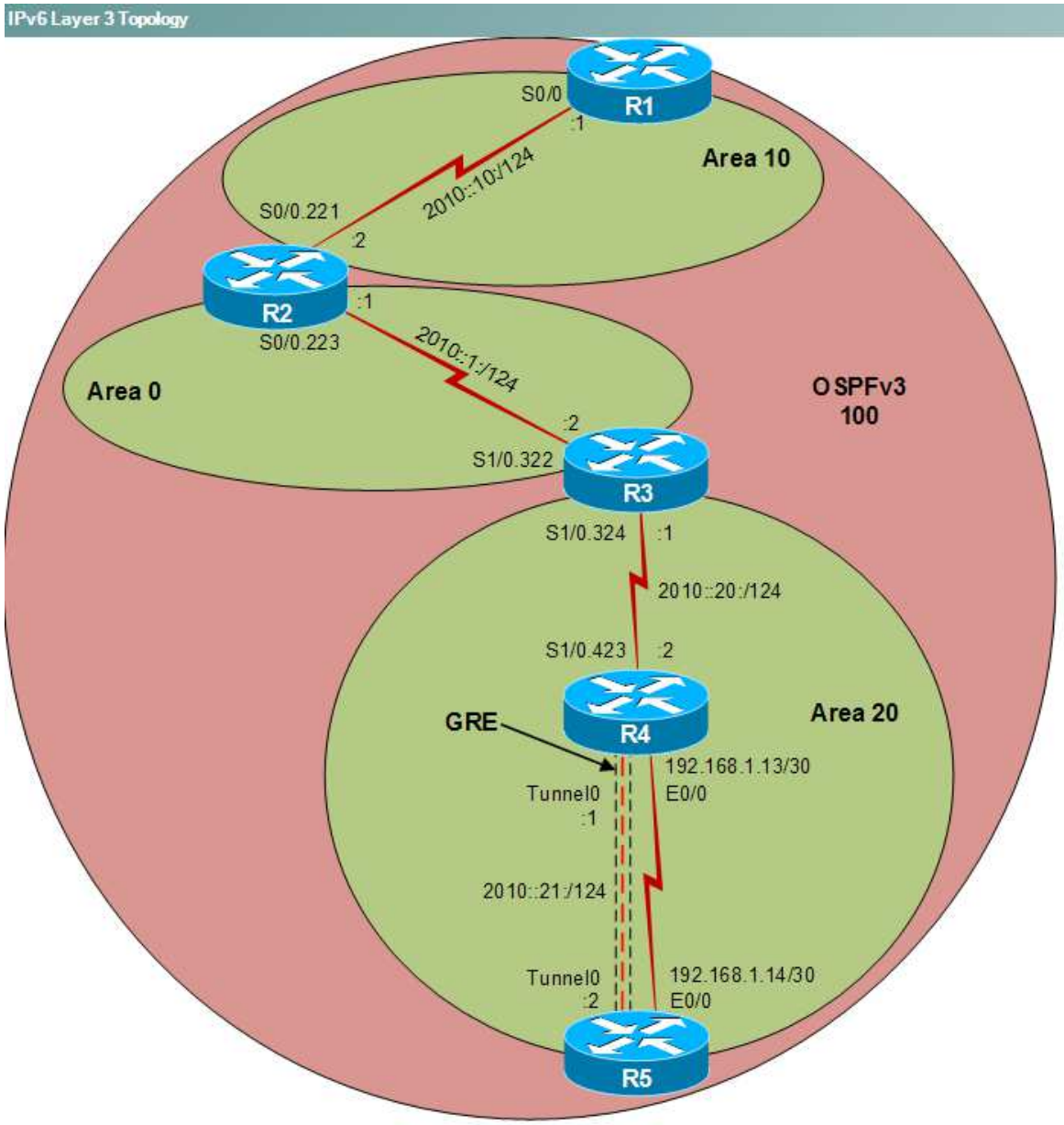
**Layer 2 Topology**




IPv4 layer 3 Topology

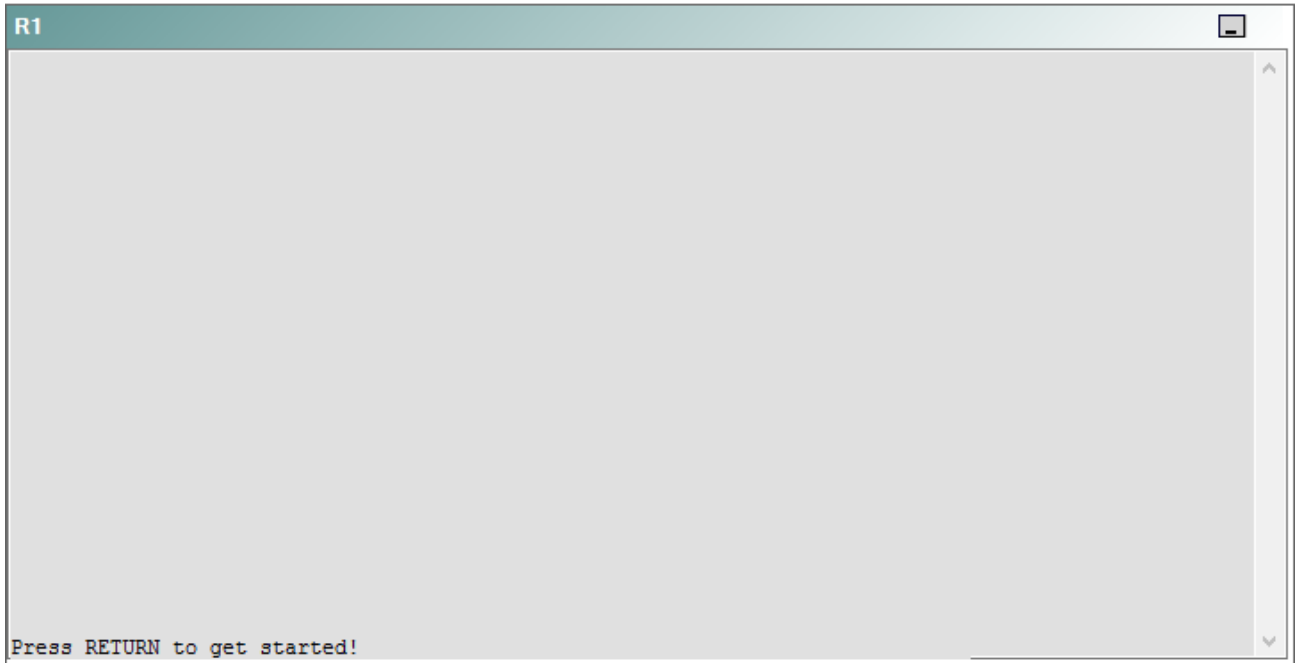

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

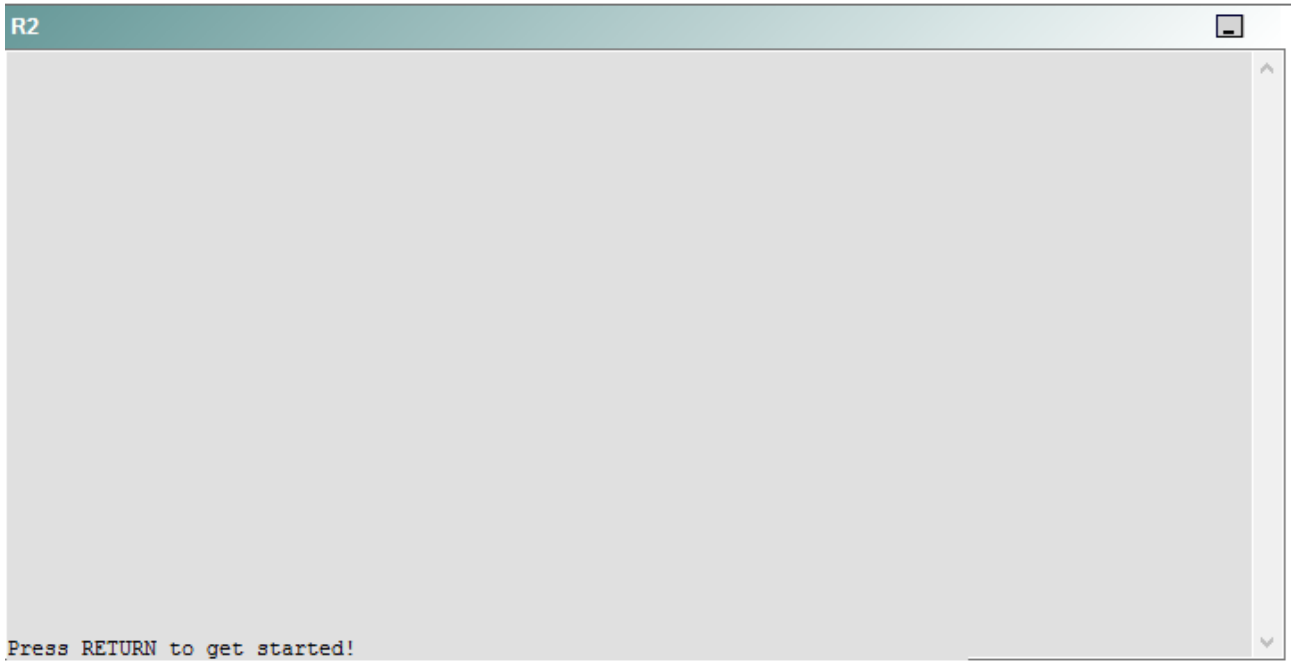



https://www.gratisexam.com/

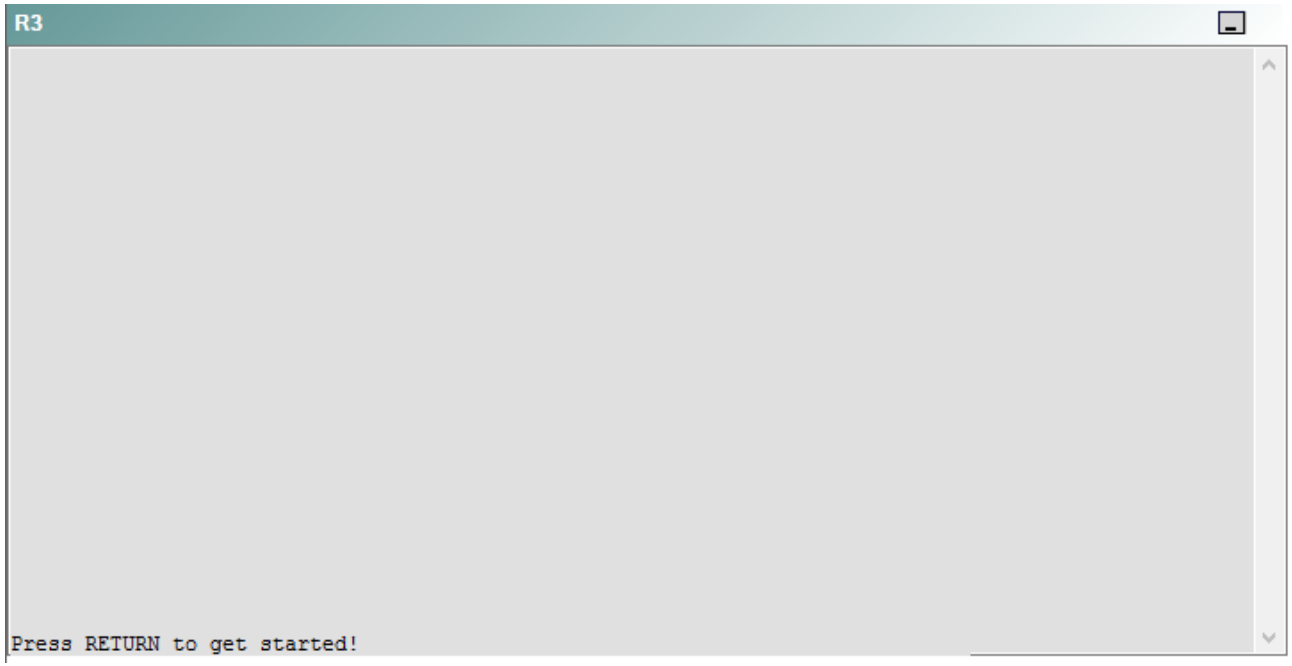
R1



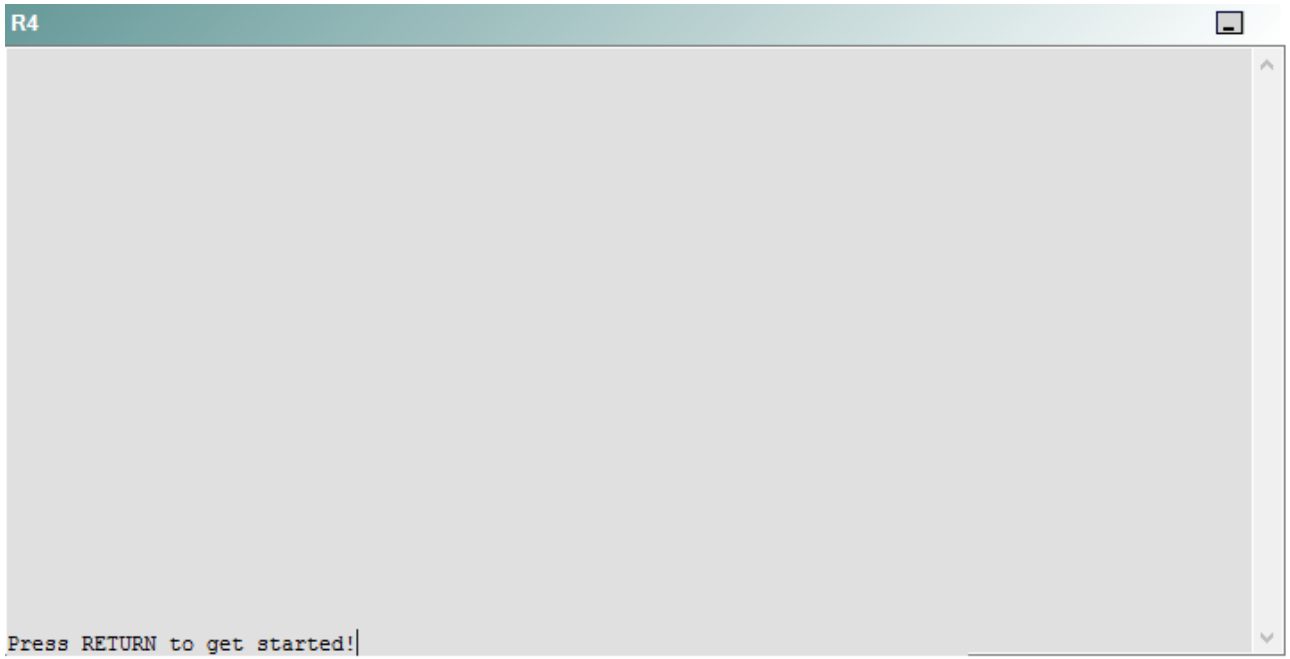

R2



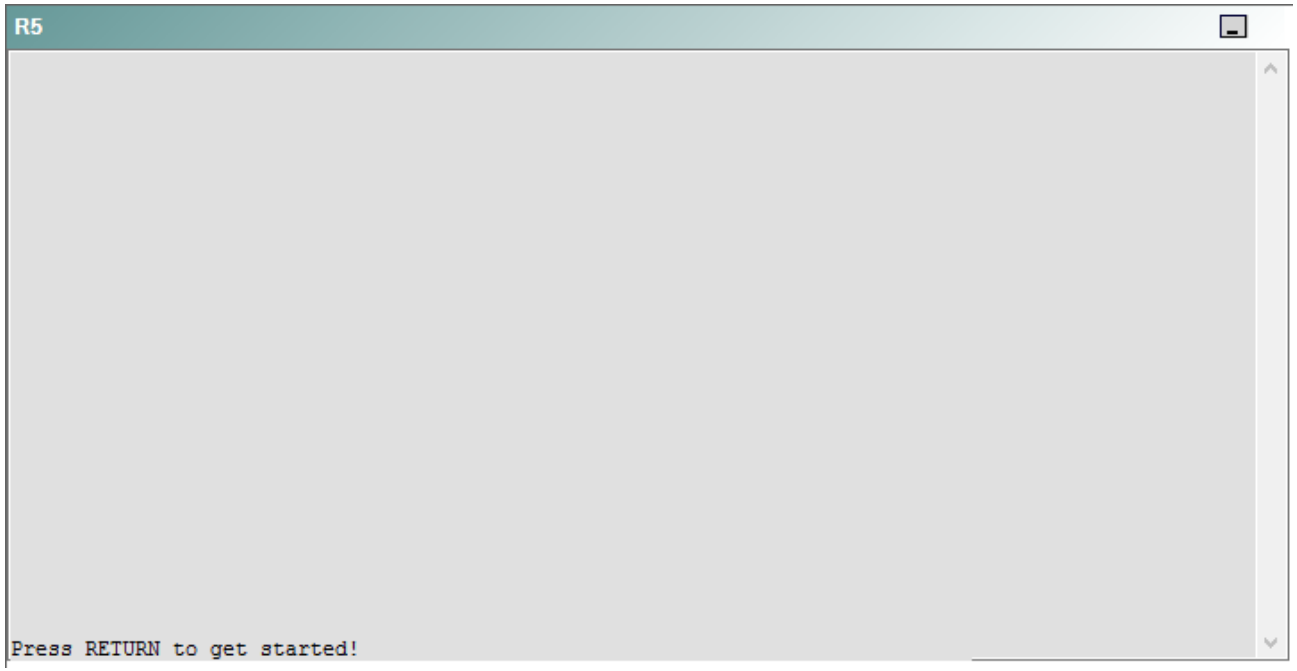

R3



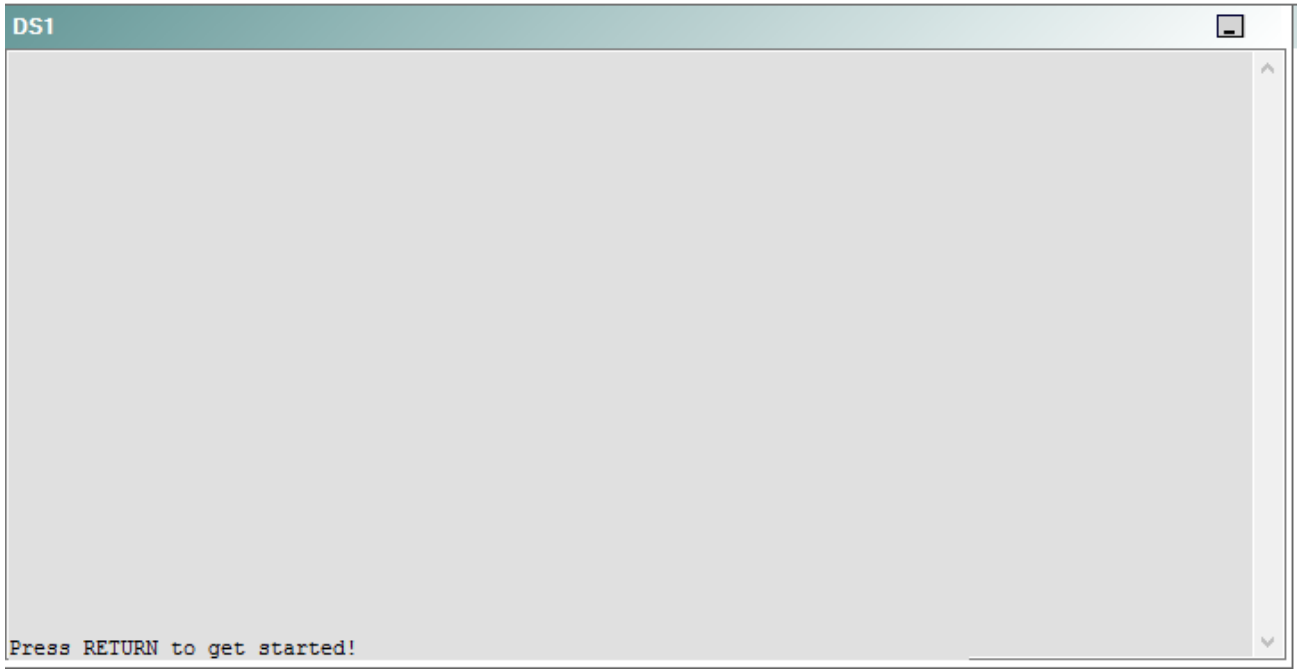

R4



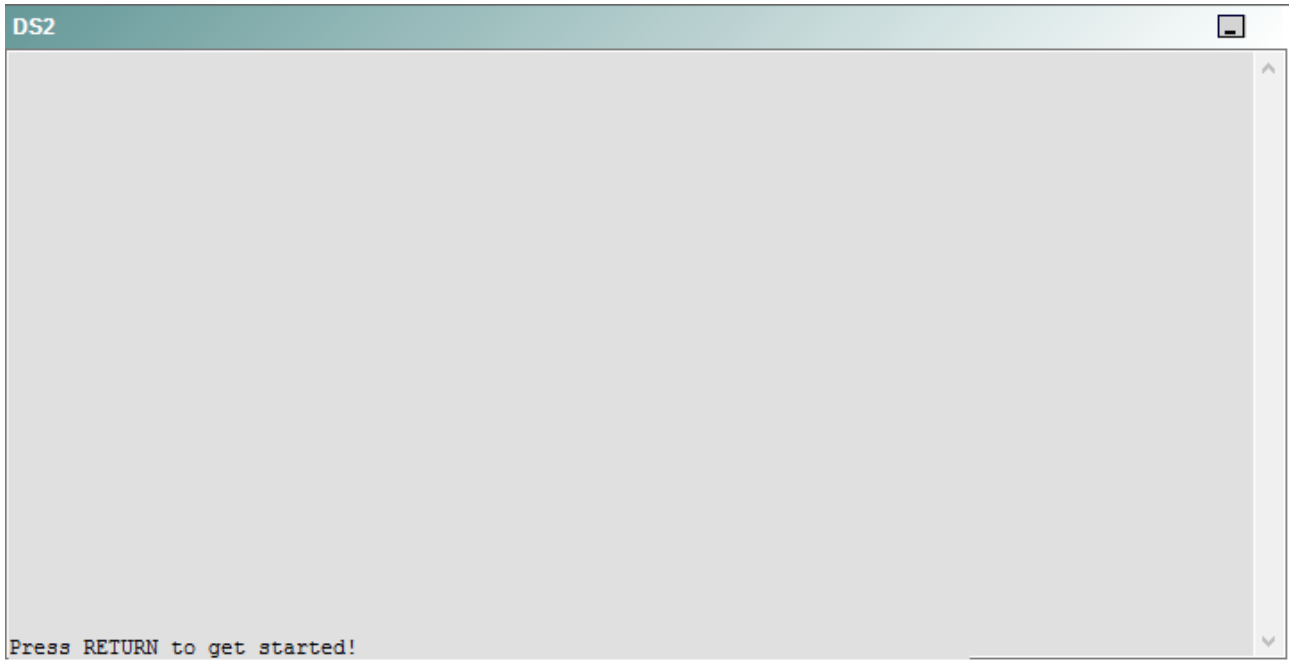

R5



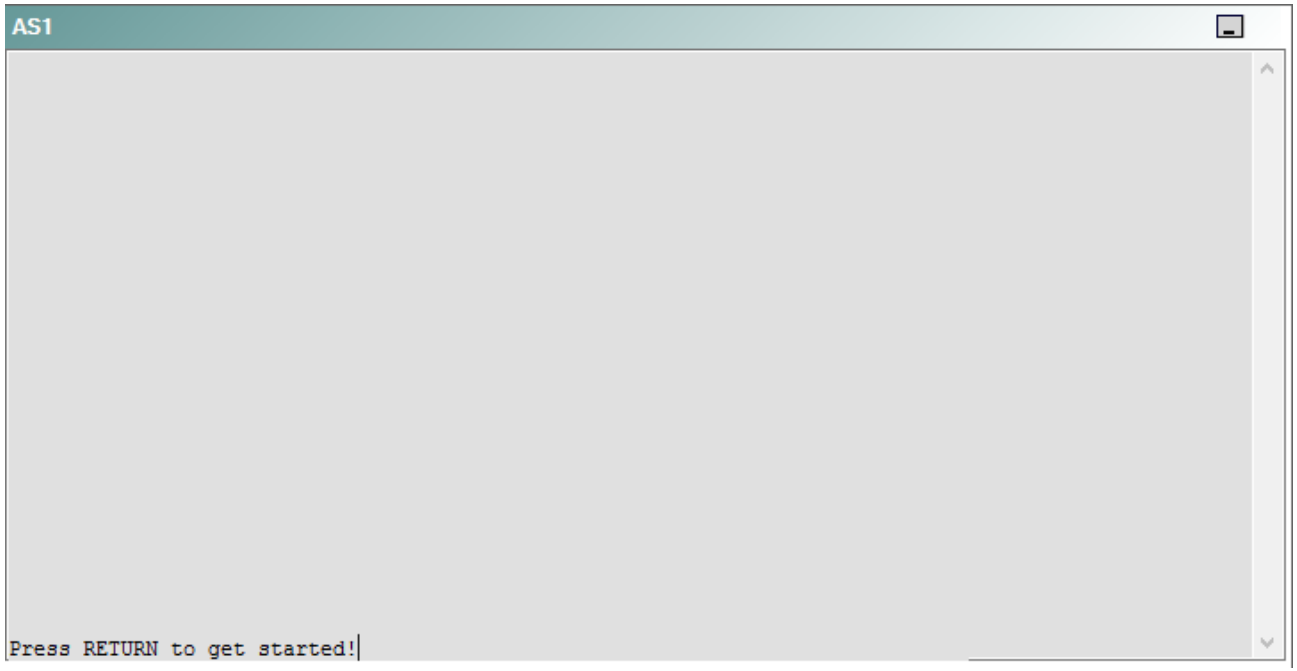

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. DHCP
C. Layer 3 addressing
D. Layer 3 security
E. Layer 2 security
F. OSPFv2
G. OSPFv3
H. interface

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 26**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

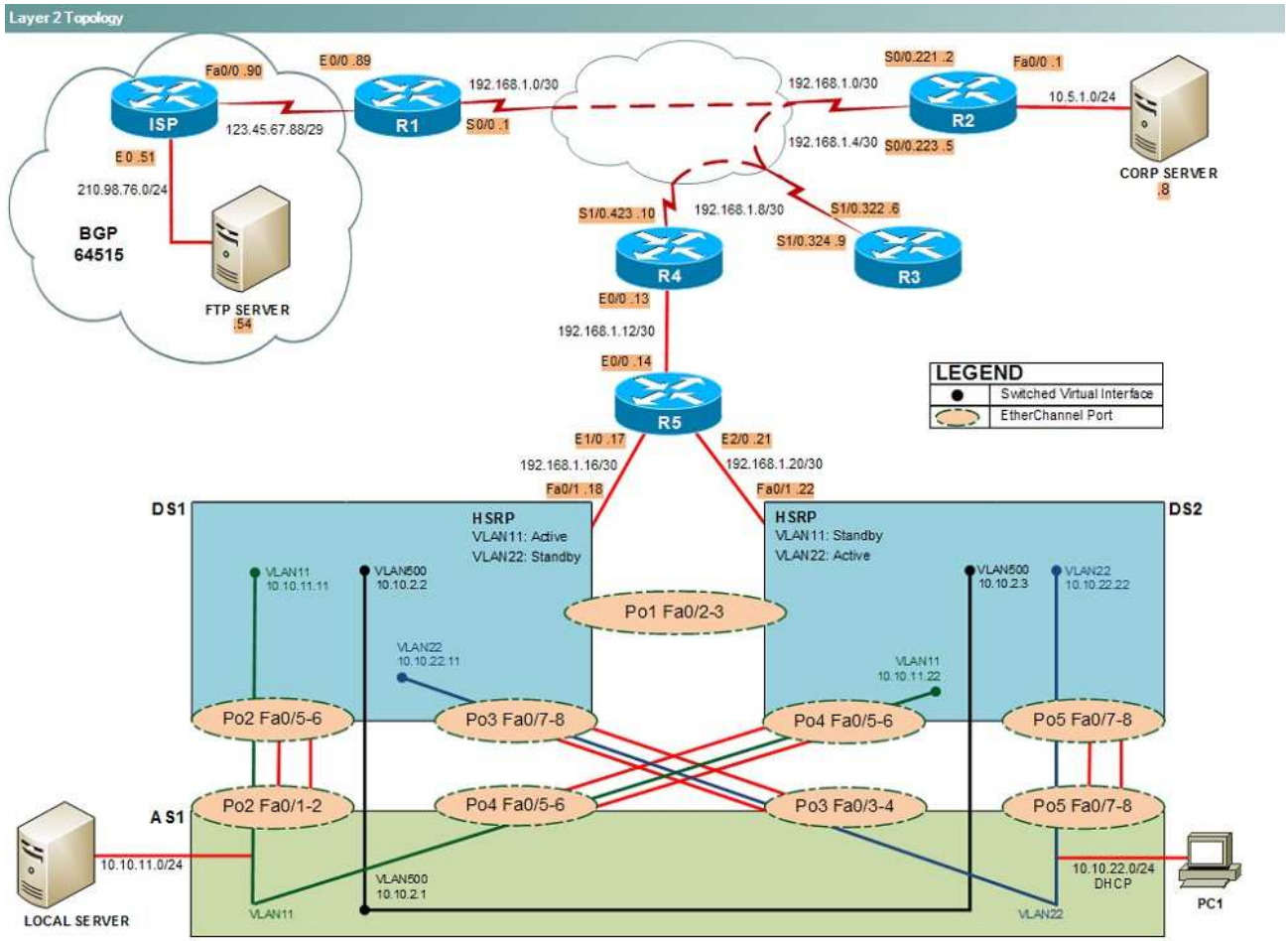
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

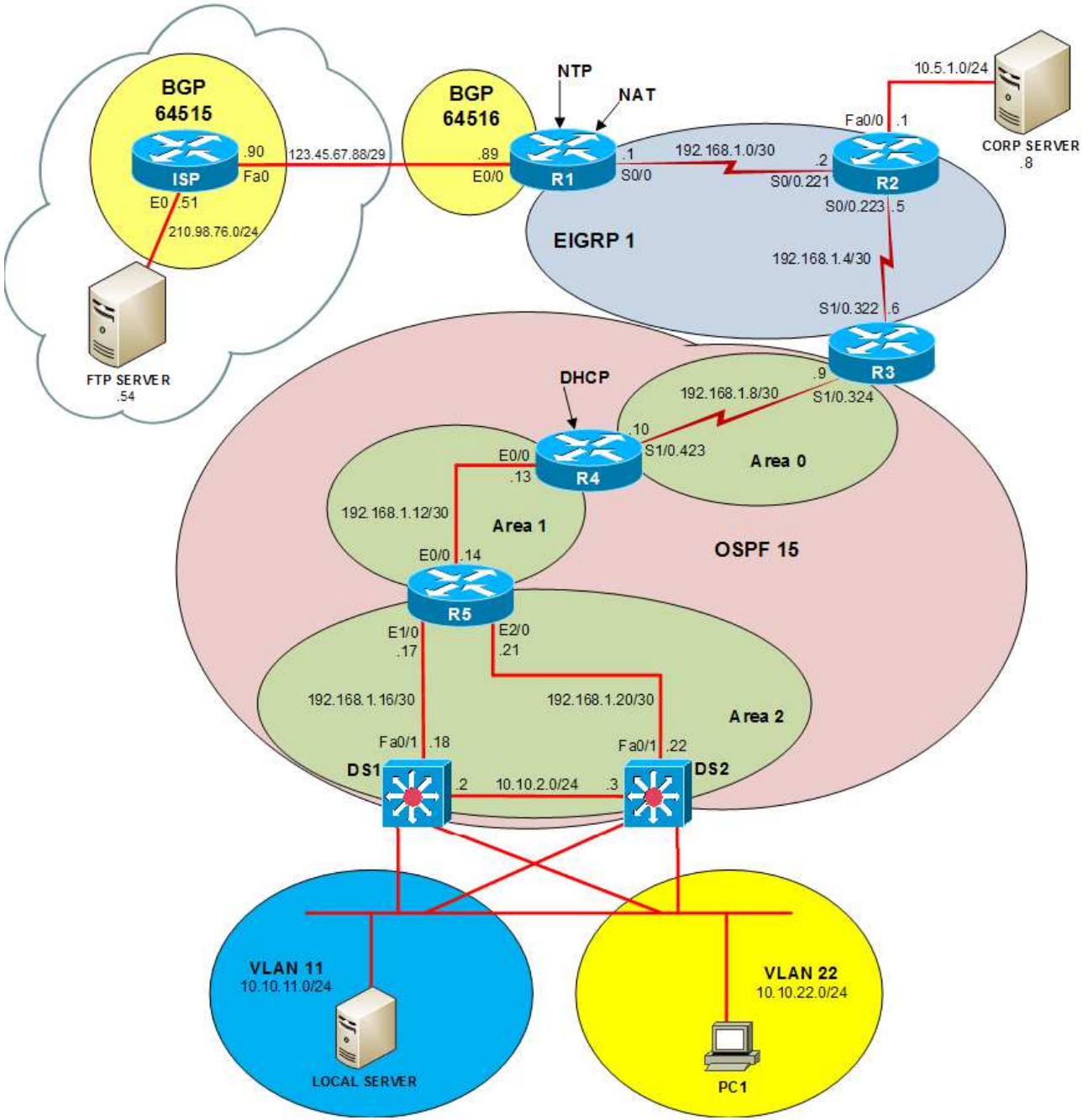
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

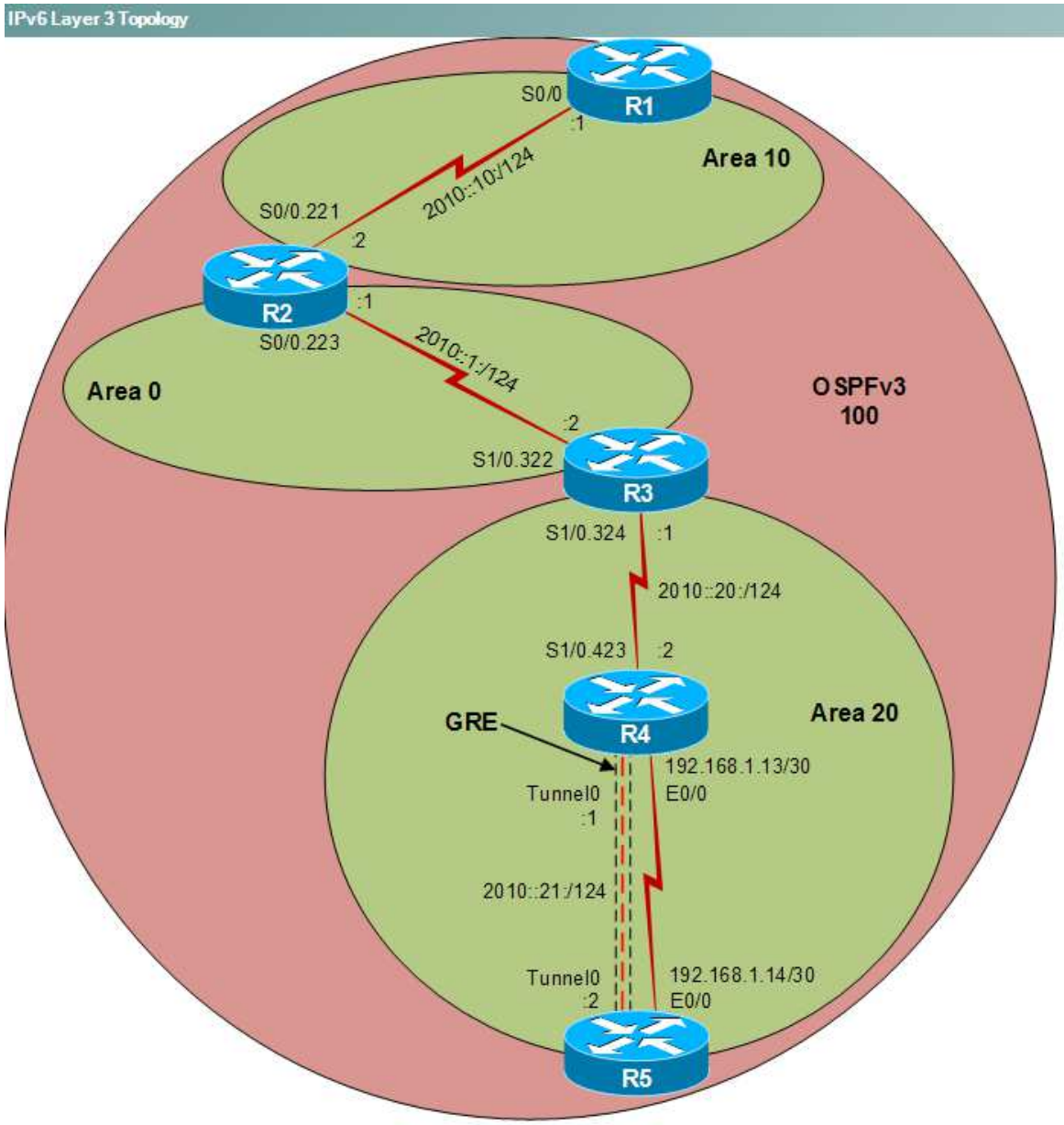
**Layer 2 Topology**




IPv4 layer 3 Topology

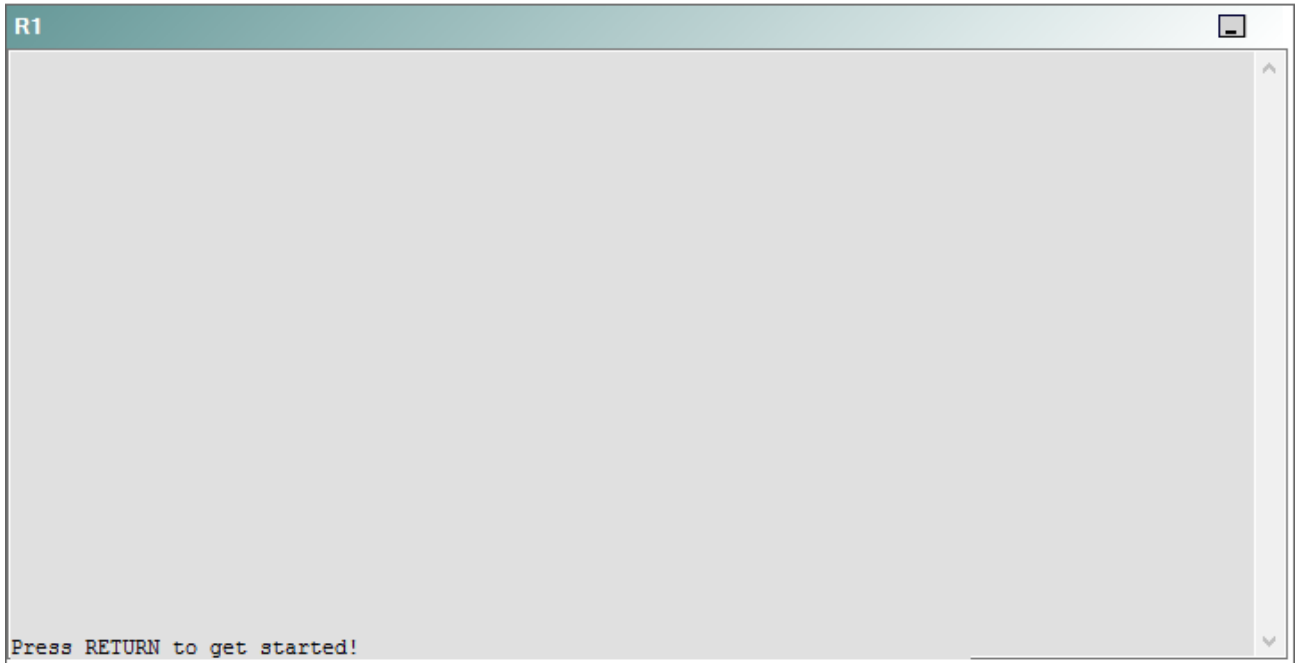

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

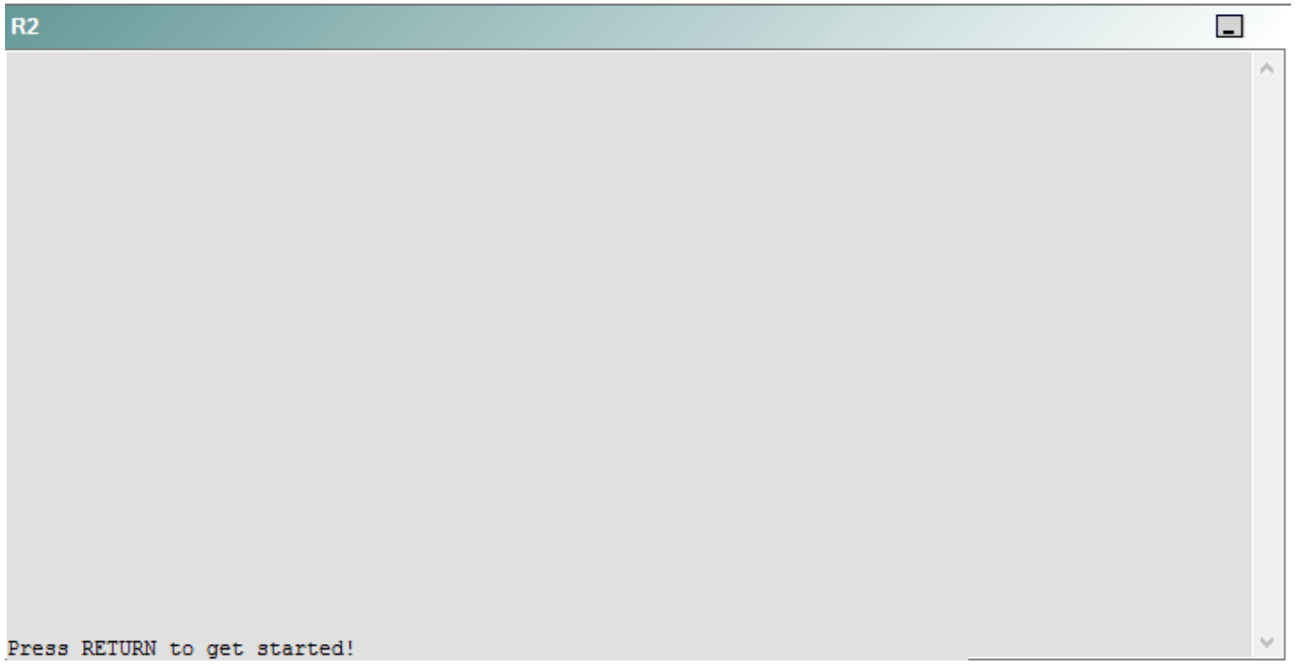



https://www.gratisexam.com/

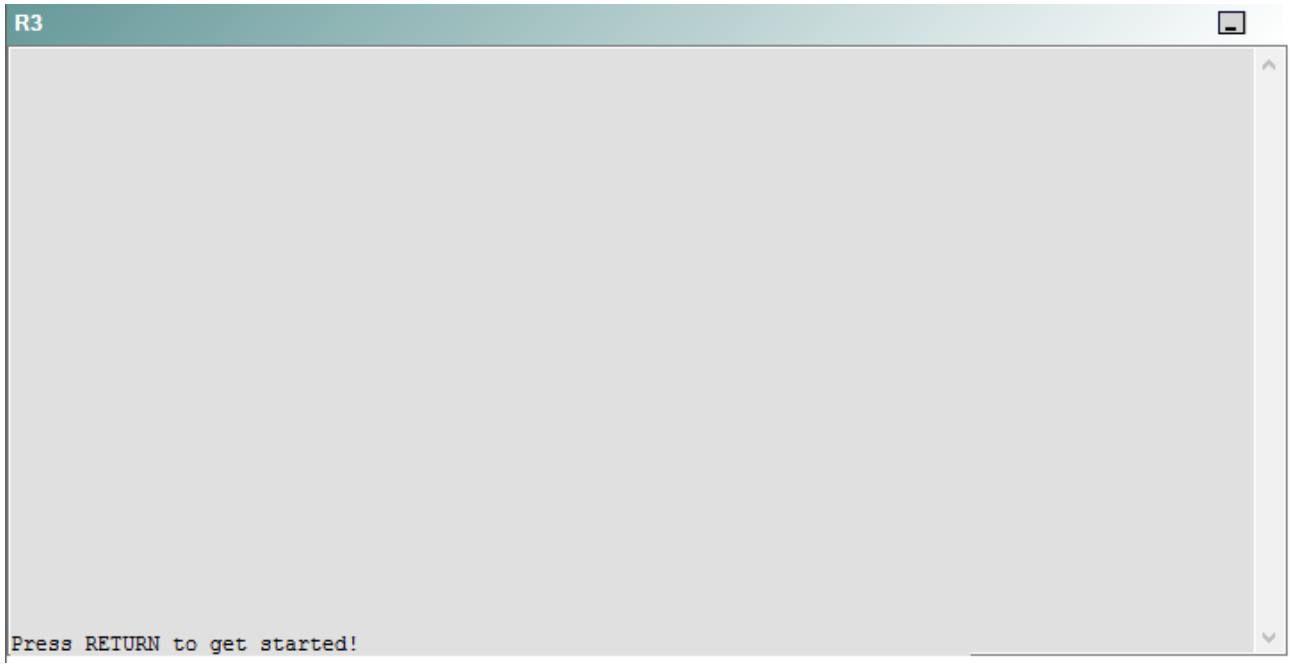
R1



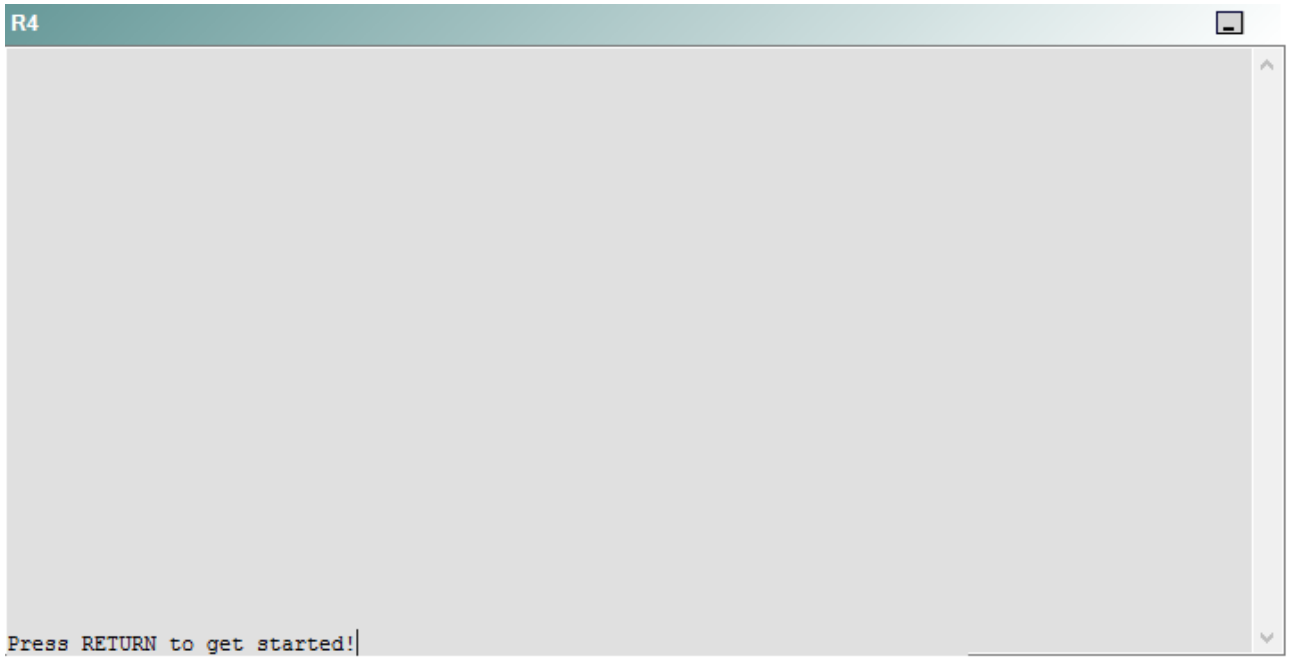

R2



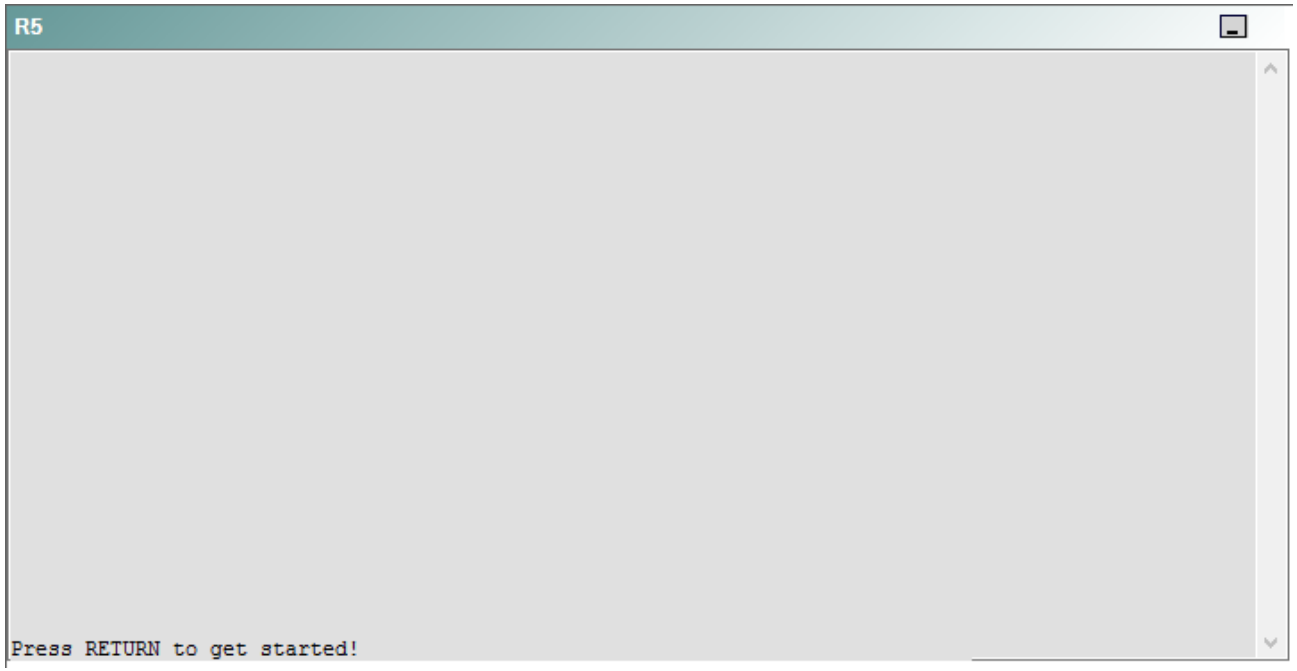

R3



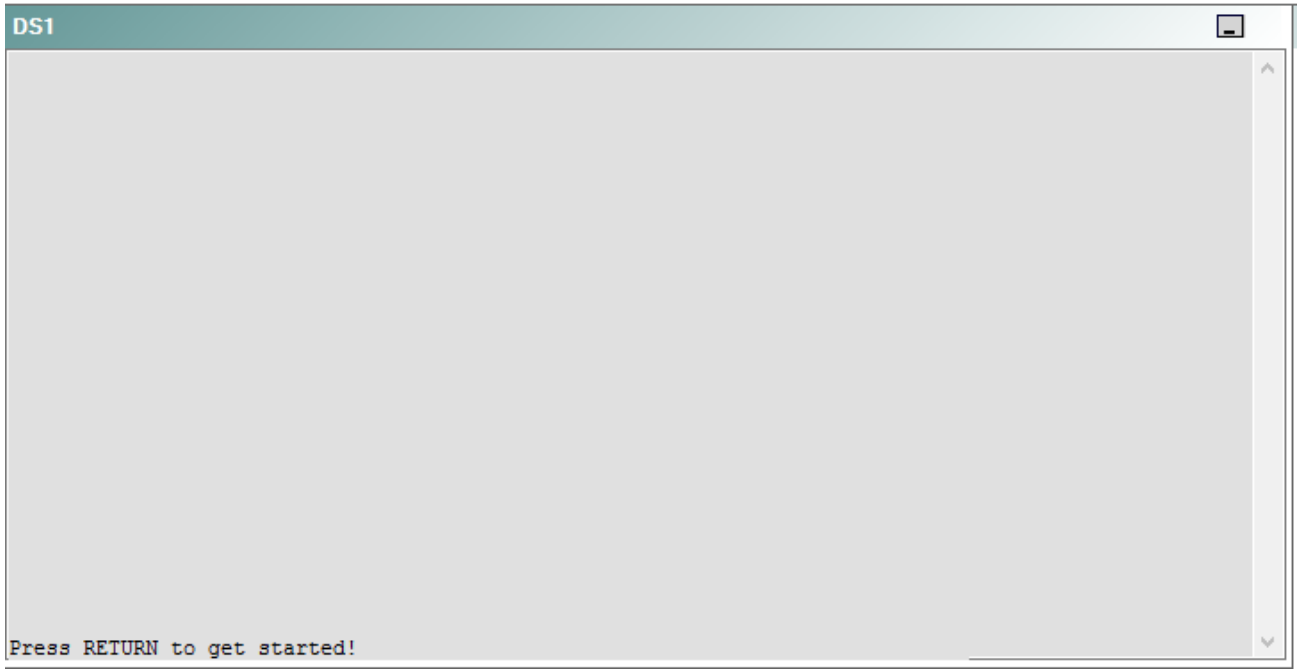

R4



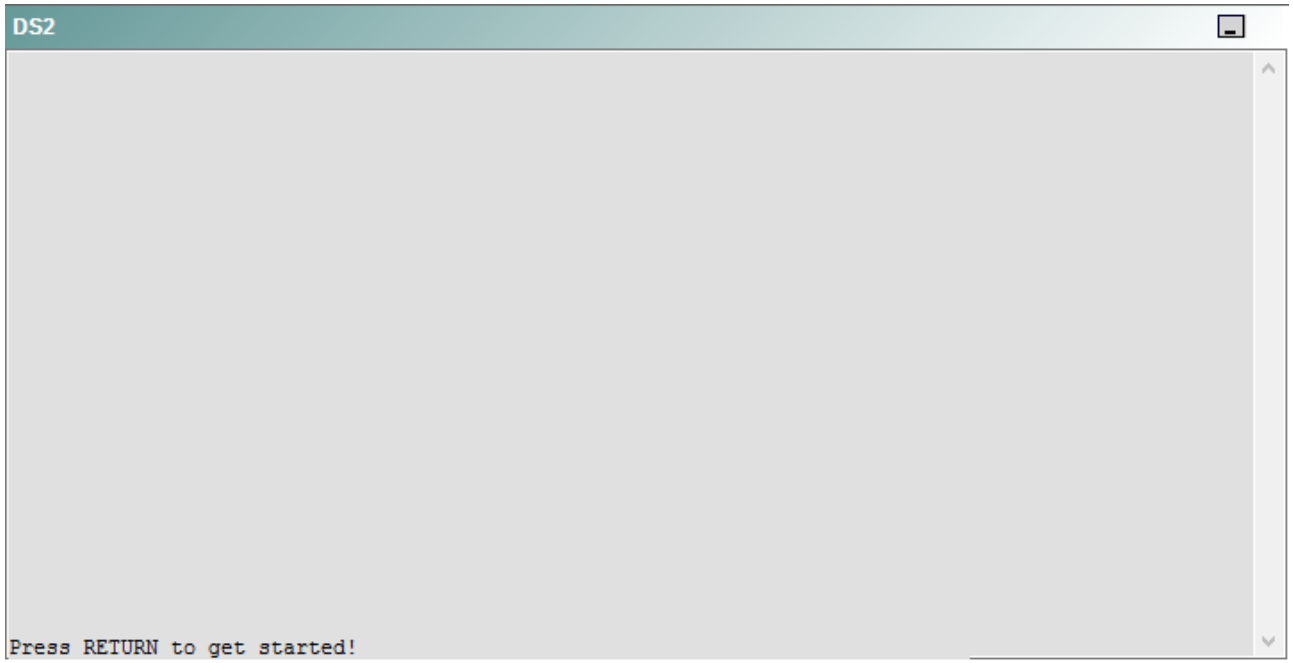

R5



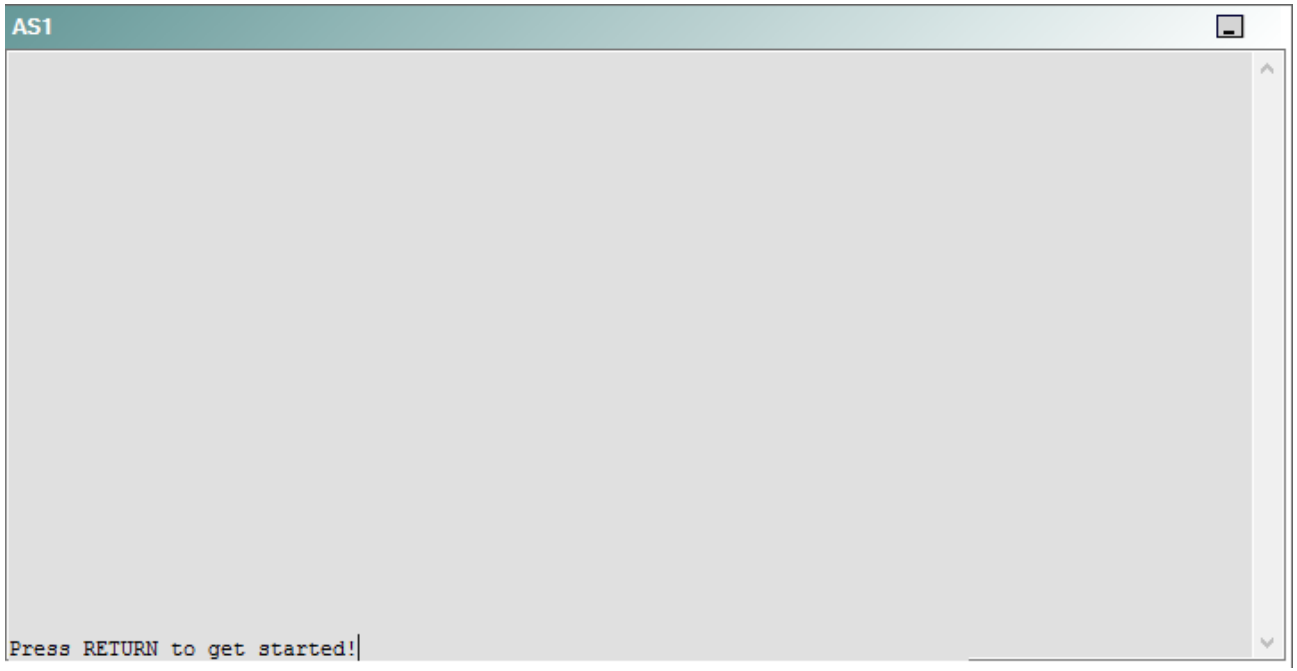

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. creating a new DHCP pool
B. modifying the DHCP exclusion range
C. modifying the IP address range assigned by the DHCP pool
D. changing the default router assigned by the DHCP pool
E. adding a default DNS server to the DHCP pool
F. creating an IP helper address
G. issuing the **ip forward-protocol udp 68** command

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

You should change the default router assigned by the Dynamic Host Configuration Protocol (DHCP) pool on R4; currently, no router is being assigned by the DHCP pool. To determine which device is the source of the problem, you can issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from PC1 to the closest device and work your way up the network until communication is lost, or you can ping from PC1to the farthest device and work your way back to PC1 until pings are successful.

In this scenario, PC1 is able to ping only the switches on the same subnet as PC1. Issuing the **ipconfig** command on PC1 will display the following output.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.10.22.31
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
```

The `Default Gateway` section is blank; the DHCP server, R4, did not assign PC1 a default gateway when it assigned an IP address to PC1. The **default-router** *address* command specifies the default gateway that is assigned to clients by the DHCP server. Therefore, you should issue the **default-router 10.10.22.25** command in DHCP pool configuration mode on R4.

You need not create a new DHCP pool on any of the devices on the network. Creating a new DHCP pool on another device with the same address range can cause IP address conflicts to arise if DHCP servers assign the same IP address to two different devices. The **ip dhcp pool** *pool-name* command creates a DHCP pool and enters DHCP configuration mode, in which you can configure various DHCP client options.

You should not modify the IP address range assigned by the DHCP pool. The DHCP pool must assign addresses from the 10.10.22.0/24 network so that DHCP clients in the Clients virtual LAN (VLAN) can receive IP addresses. The **network** *address subnet* command specifies the range of IP addresses that will be issued by DHCP.

You need not add a Domain Name System (DNS) server to the DHCP pool. DNS servers are used for domain name-to-IP address resolution. PC1 cannot ping the server 210.98.76.54 by its IP address, so a DNS server is unnecessary. The **dns-server** *address* command specifies the DNS server address that is assigned to clients by the DHCP server.

You should not modify the DHCP exclusion range on R4. A DHCP exclusion range is a range of addresses that should not be assigned to clients by the DHCP server. These addresses are typically static IP addresses that are assigned to servers and other network devices. The **ip dhcp excluded-address** *start-address*

*end-address* command is used to exclude from DHCP the range of addresses from *start-address* through *end-address*. The **ip dhcp excluded-address 10.10.22.1 10.10.22.30** command that has already been issued on R4 is sufficient to exclude the statically assigned devices on the network.

You need not create an IP helper address. DS1 and DS2 are already configured with an IP helper address so that DHCP requests from VLAN 22 can reach R4. The **ip helper-address** command is used to forward User Datagram Protocol (UDP) broadcasts to a remote server or device. DHCP server on a remote subnet. The address lease process and other communications are then returned to the originating subnet.

You need not issue the **ip forward-protocol udp 68** command. The **ip forward-protocol** command is used to specify the UDP port numbers that should be forwarded by the **ip helper-address** command. By default, the **ip helper-address** command forwards broadcasts to the following UDP ports:

- 37 - Time Protocol
- 49 - Terminal Access Controller Access Control System (TACACS)
- 53 - DNS
- 67 - Bootstrap Protocol (BOOTP) and DHCP Server
- 68 - BOOTP and DHCP Client
- 69 - Trivial File Transfer Protocol (TFTP)
- 137 - Network Basic Input/Output System (NetBIOS) Name Service
- 138 - NetBIOS Datagram

Because DHCP client requests are already sent by the **ip helper-address** command, the **ip forward-protocol udp 68** command is unnecessary.

Reference:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfdhcp.html

**QUESTION 27**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

You can access the following devices for each trouble ticket:

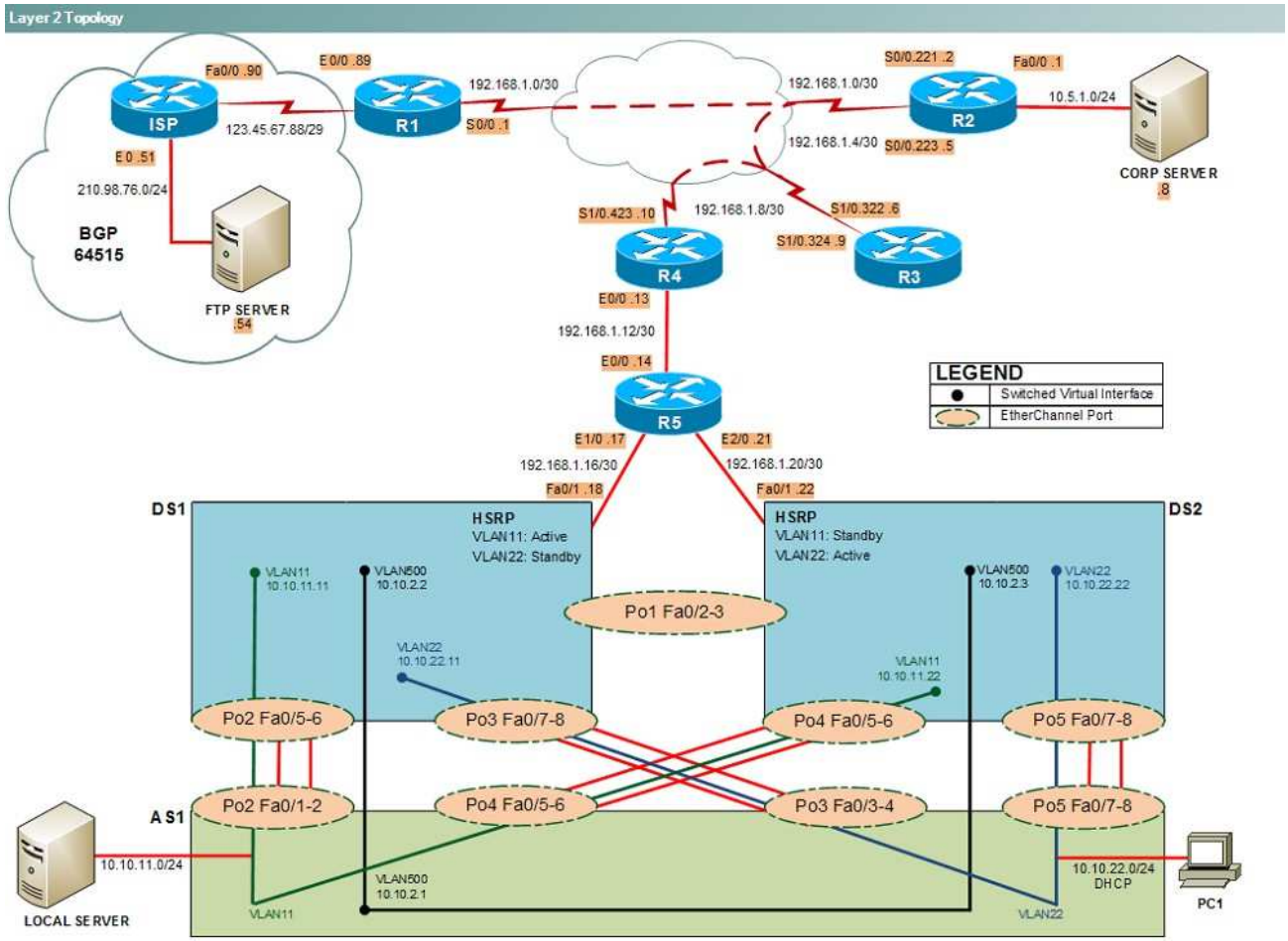
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

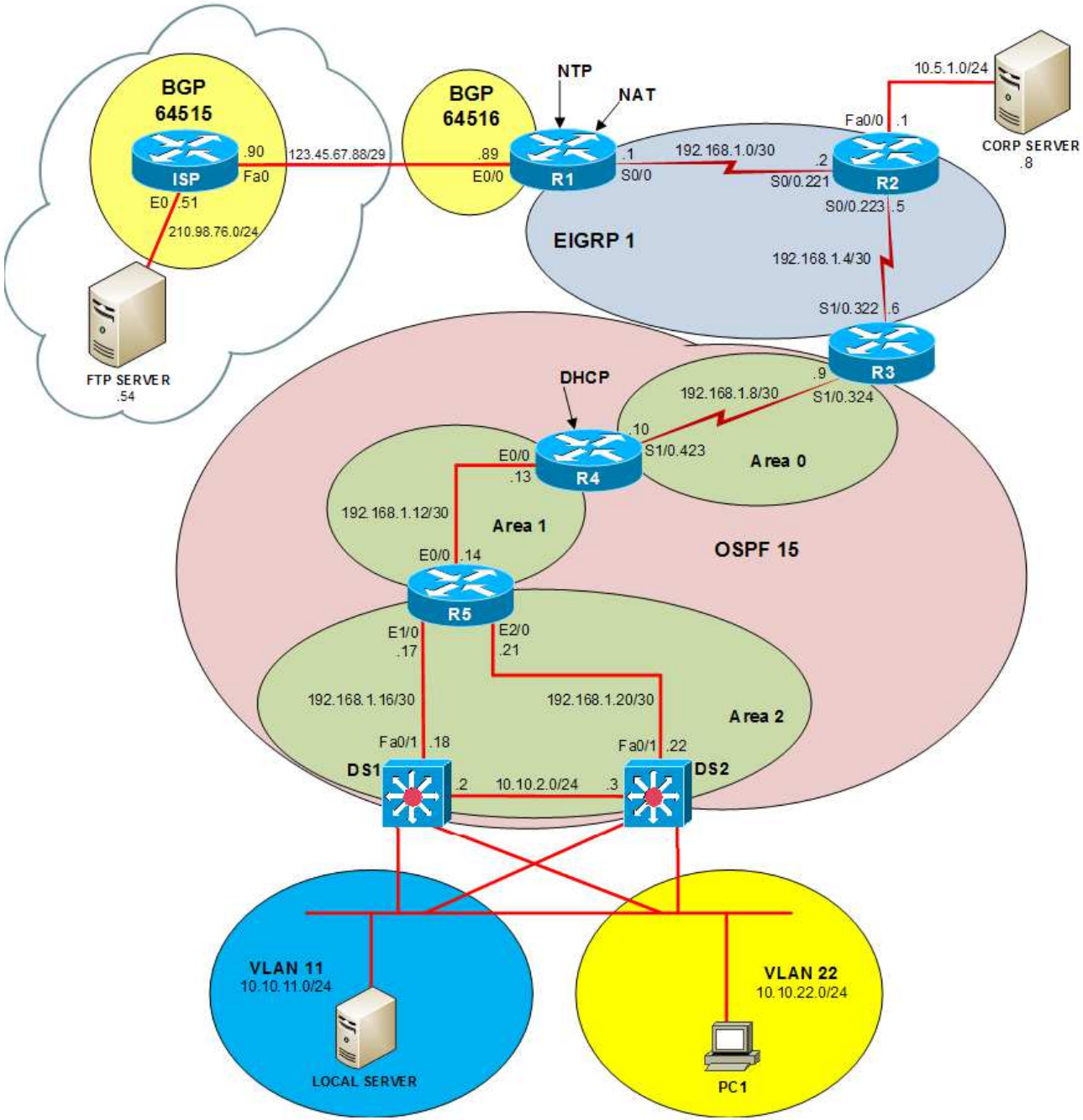
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

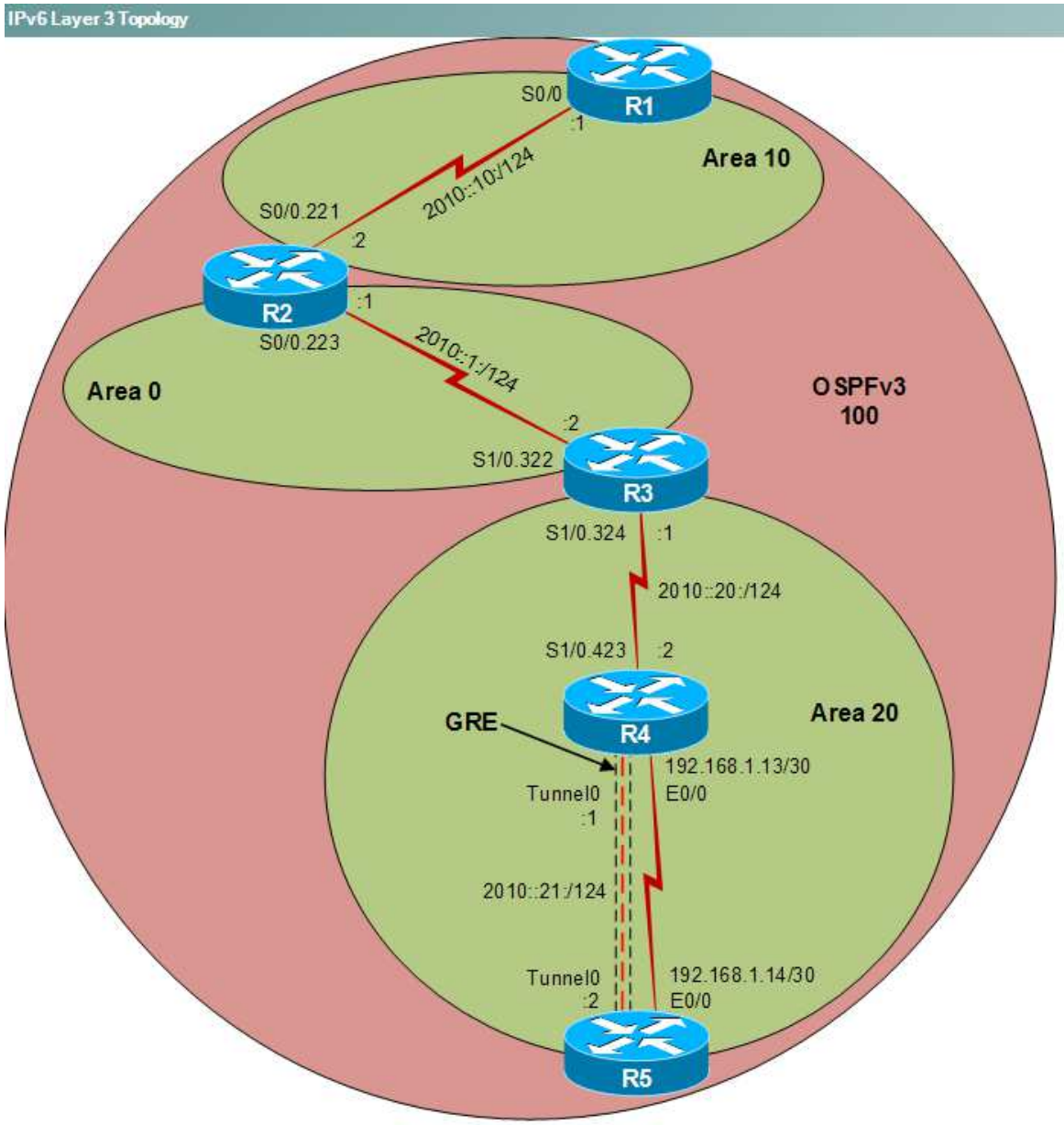
**Layer 2 Topology**




IPv4 layer 3 Topology

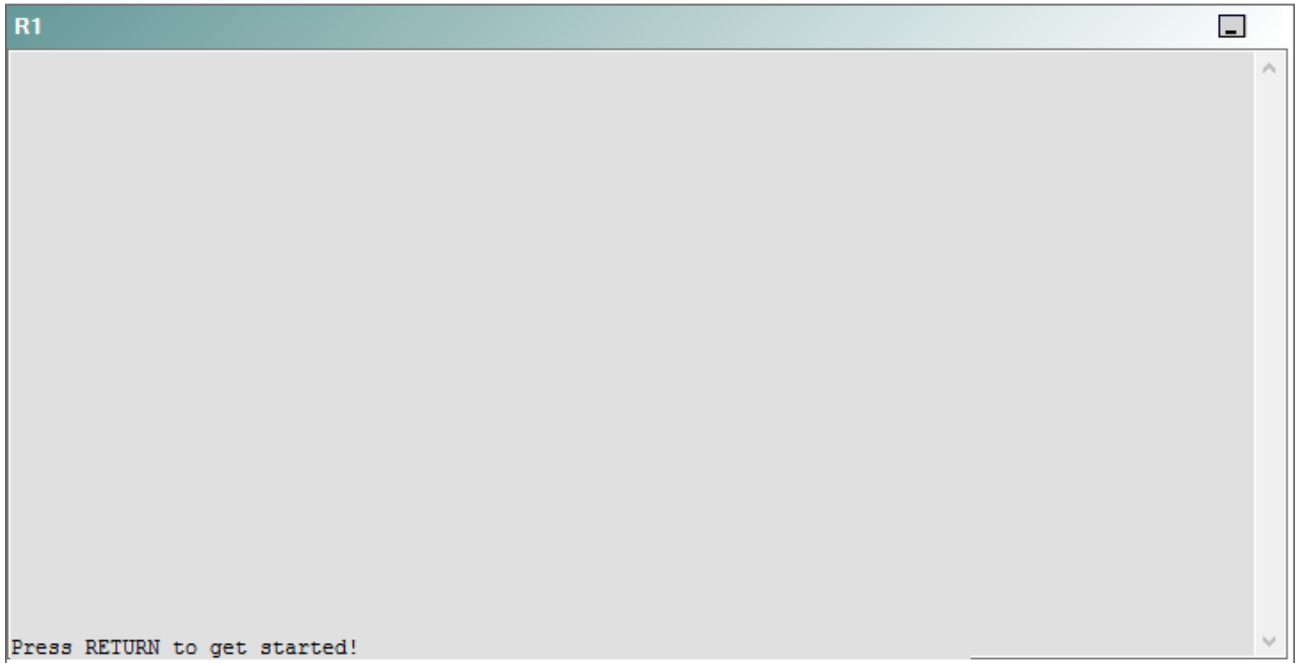

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

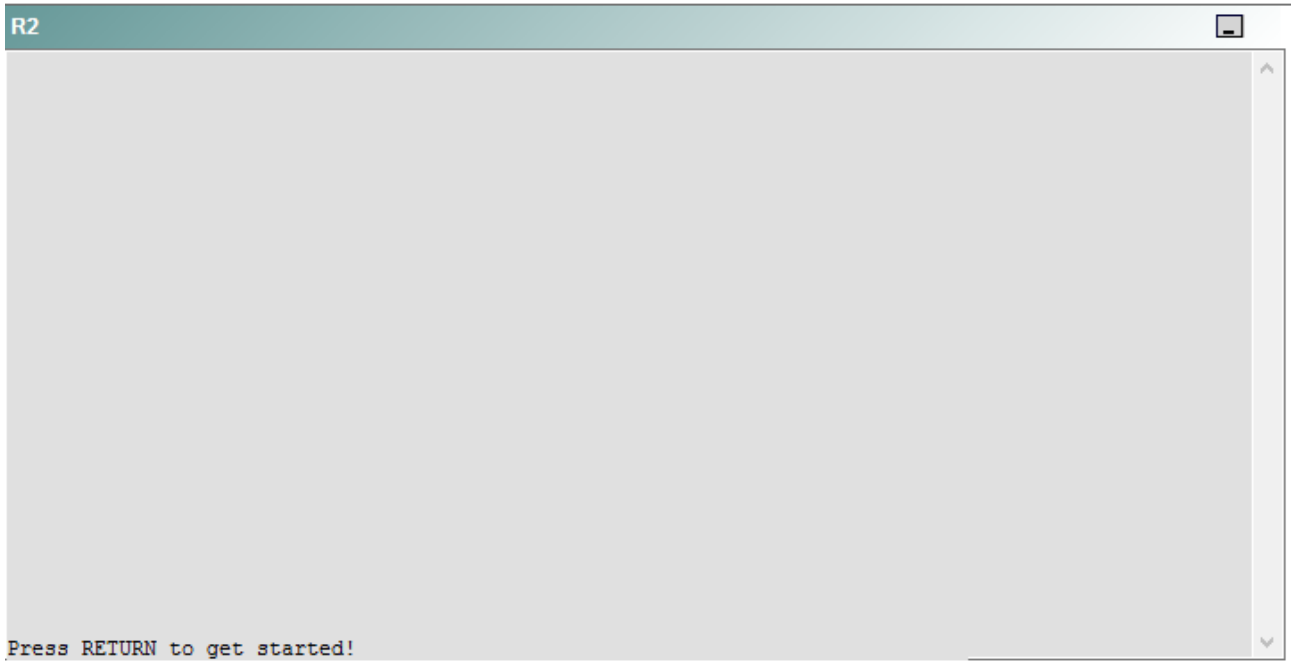



https://www.gratisexam.com/

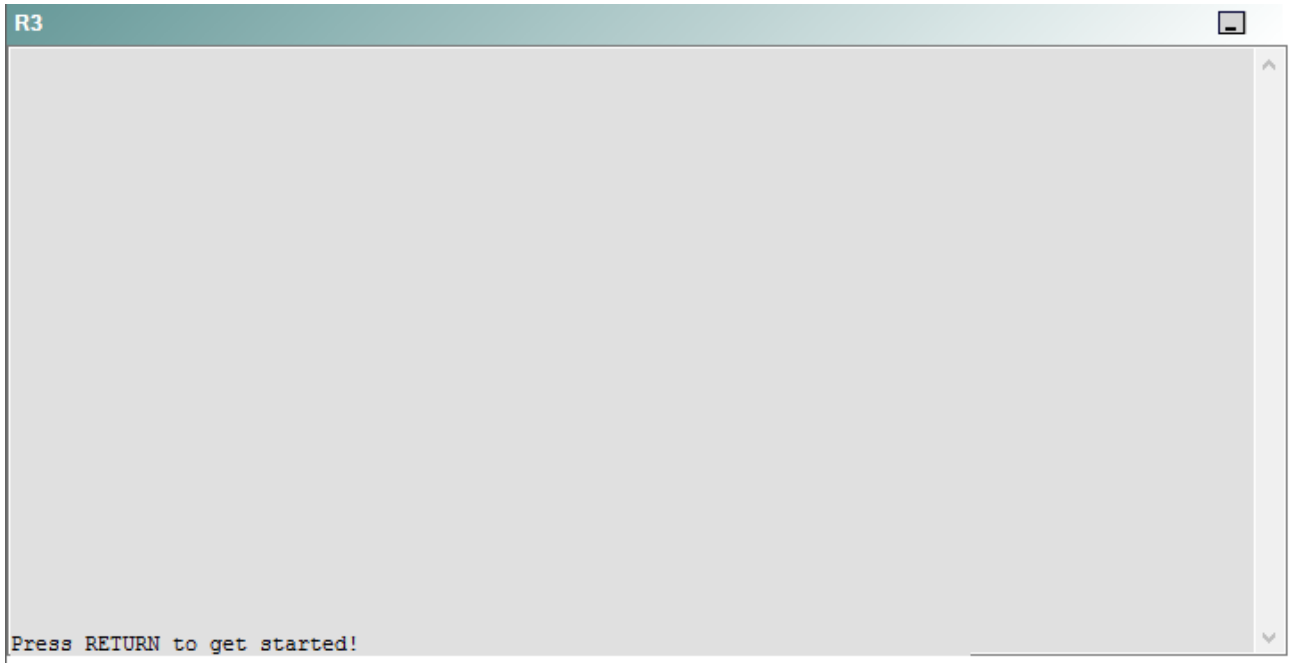
R1



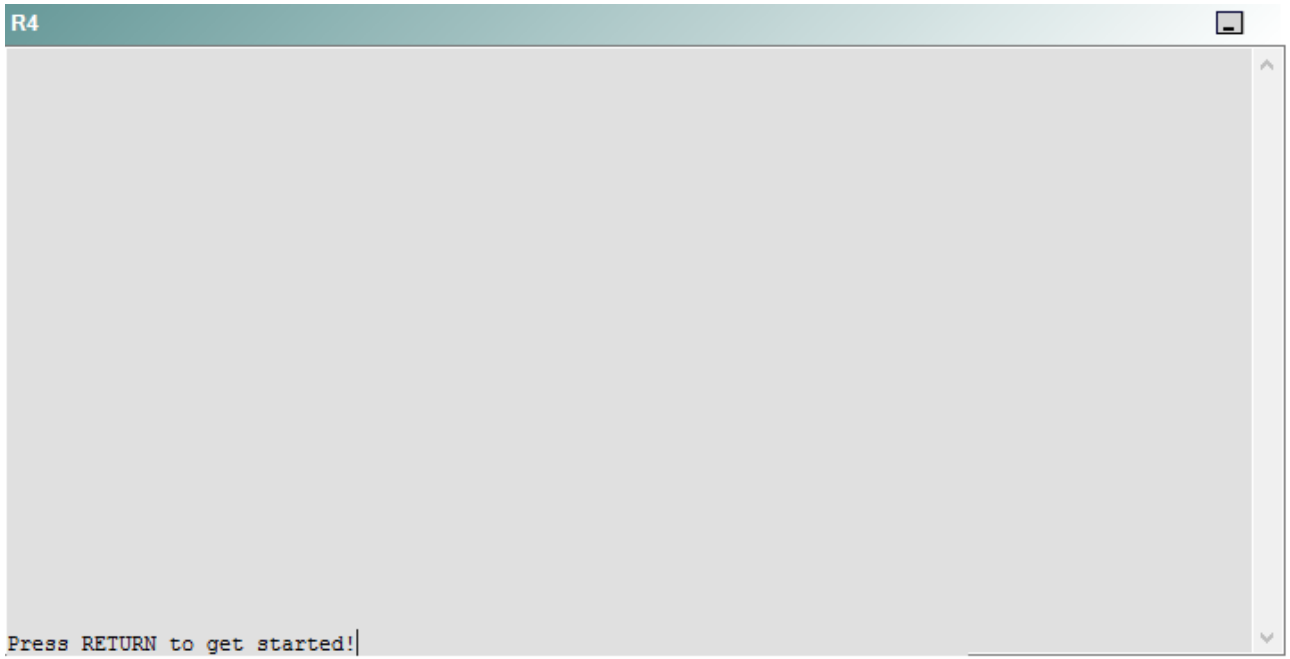

R2



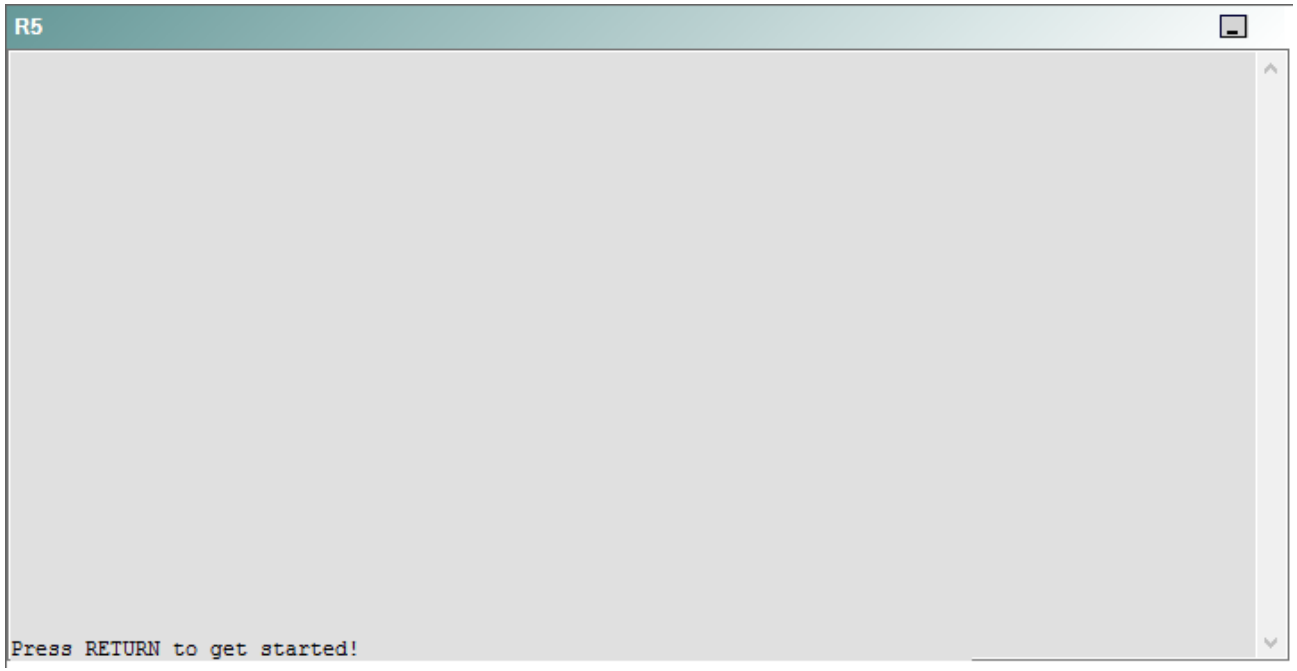

R3



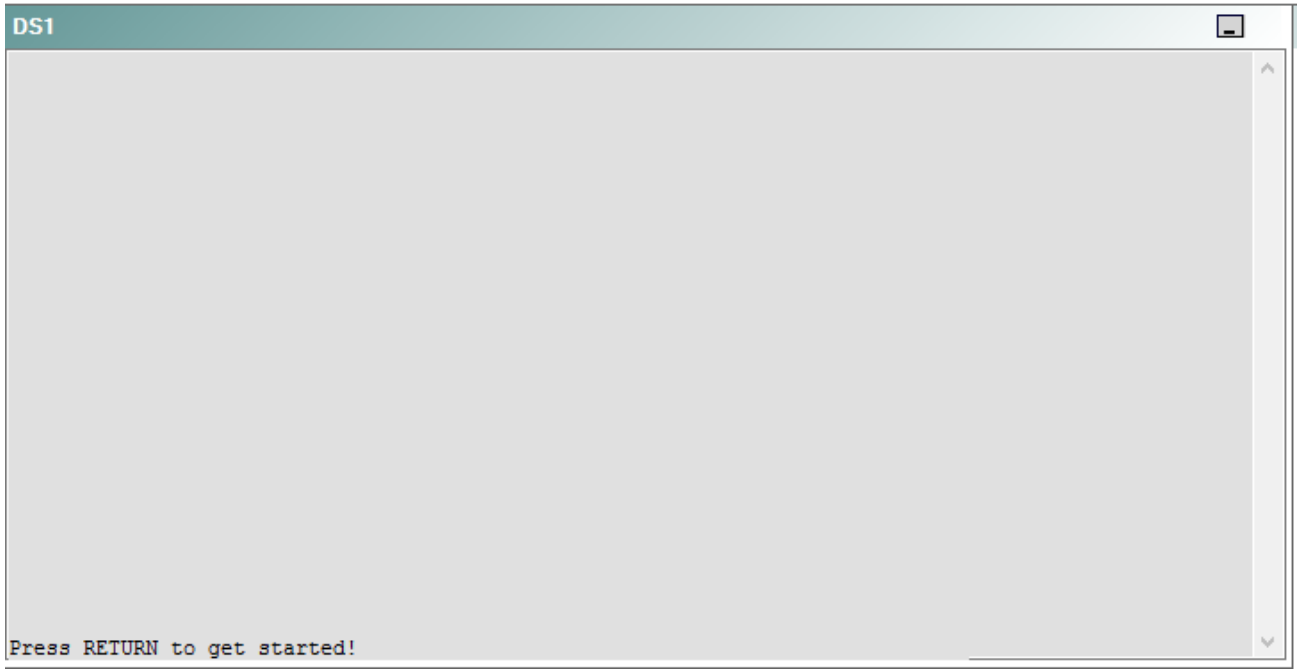

R4



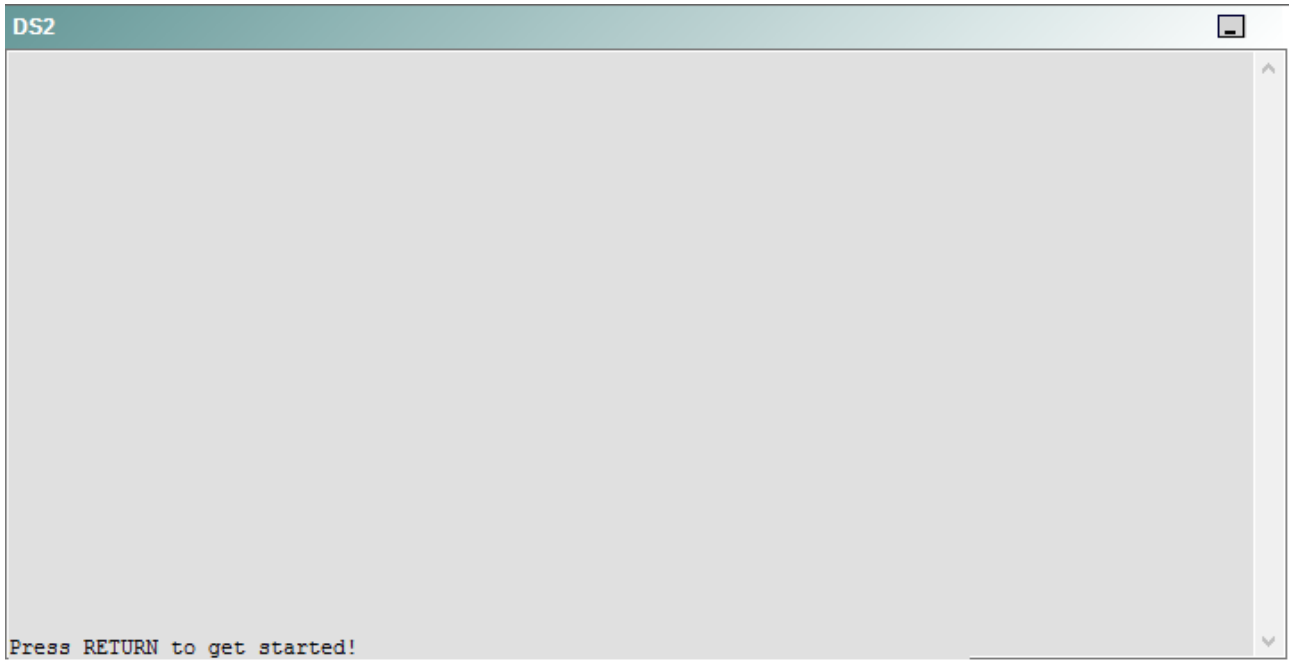

R5



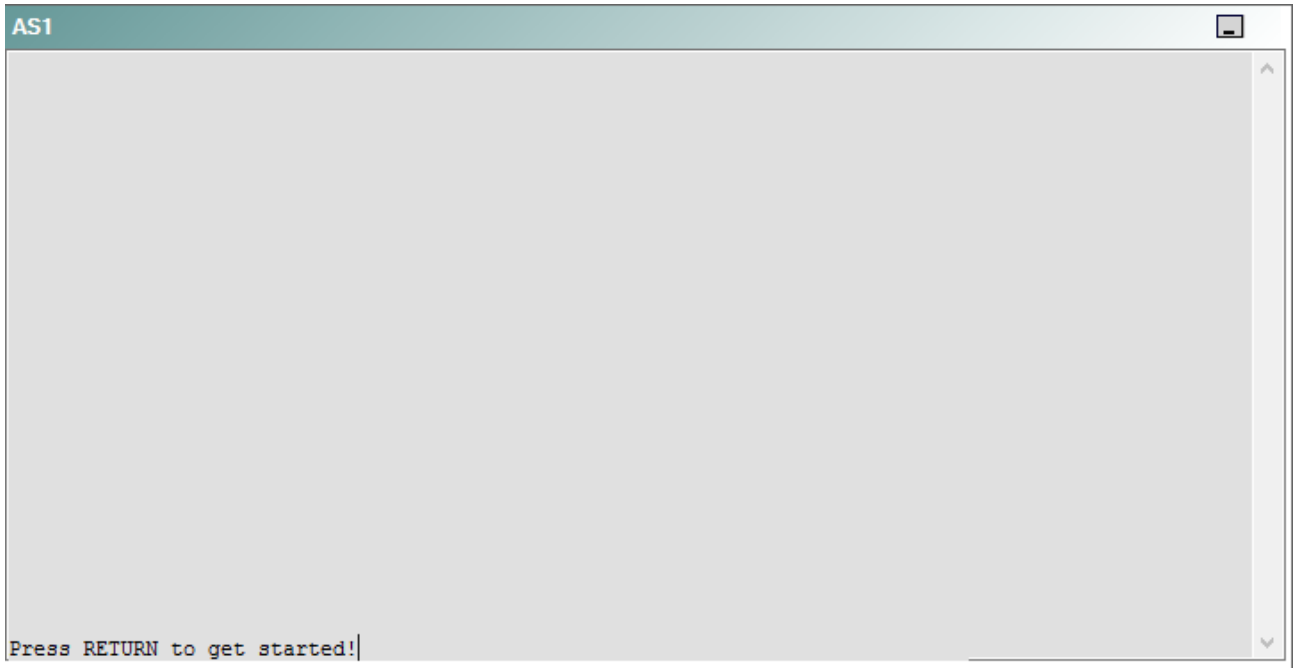

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

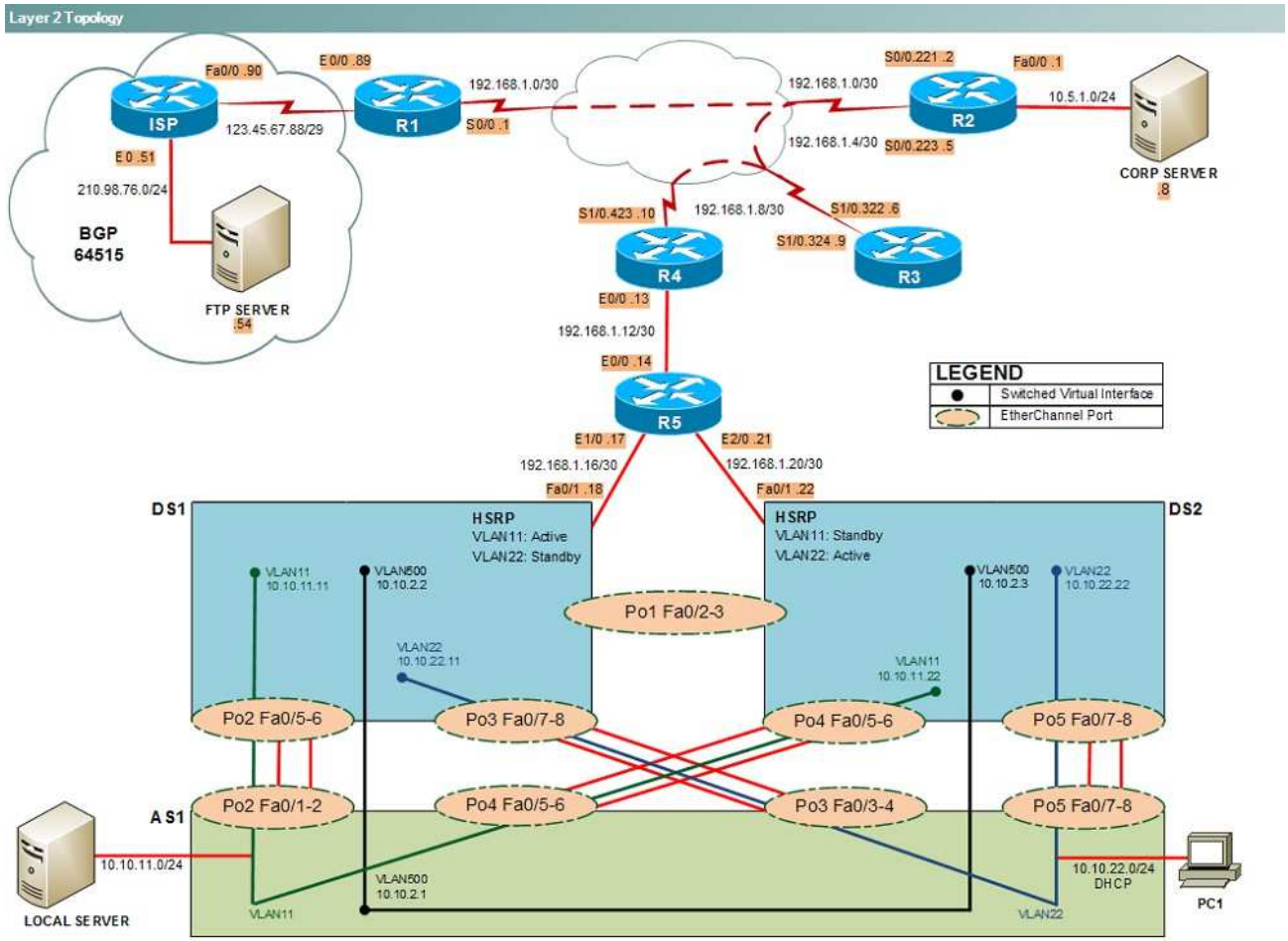
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

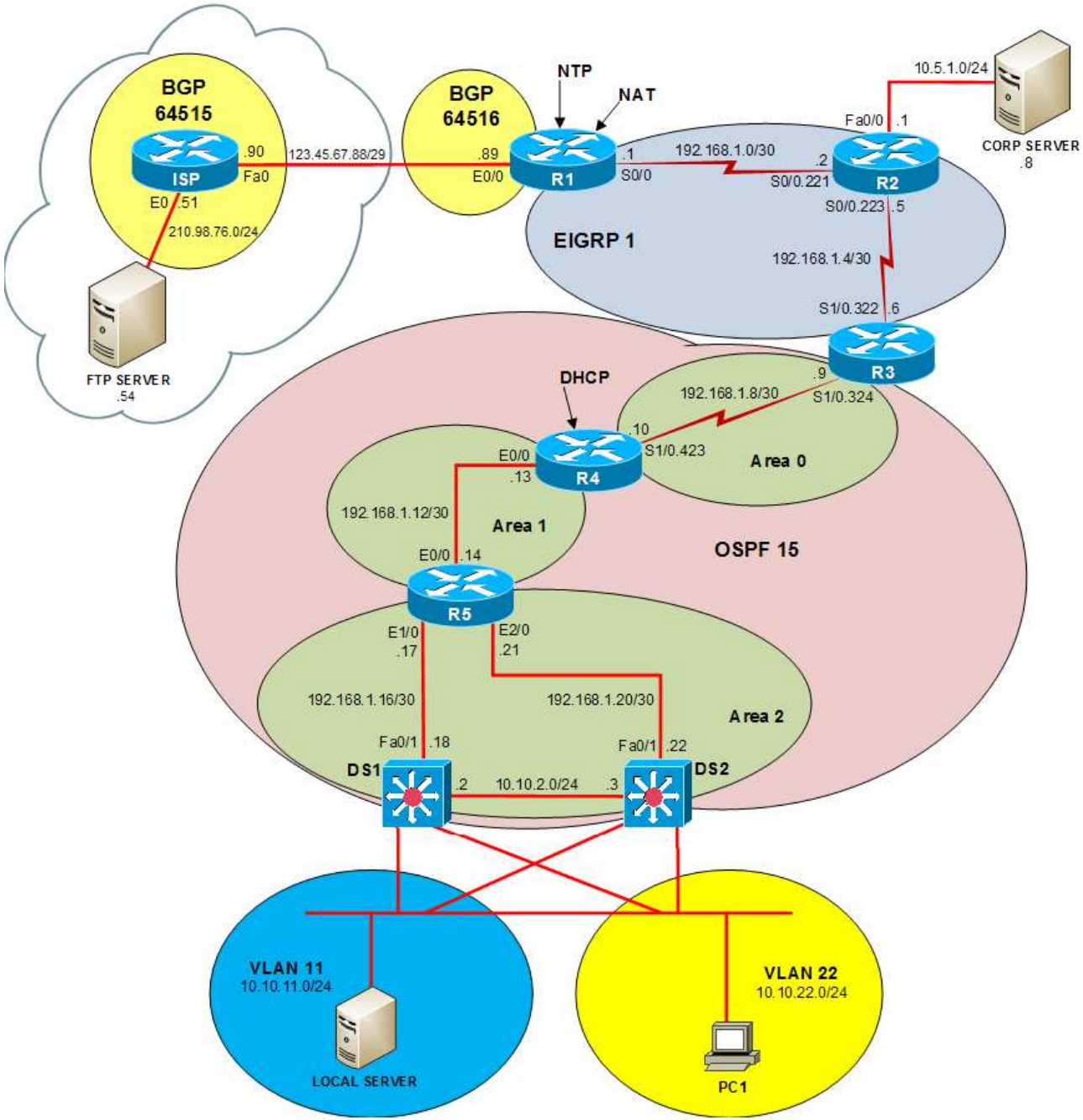
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

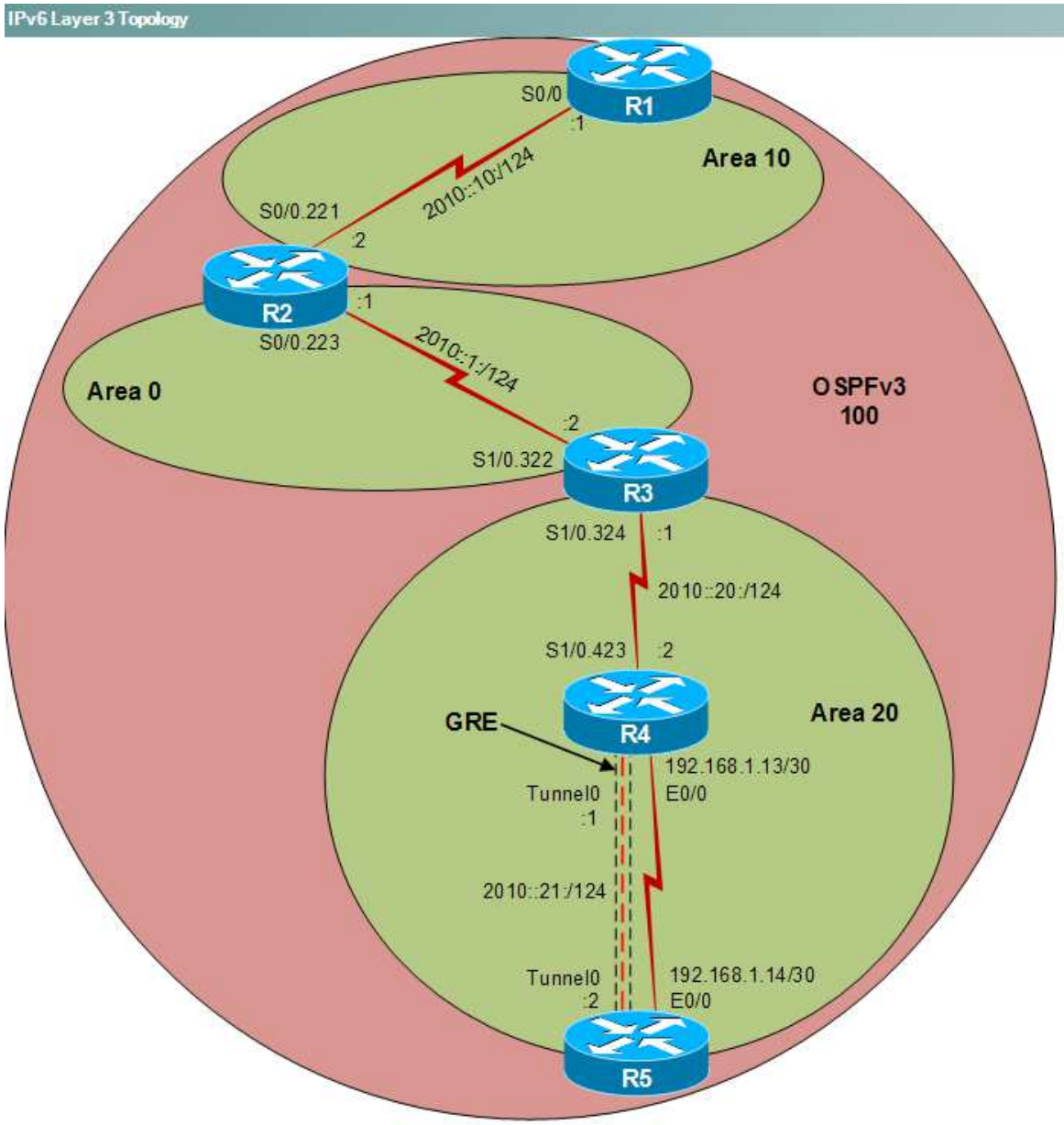
**Layer 2 Topology**




IPv4 layer 3 Topology

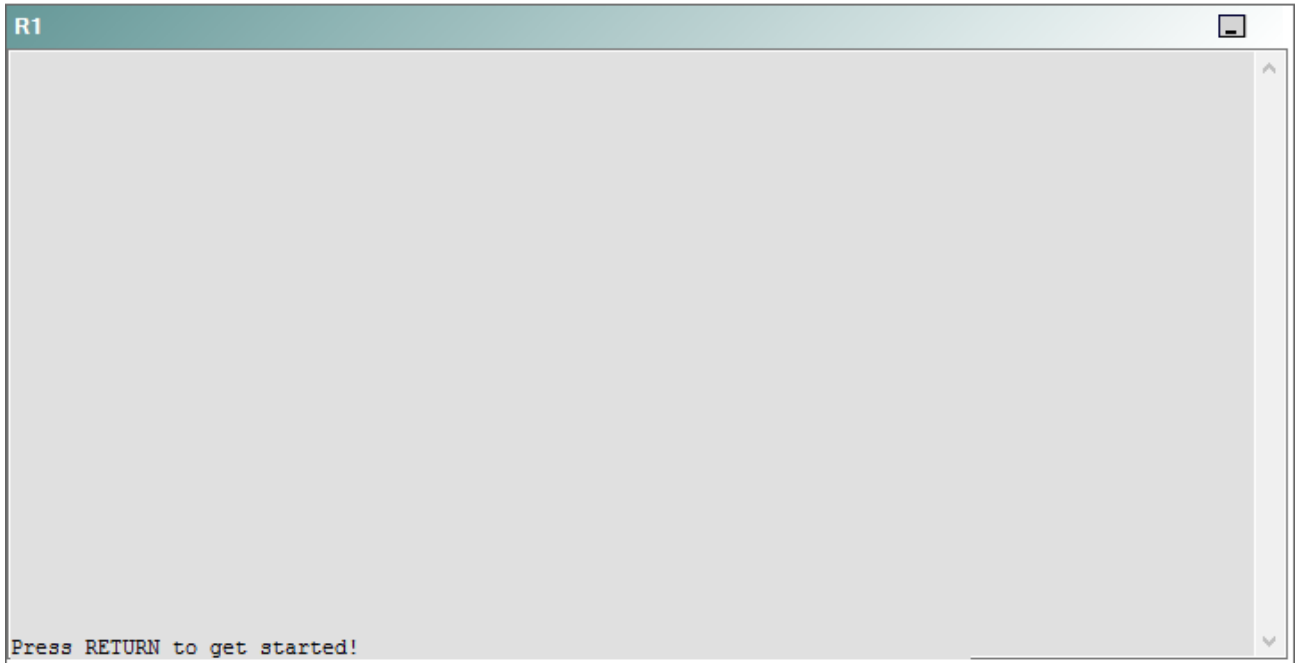

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

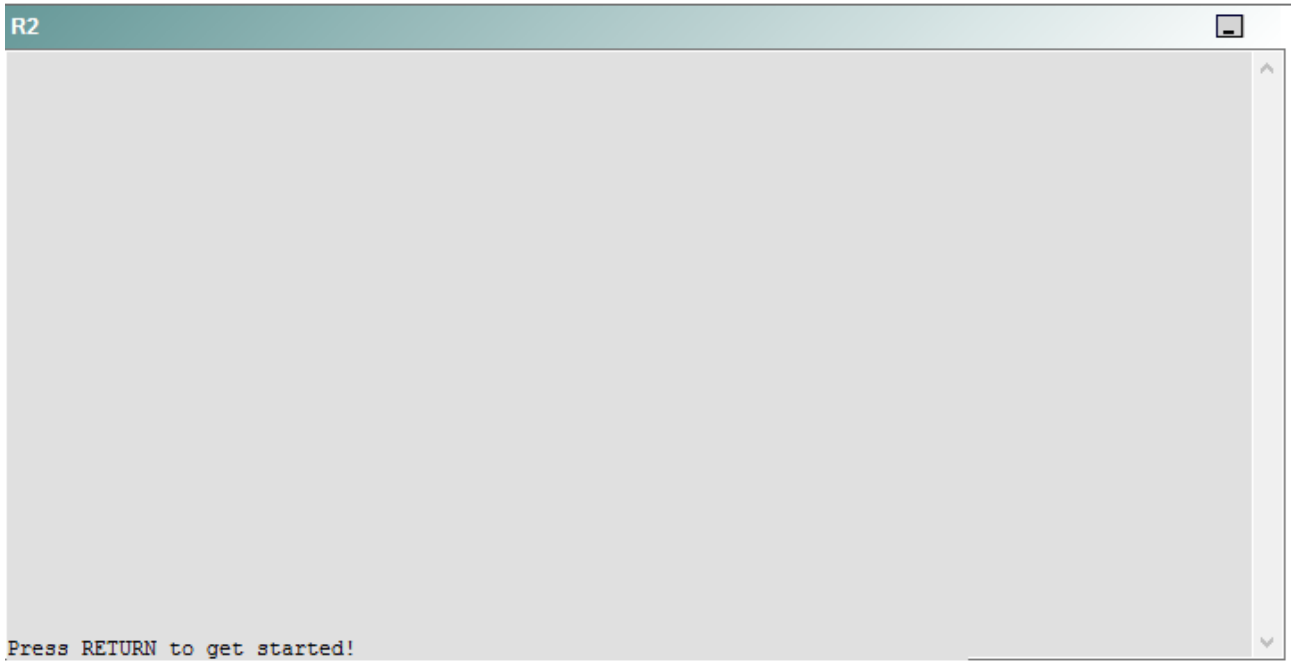



https://www.gratisexam.com/

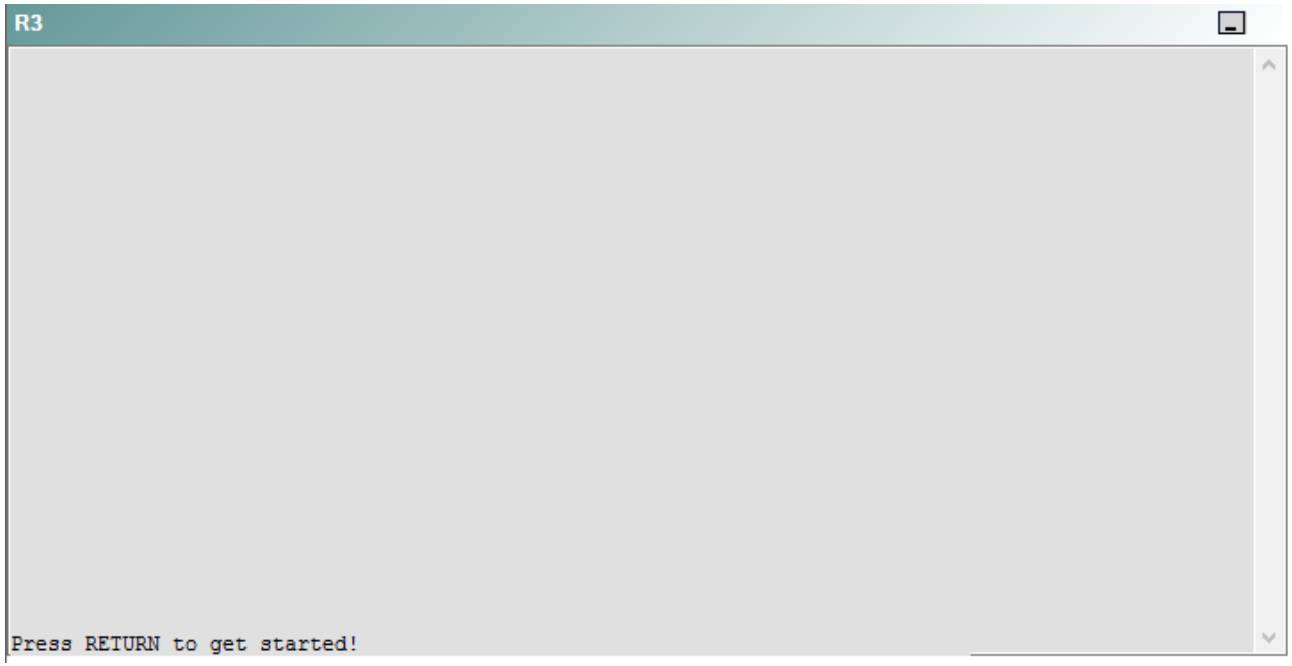
R1



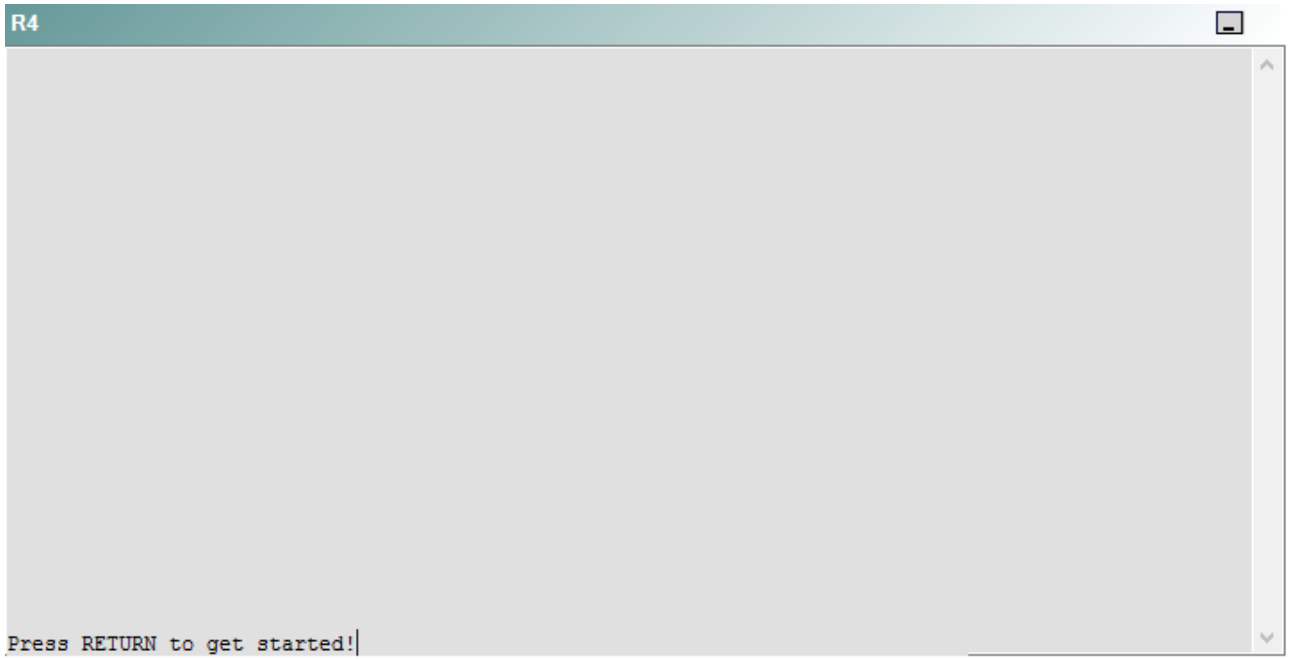

R2



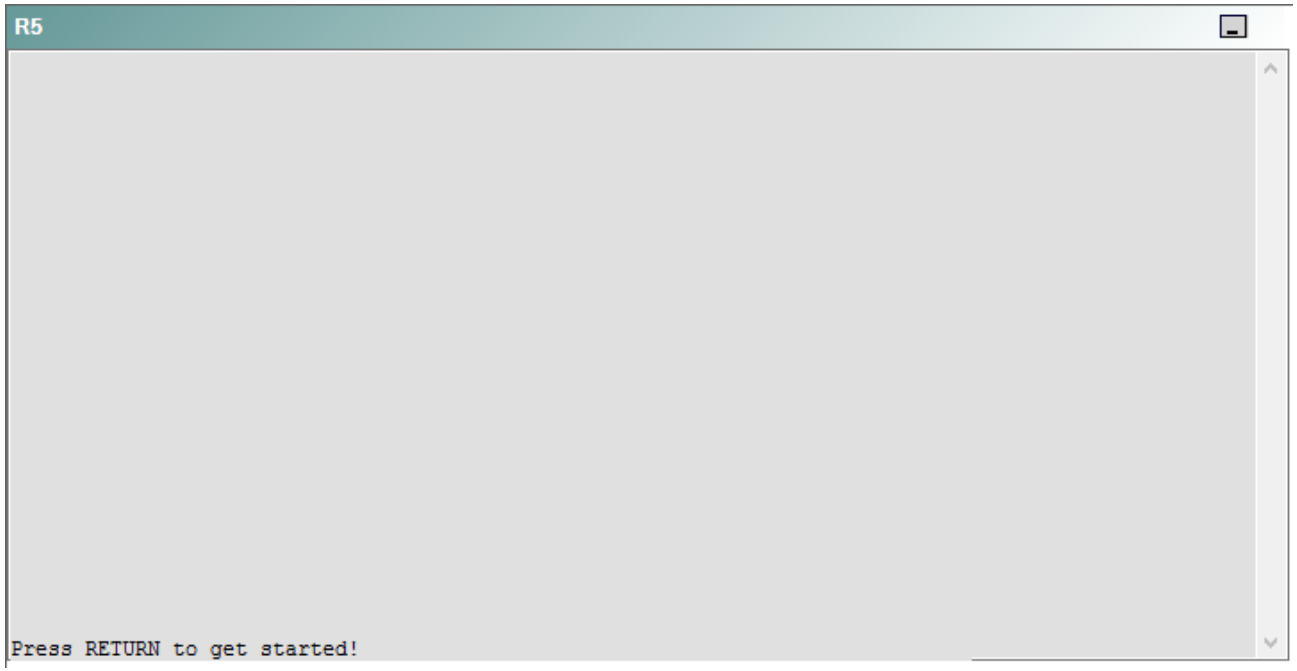

R3



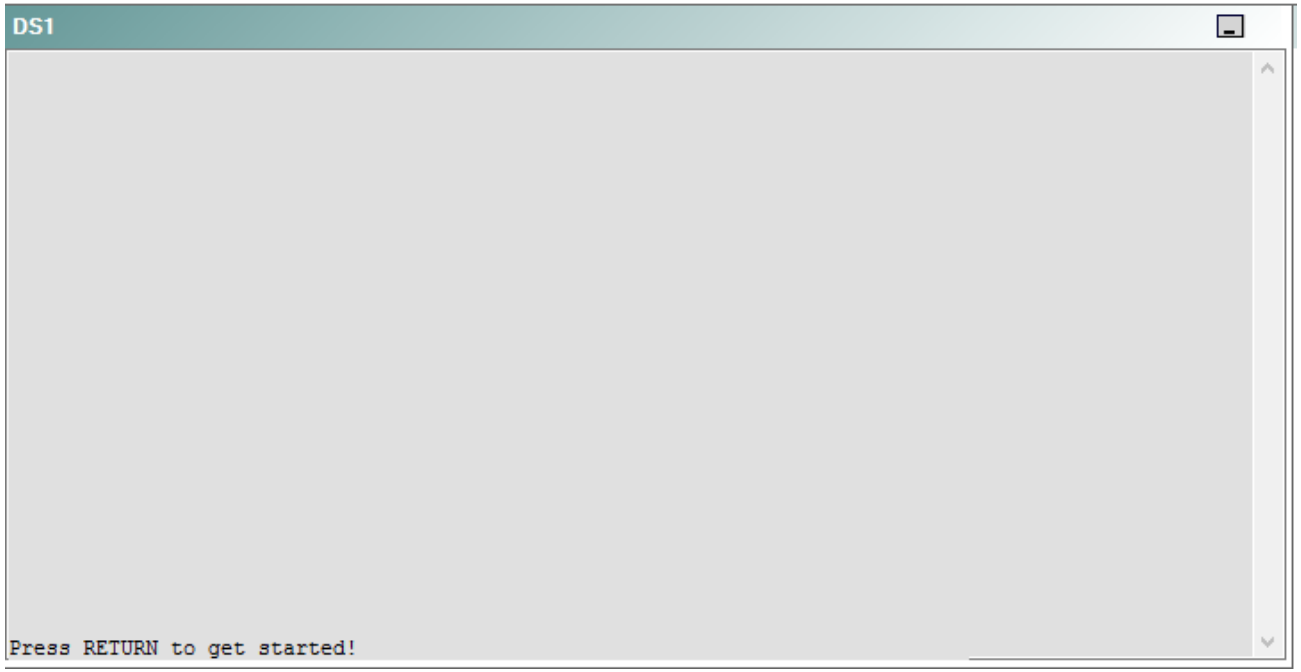

R4



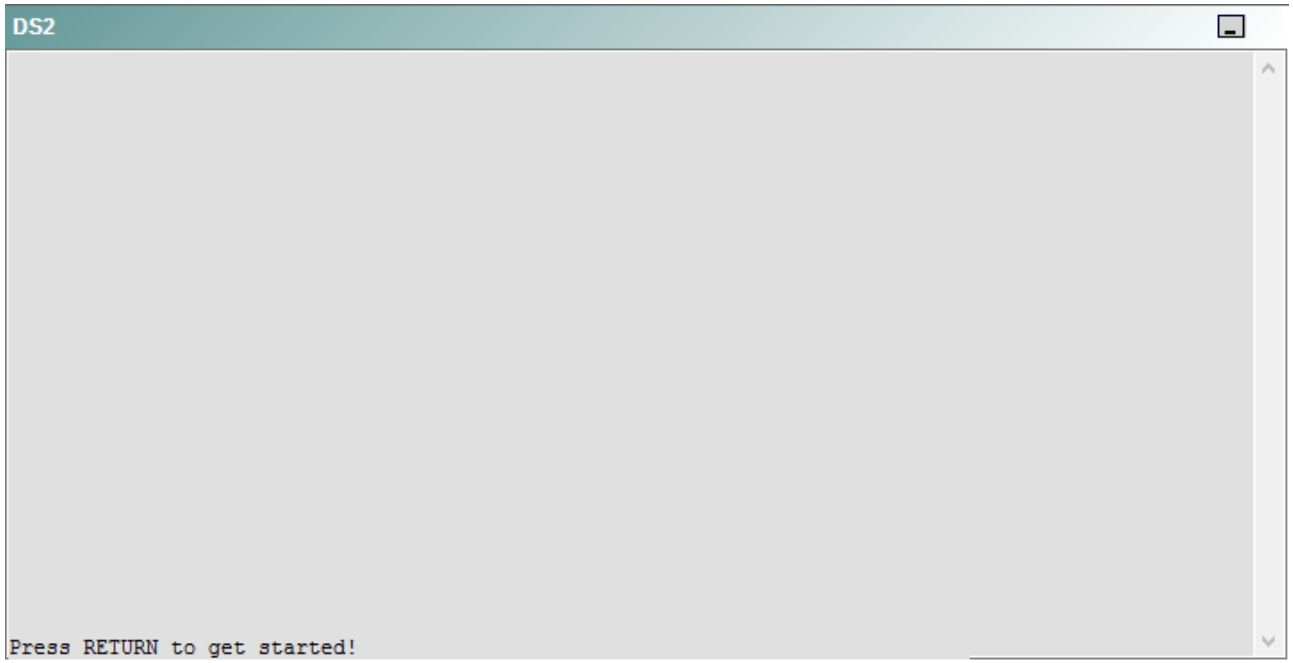

R5



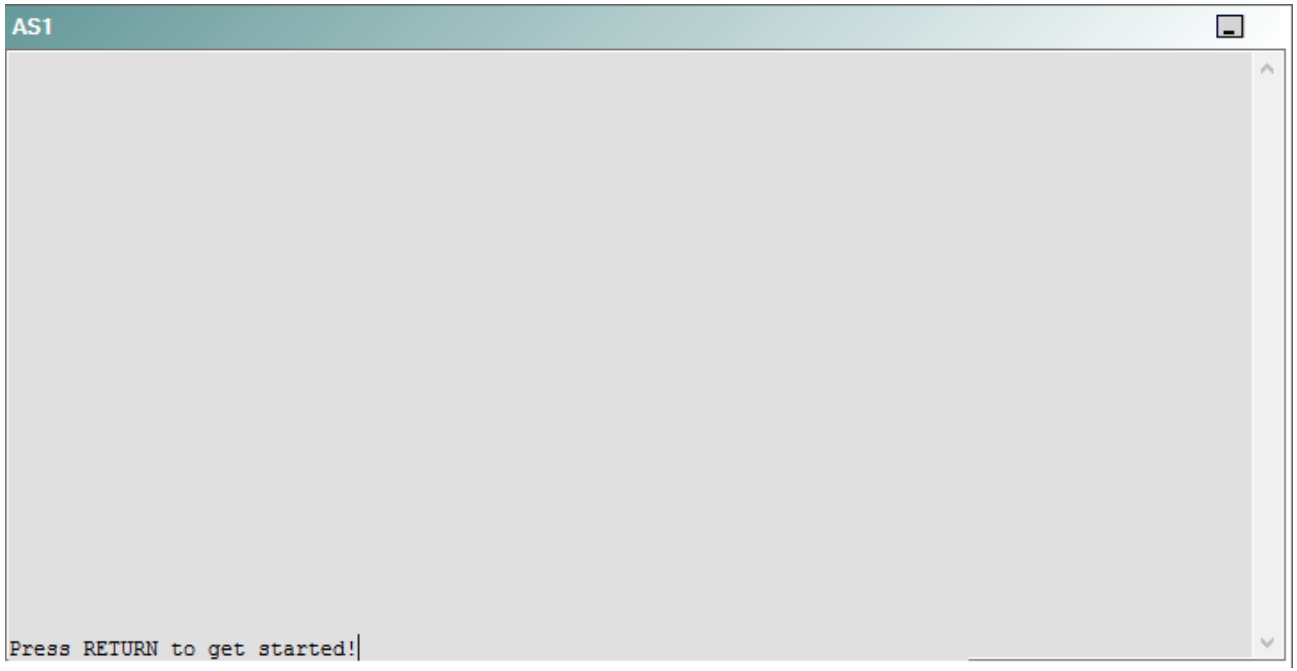

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. HSRP
C. OSPFv2
D. DHCP
E. Layer 3 addressing
F. EIGRP
G. Layer 3 security
H. OSPFv3
I. interface

**Correct Answer:** F

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

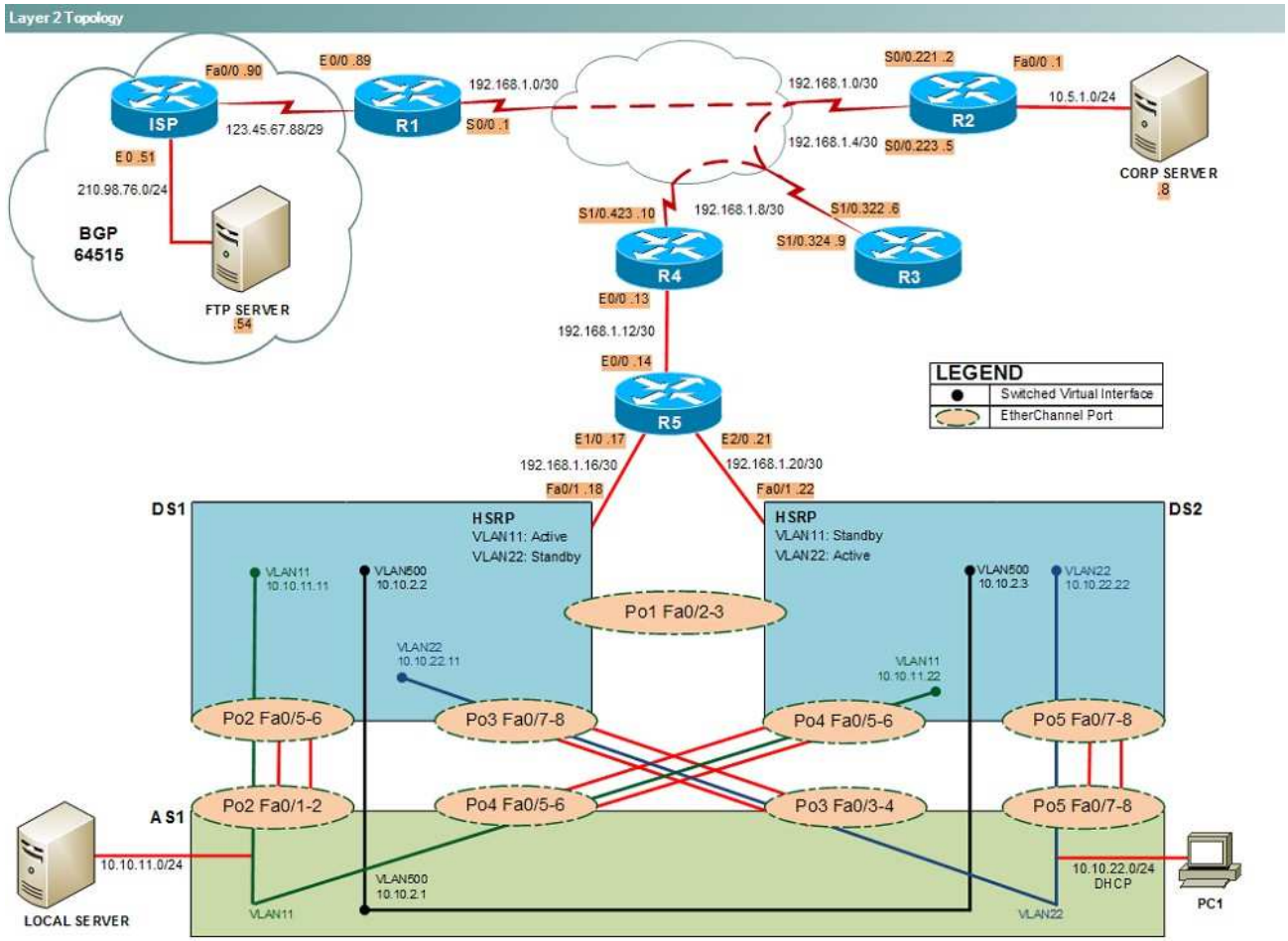
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

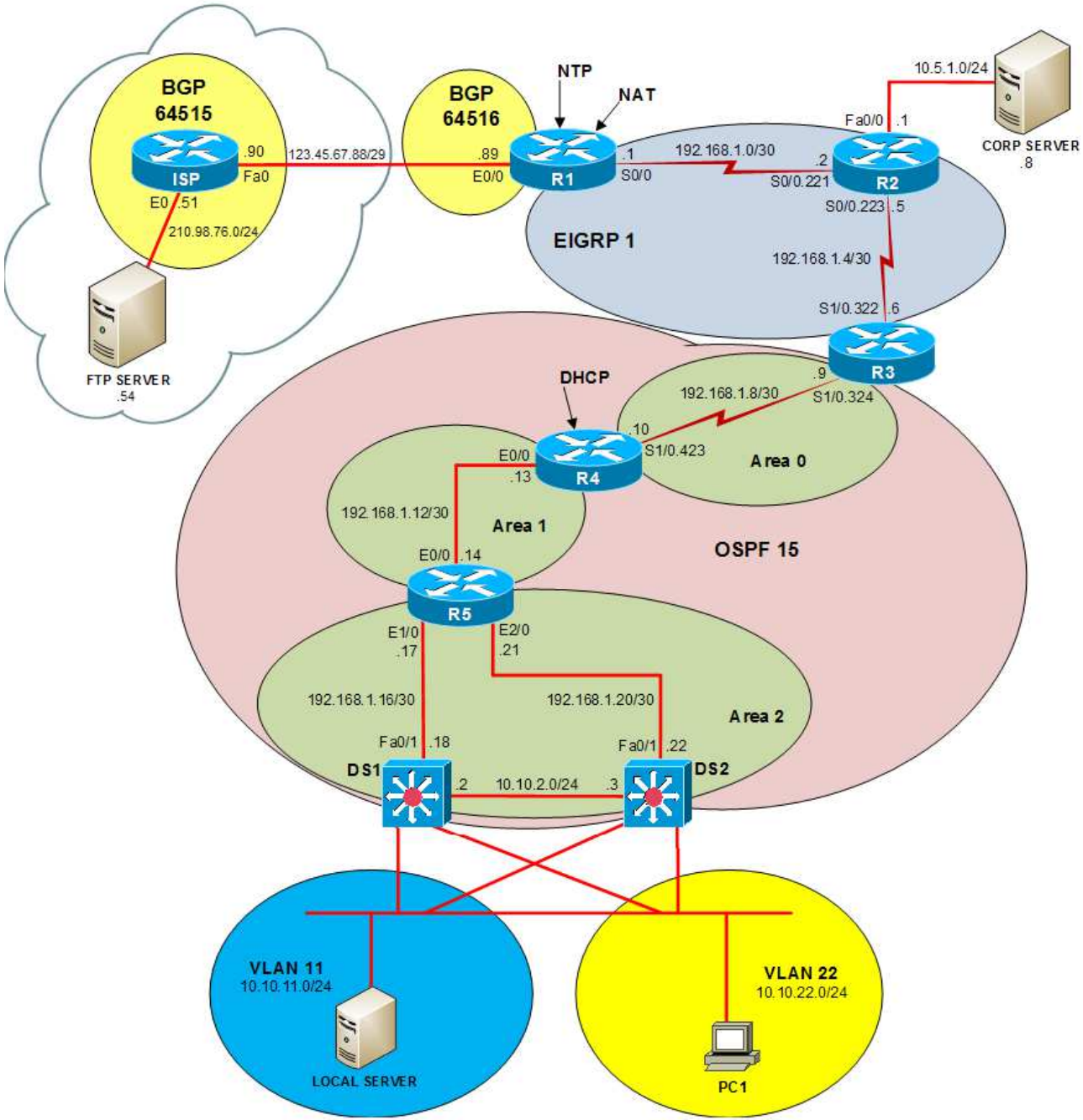
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

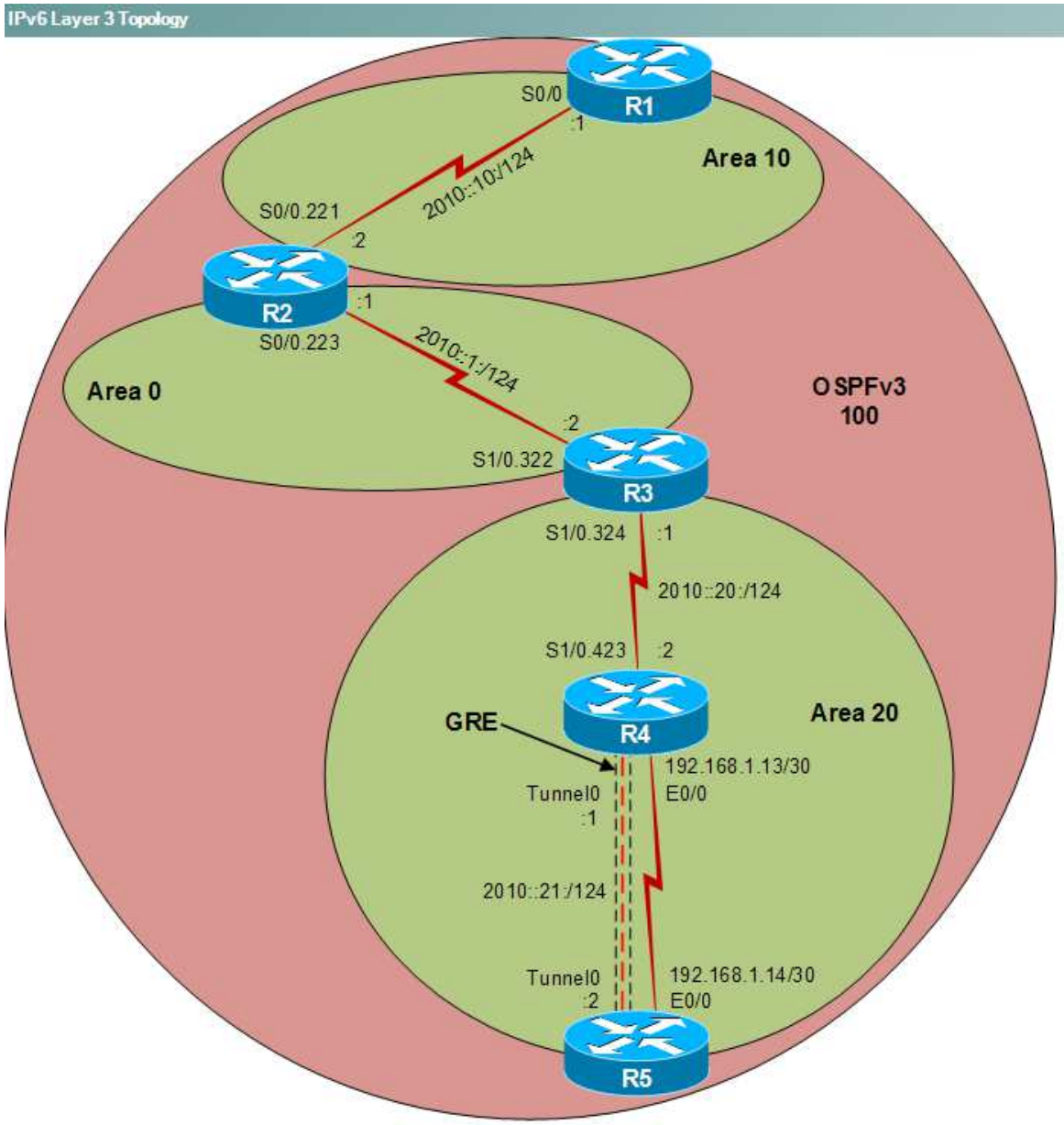
**Layer 2 Topology**




IPv4 layer 3 Topology

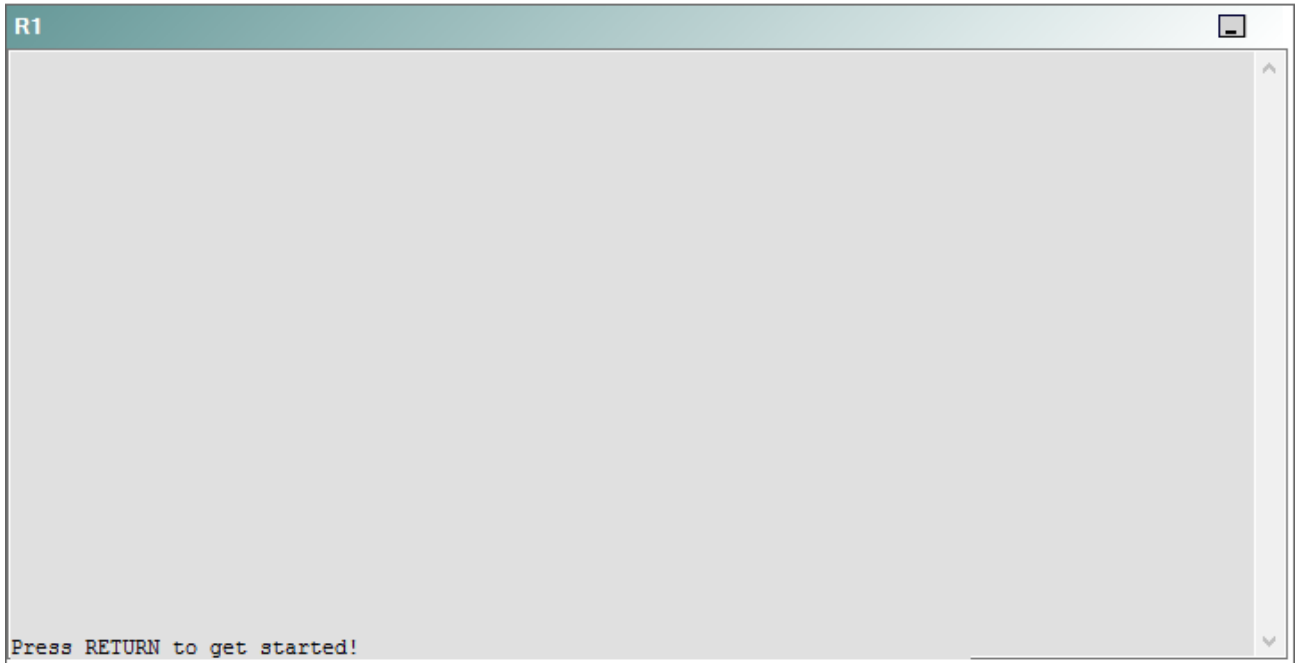

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

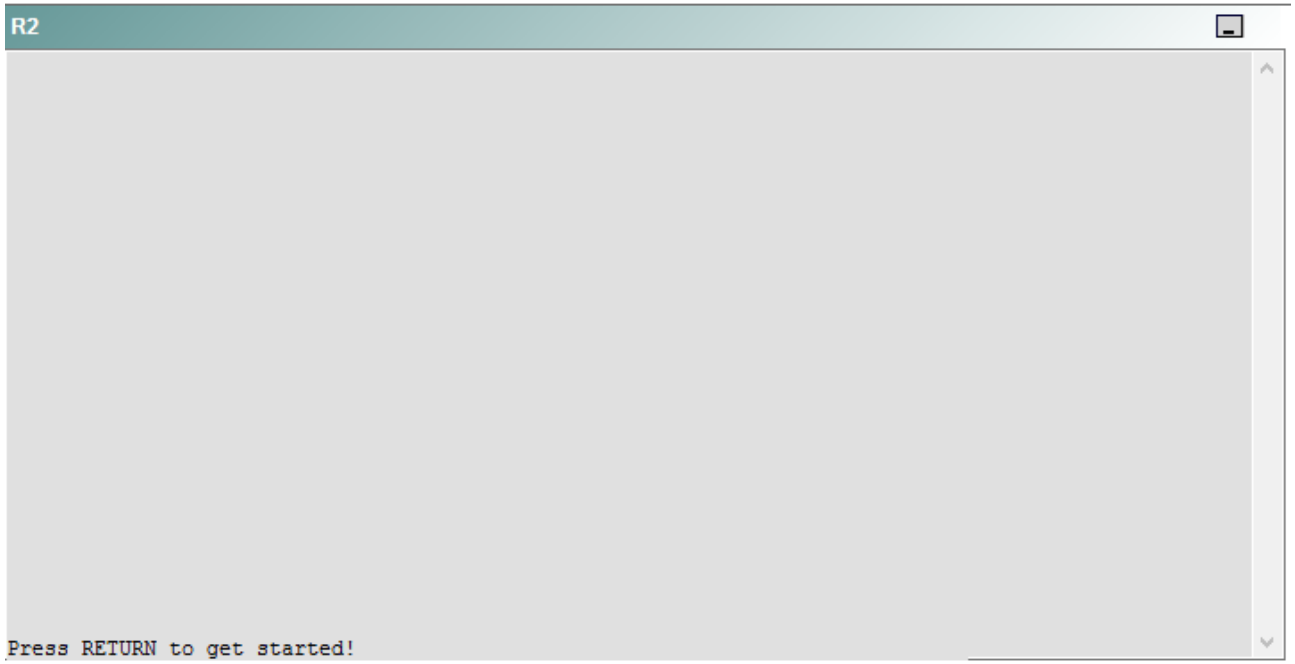



https://www.gratisexam.com/

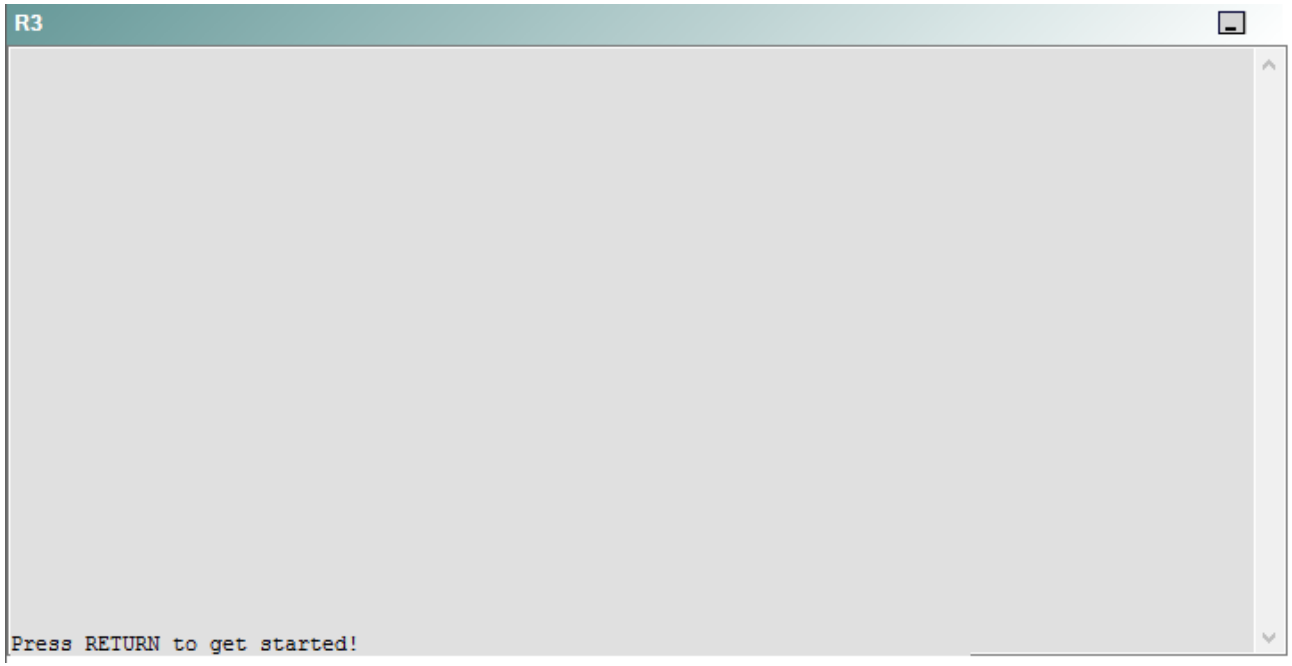
R1



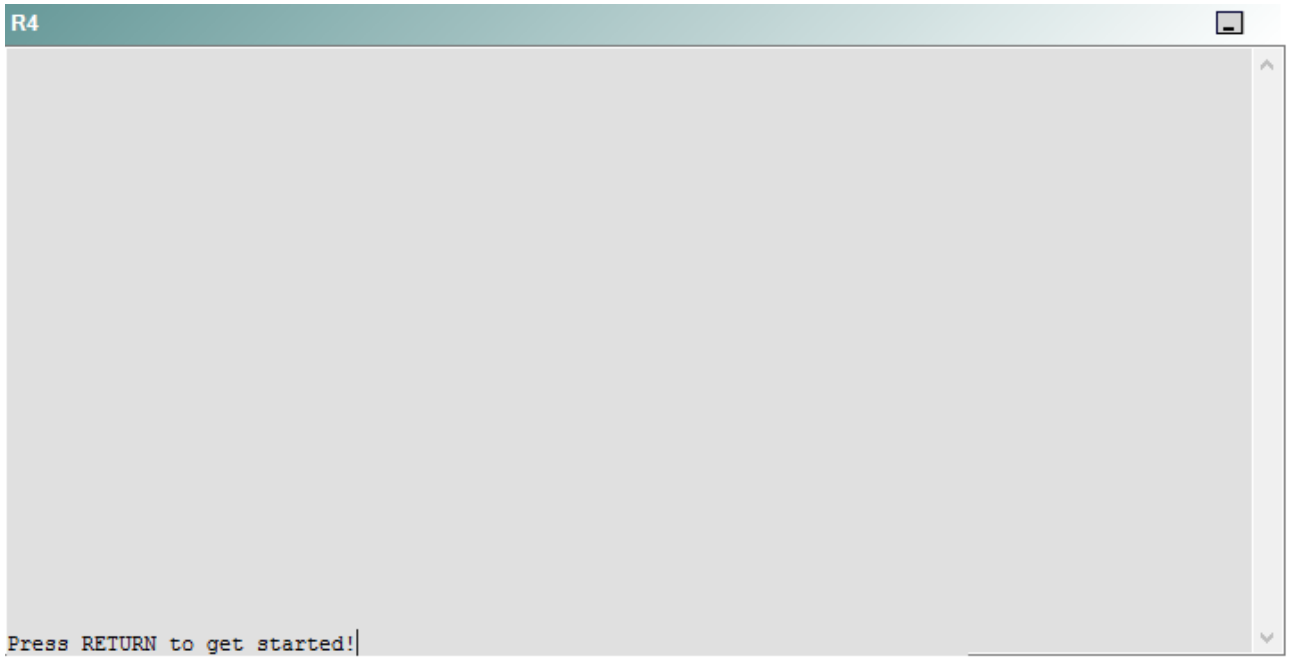

R2



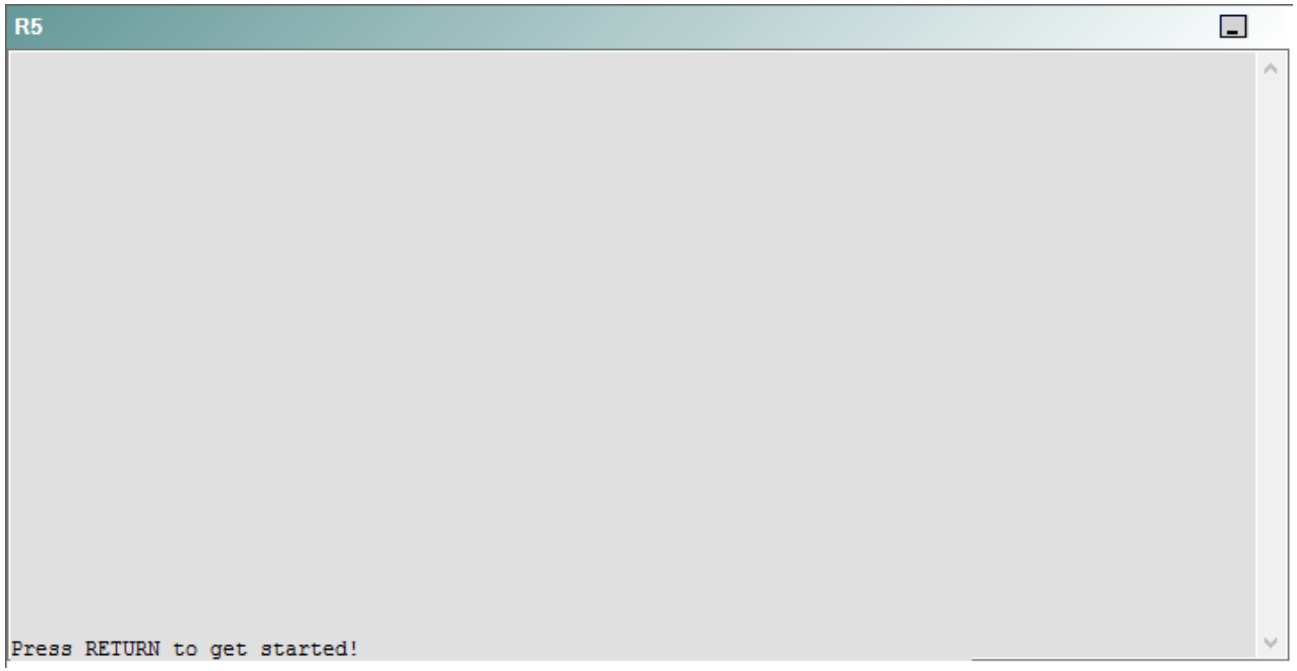

R3



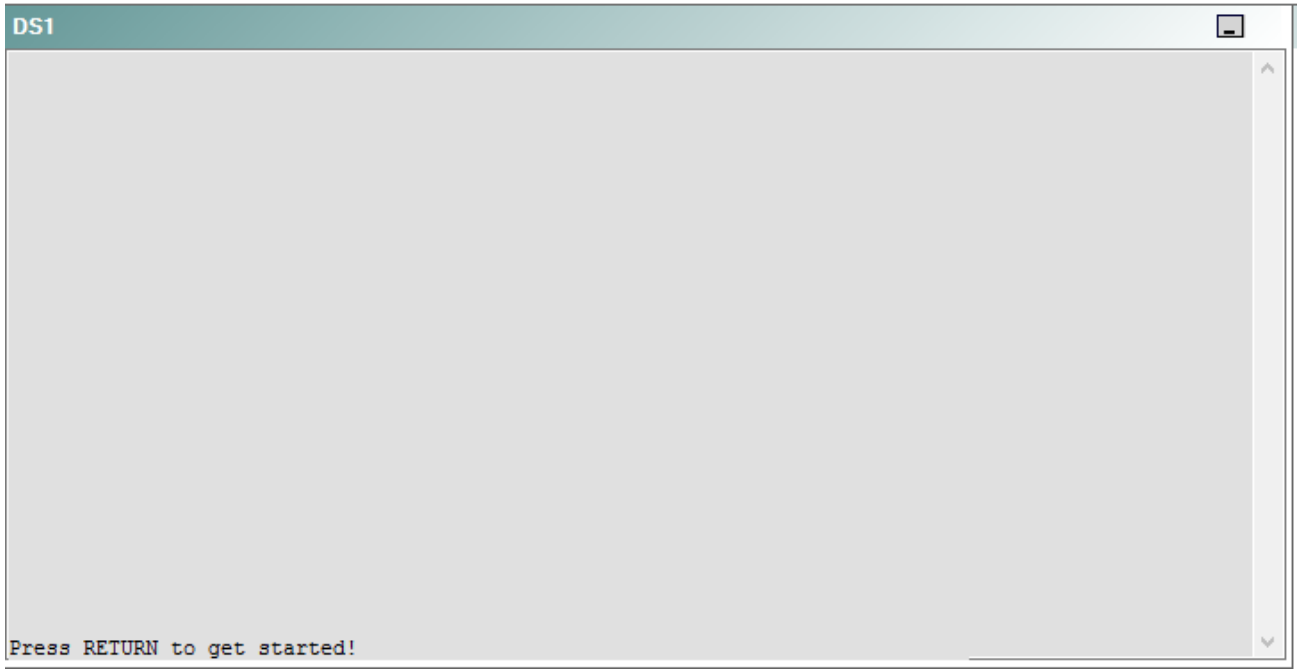

R4



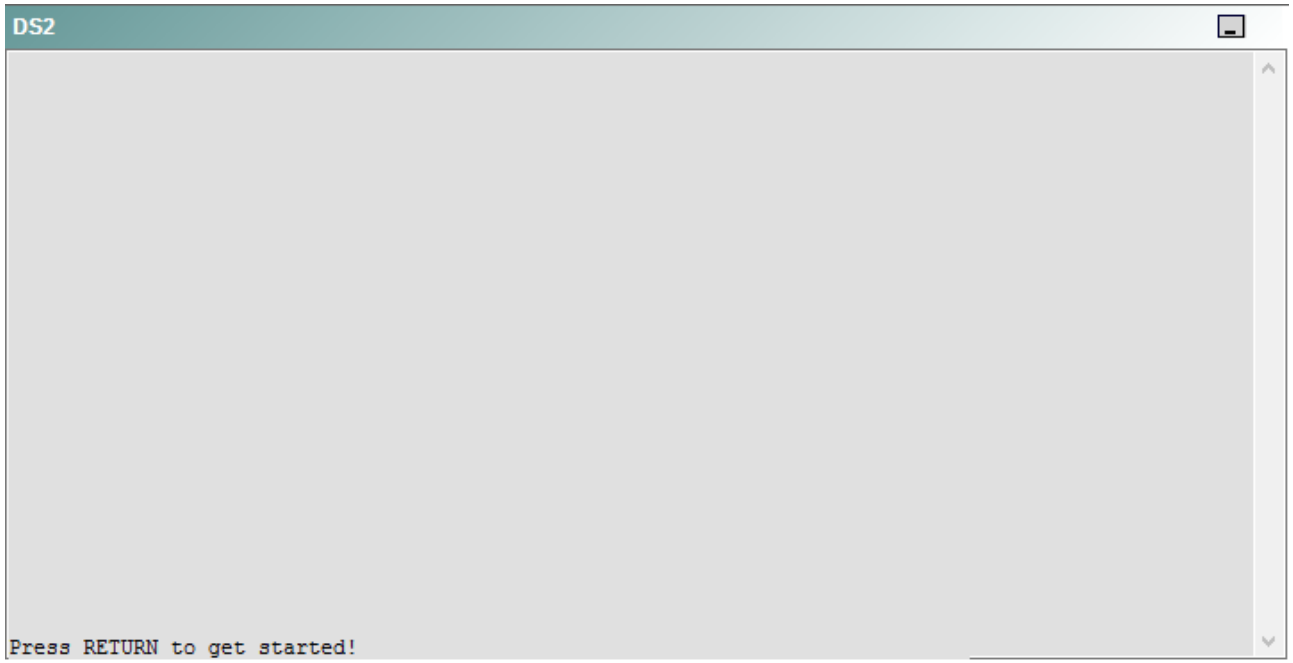

R5



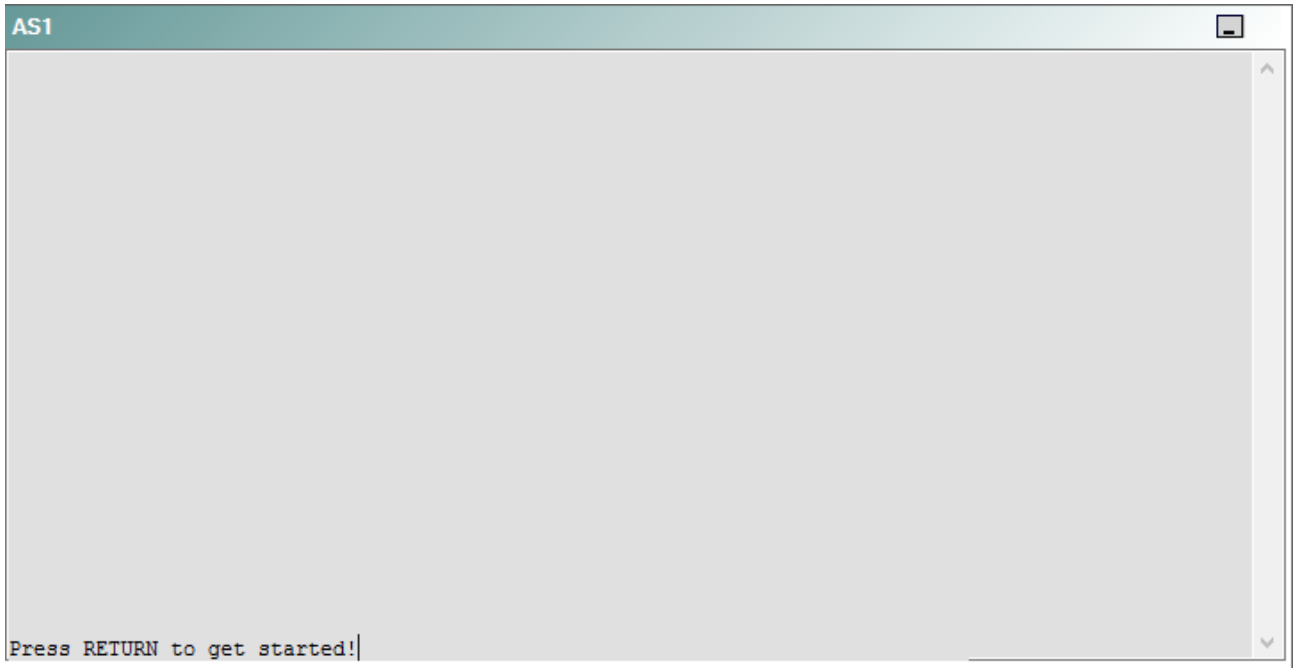

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to pong the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. changing the EIGRP AS number to 1
B. issuing the **metric weights 0 1 1 1 0 0** command
C. issuing the **metric weights 0 1 0 1 0 0** command
D. changing automatic summarization settings
E. issuing the **no poassive-interface S0/0.221** command
F. changing the EIGRP hold timer value
G. issuing the **ip addrss 192.168.1.5 255.255.255.252 secondary** command for the S0/0.223 interface

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

You should change the Enhanced Interior Gateway Routing Protocol (EIGRP) autonomous system (AS) number to 1 on R2. To determine which device is the source of the problem, you can issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from PC1 to the closest device and work your way up the network until communication is lost, or you can ping from PC1 to the farthest device and work your way back to PC1 until pings are successful.

Pings from PC1 to R3 are successful. However, pings from PC1 to R2 time out and fail. Pings from R2 to the S1/0.322 interface of R3 are successful, but pings from R2 to the S1/0.324 interface of R3 are not. Therefore, the problem likely exists on R2 or R3.

Once you have determined where connectivity is lost, you can begin to troubleshoot what is causing the problem. Issuing the **show ip eigrp neighbors** command on R2 reveals that R2 has no EIGRP neighbors. The following parameters must match for devices to establish an EIGRP neighbor relationship:

- K values
- AS numbers
- Subnet

In addition, EIGRP cannot establish an adjacency over a secondary IP address.

The **show ip eigrp neighbors** command indicates that R2 is trying to establish a neighbor relationship on EIGRP AS 10. R1 and R3 are trying to establish a neighbor relationship on AS1. Therefore, you should configure R2 to establish a neighbor relationship over AS 1. The AS number is established when the EIGRP process is started by issuing the **router eigrp** *as-number* command. If a router receives a hello packet that contains the same AS number as the AS number that is configured in the router, a neighbor relationship is established. If the AS values are different, the router ignores the packet and a neighbor relationship is not established.

You should not issue the **metric weights** command on any of the routers. The **metric weights** command is used to specify which K values are used to calculate the metric used by EIGRP. You can verify the K values on a router by issuing the **show ip protocols** command. Issuing the **show ip protocols** command on R1, R2, and R3 will show that all three routers are using the same K values, as displayed in the following output:

```
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
```

You need not change the EIGRP hello interval on any of the routers. The hello interval does not need to match for routers to establish an EIGRP neighbor adjacency. To modify the EIGRP hello interval, you would issue the **ip hello-interval eigrp** *as-number seconds* command in interface configuration mode. By default, the EIGRP hello interval is set to a value of 60 seconds for nonbroadcast multiaccess (NBMA) networks at 1.544 Mbps and slower and to a value of 5 seconds for all other networks.

You need not change the EIGRP hold timer on any of the routers. The hold timer does not need to match for routers to establish an EIGRP neighbor adjacency. To adjust the EIGRP hold timer, you would issue the **ip hold-time eigrp** *as-number seconds* command in interface configuration mode. The EIGRP hold timer should be set to three times the hello interval. Therefore, the hold timer is typically set to 15 seconds on high-bandwidth links and 180 seconds on low-bandwidth NBMA links by default.

You need not issue the **network 192.168.1.4 0.0.0.3** command on R2, because this command has already been issued. Additionally, you should not issue the **network 192.168.1.4 255.255.255.252** command on R2, because the **network** command uses wildcard masks, not subnet masks. A wildcard mask is basically an inverse subnet mask. To calculate the appropriate wildcard mask, you should subtract the subnet mask from 255.255.255.255. For example, the 192.168.1.4 network has a /30 subnet mask, which is 255.255.255.252. Subtracting 255.255.255.252 from 255.255.255.255 yields a wildcard mask of 0.0.0.3.

You need not issue the **no passive-interface S0/0.211** command on R2, because the S0/0.221 interface of R2 is not configured as a passive interface. Configuring an interface as a passive interface blocks EIGRP and Open Shortest Path First (OSPF) hello packets, which prevents the interface from sending or receiving routing updates. Issuing the **passive-interface** *interface* command configures a single interface as a passive interface. Issuing the **passive-interface default** command configures all interfaces to be a passive interfaces except those that are specified within **no passive-interface** *interface* commands.

You need not modify automatic summarization settings on any of the routers. The summarization settings currently configured on the routers are not preventing PC1 from reaching the external server at 210.98.76.54.

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html
https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/21324-trouble-eigrp.html

**QUESTION 30**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

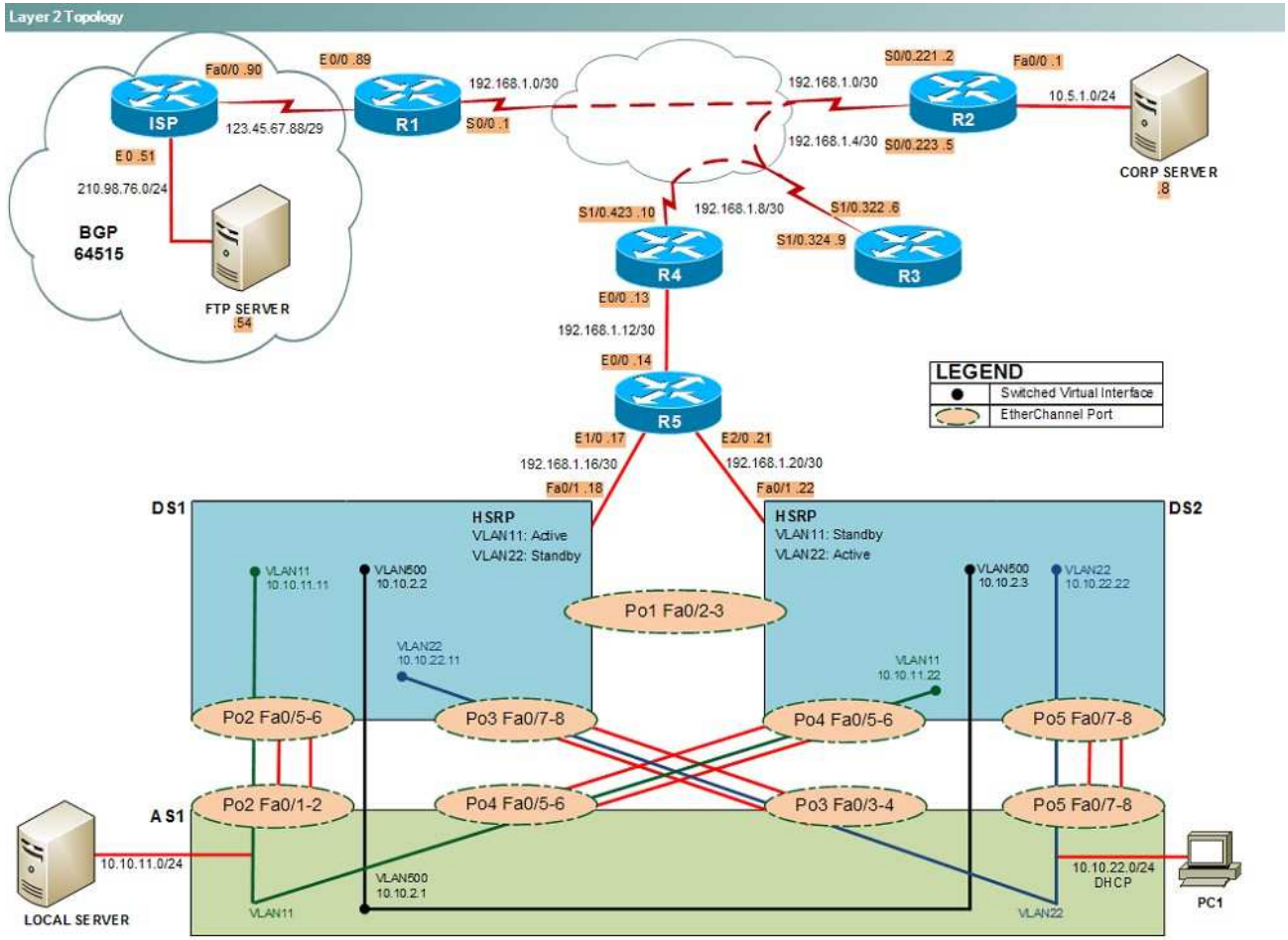
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

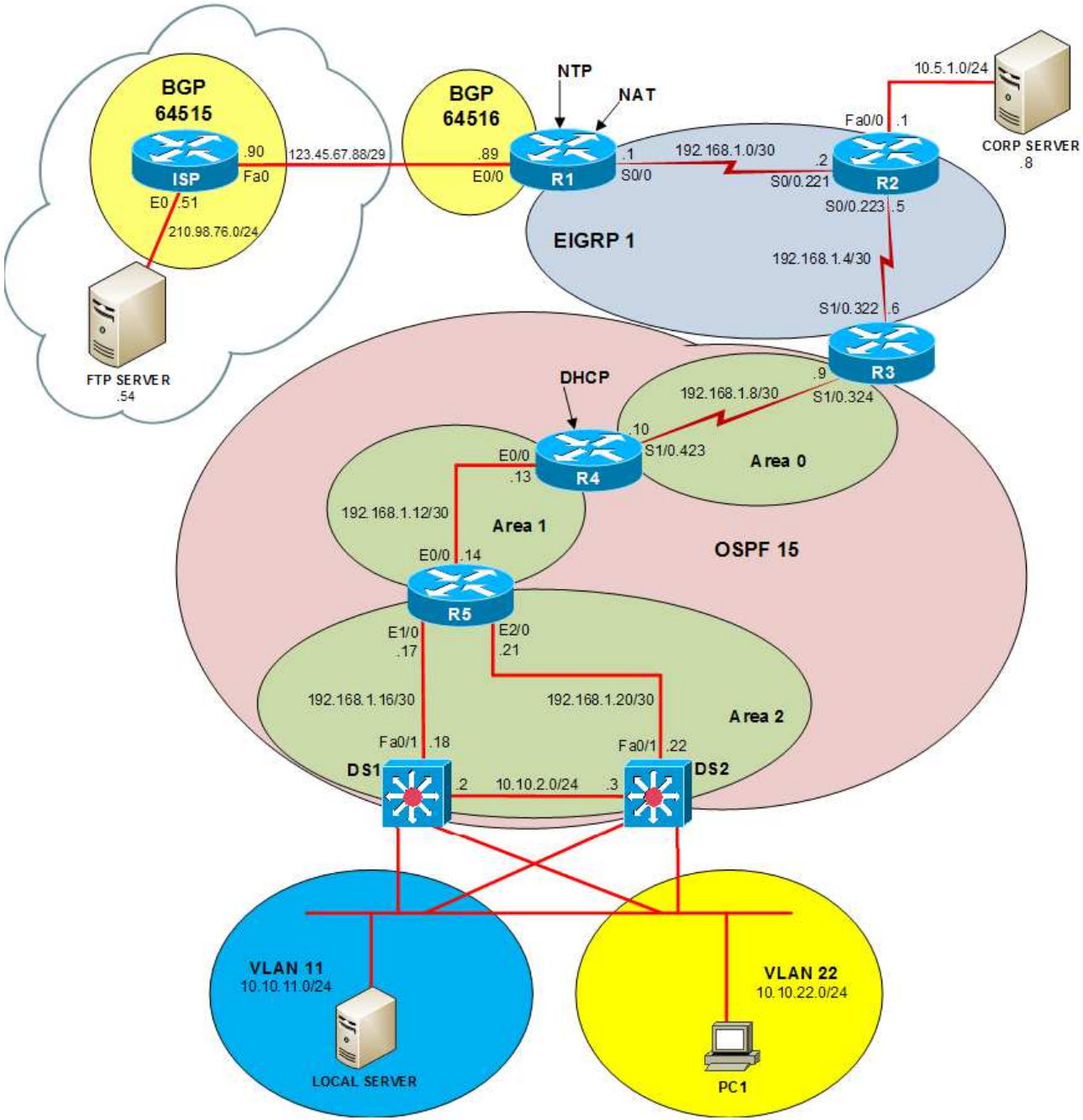
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

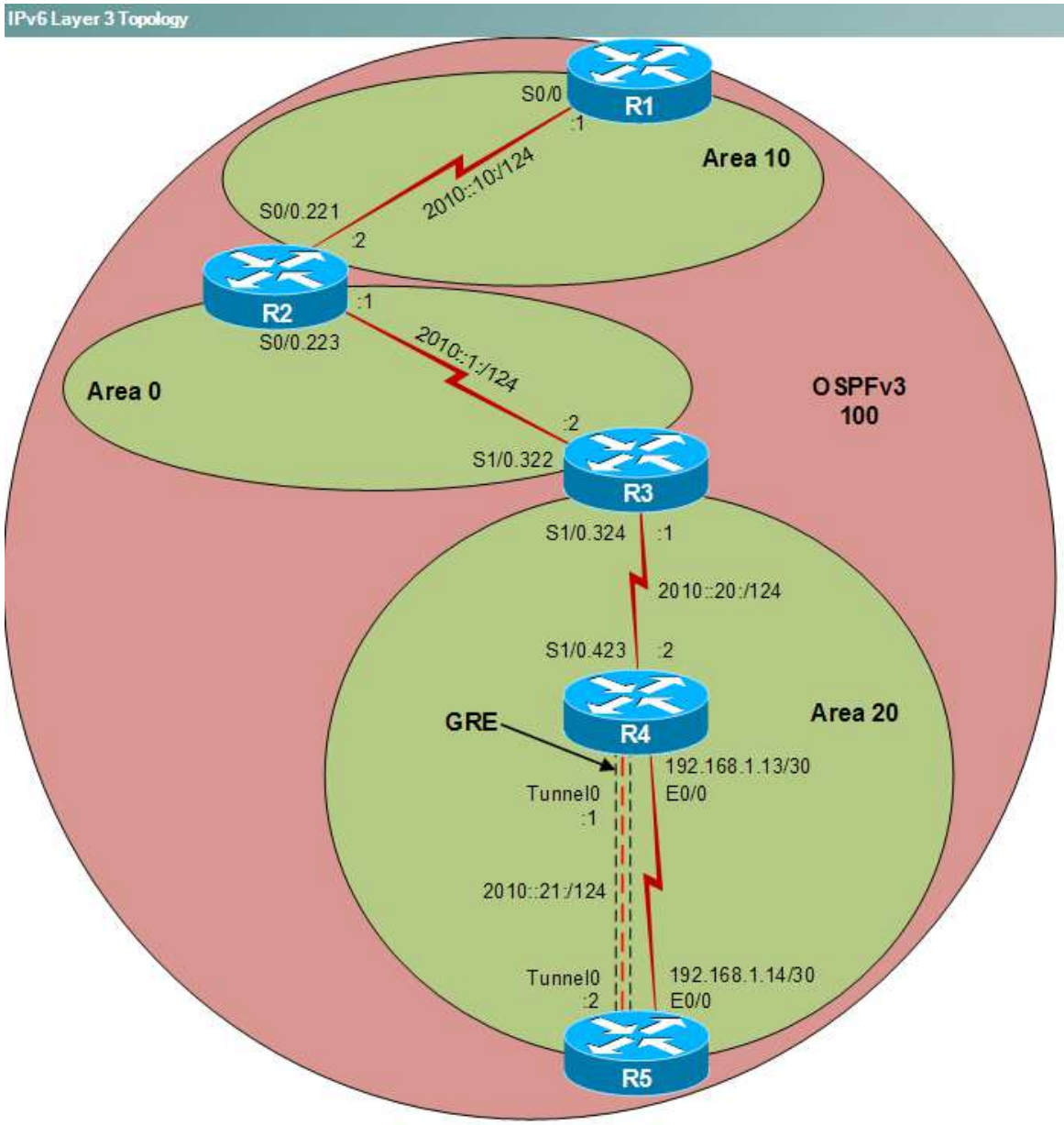
**Layer 2 Topology**



IPv4 layer 3 Topology

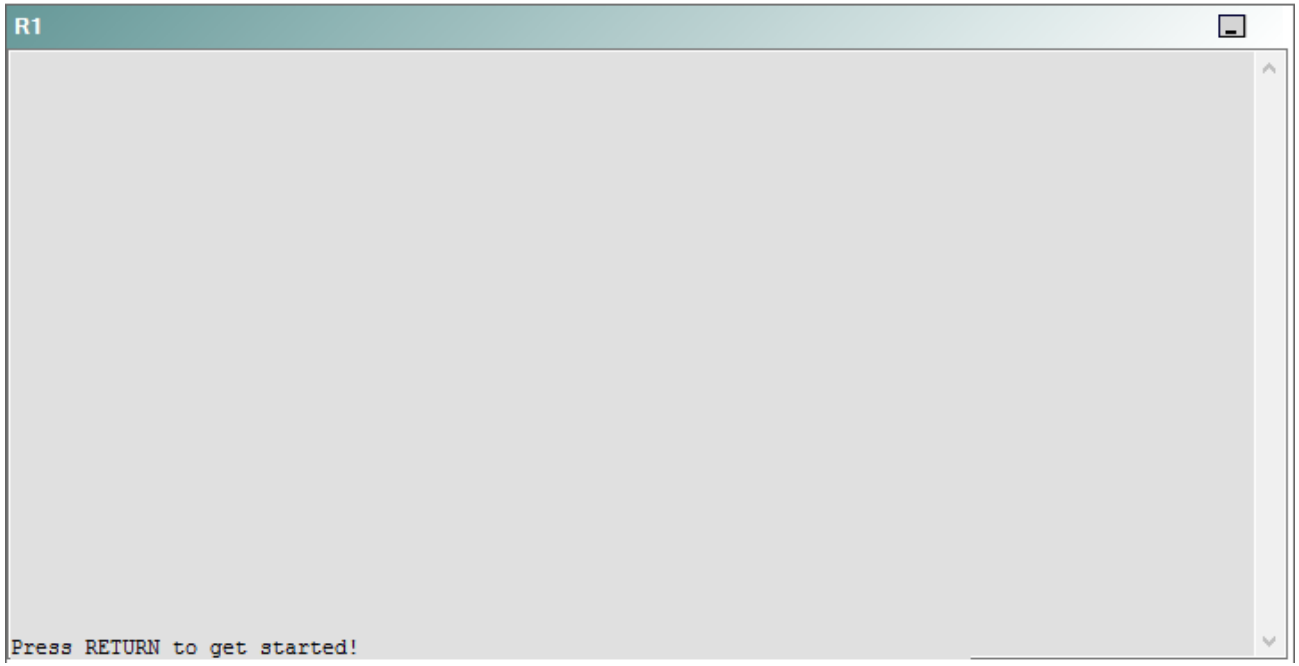

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

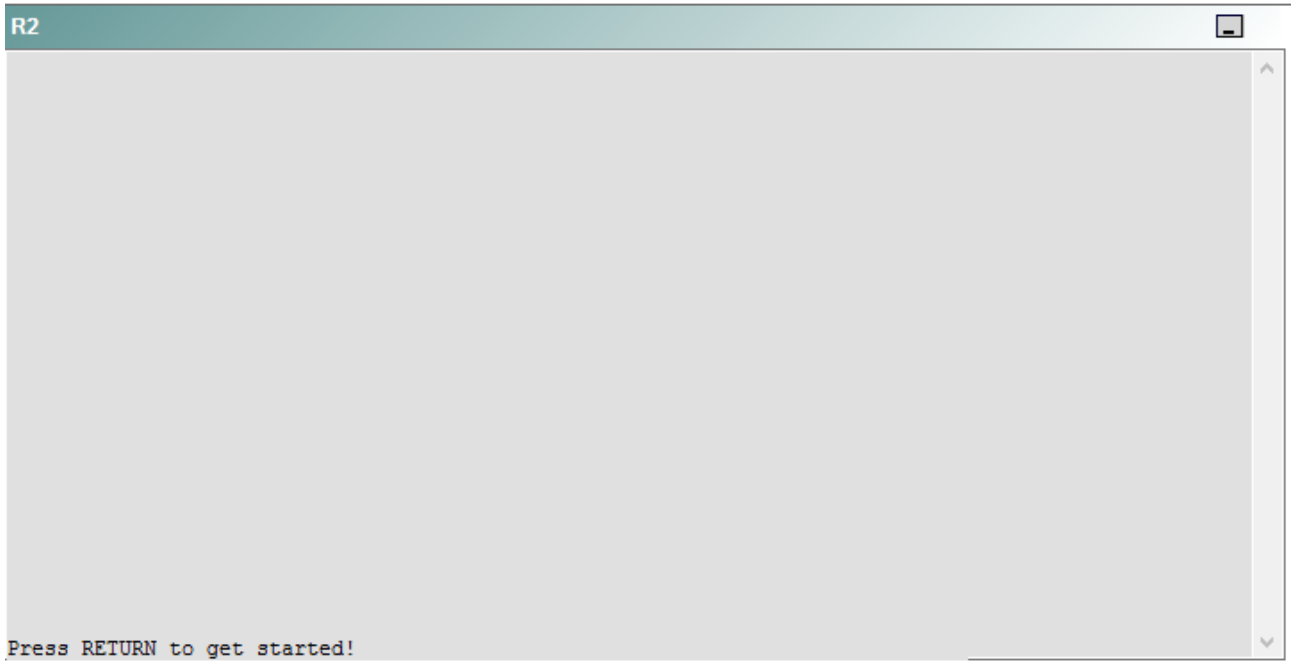



https://www.gratisexam.com/

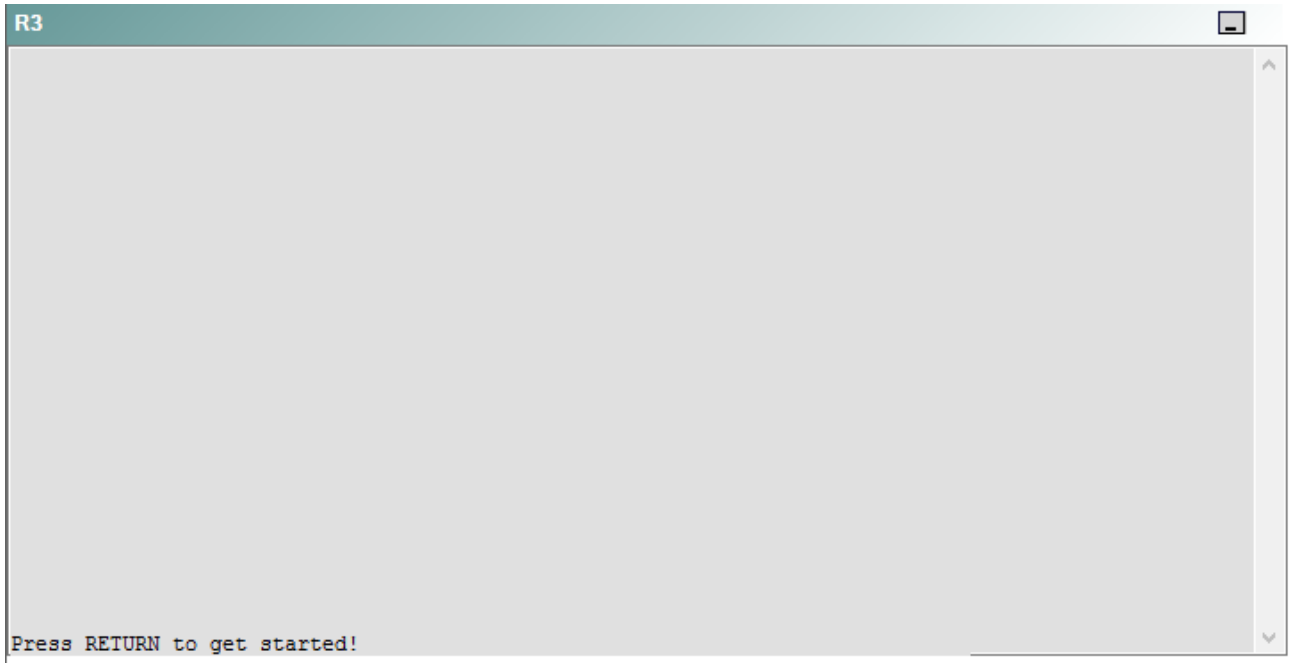
R1



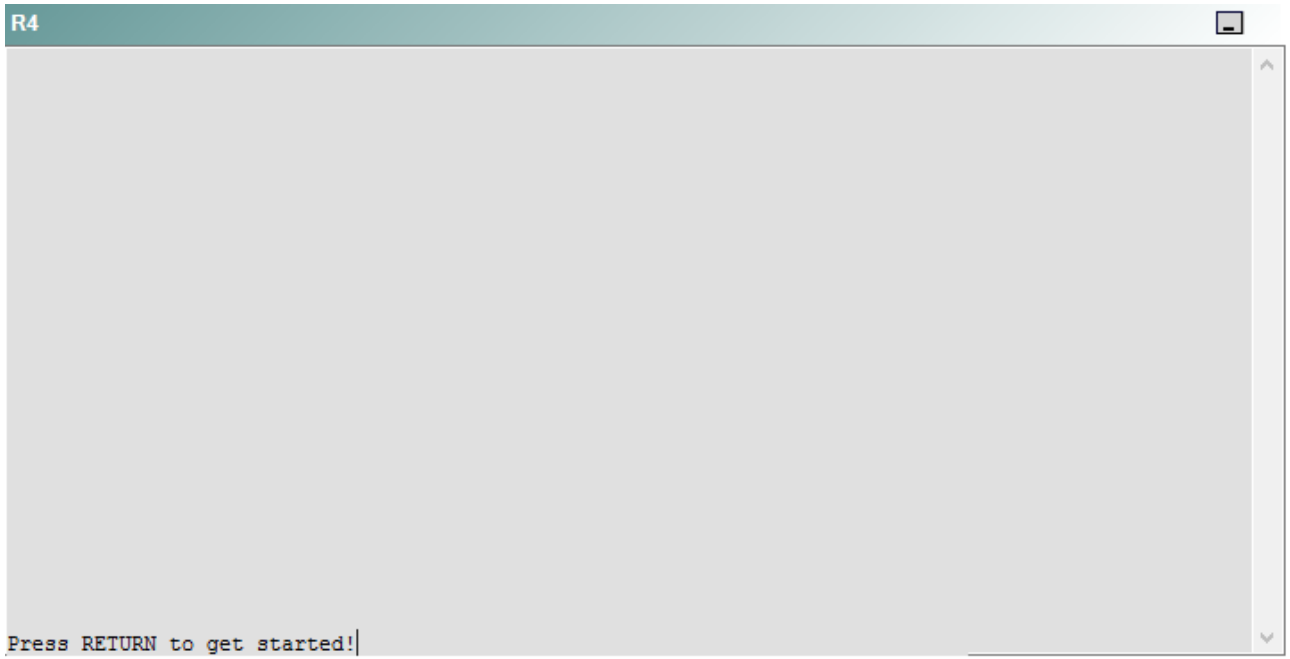

R2



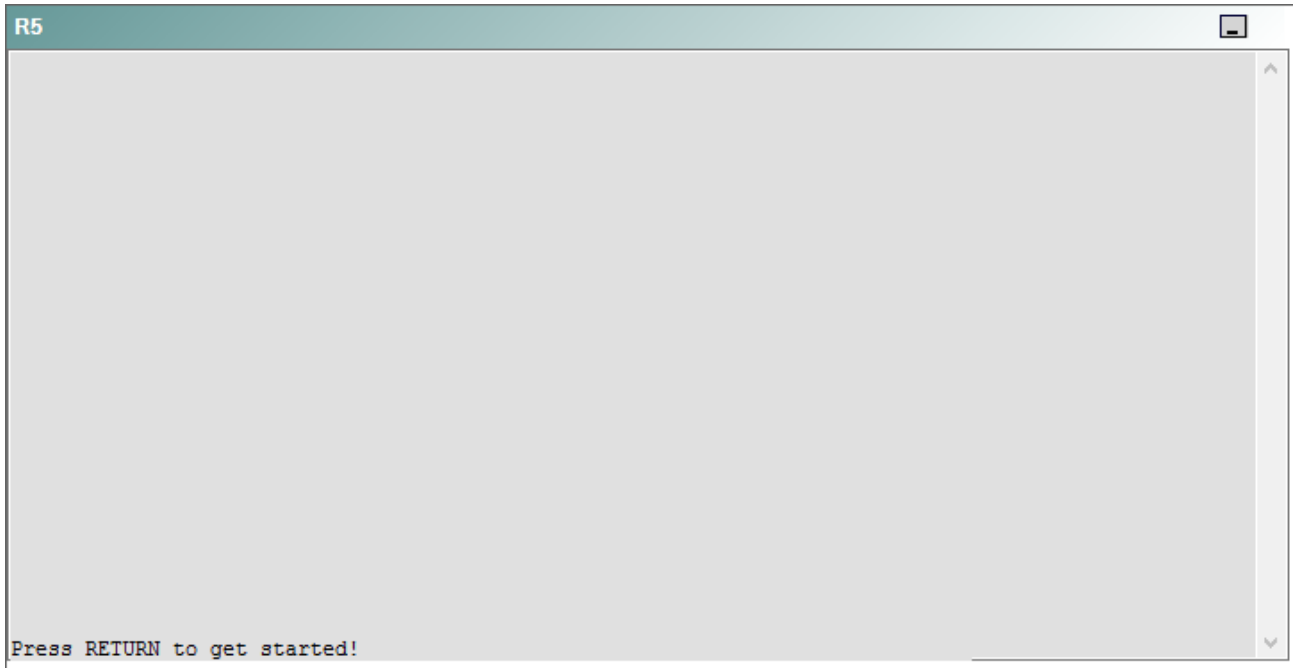

R3



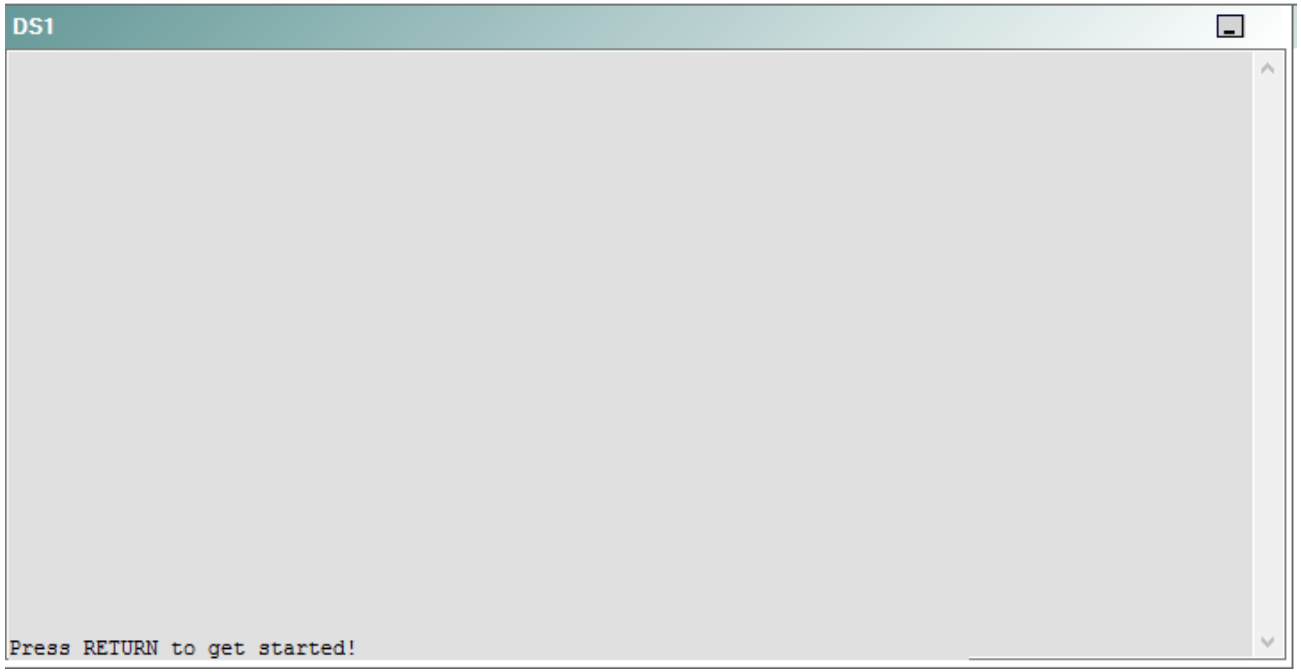

R4



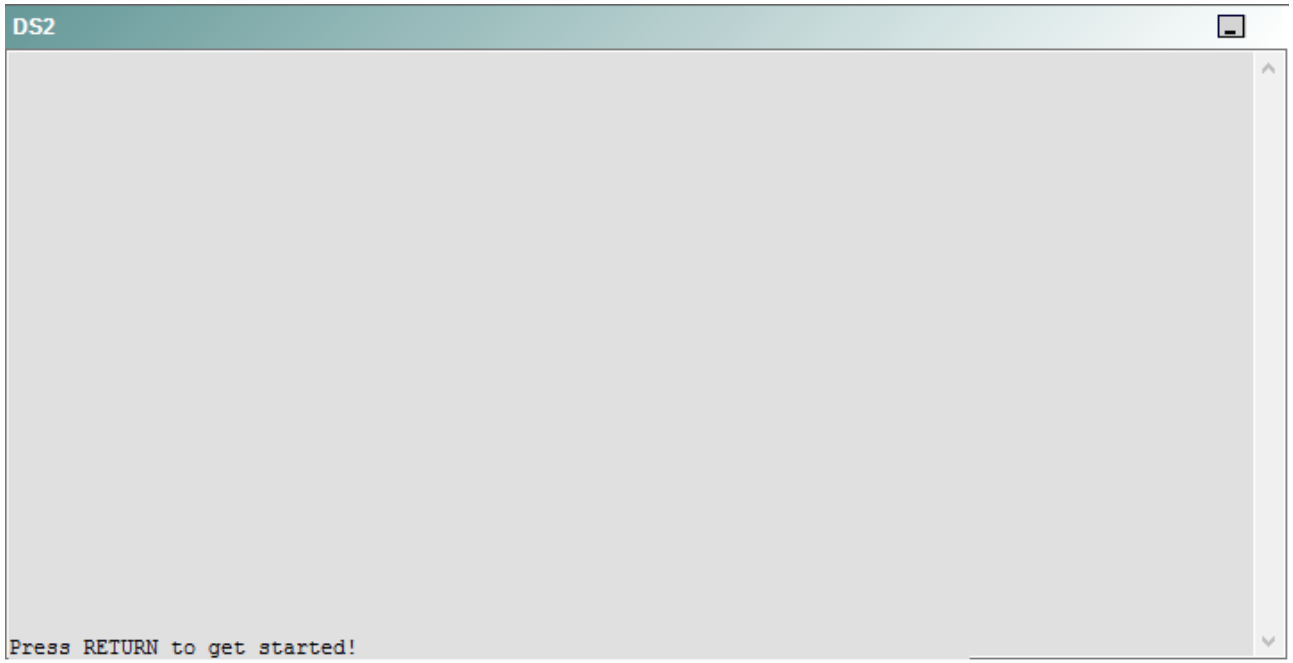

R5



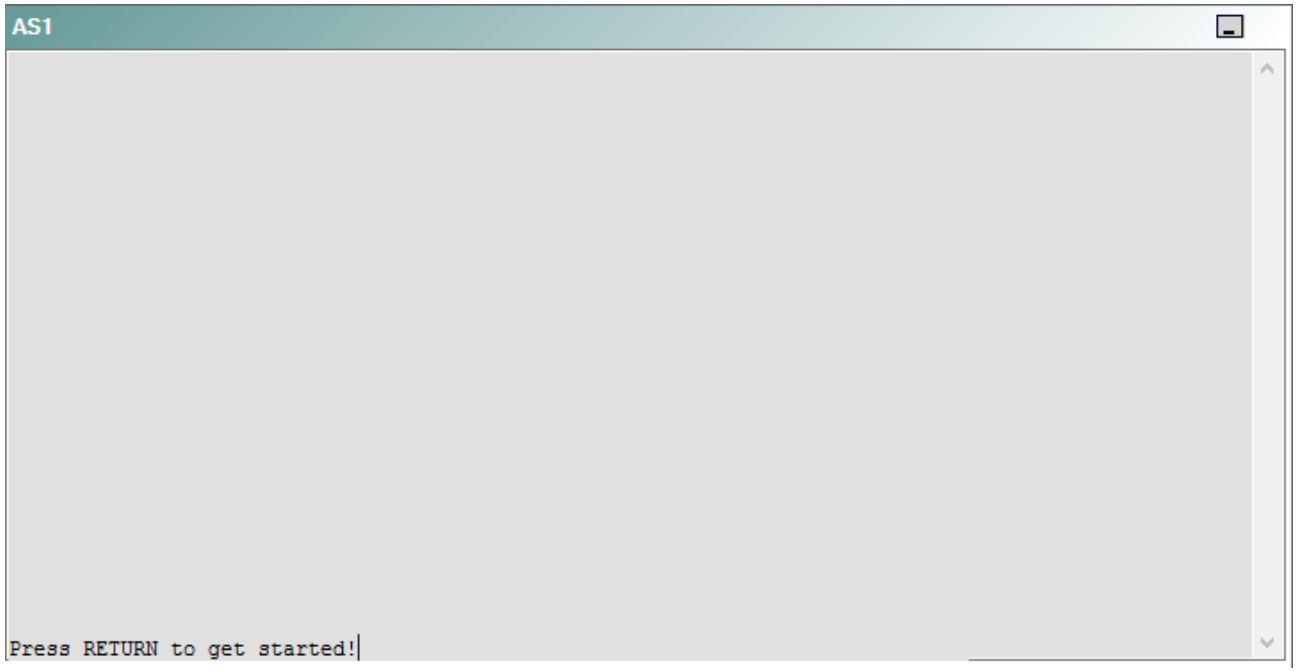

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that R5 is no longer able to ping the IPv6 address 2000::10:1 on R1.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 31**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

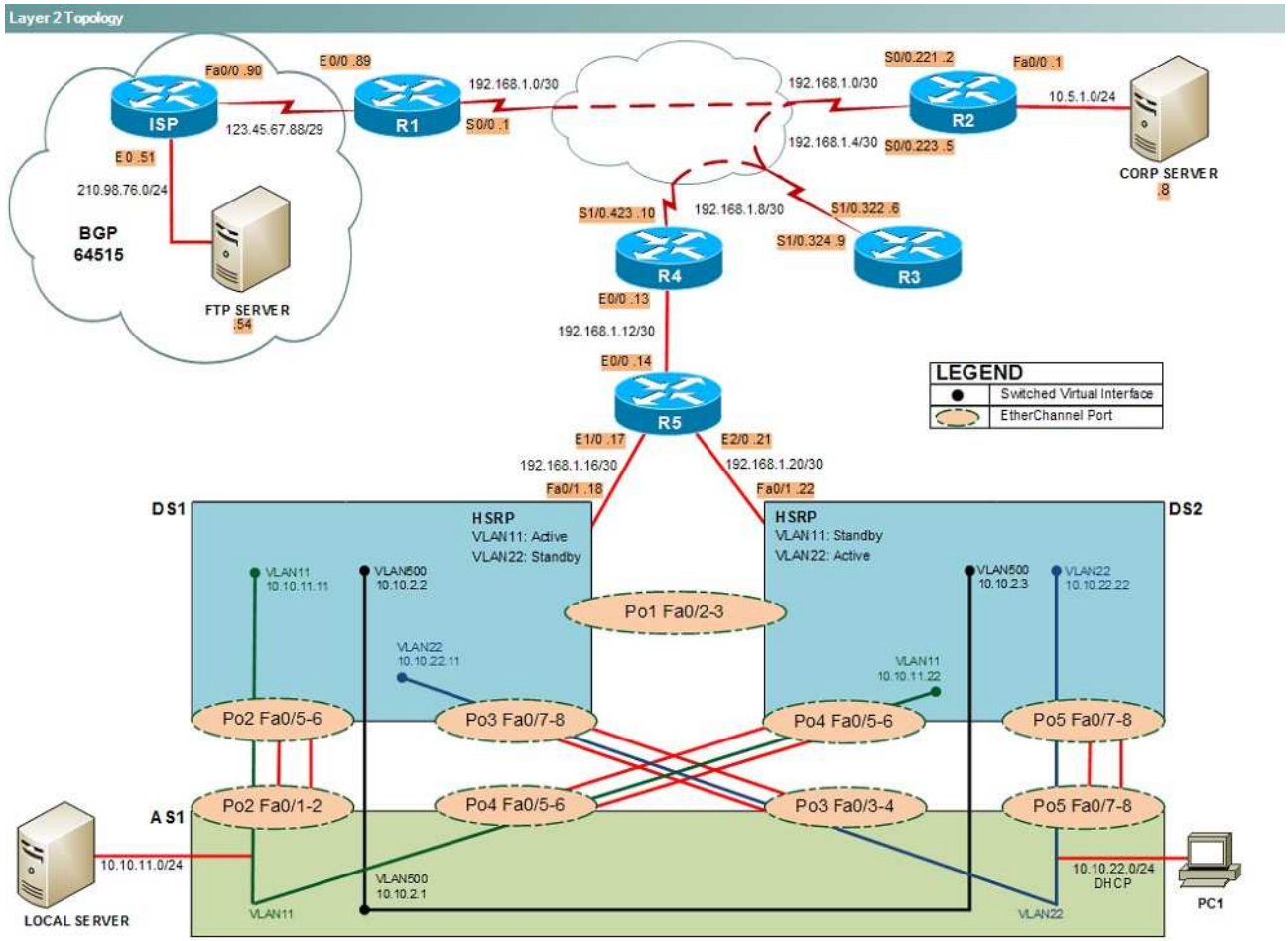
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

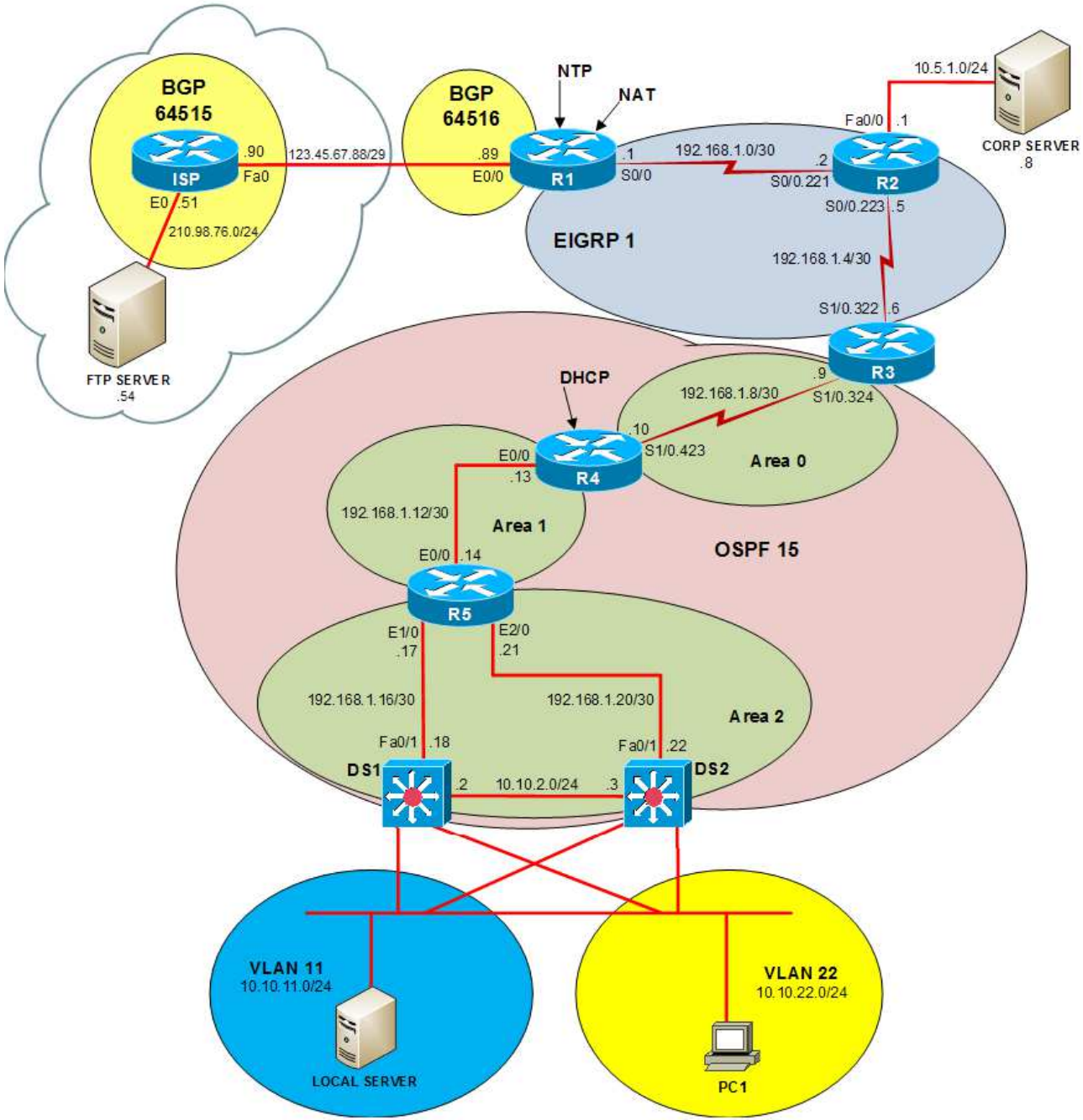
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

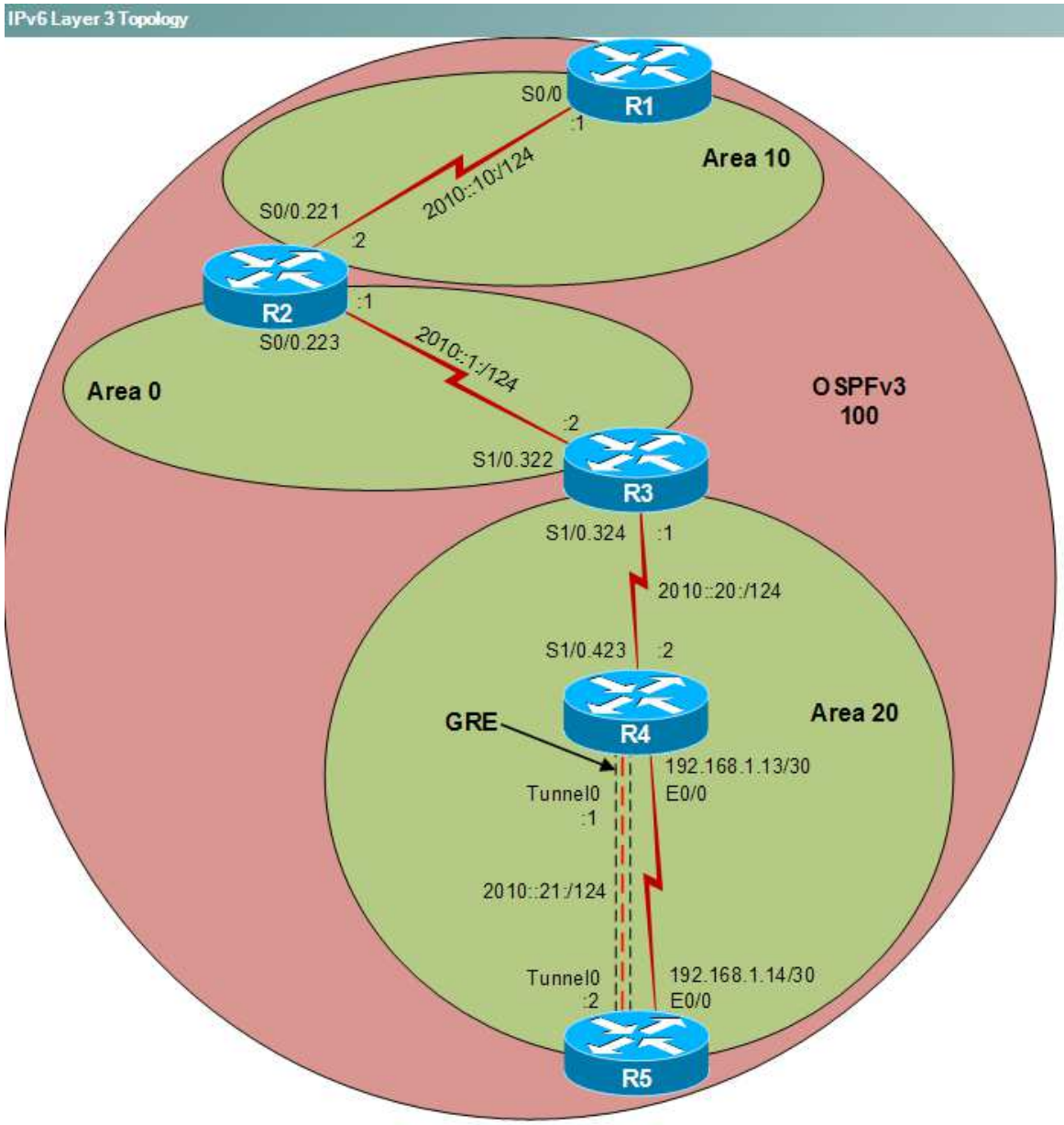
**Layer 2 Topology**




IPv4 layer 3 Topology

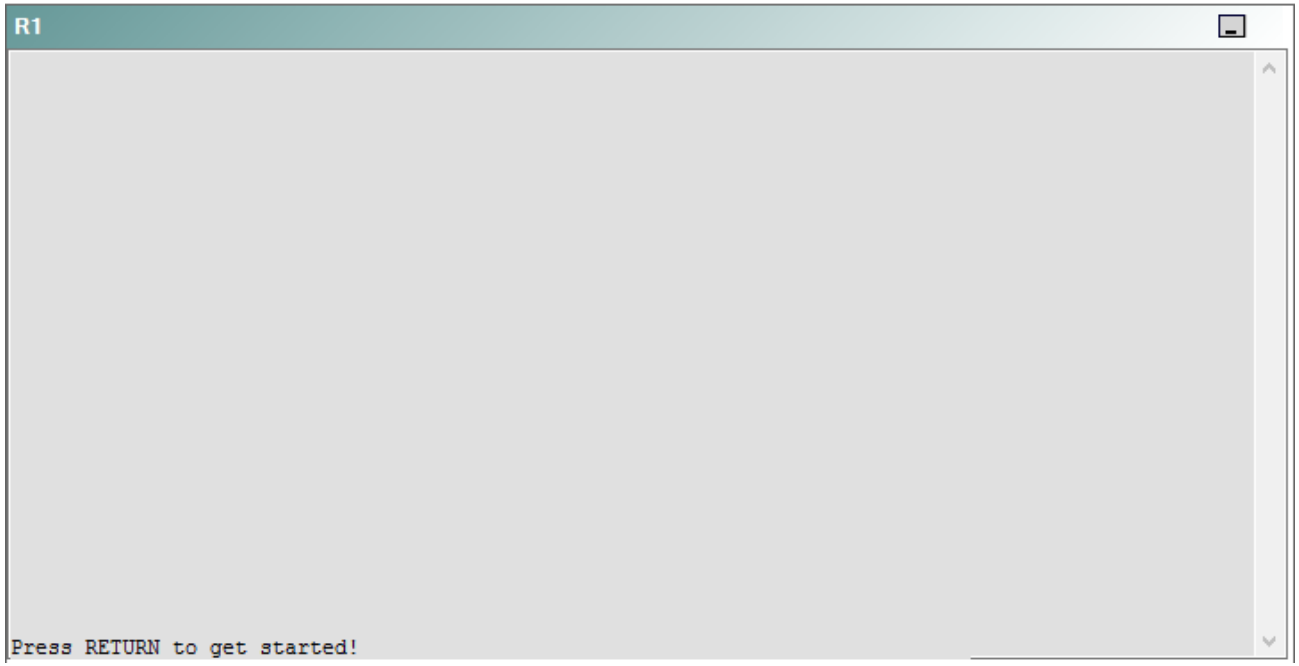

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

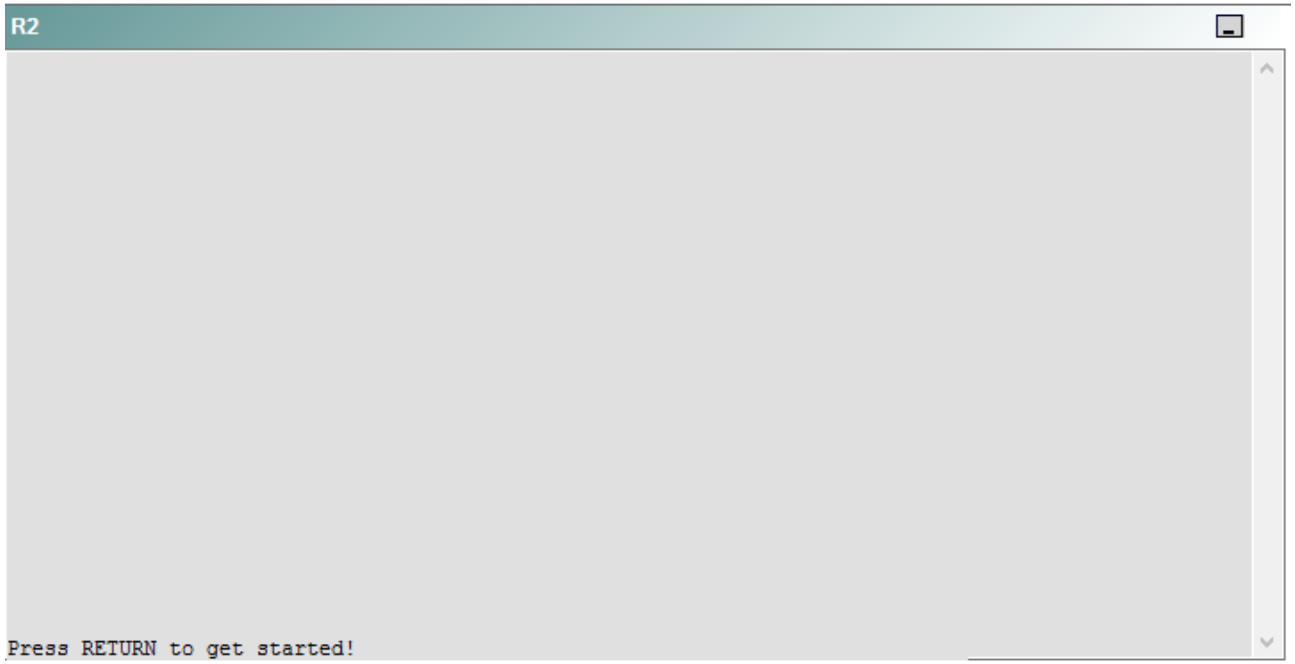



https://www.gratisexam.com/

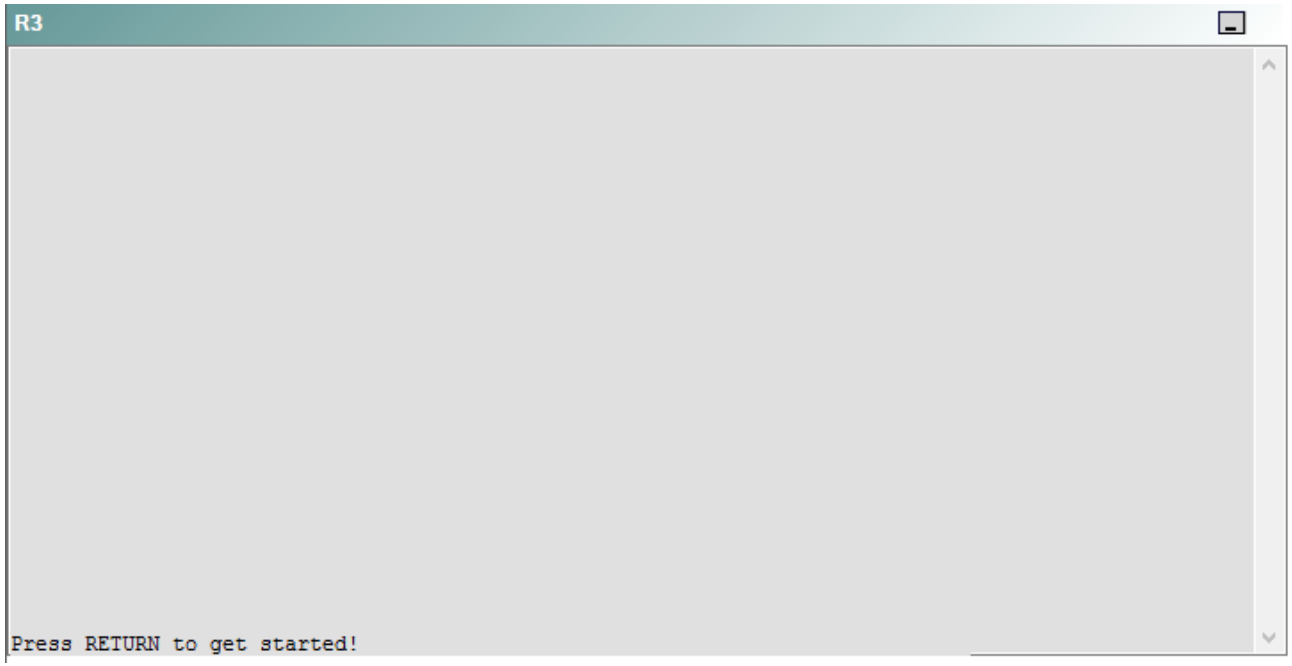
R1



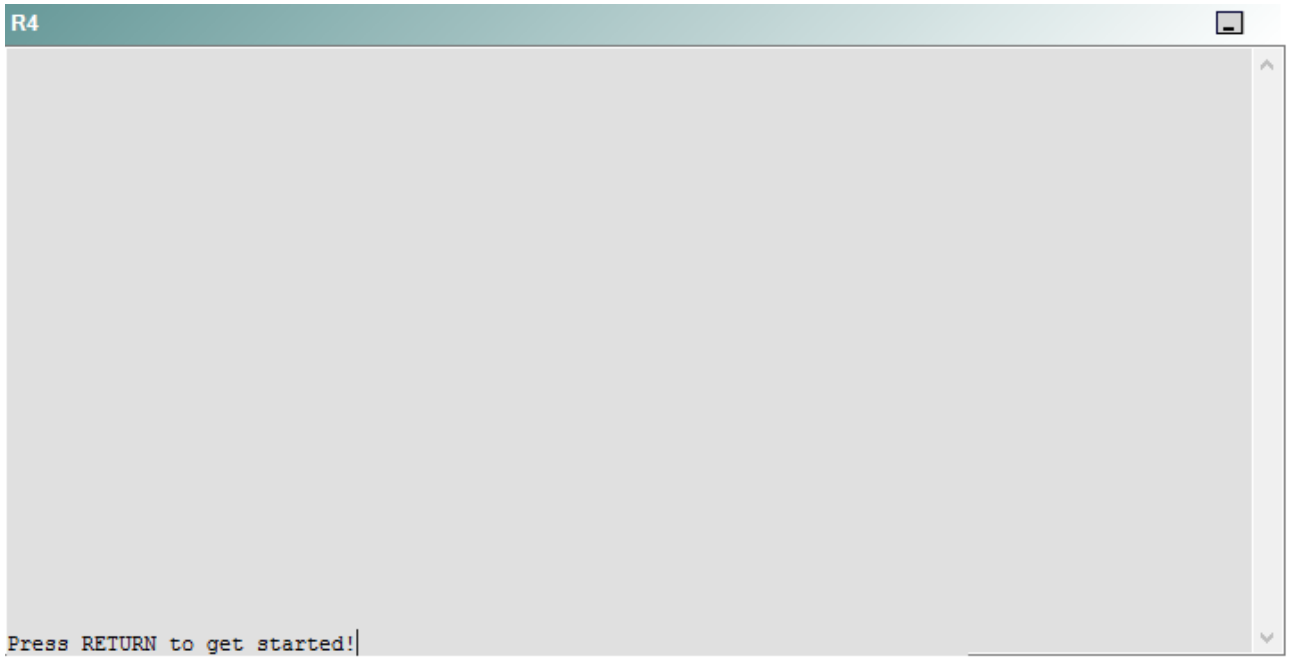

R2



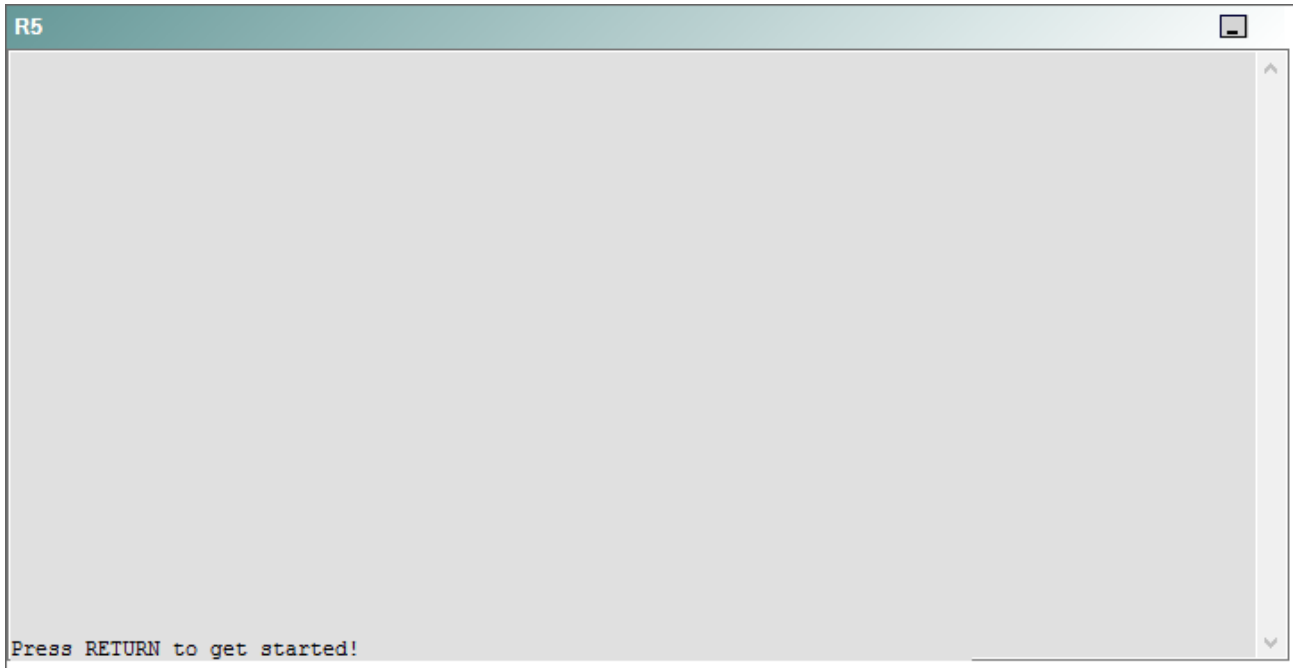

R3



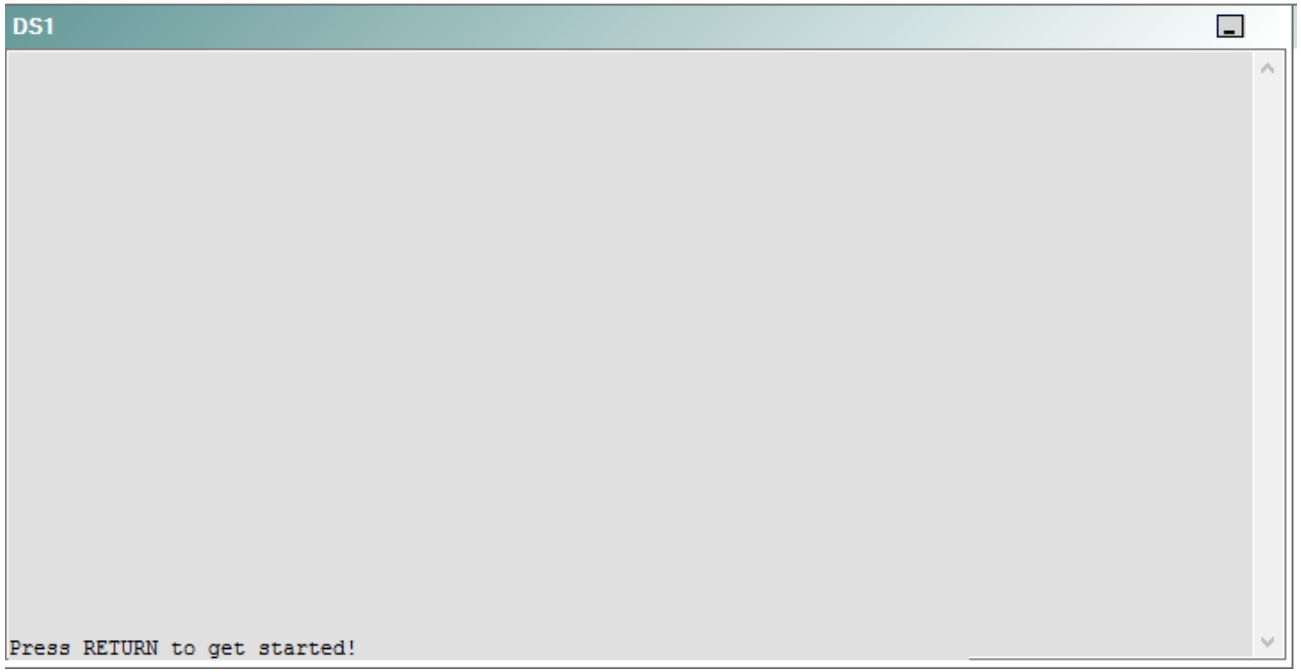

R4



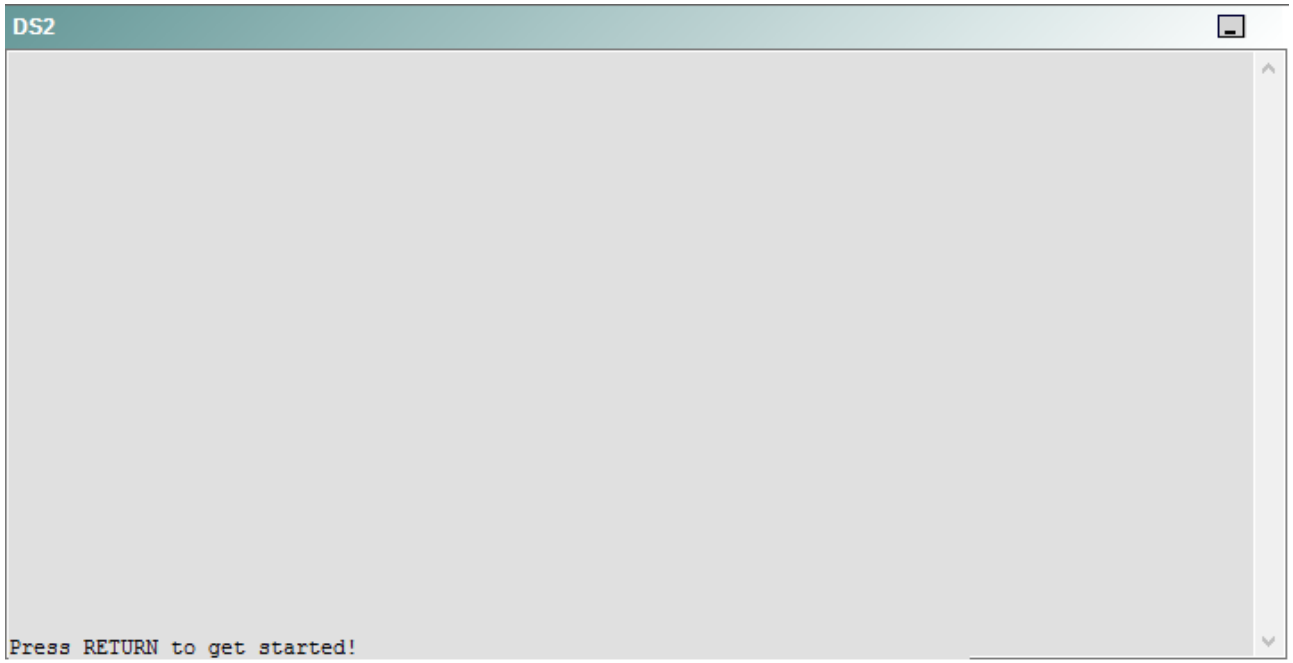

R5



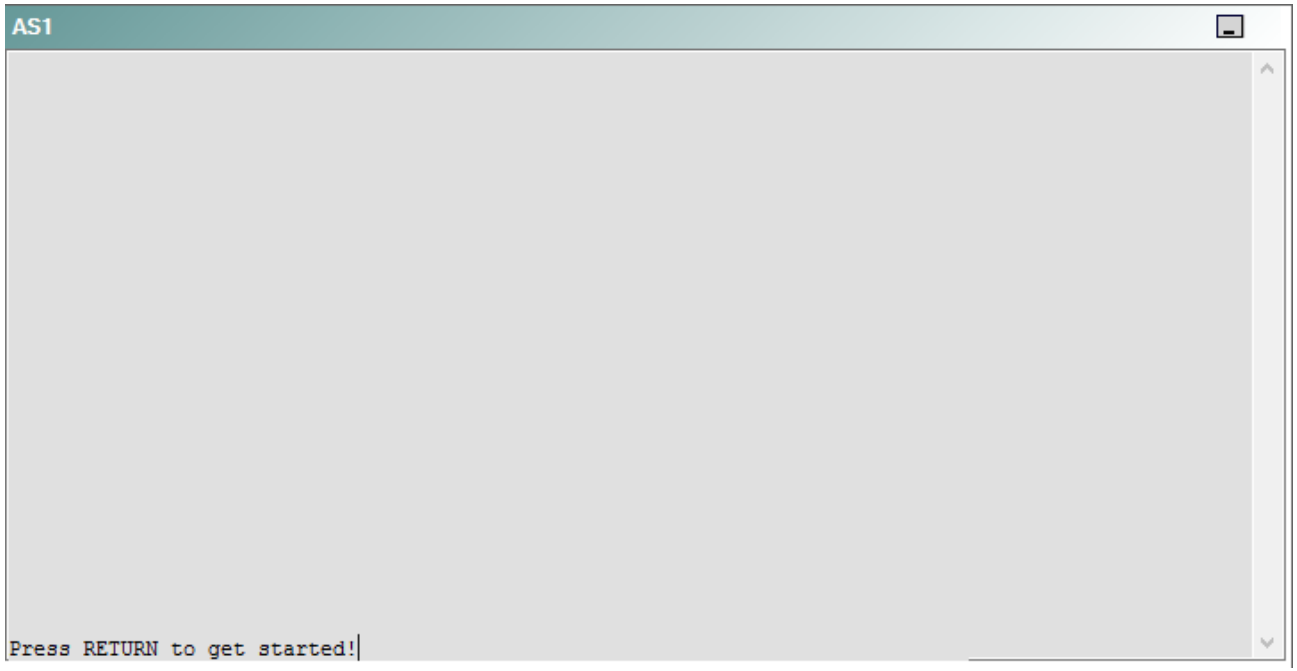

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that R5 is no longer able to ping the IPv6 address 2000::10:1 on R1.

Which of the following technologies is the source of the problem?

A. NTP
B. DHCP
C. BGP
D. OSPFv3
E. EIGRP
F. redistribution
G. layer 3 addressing
H. layer 3 security
I. interface

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 32**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

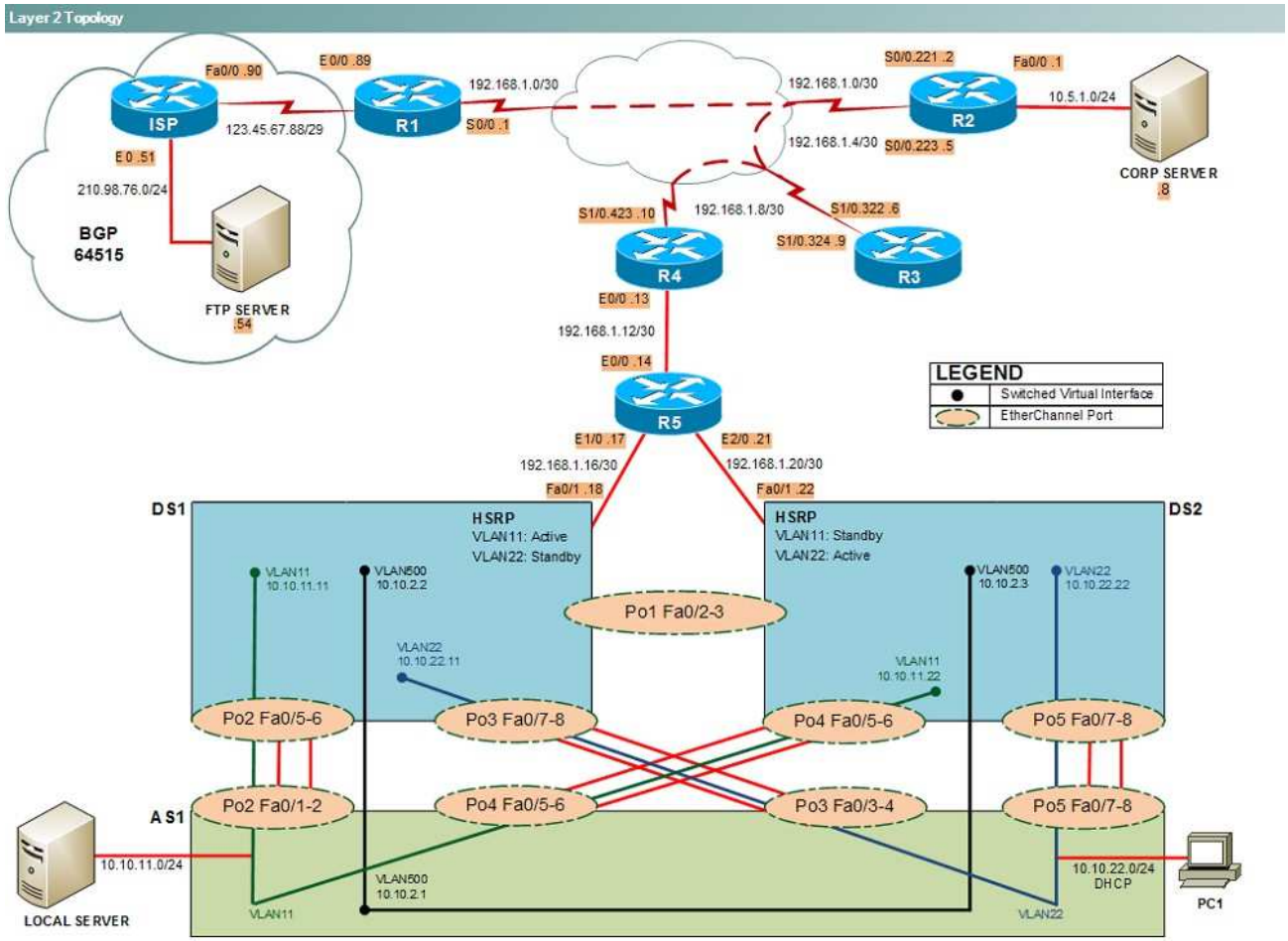
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

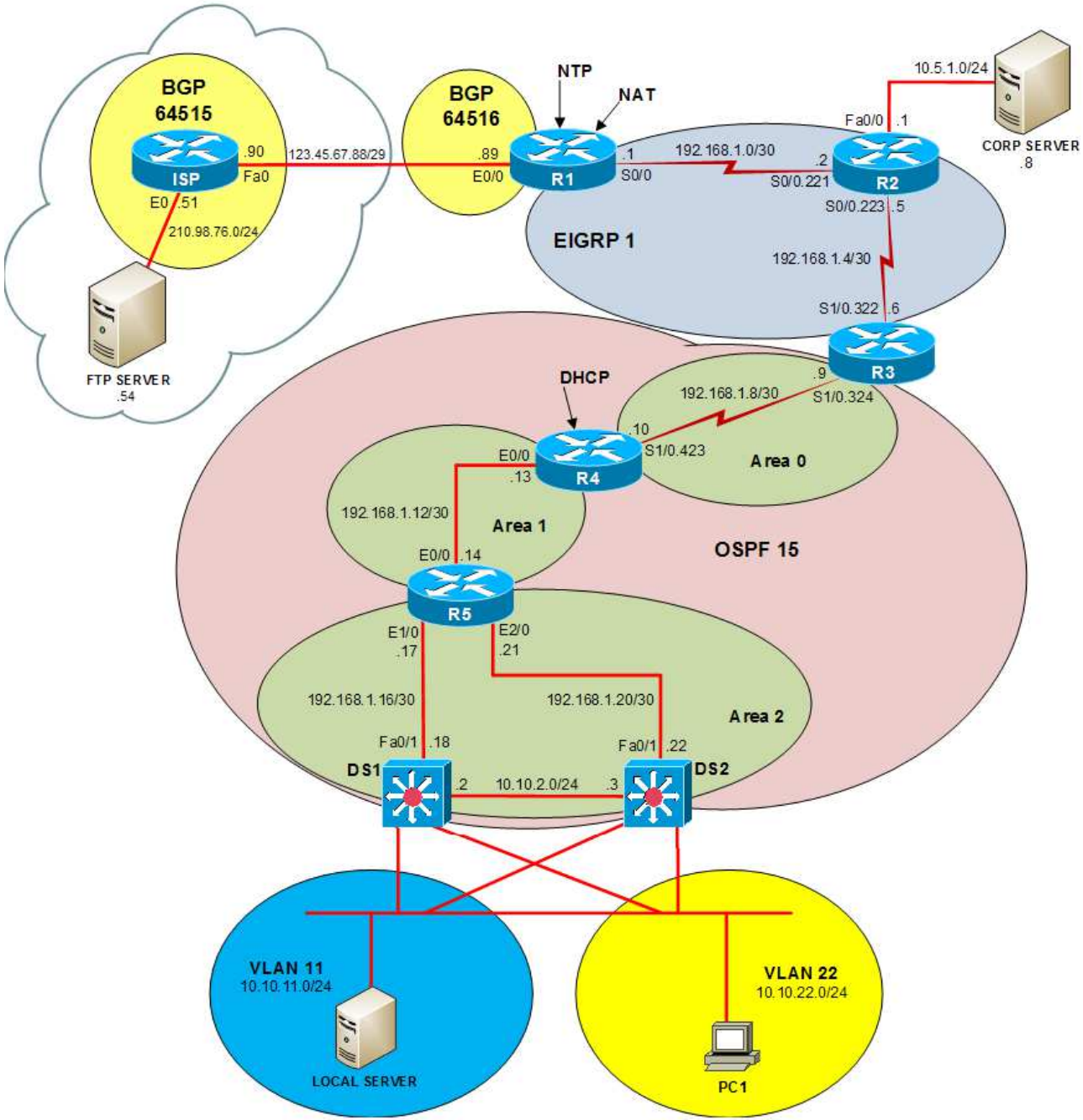
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

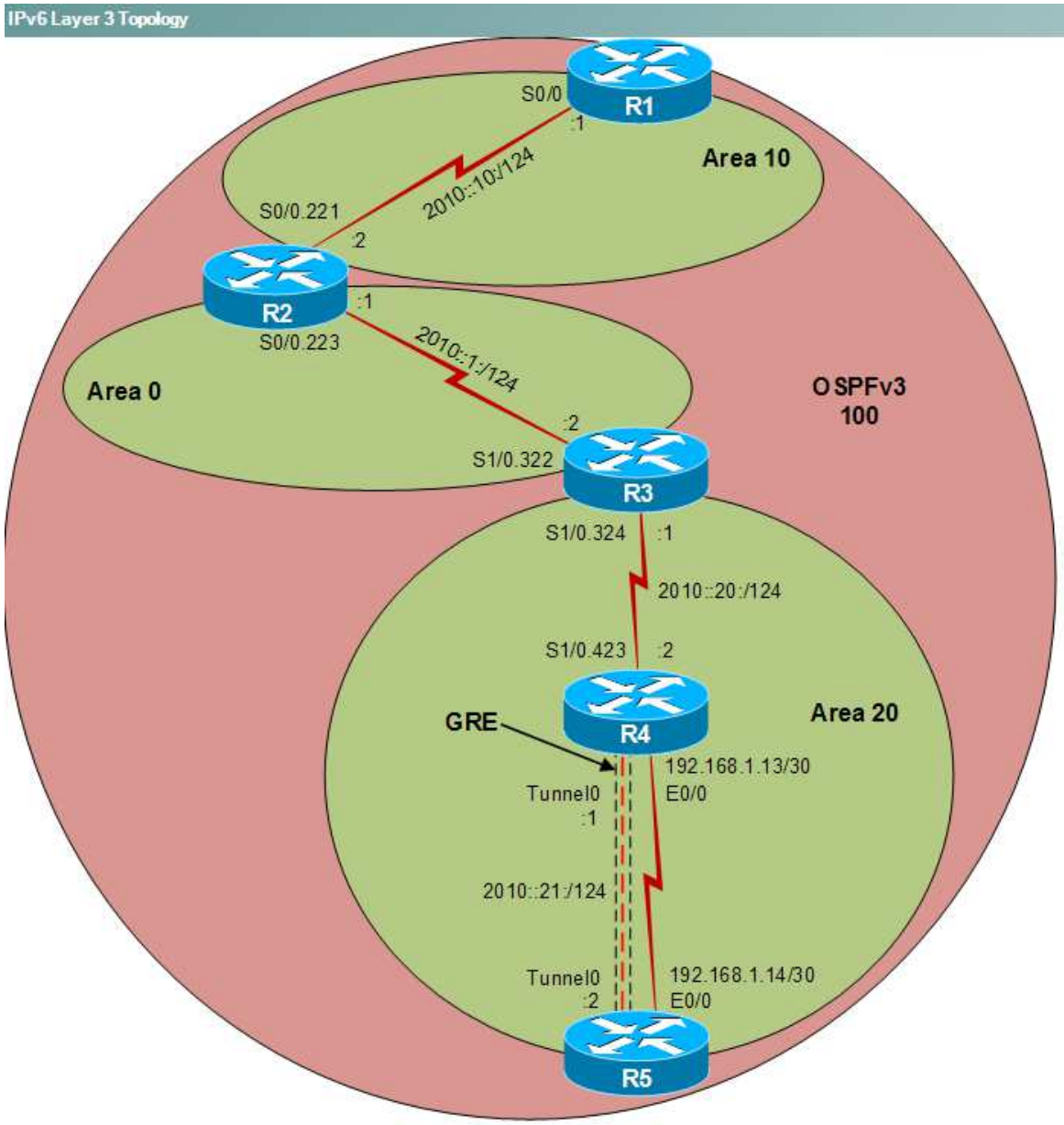
**Layer 2 Topology**




IPv4 layer 3 Topology

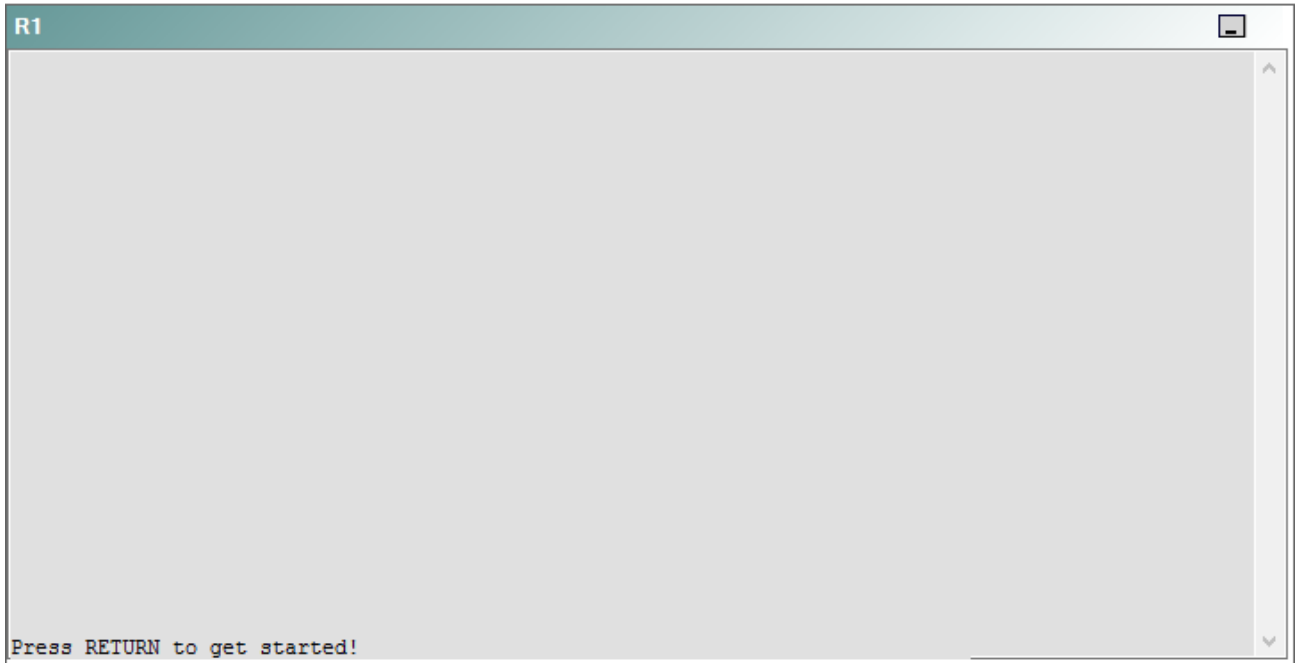

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

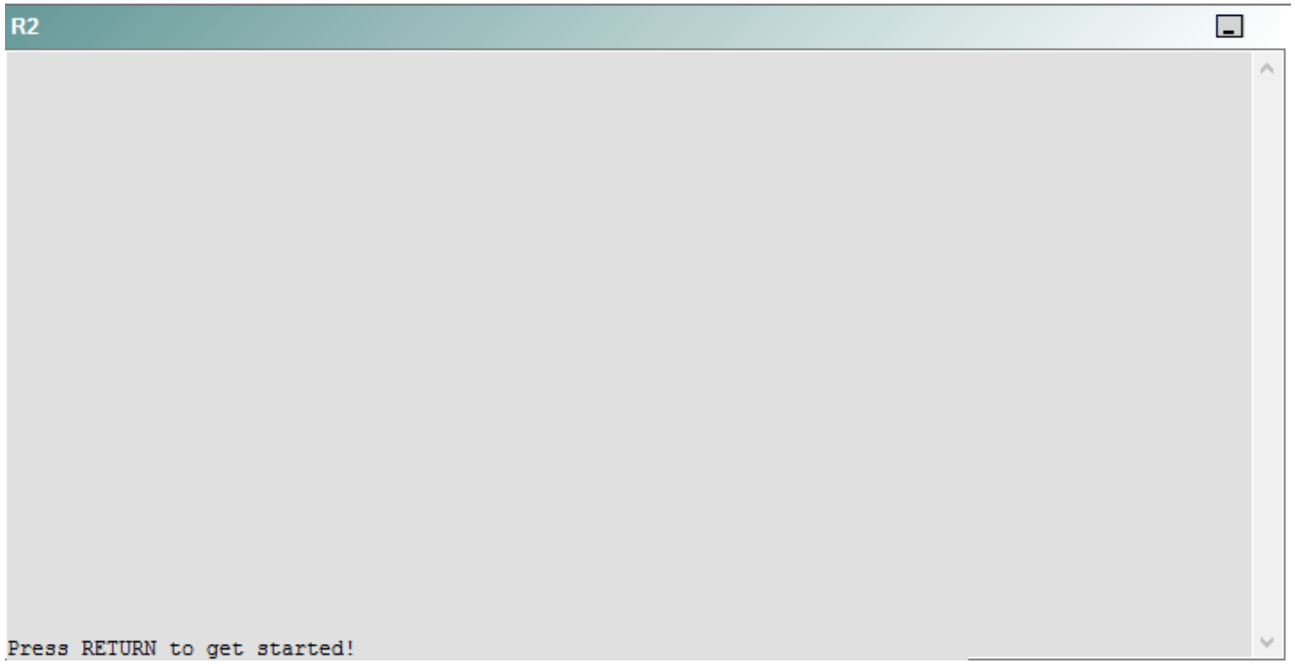



https://www.gratisexam.com/

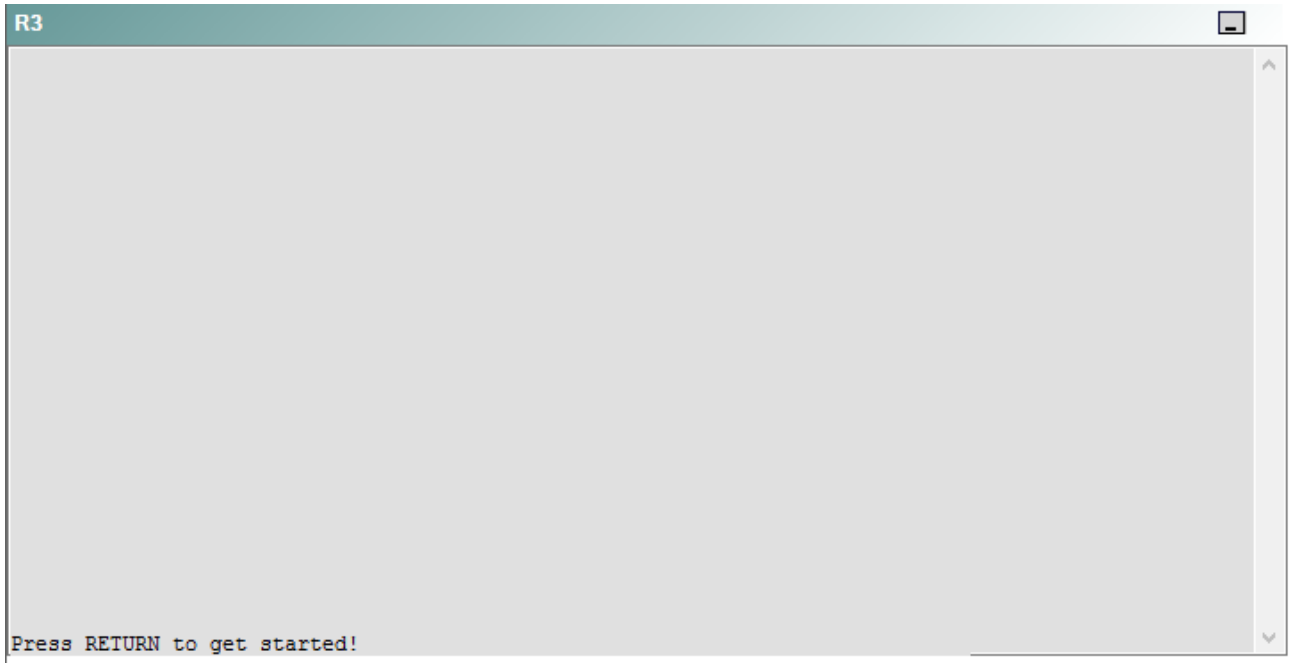
R1



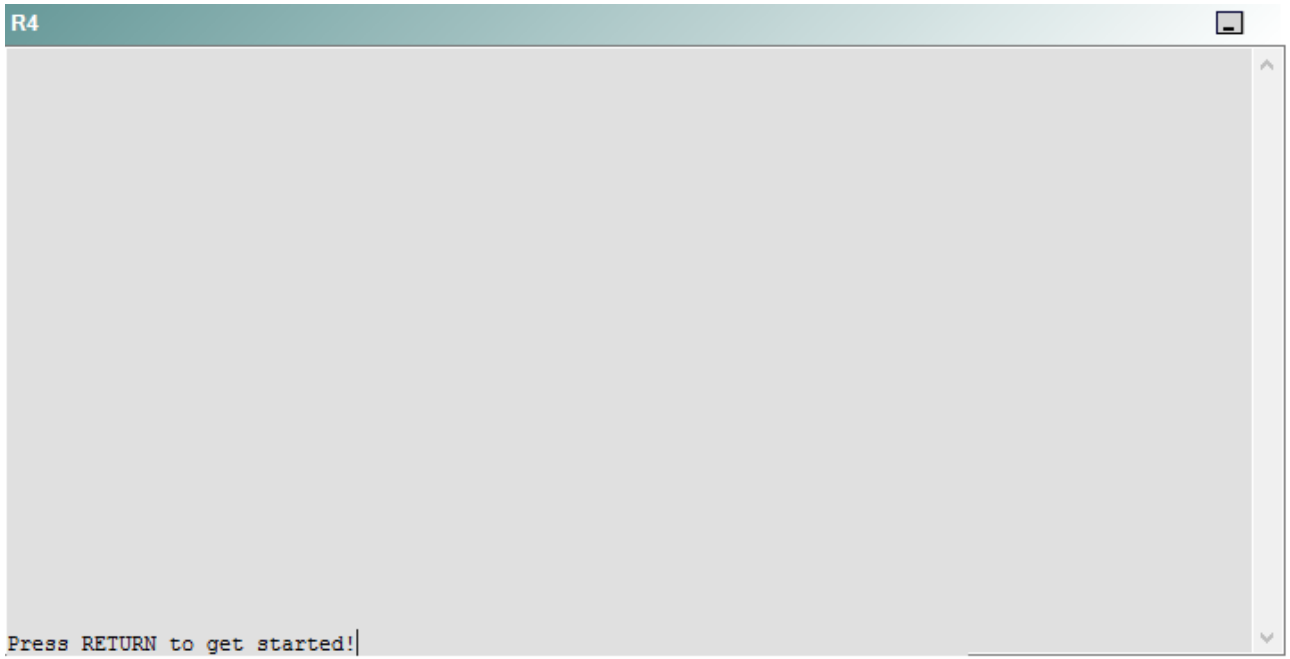

R2



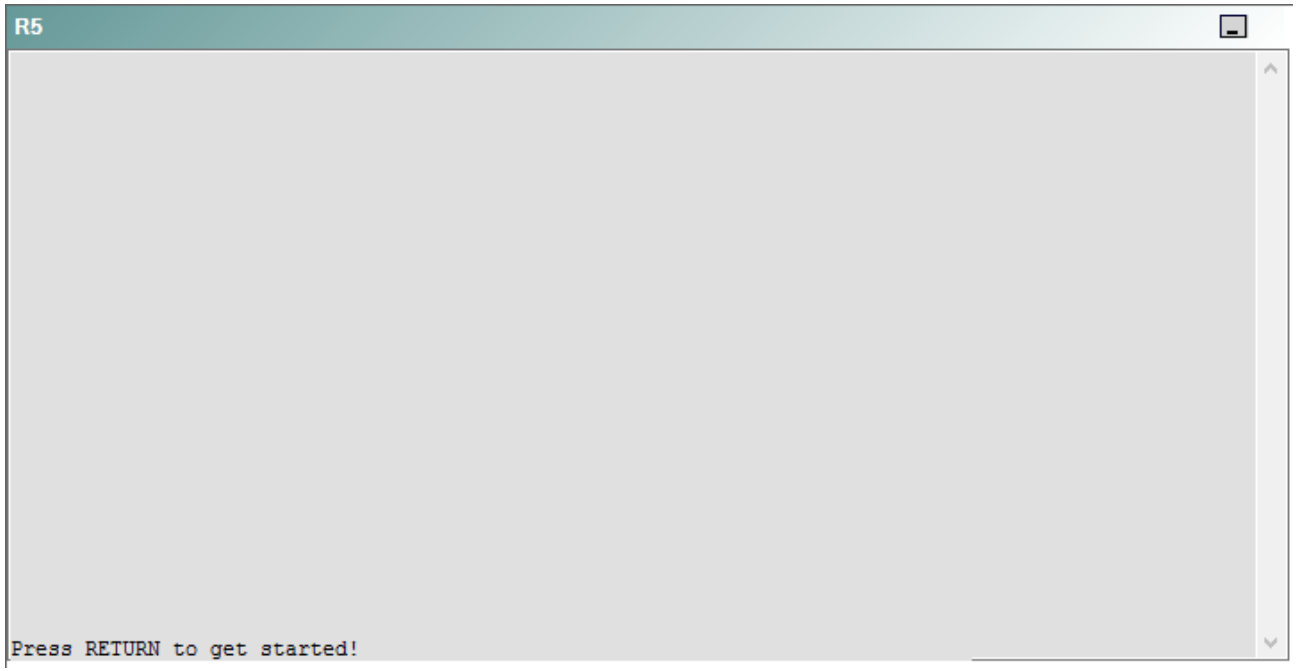

R3



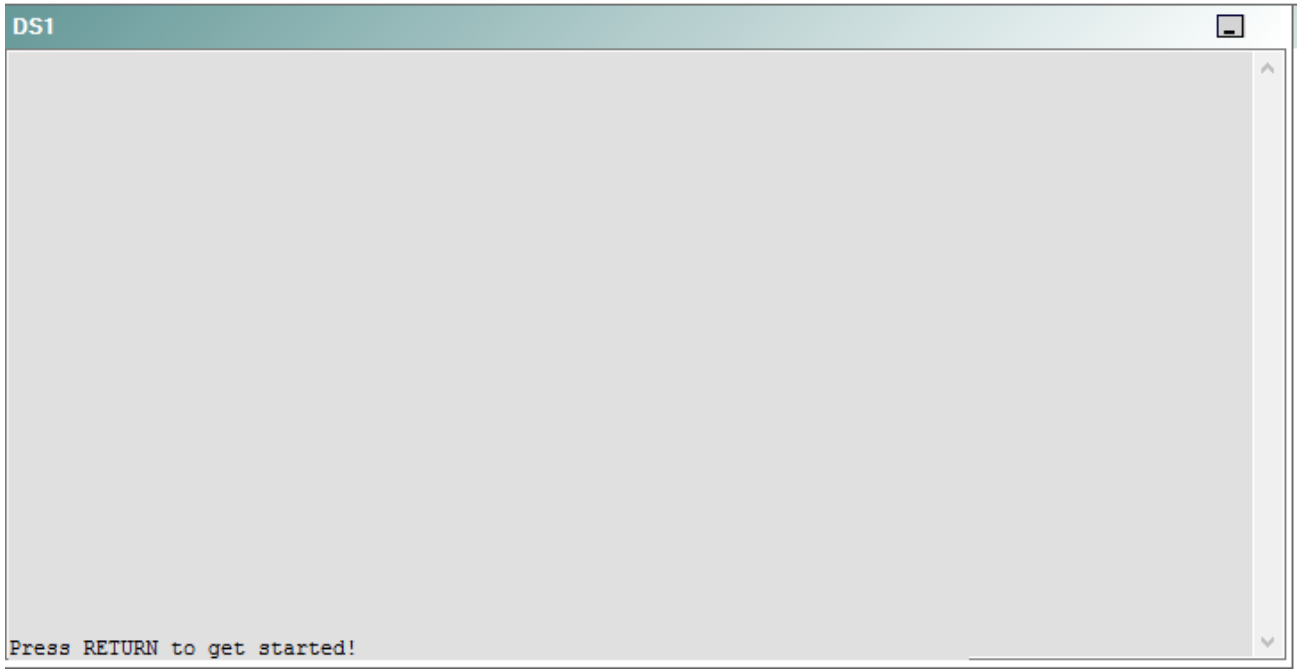

R4



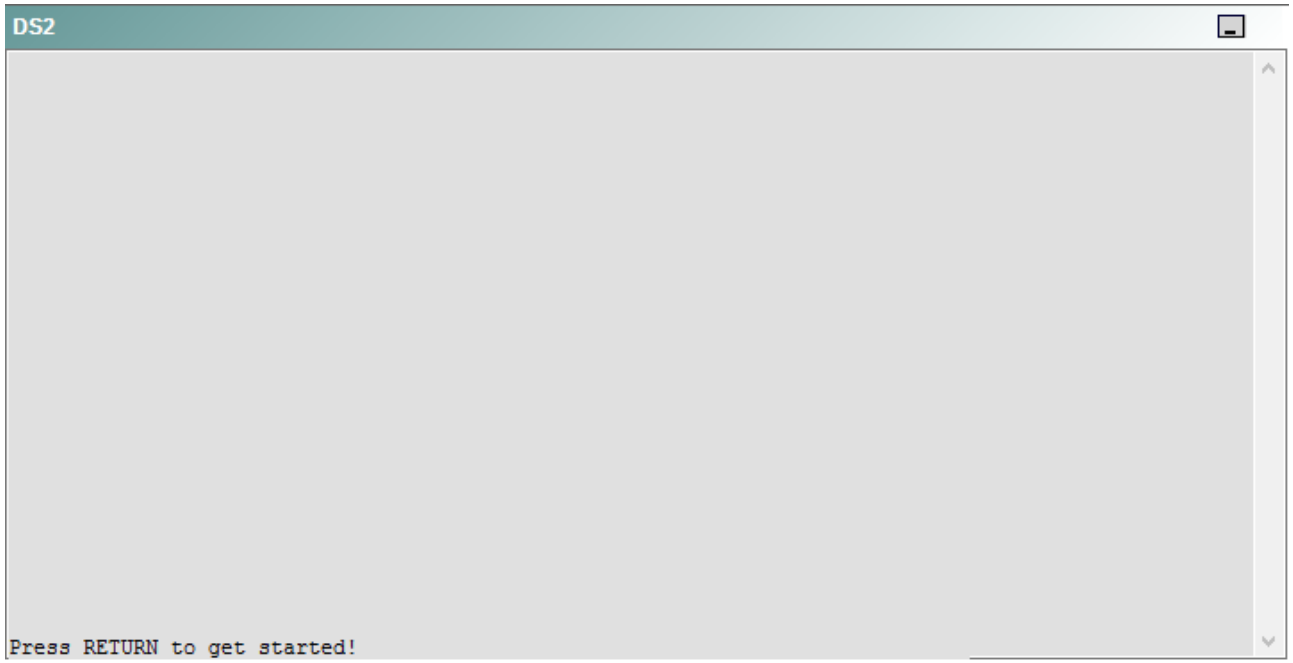

R5



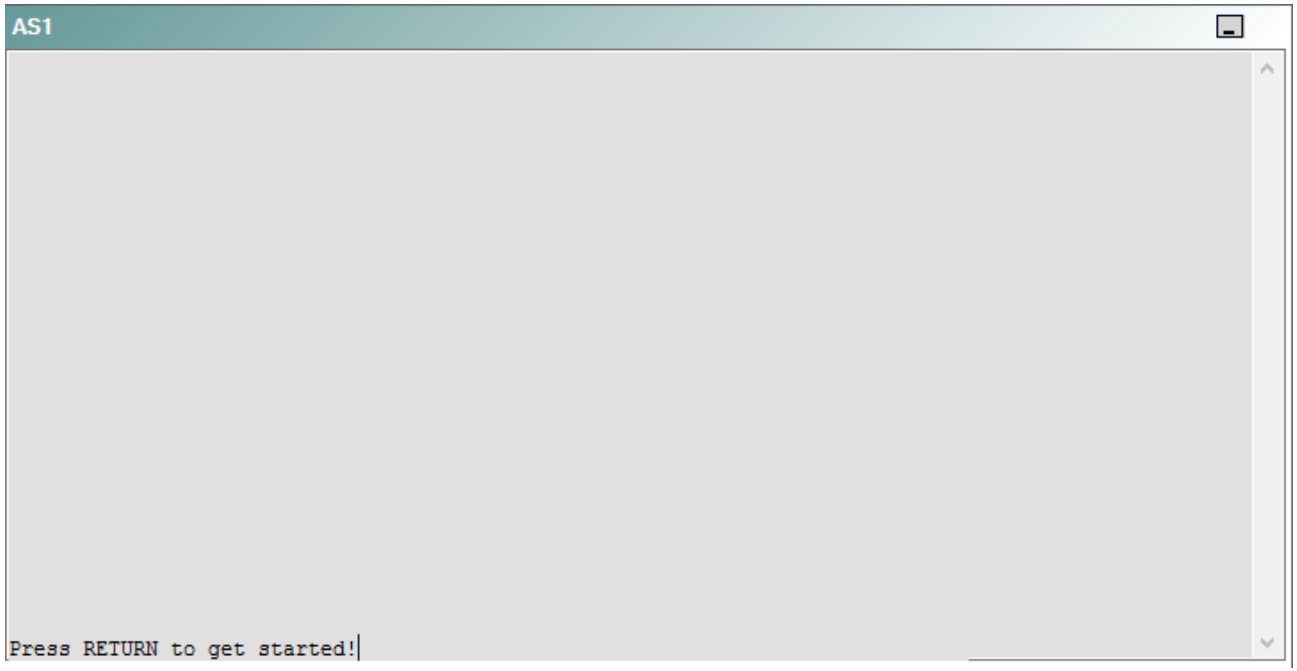

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that R5 is no longer able to ping the IPv6 loopback address 2000::10:1 on R1.

Which of the following is most likely to solve the problem?

A. issuing the **no ipv6 ospf hello-interval 80** command on S0/0
B. issuing the **no passive-interface default** command for OSPFv3 process 100
C. issuing the **ipv6 ospf 100 area 0 command on Loopback6**
D. issuing the **ipv6 ospf 100 area 10 command on Loopback6**
E. issuing the **ipv6 network 2000:10:1/128** command for OSPF 15
F. issuing the **ipv6 network 2010:10:1/128** command for OSPF 100

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

You should issue the **ipv6 ospf 100 area 10** command on the Loopback6 interface of R1. To determine which device is the source of the problem, you should issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from R5 to the closest device and work your way up the network until communication is lost, or you can ping from R5 to the farthest device and work your way back to R5 until pings are successful. Alternatively, you can trace from R5 to R1 and see where communication is lost along the path to the destination device.

In this scenario, if you were to issue the **traceroute 2000::10:1** command on R5, you would receive the following partial output:

```
Type escape sequence to abort.
Tracing the route to 2000::10:1

  1  *  *  *
  2  *  *  *
  3  *  *  *
  4  *  *  *
  5  *  *  *
```

The * * * in the output indicates that the attempt to trace the IP version 6 (IPv6) address 2000:10:1 has timed out. R5, which has a Loopback6 interface that has been assigned the IPv6 address 2000::14:1 can reach the Loopback6 IPv6 address 2000::13:1 on R4 as well as the Loopback6 IPv6 addresses assigned to R3 and R2. Therefore, the problem most likely exists on R1.

Once you have determined where connectivity is lost, you can begin to troubleshoot the cause of the problem. Issuing the **show ipv6 interface Loopback6** command on R1 reveals that the interface is up and the line protocol is up on Loopback6, which eliminates Open Systems Interconnection (OSI) Physical layer problems and OSI Data Link layer problems as possible causes of the loss of connectivity, as shown in the following output:

```
Loopback6 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::CE07:8FF:FE9C:10
  Global unicast address(es):
    2000::10:1, subnet is 2000::10:1/128
```

Therefore, you should continue troubleshooting the Network layer of the OSI model. R1 uses Open Shortest Path First version 3 (OSPFv3) to route IPv6 packets to R2. OSPFv3 is a Network layer protocol. If you were to issue the **show ipv6 ospf interface brief** command on R1, you would see the following output:

```
Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
Se0/0        100   10              3          64    P2P   1/1
```

The output above indicates that the Serial0/0 interface on R1 is included in IPv6 OSPF routing. However, the Loopback6 interface is not being reported by OSPF. The Loopback6 interfaces must be included in IPv6 OSPF routing to allow the routers to communicate by using the IP addresses of the Loopback 6 interfaces. Therefore, you should issue the **ipv6 ospf 100 area 10** command on the Loopback6 interface of R1 to solve the problem.

You should not issue the **ipv6 ospf 100 area 0** command on the Loopback6 interface on R1. In this scenario, the boundaries of Area 0 are located on R2 and R3, not R1. R1 is connected only to OSPFv3 Area 10. Therefore, the Loopback6 interface on R1 should be configured for OSPFv3 Area 10.

You should not issue an **ipv6 network** command for OSPF 15 on any device. In this scenario, the OSPF 15 process is used on R2, R4, R5, and DS2 to route IPv4 traffic, not IPv6. Additionally, you need to issue an **ipv6 network** command for OSPF 100 on any device. In this scenario, OSPF process 100 is used to route IPv6 packets between R1, R2, R3, R4, and R5; however, you should enable OSPFv3 routing at the interface level, not by issuing the **ipv6 network** command at the routing process level.

You should not issue the **no ipv6 ospf hello-interval 80** command on S0/0 on R1. In this scenario, the hello and dead intervals on all routers are set to their default values. Therefore, a hello interval mismatch cannot be the cause of the problem.

You should not issue the **no passive-interface default** command for OSPFv3 process 100 on R1. Although setting the OSPFv3 interface to passive could result in a loss of connectivity, the Loopback6 interface on R1 has not been configured as a passive interface.

**QUESTION 33**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

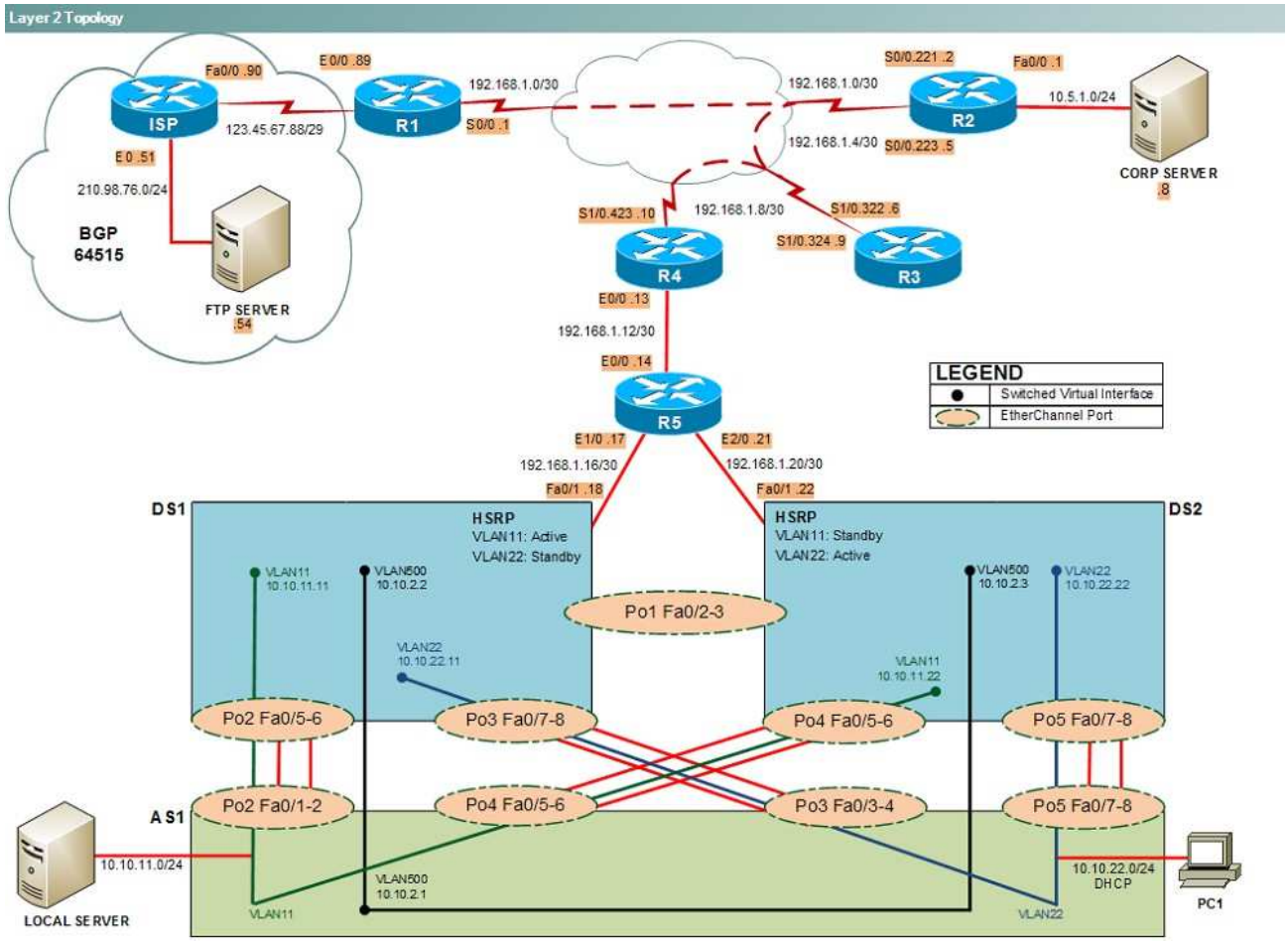
Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and

**ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

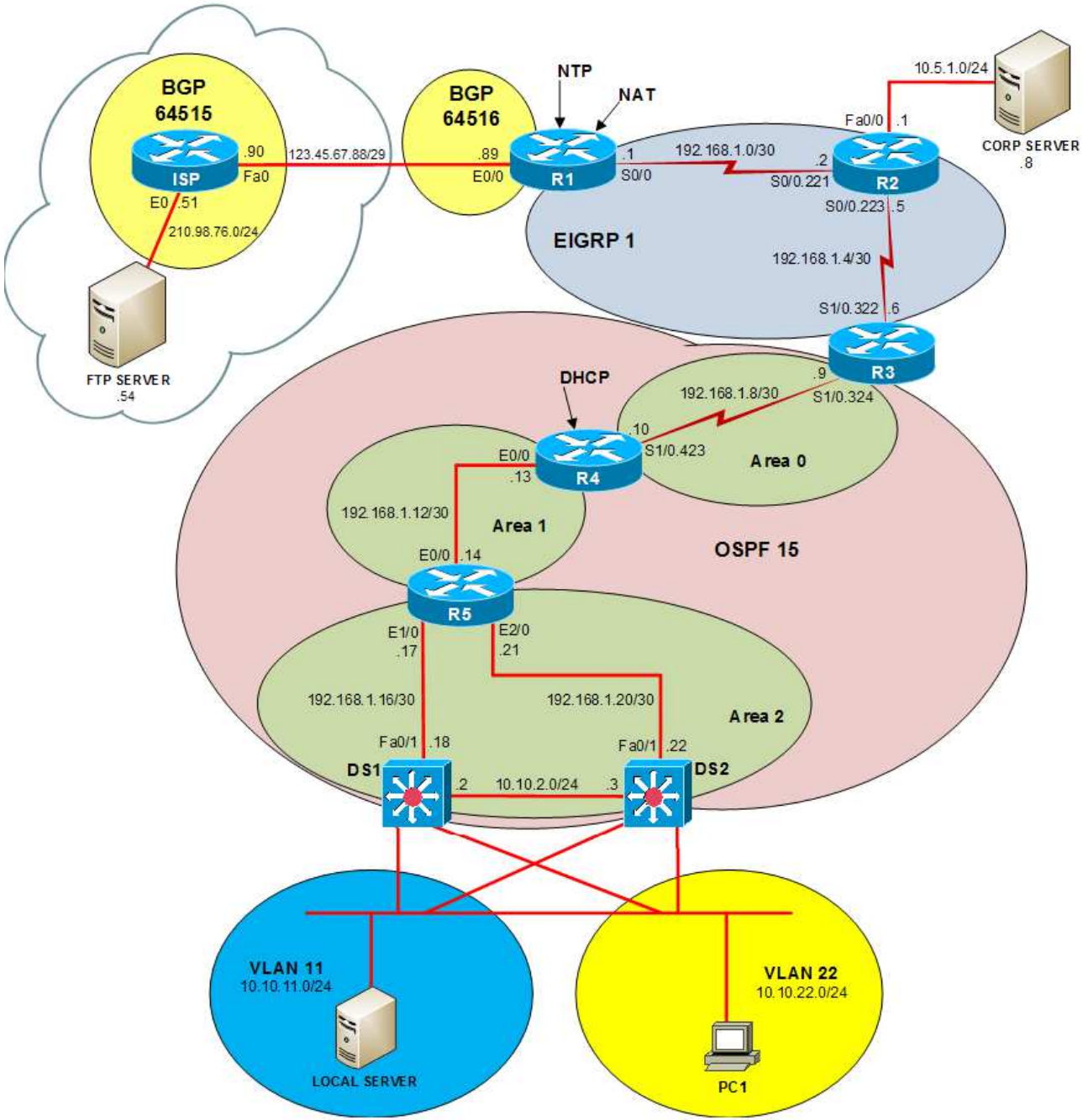
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

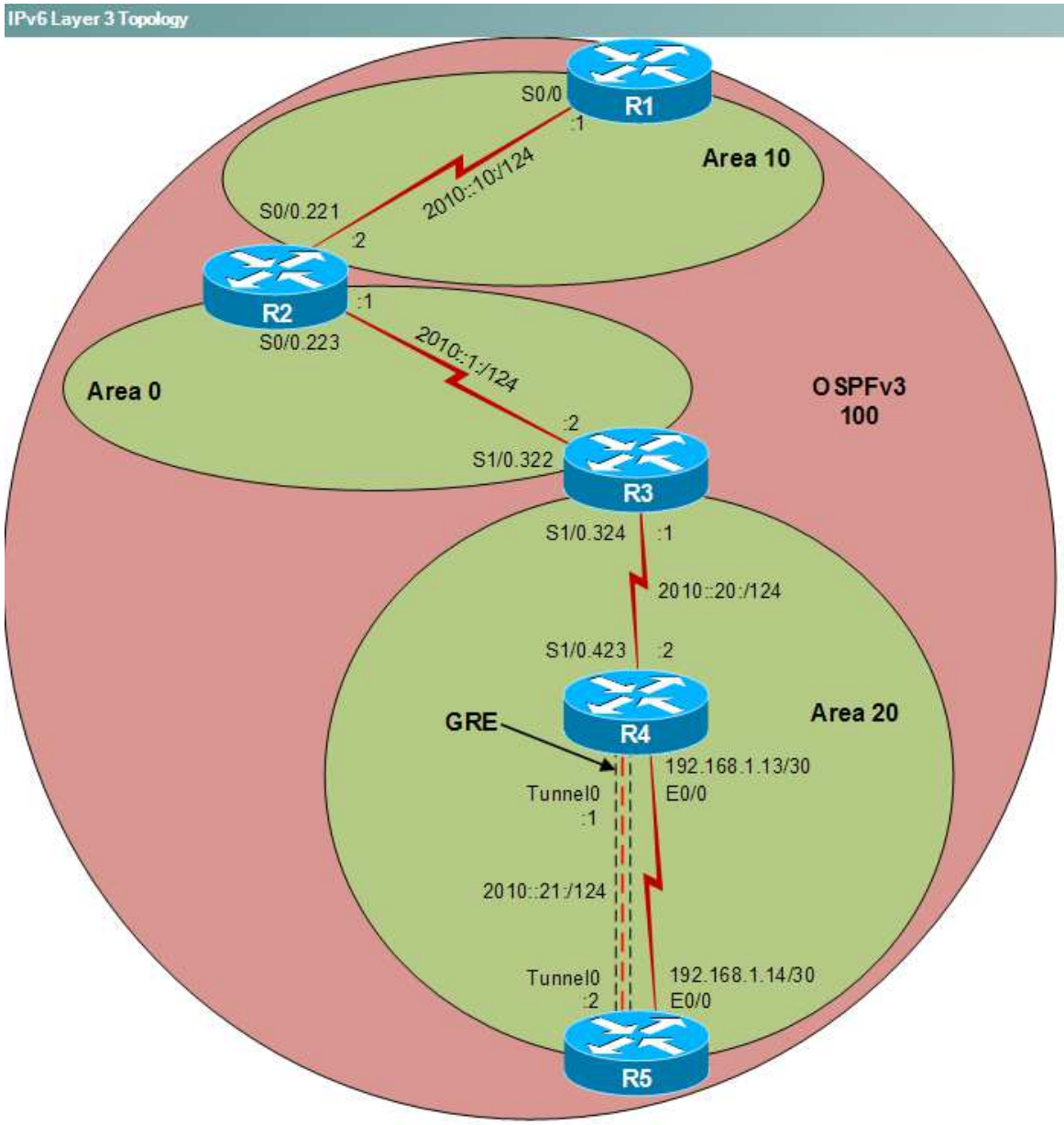
**Layer 2 Topology**




IPv4 layer 3 Topology

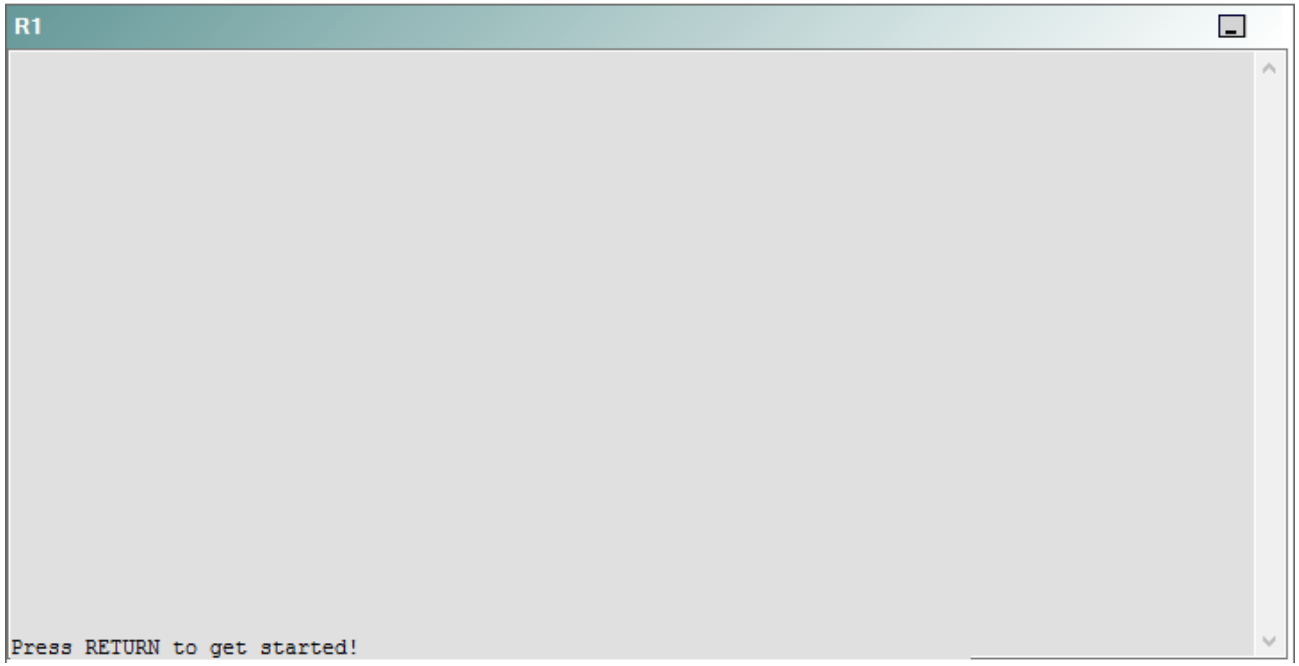

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

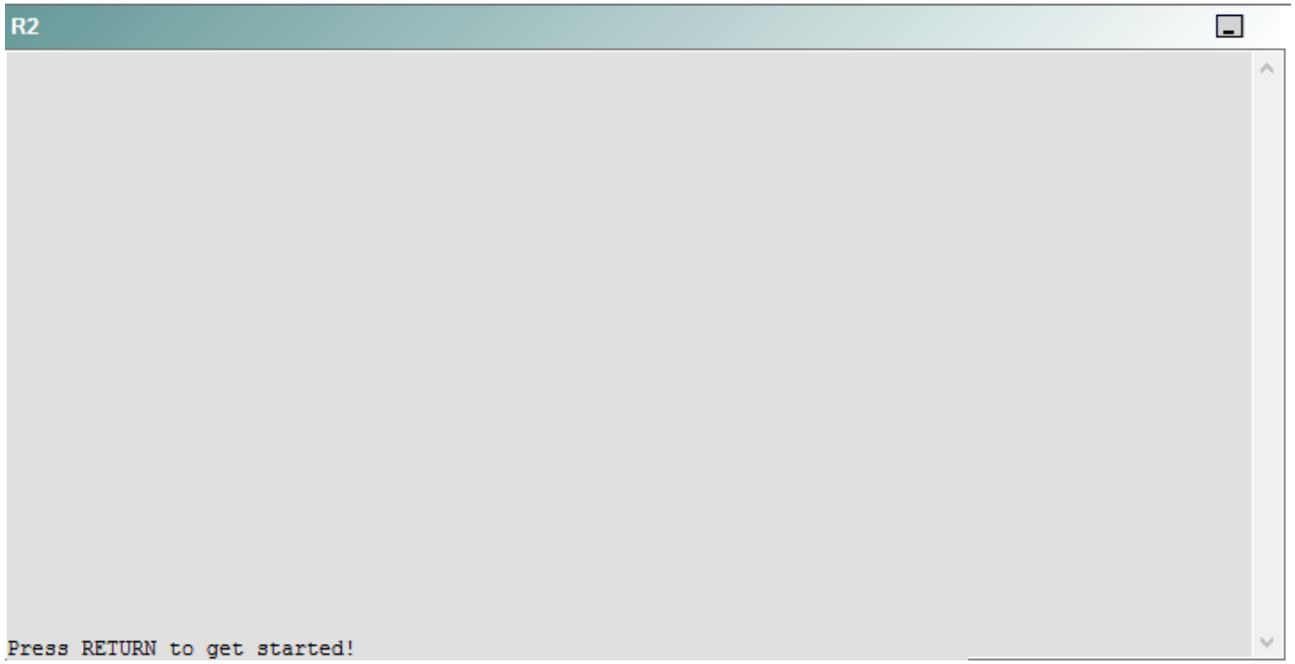



https://www.gratisexam.com/

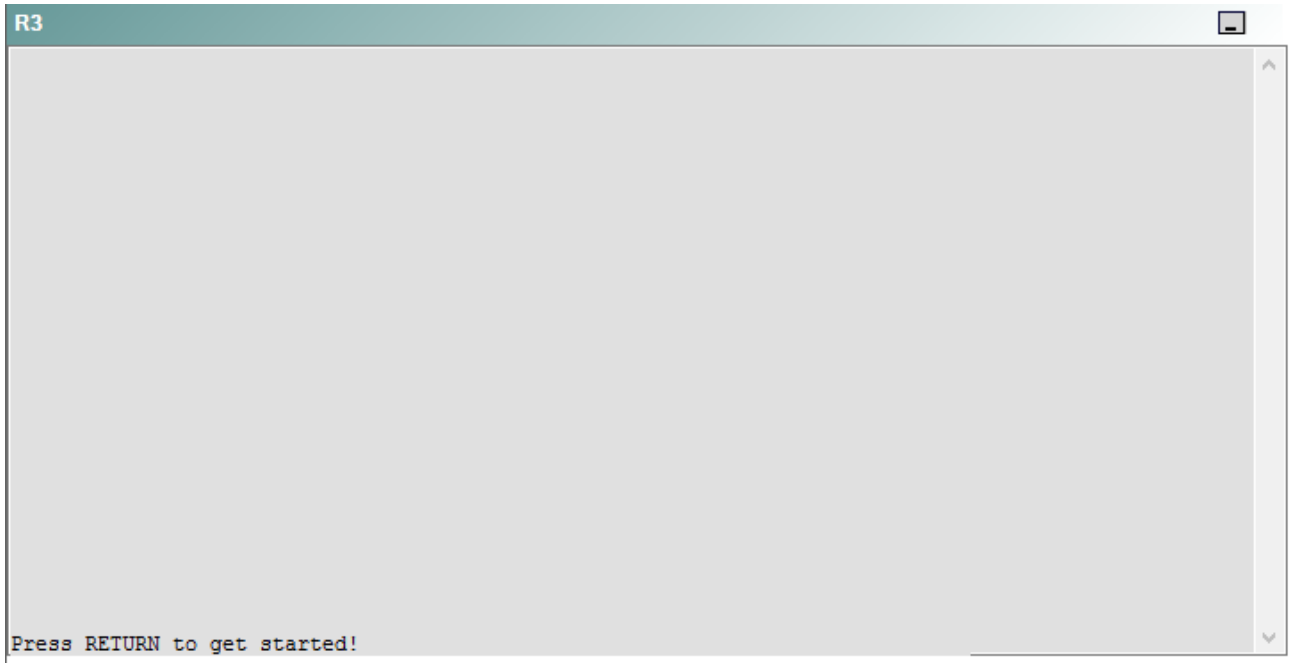
R1



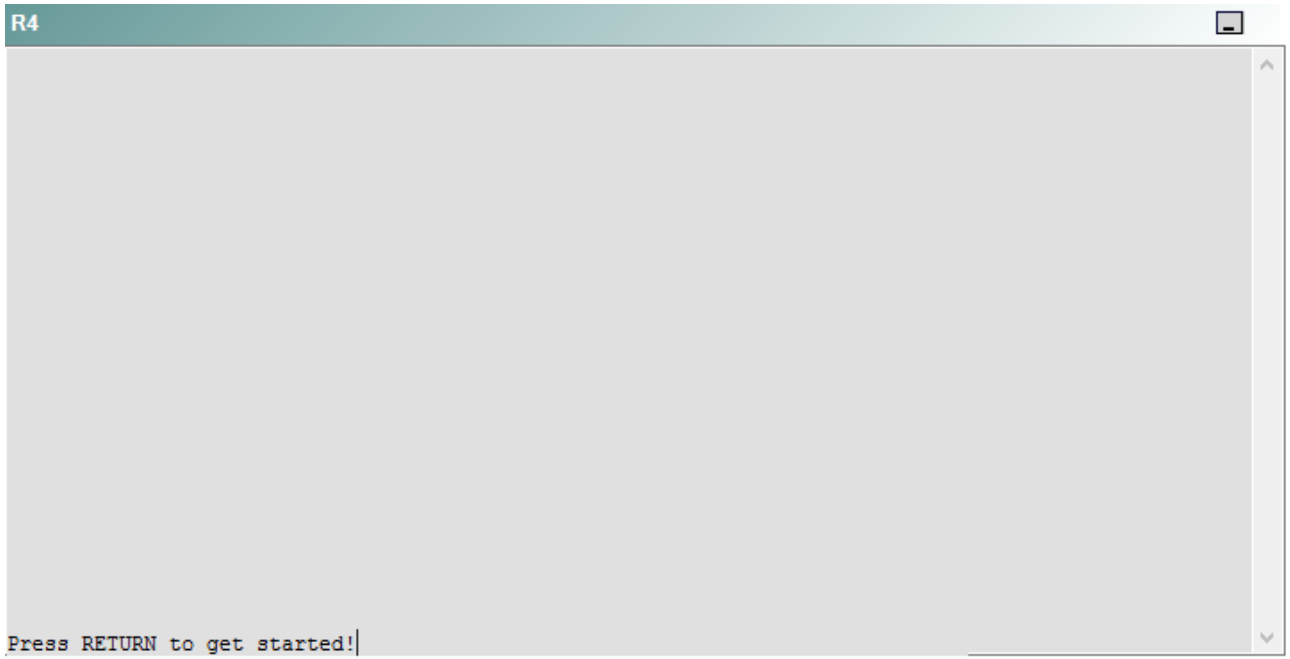

R2



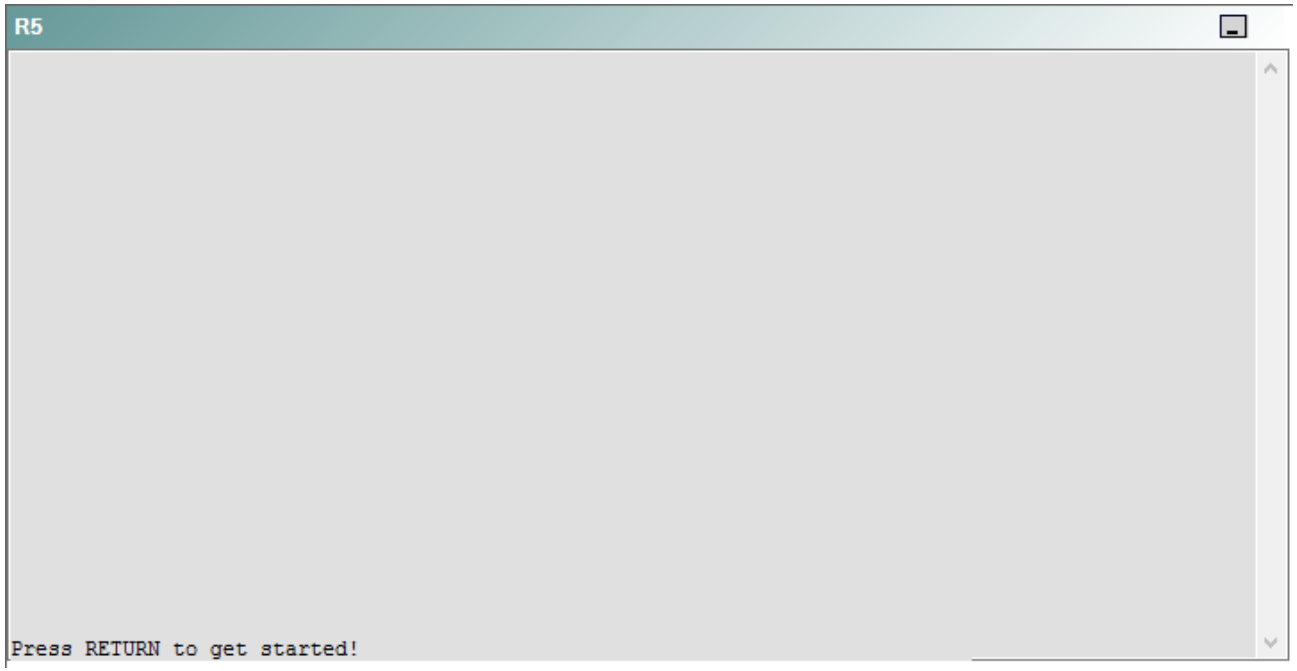

R3



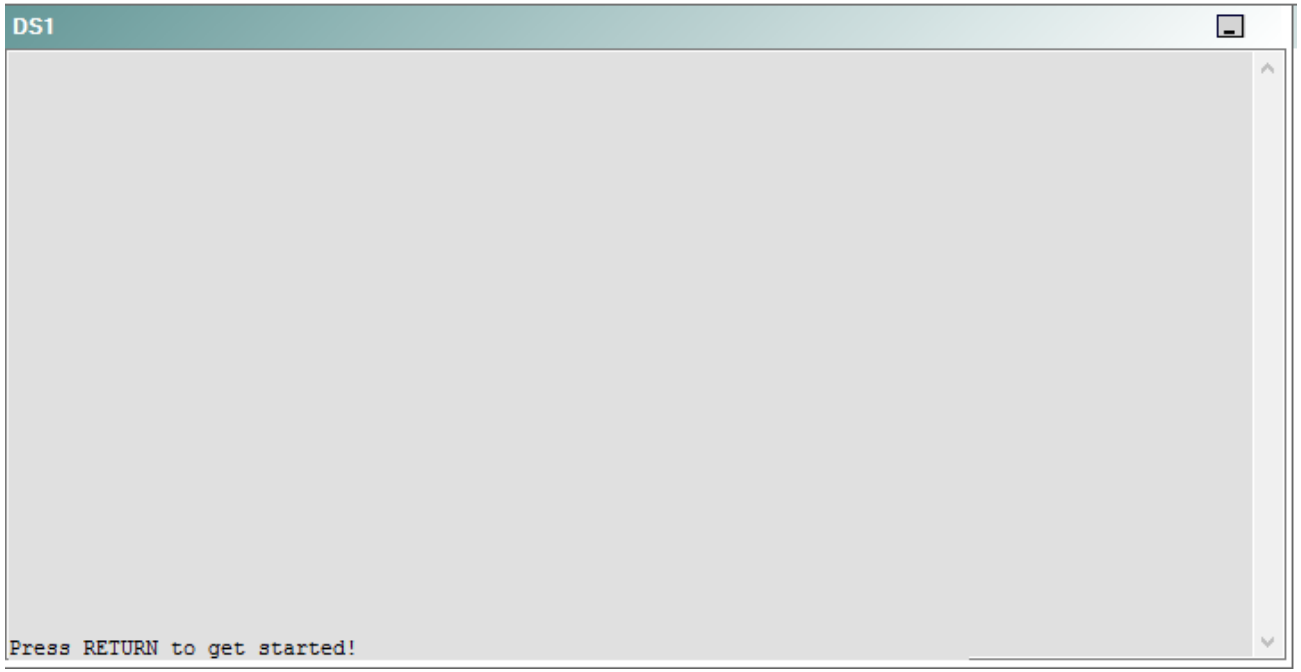

R4



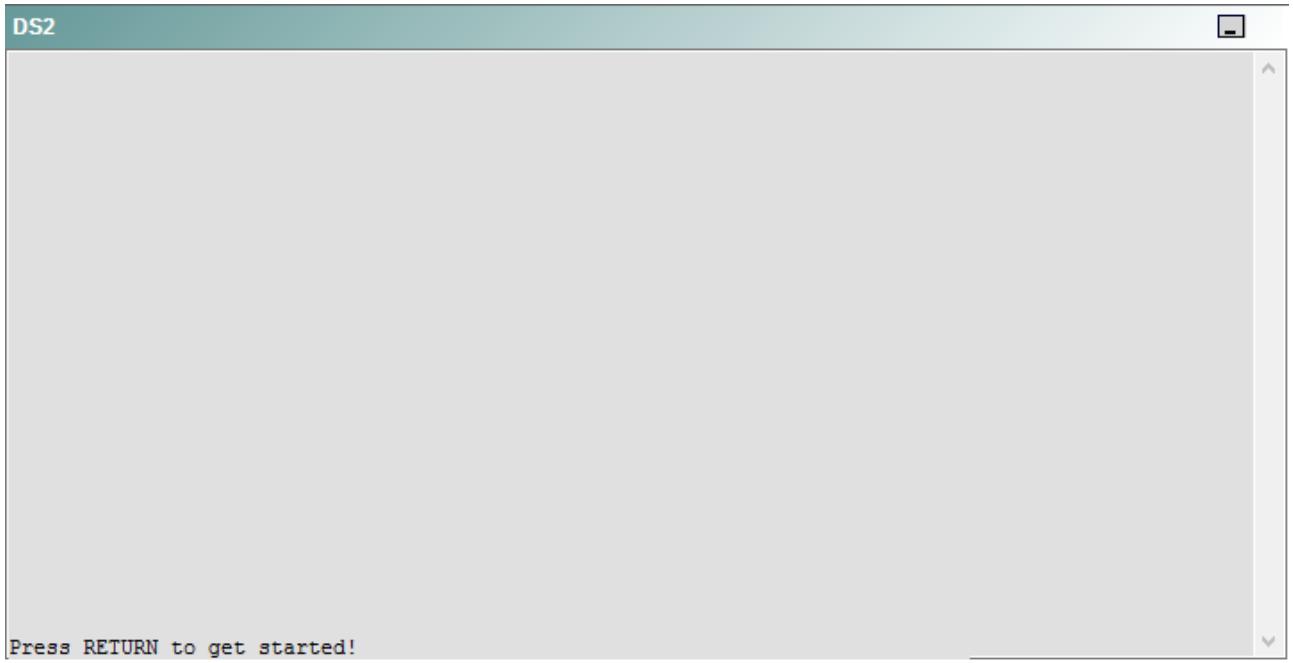

R5



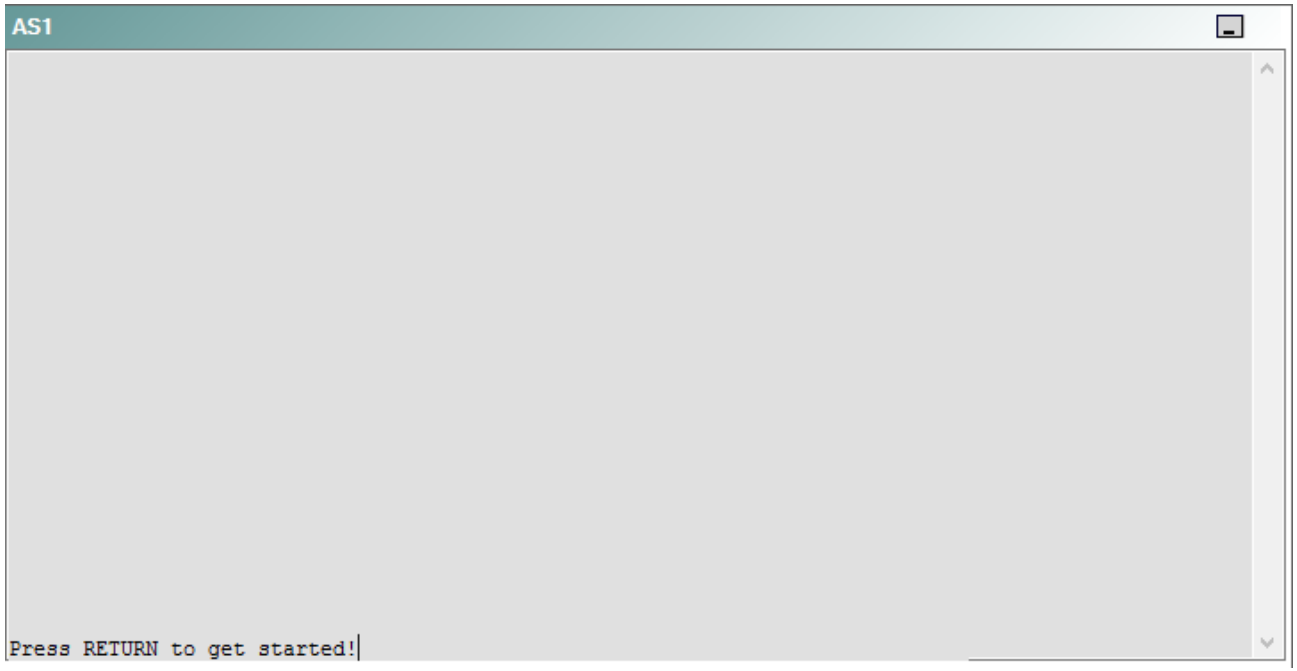

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 34**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

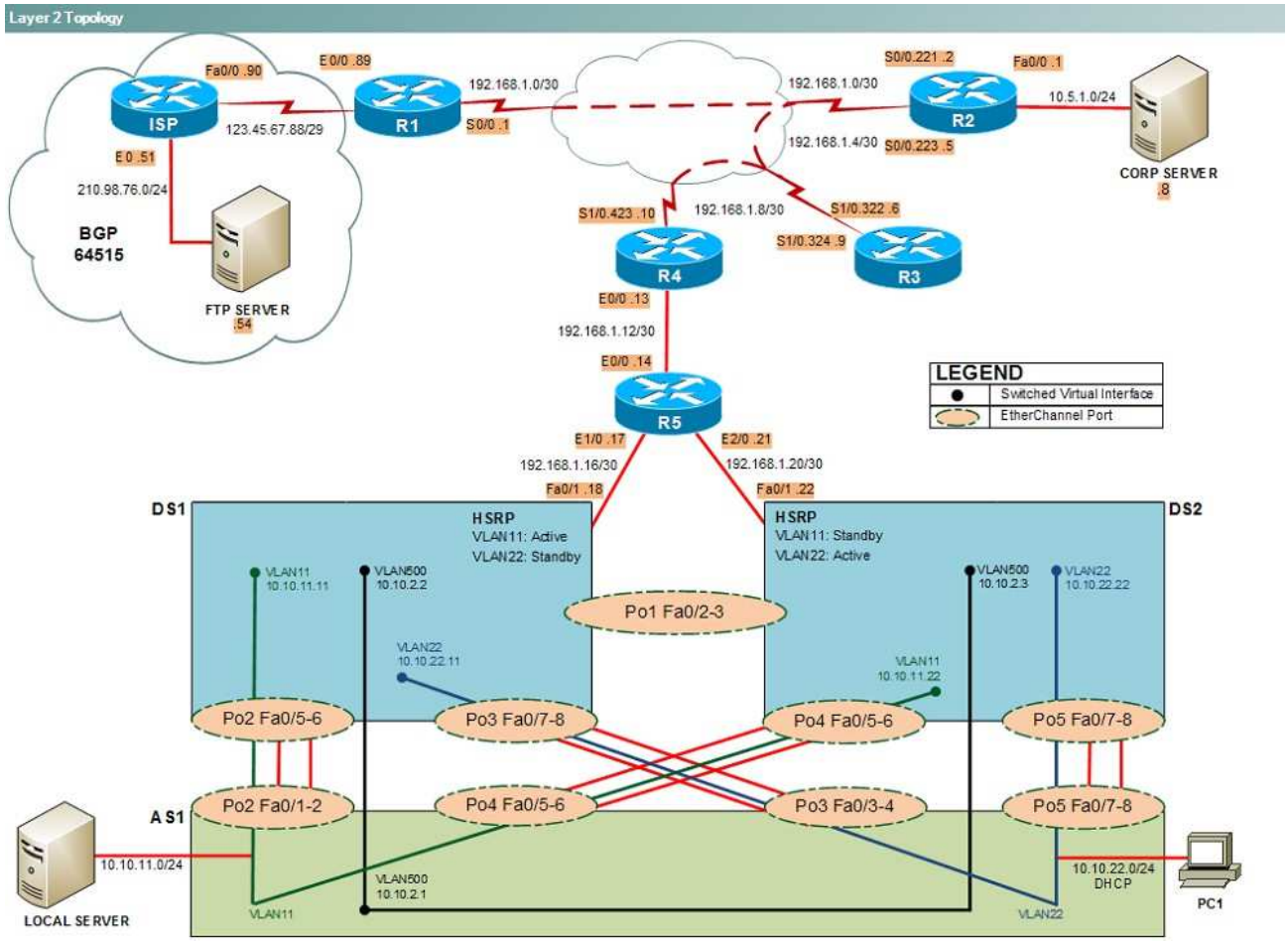
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

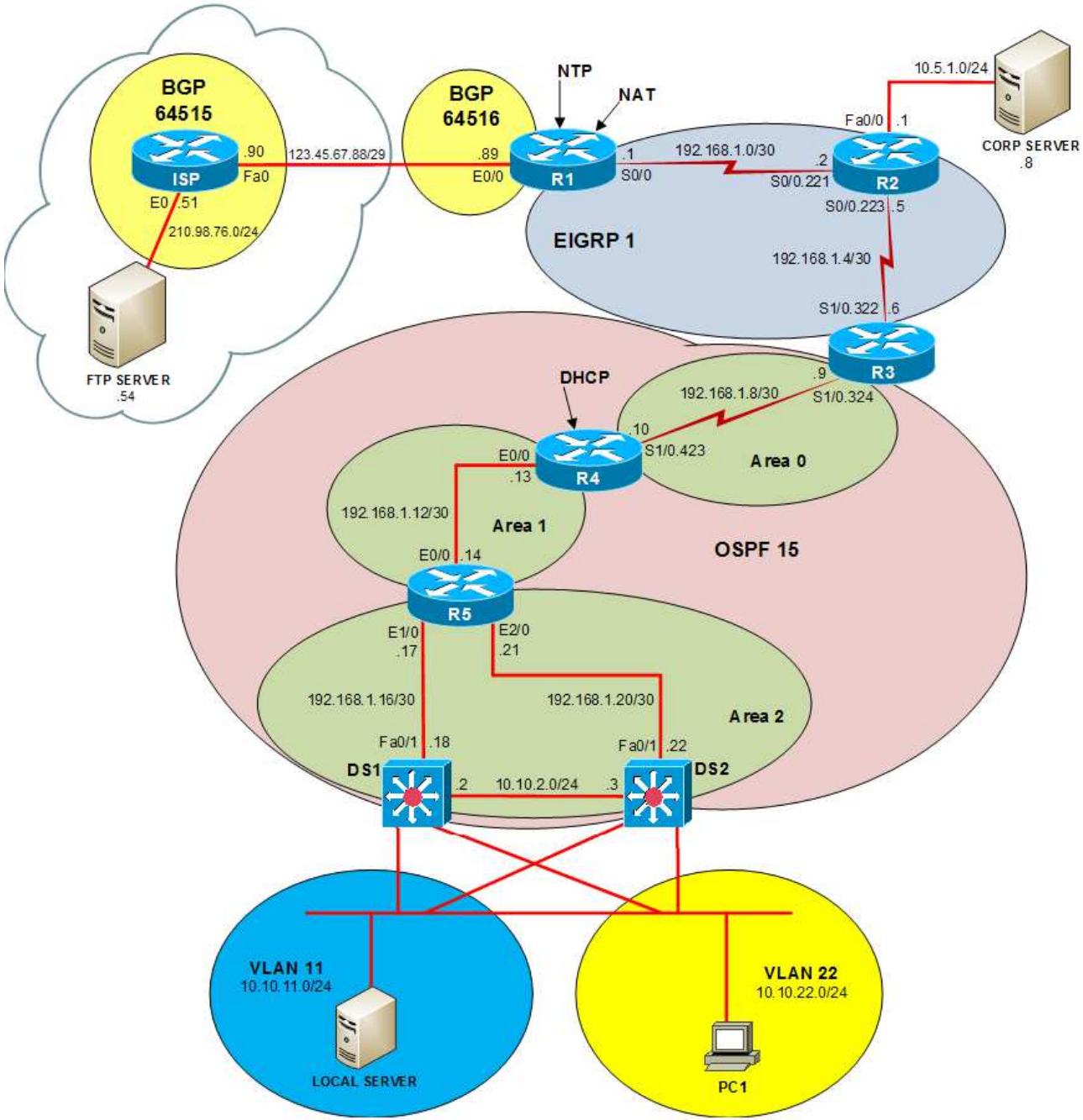
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

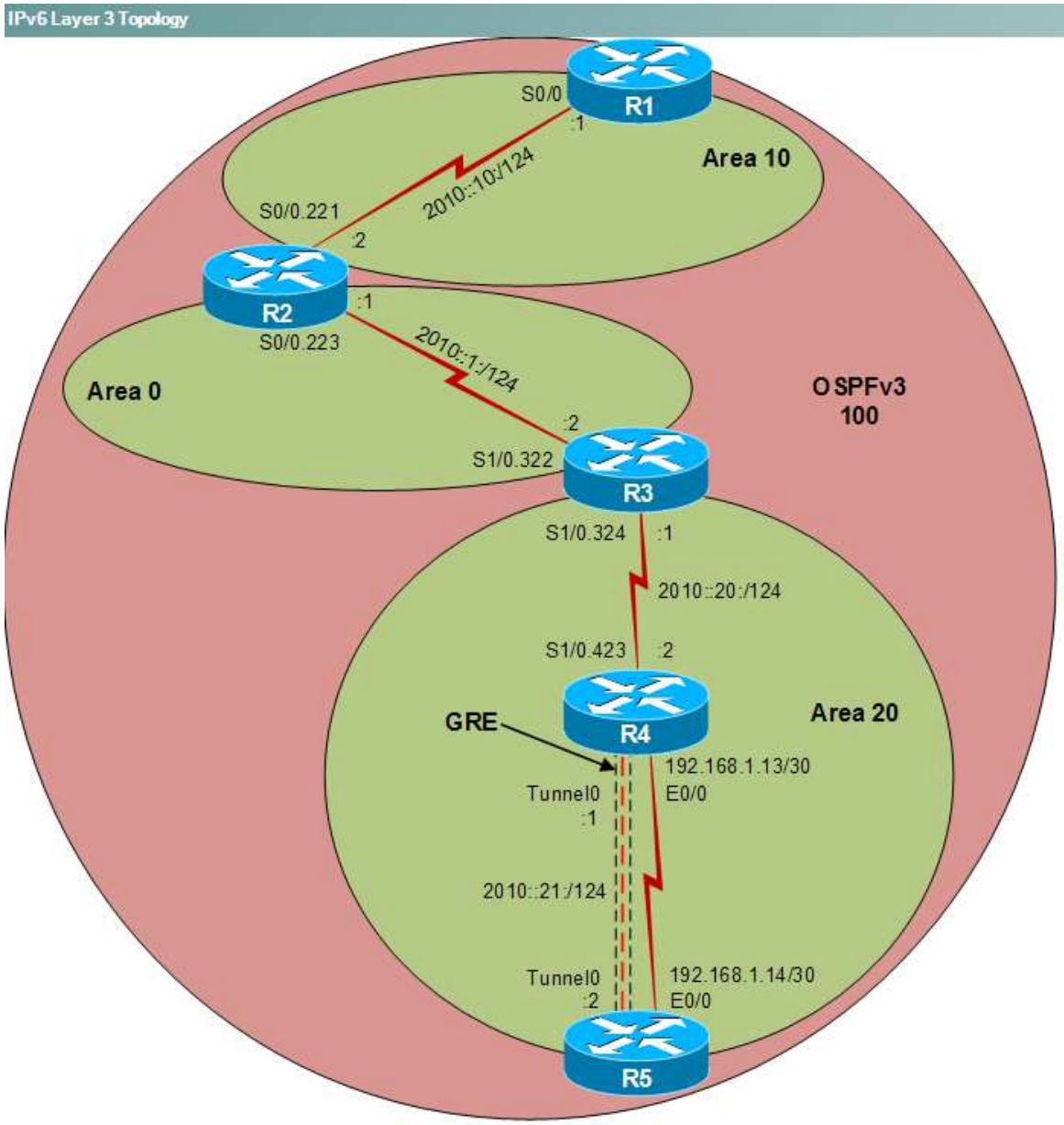
**Layer 2 Topology**




IPv4 layer 3 Topology

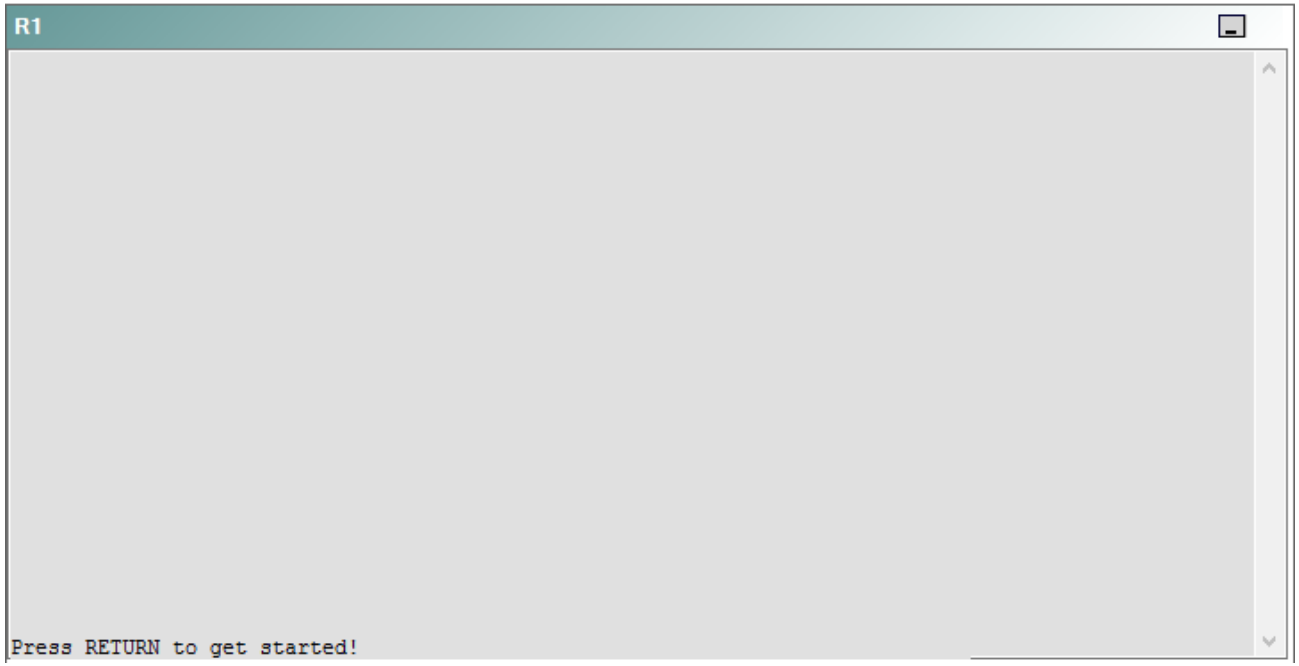

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

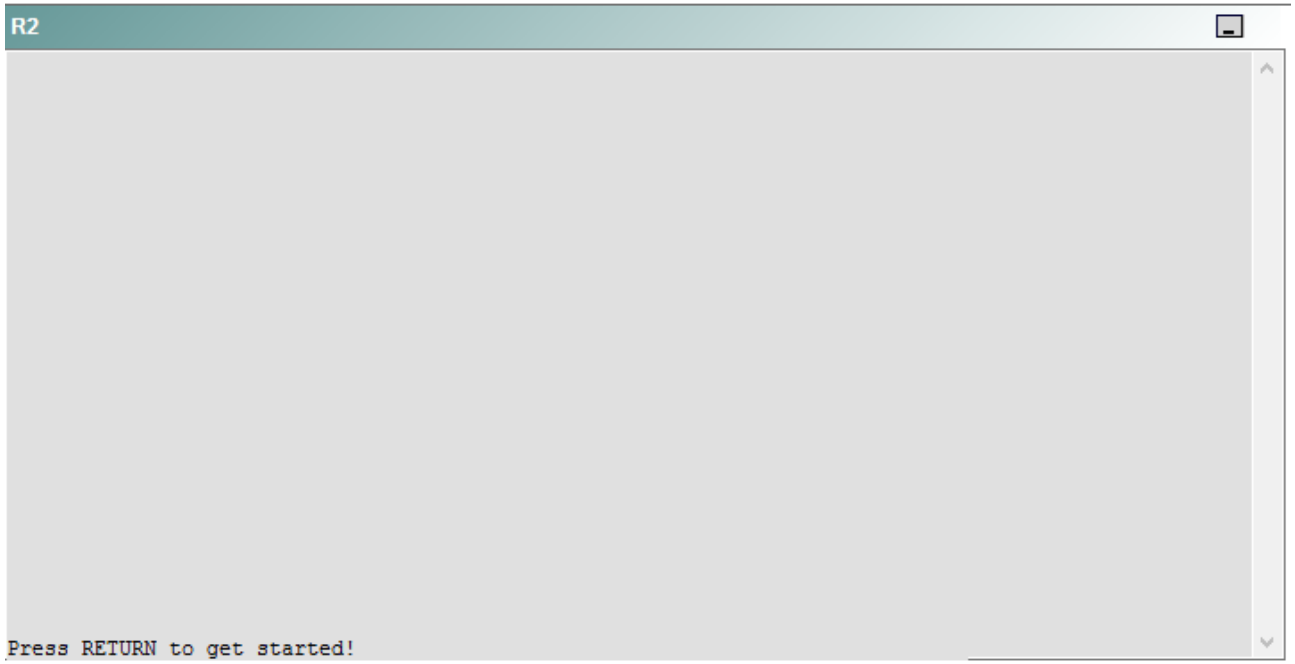



https://www.gratisexam.com/

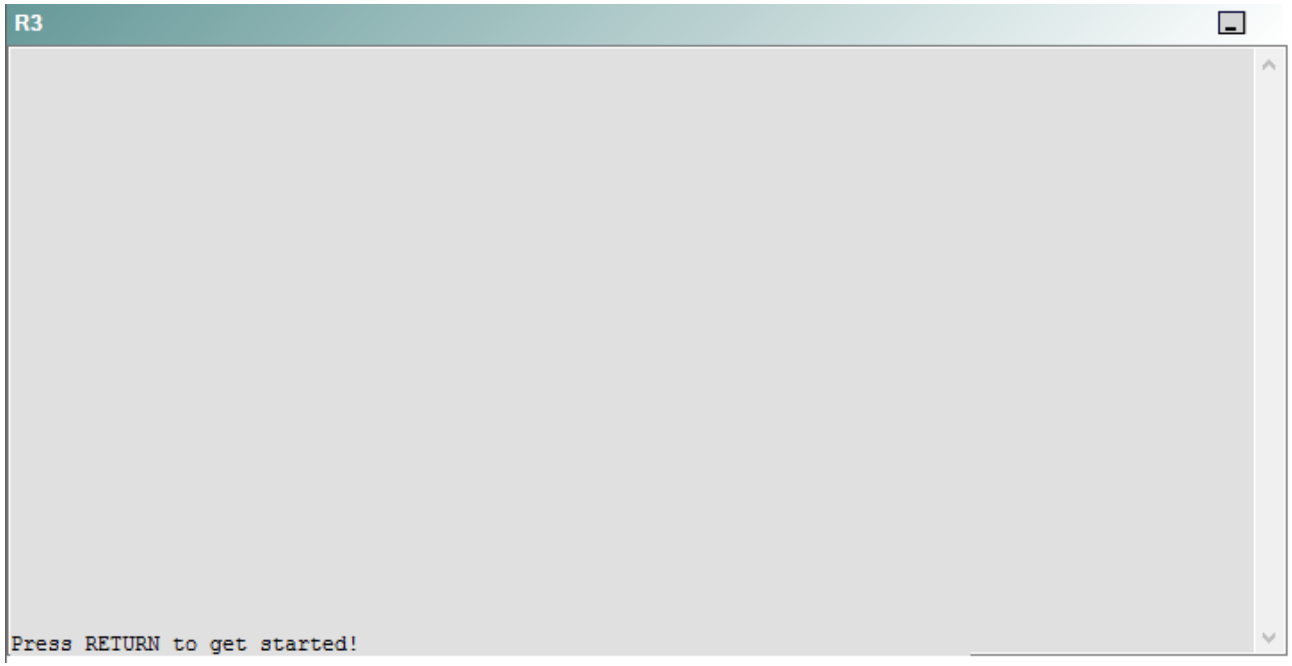
R1



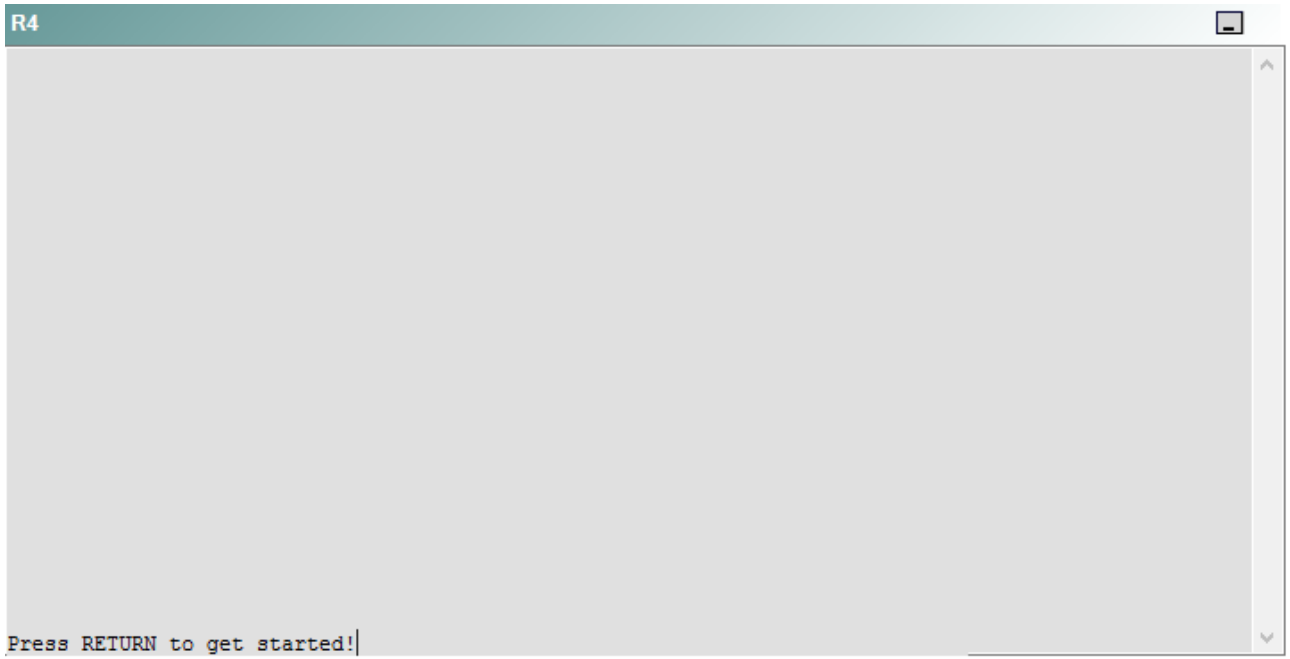

R2



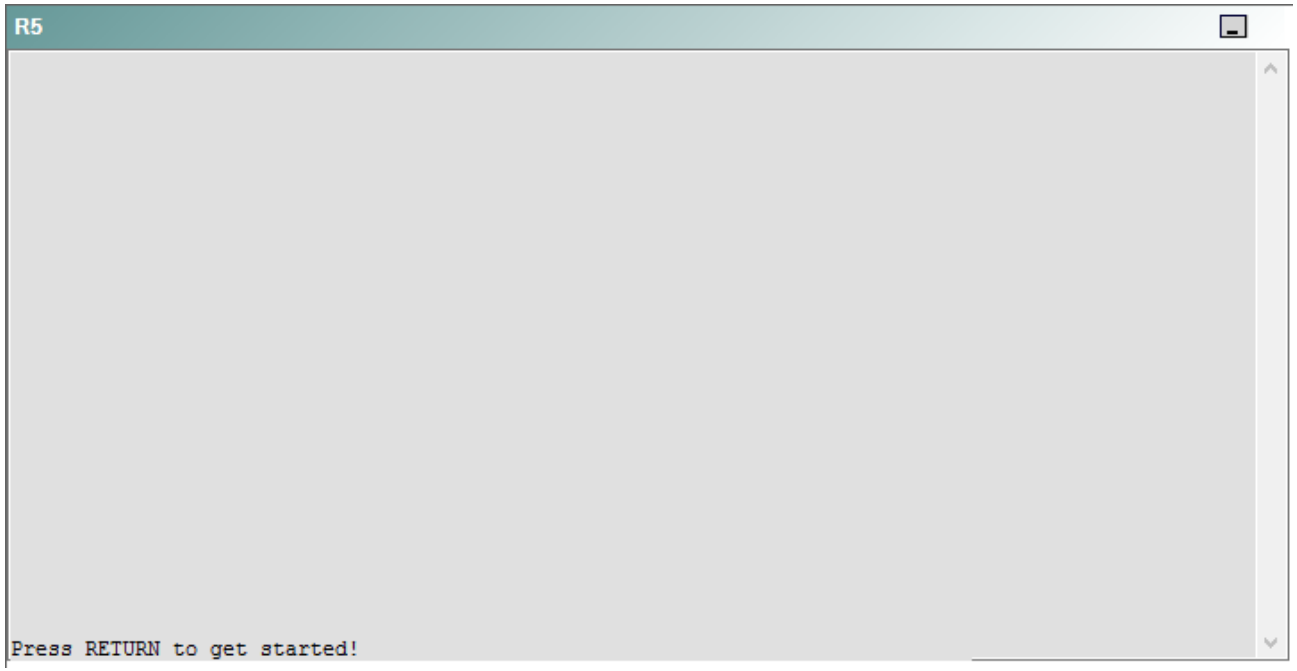

R3



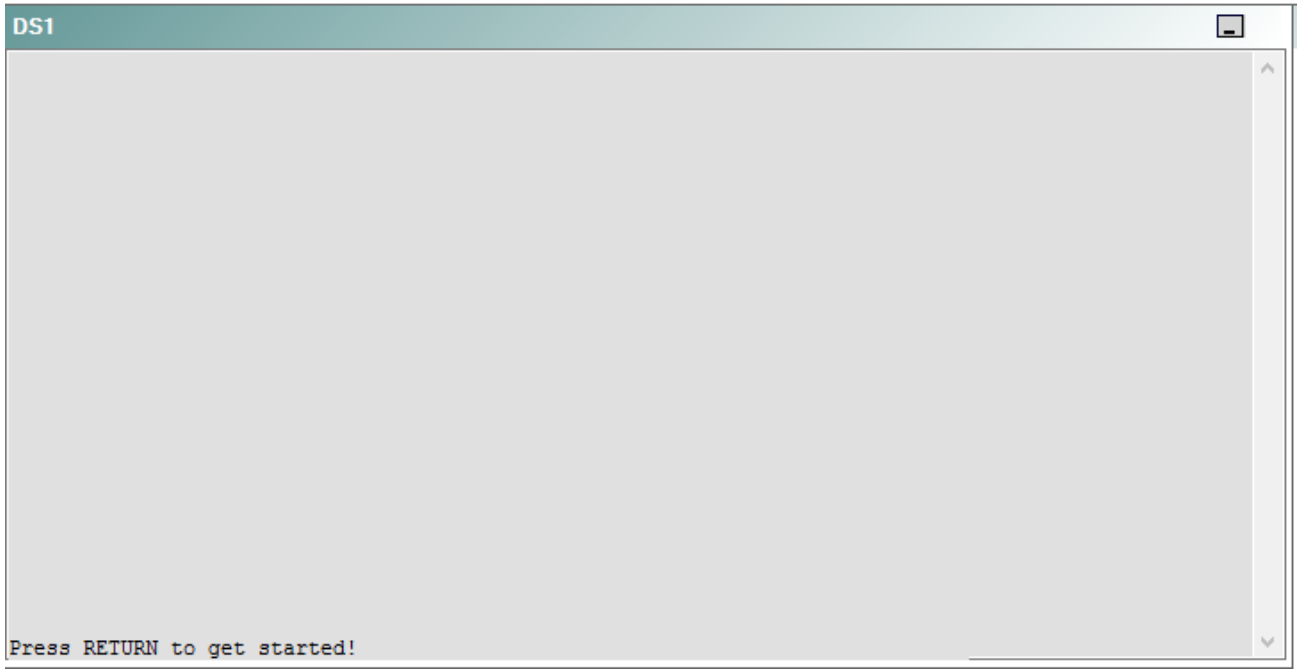

R4



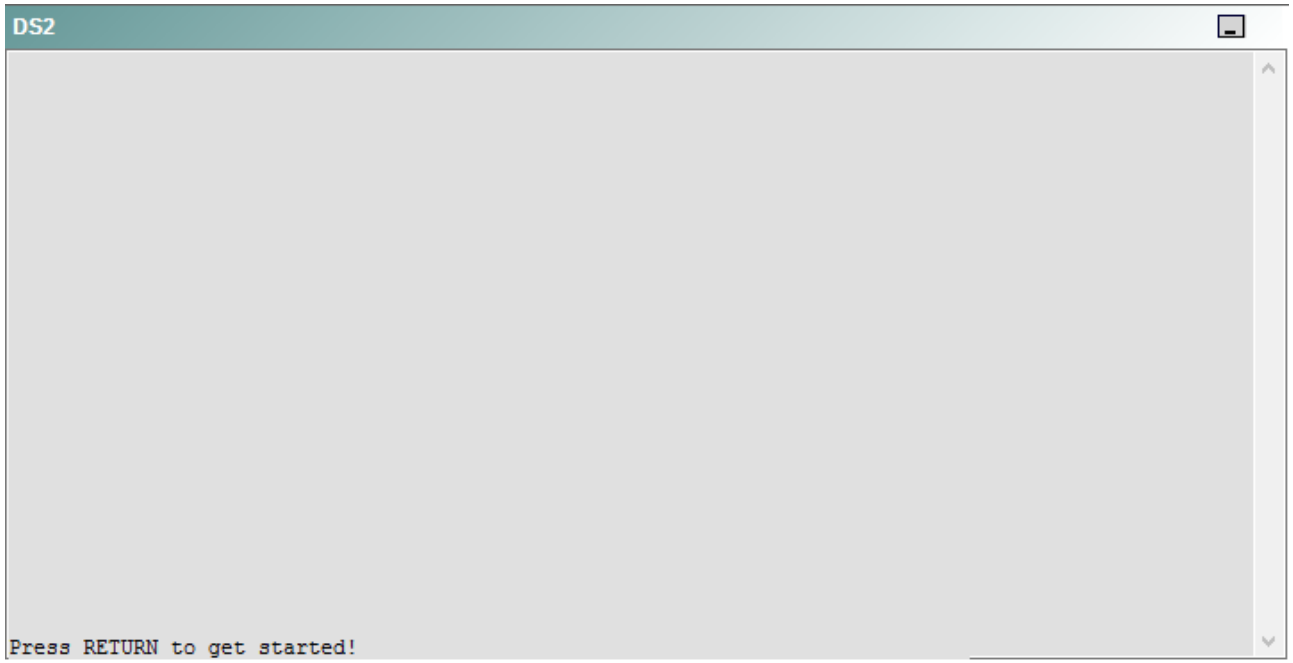

R5



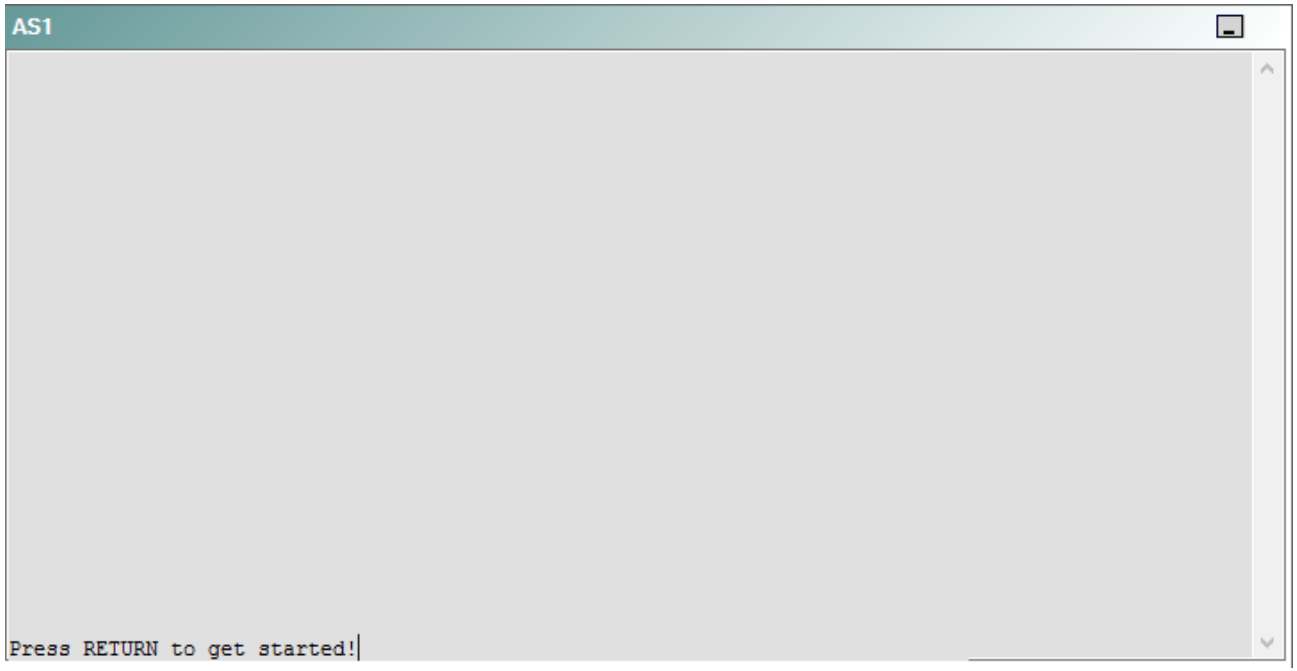

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. DHCP
C. Layer 3 addressing
D. Layer 3 security
E. Layer 2 security
F. STP
G. Etherchannel
H. VLAN configuration
I. interface

**Correct Answer:** I

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

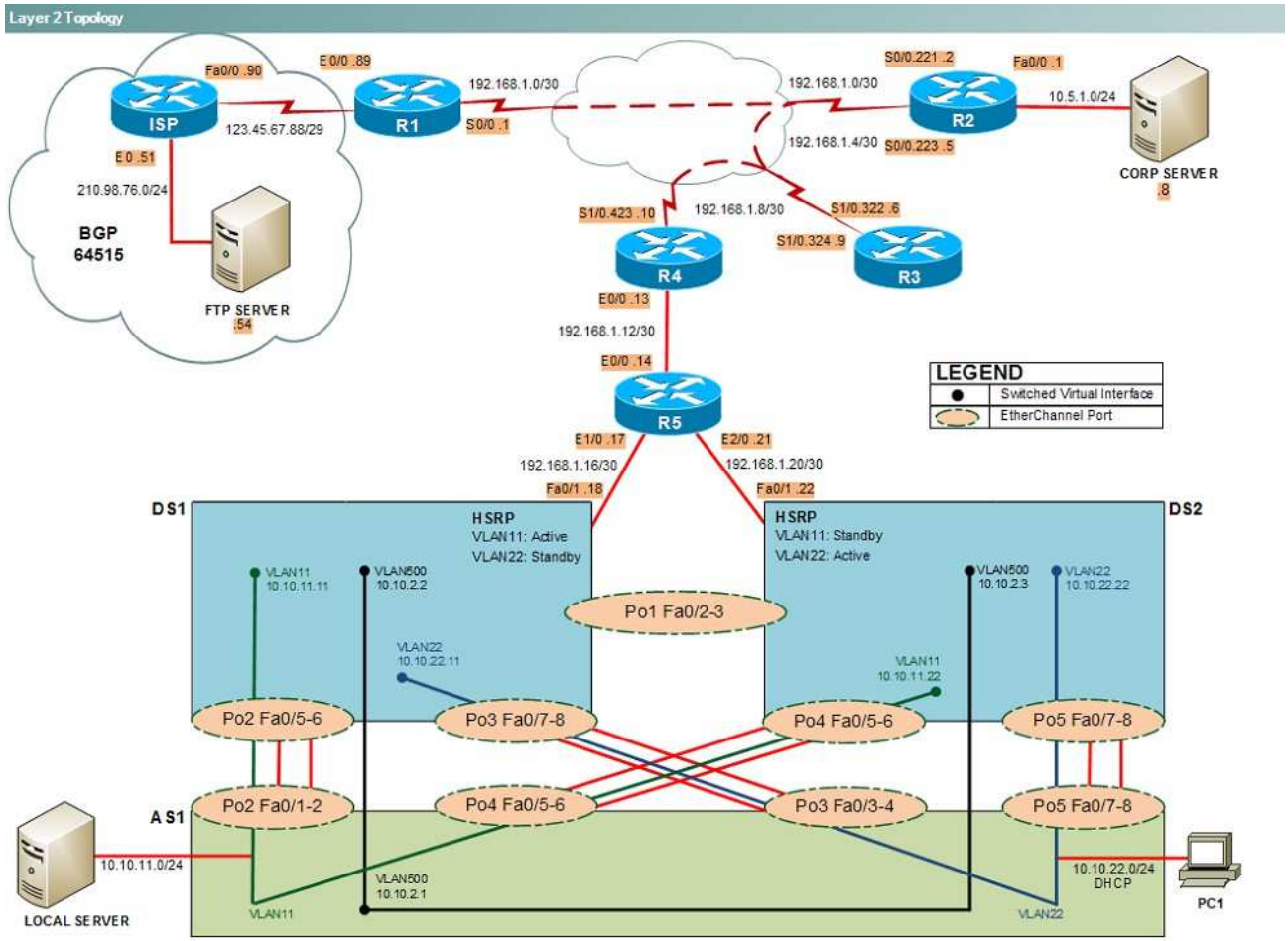
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

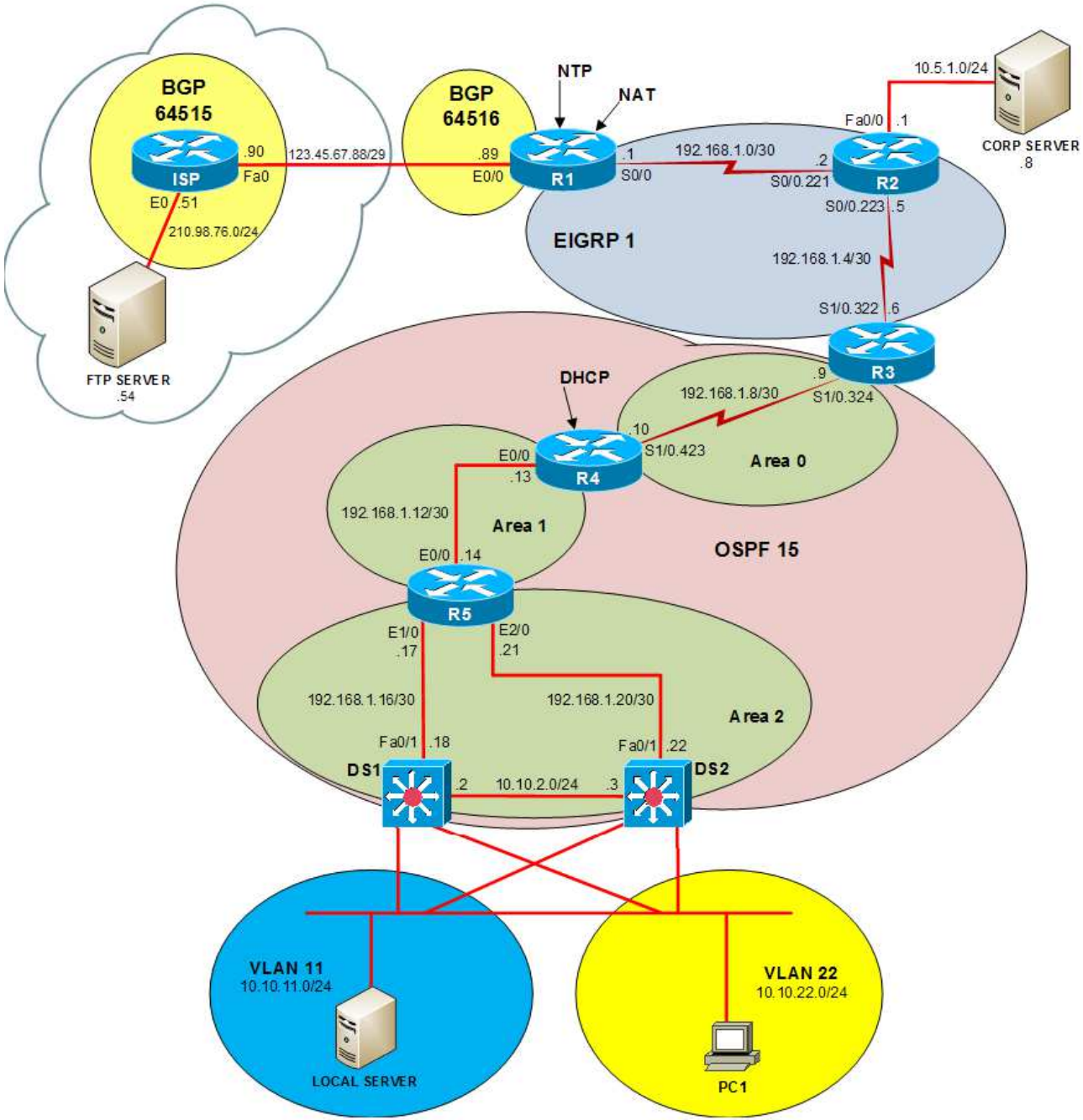
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

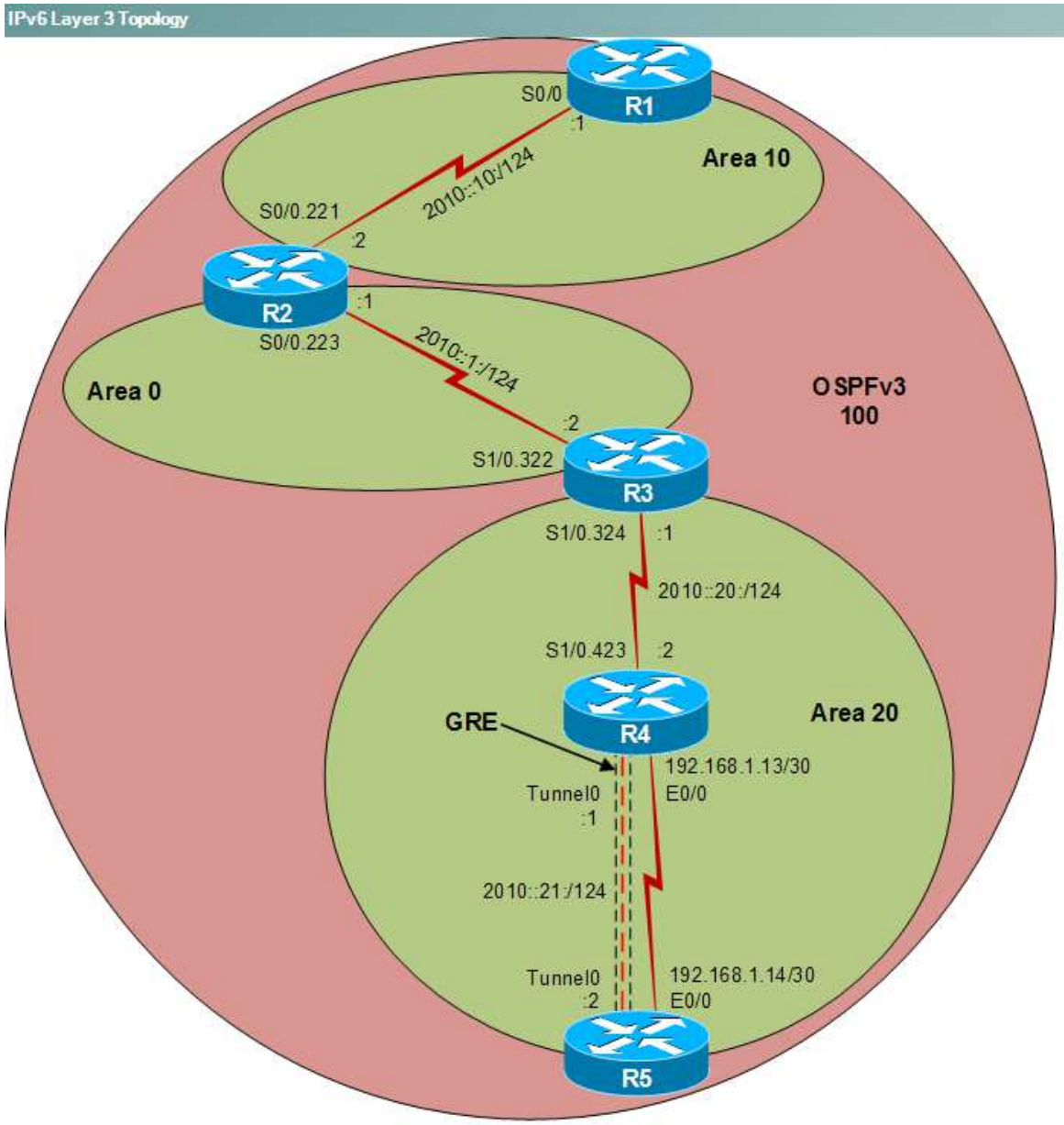
**Layer 2 Topology**




IPv4 layer 3 Topology

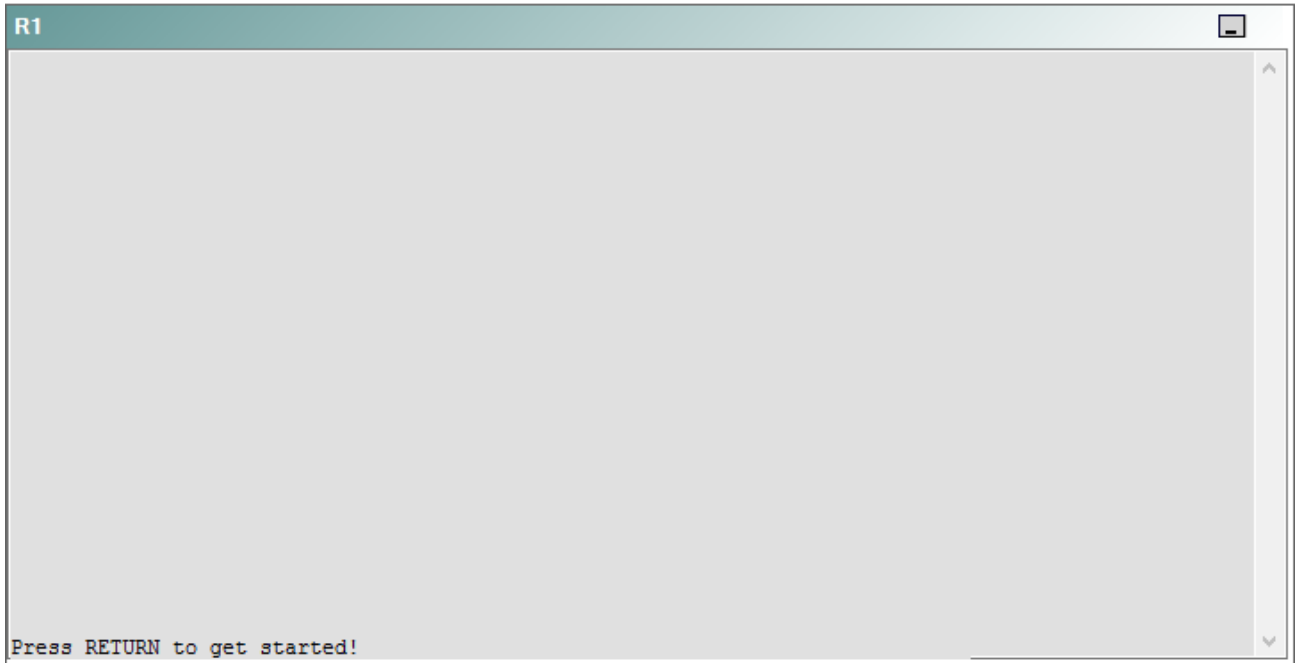

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

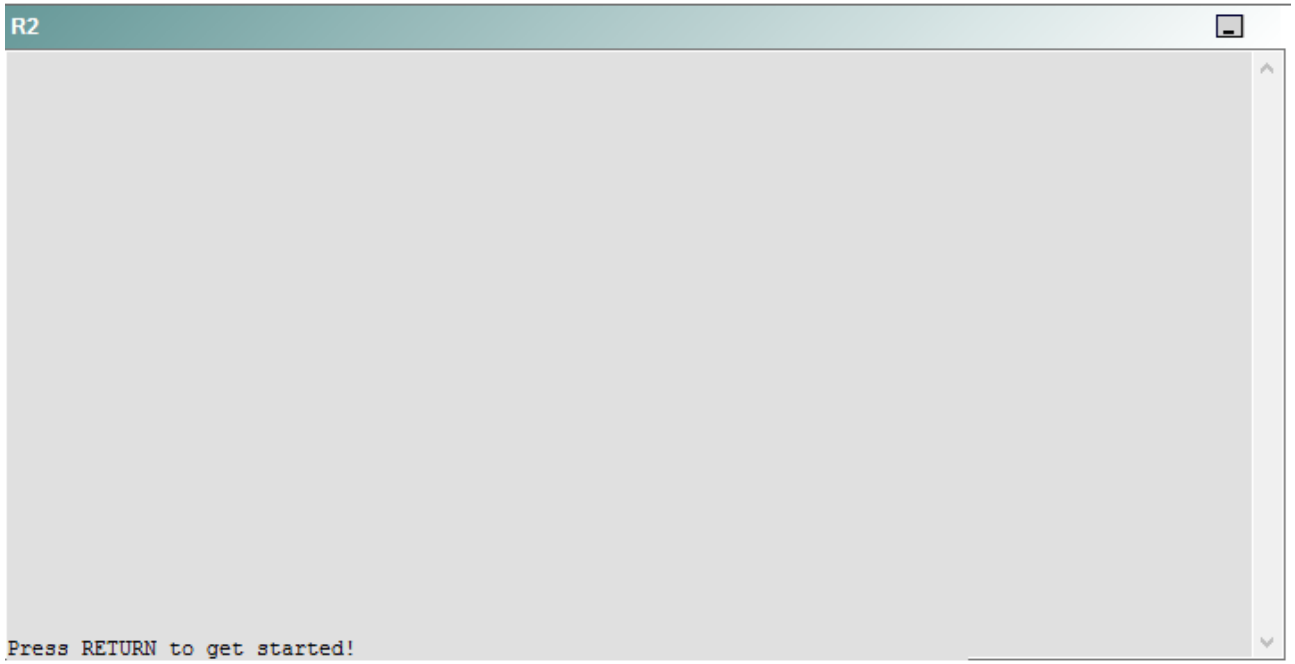



https://www.gratisexam.com/

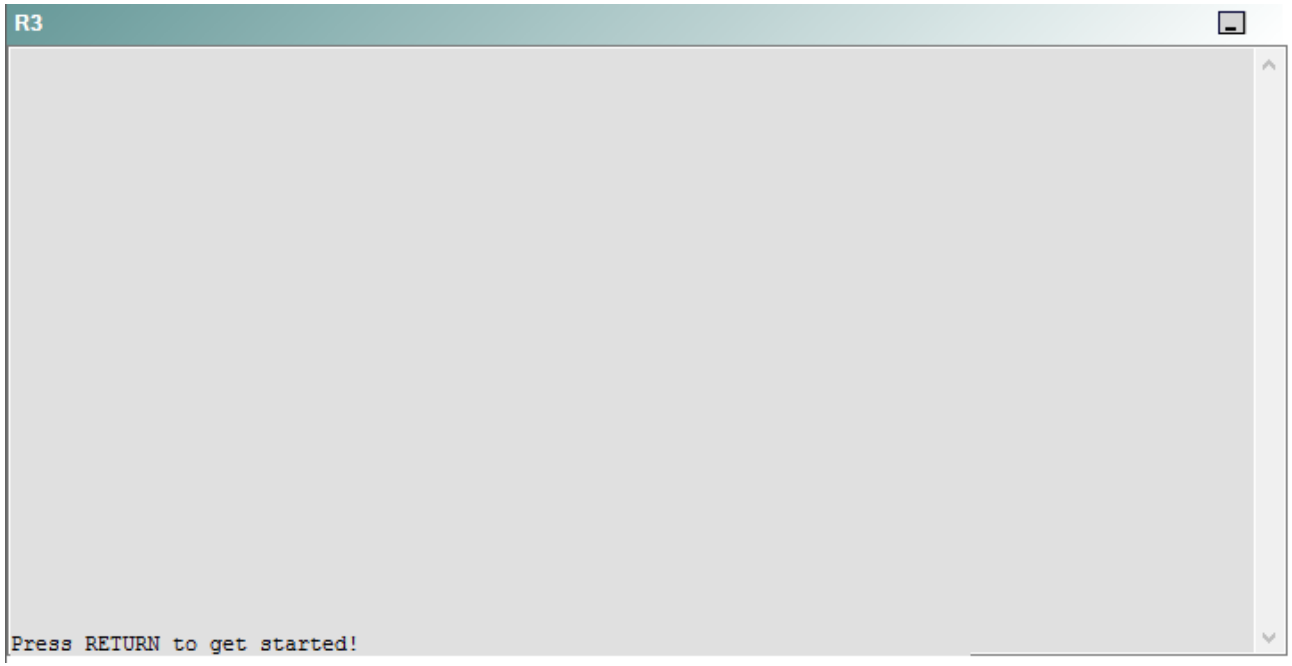
R1



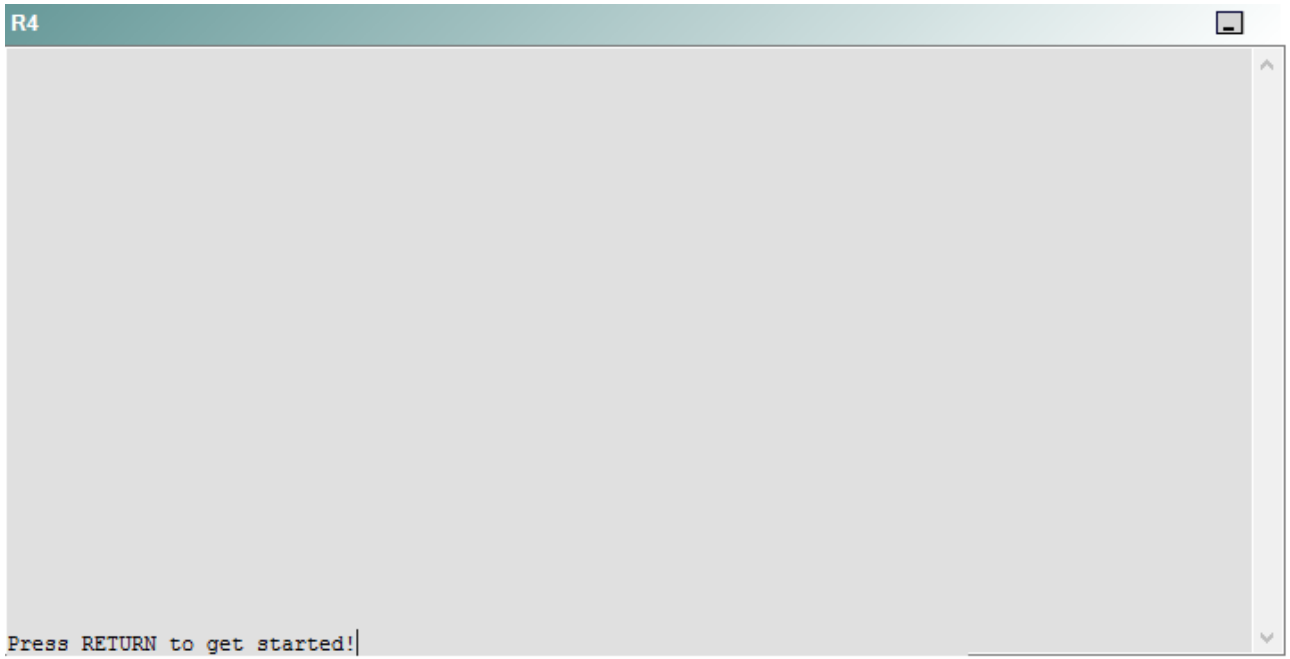

R2



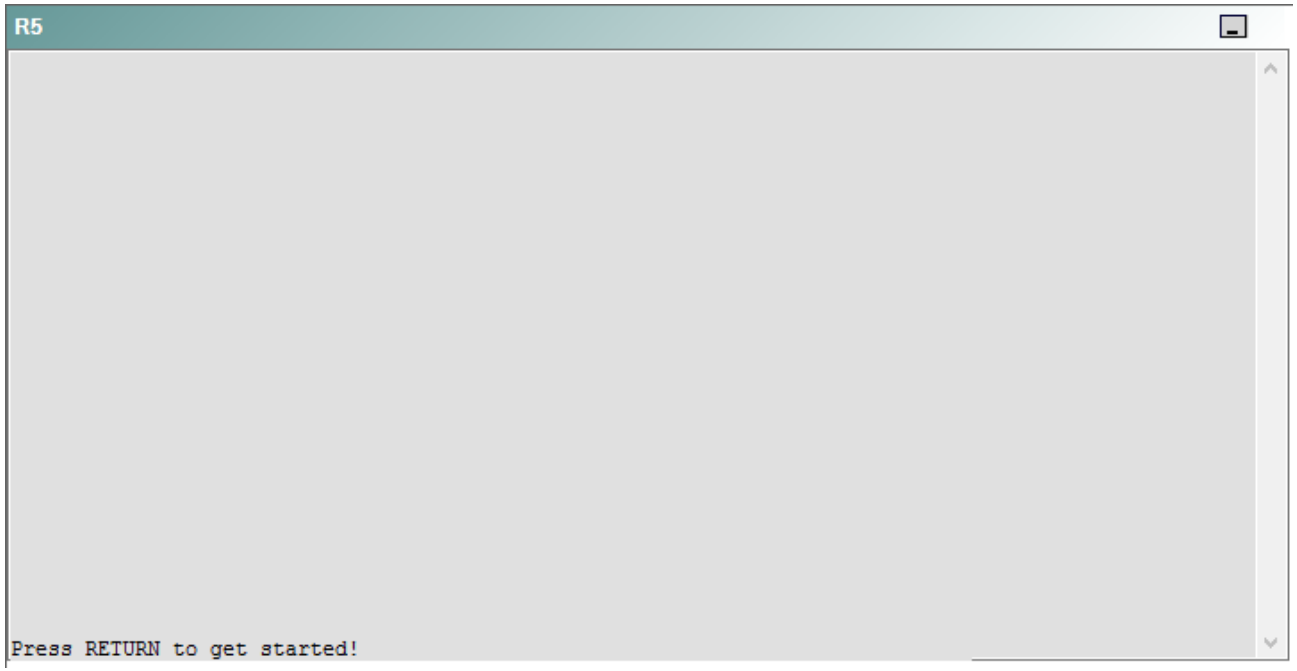

R3



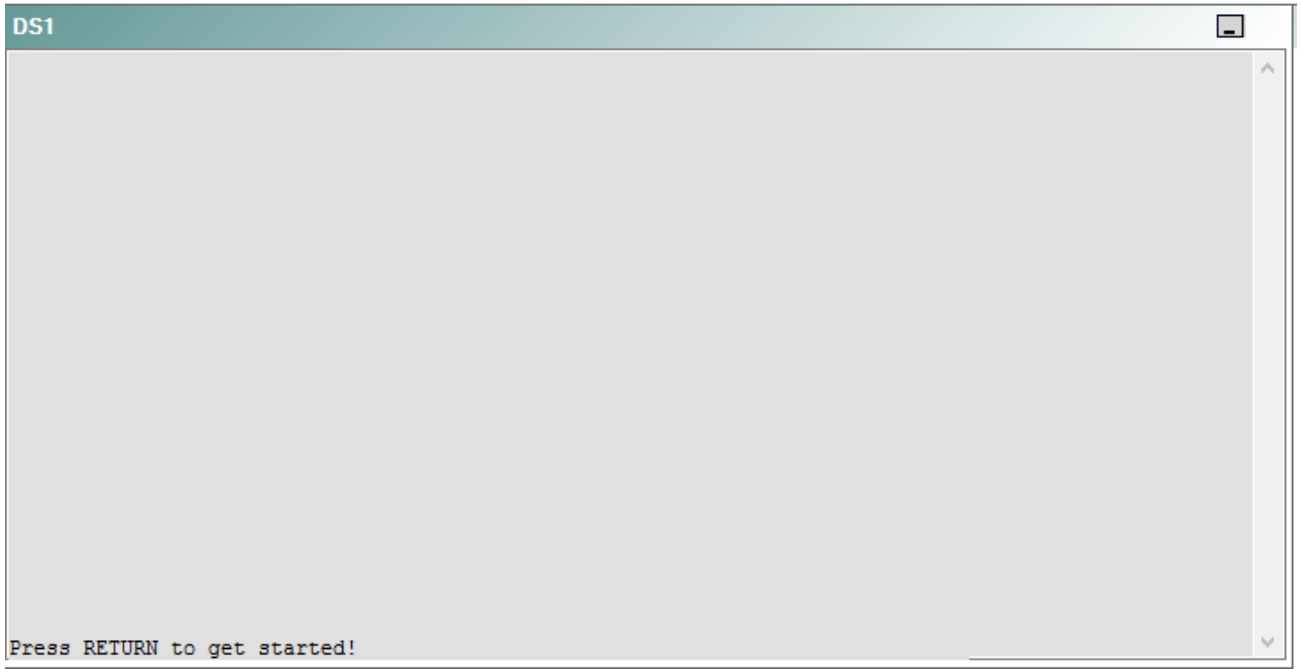

R4



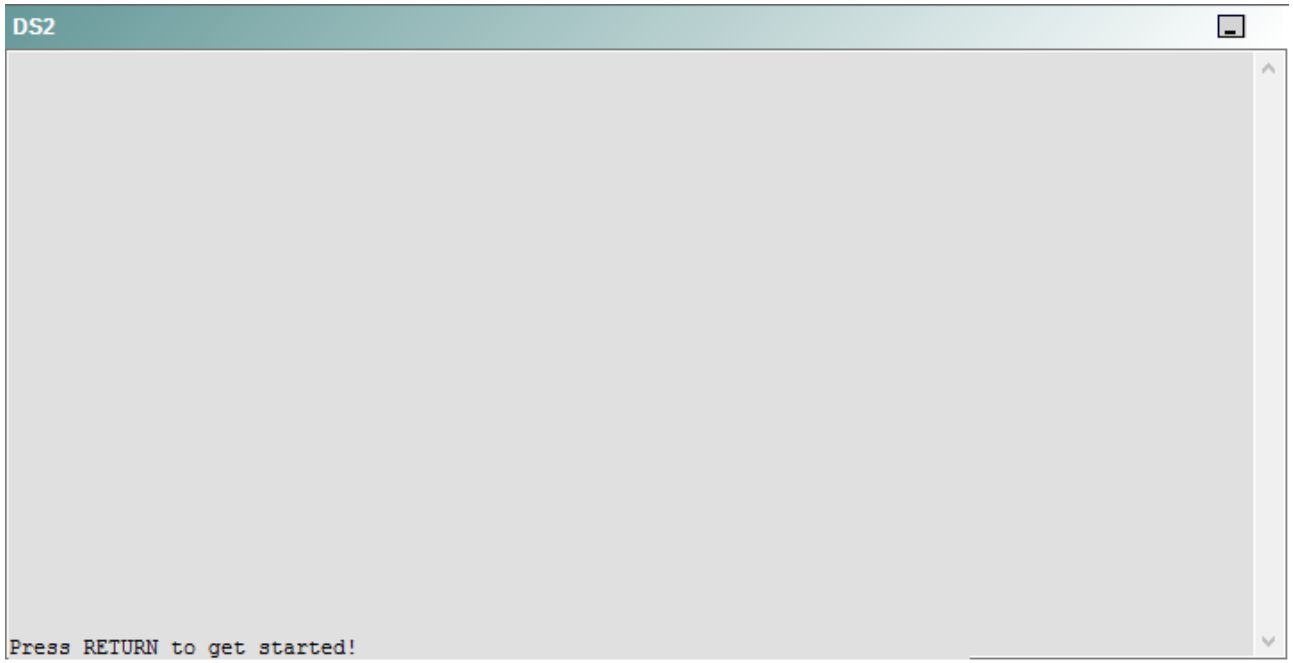

R5



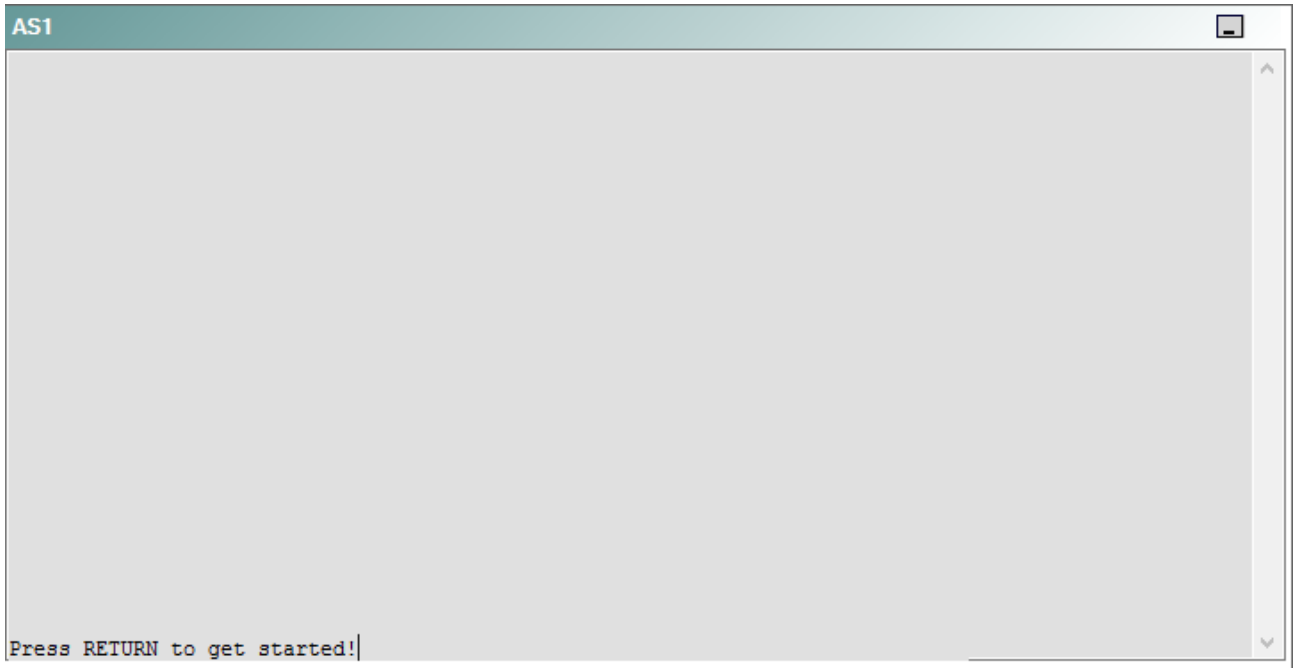

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. reconnecting the cable to the S1/0 interface
B. reconnecting the cable to the E0/0 interface
C. issuing the **no shutdown** command on the S1/0 interface
D. issuing the **no shutdown** command on the S1/0.423 interface
E. issuing the **clock rate 115200** command on the S1/0 interface
F. issuing the encapsulation frame-relay command on the S1/0.423 subinterface

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

You should reconnect the cable to the S1/0 interface on R4. To determine which device is the source of the problem, you can issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from PC1 to the closest device and work your way up the network until communication is lost, or you can ping from PC1 to the farthest device and work your way back to PC1 until pings are successful.

In this scenario, if you were to ping the E0/0 interface of R4 from PC1, the pings would be successful, as shown in the following output:

```
C:\>ping 192.168.1.13

Pinging 192.168.1.13 with 32 bytes of data:

Reply from 192.168.1.13: bytes=32 time=3ms TTL=253
Reply from 192.168.1.13: bytes=32 time=3ms TTL=253
Reply from 192.168.1.13: bytes=32 time=3ms TTL=253
Reply from 192.168.1.13: bytes=32 time=3ms TTL=253

Ping statistics for 192.168.1.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

However, if you were to ping the S1/0 interface of R4 from PC1, you would receive the following output:

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 10.10.22.22: Destination host unreachable.
Reply from 10.10.22.22: Destination host unreachable.
Reply from 10.10.22.22: Destination host unreachable.
Reply from 10.10.22.22: Destination host unreachable.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Therefore, the problem likely exists on R4 or beyond.

Once you have determined where connectivity is lost, you can begin to troubleshoot what is causing the problem. Issuing the **show interfaces Ethernet 0/0** command on R4 reveals that the interface is up and the line protocol is up. However, issuing the **show interfaces Serial 1/0** command on R4 reveals that the interface is down and the line protocol is down, as shown in the following partial output:

```
R4#show interfaces Serial 1/0
Serial1/0 is down, line protocol is down
```

The interface status message *Serial1/0 is down, line protocol is down* indicates that there is a problem at Layer 1 of the Open Systems Interconnection (OSI) model, which is the Physical layer. When you receive this interface status message, you should check both ends of the physical cable to see if they are securely connected to the proper interfaces. You can confirm whether the cable is disconnected from the S1/0 interface by issuing the **show controllers Serial 1/0** command. Because no cable is connected to the interface, you will receive the following partial output:

```
R4#show controllers Serial 1/0
CD2430 Slot 1, Port 0, Controller 0, Channel 0, Revision 19
Channel mode is synchronous serial
idb 0x82B9EBC0, buffer size 1524, No cable
```

After you connect the cable to the interface, you will receive the following partial output when you issue the **show interfaces Serial 1/0** command.

```
R4# show interfaces Serial 1/0
Serial1/0 is up, line protocol is up
```

Although the **show interfaces Serial 1/0.324** command on R3 indicates that the interface is down and the line protocol is down, this is because R3 cannot communicate with R4 and not because of a misconfiguration on R3. Therefore, you do not need to do anything on R3.

You do not need to issue the **clock rate 115200** command on the S1/0 interface of R4. If the lack of clocking were the problem, you would receive the following partial output when you issue the **show interfaces Serial 1/0** command:

```
R4#show interfaces Serial 1/0
Serial1/0 is up, line protocol is down
```

The data circuit-terminating equipment (DCE) end of the serial cable typically provides clocking, and the data terminal equipment (DTE) end of the serial cable does not. You can determine which end of the serial cable is connected to the S1/0 interface by issuing the **show controllers Serial 1/0** command. In this scenario, if the cable had been connected, you would have seen that the DTE end of the cable was connected to the S1/0 interface, as shown in the following partial output:

```
R4#show controllers Serial 1/0
CD2430 Slot 1, Port 0, Controller 0, Channel 0, Revision 19
Channel mode is synchronous serial
idb 0x82B9EBC0, buffer size 1524, V.35 DTE cable
```

If the DCE end of the cable had been connected to the S1/0 interface, you would have seen the following partial output:

```
R4#show controllers Serial 1/0
CD2430 Slot 1, Port 0, Controller 0, Channel 0, Revision 19
Channel mode is synchronous serial
idb 0x82B9EBC0, buffer size 1524, V.35 DCE cable
```

You do not need to issue the **no shutdown** command on the S1/0 interface or the S1/0.423 subinterface. The **no shutdown** command is used to enable an interface that has been administratively shut down by the **shutdown** command. If the interface had been administratively shut down, you would have seen the following partial output from the **show interfaces Serial 1/0** command:

```
R4#show interfaces Serial 1/0
Serial1/0 is administratively down, line protocol is down
```

You cannot issue the **encapsulation frame-relay** command on the S1/0.423 subinterface. The **encapsulation frame-relay** command can be issued only on the S1/0 interface.

You should not create Frame Relay maps on the S1/0.423 subinterface. Frame Relay maps cannot be created on point-to-point subinterfaces. To create a Frame Relay map, you would issue the **frame-relay map ip** *ip-address dlci* [**broadcast**] [ **ietf** | **cisco**] command.

You need not change the data link connection identifier (DLCI) on the subinterfaces. A DLCI is an address that uniquely identifies a permanent virtual circuit (PVC) connection in a Frame Relay circuit. Each DLCI is locally significant, which means that the routers at each end of the PVC can use different DLCIs to identify the same circuit.

You need no change the interface type to point-to-multipoint on the subinterfaces. The S1/0 interface on R4 is currently configured so that it can communicate only with its upstream router, not with all the routers attached to the Frame Relay cloud.
If you were to change the interface type to point-to-multipoint, you would also have to configure Frame Relay maps. To configure the interface type for a subinterface, you would issue the **interface** *type slot/ port.subinterface* [**multipoint** | **point-to-point**] command.

**QUESTION 36**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

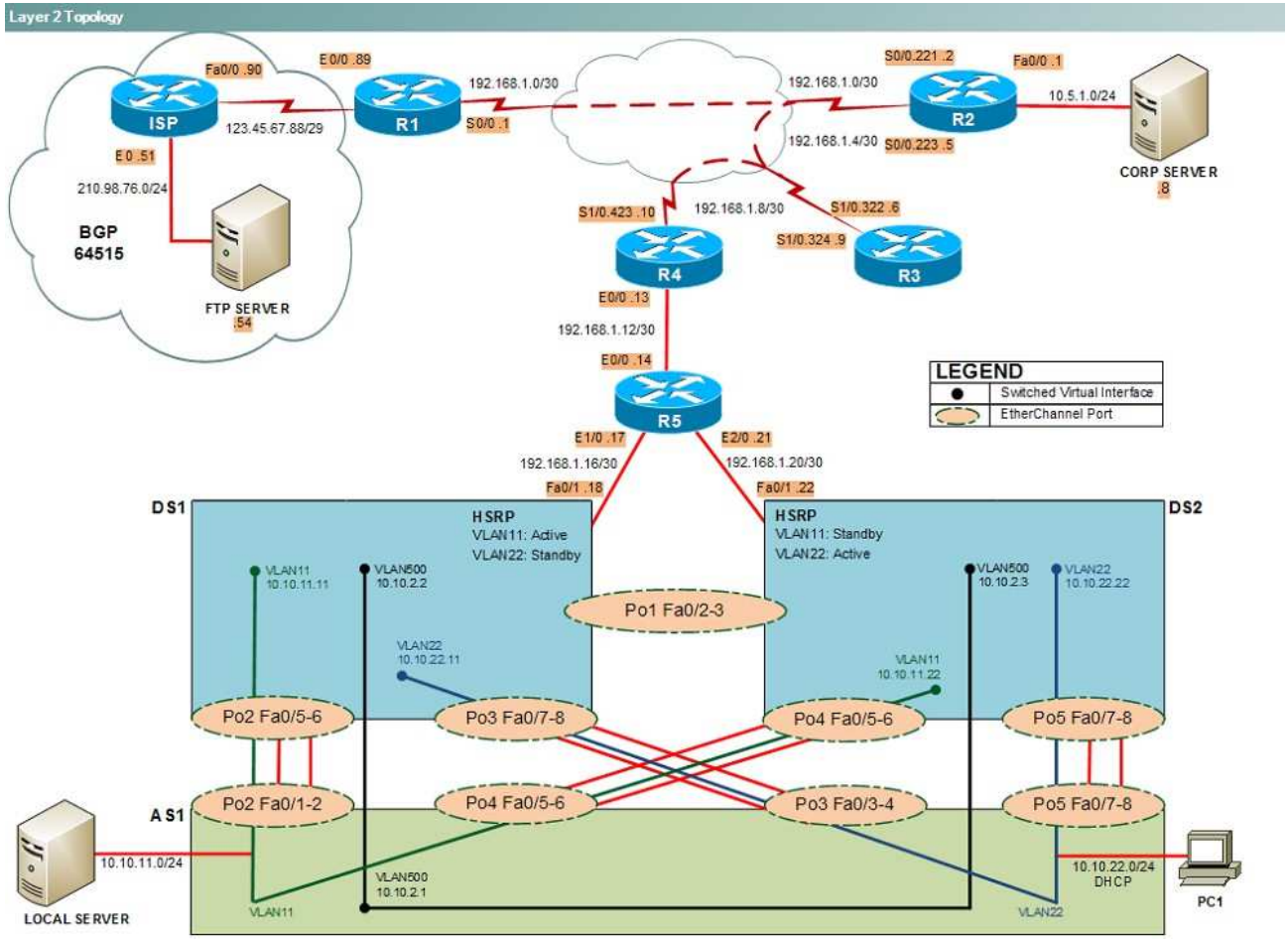
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

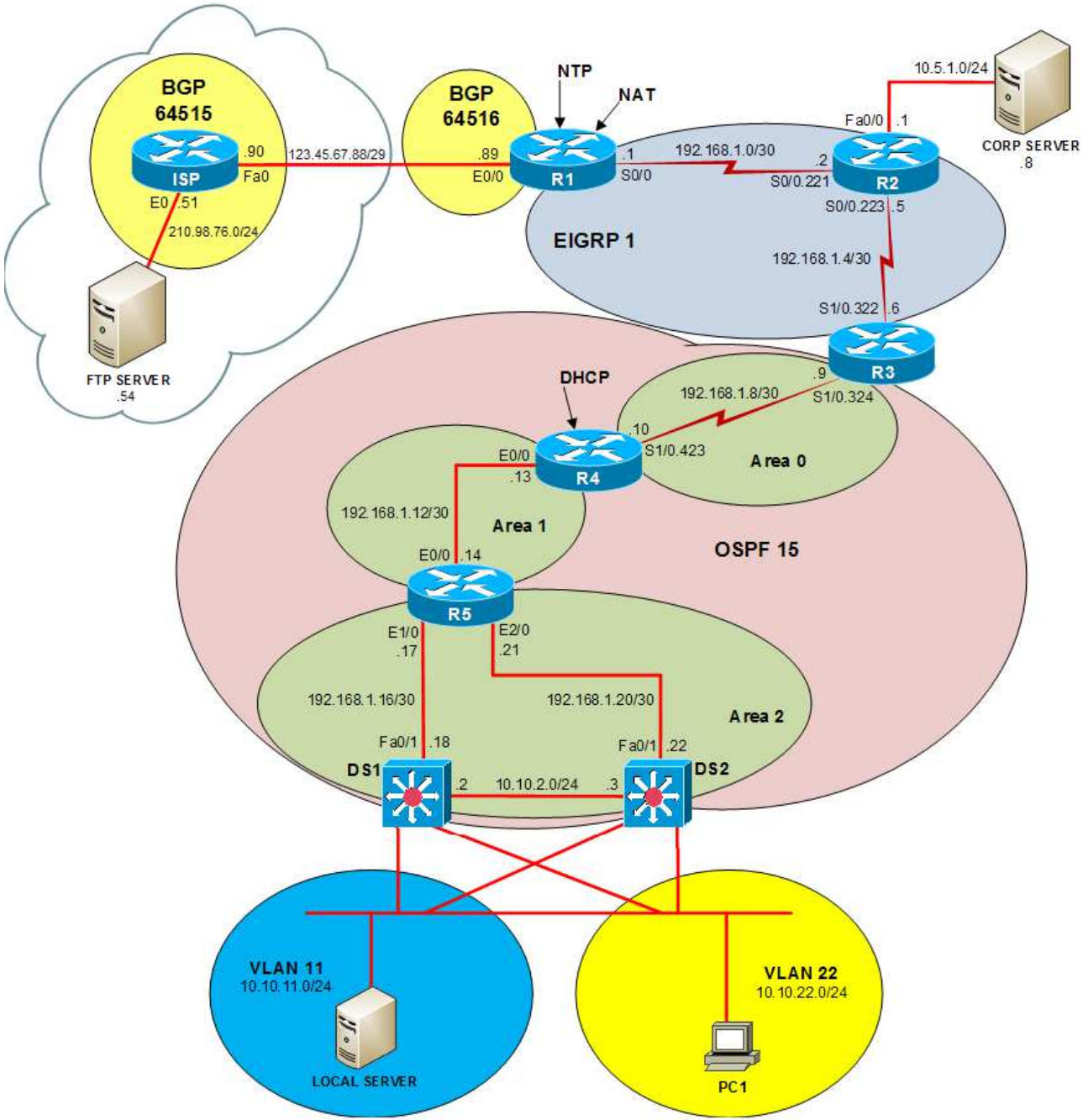
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

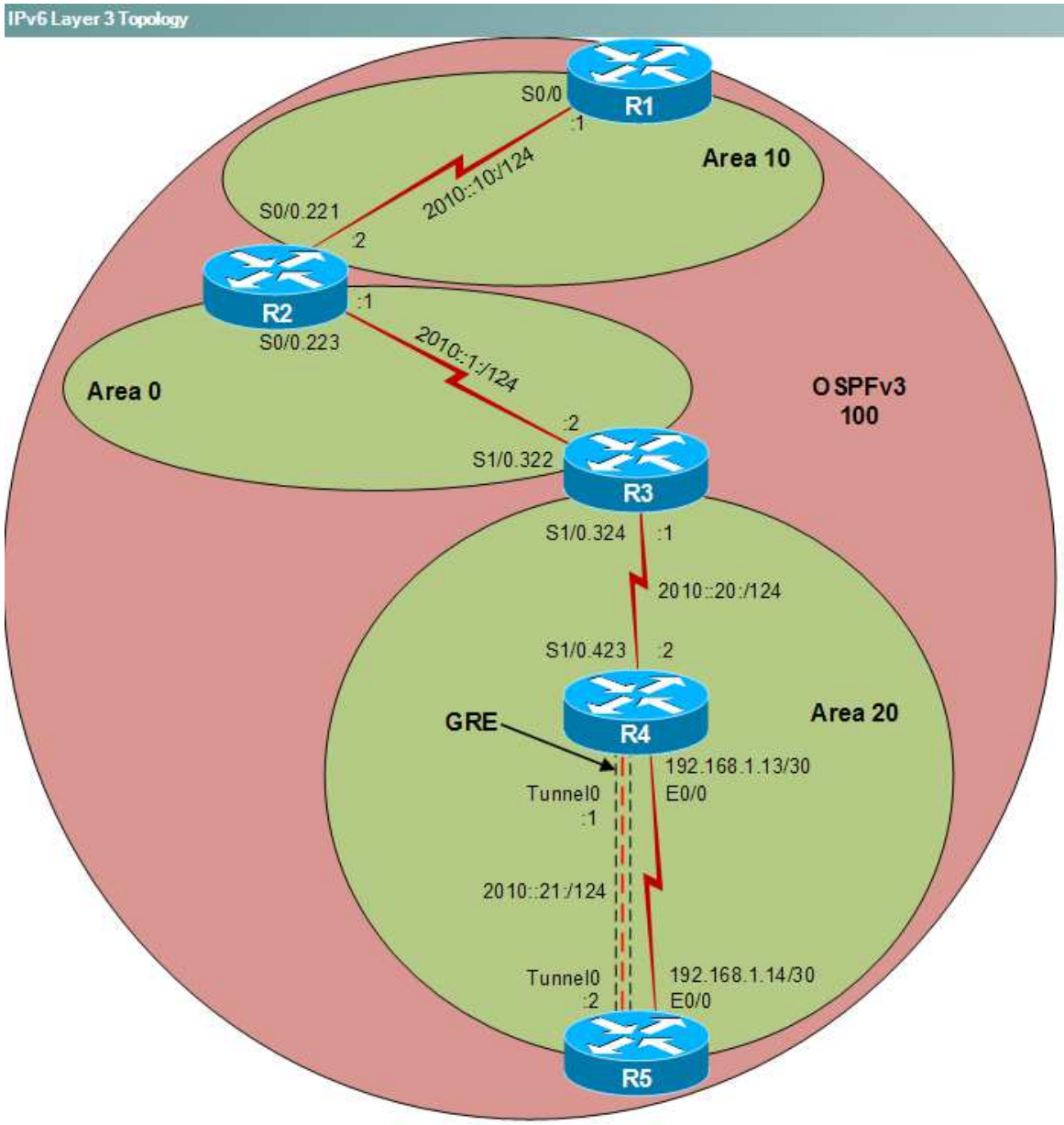
**Layer 2 Topology**




IPv4 layer 3 Topology

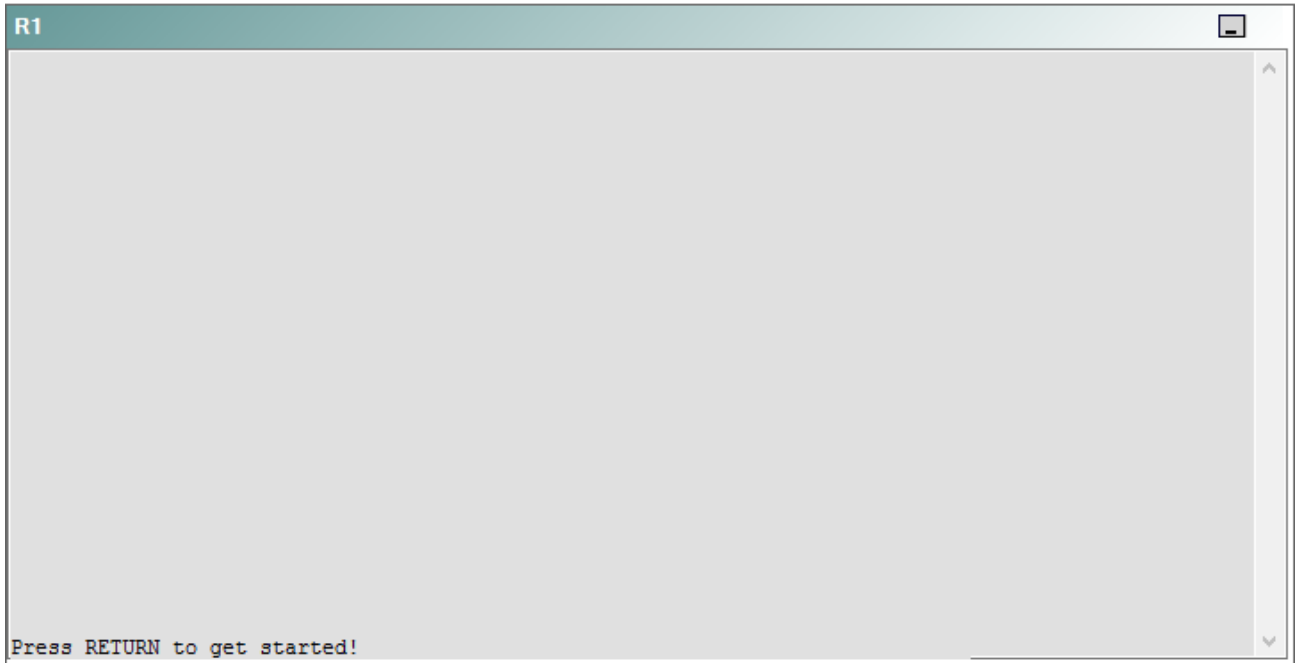

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

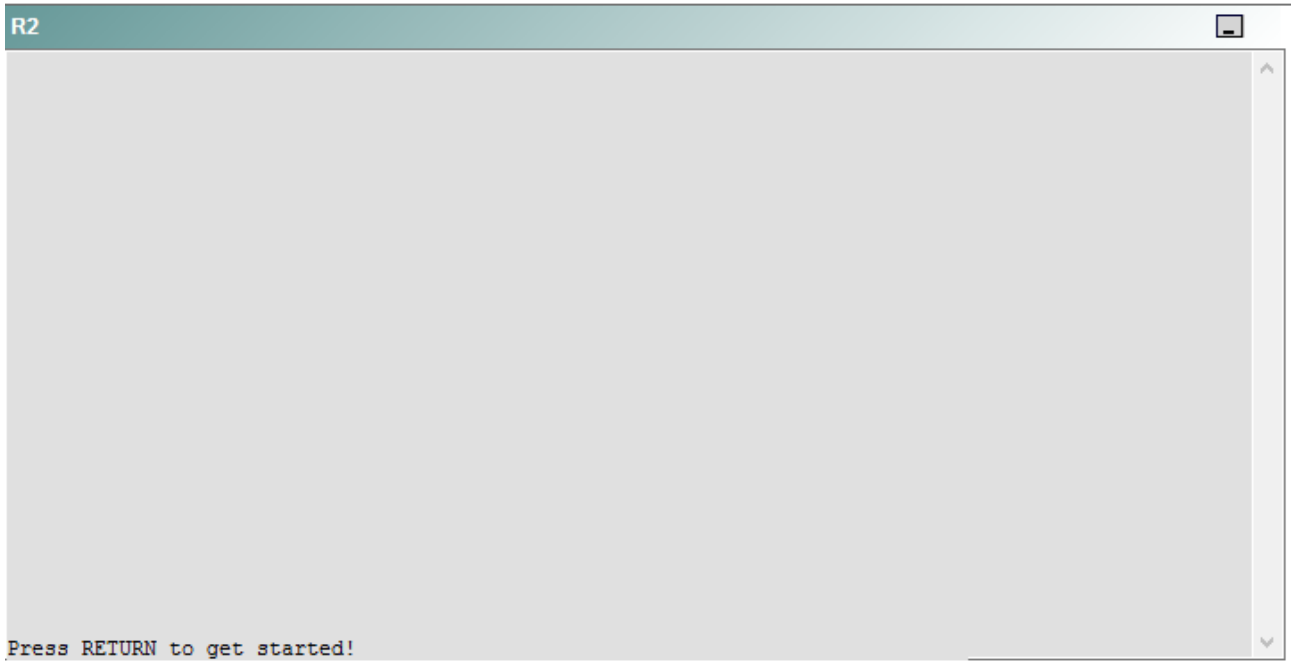



https://www.gratisexam.com/

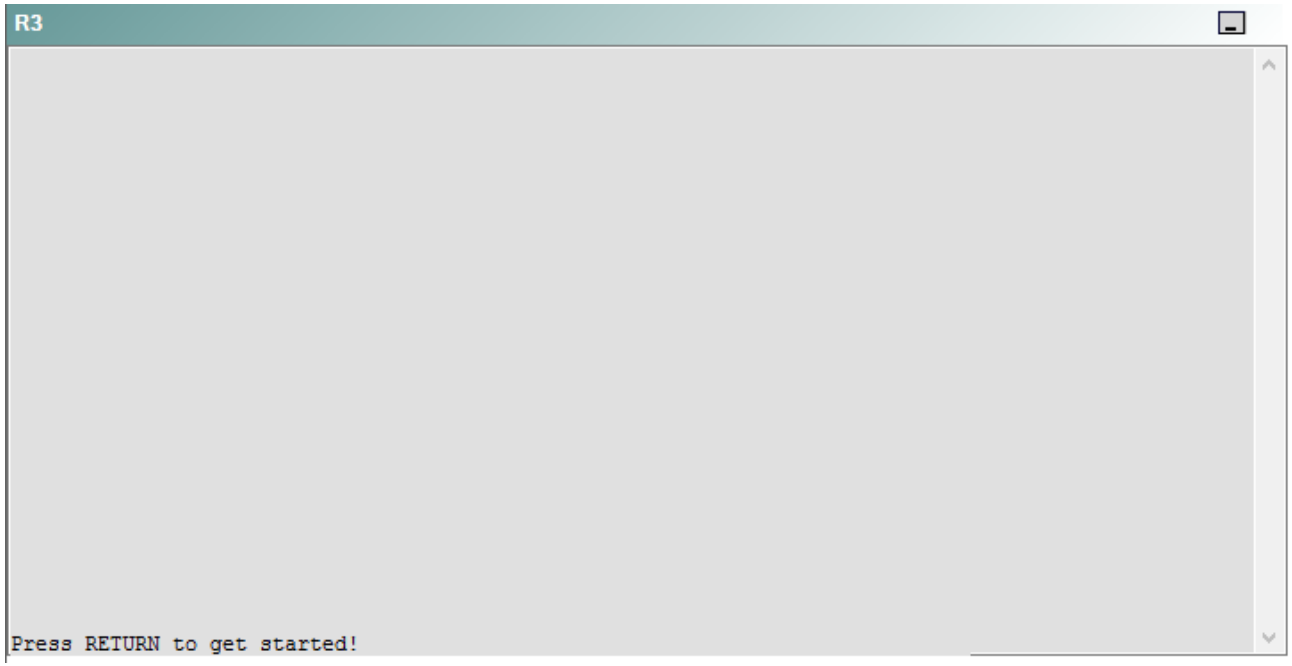
R1



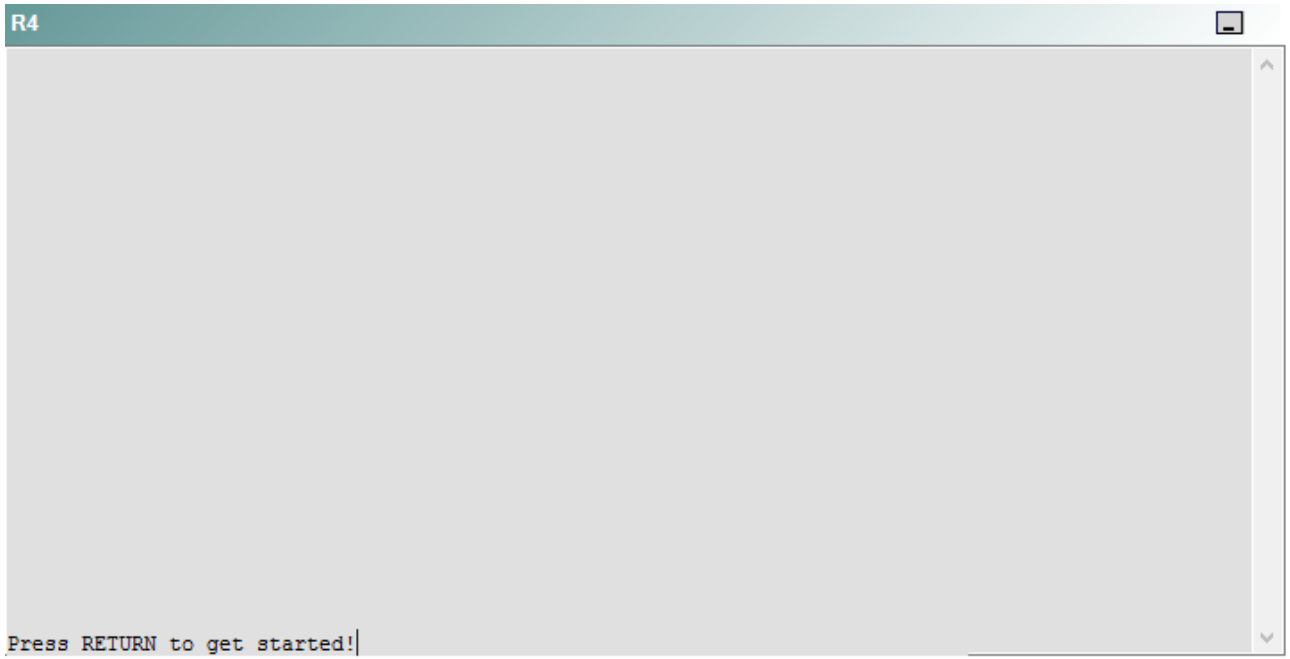

R2



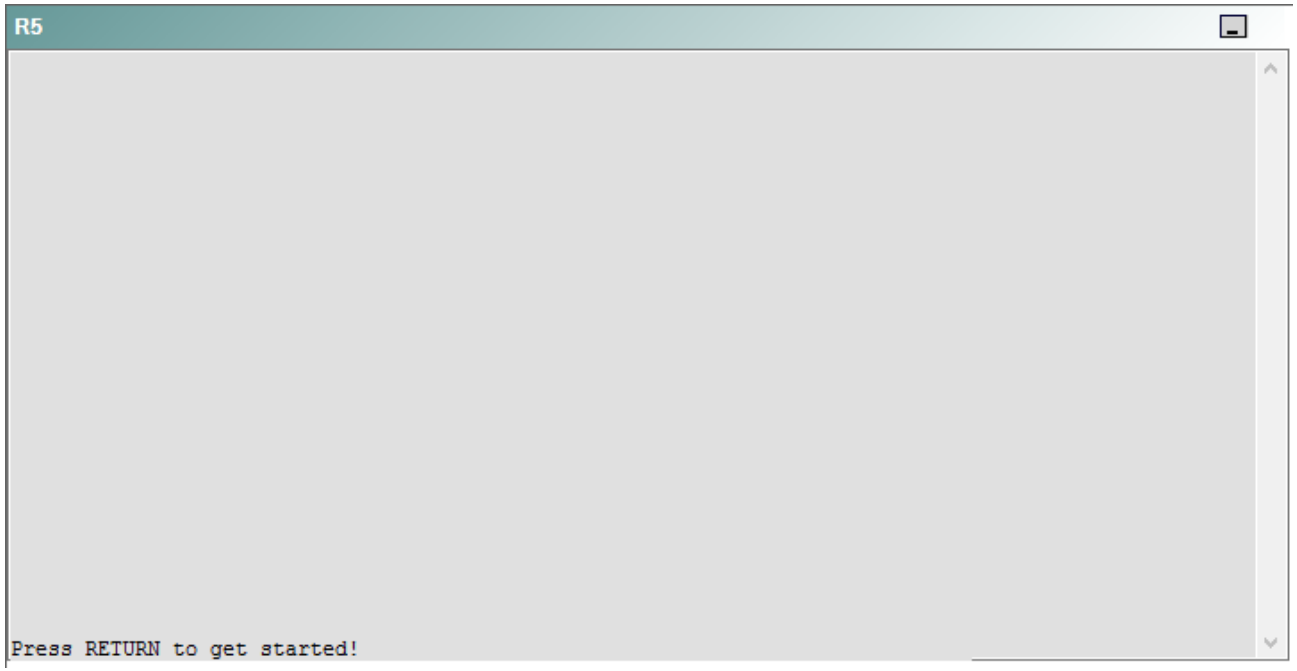

R3



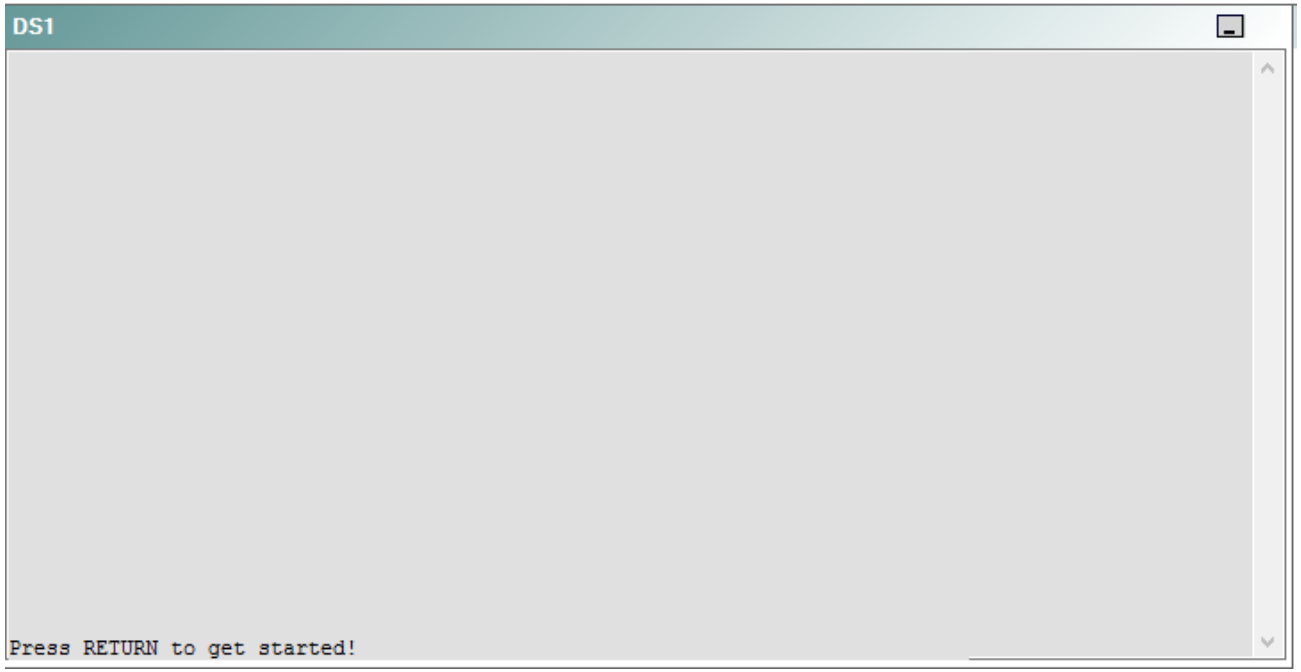

R4



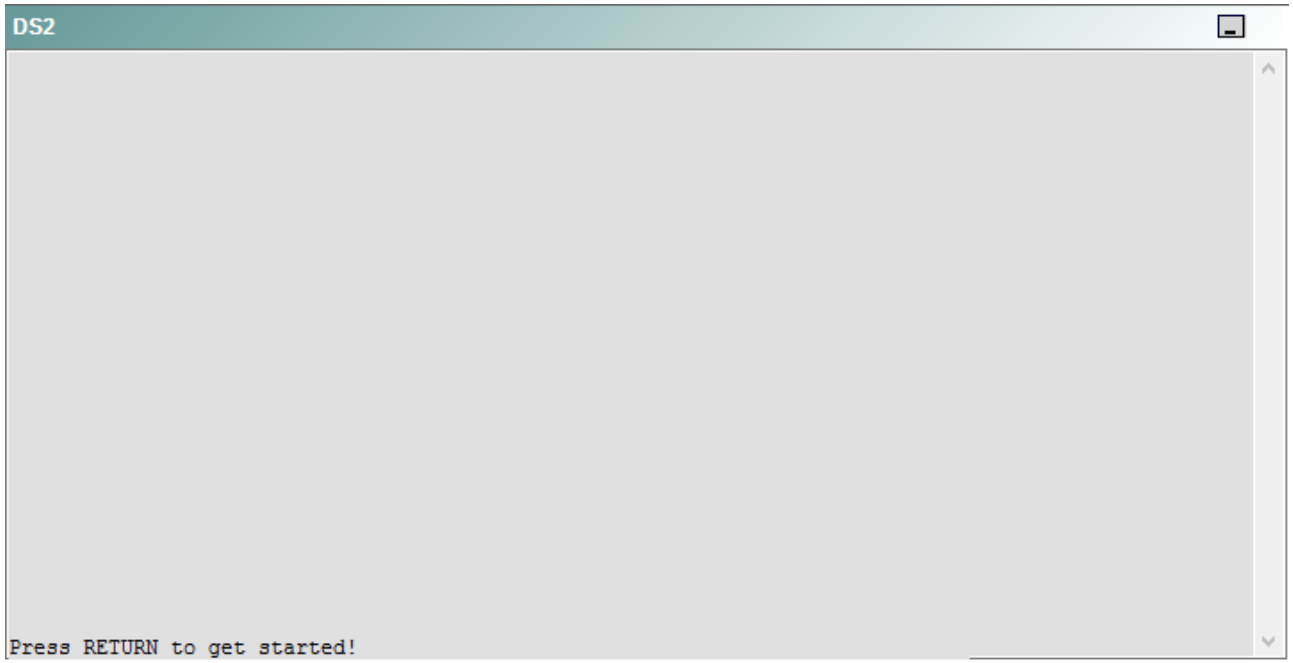

R5



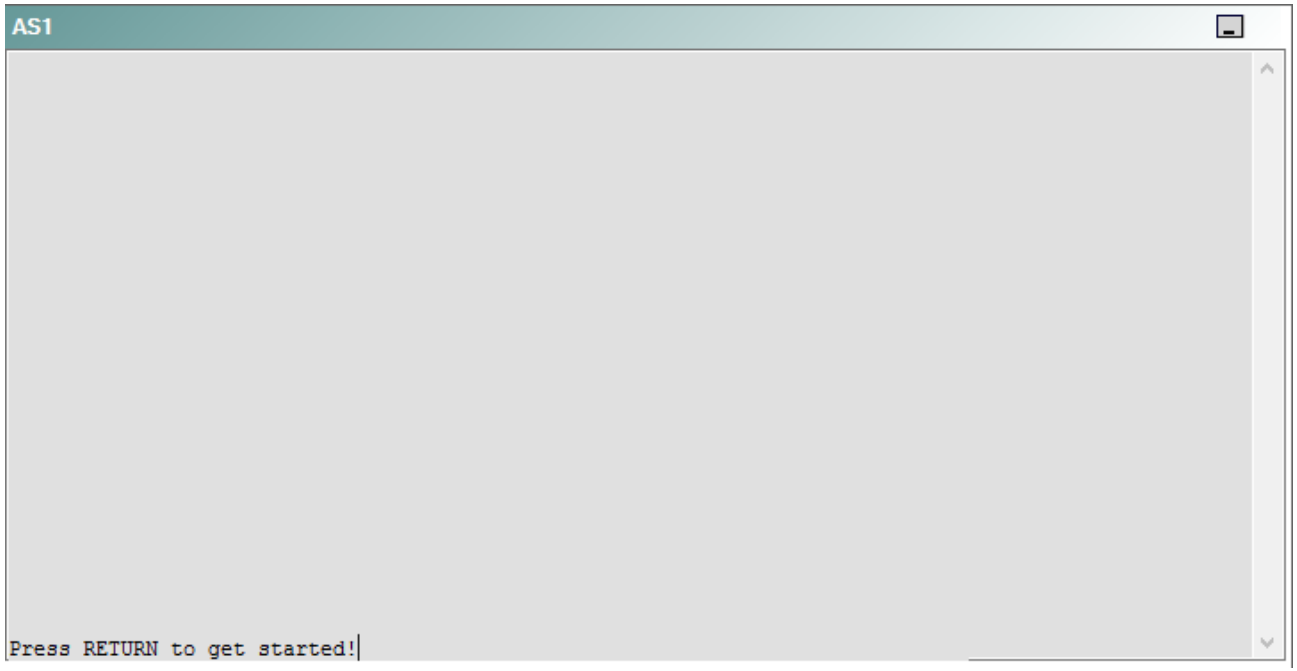

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

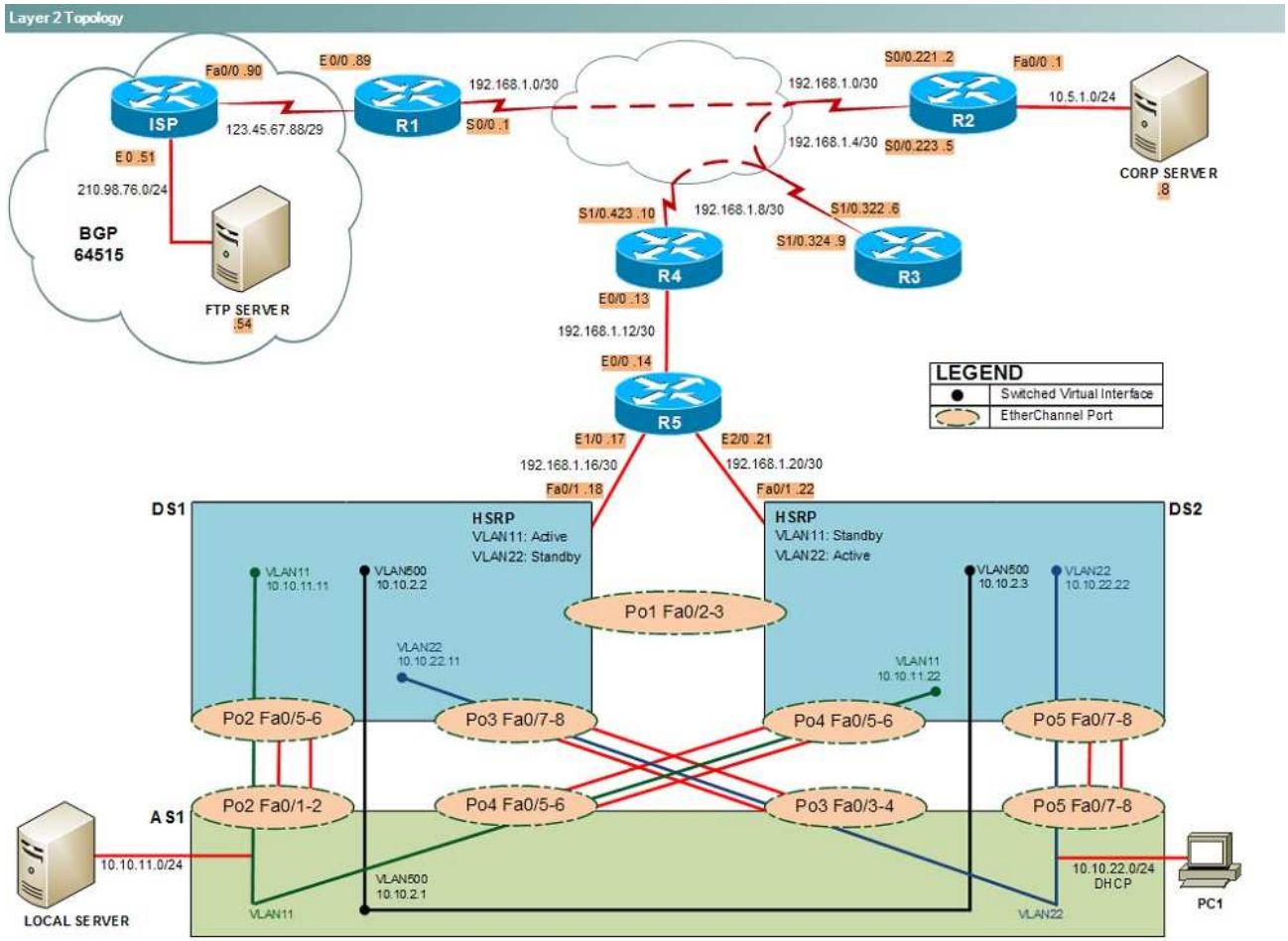
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

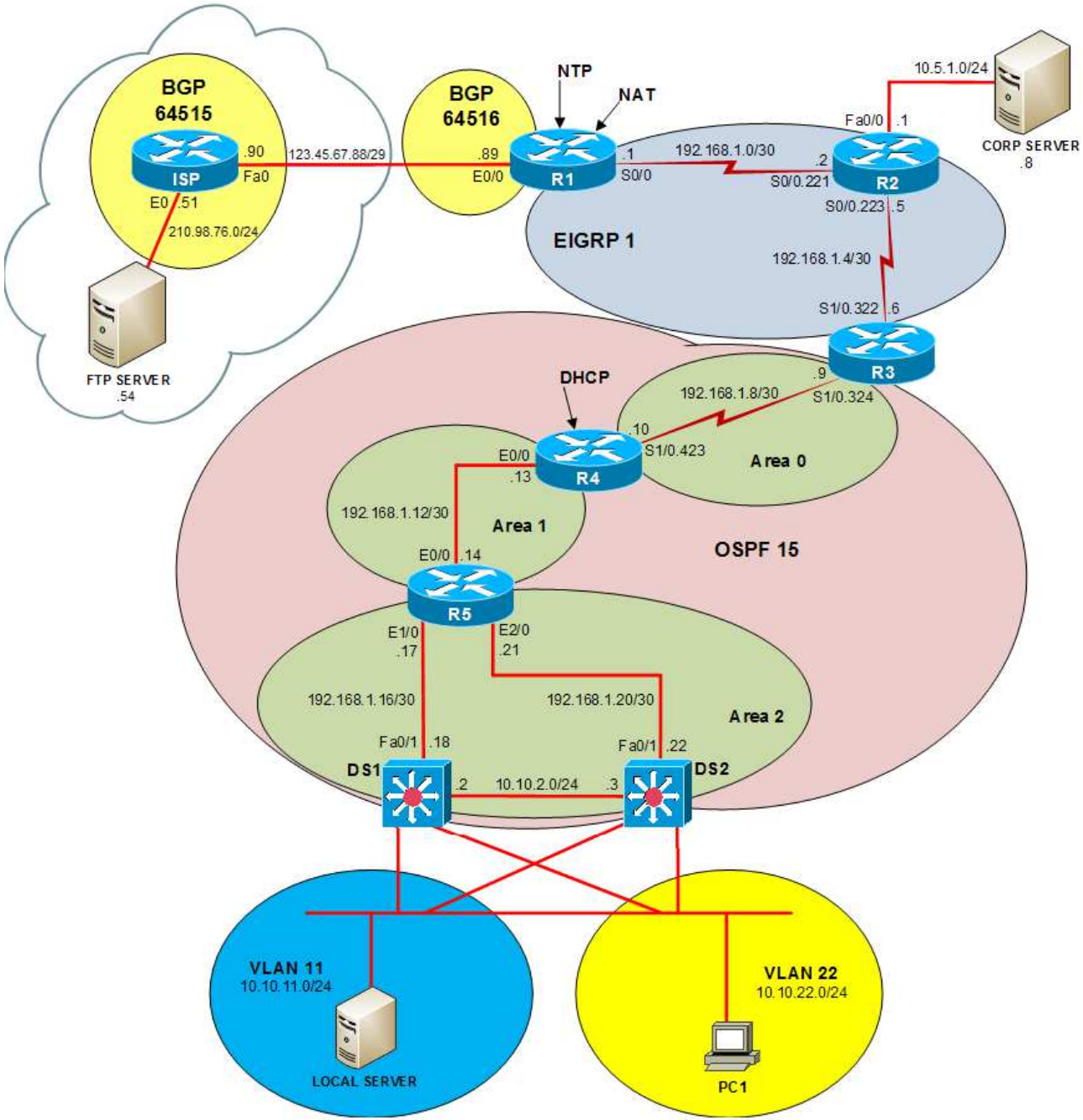
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

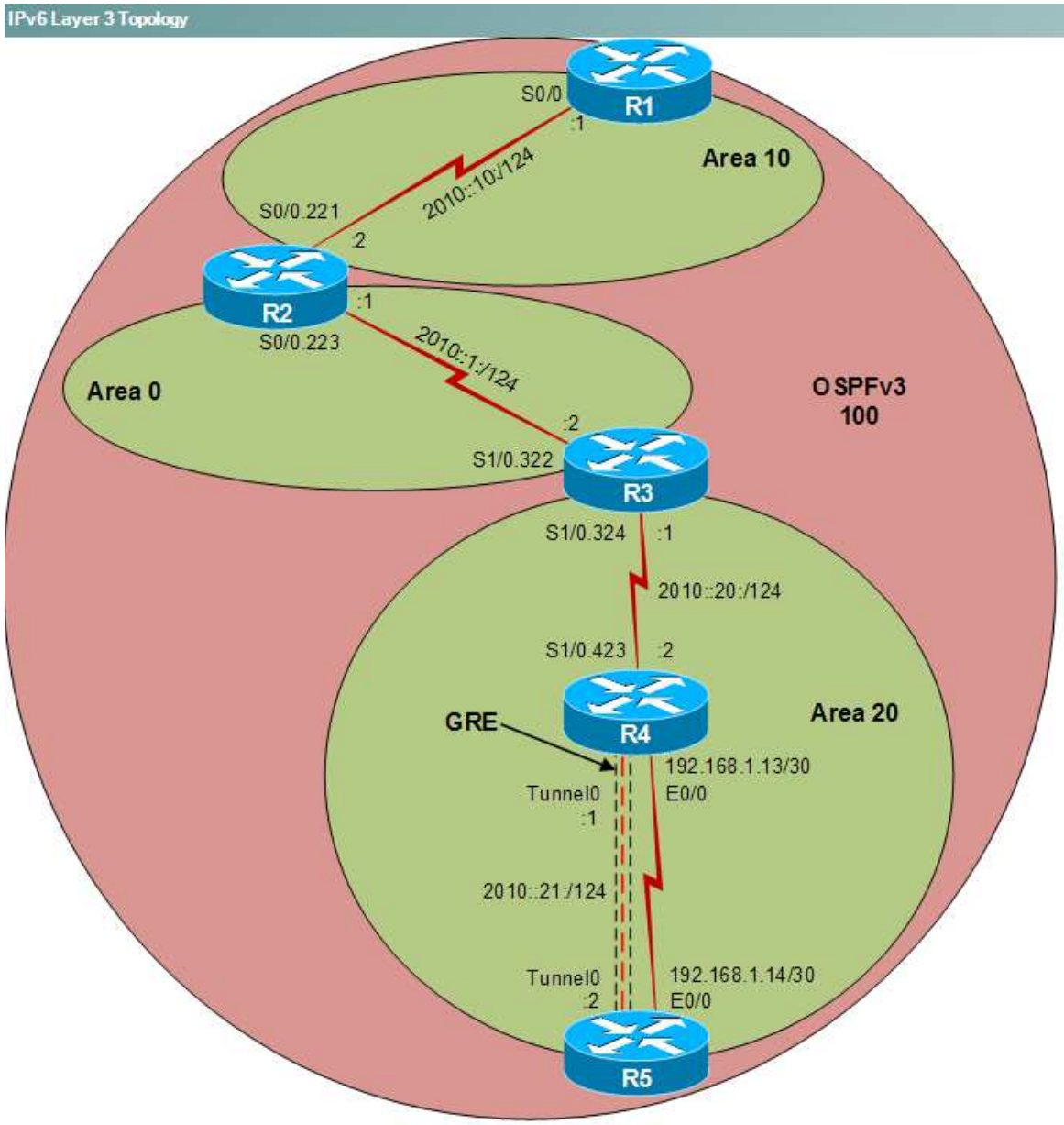
**Layer 2 Topology**




IPv4 layer 3 Topology

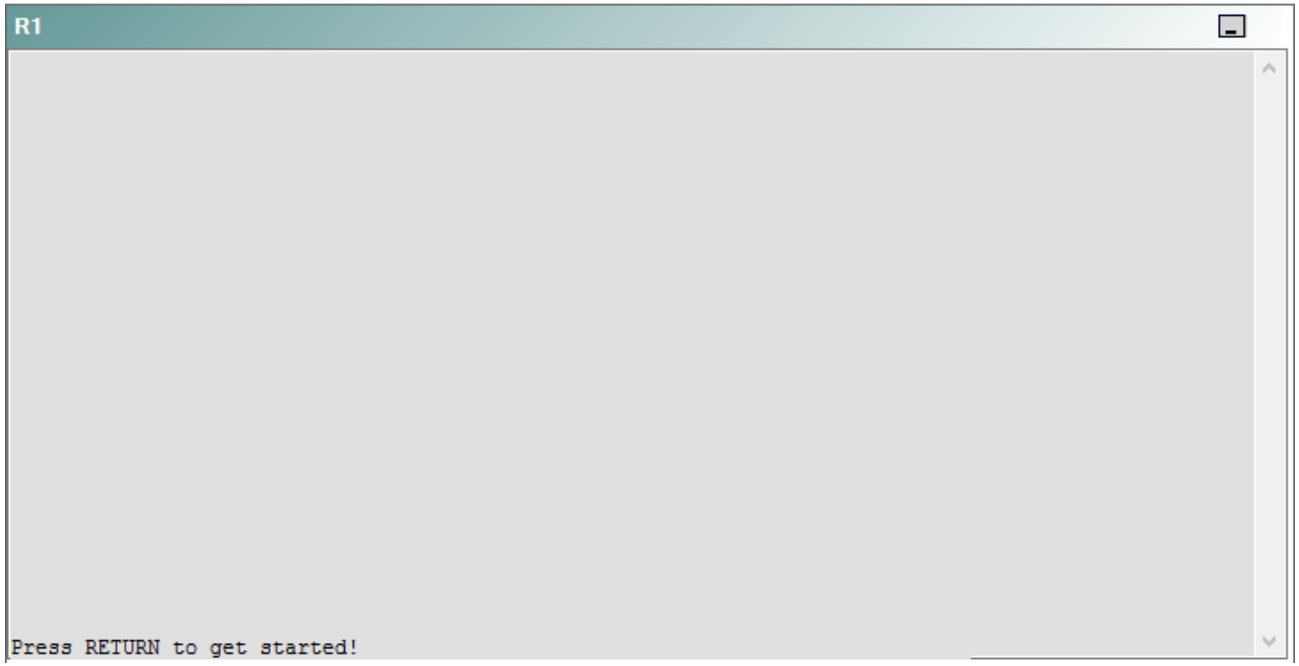

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

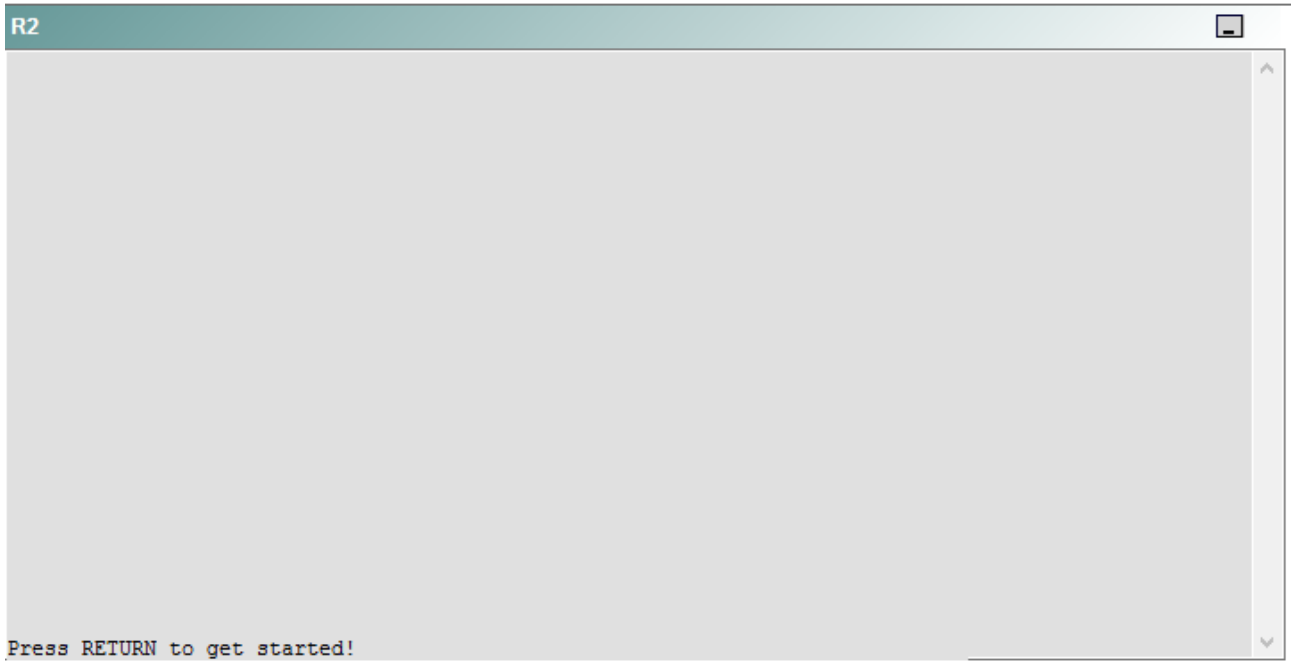



https://www.gratisexam.com/

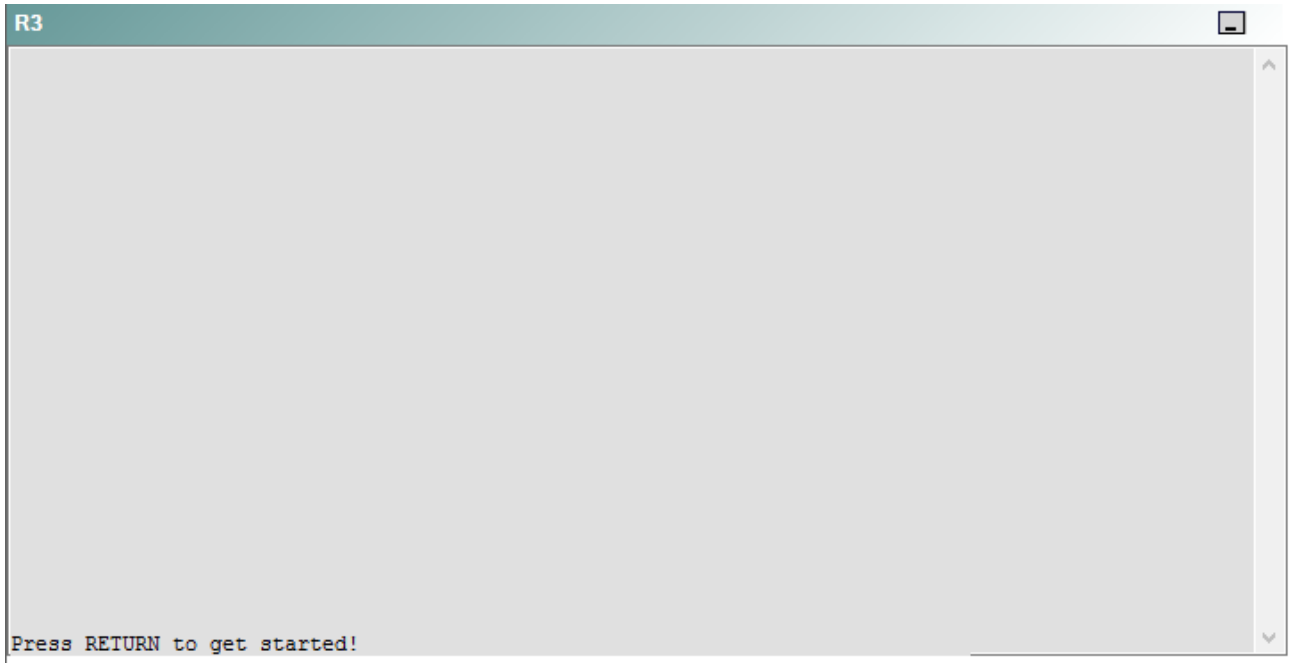
R1



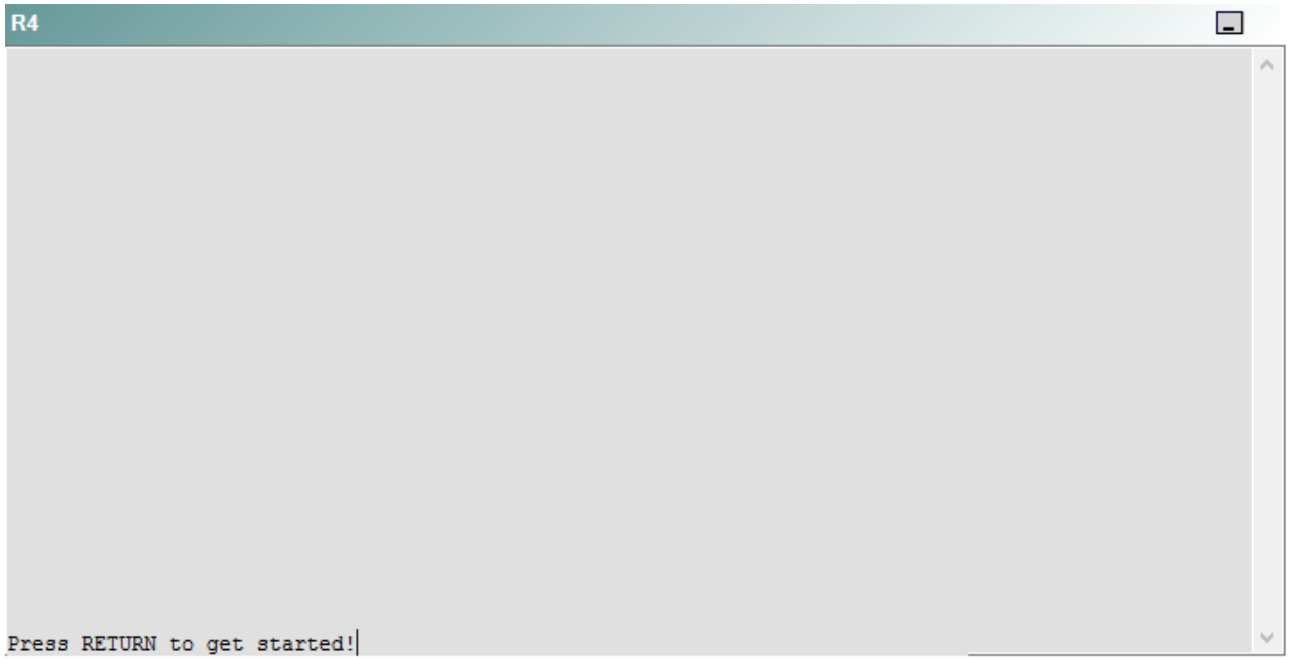

R2



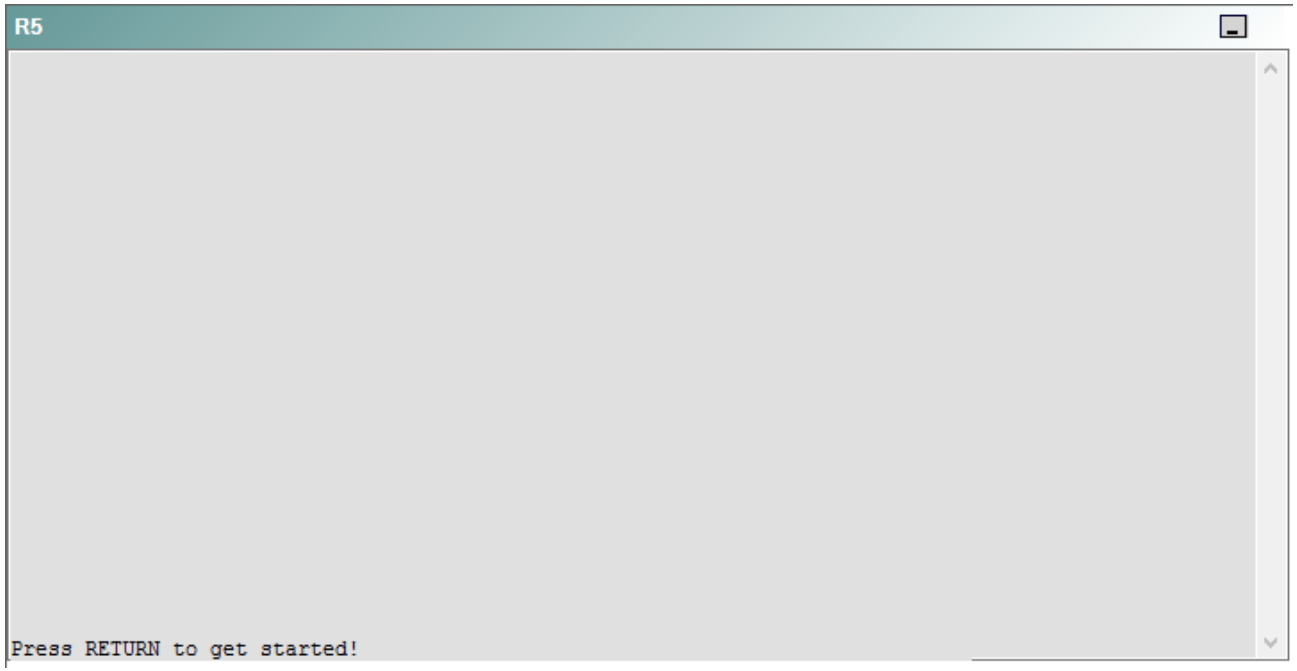

R3



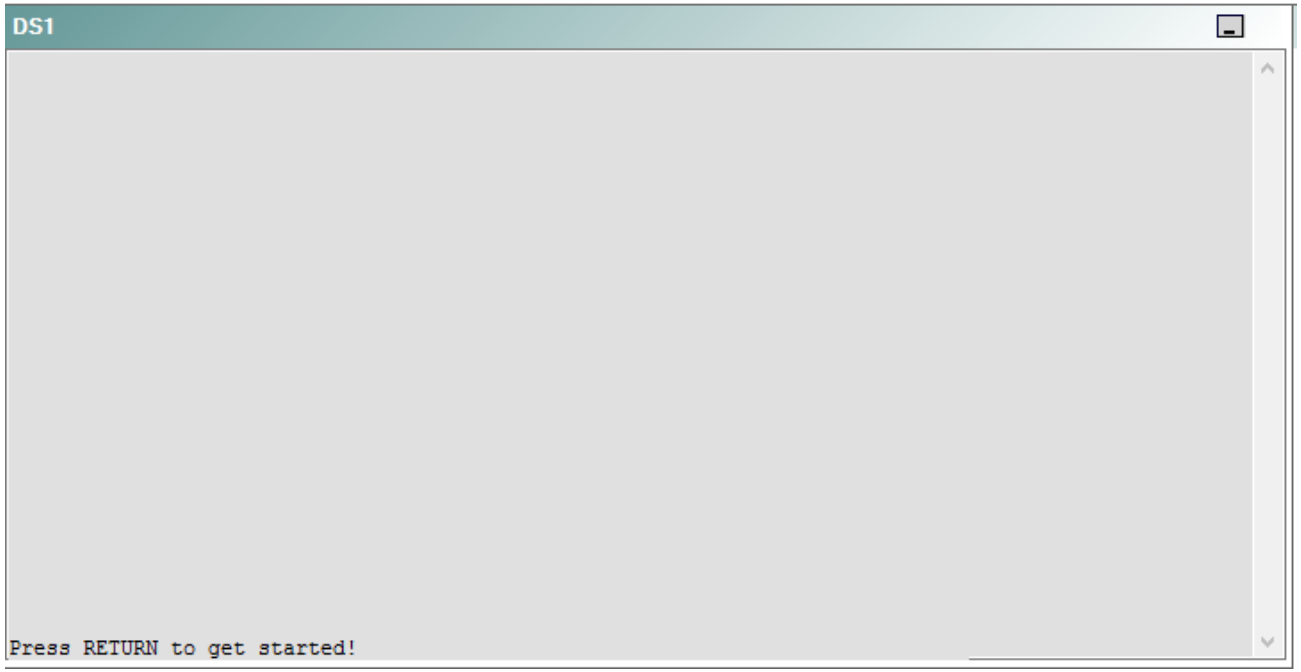

R4



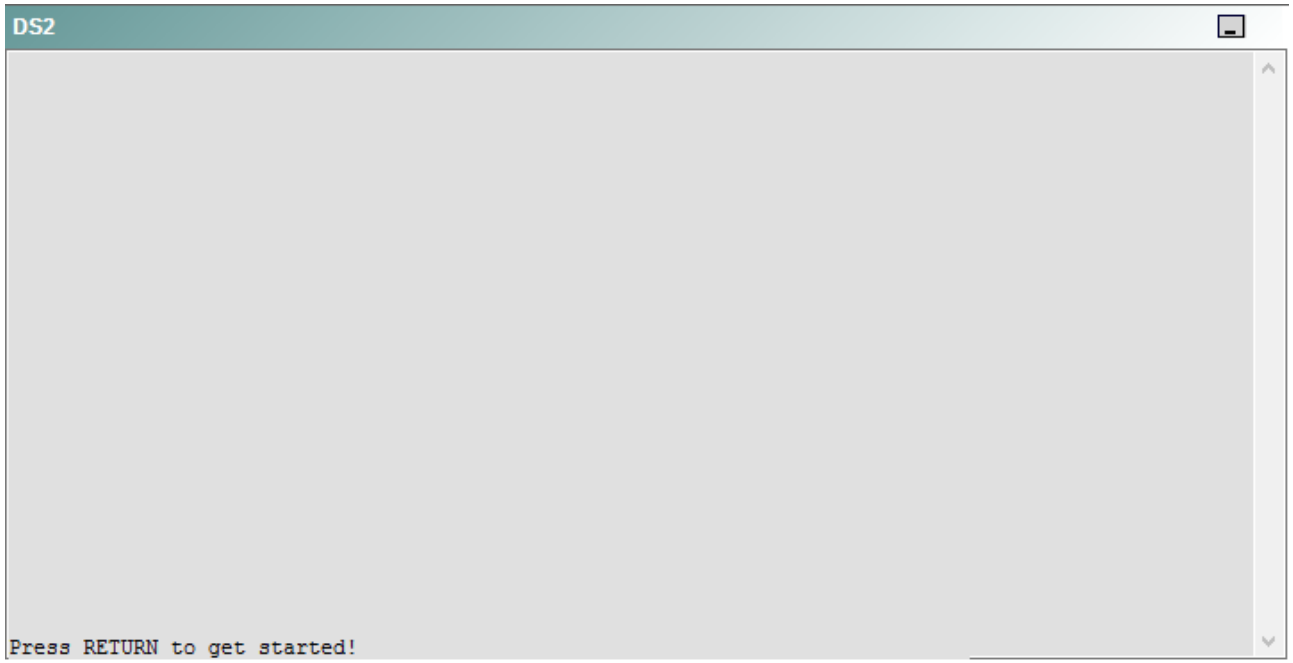

R5



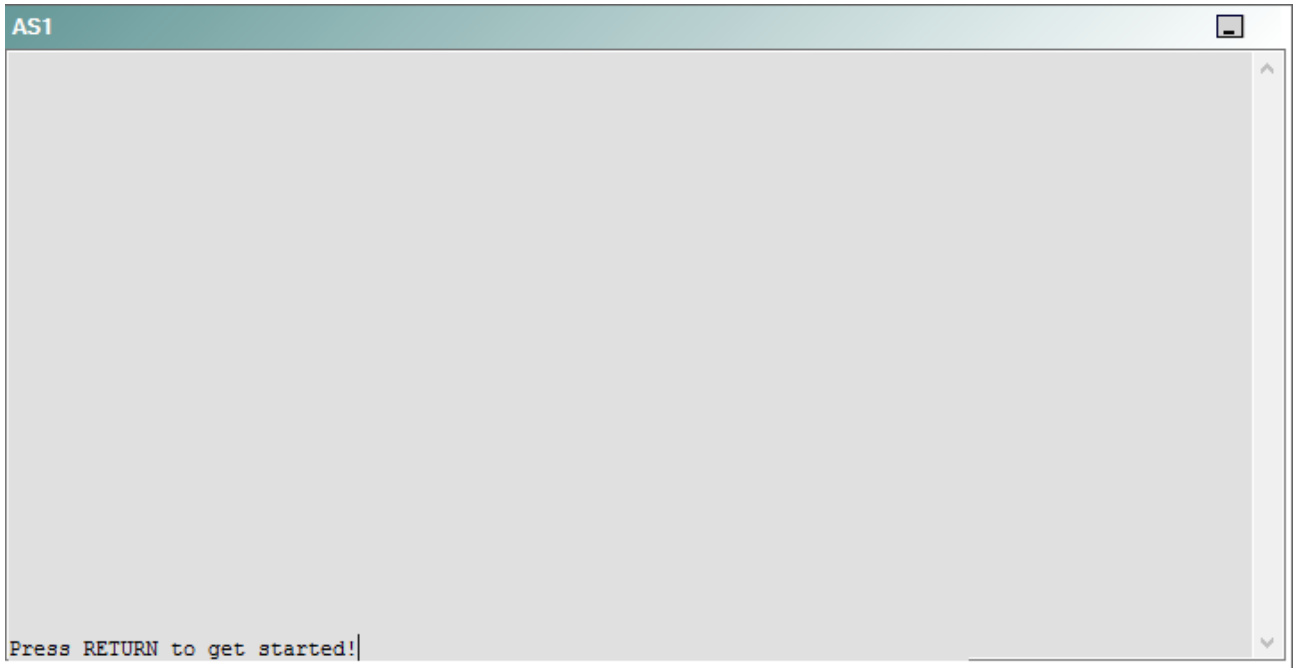

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. NAT
C. BGP
D. OSPFv3
E. Layer 3 addressing
F. STP
G. Etherchannel
H. VLAN configuration
I. interface

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 38**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

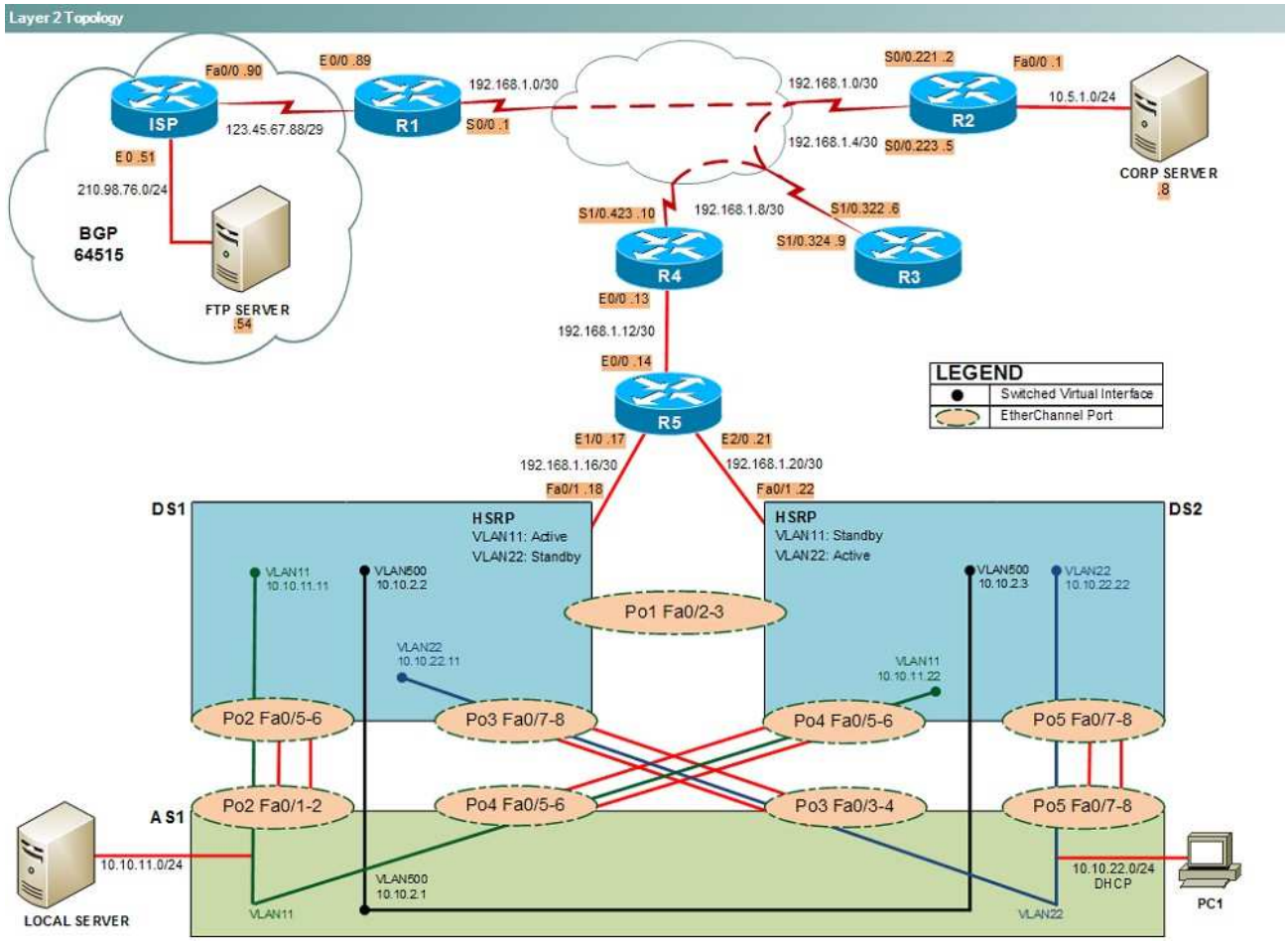
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

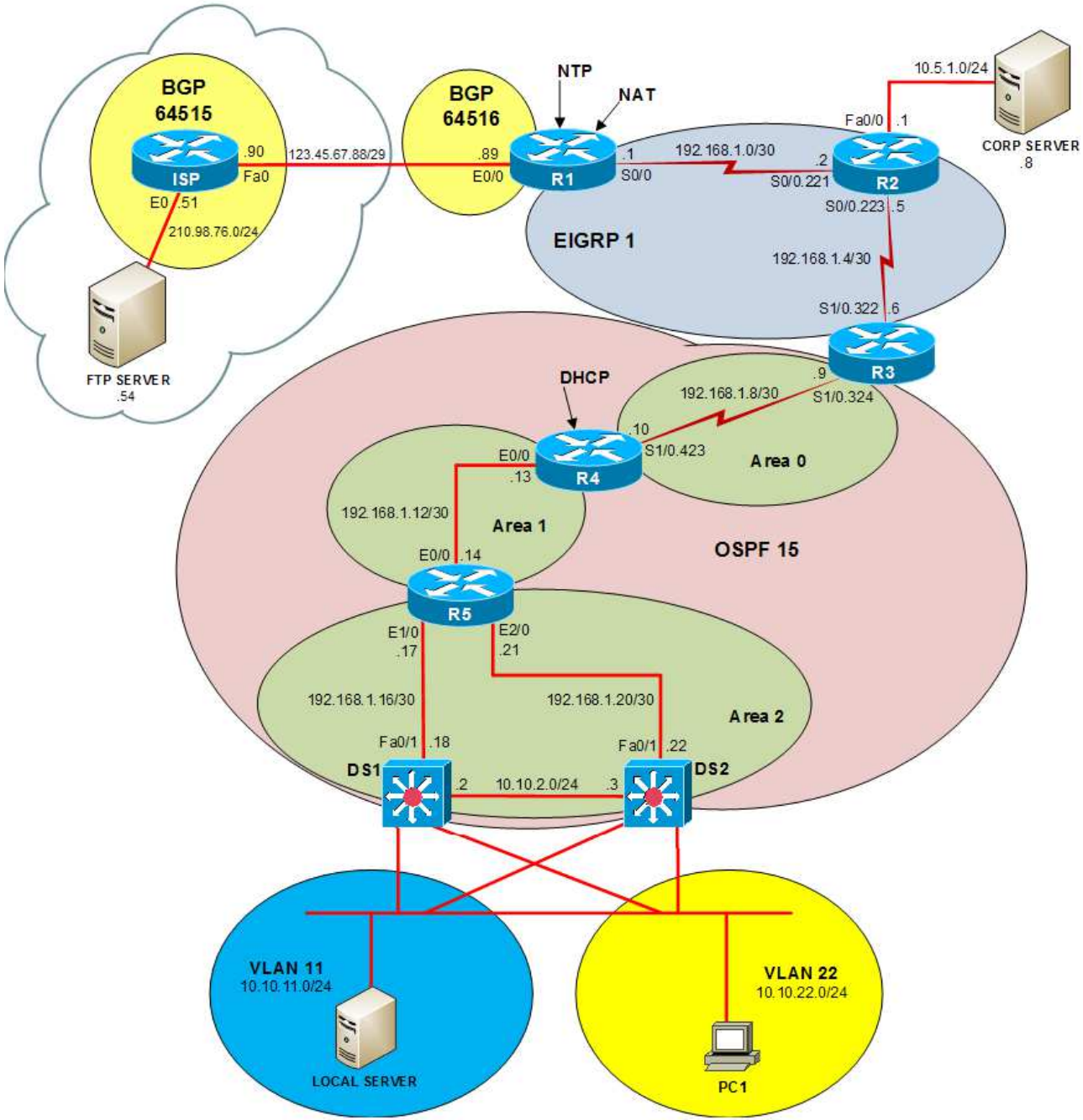
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

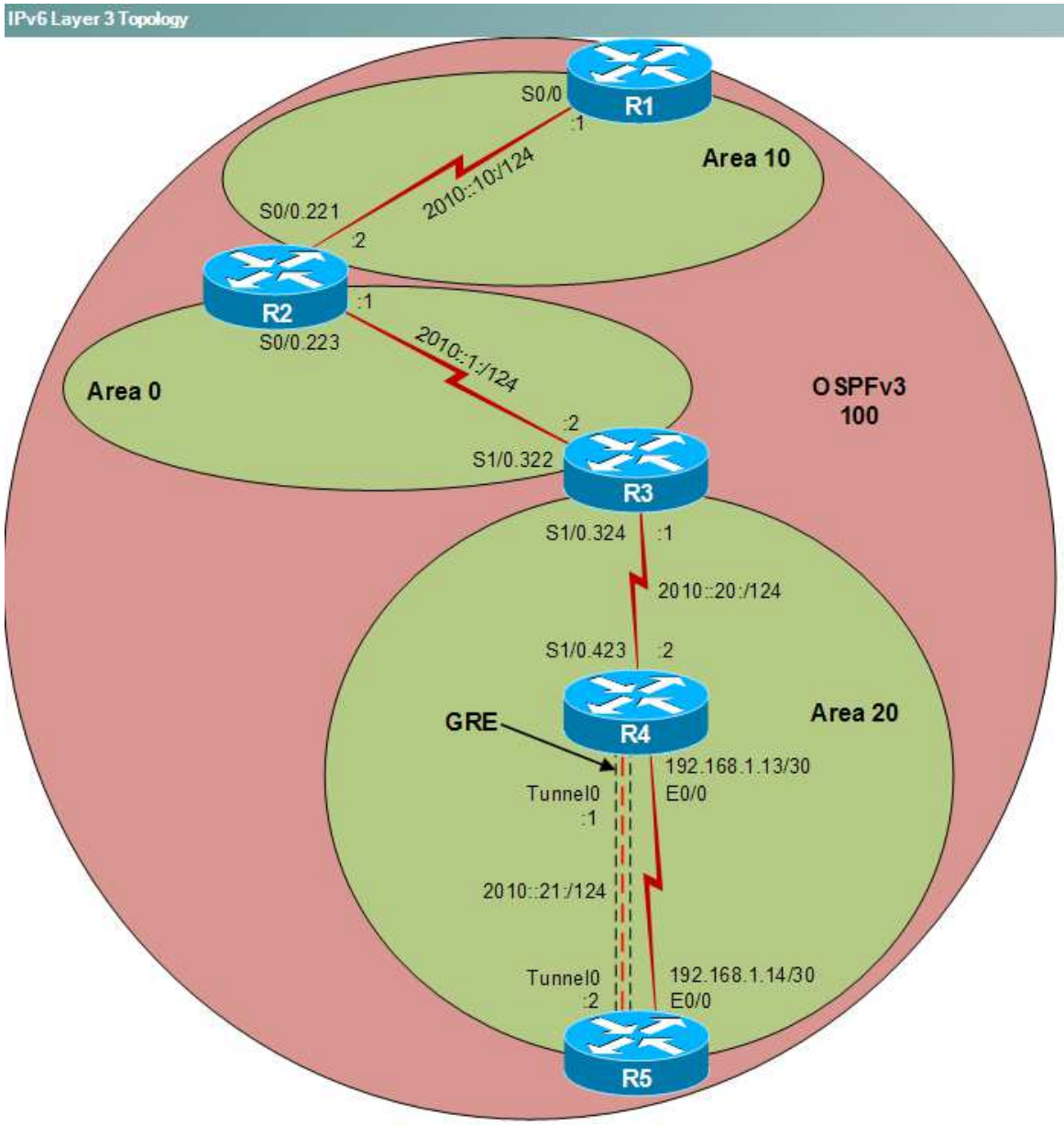
**Layer 2 Topology**




IPv4 layer 3 Topology

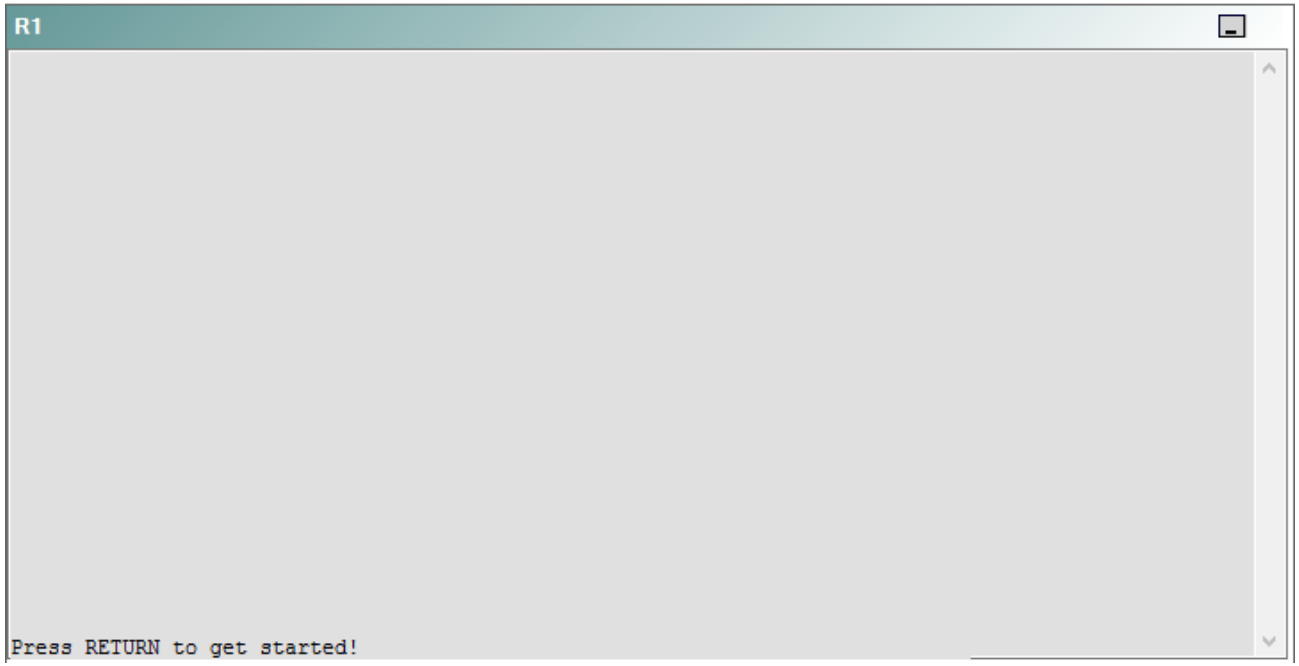

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

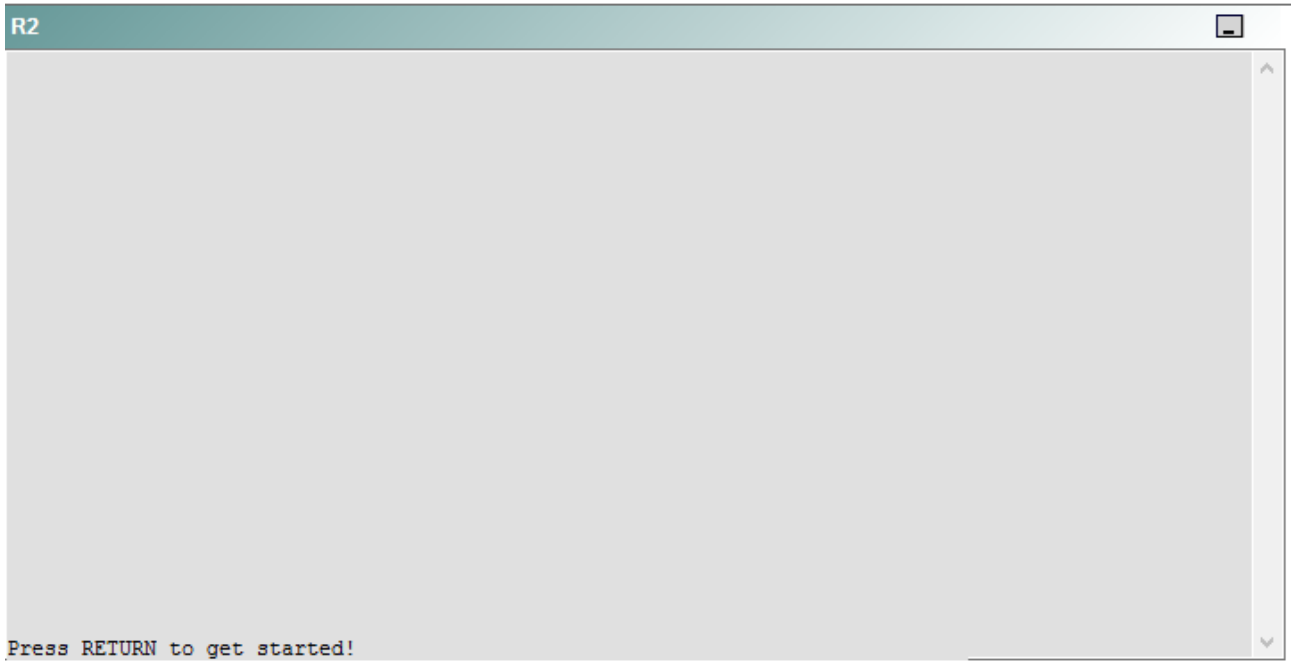



https://www.gratisexam.com/

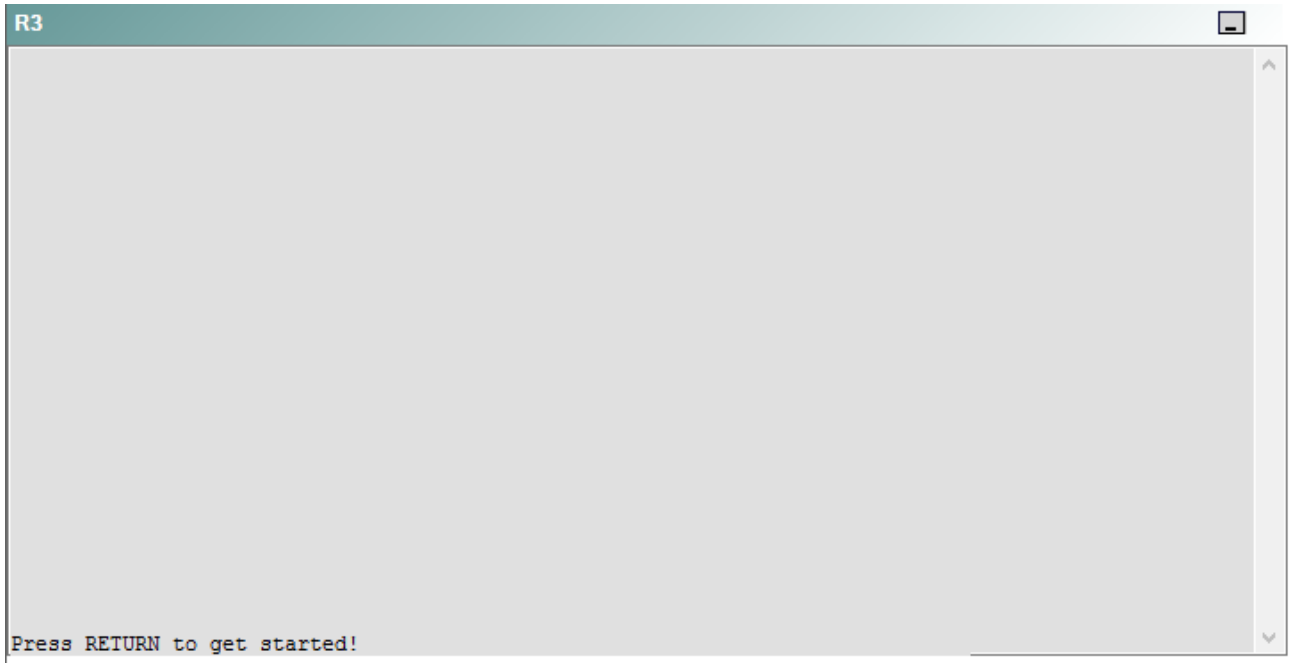
R1



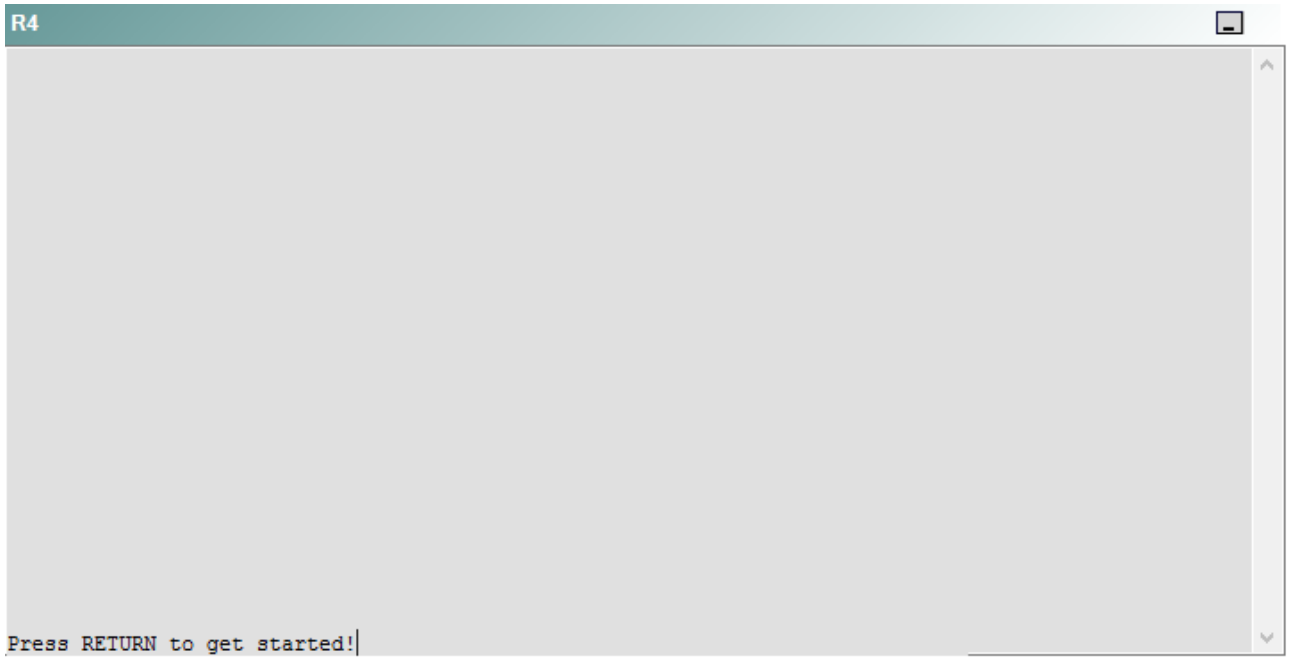

R2



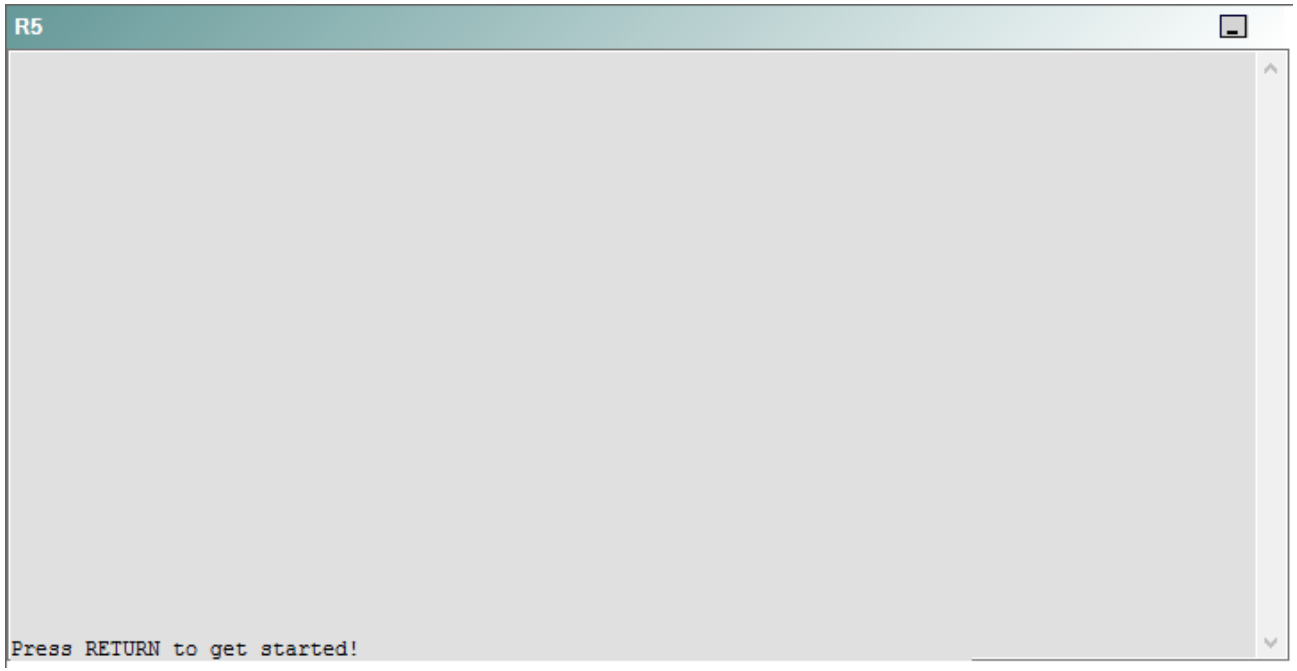

R3



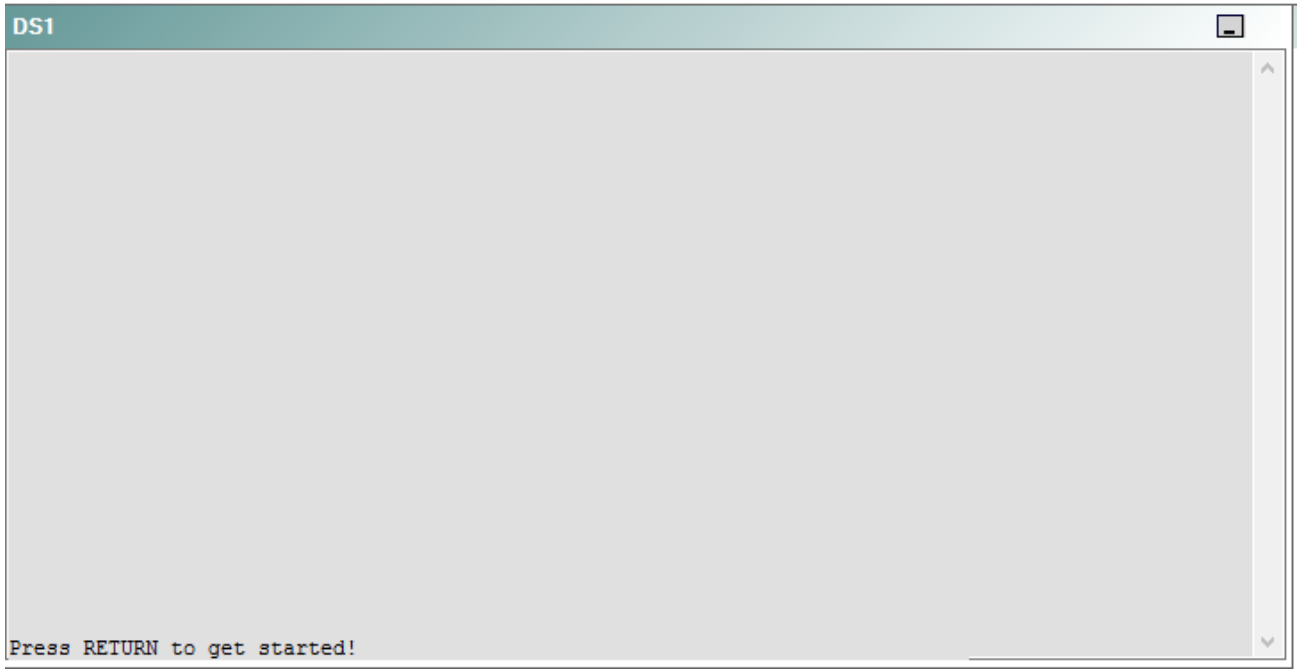

R4



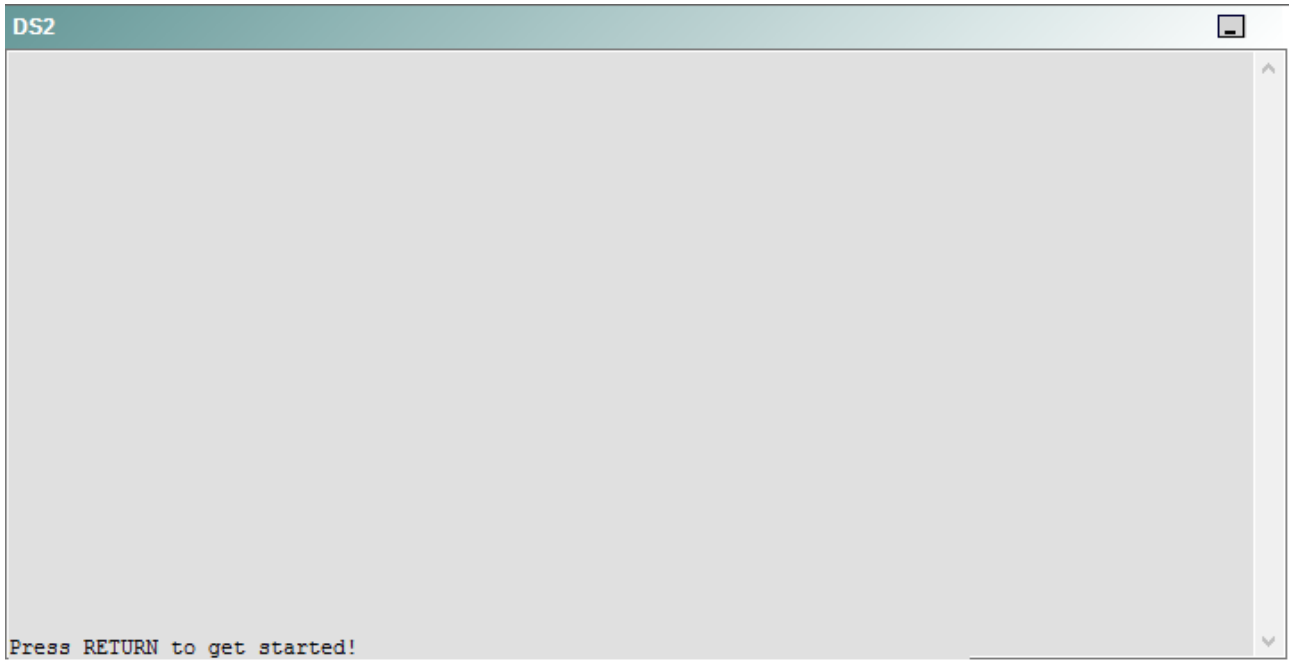

R5



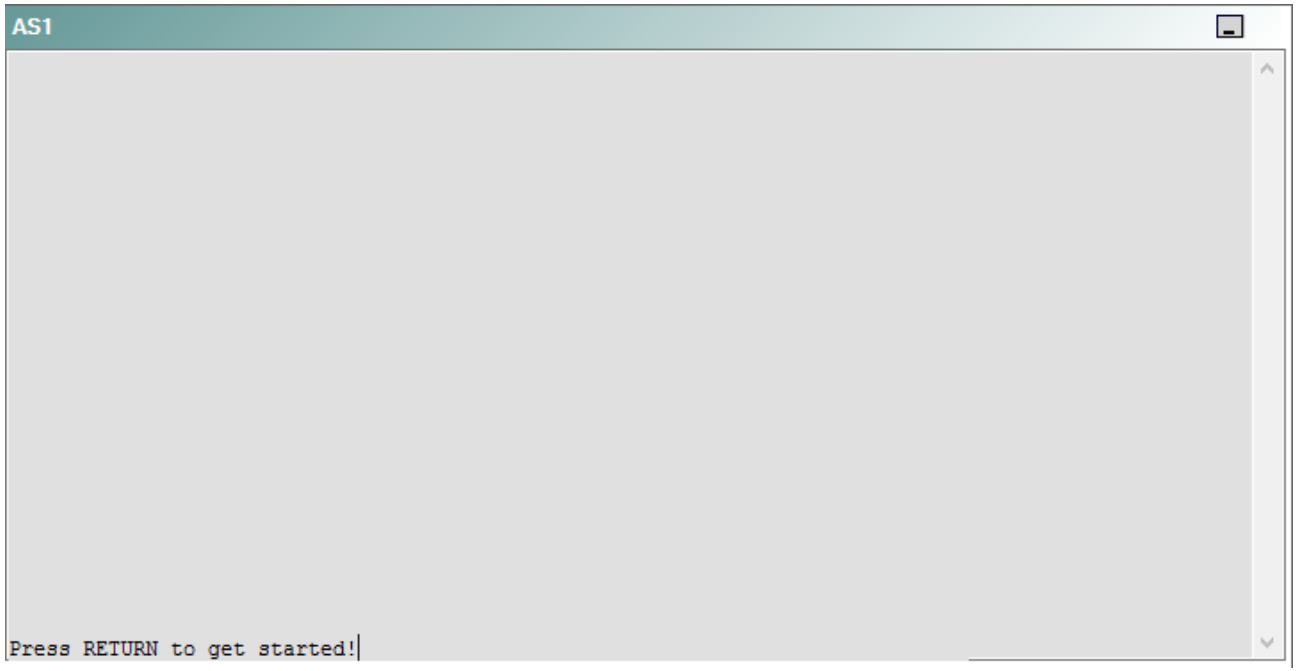

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. issuing the **ip nat outside** command on E0/0, and issuing the **ip nat inside** command on S0/0
B. issuing the **ip nat inside** command on E0/0, and issuing the **ip nat outside** command on S0/0
C. removing the **overload** keyword from the **ip nat inside source list 10 pool OUTSIDE overload** command in global configuration mode
D. adding the **overload** keyword to the **ip nat inside source list 1 pool OUTSIDE** command in global configuration mode
E. issuing the **no ip nat inside source list 10 pool OUTSIDE overload** command and the **ip nat inside source list 1 pool OUTSIDE overload** command
F. issuing the **no ip nat outside source list 1 pool OUTSIDE overload** command and the **ip nat inside source list 10 pool INSIDE overload** command
G. issuing the **no ip nat source list 10 pool INSIDE overload** command and the **ip nat outside source list 10 pool INSIDE overload** command.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

You should add the **overload** keyword to the **ip nat inside source list 1 pool OUTSIDE** command in global configuration mode on R1. To determine which device is the source of the problem, you should issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from R5 to the closest device and work your way up the network until communication is lost, or you can ping from R5 to the farthest device and work your way back to R5 until pings are successful. Alternatively, you can trace from R5 to R1 and see where communication is lost along the path to the destination device.

In this scenario, if you were to issue the **traceroute 123.45.67.90** command from R4, you would receive the following output:

```
Type escape sequence to abort.
Tracing the route to 123.45.67.90

 1 192.168.1.9 20 msec 16 msec 16 msec
 2 192.168.1.5 37 msec 32 msec 36 msec
 3 192.168.1.1 48 msec 52 msec 48 msec
 4 192.168.1.1 !H  !H  !H
```

The !H !H !H in the output above the indicates that the host at IP address 123.45.67.90 is unreachable, although there is a route available to that host. The trace reports that the host is unreachable beyond the IP address 192.168.1.1, which is R1. Similarly, if you were to issue the **ping 123.45.67.90** command on R4 or on DS2, you would receive the following output:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 123.45.67.90, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

The UUUUU in the output above indicates that the host at 123.45.67.90 is unreachable from R4 and DS2. However, 123.45.67.90 is reachable from R1, R2, R3, R5, and DS1, as shown in the following output:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 123.45.67.90, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/65/68 ms
```

In this scenario, using the bottom up or top down methods of troubleshooting can produce confusing results because R5, which lies between R4 and DS2, can ping and trace beyond the 123.45.67.89 boundary on R1, nut R4, DS2, and PC1 cannot. Therefore, the problem does not lie on R4, DS2, or PC1. The output from the **traceroute** command above indicates that R4 and DS2 can trace as far as R1, but not beyond. Thus the problem most likely lies on R1.

Once you have determined where connectivity is lost, you can begin to troubleshoot the cause of the problem. To determine which technology is most likely causing the problem, you should verify the configuration and operation of each technology. In this scenario, the fact that R1, R2, R3, R5, and DS1 are able to ping and trace to the external server at 210.98.76.54 indicates that both Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP) are functioning properly. The affected Cisco devices, R4 and DS2, contain routes that should allow communication to 210.98.76.54, so the routing protocols are operating properly on R4 and DS2.

In this scenario, NAT should be configured to allow Internet Protocol version 4 (IPv4) packets from internal, private IP addresses to traverse the ISP router and access the external server by using a small pool of four public IP addresses. R1 handles the translation of private IP addresses to public IP addresses so that the packets are sent and received by the correct devices on the network. The **ip nat inside source list 1 pool OUTSIDE** command configures R1 to use four public IP addresses to translate private IP traffic to the public network for the devices from the networks that are permitted by access list 1. The **show ip nat translations** command, which displays active NAT translations, and the **show ip nat statistics** command can be used to troubleshoot NAT. If you were to issue the **show ip nat translations** command on R1, you would receive the following output:

```
Pro Inside global  Inside local   Outside local  Outside global
--- 123.45.67.91   10.10.11.11    ---            ---
--- 123.45.67.92   192.168.1.6    ---            ---
--- 123.45.67.93   192.168.1.2    ---            ---
--- 123.45.67.94   192.168.1.14   ---            ---
```

The fields in the NAT translations table represent the following:

- `Pro` - The protocol being used to transport data from the private IP address to the public IP address
- `Inside global` - An IP address that is assigned by an ISP for use inside a private network
- `Inside local` - An unregistered IP address that is not routable over the Internet
- `Outside local` - An IP address that can be used by the NAT router and routed from the private network
- `Outside global` - A globally routable IP address that is assigned to a device outside the private network

The `Inside global` column in the output above indicates that the IP addresses 123.45.67.91, 123.45.67.92, 123.45.67.93, and 123.45.67.94 on R1 are inside global addresses. The `Inside local` column indicates that the IP addresses 192.168.1.2 on R2, 192.168.1.6 on R3, 192.168.1.14 on R4, and 10.10.11.11 on DS2 are inside local addresses. The `Pro`, `Outside local`, and `Outside global` columns contain no values, which indicates that all protocols are being translated from private to public for only the four devices that have been assigned the IP addresses that appear in the `Inside local` column. IP addresses that have been assigned to R4, DS2, and PC1 are not being translated; therefore, an error in the NAT configuration on R1 is most likely the cause of the problem.

After you isolated the cause of the problem, you should issue the **show running-config** command on R1 to verify the NAT configuration. If you were to issue the **show running-config** command on R1 in this scenario, you would receive the following partial output:

```
ip nat pool OUTSIDE 123.45.67.91 123.45.67.94 netmask 255.255.255.248
ip nat inside source list 1 pool OUTSIDE
```

The output above indicates that NAT is configured to map a pool of four publicly routable IP addresses to IP addresses on the private side of the network. The **ip nat inside source list 1 pool OUTSIDE** command configures NAT to map the four IP addresses in the pool named OUTSIDE to four unspecified IP addresses inside the private network. Additionally, the **ip nat inside source list 1 pool OUTSIDE** command limits the private network ranges that can be translated by NAT to those specified in access list 1. Because the **ip nat inside source list 1 pool OUTSIDE** command will only map four private IP addresses to the four public IP addresses, the first four unique private IP addresses to require NAT will be automatically mapped by NAT, exhausting the pool. To configure NAT to map public IP addresses to private IP addresses on a one-to-many basis, you must issue the **ip nat inside source list 1 pool** OUTSIDE command with the **overload** keyword. If the **overload** keyword had been issued, NAT would have been configured to use port numbers in addition to private IP addresses to map public IP addresses to private IP addresses on a one-to-many basis. This NAT configuration is also known as Port Address Translation (PAT) or Network Address Port Translation (NAPT); it is typically used when a private network has a larger range of IP addresses that require access to the public network than are available for one-to-one mapping in the public network IP address range. Therefore, issuing the **ip nat inside source list 1 pool OUTSIDE** command with the **overload** keyword would solve the problem.

You cannot remove the **overload** keyword from the **ip nat inside source list 10 pool OUTSIDE overload** command in global configuration mode on R1, nor can you issue the **no ip nat inside source list 10 pool OUTSIDE overload** command, because the **ip nat inside source list 10 pool OUTSIDE overload** command has not been issue don R1. In this scenario, the **overload** keyword is missing from the **ip nat inside source list 1 pool** command.

You should not issue the **ip nat inside** command on the E0/0 interface and **the ip nat outside** command on the S0/0 interface on R1. The E0/0 interface is the interface on R1 that faces the public network and should therefore be configured with **the ip nat outside** command. The S0/0 interface is the interface on R1 that faces the private network and should therefore be configured with the **ip nat inside** command. The E0/0 interface has already been configured with the **ip nat outside** command and the S0/0 interface has already been configured with the **ip nat inside** command in this scenario.

You should not issue the **no ip outside source list 1 pool OUTSIDE overload** command and the **ip nat outside source list 10 pool OUTSIDE** overload command on R1. In this scenario, access list 1 on R1 contains the proper permit policies to enable NAT to translate between the private IP addresses on the network and the public IP addresses outside R1.

You should not issue the **no ip outside source list 10 pool INSIDE overload** command and **the ip nat outside source list 1 pool INSIDE overload** command on R1. Additionally, you should not issue the **no ip nat outside source list 1 pool INSIDE overload** command and the **ip outside source list 10 pool INSIDE overload** command on R1. The name of the public IP address pool in this scenario is OUTSIDE; there is no IP address pool named INSIDE.

Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/12-4t/nat-12-4t-book/iadnat-addr-consv.html#GUID-CF45A807-ED0B-4E0A-B84D-06ACBDF3D5AE

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

**QUESTION 39**
You want to issue an extended **traceroute** command that allows only one probe per TTL level.

Which of the following features should you modify?

A. Target IP address
B. Maximum Time to Live
C. Source address
D. Probe count
E. Port Number

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 40**
Which of the following fields are optional GRE header fields? (Select four.)

A. Checksum
B. Protocol Type
C. Sequence Number
D. Reserved 0
E. Reserved 1
F. Key
G. Version

**Correct Answer:** ACEF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 41**

**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

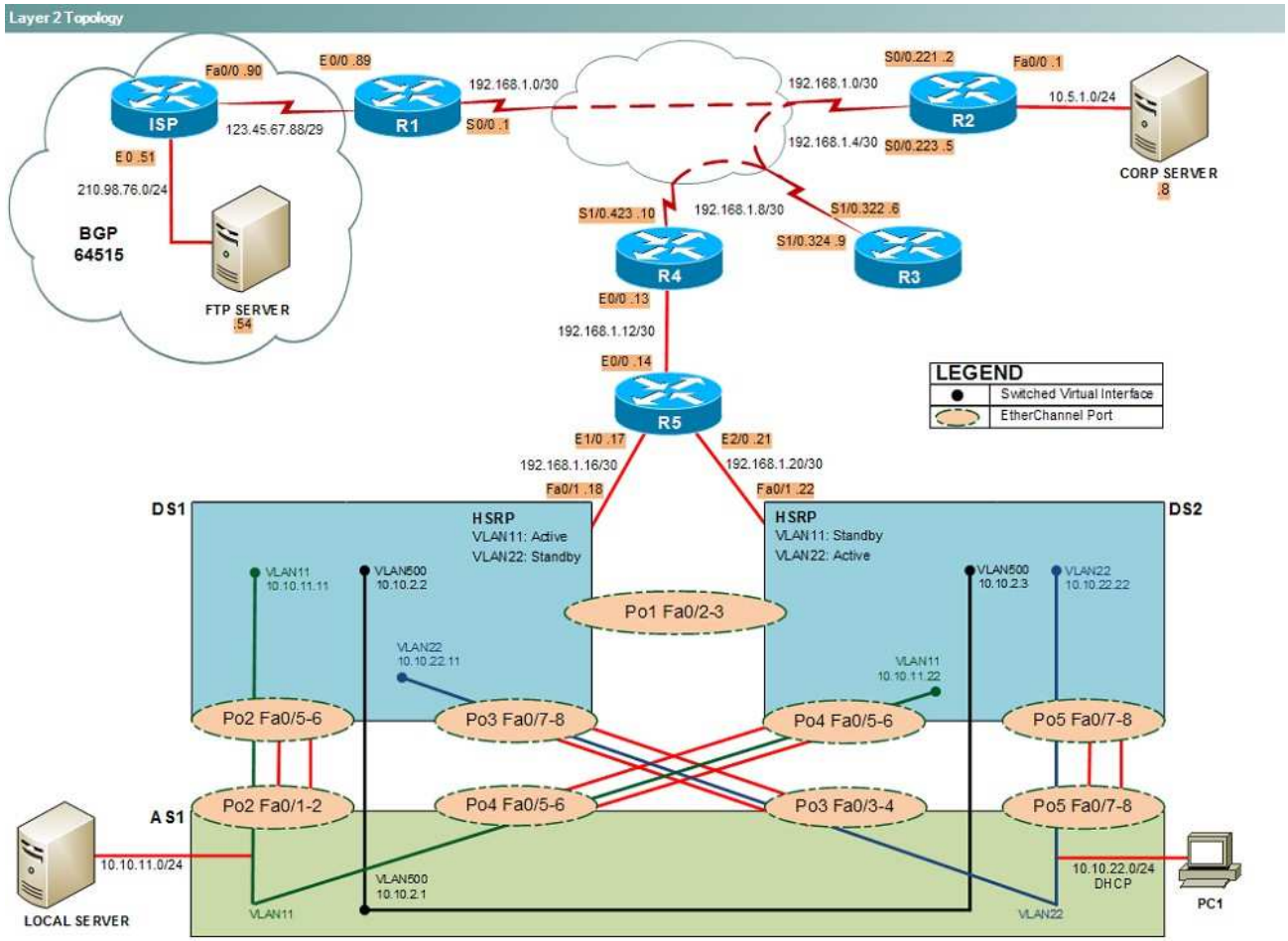
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

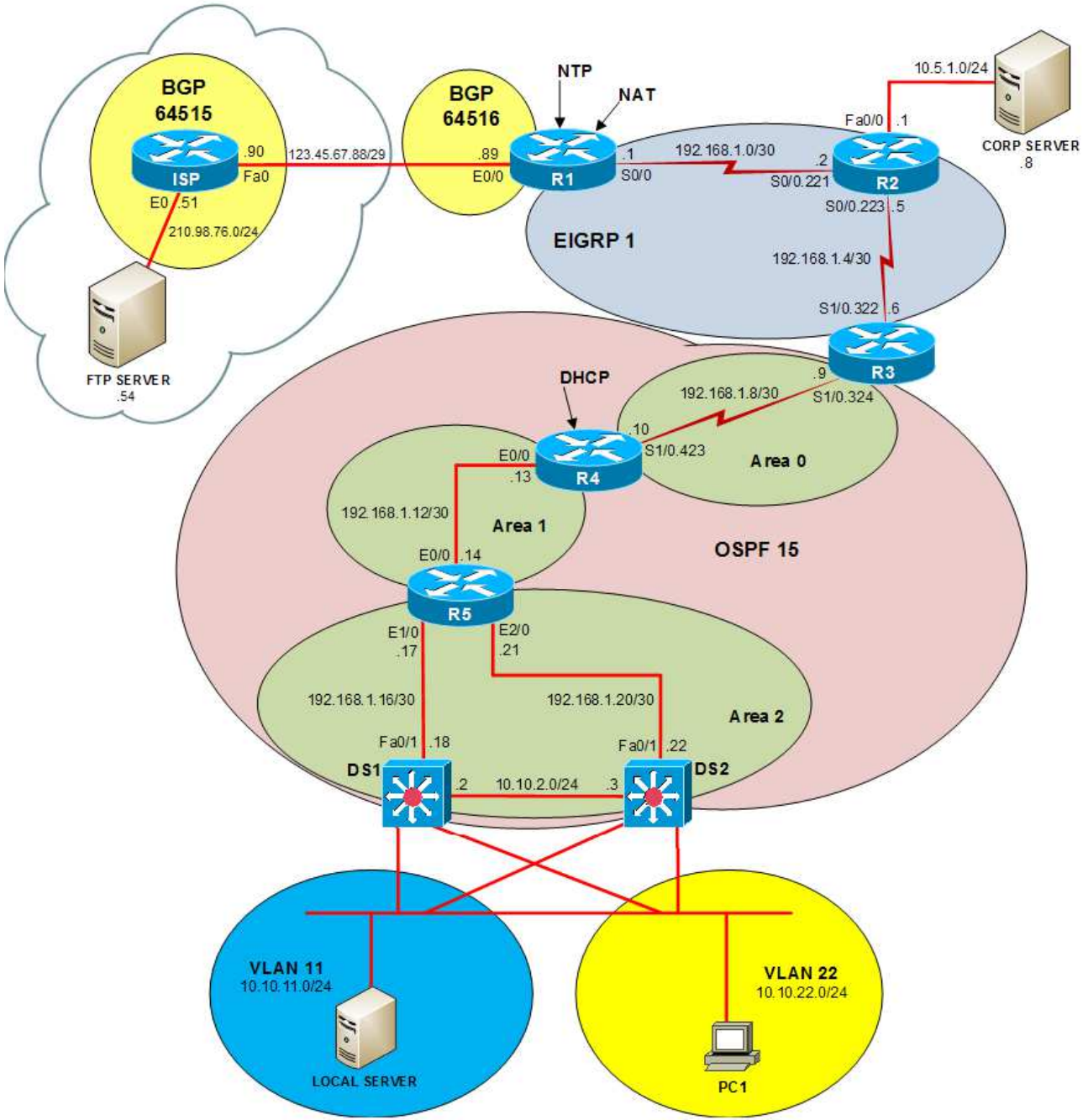
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

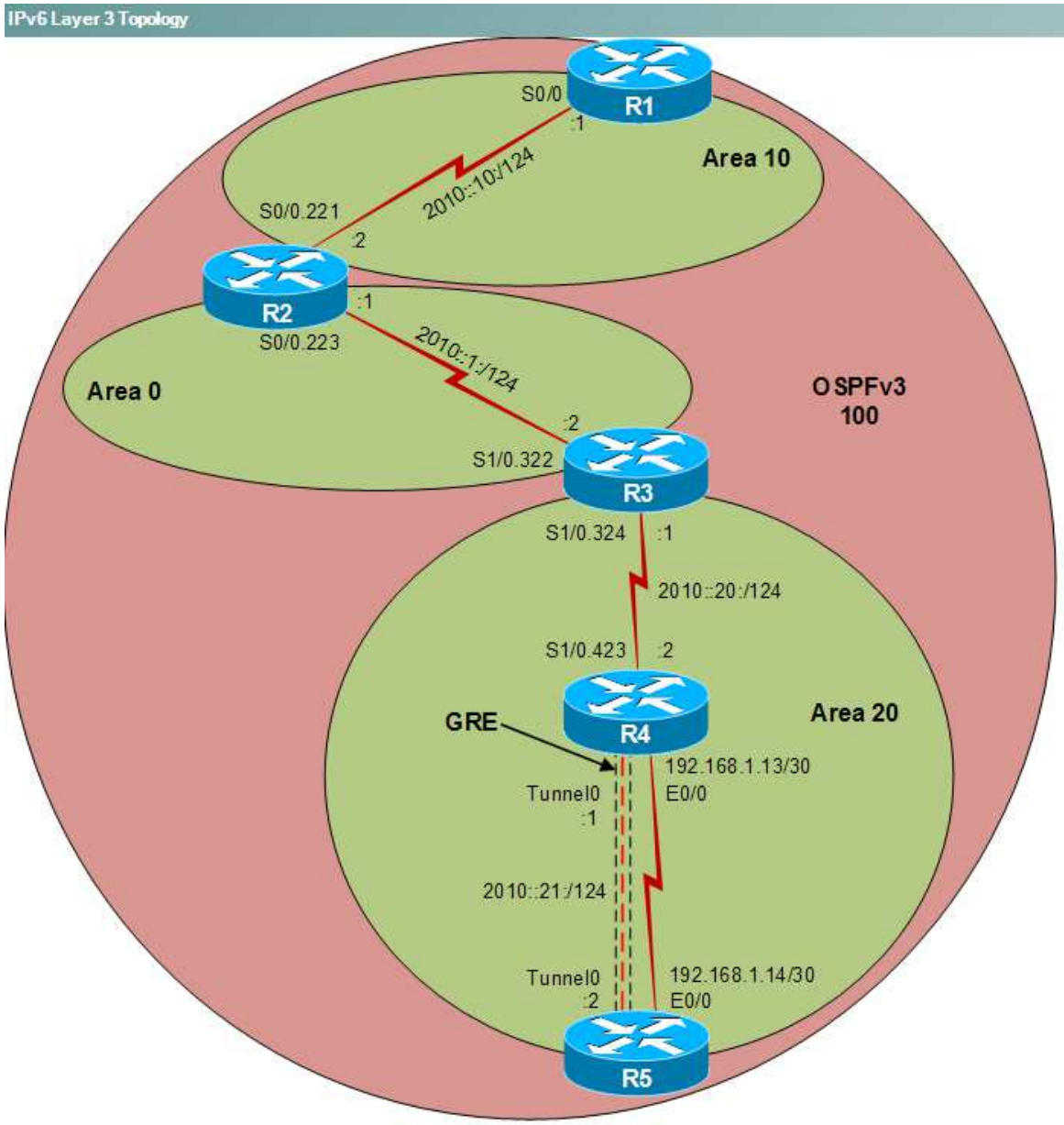
**Layer 2 Topology**




IPv4 layer 3 Topology

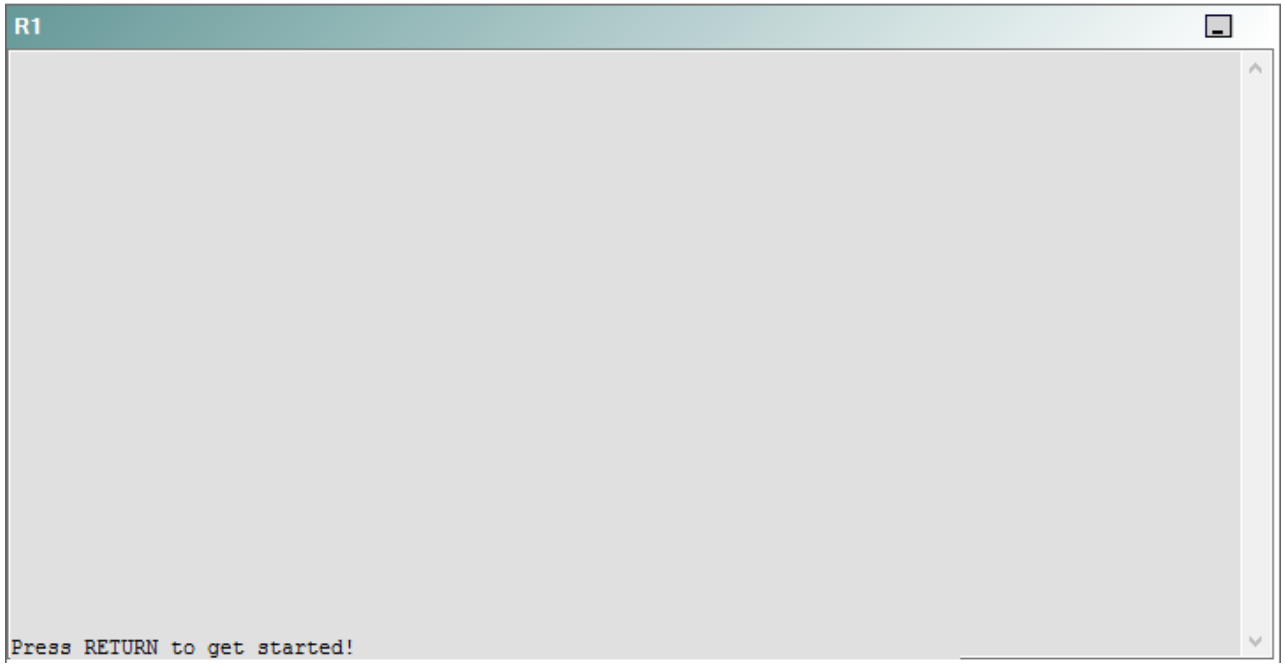

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

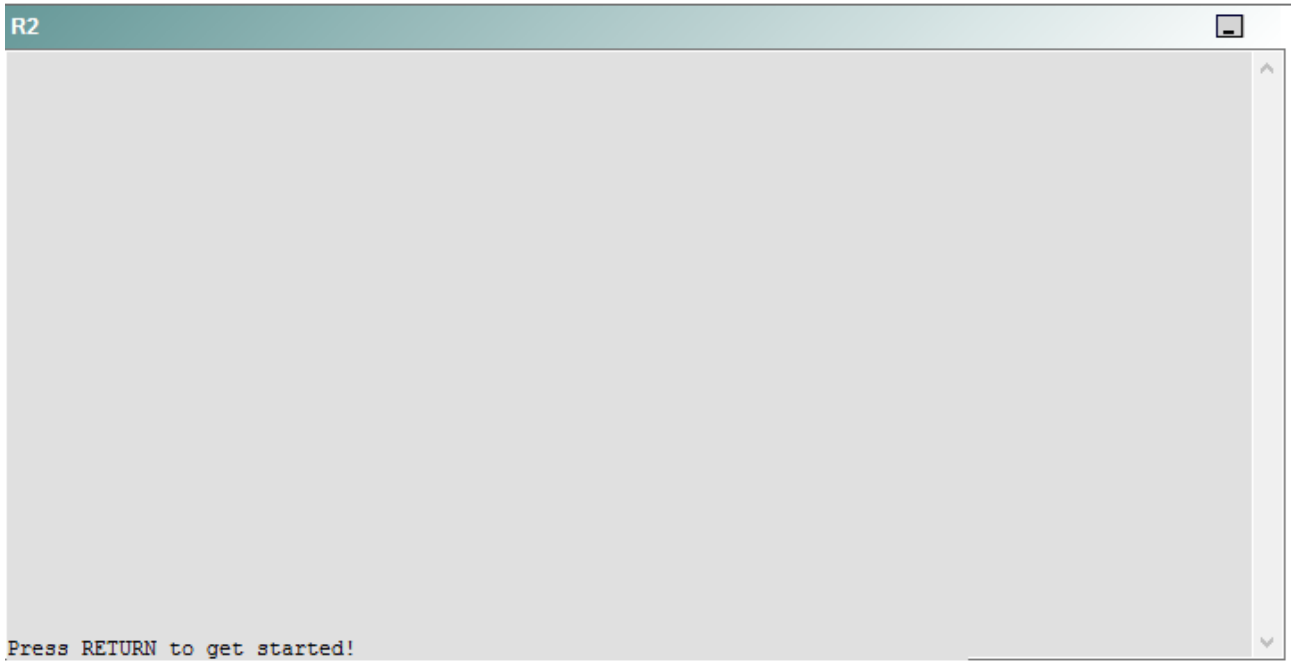



https://www.gratisexam.com/

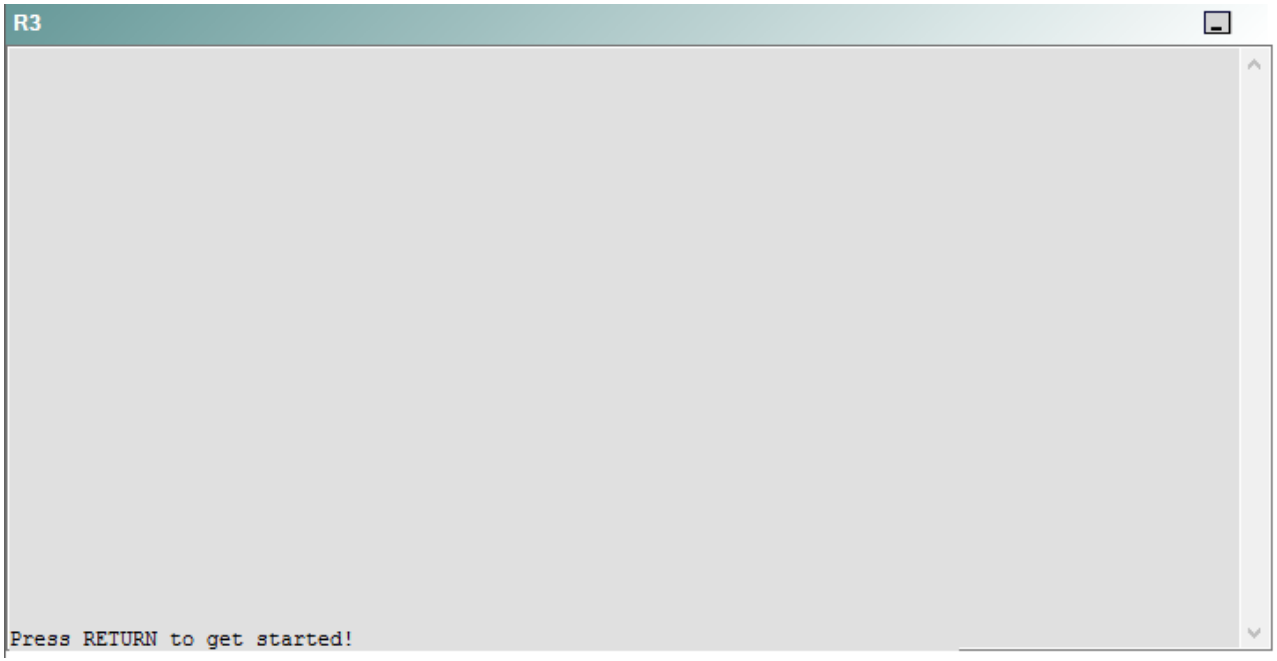
R1



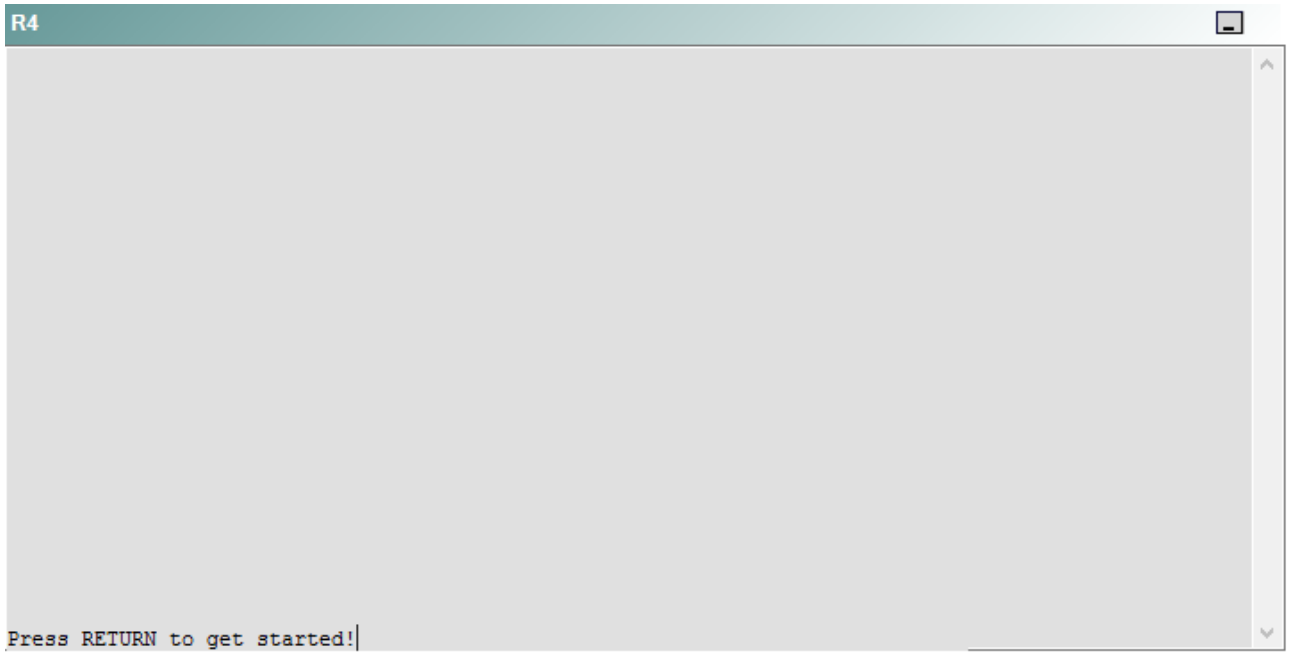

R2



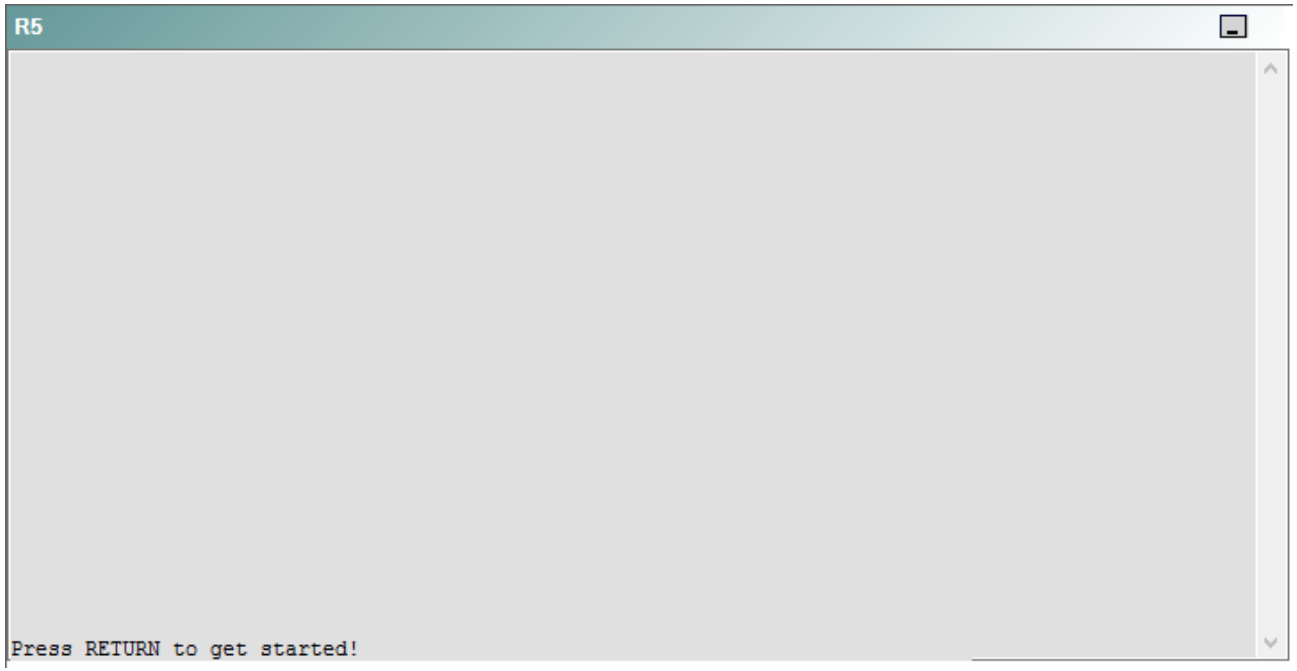

R3



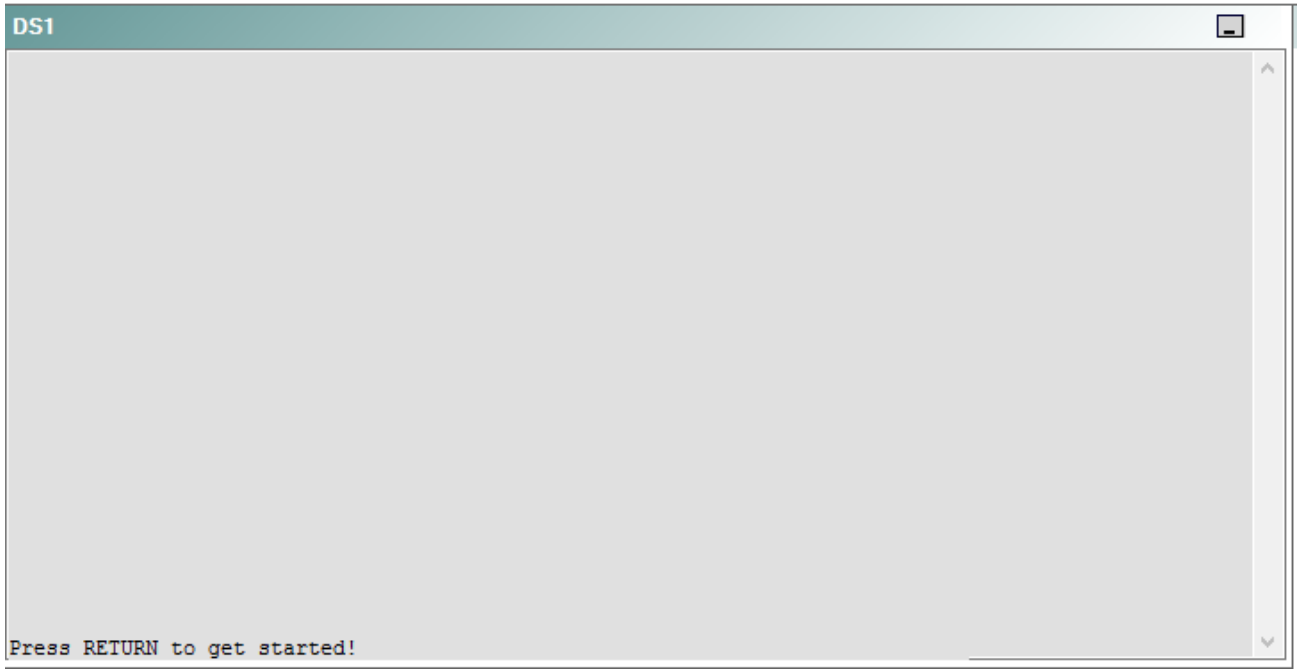

R4



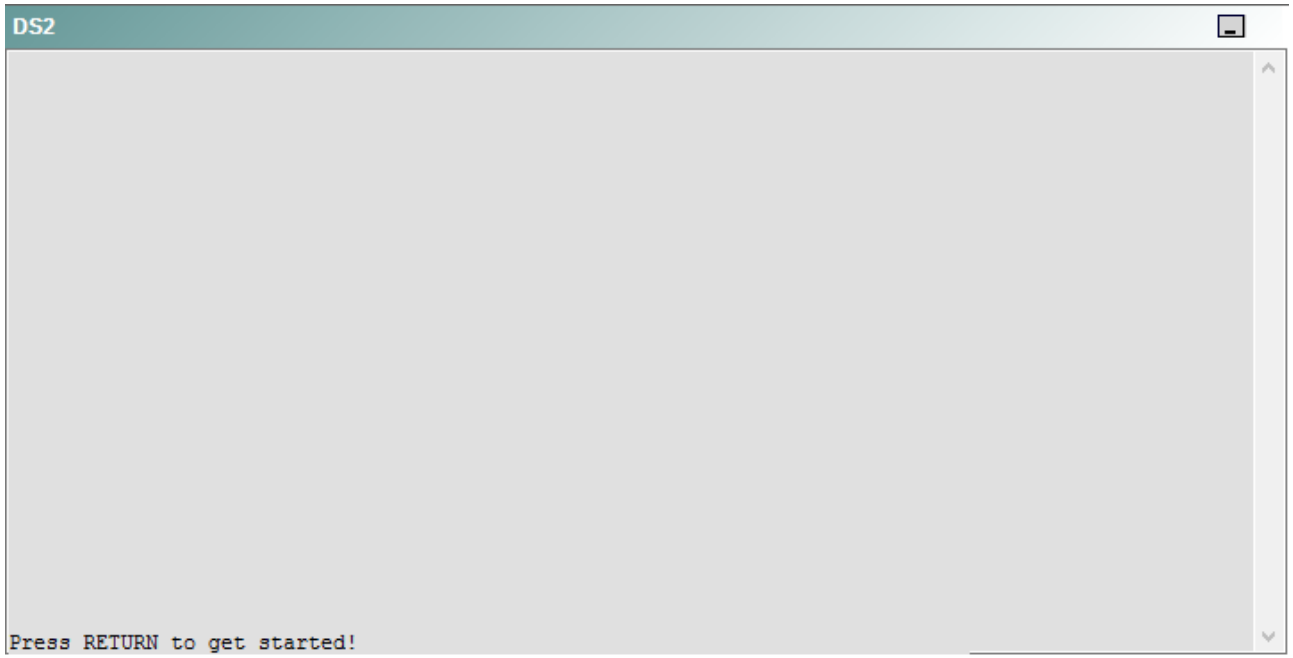

R5



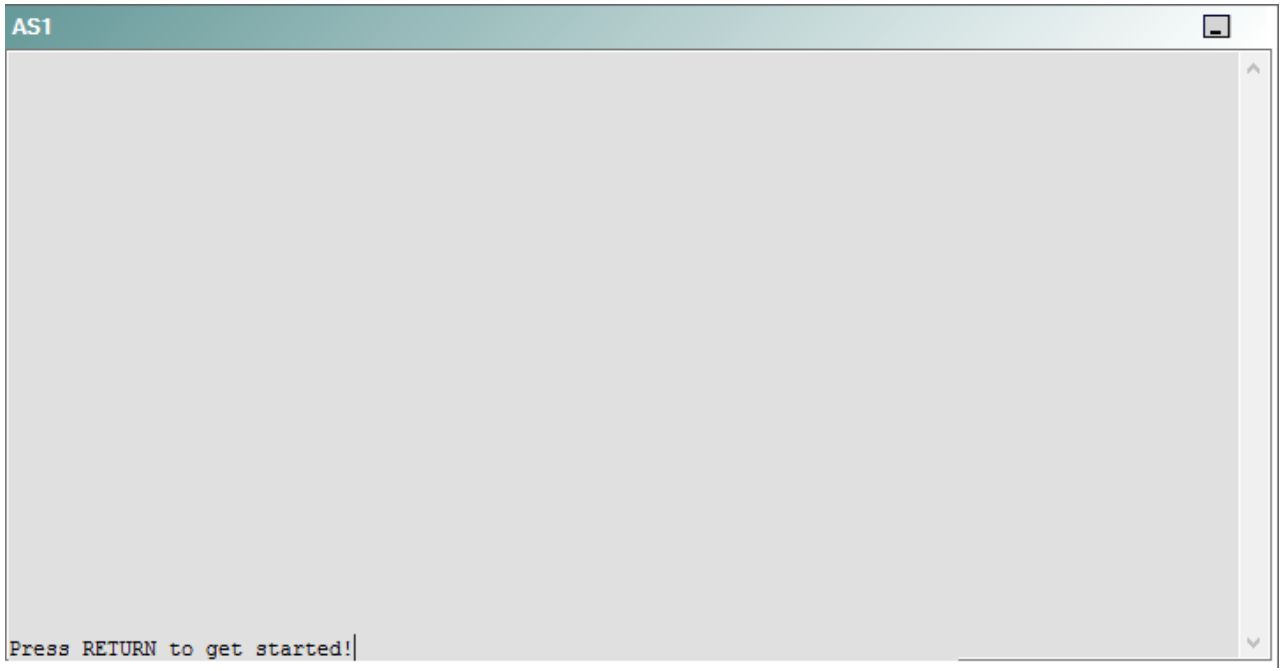

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 42**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

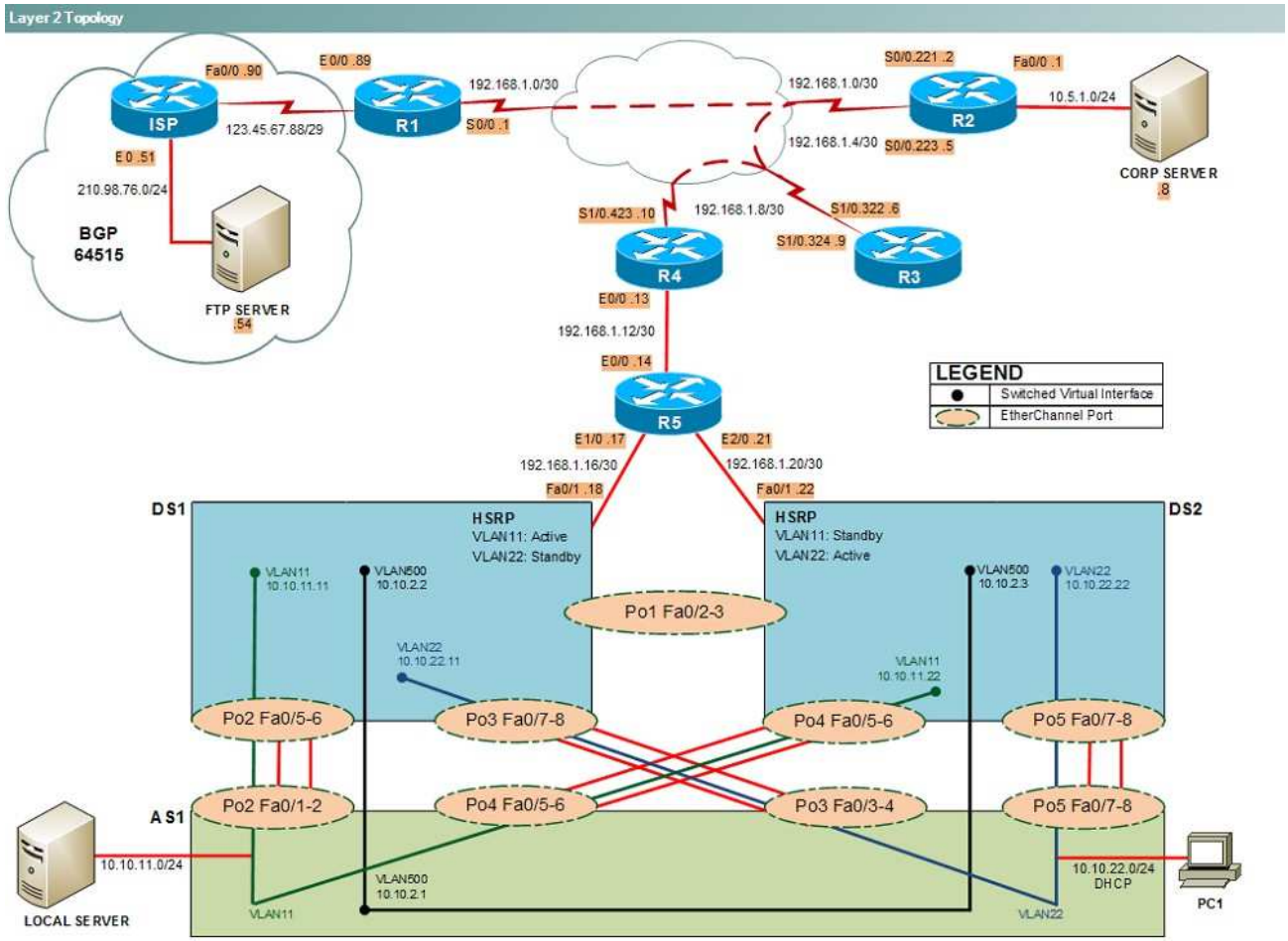
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

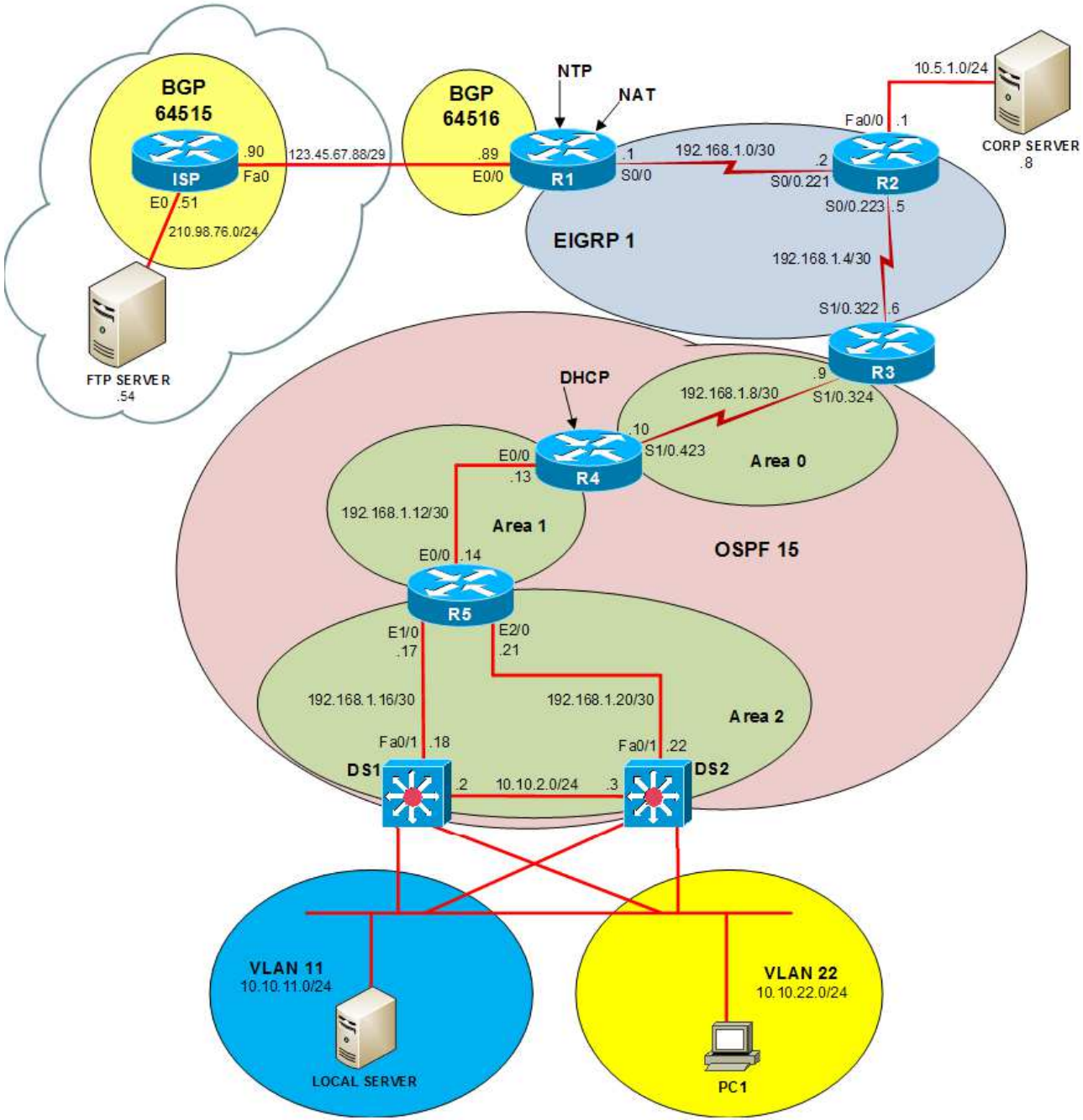
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

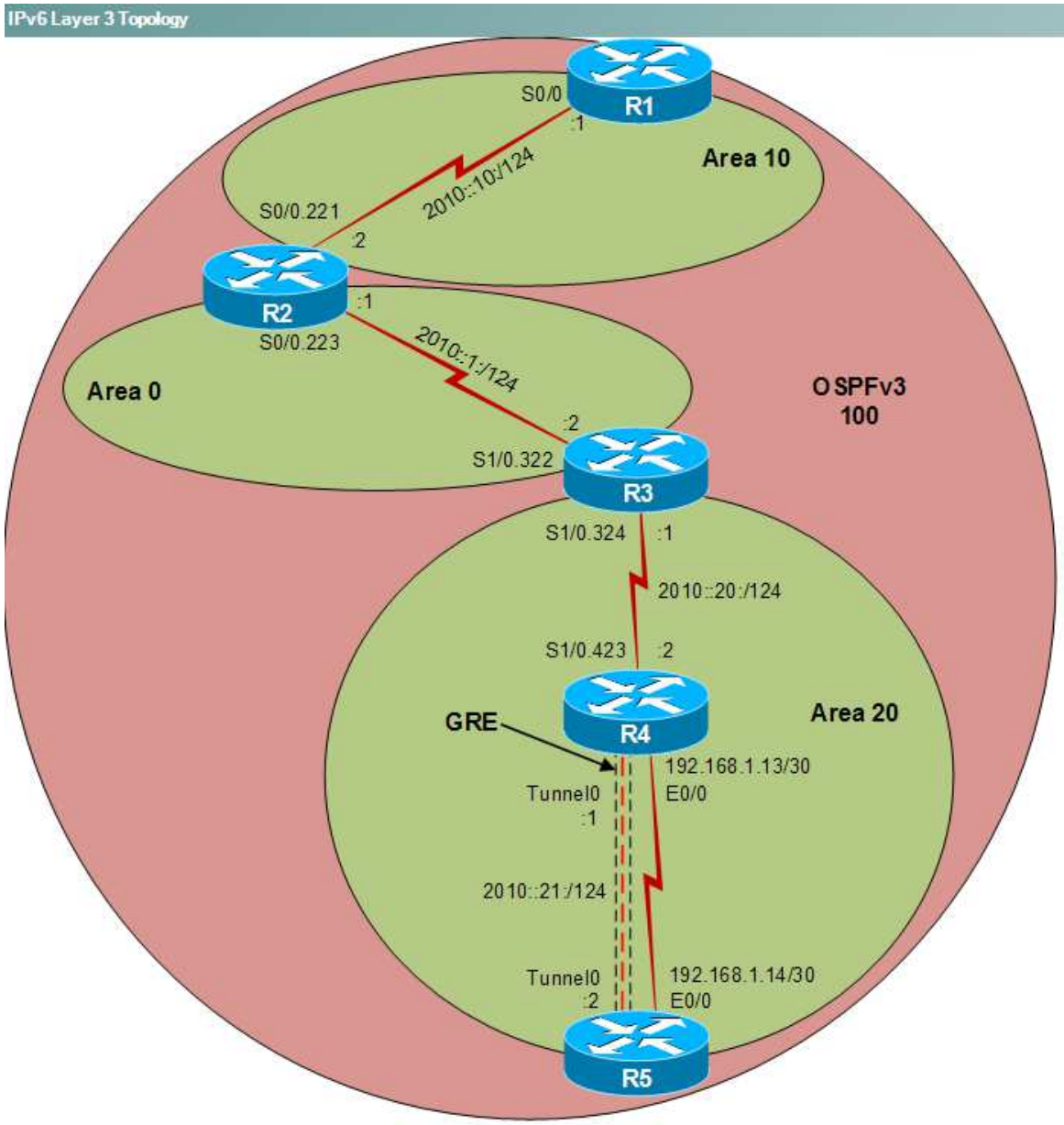
**Layer 2 Topology**




IPv4 layer 3 Topology

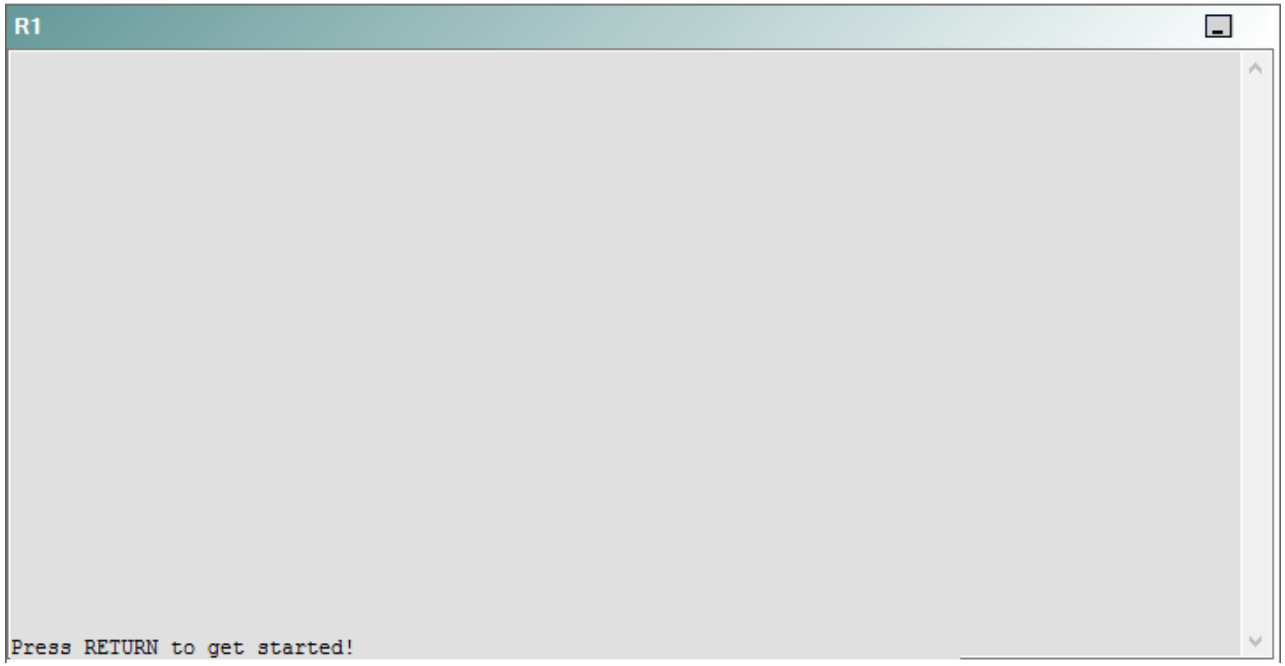

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

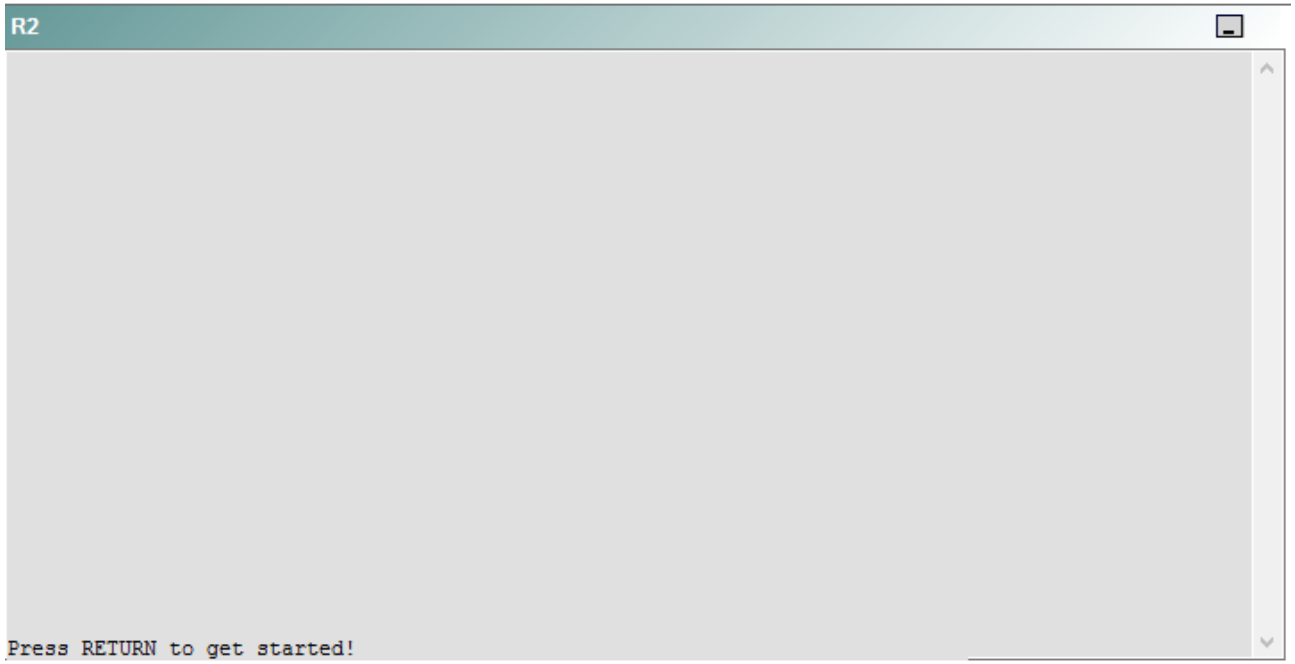



https://www.gratisexam.com/

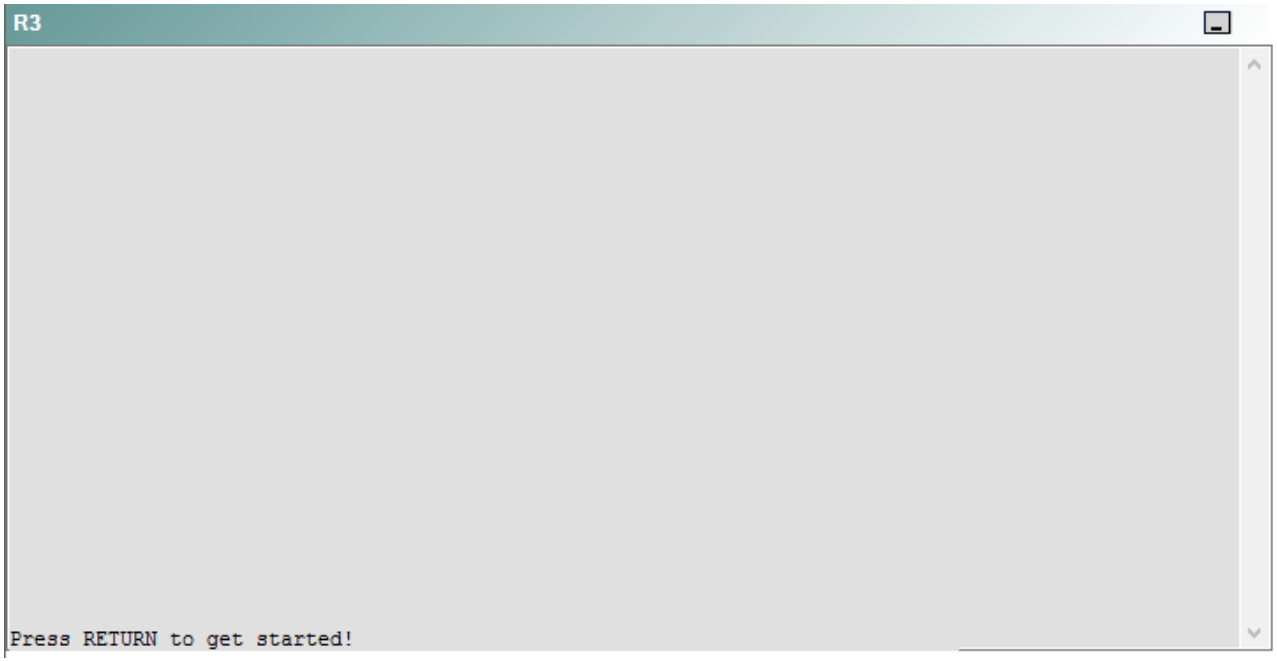
R1



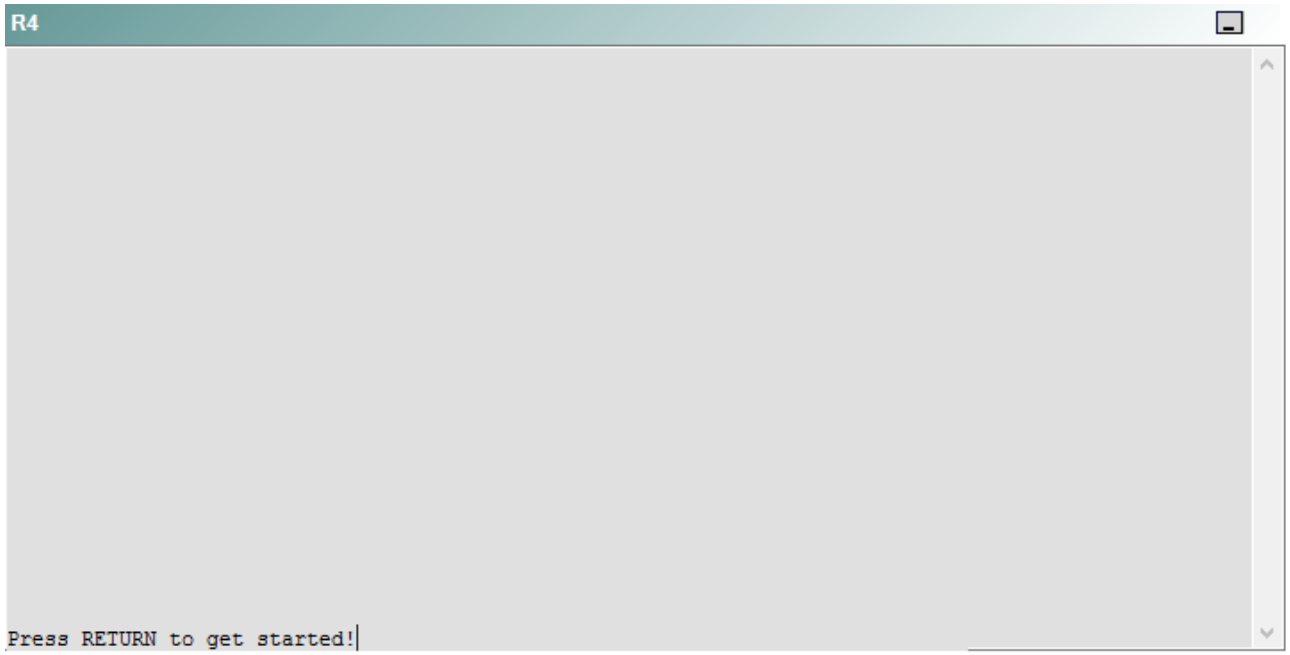

R2



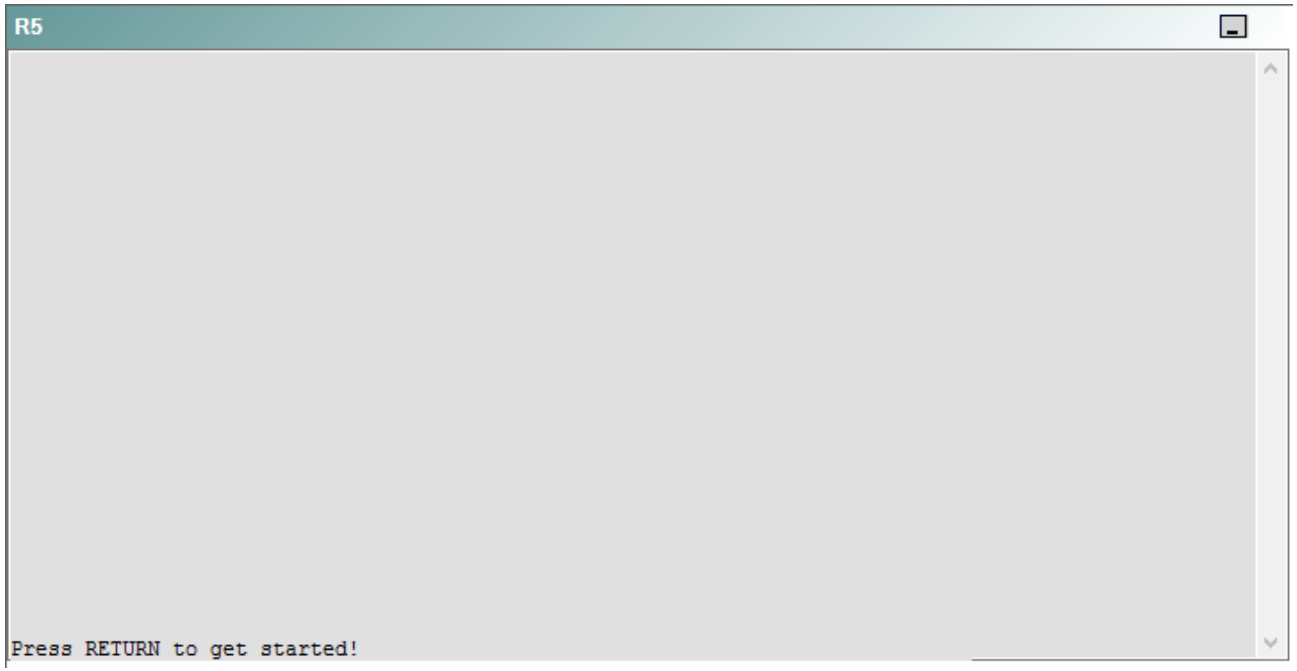

R3



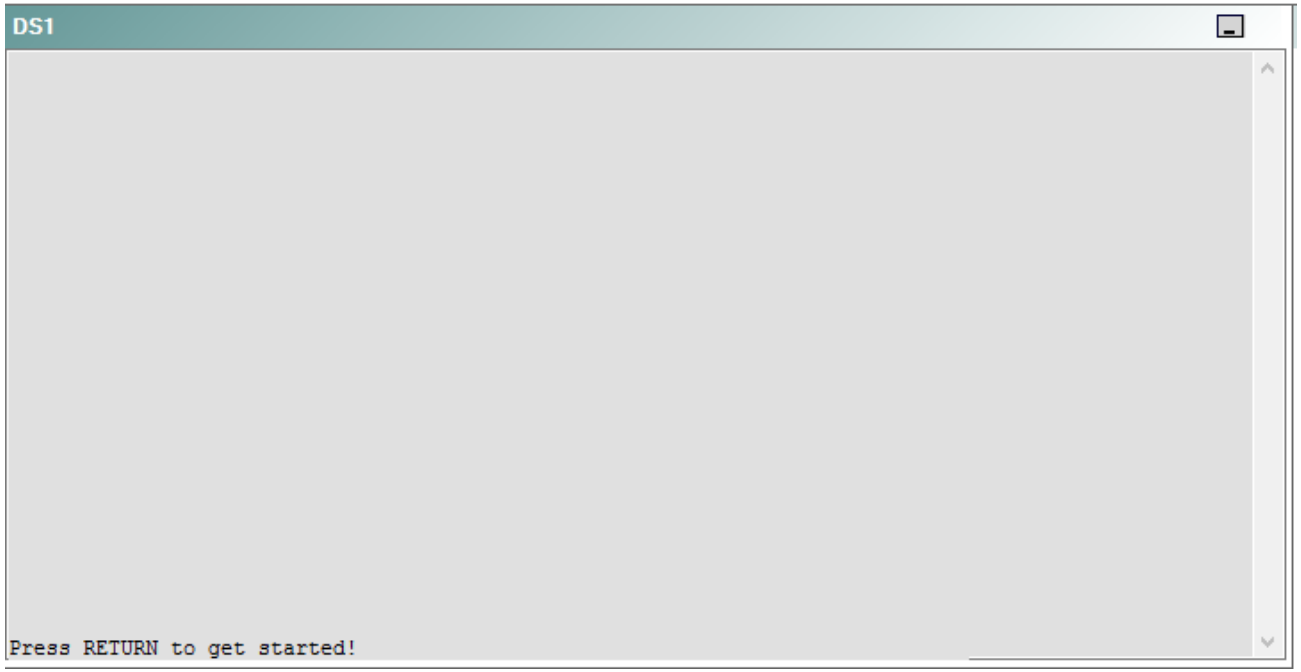

R4



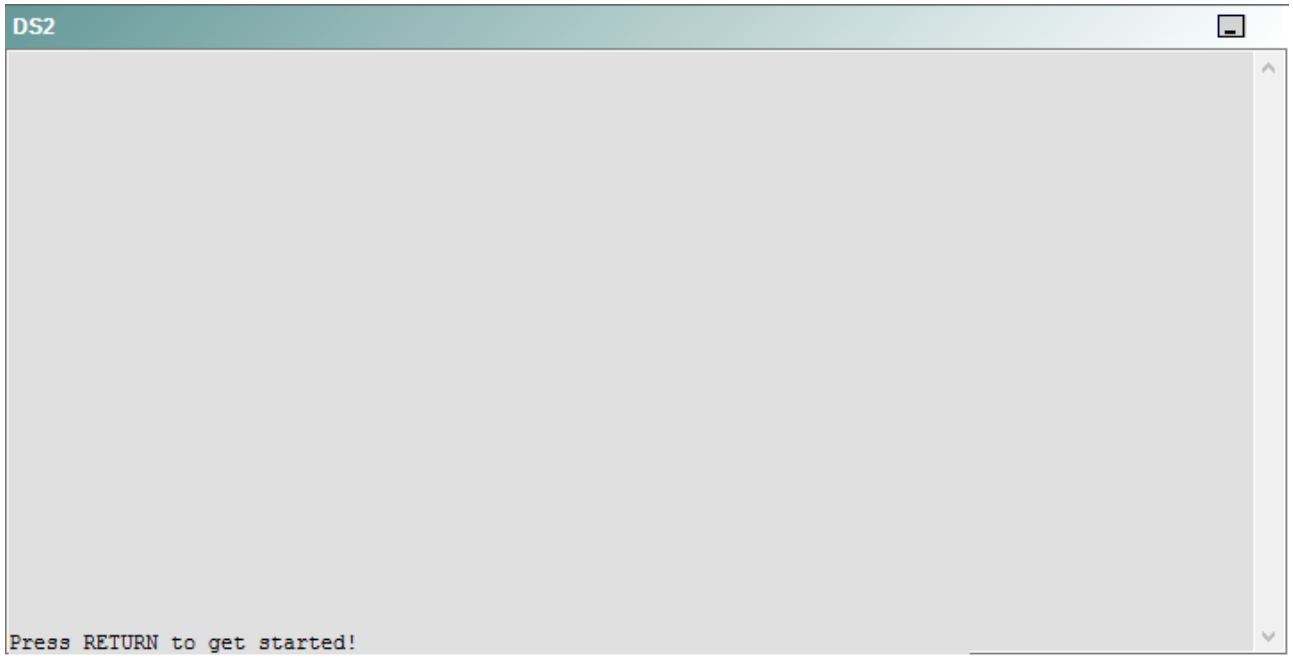

R5



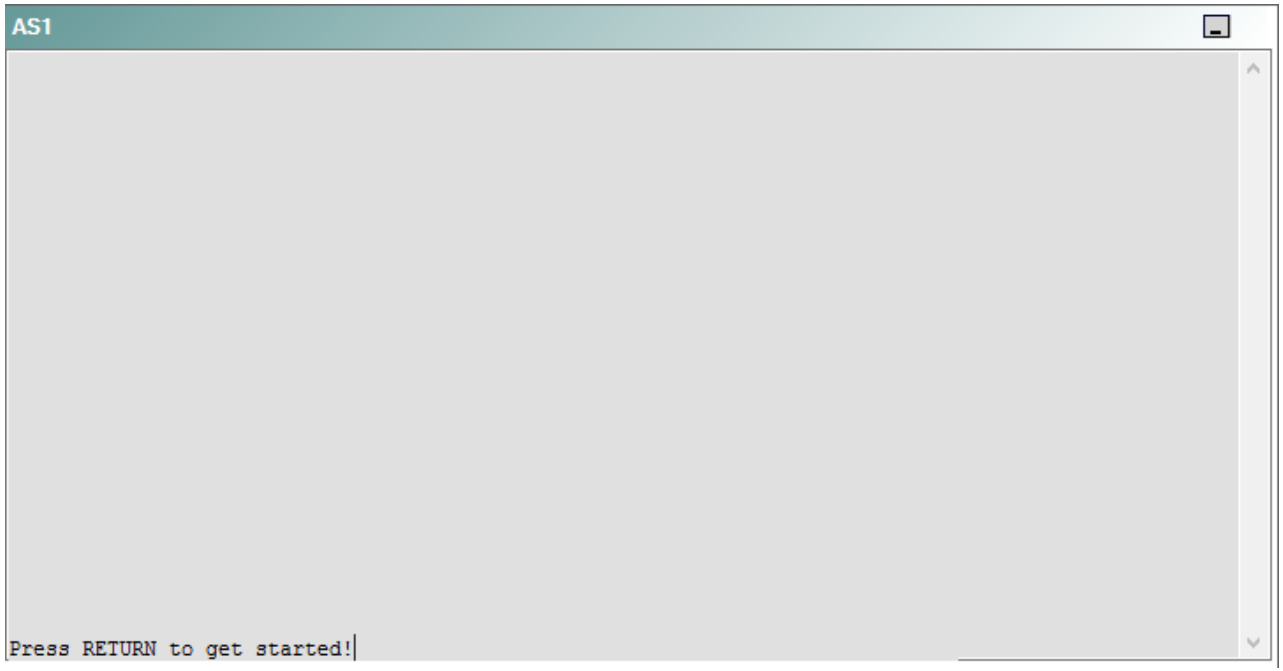

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. HSRP
C. OSPFv2
D. DHCP
E. Layer 3 addressing
F. STP
G. Etherchannel
H. VLAN configuration
I. interface

**Correct Answer:** C
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 43**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

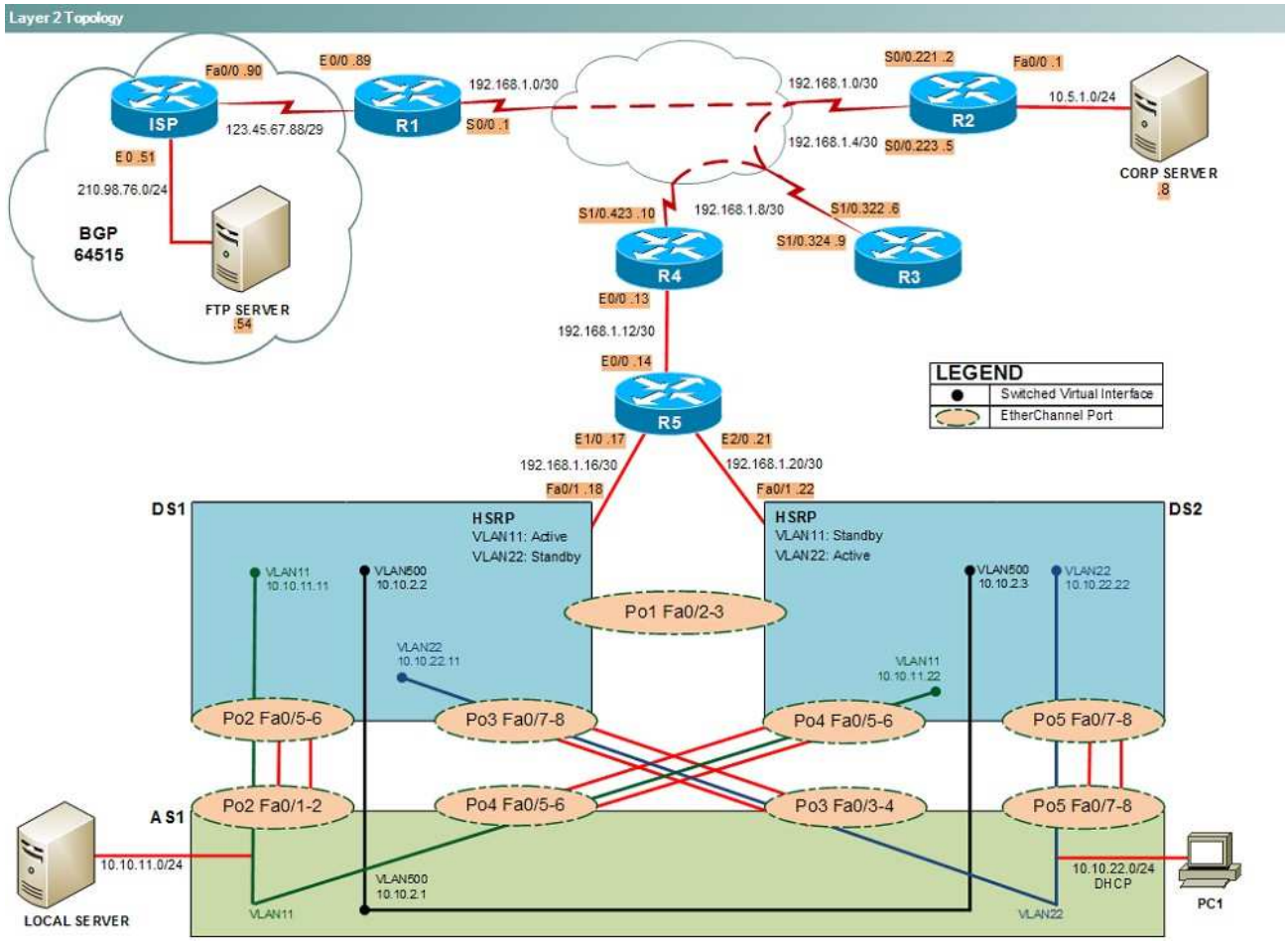
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

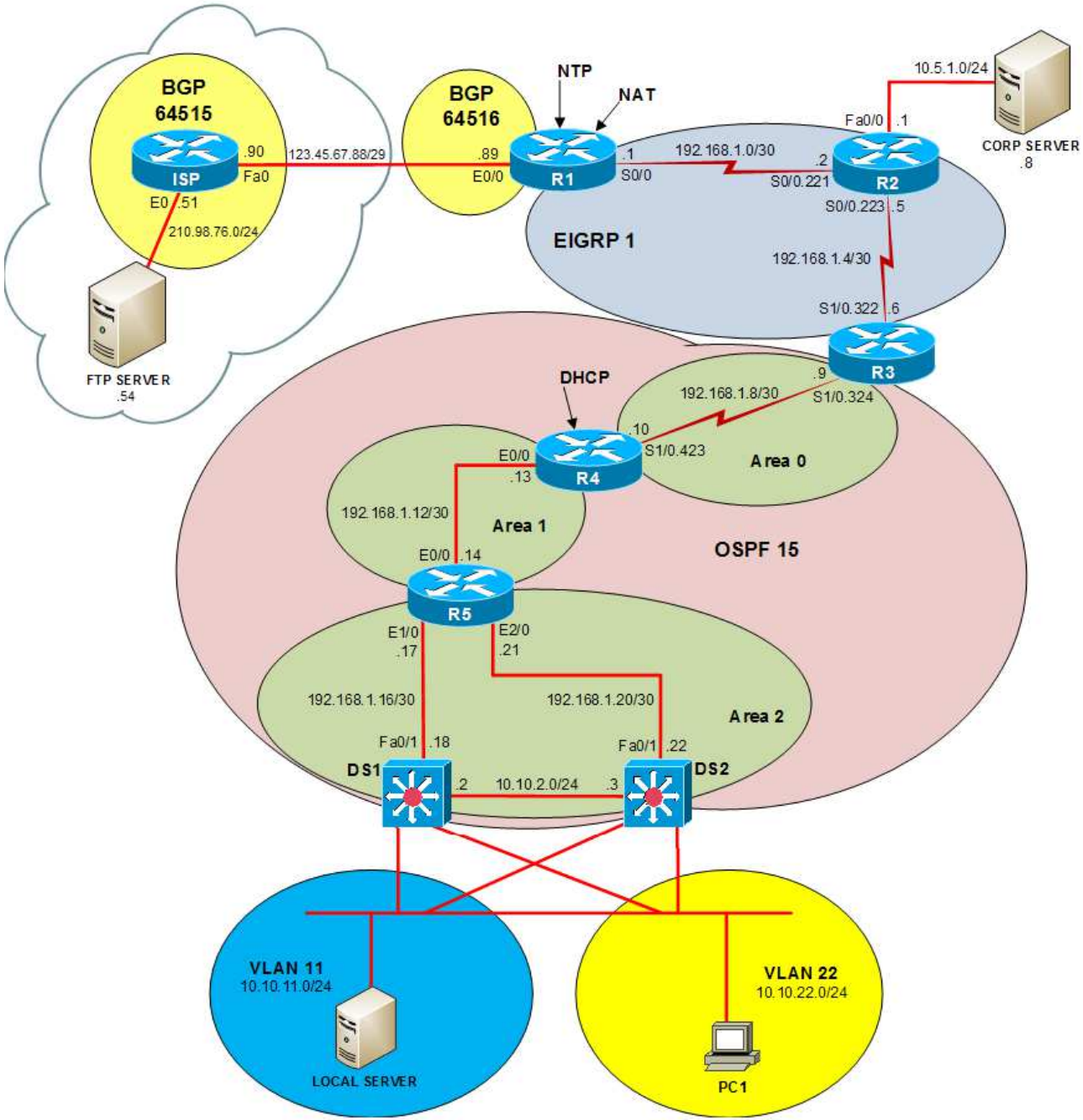
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

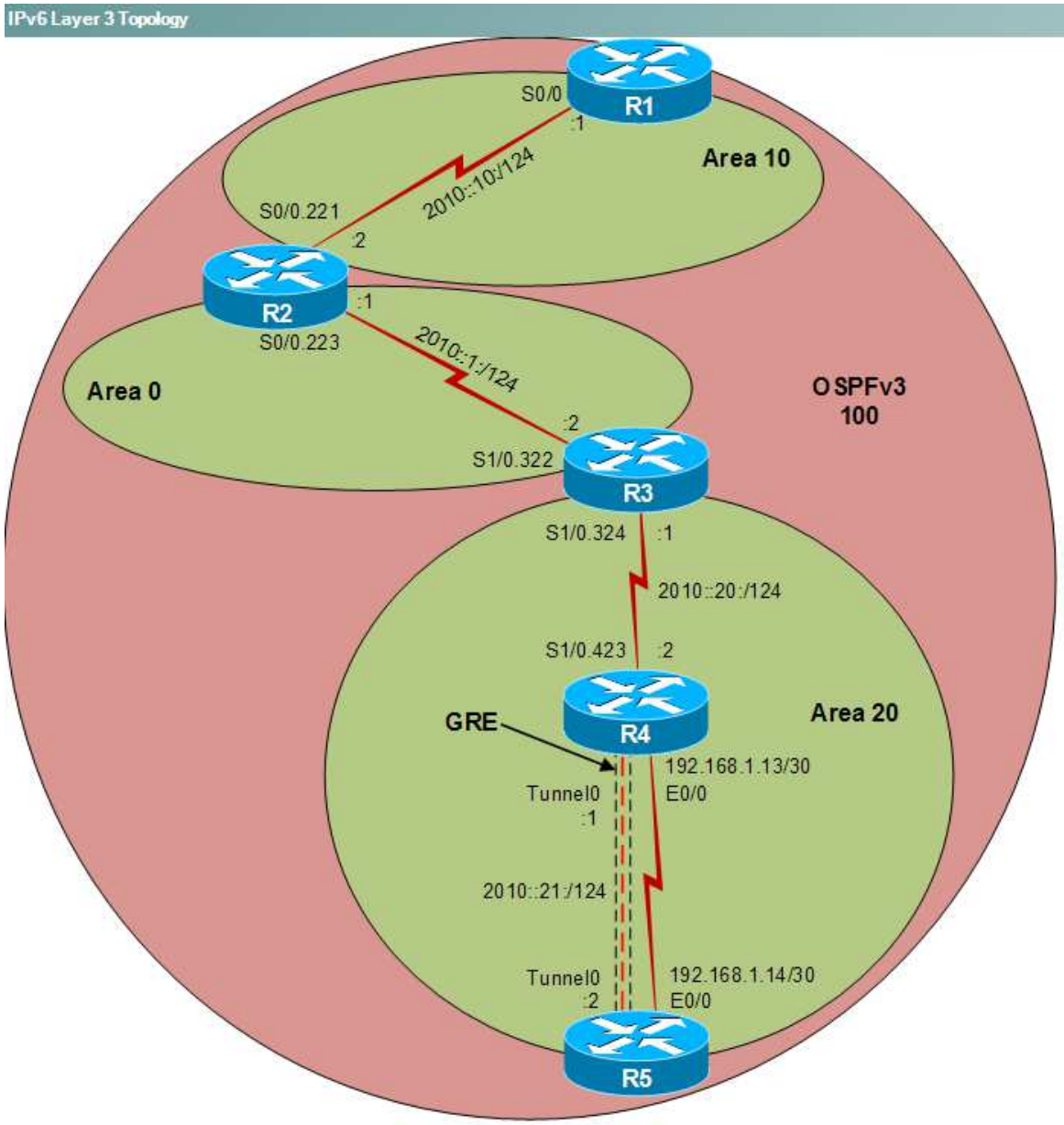
**Layer 2 Topology**




IPv4 layer 3 Topology

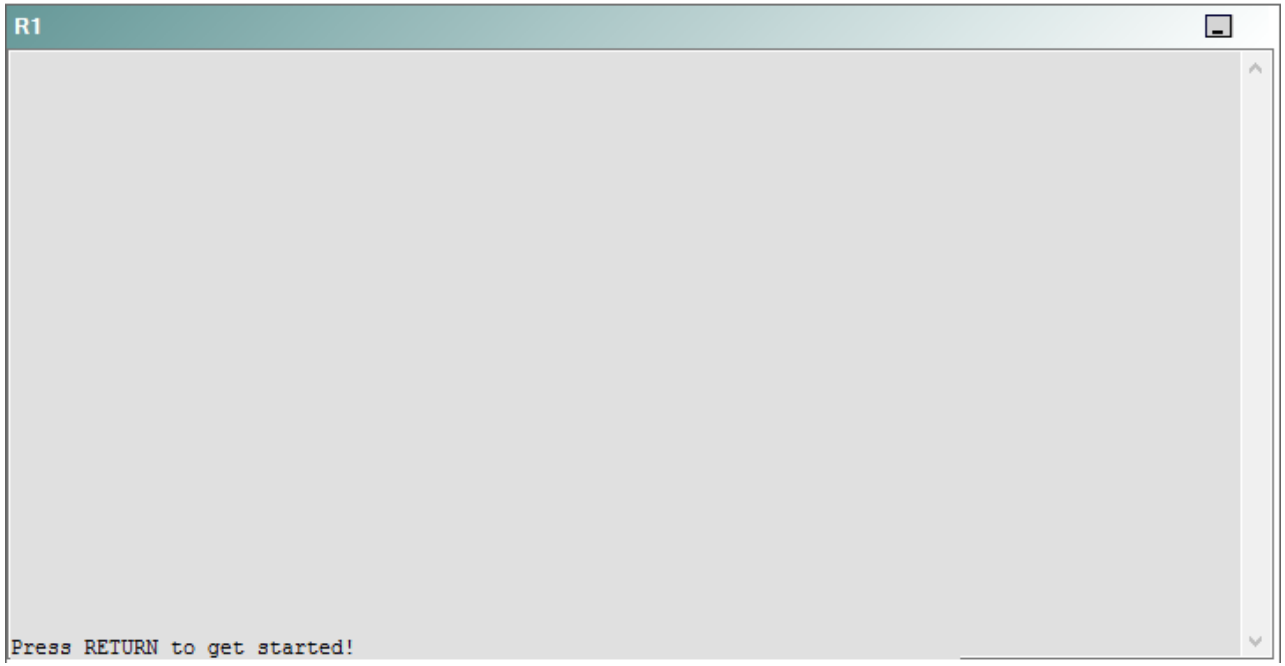

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

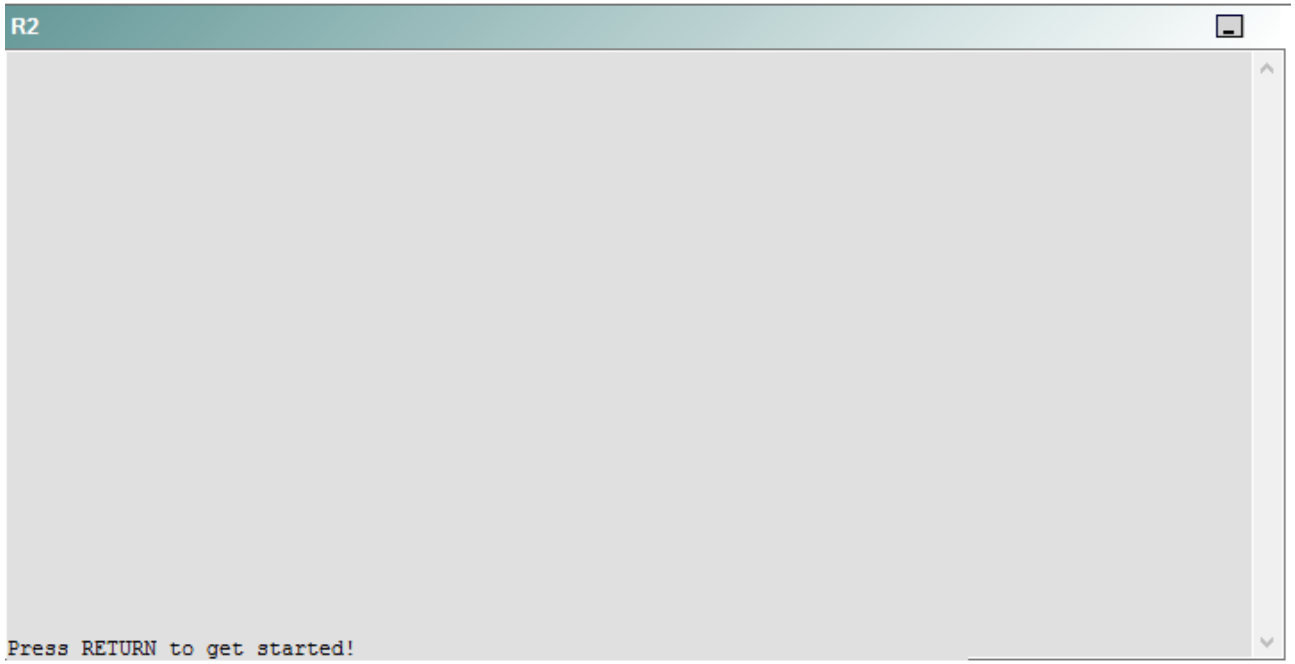



https://www.gratisexam.com/

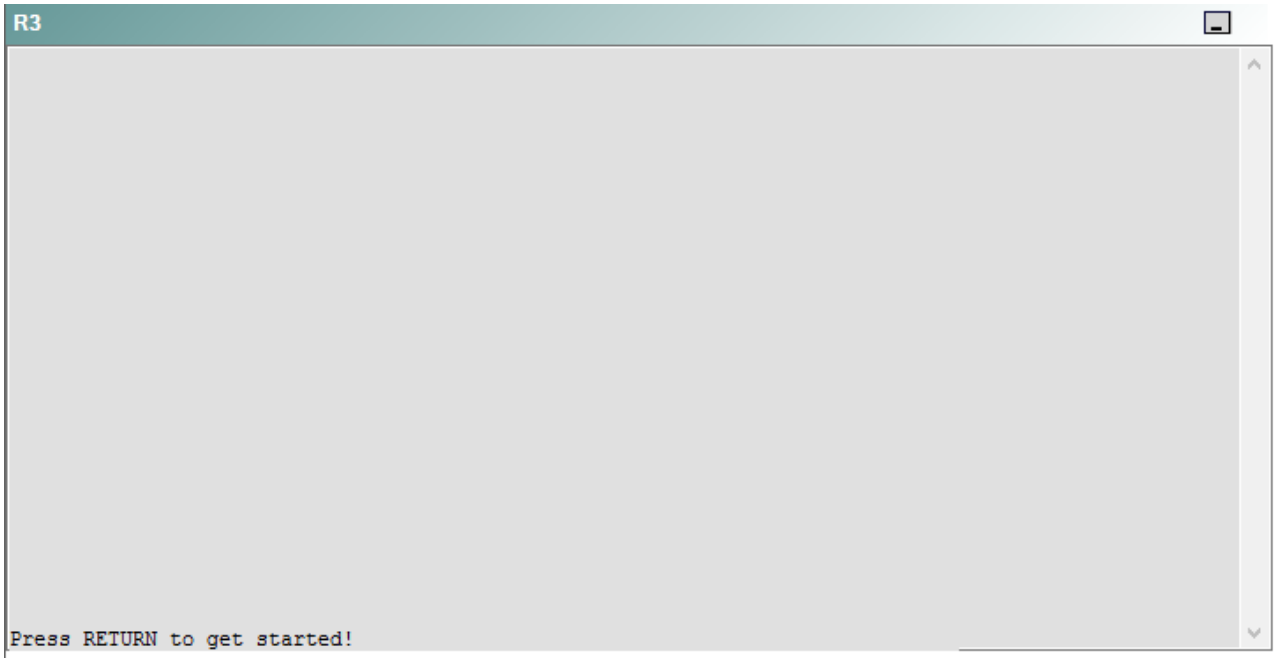
R1



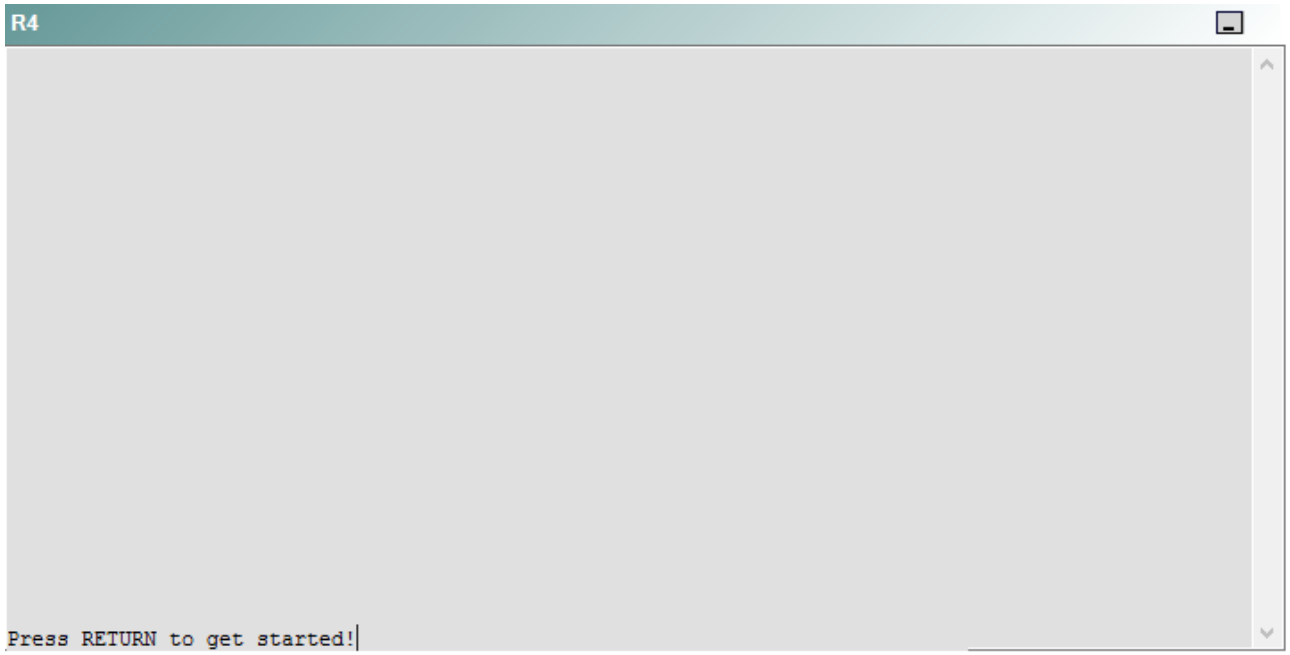

R2



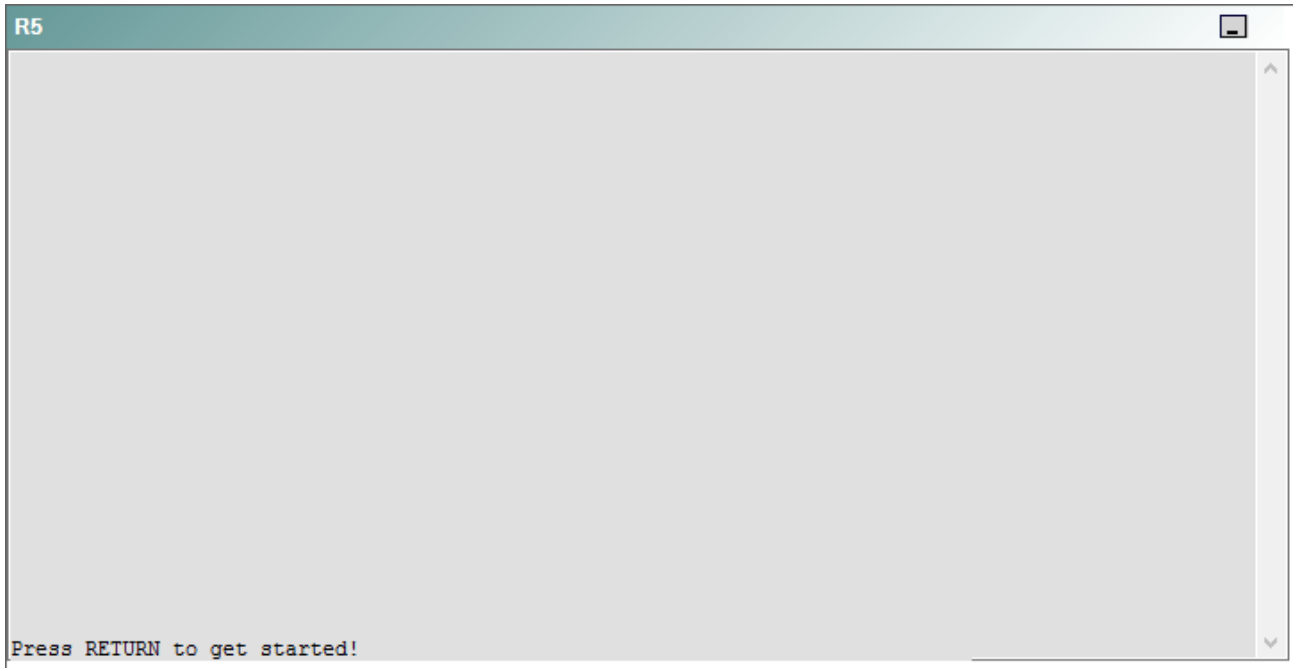

R3



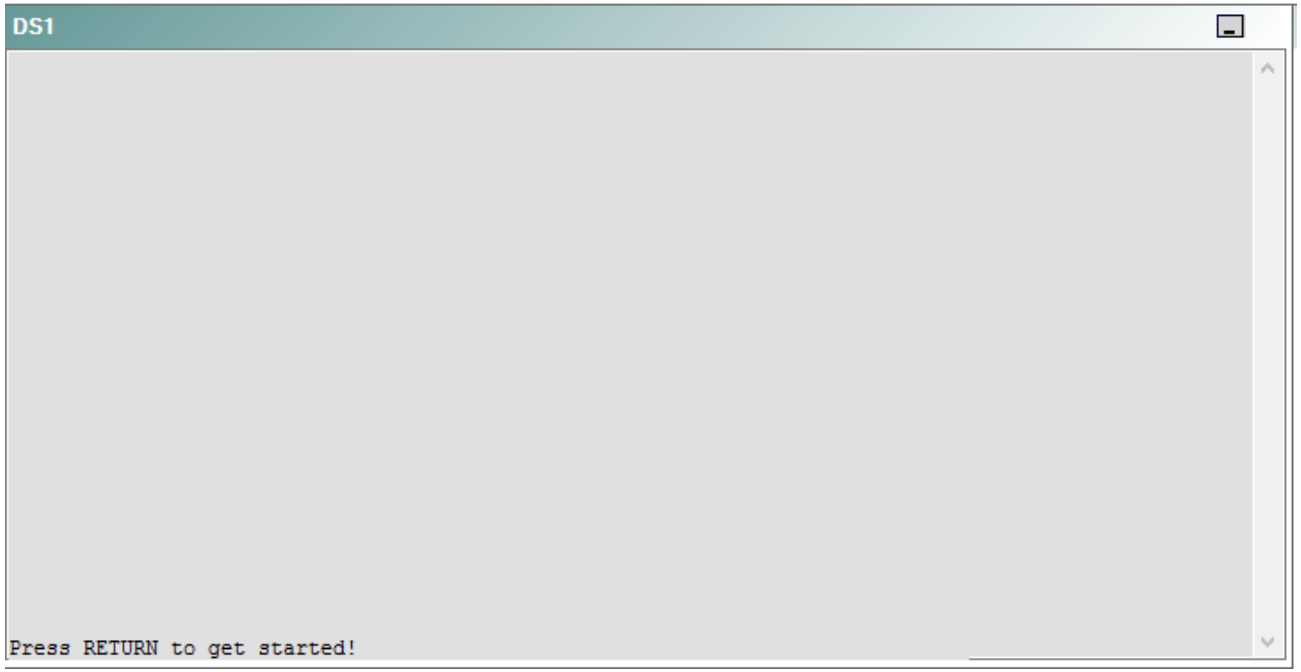

R4



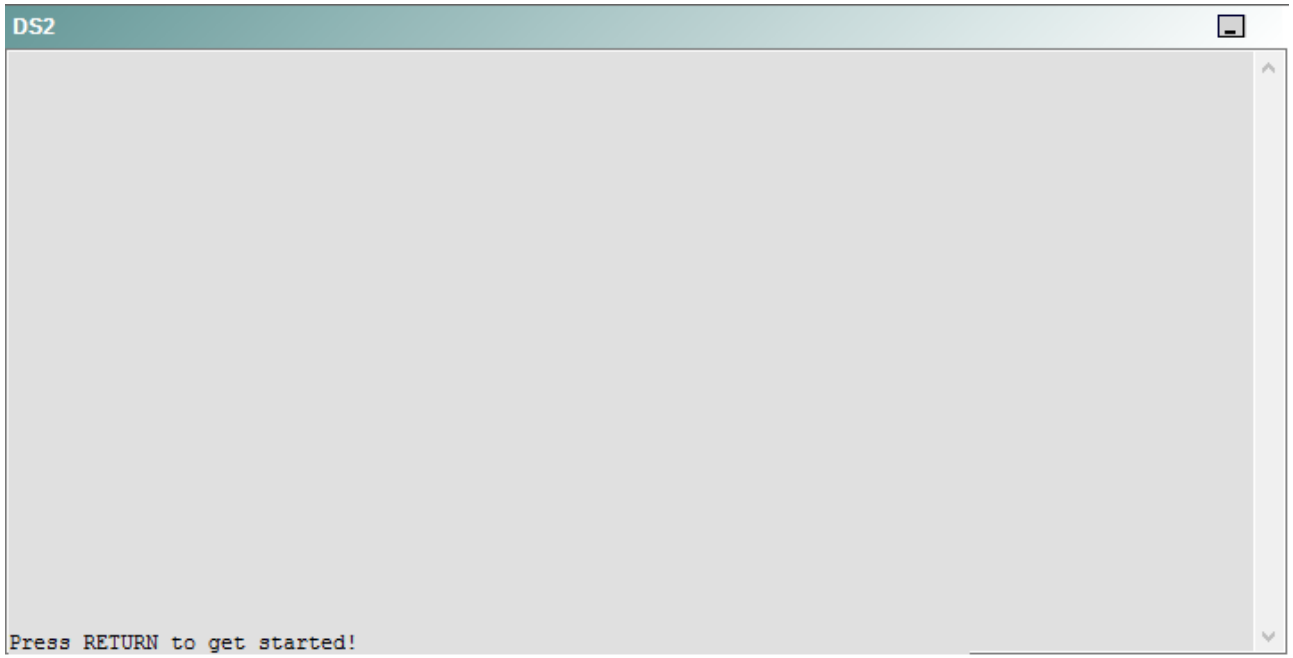

R5



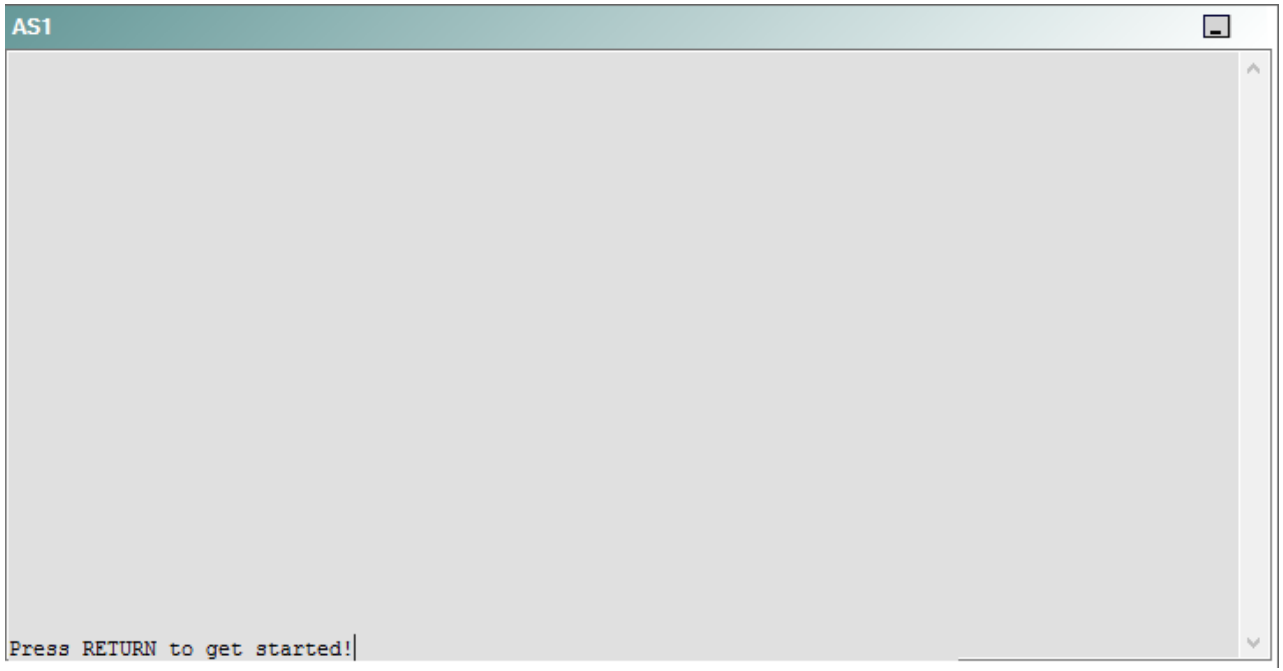

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. issuing the **network 192.168.1.12 0.0.0.3 area 1** command
B. issuing the **network 192.168.1.12 0.0.0.3 area 2** command
C. issuing the **area 1 virtual-link 192.168.99.5** command
D. issuing the **area 2 virtual-link 192.168.99.5** command
E. changing the OSPF routing process to 15
F. changing the OSPF network type
G. changing the masks on the OSPF network statements
H. issuing the **no ip ospf hello-interval** command on the E0/0 interface
I. changing the OSPF router ID

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

You should issue the **area 1 virtual-link 192.168.99.5** command on R4. To determine which device is the source of the problem, you can issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from PC1 to the closest device and work your way up the network until communication is lost, or you can ping from PC1 to the farthest device and work your way back to PC1 until pings are successful.

In this scenario, PC1 is unable to ping any device on the network. Issuing the **ipconfig** command on PC1 will display the following output:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Autoconfiguration IP Address. . . : 169.254.133.250
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :
```

An address that begins with 169.254 indicates that the computer is using an Automatic Private IP Addressing (APIPA) address. A computer will assign itself an APIPA address if it fails to receive an IP address from a Dynamic Host Configuration Protocol (DHCP) server. Therefore, PC1 is unable to communicate with the DHCP server on R4, and the problem must exist somewhere between them.

R4 can ping the File Transfer Protocol (FTP) server at 210.98.76.54, but it cannot ping anything beyond R5. However, R5 can ping the FTP server at 210.98.76.54 and the local server at 10.10.11.5. Therefore, something must be blocking communication between R4 and R5.

R3, R4, R5, DS1, and DS2 are currently configured to use Open Shortest Path First version 2 (OSPFv2). All areas in an OSPF internetwork must be connected to the backbone area, Area 0. However, Area 2 does not connect to Area 0. Therefore, a virtual link must be created between R4 and R5 to connect Area 2 to Area 0 through a transit area, Area 1. The following restrictions apply to virtual links:

The routers at each end of the virtual link must share a common area.
The transit area cannot be a stub area.
One router must connect to the backbone area.

To create a virtual link, you must issue the **area virtual-link** command on each Area Border Router (ABR). The syntax of the **area virtual-link** command is **area**

*area-id* **virtual-link** *router-id*, where *area-id* is the transit area ID, and *router-id* is the router ID of the router at the other end of the router at the other end of the virtual link. Issuing the **show running-config** command on R5 indicates the presence of the **area 1 virtual-link 192.168.99.4** command. However, the **area 1 virtual-link 192.168.99.5** command is missing from R4. Issuing this command will enable R4 to communicate with the rest of the network.

You should not issue the **area 2 virtual-link 192.168.99.5** command on R4 or the **area 2 virtual-link 192.168.99.4** command on R5, because Area 1, not Area 2, is the transit area. You should not issue the **area 1 virtual-link 192.168.1.14** command on R4 or the **area 1 virtual-link 192.168.1.13** command on R5, because you should use the router ID of the router at the other end of the virtual link for the *router-id* parameter; you should not use the router's interface IP address. You should not issue the **area 2 virtual-link 192.168.99.5** command on R3, because R3 is not command to the transit area.

You should not issue the **no ip ospf hello-interval** command on any of the devices on the network. By default, the hello timer is set to 10 seconds on point-to-point and broadcast links and 30 seconds on nonbroadcast multiaccess (NBMA) links. You can verify the hello timer settings by issuing the show ip ospf interface command, as shown in the following output:

```
Ethernet0/0 is up, line protocol is up
  Internet Address 192.168.1.13/30, Area 1
  Process ID 15, Router ID 192.168.99.4, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.99.4, Interface address 192.168.1.13
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

You need not change the OSPF routing process on R5 to 15, nor do you need to change the OSPF routing process on the other devices to 10. The OSPF routing process number is locally significant, so two OSPF routers with different routing process numbers can still form an adjacency as long as the following parameters match:

- Hello timer
- Dead timer
- Area number and type
- Network type
- Subnet
- Authentication type and password

In addition, OSPF cannot establish an adjacency over a secondary IP address.

You need not change the OSPF network type on the E0/0 interface of R4 or R5. The OSPF network type must match so that connected interfaces can form an adjacency. The E/0 interfaces on R4 and R5 are both set to the broadcast OSPF network type. You can determine the OSPF network type by issuing the **show ip ospf interface** command. To change the OSPF network type for an interface, you would issue the **ip ospf network {broadcast** | **non-broadcast** | **point-to-multipoint** | **point-to-point}** command from interface configuration mode.

You need not change the masks on the OSPF **network** statements. The **network** command uses wildcard masks, which are basically inverse subnet masks. To calculate the appropriate wildcard mask, you should subtract the subnet mask from 255.255.255.255. For example, the 192.168.1.12 network has a /30 subnet mask, which is 255.255.255.252. Subtracting 255.255.255.252 from 255.255.255.255 yields a wildcard mask of 0.0.0.3.

You need not change the router ID on any of the routers. A long as the router ID is unique, OSPF routers will form an adjacency. The first line in the output of the **show ip ospf** command displays the router ID. To change the router ID on a router, you would issue the **router-id** *A.B.C.D* command from OSPF router configuration mode, where *A.B.C.D* is a 32-bit router ID in dotted decimal notation.

You need not enable OSPF Message Digest 5 (MD5) authentication, because OSPF MD5 authentication is not enabled on any of the routers on the network. OSPF authentication can be enabled for an interface or for an area. To configure OSPF MD5 authentication for an interface, you would issue the **ip ospf authentication message-digest** command in interface configuration mode. To configure OSPF MD5 authentication for an area, you would issue the **area** *area-id* **authentication message-digest** command in router configuration mode. To configure the key that should be used for MD5 authentication, you would issue the **ip ospf message-digest-key** *key-id* **md5** *key* command in interface configuration mode.

You need not issue the **network 192.168.1.12 0.0.0.3 area** 1 command on R4 or R5, because this command has already been issued on both routers. You should not issue the **network 192.168.1.12 0.0.0.3 area 2** command on R4 or R5, because the 192.168.1.12/30 network should exist in Area 1, not Area 2.

Reference:

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/47866-ospfdb7.html
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13699-29.html#seventh

**QUESTION 44**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640

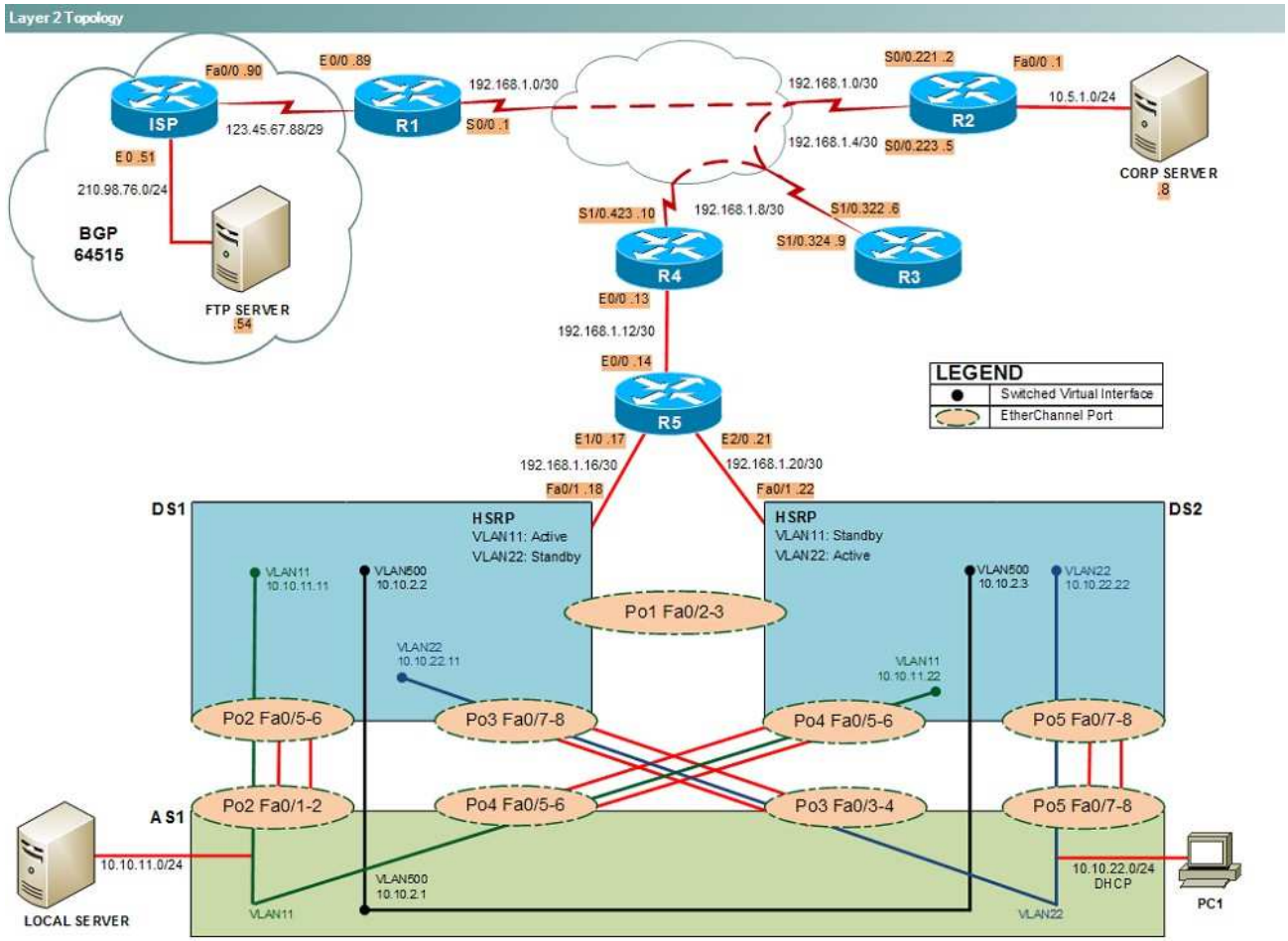
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

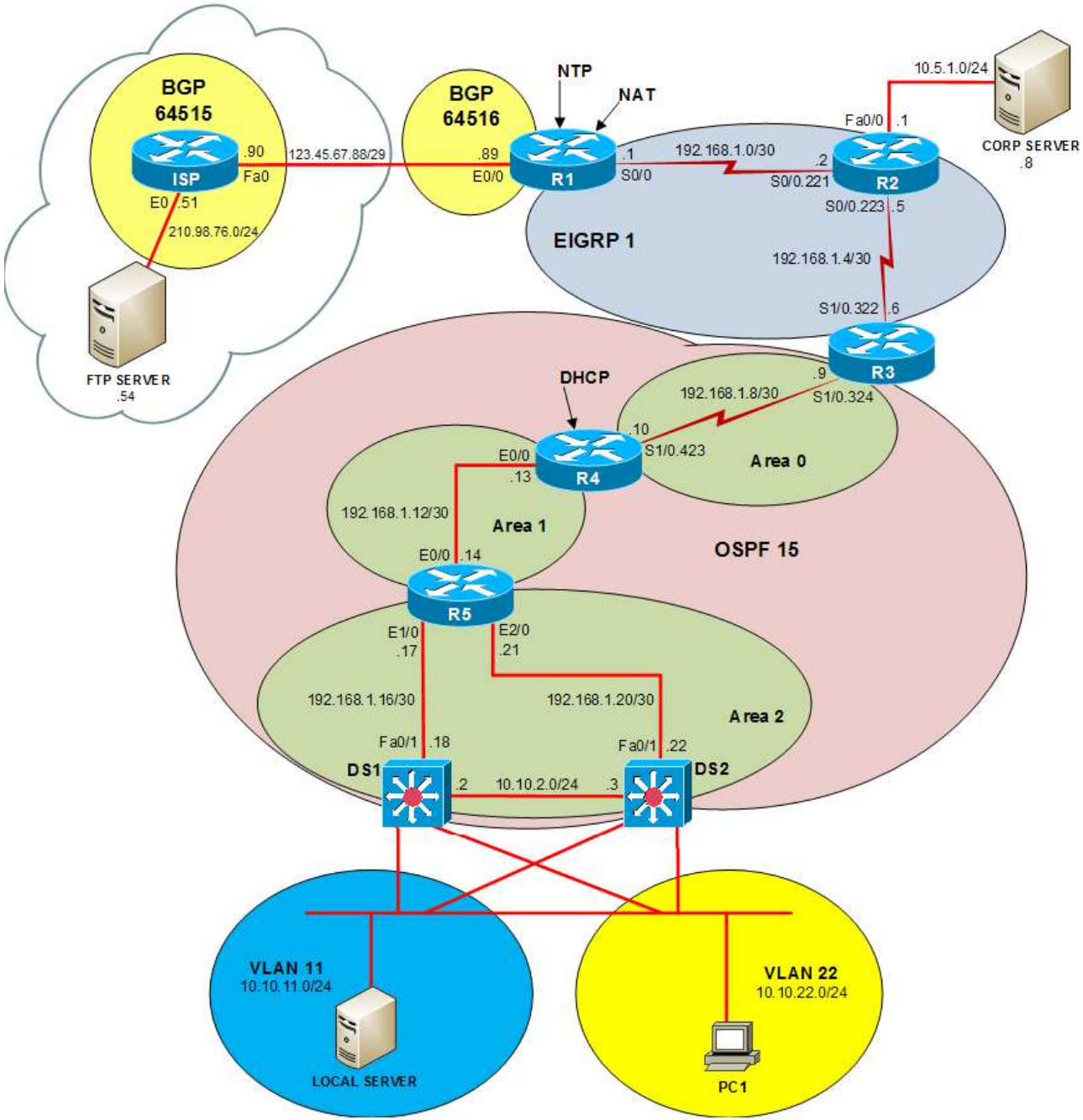
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

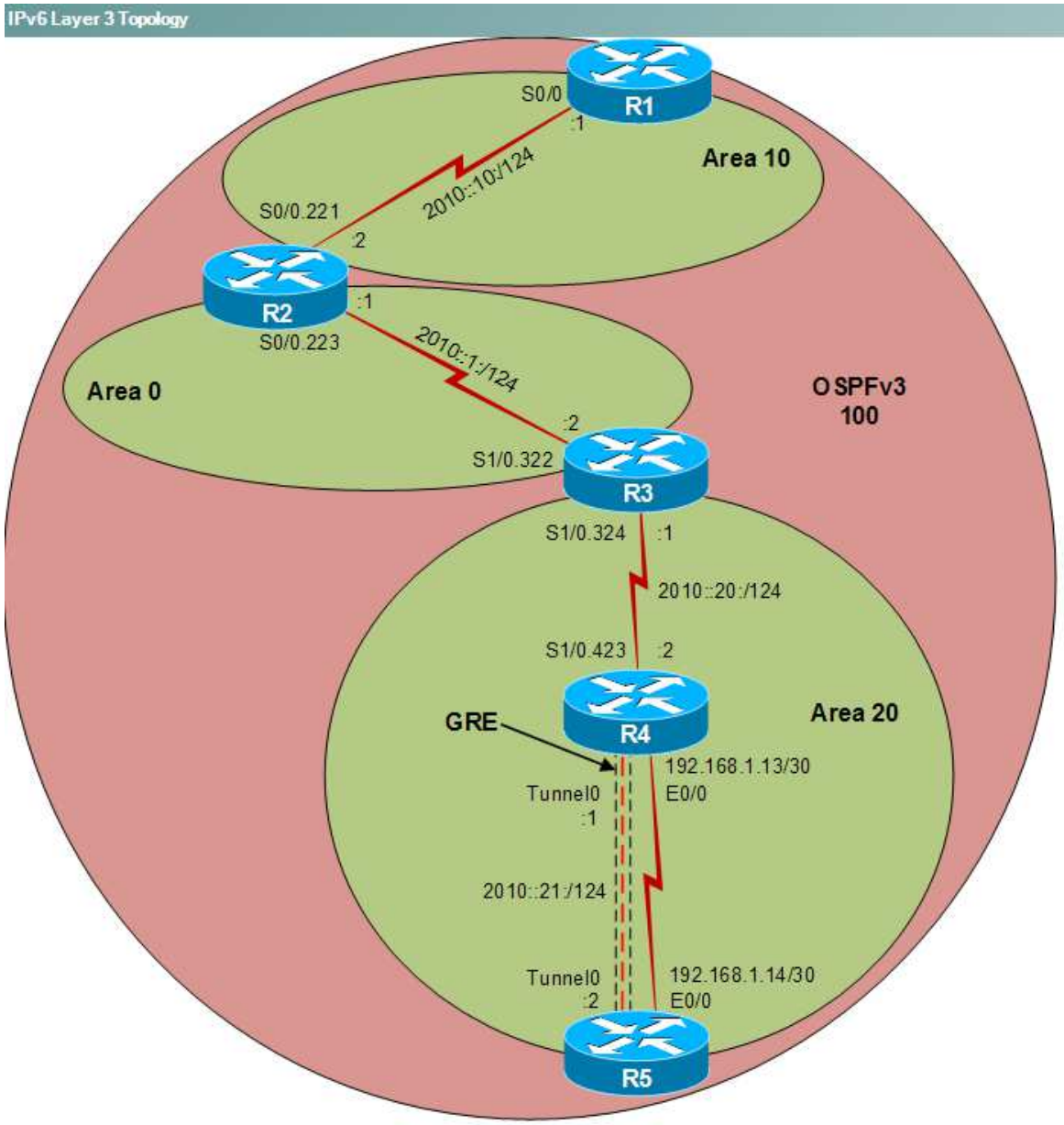
**Layer 2 Topology**




IPv4 layer 3 Topology

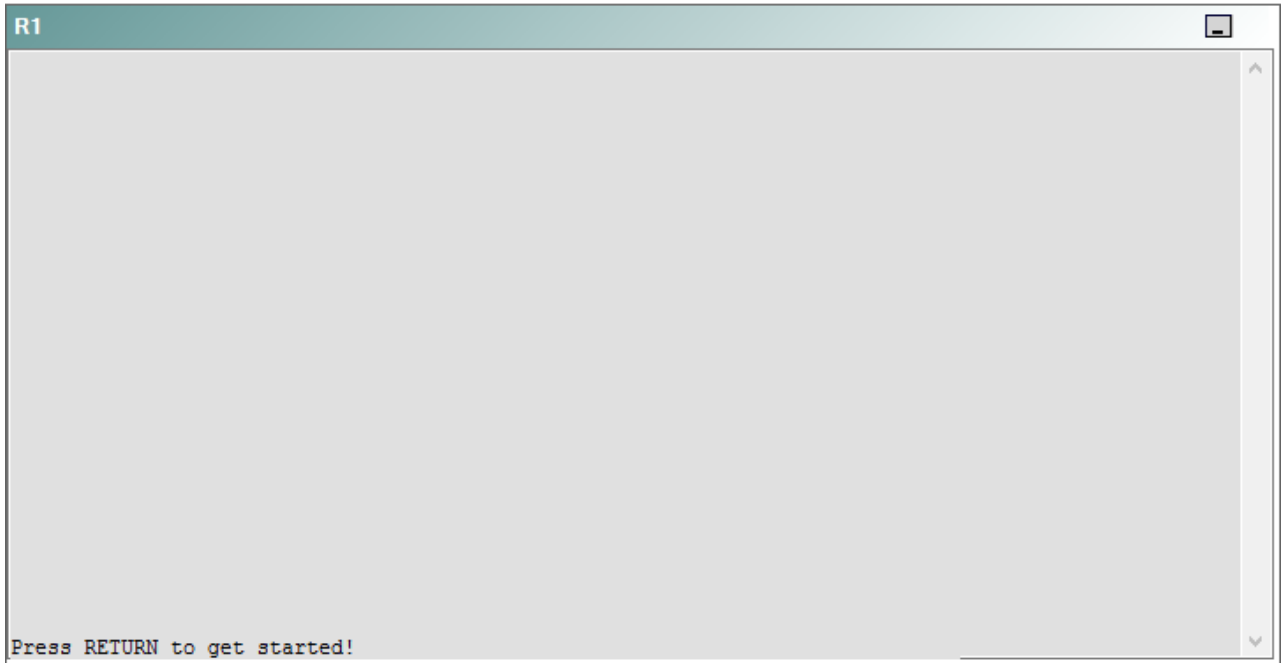

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

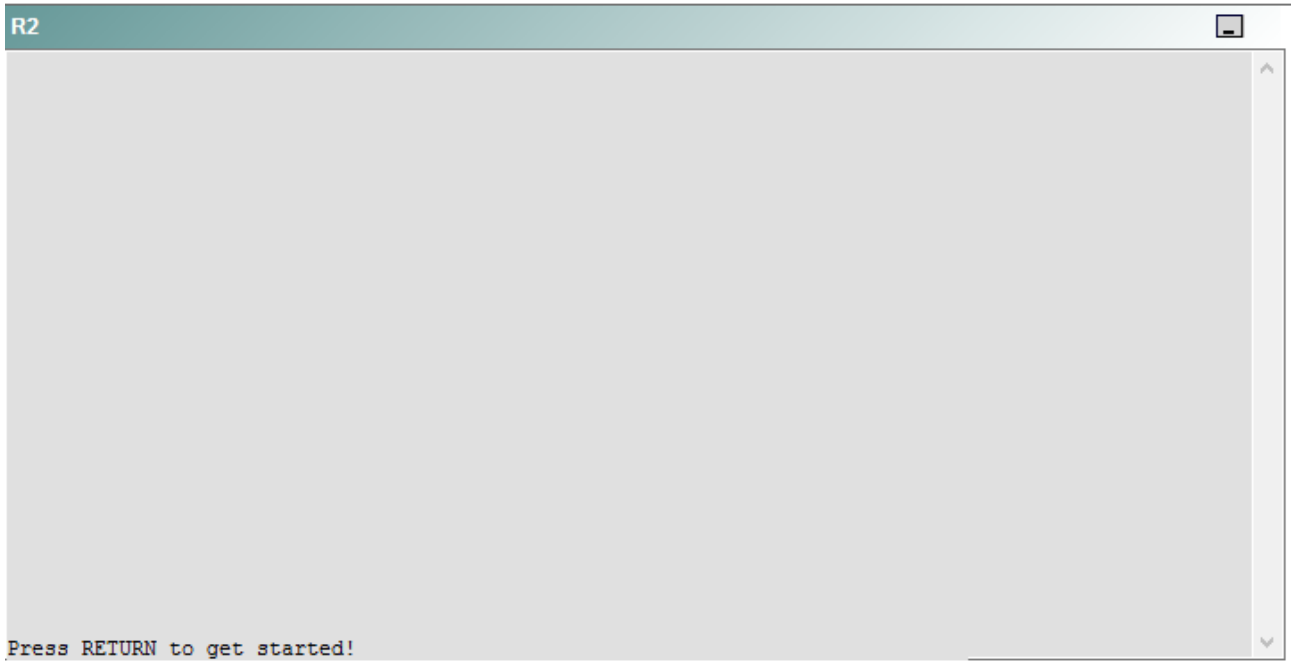



https://www.gratisexam.com/

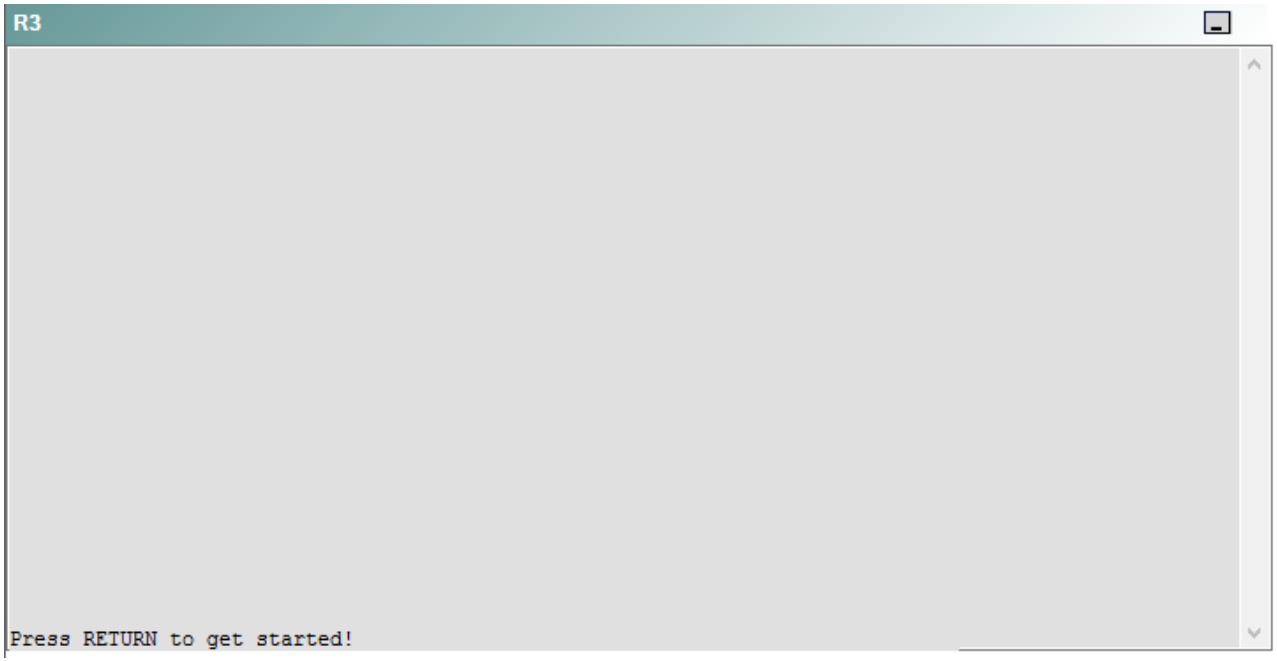
R1



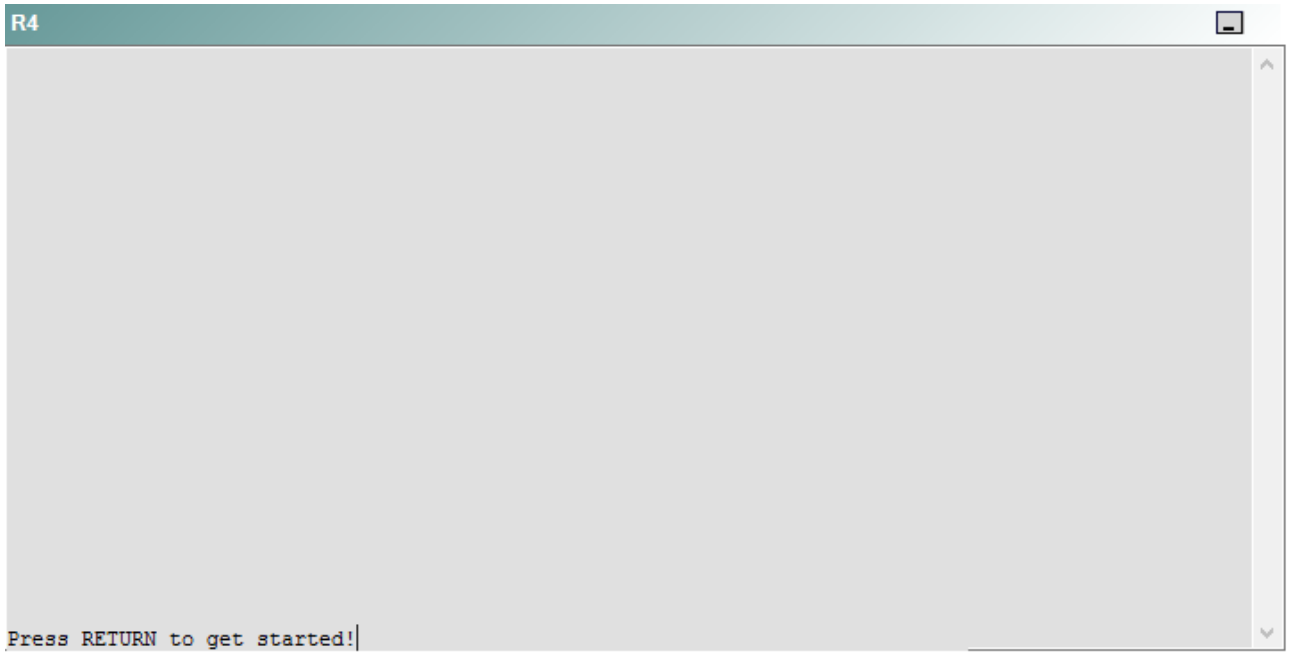

R2



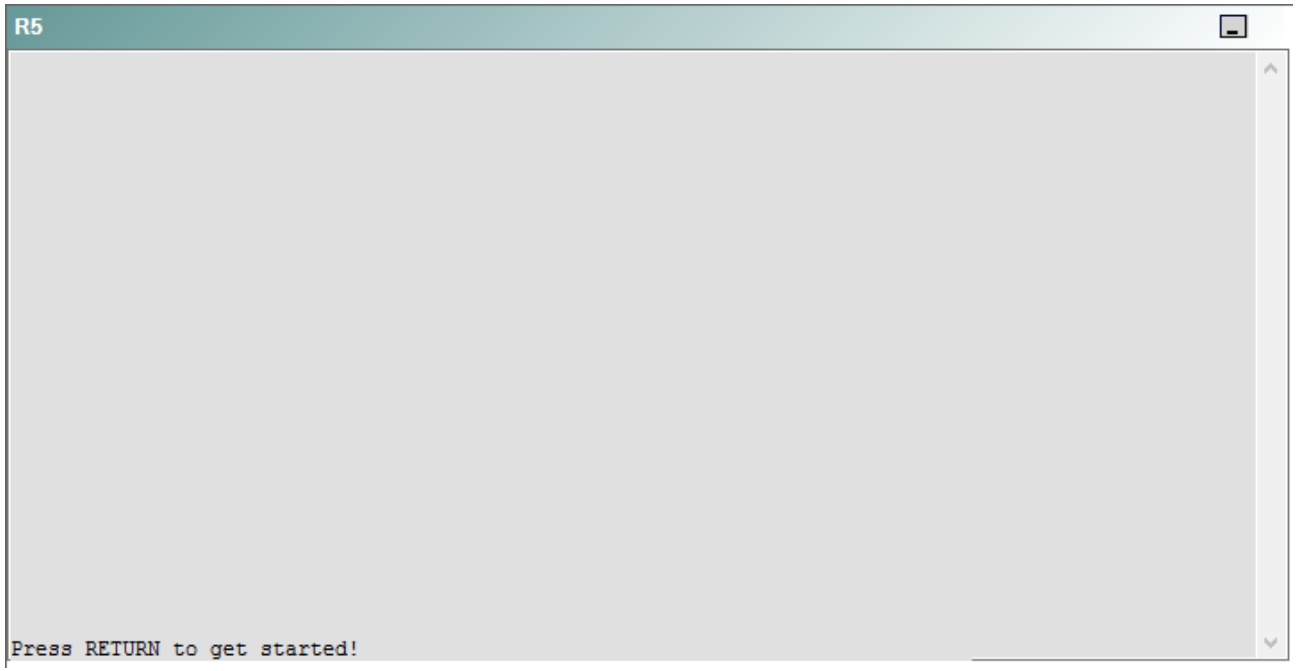

R3



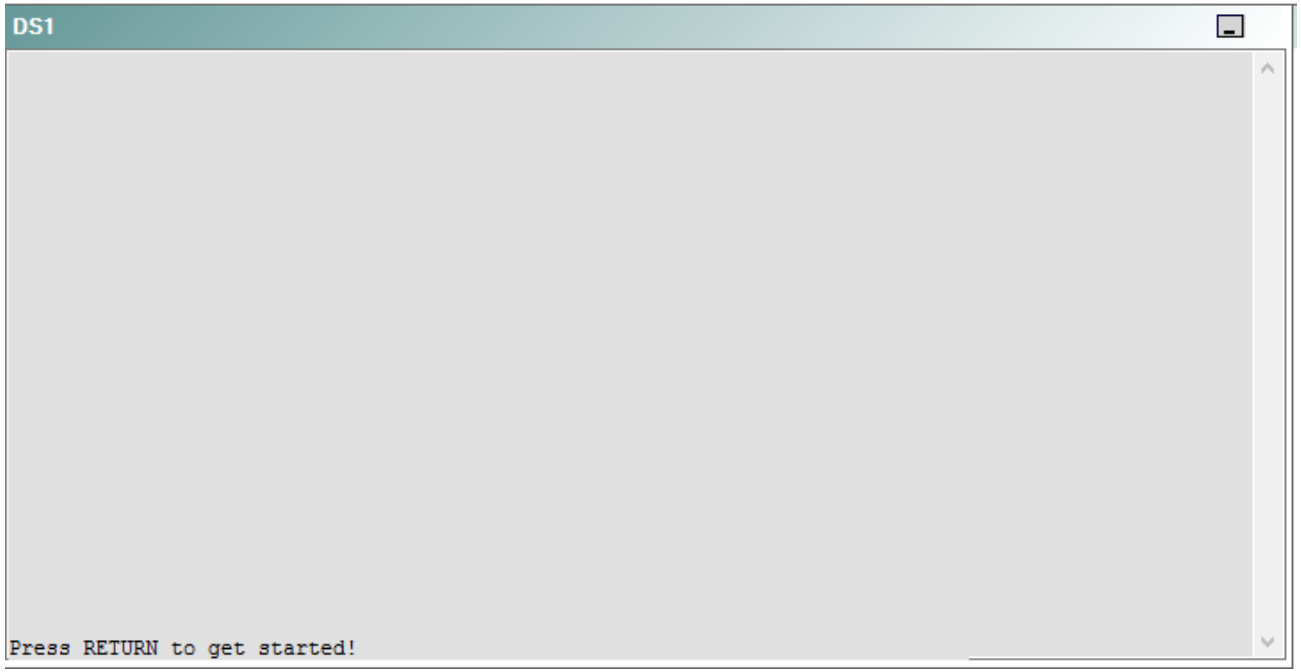

R4



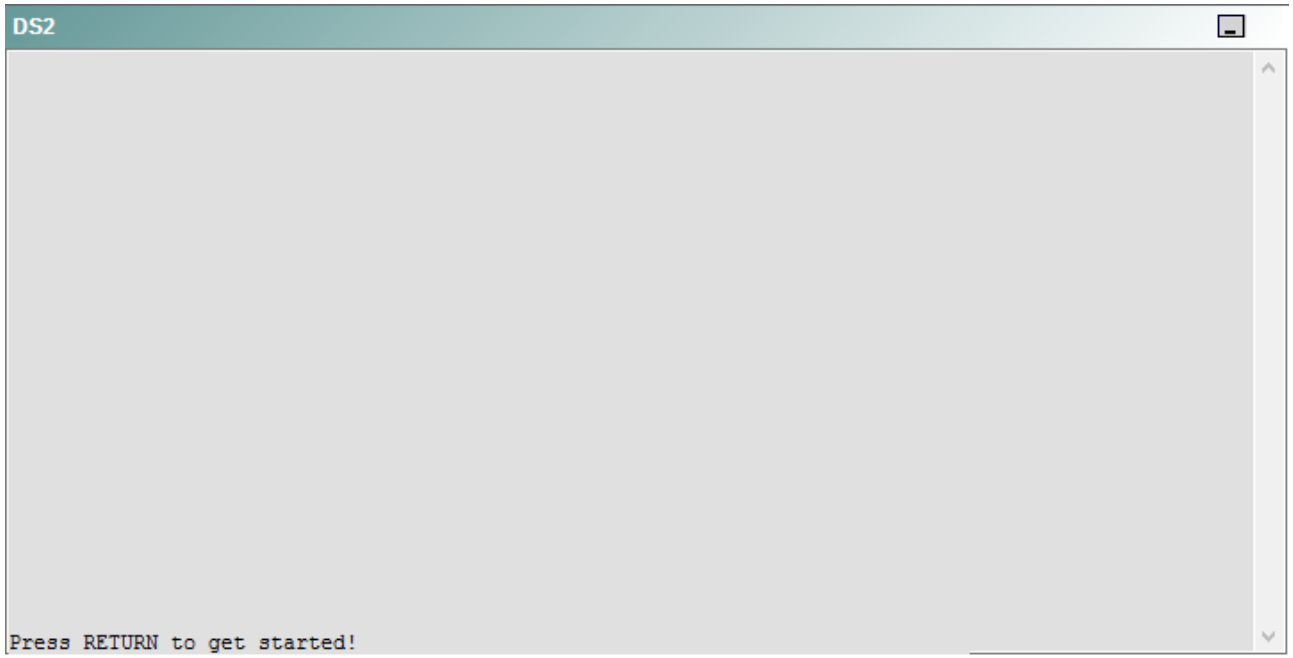

R5



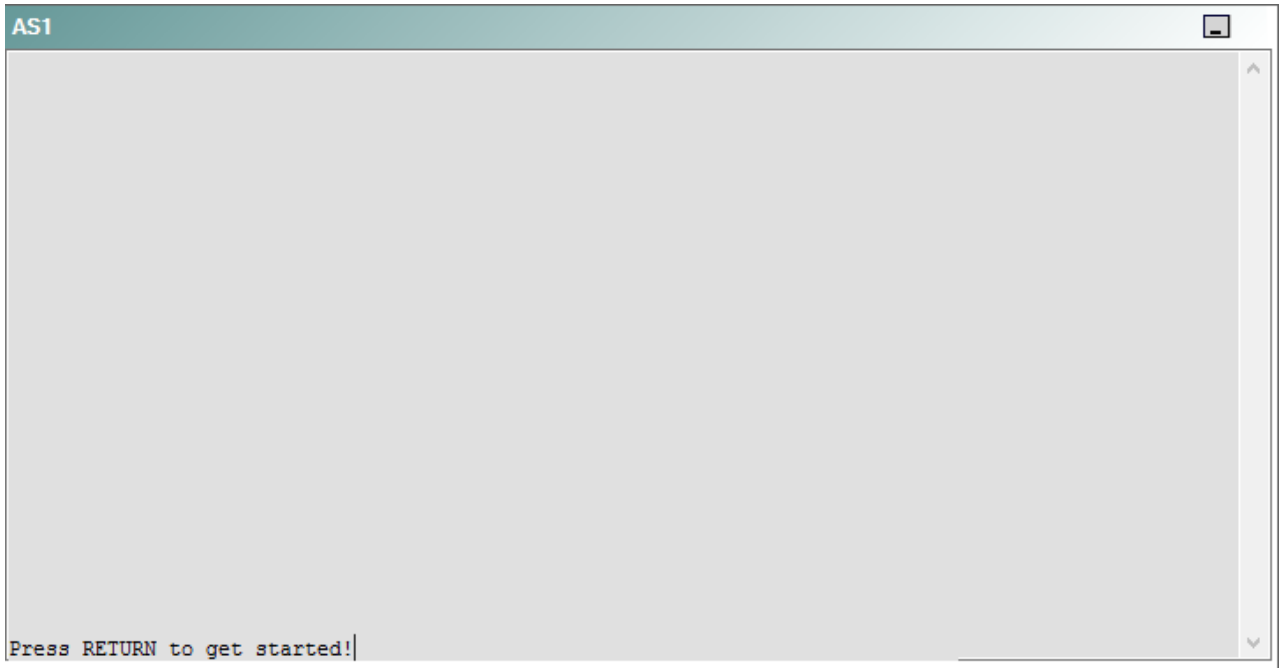

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 45**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

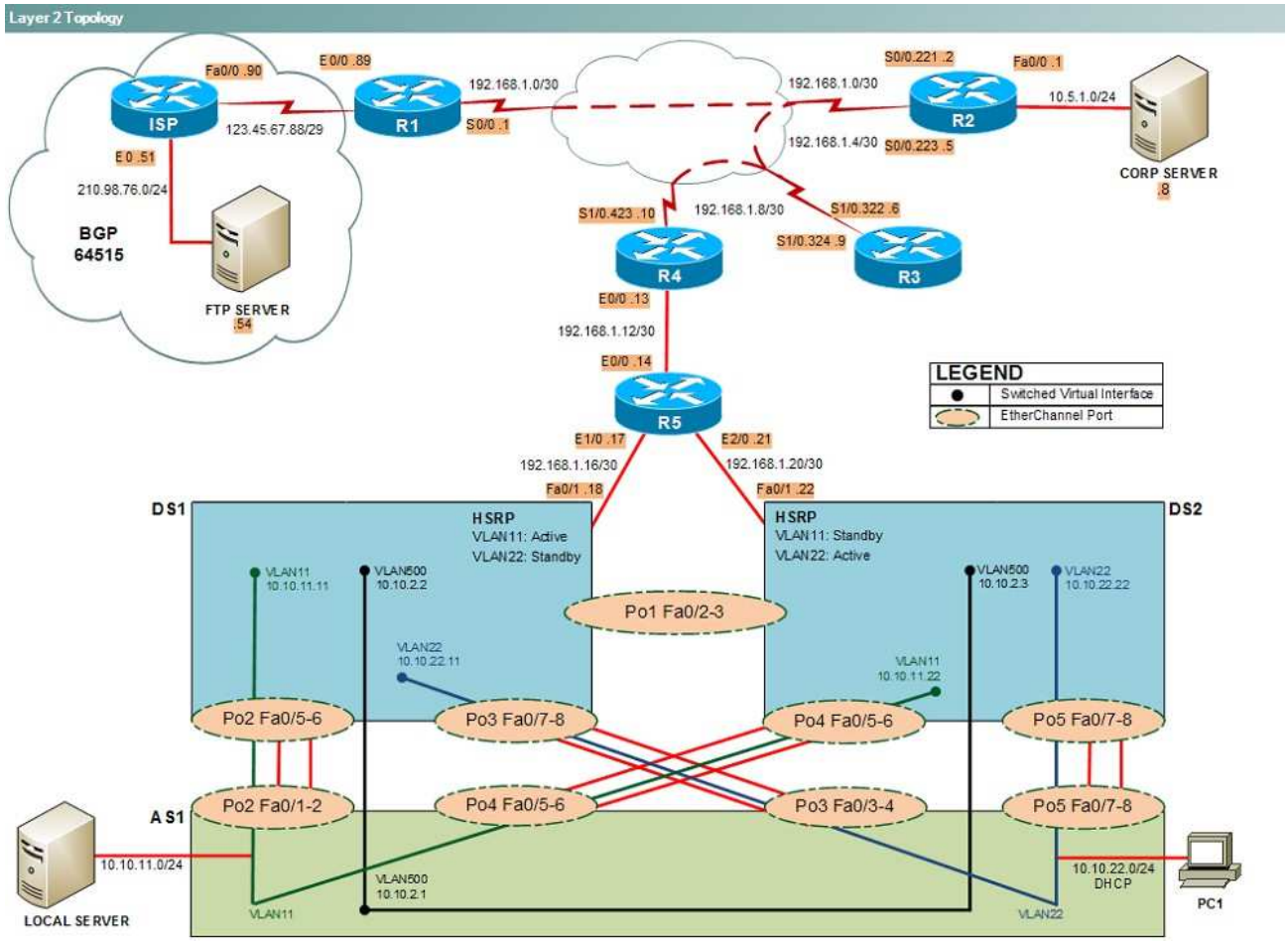
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

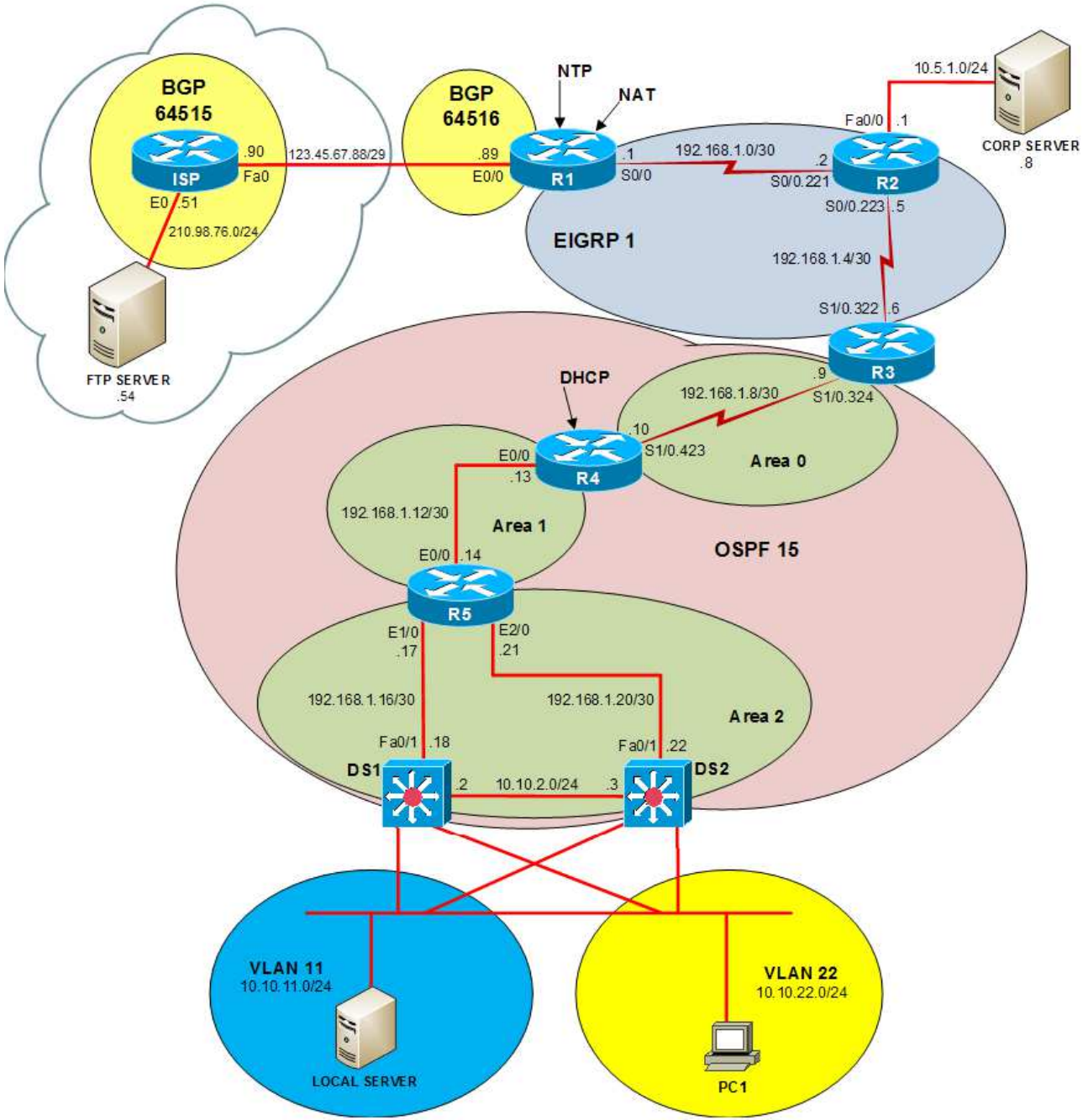
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

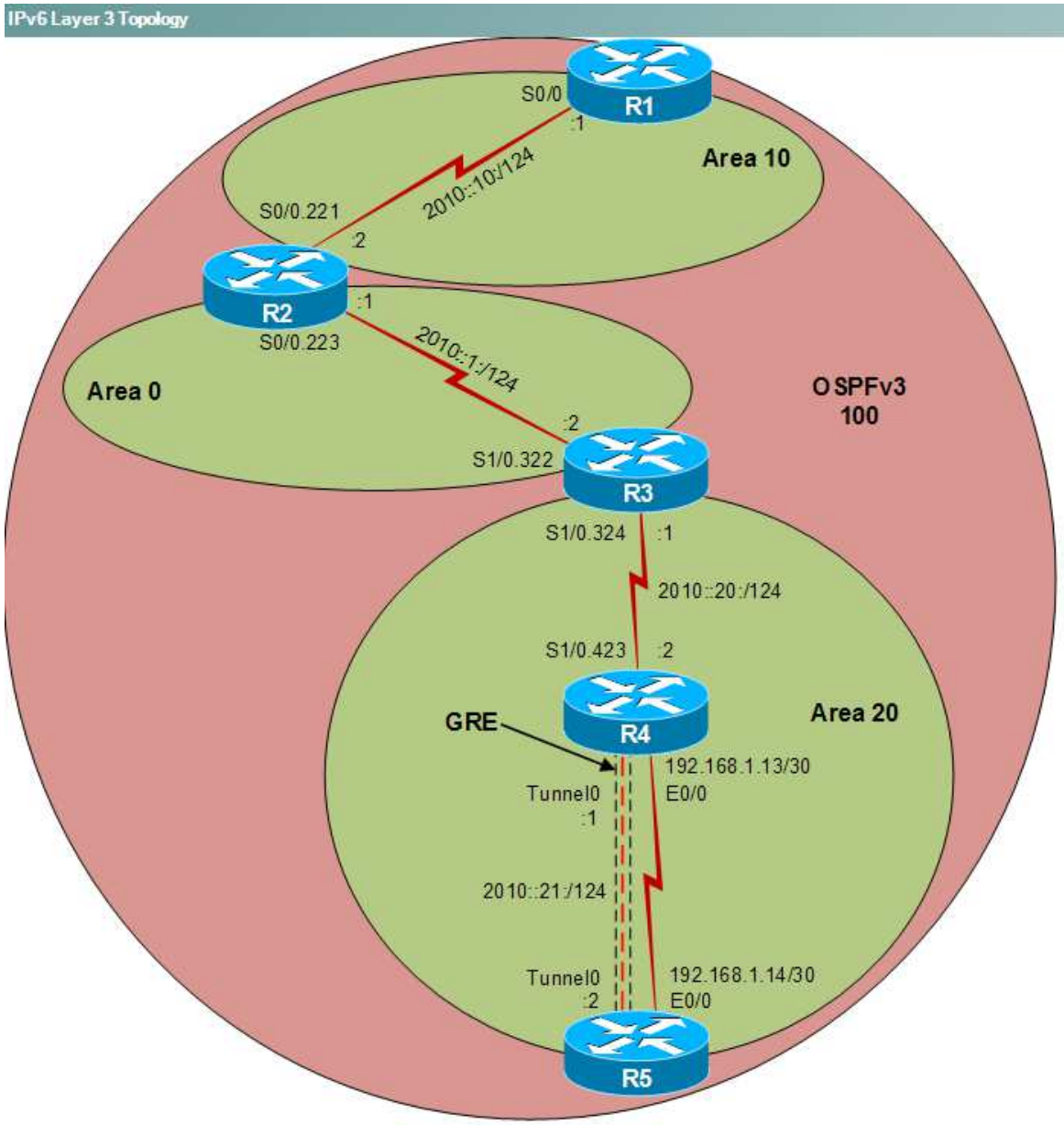
**Layer 2 Topology**




IPv4 layer 3 Topology

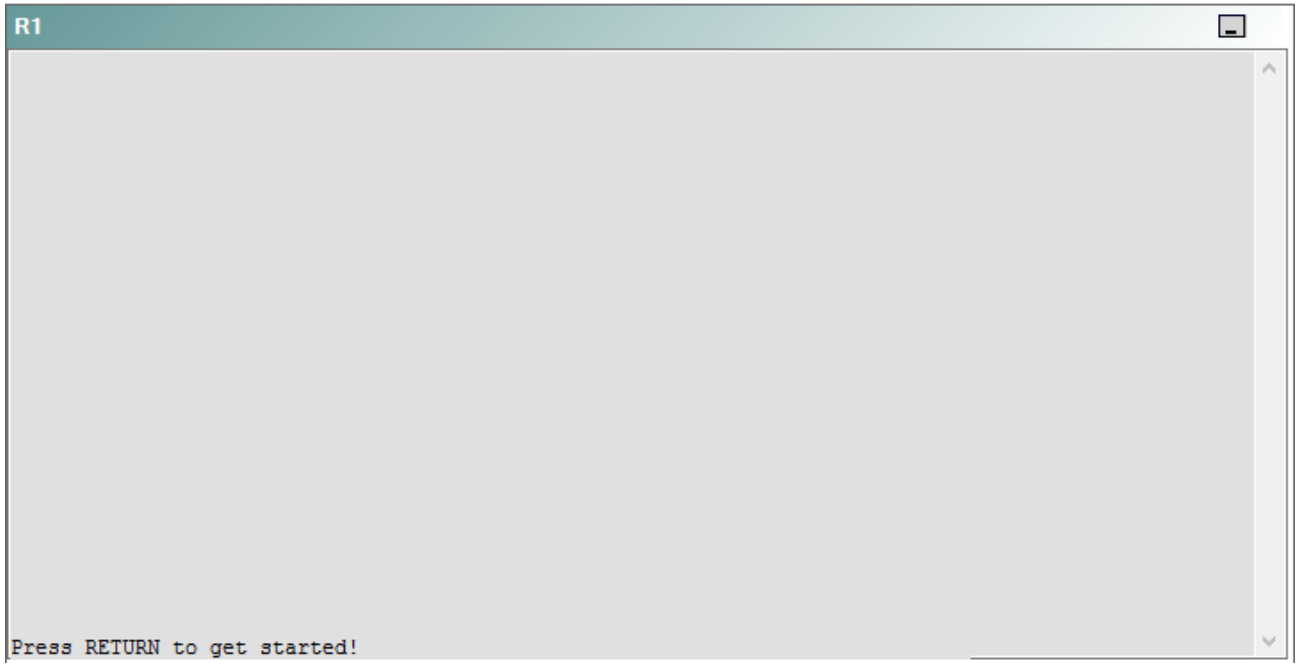

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

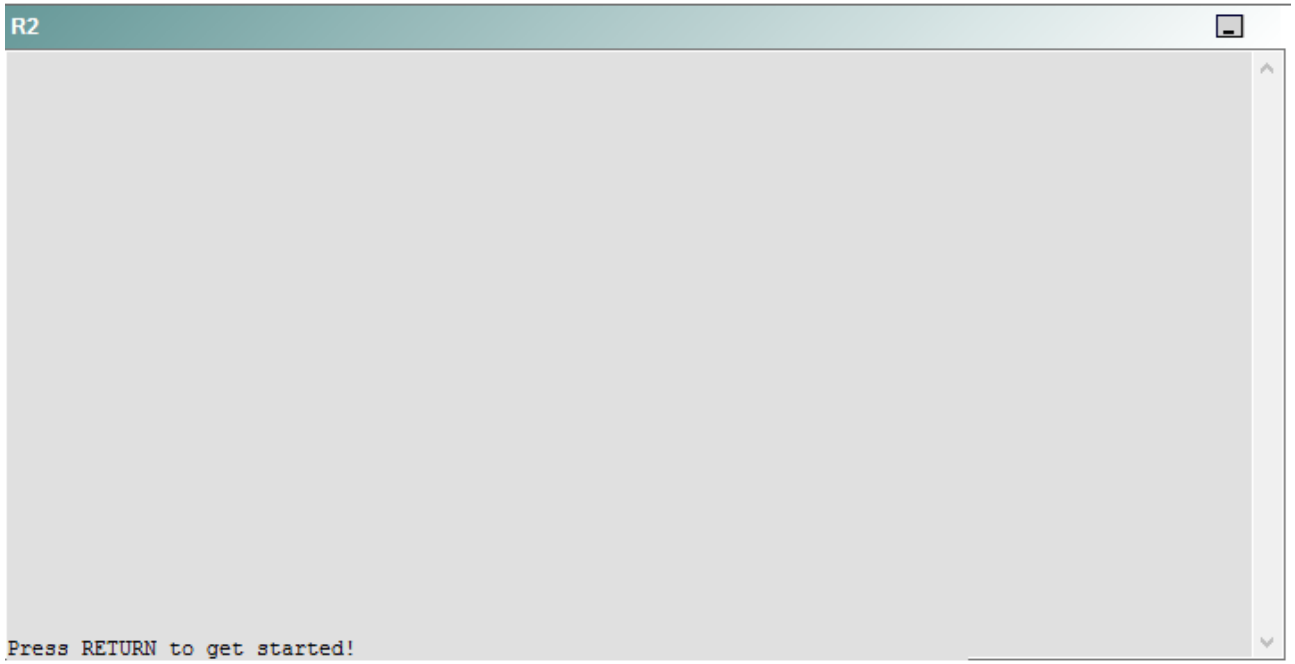



https://www.gratisexam.com/

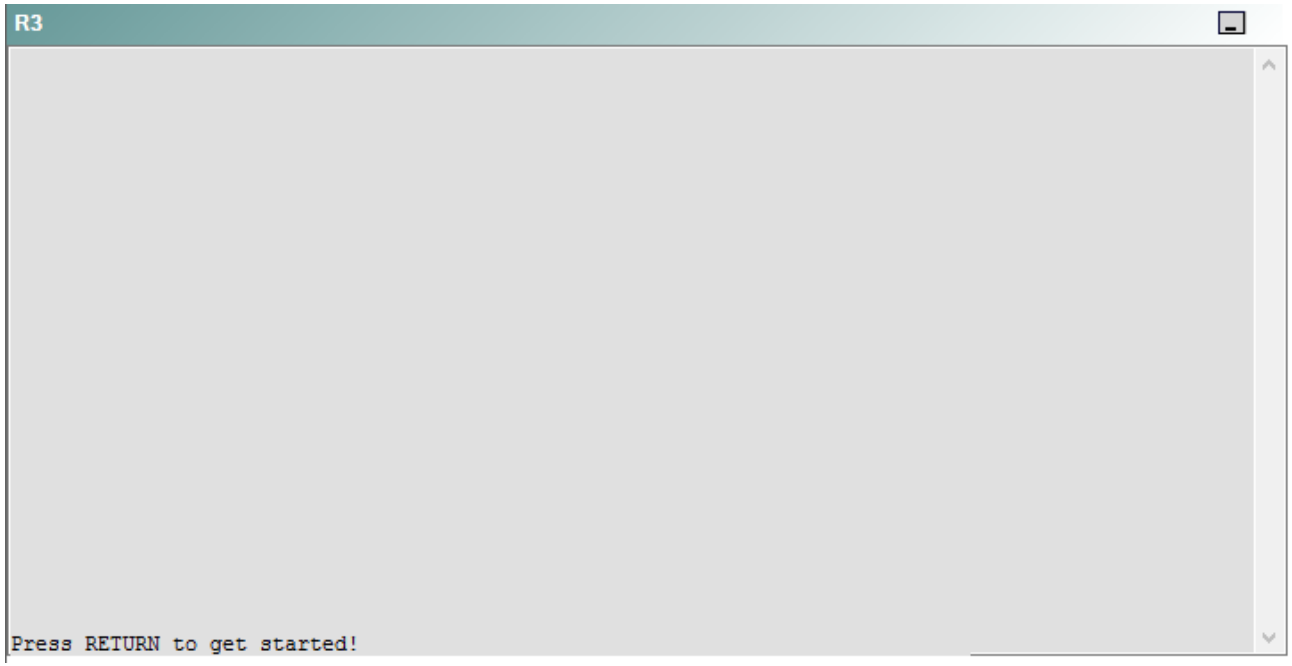
R1



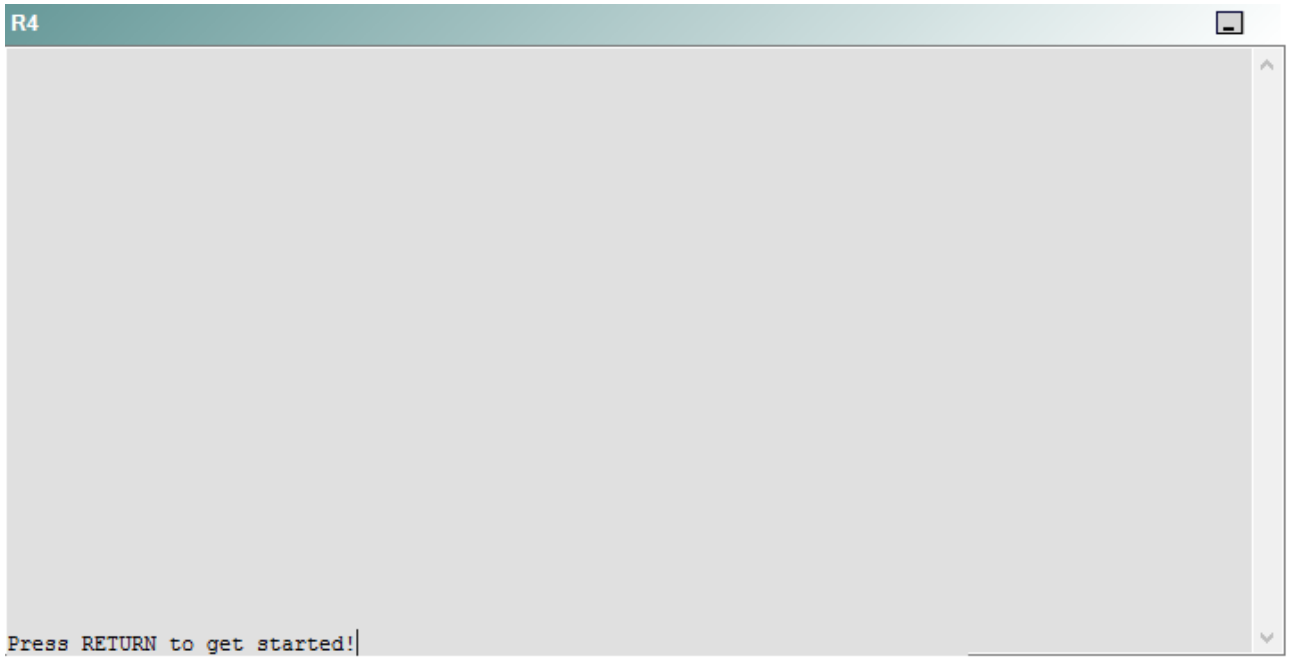

R2



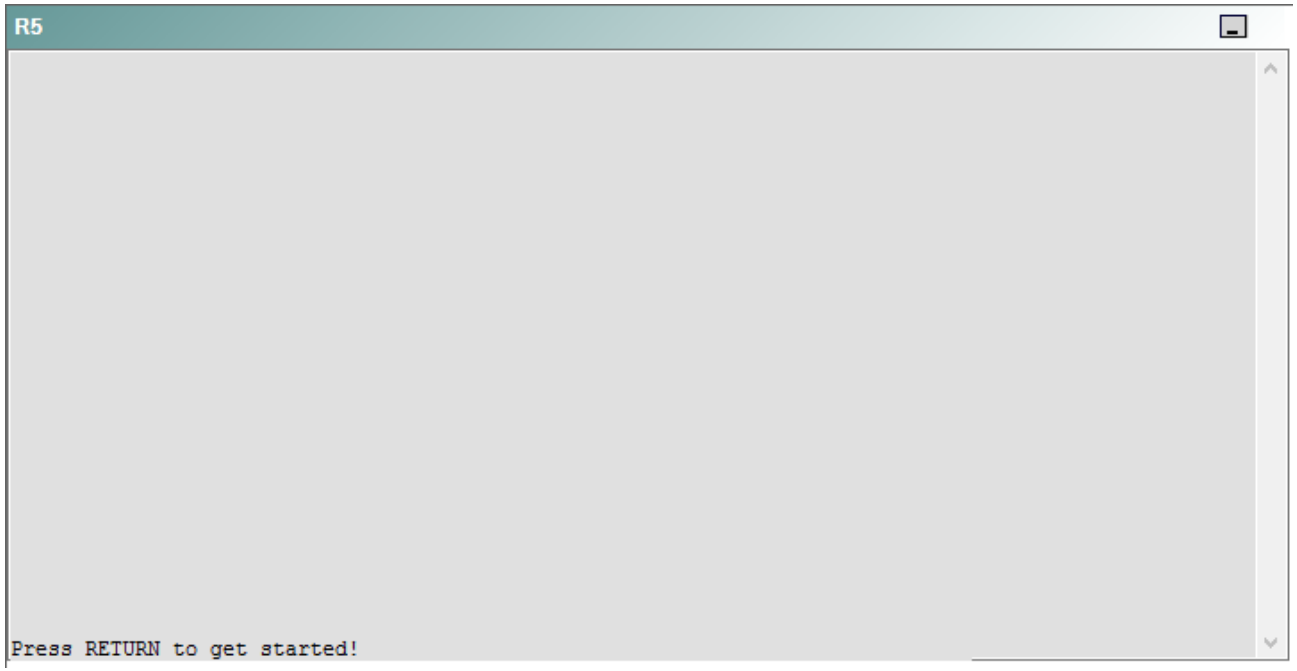

R3



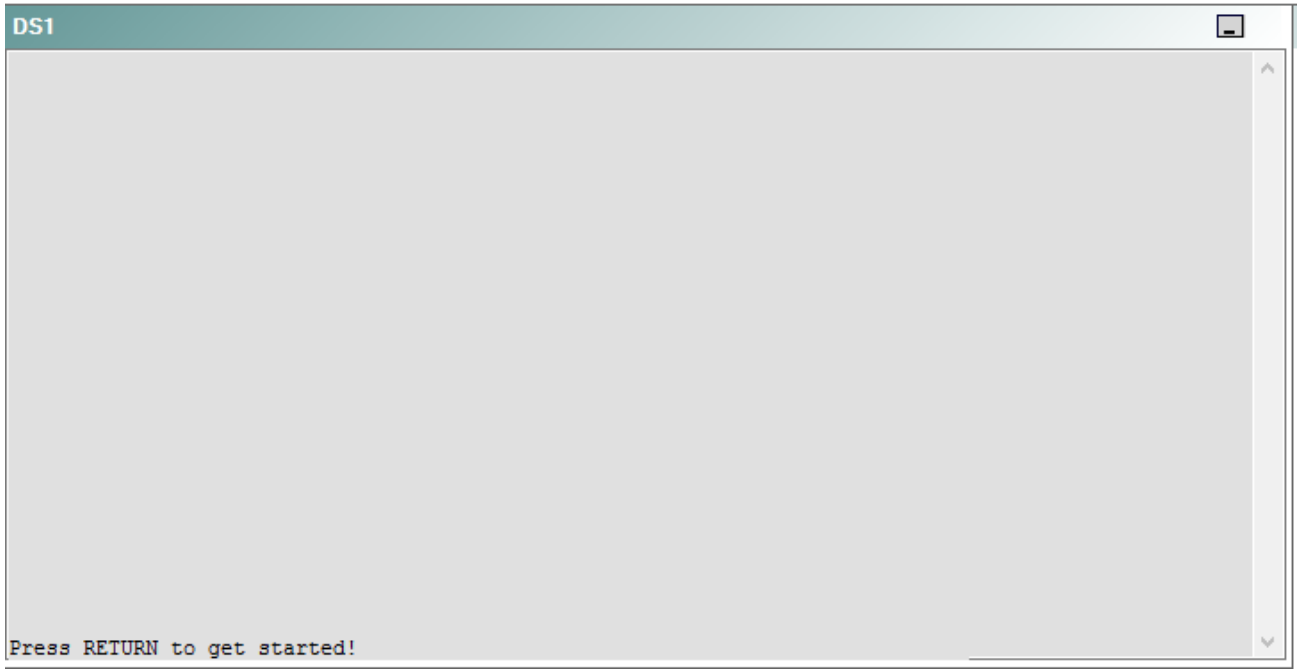

R4



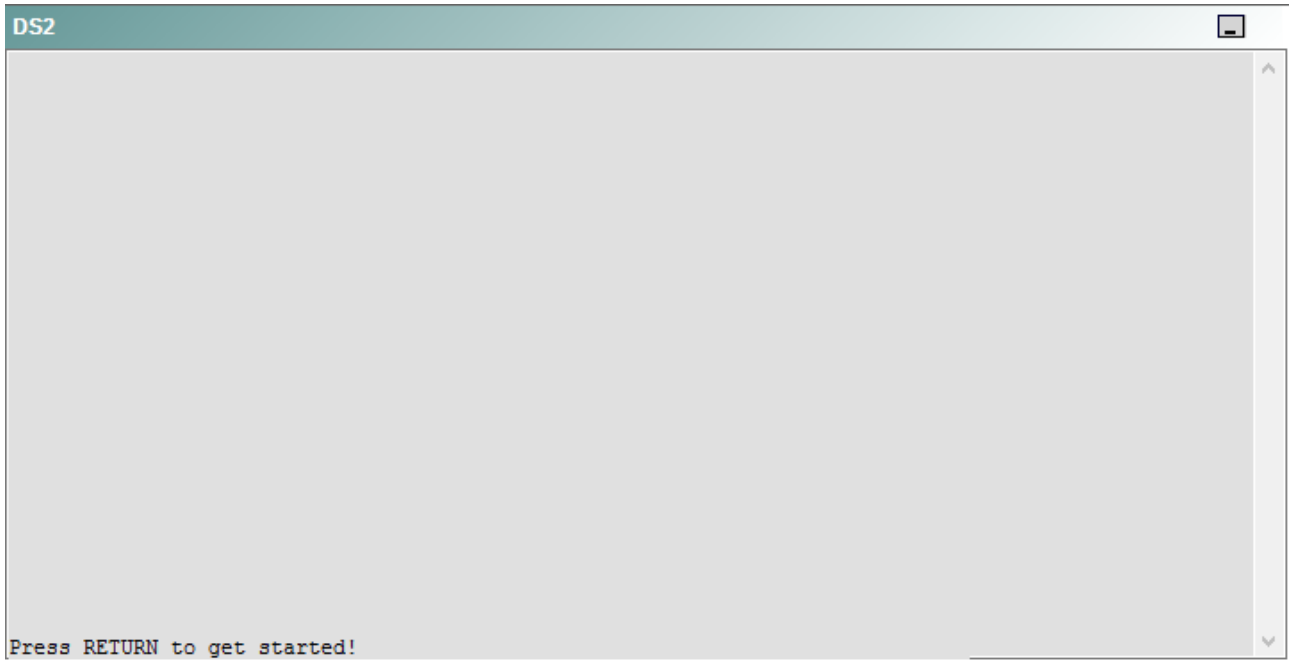

R5



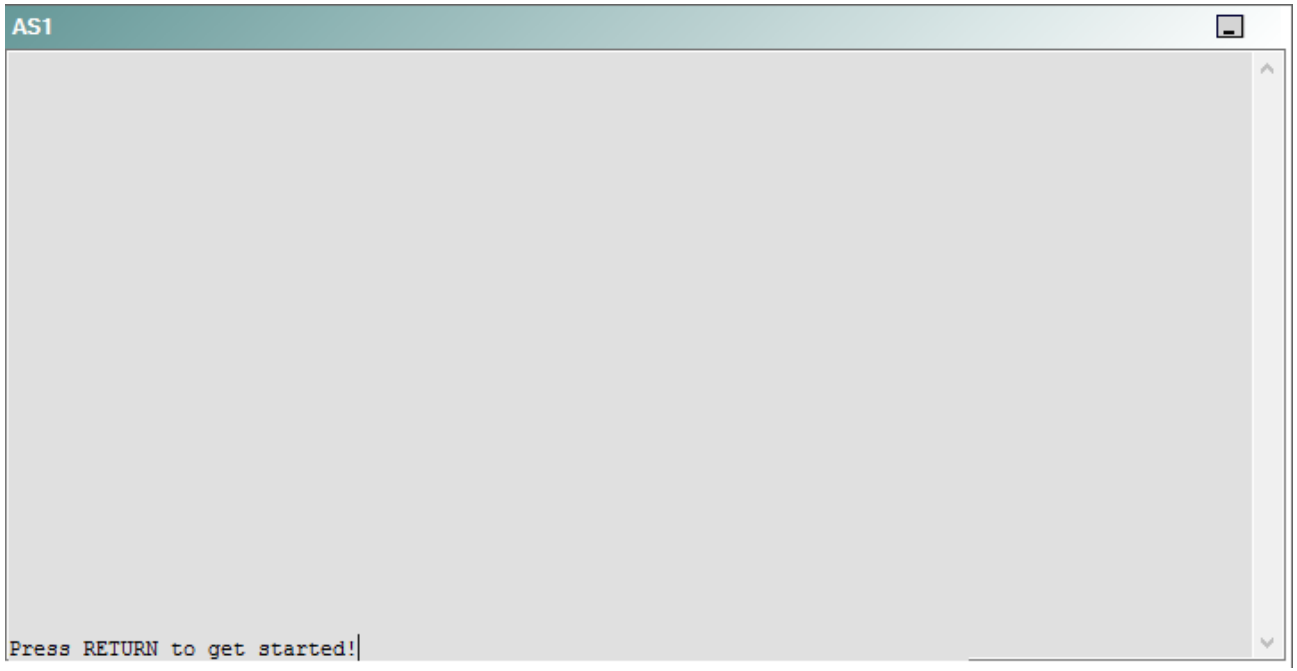

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. NAT
C. BGP
D. OSPFv3
E. EIGRP
F. redistribution
G. Layer 3 security
H. Layer 3 addressing
I. interface

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 46**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

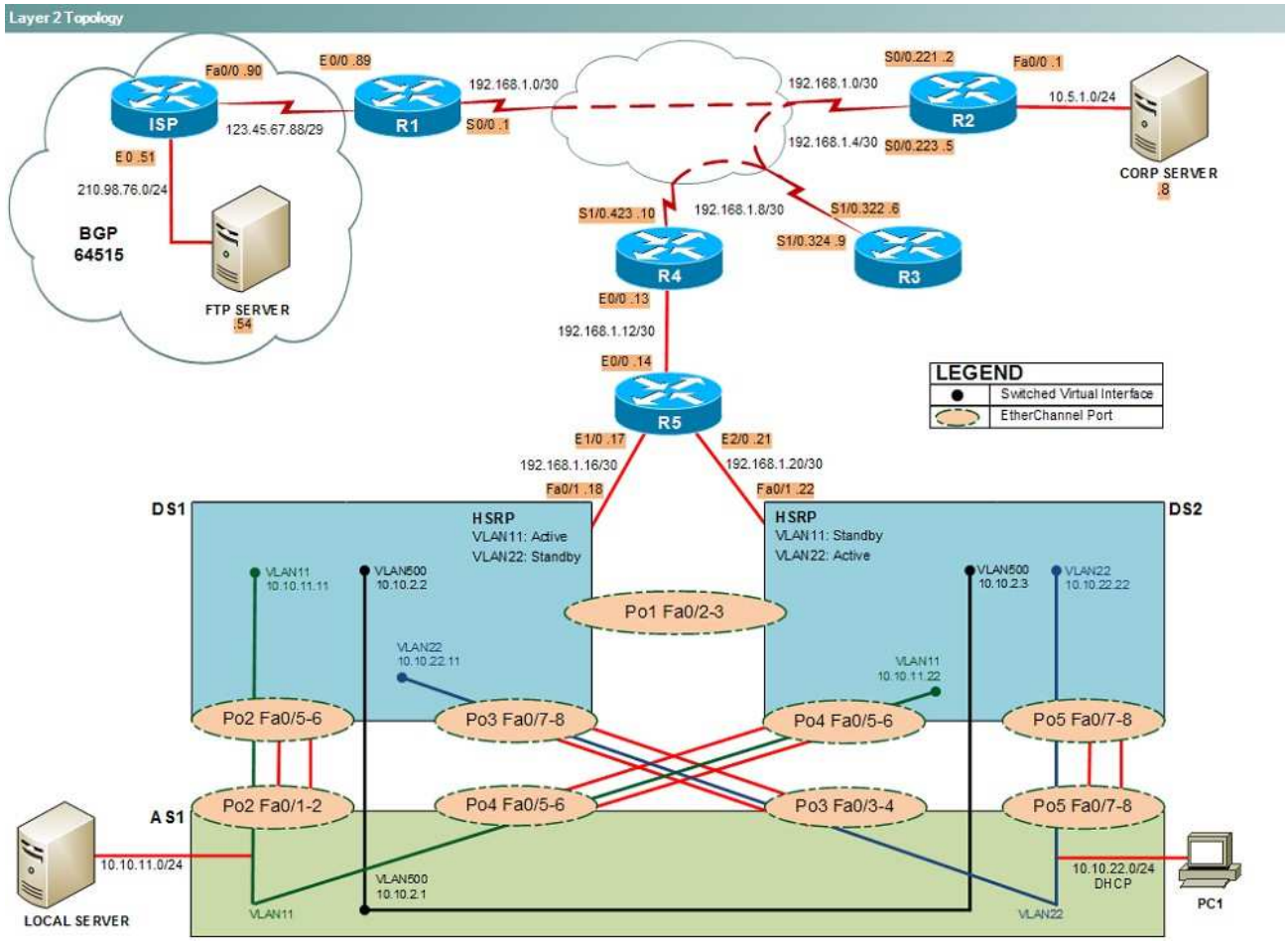
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

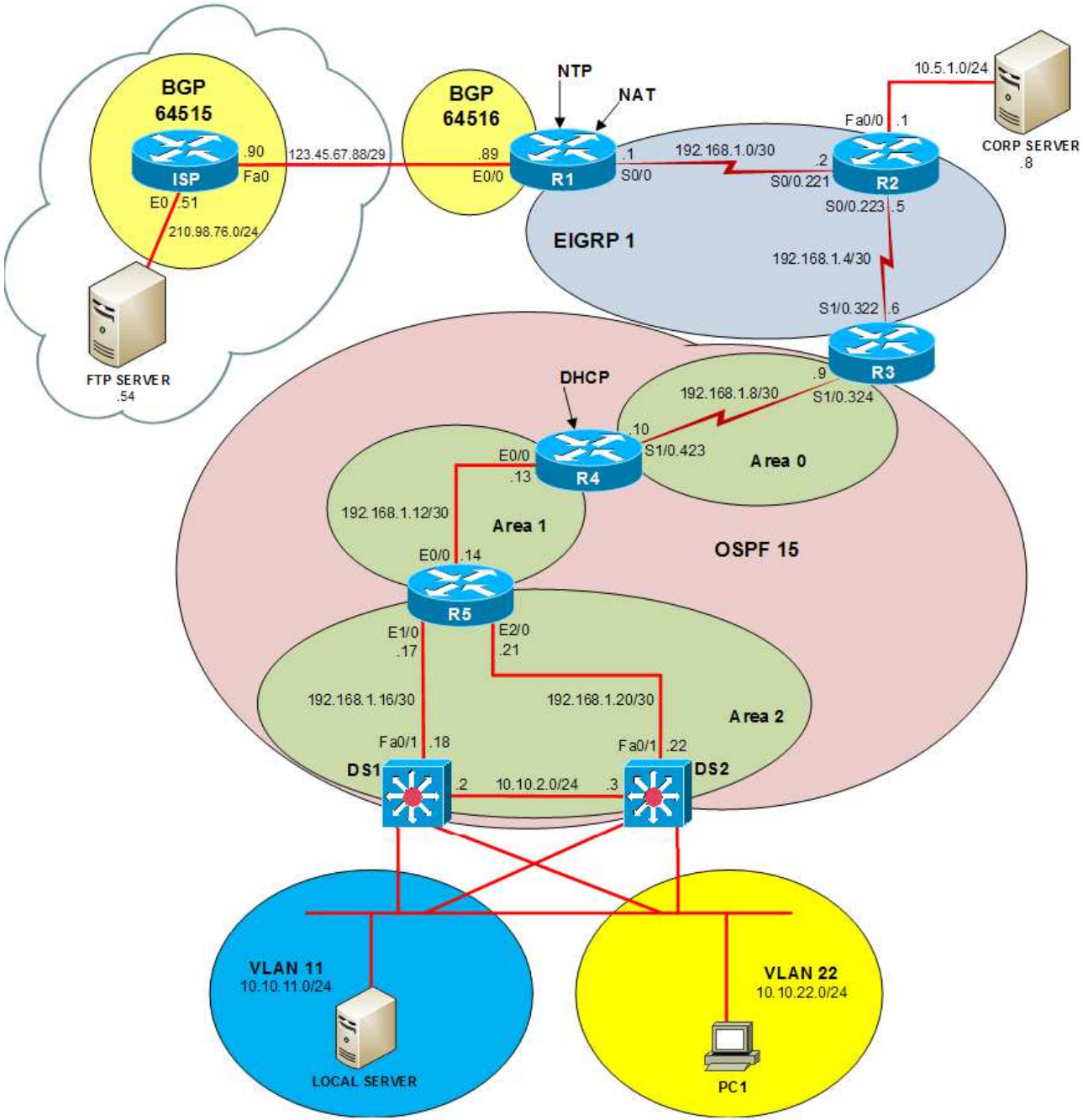
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

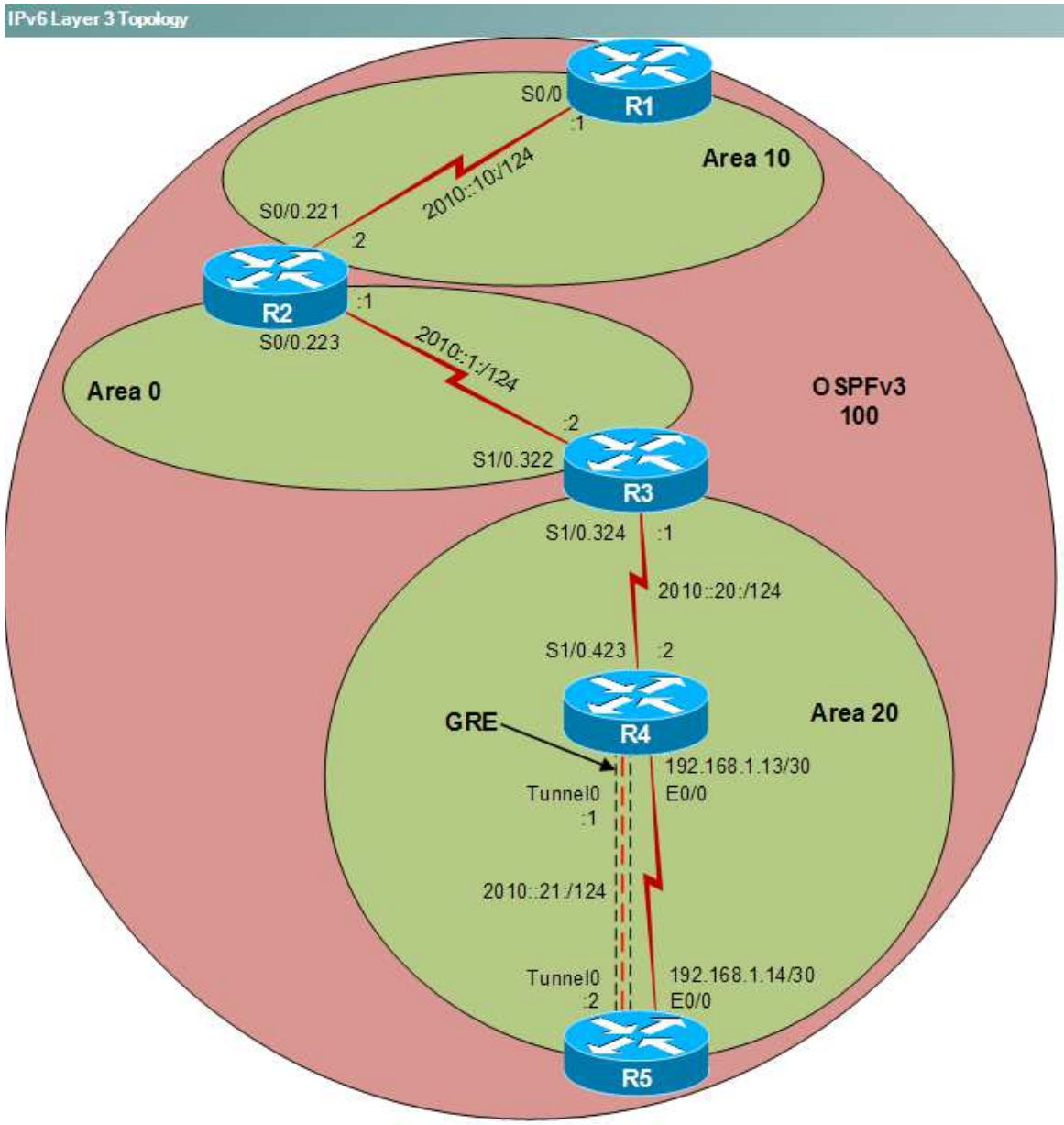
**Layer 2 Topology**




IPv4 layer 3 Topology

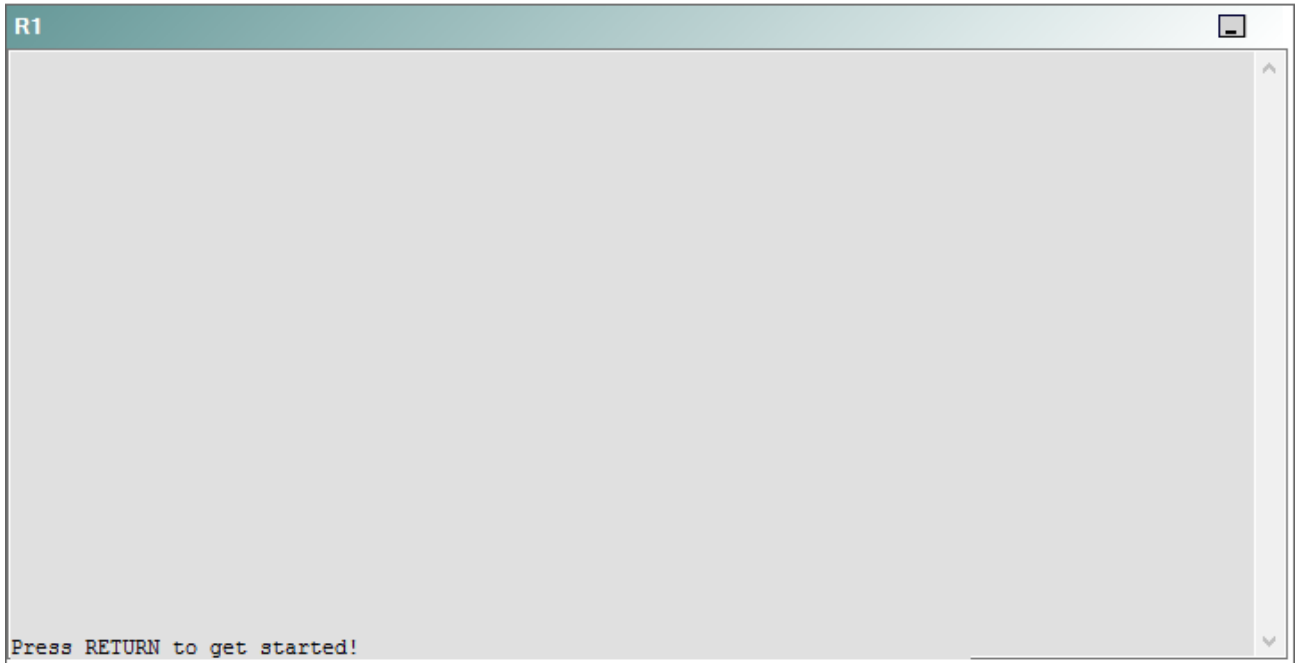

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

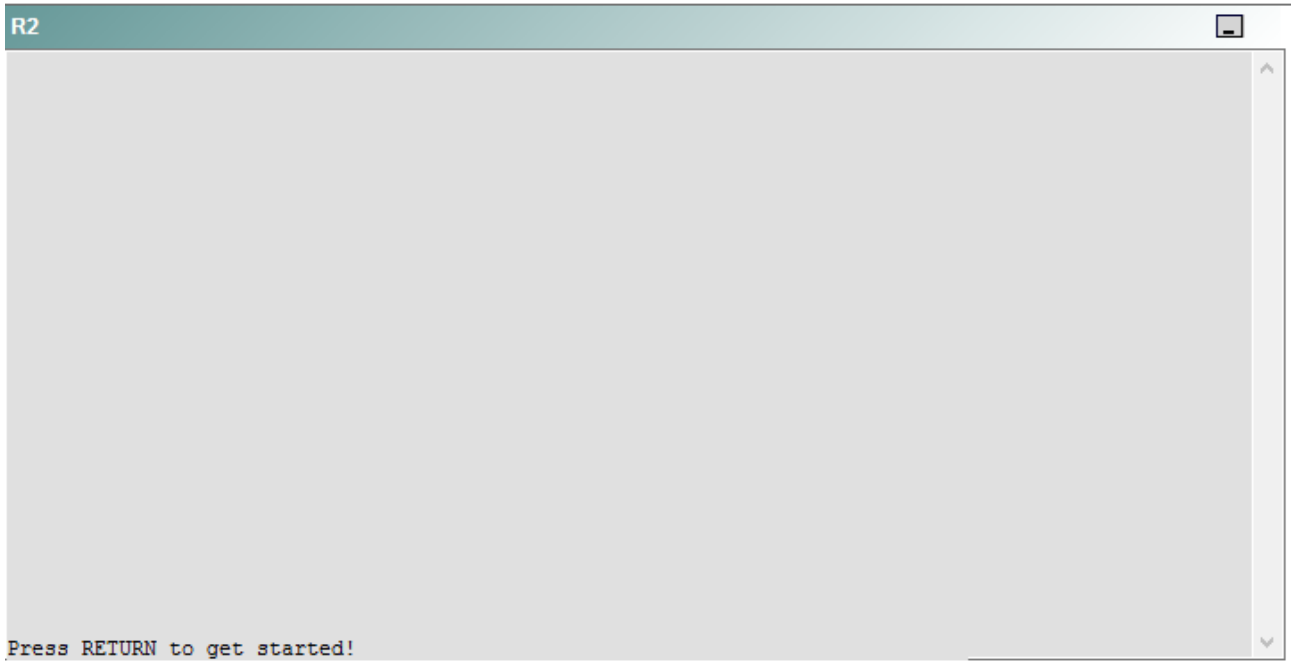



https://www.gratisexam.com/

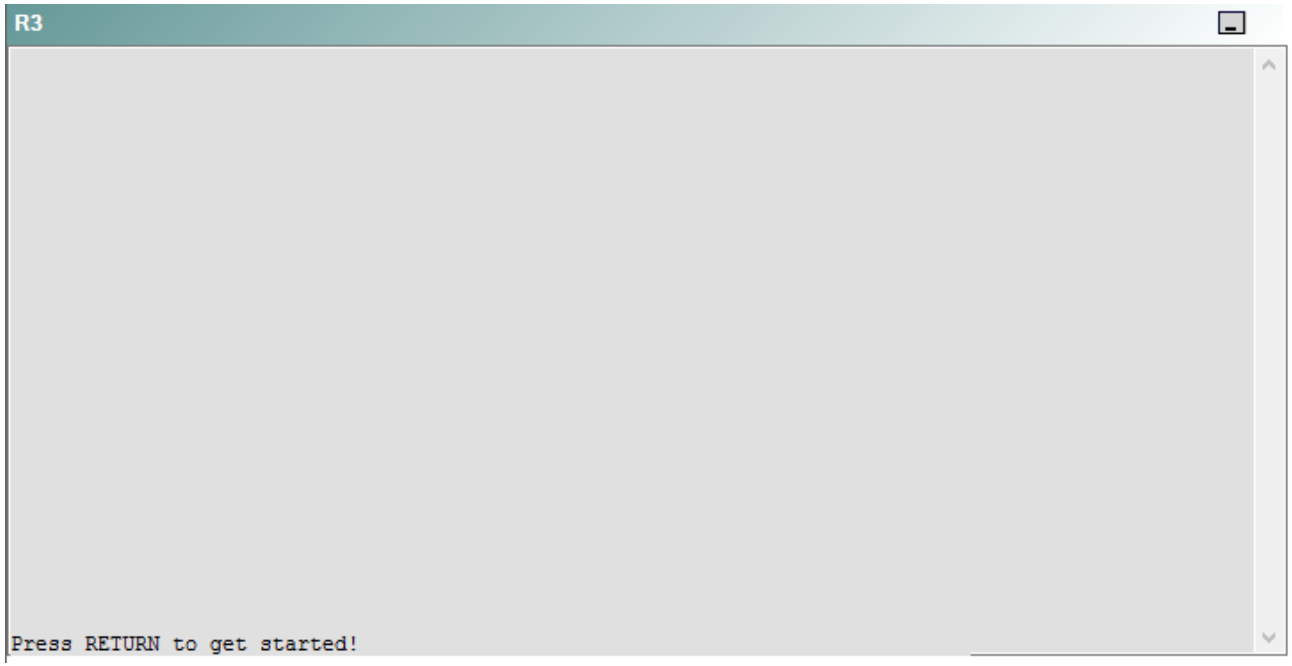
R1



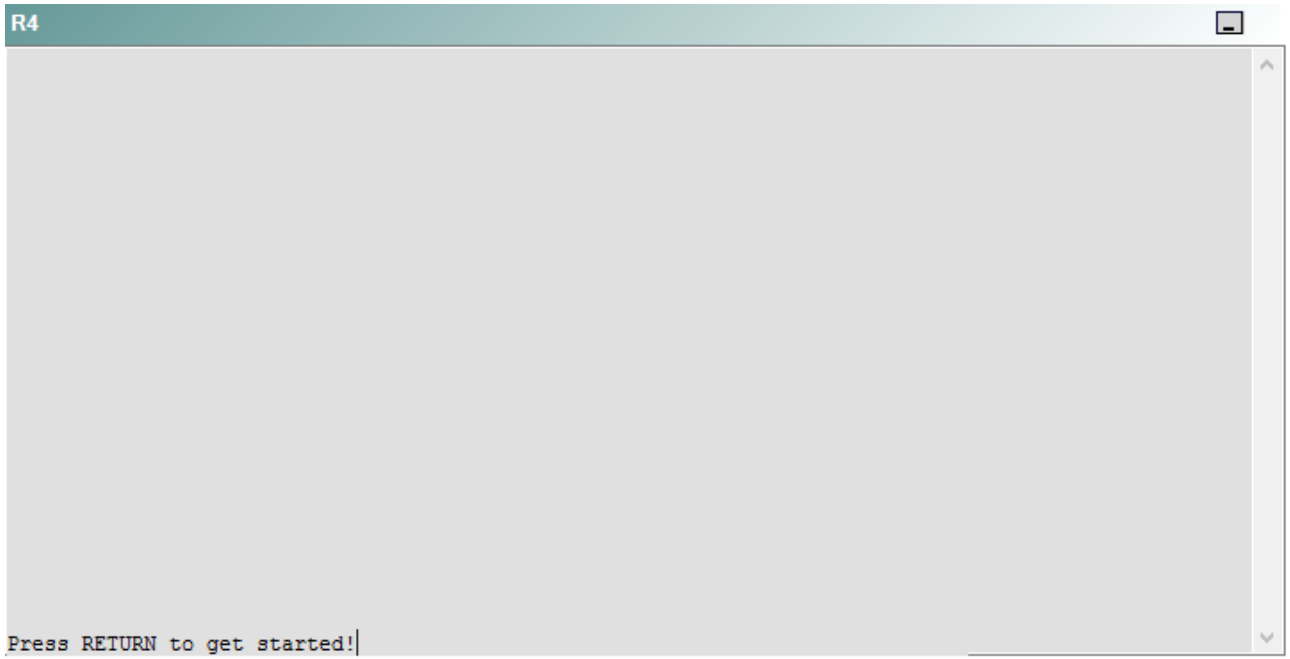

R2



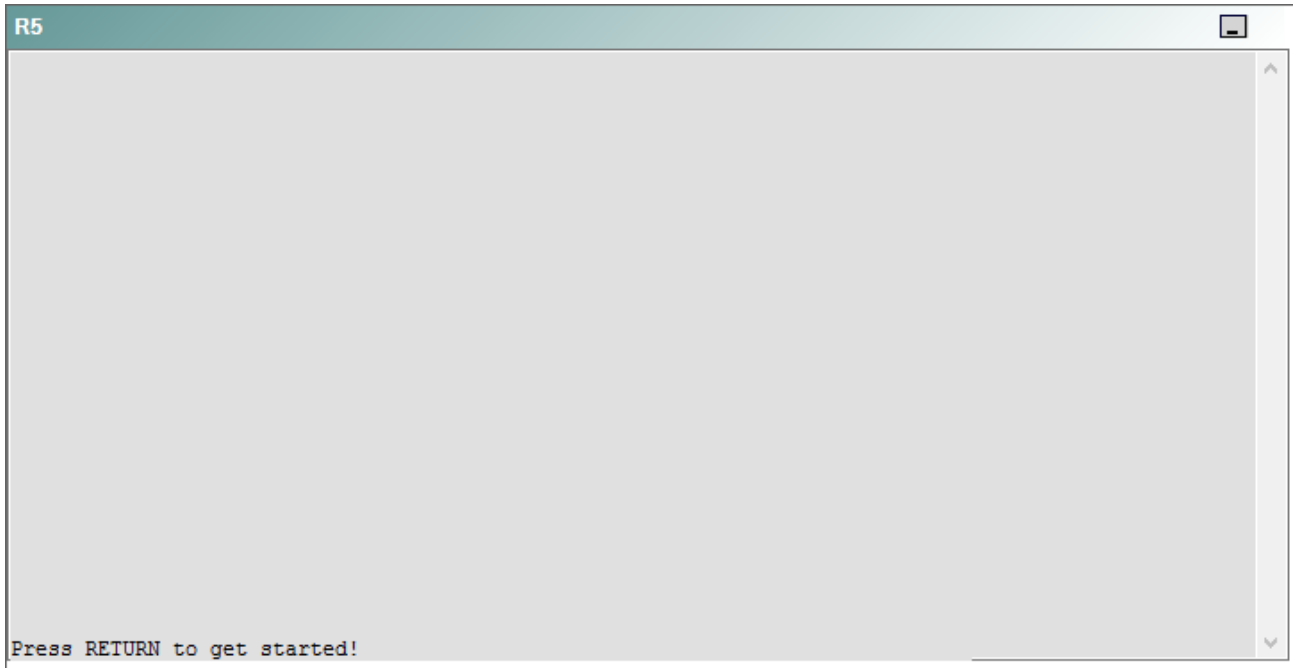

R3



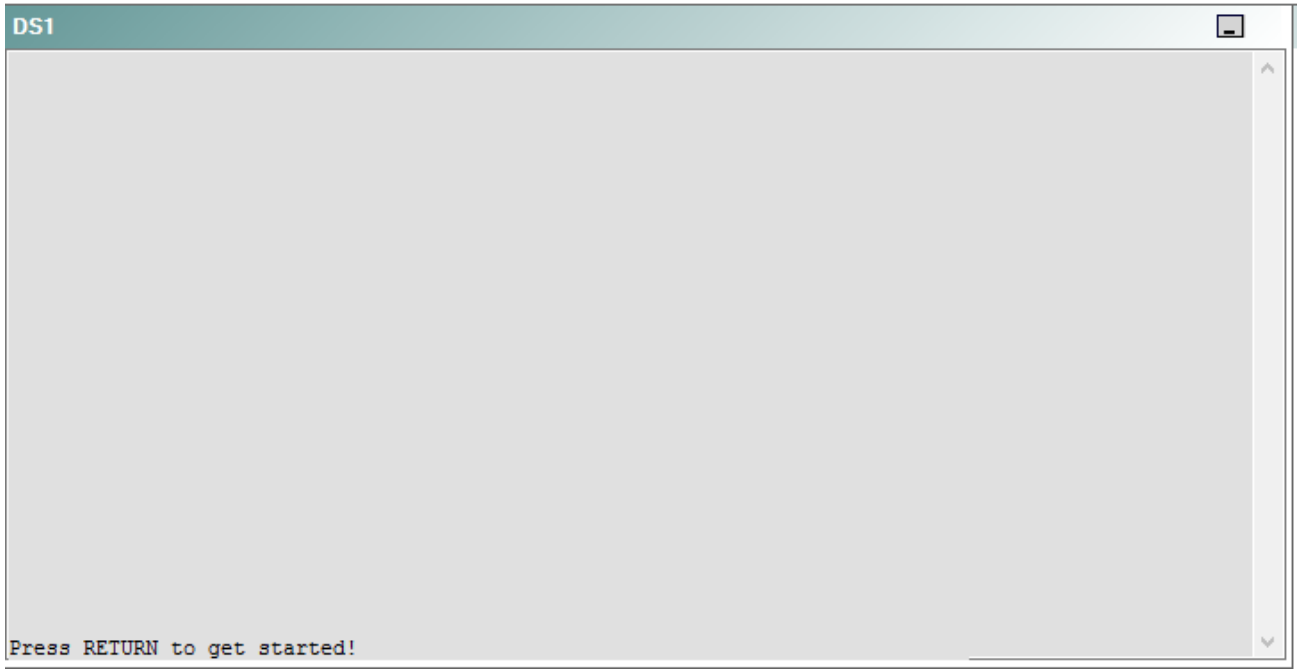

R4



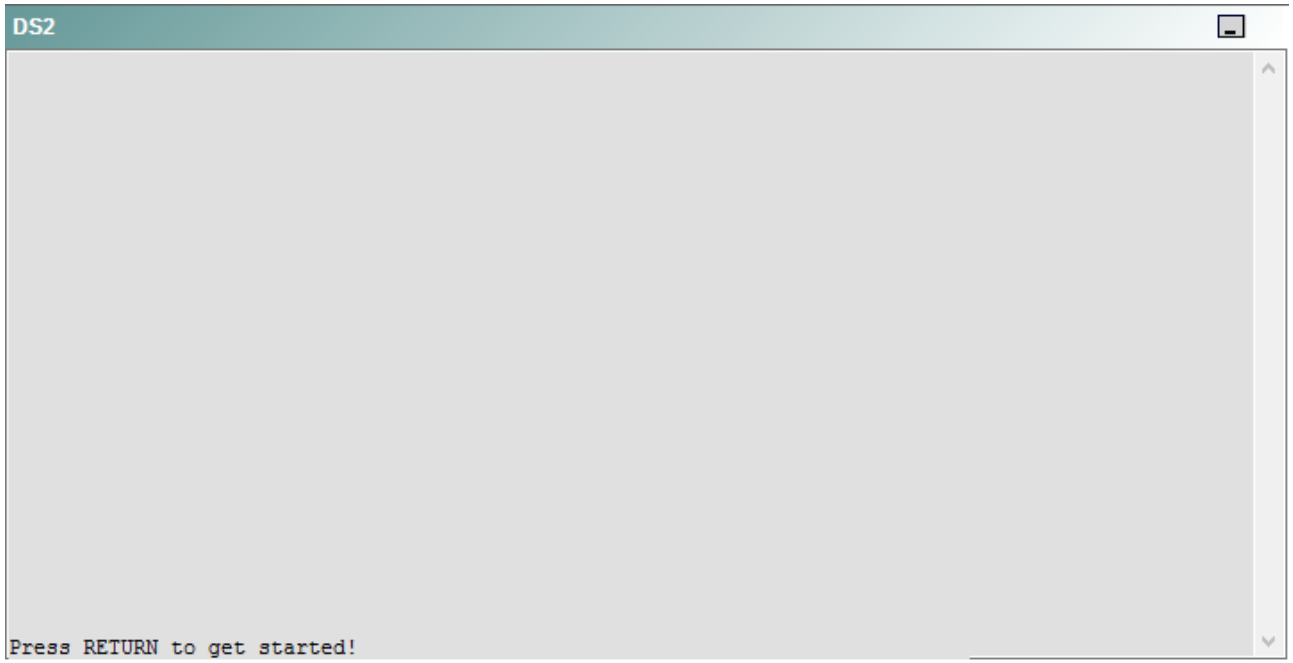

R5



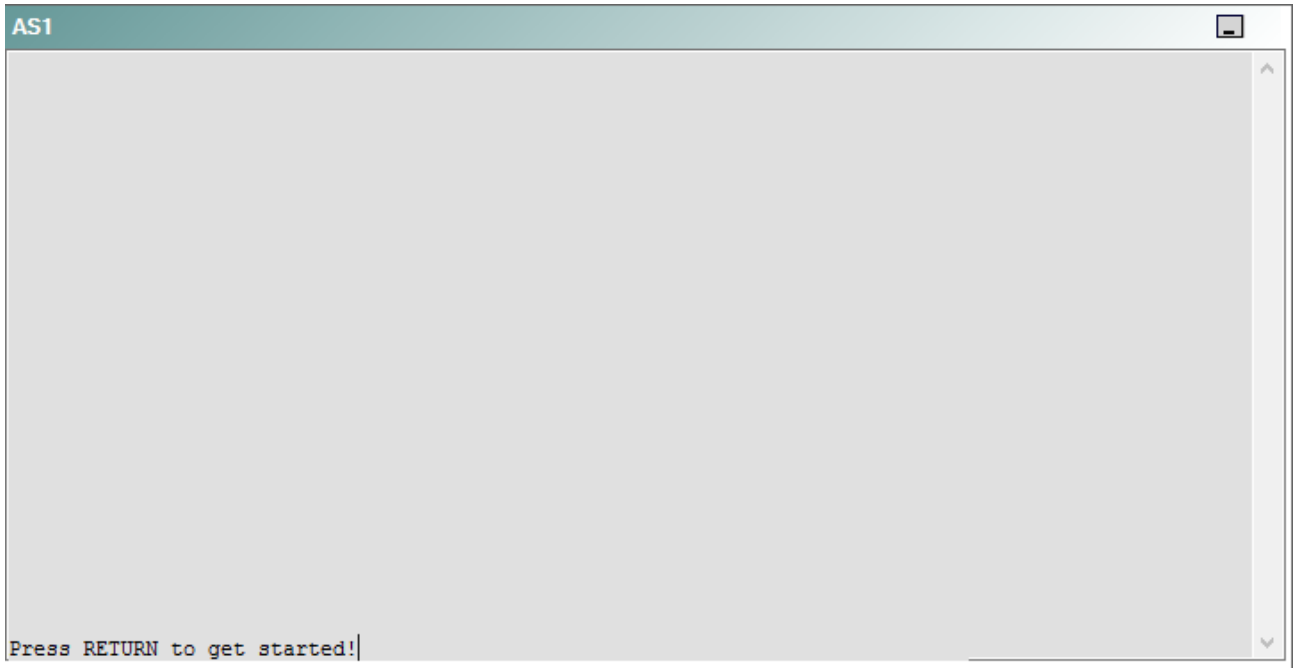

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 47**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

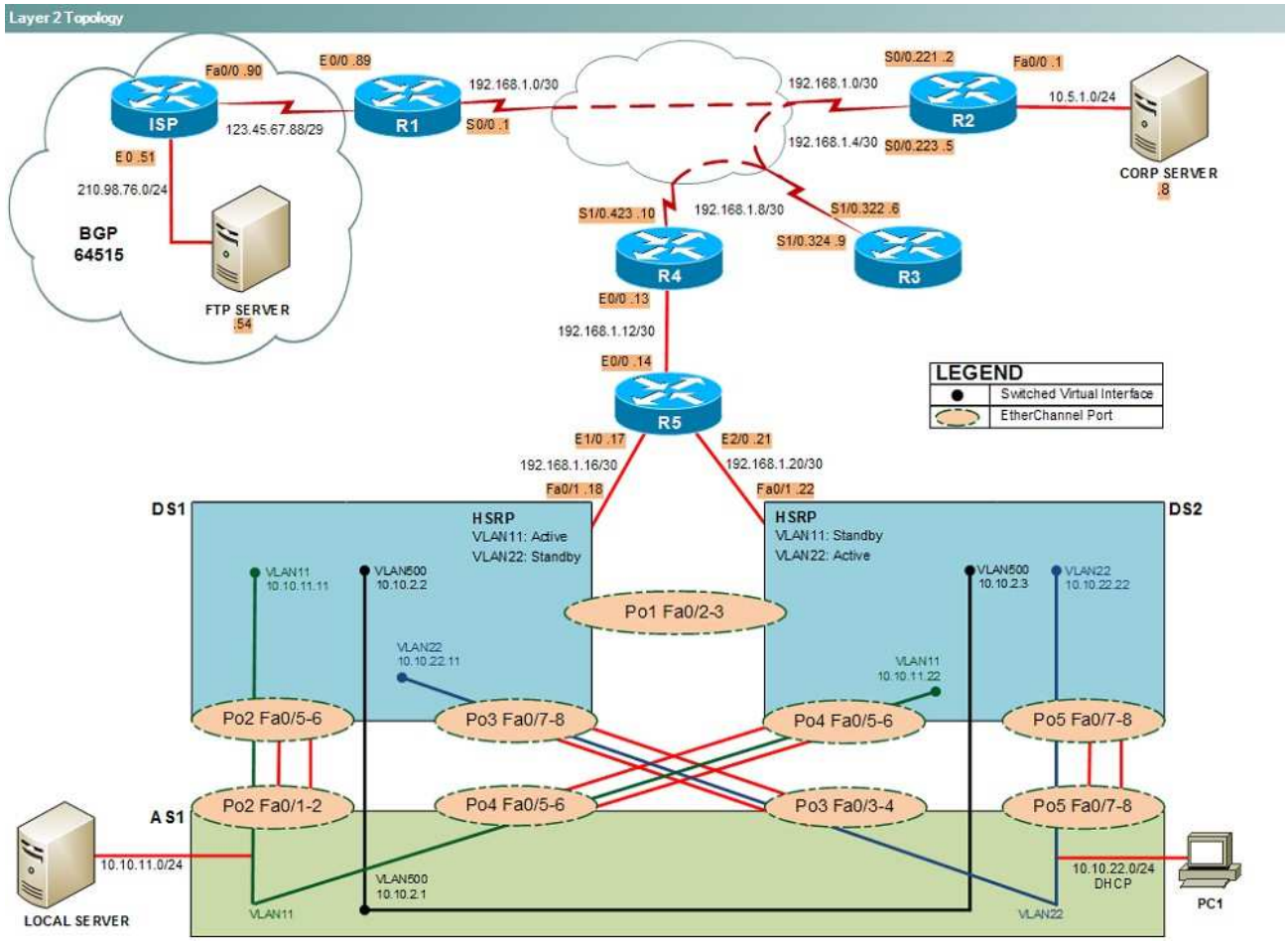
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

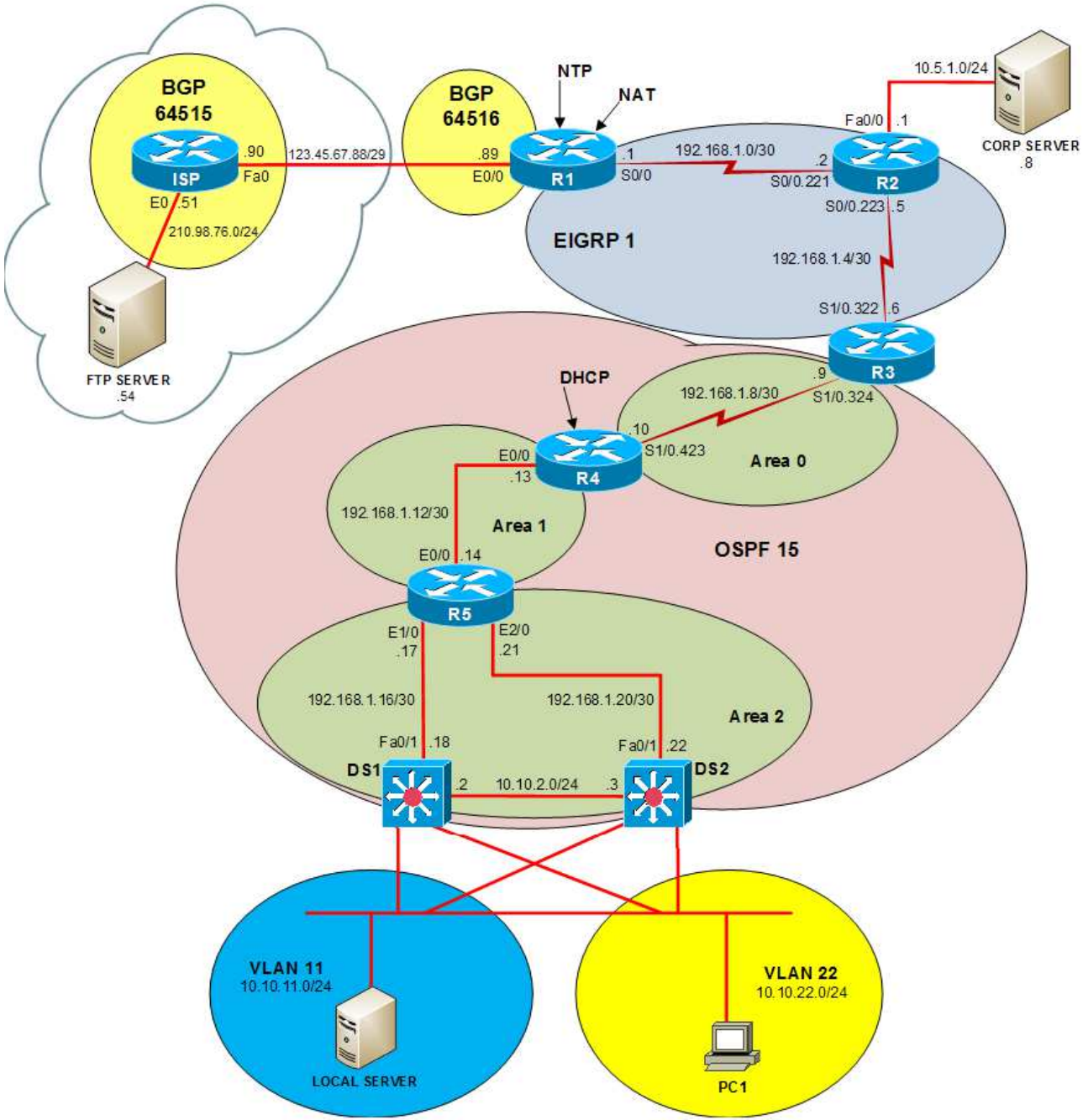
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

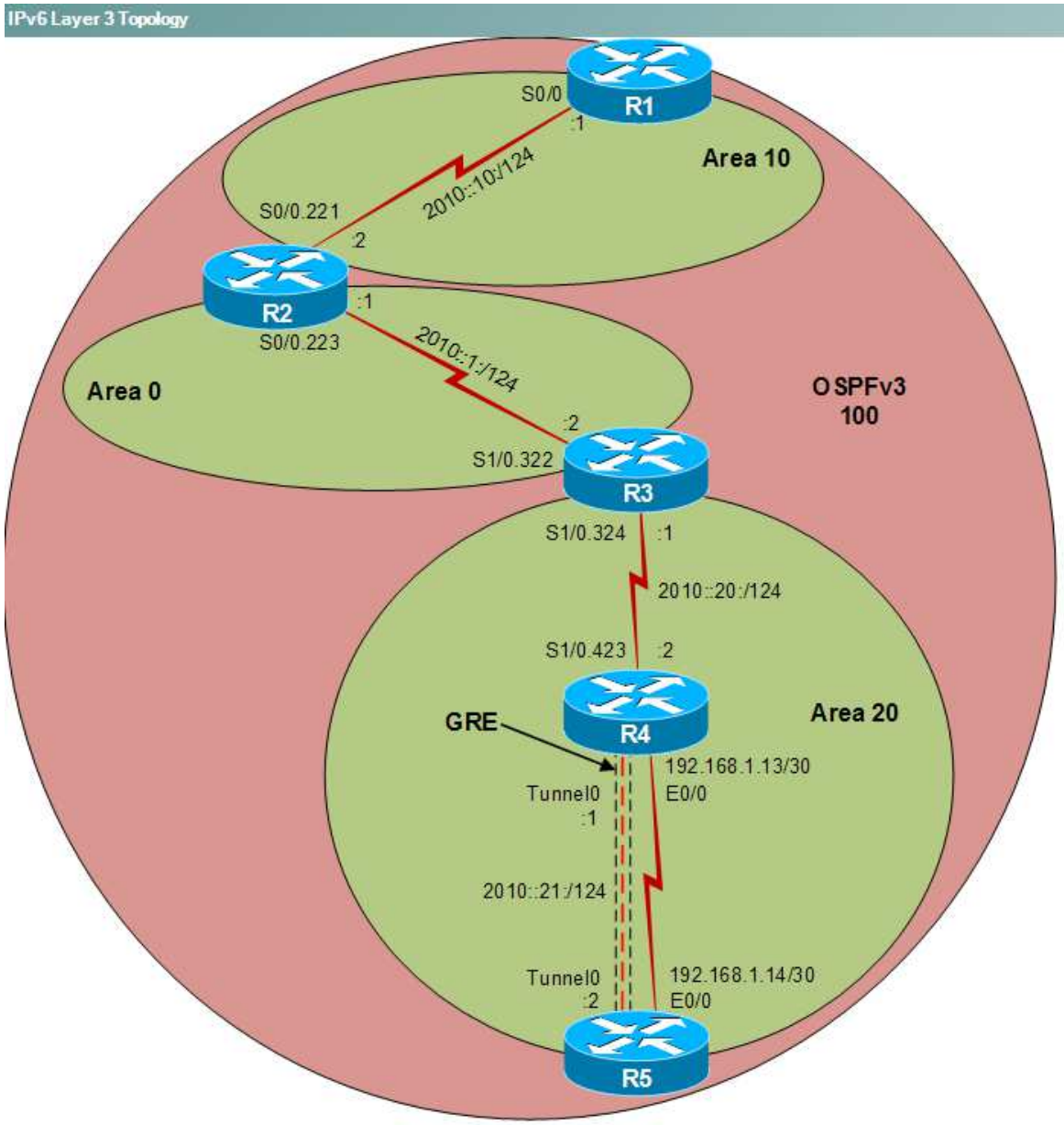
**Layer 2 Topology**




IPv4 layer 3 Topology

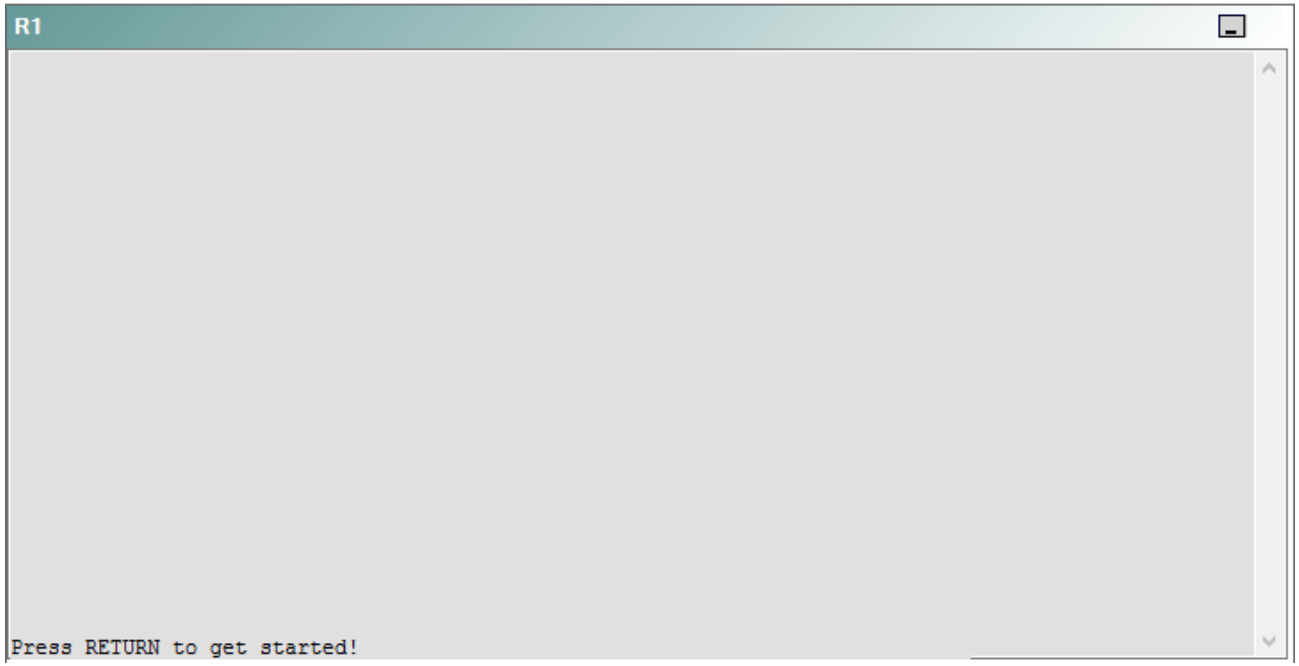

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

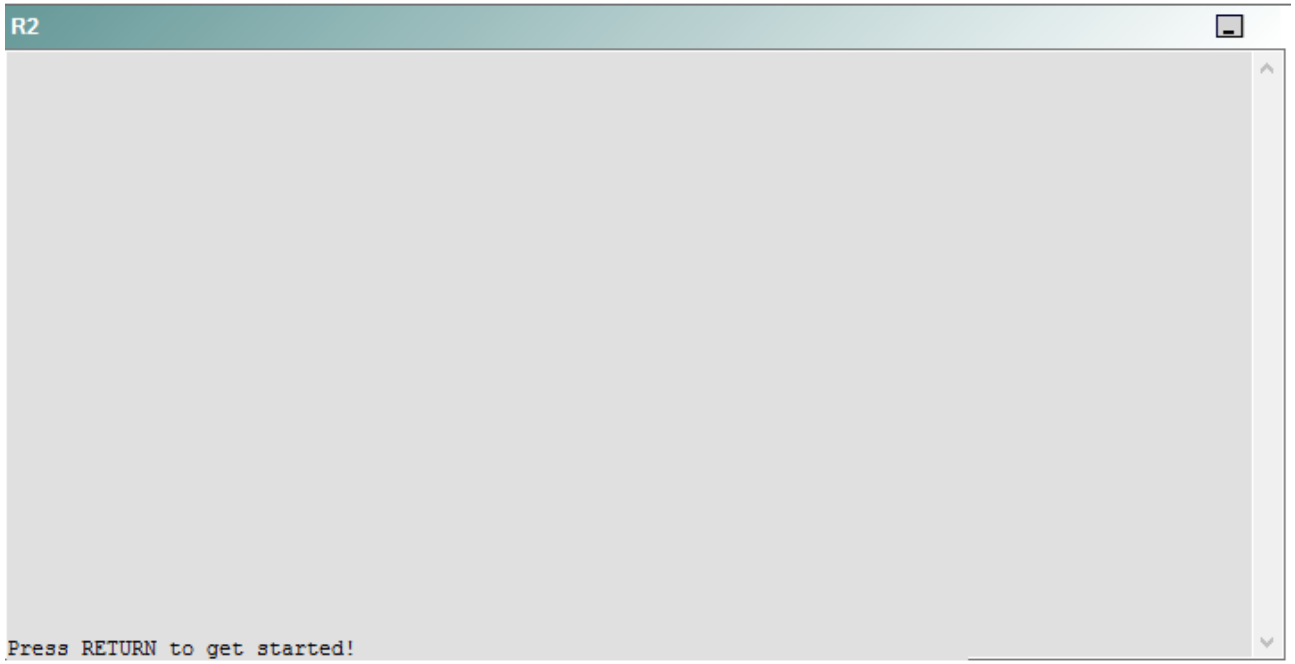



https://www.gratisexam.com/

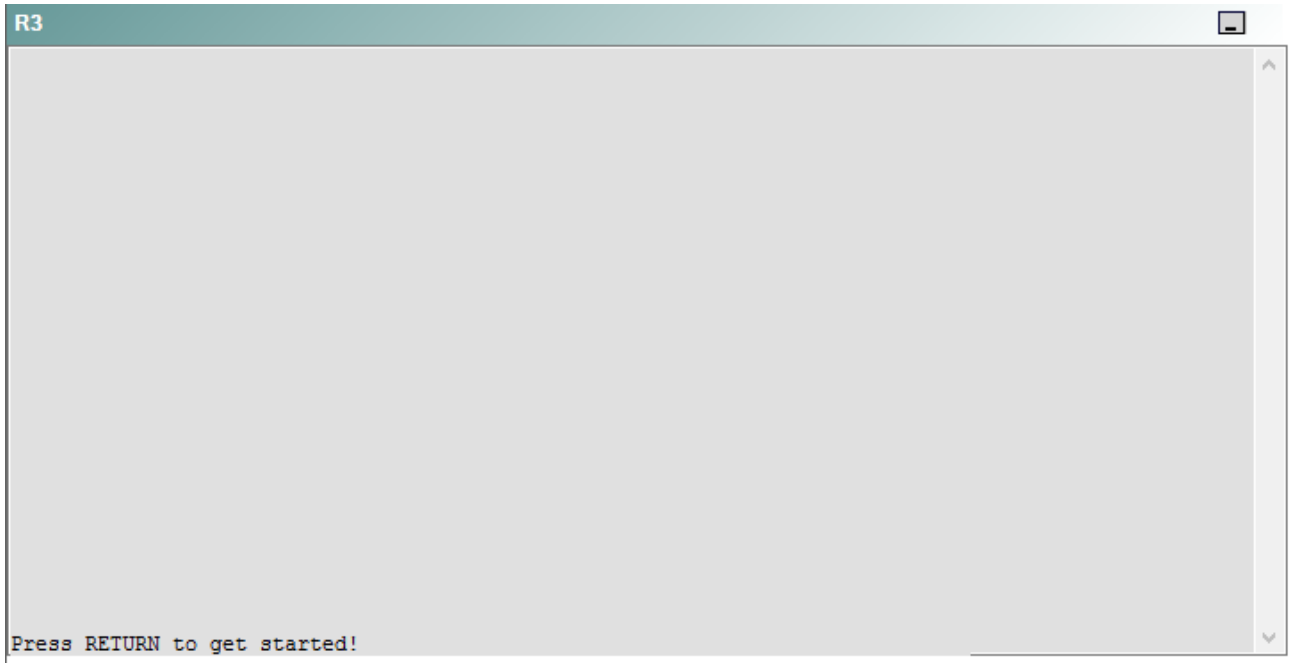
R1



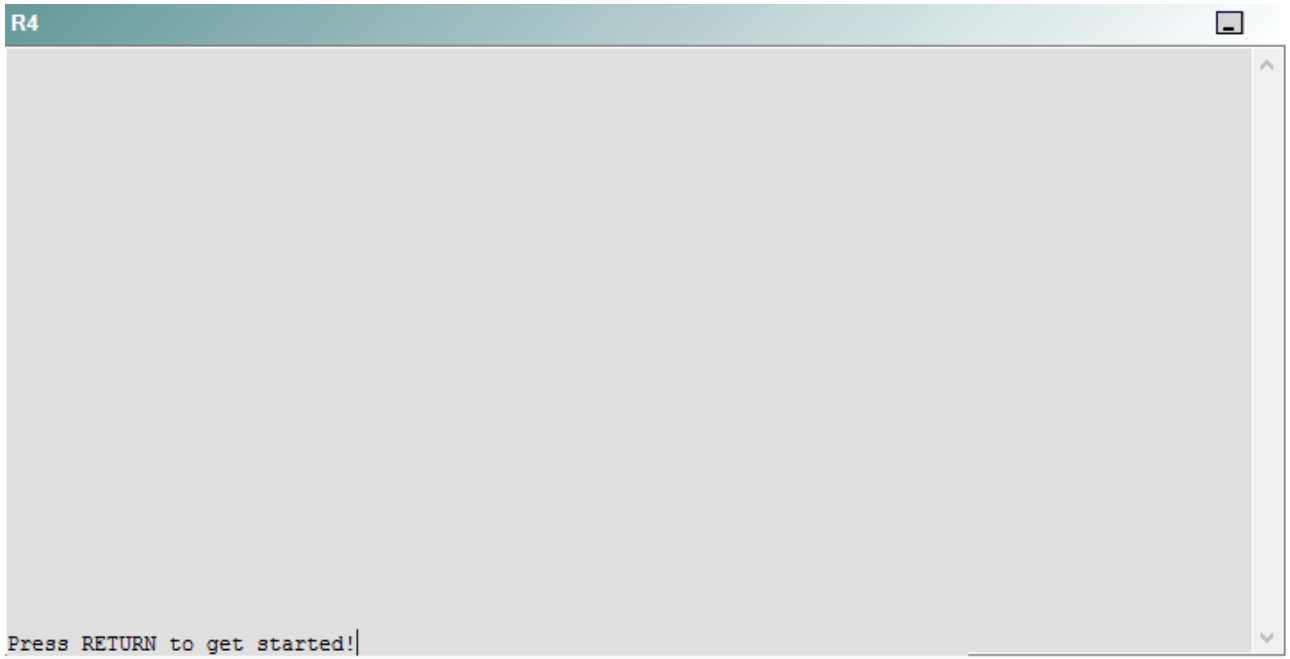

R2



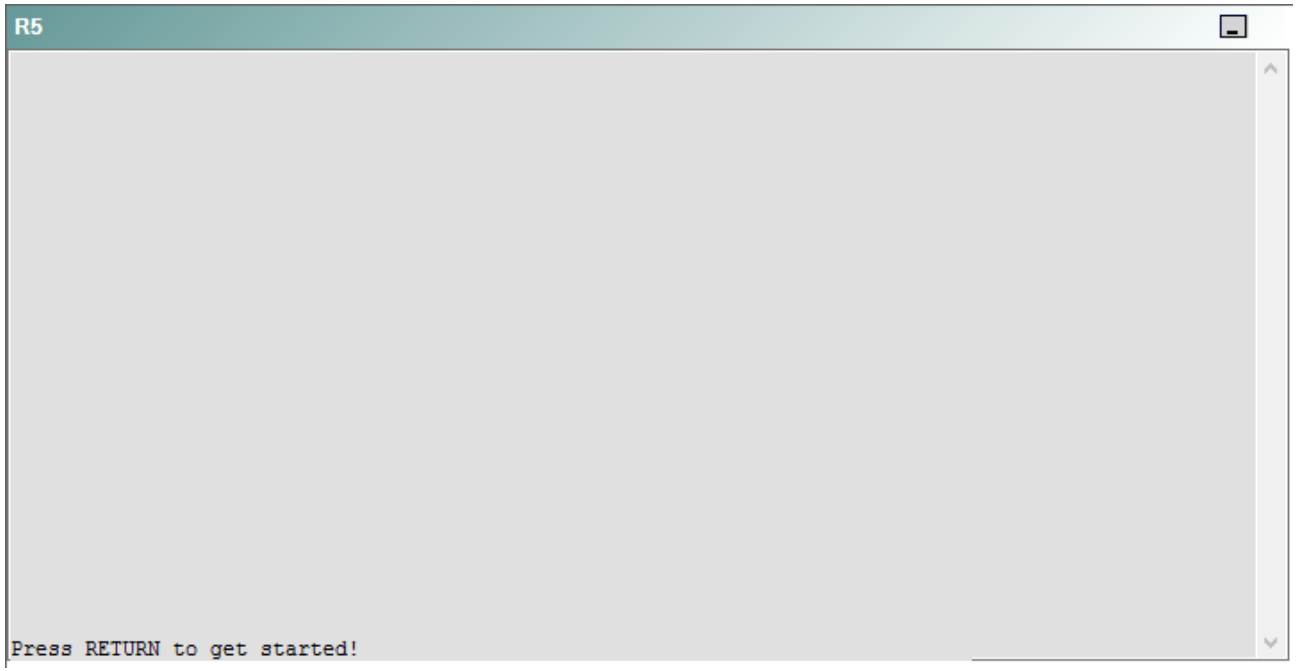

R3



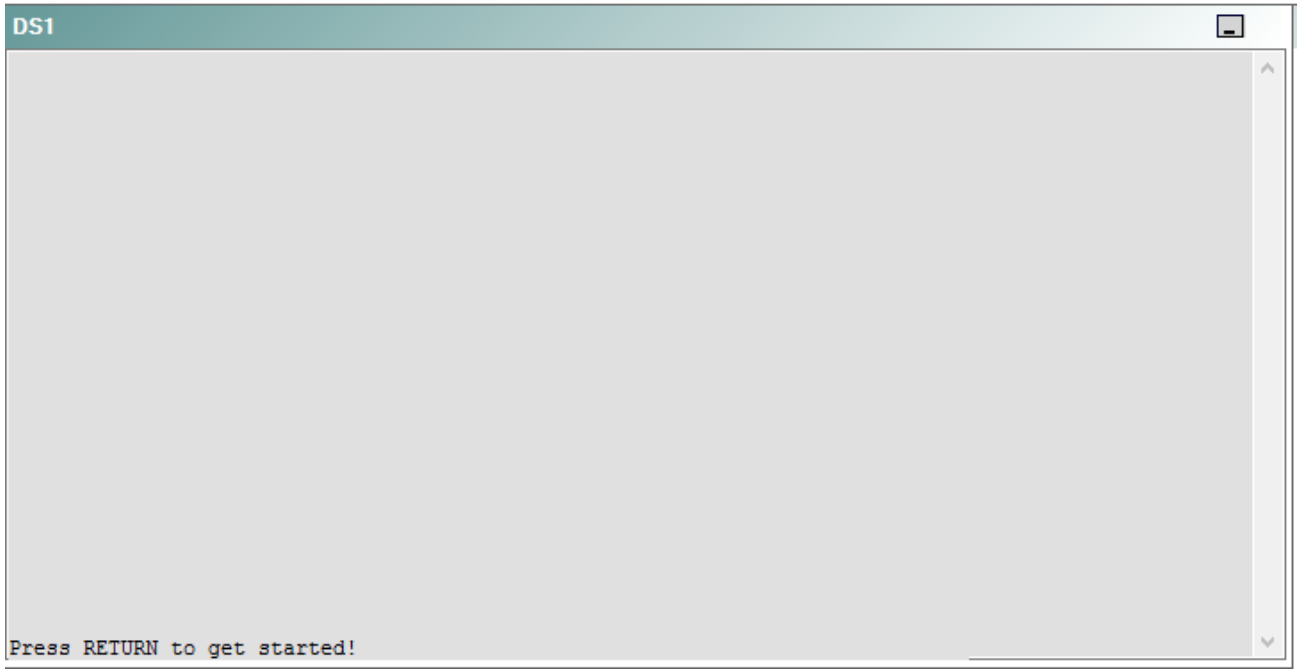

R4



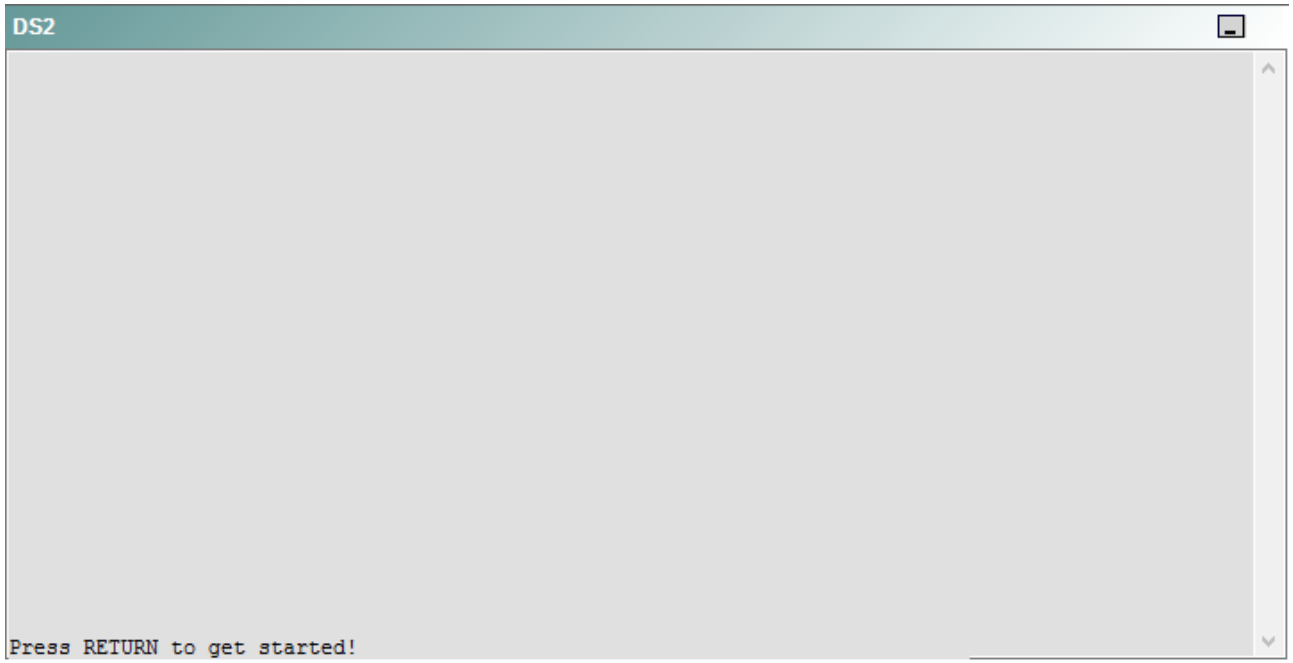

R5



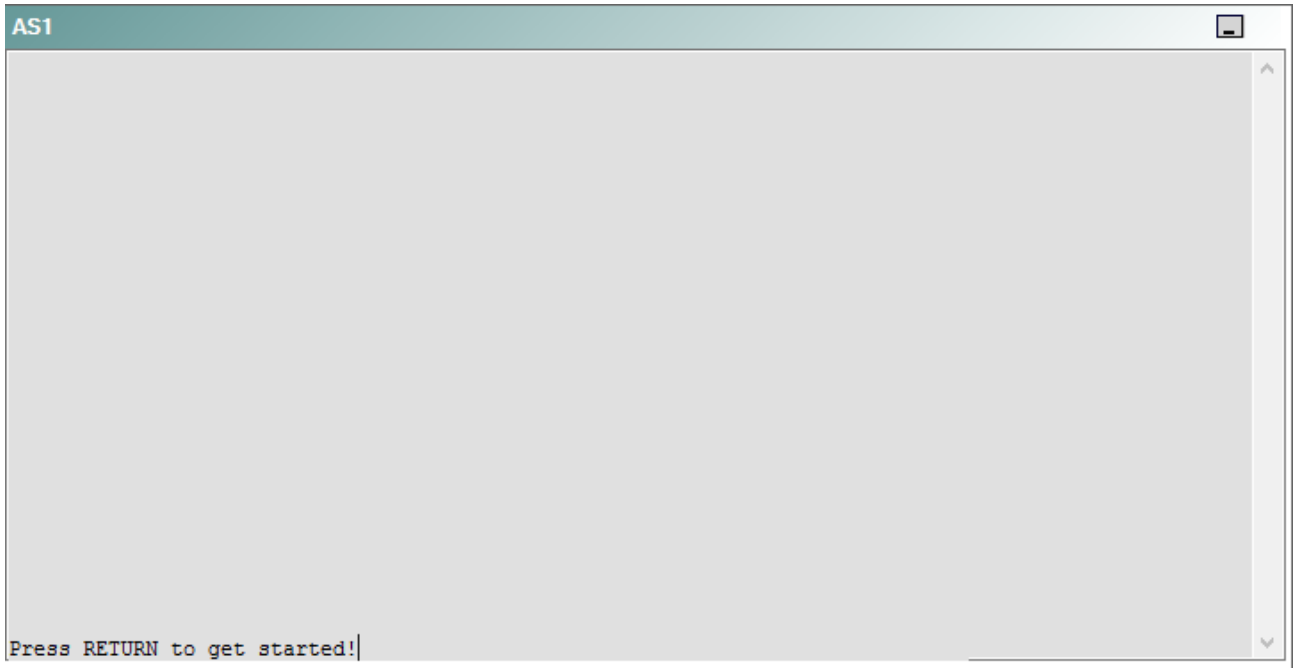

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. OSPFv3
C. EIGRP
D. redistribution
E. Layer 3 security
F. Layer 3 addressing
G. interface

**Correct Answer:** G
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 48**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

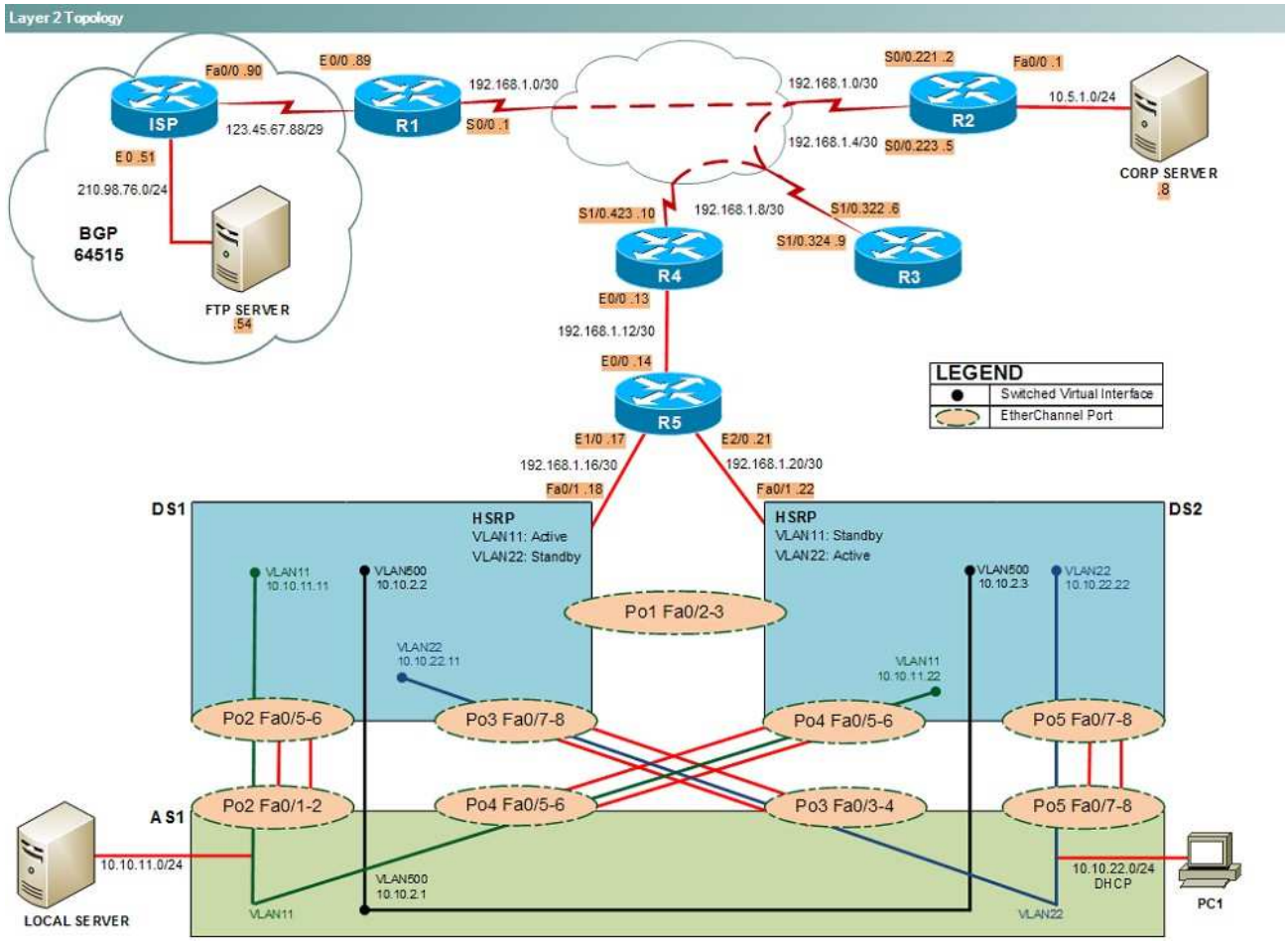
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

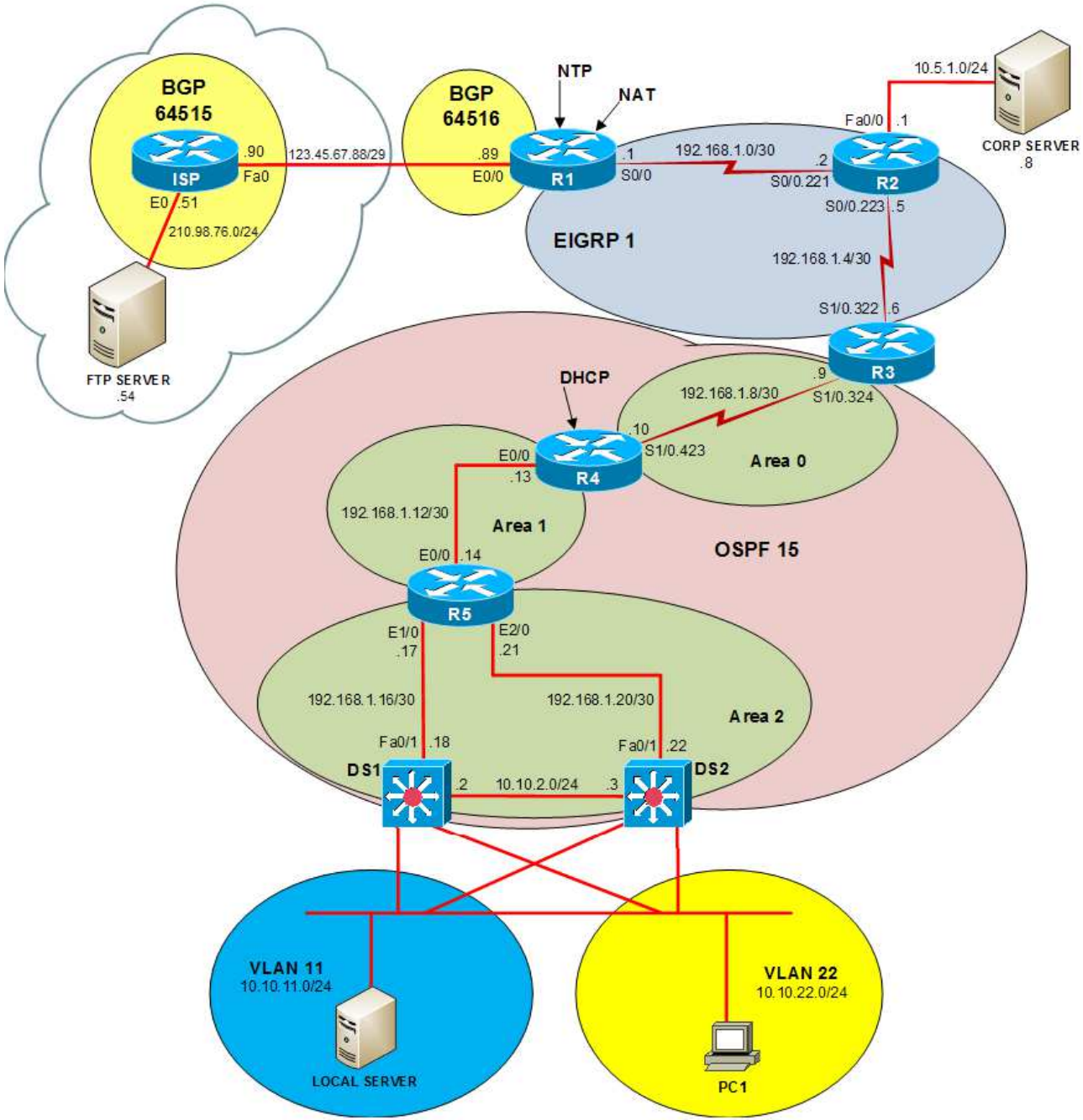
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

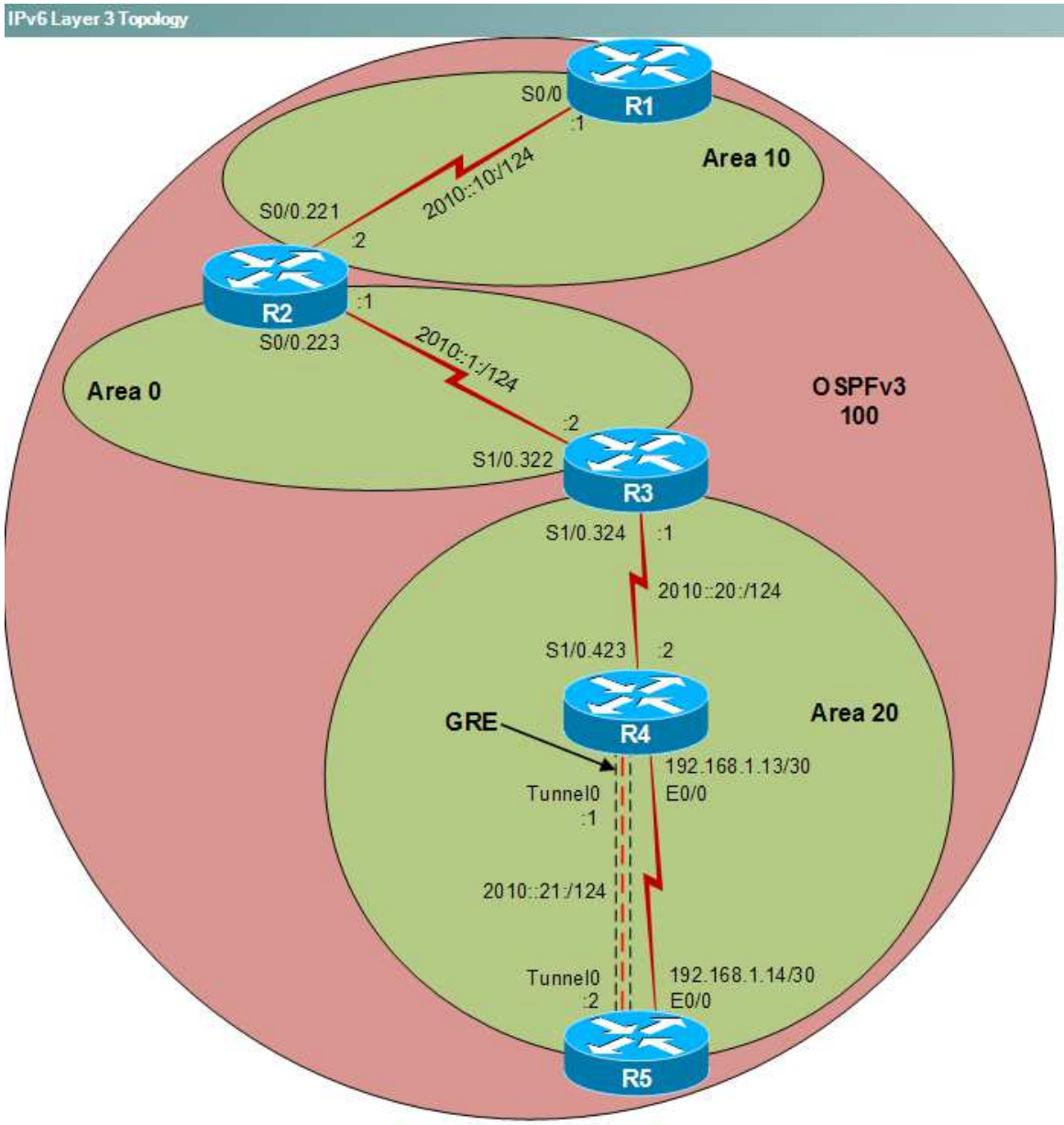
**Layer 2 Topology**




IPv4 layer 3 Topology

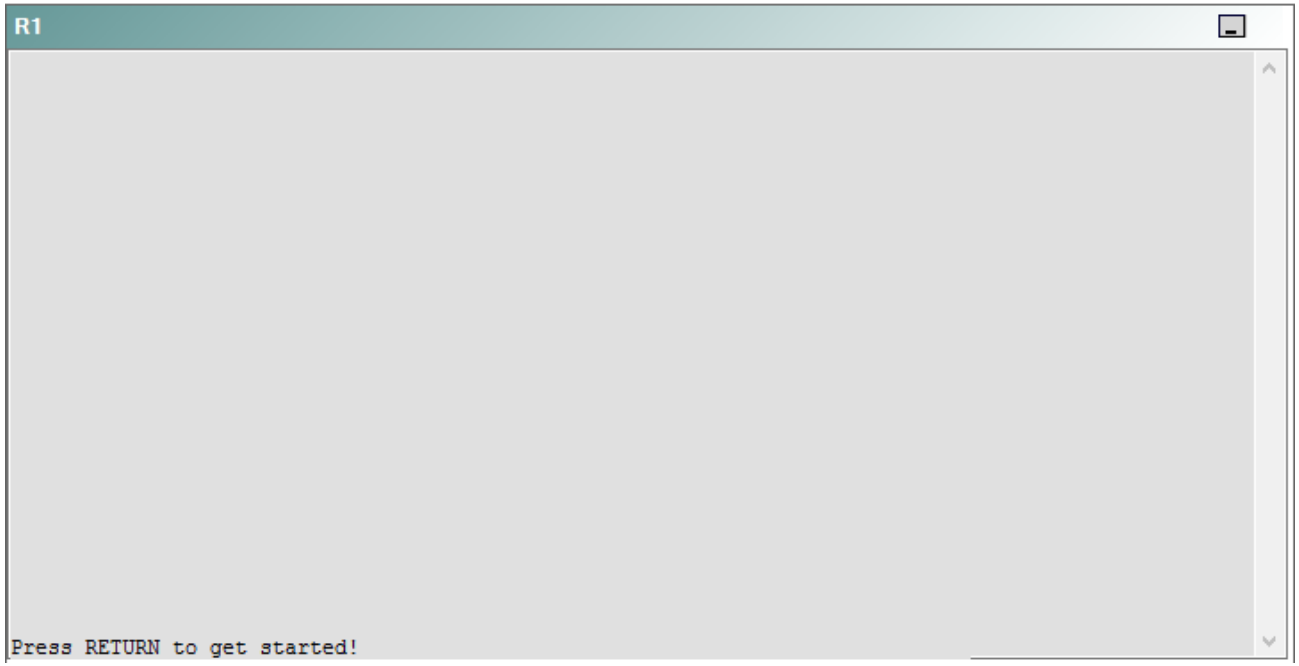

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

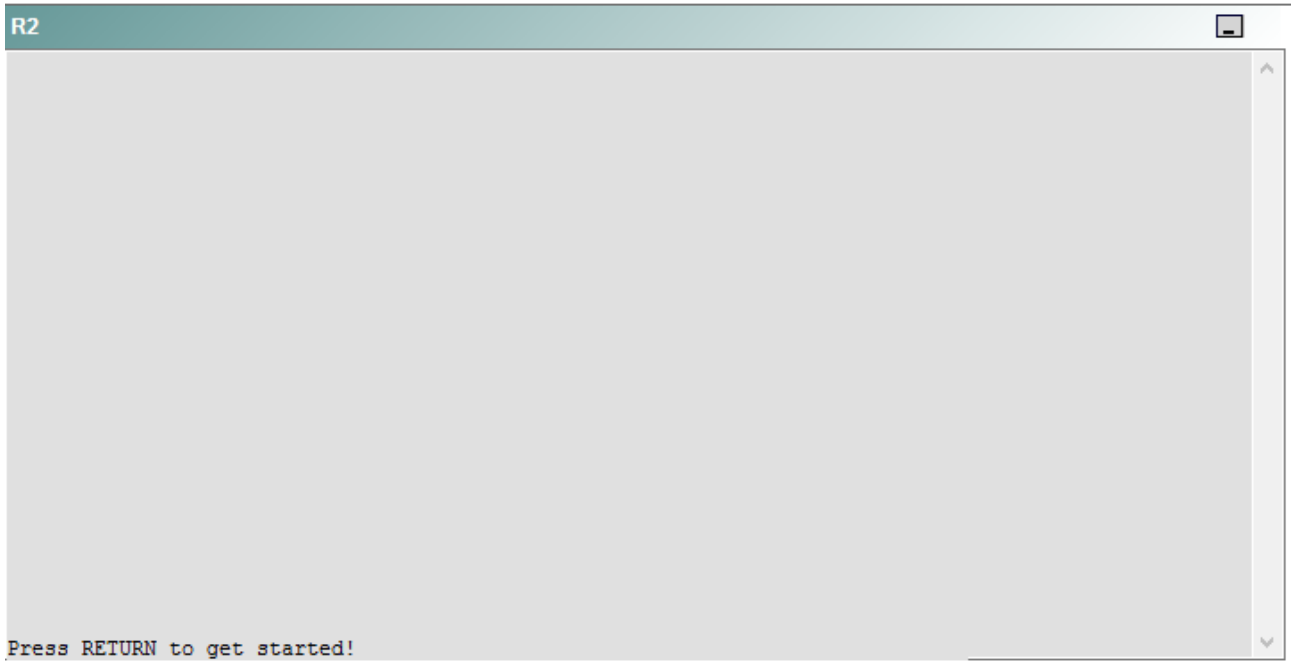



https://www.gratisexam.com/

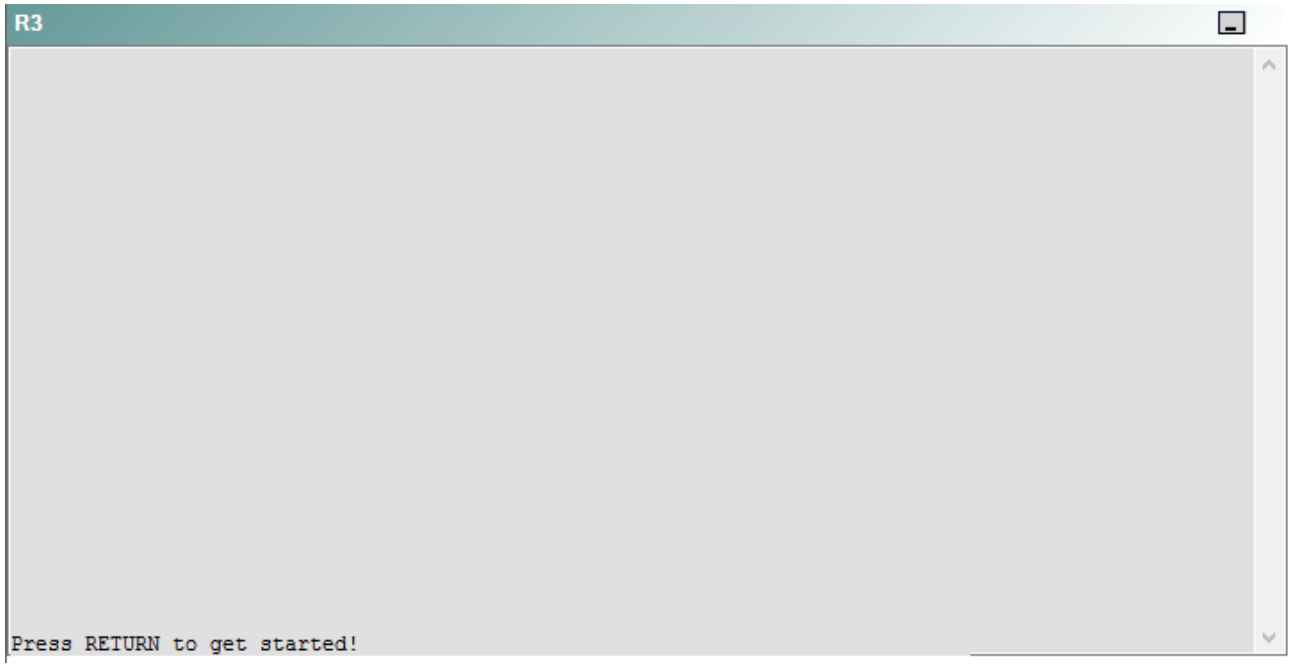
R1



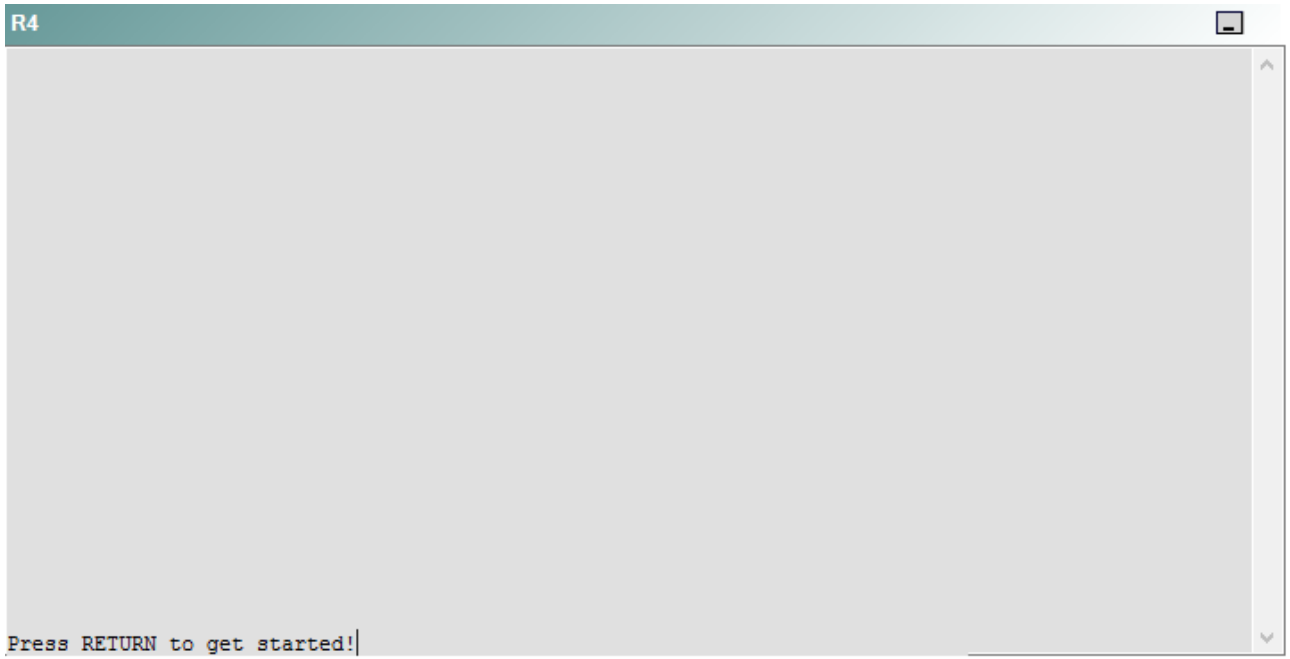

R2



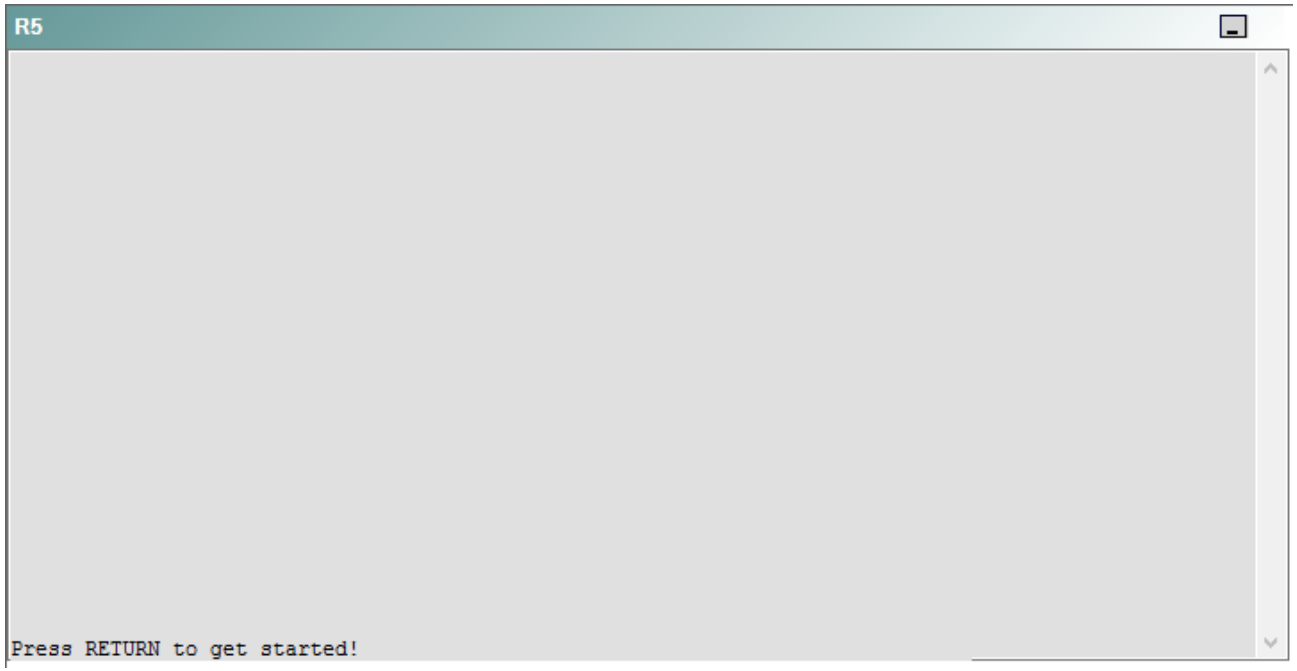

R3



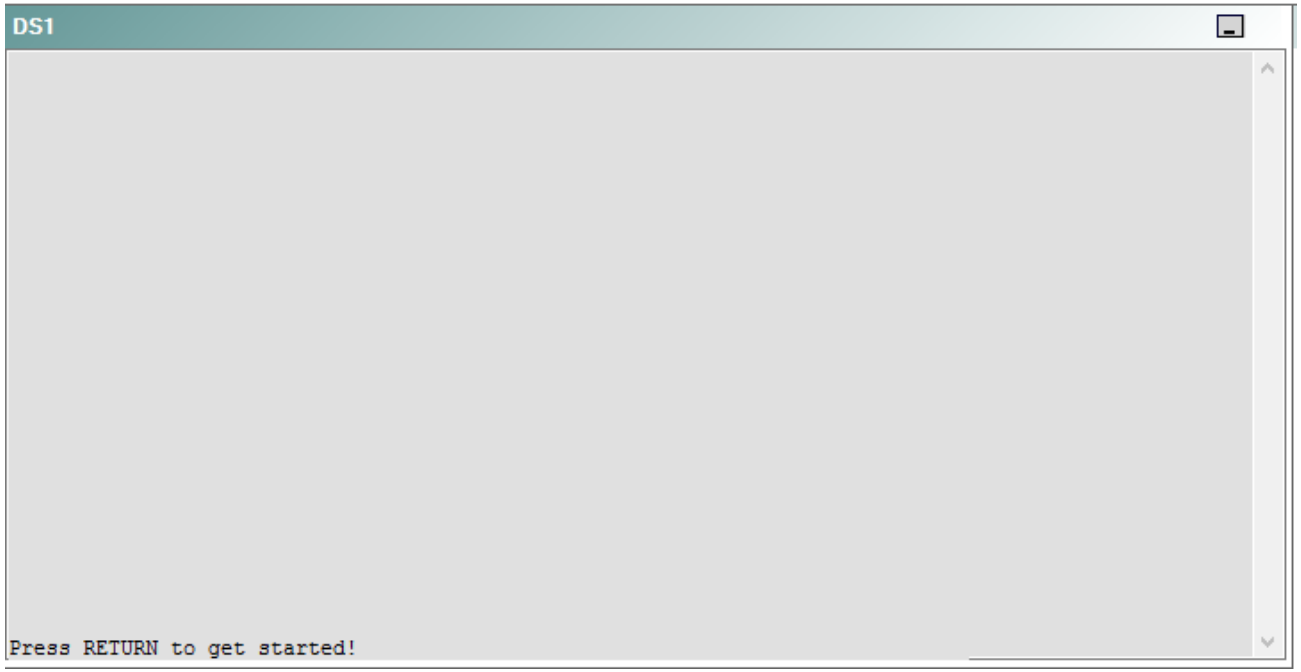

R4



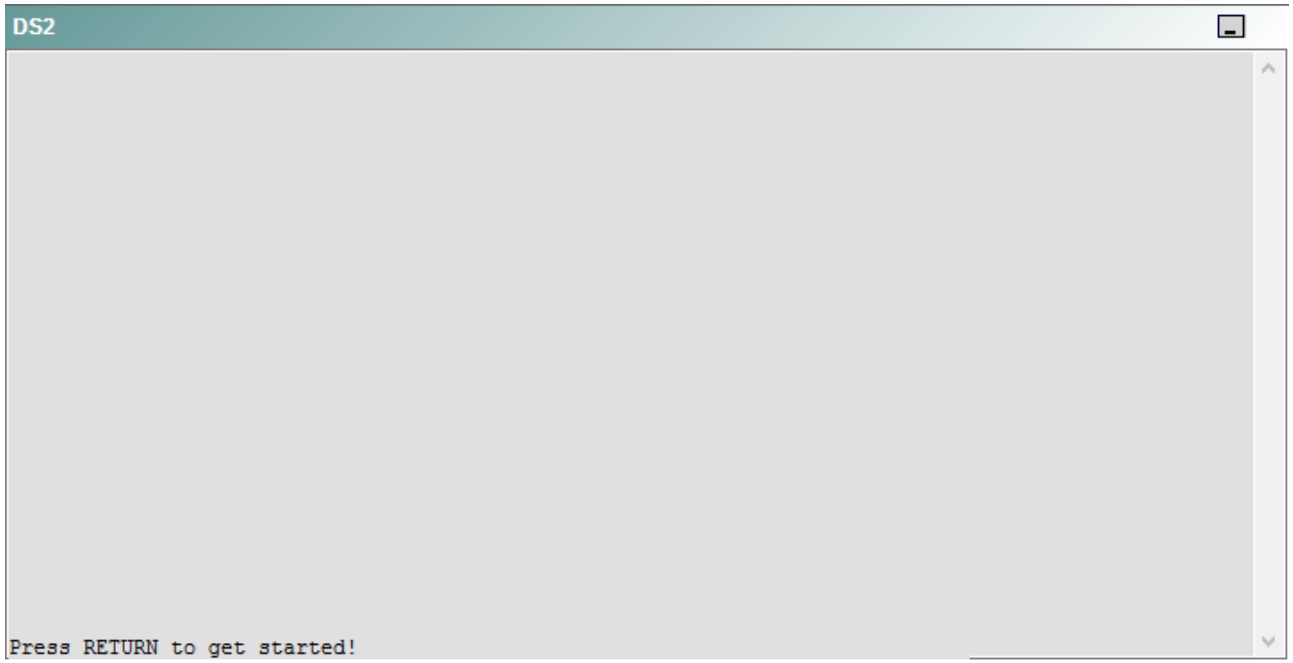

R5



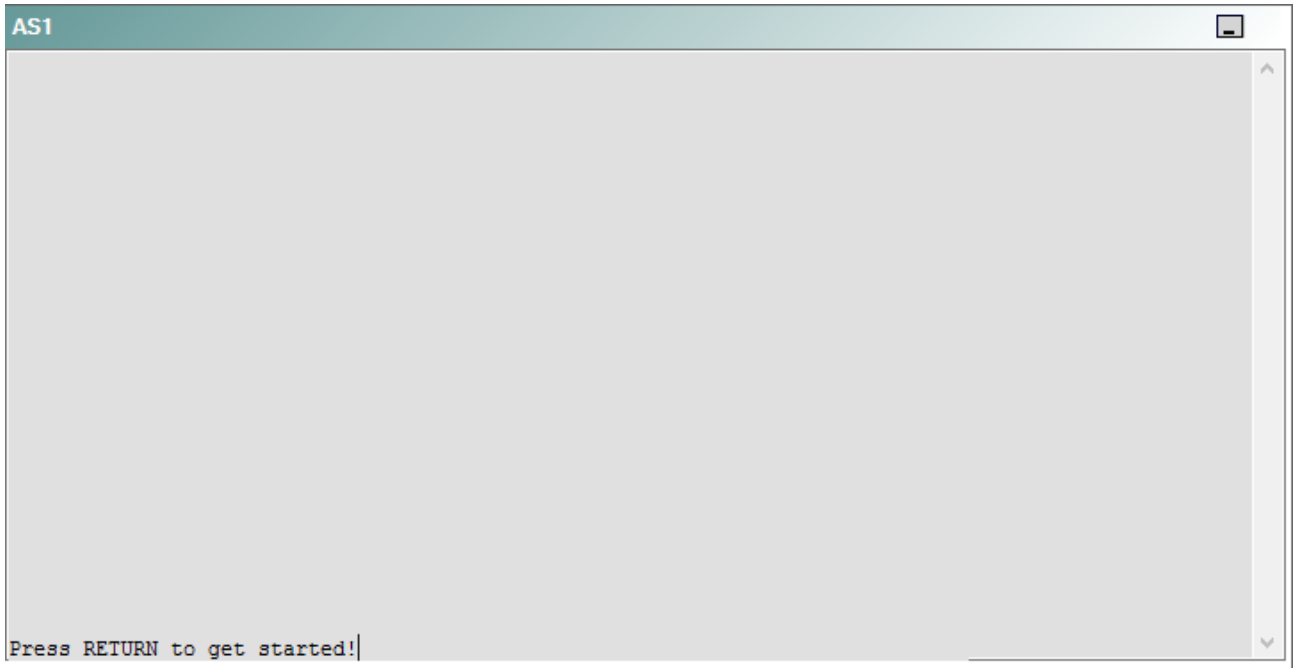

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. reconnecting the cable to the S0/0 interface
B. issuing the **no shutdown** command on the S0/0 interface
C. issuing the **no shutdown** command on the S0/0.221 and S0/0.223 subinterfaces
D. issuing the **clock rate 115200** command on the S0/0 interface
E. issuing the **encapsulation frame-relay** command on the S0/0.221 and S0/0.223 subinterfaces
F. creating frame relay maps on the S0/0.221 and S0/0.223 subinterfaces
G. changing the DLCI on the S0/0.221 to 122, and changing the DLCI on S0/0.223 to 322
H. changing the interface type to point-to-multipoint on the subinterfaces

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

You should issue the **no shutdown** command on the S0/0 interface of R2. To determine which device is the source of the problem, you should issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from PC1 to the closest device and work your way up the network until communication is lost, or you can ping from PC1 to the farthest device and work your way back to PC1 until pings are successful. Alternatively, you can trace from DS2 to the Web server and see where communication is lost along the path to the destination device.

In this scenario, if you were to issue the ping the **traceroute 210.98.76.54** command on DS2, you would receive the following output:

```
Tracing the route to 210.98.76.54

  1 192.168.1.21 0 msec 0 msec 0 msec
  2 192.168.1.13 8 msec 0 msec 0 msec
  3 192.168.1.9 17 msec 17 msec 25 msec
  4 192.168.1.9 !H  !H  !H
```

The !H in the output indicates that the host is unreachable. R3 is using IP address 192.168.1.9, R3 cannot reach 210.98.76.54. Therefore, the problem likely exists on R3 or beyond.

Once you have determined where connectivity is lost, you can begin to troubleshoot what is causing the problem. Issuing the **show interfaces Serial 1/0** command on R3 reveals that the interfaces is up and the line protocol is up. However, issuing the **show interfaces Serial 0/0** command on R2 reveals that the interface is administratively down, as shown in the following partial output:

```
R2#show interfaces Serial 0/0
Serial0/0 is administratively down, line protocol is down
```

After you issue the **no shutdown** command on the S0/0 interface, you will receive the following partial output from the **show interfaces Serial 0/0** command:

```
R2# show interfaces Serial 0/0
Serial0/0 is up, line protocol is up
```

You should not issue the **no shutdown** command on the S0/0.221 or S0/0.223 subinterfaces. Although the output from the **show interfaces Serial 0.0.211** and **show interfaces Serial 0/0.223** command would reveal that the subinterfaces are administratively down, issuing the **no shutdown** command on the subinterfaces would not enable them, because the S0/0 interface has been shut down. If a subinterface has been marked as administratively down, but the S0/0 interface is up, then you would have to issue the **no shutdown** command on the subinterface instead of on the interface.

There is no reason to suspect that the cable is disconnected from the S0/0 interface. If the cable were disconnected, you would see the following partial output from the **show interfaces Serial 0/0** command.

```
R2#show interfaces Serial 0/0
Serial0/0 is down, line protocol is down
```

You do not need to issue the **clock rate 115200** command in the S0/0 interface, because the command has already been issued on the interface. If the **clock rate 115200** command had not been issued on the S0/0 interface, you would see the following partial output from the **show interfaces Serial 0/0** command:

```
R2#show interfaces Serial 0/0
Serial0/0 is up, line protocol is down
```

The data circuit-terminating equipment (DCE) end of the serial cable typically provides clocking, and the data terminal equipment (DTE) end of the serial cable does not. You can determine which end of the serial cable is connected to the S0/0 interface by issuing the **show-controllers Serial 0/0** command, as shown in the following partial output:

```
R2#show controllers Serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 115200
idb at 0x82C10EDC, driver data structure at 0x82C18CB0
```

You cannot issue the **encapsulation frame-relay** command on the S0/0.221 and S0/0.223 subinterfaces. The **encapsulation frame-relay** command can be issued only on the interface.

You should not create Frame Relay maps on the S0/0.221 and S00/0.223 subinterfaces. Frame Relay maps cannot be created on point-to-point subinterfaces. To create a Frame Relay map, you would issue the **frame-relay map ip** *ip-address dlci* [**broadcast**] [**ietf** | **cisco**] command.

You need not change the data link connection identifier (DLCI) in the subinterfaces. A DLCI is an address that uniquely identifies a permanent virtual circuit (PVC) connection in a Frame Relay circuit. Each DLCI is locally significant, which means that the routers at each end of the PVC can use different DLCIs to identify the same circuit. To associate a subinterface with a DLCI, you would issue the **frame-relay interface-dlci** *dlci* command in subinterface configuration mode.

You need not change interface type to point-to-multipoint on the subinterfaces. R2 is currently configured so that it can communicate only with its upstream router and its downstream router, not with all the routers attached to the Frame Relay cloud. If you were to change the interface type to point-to-multipoint, you would also have to configure Frame Relay maps. To configure the interface type for a subinterface, you would issue the **interface** *type slot/ port.subinterface* [**multipoint** | **point-to-point**] command.

Reference:
https://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1915.html#wp1020558

**QUESTION 49**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

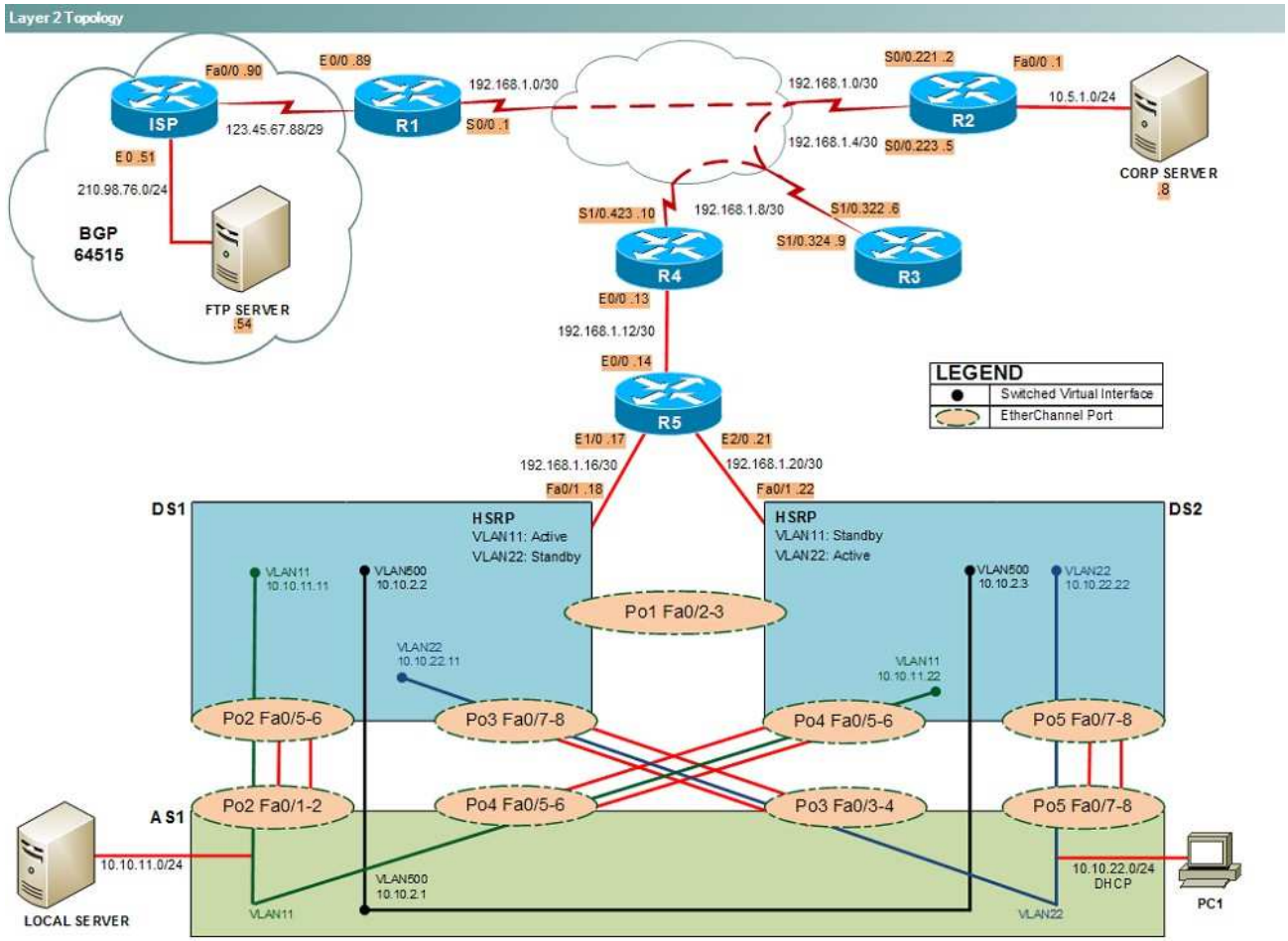
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

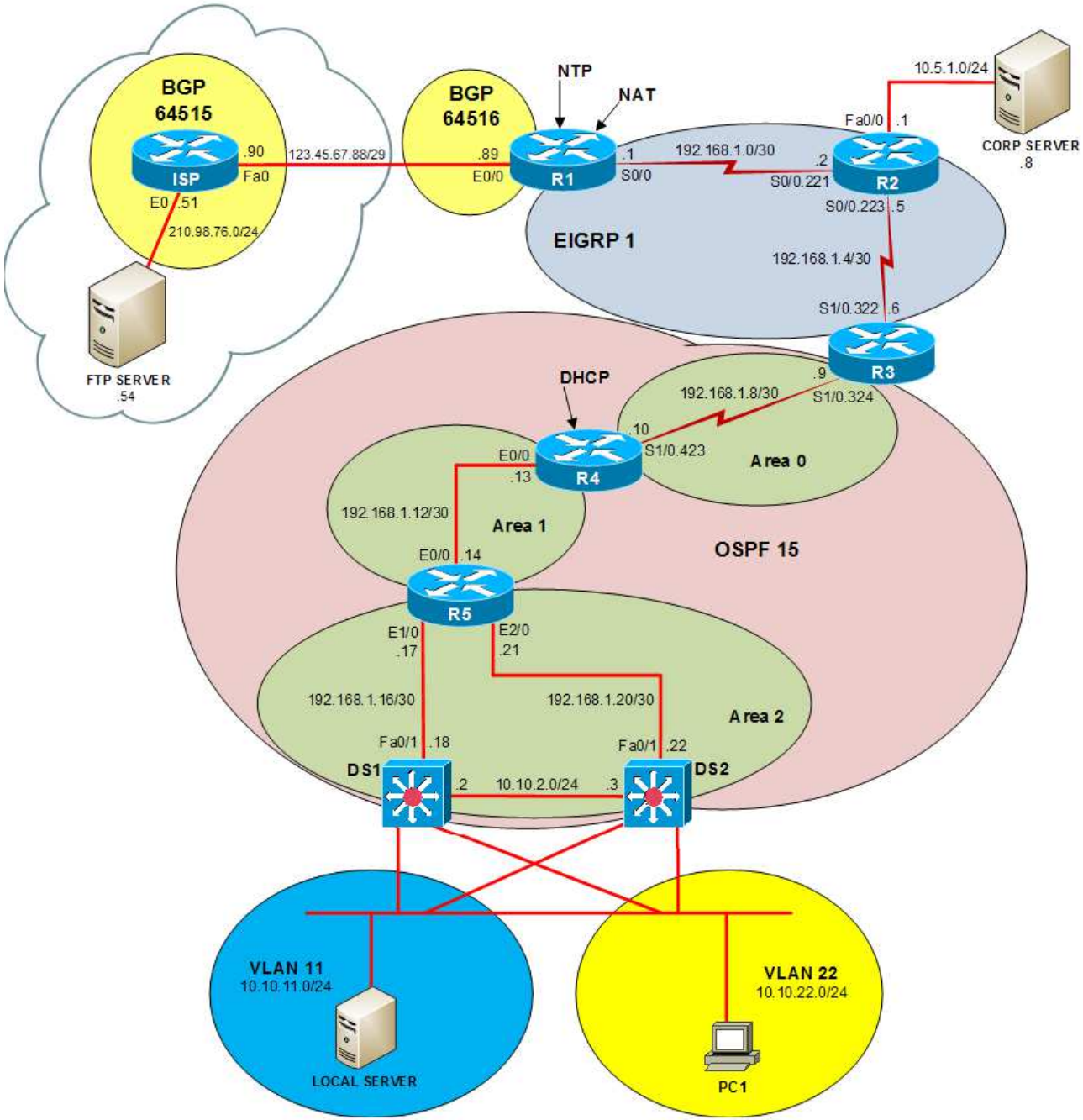
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

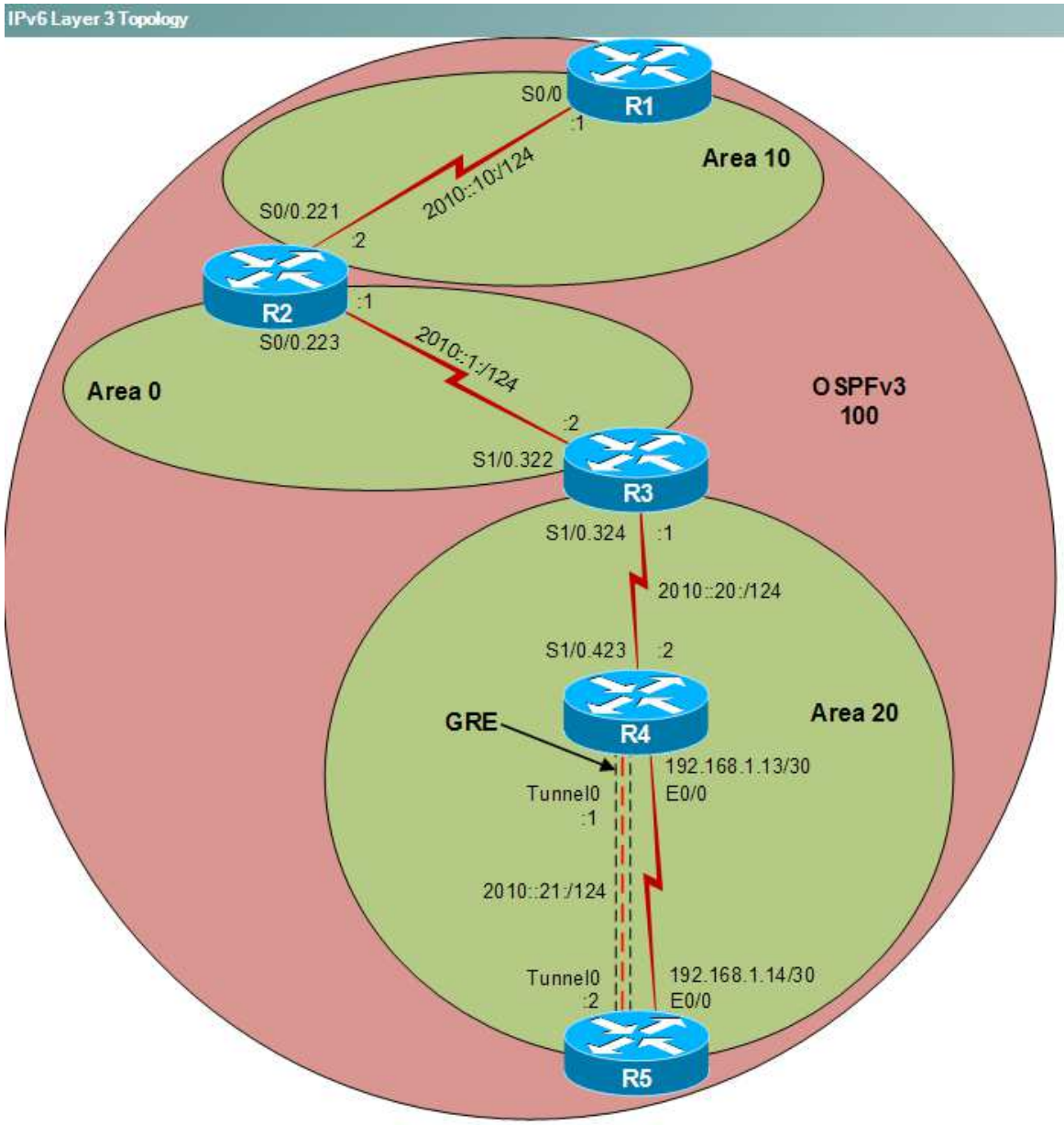
**Layer 2 Topology**




IPv4 layer 3 Topology

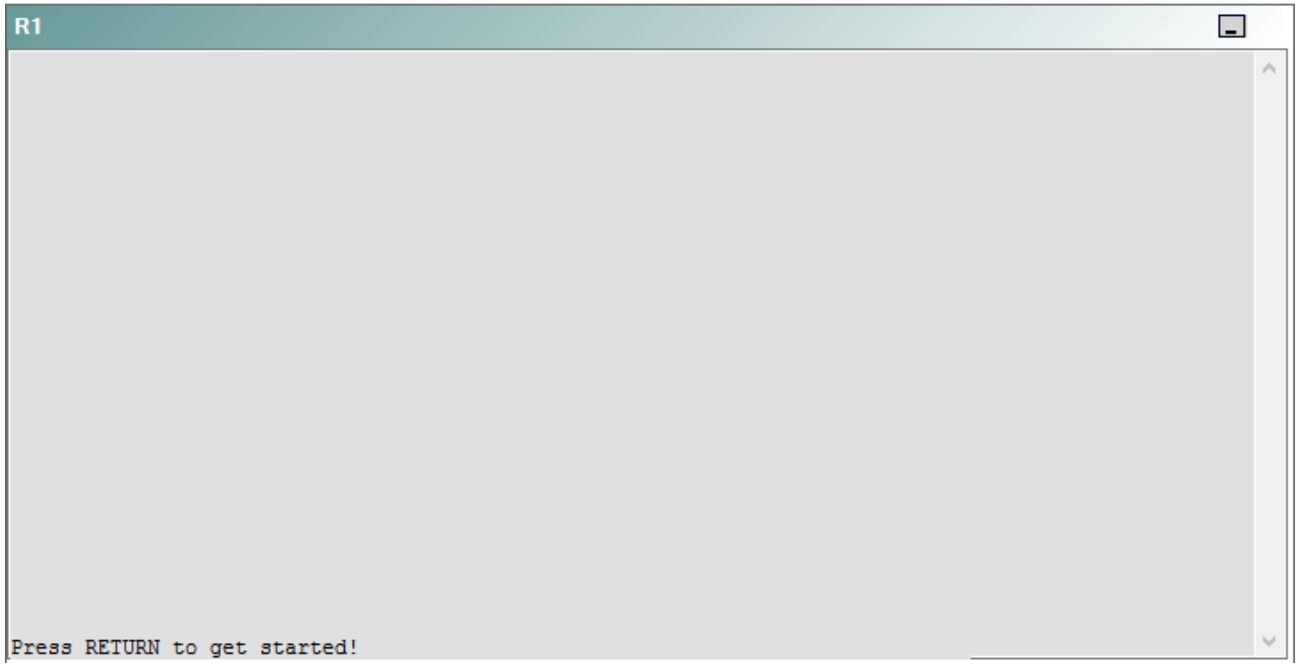

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

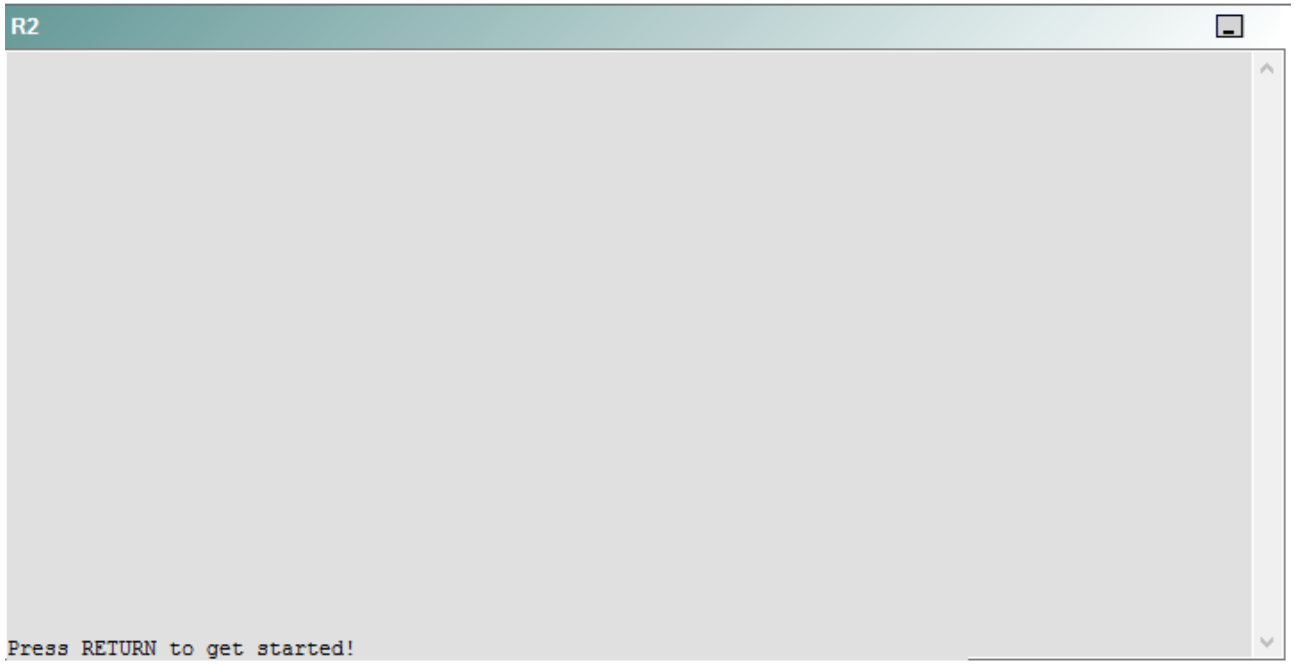



https://www.gratisexam.com/

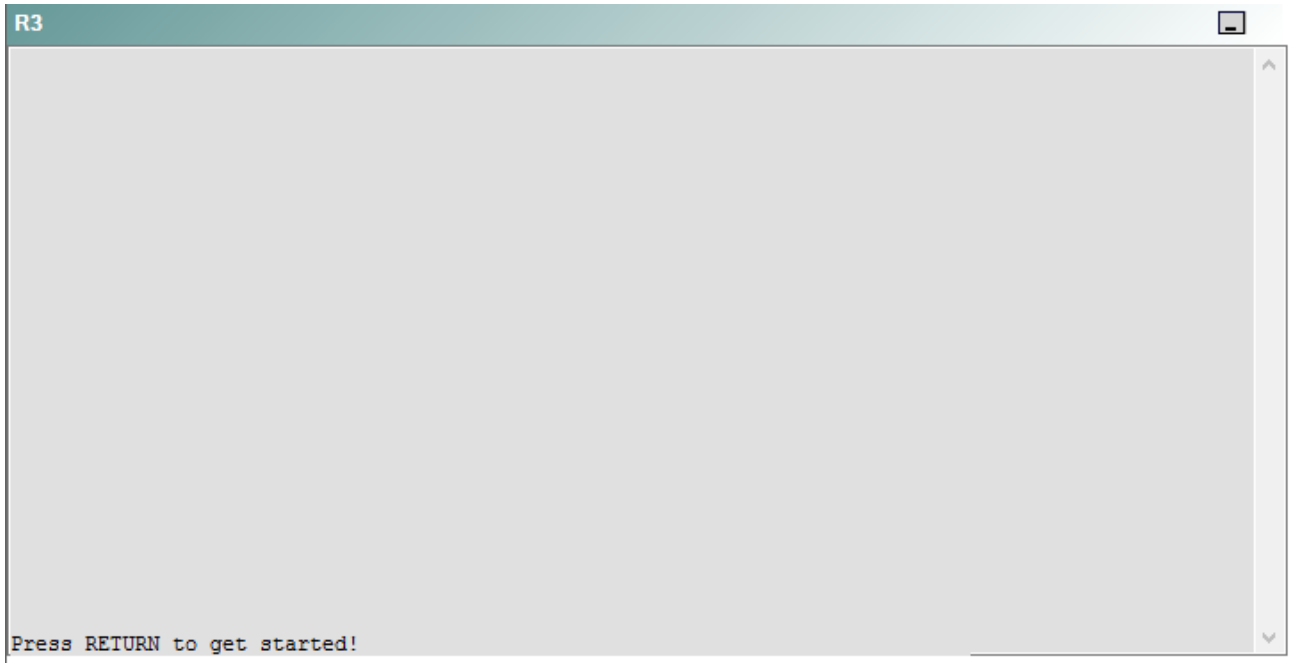
R1



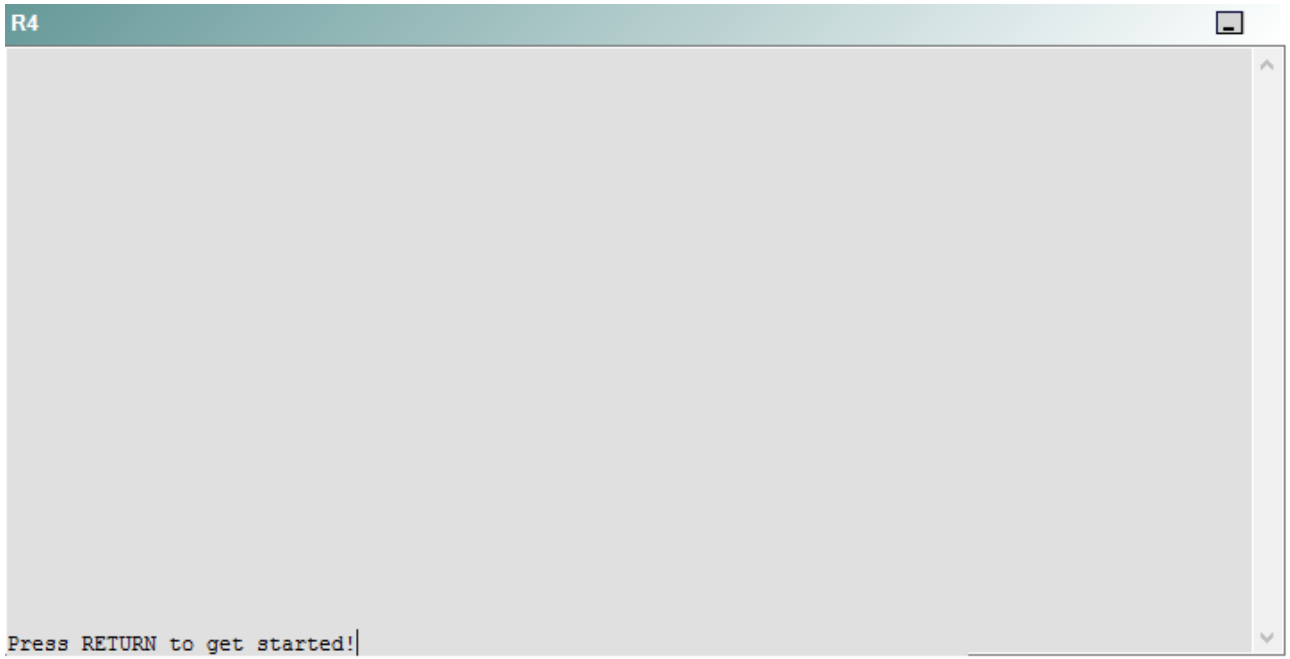

R2



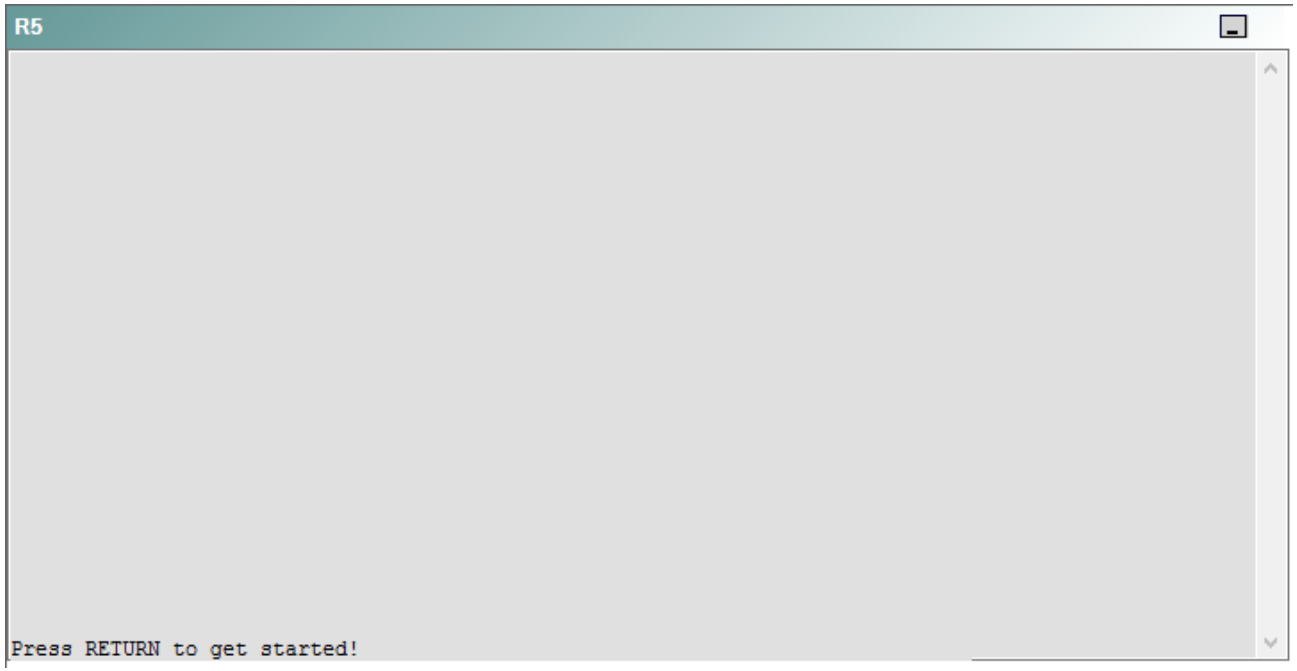

R3



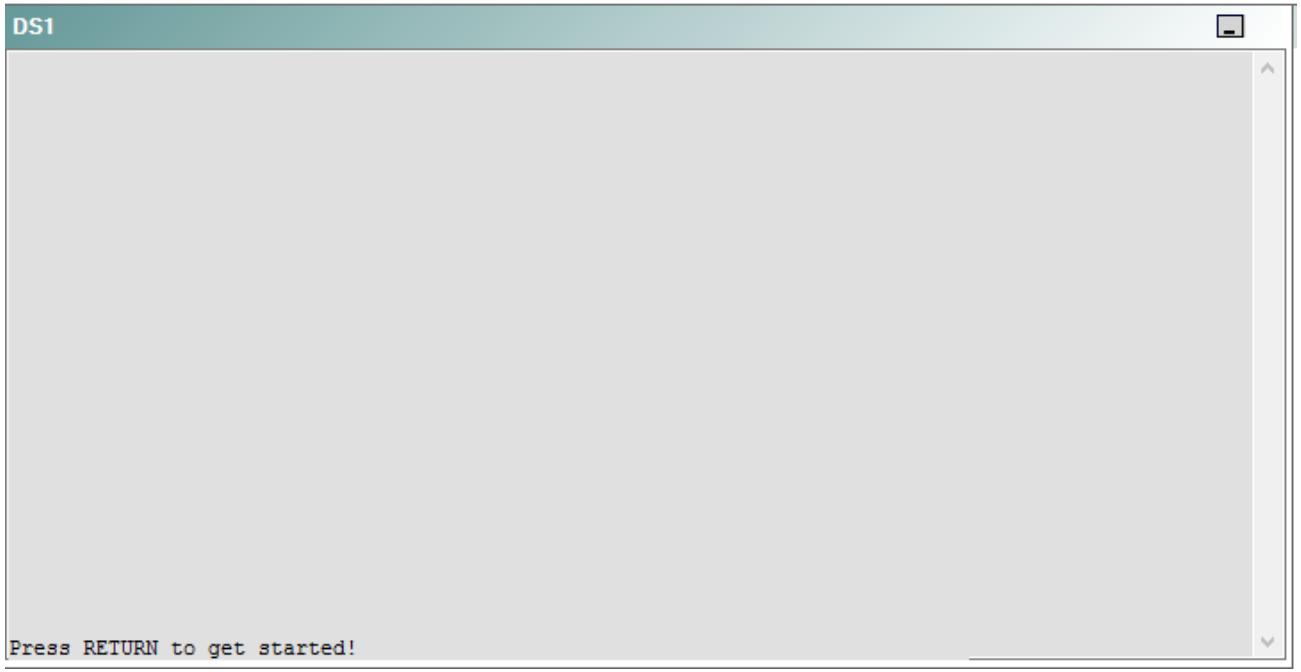

R4



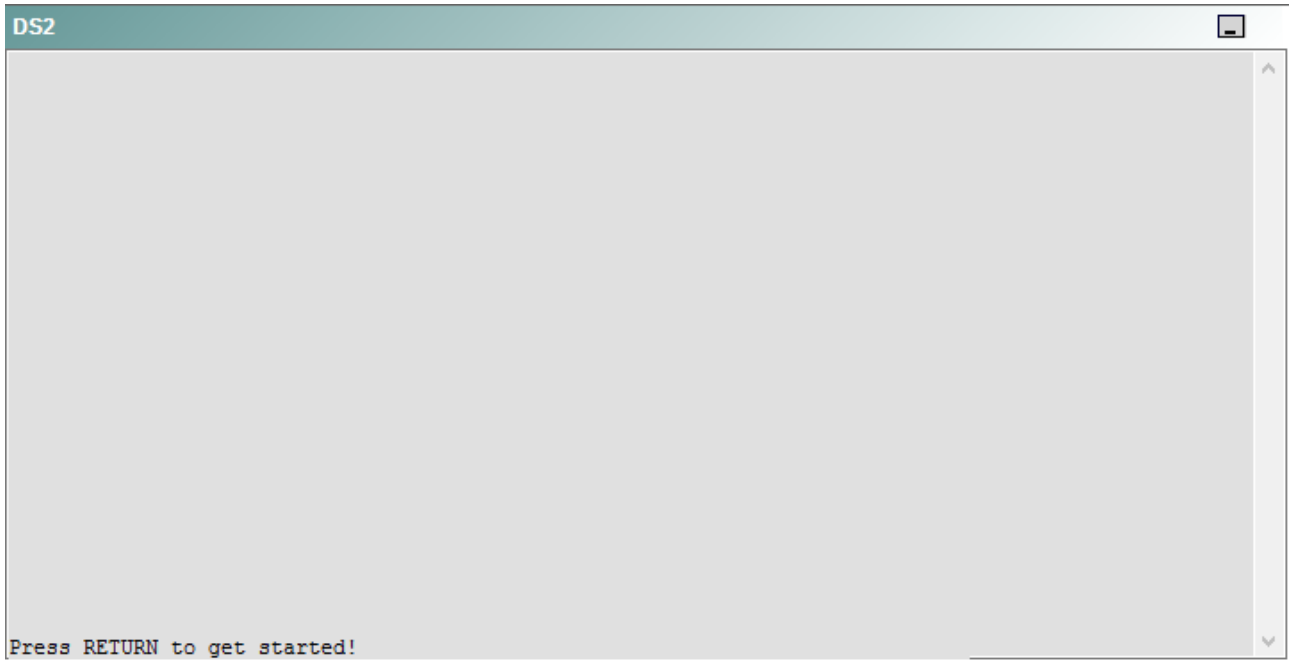

R5



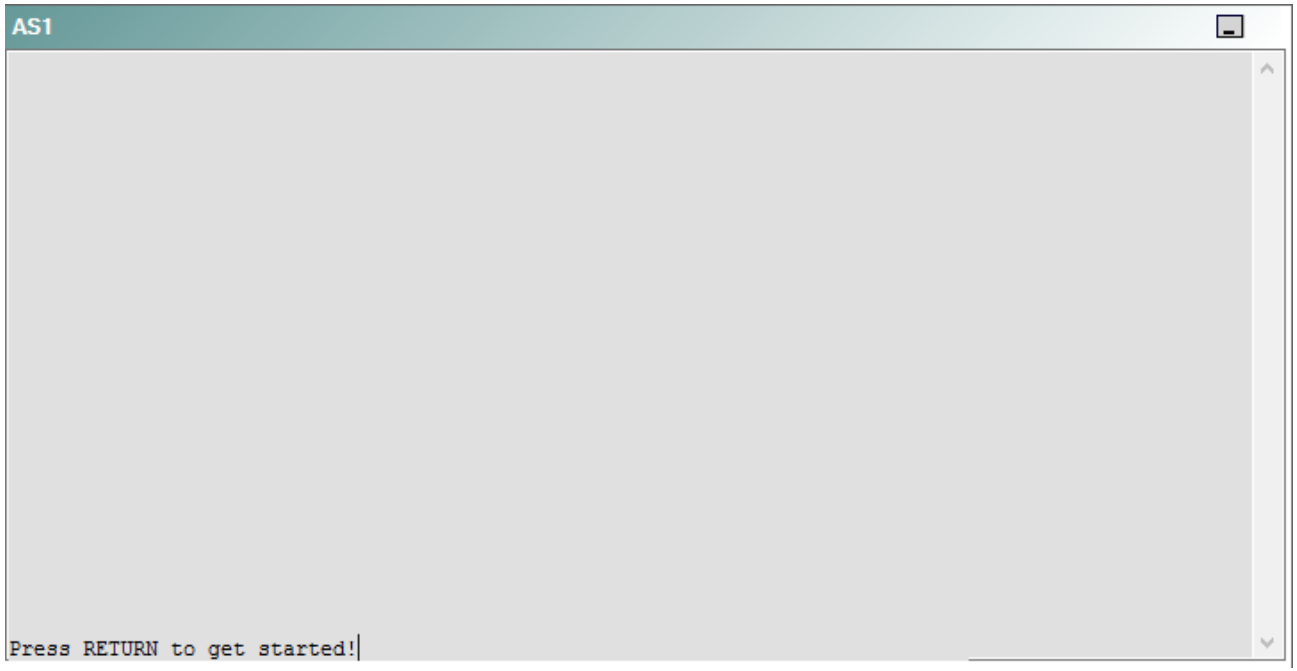

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** H
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 50**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

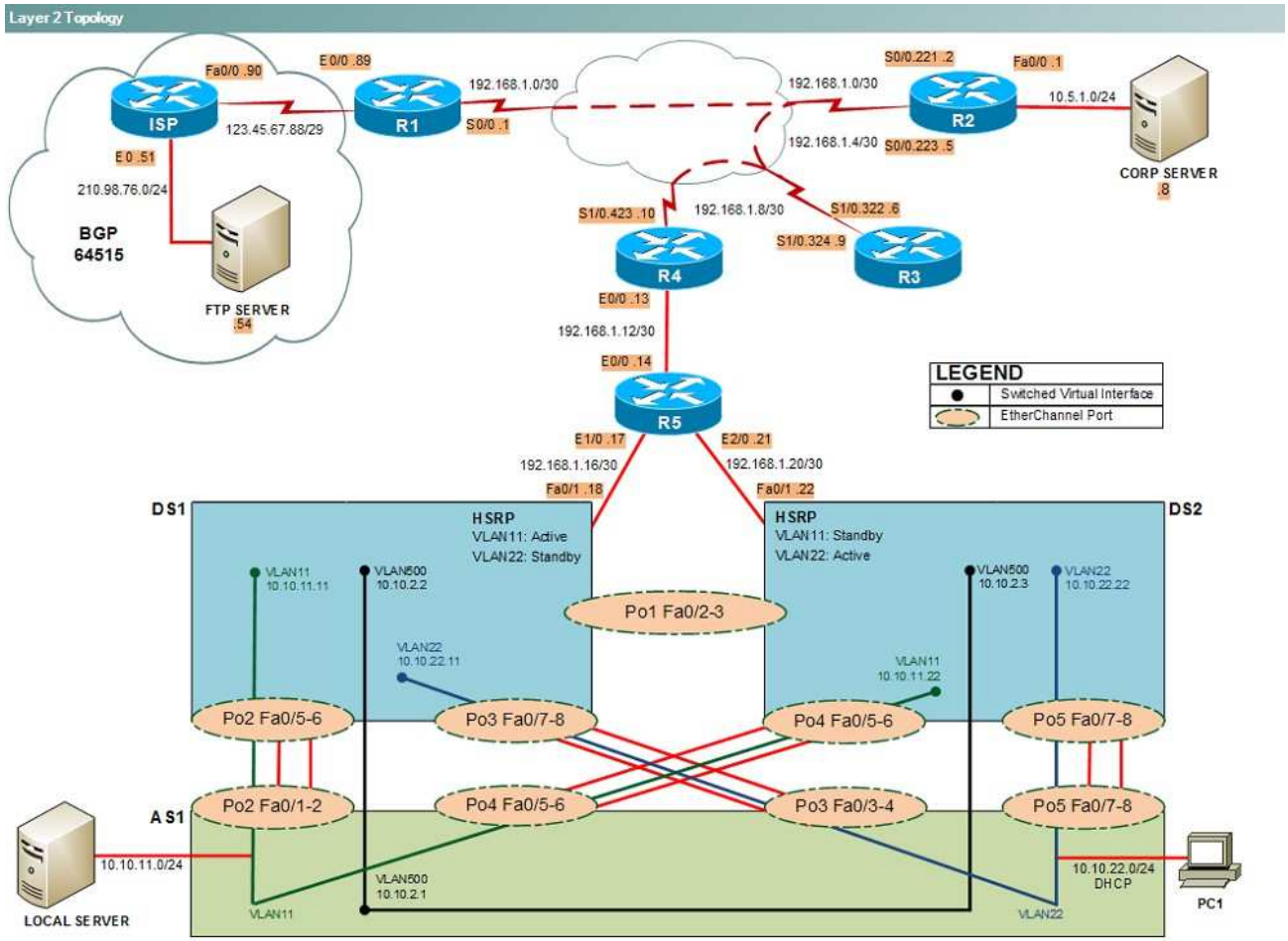
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

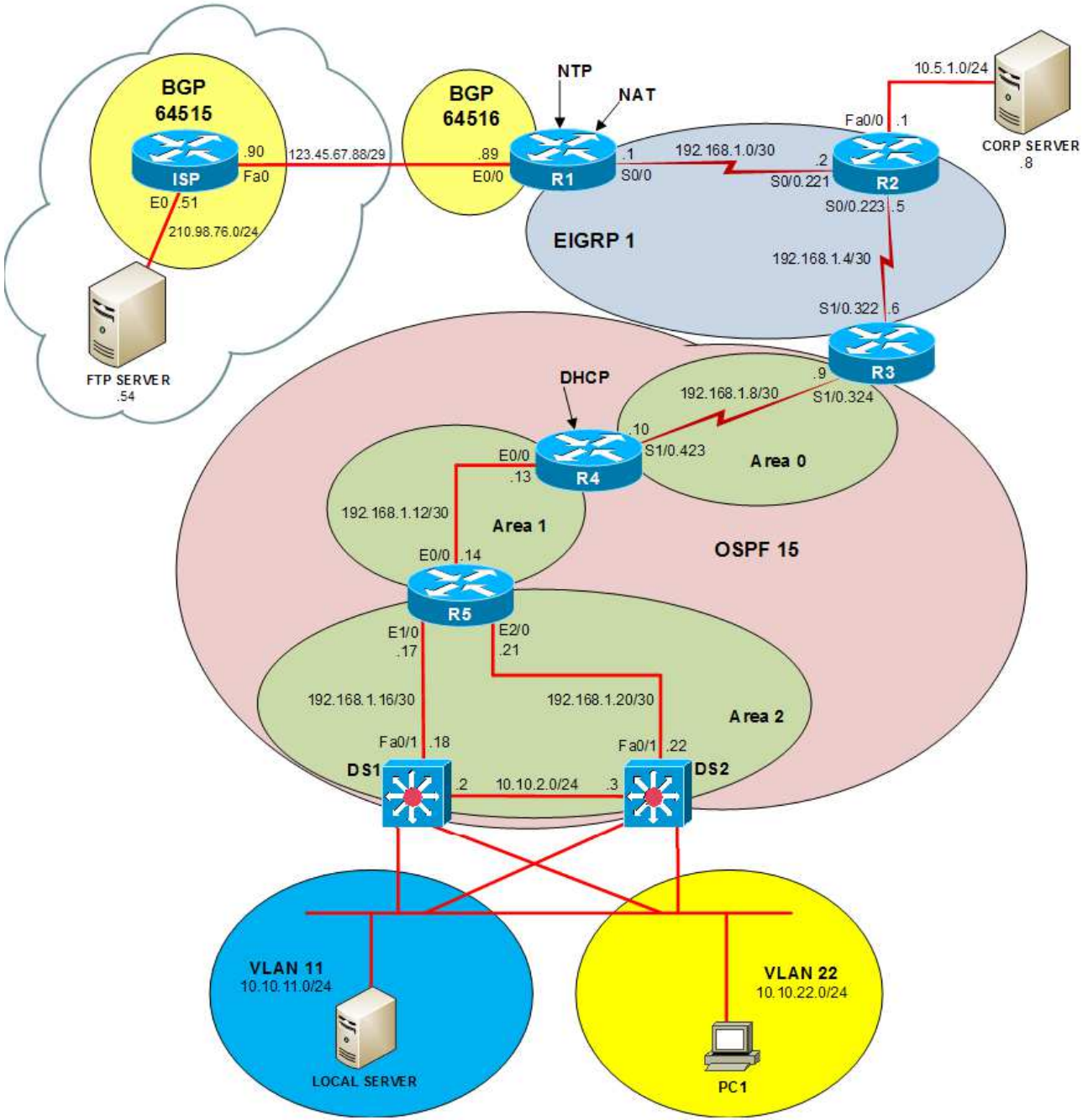
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

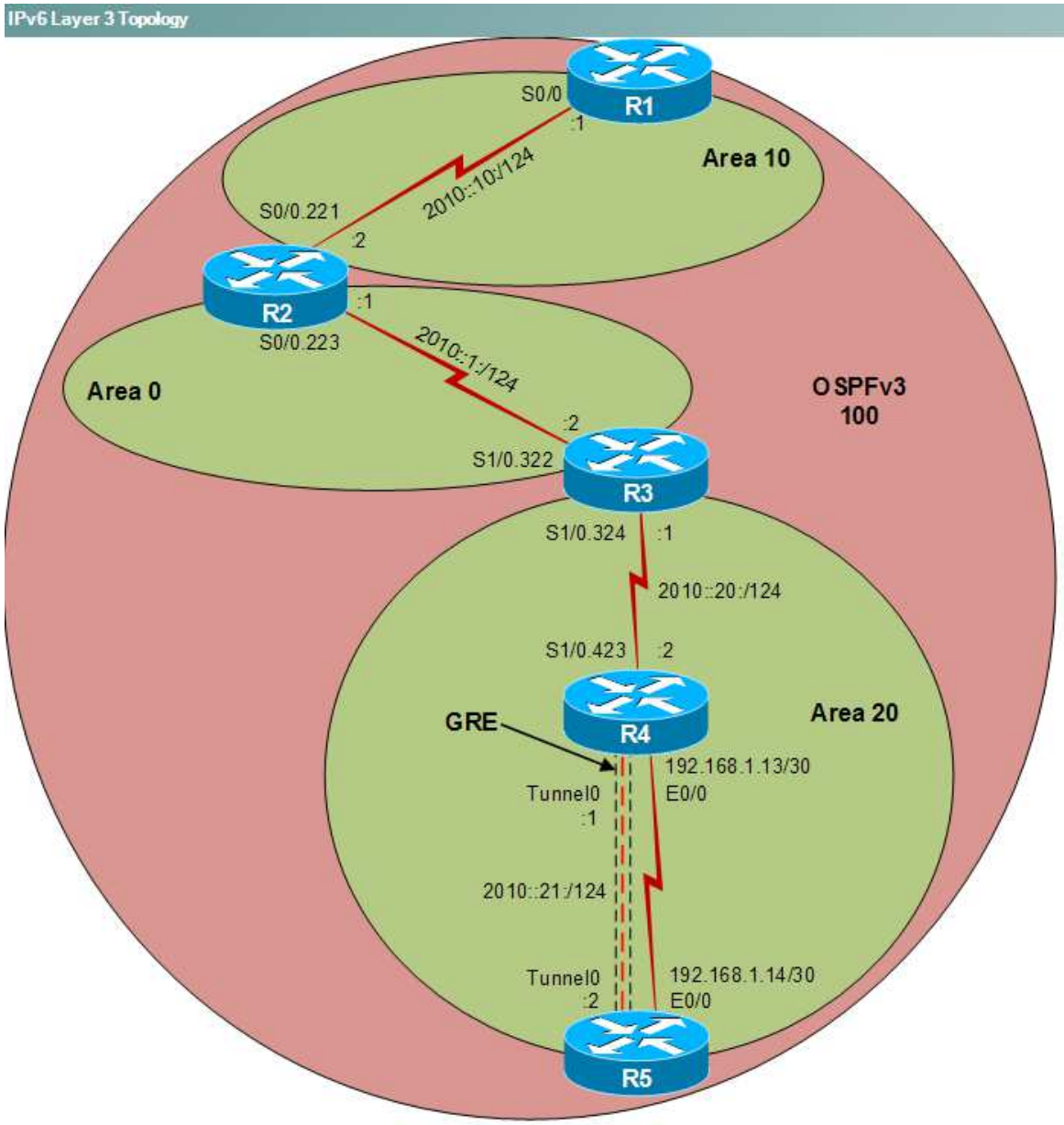
**Layer 2 Topology**




IPv4 layer 3 Topology

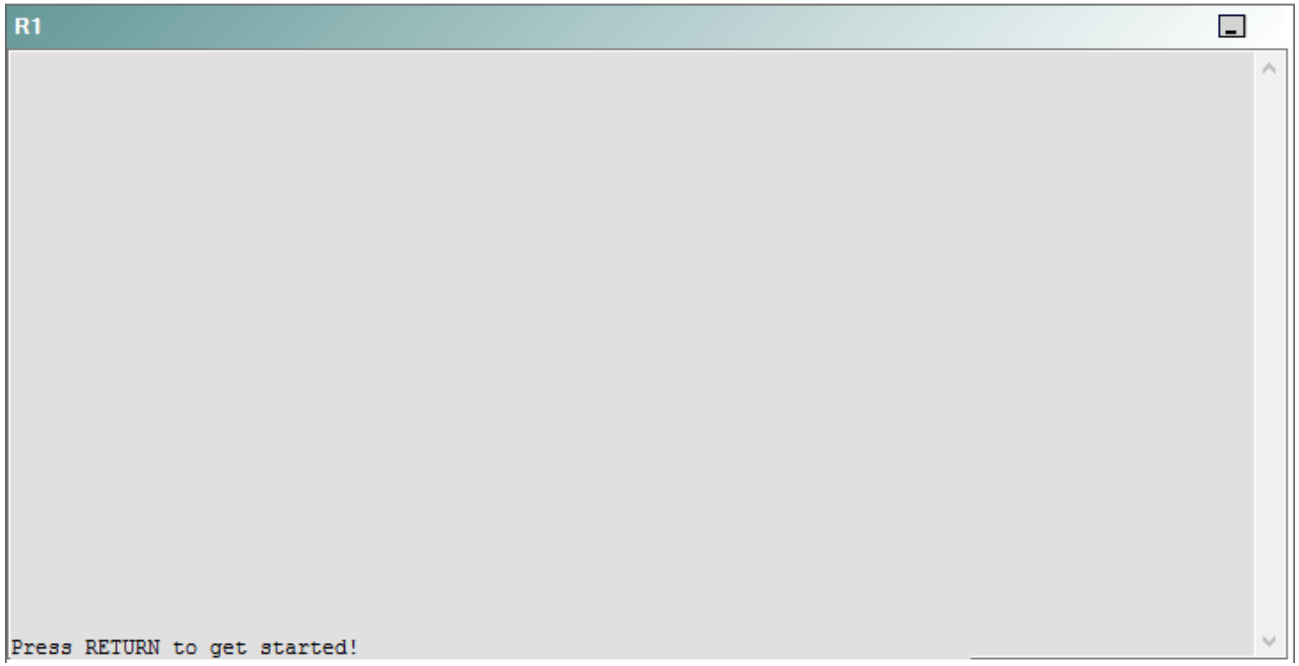

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

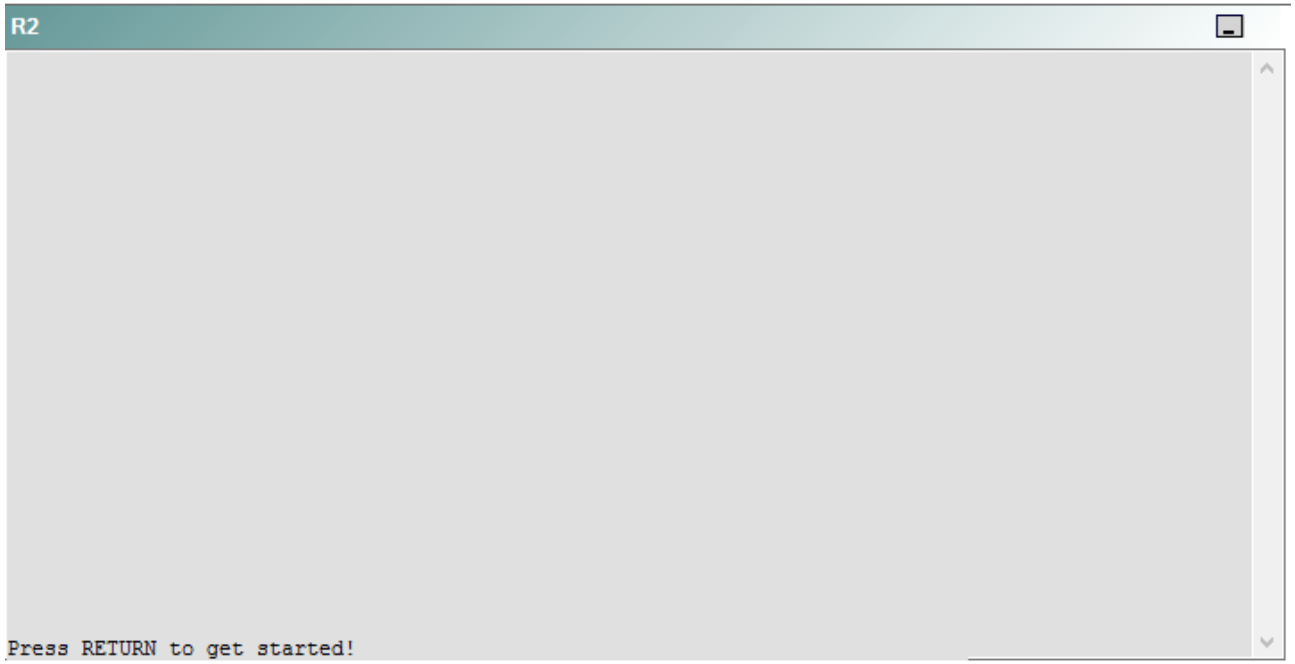



https://www.gratisexam.com/

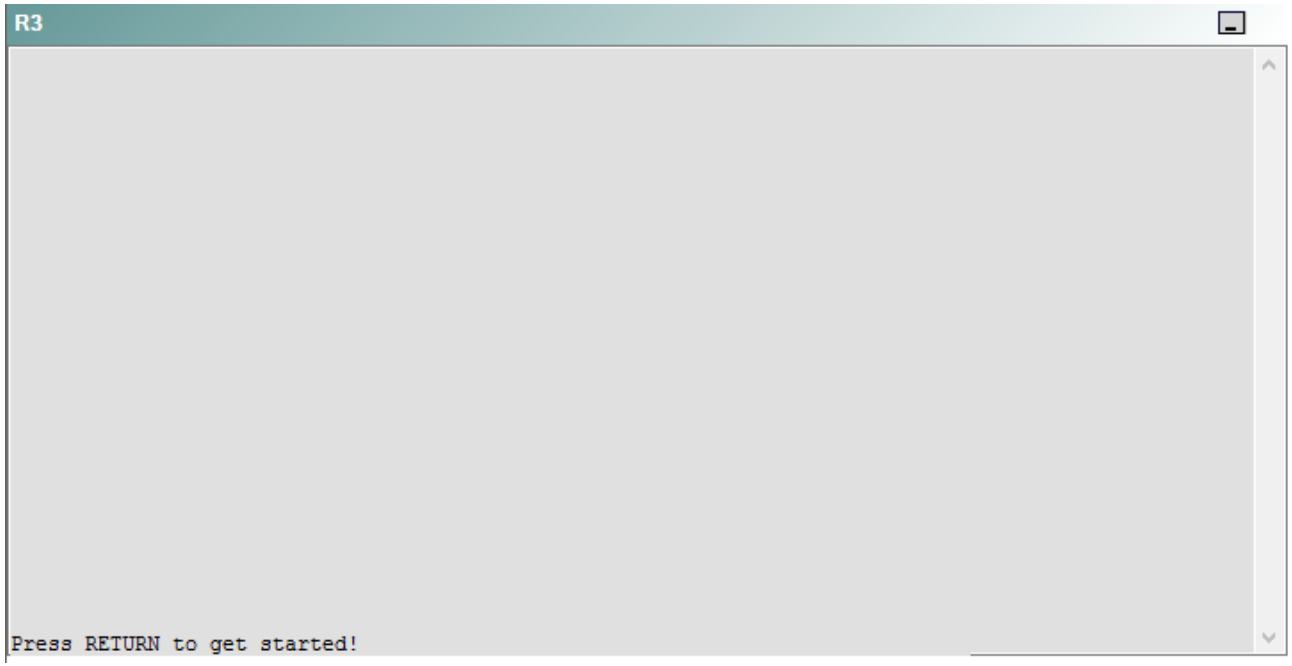
R1



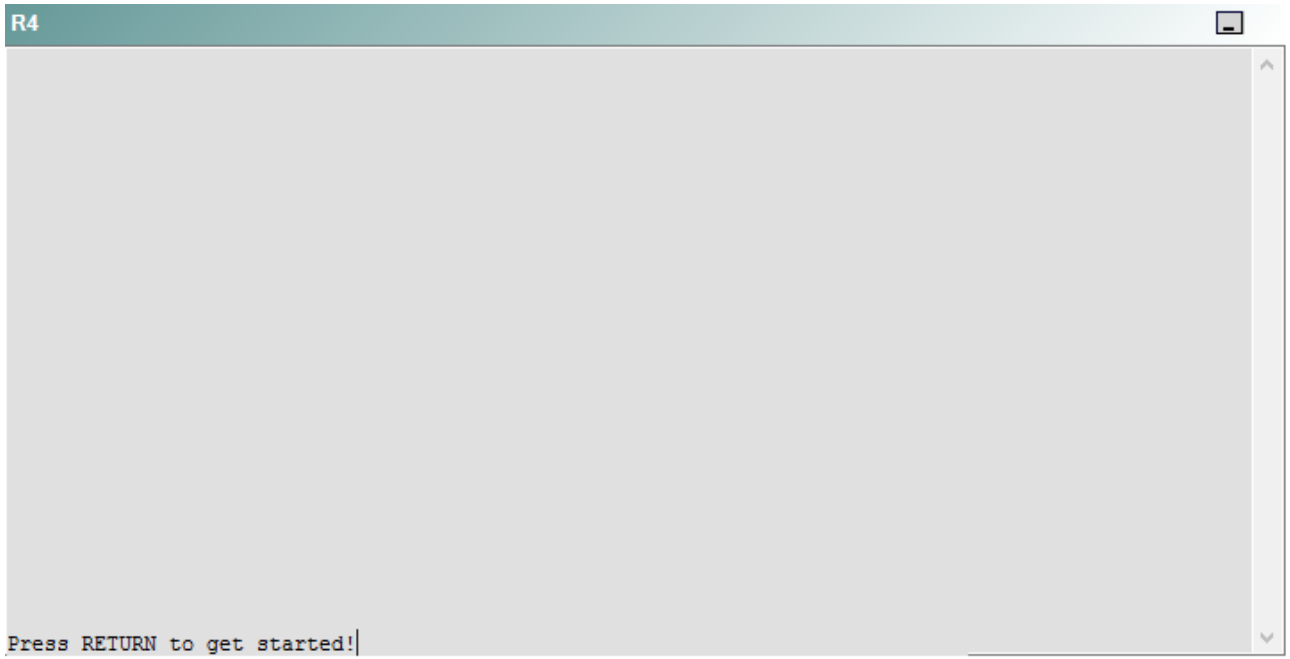

R2



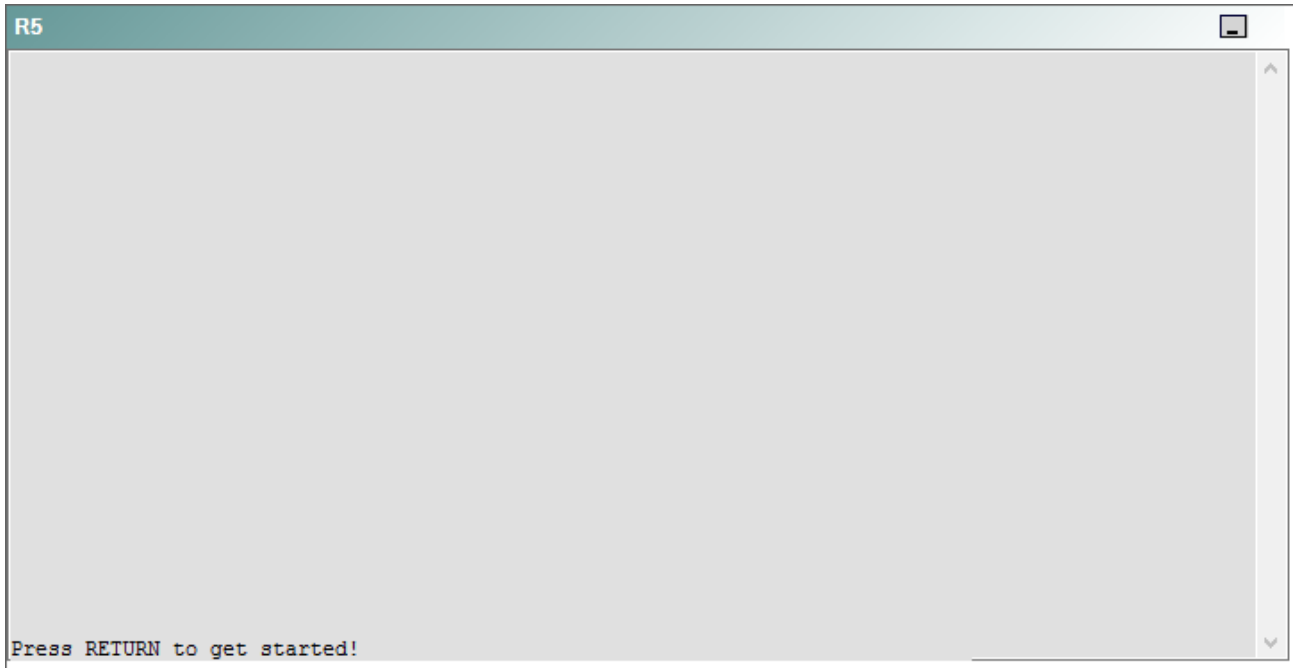

R3



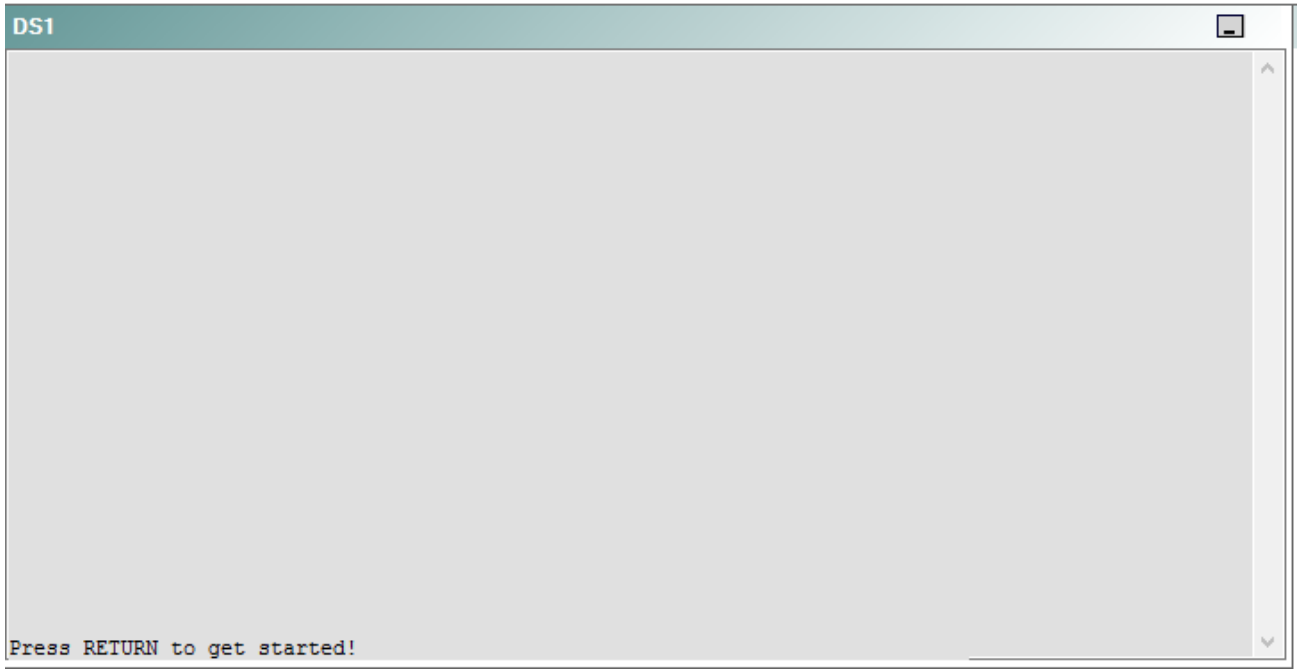

R4



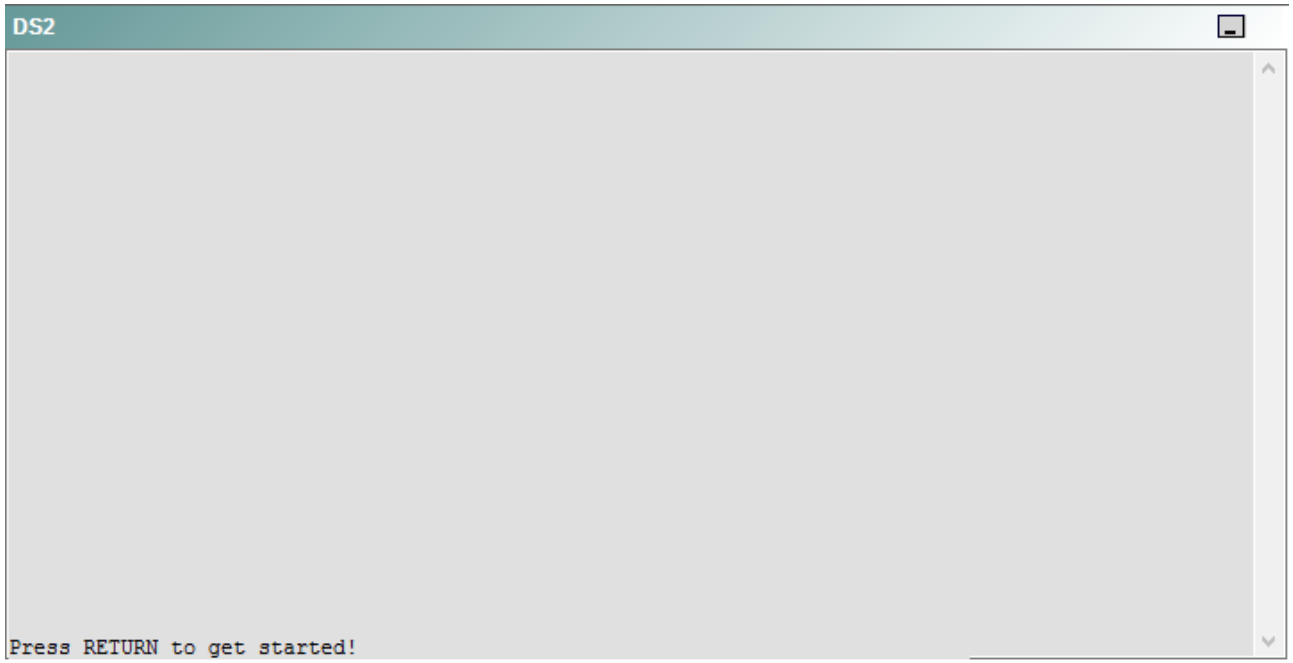

R5



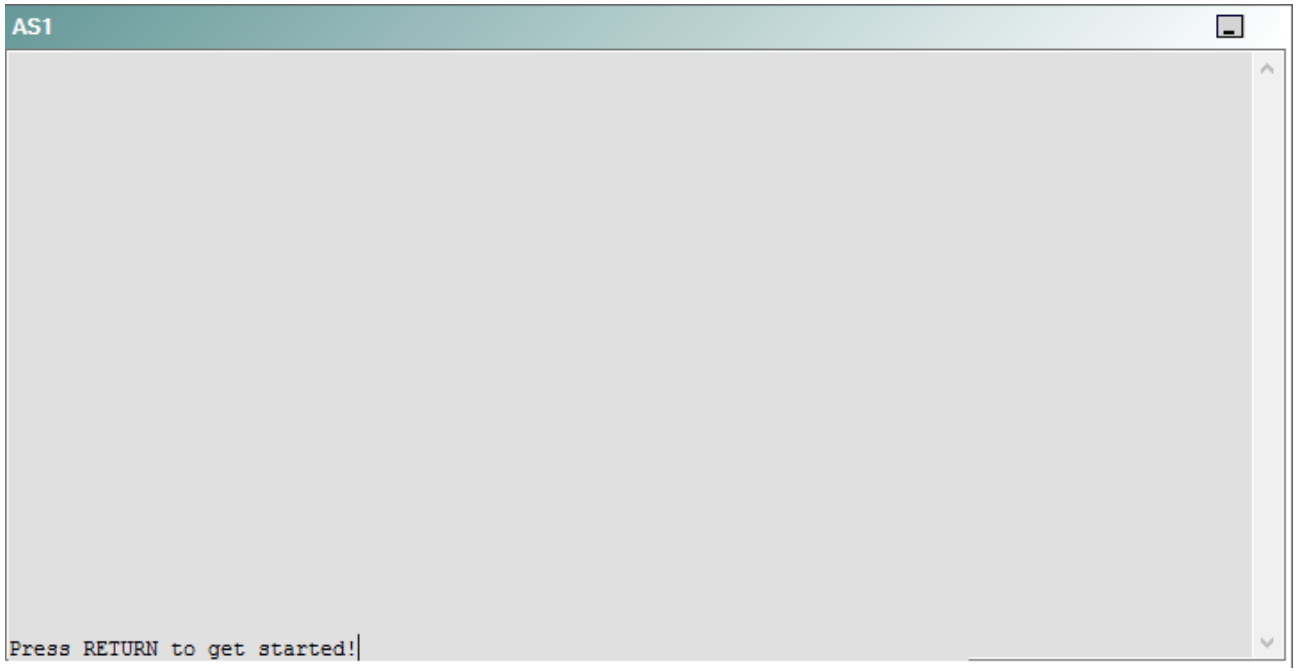

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. DHCP
C. Layer 3 addressing
D. Layer 3 security
E. Layer 2 security
F. STP
G. Etherchannel
H. VLAN configuration
I. interface

**Correct Answer:** H

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 51**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

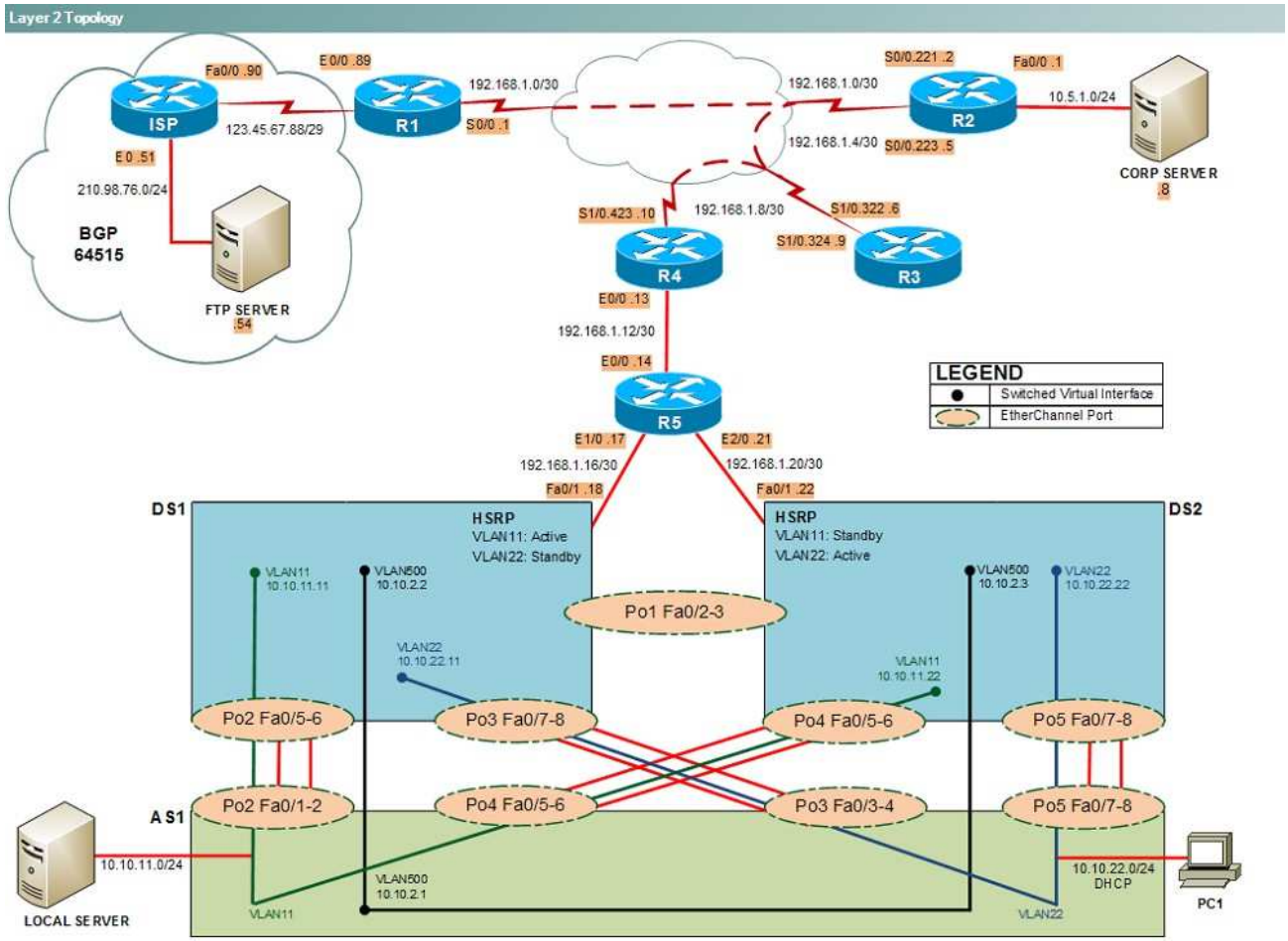
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

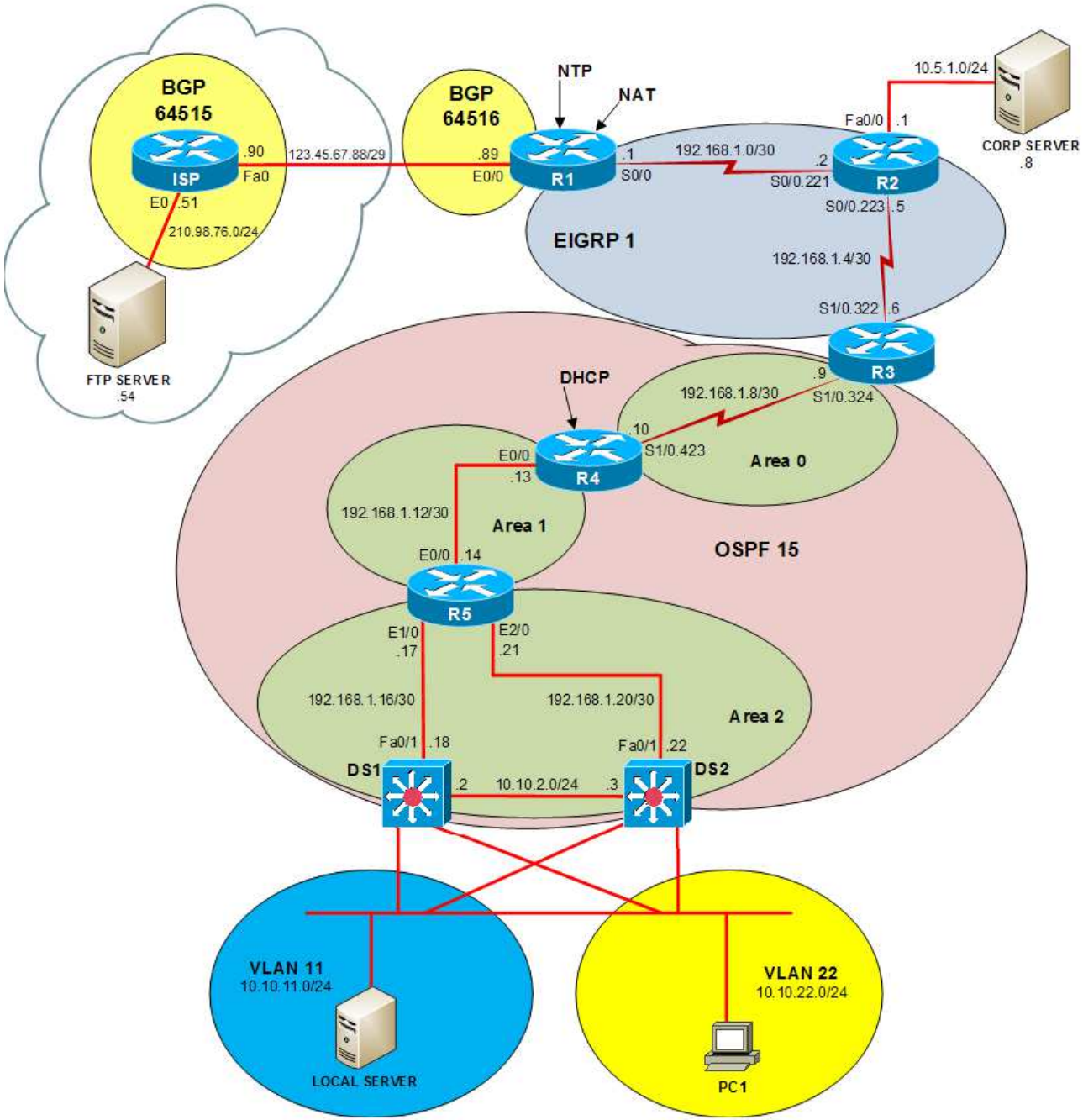
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

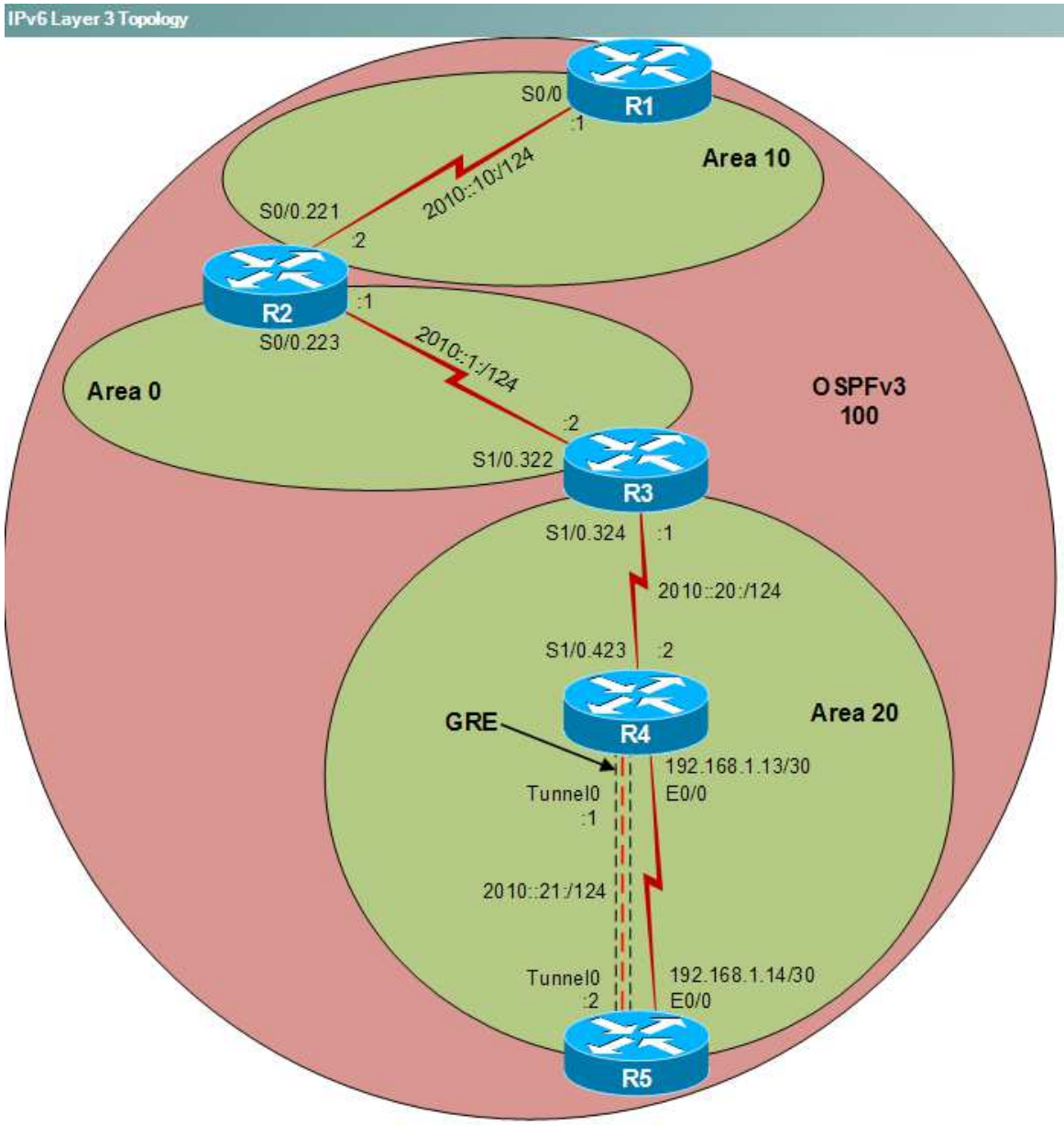
**Layer 2 Topology**




IPv4 layer 3 Topology

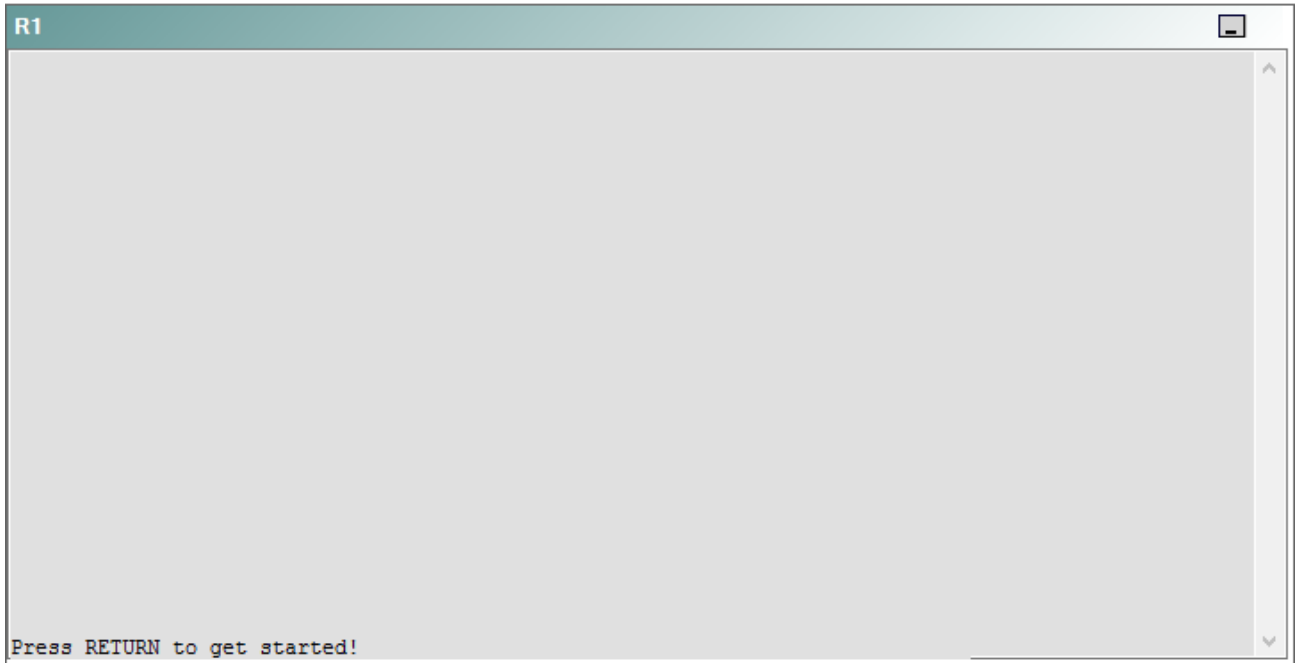

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

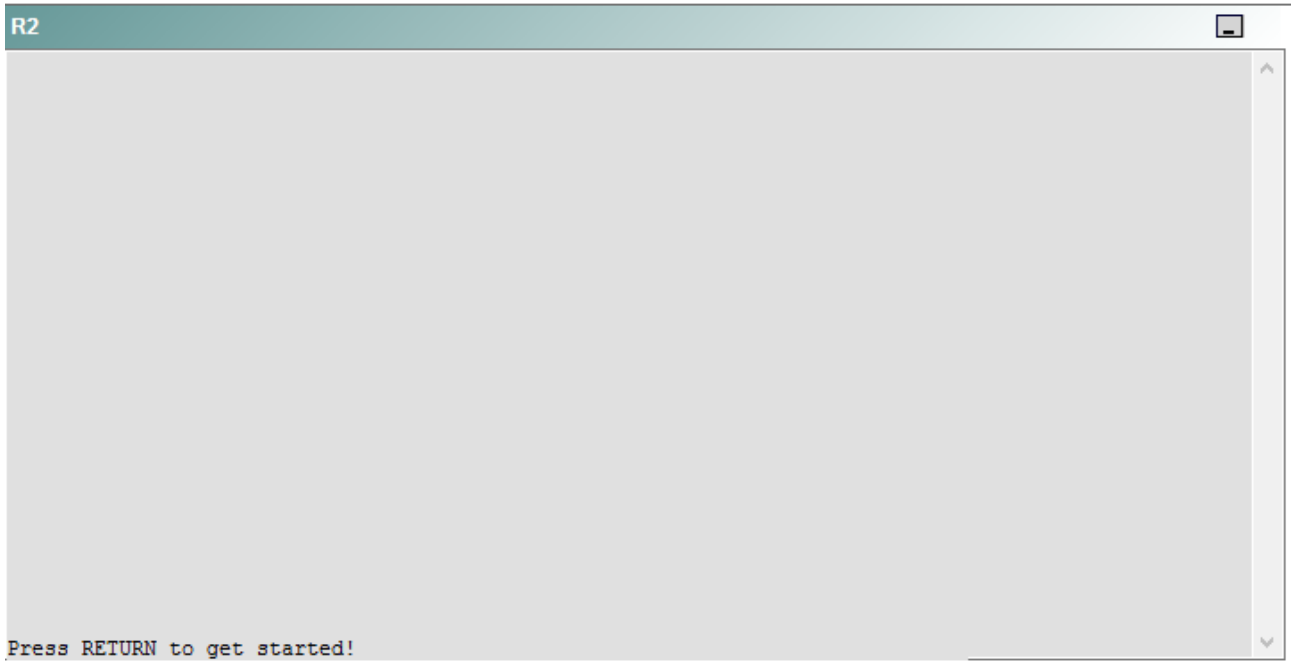



https://www.gratisexam.com/

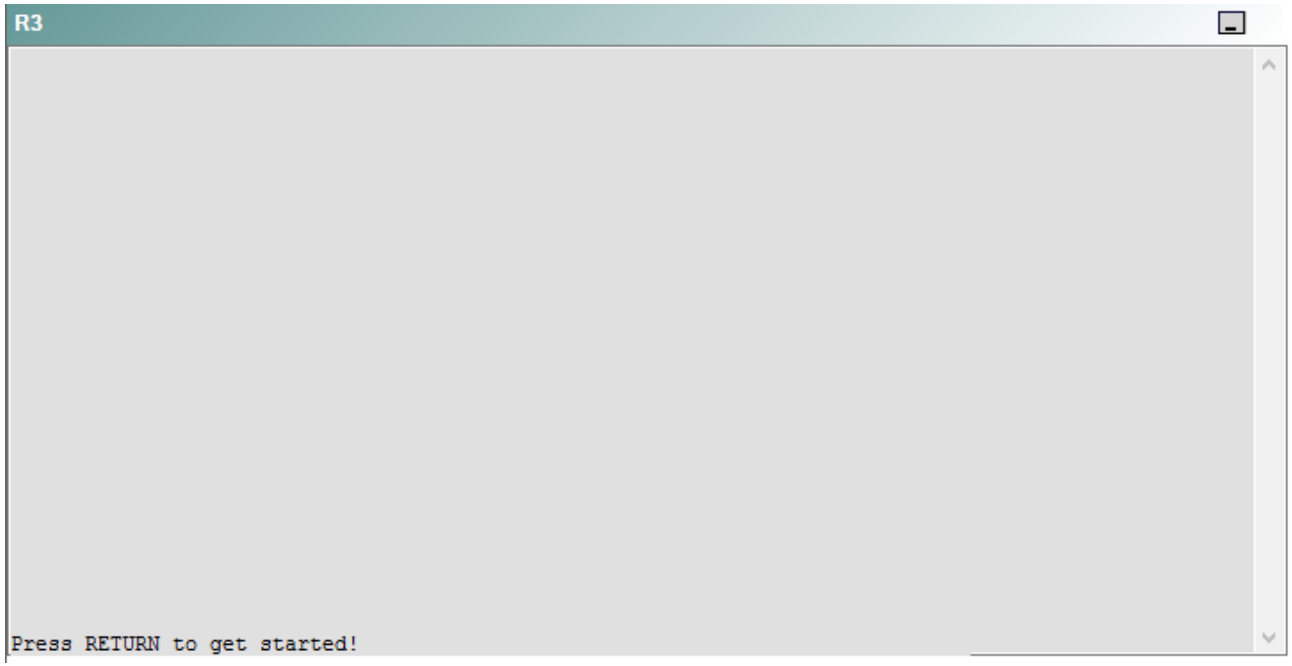
R1



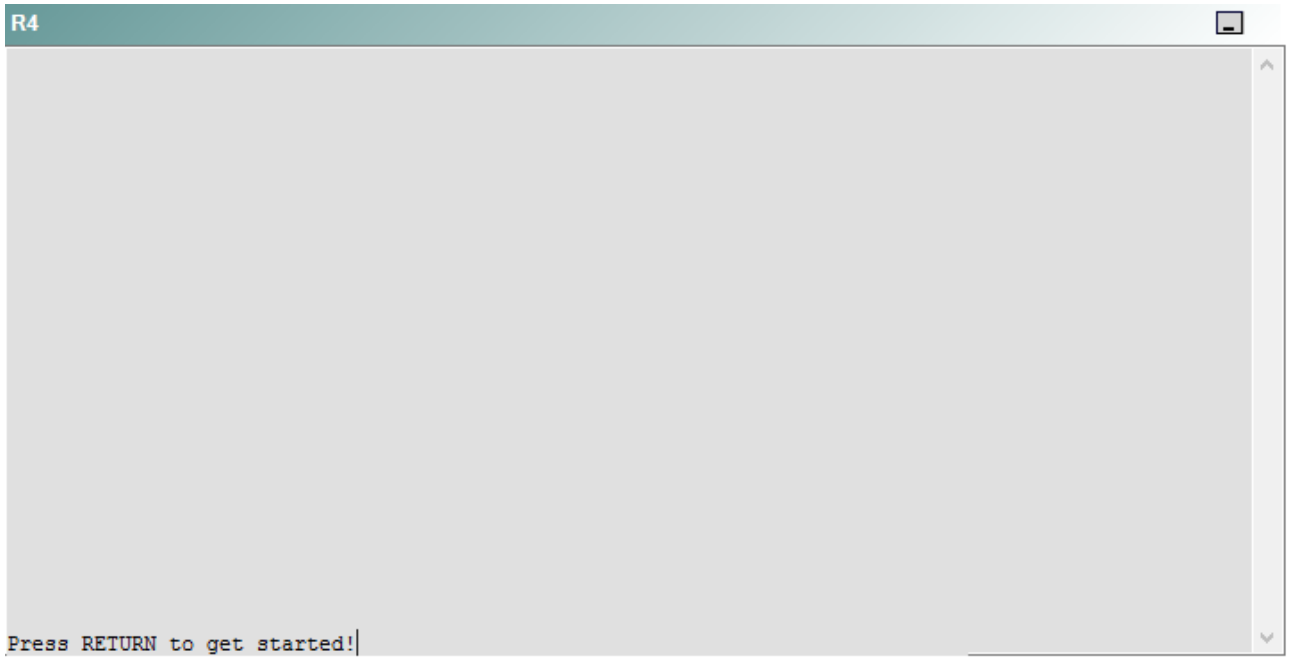

R2



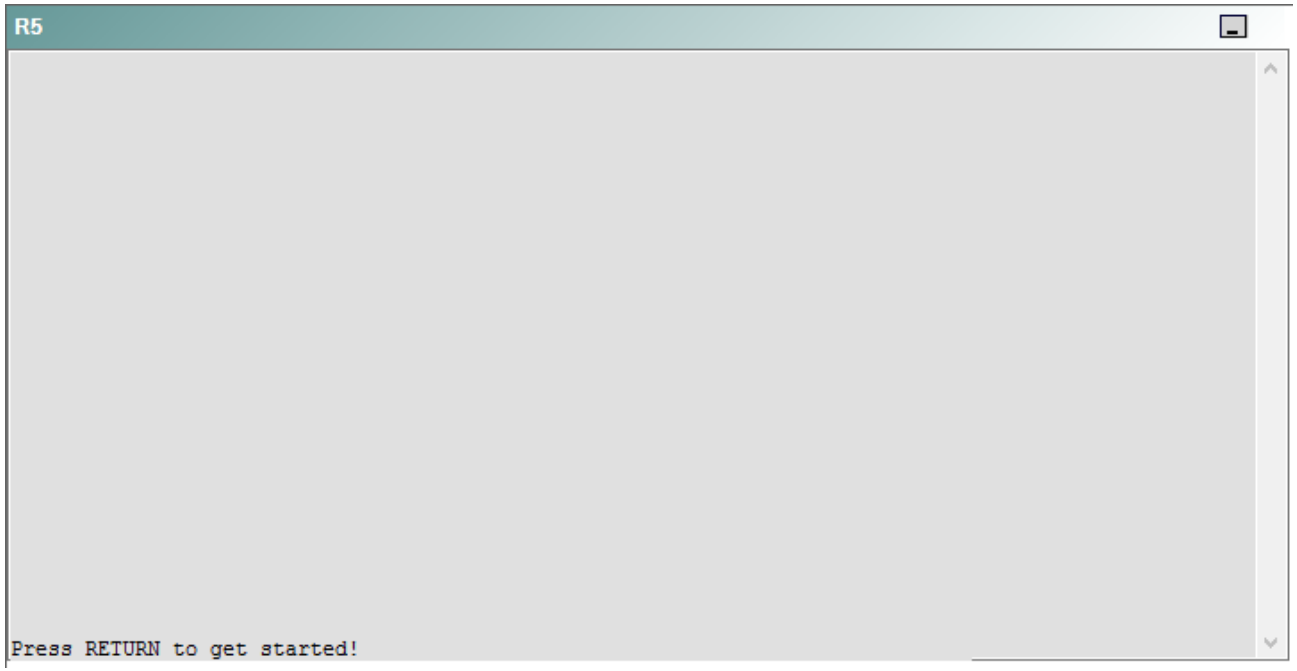

R3



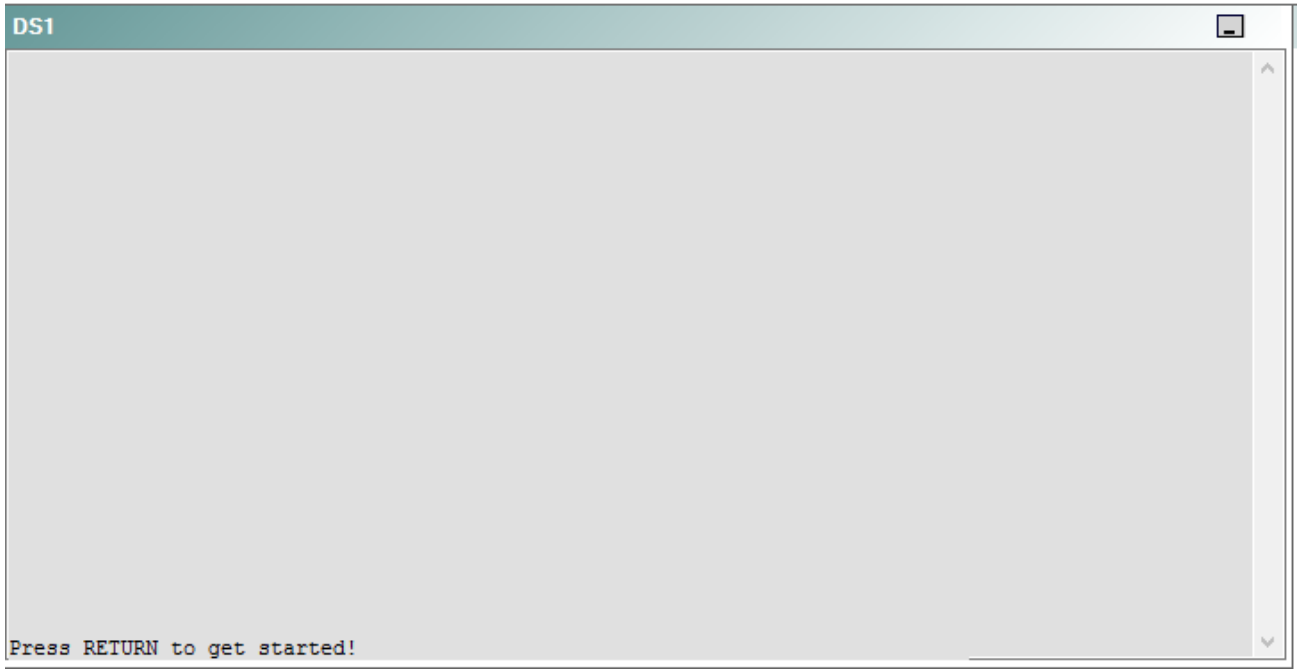

R4



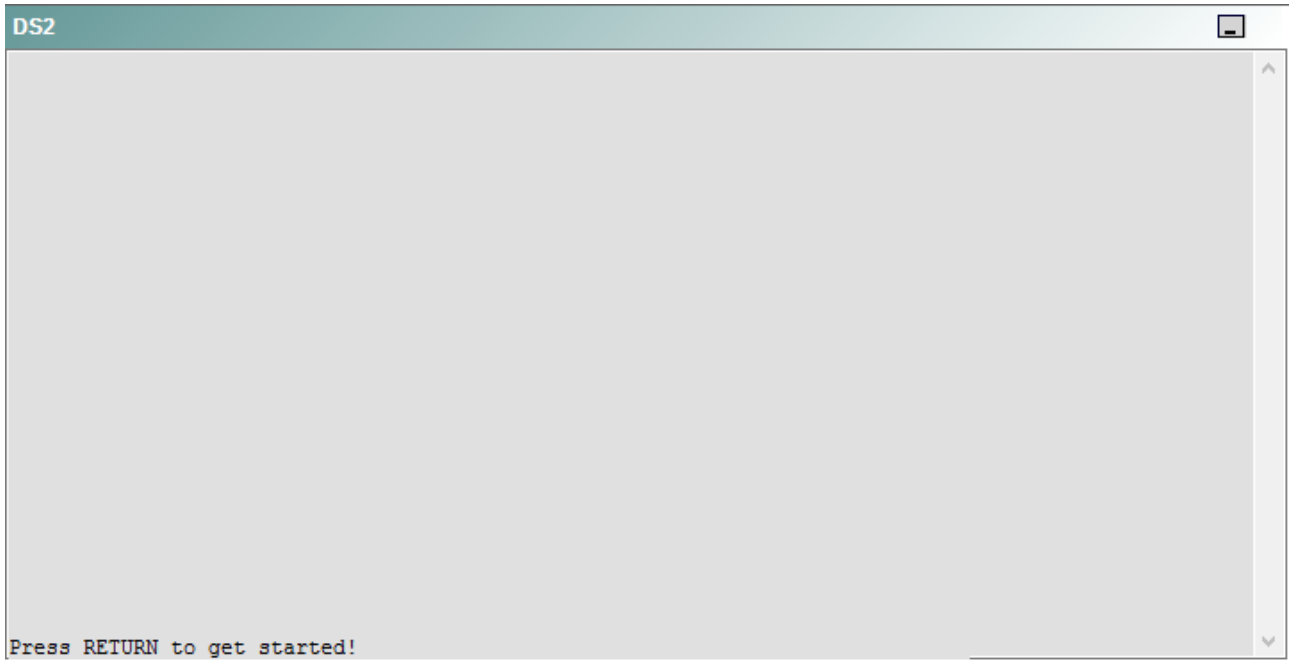

R5



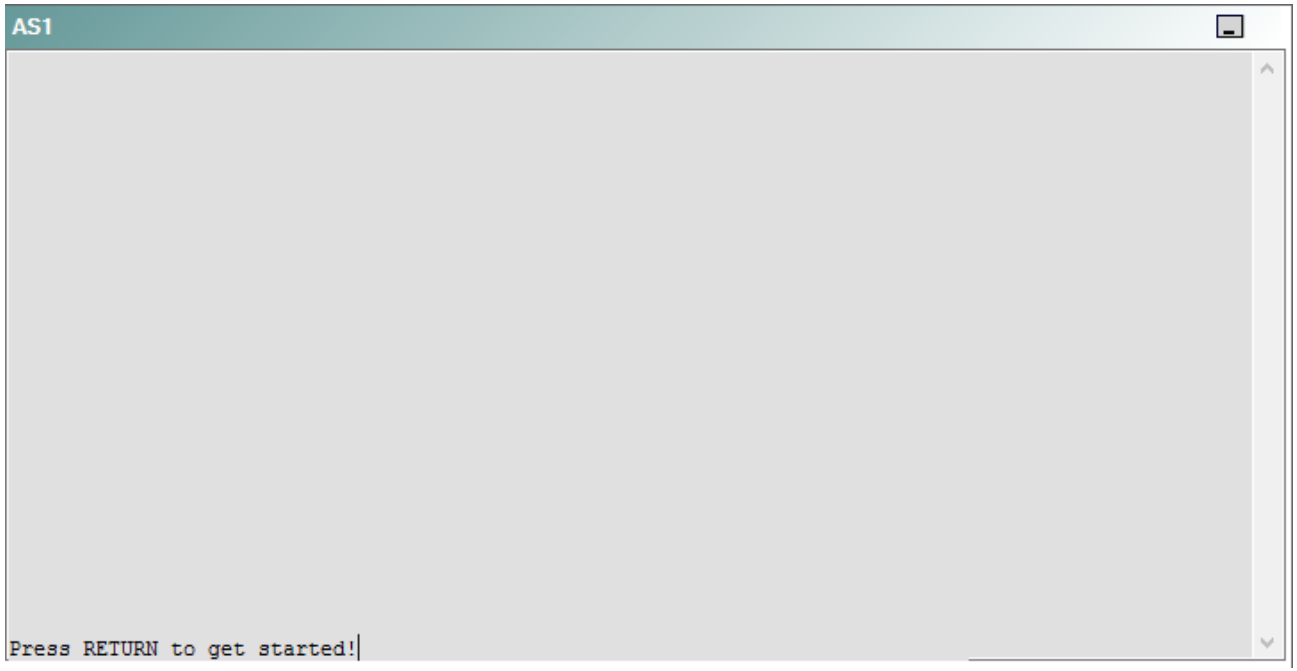

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that R5 is no longer able to ping the IPv6 address 2010::10:2 on R2.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 52**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

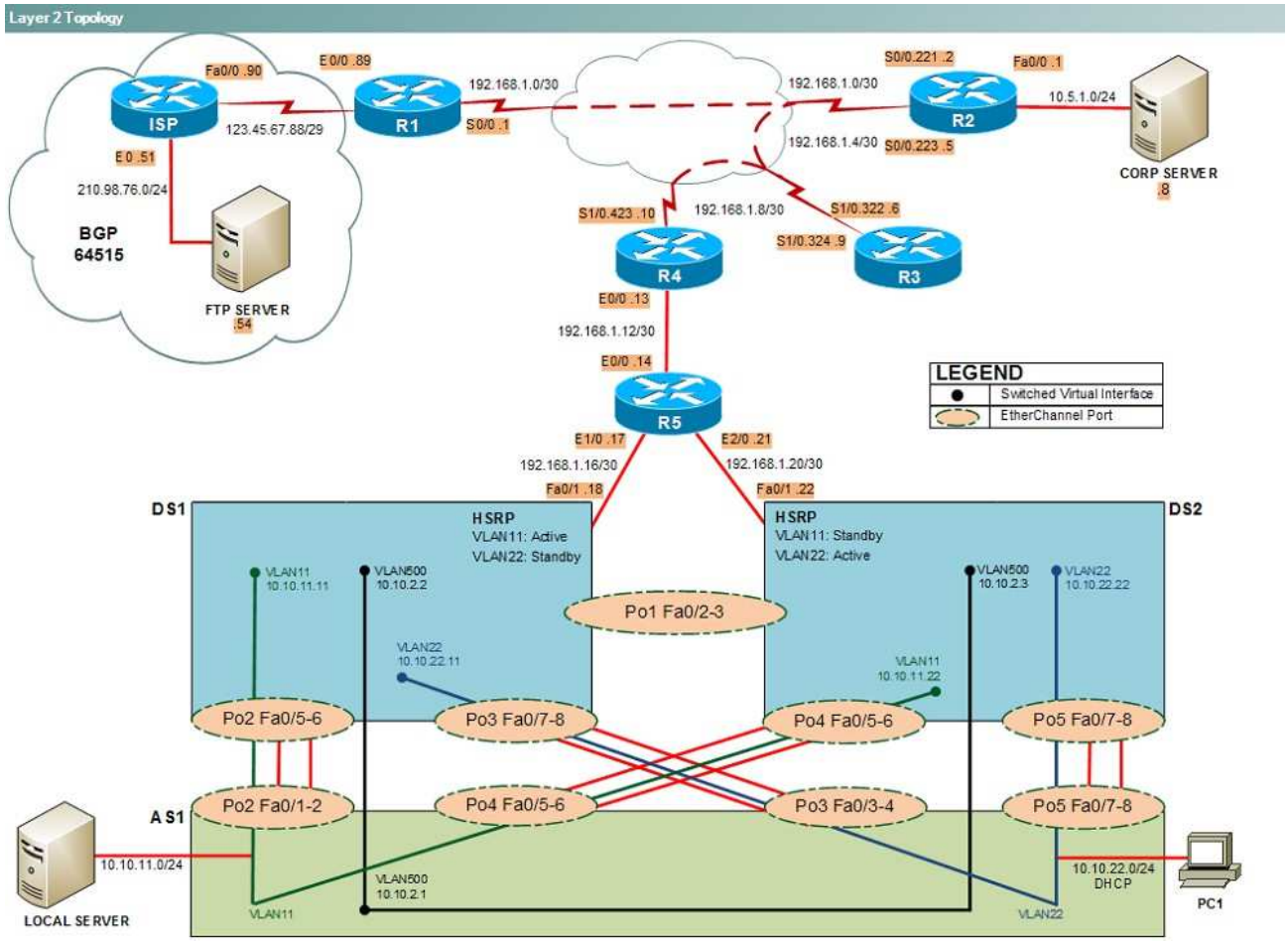
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

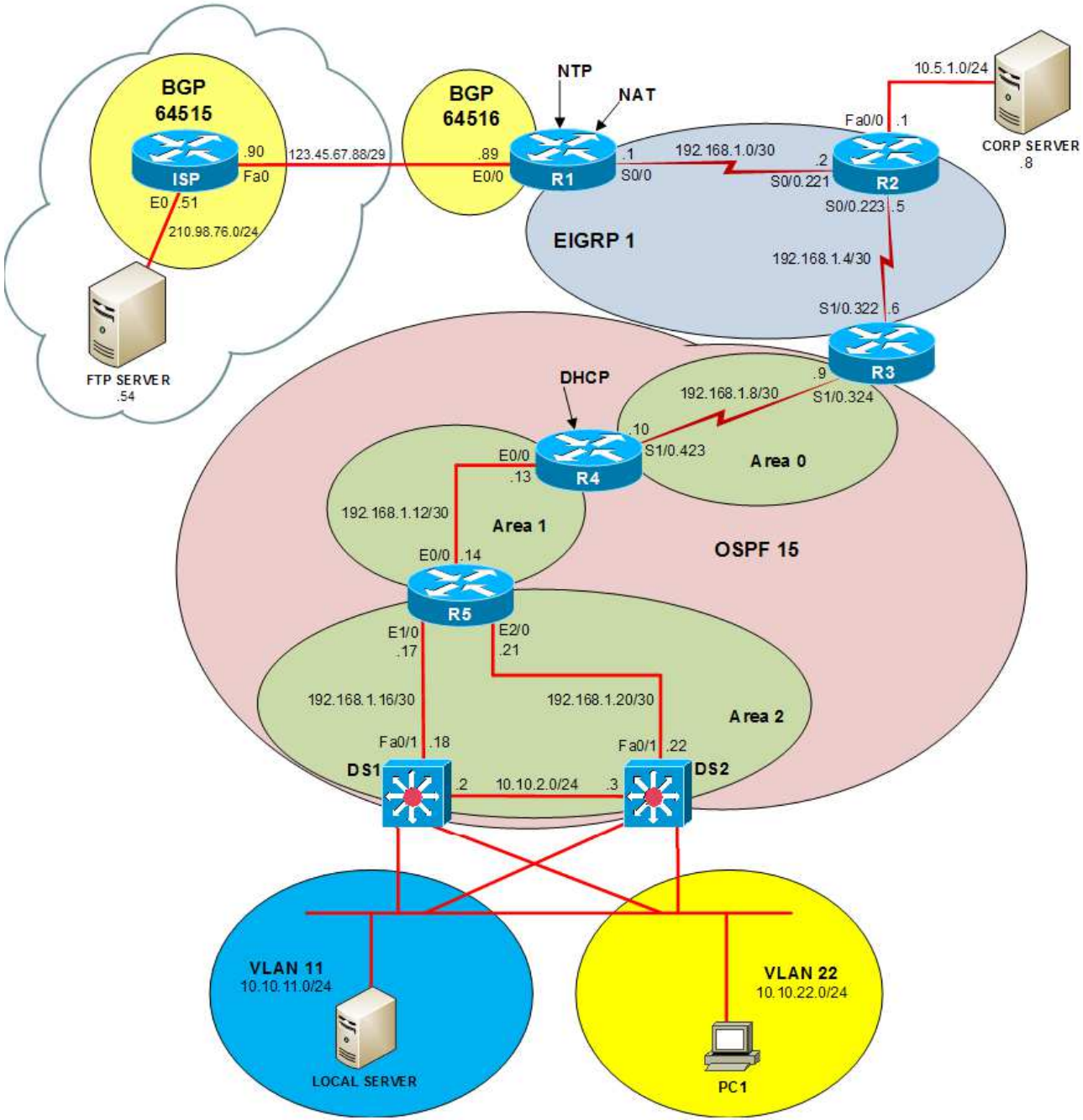
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

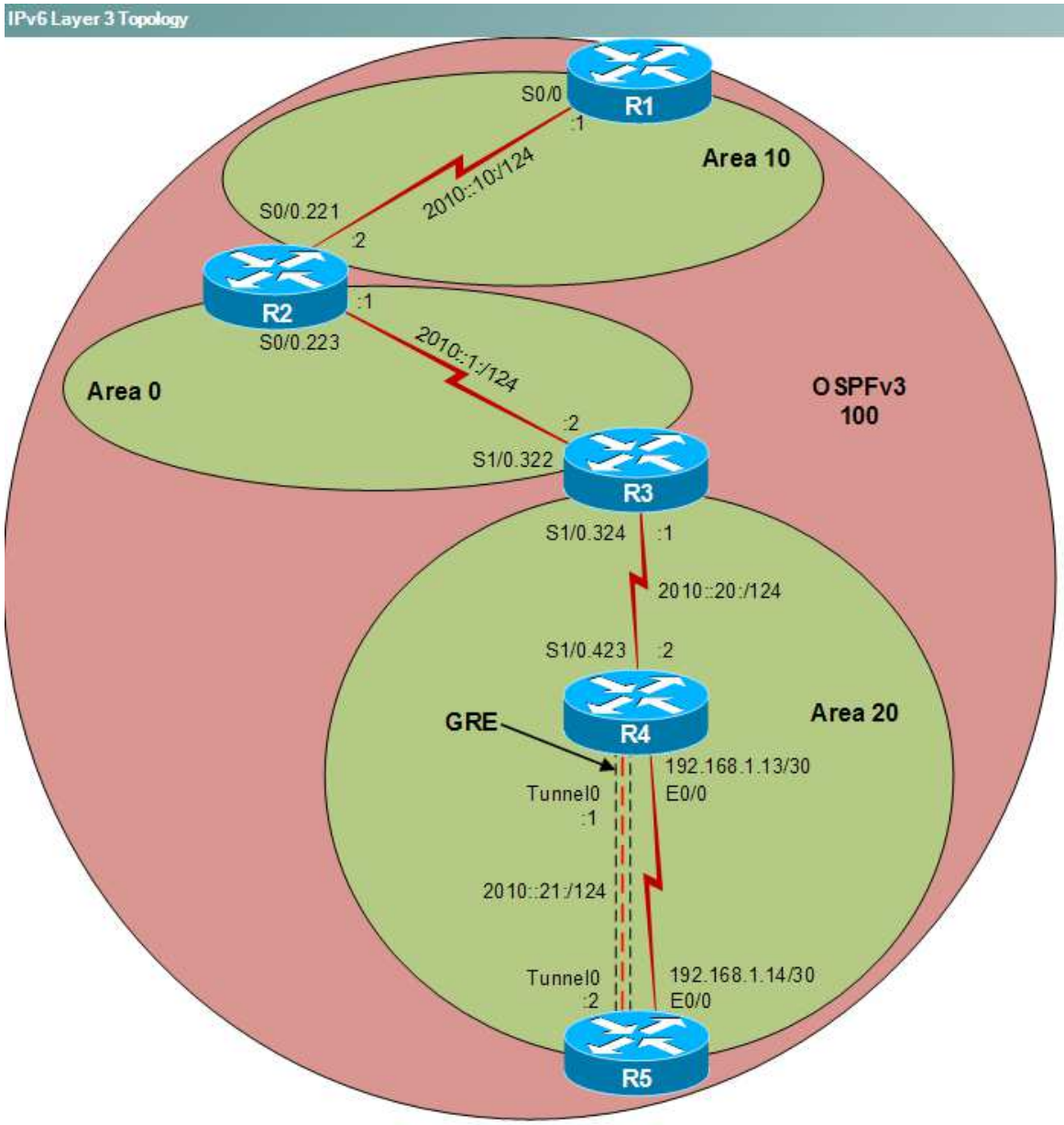
**Layer 2 Topology**




IPv4 layer 3 Topology

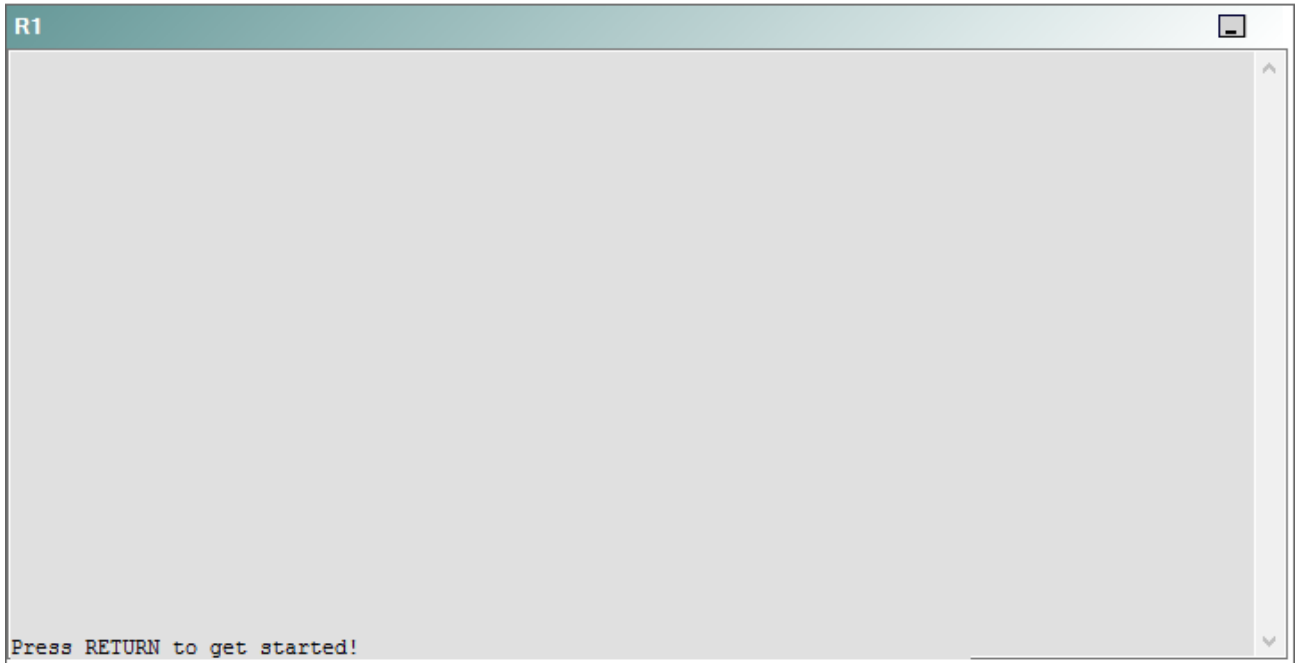

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

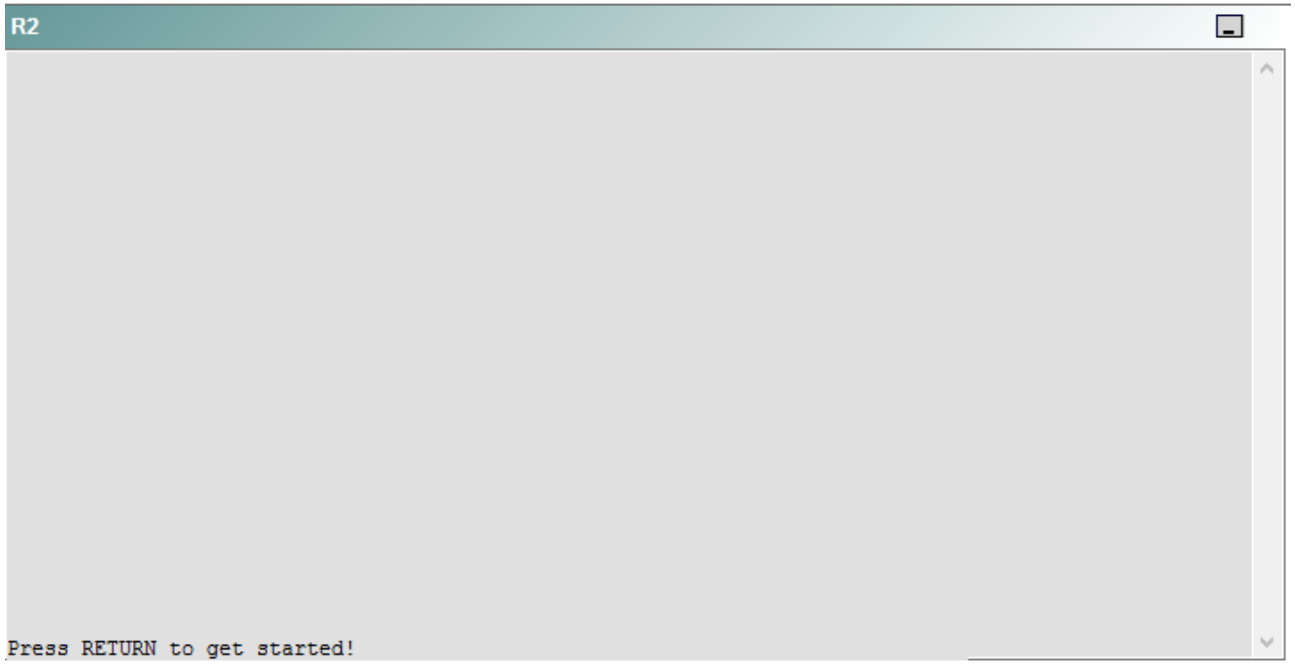



https://www.gratisexam.com/

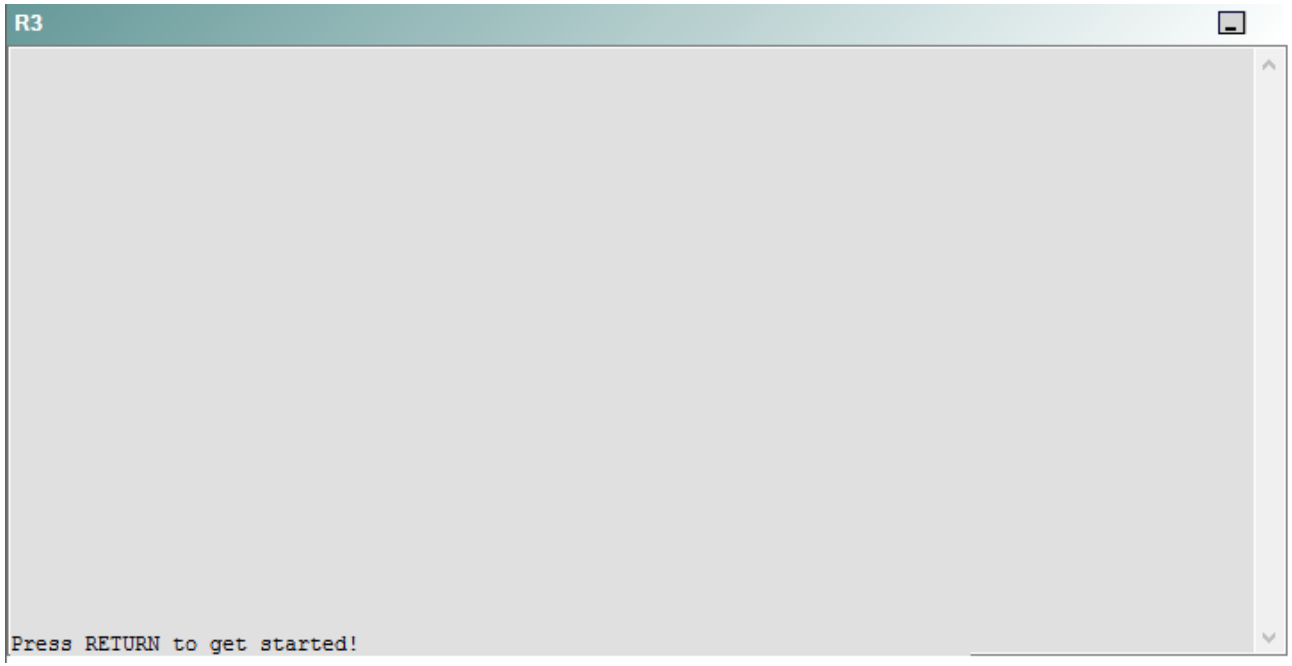
R1



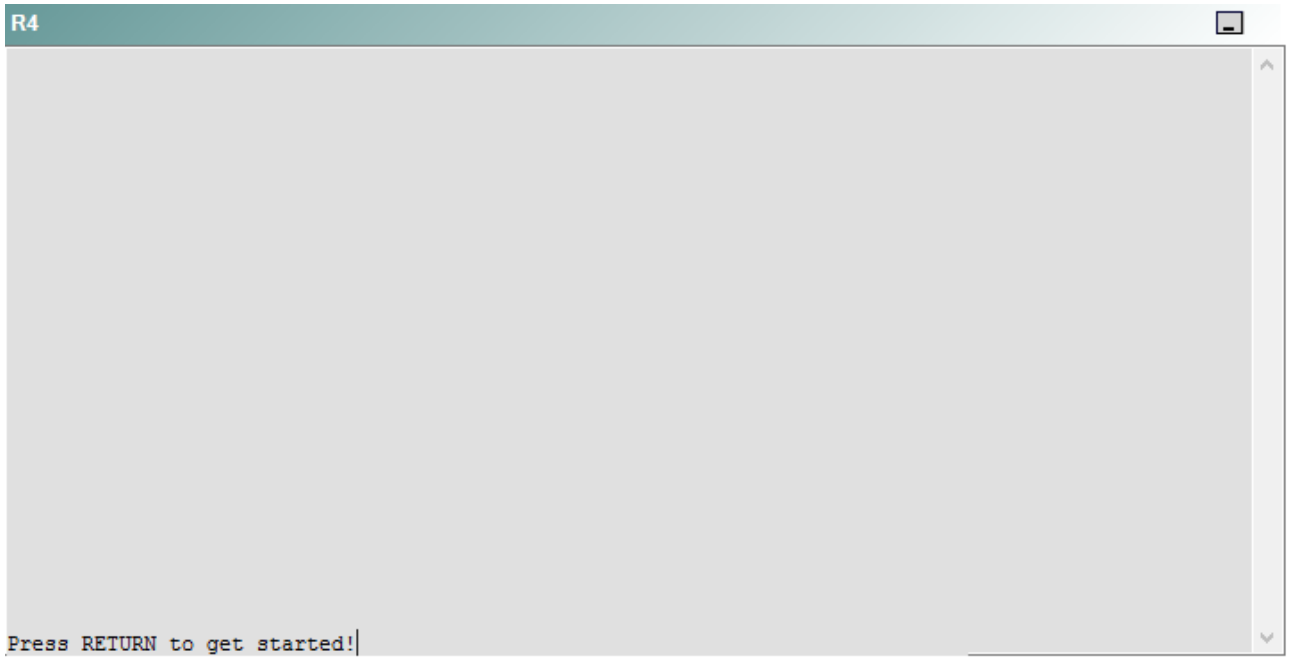

R2



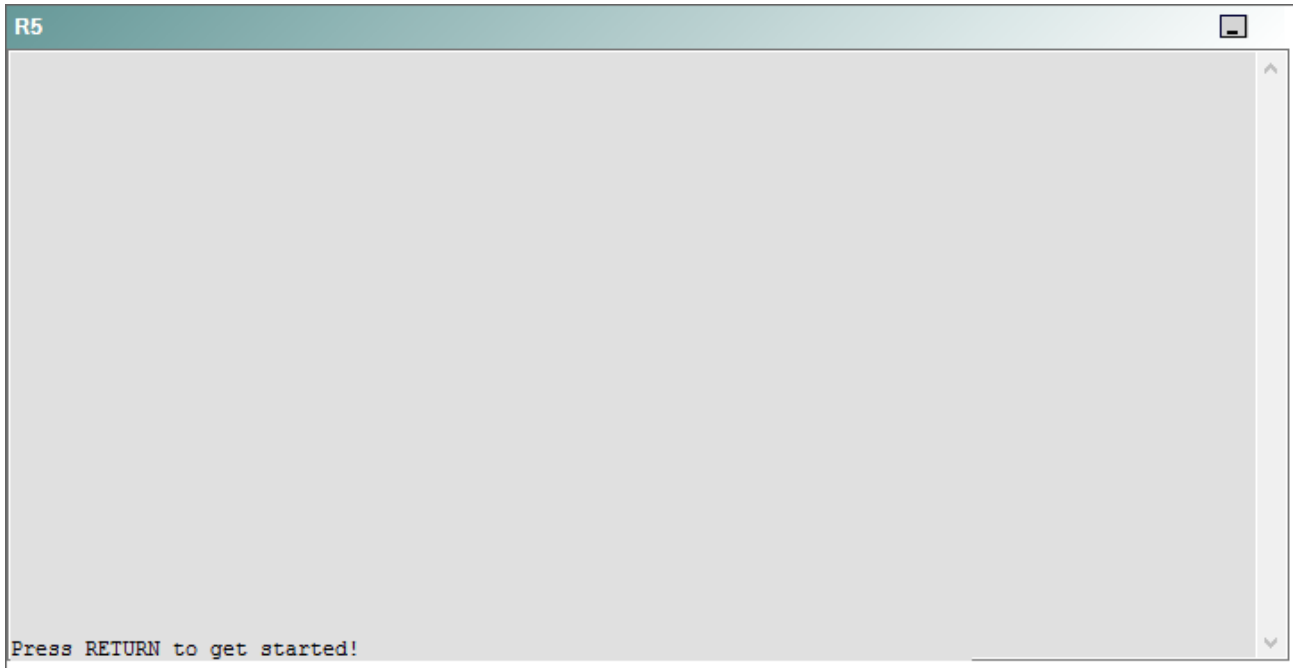

R3



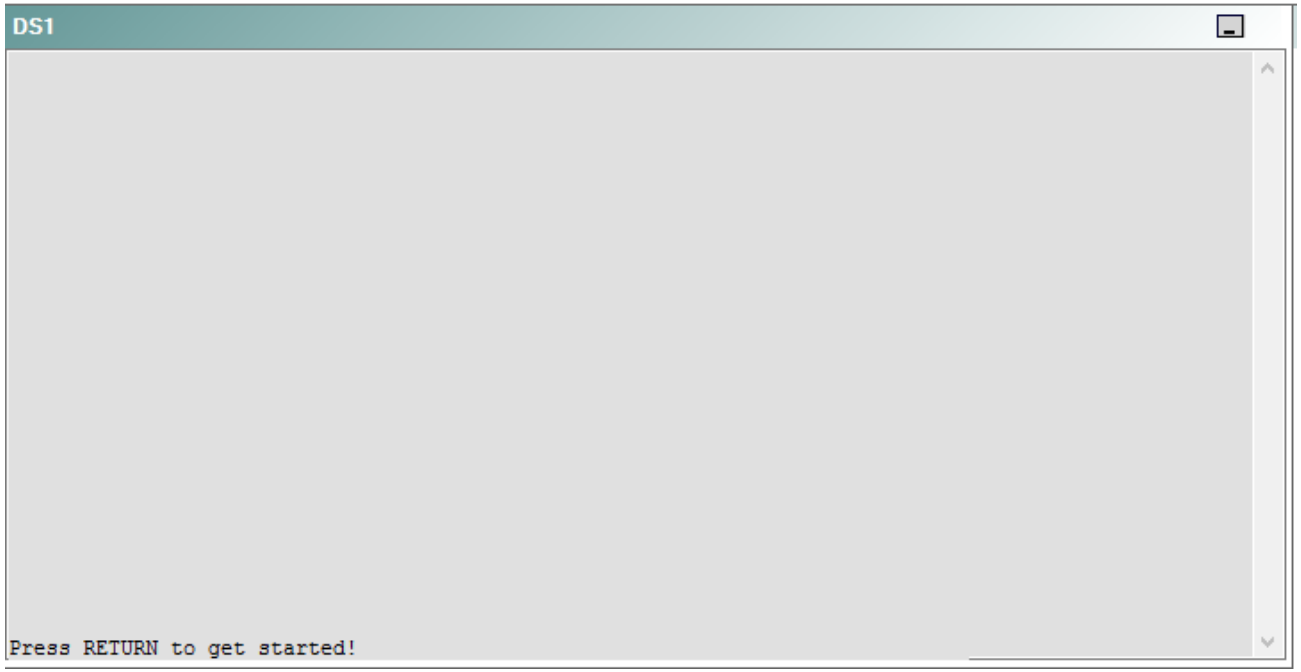

R4



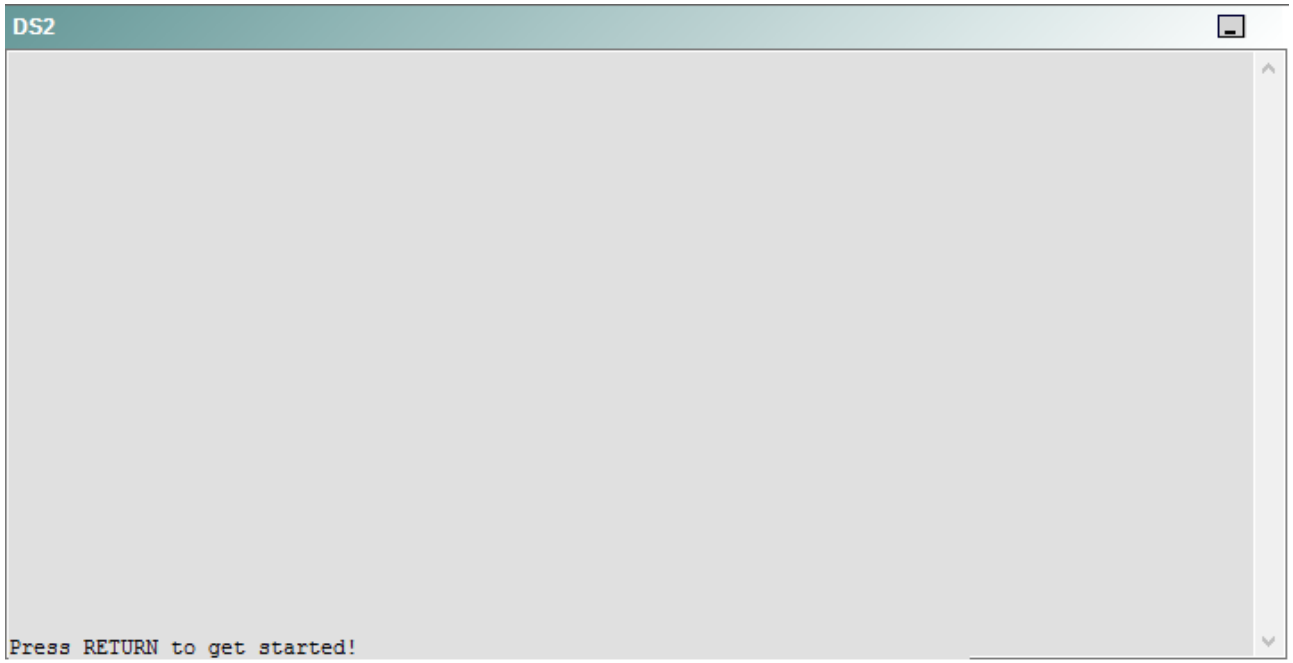

R5



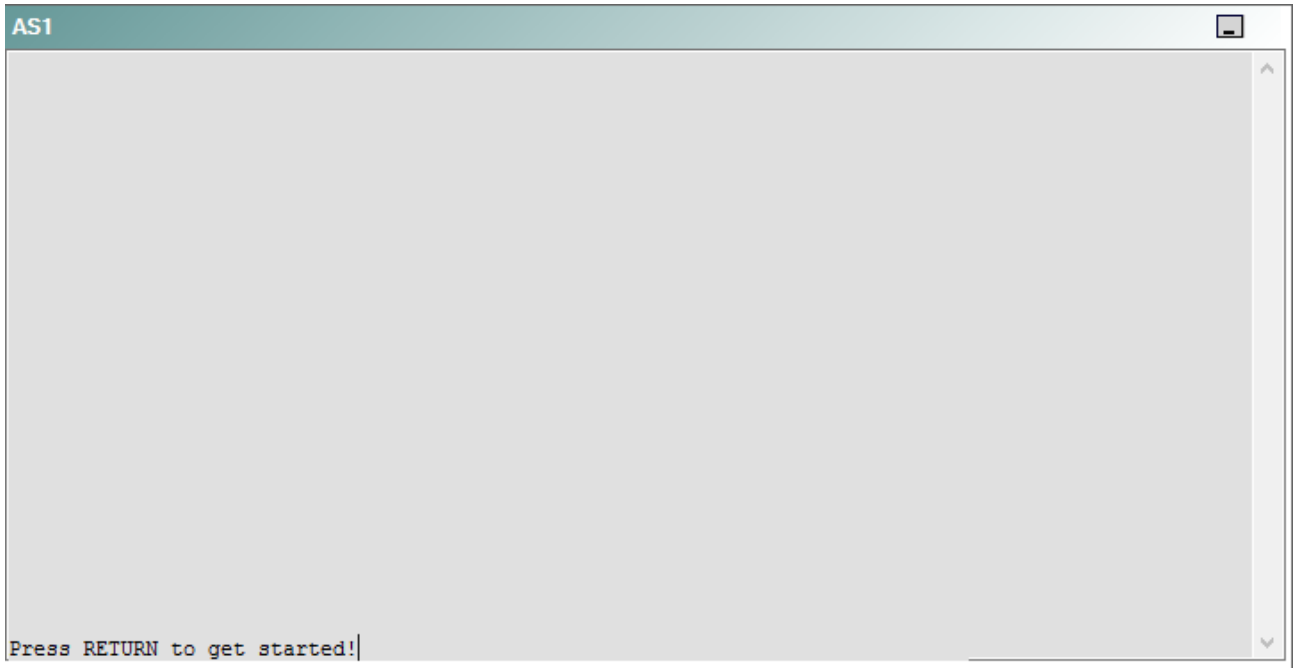

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that R5 is no longer able to ping the IPv6 address 2010::10:2 on R2.

Which of the following technologies is the source of the problem?

A. NTP
B. GRE
C. OSPFv2
D. OSPFv3
E. redistribution
F. DHCP
G. Layer 3 addressing
H. interface

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 53**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

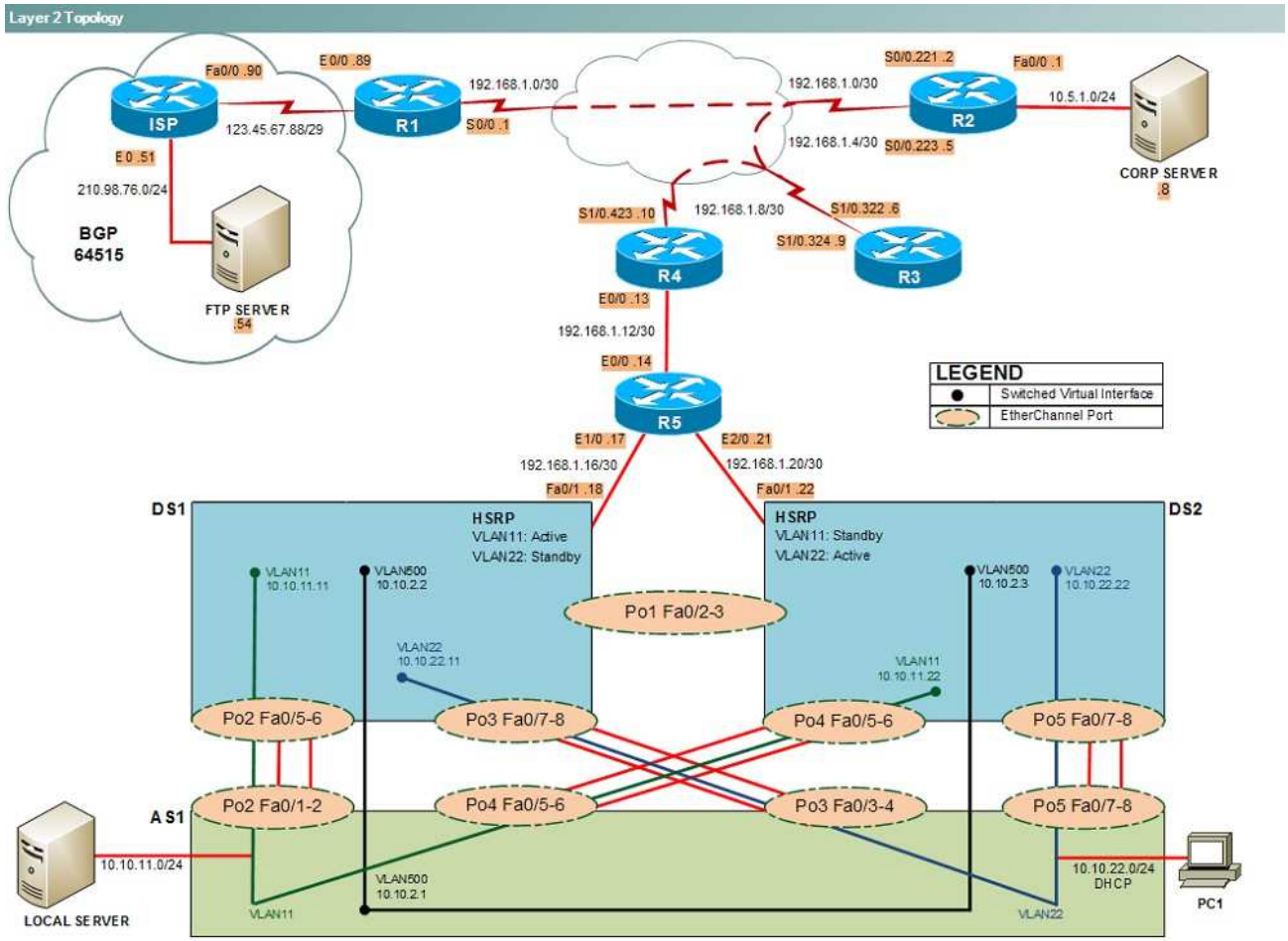
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

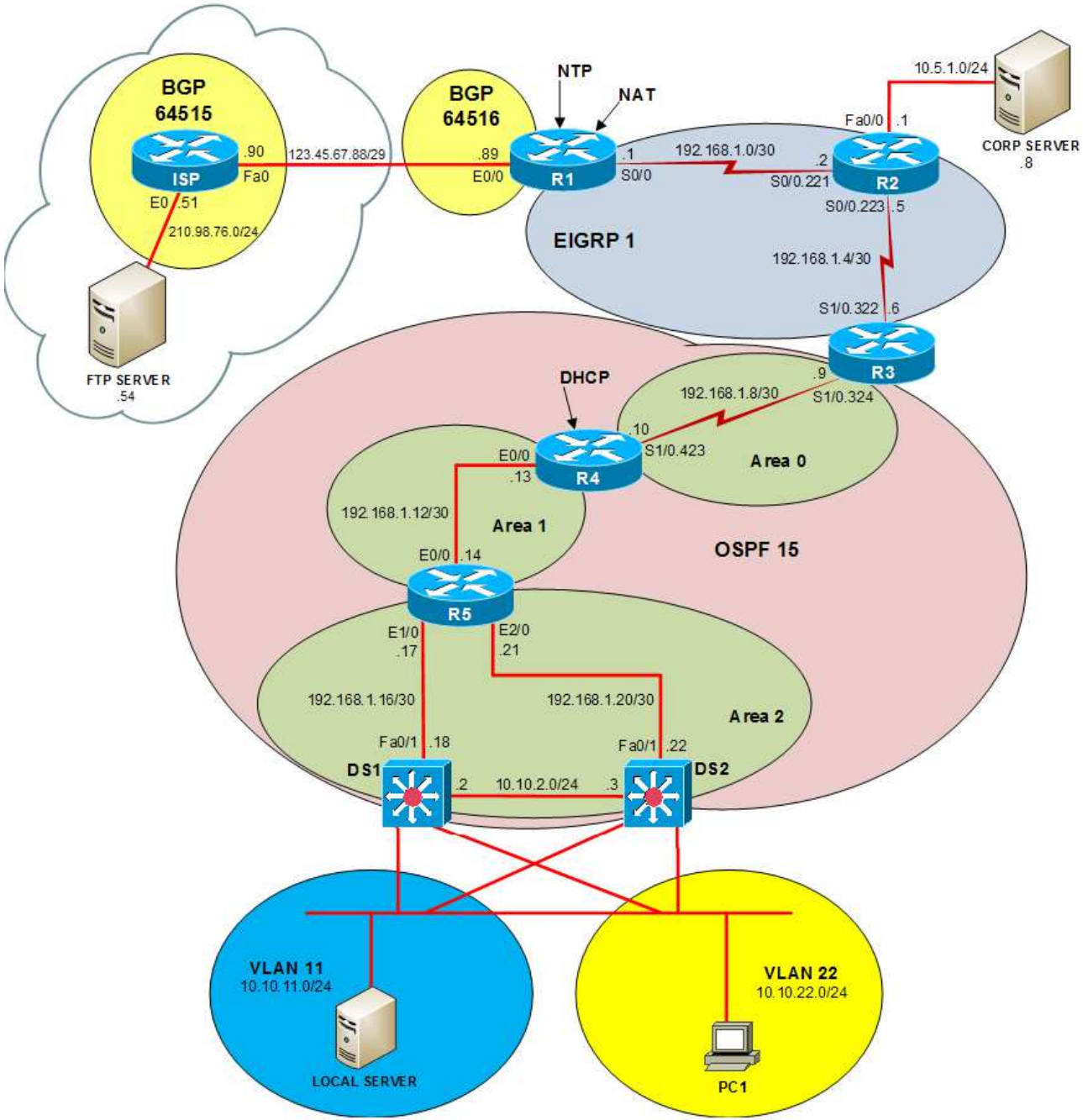
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

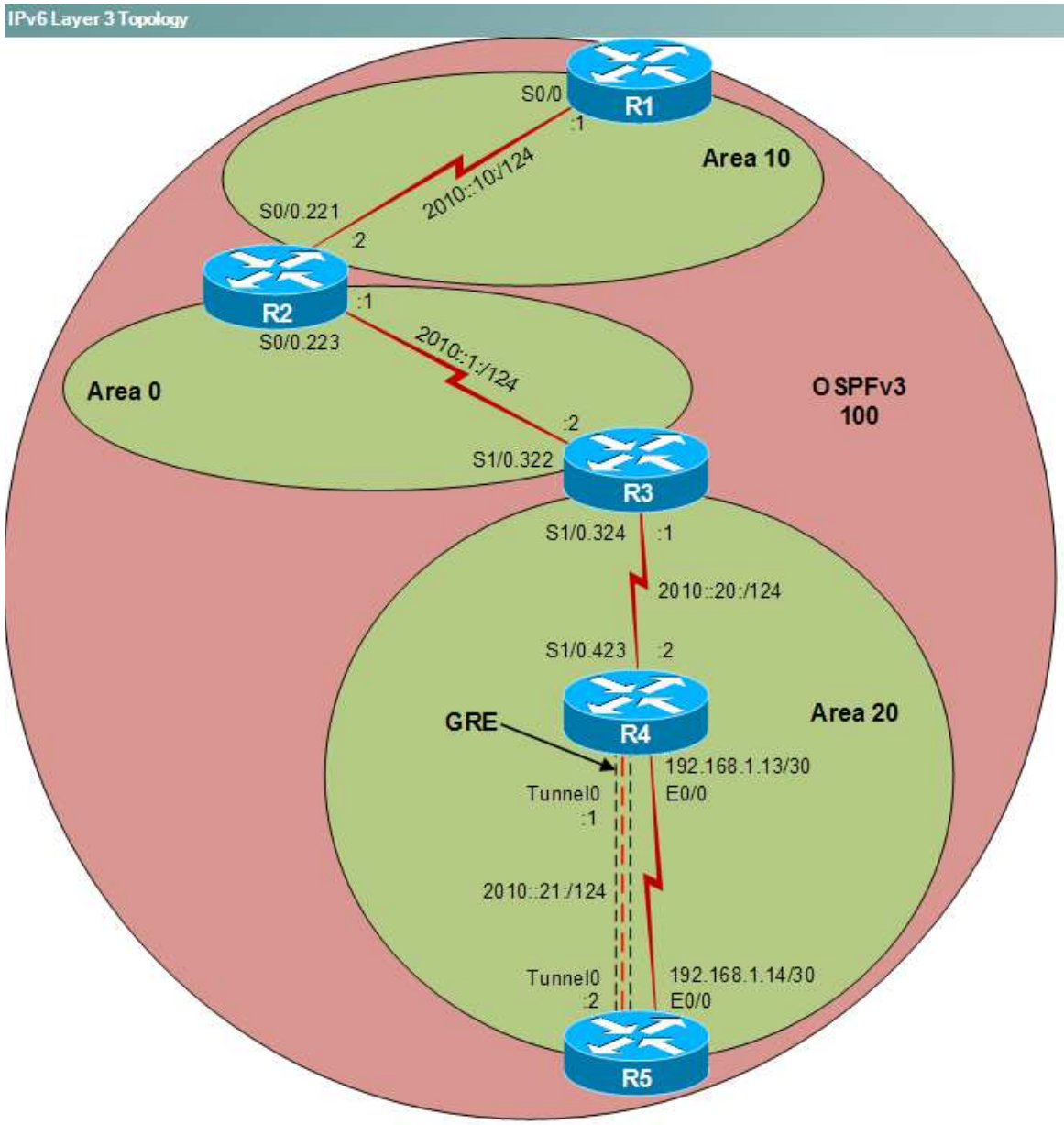
**Layer 2 Topology**




IPv4 layer 3 Topology

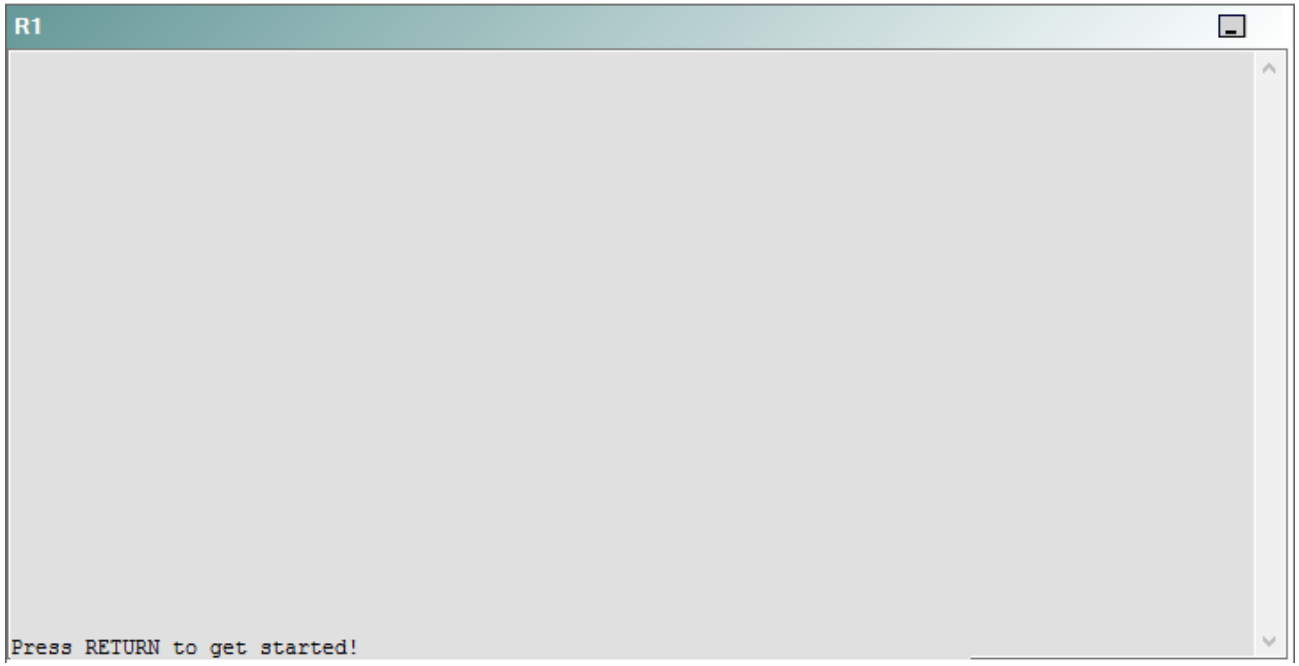

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

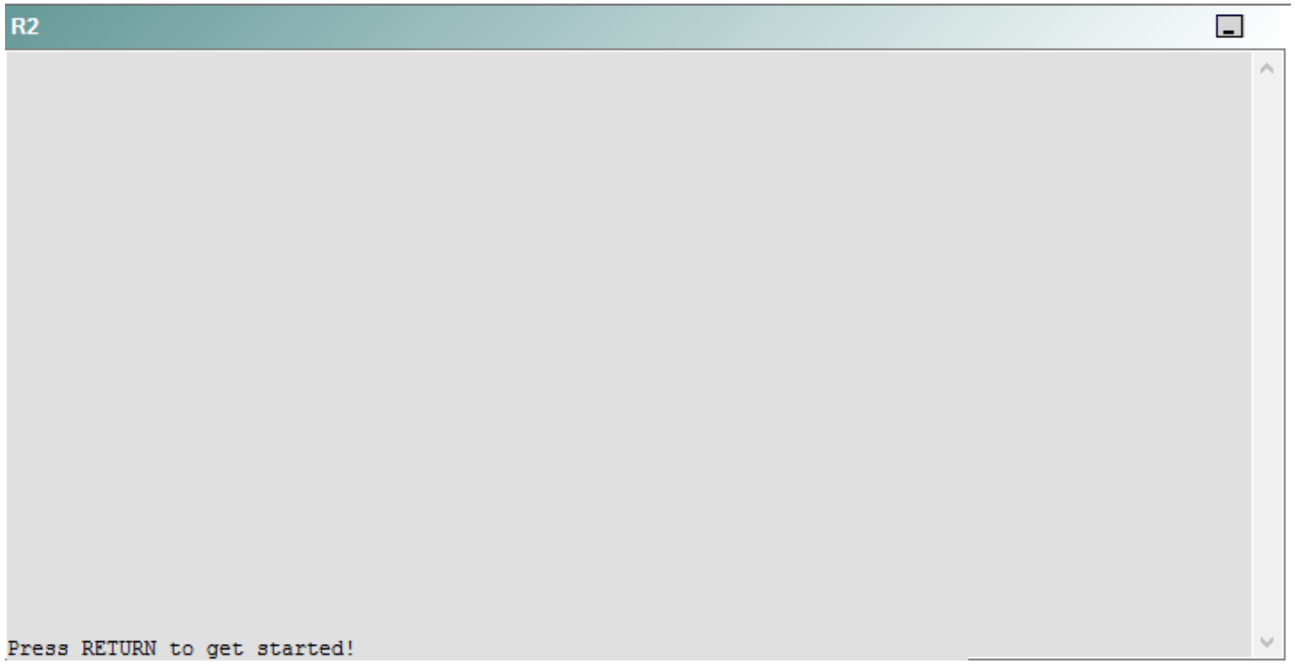



https://www.gratisexam.com/

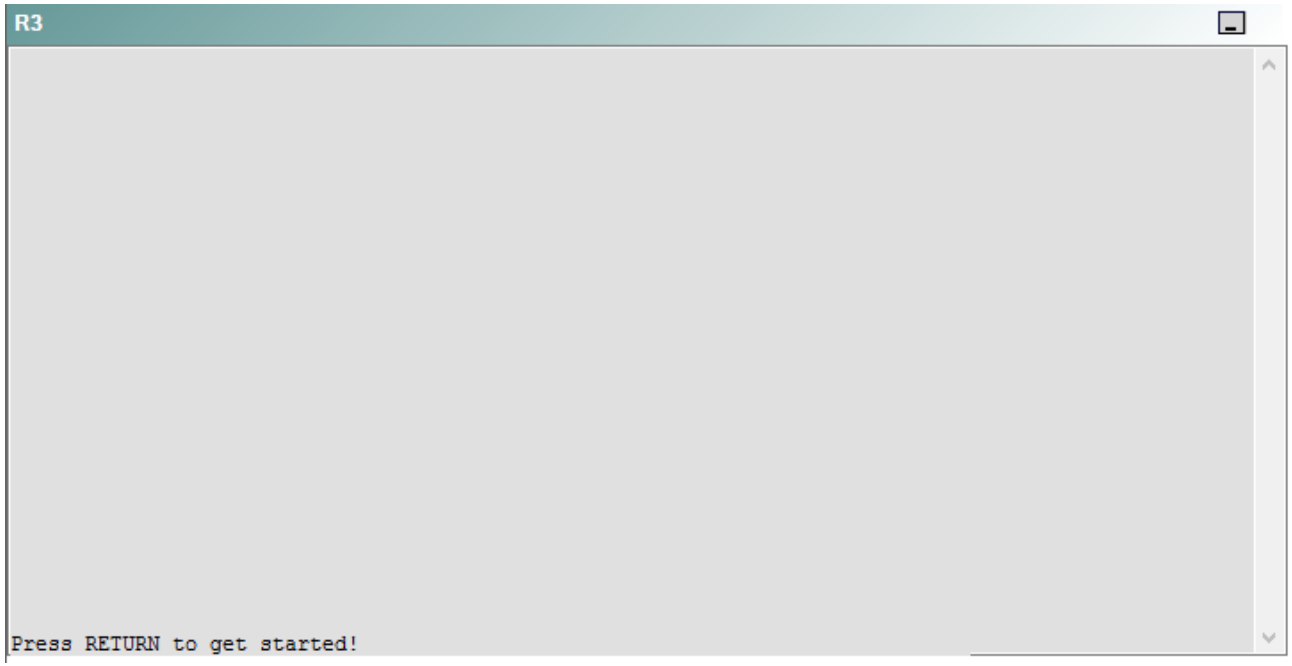
R1



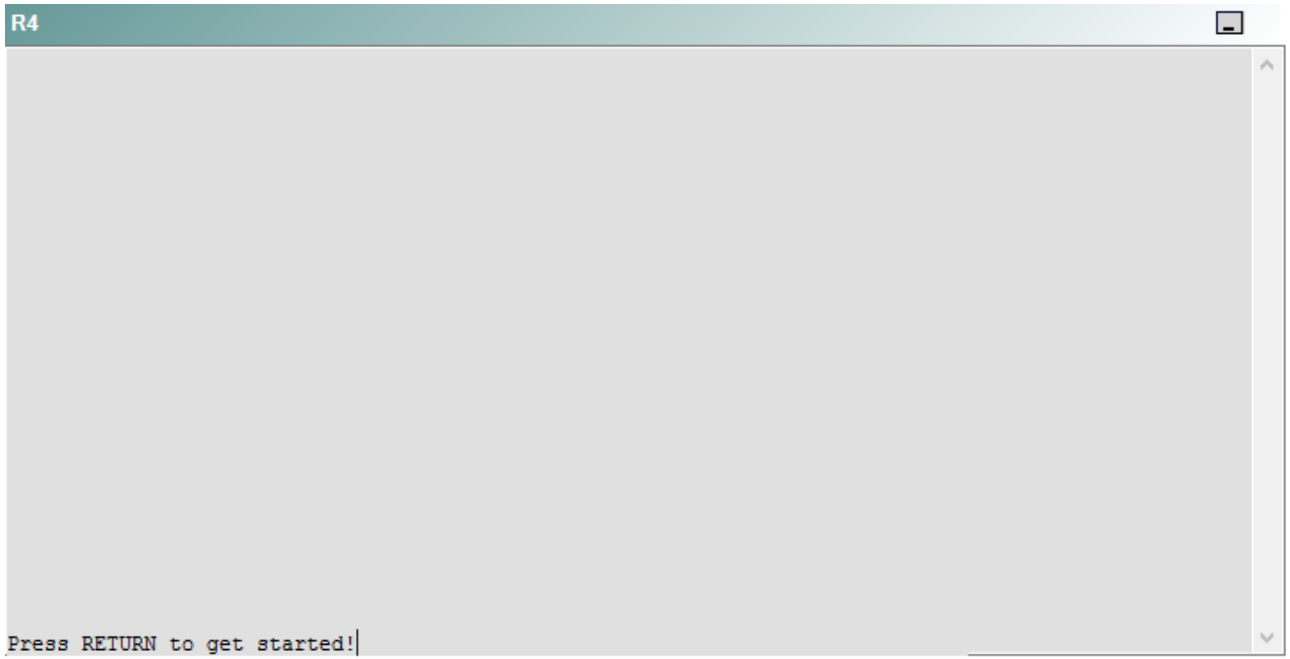

R2



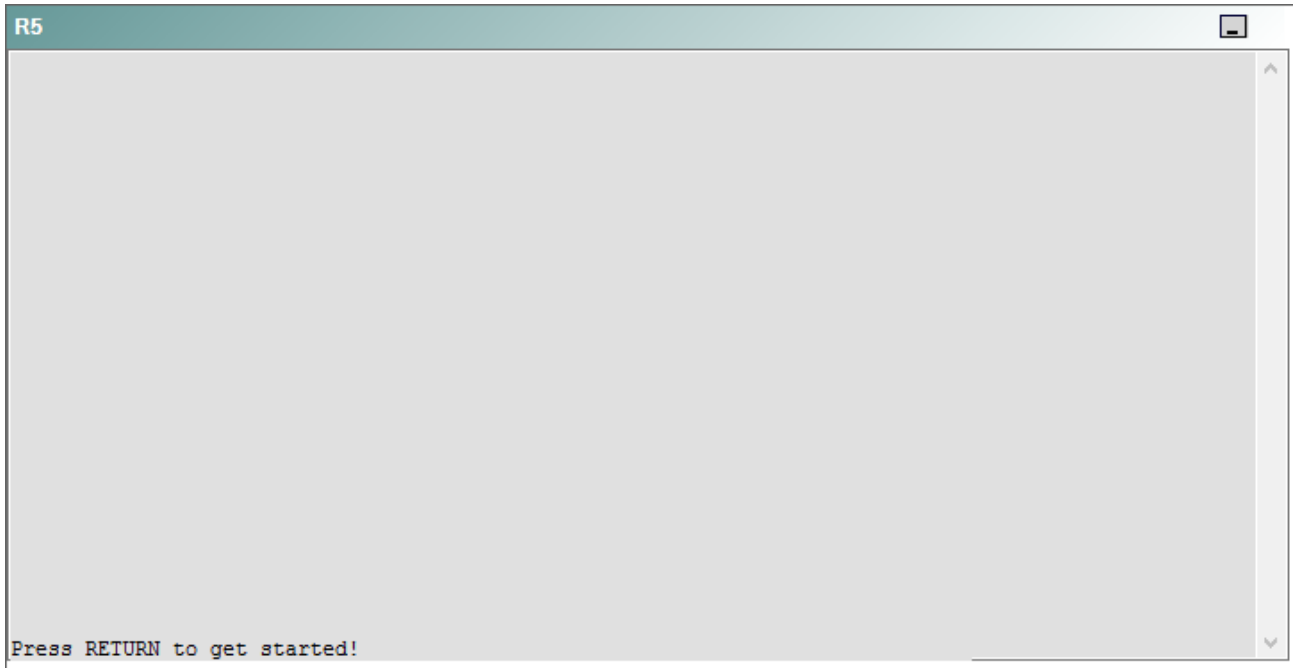

R3



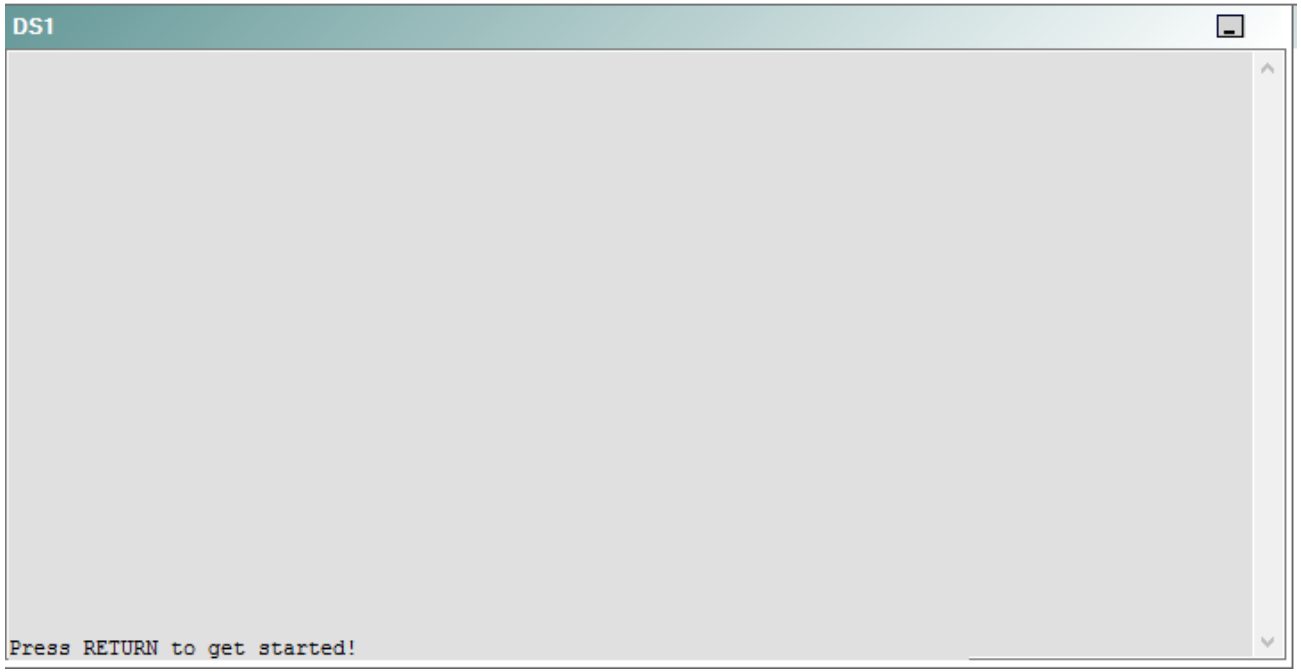

R4



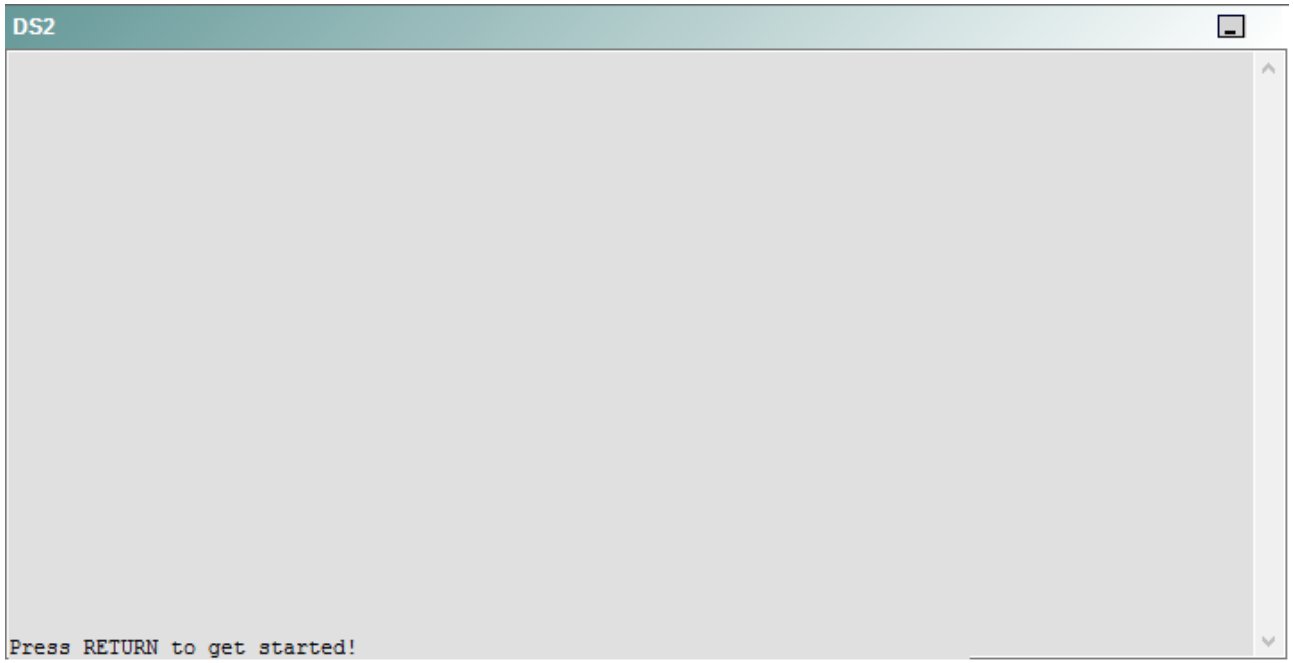

R5



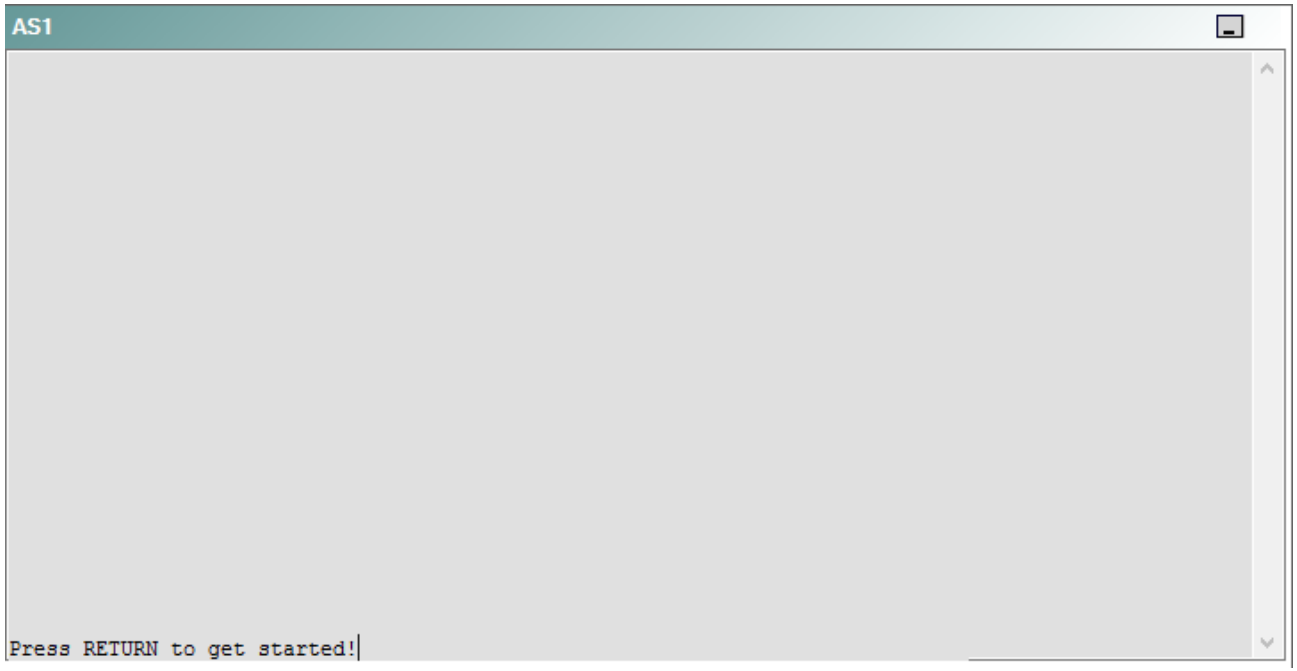

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that R5 is no longer able to ping the IPv6 address 2010::10:2 on R2.

Which of the following is most likely to solve the problem?

A. issuing the **tunnel mode gre ipv6** command on the Tunnel0 interface
B. issuing the **tunnel mode gre ip** command on the Tunnel0 interface
C. issuing the **ipv6 address 2010::21:1** command on the Tunnel0 interface
D. issuing the **ipv6 address 2010::21:2** command on the Tunnel0 interface
E. issuing the **tunnel source Ethernet0/0** command on the Tunnel 0 interface
F. issuing the **tunnel source Serial0/1** command on the Tunnel 0 interface
G. issuing the **tunnel destination 192.168.1.13** command on the Tunnel 0 interface
H. issuing the **tunnel destination 192.168.1.14** command on the Tunnel 0 interface

**Correct Answer:** E
**Section: (none)**

**Explanation**

**Explanation/Reference:**
Explanation:

You should issue the **tunnel source Ethernet 0/0** command in the Tunnel0 interface of R4. To determine which device is the source of the problem, you should issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from R5 to the closest device and work your way up the network until communication is lost, or you can ping from R5 to the farthest device and work your way back to R5 until pings are successful. Alternatively, you can trace from R5 to R1 and see where communication is lost along the path to the destination device.

In this scenario, if you were to issue the **ping 2010::21:1** command from R2, you would receive the following output:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010::21:1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

The ……in the output above indicates that the attempts to ping the IP version 6 (IPv6) address 2010::21:1 has timed out. Therefore, Internet Control Message (ICMP) packets from R5, which has been assigned the IPv6 address 2010::21:2, cannot reach 2010::21:1, which has been assigned to R4. However, if you were to issue the **ping 192.168.1.14** command on R4, you would receive the following output:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

The !!!!! in the output above indicates that R4 is able to ping the IP version 4 (IPv4) address 192.168.1.14, which has been assigned to the Ethernet0/0 interface on R5. The successful IPv4 ping indicates that the connectivity problem is limited to the IPv6 tunnel configured between R4 and R5. The Tunnel0 interfaces on R4 and R5 form a Generic Routing Encapsulation (GRE) overlay tunnel between the two routers. An overlay tunnel encapsulates IPv6 traffic into IPv4 traffic and can be used as an intermediate migration tool from IPv4-based networks to IPv6-based networks.

Once you have determined where connectivity is lost, you can begin to troubleshoot the cause of the problem. If you were to issue the **show interface Tunnel0** command on R5, the output would reveal that the interface is up and that the line protocol is up on the Tunnel0 interface. However, issuing the **show interface Tunnel0** command on R4 reveals that the interface sis up and that the line protocol is down, as shown in the following partial output from R4:

```
Tunnel0 is up, line protocol is down
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 0.0.0.0 (Serial1/0), destination 192.168.1.14
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
```

Additionally, the partial output above indicates that the source for interface Tunnel0 has been configured as Serial1/0, which is the interface that connects R4 to R3, not the interface that connects R4 to R5. Therefore, the tunnel source for the Tunnel0 interface on R4 is not properly configured. Tunnel0 is a virtual interface configured on each device that uses the physical interface Ethernet0/0 on that device as a source and the IPv4 address of the remote device as a destination. The Ethernet0/0 interface should be the source for the Tunnel0 interface on R4 because it is the interface that is directly connected to the remote end of the GRE overlay tunnel. For example, R5 uses its own Ethernet0/0 interface as the source of its Tunnel0 interface; the destination for the Tunnel0 interface on R5 is set to the IPv4 address assigned to the Ethernet0/0 interface on R4. Issuing the **tunnel source Ethernet0/0** command on R4 will correctly configure the tunnel source for the Tunnel0 interface on R4 and will restore IPv6 connectivity between R4 and R5 on the overlay tunnel.

You should not issue the **tunnel mode gre ipv6** command or the **tunnel mode gre ip** command on the Tunnel0 interface on R4 or R5. You would issue the **tunnel mode gre ipv6** command on the Tunnel0 interface of R4 and R5 to encapsulate IPv4 traffic over an IPv6 network. In this scenario, the GRE tunnel between R4 and R5 is an IPv6 overlay tunnel, which encapsulates IPv6 traffic over an IPv4 network. Additionally, the **tunnel mode gre ip** command is the default encapsulation mode when you establish a GRE tunnel that encapsulates IPv6 over IPv4. If you were to issue the **show interface Tunnel0** command on R4 and R5, you would see that the encapsulation mode on the Tunnel0 interface on R4 is configured to use the same encapsulation mode as the Tunnel0 interface on R5, as shown in the following partial output:

```
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.1.14 (Ethernet0/0), destination 192.168.1.13
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
```

You need not issue **the ipv6 address 2010::21:1** command or the **ipv6 address 2010::21:2** command on the Tunnel0 interface on R4 and R5. If you were to issue the **show ipv6 interface Tunnel0** command on R4 and on R5 in this scenario, the output would reveal that the Tunnel0 interface on R4 has already been assigned the IPv6 address 2010::21:1 and that the Tunnel0 interface on R5 has already been assigned the IPv6 address 2010::21:2, as shown in the following output:

```
R4#show ipv6 interface Tunnel 0
Tunnel0 is up, line protocol is down
  IPv6 is enabled, link-local address is FE80::CE0B:8FF:FE84:0 [TEN]
  Global unicast address(es):
    2010::21:1, subnet is 2010::21:0/124 [TEN]

R5#show ipv6 interface Tunnel 0
Tunnel0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::CE0C:8FF:FE84:0
  Global unicast address(es):
    2010::21:2, subnet is 2010::21:0/124
```

You should not issue the **tunnel source Serial0/1** command on the Tunnel0 interface on either R4 or R5, because the Ethernet0/0 interface on each device is the direct physical connection between R4 and R5. If you were to issue the **show running-config** command on each device, the resulting output would indicate that the source of the Tunnel0 interface on R4 has been configured to use the incorrect Serial1/0 interface and that the source of the Tunnel0 interface on R5 has been configured to use the correct Ethernet0/0 interface, as shown in the following partial output:

```
R4#show running-config
...
intertace Tunnel0
 no ip address
 ipv6 address 2010::21:1/124
 ipv6 ospf 100 area 20
 tunnel source Serial1/0
 tunnel destination 192.168.1.14
!

R4#show running-config
...
interface Tunnel0
 no ip address
 ipv6 address 2010::21:2/124
 ipv6 ospf 100 area 20
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.13
!
```

You should not use the **tunnel destination 192.168.1.13** command or the **tunnel destination 192.168.1.14** command on either R4 or R5, because the destination for each Tunnel0 interface is already configured correctly. The tunnel destination for the Tunnel0 interface on R4 should be configured to the IPv4 address of the Ethernet0/0 interface on R5 because 192.168.1.14 is the IPv4 address of the device to which the Ethernet0/0 interface on R4 is connected. The tunnel destination for the Tunnel0 interface on R5 should be configured to the IPv4 address of the Ethernet0/0 interface on R4 because 192.168.1.13 is the IPv4 address of the device to which the Ethernet0/0 interface on R5 is connected.

**QUESTION 54**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

You can access the following devices for each trouble ticket:

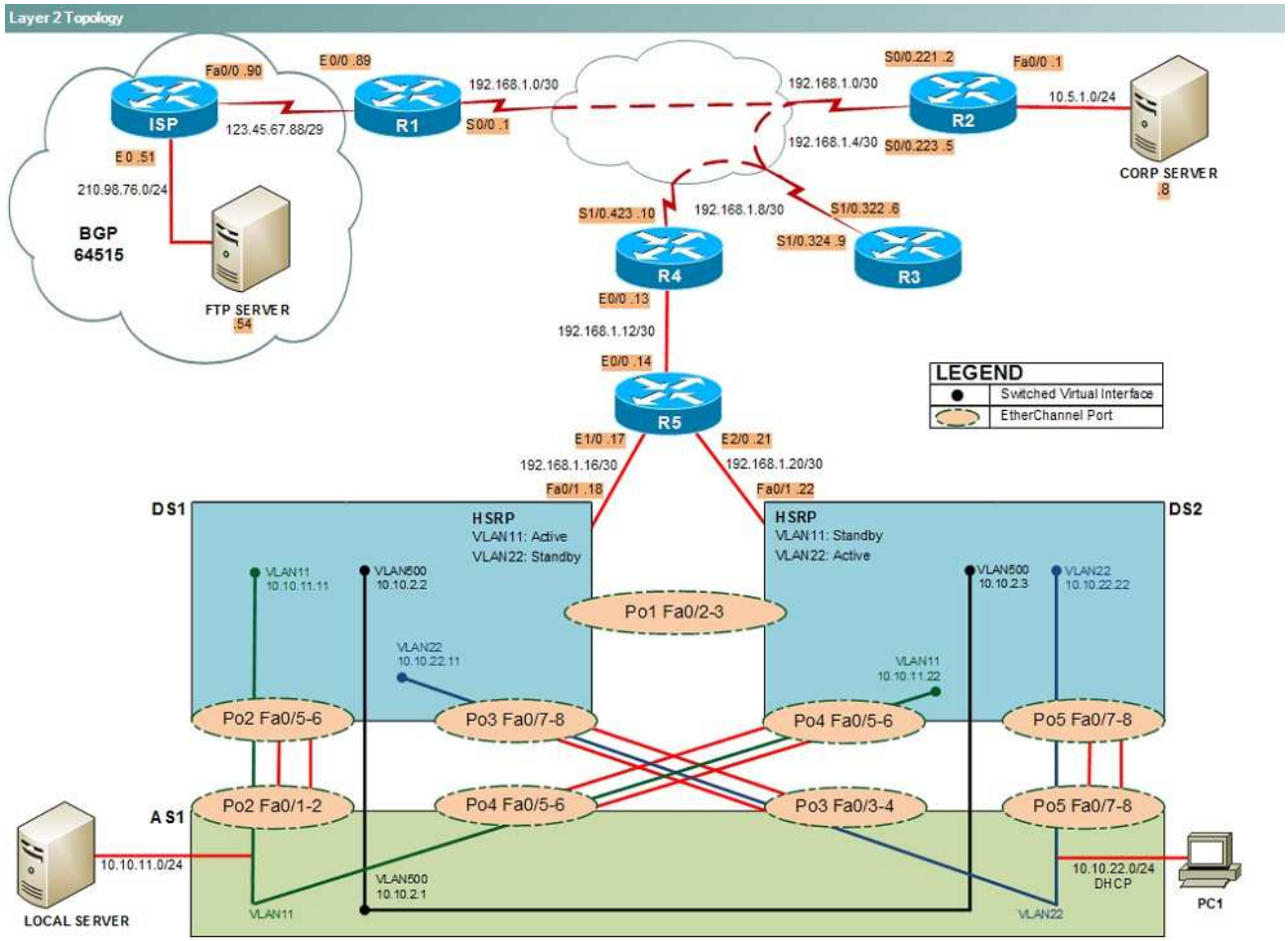
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

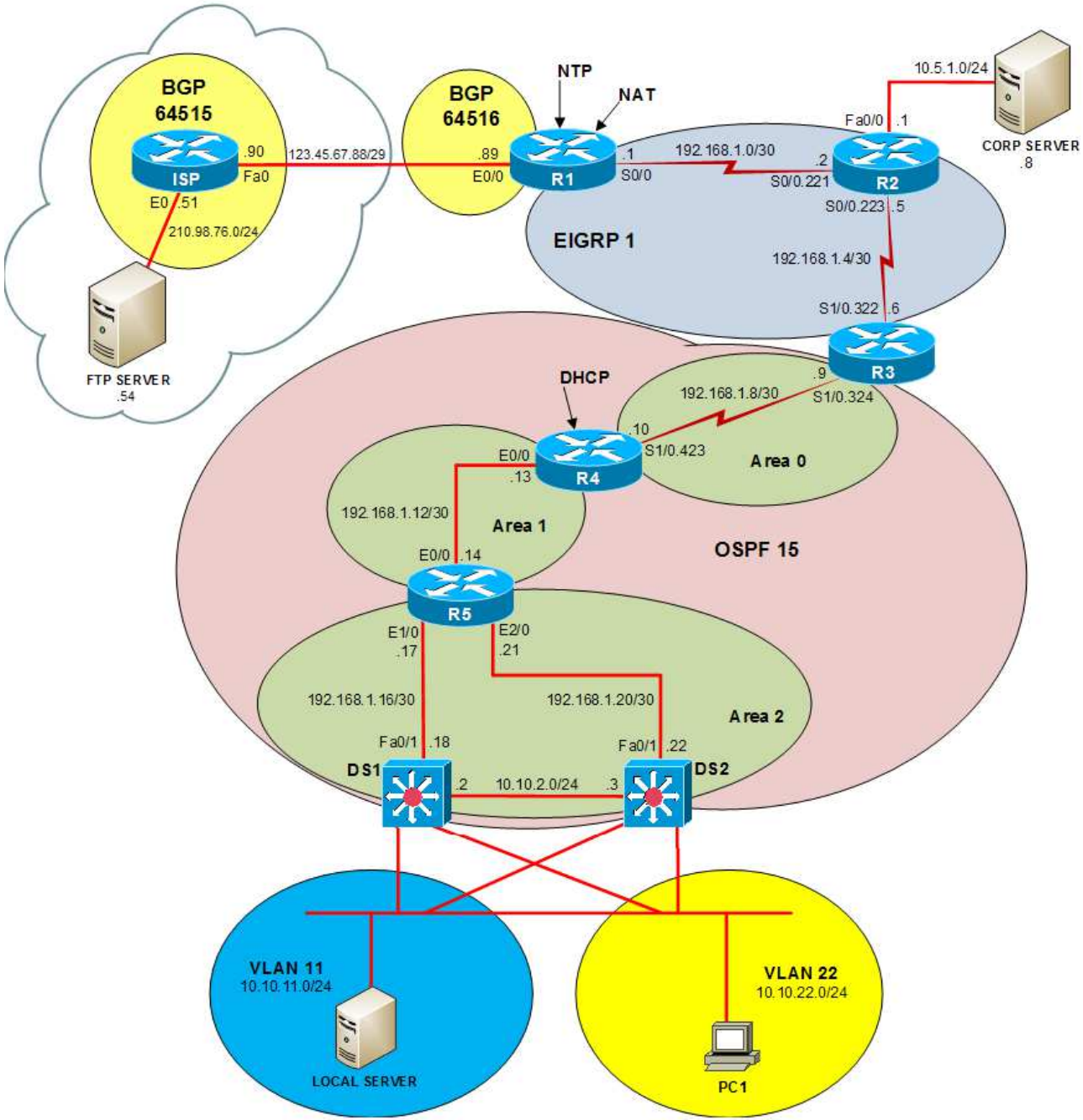
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

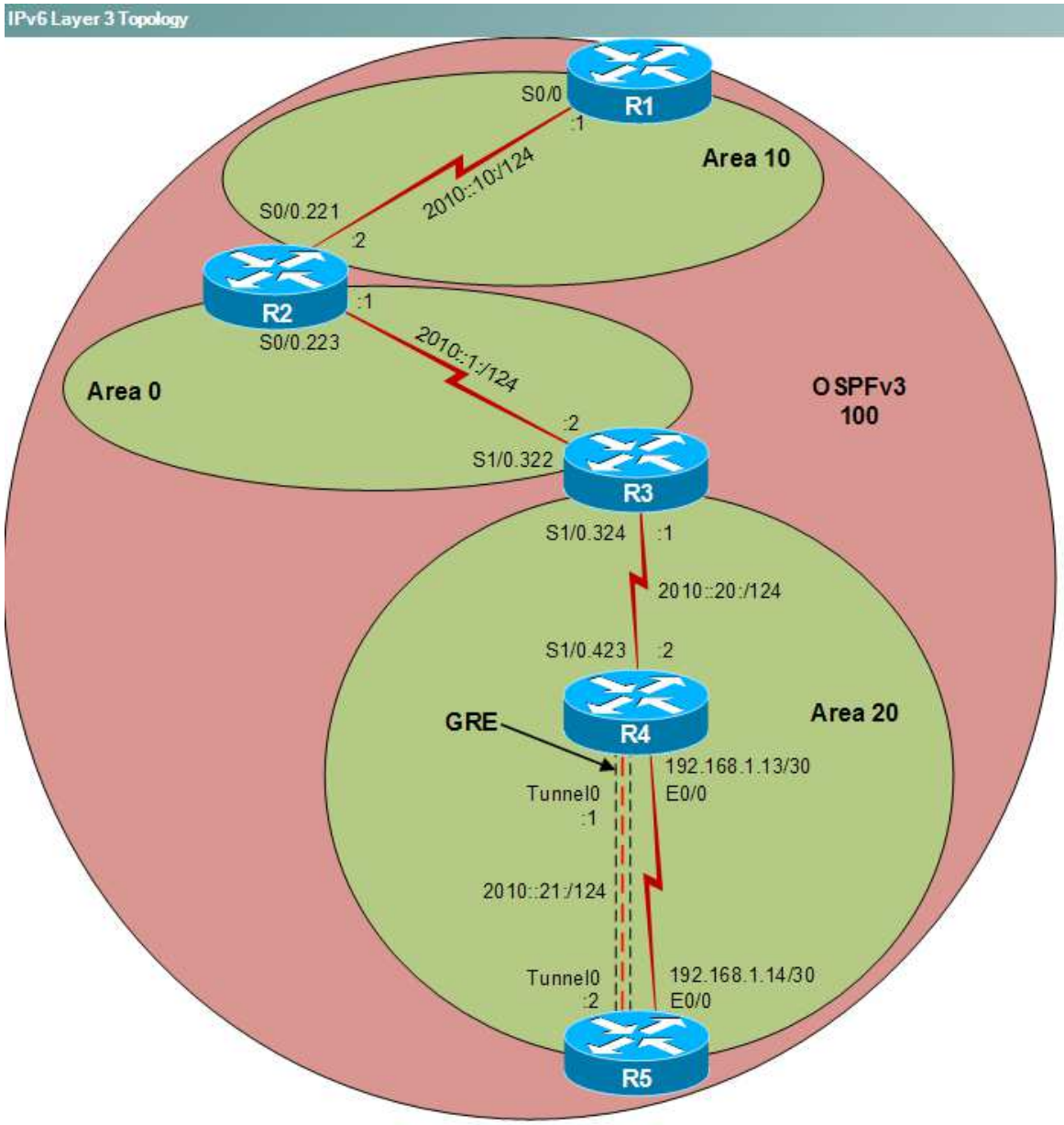
**Layer 2 Topology**




IPv4 layer 3 Topology

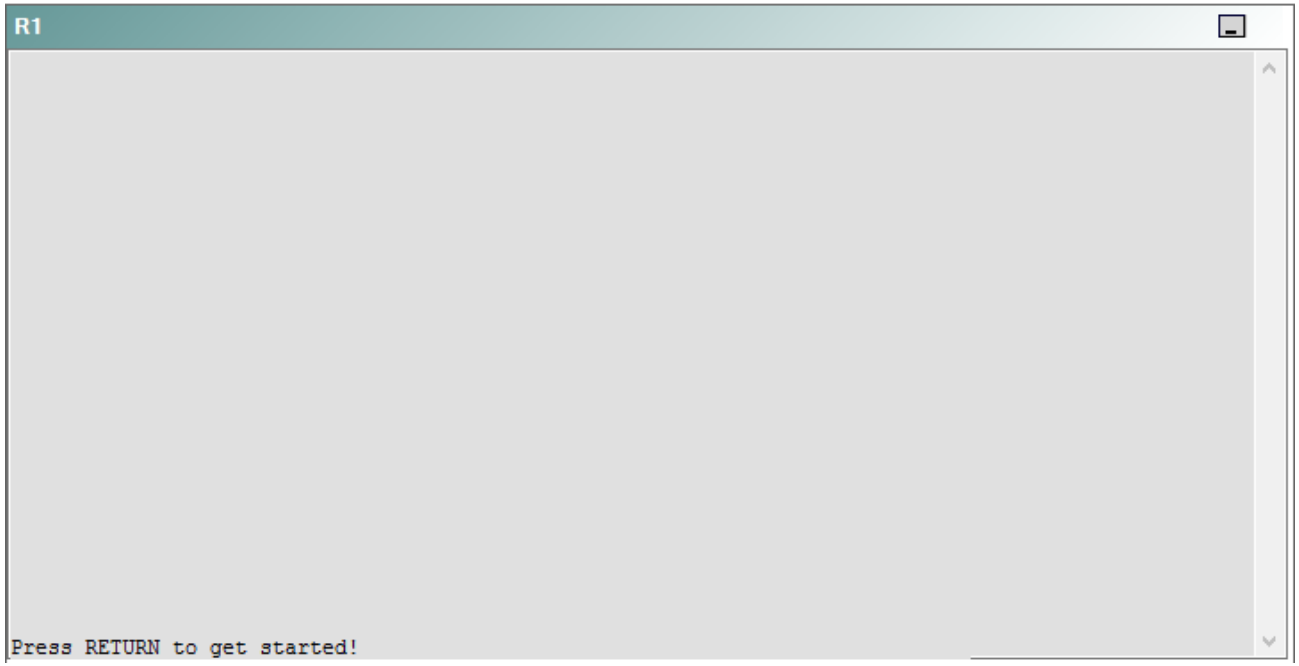

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

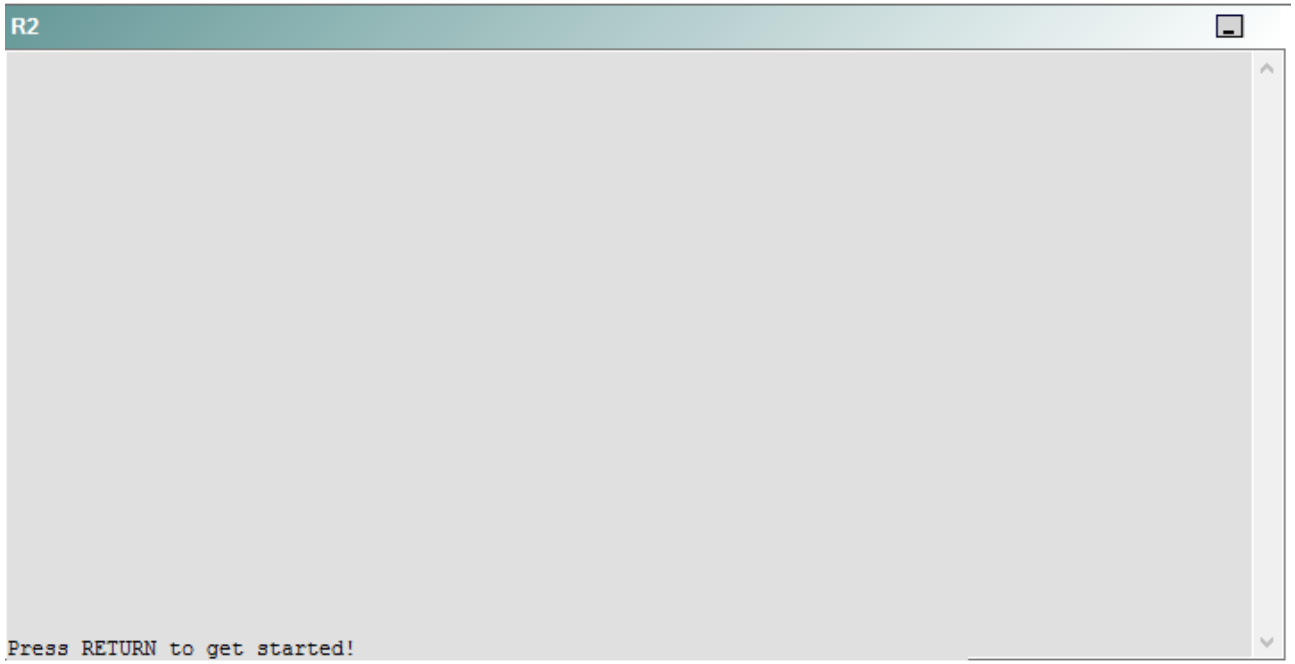



https://www.gratisexam.com/

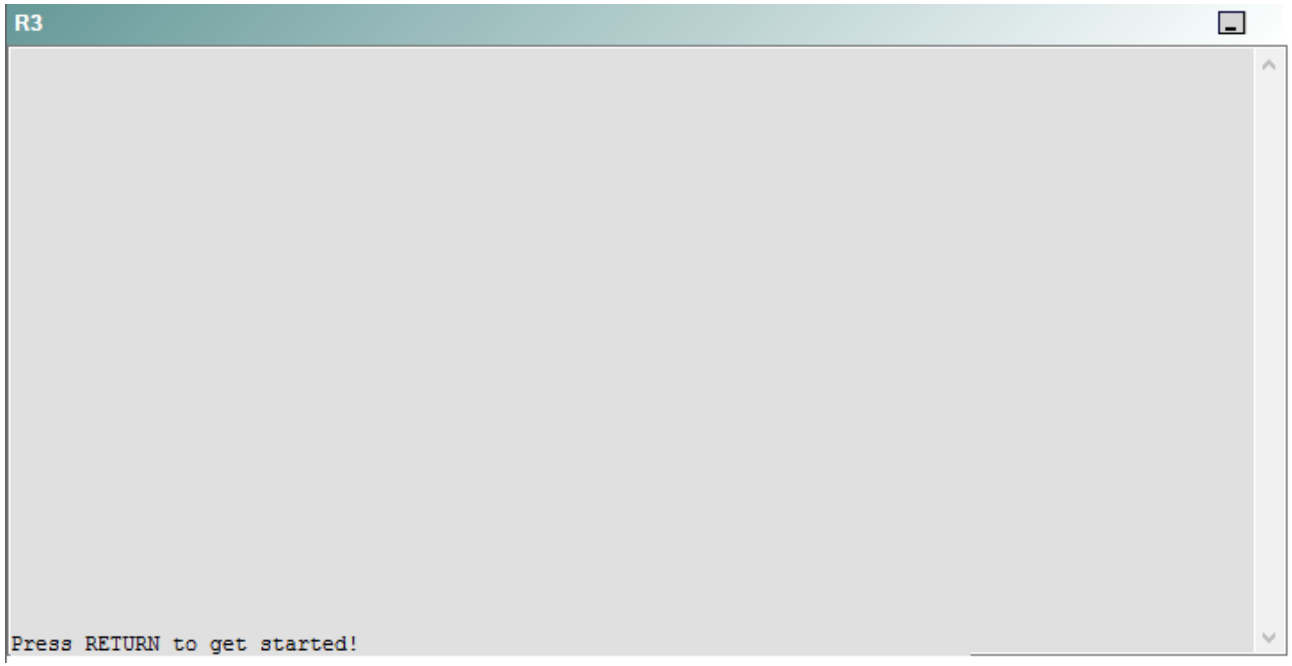
R1



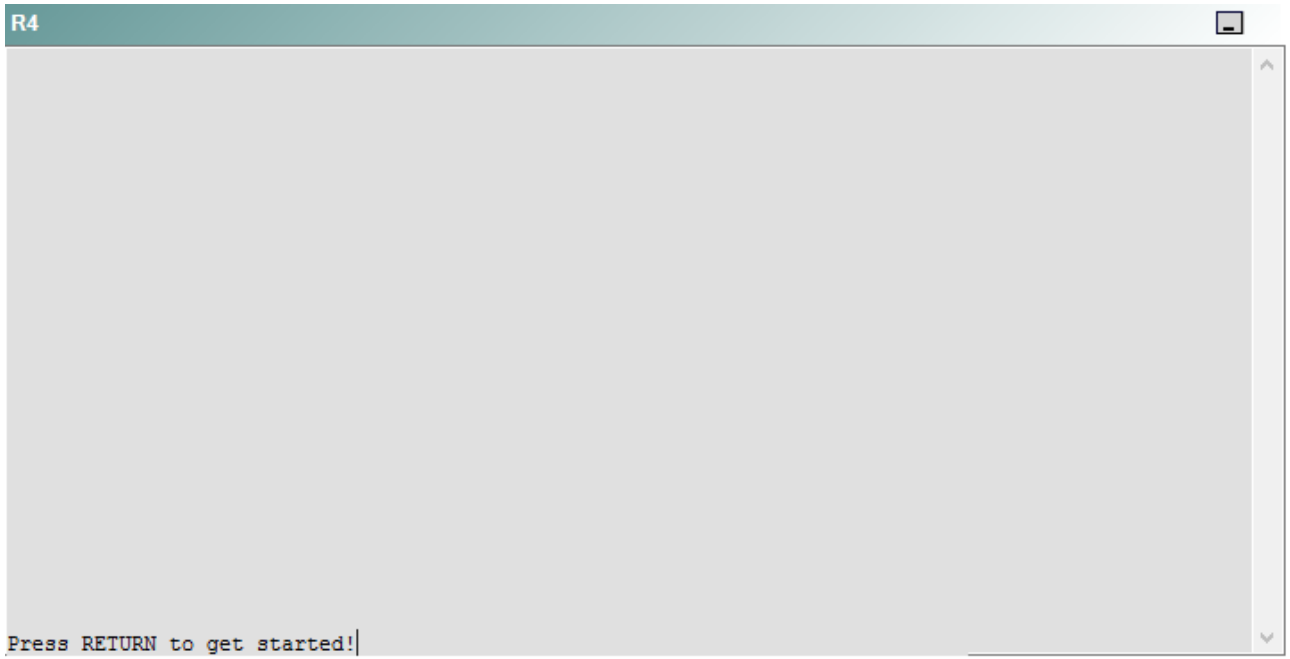

R2



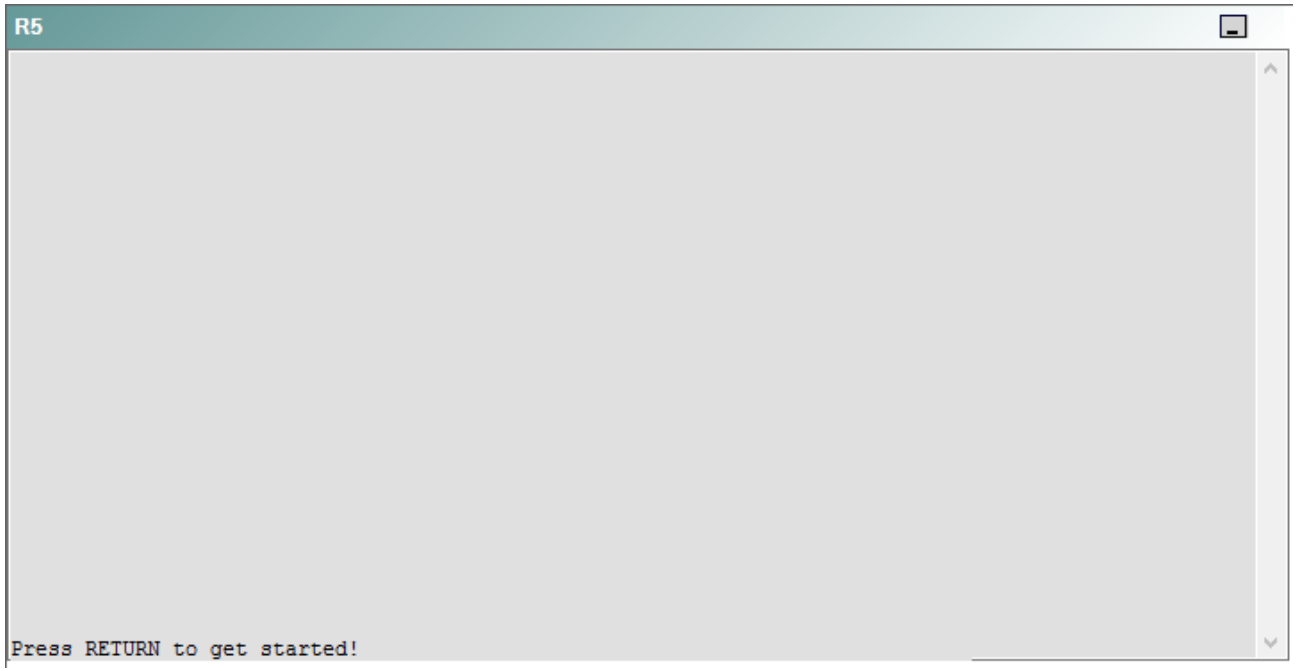

R3



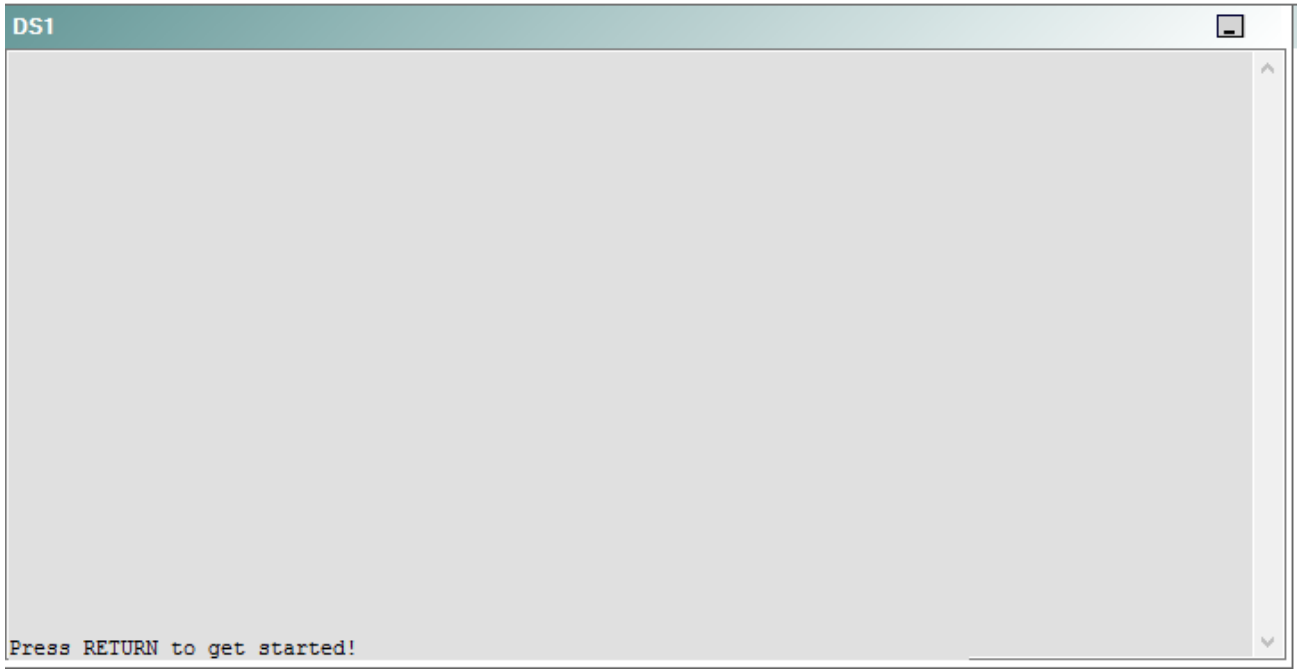

R4



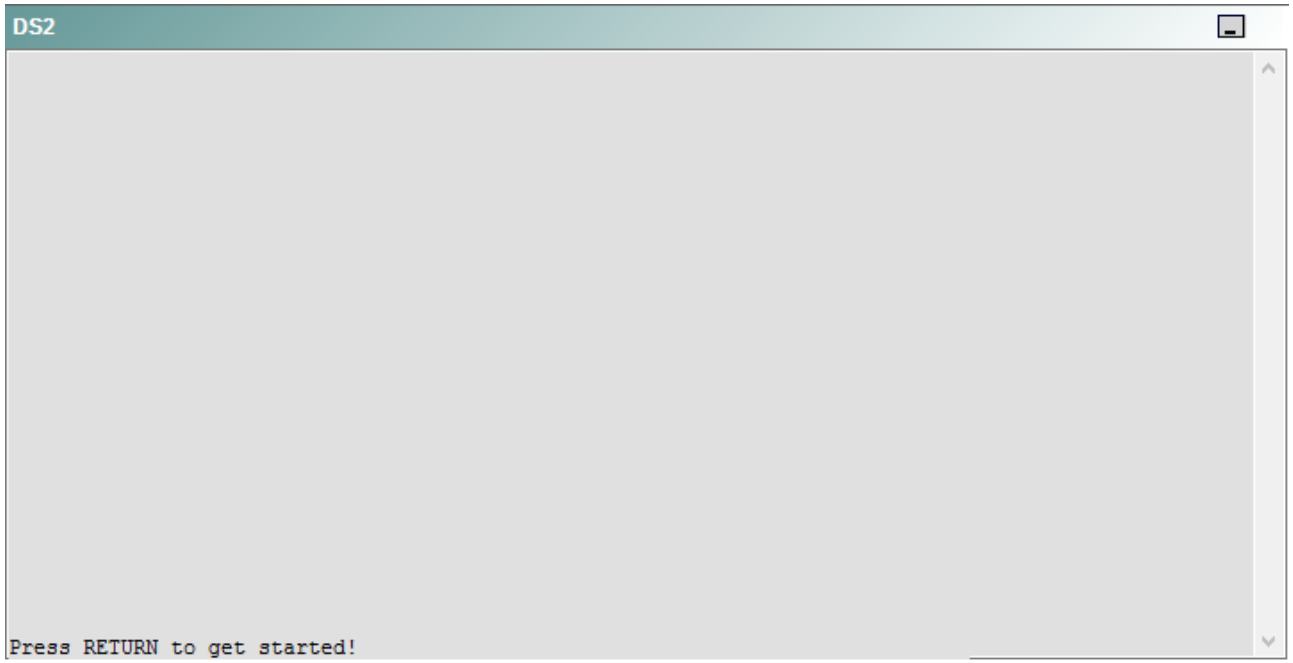

R5



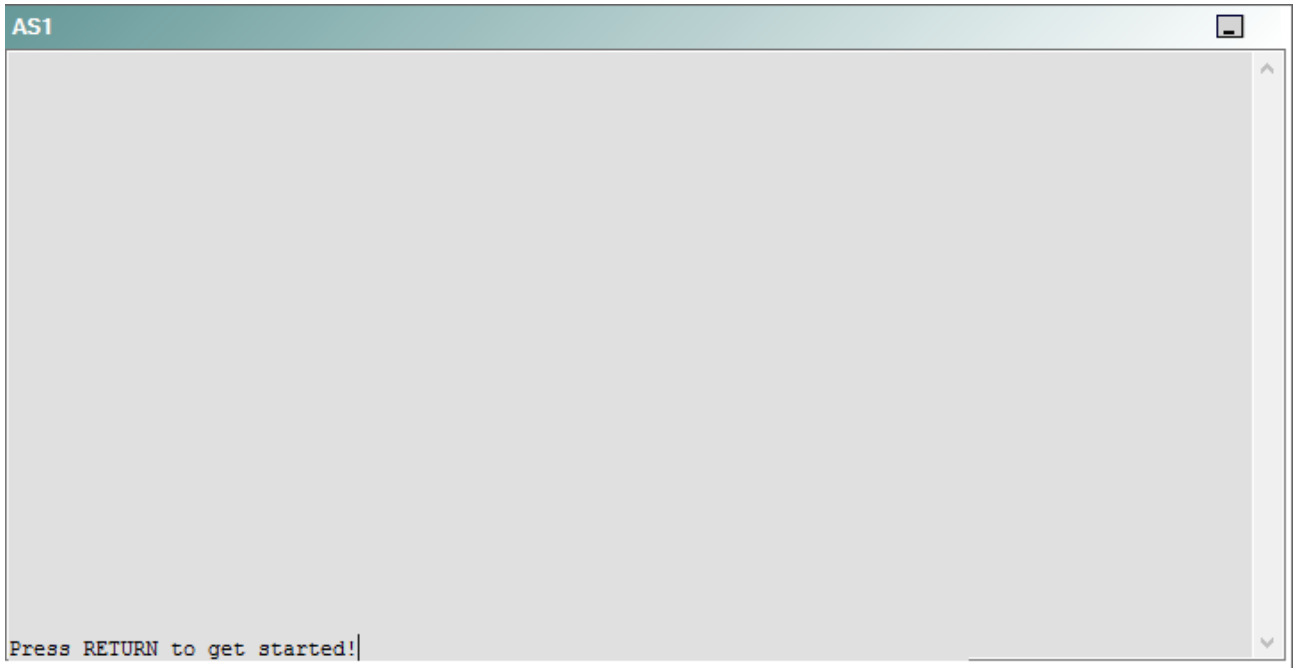

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that R5 is no longer able to ping the IPv6 address 2000::10:1 on R1.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 55**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

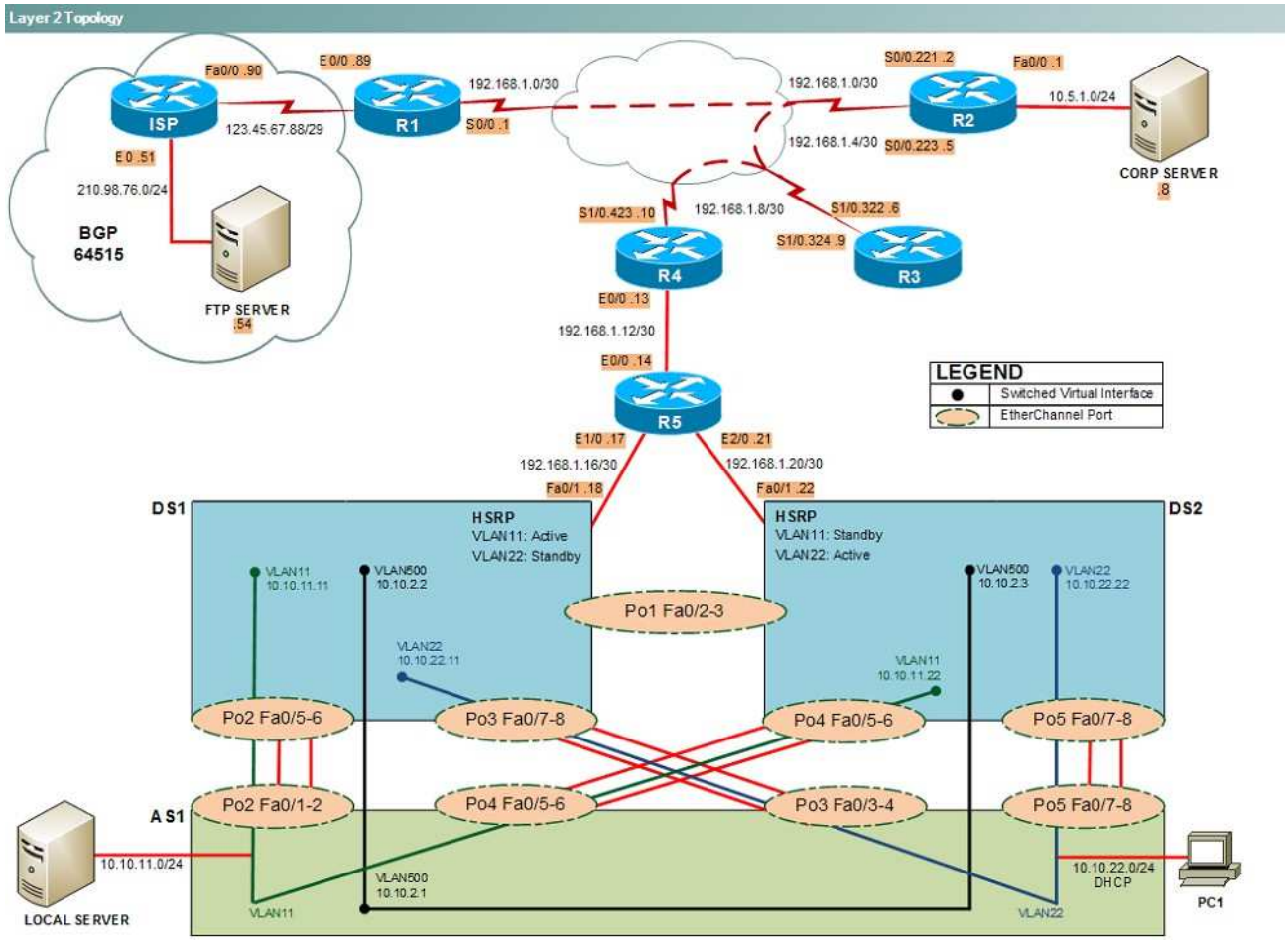
Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you

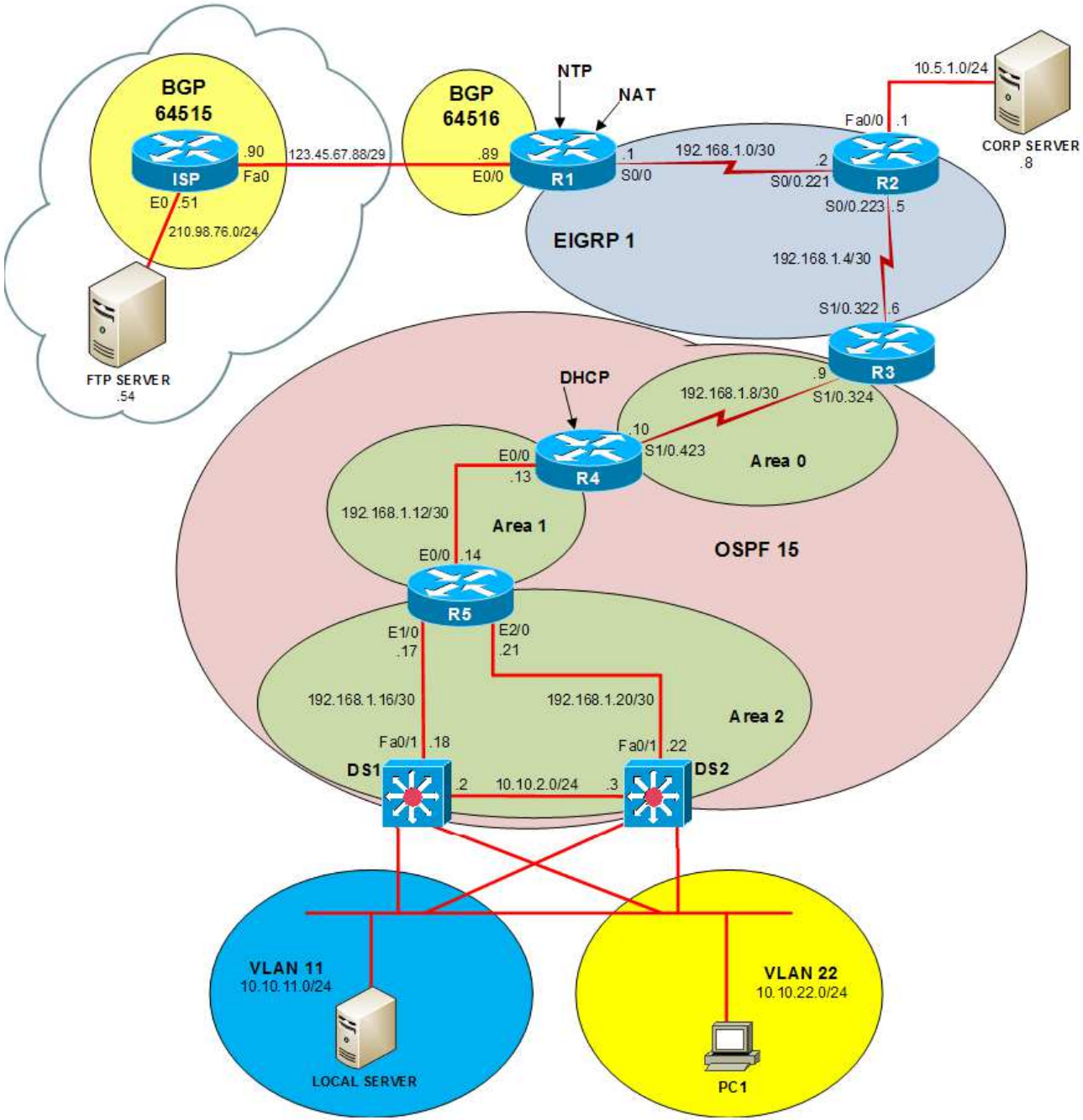
can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

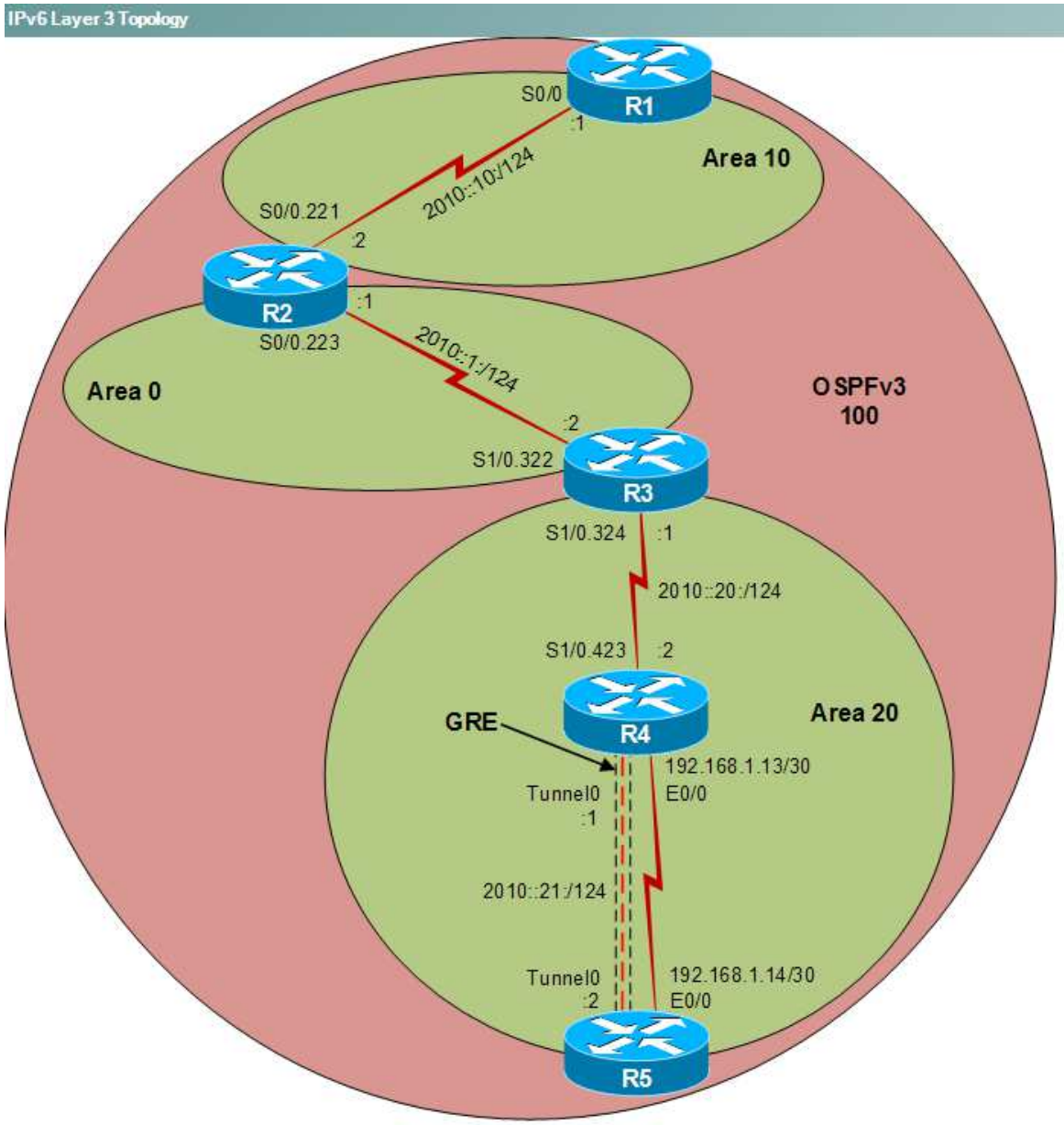
**Layer 2 Topology**



IPv4 layer 3 Topology

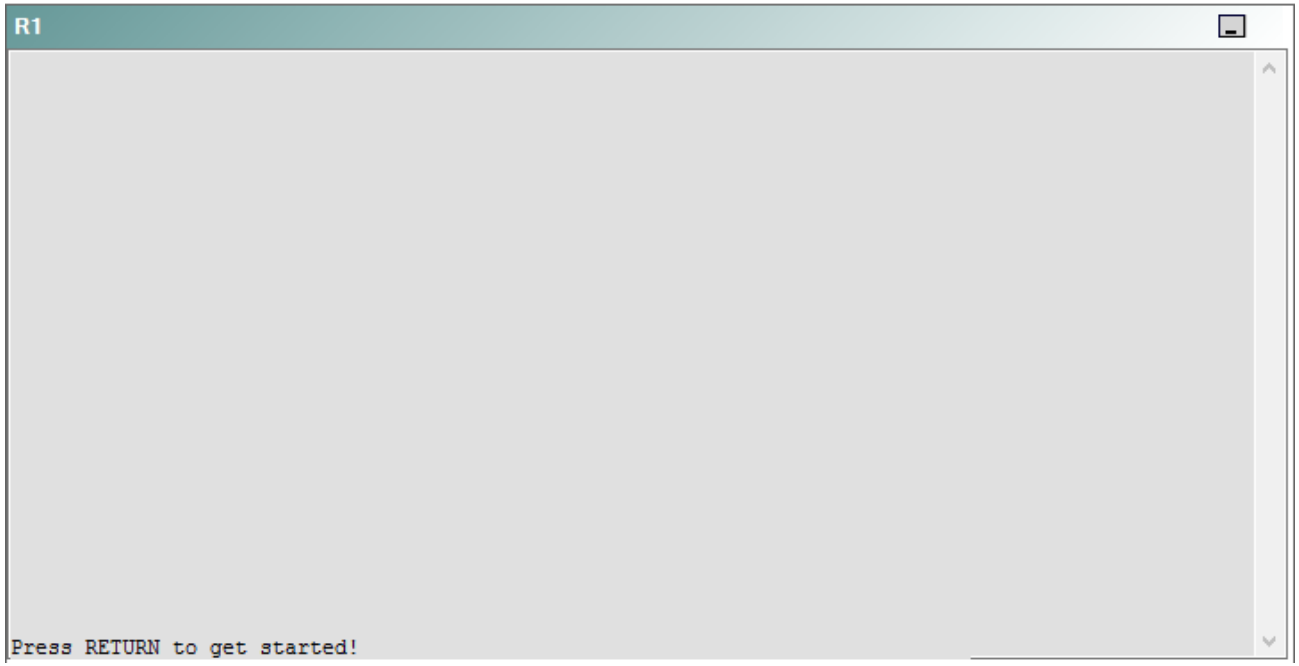

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

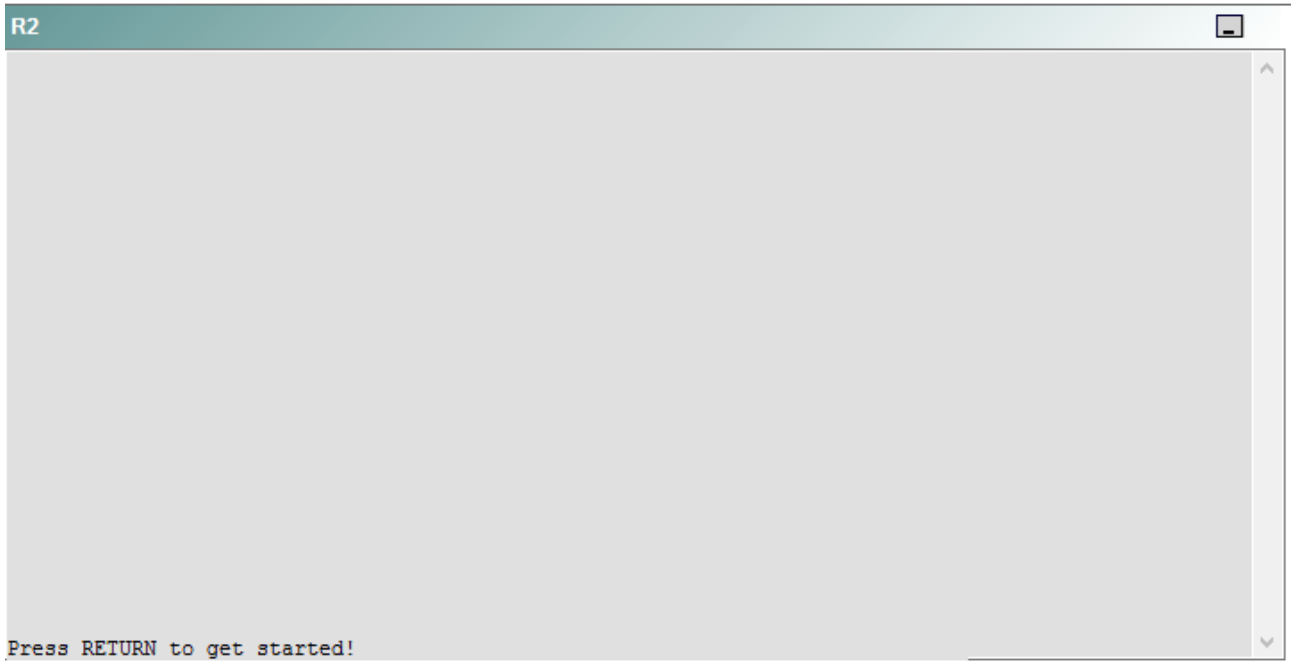



https://www.gratisexam.com/

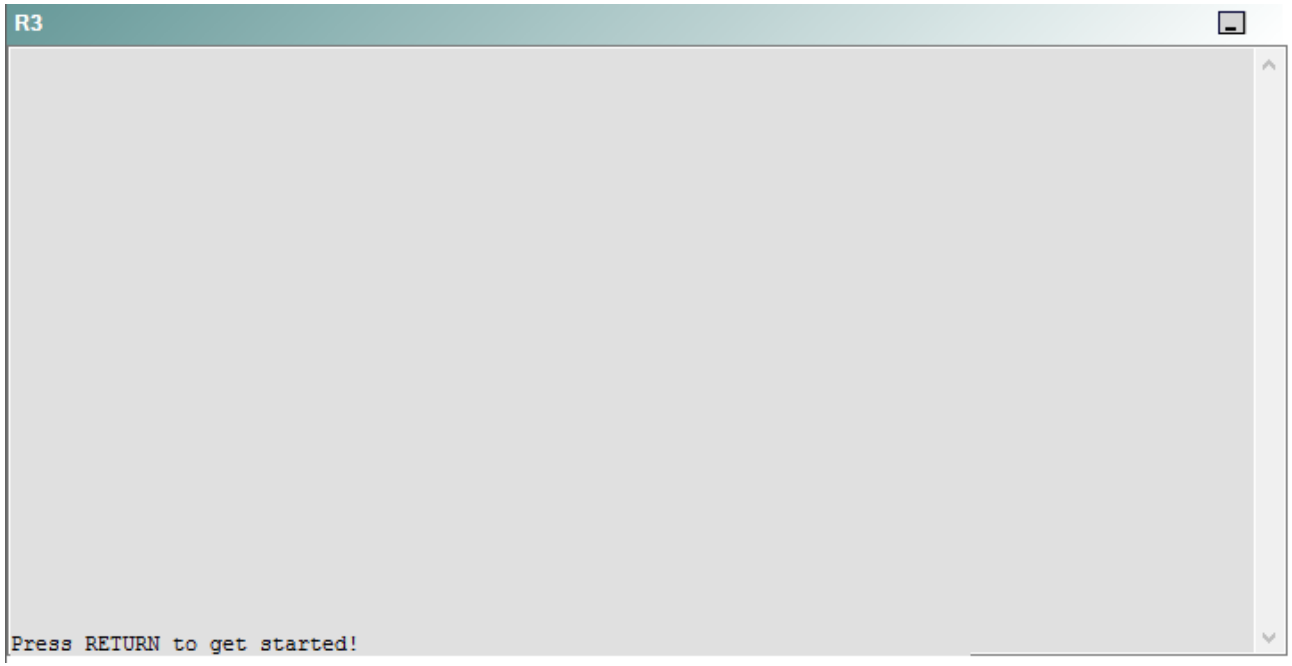
R1



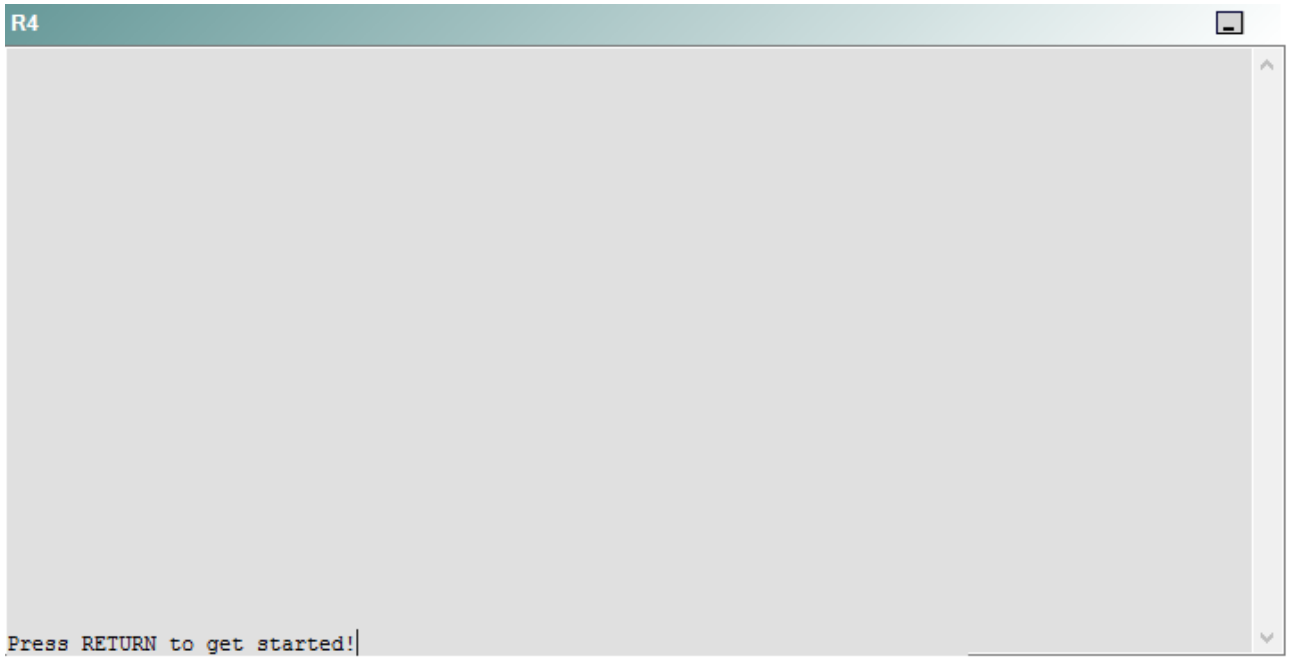

R2



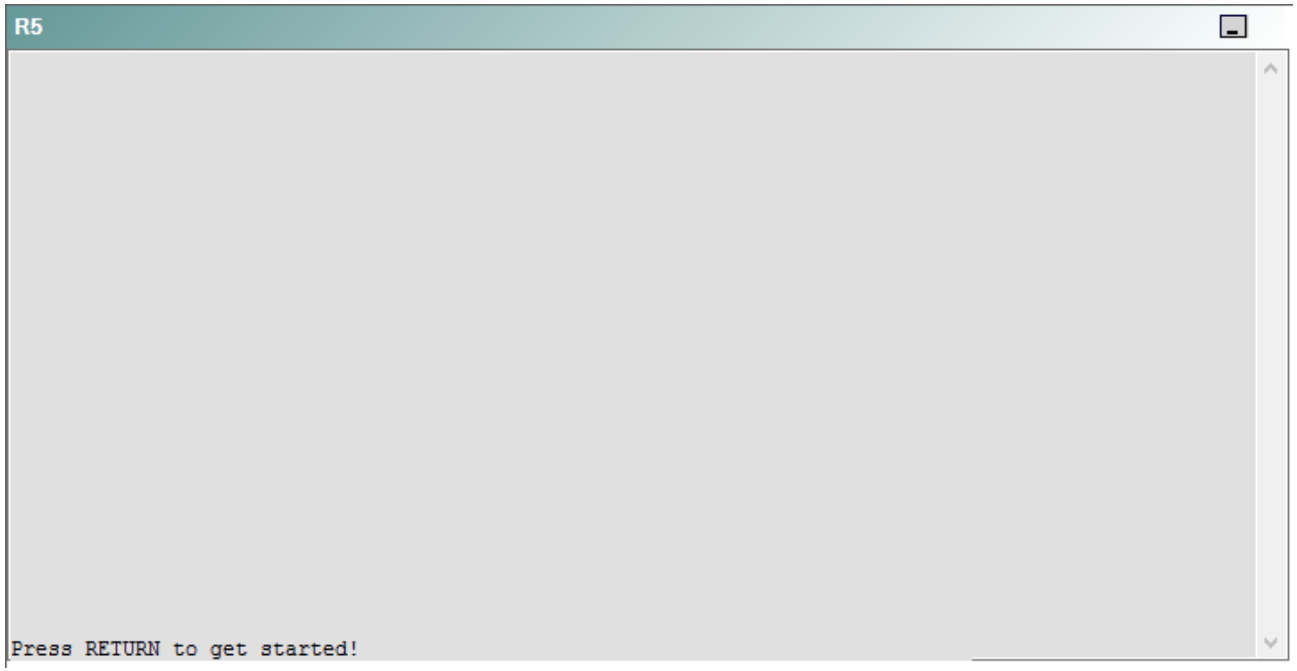

R3



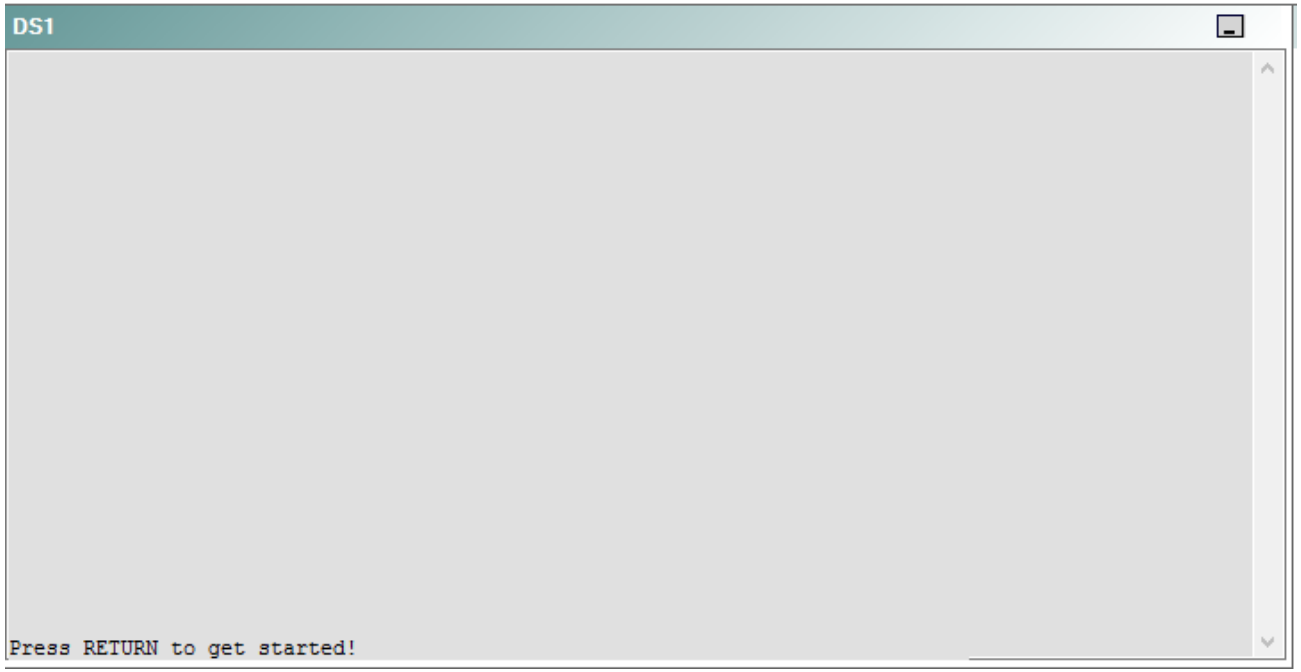

R4



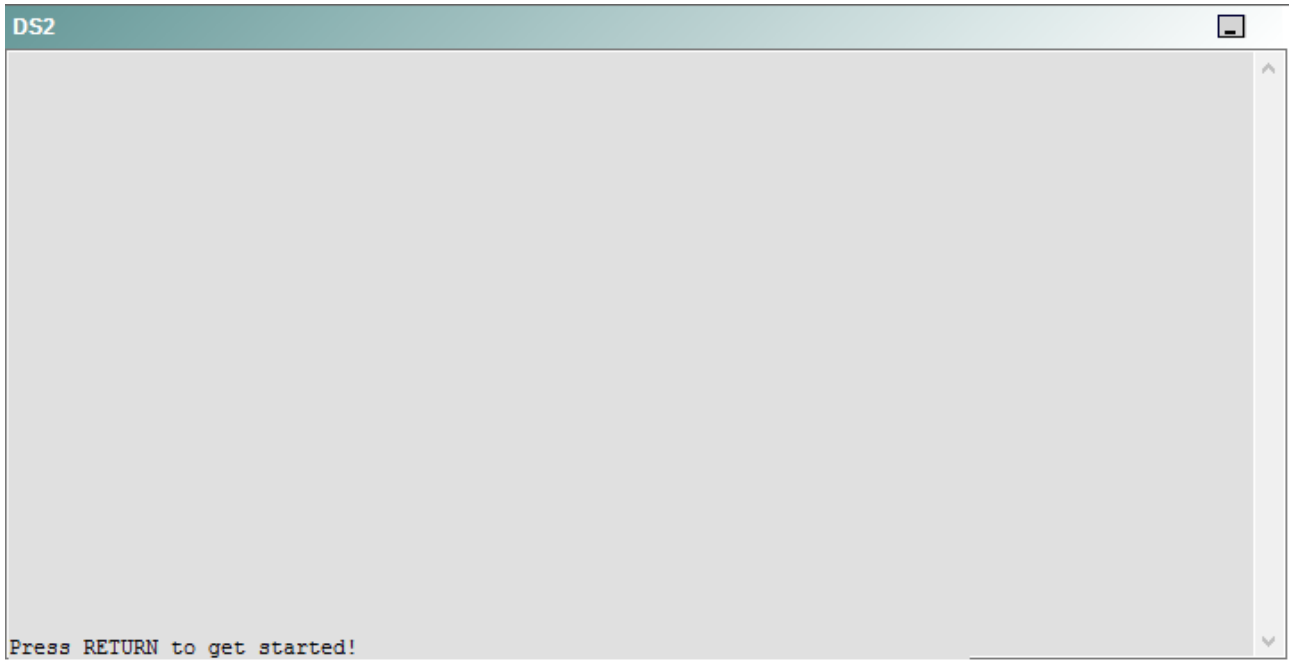

R5



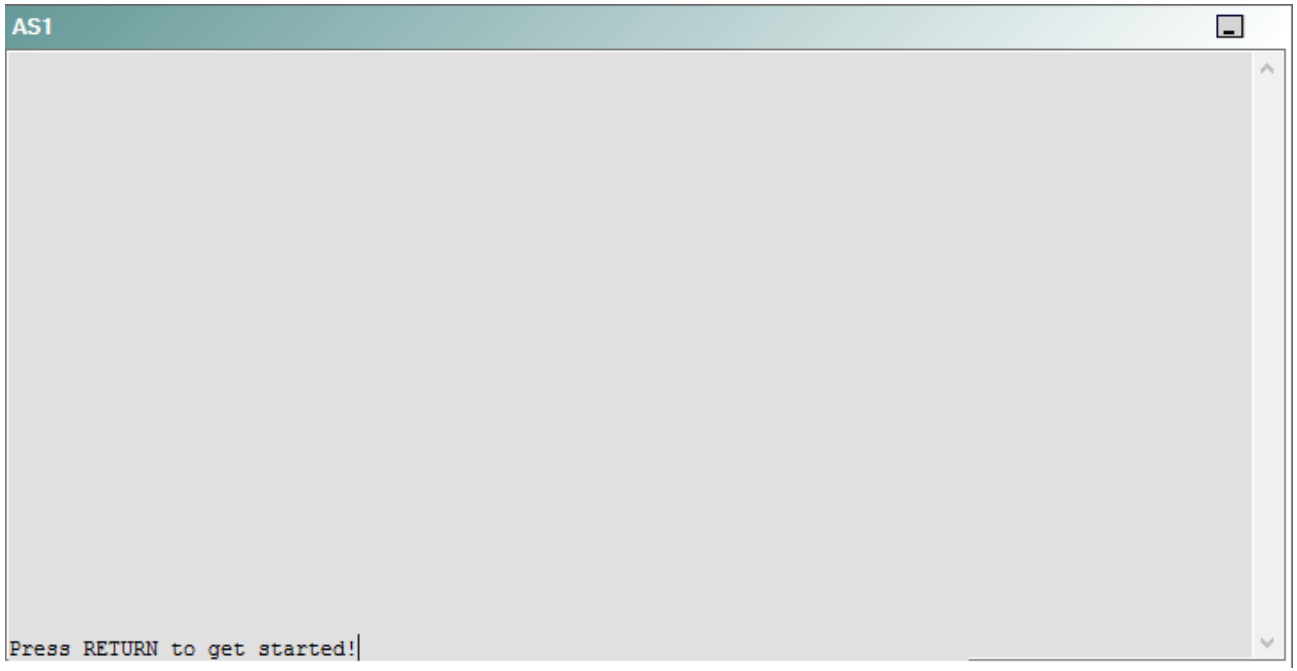

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that R5 is no longer able to ping the IPv6 address 2000::10:1 on R1.

Which of the following technologies is the source of the problem?

A. NTP
B. OSPFv3
C. EIGRP
D. redistribution
E. Layer 3 security
F. Layer 3 addressing
G. interface

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 56**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

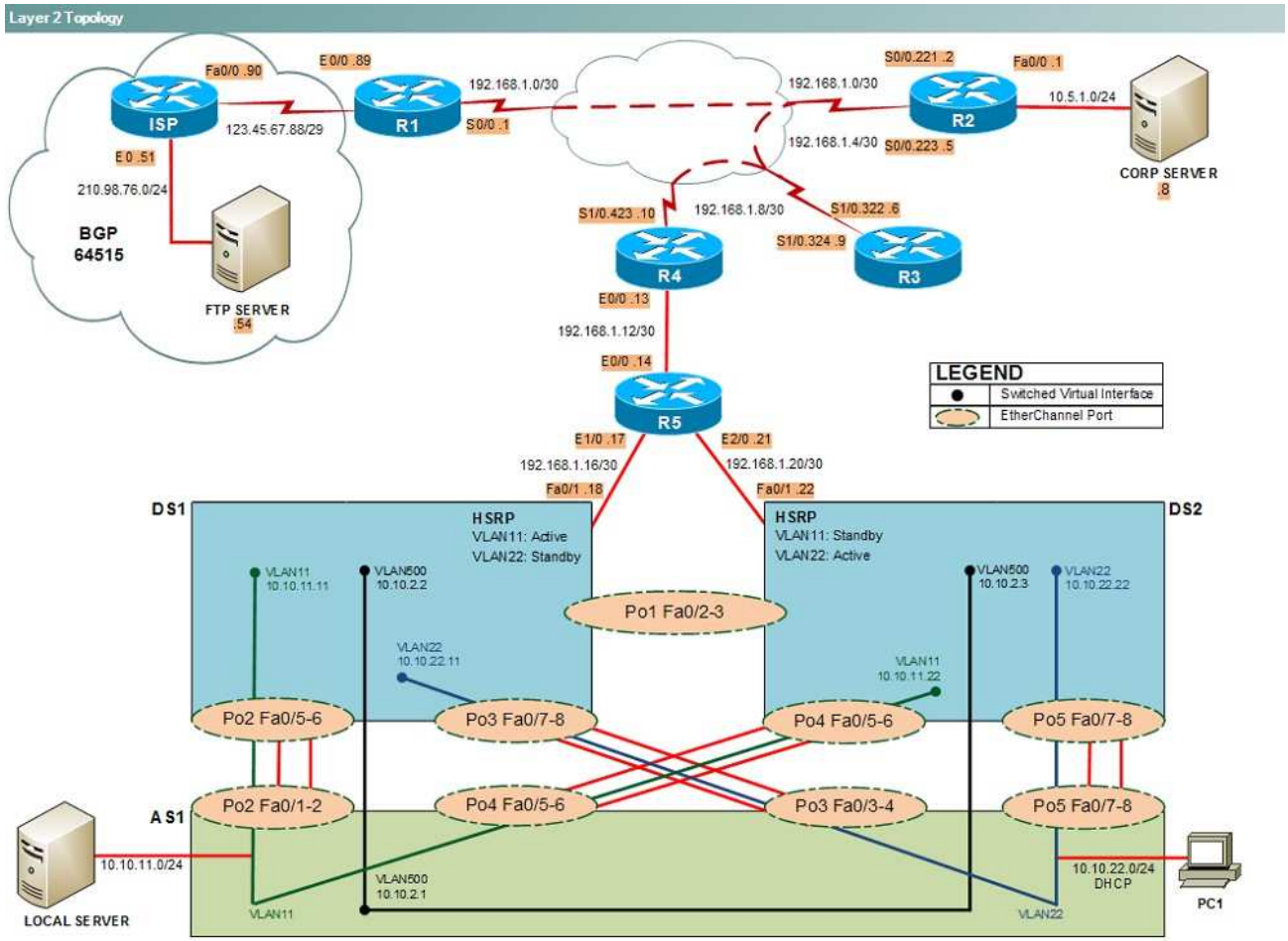
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

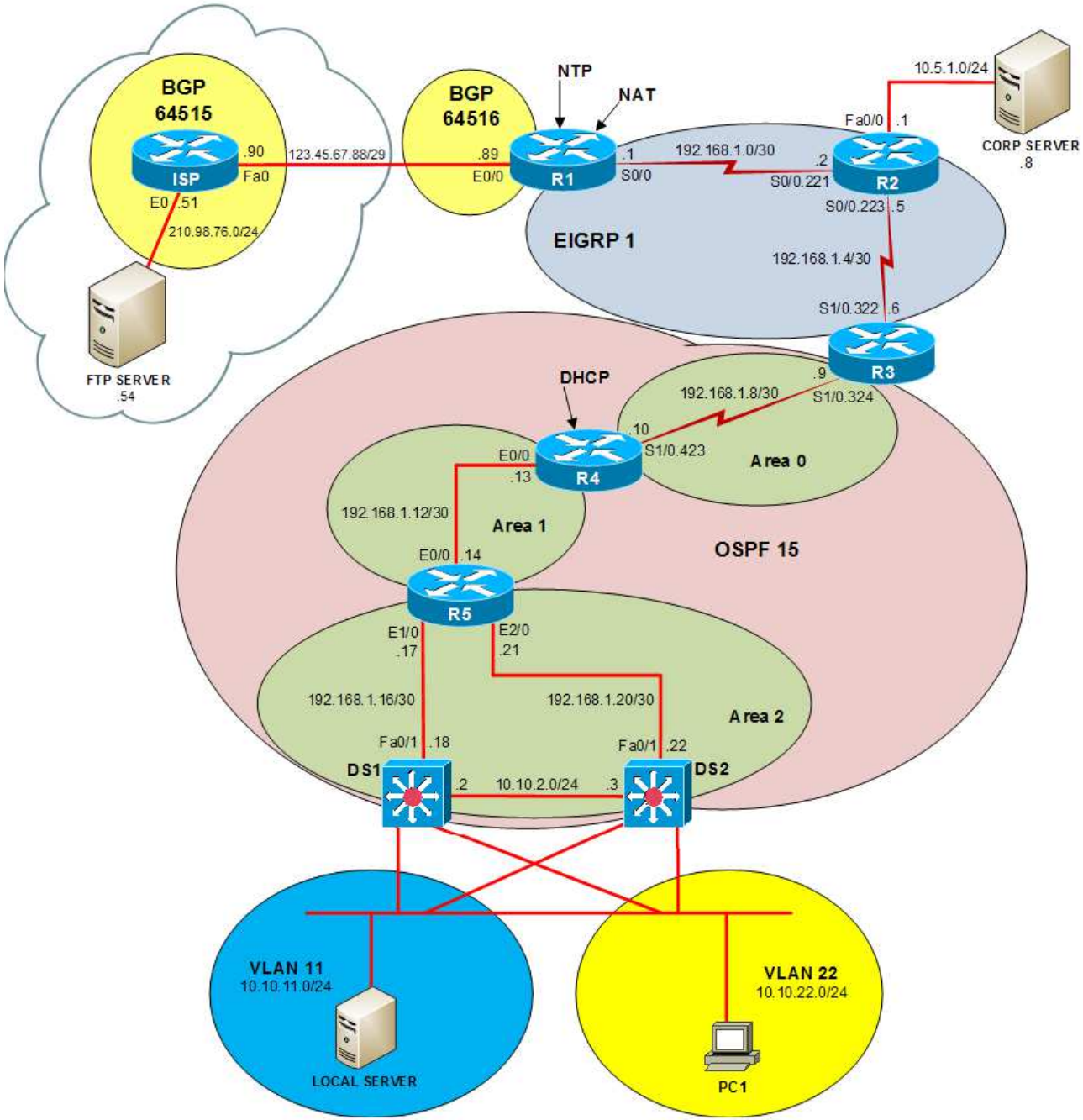
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

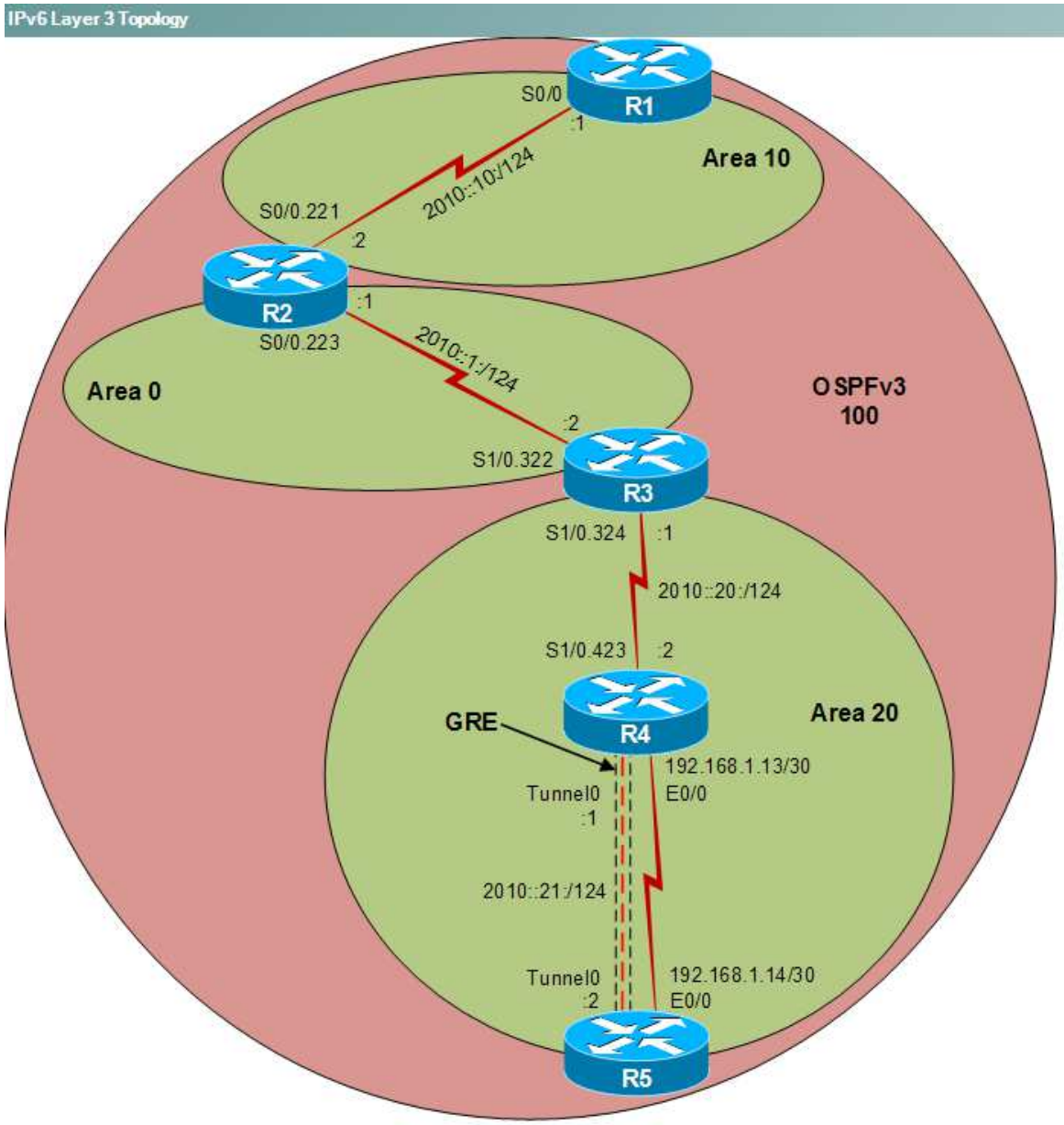
**Layer 2 Topology**




IPv4 layer 3 Topology

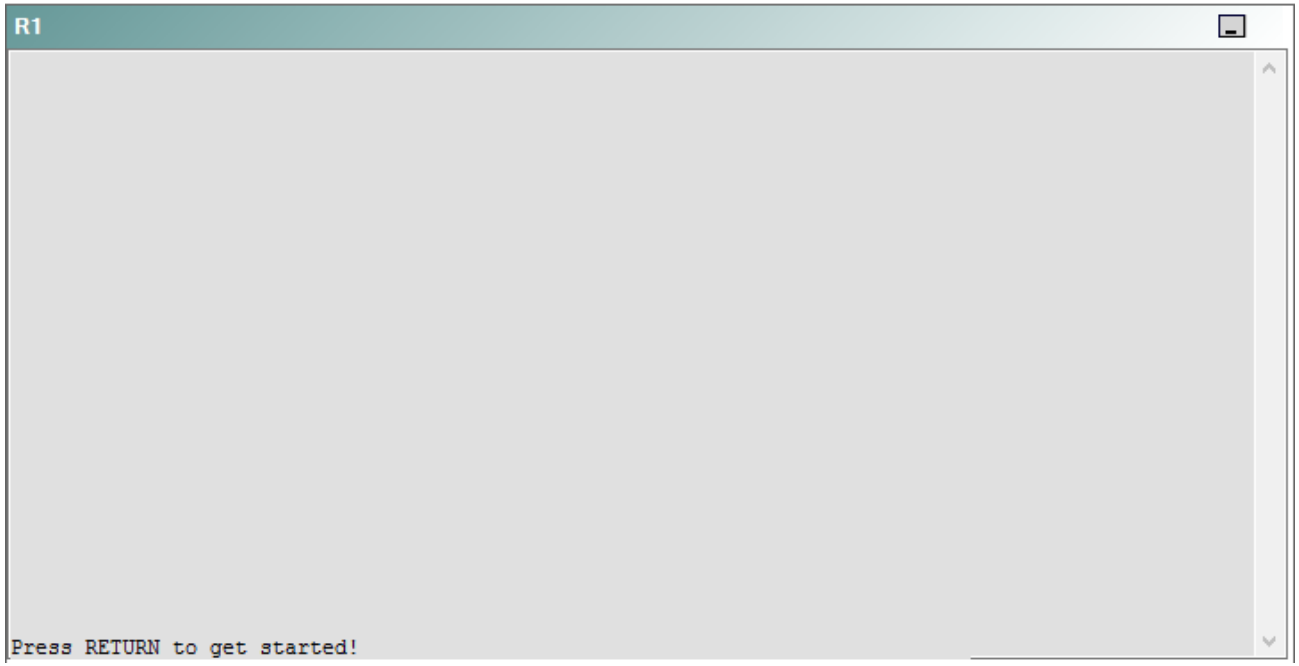

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

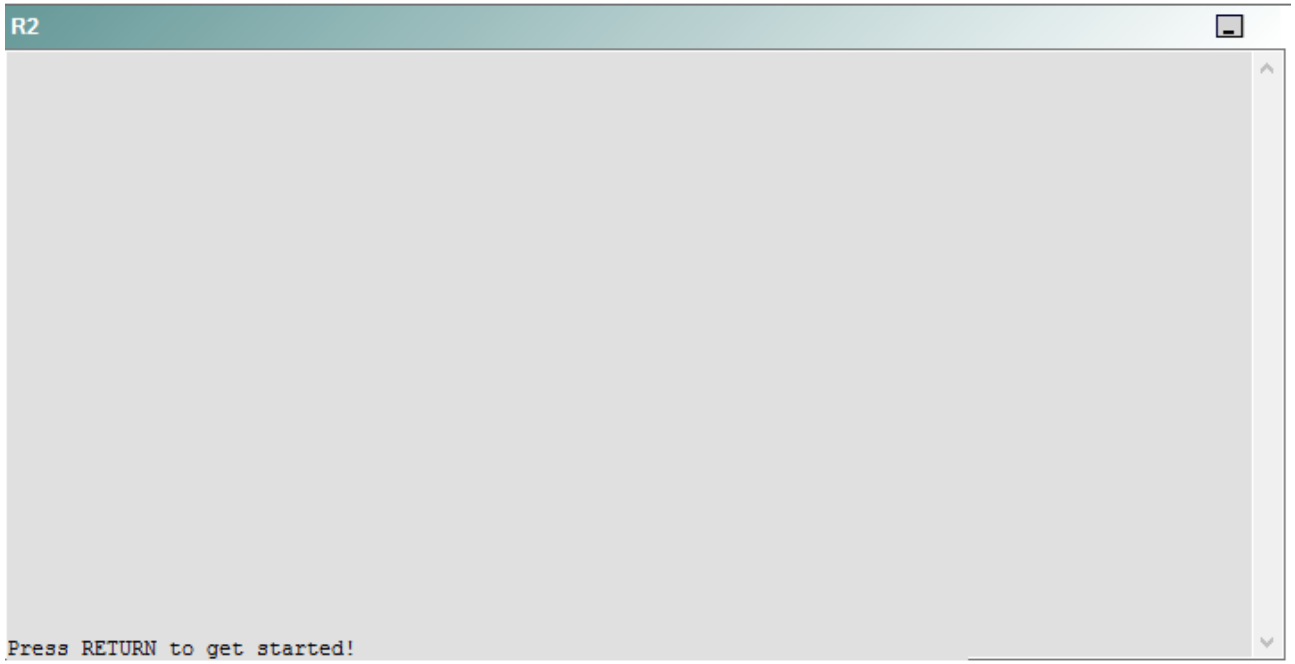



https://www.gratisexam.com/

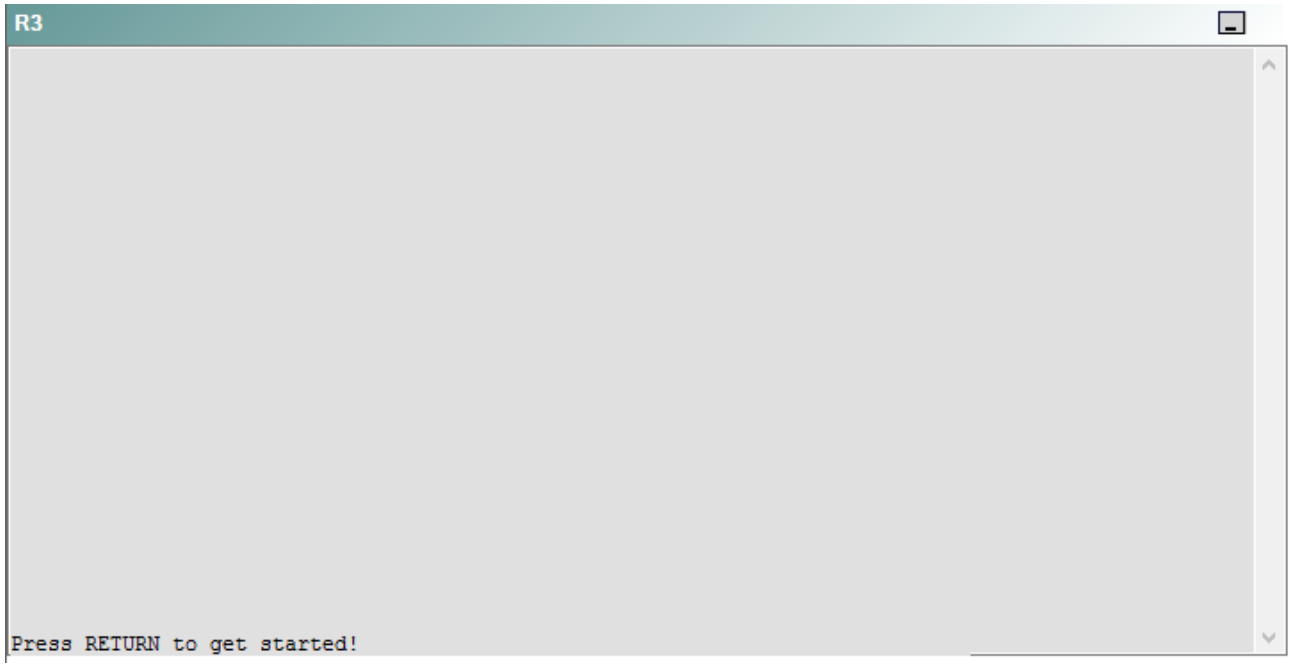
R1



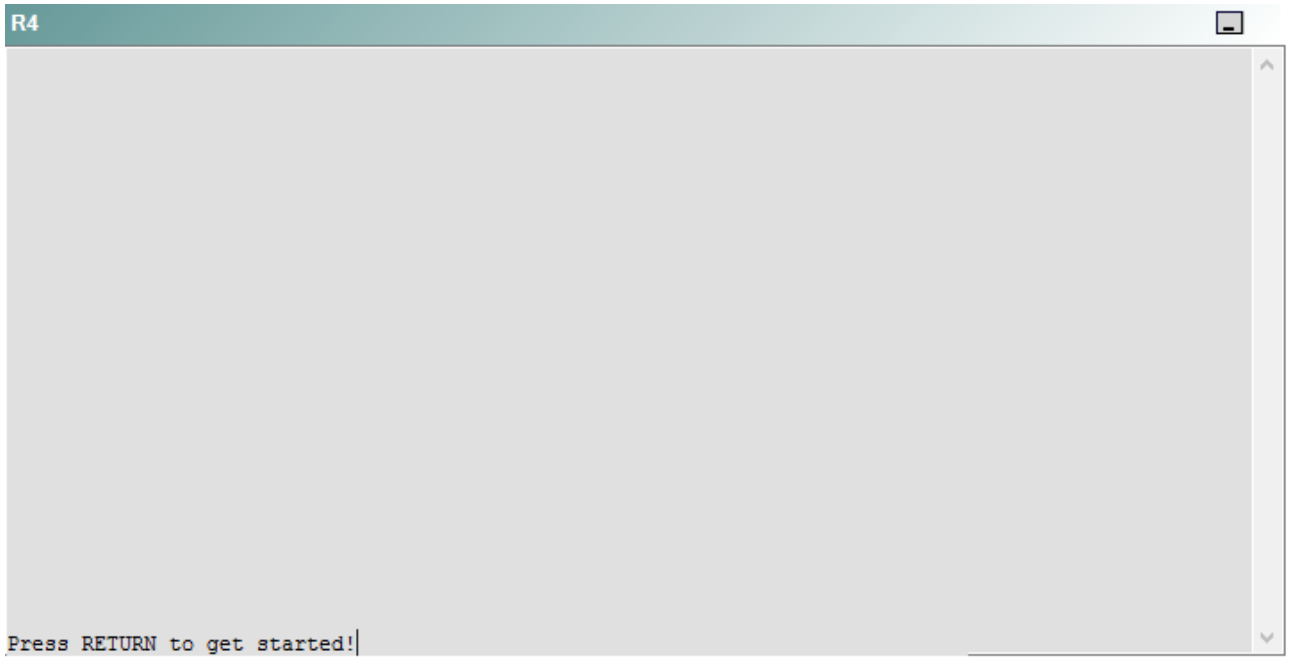

R2



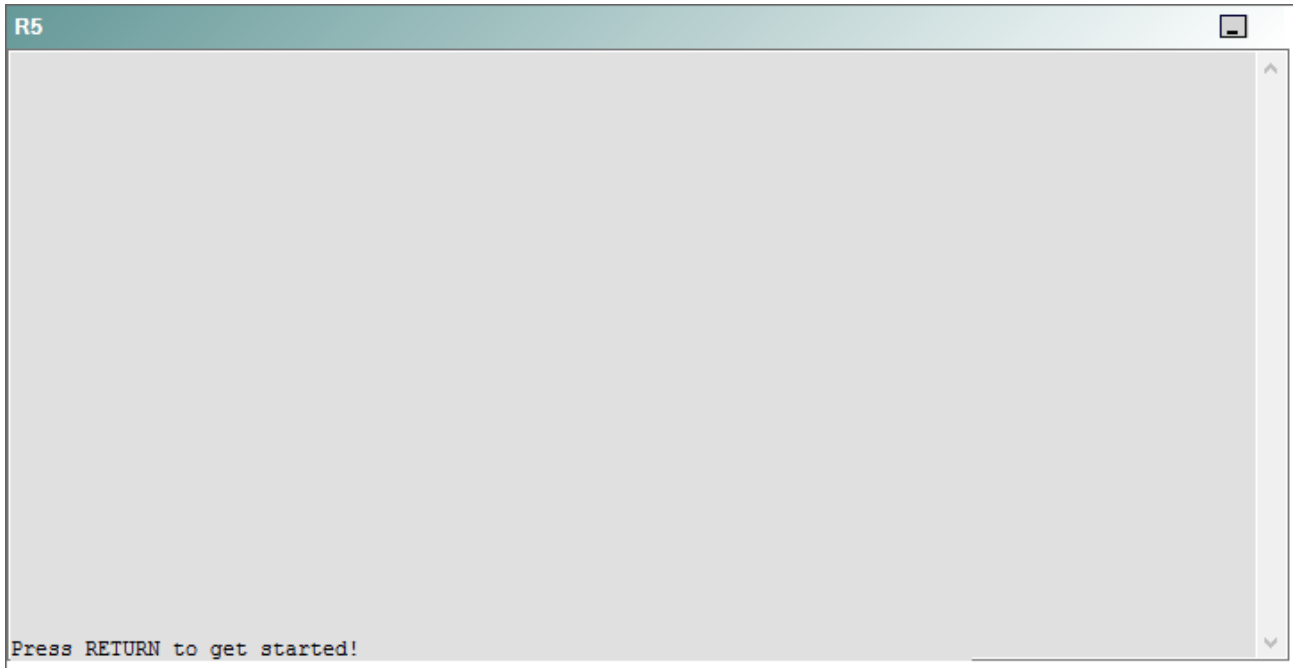

R3



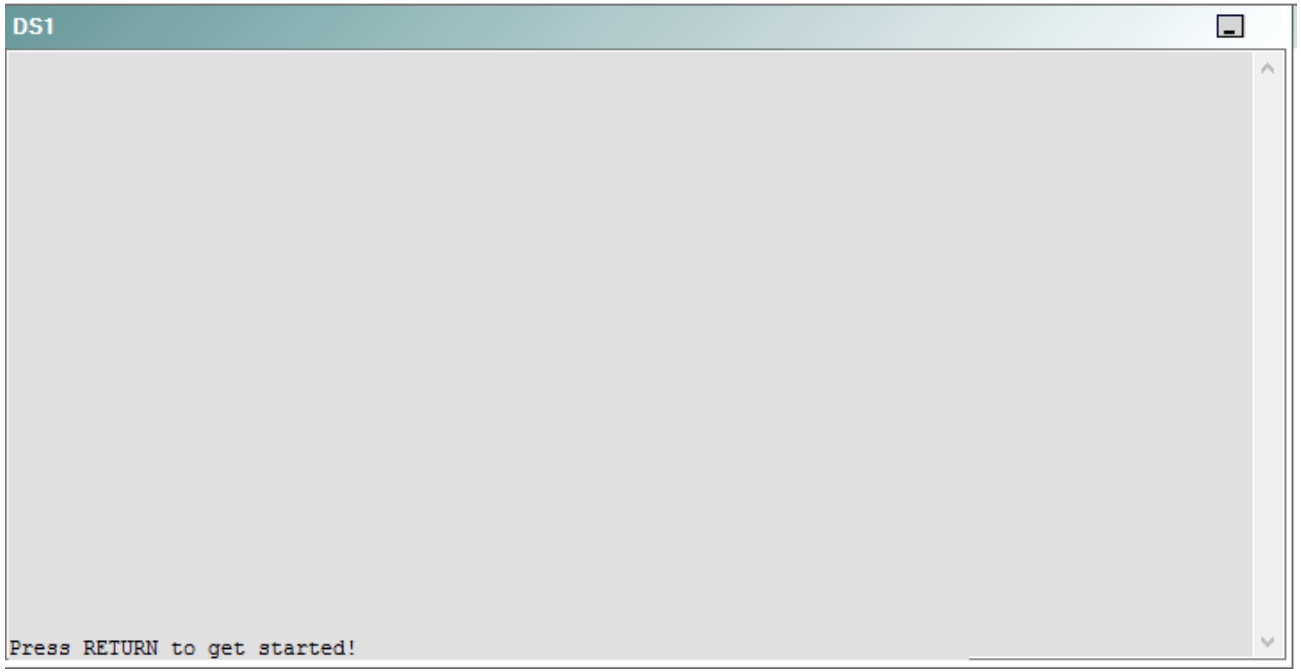

R4



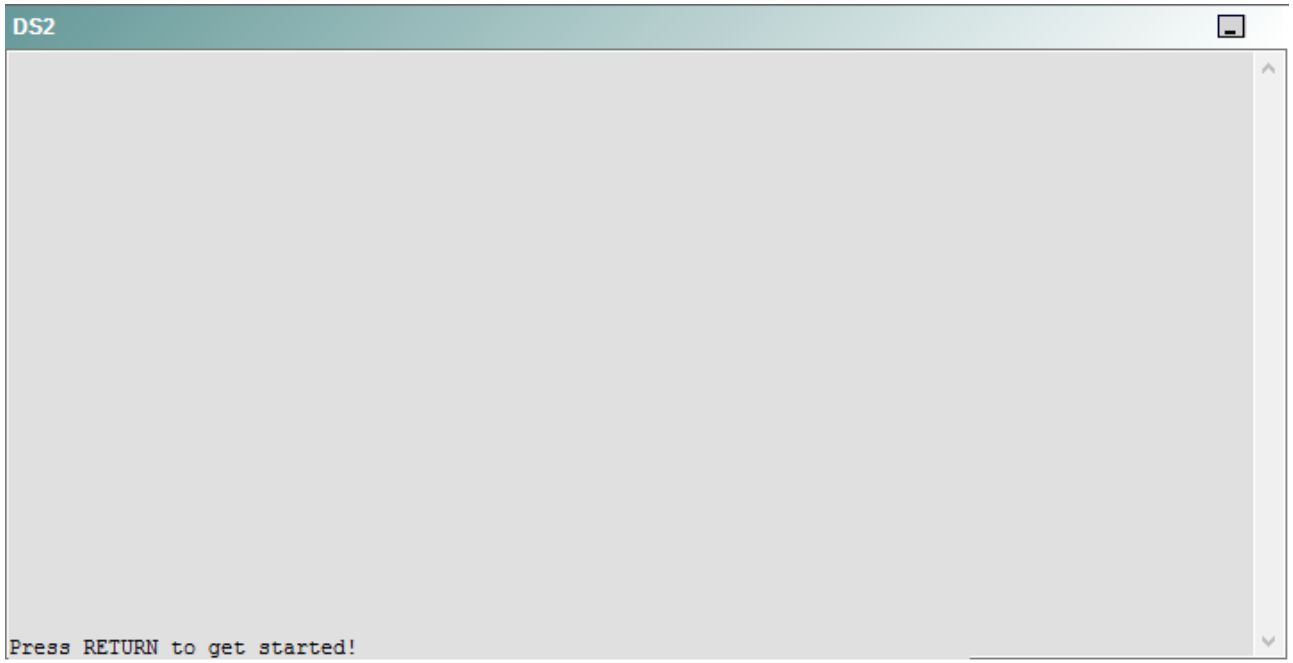

R5



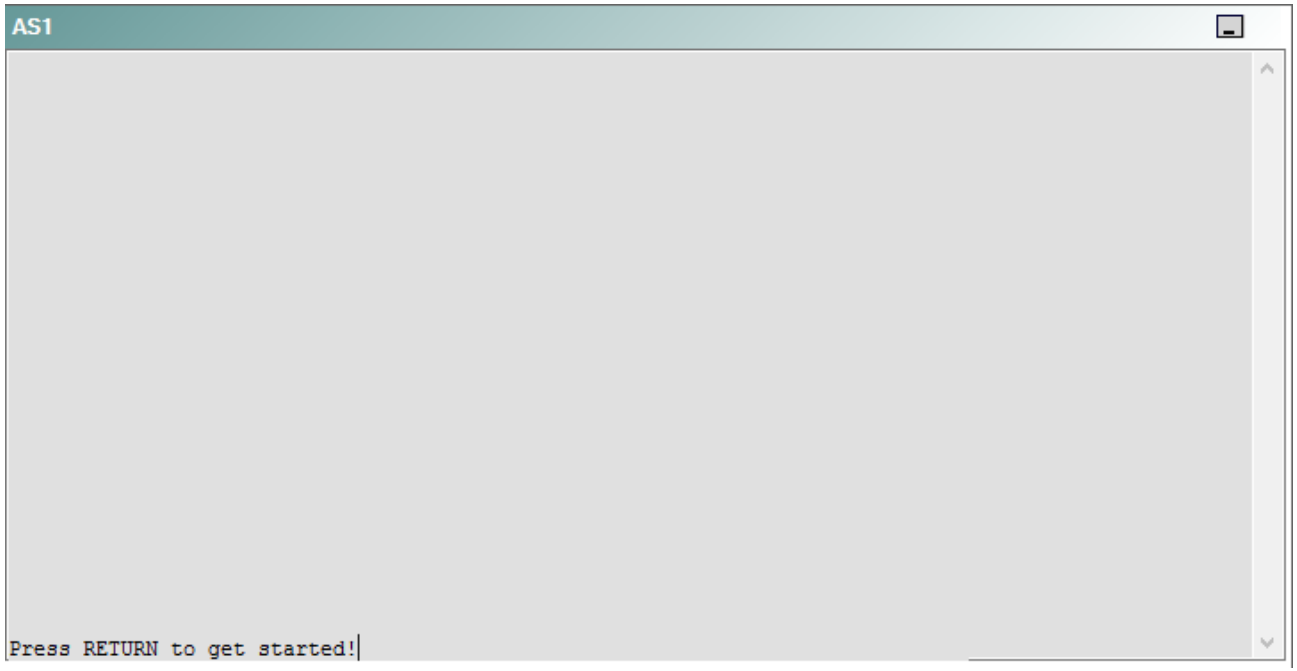

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that R5 is no longer able to ping the IPv6 loopback address 2000::10:1 on R1.

Which of the following is most likely to solve the problem?

A. issuing the **ipv6 ospf 100 area 0 command on Serial0/0.223**
B. issuing the **ipv6 ospf 100 area 10 command on Serial0/0.221**
C. issuing the **ipv6 ospf 100 area 0** command on Serial0/0.221
D. issuing the **ipv6 ospf 100 area 10** command on Serial0/0.223
E. issuing the **ipv6 network 2000:10:1/128** command for OSPF 15
F. issuing the **ipv6 network 2010:10:1/128** command for OSPF 100
G. issuing the **redistribute static** command for OSPF 15
H. issuing the **redistribute static** command for OSPF 100

**Correct Answer:** B
**Section: (none)**

**Explanation**

**Explanation/Reference:**
Explanation:

You should issue the **ipv6 ospf 100 area 10** command on the Serial0/0.221 interface of R2. To determine which device is the source of the problem, you should issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from R5 to the closest device and work your way up the network until communication is lost, or you can ping from R5 to the farthest device and work your way back to R5 until pings are successful. Alternatively, you can trace from R5 to R1 and see where communication is lost along the path to the destination device.

In this scenario, if you were to issue the **ping 2010::10:1** command from R5, you would receive the following output:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010::10:1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

The ….. in the output indicates that the attempt to trace to the IP version 6 (IPv6) address 2010::10:1, which has been assigned to the Serial0/0 interface on R1, has timed out. R5, which has a Tunnel0 interface that has been assigned the IPv6 address 2010::21:2 can reach the IPv6 address 2010::21:1 on R4 as well as the IPv6 address assigned to R3. Additionally, if you were to issue the ping **2010::10:2** command on R5, you would receive the following output:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010::10:2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 308/492/900 ms
```

The IPv6 address 2010::10:2 has been assigned to the Serial0/0.221 interface of R2. The !!!!! in the output indicates that the attempt to ping the IPv6 address 2010::10:2 was successful. Because you are able to ping the Serial0/0.221 interface on R2, but not the Serial0/0 interface on R1, the problem is most likely located between R2 and R1.

Once you have determined where connectivity is lost, you can begin to troubleshoot the cause of the problem. Issuing the **show ipv6 interface Serial0/0** command on R1 reveals that the interface is up and the line protocol is up on Serial0/0, which eliminates Open Systems Interconnection (OSI) Physical layer problems and OSI Data Link layer problems on R1 as possible causes of the loss of connectivity, as shown in the following partial output:

```
R1#show ipv6 interface Serial 0/0
Serial0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::CE00:9FF:FEB0:10
  Description: Link to R2
  Global unicast address(es):
    2010::10:1, subnet is 2010::10:0/124
```

Additionally, issuing the **show ipv6 interface Serial0/0.221** command on R2 reveals that the interface is up and the line protocol is up on Serial0/0.221, thus eliminating Physical layer problems and Data Link layer problems on R2. Therefore, you should continue troubleshooting at the Network layer of the OSI model.

All the routers in this scenario are using Open Shortest Path First version 3 (OSPFv3) to route IPv6 traffic. If you were to issue the **show ipv6 ospf** command on R1, you would receive the following output:

```
Routing Process "ospfv3 100" with ID 192.168.99.1
 It is an autonomous system boundary router
 Redistributing External Routes from,
    static
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Reference bandwidth unit is 100 mbps
    Area 10
      Number of interfaces in this area is 2
      SPF algorithm executed 8 times
      Number of LSA 15. Checksum Sum 0x0817DD
      Number of DCbitless LSA 0
      Number of indication LSA 0
      Number of DoNotAge LSA 0
      Flood list length 0
```

The output above indicates that R1 has two interfaces that have been configured in Area 10 of OSPFv3 process 100. If you were to issue the **show running-config**

command on R1, you would receive the following partial output:

```
interface Loopback6
 no ip address
 ipv6 address 2000::10:1/128
 ipv6 ospf 100 area 10
!
interface Serial0/0
 description Link to R2
 ip address 192.168.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 encapsulation frame-relay
 ntp broadcast
 ipv6 address 2010::10:1/124
 ipv6 ospf network point-to-point
 ipv6 ospf 100 area 10
 serial restart-delay 0
 clock rate 115200
```

The output above indicates that both the Loopback6 interface and the Serial0/0 interface have been configured for Area 10 of OSPFv3 process 100. However, if you were to issue the **show ipv6 ospf** command on R2, you would receive the following output:

```
Routing Process "ospfv3 100" with ID 192.168.99.2
 It is an area border and autonomous system boundary router
 Redistributing External Routes from,
    static
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 2. 2 normal 0 stub 0 nssa
 Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
      Number of interfaces in this area is 2
      SPF algorithm executed 8 times
      Number of LSA 15. Checksum Sum 0x067522
      Number of DCbitless LSA 0
      Number of indication LSA 0
      Number of DoNotAge LSA 0
      Flood list length 0
    Area 10
 Number of interfaces in this area is 1
SPF algorithm executed 9 times
Number of LSA 14. Checksum Sum 0x089415
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

The output above indicates that R2 has two interfaces that are configured for OSPFv3 Area 0 and one interface that is configured for OSPFv3 Area 10. Although R2 has an interface configured for Area 10, issuing the **show running-config** command on R2 reveals that the interface configured for Area 10 is the Loopback 6 interface, not the Serial0/0.221 interface that connects to R1, as shown in the following partial output:

```
interface Loopback6
 no ip address
 ipv6 address 2000::11:1/128
 ipv6 ospf 100 area 10
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 clock rate 115200
 no frame-relay inverse-arp
!
interface Serial0/0.221 point-to-point
 description Link to R1
 ip address 192.168.1.2 255.255.255.252
 snmp trap link-status
 ipv6 address 2010::10:2/124
 ipv6 ospf 100 area 0
 frame-relay interface-dlci 221
!
interface Serial0/0.223 point-to-point
 description Link to R3
 ip address 192.168.1.5 255.255.255.252
 snmp trap link-status
 ipv6 address 2010::1:1/124
 ipv6 ospf 100 area 0
 frame-relay interface-dlci 223
```

Therefore, an OSPFv3 area mismatch exists on R2. Issuing the **ipv6 ospf 100 area 10** command on the Serial0/0.221 interface on R2 will configure the Serial0/0.221 interface for OSPFv3 Area 10 and restore connectivity between R1 and the rest of the network.

You should not issue the **ipv6 ospf 100 area 0** command on Serial0/0.221 or on Serial0/0.223 on R2. Area 0 is the OSPFv3 backbone area and should directly connected to every other area in the OSPFv3 configuration. Therefore, the R2 interface Serial0/0.221 should be configured in Area 10/ Additionally, the R2 interface Serial0/0.223 has already been configured in Area 0 in this scenario.

You should not issue the **ipv6 ospf 100 area 10** command on Serial0/0.223 on R2. Area 0 is the OSPFv3 backbone area and should directly connect to every other

area in the OSPFv3 configuration. Therefore, the R2 interface Serial0/0.223 should remain configured in Area 0.

You should not issue an **ipv6 network** command for OSPF 15 on any device. In this scenario, the OSPF 15 process is used on R3, R4, R5, DS1, and DS2 to route IPv4 traffic, not IPv6. Additionally, you need not issue an **ipv6 network** command for OSPF 100 on any device. In this scenario, OSPF process 100 is used to route Ipv6 packets between R1, R2, R3, R4, and R5; however, you should enable OSPFv3 routing at the interval level, not by issuing the **ipv6 network** command at the routing process level.

You need not issue the **redistribute static** command or the **redistribute connected** command on any device. In this scenario, all Ipv6 traffic is routed through OSPFv3. There are no static IPv6 routes that need to be redistributed into OSPFv3.

You should not issue the **no ipv6 ospf hello-interval 80** command on S0/0 on R1. In this scenario, the hello and dead intervals on all routers are set to their default values. Therefore, a hello interval mismatch cannot be the cause of the problem.

You should not issue the **no passive-interface default** command for OSPFv3 process 100 on R1. Although setting the OSPFv3 interface to passive could result in a loss of connectivity, the Loopback6 interface on R1 has not been configured as a passive interface.

**QUESTION 57**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

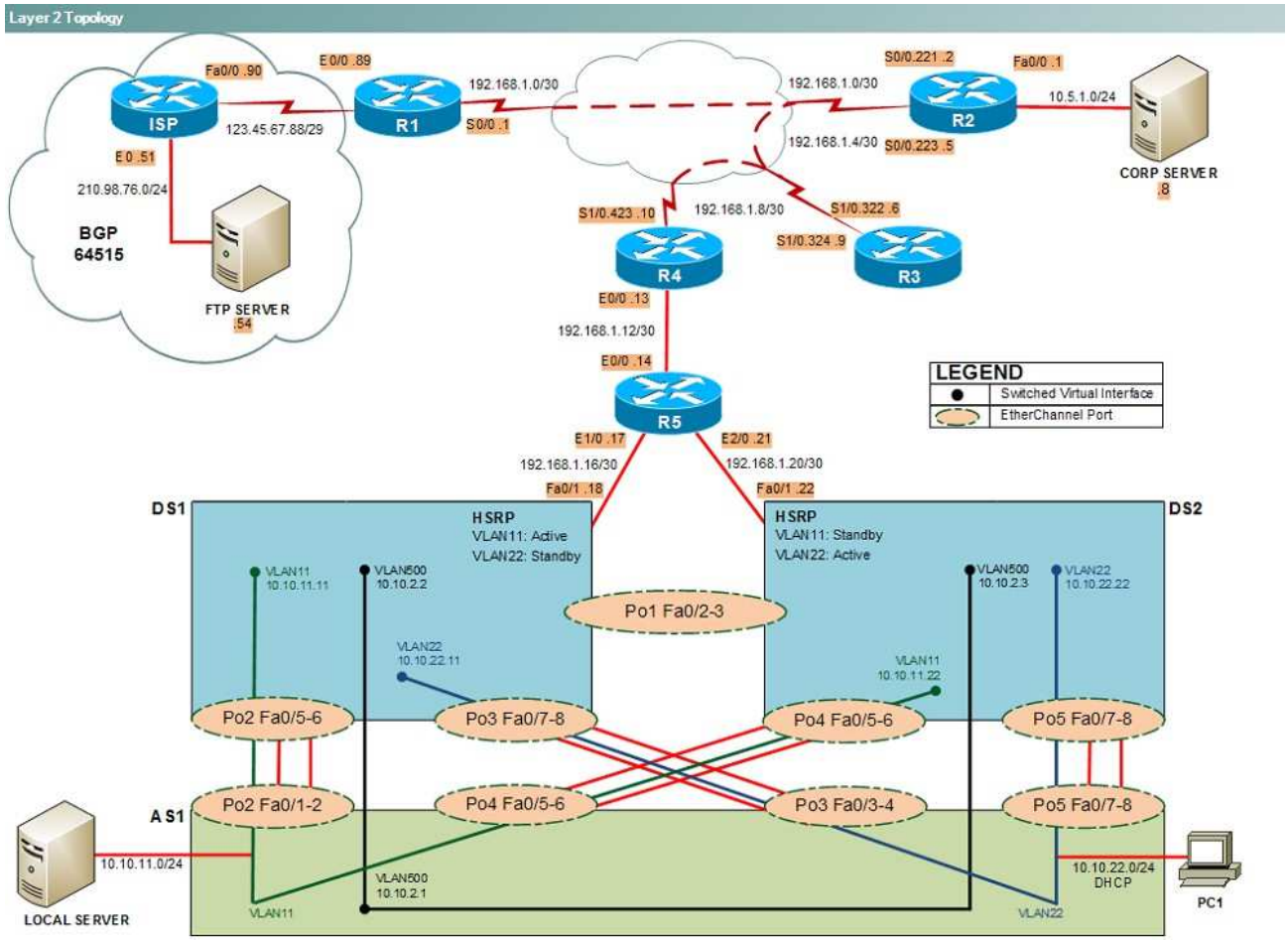
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

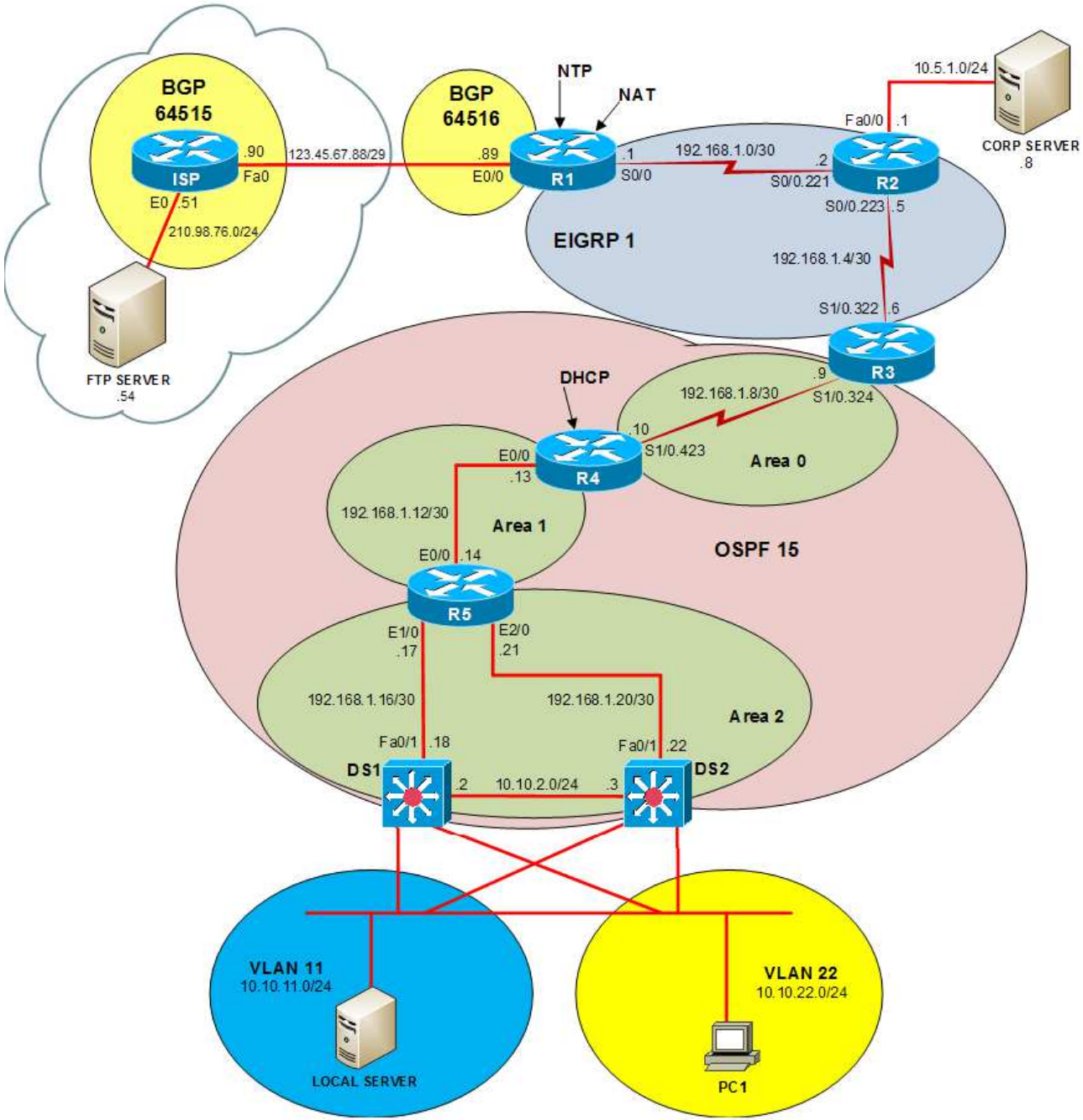
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

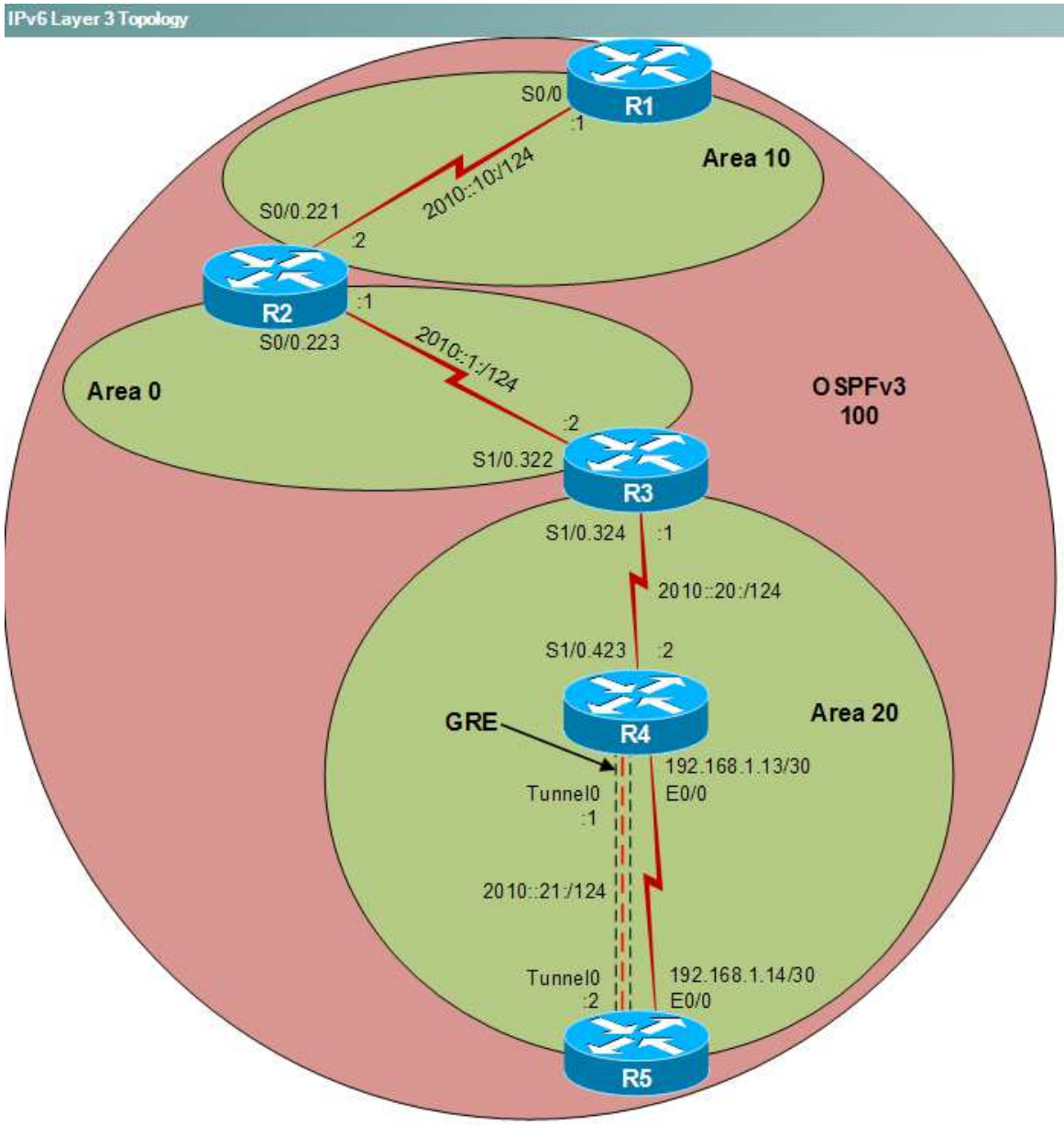
**Layer 2 Topology**



IPv4 layer 3 Topology

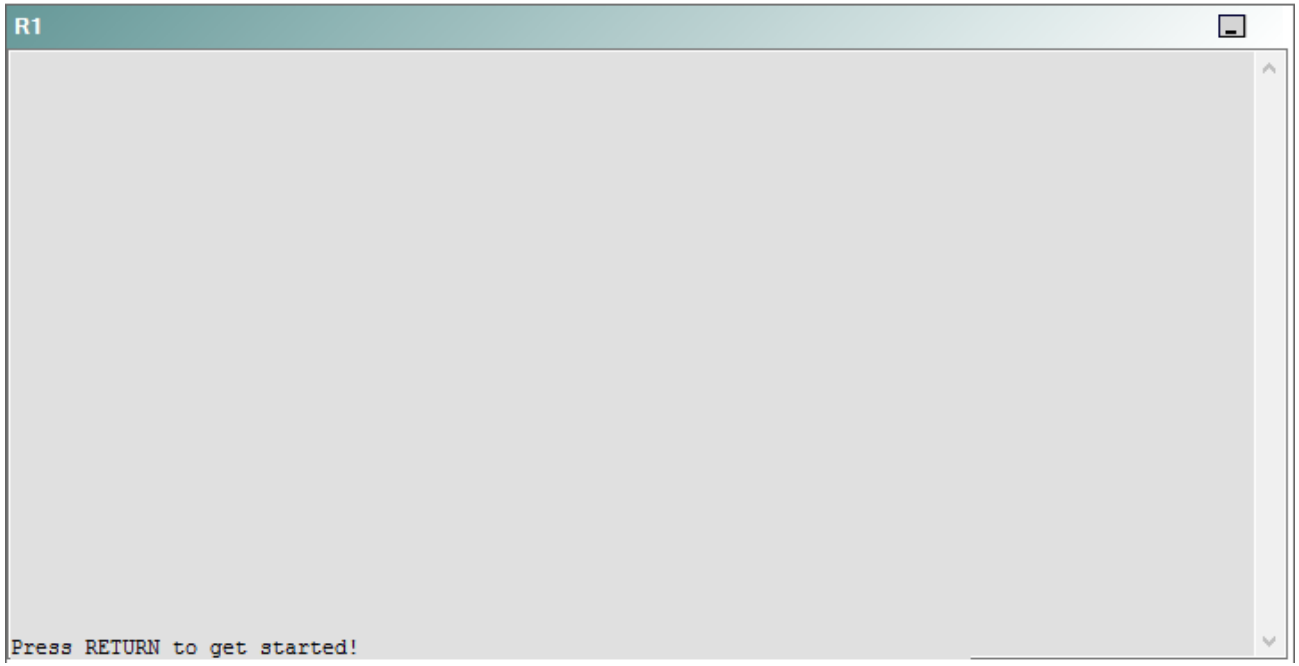

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

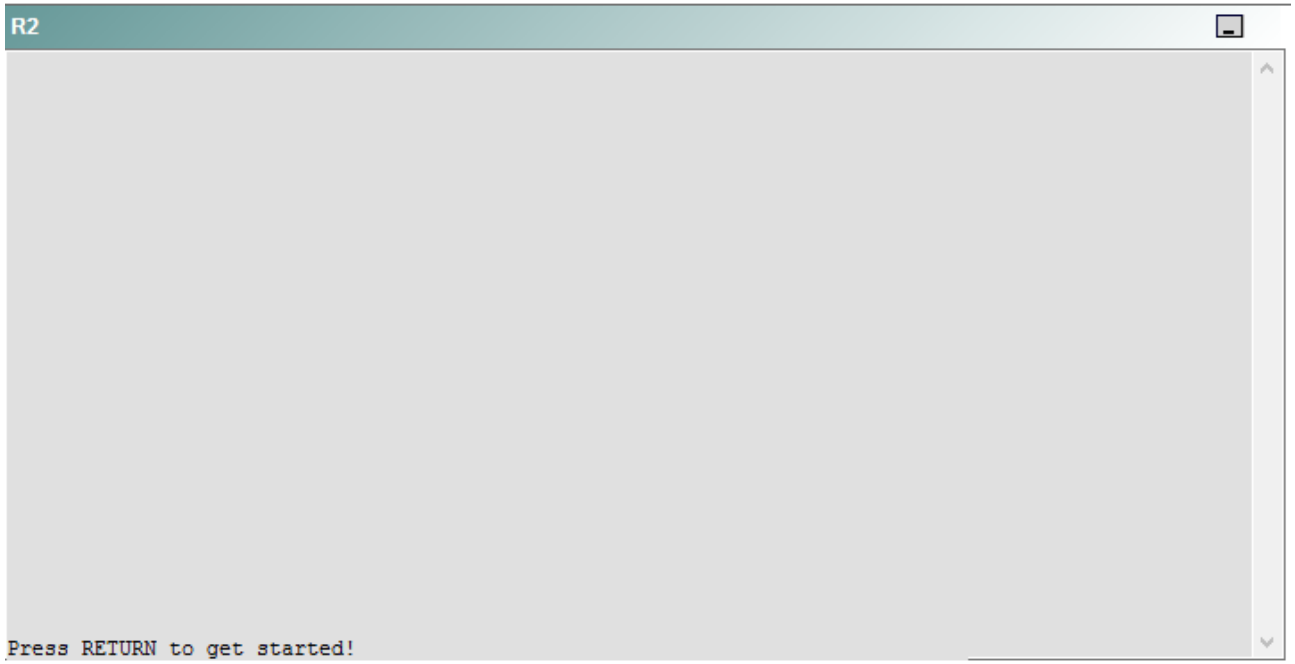



https://www.gratisexam.com/

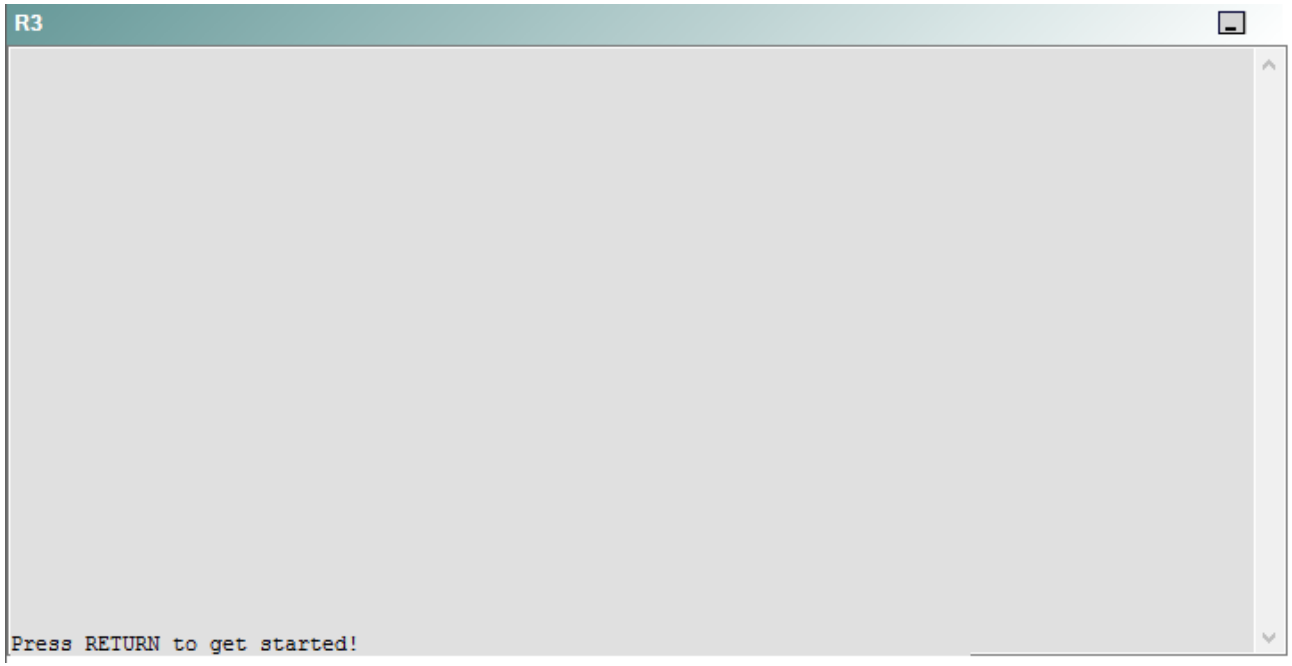
R1



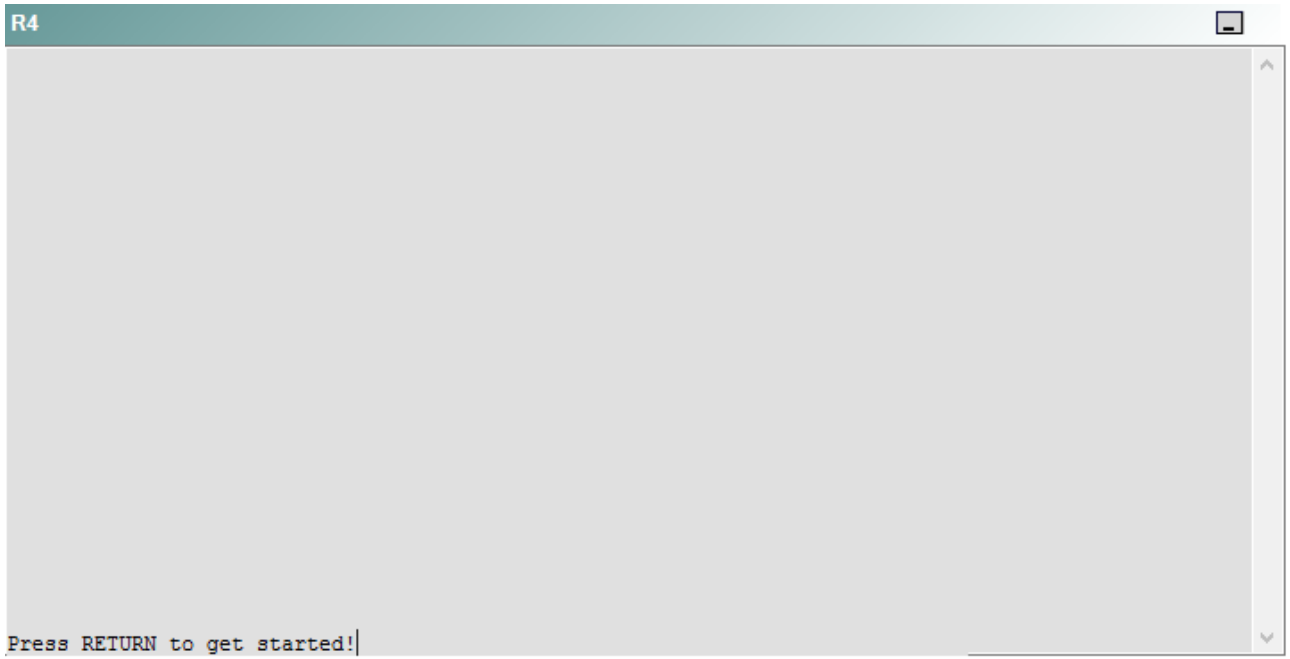

R2



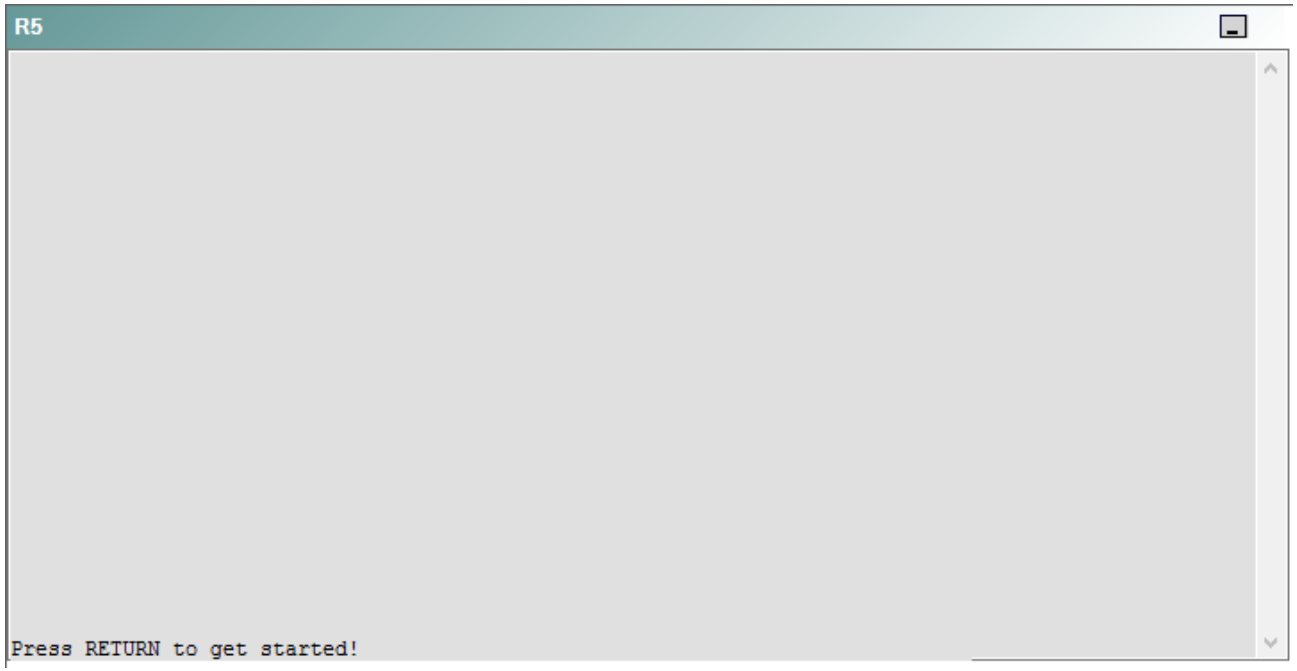

R3



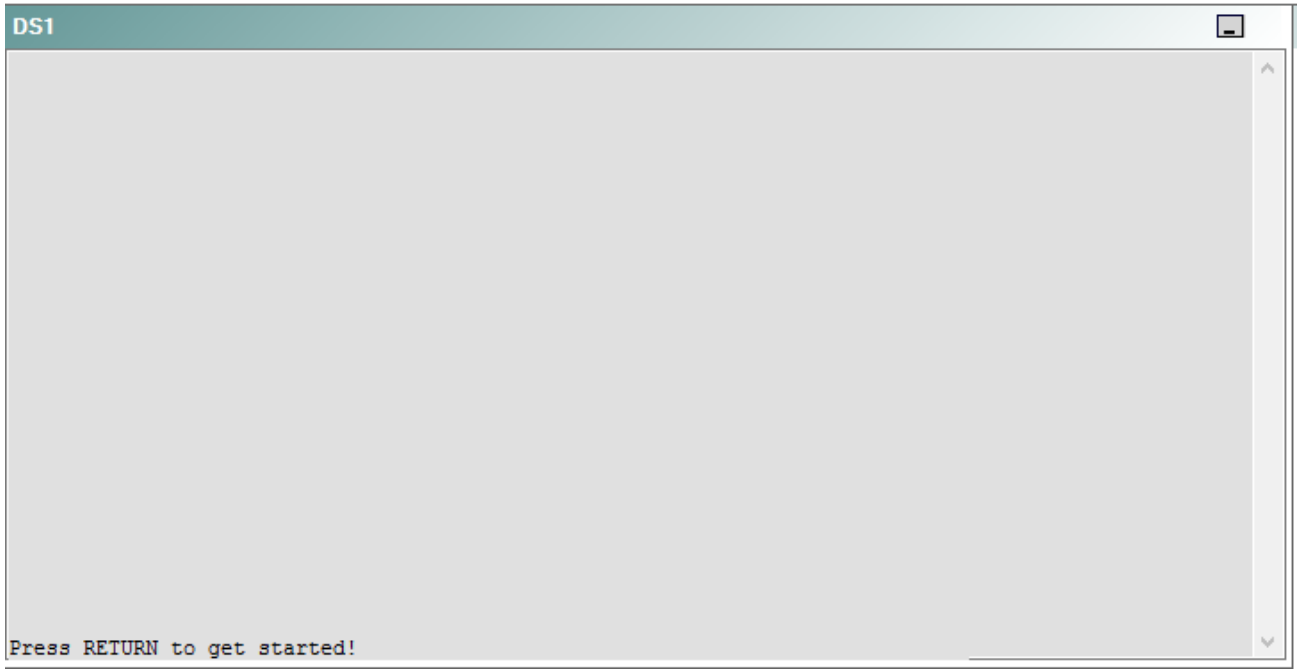

R4



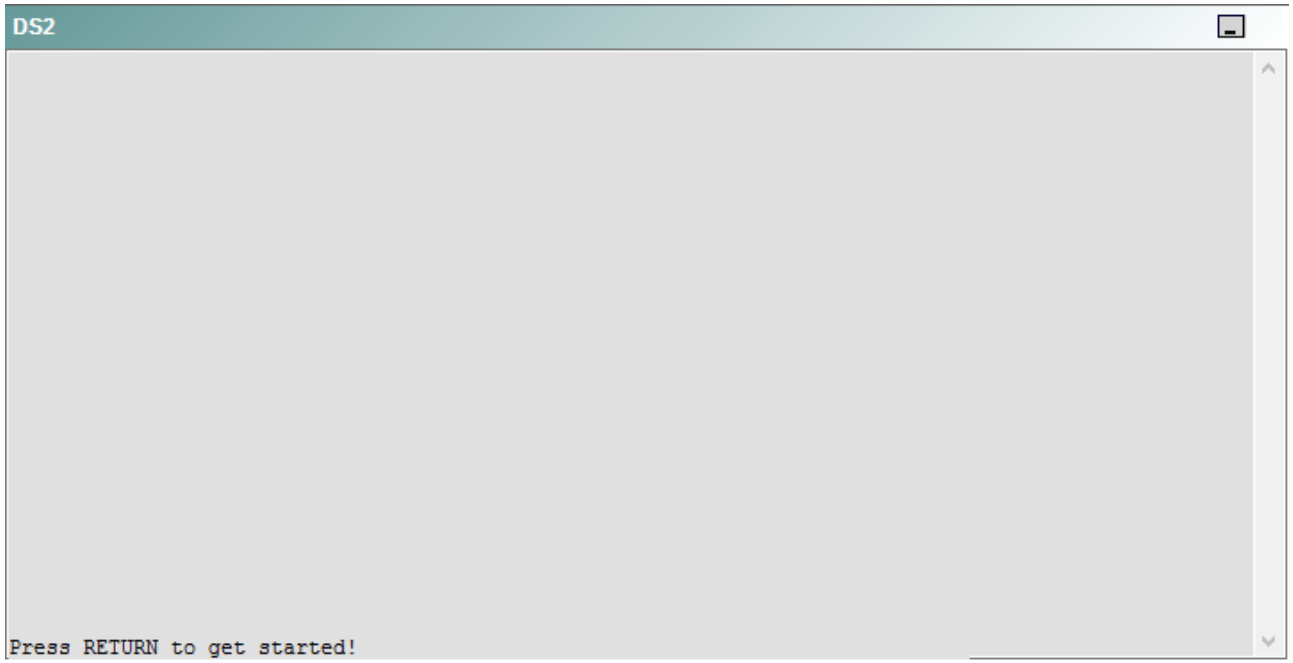

R5



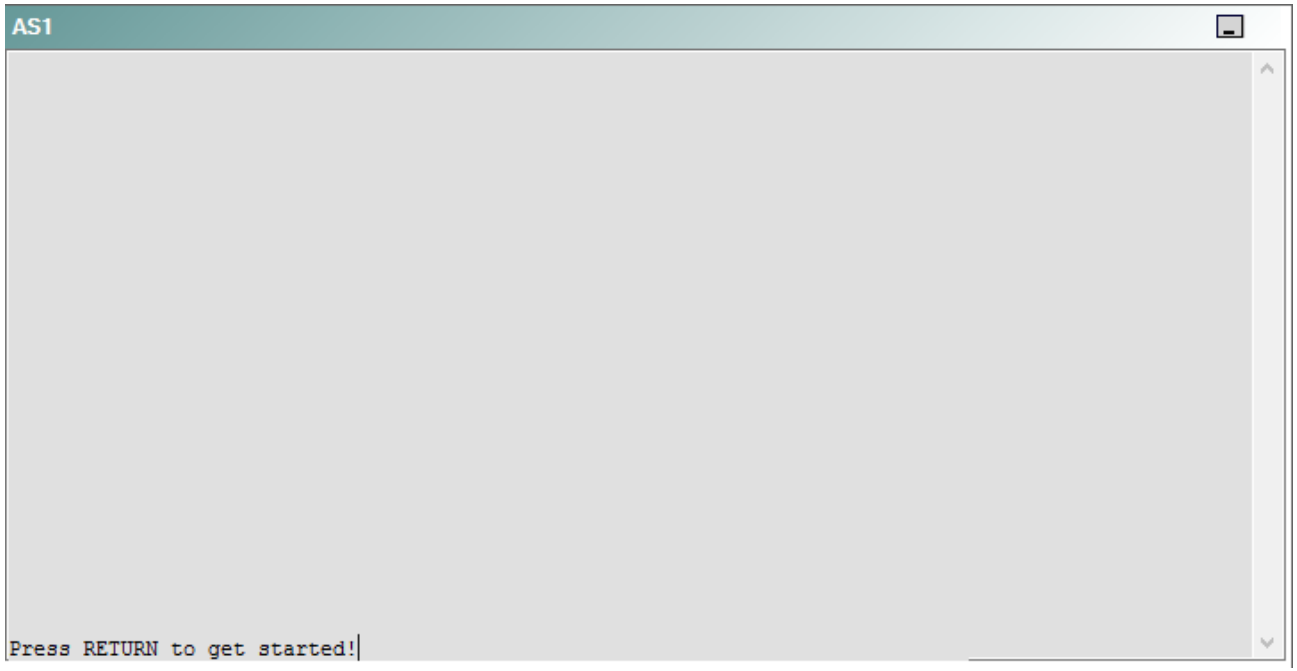

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. DHCP
C. Layer 3 addressing
D. Layer 3 security
E. Layer 2 security
F. STP
G. Etherchannel
H. VLAN configuration
I. interface

**Correct Answer:** E

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 58**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

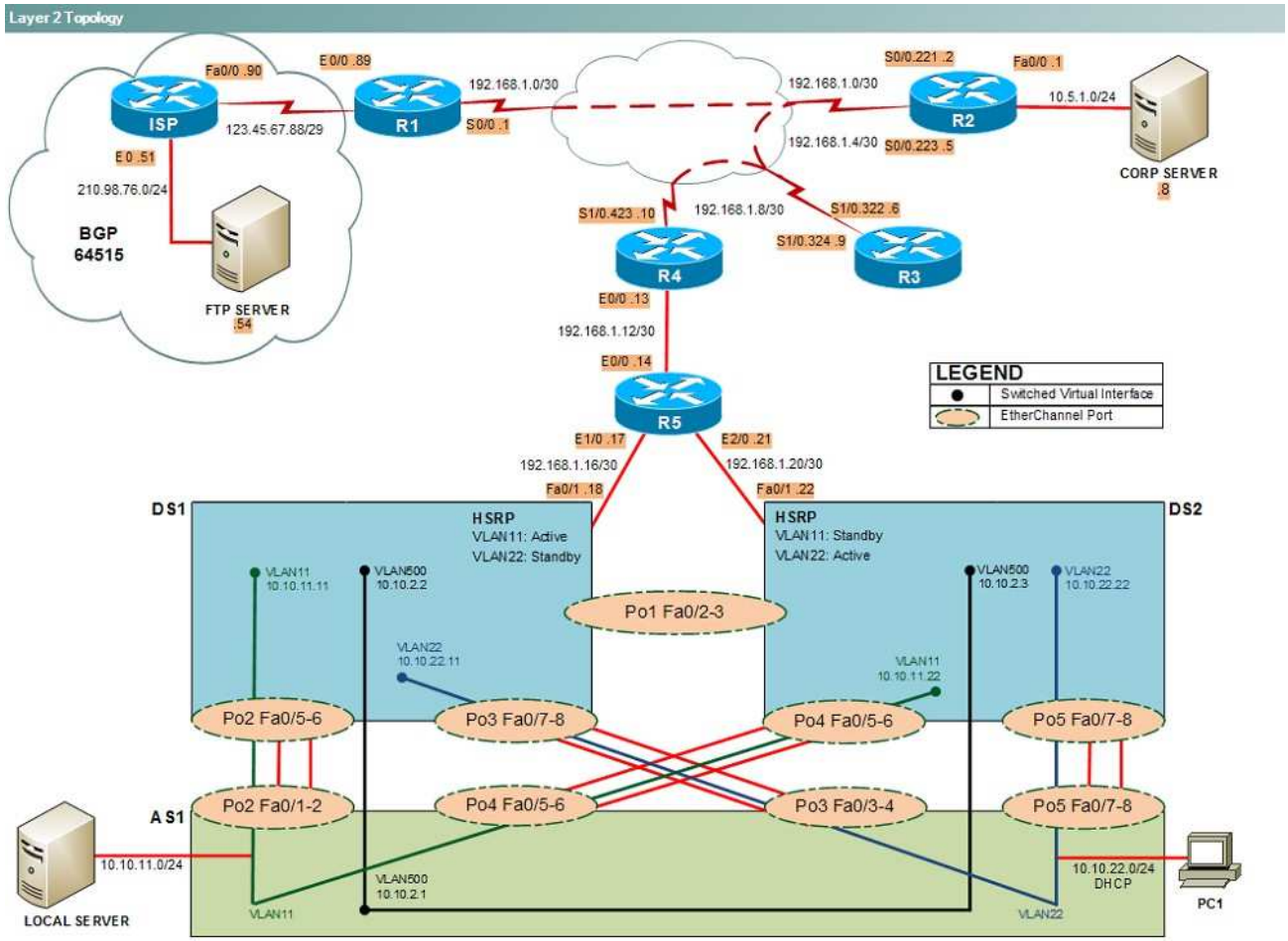
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

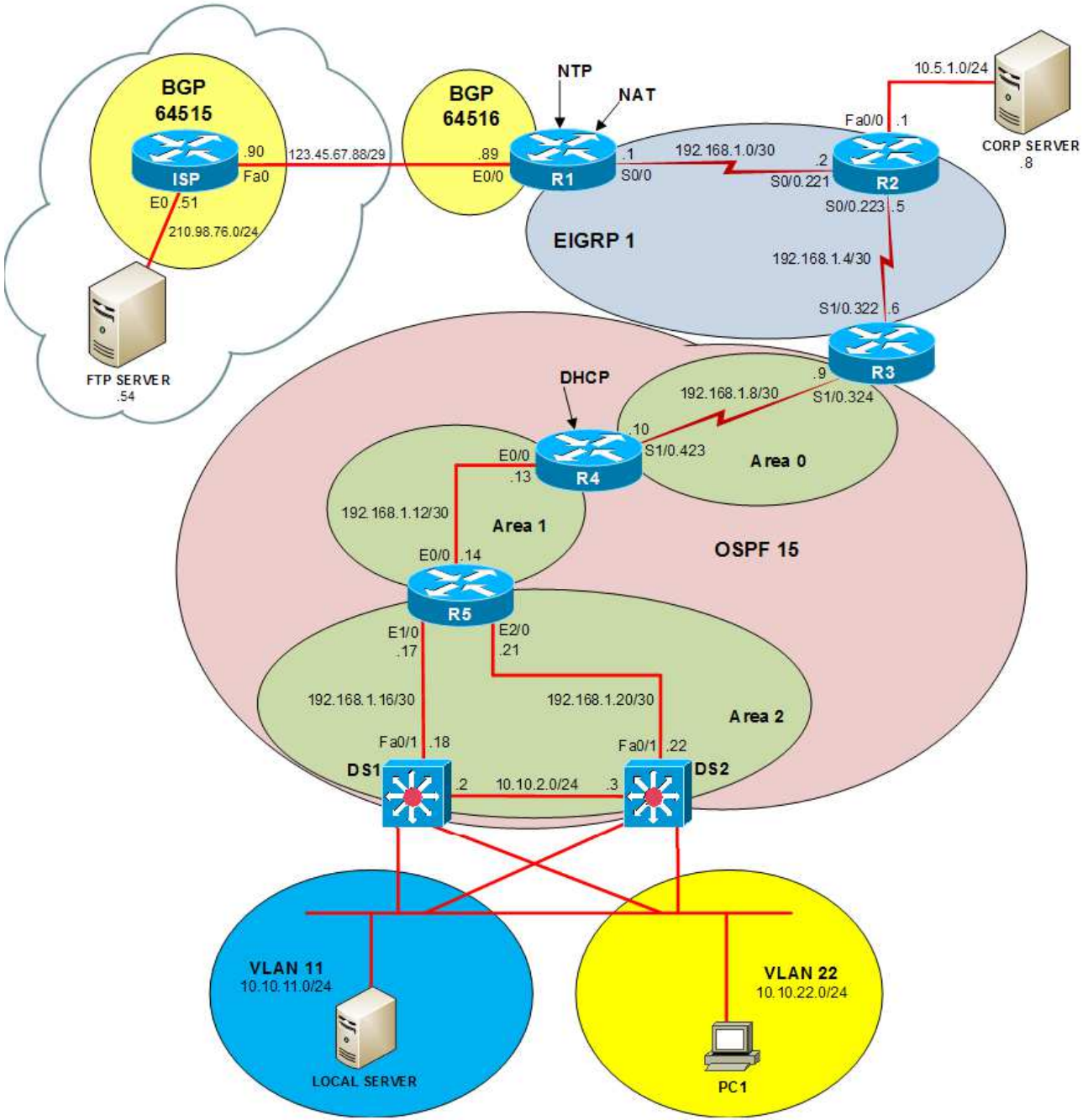
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

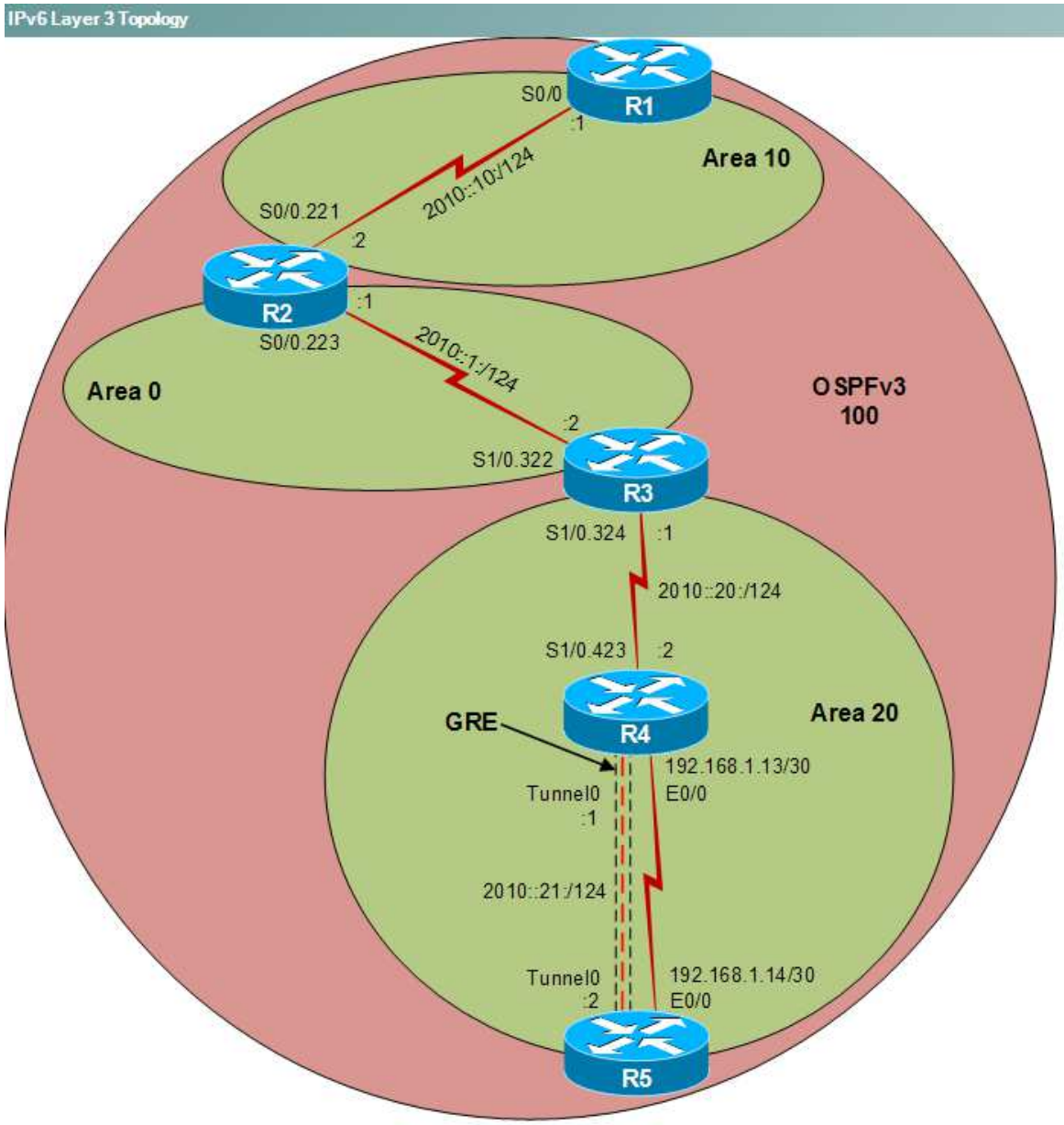
**Layer 2 Topology**




IPv4 layer 3 Topology

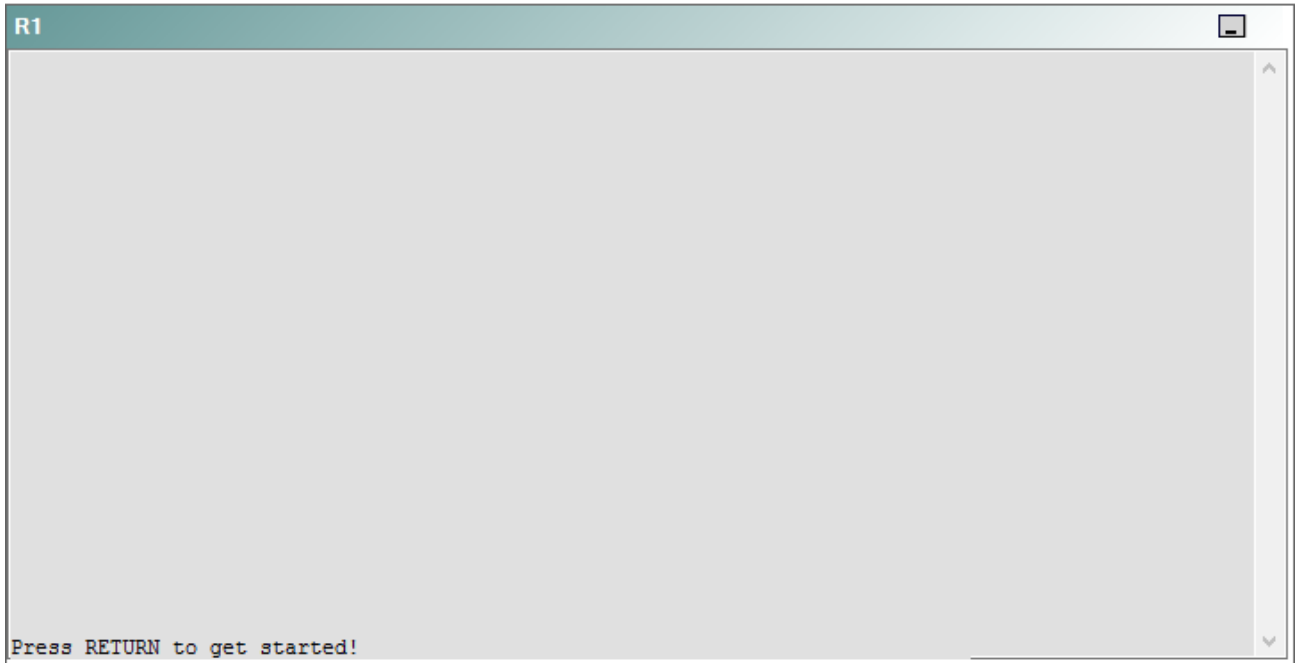

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

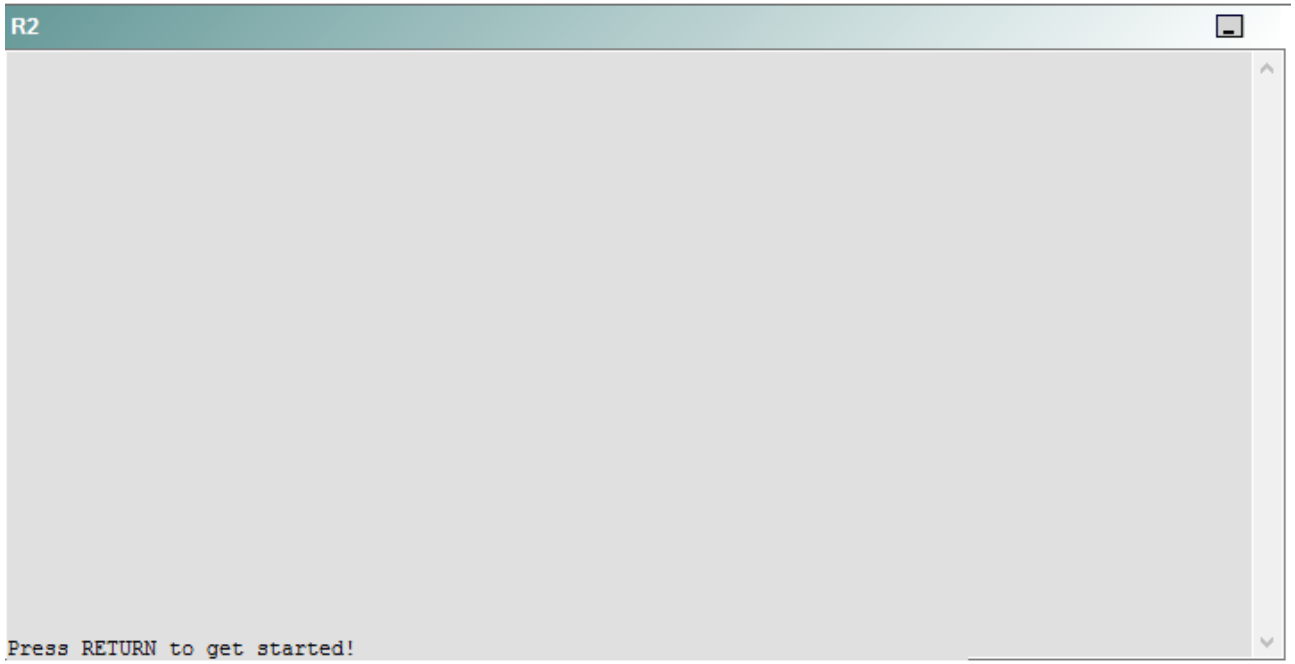



https://www.gratisexam.com/

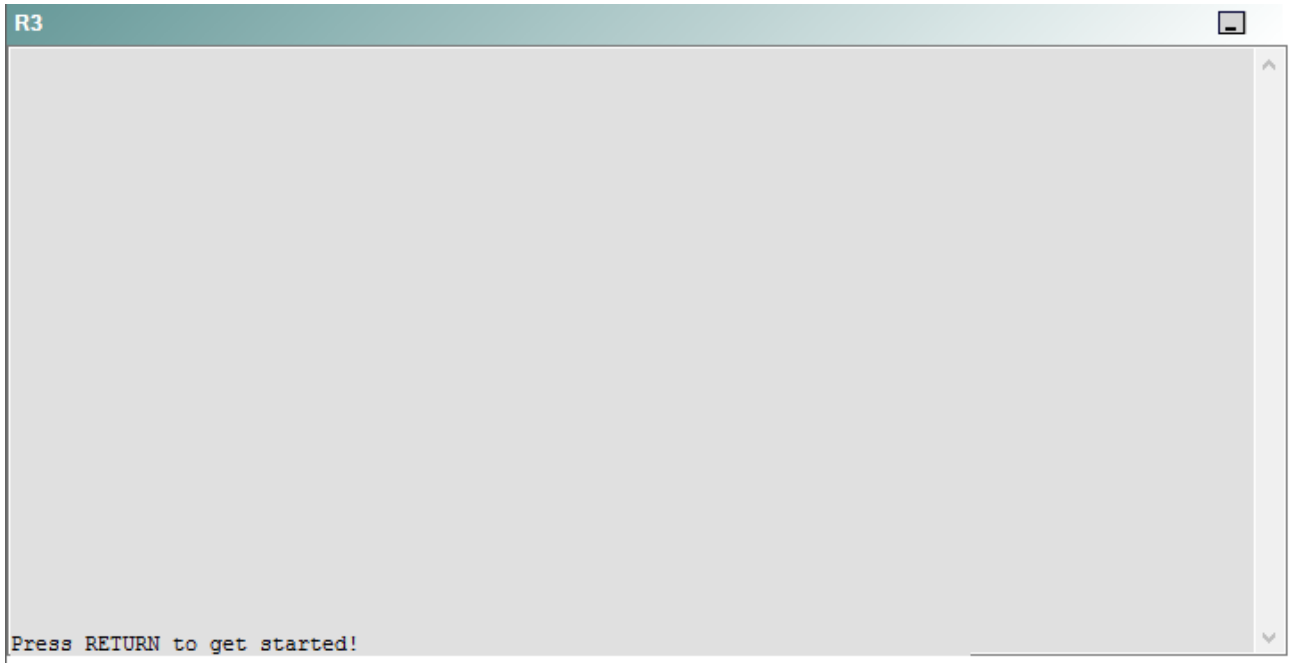
R1



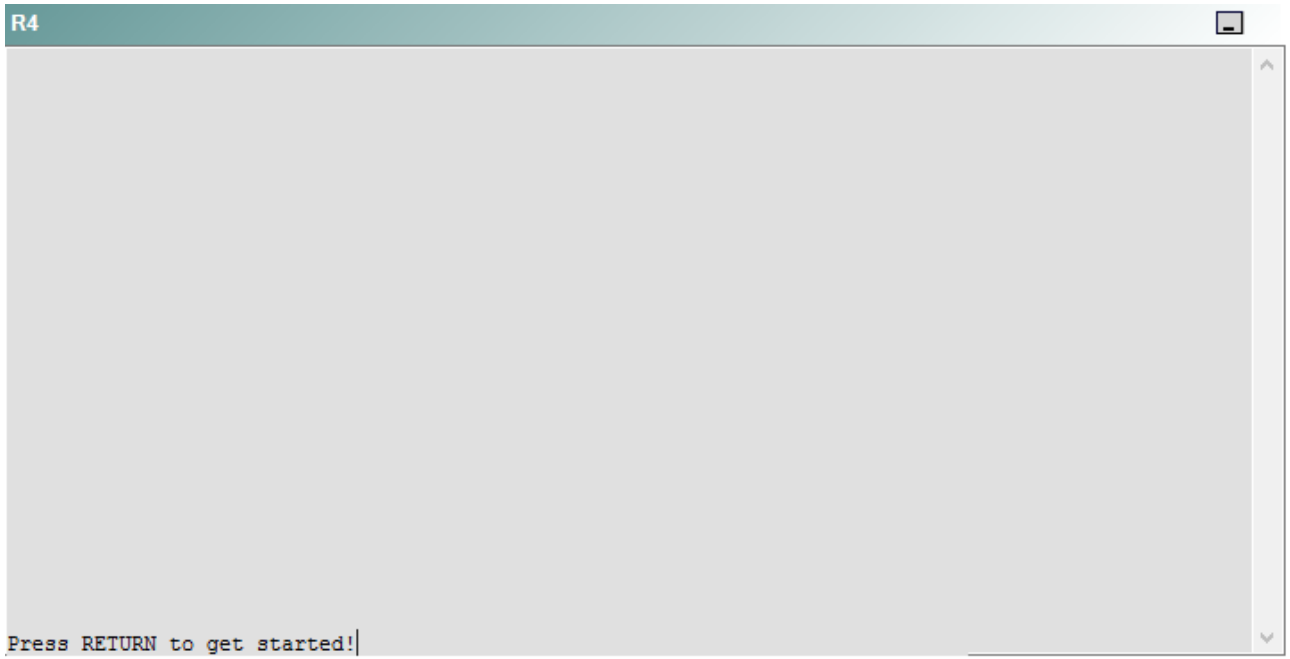

R2



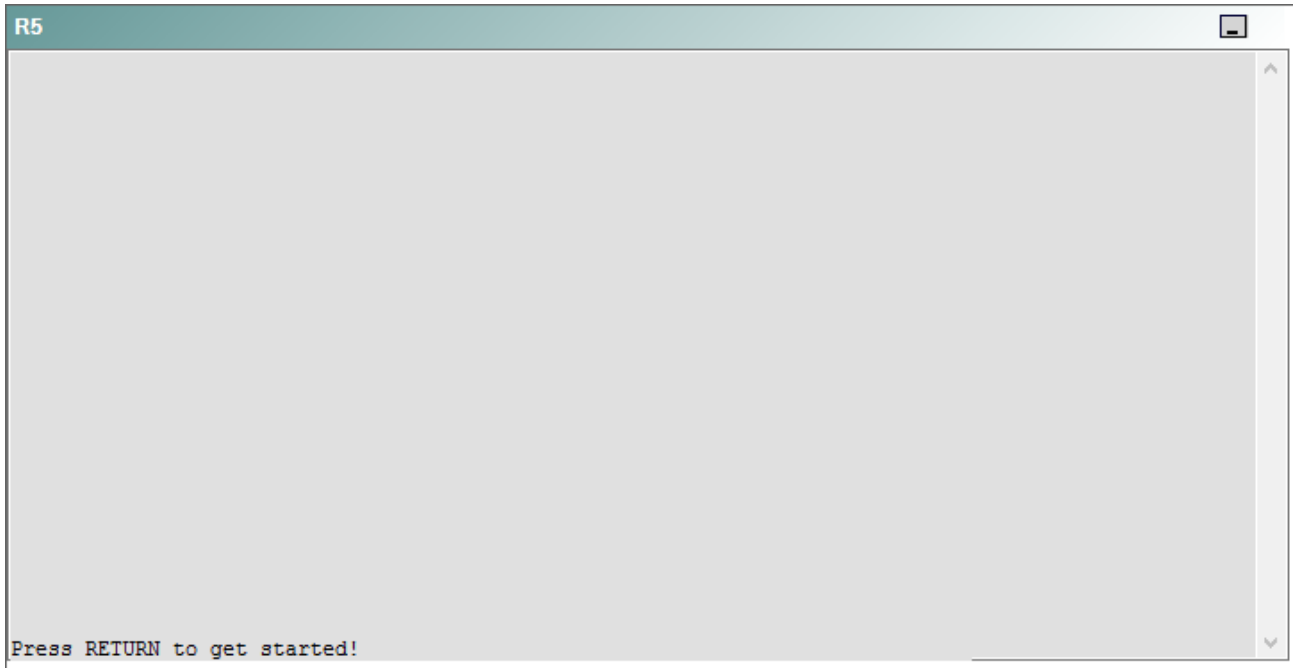

R3



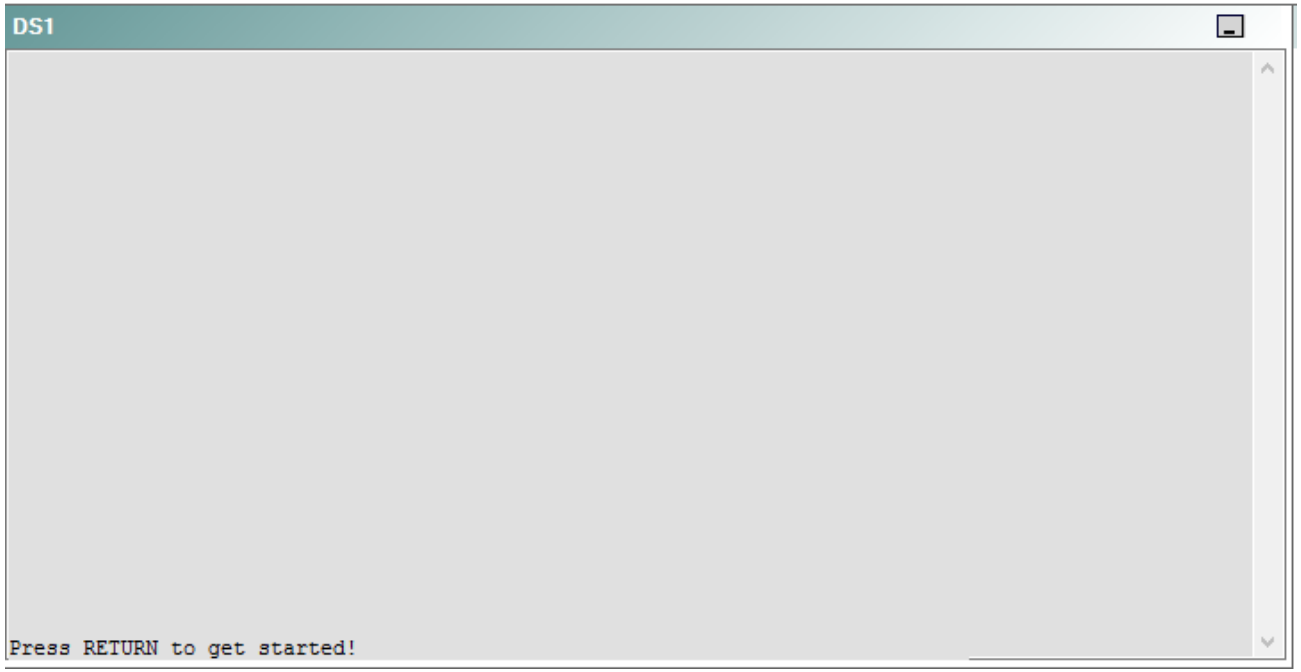

R4



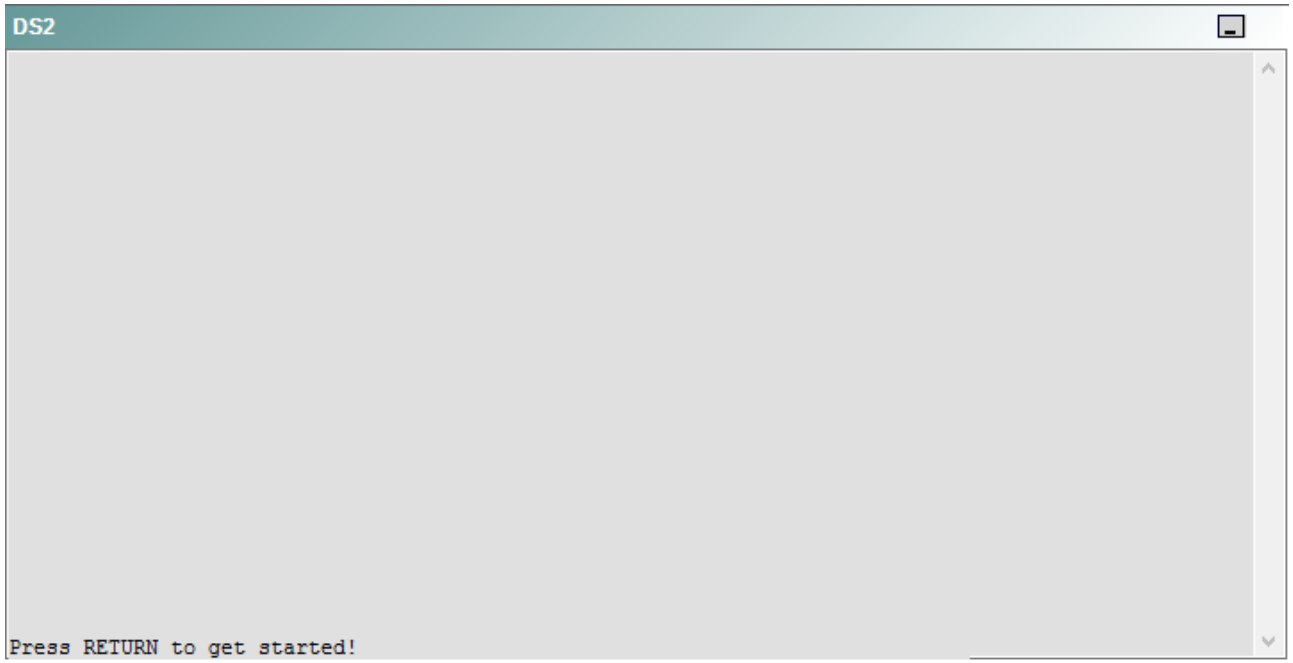

R5



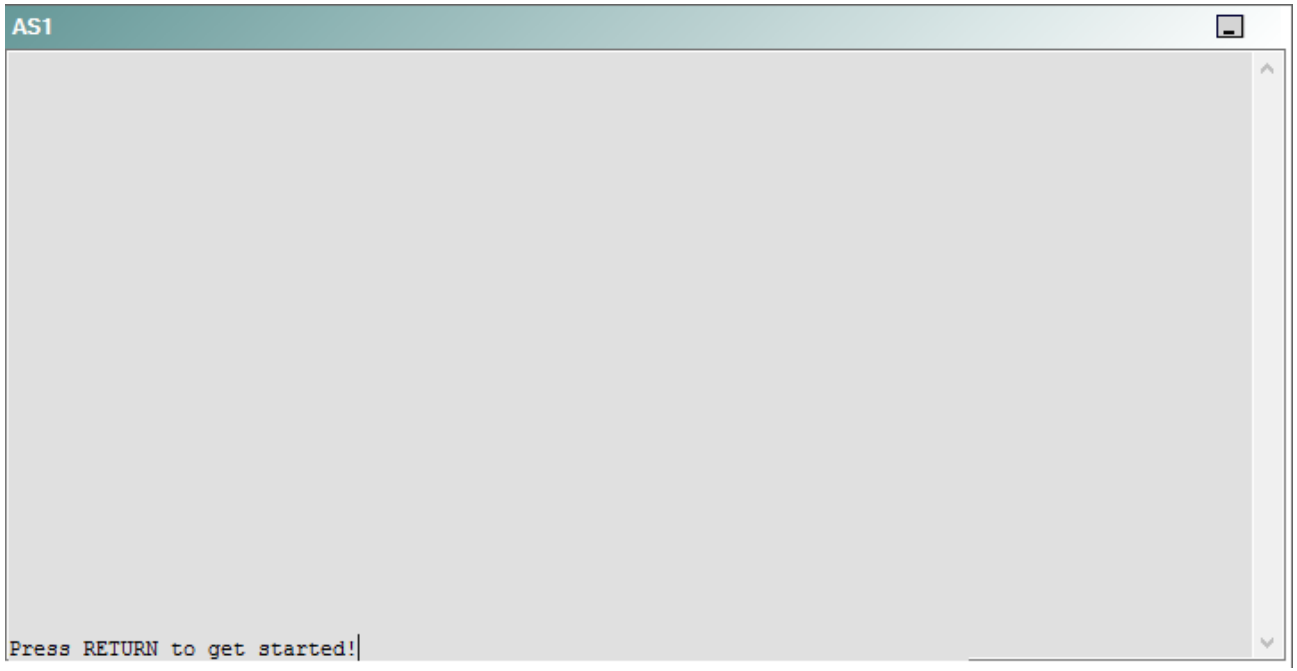

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. issuing the **no port security** command and the **no shutdown** command on Fa0/1 through Fa0/4
B. issuing the **no port security** command and the **no shutdown** command on Fa0/5 through Fa0/8
C. issuing the **no port security** command and the **no shutdown** command on Fa0/11
D. issuing the **no port protected** command on Fa0/11
E. issuing the **port security max-mac-count 0** command on Fa0/1 through Fa0/8
F. issuing the **port security max-mac-count 0** command on Fa0/1 through Fa0/11

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

You should issue the **no port security** command and the **no shutdown** command on interface FastEthernet0/11 on AS1. To determine which device is the source of the problem, you should issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from R5 to the closest device and work your way up the network until communication is lost, or you can ping from R5 to the farthest device and work your way back to R5 until pings are successful. Alternatively, you can trace from R5 to R1 and see where communication is lost along the path to the destination device.

In this scenario, if you were to issue the ping **210.98.76.54** command from R2, you would receive the following output:

```
Pinging 210.98.76.54 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
```

The *Destination host unreachable* message in the output above indicates that there is no route from PC1 to the IP address 210.98.76.54, which is the IP address assigned to the external server. You would receive similar output if you were to issue the **ping 10.10.22.25** command from PC1. The IP address 10.10.22.25 is the virtual IP address assigned to the Hot Standby Router Protocol (HSRP) configuration on DS1 and DS2.

Additionally, if you were to issue the **ipconfig** command on PC1, you would receive the following partial output:

```
Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Media disconnected
```

The output above indicates that an Open Systems Interconnection (OSI) Physical layer problem exists between PC1 and AS1, the device to which PC1 is directly connected. The *Media disconnected* message indicates that there is no active link between PC1 and AS1; therefore, the problem most likely lies between PC1 and AS1.

If you were to issue the **show interface FastEthernet0/11** command on AS1, you would receive the following partial output:

```
FastEthernet0/11 is administratively down, line protocol is down
  Hardware is Fast Ethernet, address is 0001.4213.e60b (bia 0001.4213.e60b)
  Description: Link to Client
```

The output above indicates that the FastEthernet0/11 interface is in the administratively down state. However, issuing the **no shutdown** command on AS1 would not resolve the problem. If you were to issue the **show port security** command on AS1 in this scenario, you would receive the following output:

```
Secure Port          Secure Addr    Secure Addr  Security   Security Action
                     Cnt (Current)  Cnt (Max)    Reject Cnt
-------------------  -------------  -----------  ---------- ------------------
FastEthernet0/11     1               1           1          Send Trap/Shut Down
```

In the output above indicates that the FastEthernet0/11 interface on AS1 has been configured with the **port security max-mac-count 1** command. The maximum number of Media Access Control (MAC) addresses that can connect to the FastEthernet0/11 interface has been configured to 1. Additionally, the *Security Reject Cnt* field in the output above indicates that a single security incident has occurred on the FastEthernet0/11 interface, which means that a second MAC address attempted to connect to the secured port. The **port security max-mac-count 1** command configures a switch port to allow only a single MAC address to connect to the configured port. If a device with a different MAC address connects to the port that is configured with port security, the port security configuration will either send a Simple Network Messaging Protocol (SNMP) trap message or shut down the port, depending on the configuration of the **port security action** command. In this scenario, the **port security action shutdown** command has been issued for the FastEthernet0/11 interface, as shown in the following partial output from the **show running-config** command on AS1.

```
AS1#show running-config
...
interface FastEthernet0/11
 description Link to Client
 shutdown
 port security
 port security max-mac-count 1
 port security action shutdown
 switchport access vlan 22
 switchport trunk native vlan 500
 spanning-tree portfast
```

Therefore, the port security configuration in this scenario has placed the FastEtherner0/11 interface in the administratively down state.

To resolve the problem, you should issue the **no port security** command on the FastEthernet0/11 interface on AS1. You should also issue the **no shutdown** command on AS1 because the interface will not automatically return from the administratively down state when port security is removed. Additionally, if you were to issue only the **no shutdown** command while the second MAC address was still connected to the FastEthernet0/11 interface, you would see the interface briefly enter the up state and when return to the administratively down state. Depending on the configuration of the **logging console** command, you might also see a security violation message regarding FastEthernet0/11.

You need not issue the **no port security** command and the **no shutdown** command on interfaces FastEthernet0/1 through FastEthernet0/8 on AS1, DS1, or DS2. Port security commands have not been issued on those interfaces in this scenario. Therefore, port security is not causing a problem on the interfaces from FastEthernet0/1 through FastEthernet0/8 on AS1, DS1, or DS2.

You need not issue the **no port protected** command on any interface on AS1, DS1, or DS2. The **no port protected** command disables Layer 2 port protection on

an interface. Layer 2 port protection prevents Layer 2 traffic from being forwarded between protected ports on the same switch. In this scenario, Layer 2 port protection has not been enabled on any interfaces on AS1, DS1, or DS2.

You should not issue the **port security max-mac-count 0** command on any interfaces on AS1, DS1, or DS2. The **port security max-mac-count** *number* command indicates the number of MAC addresses that can communicate through the port. The *number* parameter can be set to a value from 1 through 132. Therefore, the **port security max-mac-count 0** command contains invalid syntax.

**QUESTION 59**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

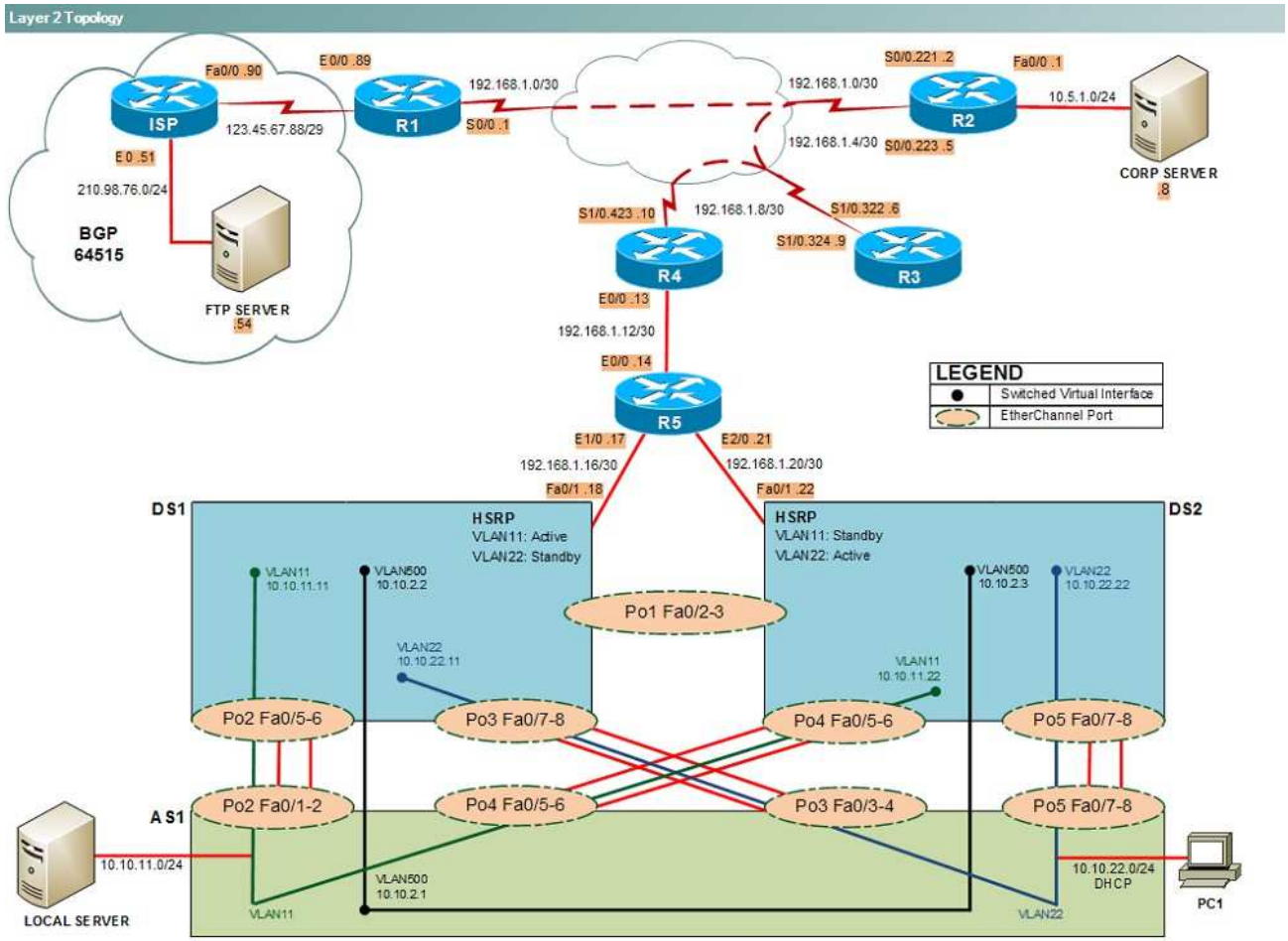
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

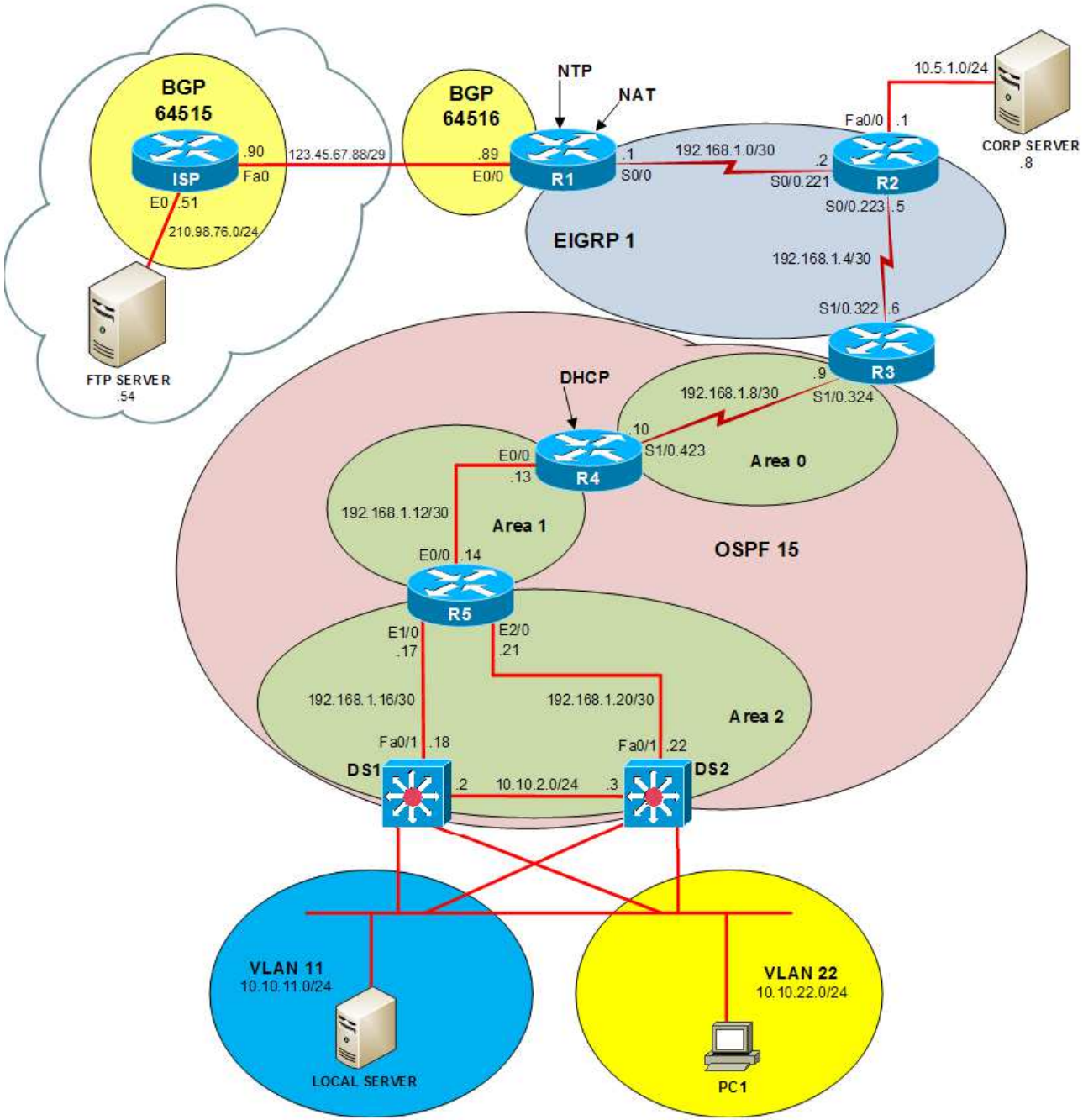
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

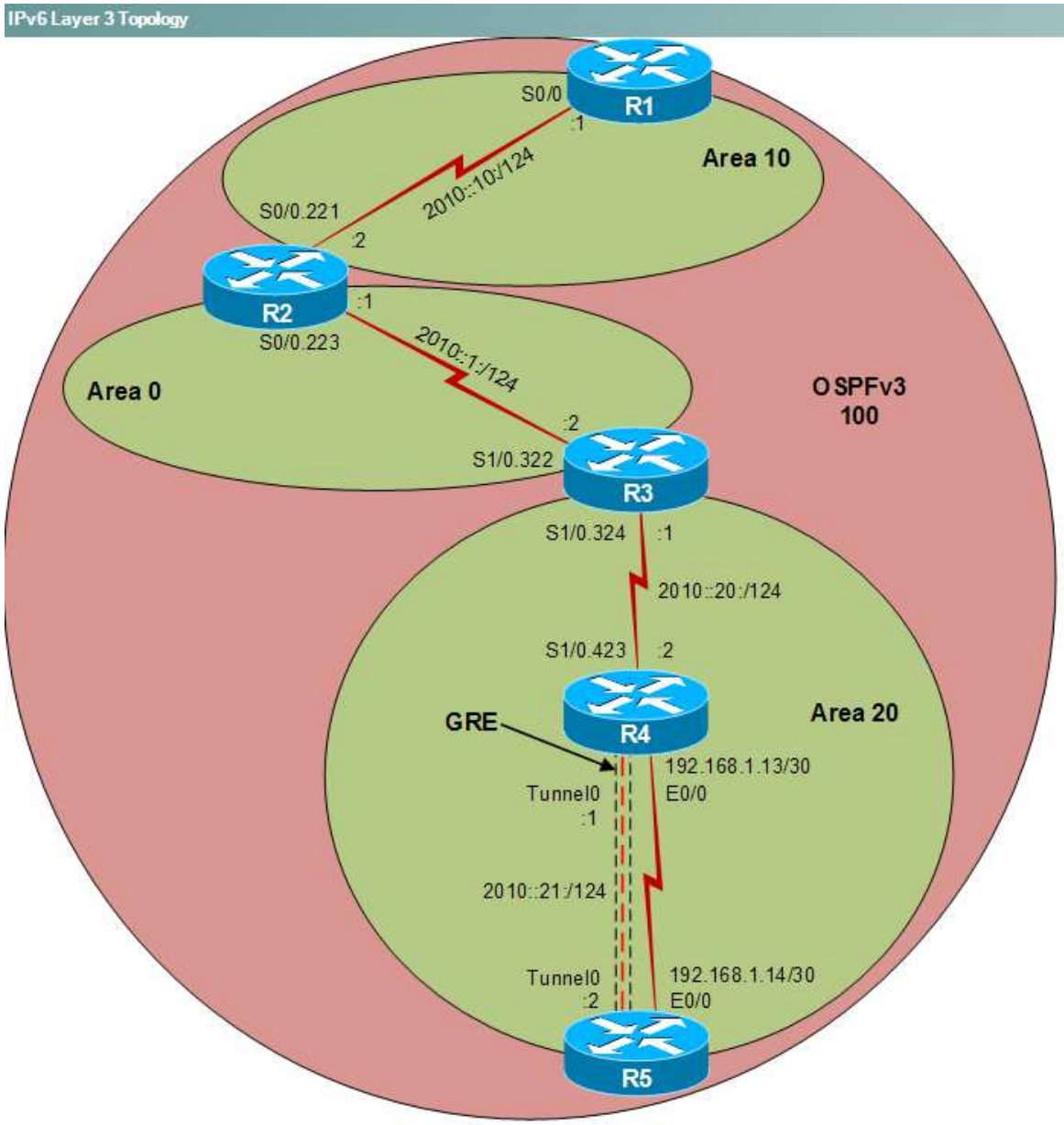
**Layer 2 Topology**




IPv4 layer 3 Topology

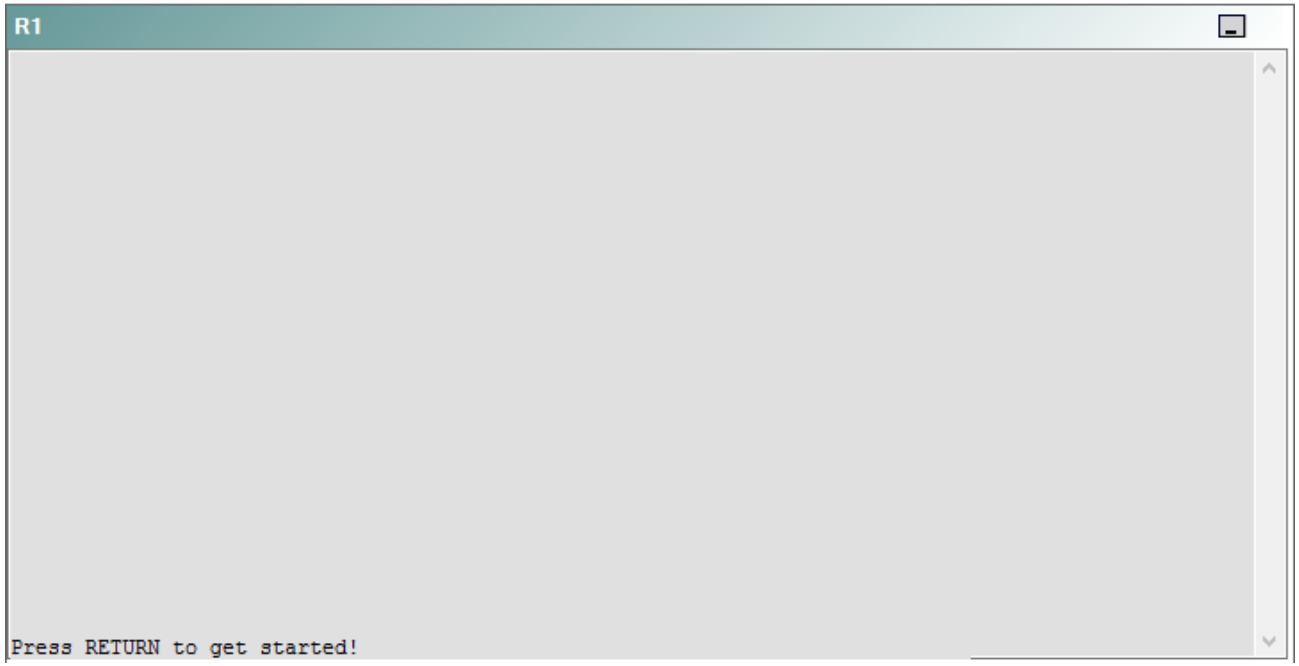

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

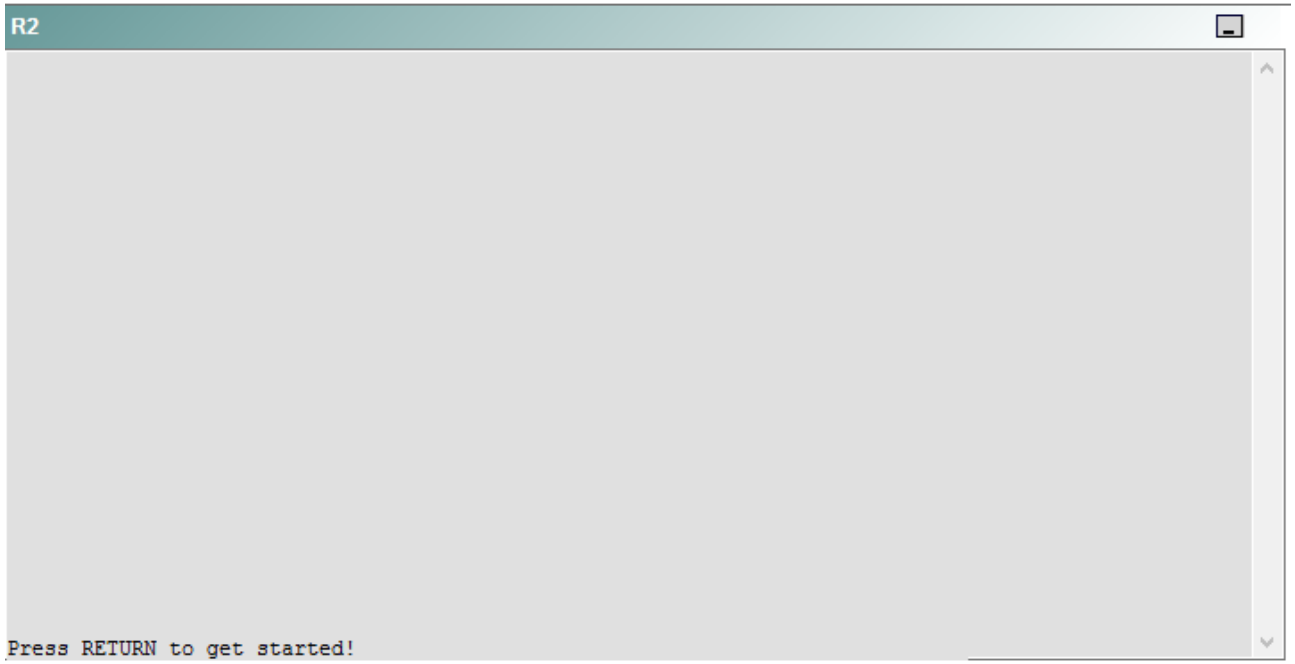



https://www.gratisexam.com/

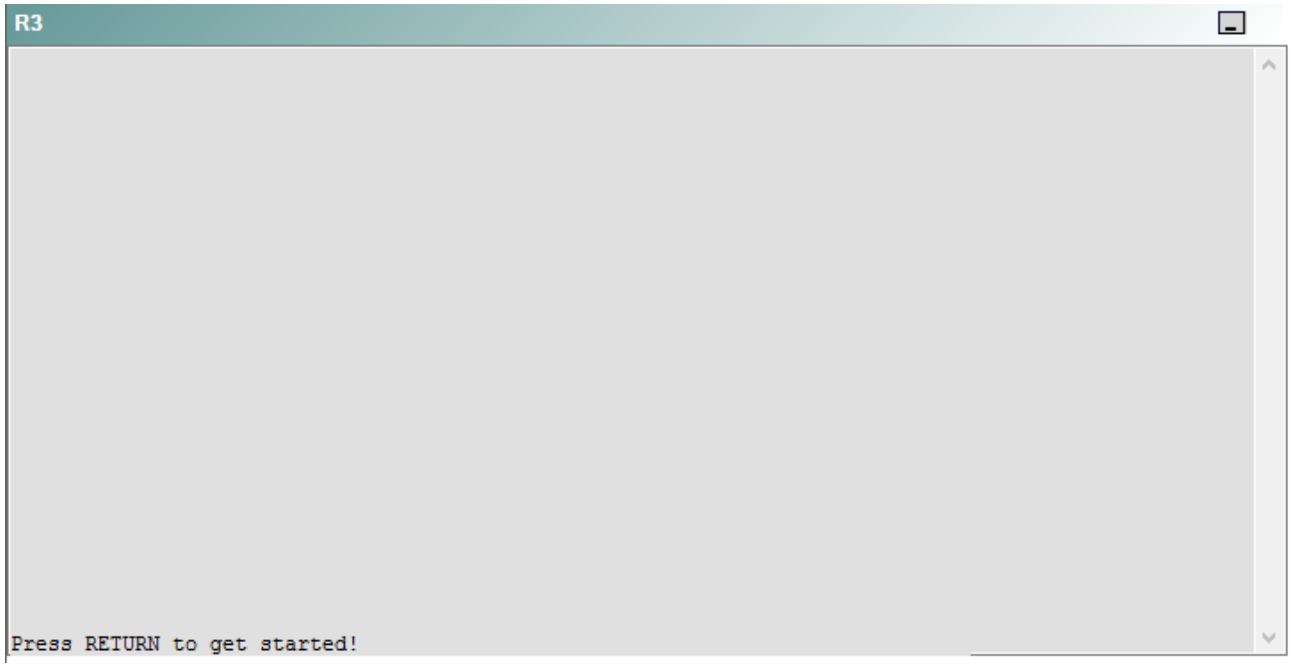
R1



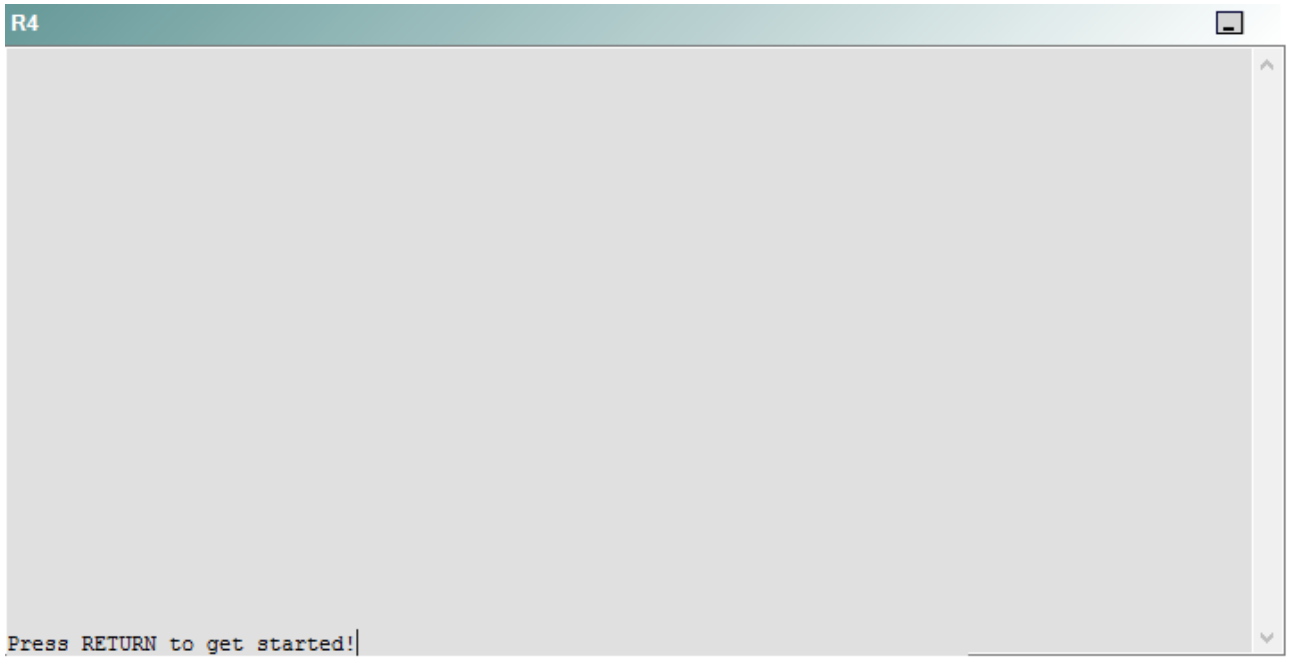

R2



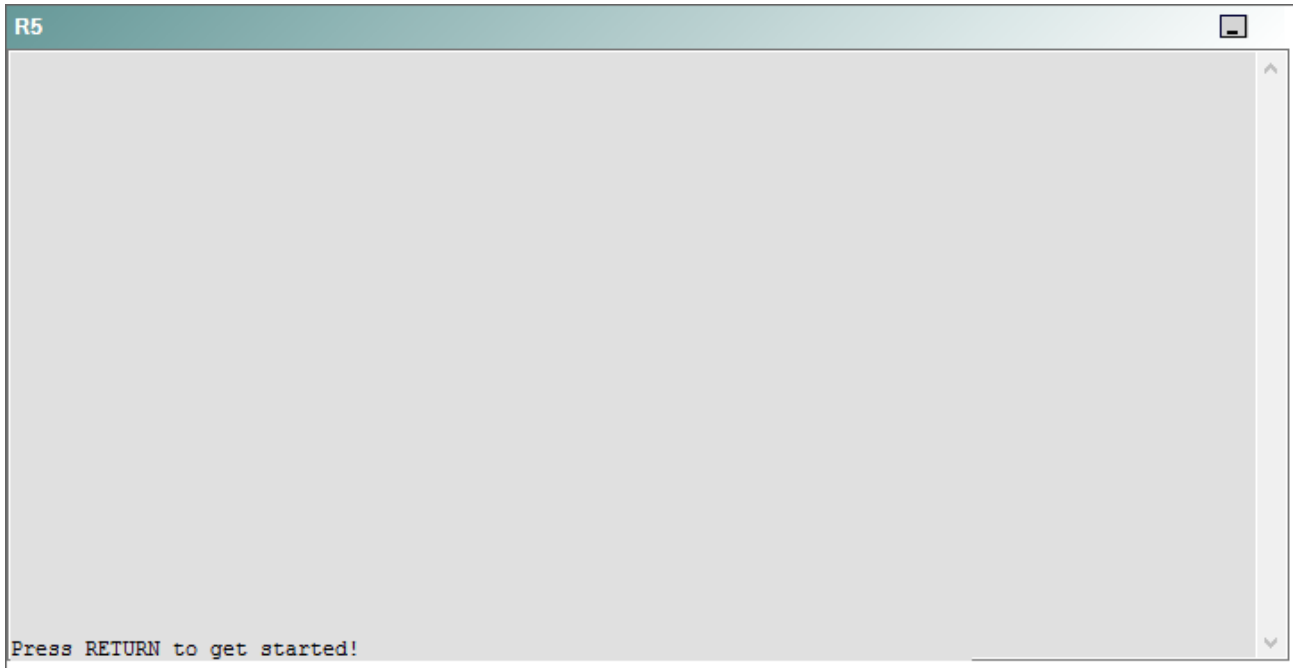

R3



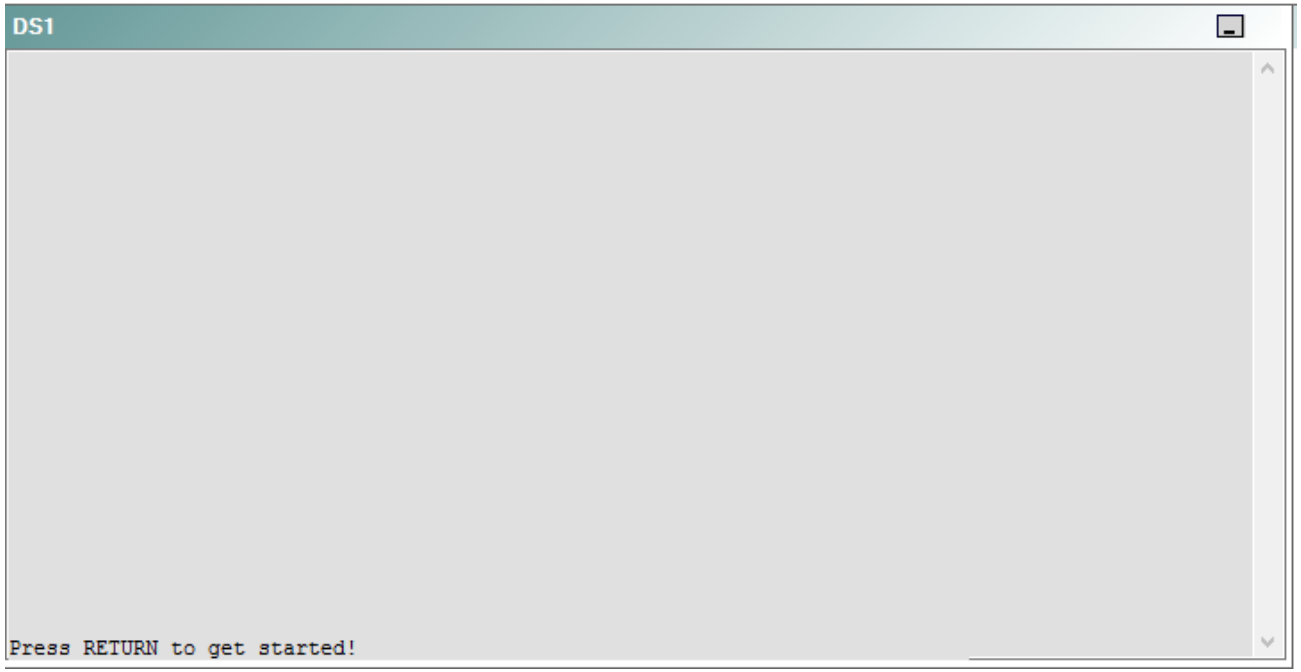

R4



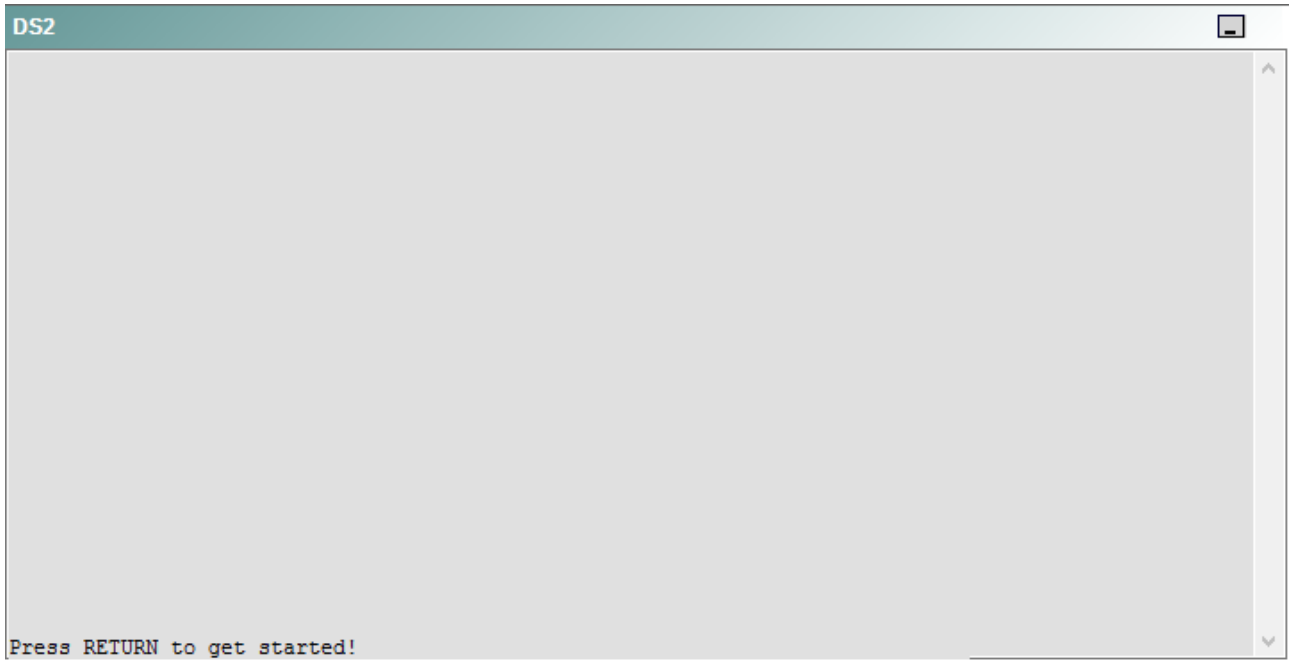

R5



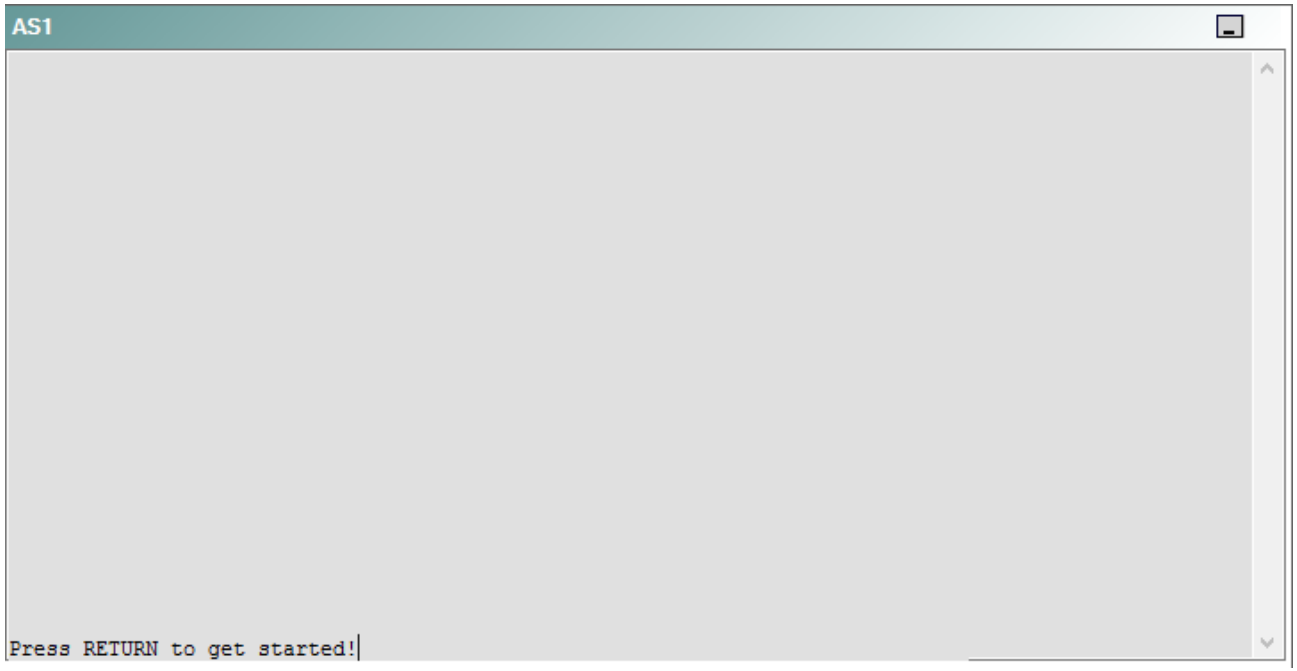

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the device at 123.45.67.90.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 60**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

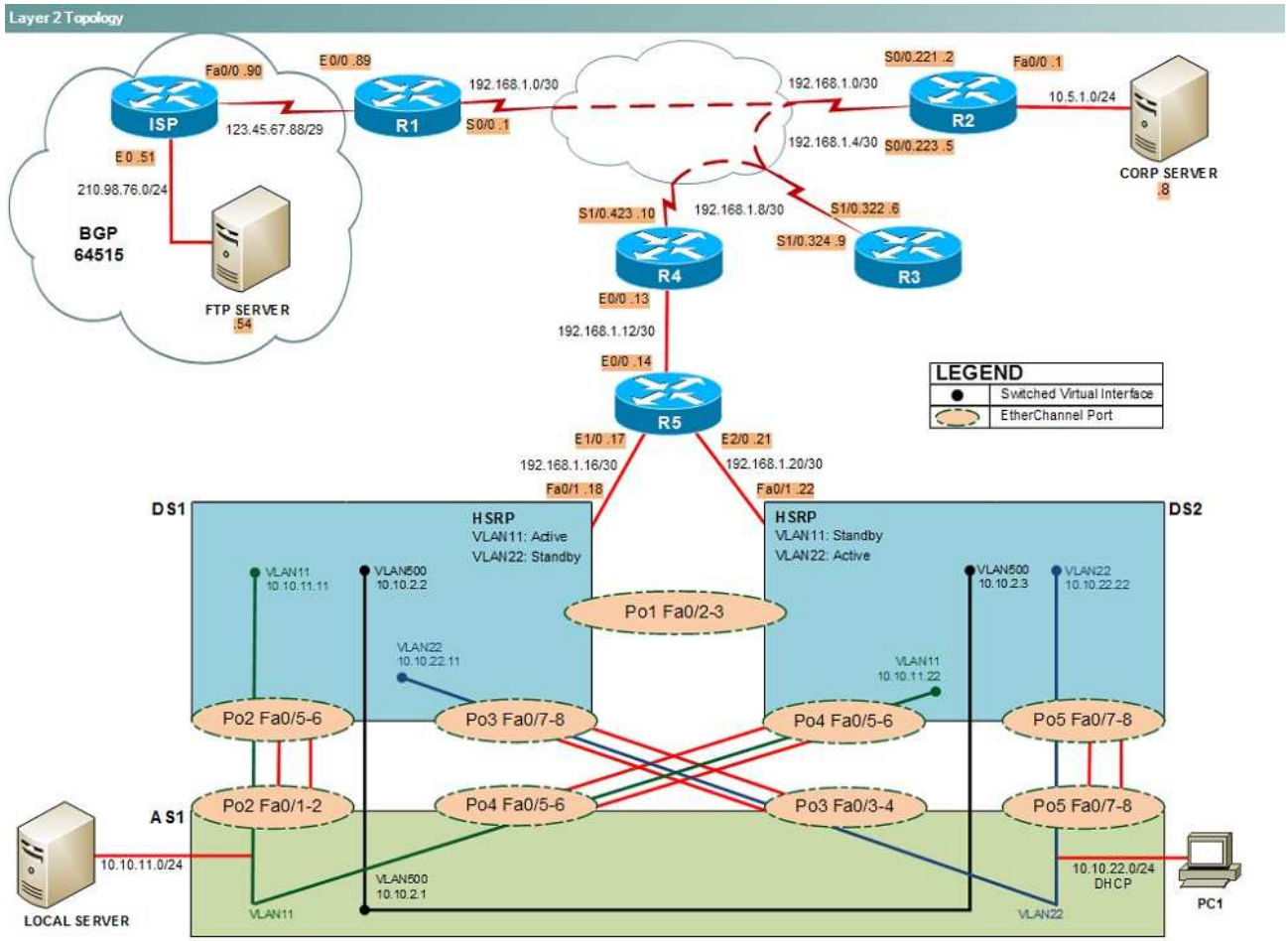
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

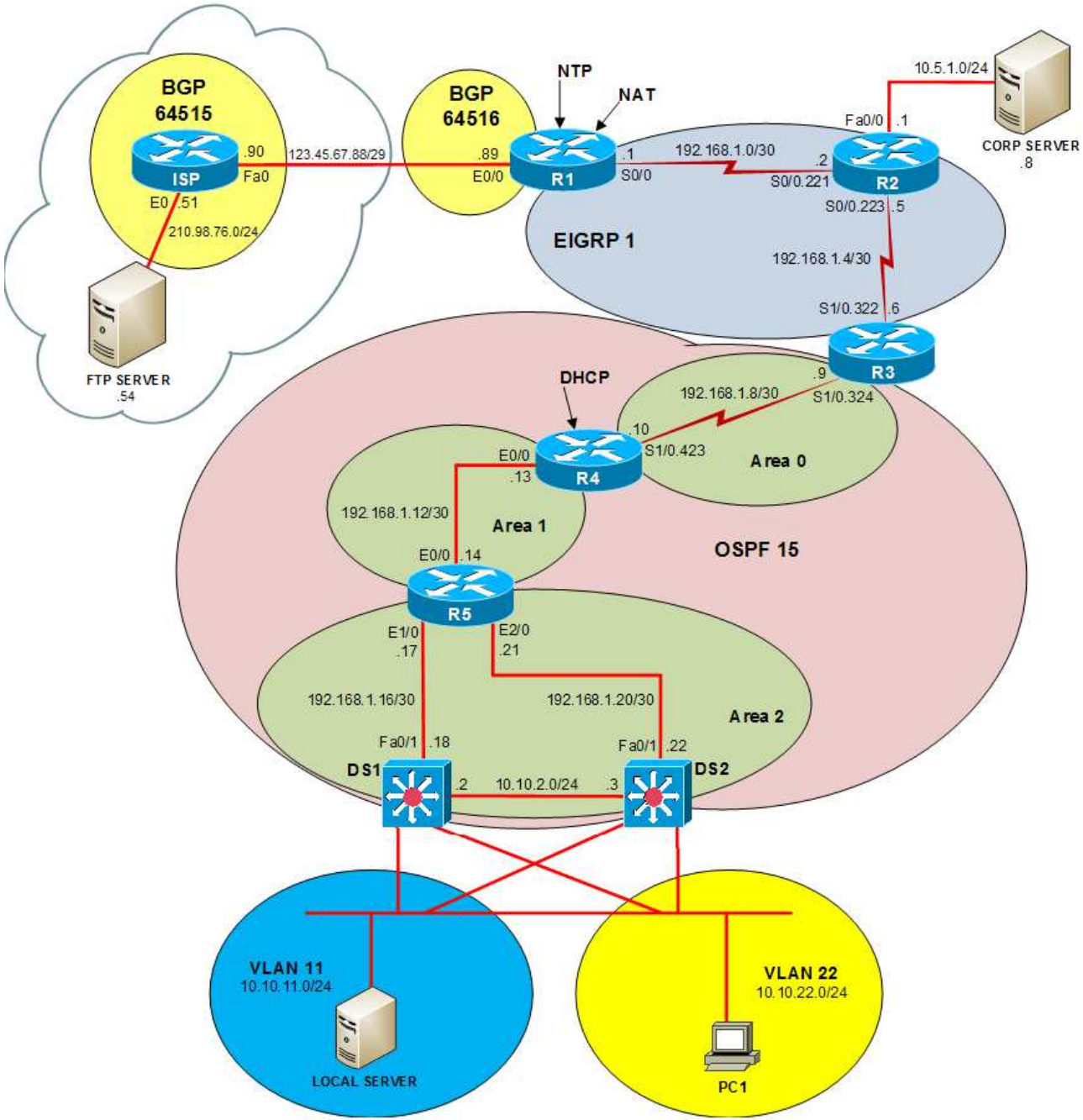
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

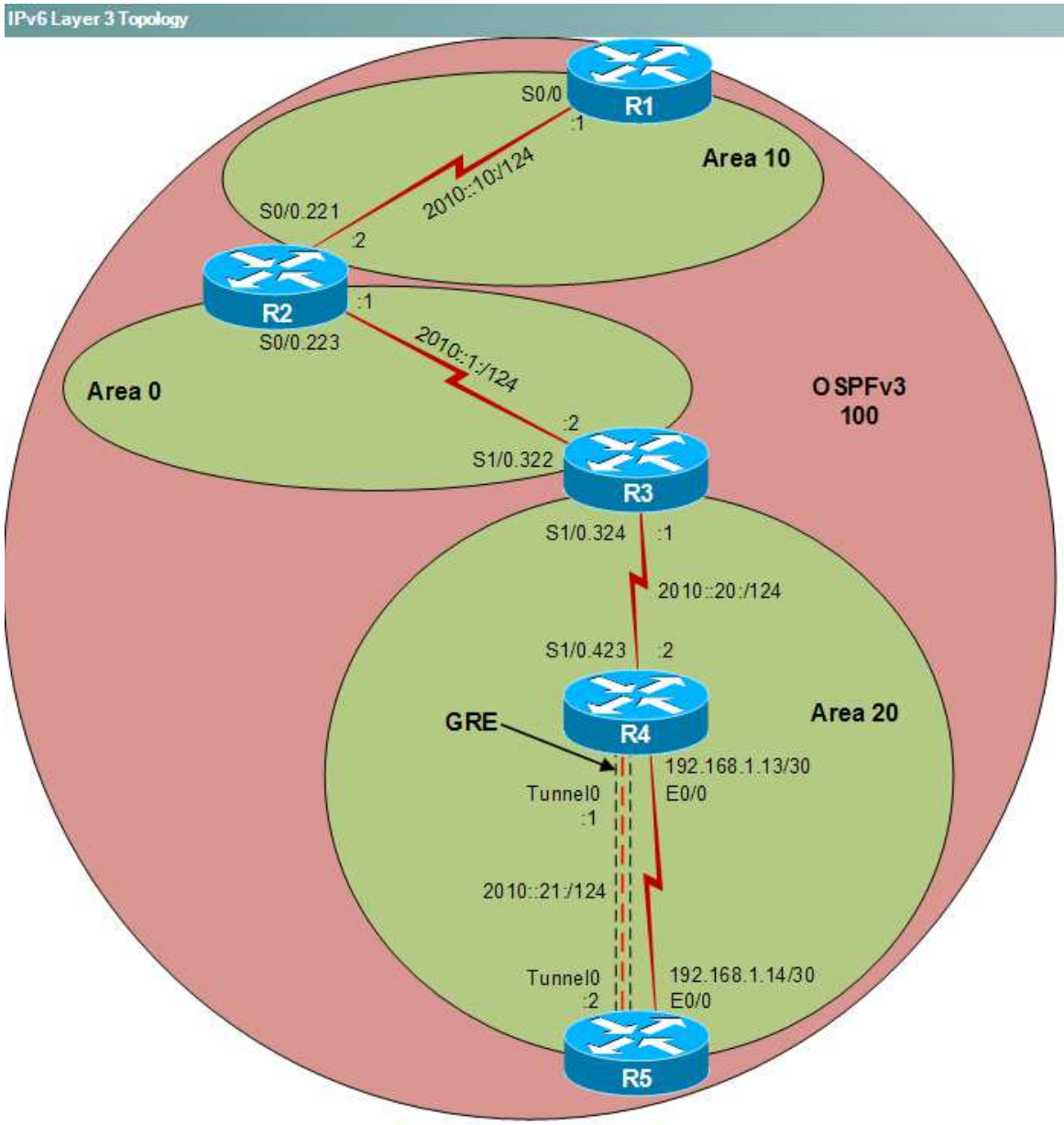
**Layer 2 Topology**




IPv4 layer 3 Topology

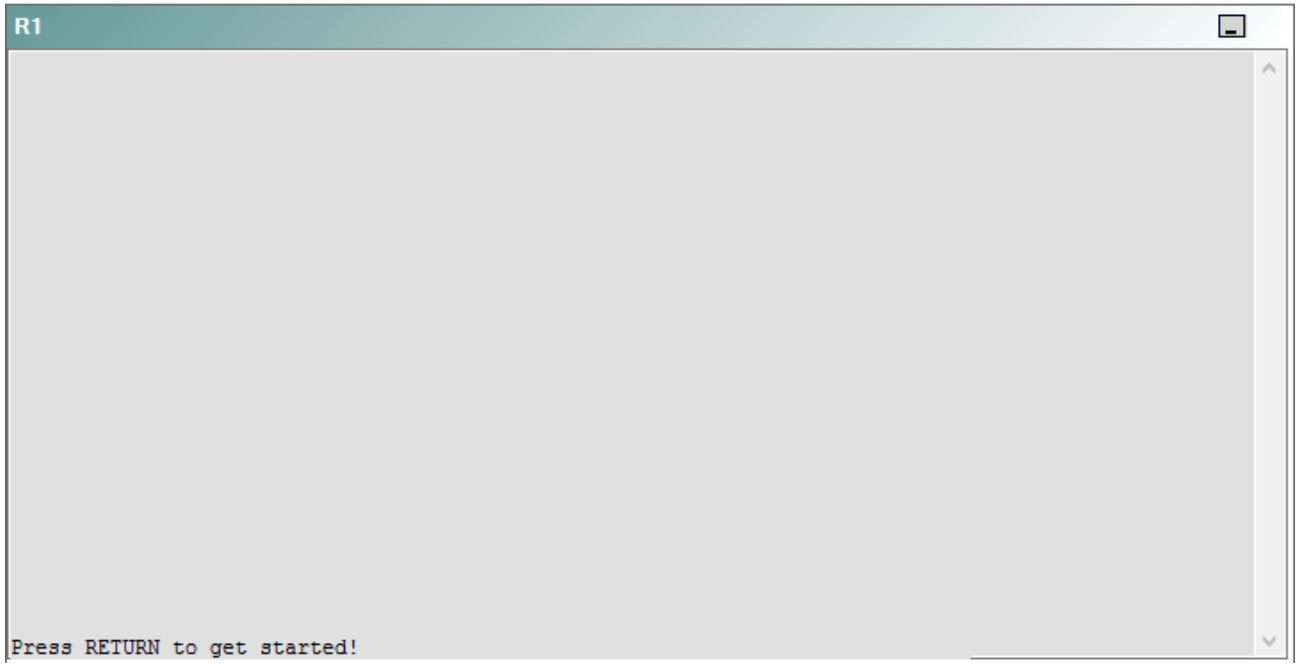

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

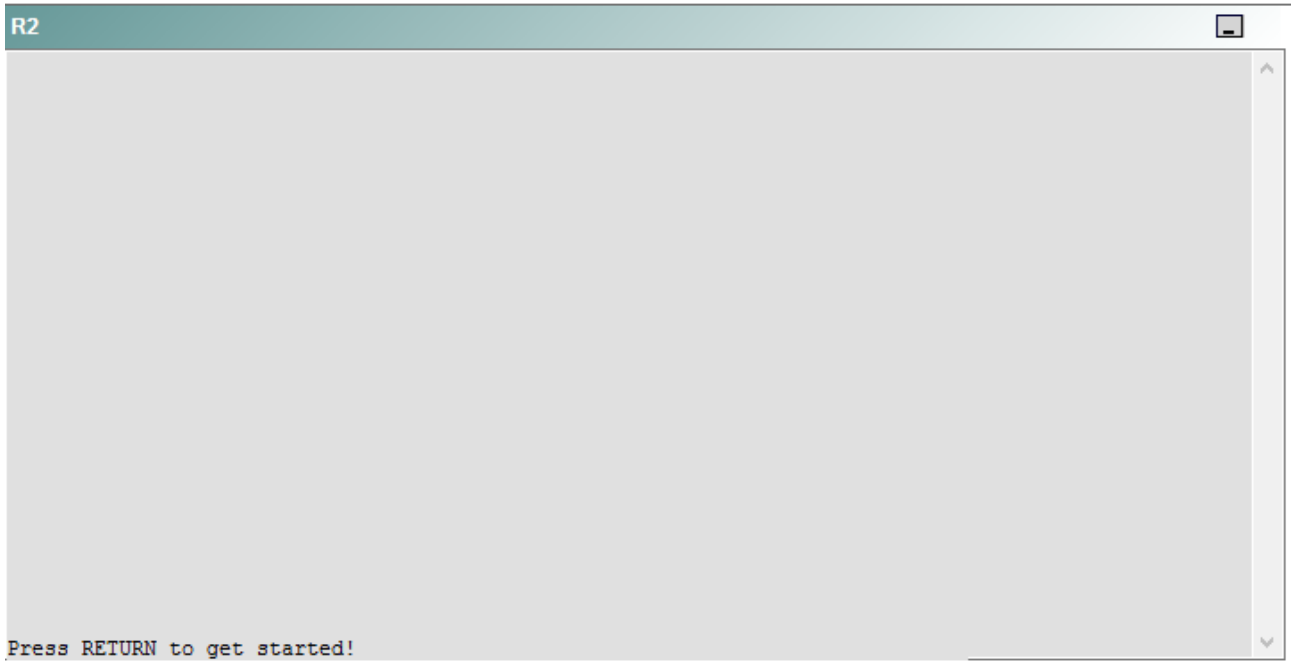



https://www.gratisexam.com/

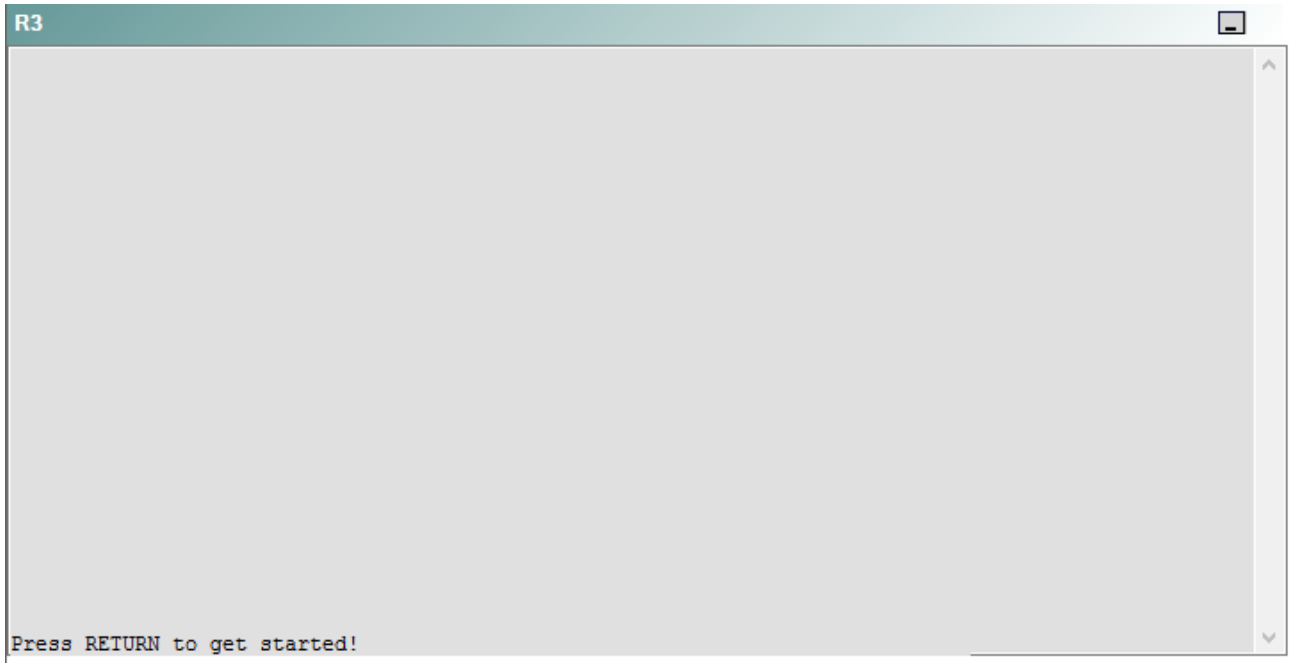
R1



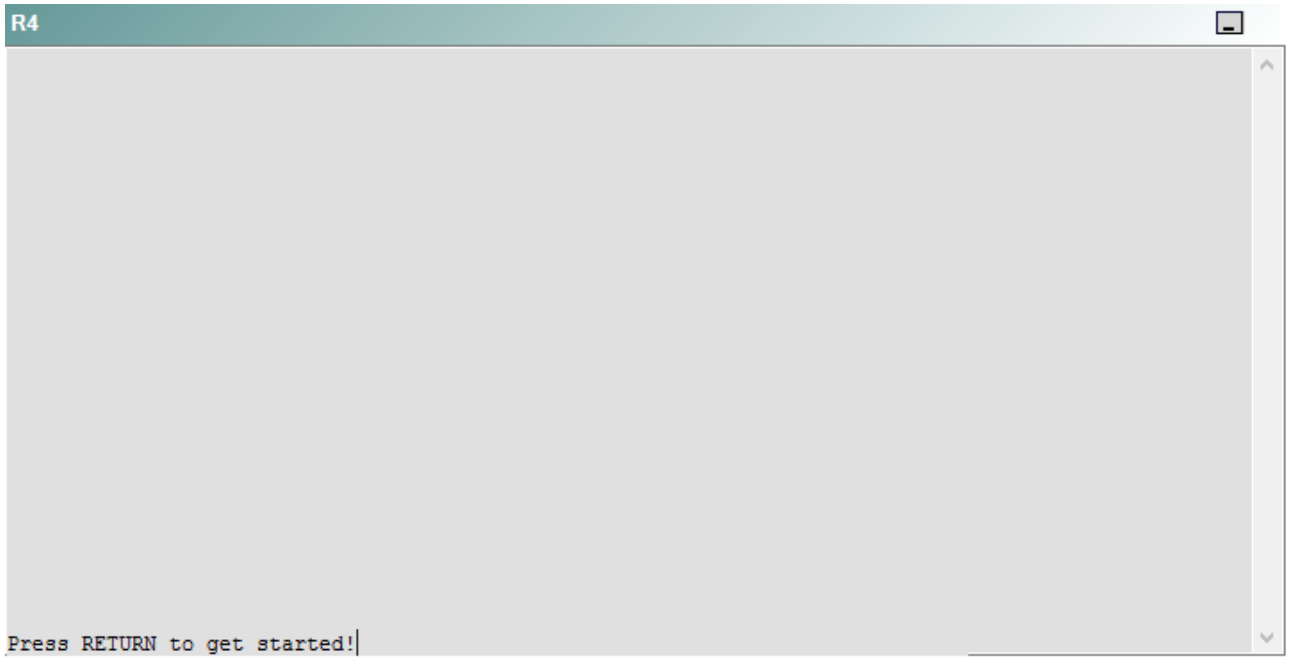

R2



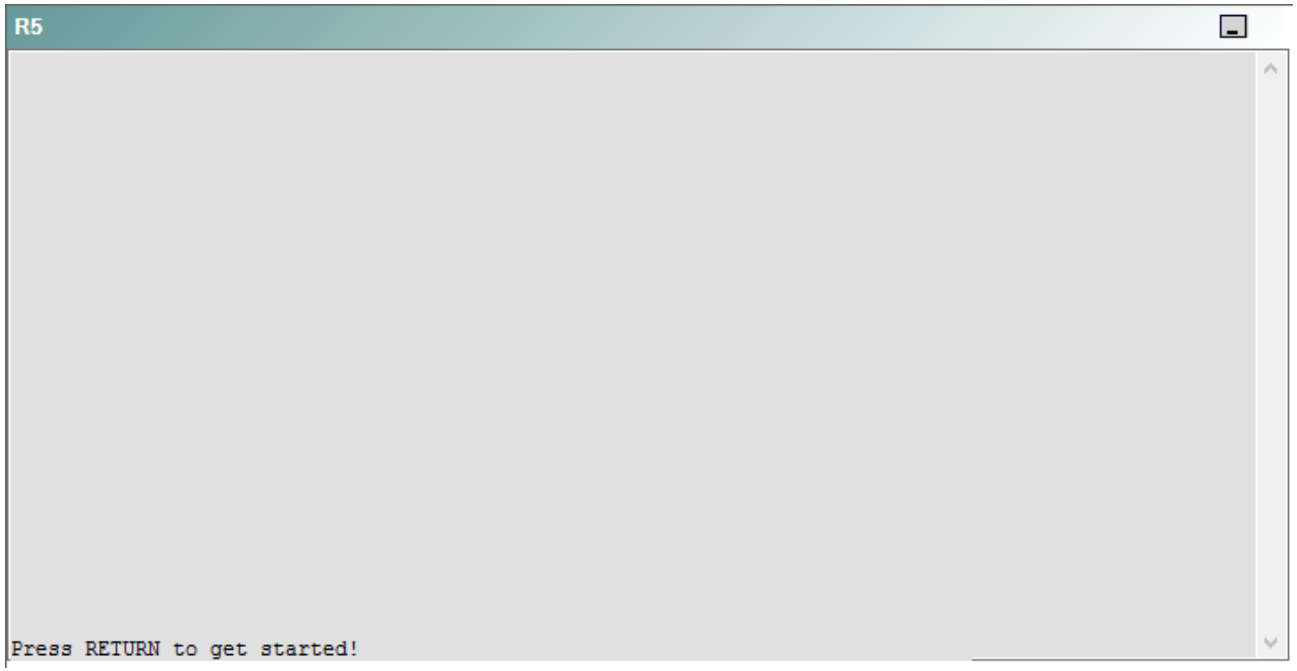

R3



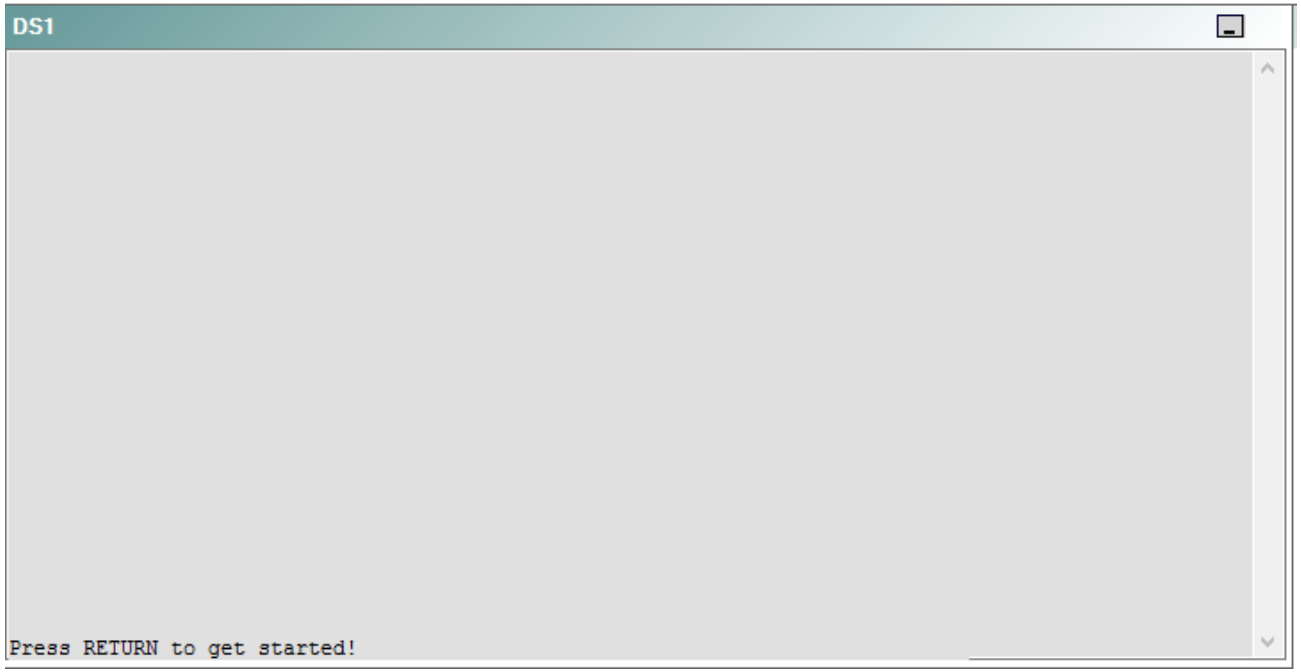

R4



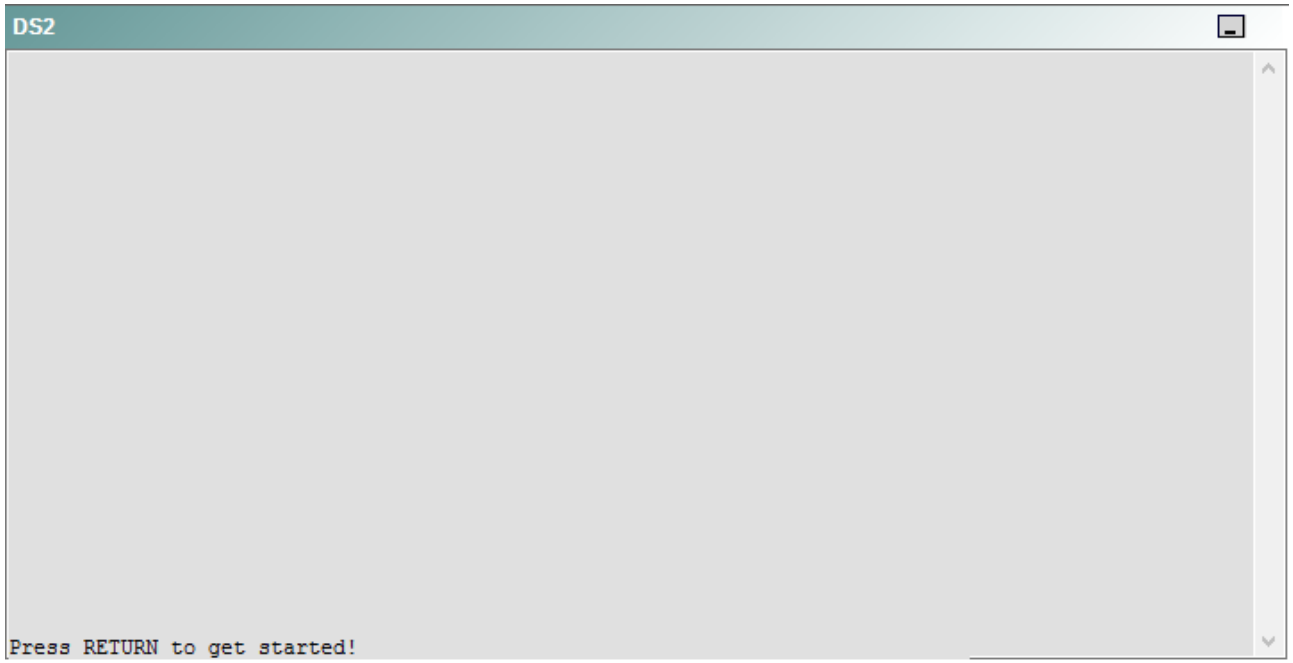

R5



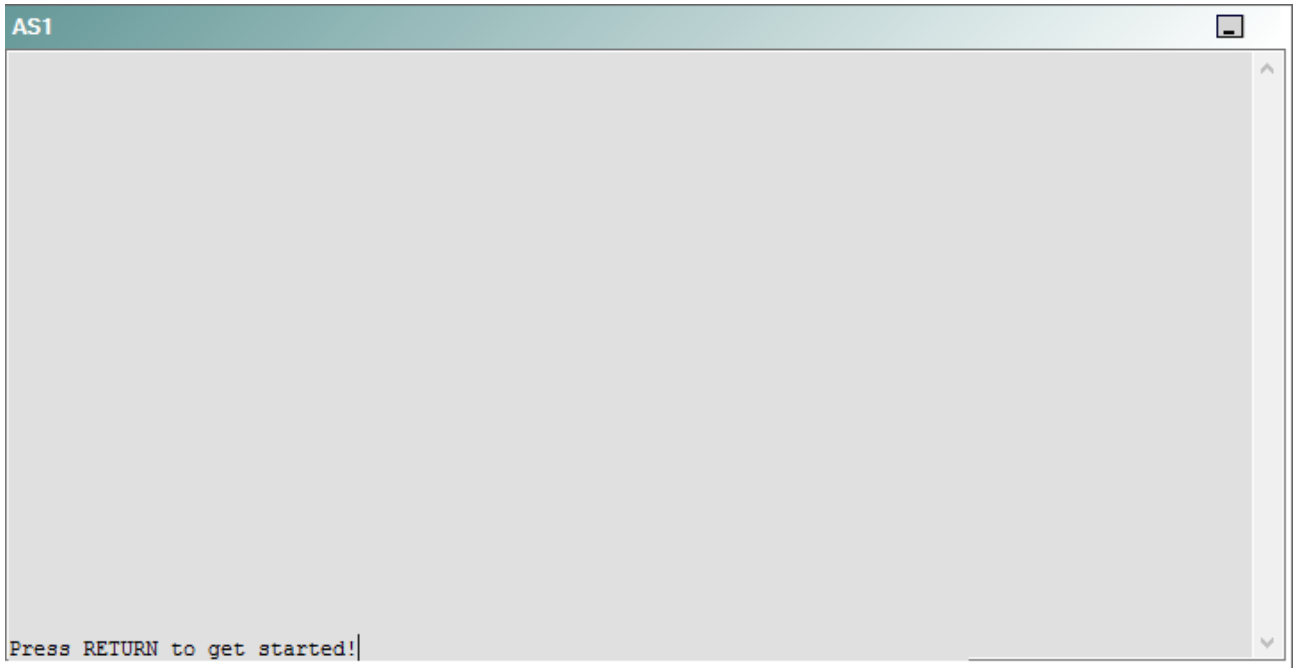

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the device at 123.45.67.90.

Which of the following technologies is the source of the problem?

A. NTP
B. NAT
C. Layer 3 addressing
D. Layer 3 security
E. BGP
F. redistribution
G. OSPFv3
H. interface

**Correct Answer:** E
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 61**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

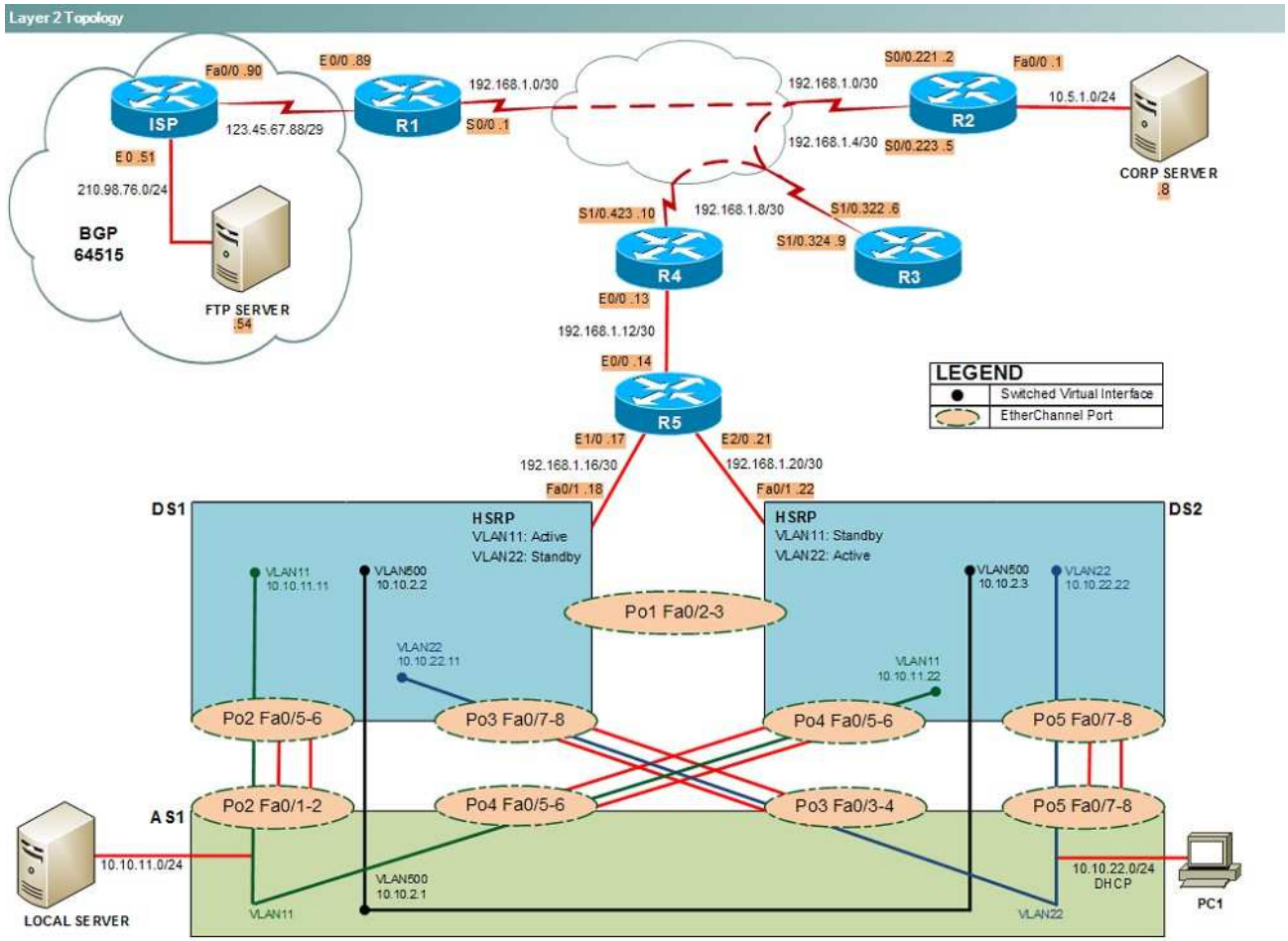
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

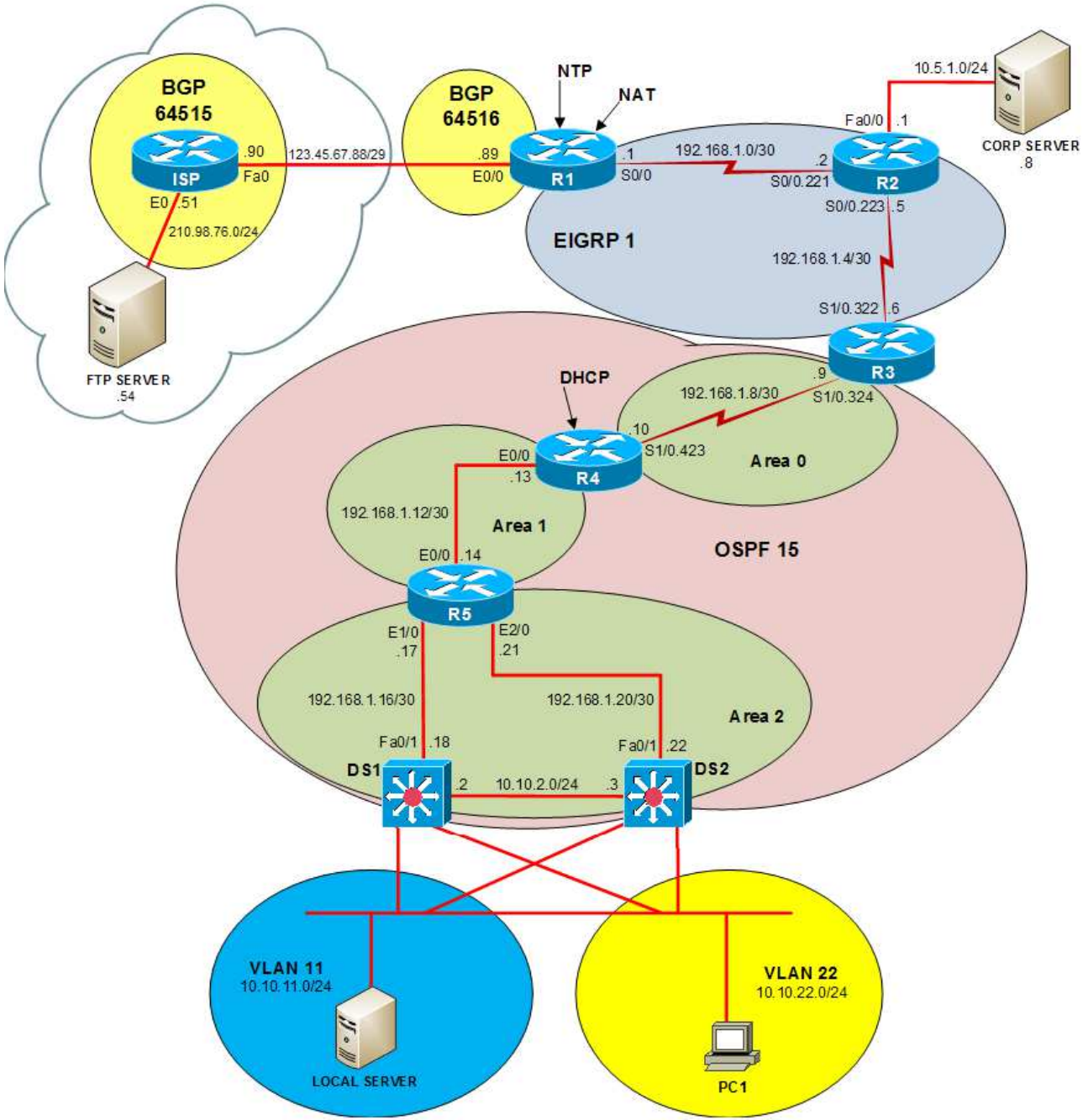
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

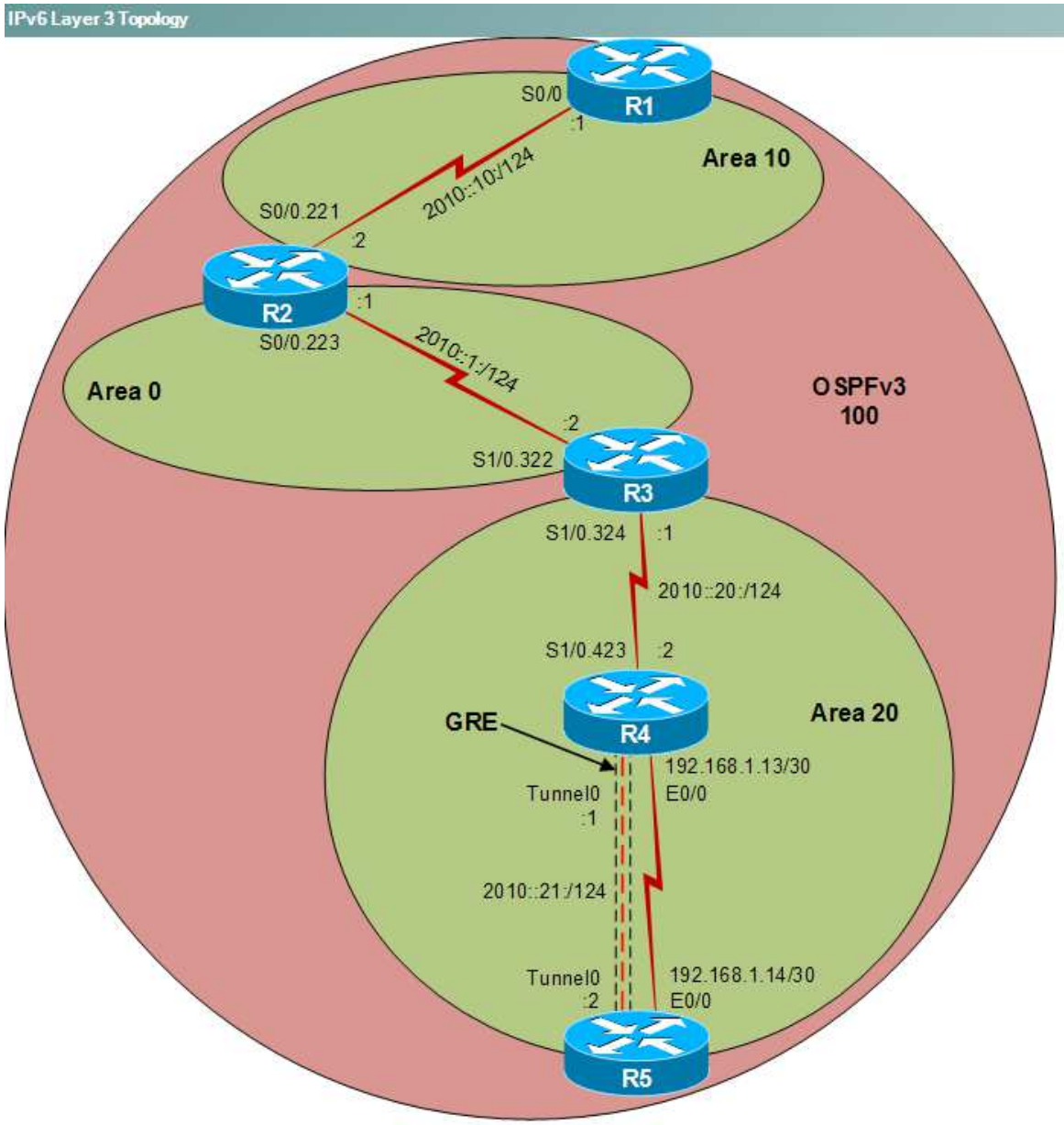
**Layer 2 Topology**




IPv4 layer 3 Topology

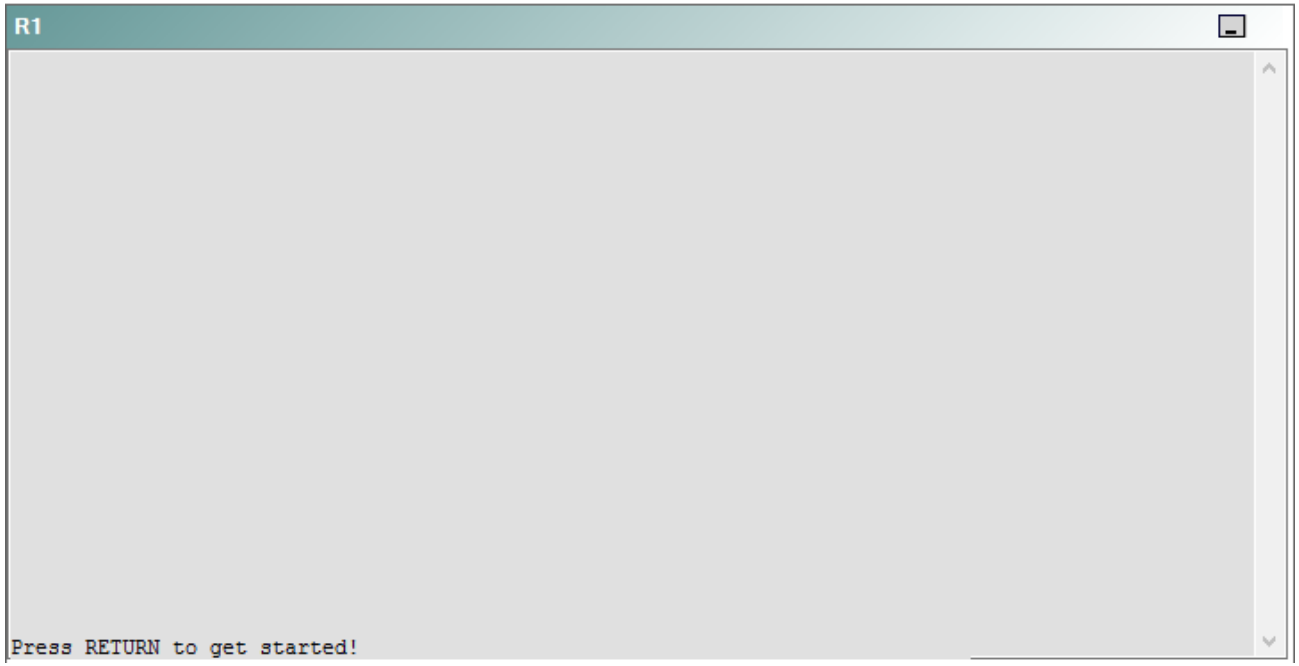

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

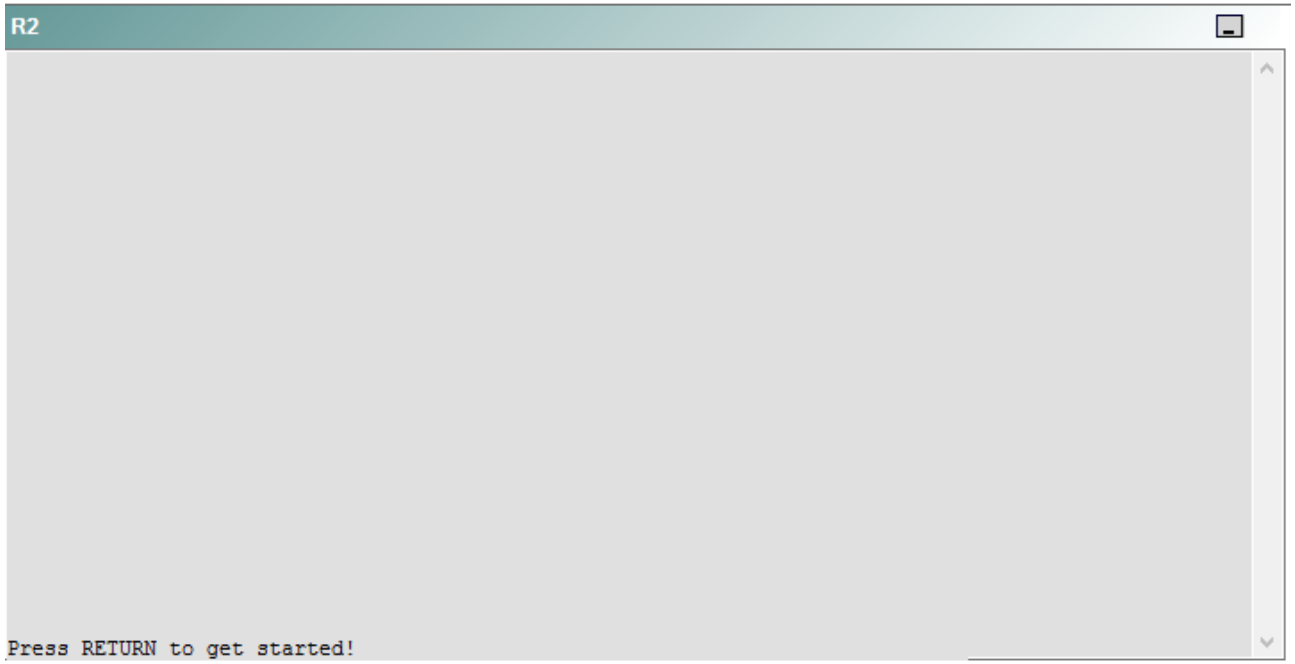



https://www.gratisexam.com/

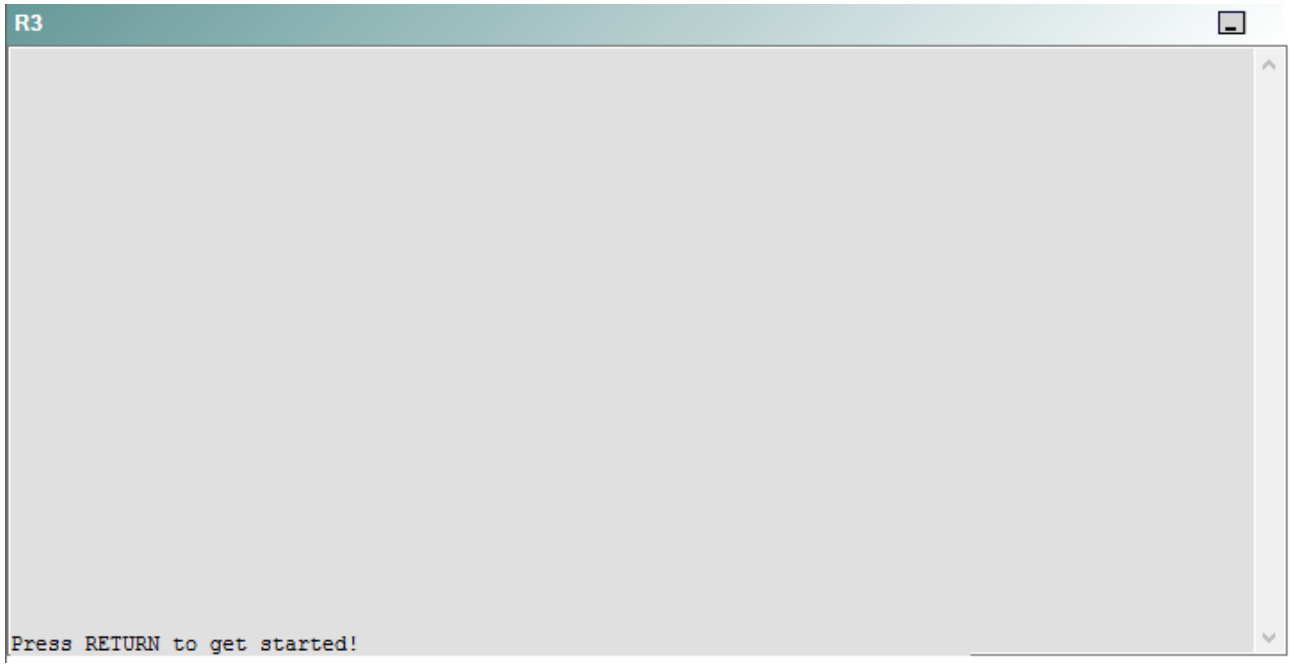
R1



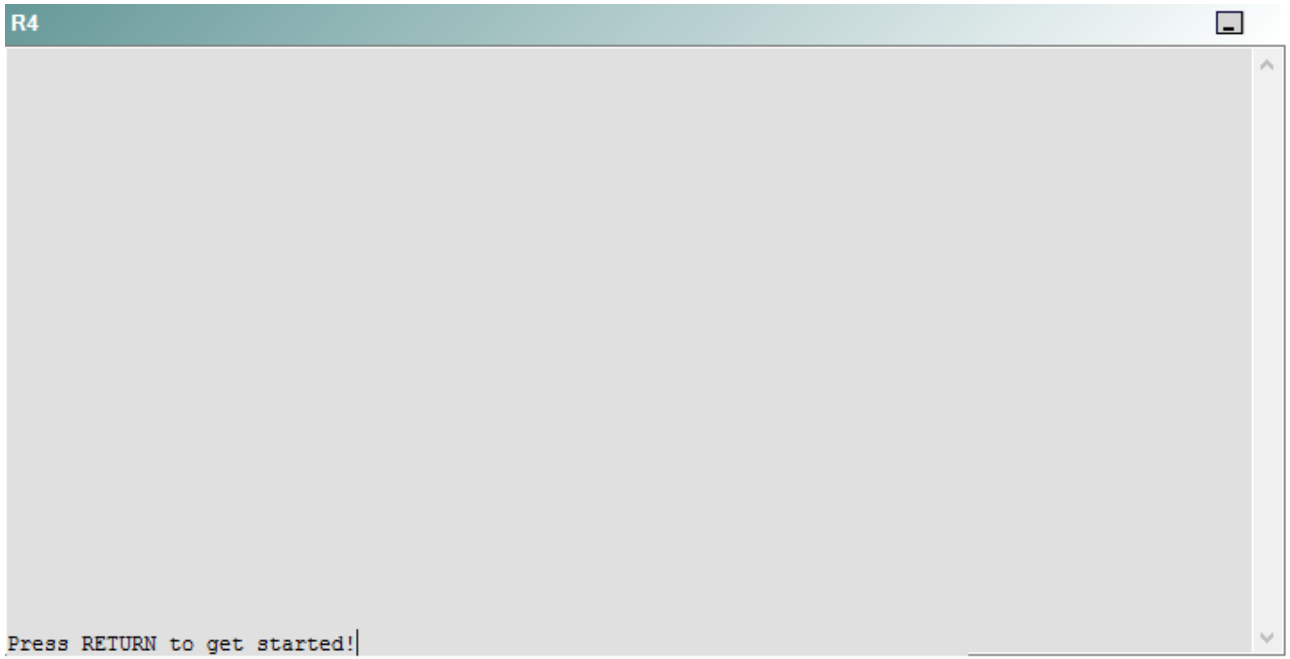

R2



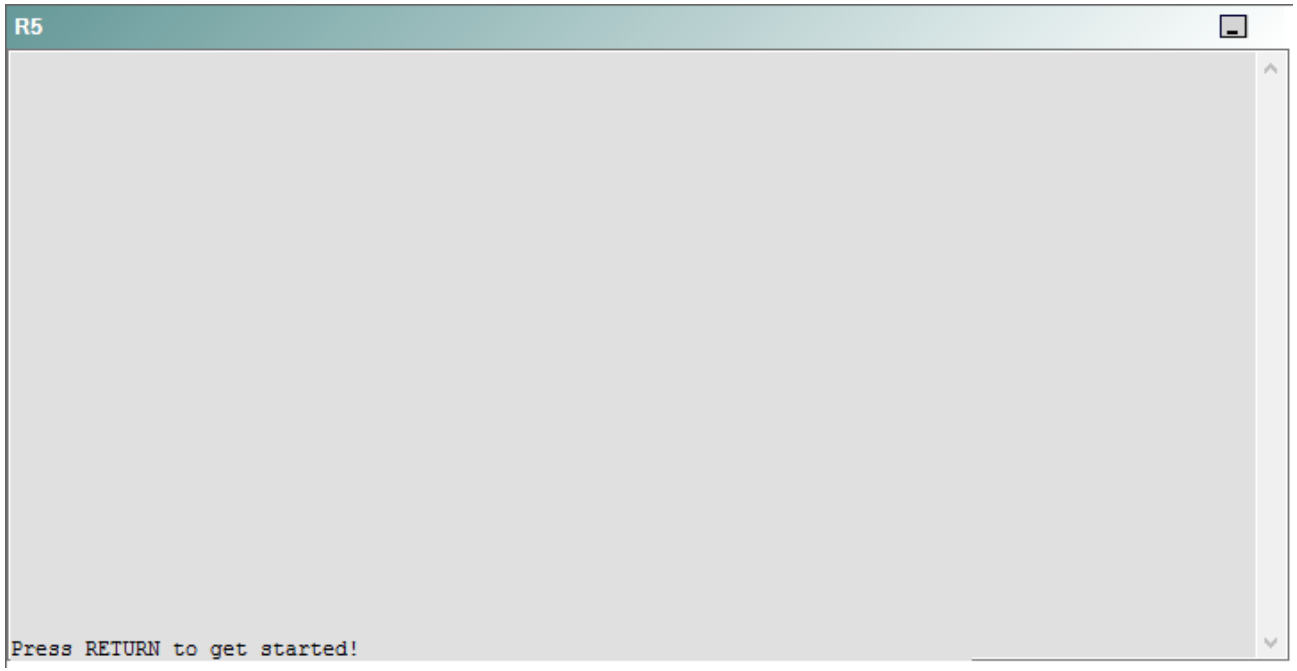

R3



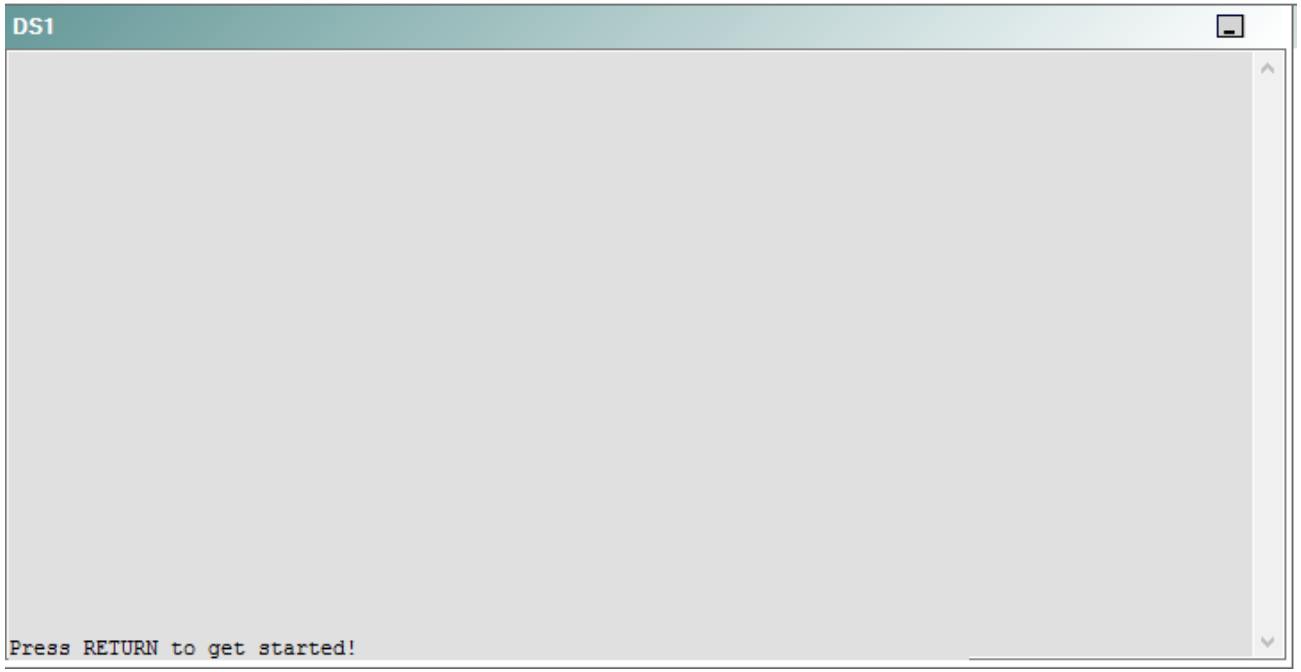

R4



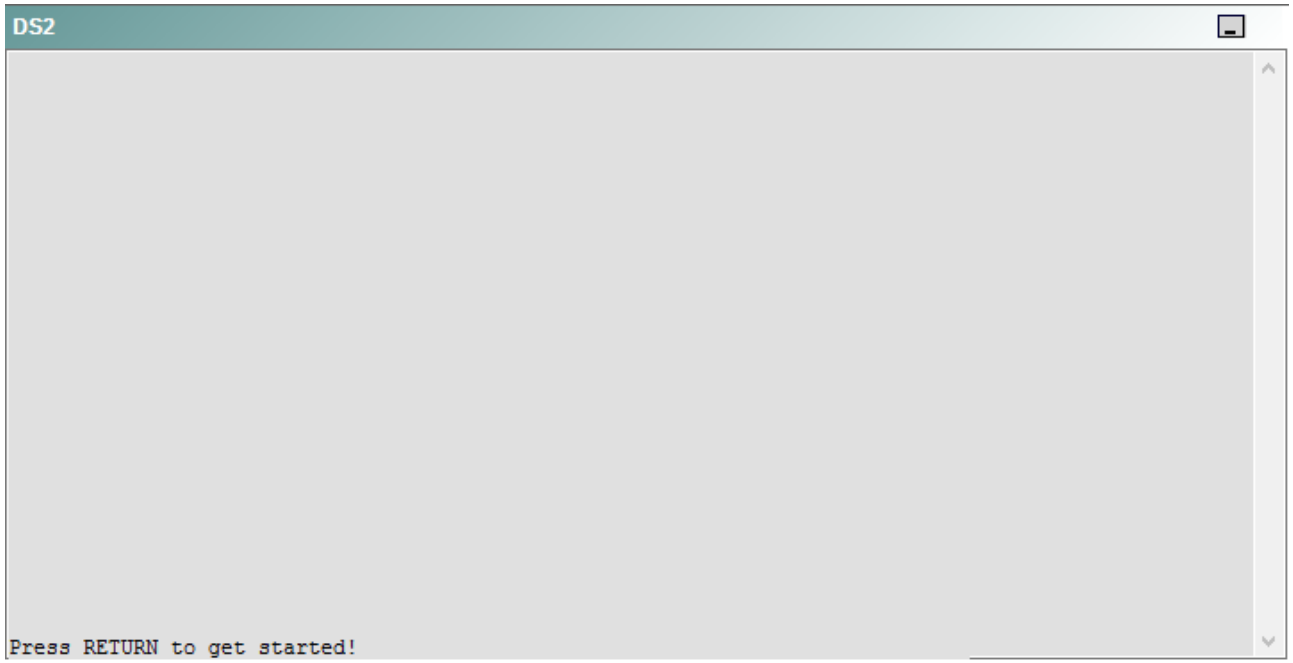

R5



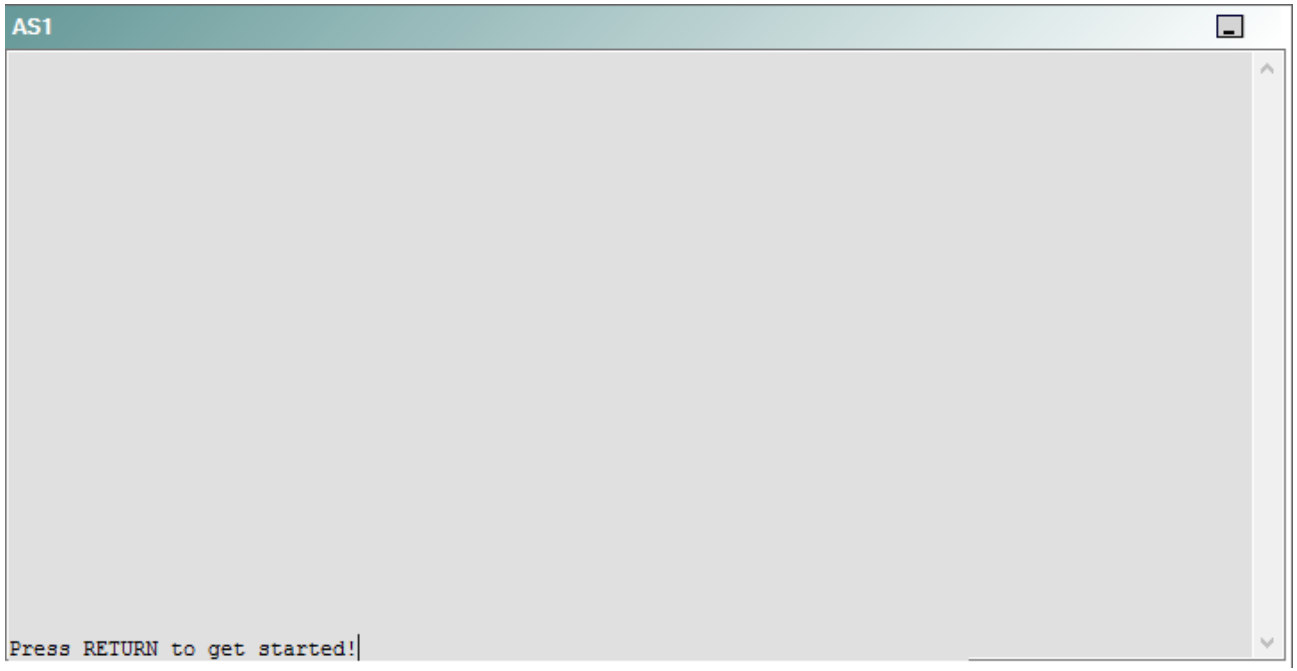

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the device at 123.45.67.90.

Which of the following is most likely to solve the problem?

A. issuing the **no neighbor 123.45.67.90 remote-as 64515** command, and issuing the **neighbor 123.45.67.90 remote-as 64516** command.
B. issuing the **no neighbor 123.45.67.90 remote-as 64516** command, and issuing the **neighbor 123.45.67.90 remote-as 64515** command.
C. issuing the **no network 123.45.67.80 mask 255.255.255.248** command, and issuing the **network 210.98.76.0 mask 255.255.255.0** command.
D. issuing the **no network 123.45.67.80 mask 255.255.255.248** command, and issuing the **network 210.98.76.50 mask 255.255.255.248** command.
E. issuing the **no network 123.45.67.80 mask 255.255.255.248** command, and issuing the **network 123.45.67.88 mask 255.255.255.248** command.
F. issuing the **no network 123.45.67.80 mask 255.255.255.248** command, and issuing the **network 123.45.67.90 mask 255.255.255.248** command
G. issuing the **synchronization** command
H. issuing the **no auton-summary** command

**Correct Answer:** E
**Section: (none)**

**Explanation**

**Explanation/Reference:**
Explanation:

You should issue the **no network 123.45.67.80 mask 255.255.255.248** command and issue the **network 123.45.67.88 mask 255.255.255.248** command for Border Gateway Protocol (BGP) autonomous system (AS) 64516 on R1. To determine which device is the source of the problem, you should issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from R5 to the closest device and work your way up the network until communication is lost, or you can ping from R5 to the farthest device and work your way back to R5 until pings are successful. Alternatively, you can trace from R5 to R1 and see where communication is lost along the path to the destination device.

In this scenario, if you were to issue the ping **123.45.67.90** command from R2, you would receive the following output:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 123.45.67.90, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

The ……in the output from R2 indicates that attempts by R2 to connect to the destination IP address at 123.45.67.90 have timed out even though R2 has a route to R1. In this scenario, R2 can ping and trace as far as the IP address 192.168.1.1, which has been assigned to the Serial0/0 interface on R1. The Serial0/0/ interface on R1 is an Enhanced Interior Gateway Routing Protocol (EIGRP) boundary. R2 cannot ping and trace to the IP address 123.45.67.89 or to the IP address 123.45.67.90. The IP address 123.45.67.89 is assigned to the Ethernet0/0 interface on R1, which is the BGP boundary for AS 64516. Therefore, the problem most likely exists on R1.

Once you have determined where connectivity is lost, you can begin to troubleshoot the cause of the problem. There are two routing protocols that are operating on R1: EIGRP and BGP. To determine which protocol is most likely causing the problem, you should verify the configuration and operation of each protocol. If you were to issue the **show ip route bgp** command on R1, you would receive the following output:

```
B    210.98.76.0/24 [20/0] via 123.45.67.90, 00:42:24
```

The output above indicates that R1 has a route to 210.98.76.0/24 that was obtained through the Ethernet0/0 interface that is connected to the ISP router. Additionally, if you were to issue the **show bgp neighbors** command on R1, you would receive the following partial output:

```
BGP neighbor is 123.45.67.90,  remote AS 64515, external link
  BGP version 4, remote router ID 210.98.76.51
  BGP state = Established, up for 00:42:00
```

The output above indicates that the BGP process on R1 has formed an external BGP (eBGP) relationship with the ISP router, which is operating in AS 64515. Based on the output above, the BGP process on R1 is correctly receiving the route to the ISP router and beyond. However, if you were to issue the **show running-**

**config** command on R1, you would receive the following partial output:

```
router bgp 64516
 no synchronization
 bgp log-neighbor-changes
 network 123.45.67.80 mask 255.255.255.248
 neighbor 123.45.67.90 remote-as 64515
 auto-summary
```

The output above indicates that BGP is running on R1 with an AS number of 64516 and that BGP is advertising the network 123.45.67.80/29. In this scenario, the Ethernet0/0 interface on R1 has been assigned the IP address 123.45.67.89 and is directly connected to the FastEthernet0/0 interface on ISP, which has been assigned the IP address 123.45.67.90. The 123.45.67.80/29 network only contains hosts that have been assigned IP addresses in the range from 123.45.68.81 to 123.45.67.86, none of which are in use on the network. BGP, EIGRP, Open Shortest Path First (OSPF), and all other routing protocols require a correct network statement in order to advertise networks to other routers. In this scenario, the BGP process on R1 is not advertising the correct network; therefore, you should issue the **no network 123.45.67.80 mask 255.255.255.248** command and the **network 123.45.67.88 mask 255.255.255.248** command on R1 to solve the problem.

You should not issue the **no neighbor 123.45.67.90 remote-as 64515** command on R1. Additionally, you should not issue the **neighbor 123.45.67.90 remote-as 645-16** command on R1. Issuing the **neighbor 123.45.67.90 remote-as 64516** command forms an internal BGP (iBGP) relationship with the ISP router. iBGP relationship are formed between BGP routers that are in the same AS. The relationship between R1 and ISP should be an eBGP relationship because R1 is in AS 64516 and ISP is in AS 64515.

You need not issue the **neighbor 123.45.67.90 remote-as 64515** command on R1. The **neighbor 123.45.67.90** remote-as 64515 command forms an eBGP relationship between R1 and ISP; it has already been issued in this scenario.

You should not issue the **network 210.98.76.0 mask 255.255.255.0** command on R1. The Ethernet0/0 interface on R1 has been assigned an IP address on the 123.45.67.88/29 network, not the 210.98.76.0/24 network.

You should not issue the **network 210.98.76.50 mask 255.255.255.248** command on R1. The Ethernet0/0 interface on R1 resides on the 123.45.67.88/29 network, not the 210.98.76.50 network.

You should not issue the **network 123.45.67.90 mask 255.255.255.248** command on R1. You cannot issue the BGP **network** command with an interface IP address; you must use the network address.

You should not issue the **synchronization** command on R1. Enabling BGP synchronization prevents BGP from advertising iBGP routes to eBGP neighbors. Disabling BGP synchronization prevents BGP from validating routes from internal routing protocols. In this scenario, neither enabling synchronization nor disabling synchronization will solve the problem.

You should not issue the **no auto-summary** command on R1. When automatic summarization is disables, local routers in the BGP table will not be summarized to their classful boundaries. In this scenario, neither enabling automatic summarization nor disabling automatic summarization will solve the problem.

**QUESTION 62**

**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

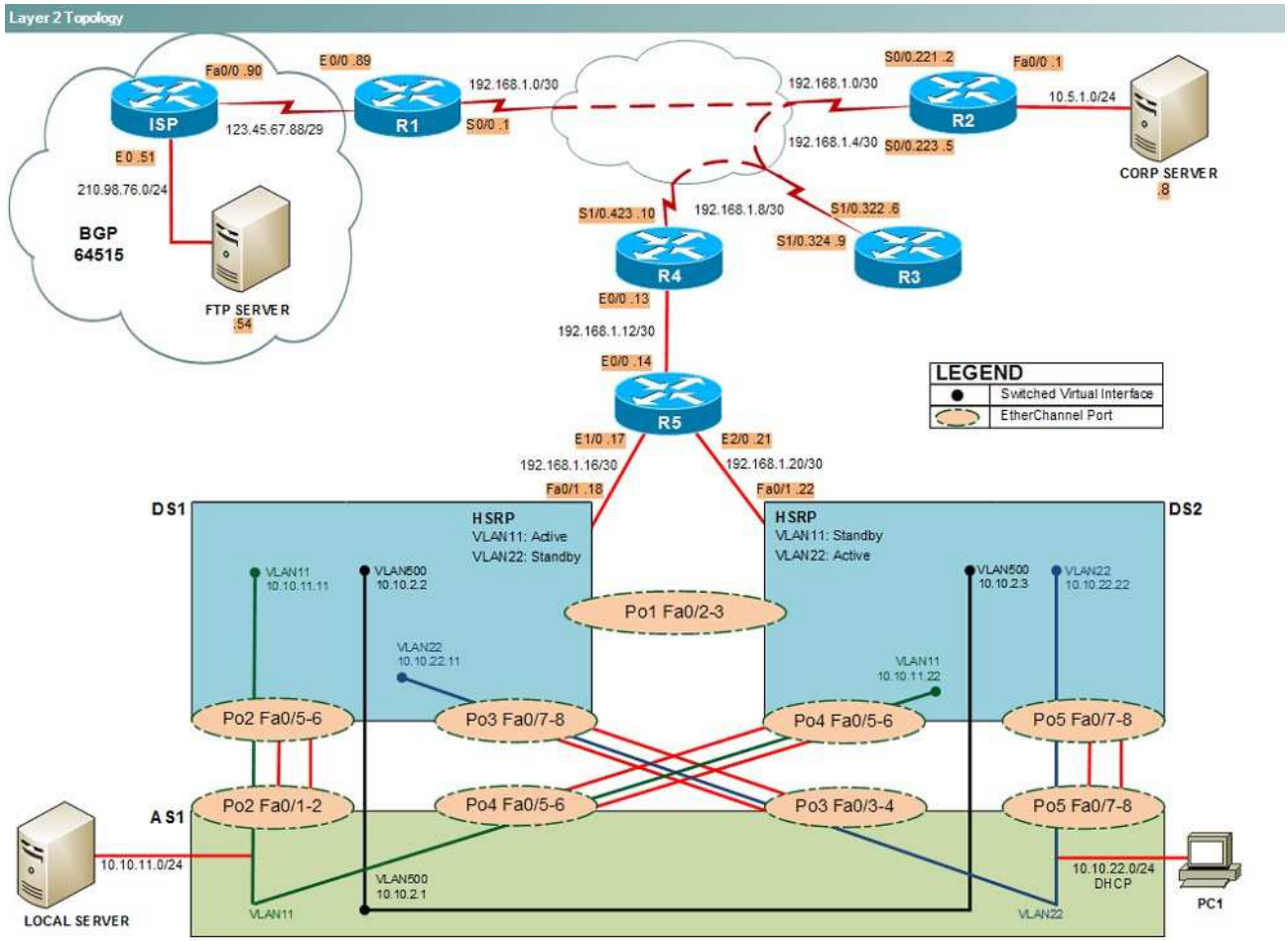
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

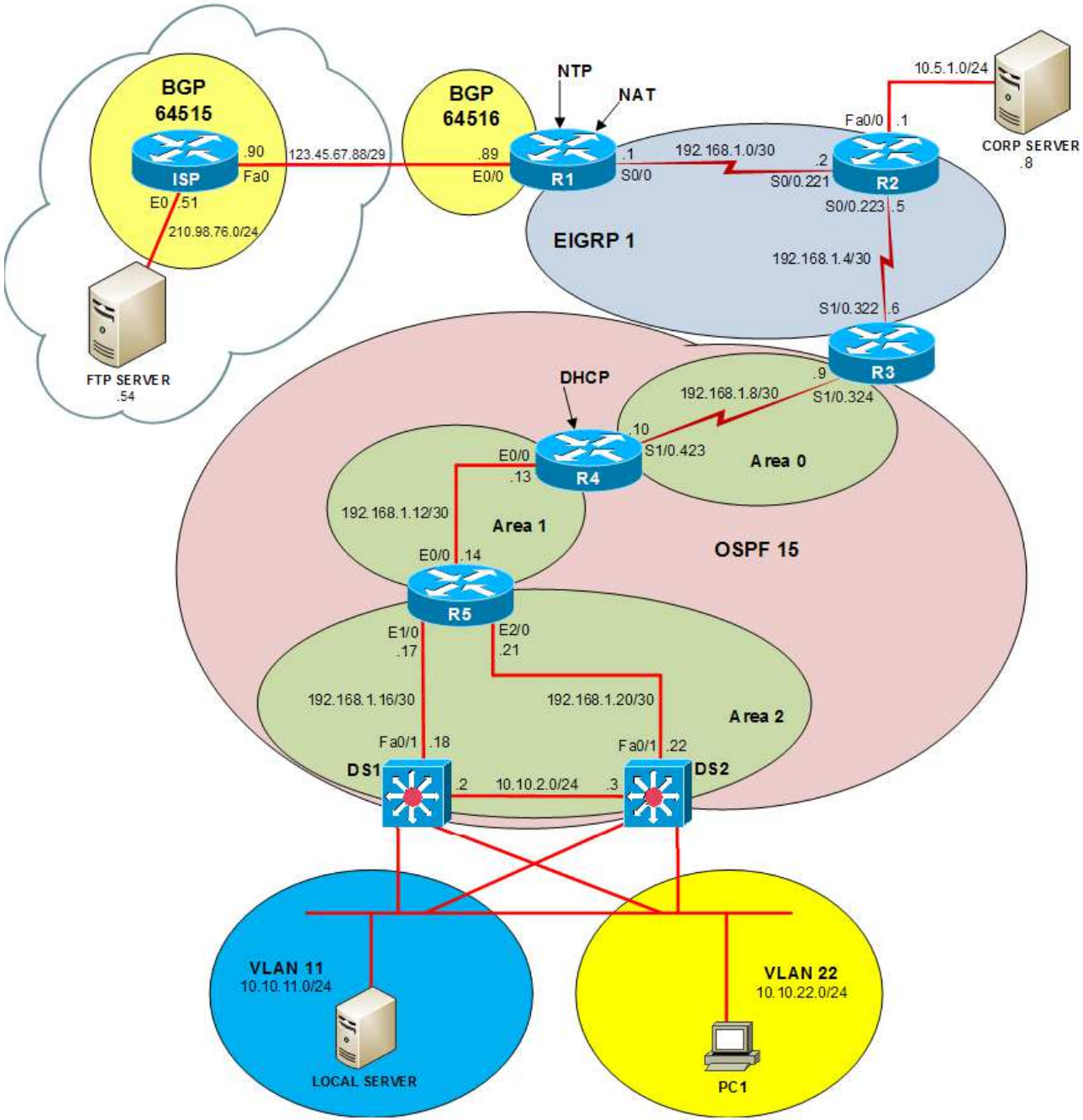
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

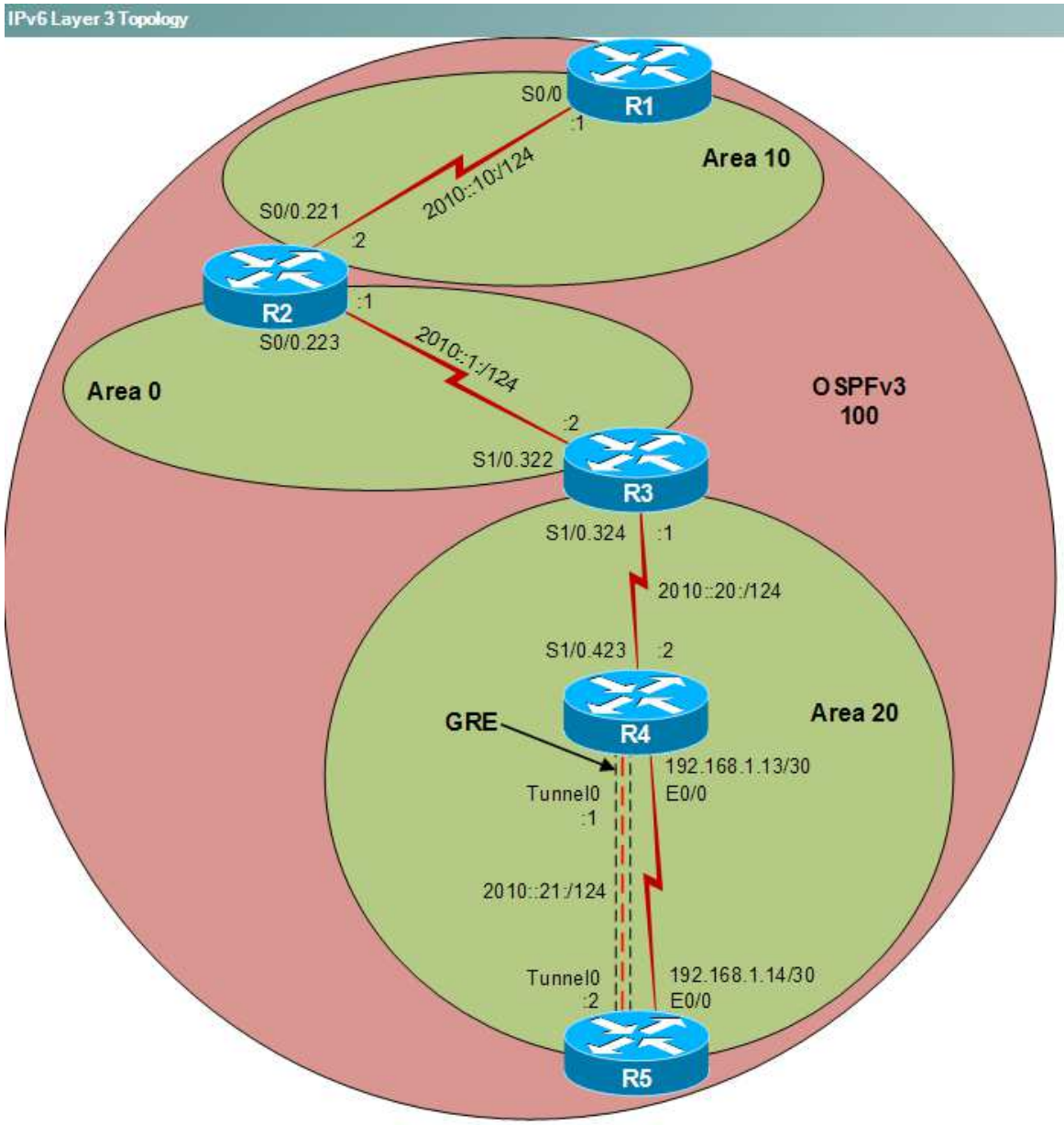
**Layer 2 Topology**




IPv4 layer 3 Topology

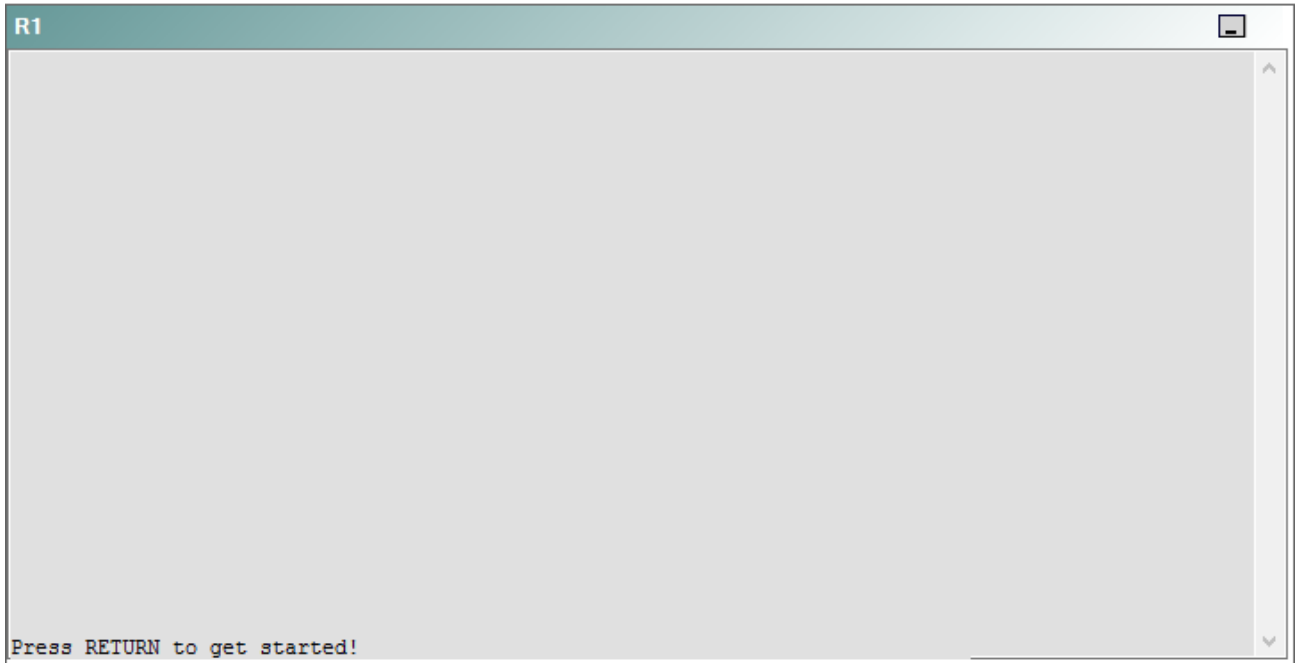

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

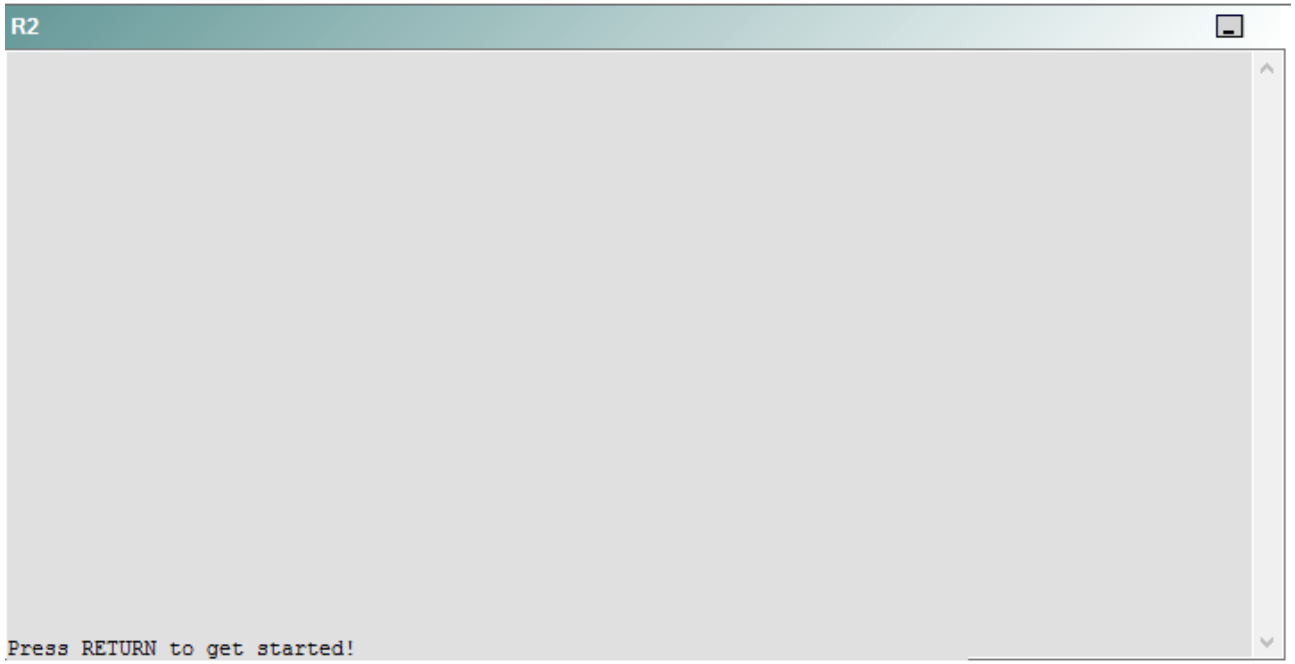



https://www.gratisexam.com/

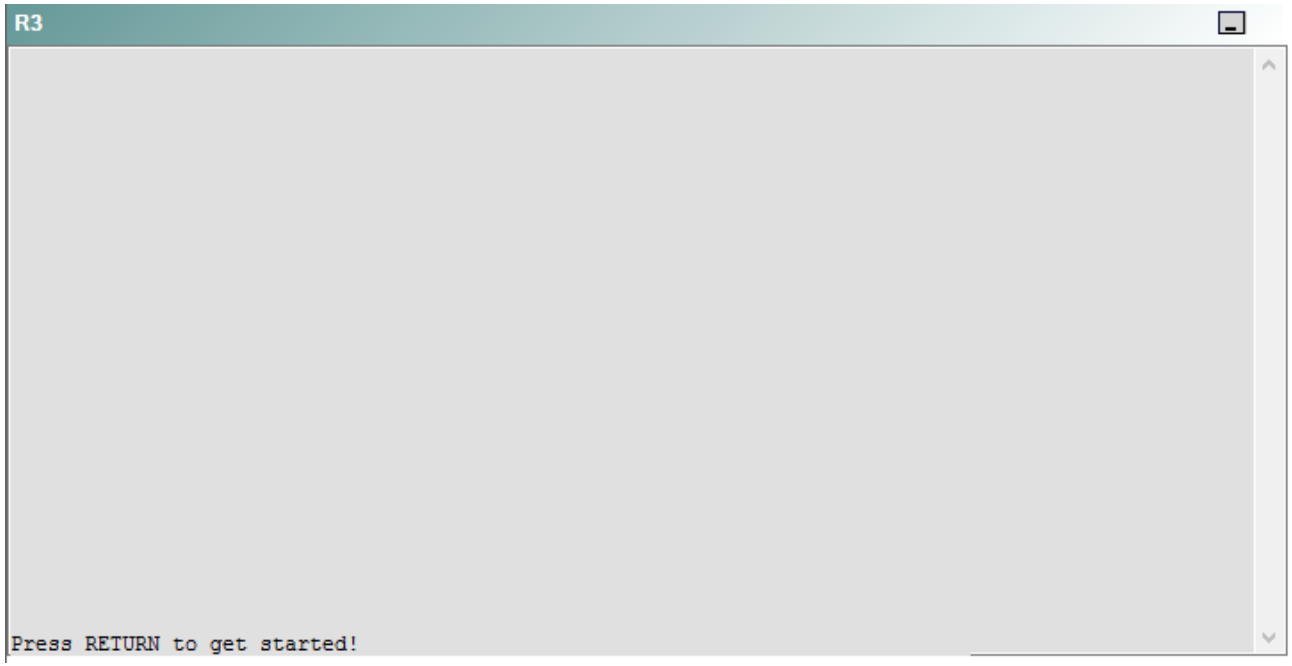
R1



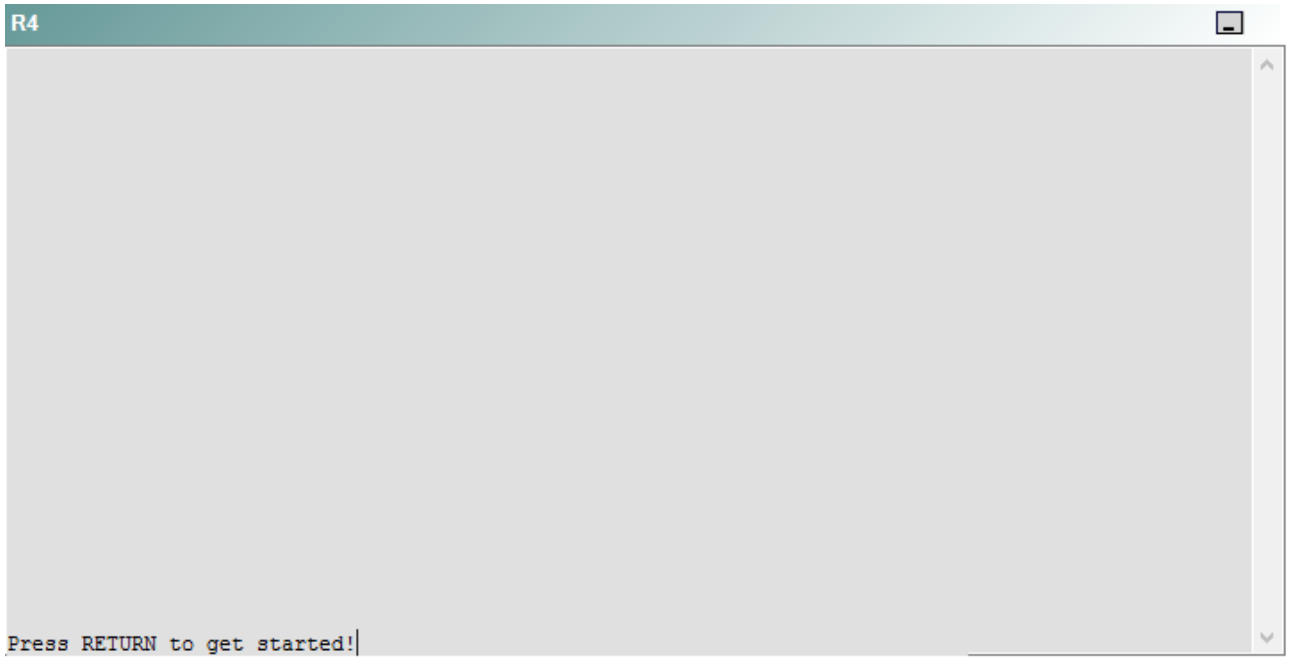

R2



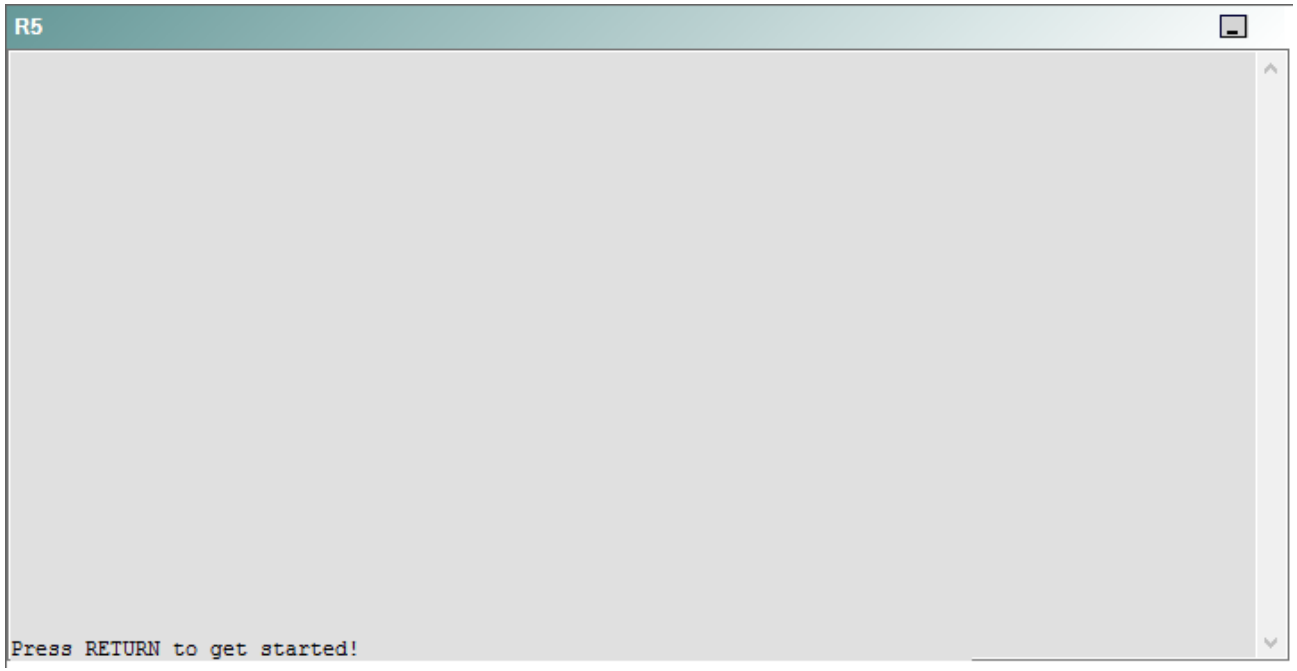

R3



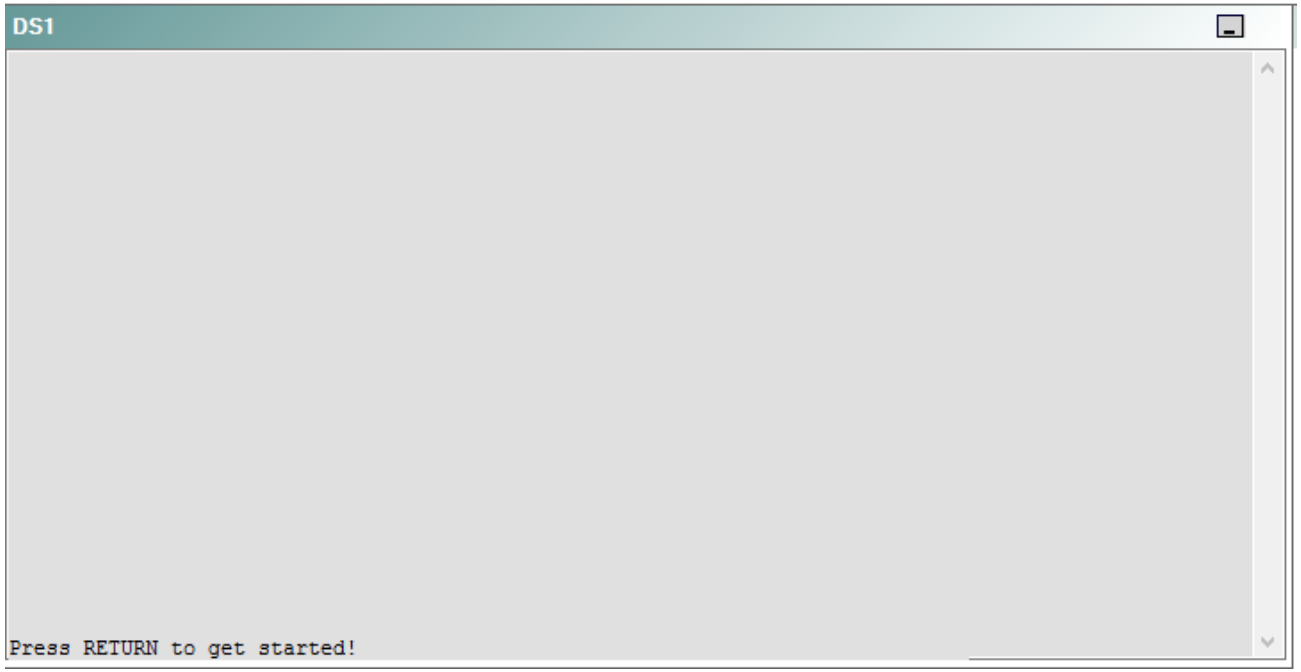

R4



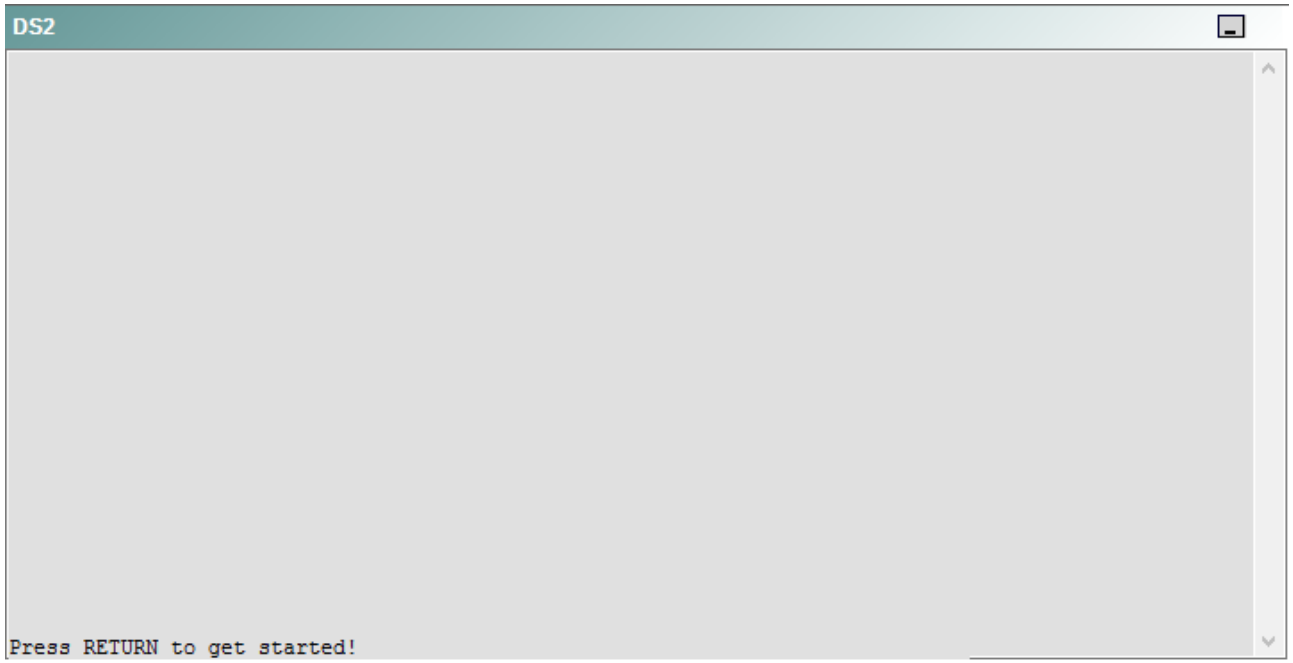

R5



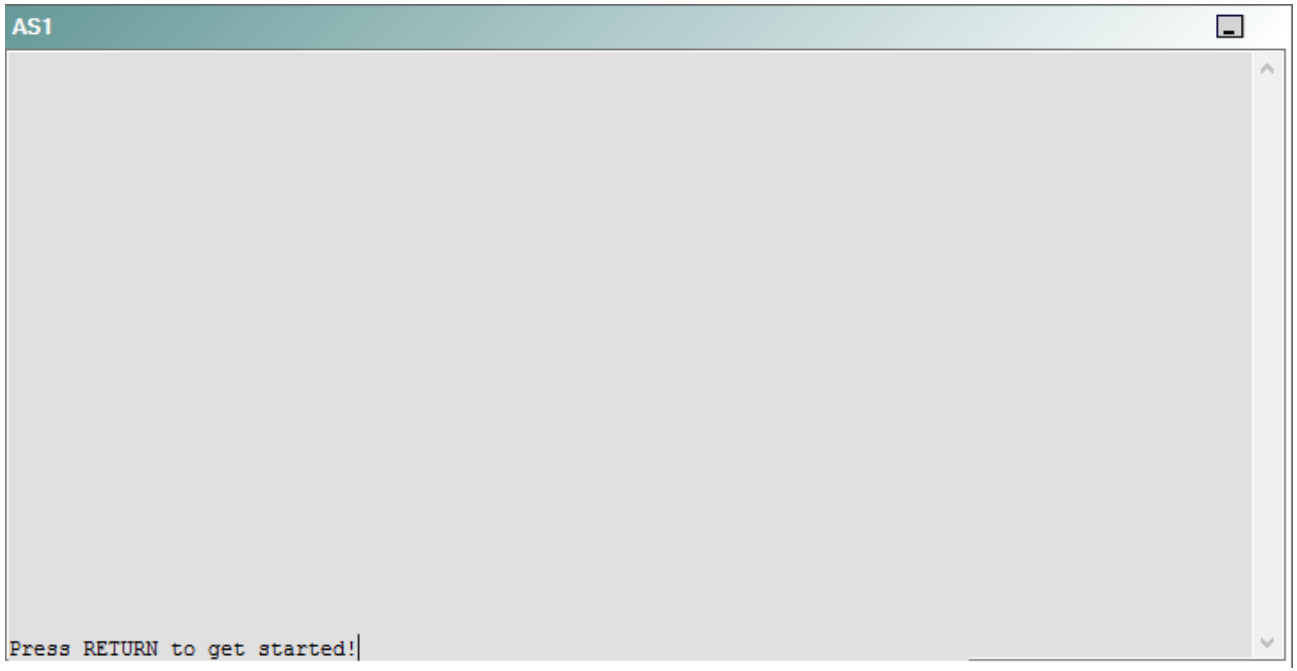

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that DS1 is not becoming the active router for devices on VLAN 22 when a manual interface shutdown test is conducted on DS2. DS2 should be the active router for devices on VLAN 22 when the FastEthernet0/1 interface on DS2 is up, but DS1 should become the active router when the FastEthernet0/1 interface on DS2 is down.

Which of the following technologies is the source of the problem?

A. NTP
B. HSRP
C. OSPFv2
D. DHCP
E. Layer 3 addressing
F. STP
G. Etherchannel
H. VLAN configuration
I. interface

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 63**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

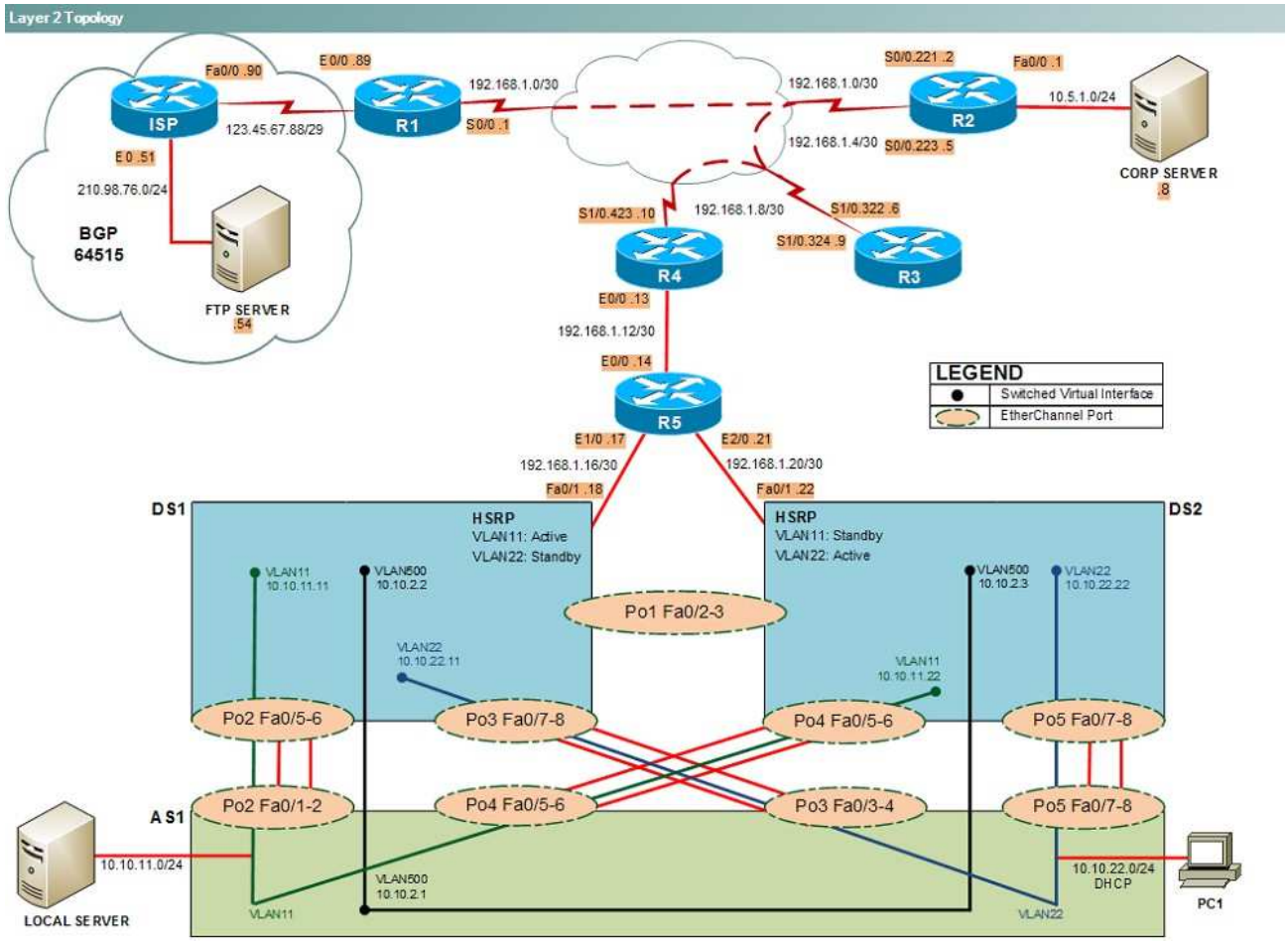
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

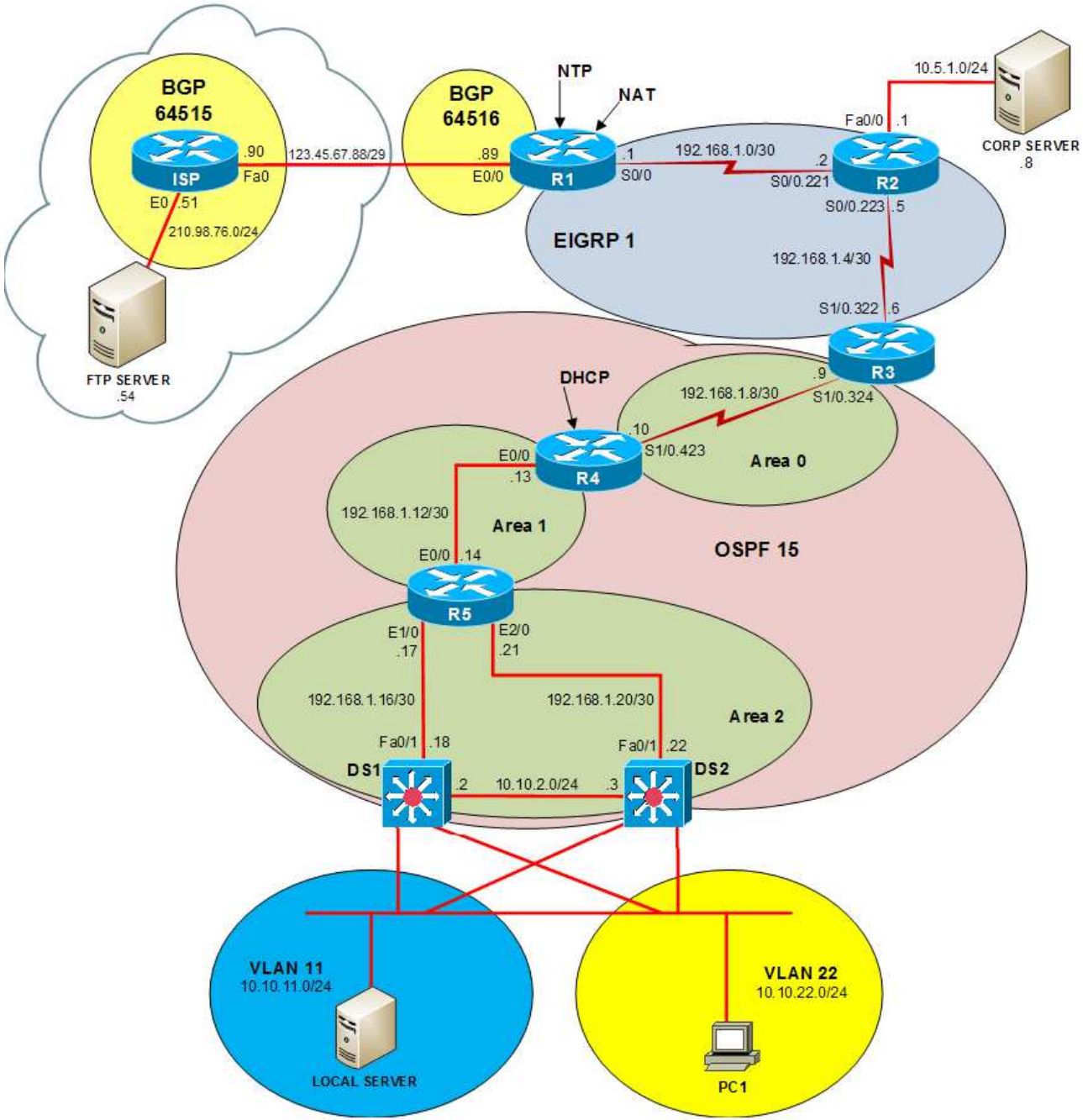
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

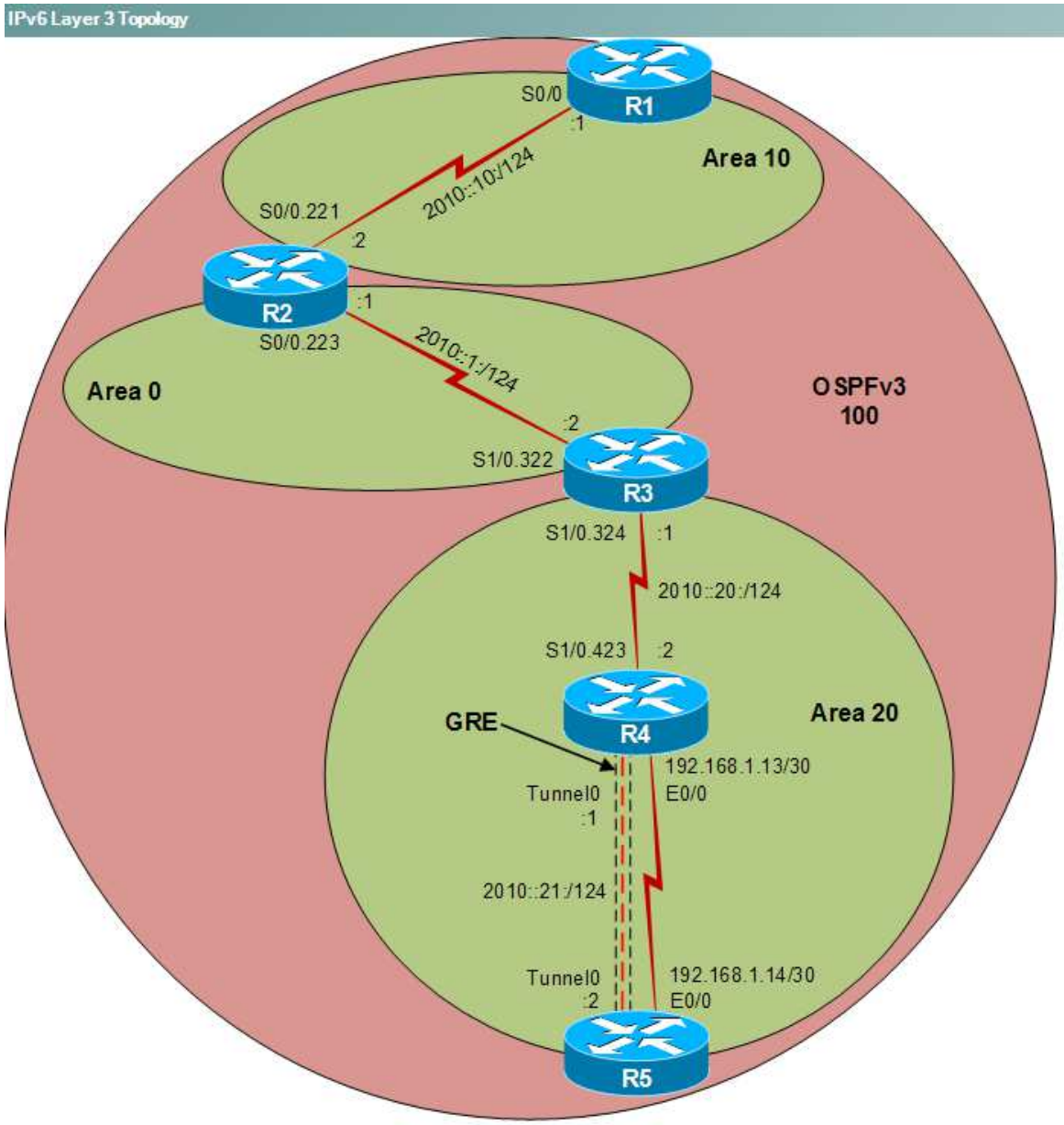
**Layer 2 Topology**




IPv4 layer 3 Topology

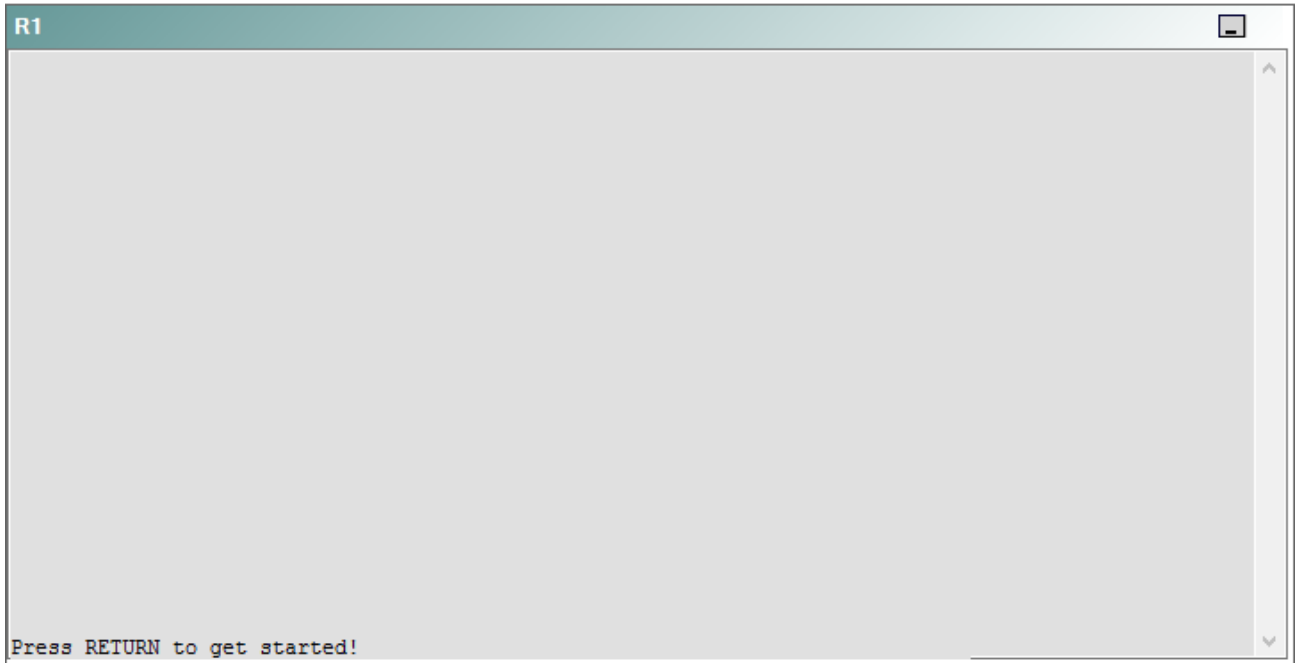

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

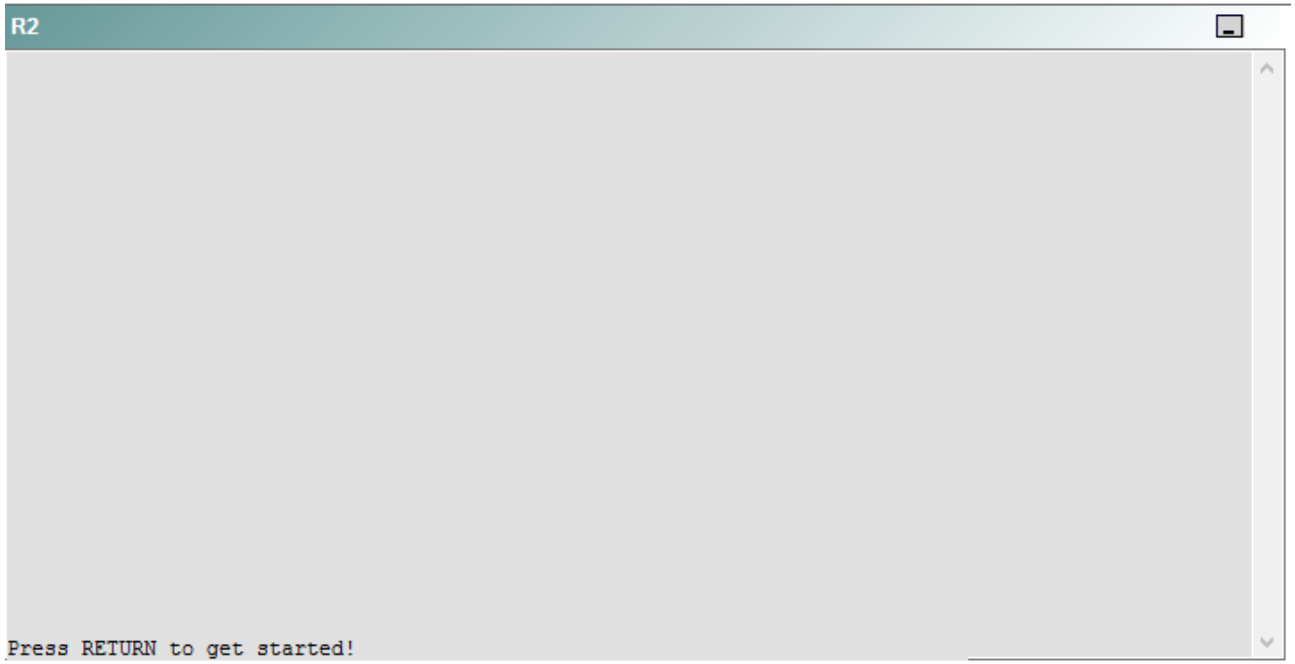



https://www.gratisexam.com/

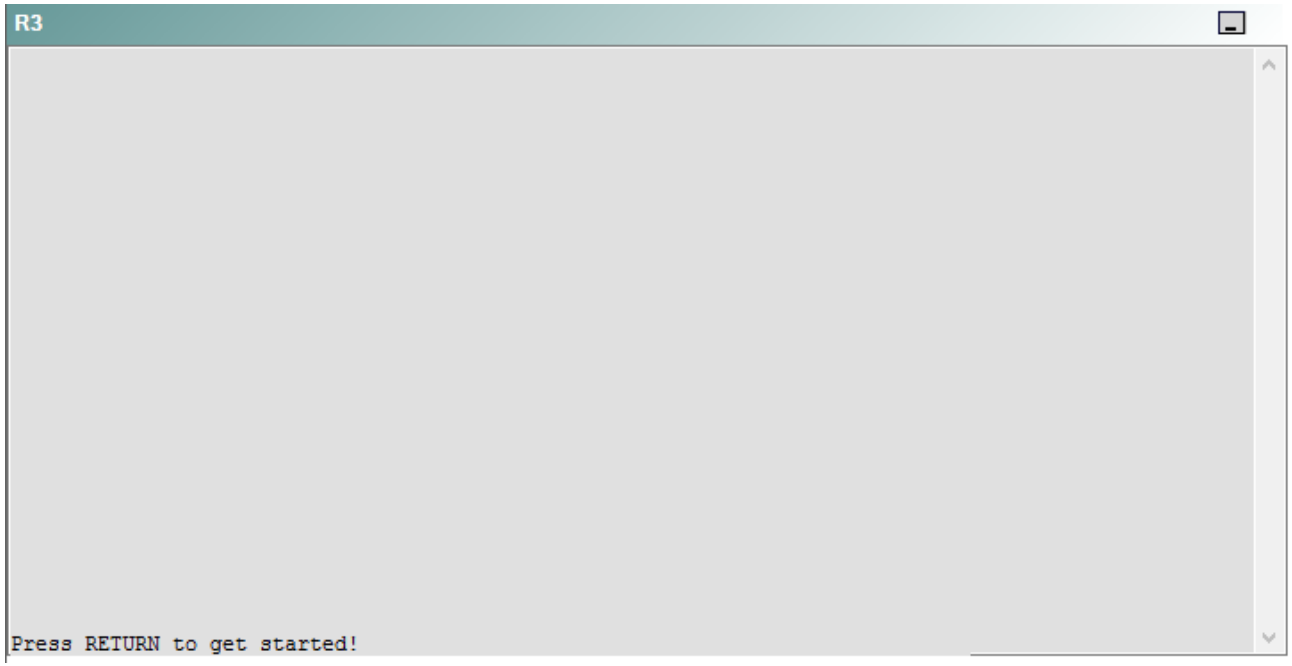
R1



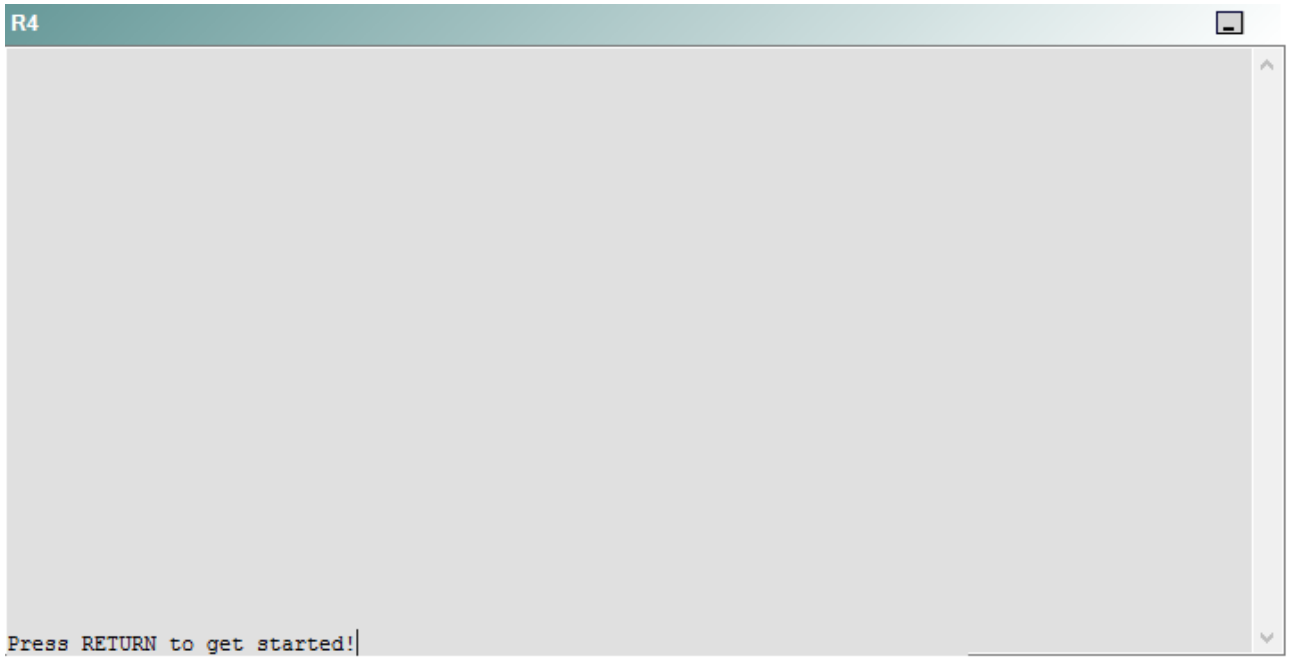

R2



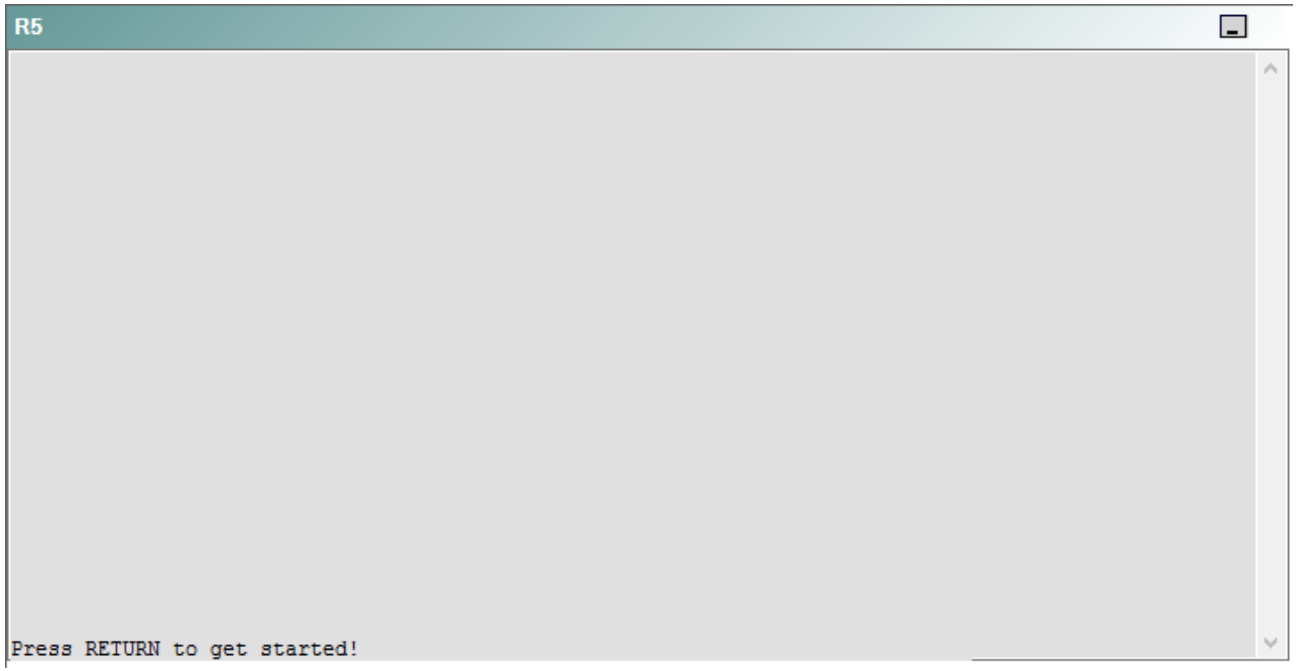

R3



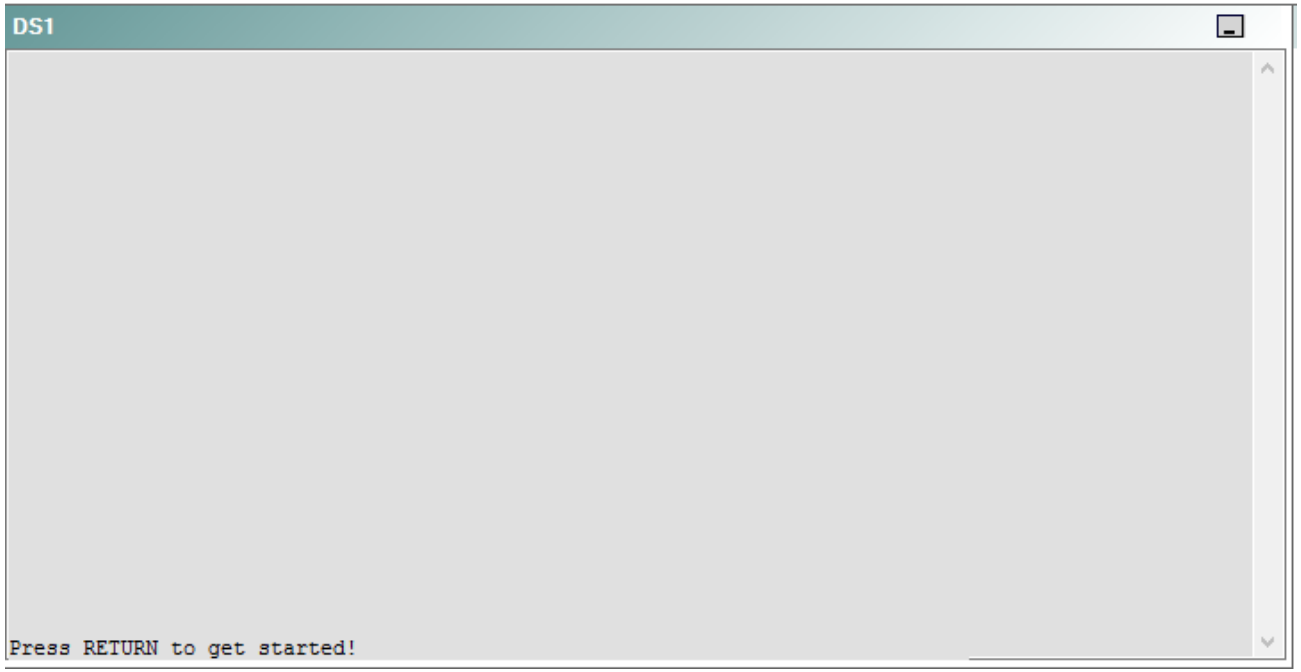

R4



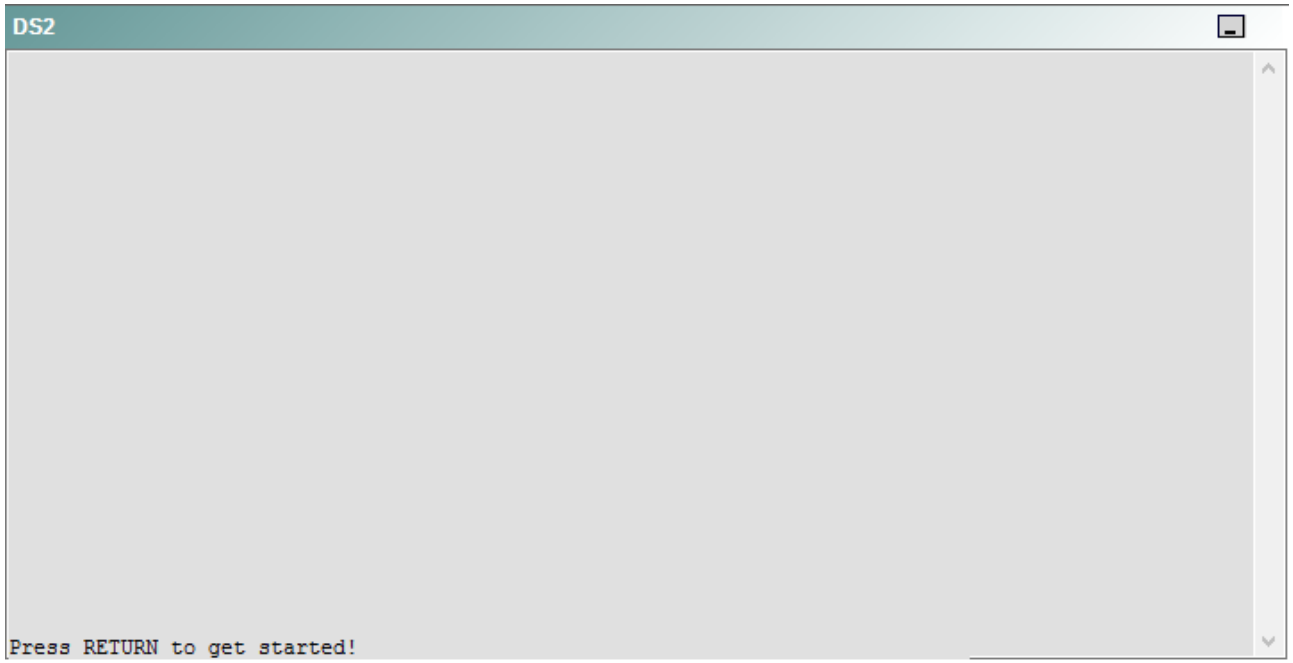

R5



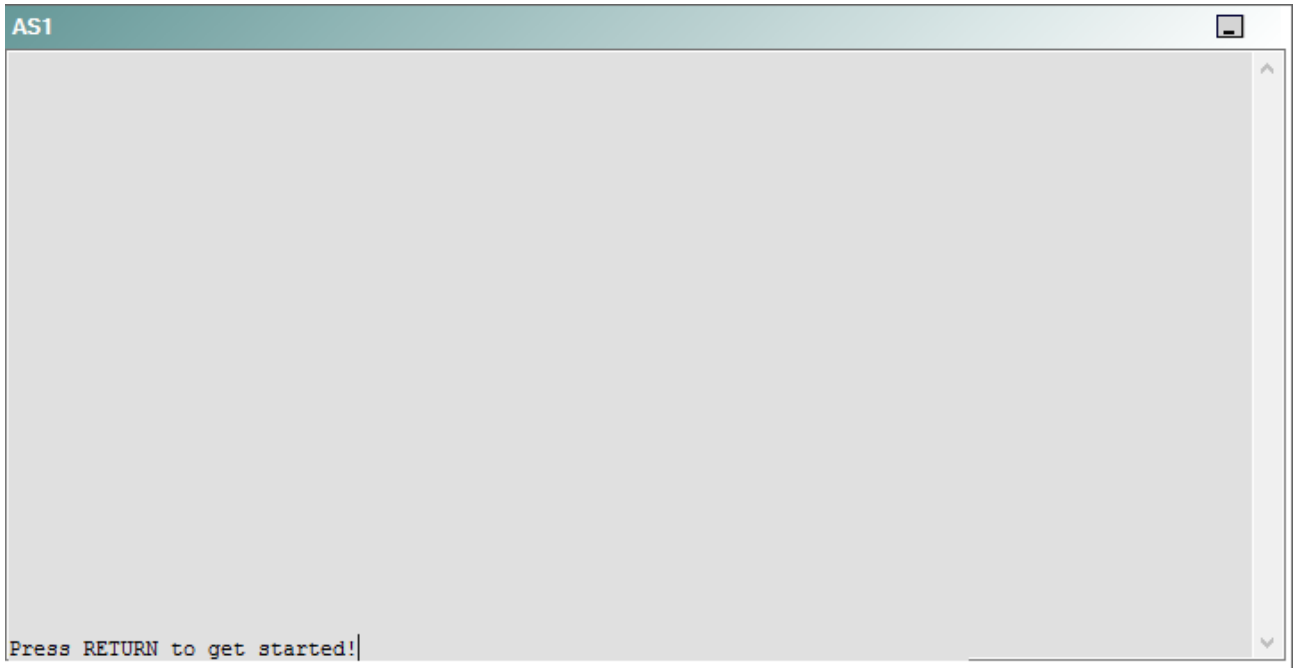

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that the clock on AS1 is not synchronized with the clock on R1. You need to ensure that all devices are synchronized with the clock on R1.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 64**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

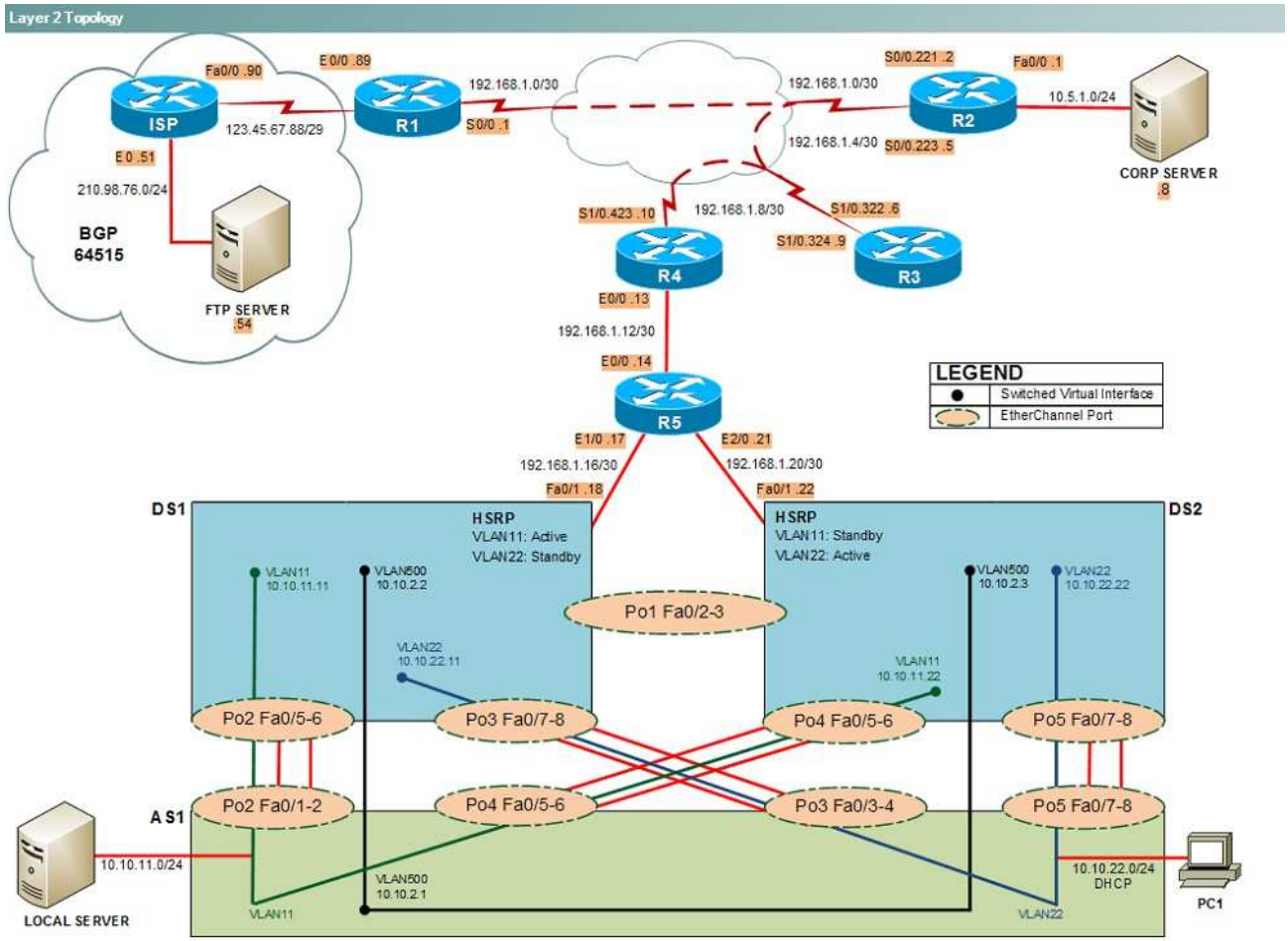
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

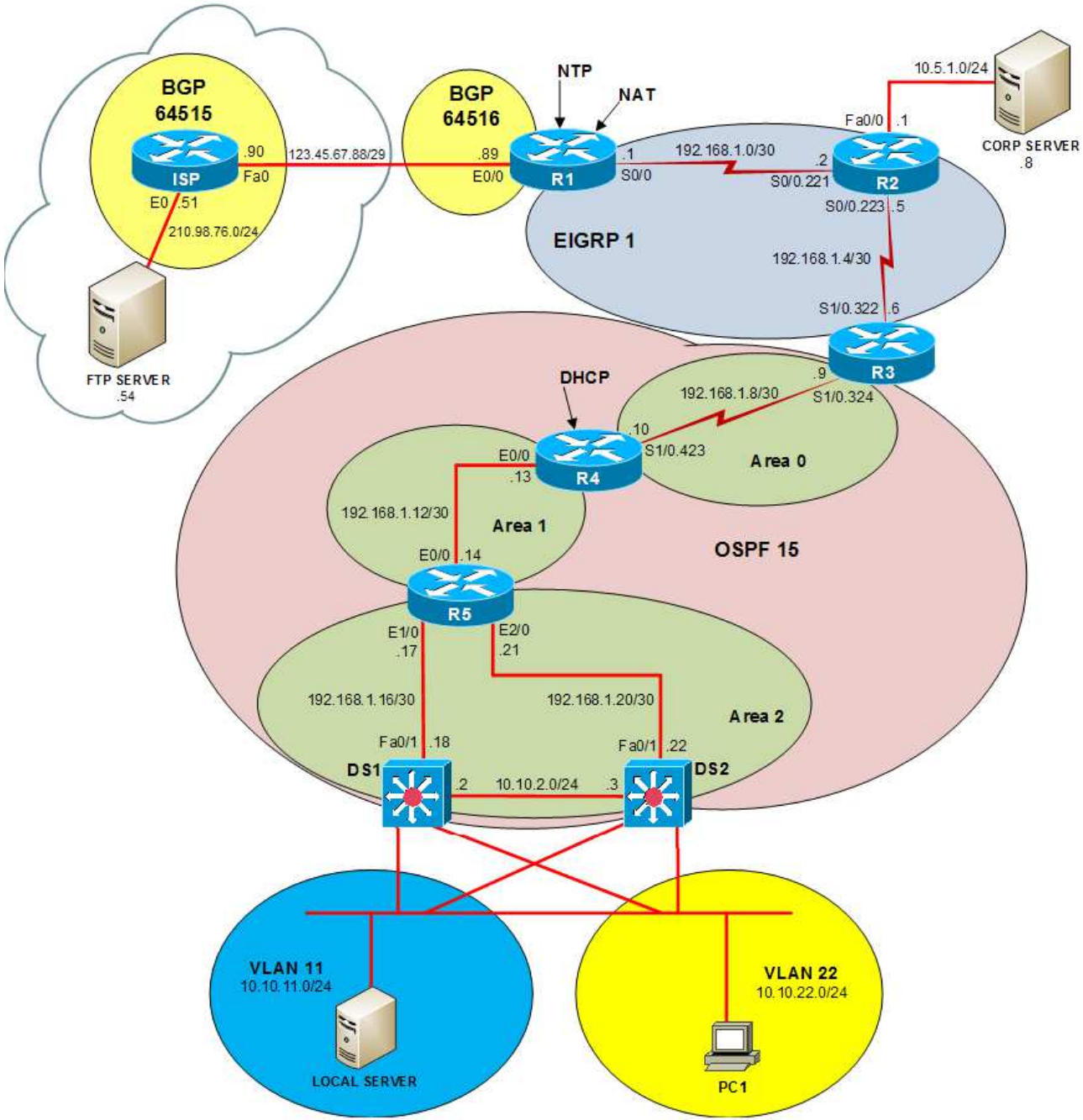
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

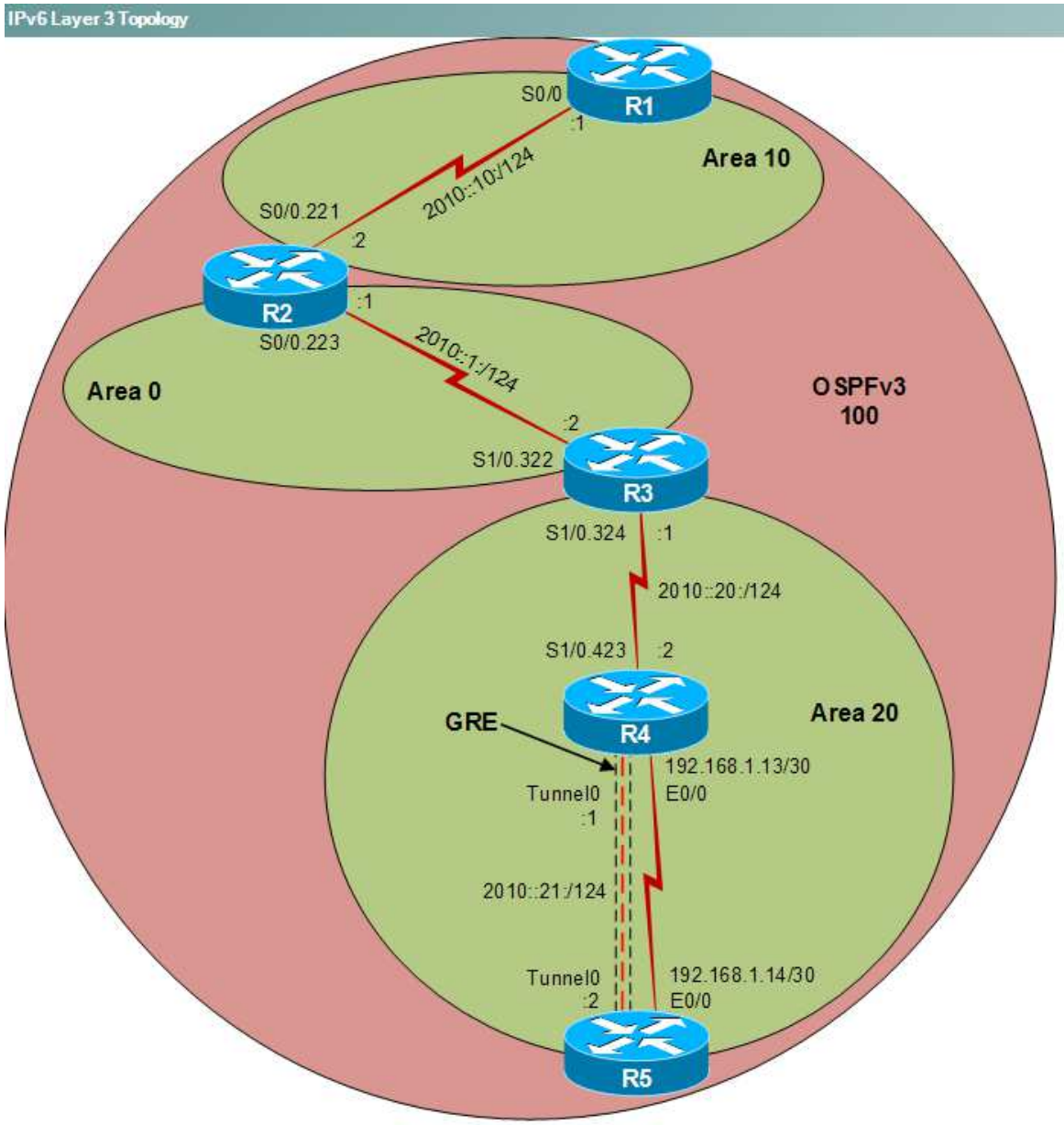
**Layer 2 Topology**




IPv4 layer 3 Topology

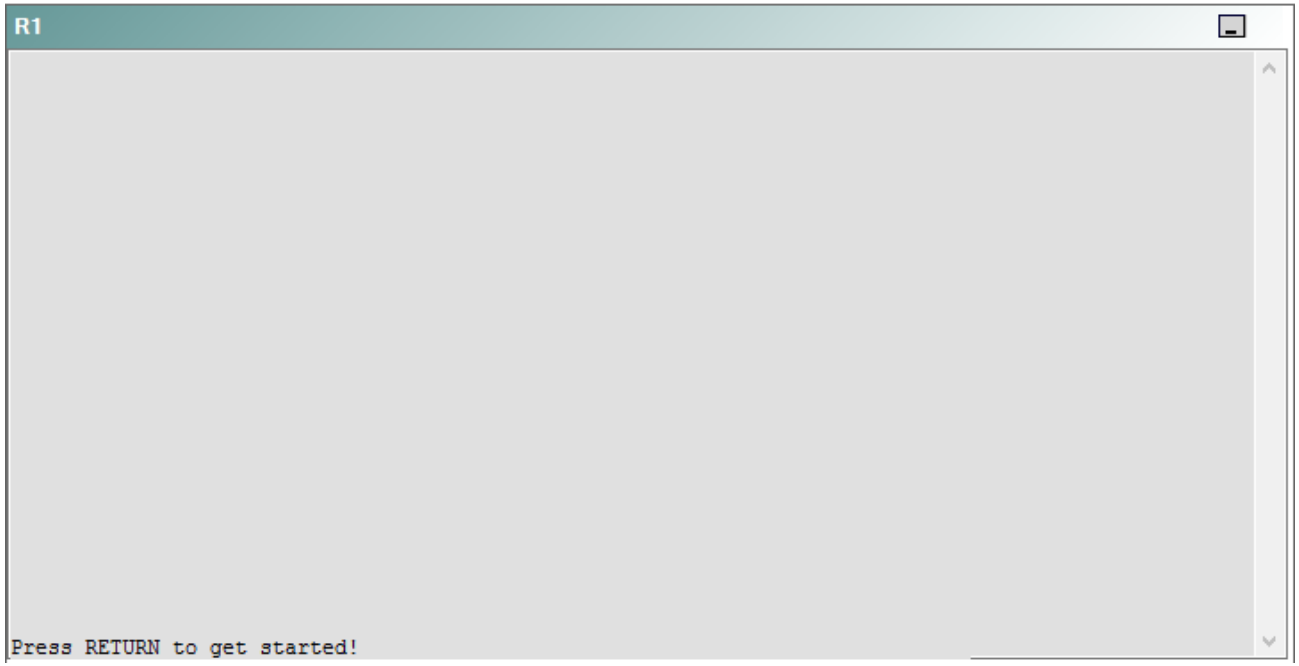

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

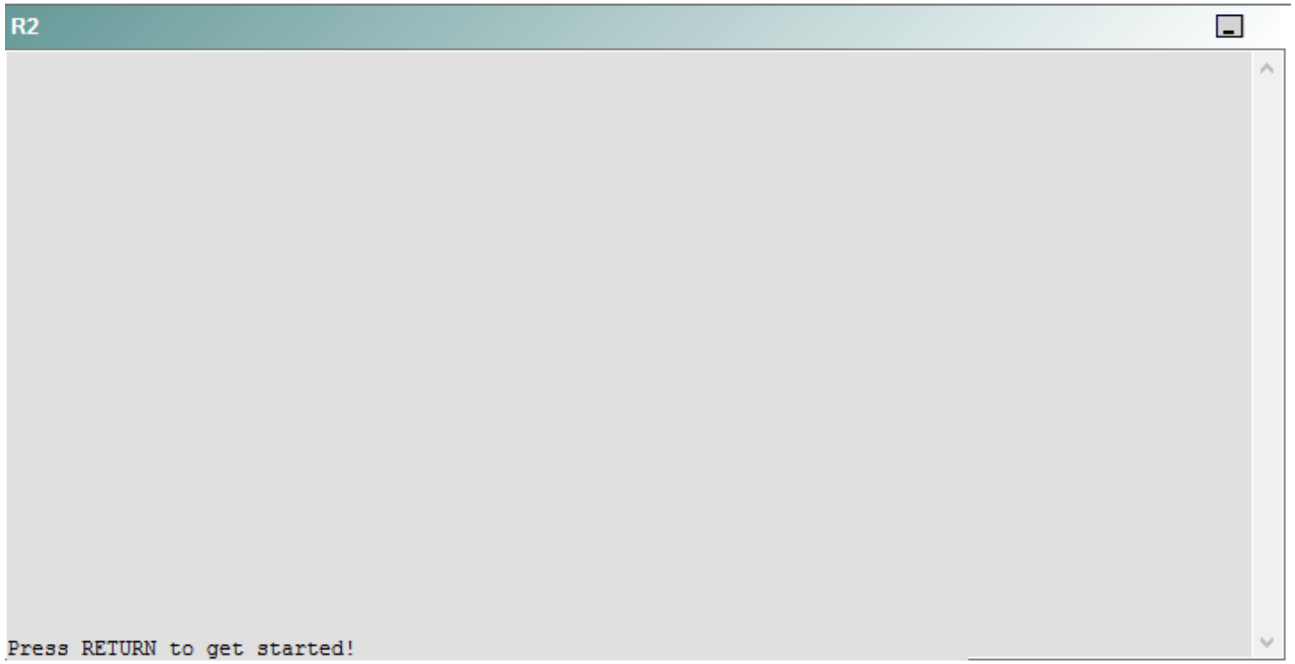



https://www.gratisexam.com/

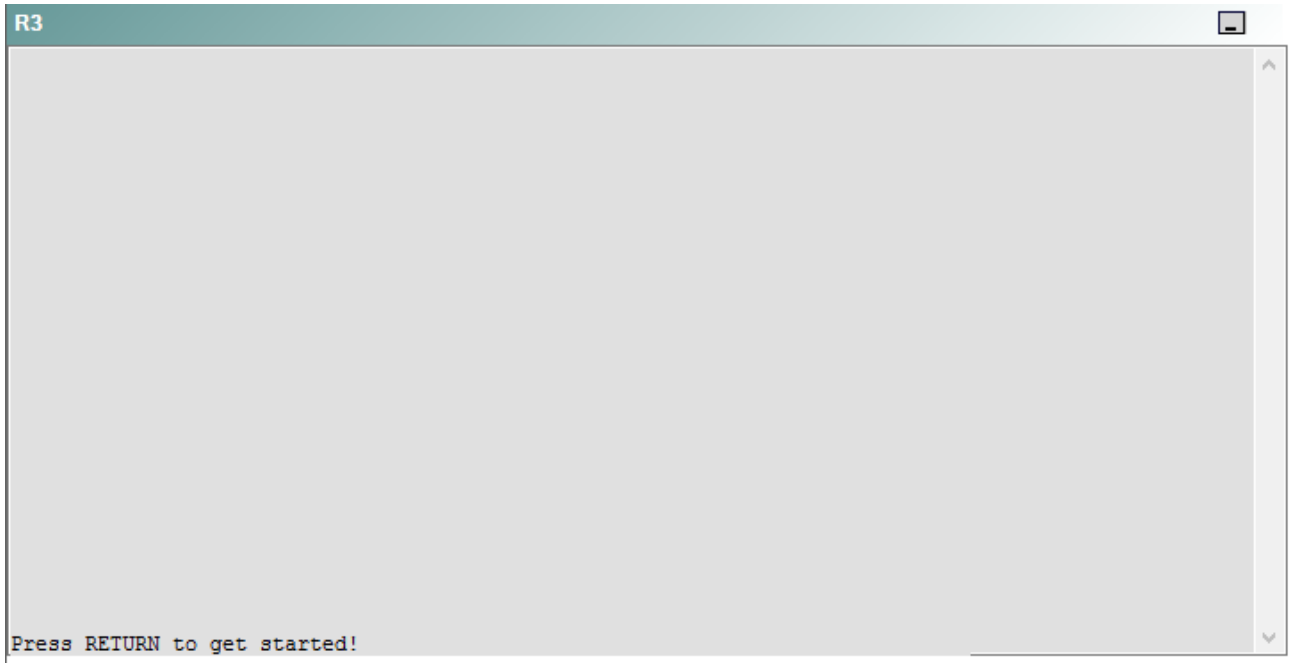
R1



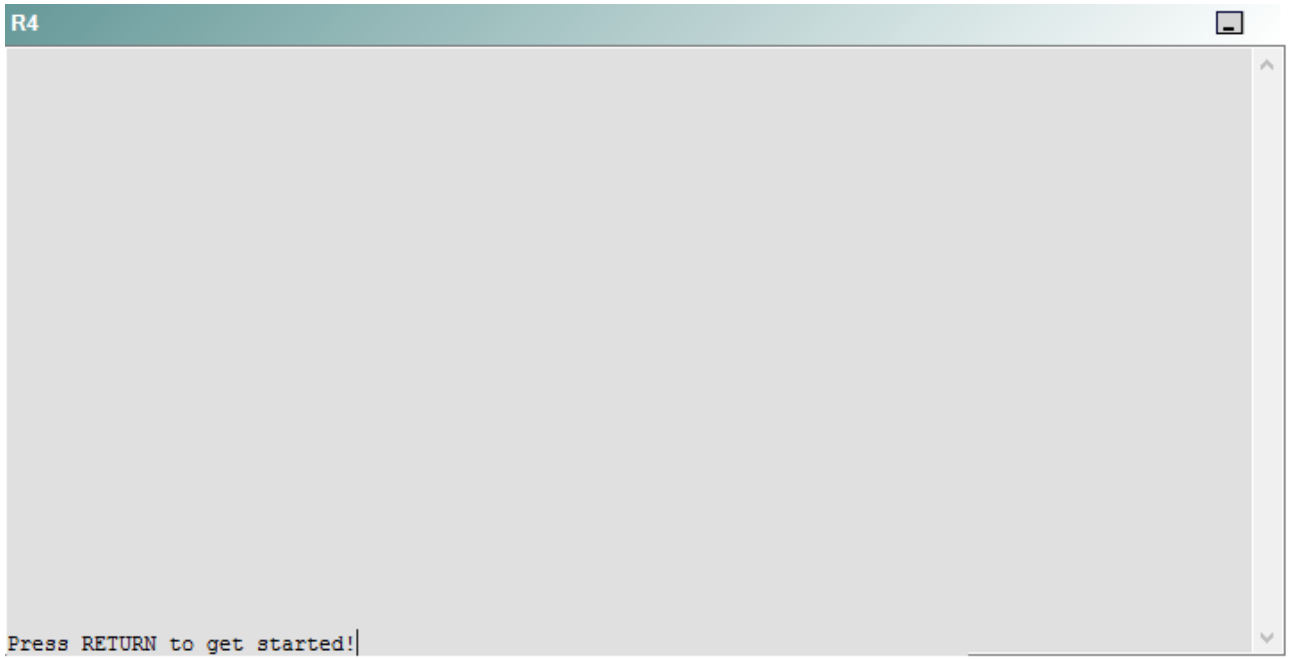

R2



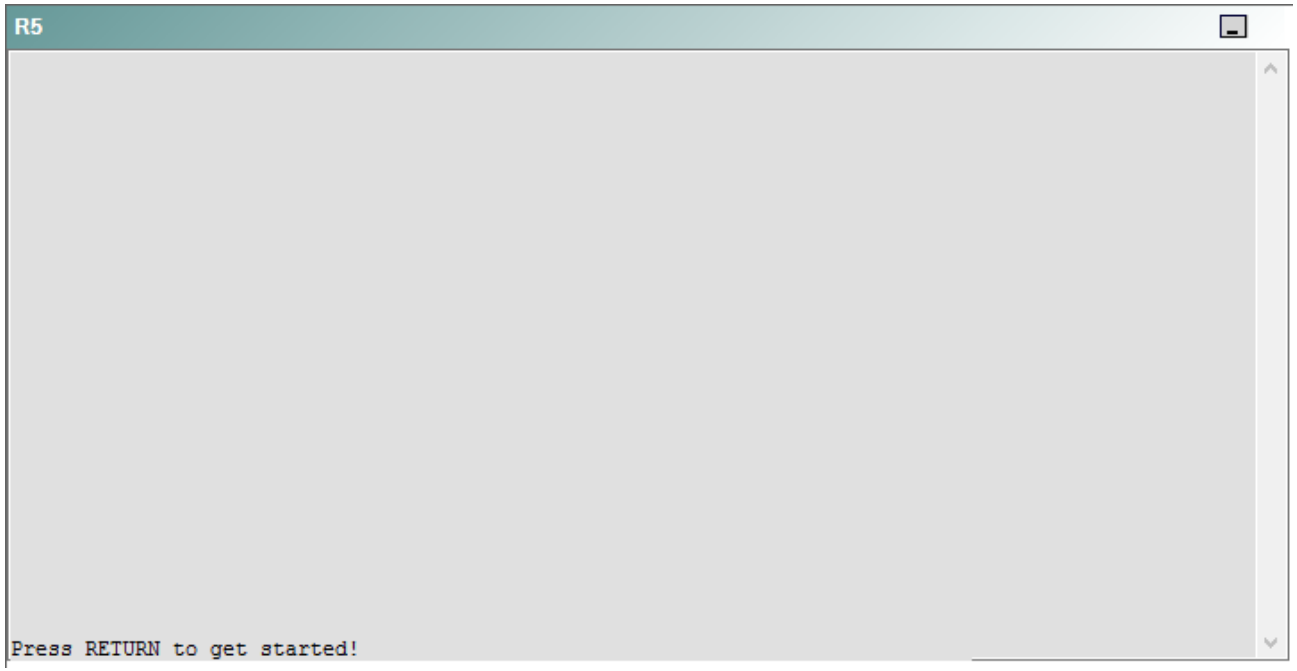

R3



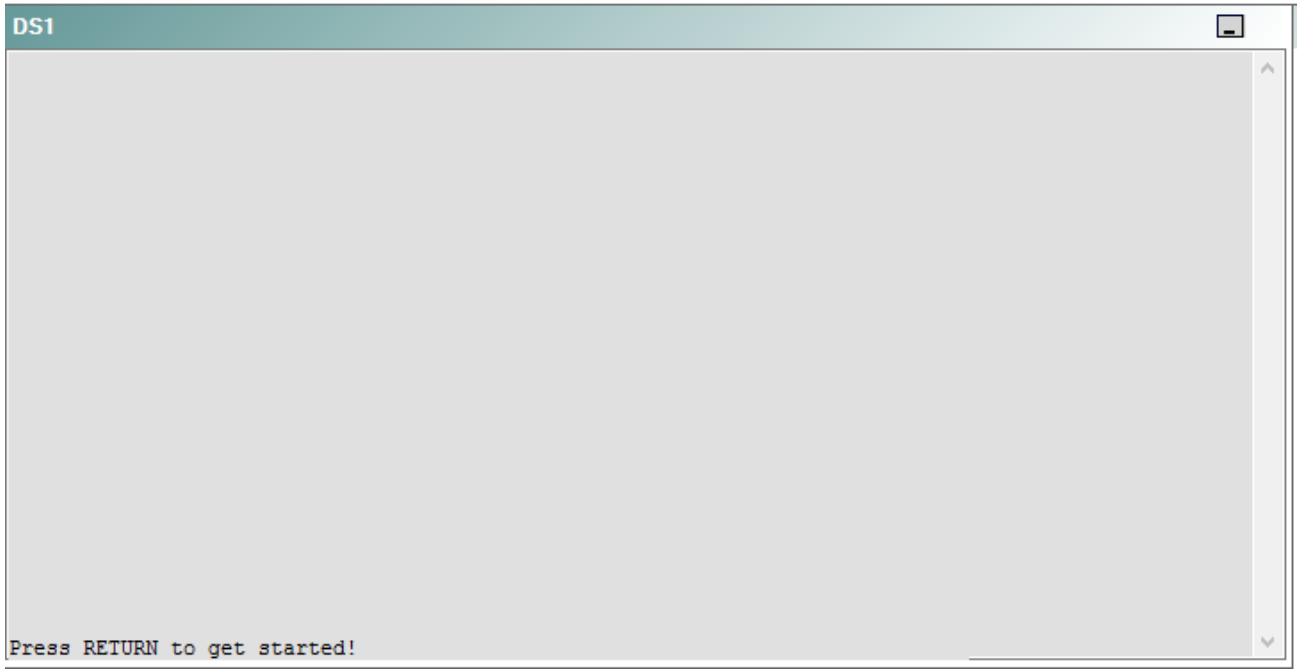

R4



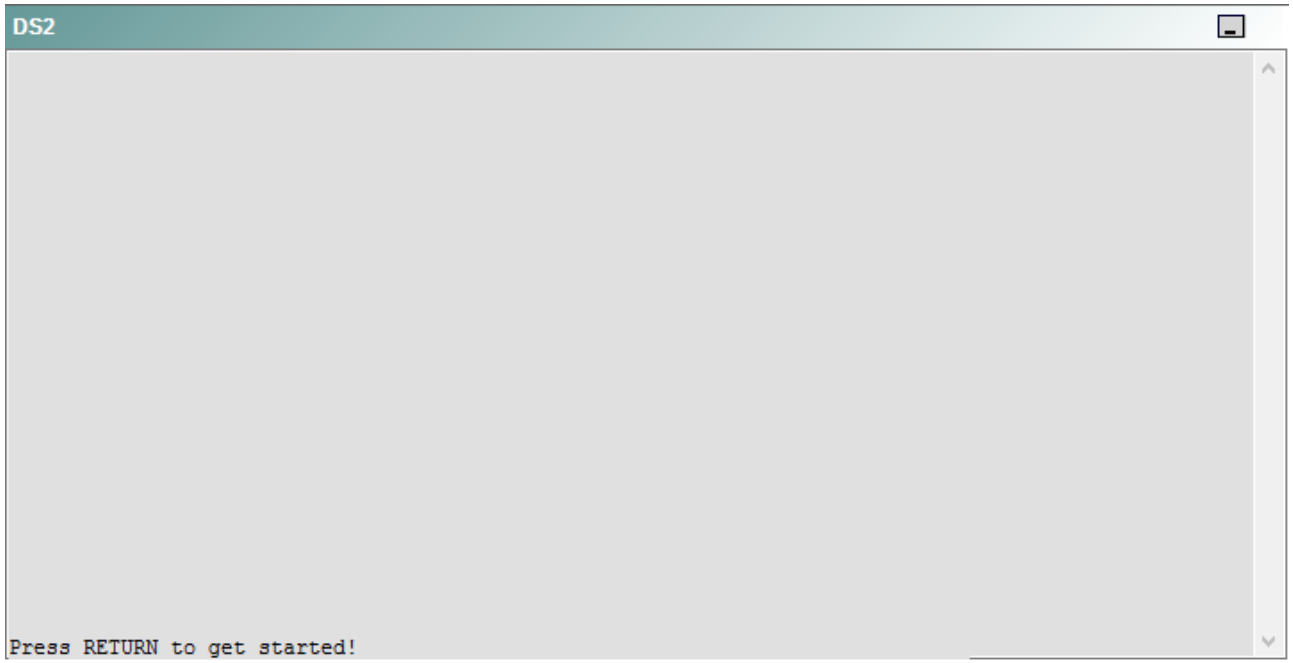

R5



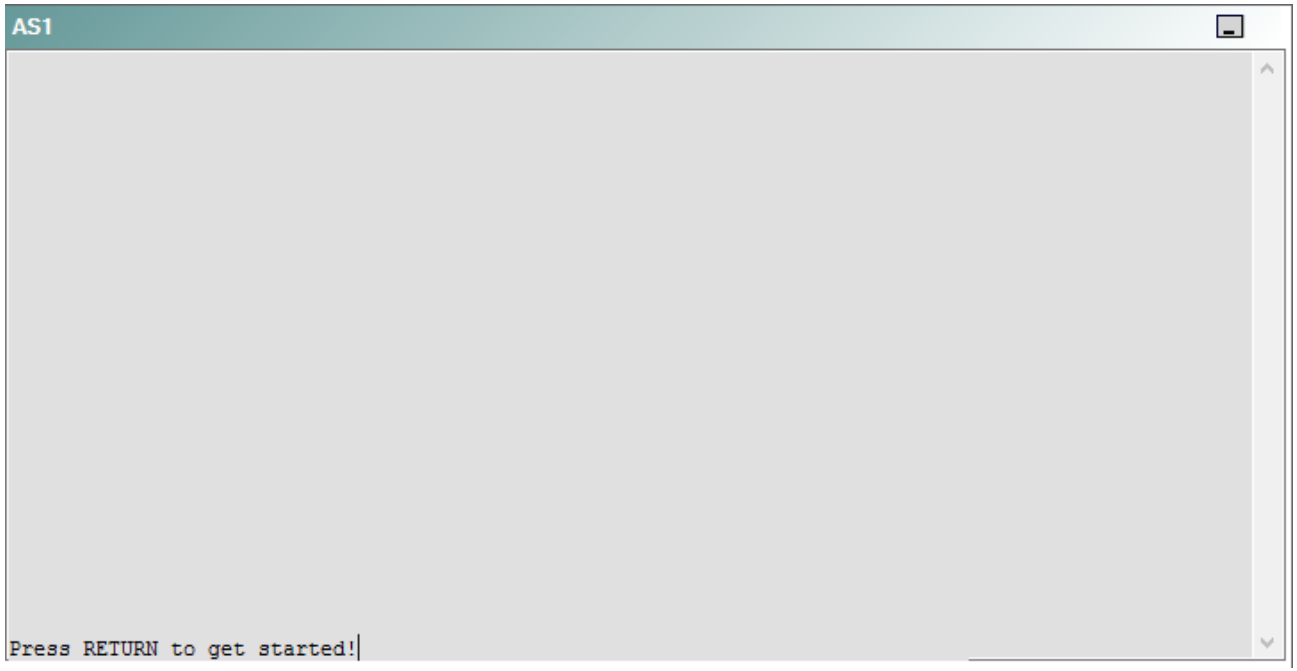

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that the clock on AS1 in not synchronized with the clock on R1. You need to ensure that all devices are synchronized with the clock on R1.

Which of the following technologies is the source of the problem?

A. NTP
B. OSPFv3
C. Layer 3 addressing
D. Layer 3 security
E. redistribution
F. interface

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

**QUESTION 65**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

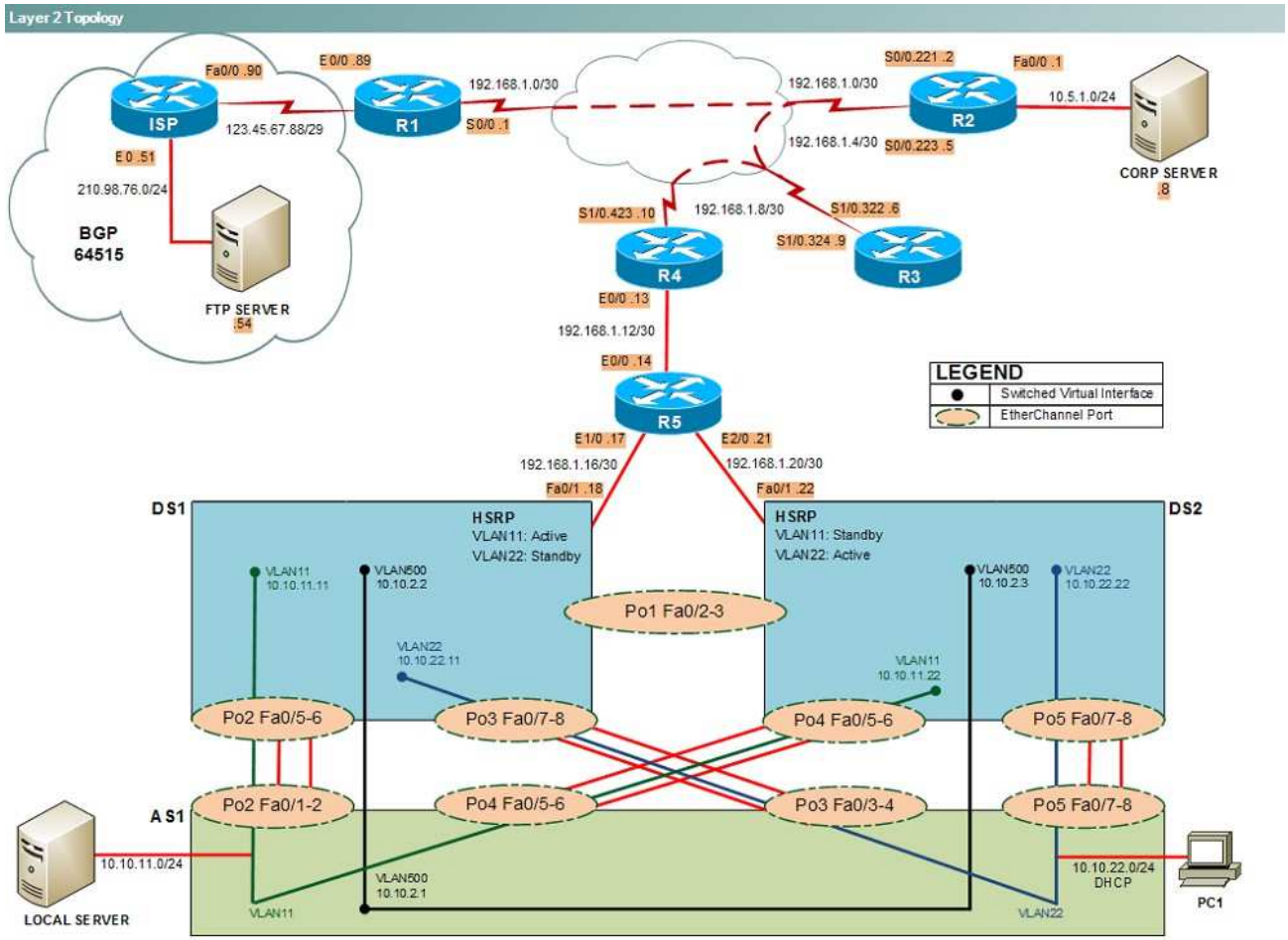
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

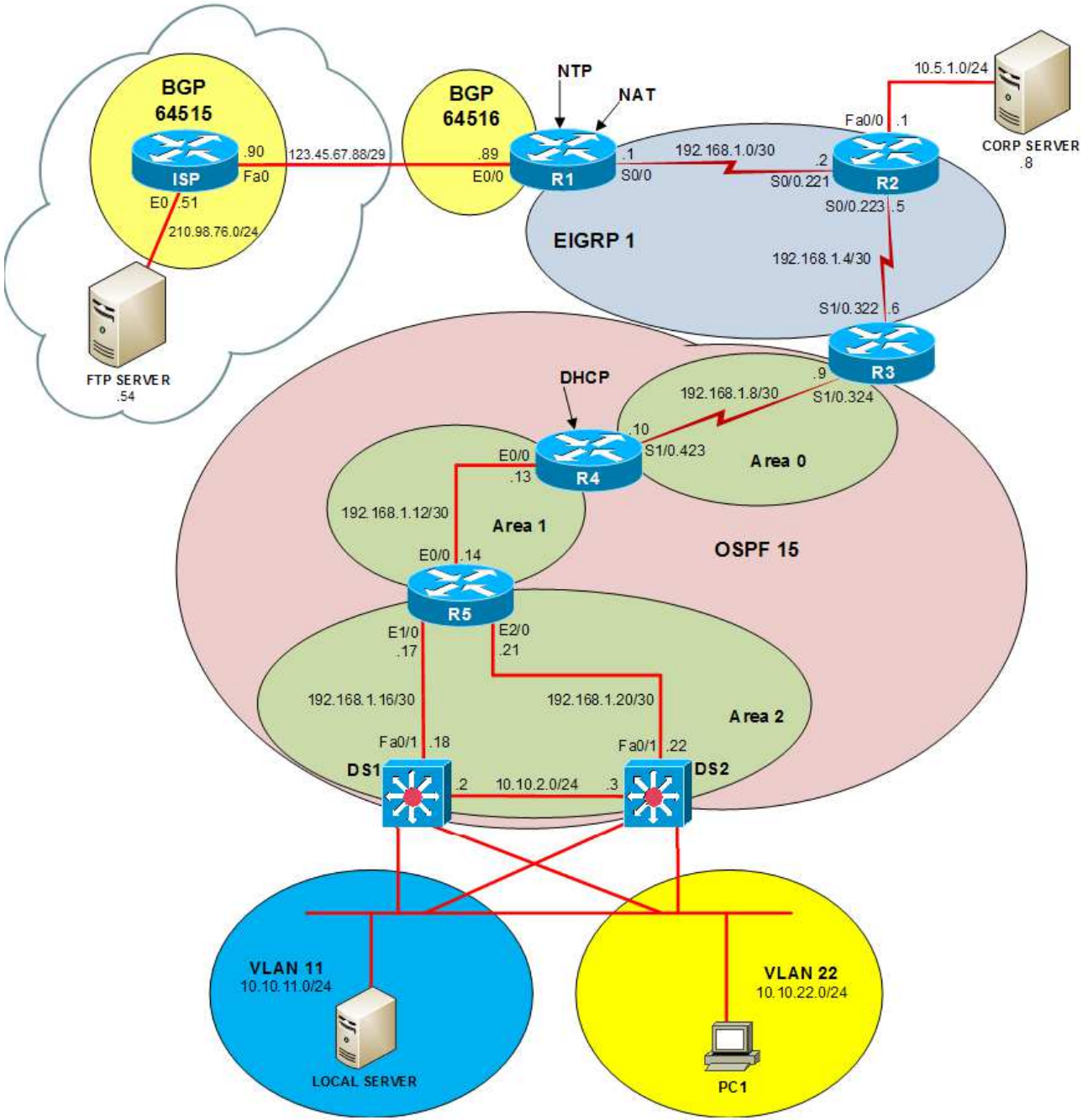
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

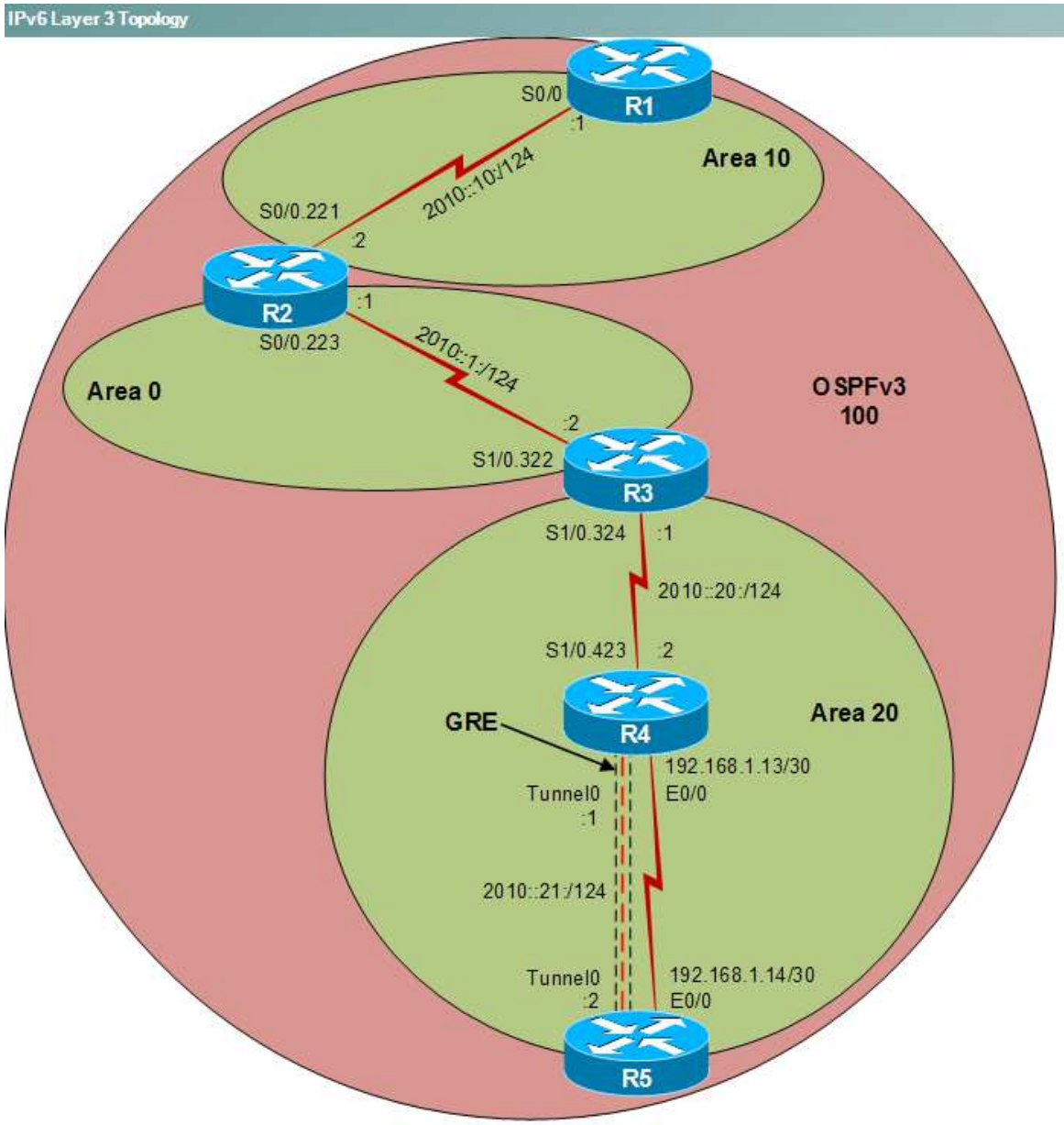
**Layer 2 Topology**




IPv4 layer 3 Topology

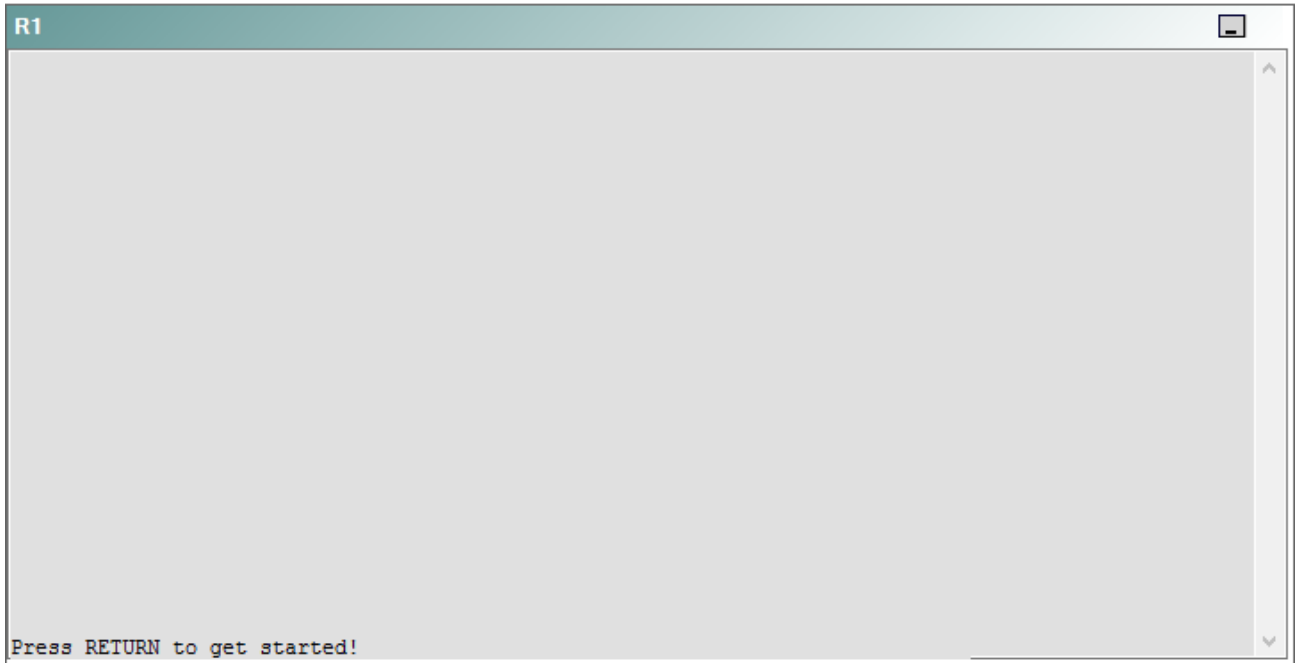

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

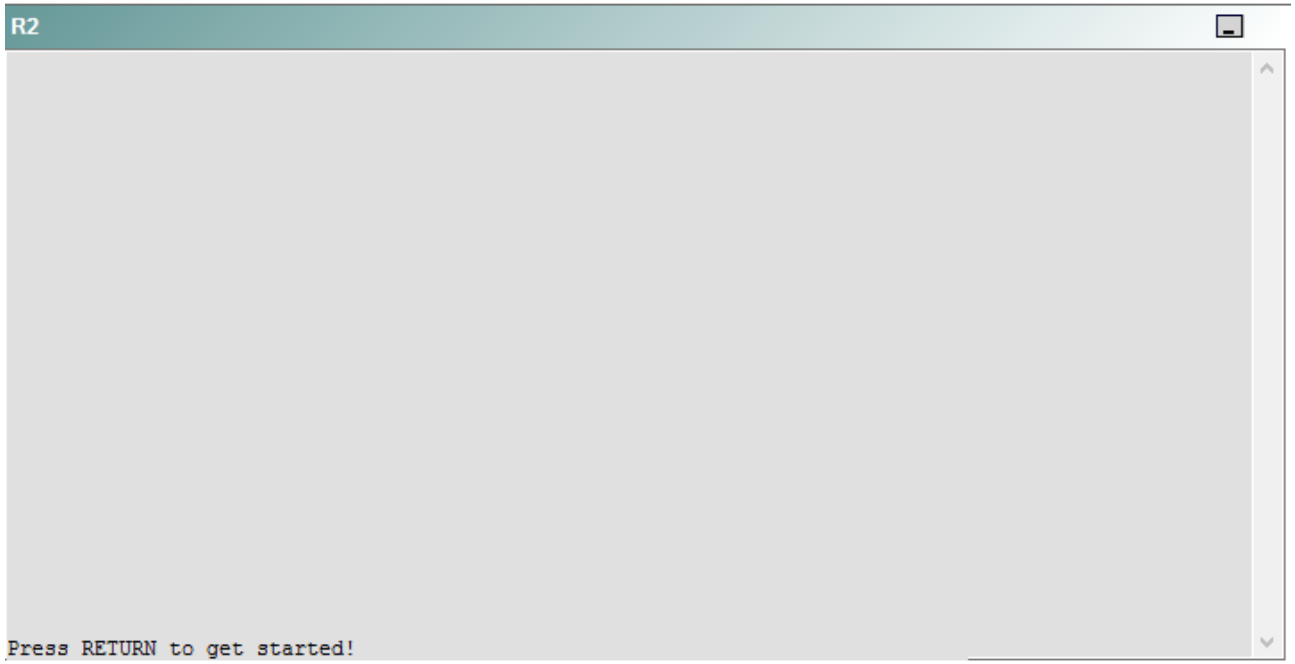



https://www.gratisexam.com/

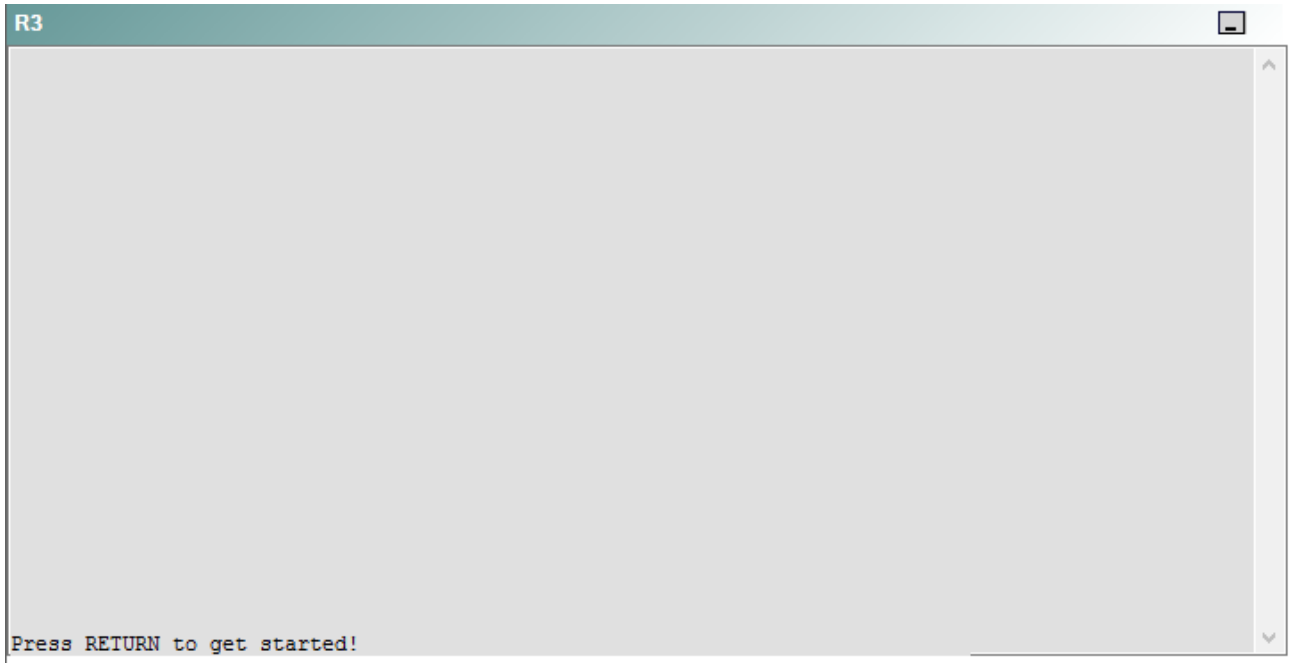
R1



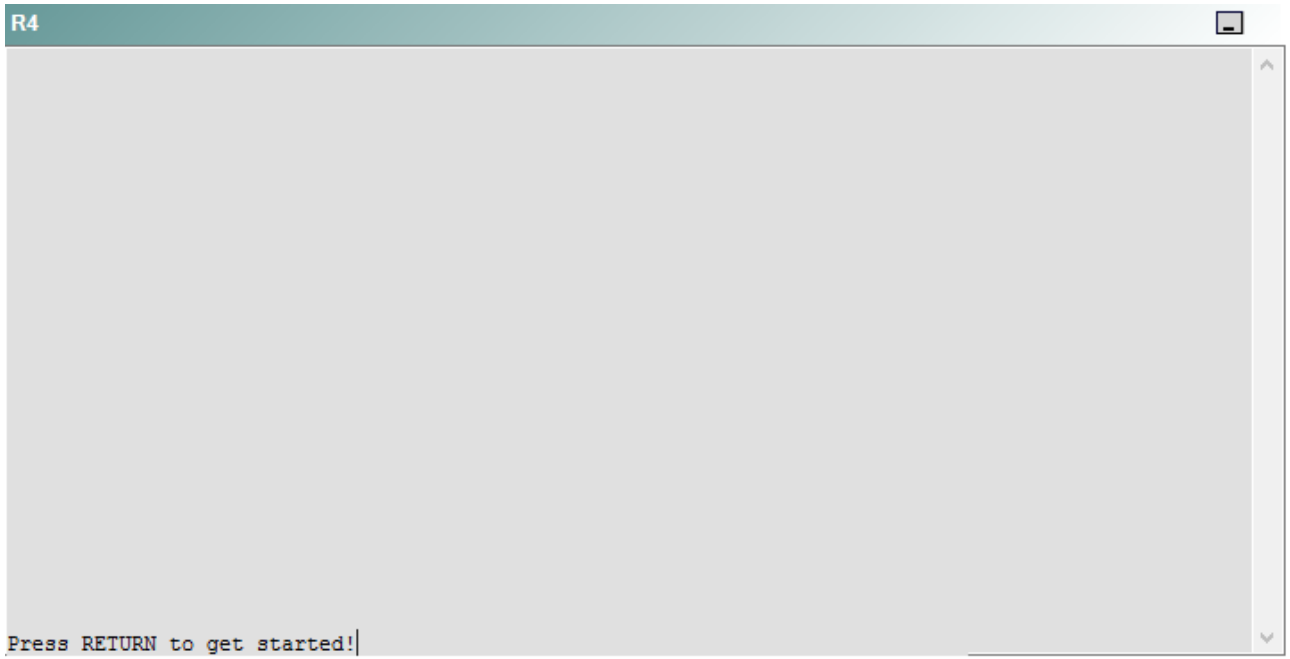

R2



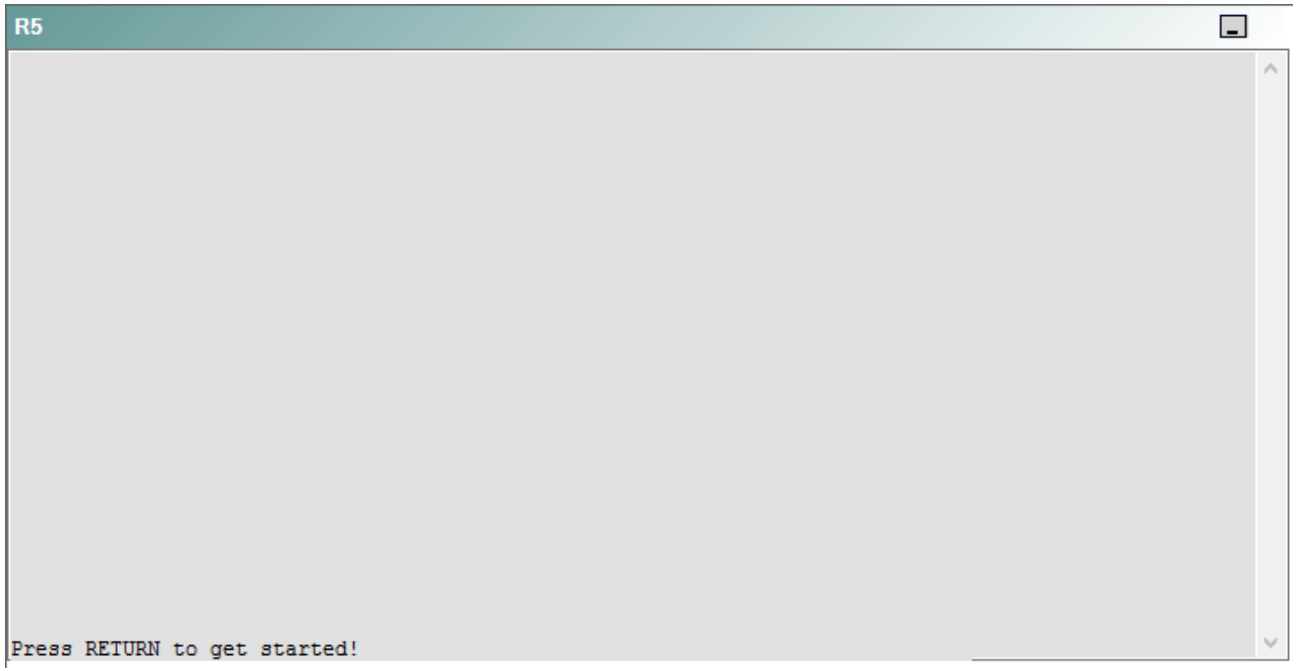

R3



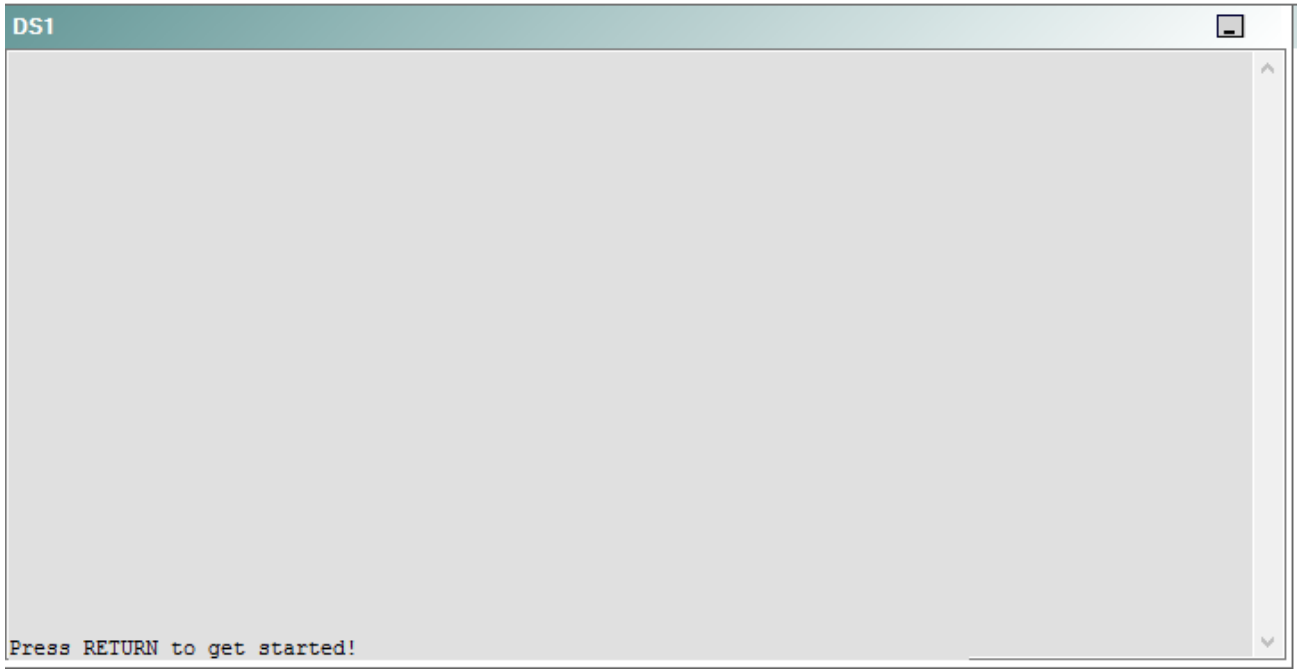

R4



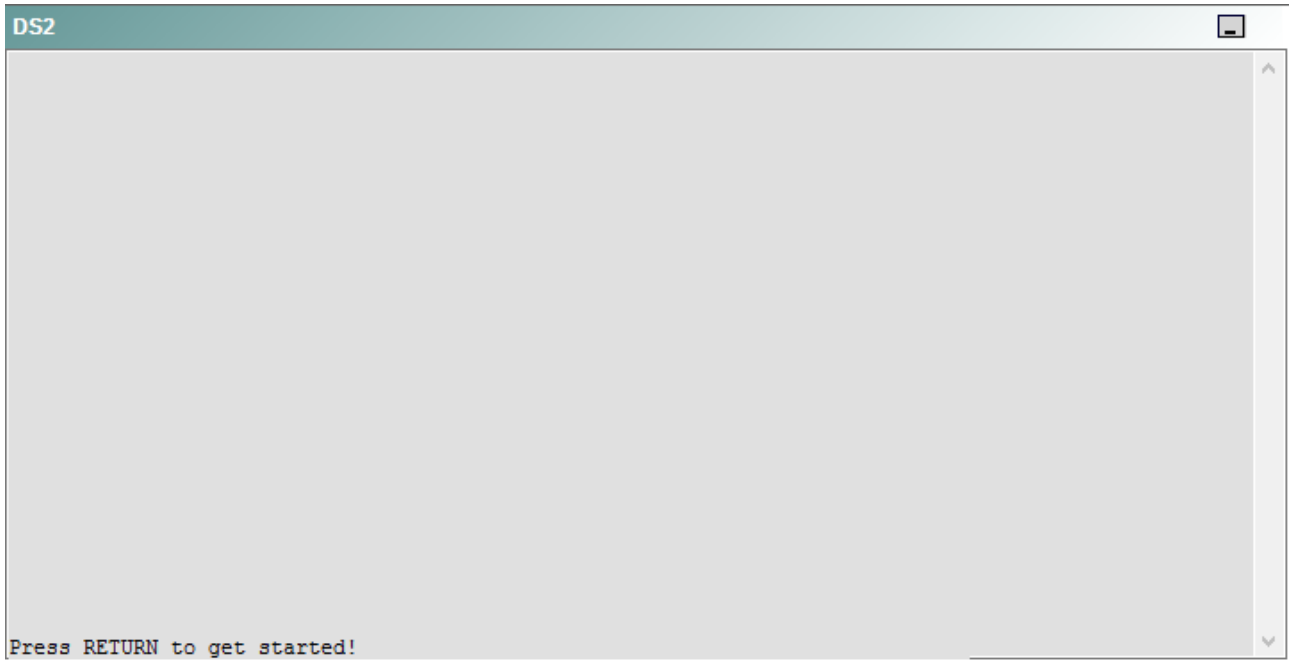

R5



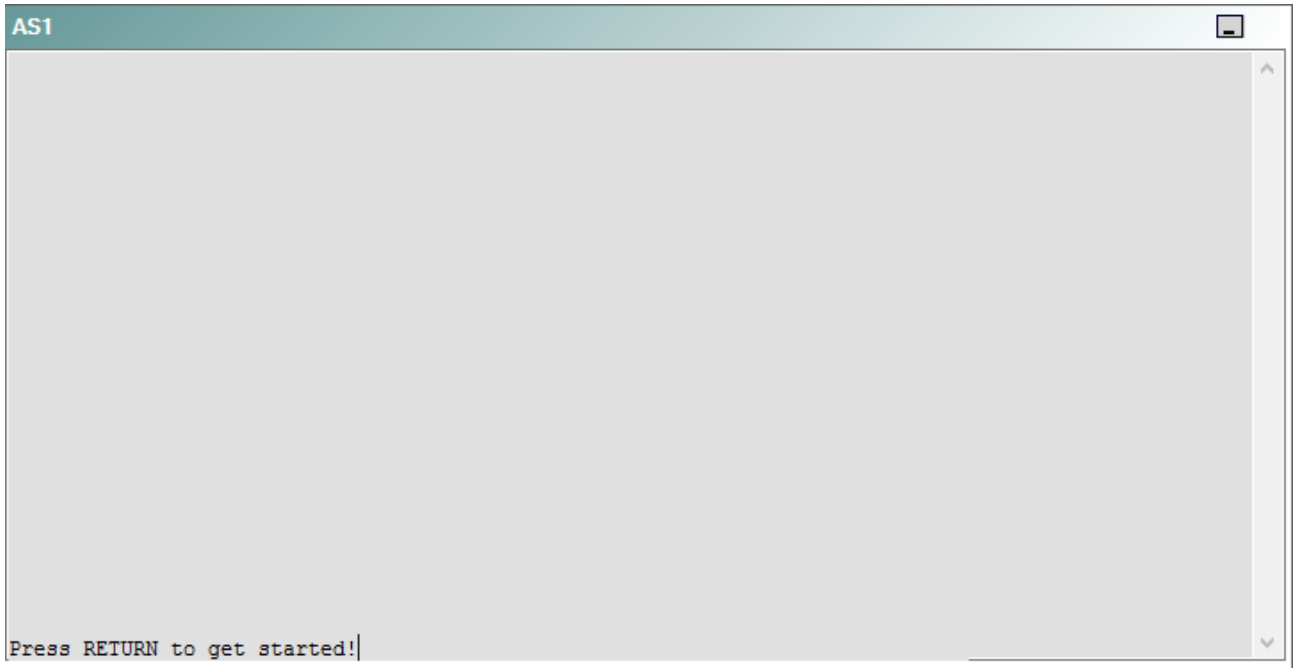

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that the clock on AS1 is not synchronized with the clock on R1. You need to ensure that all devices are synchronized with the clock on R1.

Which of the following is most likely to solve the problem?

A. issuing the **no ntp master** command in global configuration mode
B. issuing the **ntp master 1** command in global configuration mode
C. issuing the **ntp master 192.168.1.1** command in global configuration mode
D. issuing the **ntp server 192.168.1.5** command in global configuration mode
E. removing the current **NTP server** command, and issuing the ntp server 192.168.1.1 command in global configuration mode
F. issuing the **clock set** command

**Correct Answer:** E
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

You should remove the currently configured **ntp server** command from R2 and issue the **ntp server 192.168.1.1** command in global configuration mode. To determine which device is the source of the problem, you can issue the **show running-config** command on each device to view the Network Time Protocol (NTP) configuration. In addition, you can issue the **show ntp associations** command to list the time sources that are configured for the device, and you can issue the **show ntp status** command to display detailed synchronization information. However, one of the simplest methods you can use to determine the synchronization status of a device is to issue the **show clock** command. If the clock is synchronized or has been set manually, no symbol will appear before the time, as shown in the following output:

```
00:20:14.301 CST Wed Apr 1 2009
```

If the clock has never been synchronized or has never been set, an asterisk will appear before the time, as shown in the following output:

```
*00:20:14.301 CST Wed Apr 1 2009
```

If the clock is not currently synchronized but had been synchronized in the past, a dot will appear before the time, as shown the following output:

```
.00:20:14.301 CST Wed Apr 1 2009
```

Issuing the **show running-config** command on all of the devise will show that each of the devices from AS1 to R3 is receiving time from a directly connected upstream device. However, R2 is receiving its time from the server at 10.10.11.5. The **ntp server** command configures a Cisco router to be an NTP static client that is synchronized by an NTP server. The syntax of the **ntp server** command is **ntp server** *ip-address*, where *ip-address* is the IP address of the NTP server that the client will use to receive its time. Therefore, removing the **ntp server 10.10.11.5** command will configure R2 to stop receiving time from the server at 10.10.11.5. Issuing the **ntp server 192.168.1.1** command will configure R2 to start reviving time from R1.

You should not issue the **ntp master** command. The **ntp master** command configures a device to act as a master clock source. The syntax of the **ntp master** command is **ntp master** *stratum*, where *stratum* is a value from 1 through 15. A clock source with a lower stratum number is preferred over a clock source with a higher stratum number. You need not issue the **no ntp master** command on any devices, because only R1 is configured as a master clock source.

You cannot issue the **ntp master 192.168.1.1** command, because it contains invalid syntax. The **ntp master** command accepts a stratum number as a keyword; it cannot accept an IP address.

You should not issue the **ntp authentication-key** command or the **ntp trusted-key** command, because none of the Cisco devices are configured to use NTP authentication. To configure a Message Digest 5 (MD5) authentication key for a Cisco device, you would issue the **ntp authentication-key** *number* **md5** *value* command, where *number* is a number from 1 through 4294967295 and *value* an eight-character string that represents the value of the MD5 key. Only MD5 keys are supported by NTP authentication. After defining an authentication key, you would issue the **ntp-trusted key** *key-number* command, where *key-number* is the number of the key defined in the **ntp authentication-key** command.

You should not issue the **clock set** command. The **clock set** command is used to manually configure the time on a Cisco device.

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html#wp1123176

**QUESTION 66**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

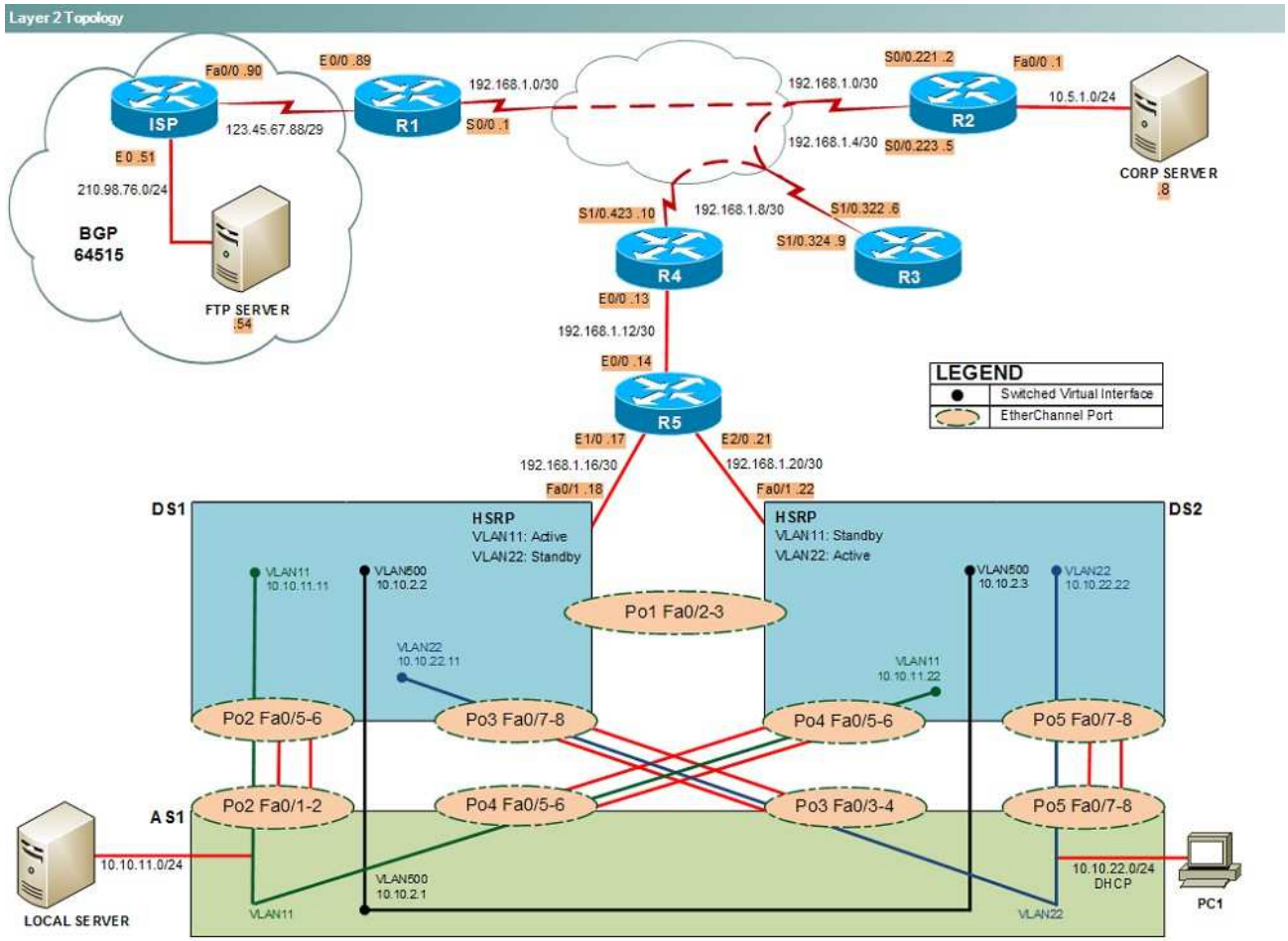
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

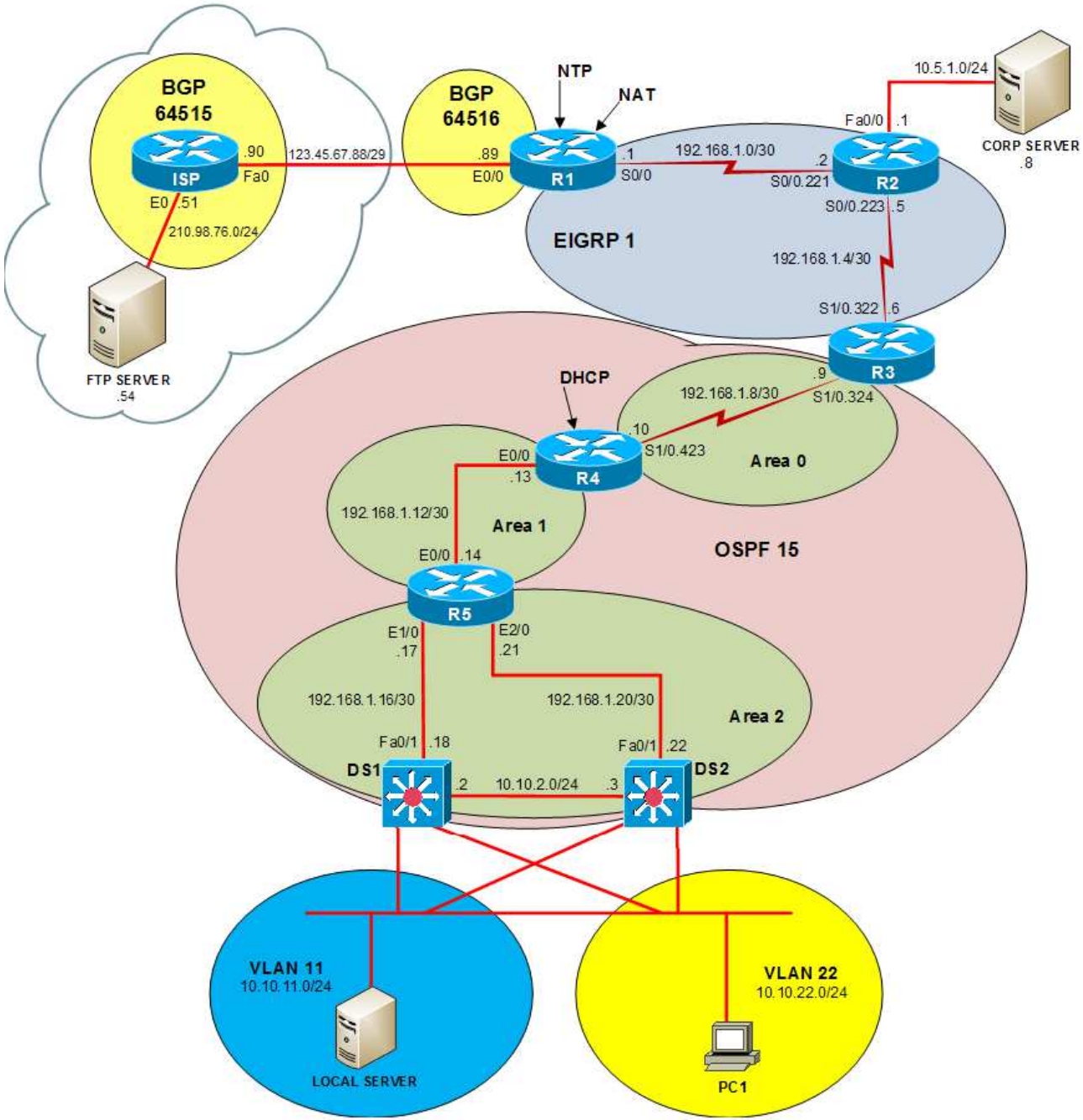
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

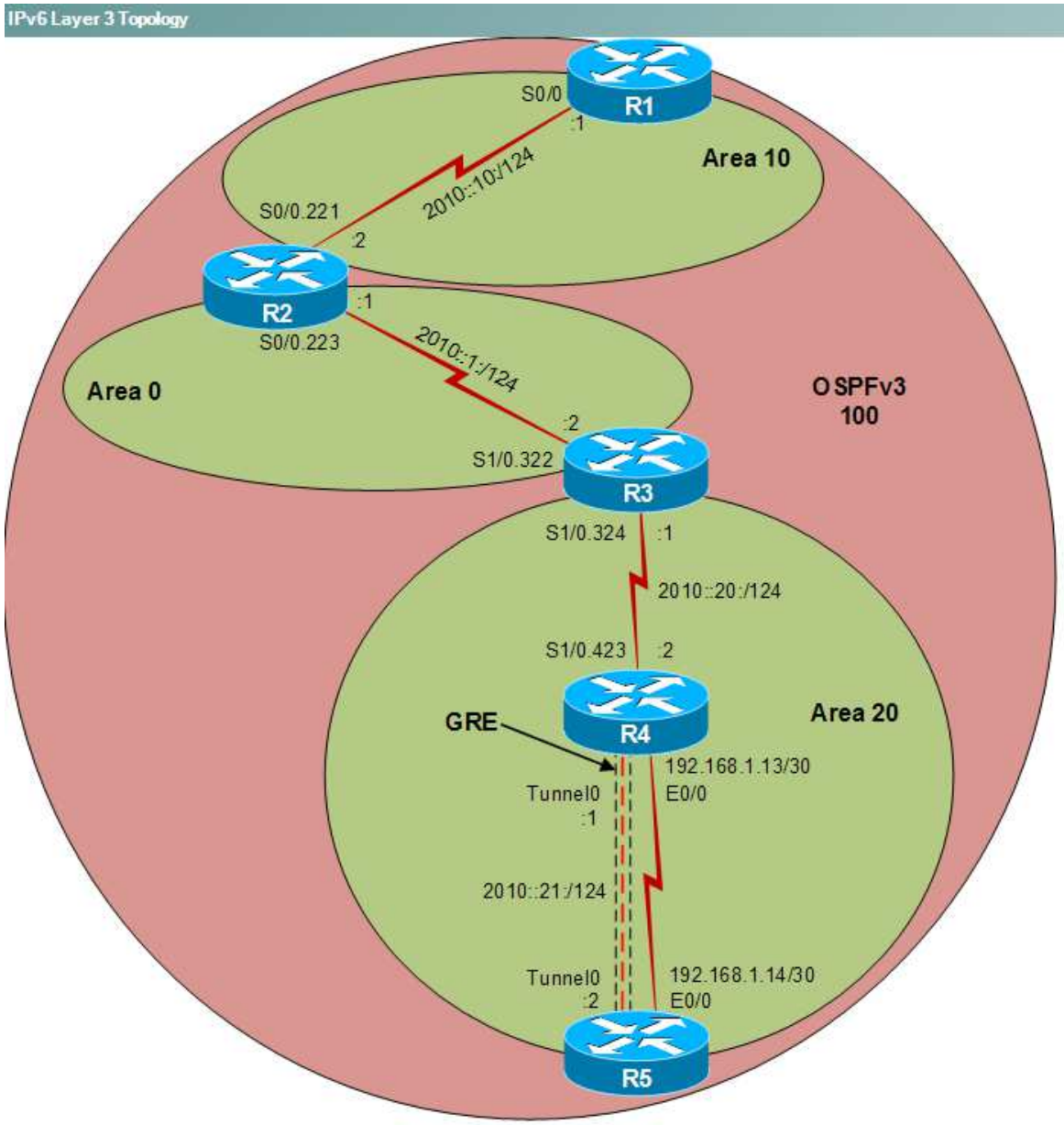
**Layer 2 Topology**




IPv4 layer 3 Topology

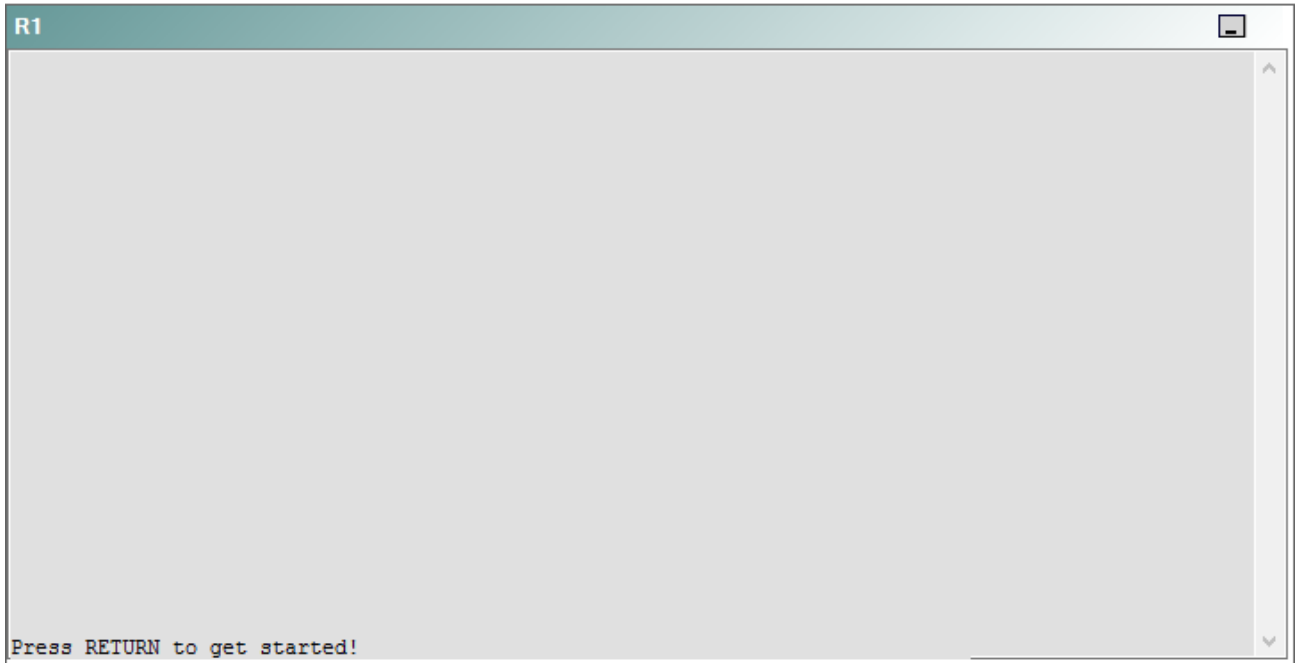

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

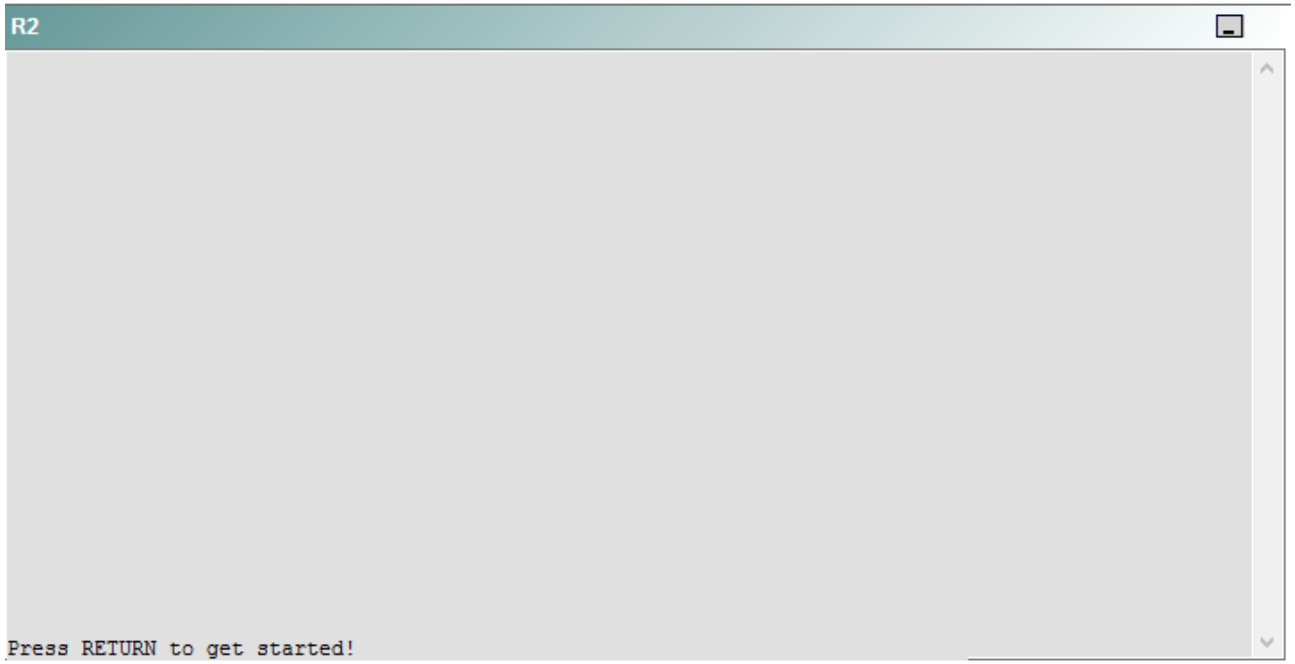



https://www.gratisexam.com/

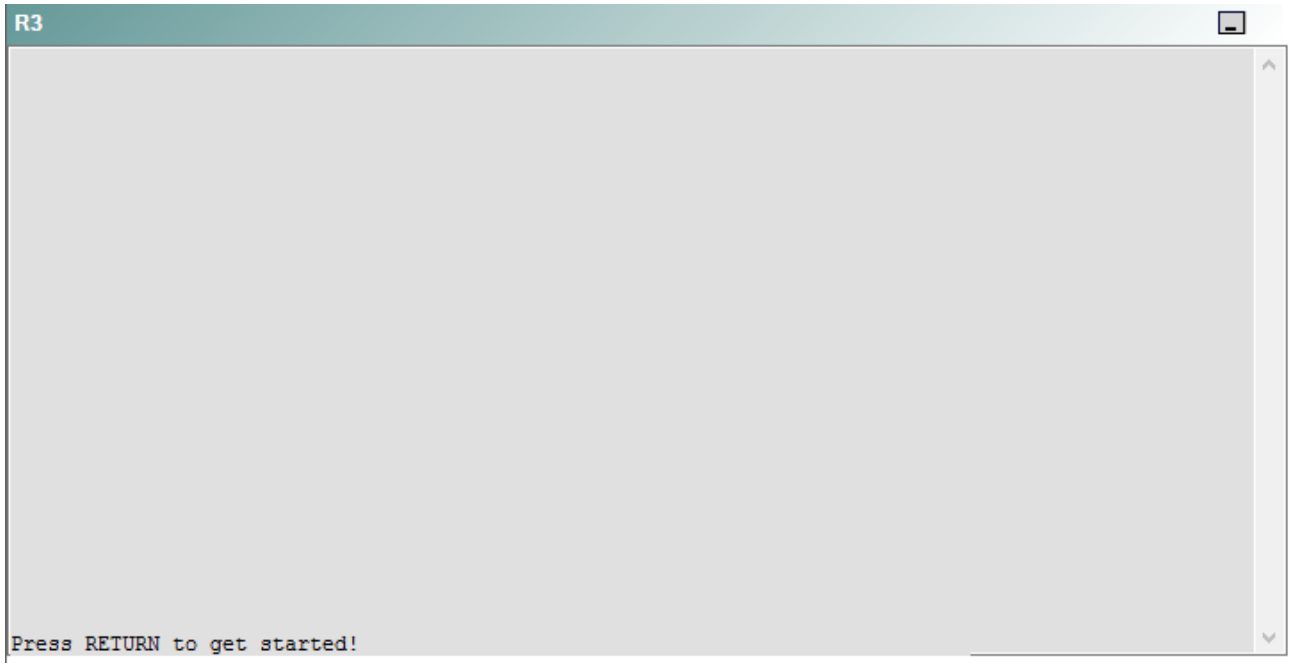
R1



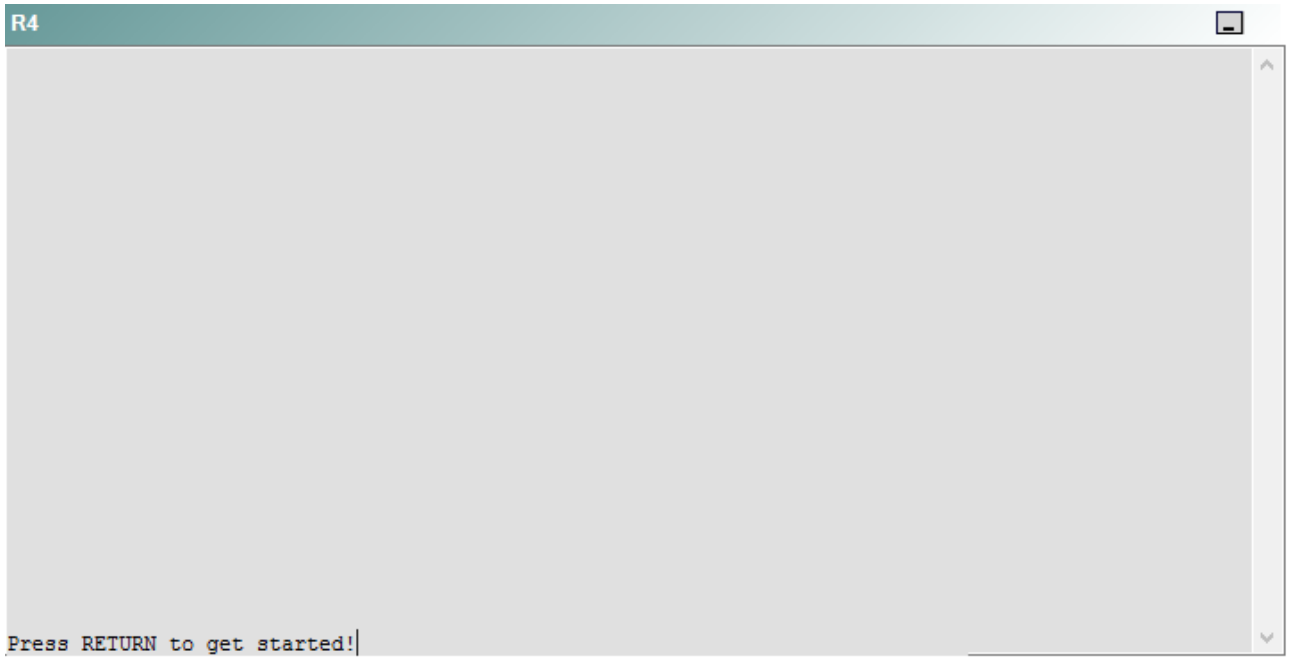

R2



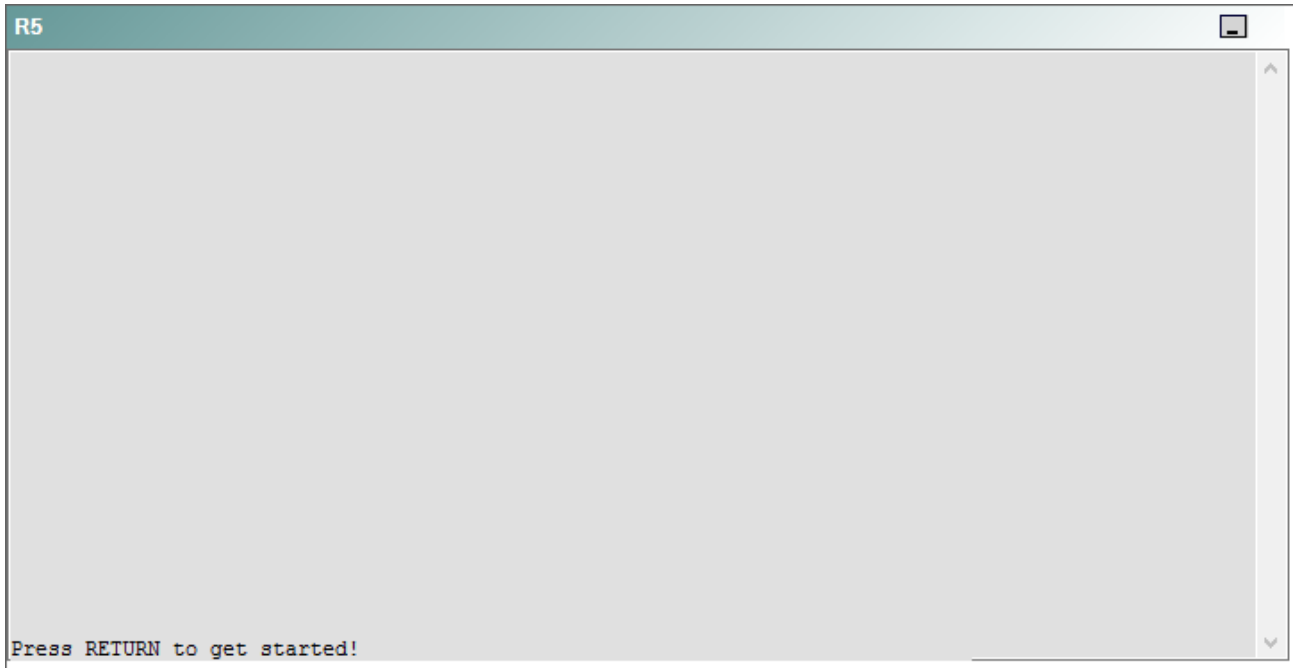

R3



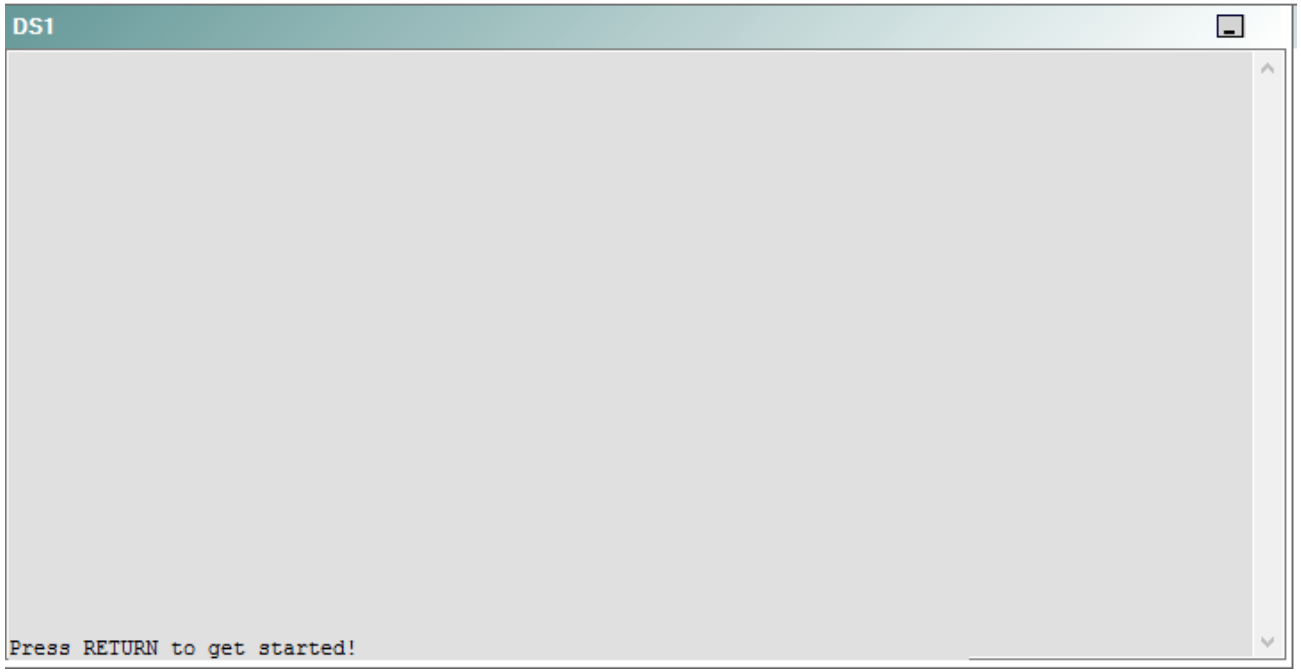

R4



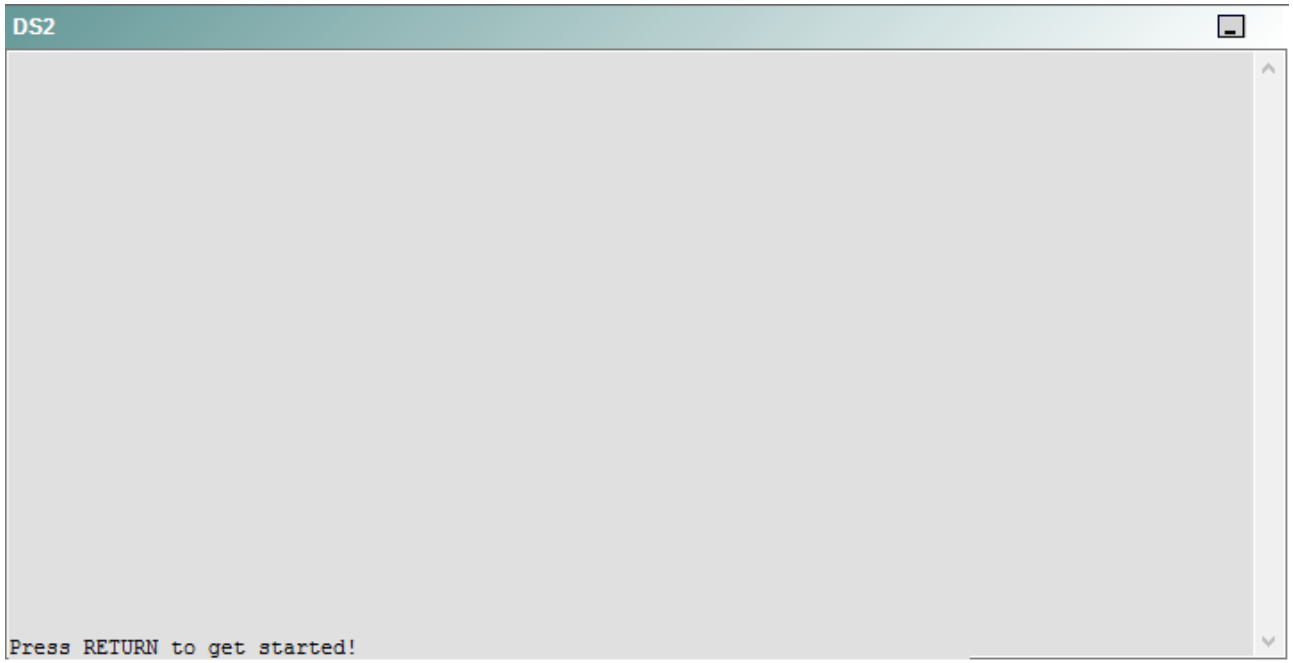

R5



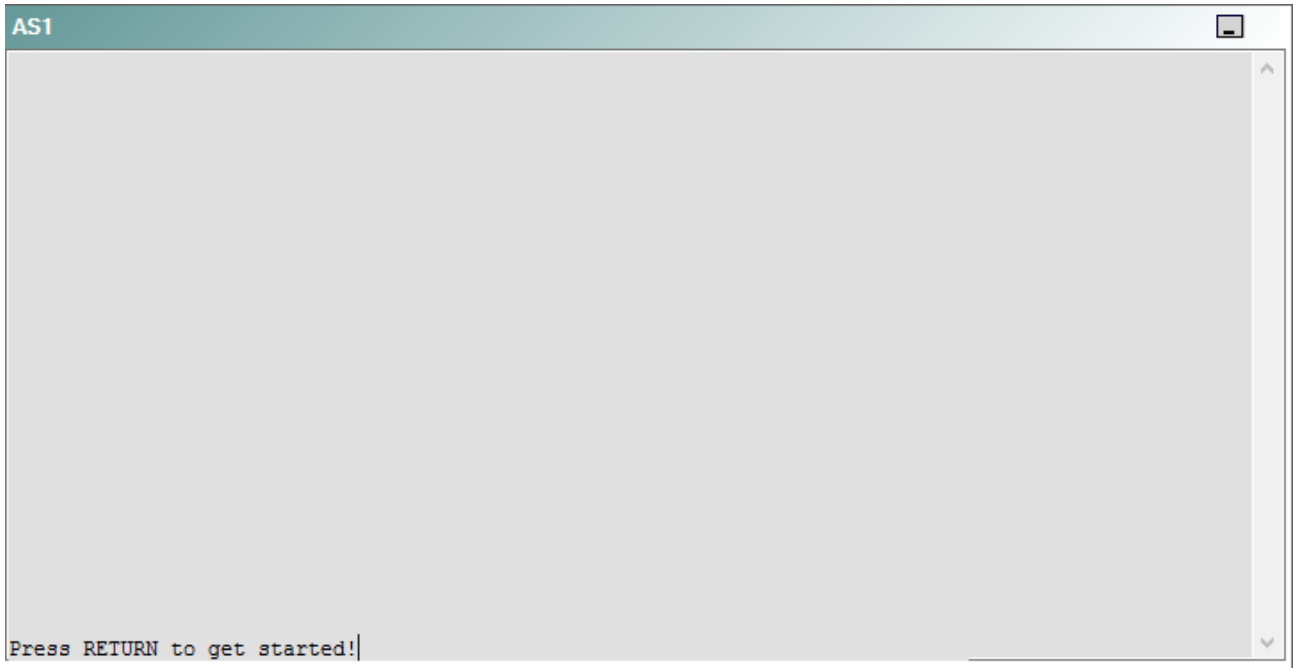

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 67**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

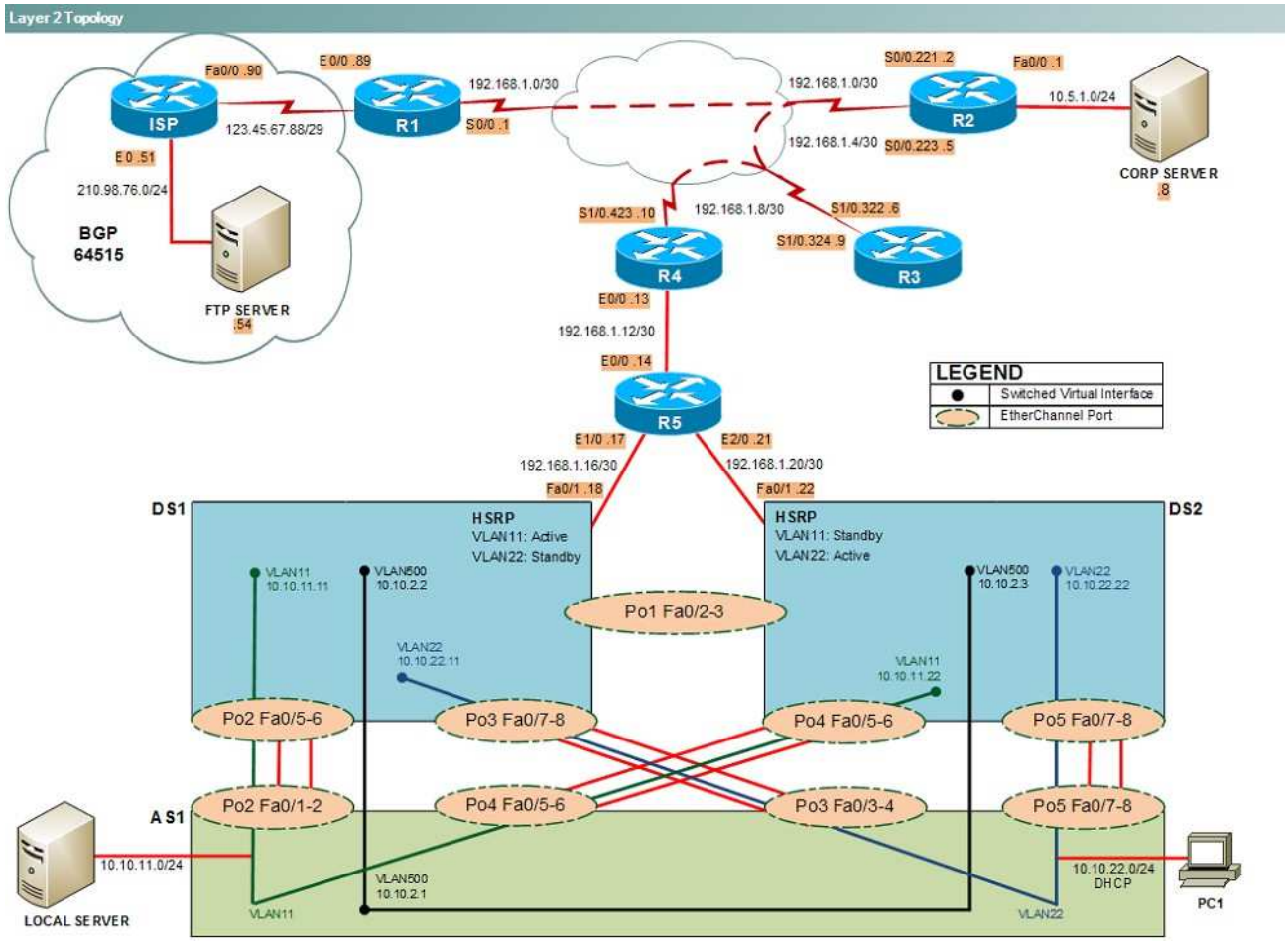
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

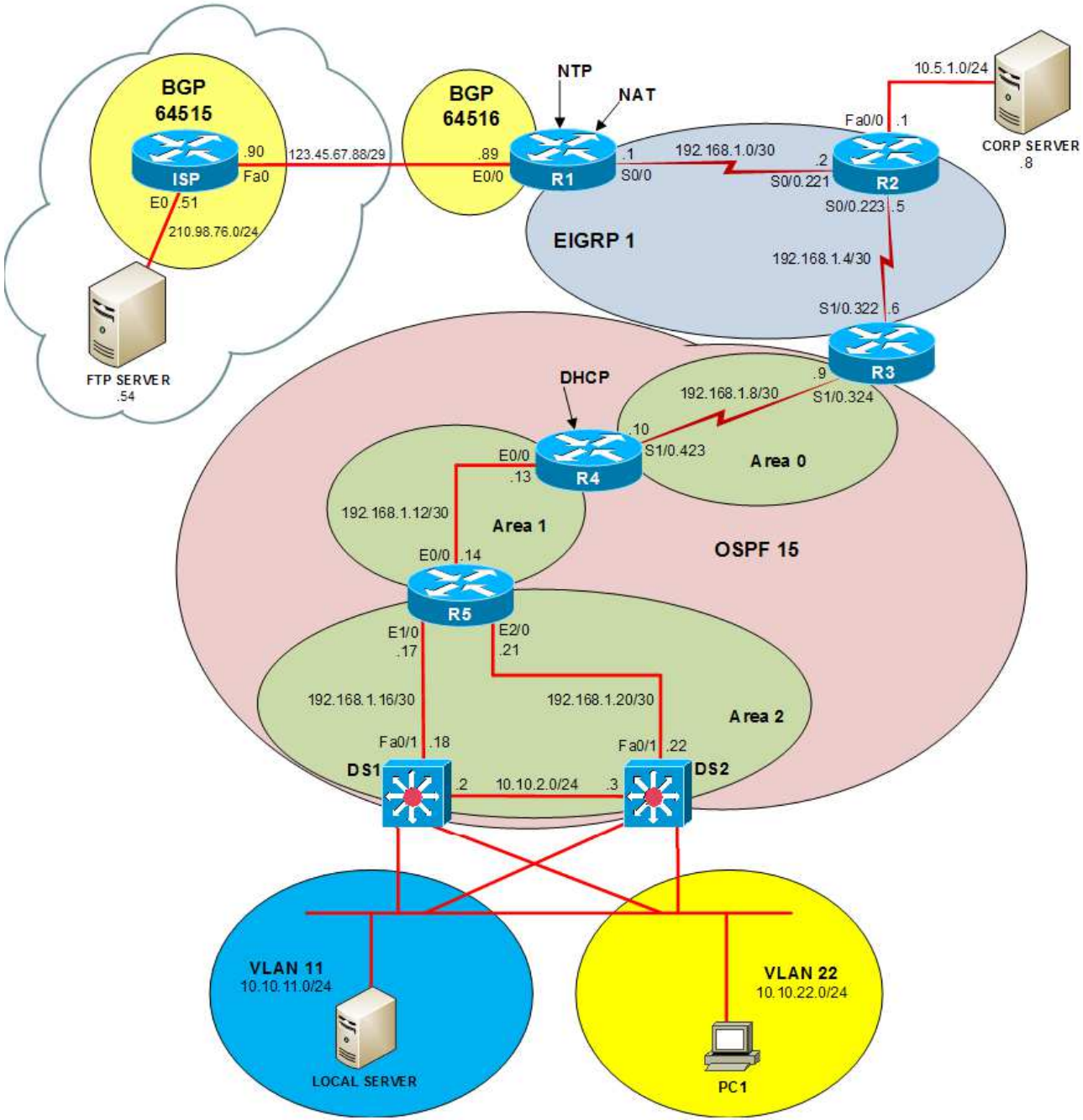
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

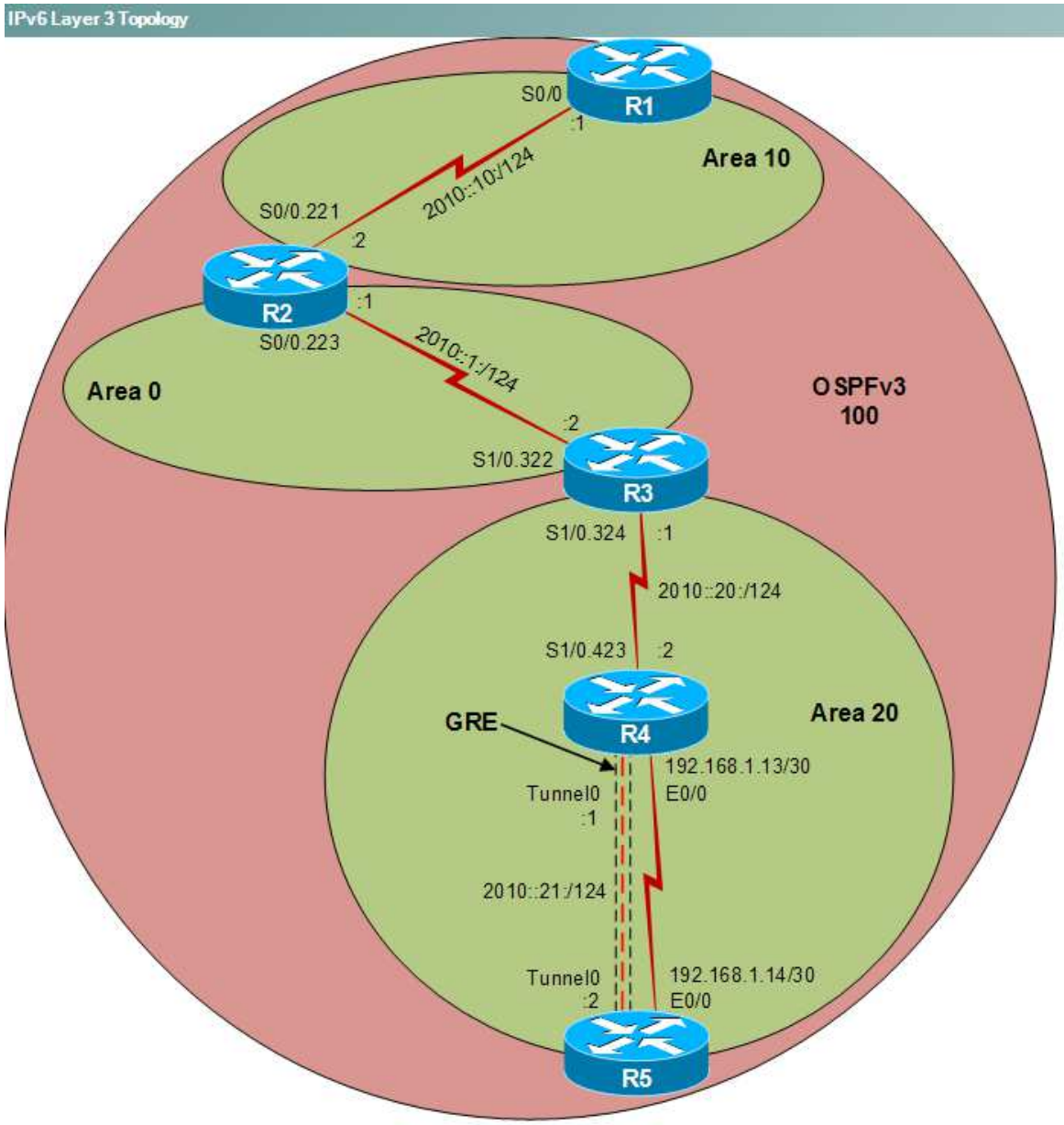
**Layer 2 Topology**




IPv4 layer 3 Topology

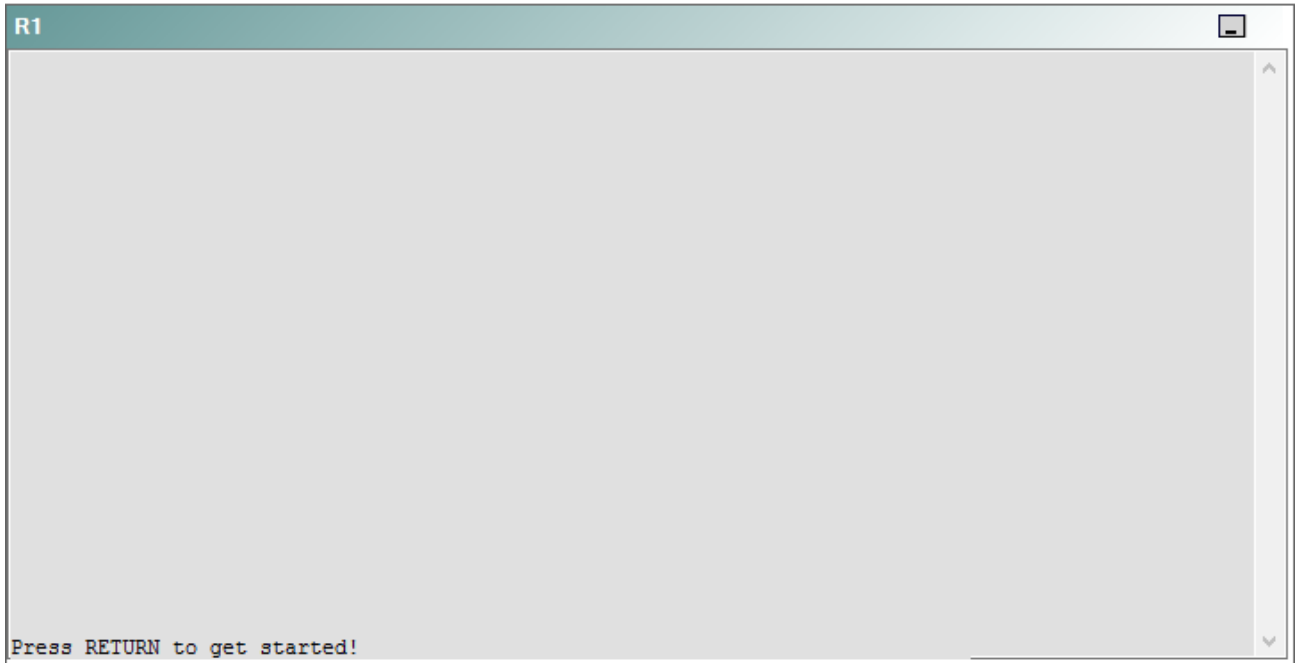

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

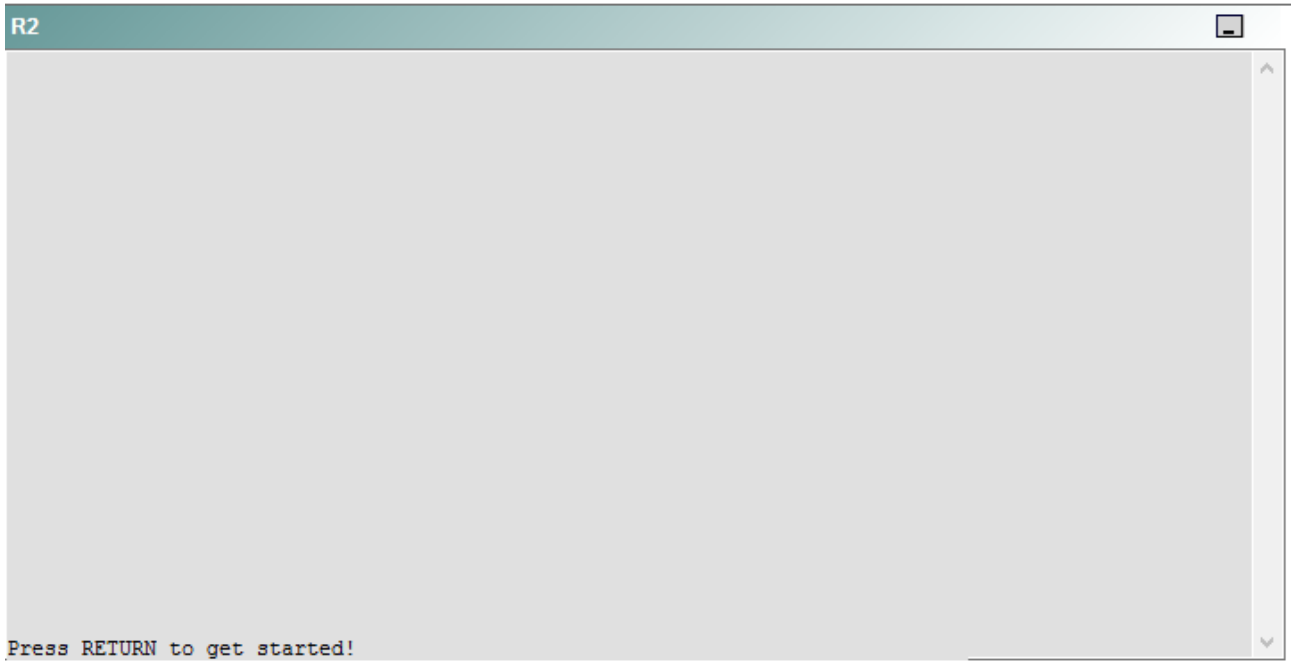



https://www.gratisexam.com/

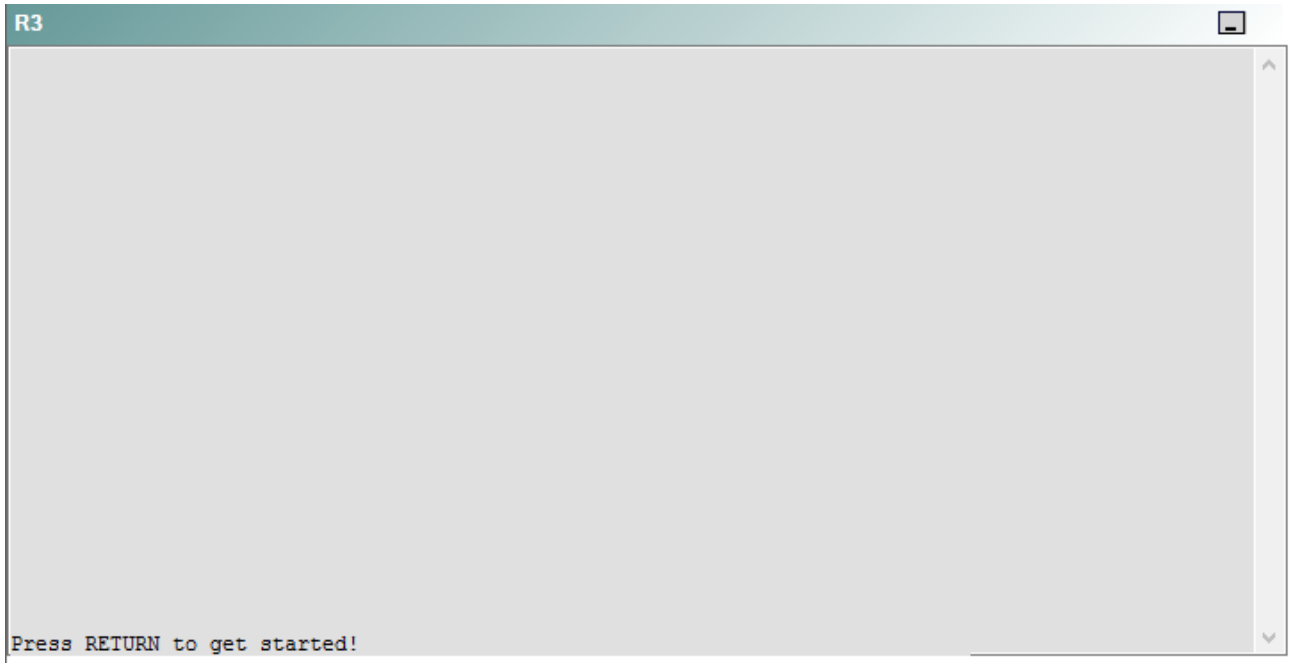
R1



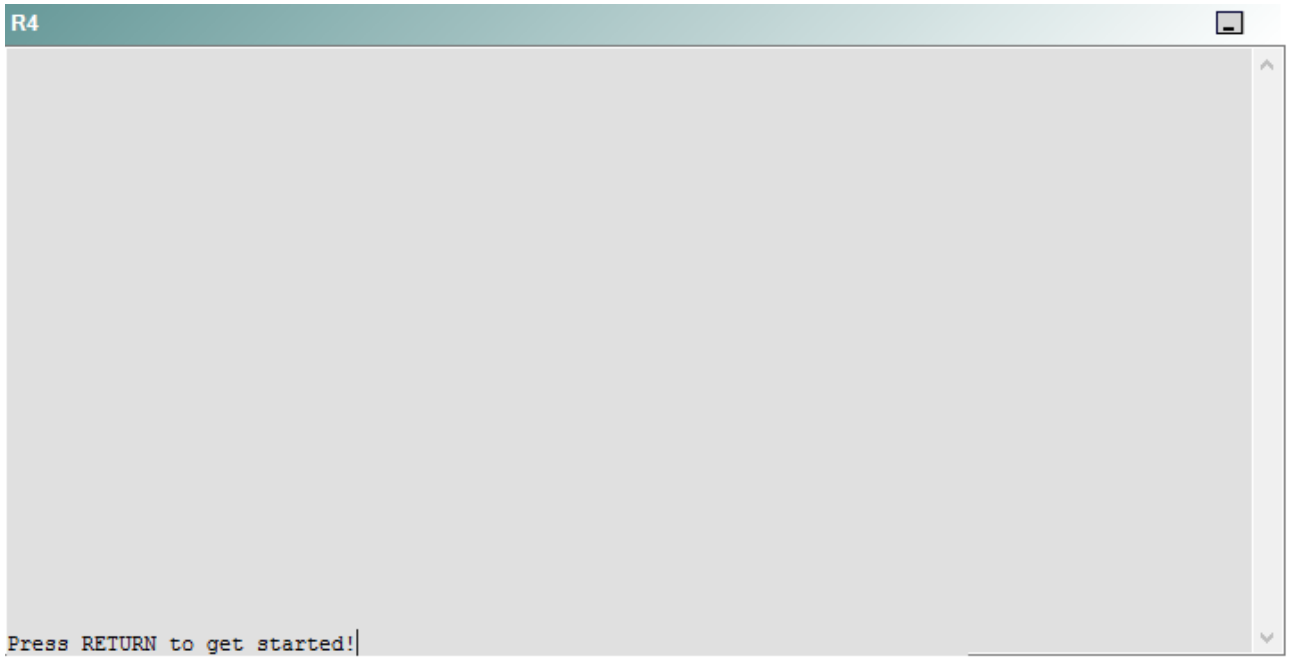

R2



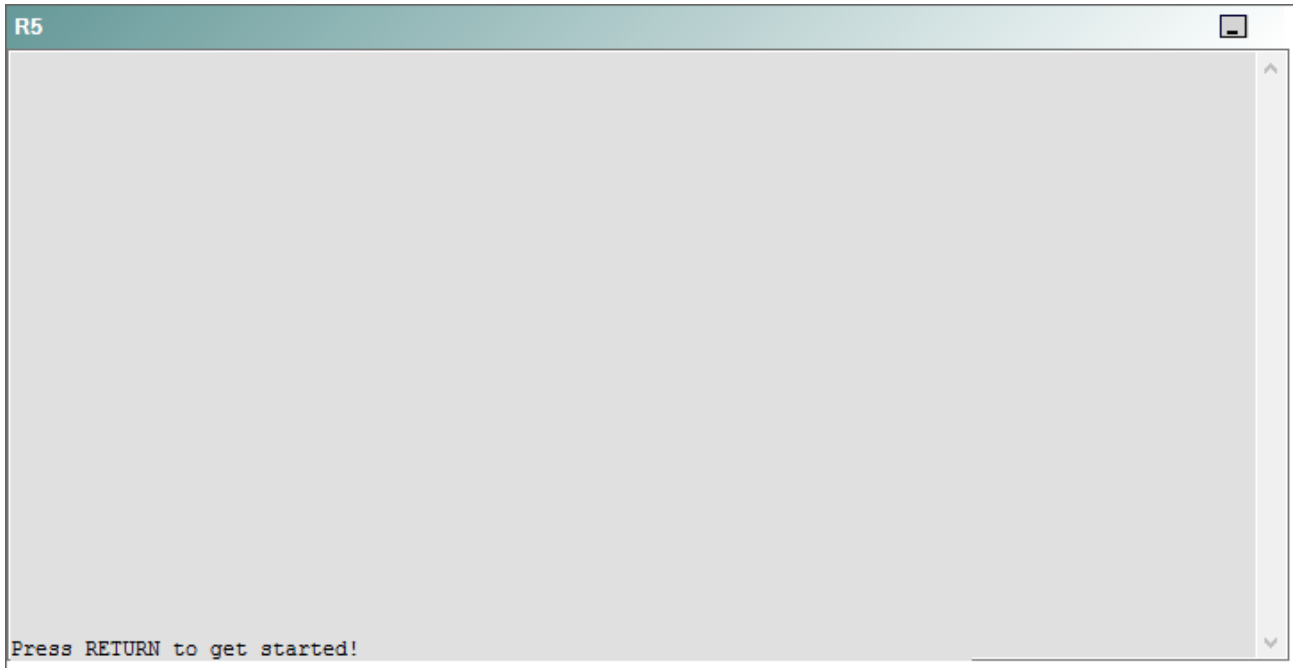

R3



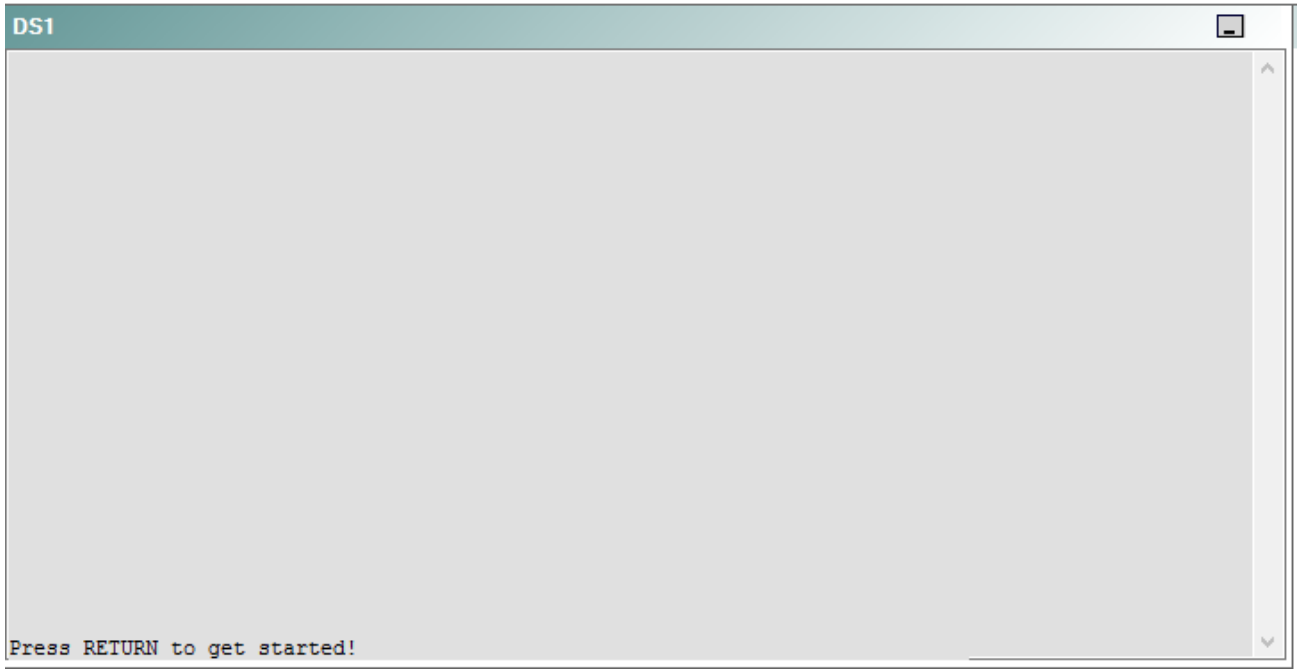

R4



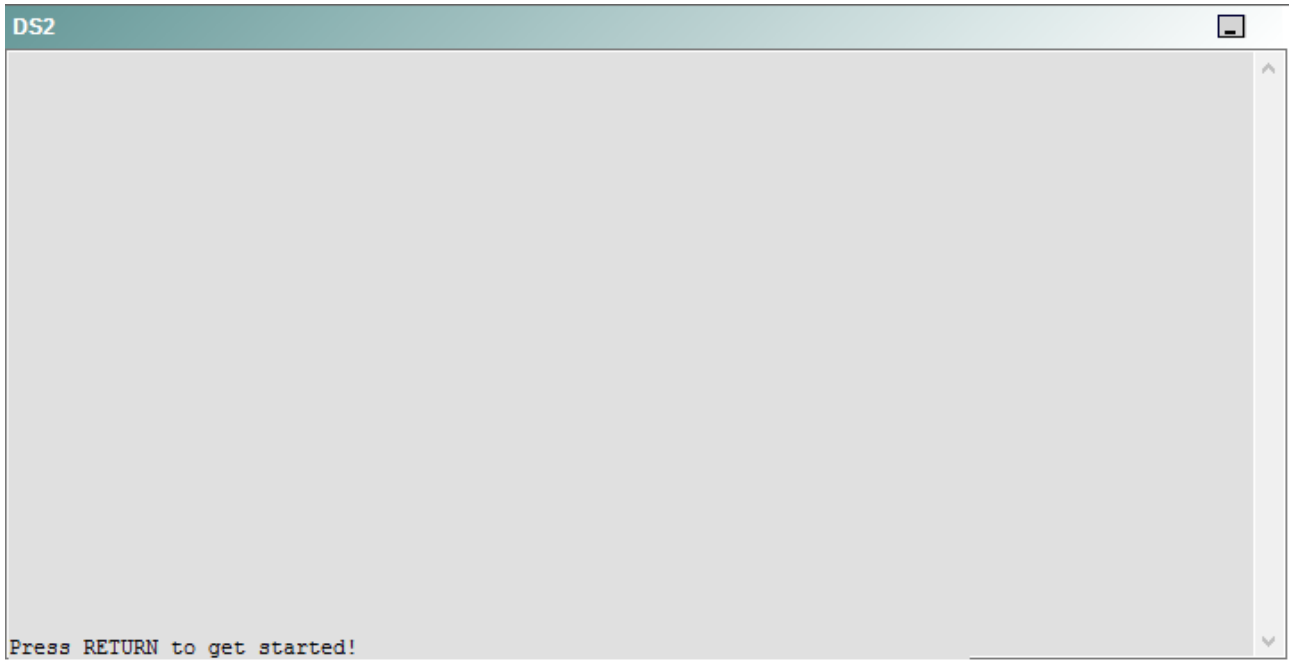

R5



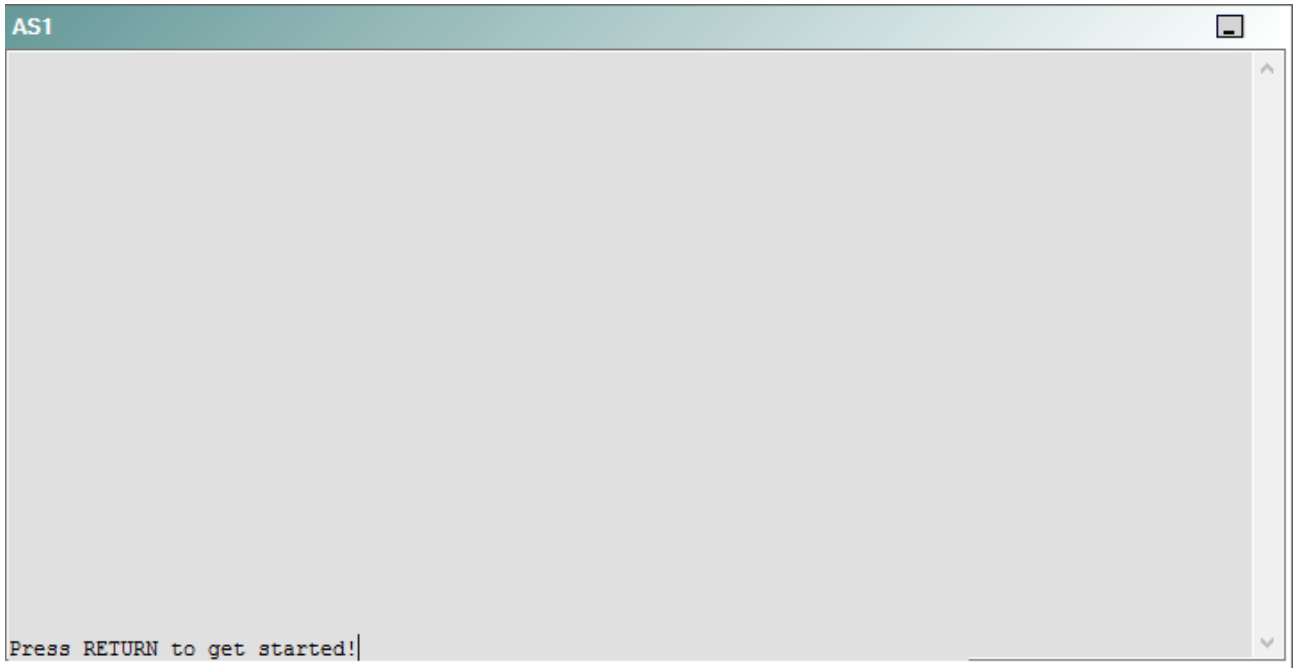

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. NAT
C. Layer 3 addressing
D. Layer 3 security
E. Layer 2 security
F. EIGRP
G. BGP
H. OSPFv3
I. interface

**Correct Answer:** F

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 68**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

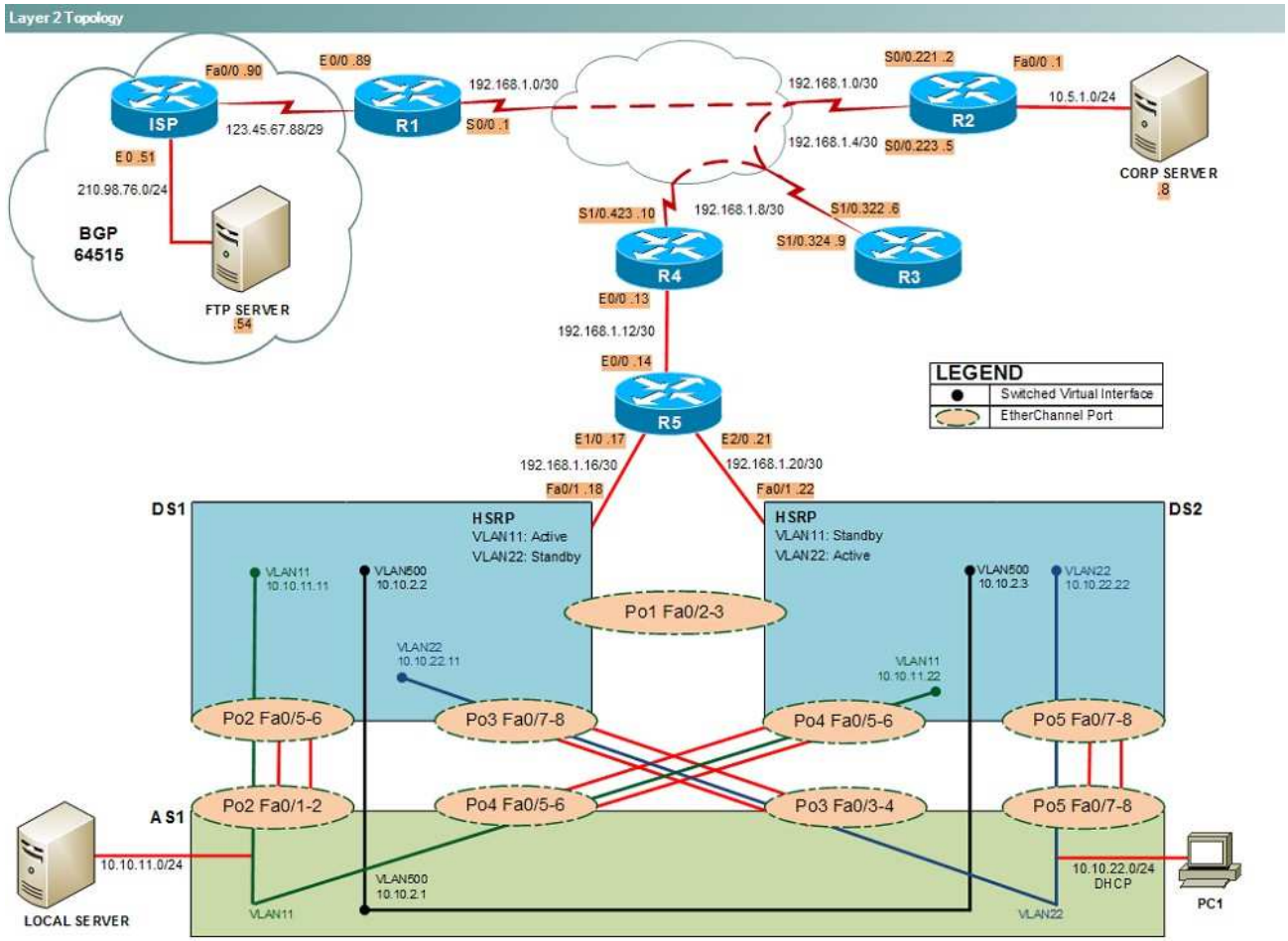
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

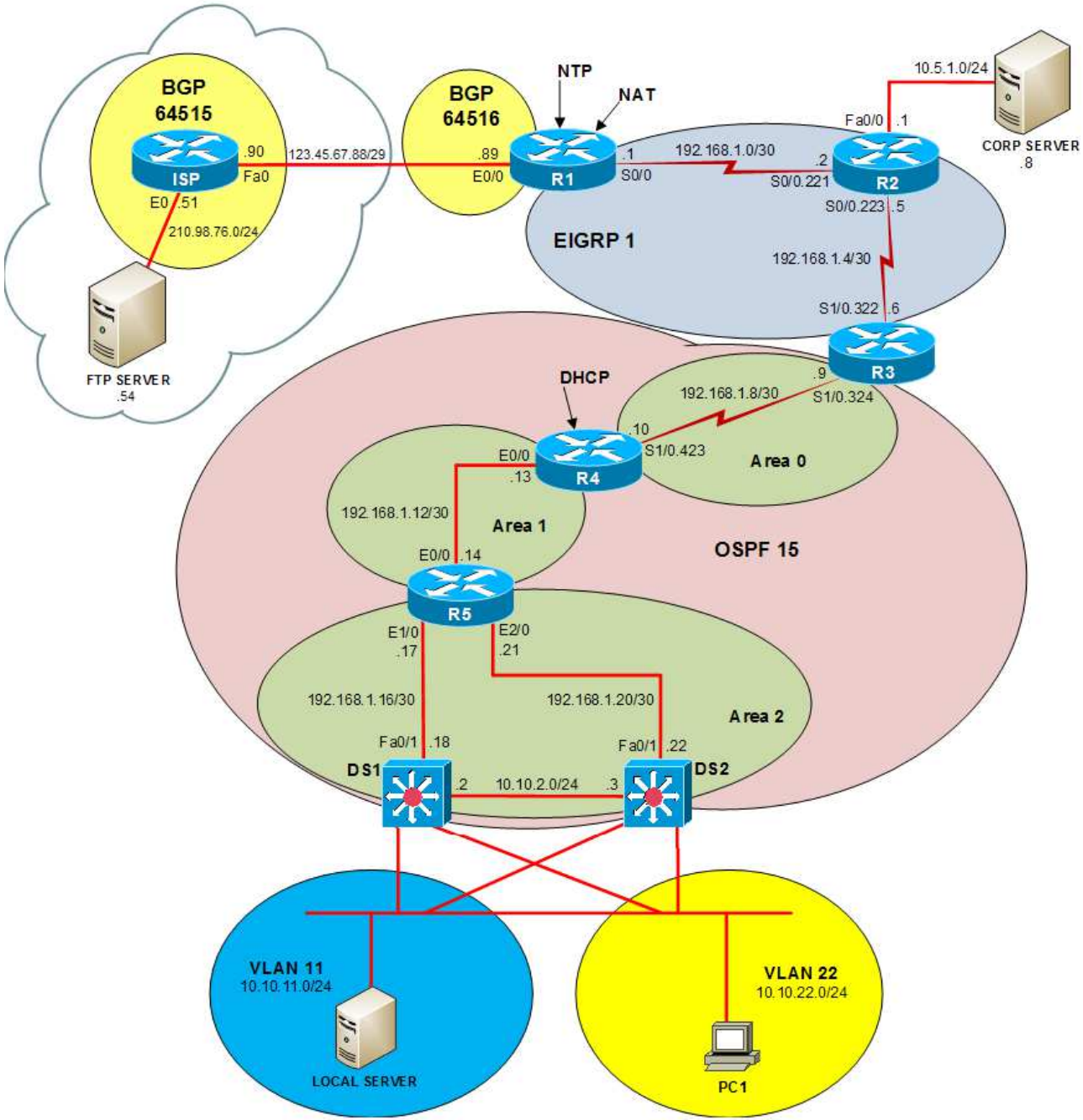
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

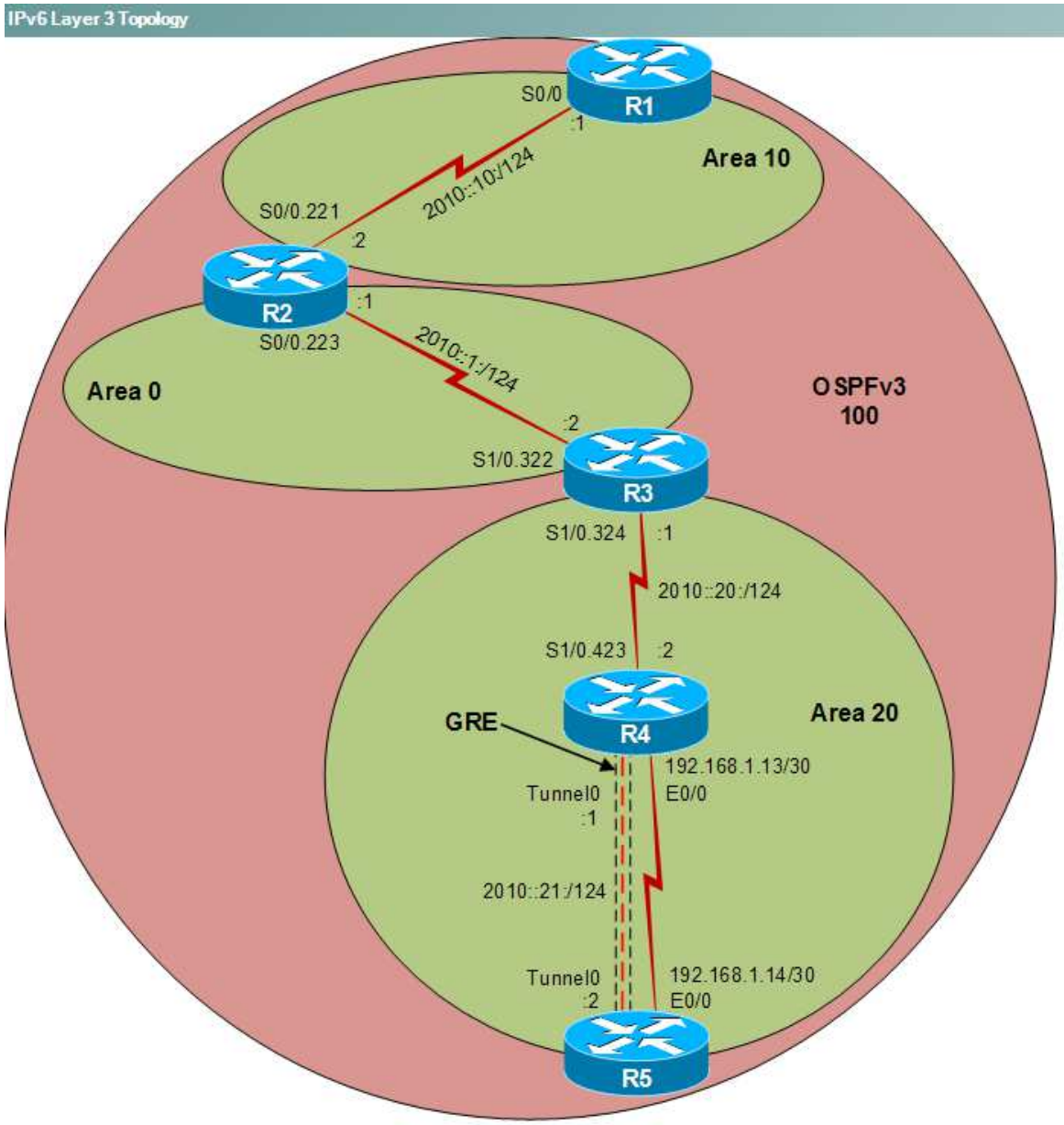
**Layer 2 Topology**




IPv4 layer 3 Topology

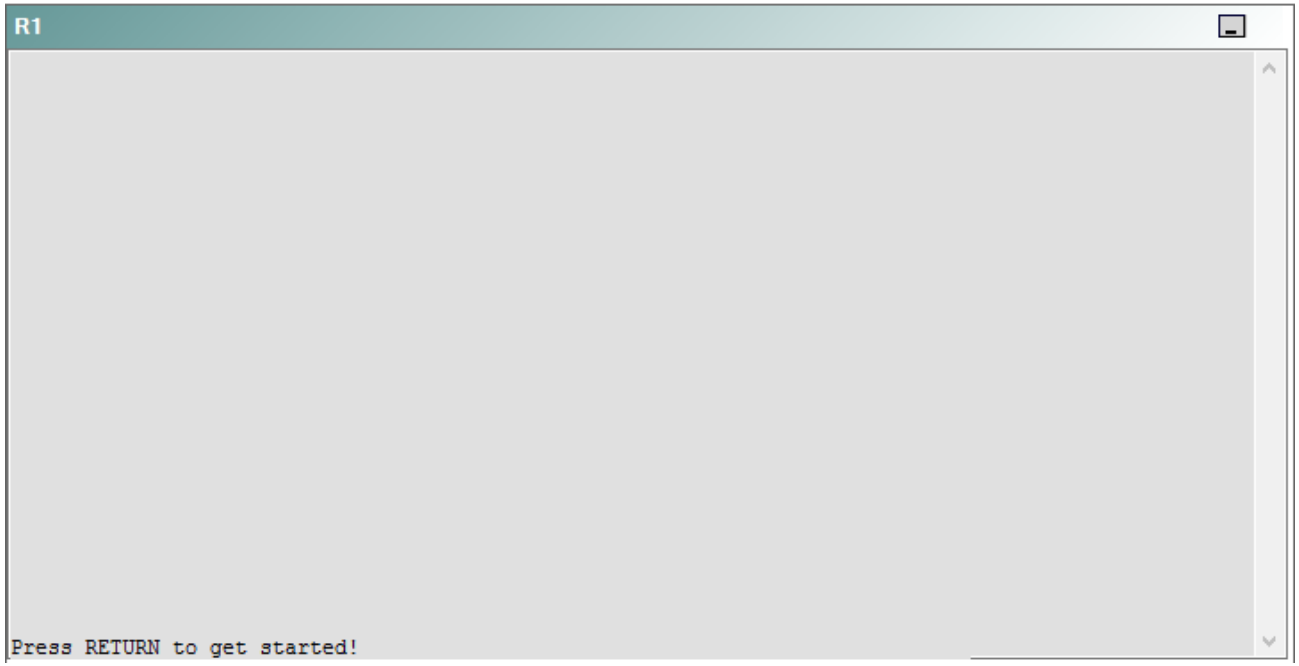

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

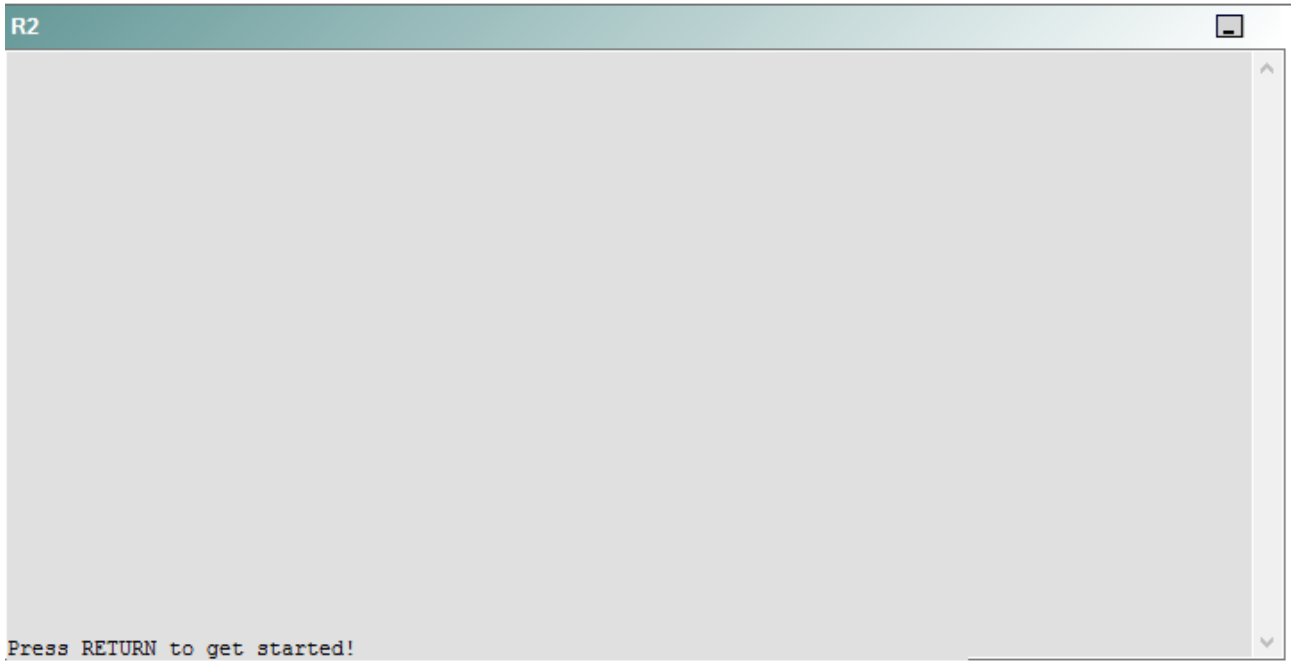



https://www.gratisexam.com/

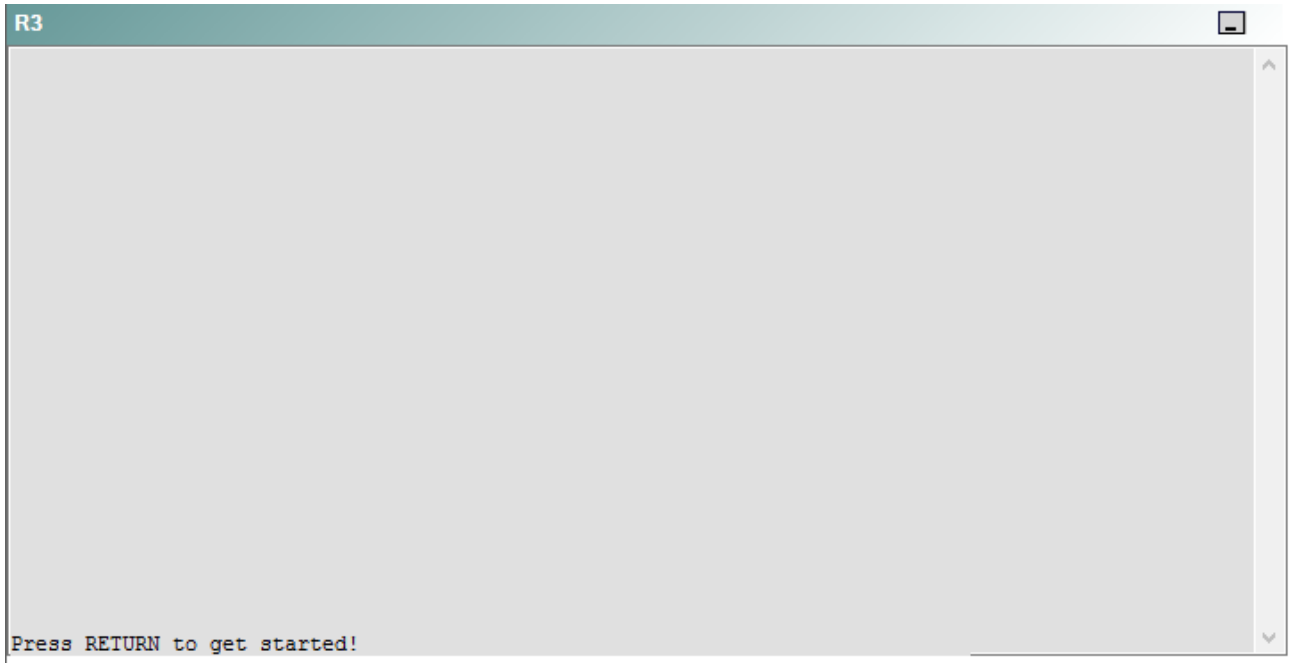
R1



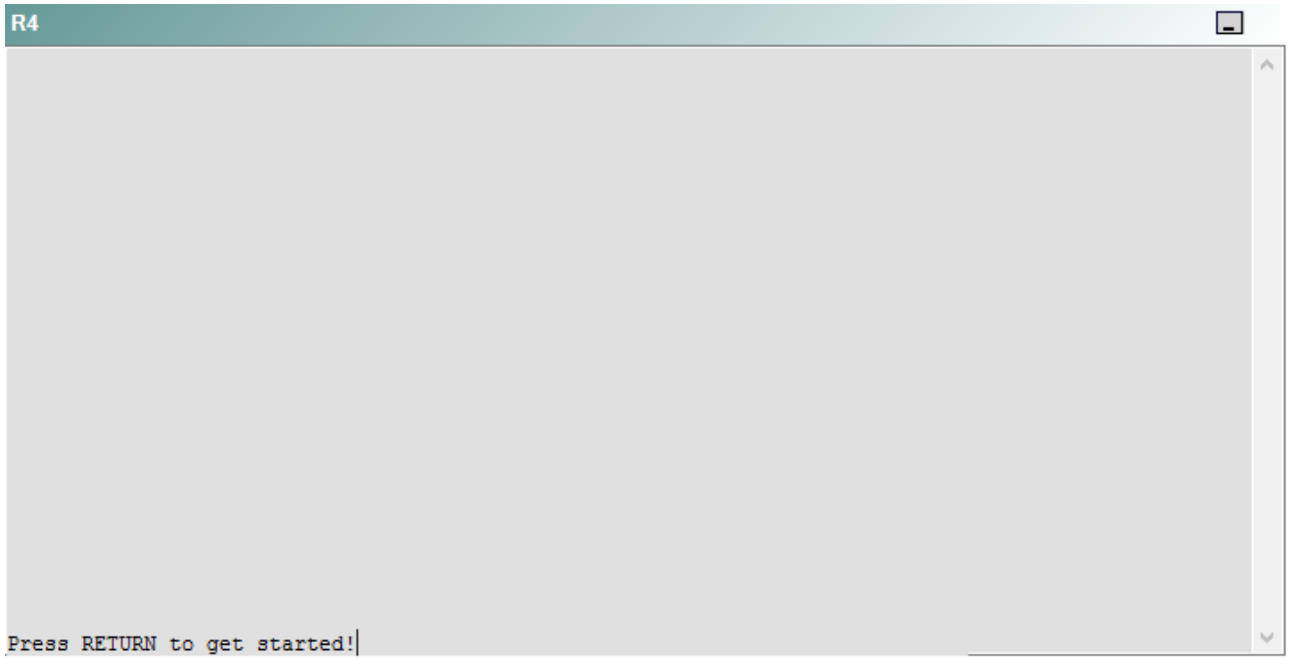

R2



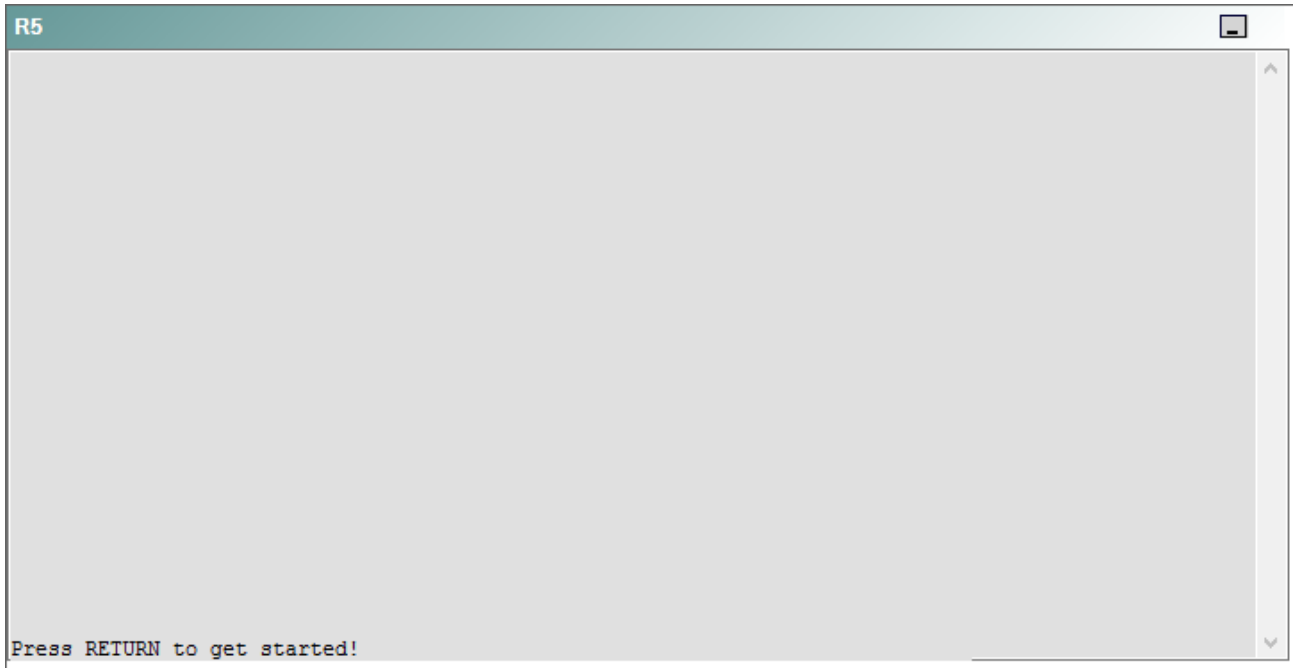

R3



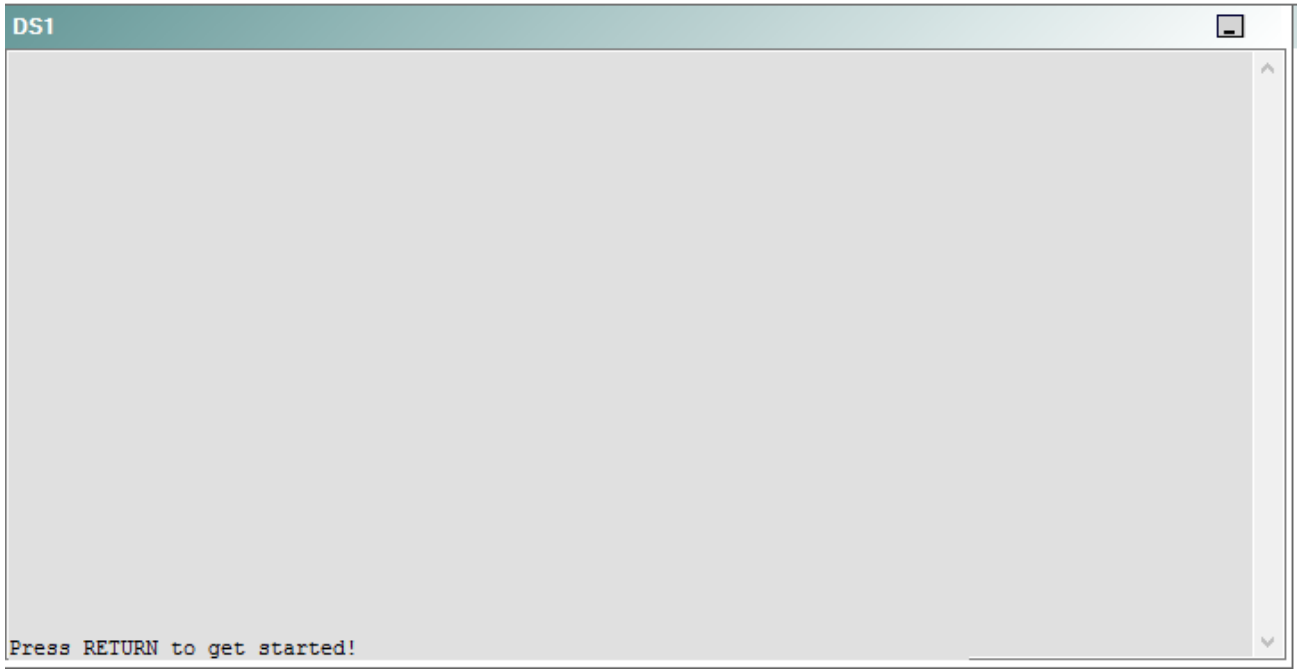

R4



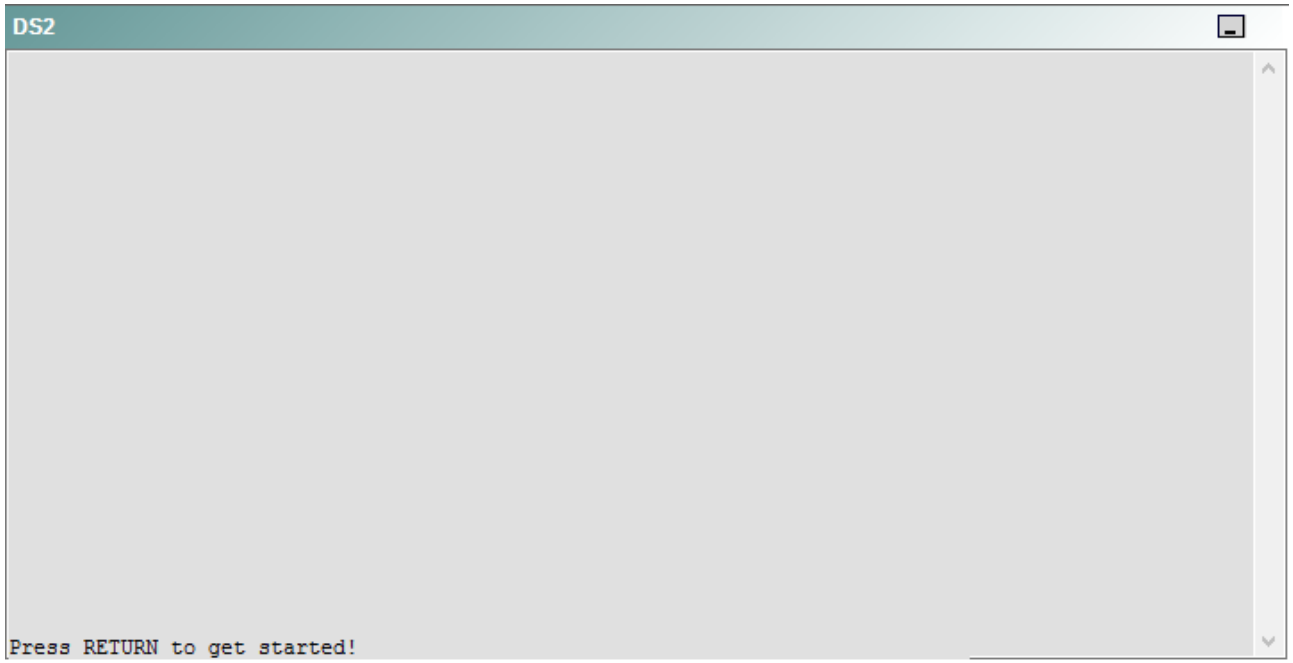

R5



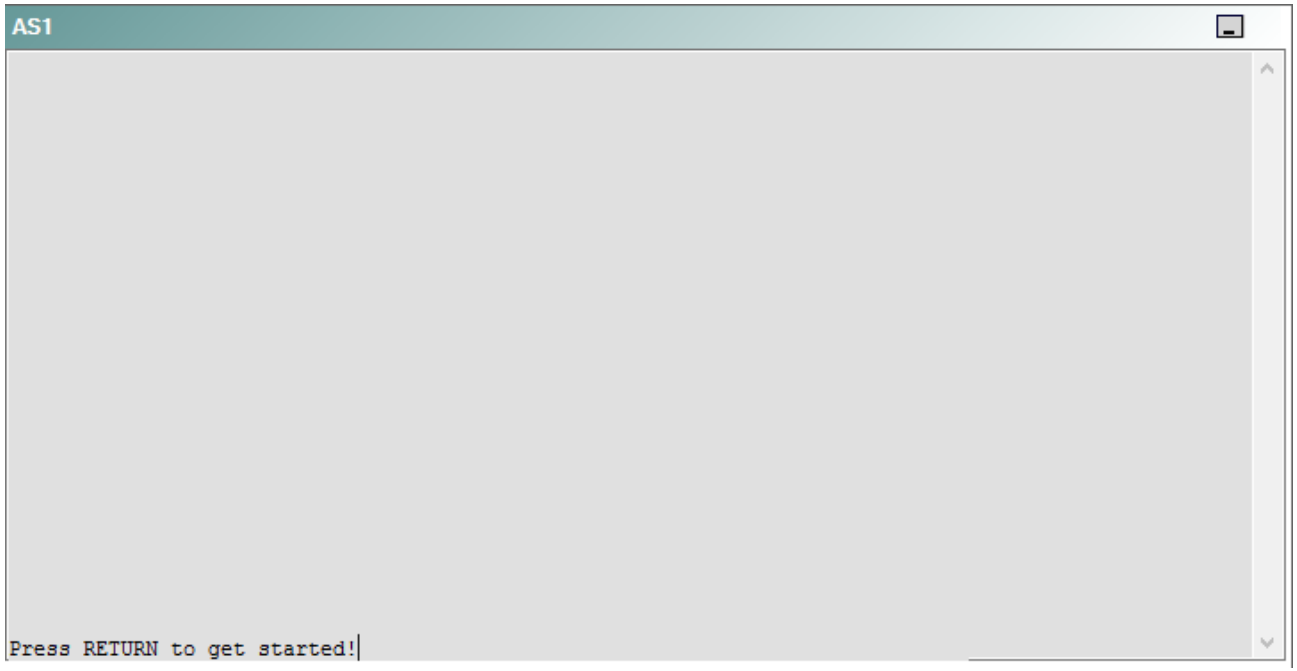

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. changing the EIGRP AS number to AS 10
B. issuing the **metric weights 0 0 1 1 0 0** command
C. issuing the **metric weights 0 1 0 1 0 0** command
D. changing the automatic summarization settings
E. issuing the **passive-interface S1/0.322** command
F. changing the EIGRP hello interval
G. issuing the **ip address 192.168.1.1 255.255.255.252** command for the S0/0 interface
H. issuing the **network 192.168.1.8 0.0.0.3** command
I. issuing the **network 192.168.1.0 255.255.255.252** command

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

You should issue the **metric weights 0 1 0 1 0 0** command on R1. To determine which device is the source of the problem, you can issue the **ping and traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from PC1 to the closest device and work your way up the network until communication is lost, or you can ping from PC1 to the farthest device and work your way back to PC1 until pings are successful.

Pings from PC1 to the S0/0.221 interface of R2 are successful. However, pings from PC1 to the S0/0 interface of R1 time out and fail. Pings from R1 to the S0/0.221 interface of R2 are successful, but pings from R1 to the S0/0.223 interface of R2 are not. Therefore, the problem key exists on R1 or R2.

Once you have determined where connectivity is lost, you can begin to troubleshoot what is causing the problem. Issuing the **show ip eigrp neighbors** command on R1 reveals the absence of Enhanced Interior Gateway Routing Protocol (EIGRP) routes, and issuing the **show ip eigrp neighbors** command on R1 confirms the absence of EIGRP neighbors. The following parameters must match for devices to establish an EIGRP neighbor relationship:

- K values
- Autonomous system (AS) numbers
- Subnet

In addition, EIGRP cannot establish an adjacency over a secondary IP address.

K values are used to calculate the metric used by EIGRP. By default, EIGRP uses K1, which is related to bandwidth, and K3, which is related to delay, to calculate the metric. The K2 value, which is set to 0 by default, can be set to a nonzero value so that load is used in metric calculations. The K4 and K5 values, which are set to 0 by default, can be set to nonzero values so that reliability is used in metric calculations. Cisco recommends leaving the K values at their default settings. If K values are changed, they must be changed throughout the network.

You can verify whether K values match by issuing the **show ip protocols** command. Issuing the **show ip protocols** command on R1 will display the following partial output:

```
EIGRP metric weight K1=1, K2=1, K3=1, K4=0, K5=0
```

Issuing the **show ip protocols** command on R2 and R3 will display the following partial output:

```
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
```

Therefore, R1 is not establishing a neighbor relationship with R2, because R2 and R3 are using the default K values and R1 is using modified K values. Issuing the **metric weights 0 1 0 1 0 0** command in router configuration mode on R1 will configure R1 so that it matches R2 and R3. The syntax of the **metric weights**

command is **metric weights** *tos k1 k2 k3 k4 k5*, where *tos* is the type of service (ToS) value, which should always be set to 0.

You should not issue the **metric weights 0 0 1 1 0 0** command on any of the EIGRP routers. Issuing the **metric weights 0 0 1 1 0 0** command would set K1 to a value of 0, K2 to a value of 1, and K3 to a value of 1.

You should not issue the **metric weights 0 1 1 1 0 0** command on R2. Although issuing the **metric weights 0 1 1 1 0 0** command on R2 would enable R1 and R2 to establish a neighbor relationship, it would break the neighbor relationship between R2 and R3.

You need not change the EIGRP AS values on any of the routers, because all of the AS values are set to 1. The AS number is established when the EIGRP process is started by issuing the **router eigrp** *as-number* command. If a router receives a hello packet that contains the same AS number as the AS number that is configured on the router, a neighbor relationship is established. If the AS values are different, the router ignores the packet and a neighbor relationship is not established.

You need not change the EIGRP hello interval on any of the routers. The hello interval does not need to match for routers to establish an EIGRP neighbor adjacency. To modify the EIGRP hello interval, you would issue the **ip hello-interval eigrp** *as-number seconds* command in interface configuration mode. By default, the EIGRP hello interval is set to a value of 60 seconds for nonbroadcast multiaccess (NBMA) networks at 1.544 Mbps and slower and to a value of 5 seconds for all other networks.

You need not change the EIGRP hold timer on any of the routers. The hold timer does not need to match for routers to establish an EIGRP neighbor adjacency. To adjust the EIGRP hold timer, you would issue the **ip hold-time eigrp** *as-number seconds* command in interface configuration mode. The EIGRP hold timer should be set to three times the hello interval. Therefore, the hold timer is typically set to 15 seconds on high-bandwidth links and 180 seconds on low-bandwidth NBMA links by default.

You need not issue the **network 192.168.1.0 0.0.0.3** command on R1, because this command has already been issued. Additionally, you should not issue the **network 192.168.1.0 255.255.255.252** command on R1, because the network command uses wildcard masks, not subnet masks. A wildcard mask is basically an inverse subnet mask. To calculate the appropriate wildcard mask, you should subtract the subnet mask from 255.255.255.255. For example, the 192.168.1.0 network has a /30 subnet mask, which is 255.255.255.252. Subtracting 255.255.255.252 from 255.255.255.255 yields a wildcard mask of 0.0.0.3.

You need not issue the **no passive-interface S0/0** command on R1, because the S0/0 interface of R1 is not configured as a passive interface. Configuring an interface as a passive interface blocks EIGRP and Open Shortest Path First (OSPF) hello packets, which prevents the interface from sending or receiving routing updates. Issuing the **passive-interface** *interface* command configures a single interface as a passive interface. Issuing the **passive-interface default** command configures all interface to be passive interfaces except those that are specified within **no passive-interface** *interface* commands.

You need not modify automatic summarization setting on any of the routers. The summarization settings currently configures on the routers are not preventing PC1 from reaching the external server at 210.98.76.54.

Reference:

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#eigrpmetrics

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/21324-trouble-eigrp.html

**QUESTION 69**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

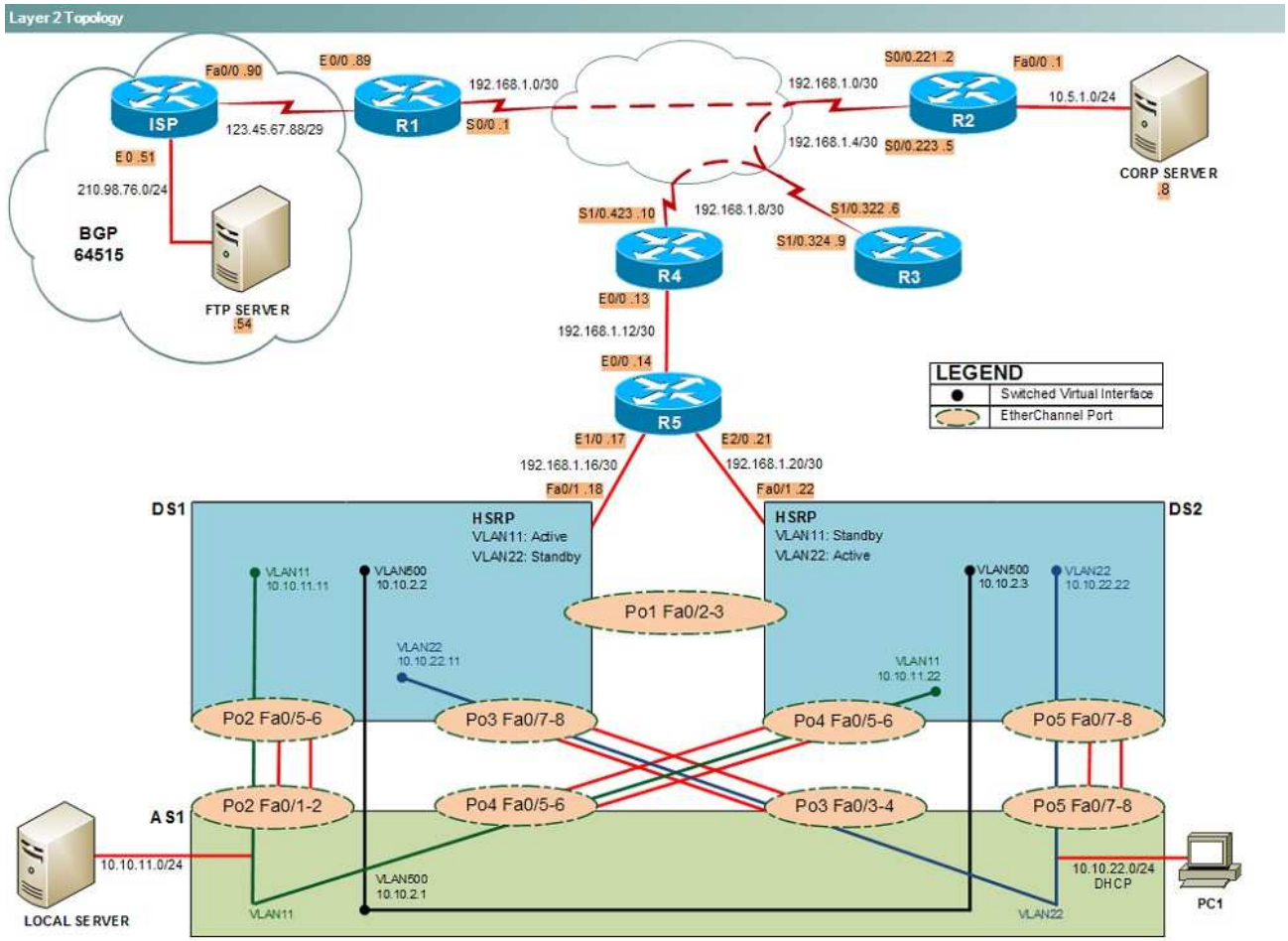
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

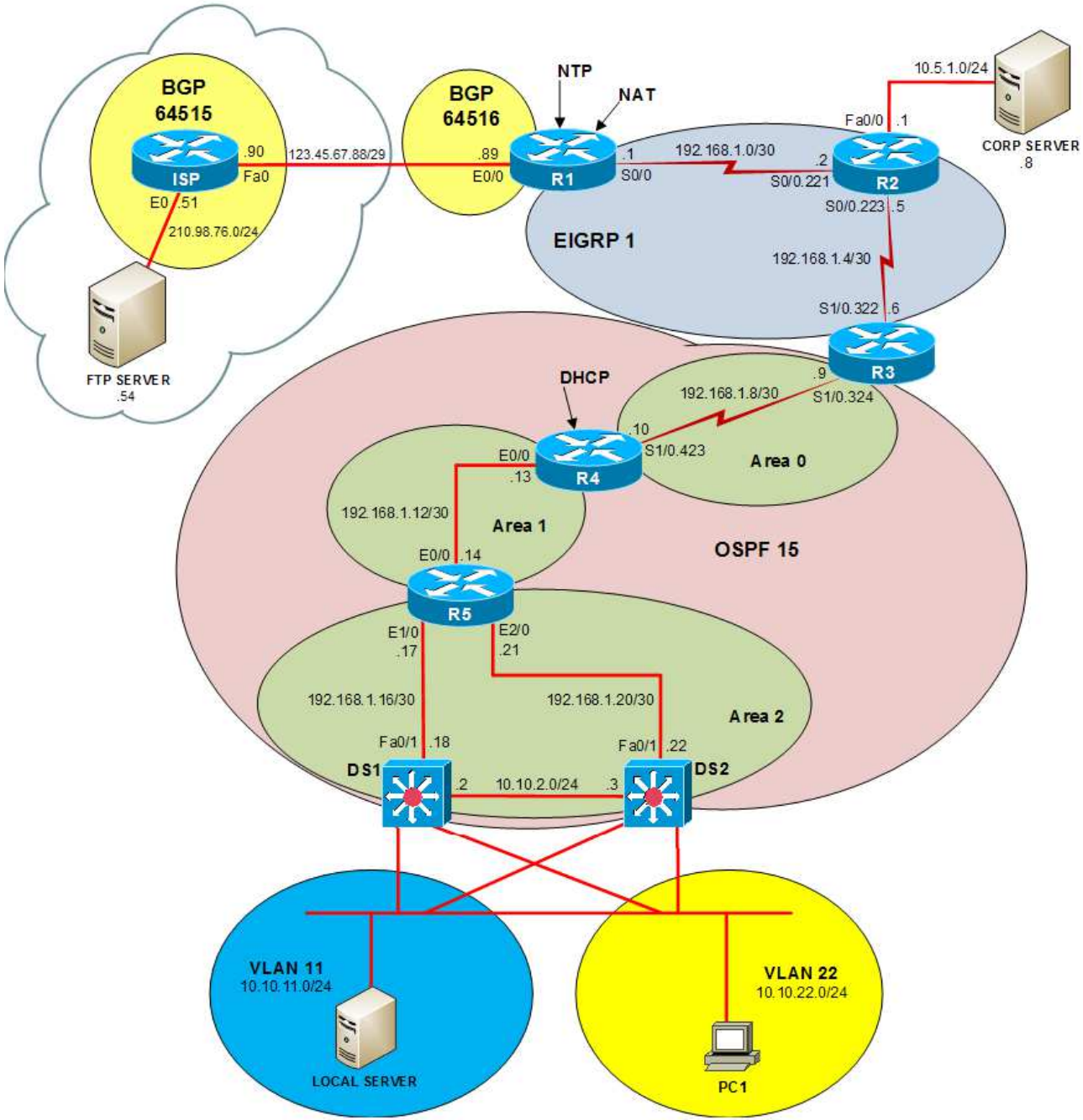
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

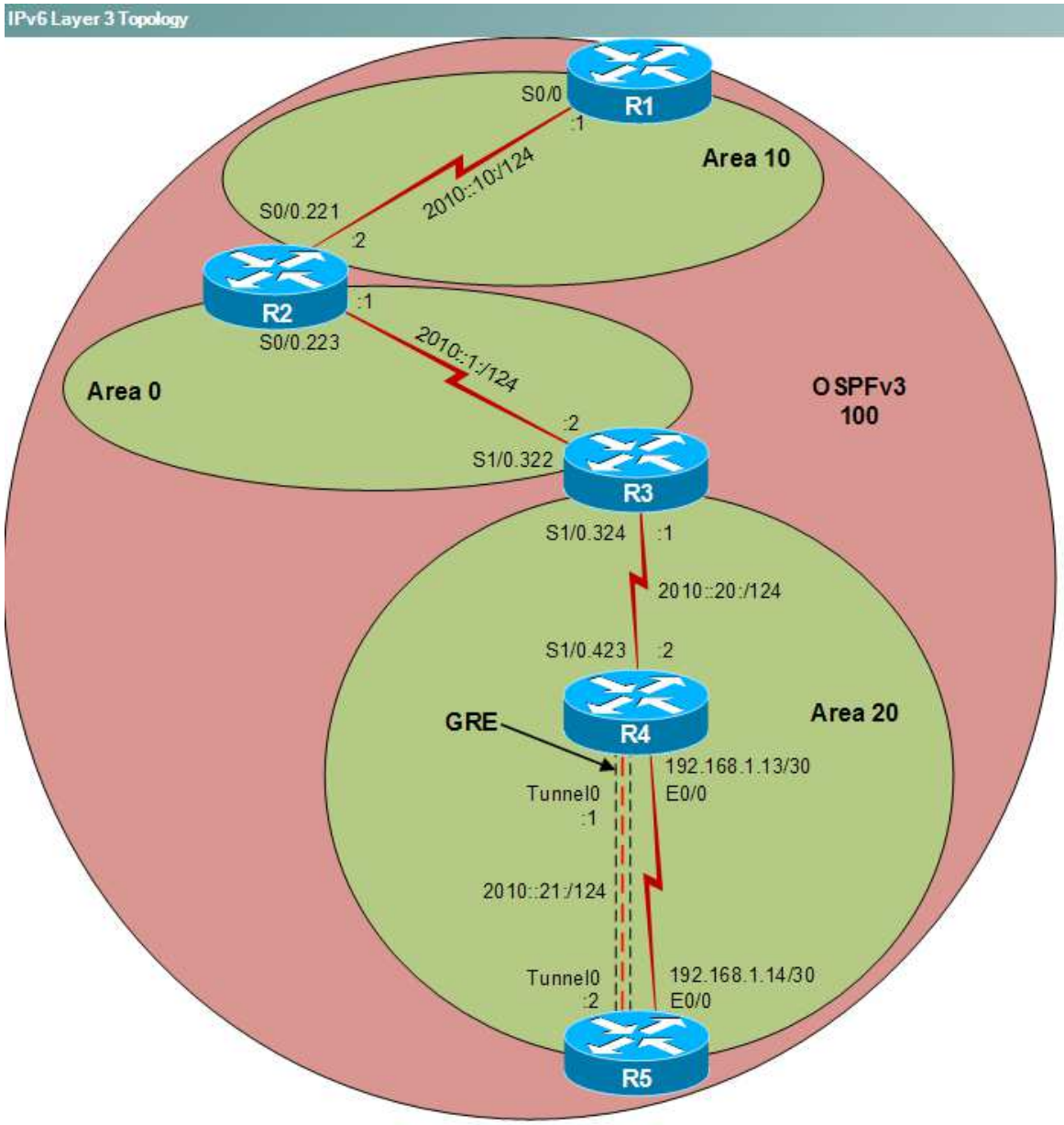
**Layer 2 Topology**




IPv4 layer 3 Topology

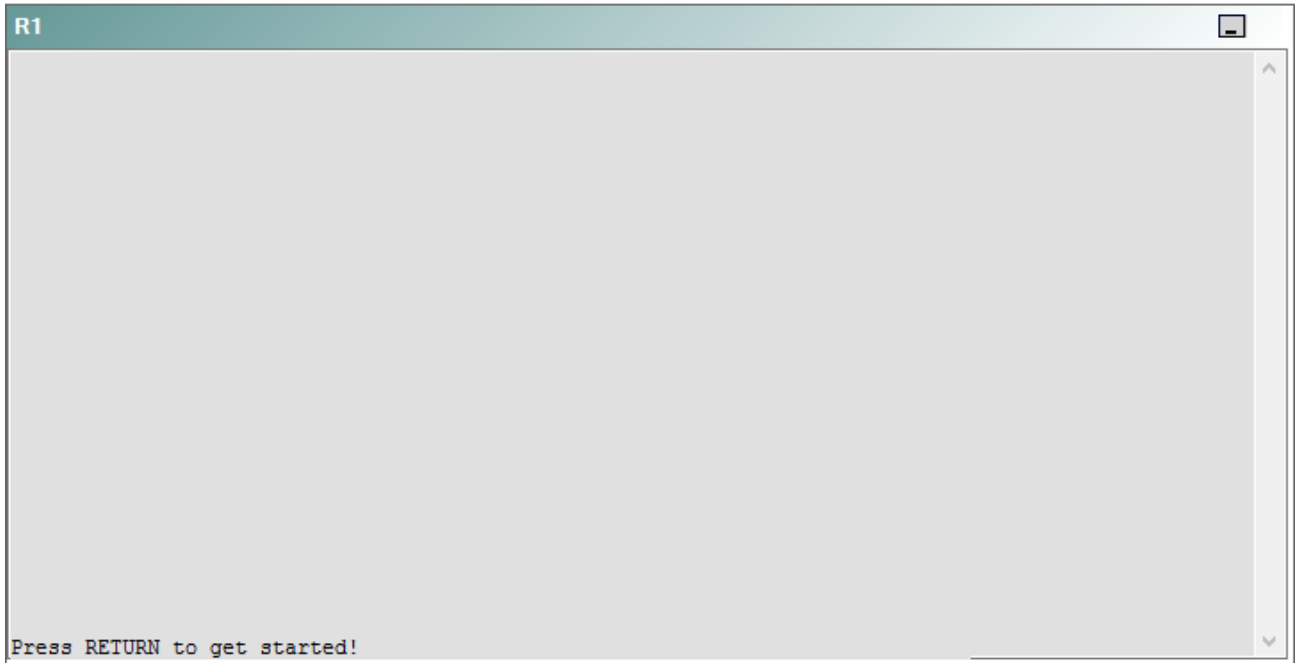

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

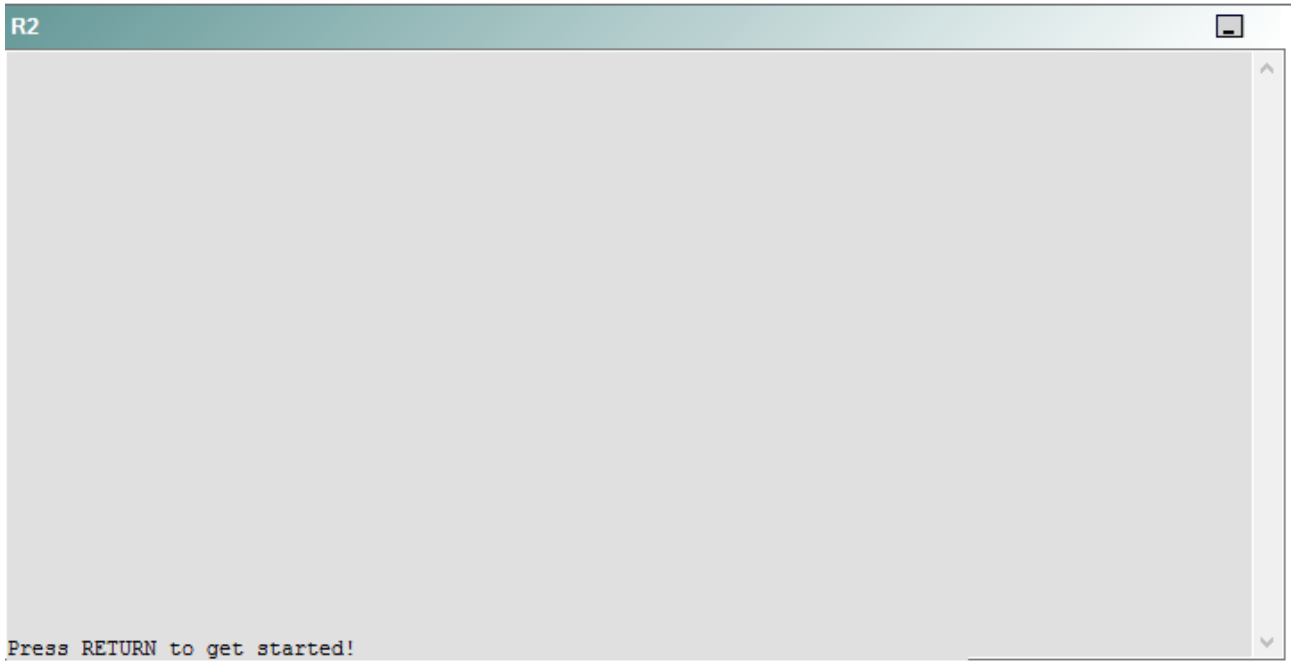



https://www.gratisexam.com/

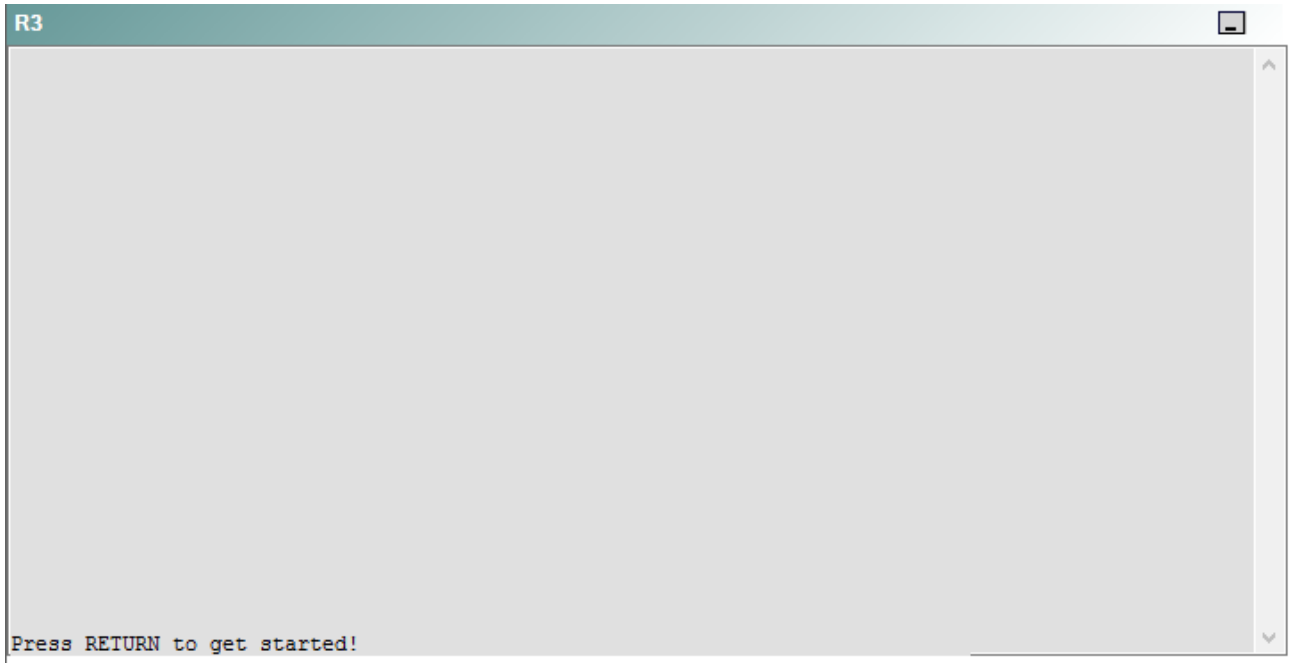
R1



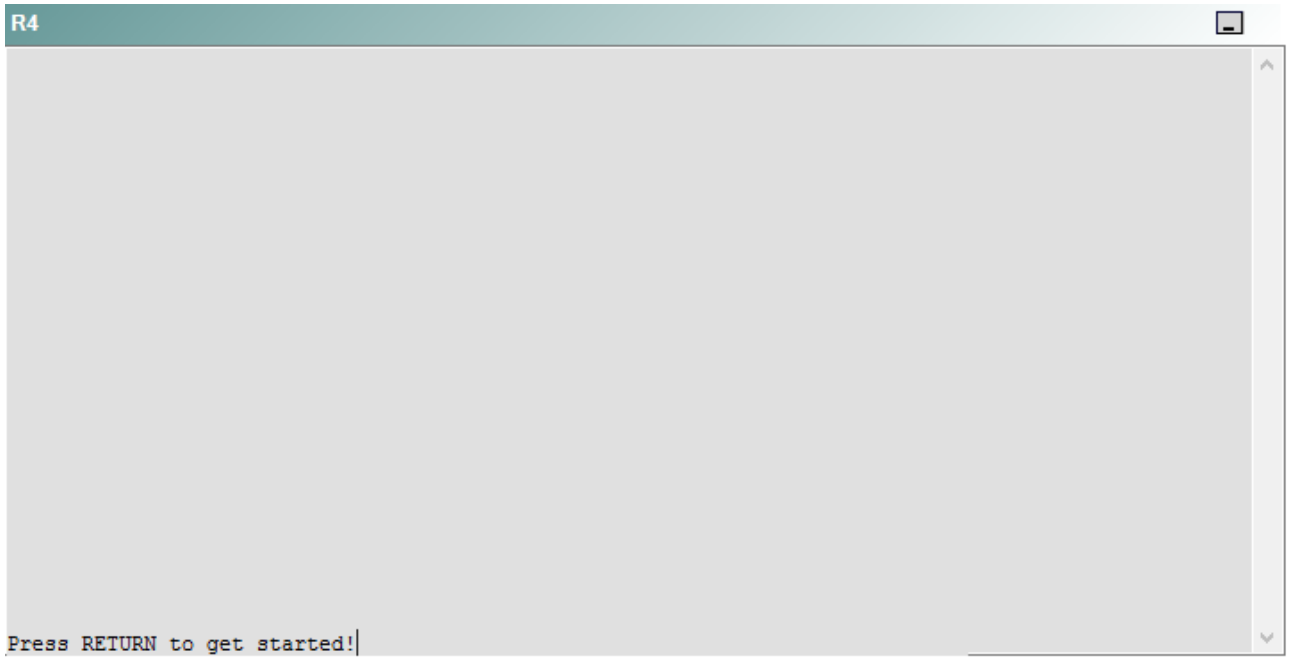

R2



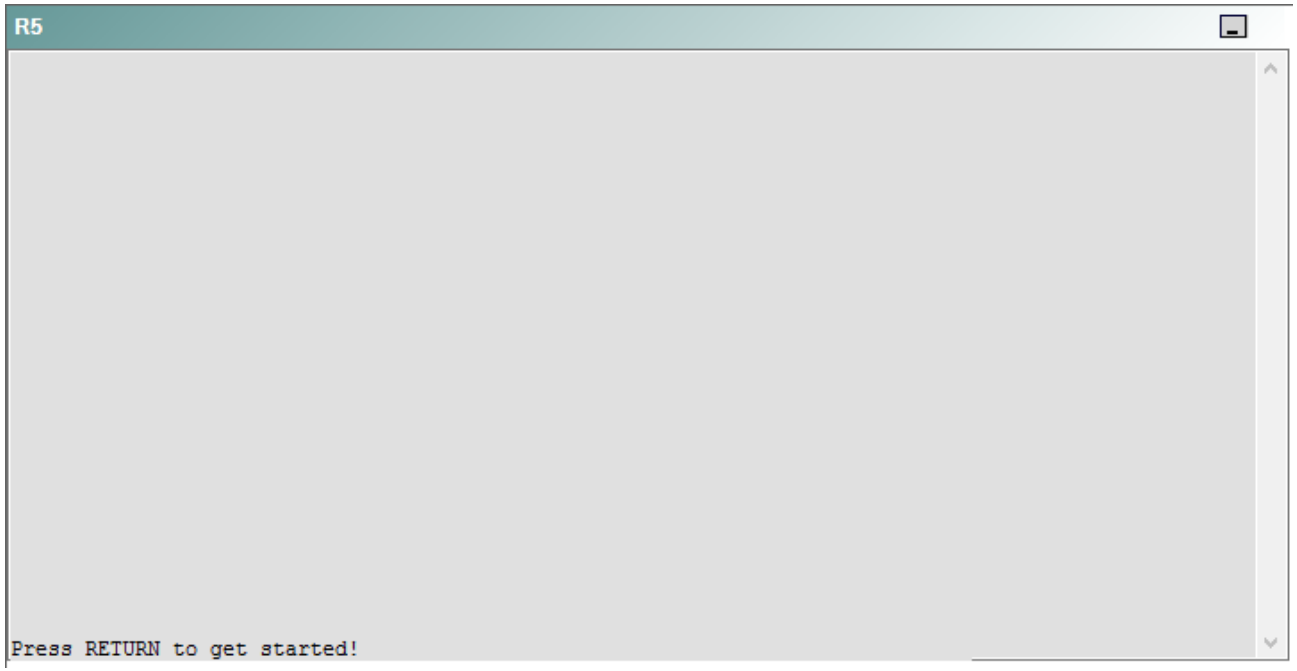

R3



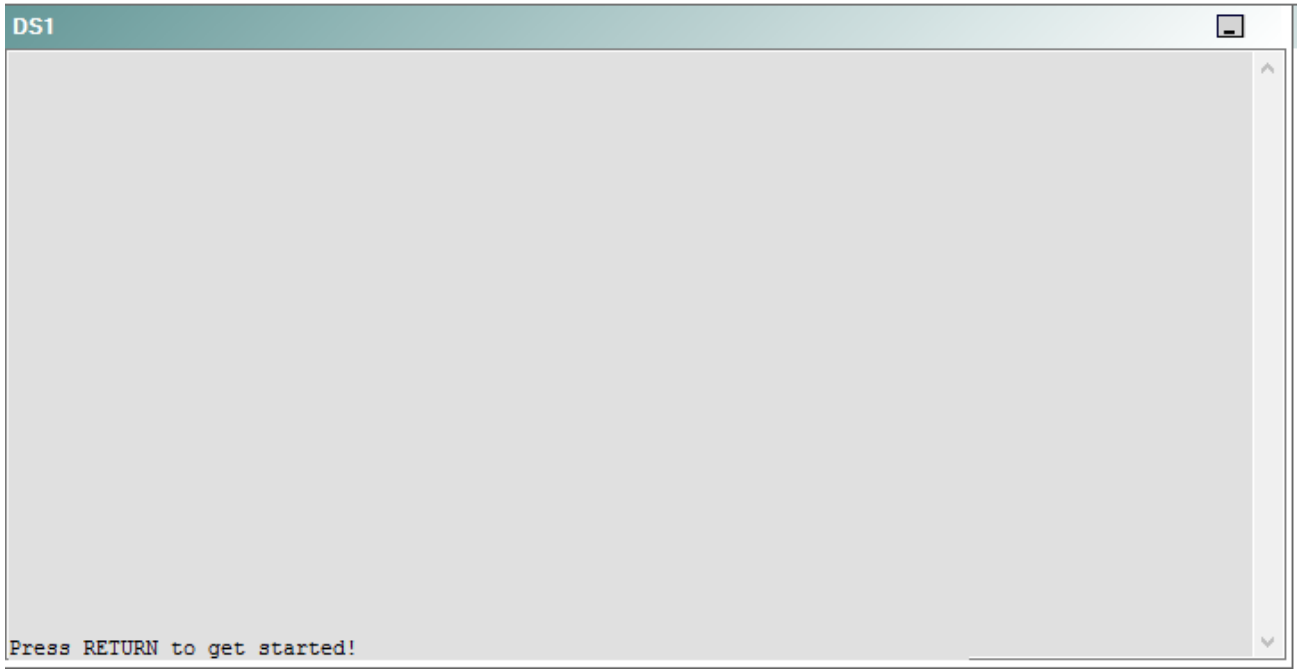

R4



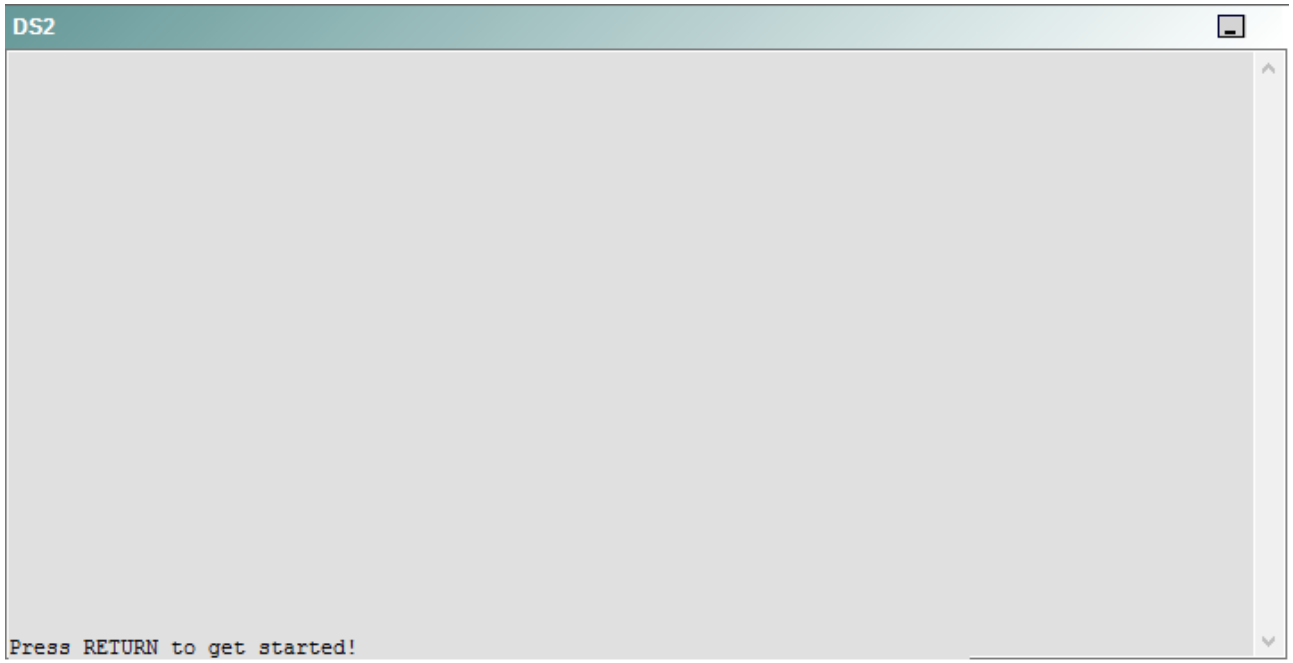

R5



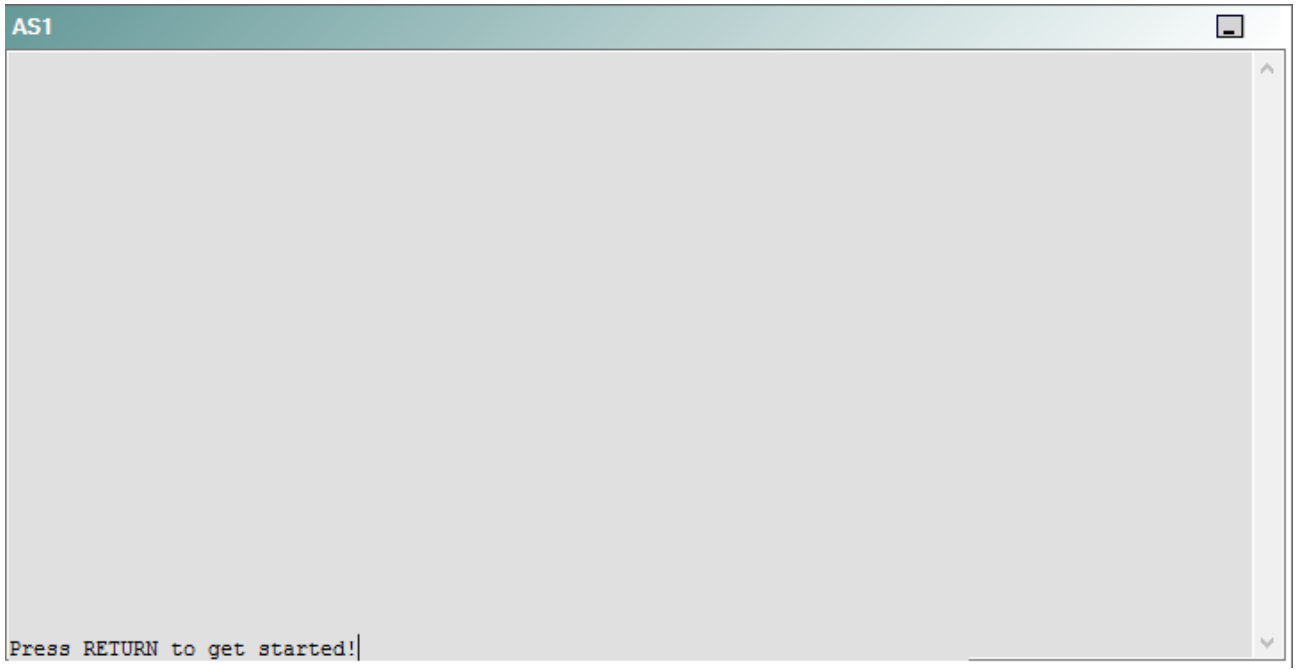

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following devices is the source of the problem?

A. R1
B. R2
C. R3
D. R4
E. R5
F. DS1
G. DS2
H. AS1

**Correct Answer:** G
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 70**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

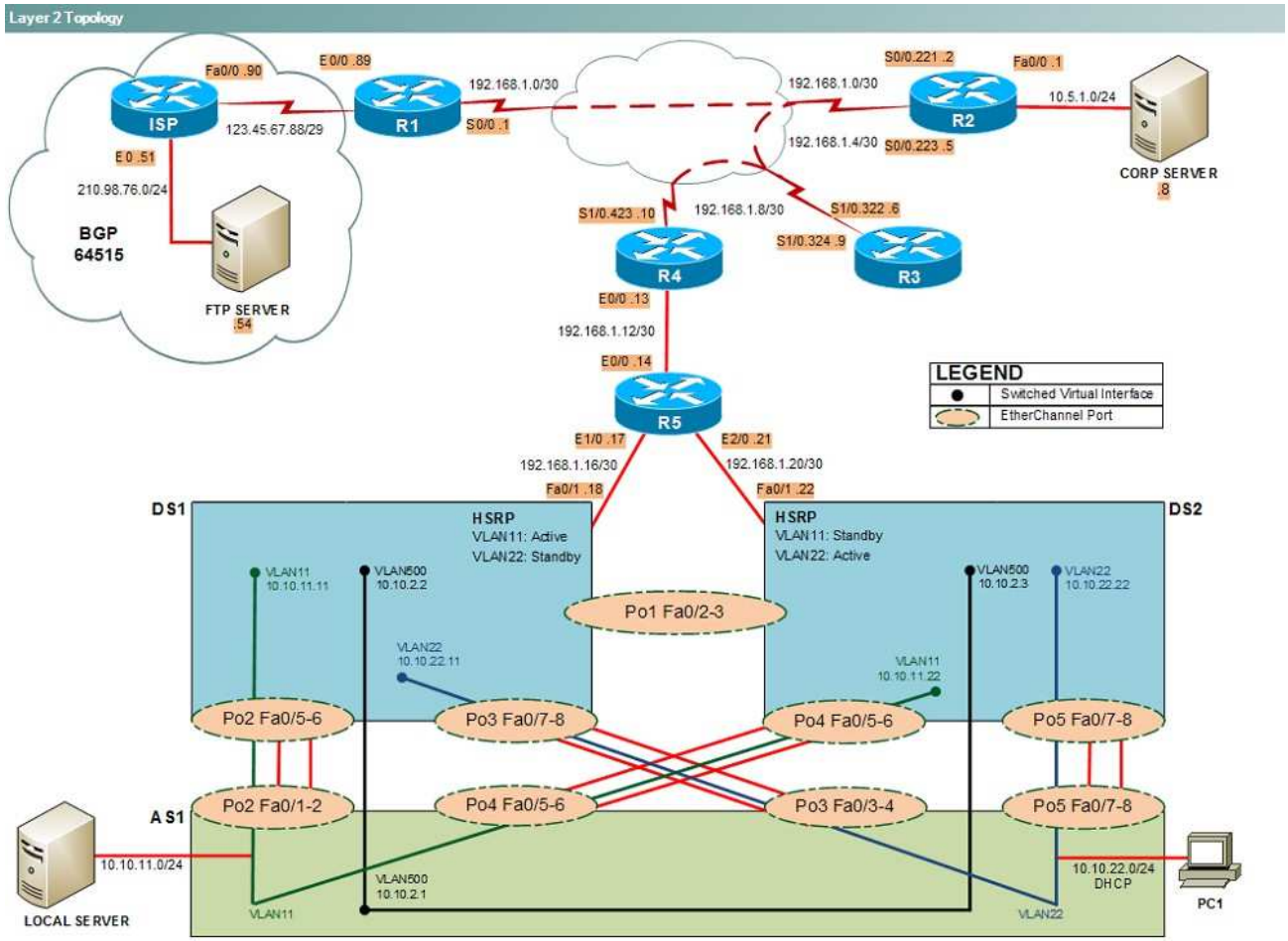
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

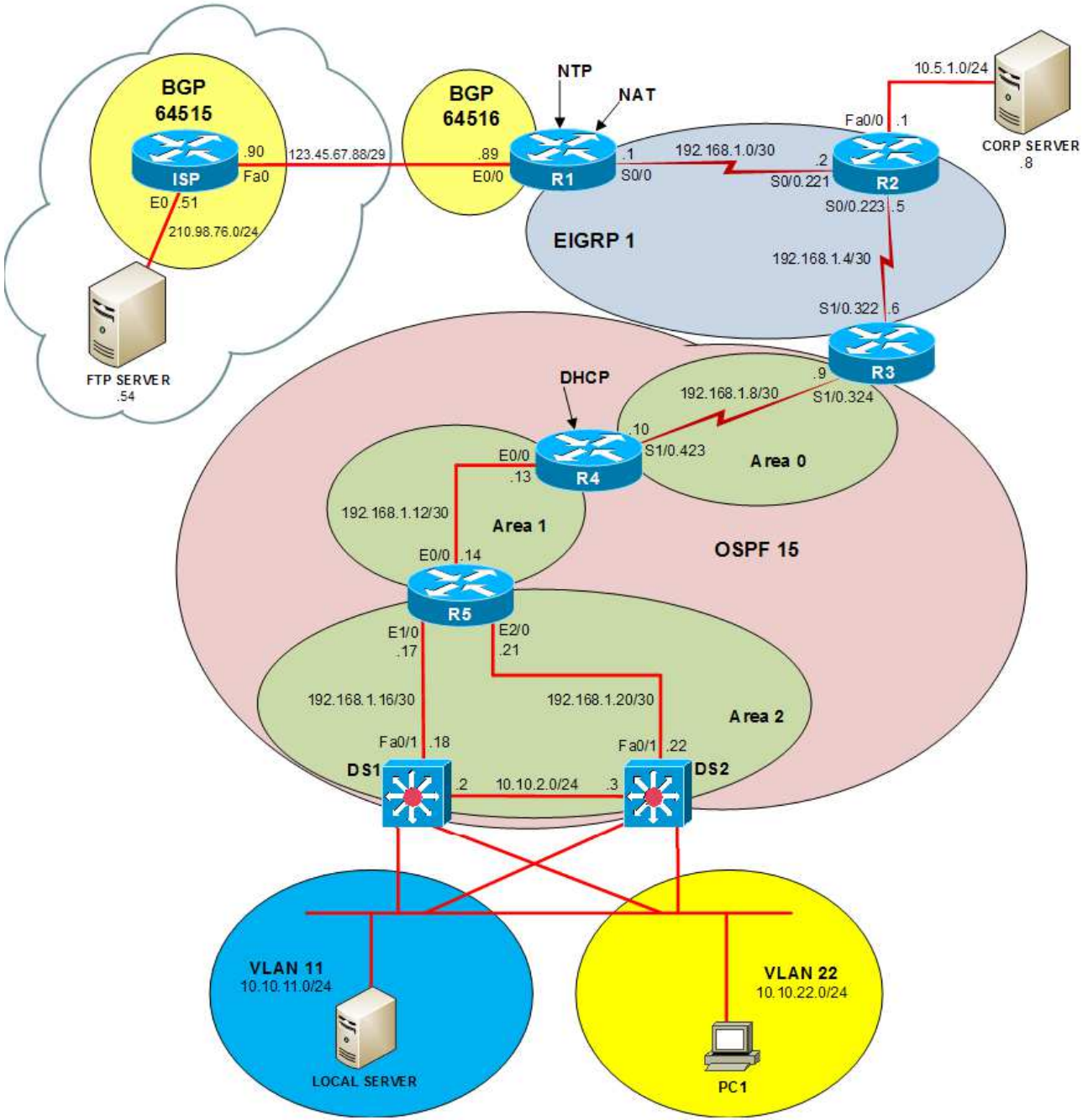
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

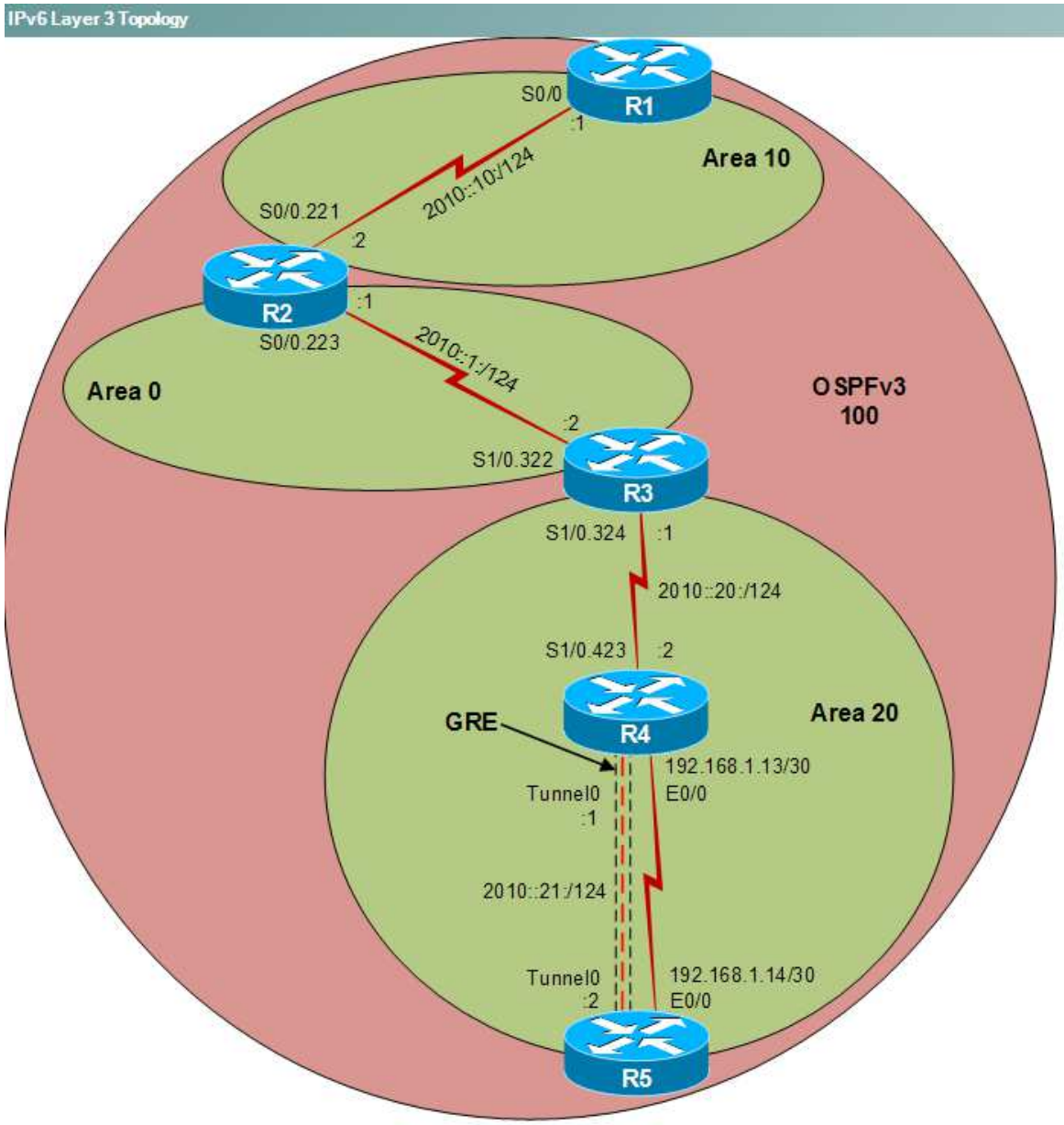
**Layer 2 Topology**




IPv4 layer 3 Topology

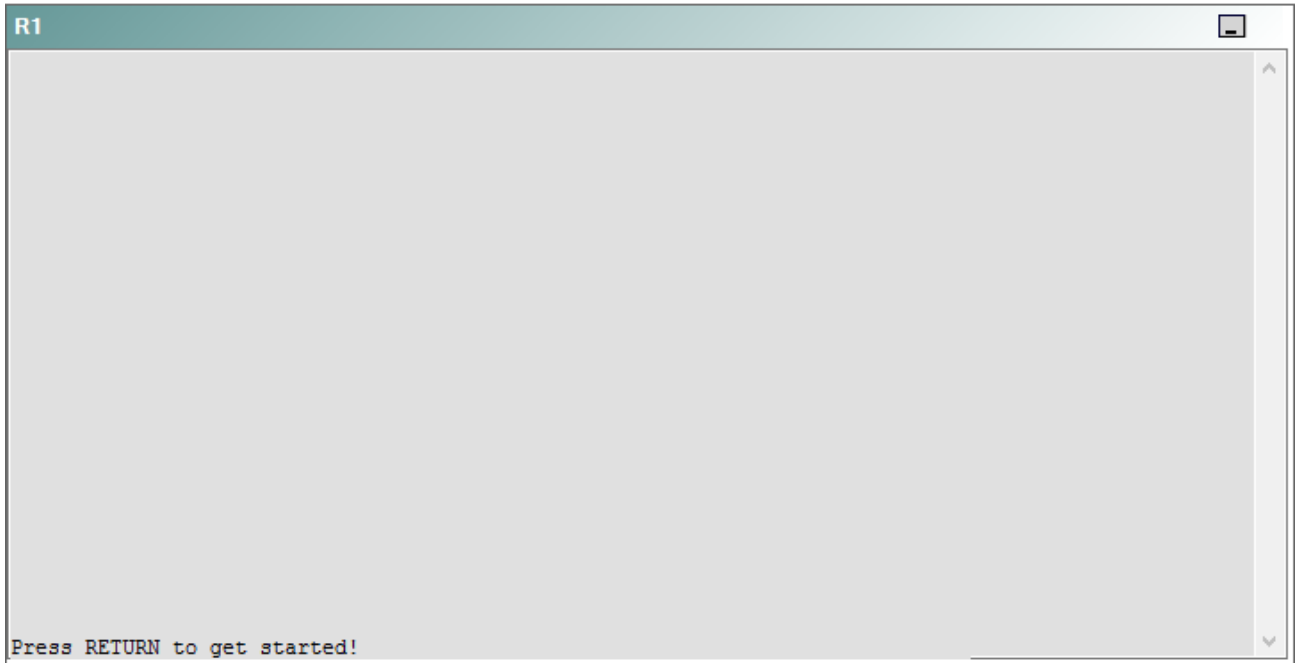

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

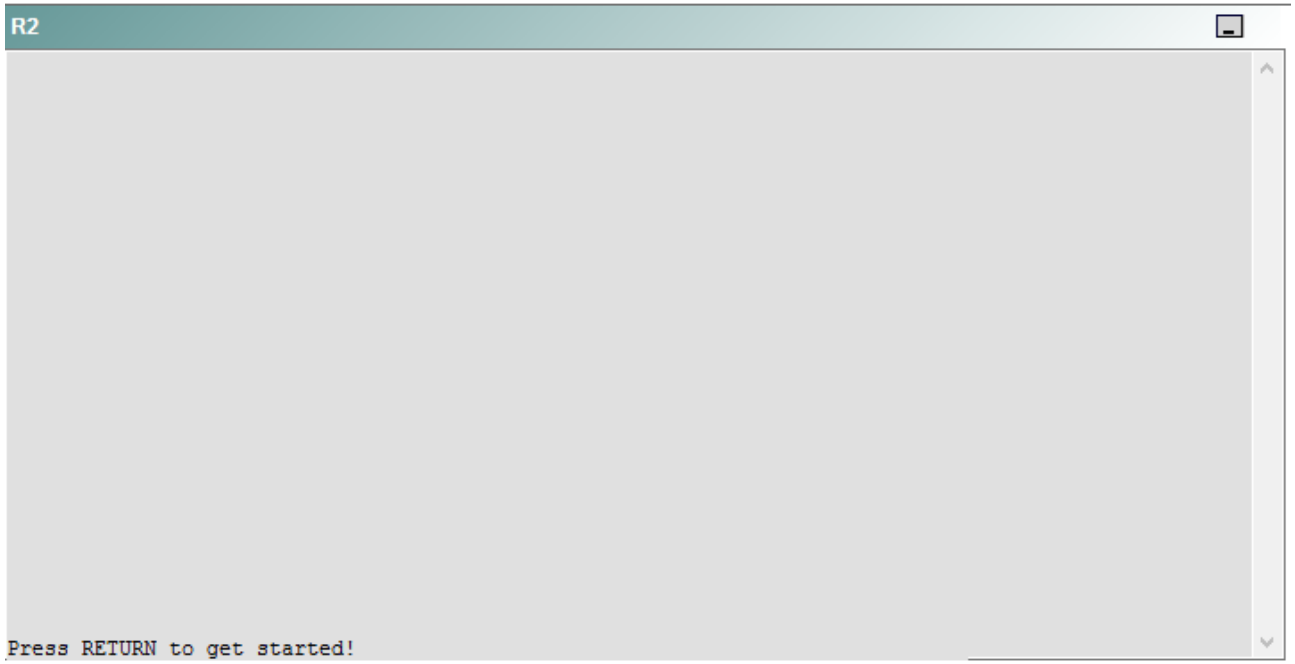



https://www.gratisexam.com/

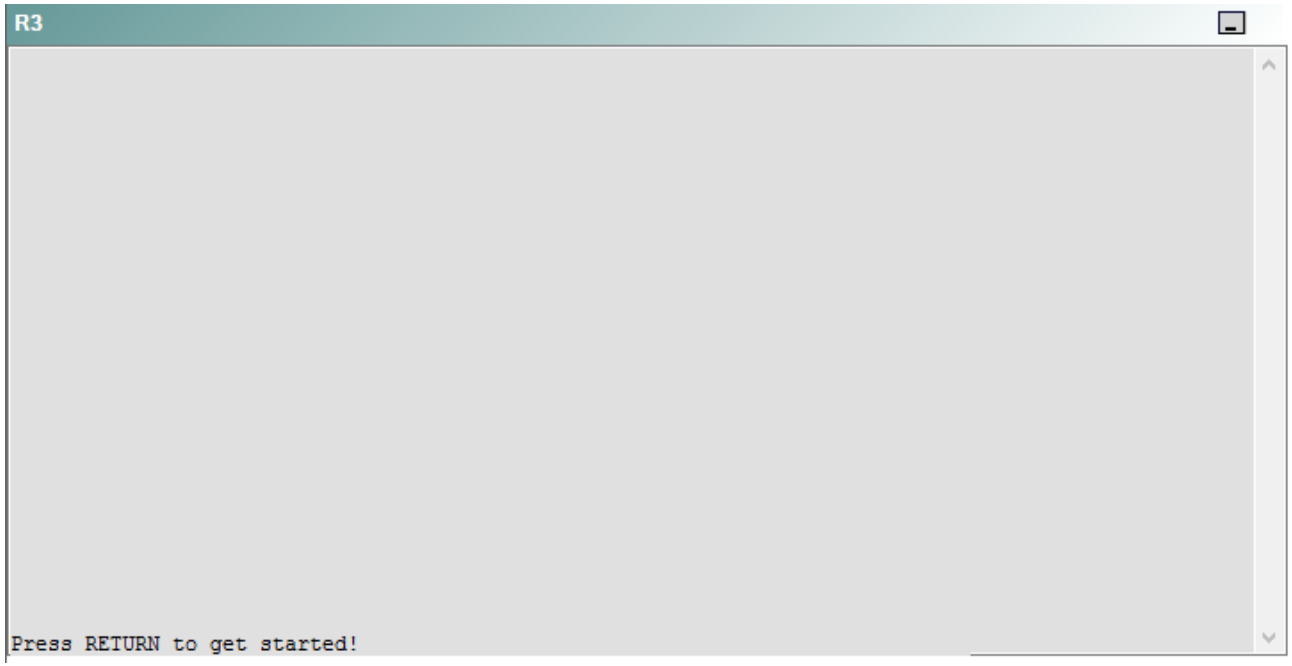
R1



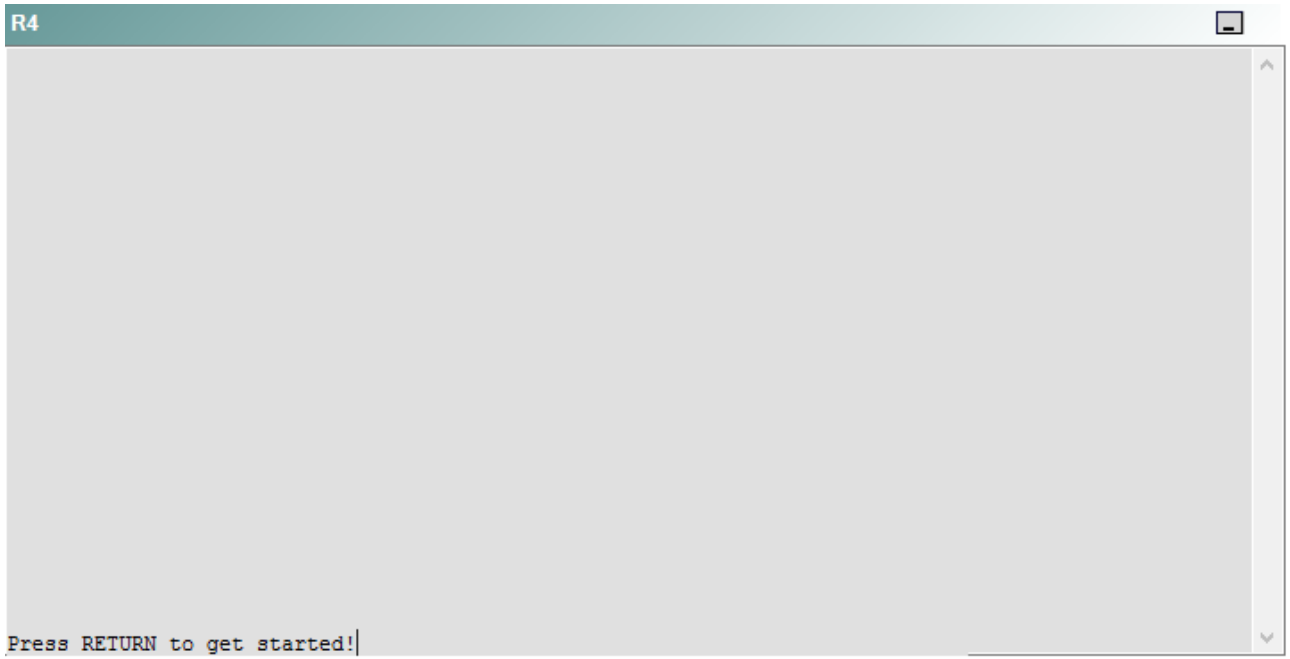

R2



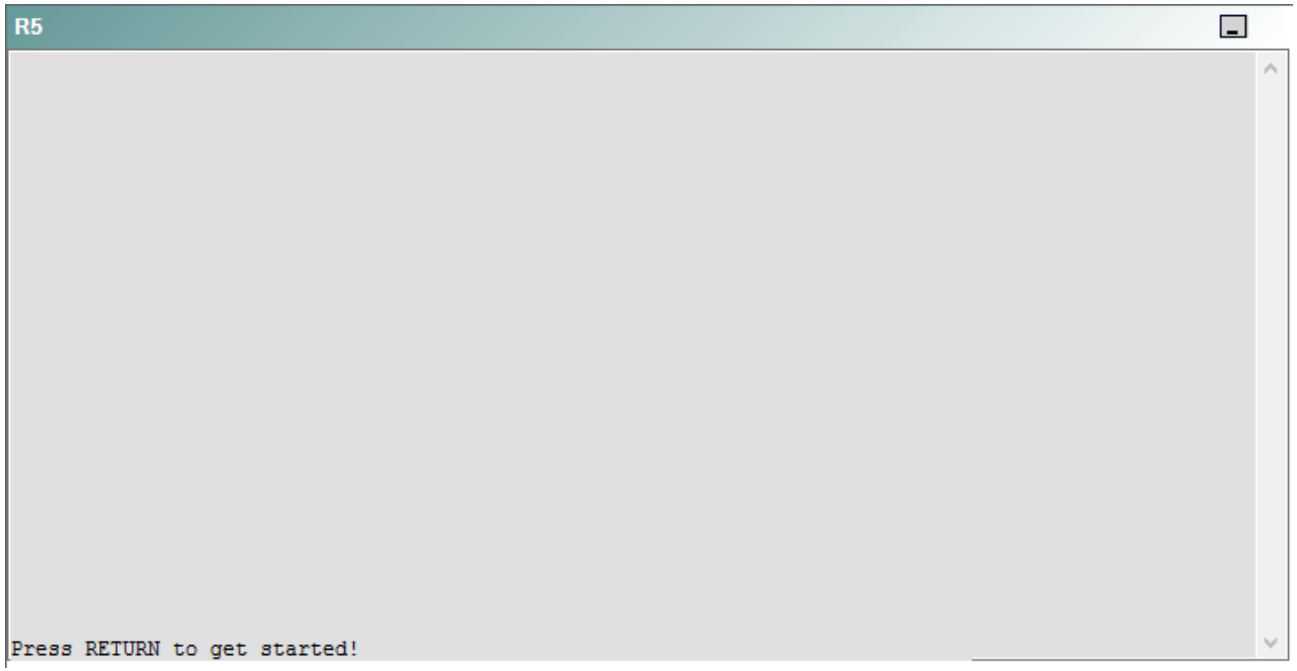

R3



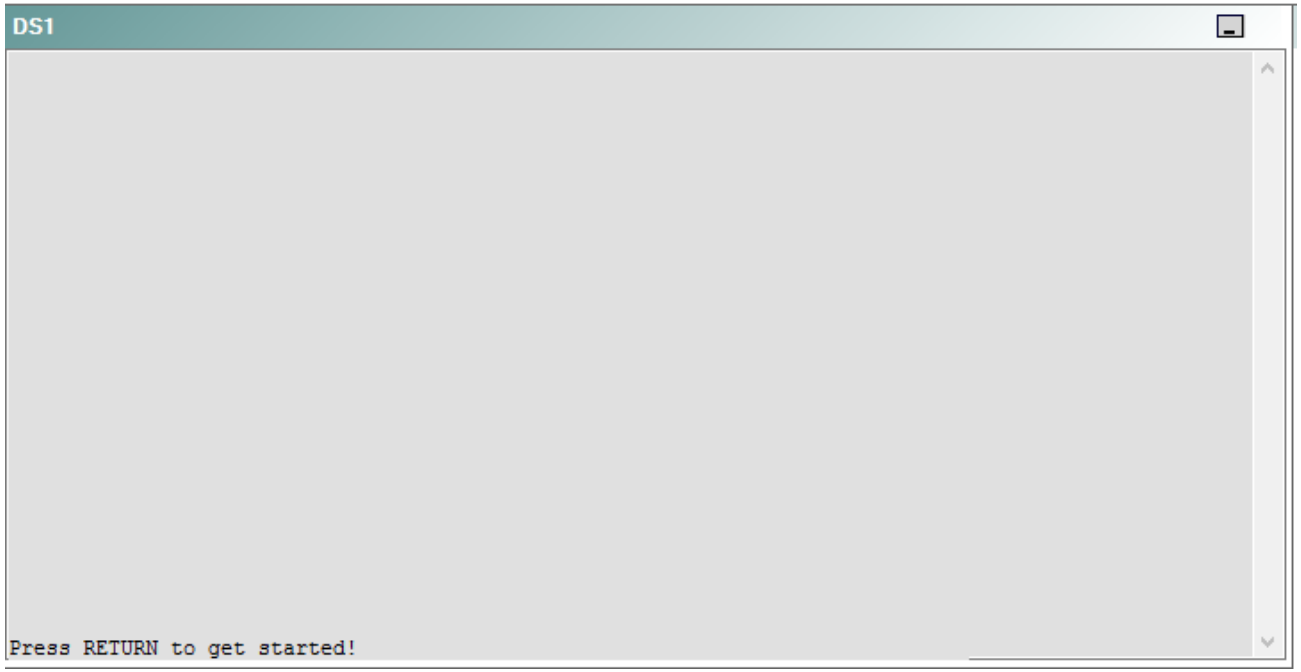

R4



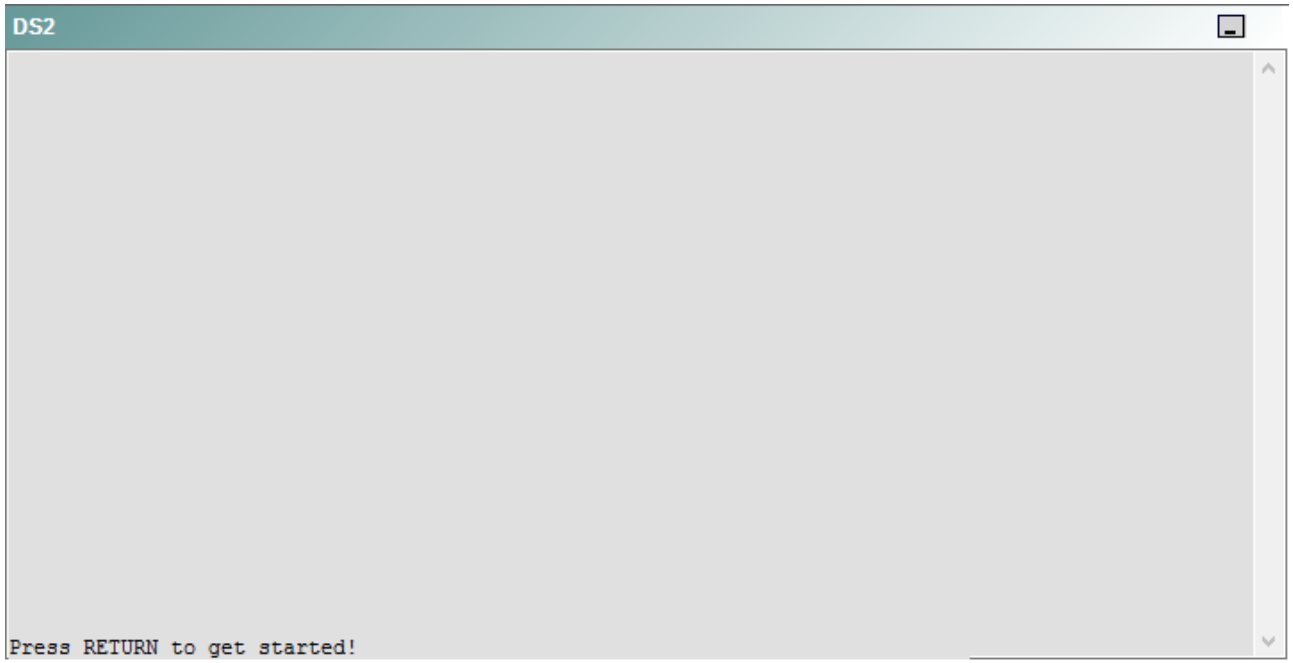

R5



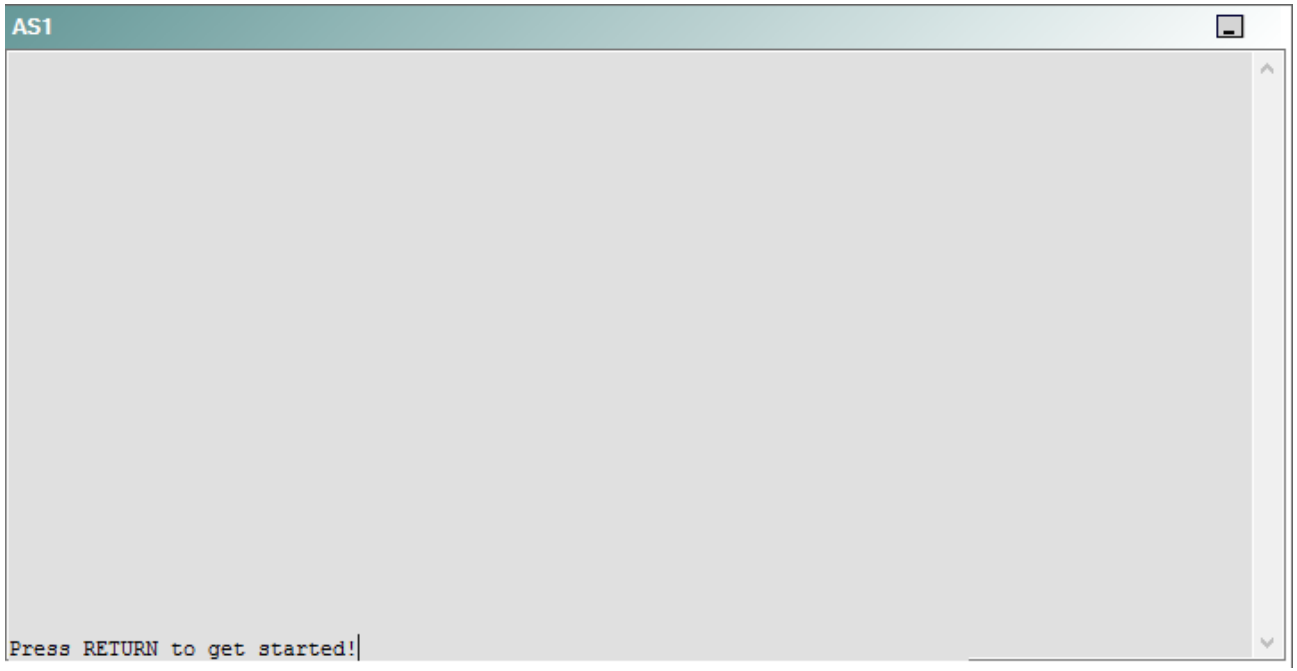

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following technologies is the source of the problem?

A. NTP
B. DHCP
C. Layer 3 addressing
D. Layer 3 security
E. Layer 2 security
F. STP
G. Etherchannel
H. VLAN configuration
I. interface

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 71**
**Instructions**

This item contains a trouble ticket covering a single network topology. You will need to troubleshoot the problem by issuing commands on the devices. To begin troubleshooting a ticket, click on the **BLUE** trouble ticket button on the right.

For each ticket, you will be required to answer the following three questions:

- Which of the following devices is the source of the problem?
- Which of the following technologies is the source of the problem?
- Which of the following is most likely to solve the problem?

Although the ticket scenarios might look similar, the devices are configured differently for each ticket. You can access a device by clicking on its button at the bottom of the screen or by clicking on its picture in any of the topology diagrams. You can open the topology diagrams by clicking on the topology buttons at the bottom of the screen. You can have multiple devices and topology diagrams open at the same time.

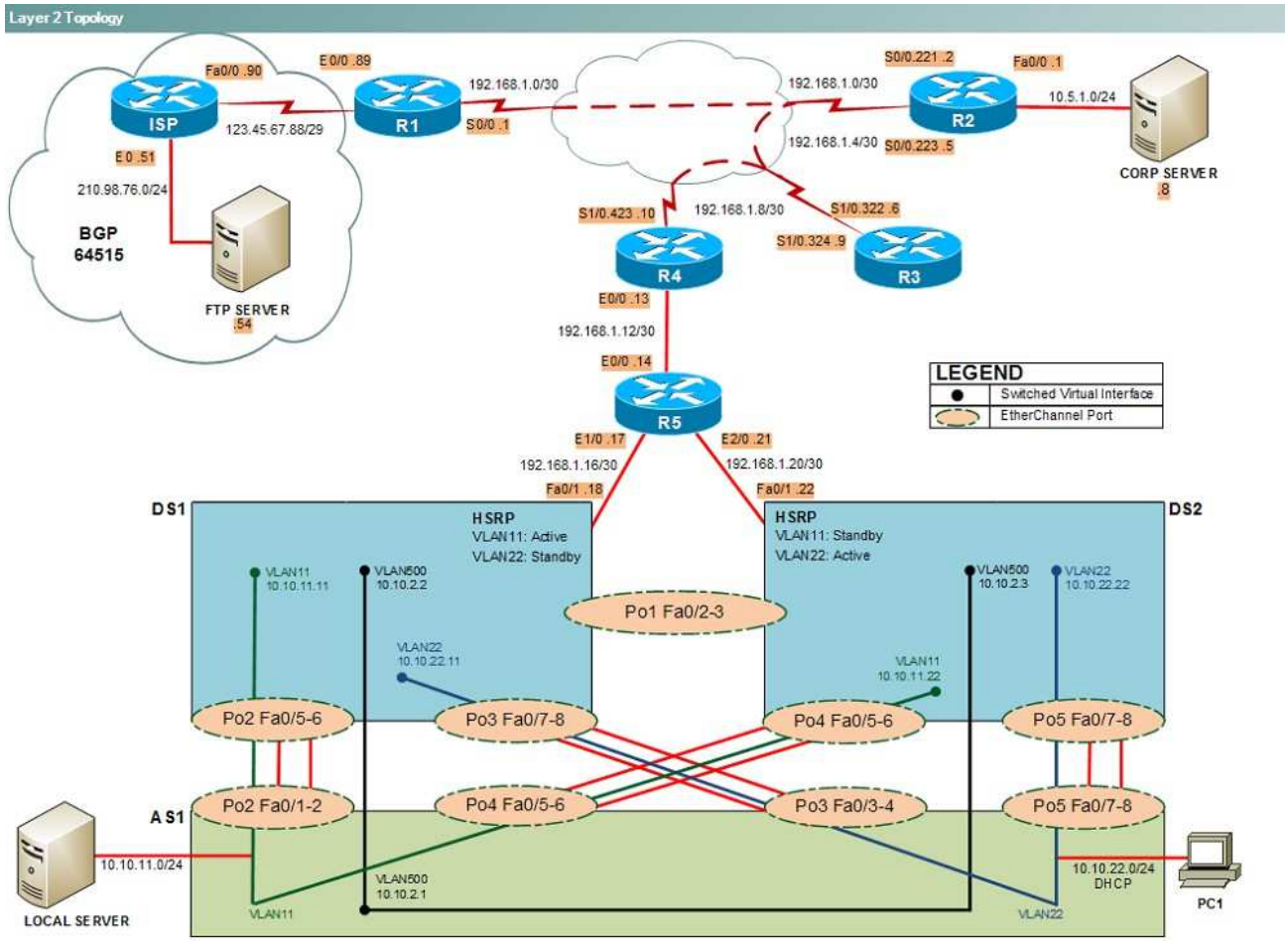
You can access the following devices for each trouble ticket:
- R1, R2, R3, and R4: Cisco 2600s
- R5: Cisco 3640
- DS1 and DS2: Cisco Catalyst 3560s
- AS1: Cisco Catalyst 2912XL
- PC1: Windows-based client operating system

Not all commands are available on each device. Only certain **show**, **ping**, and **traceroute** commands are available on the routers and switches. Only the **ping** and **ipconfig** commands are available on PC1. You cannot access the ISP router or any of the servers.

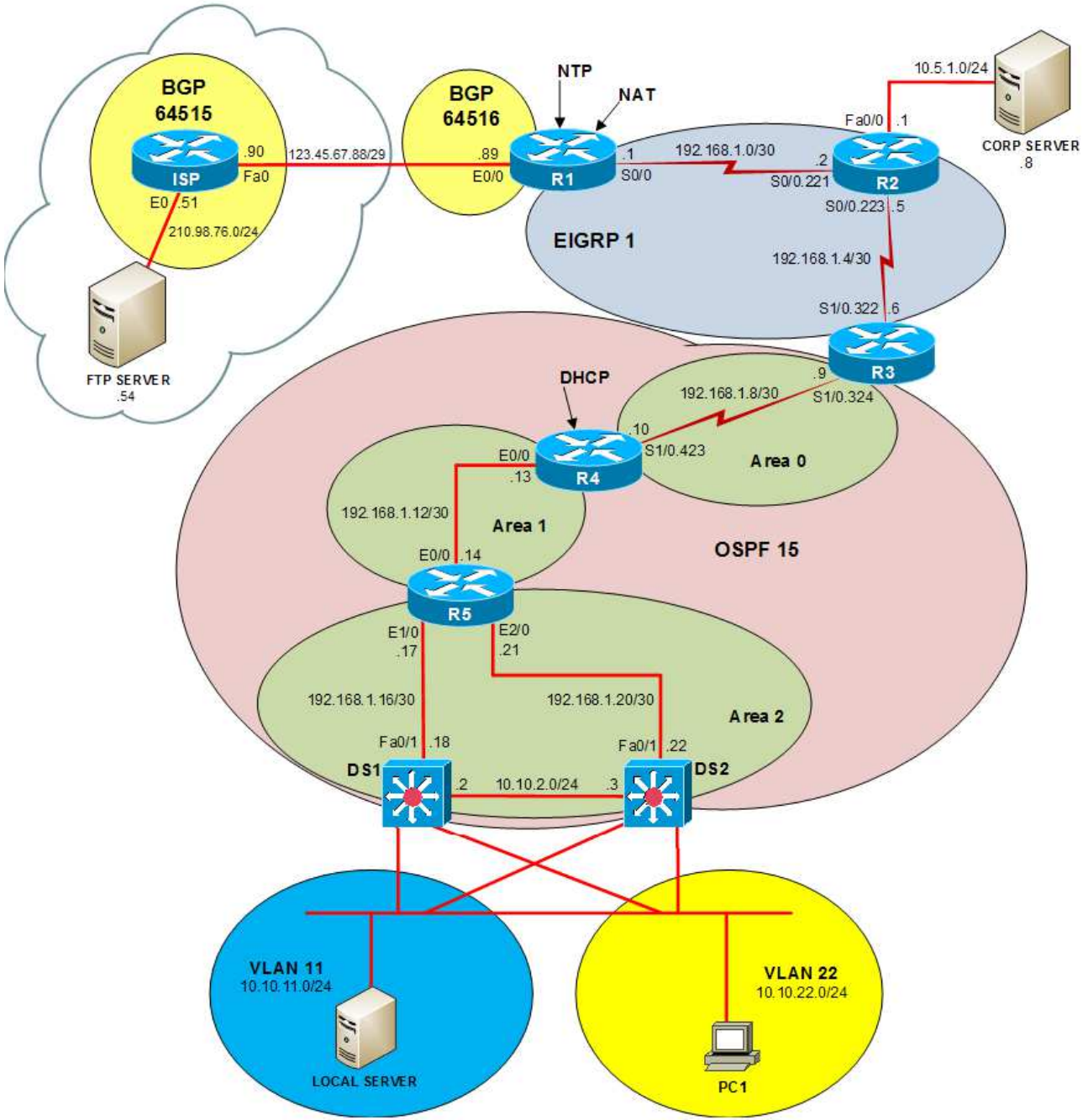
You can move among the three questions in the trouble ticket by clicking **Previous Question** and **Next Question**. After you have answered the third question, you can click **Done** to complete the trouble ticket. In study mode, you can complete a trouble ticket and display the explanation by clicking **Done + Show Explanation**. However, once you have clicked either of these two **GREEN** buttons, your responses will be recorded and the ticket button will turn **RED**. In simulation mode, you will be unable to reopen the ticket.

Click the **CLOSE** button at the bottom right when you are ready to end the troubleshooting simulation.

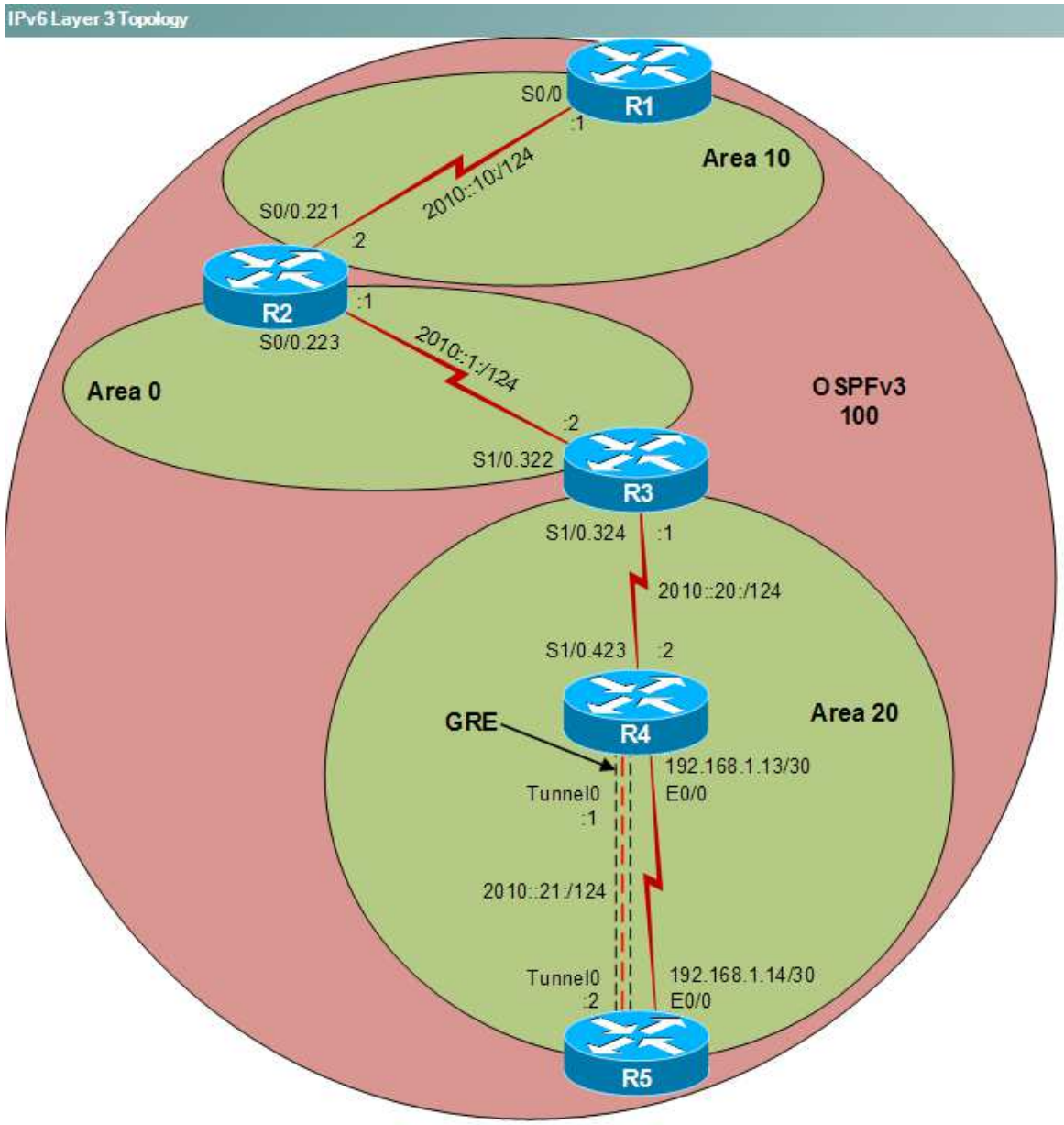
**Layer 2 Topology**




IPv4 layer 3 Topology

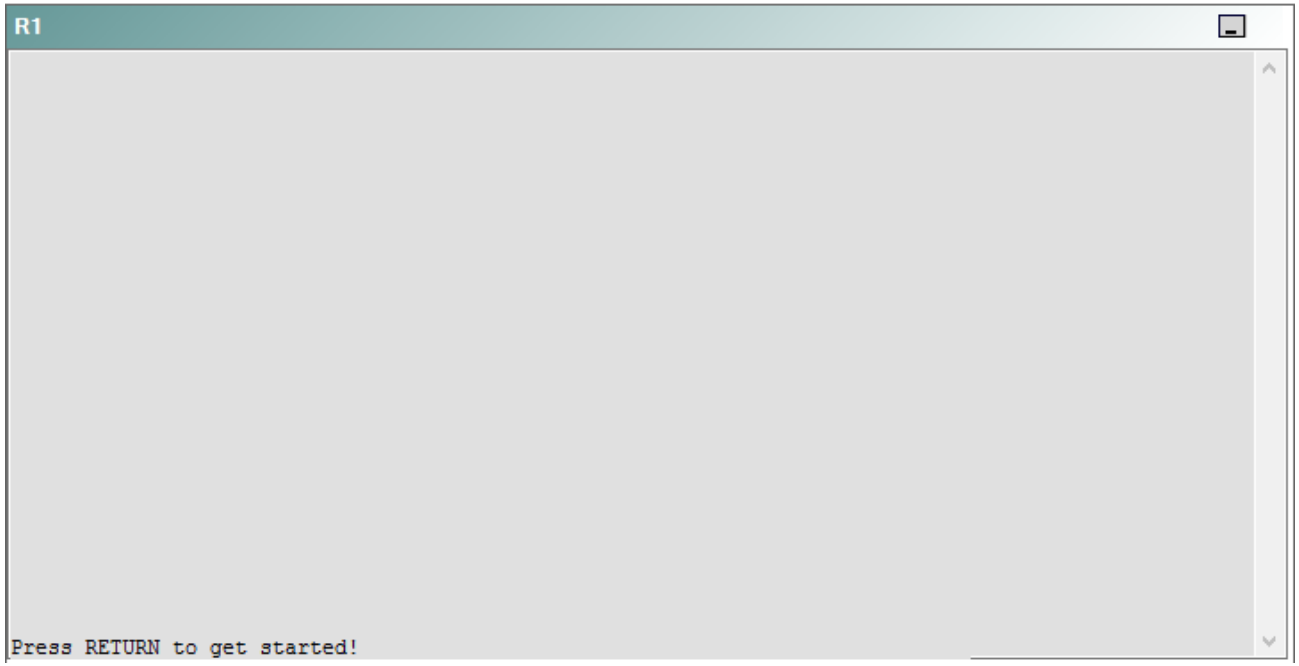

BGP
64515
ISP
.90
Fa0
123.45.67.88/29
E0 .51
210.98.76.0/24
FTP SERVER
.54
BGP
64516
.89
E0/0
NTP
NAT
R1
.1
S0/0
192.168.1.0/30
.2
S0/0.221
R2
Fa0/0 .1
10.5.1.0/24
CORP SERVER
.8
S0/0.223 .5
EIGRP 1
192.168.1.4/30
S1/0.322 .6
R3
.9
S1/0.324
192.168.1.8/30
DHCP
.10
S1/0.423
R4
E0/0
.13
Area 0
192.168.1.12/30
Area 1
E0/0 .14
OSPF 15
R5
E1/0
.17
E2/0
.21
192.168.1.16/30
192.168.1.20/30
Area 2
Fa0/1 .18
Fa0/1 .22
DS1
DS2
.2
10.10.2.0/24
.3
VLAN 11
10.10.11.0/24
LOCAL SERVER
VLAN 22
10.10.22.0/24
PC1

IPv6 Topology

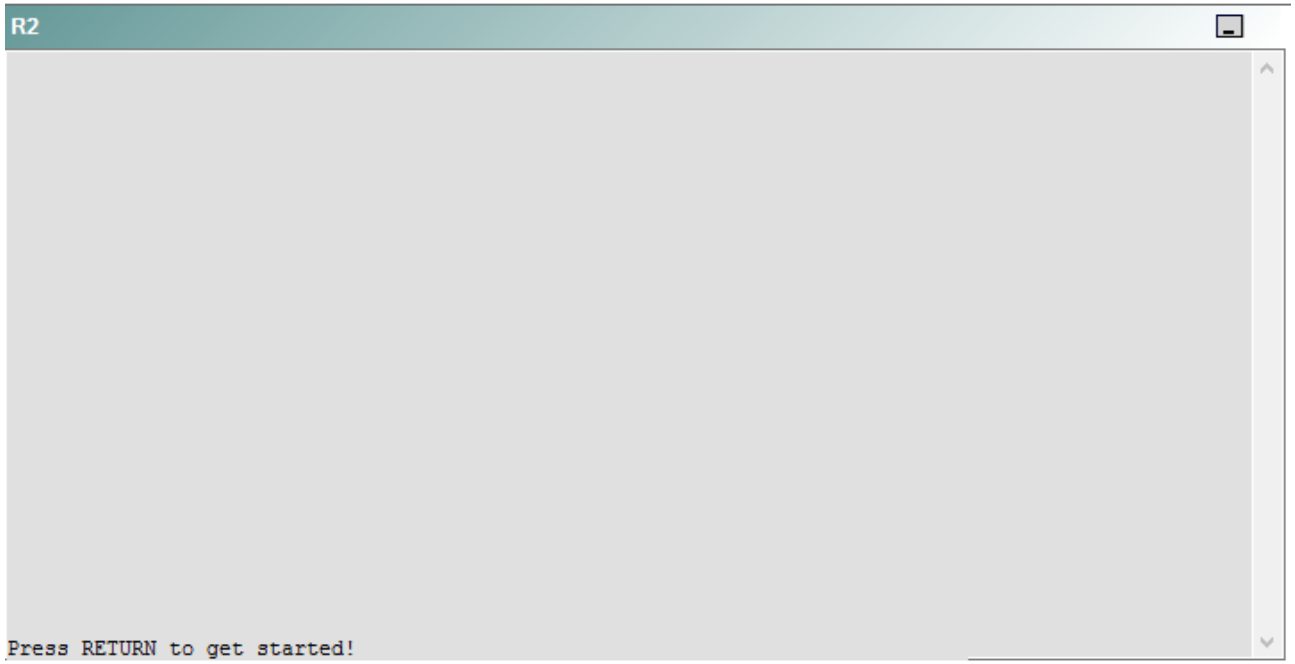



https://www.gratisexam.com/

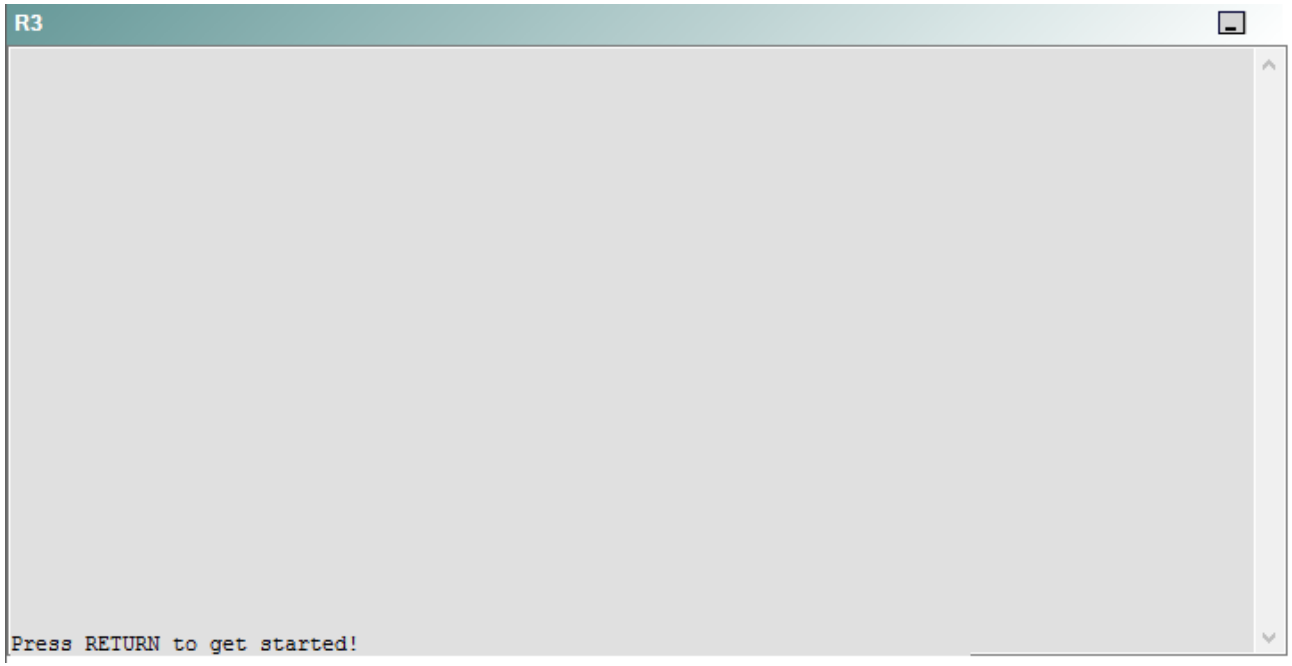
R1



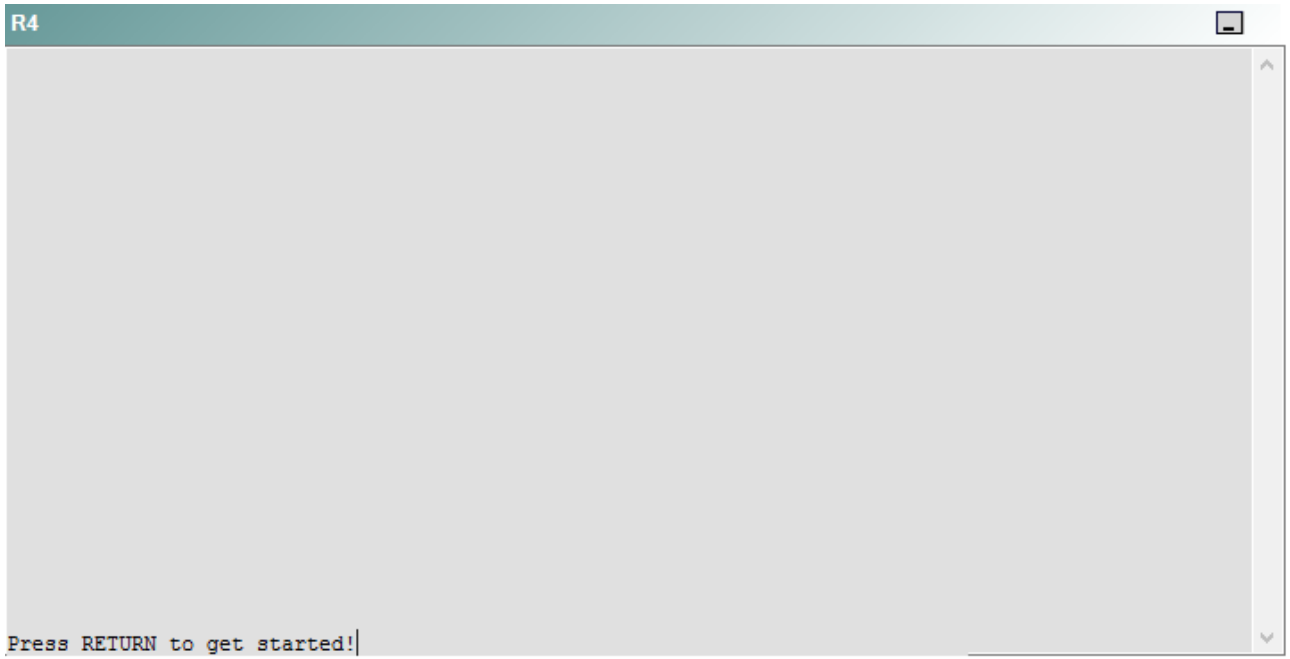

R2



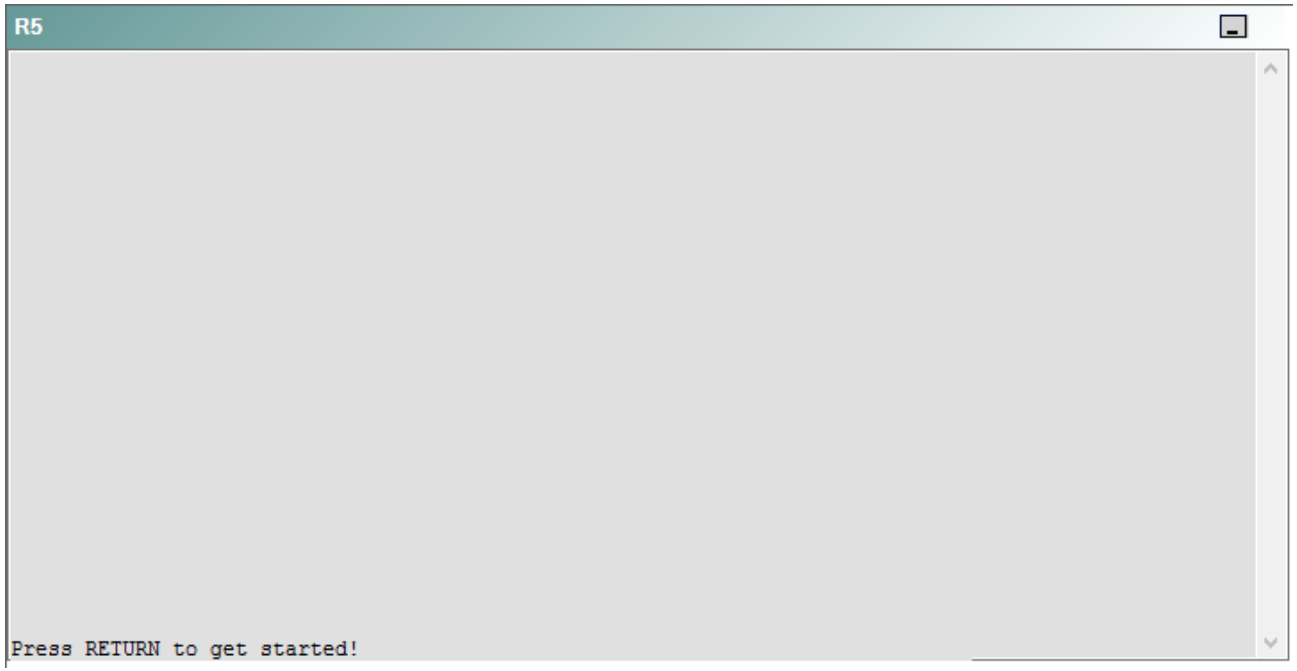

R3



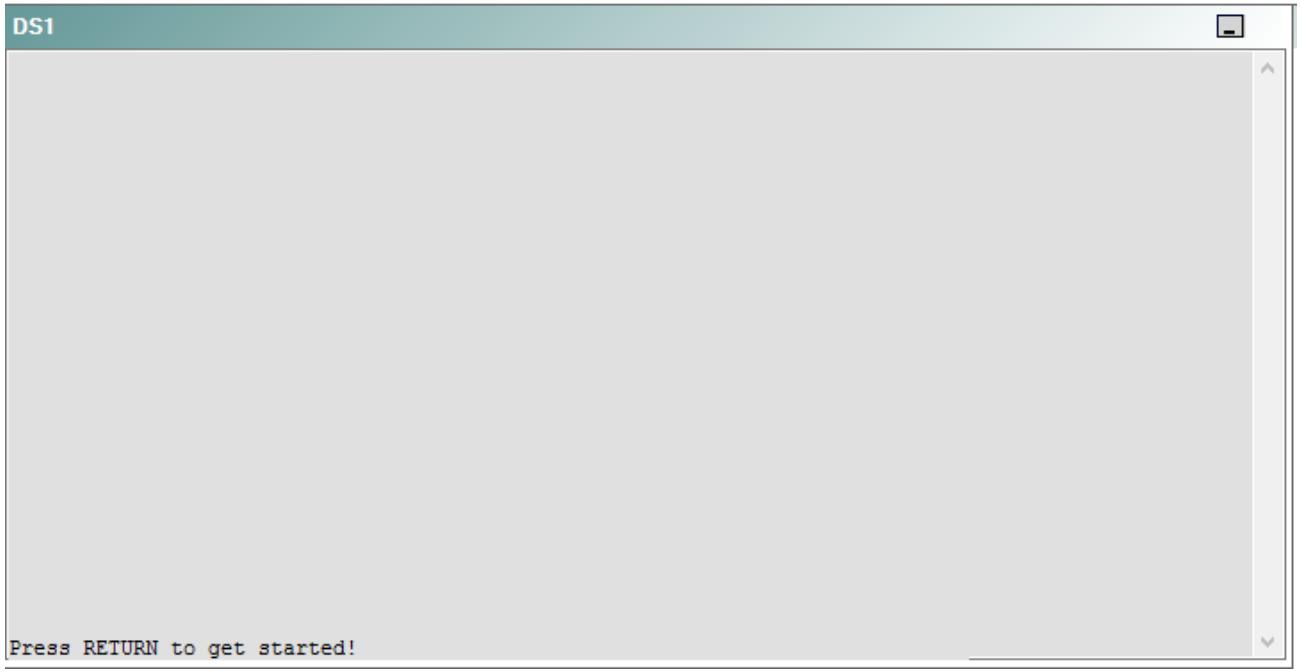

R4



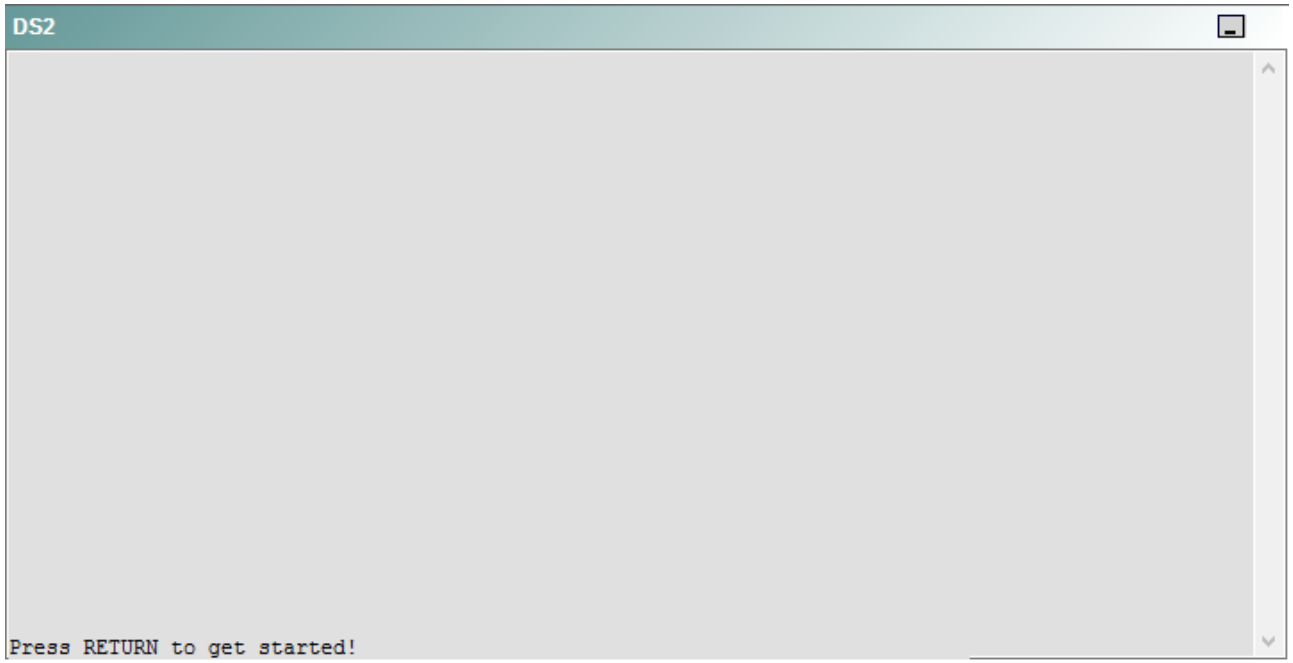

R5



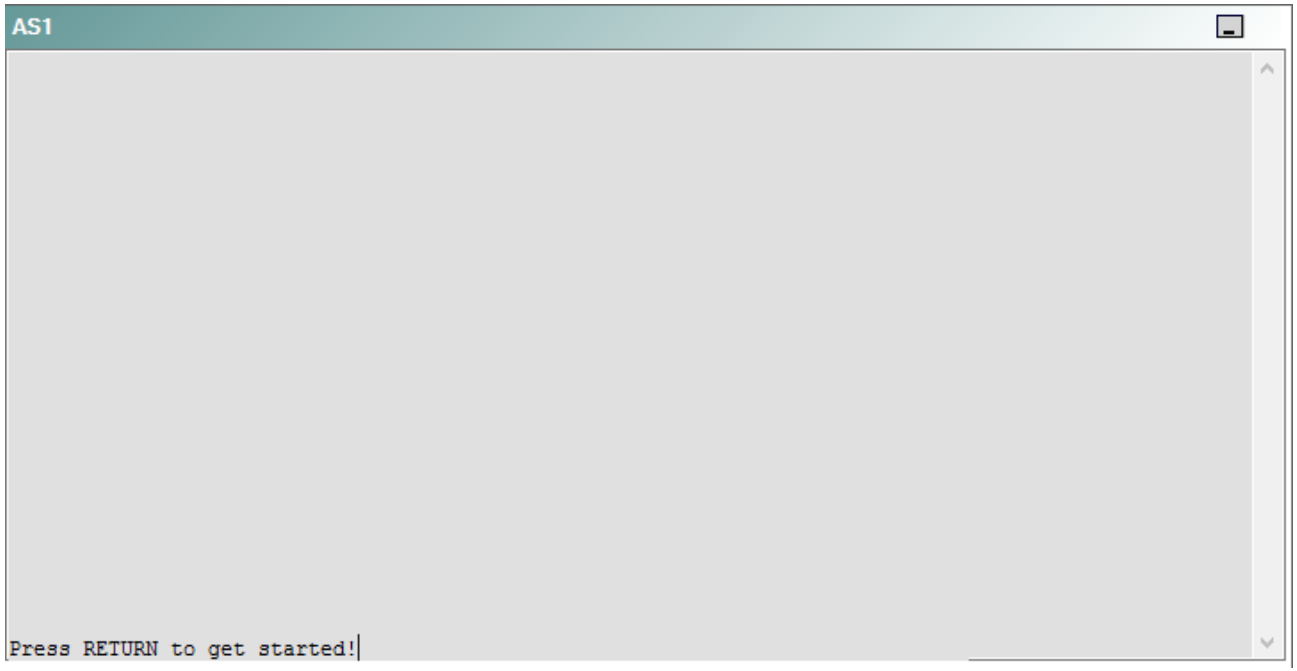

DS1




DS2




AS1




PC1


A network engineer has recently made several changes to your company's network. A trouble ticket has been opened reporting that PC1 is no longer able to ping the external server at 210.98.76.54.

Which of the following is most likely to solve the problem?

A. creating a new DHCP pool
B. modifying the DHCP exclusion range
C. modifying the IP address range assigned by the DHCP pool
D. changing the default router assigned by the DHCP pool
E. adding a default DNS server to the DHCP pool
F. creating an IP helper address
G. issuing the **ip forward-protocol udp 68** command.

**Correct Answer:** F
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

You should create an IP helper address on DS2. To determine which device is the source of the problem, you should issue the **ping** and **traceroute** commands to test connectivity between devices. You can use any troubleshooting method you want, as long as you follow a systematic procedure. For example, you can ping from R1 to the closest device and work your way up the network until communication is lost, or you can ping from R1 to the farthest device and work your way back to R1 until pings are successful.

In this scenario, PC1 is unable to ping any device on the network. Issuing the **ipconfig** command on PC1 will display the following output:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Autoconfiguration IP Address. . . : 169.254.133.250
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :
```

An address that begins with 169.254 indicates that the computer is using an Automatic Private IP Addressing (APIPA) address. A computer will assign itself an APIPA address if it fails to receive an IP address from a Dynamic Host Configuration Protocol (DHCP) server. Therefore, PC1 is unable to communicate with the DHCP server on R4, and the problem must exist somewhere between them. DS2 and DS1 are both able to ping R4; therefore, there must be some other reason why the DHCP requests from PC1 are not reaching R4.

In order to forward DHCP requests across a routed network, an IP helper address is required. The **ip helper-address** command is used to forward User Datagram Protocol (UDP) broadcasts to a remote server or device. DHCP requests use UDP broadcasts, so a device configured as an IP helper can intercept a DHCP request and forward it to a DHCP server on a remote subnet. The address lease process and other communications are then returned to the originating subnet.

Issuing the **show running-config** command on DS1 and DS2 indicates the absence of the **ip helper-address** command on both devices. DS2 is currently configured as the active gateway for virtual LAN (VLAN) 22; therefore, you should issue the **ip helper-address 192.168.99.4** command in interface configuration mode for VLAN 22 on DS2. DS1 is the standby gateway; therefore, it is not required that you issue the **ip helper-address** command on DS1 unless DS2 were to fail. You should not create an IP helper address on R5, because DHCP requests from clients on VLAN 22 will not forwarded across the routed network to reach R5.

You need not issue the **ip forward-protocol udp 68** command. The **ip forward-protocol** command is used to specify the UDP port numbers that should be forwarded by the **ip helper-address** command. By default, the **ip helper-address** command forwards broadcasts to the following UDP ports:

- 37 - Time Protocol
- 49 - Terminal Access Controller Access Control System (TACACS)
- 53 - Domain Name System (DNS)
- 67 - Bootstrap Protocol (BOOTP) and DHCP Server
- 68 - BOOTP and DHCP Client
- 69 - Trivial File Transfer Protocol (TFTP)
- 137 - Network Basic Input/Output System (NetBIOS) Name Service
- 138 - NetBIOS Datagram

Because DHCP client requests are already sent by the **ip helper-address** command, the **ip forward-protocol udp 68** command is unnecessary.

You need not create a new DHCP pool on any of the devices on the network. Creating a new DHCP pool on another device with the same address range can cause IP address conflicts to arise if both DHCP servers assign the same IP address to two different devices. The **ip dhcp pool** *pool-name* command creates a DHCP pool and enters DHCP configuration mode, in which you can configure various DHCP client options.

You should not modify the IP address range assigned by the DHCP pool. The DHCP pool must assign addresses from the 10.10.22.0/24 network so that DHCP clients in the Clients VLAN can receive IP addresses. The **network** *address* subnet command specifies the range of IP addresses that will be issued by DHCP.

You should not change the default router assigned by the DHCP pool. Clients in VLAN 22 should use the default gateway at 10.10.22.25, which is the shared gateway used by the Hot Standby Routing Protocol (HSRP) switches, DS1 and DS2. The **default-router** *address* command specifies the default gateway that is assigned to clients by the DHCP server.

You need not add a DNS server to the DHCP pool. DNS servers are used for domain name-to-IP address resolution. PC1 cannot ping the server 210.98.76.54 by its IP address, so a DNS server is unnecessary. The **dns-server** *address* command specifies the DNS server address that is assigned to clients by the DHCP server.

You should not modify the DHCP exclusion range on R4. A DHCP exclusion range is a range of addresses that should not be assigned to clients by the DHCP server. These addresses are typically static IP addresses that are assigned to servers and other network devices. The **ip dhcp excluded-address** *start-address end-address* command is used to exclude from DHCP the range of addresses from *start-address* through *end-address*. The **ip dhcp excluded-address 10.10.22.1 10.10.22.30** command that has already been issued on R4 is sufficient to exclude the statically assigned devices on the network.

Reference:
https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html#configdhcpbootpciscoios

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/