# Cisco

## Exam Questions 100-105

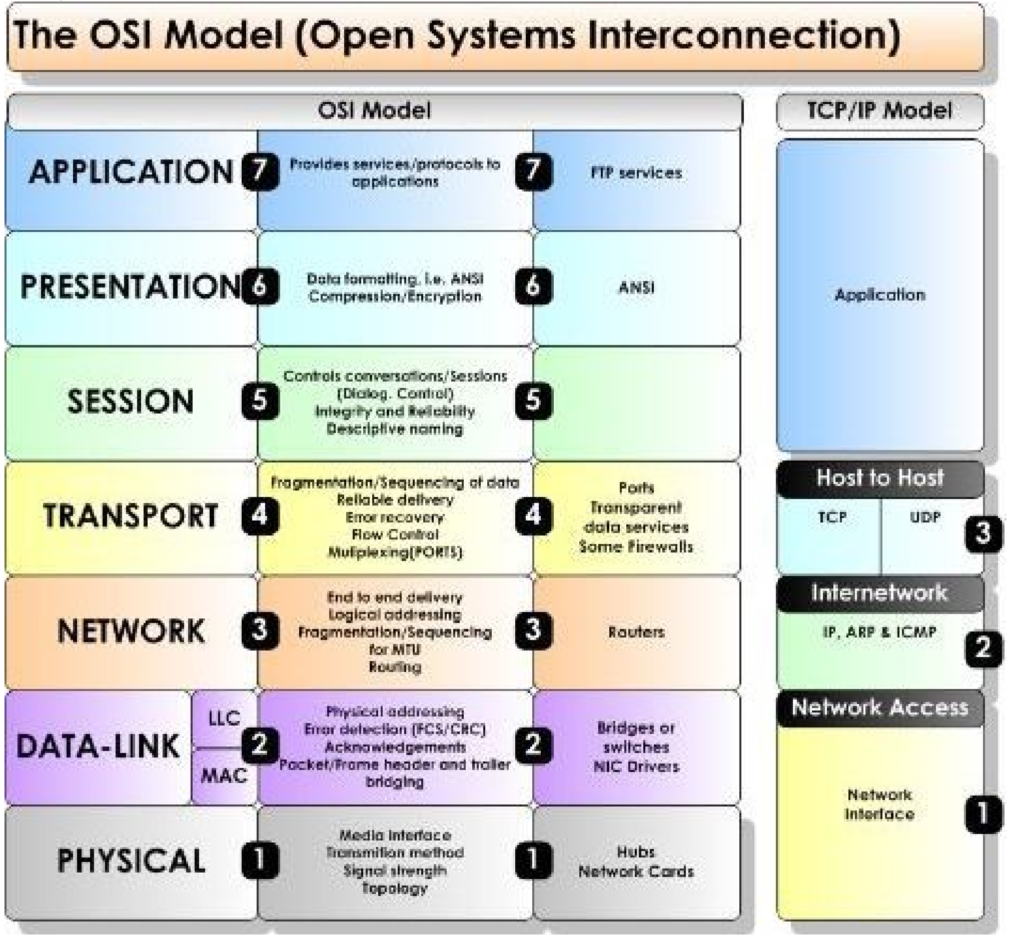
Cisco Interconnecting Cisco Networking Devices Part 1 (ICND1 v3.0)

**NEW QUESTION 1**
Which layer of the TCP/IP stack combines the OSI model physical and data link layers?

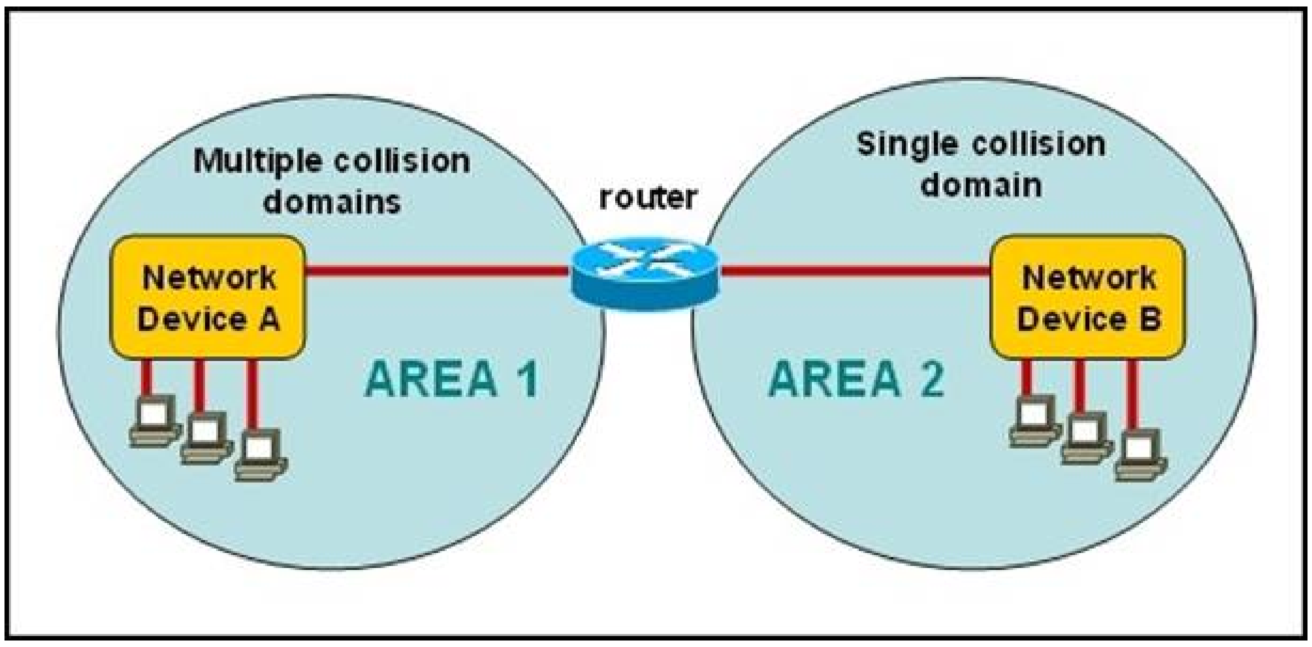
A. Internet layer
B. transport layer
C. application layer
D. network access layer

**Answer:** D

**Explanation:** The Internet Protocol Suite, TCP/IP, is a suite of protocols used for communication over the internet. The TCP/ IP model was created after the OSI 7 layer model for two major reasons. First, the foundation of the Internet was built using the TCP/IP suite and through the spread of the World Wide Web and Internet, TCP/IP has been preferred. Second, a project researched by the Department of Defense (DOD) consisted of creating the TCP/IP protocols. The DOD's goal was to bring international standards which could not be met by the OSI model.
Since the DOD was the largest software consumer and they preferred the TCP/IP suite, most vendors used this model rather than the OSI. Below is a side by side comparison of the TCP/IP and OSI models.


The OSI Model (Open Systems Interconnection)
OSI Model
APPLICATION 7
Provides services/protocols to applications
7
FTP services
PRESENTATION 6
Data formatting, i.e. ANSI Compression/Encryption
6
ANSI
SESSION 5
Controls conversations/Sessions (Dialog. Control) Integrity and Reliability Descriptive naming
5
TRANSPORT 4
Fragmentation/Sequencing of data Reliable delivery Error recovery Flow Control Mulipexing(PORTS)
4
Ports Transparent data services Some Firewalls
NETWORK 3
End to end delivery Logical addressing Fragmentation/Sequencing for MTU Routing
3
Routers
DATA-LINK
LLC
MAC
2
Physical addressing Error detection (FCS/CRC) Acknowledgements Packet/Frame header and trailer bridging
2
Bridges or switches NIC Drivers
PHYSICAL 1
Media interface Transmition method Signal strength Topology
1
Hubs Network Cards
TCP/IP Model
Application
Host to Host
TCP
UDP
3
Internetwork
IP, ARP & ICMP
2
Network Access
Network Interface
1

**NEW QUESTION 2**
Refer to the exhibit.



A network has been planned as shown. Which three statements accurately describe the areas and devices in the network plan? (Choose three.)

A. Network Device A is a switch.
B. Network Device B is a switch.
C. Network Device A is a hub.
D. Network Device B is a hub.
E. Area 1 contains a Layer 2 device.
F. Area 2 contains a Layer 2 device.

**Answer:** ADE

**Explanation:** Switches use a separate collision domain for each port, so device A must be a switch. Hubs, however, place all ports in the same collision domain so device B is a hub. Switches reside in layer 2 while hubs are layer 1 devices.

**NEW QUESTION 3**
At which layer of the OSI model does the protocol that provides the information that is displayed by the show cdp neighbors command operate?

A. application
B. transport
C. network
D. physical
E. data link

**Answer:** E

**Explanation:** CDP is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco- manufactured devices (routers, bridges, access servers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. With CDP, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices running lower-layer, transparent protocols.
CDP allows devices to share basic configuration information without even configuring any protocol specific information and is enabled by default on all interfaces.
CDP is a Datalink Protocol occurring at Layer 2 of the OSI model.
CDP is not routable and can only go over to directly connected devices.
CDP is enabled, by default, on all Cisco devices. CDP updates are generated as multicasts every 60 seconds with a hold-down period of 180 seconds for a missing neighbor. The no cdp run command globally disables CDP, while the no cdp enable command disables CDP on an interface. Use show cdp neighbors to list out your directly connected Cisco neighboring devices. Adding the detail parameter will display the layer-3 addressing configured on the neighbor.
Reference: http://computernetworkingnotes.com/cisco-devices-administration-and-configuration/cisco-discoveryprotocol.html

**NEW QUESTION 4**
Which layer of the OSI model controls the reliability of communications between network devices using flow control, sequencing and acknowledgments?

A. Physical
B. Data-link
C. Transport
D. Network

**Answer:** C

**NEW QUESTION 5**
Which transport layer protocol provides best-effort delivery service with no acknowledgment receipt required?

A. HTTP
B. IP
C. TCP
D. Telnet
E. UDP

**Answer:** E

**Explanation:** UDP provides a connectionless datagram service that offers best-effort delivery, which means that UDP does not guarantee delivery or verify sequencing for any datagrams. A source host that needs reliable communication must use either TCP or a program that
provides its own sequencing and acknowledgment services.

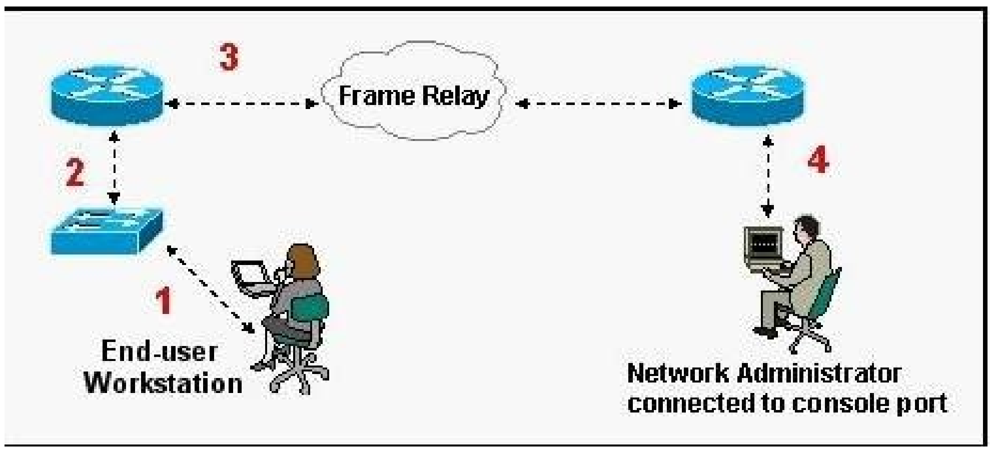
**NEW QUESTION 6**
What must occur before a workstation can exchange HTTP packets with a web server?

A. A UDP connection must be established between the workstation and its default gateway.
B. A UDP connection must be established between the workstation and the web server.
C. A TCP connection must be established between the workstation and its default gateway.
D. A TCP connection must be established between the workstation and the web server.
E. An ICMP connection must be established between the workstation and its default gateway.
F. An ICMP connection must be established between the workstation and the web server.

**Answer:** D

**Explanation:** HTTP uses TCP port 80, and a TCP port 80 connection must be established for HTTP communication to occur.
http://pentestlab.wordpress.com/2012/03/05/common-tcpip-ports/

**NEW QUESTION 7**
Refer to the exhibit.



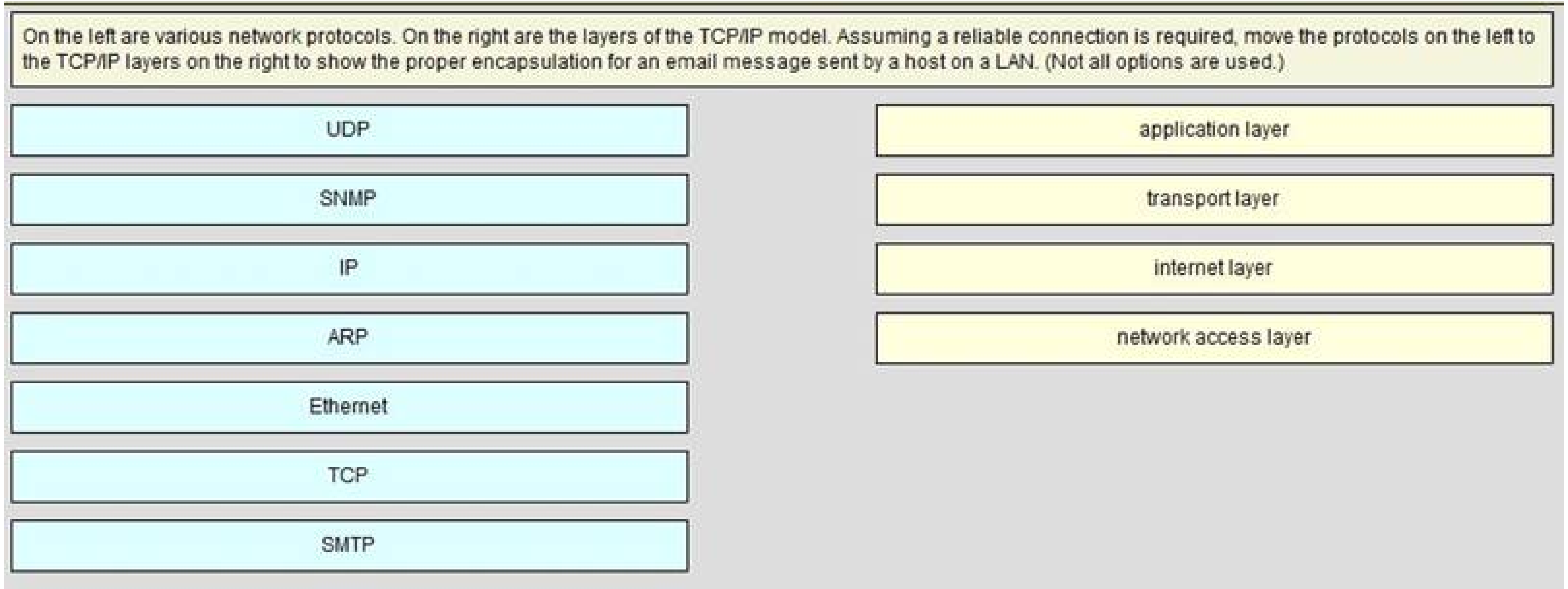
What kind of cable should be used to make each connection that is identified by the numbers shown?

A. 1 - Ethernet Crossover cable2 - Ethernet straight-through cable 3 - Fiber Optic cable4 - Rollover cable
B. 1 - Ethernet straight-through cable 2 - Ethernet straight-through cable3 - Serial cable4 - Rollover cable
C. 1 - Ethernet rollover cable 2 - Ethernet crossover cable 3 - Serial cable4 - Null-modem cable
D. 1 - Ethernet straight-through cable 2 - Ethernet Crossover cable3 - Serial cable4 - Rollover cable
E. 1 - Ethernet straight-through cable 2 - Ethernet Crossover cable3 - Serial cable4 - Ethernet Straight-through cable

**Answer:** B

**Explanation:** When connecting a PC to a switch, a standard Ethernet straight through cable should be used. This same cable should also be used for switch to router connections. Generally speaking, crossover cables are only needed when connecting two like devices (PC-PC, switch-switch, router-router, etc).
Routers connect to frame relay and other WAN networks using serial cables. Rollover cables are special cables used for connecting to the console ports of Cisco devices.

**NEW QUESTION 8**
DRAG DROP
On the left are various network protocols. On the right are the layers of the TCP/IP model. Assuming a reliable connection is required, move the protocols on the left to the TCP/IP layers on the right to show the proper encapsulation for an email message sent by a host on a LAN. (Not all options are used.)



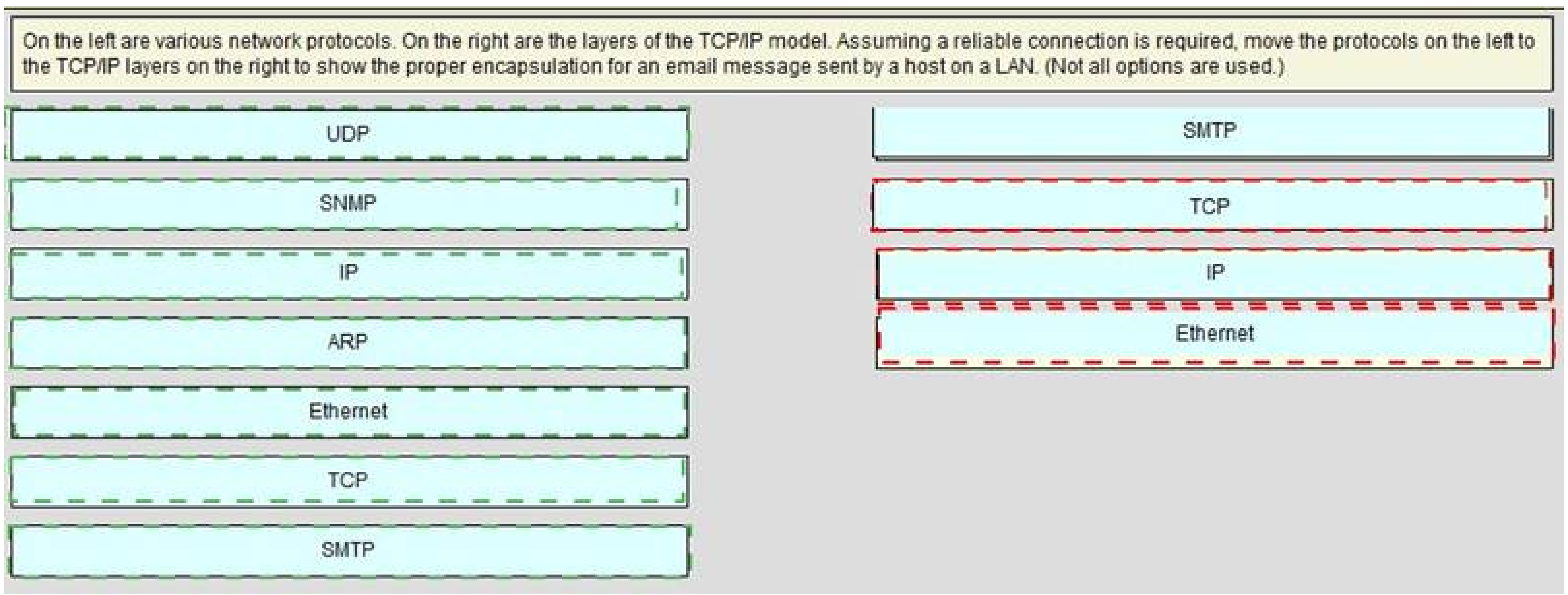
On the left are various network protocols. On the right are the layers of the TCP/IP model. Assuming a reliable connection is required, move the protocols on the left to the TCP/IP layers on the right to show the proper encapsulation for an email message sent by a host on a LAN. (Not all options are used.)

UDP
SNMP
IP
ARP
Ethernet
TCP
SMTP

application layer
transport layer
internet layer
network access layer

**Answer:**

**Explanation:**



On the left are various network protocols. On the right are the layers of the TCP/IP model. Assuming a reliable connection is required, move the protocols on the left to the TCP/IP layers on the right to show the proper encapsulation for an email message sent by a host on a LAN. (Not all options are used.)

UDP
SNMP
IP
ARP
Ethernet
TCP
SMTP

SMTP
TCP
IP
Ethernet

**NEW QUESTION 9**
Which two characteristics apply to Layer 2 switches? (Choose two.)

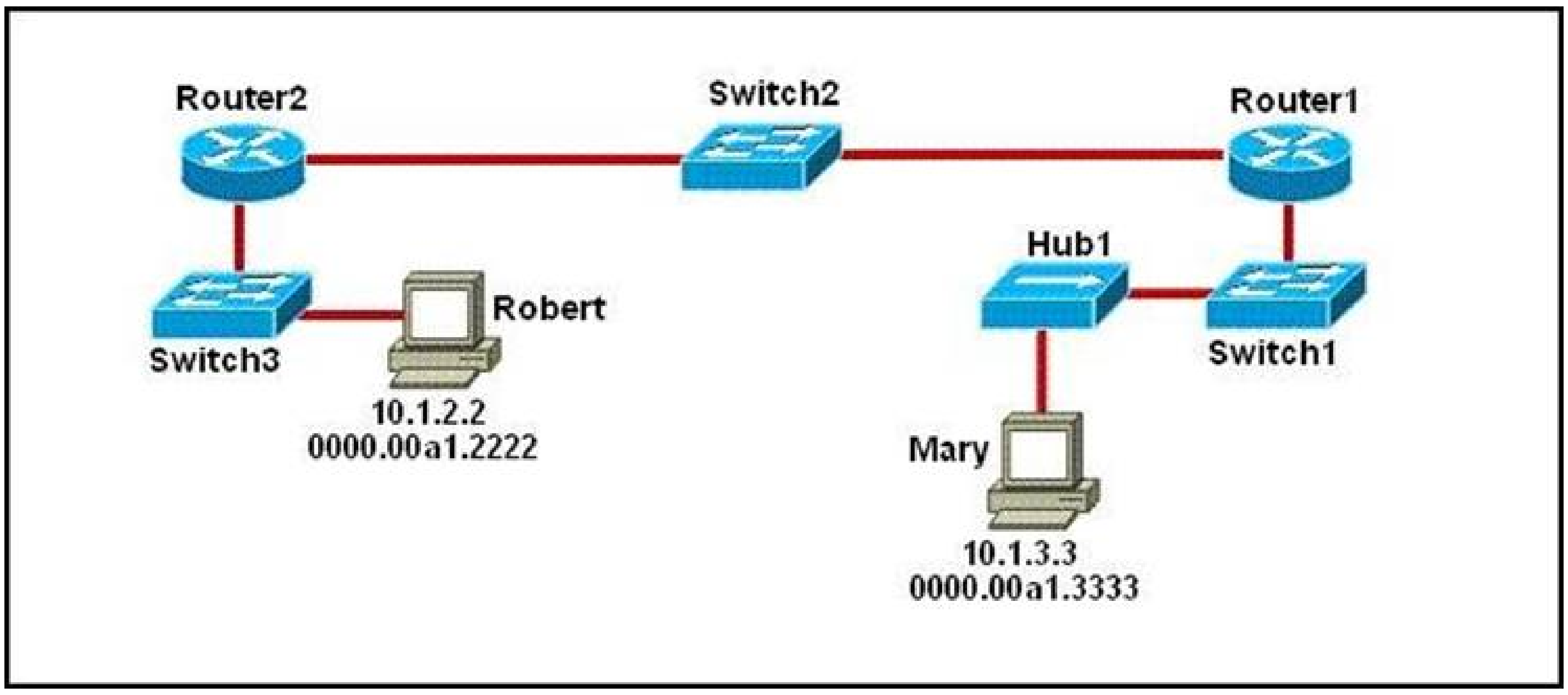
A. Increases the number of collision domains

B. Decreases the number of collision domains
C. Implements VLAN
D. Decreases the number of broadcast domains
E. Uses the IP address to make decisions for forwarding data packets

**Answer:** AC

**Explanation:** Layer 2 switches offer a number of benefits to hubs, such as the use of VLANs and each switch port is in its own separate collision domain, thus eliminating collisions on the segment.

**NEW QUESTION 10**
Refer to the exhibit.



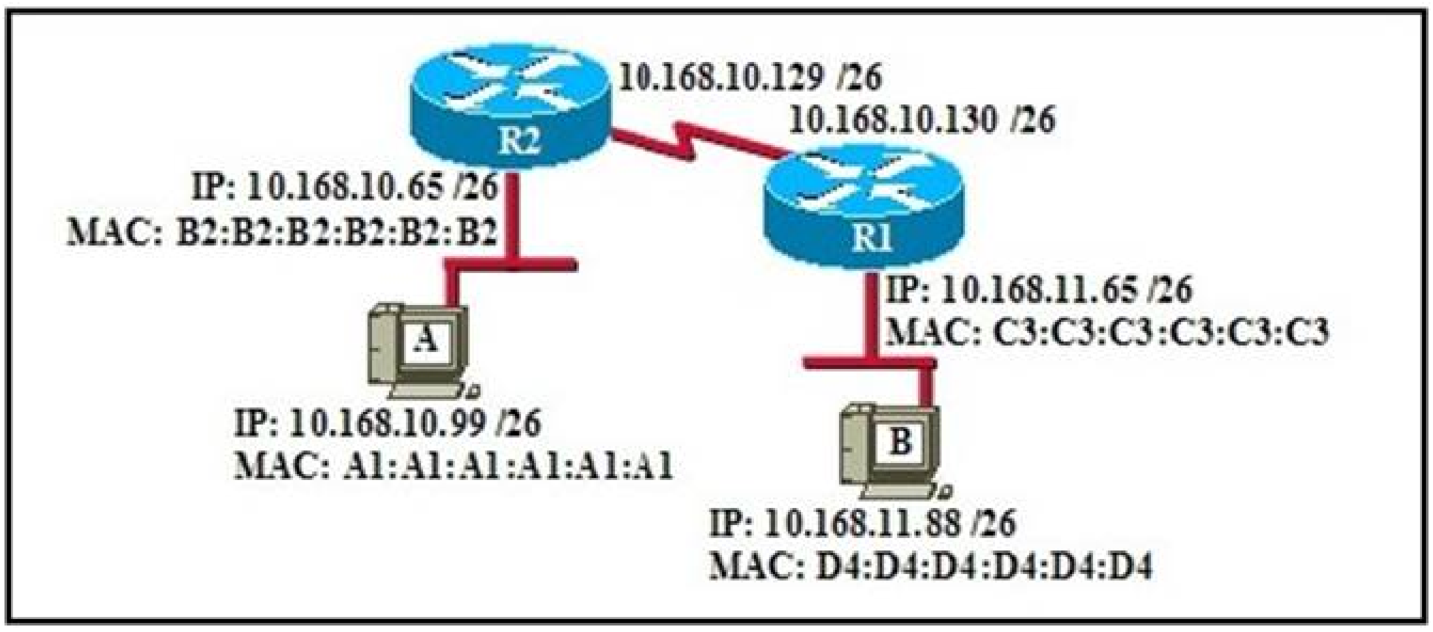
As packets travel from Mary to Robert, which three devices will use the destination MAC address of the packet to determine a forwarding path? (Choose three.)

A. Hub1
B. Switch1
C. Router1
D. Switch2
E. Router2
F. Switch3

**Answer:** BDF

**Explanation:** Switches use the destination MAC address information for forwarding traffic, while routers use the destination IP address information.
Local Area Networks employ Layer 2 Switches and Bridges to forward and filter network traffic. Switches and Bridges operate at the Data Link Layer of the Open System Interconnect Model (OSI). Since Switches and Bridges operate at the Layer 2 they operate more intelligently than hubs, which work at Layer 1 (Physical Layer) of the OSI. Because the switches and bridges are able to listen to the traffic on the wire to examine the source and destination MAC address. Being able to listen to the traffic also allows the switches and bridges to compile a MAC address table to better filter and forward network traffic.
To accomplish the above functions switches and bridges carry out the following tasks: MAC address learning by a switch or a bridge is accomplished by the same method. The switch or bridge listens to each device connected to each of its ports and scan the incoming frame for the source MAC address. This creates a MAC address to port map that is cataloged in the switches/bridge MAC database. Another name for the MAC address table is content addressable memory or CAM table.
When a switch or bridge is listening to the network traffic, it receives each frame and compares it to the MAC address table. By checking the MAC table the switch/ bridge are able o determine which port the frame came in on. If the frame is on the MAC table the frame is filtered or transmitted on only that port. If the switch determines that the frame is not on the MAC table, the frame is forwarded out to all ports except the incoming port.

**NEW QUESTION 10**
Refer to the exhibit.



If host A sends an IP packet to host B, what will the source physical address be in the frame when it reaches host B?

A. 10.168.10.99
B. 10.168.11.88
C. A1:A1:A1:A1:A1:A1
D. B2:B2:B2:B2:B2:B2
E. C3:C3:C3:C3:C3:C3
F. D4:D4:D4:D4:D4:D4

**Answer:** E

**Explanation:** When packets transfer from one host to another across a routed segment, the source IP address always remains the same source IP address, and the source physical (MAC) address will be the existing router's interface address. Similarly, the destination IP address always remains the same and the destination physical (MAC) address is the destination router's interface address.

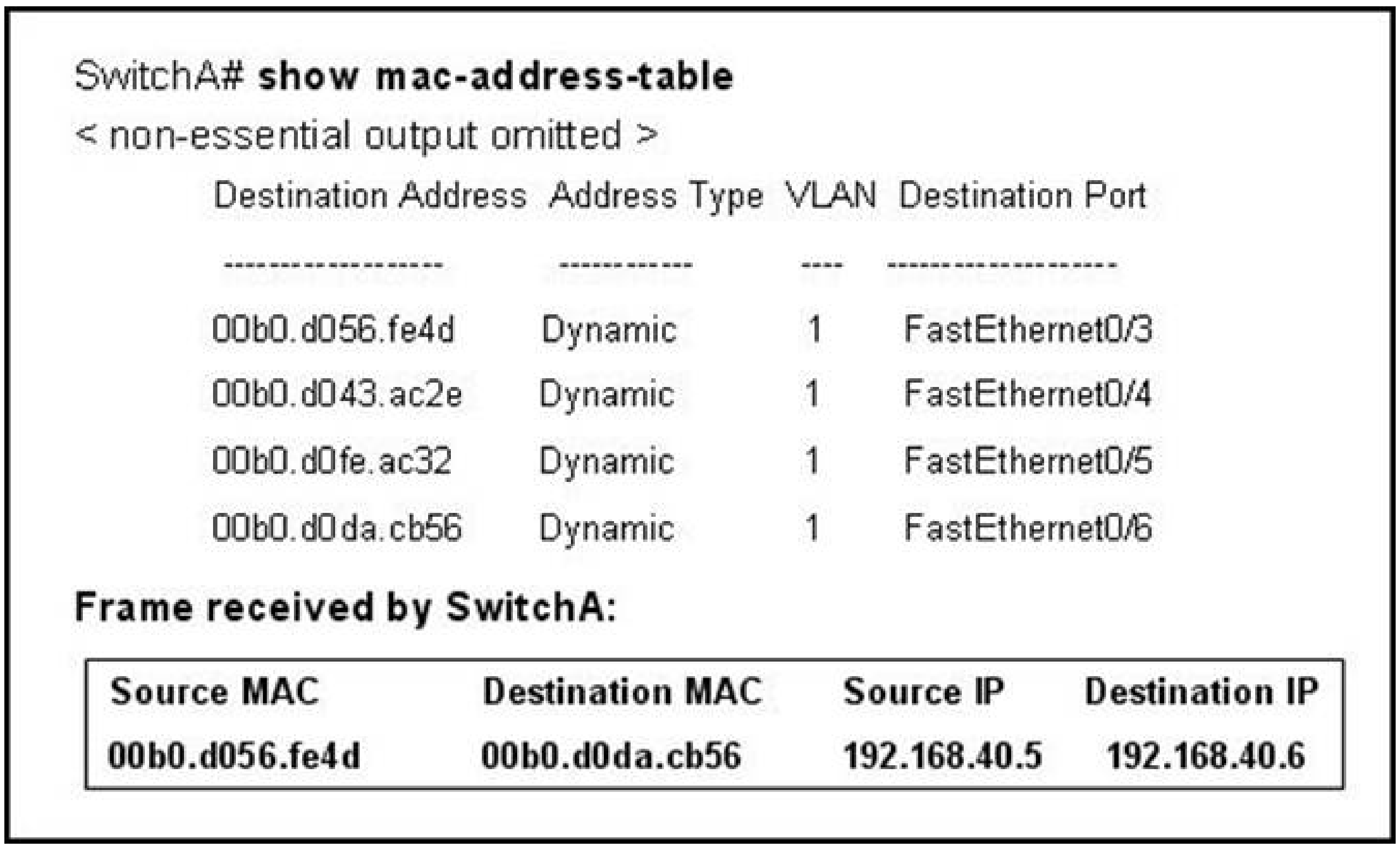
**NEW QUESTION 14**
Which of the following are types of flow control? (Choose three.)

A. buffering
B. cut-through
C. windowing
D. congestion avoidance
E. load balancing

**Answer:** ACD

**Explanation:** During Transfer of data, a high speed computer is generating data traffic a lot faster than the network device can handle in transferring to destination, so single gateway or destination device cannot handle much amount of traffic that is called "Congestion". Buffering
The Technie is used to control the data transfer when we have congestion, when a network device receive a data it stores in memory section and then transfer to next destination this process called "Buffering".
Windowing Whereas Windowing is used for flow control by the Transport layer.
Say the sender device is sending segments and the receiver device can accommodate only a fixed number of segments before it can accept more, the two devices negotiate the window size during the connection setup.
This is done so that the sending device doesn't overflow the receiving device's buffer. Also the receiving device can send a single acknowledgement for the segments it has received instead of sending an acknowledgement after every segment received.
Also, this window size is dynamic meaning, the devices can negotiate and change the window size in the middle of a session. So if initially the window size is three and the receiving device thinks that it can accept more number of segments in its buffer it can negotiate with the sending device and it increases it to say 5 for example.
Windowing is used only by TCP since UDP doesn't use or allow flow control. Reference: http://www.info-it.net/cisco/ccna/exam-tips/flow-control.php

**NEW QUESTION 19**
Refer to the exhibit.



```
SwitchA# show mac-address-table
< non-essential output omitted >
        Destination Address  Address Type  VLAN  Destination Port
        -------------------  ------------  ----  --------------------
        00b0.d056.fe4d       Dynamic        1     FastEthernet0/3
        00b0.d043.ac2e       Dynamic        1     FastEthernet0/4
        00b0.d0fe.ac32       Dynamic        1     FastEthernet0/5
        00b0.d0da.cb56       Dynamic        1     FastEthernet0/6
```

**Frame received by SwitchA:**

| Source MAC | Destination MAC | Source IP | Destination IP |
|---|---|---|---|
| 00b0.d056.fe4d | 00b0.d0da.cb56 | 192.168.40.5 | 192.168.40.6 |

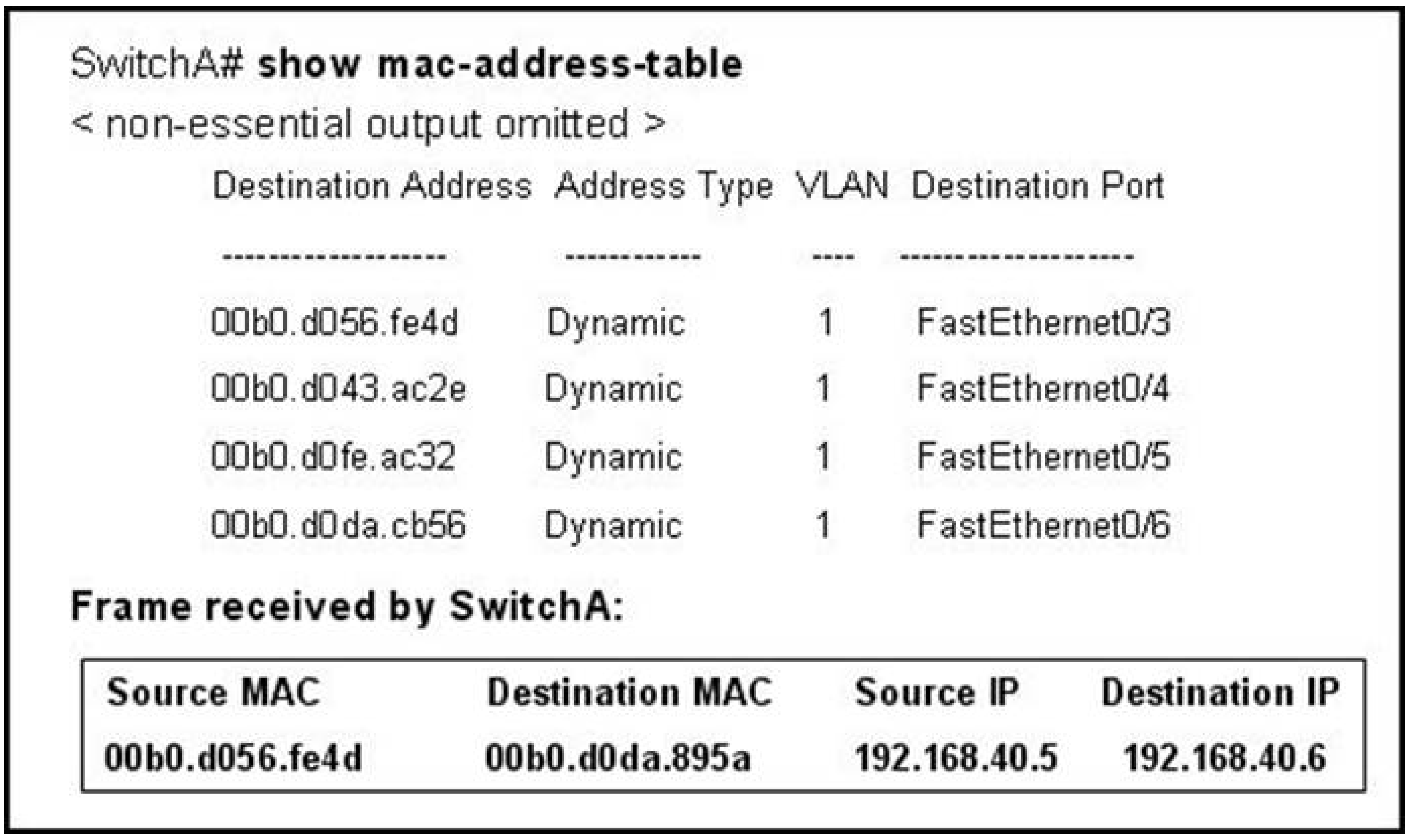
SwitchA receives the frame with the addressing shown. According to the command output also shown in the exhibit, how will SwitchA handle this frame?

A. It will drop the frame.
B. It will forward the frame out port Fa0/6 only.
C. It will flood the frame out all ports.
D. It will flood the frame out all ports except Fa0/3.

**Answer:** B

**Explanation:** Switches keep the learned MAC addresses in a table, so that when a frame comes in with a destination MAC address that the switch has already learned, it will forward it to that port only. If a frame comes in with a destination MAC that is not already in the MAC address table, then the frame will be flooded to all ports except for the one that it came in on. In this case, Switch A already knows that 00b0.d0da.cb56 resides on port fa0/6, so it will forward the from out that port.

**NEW QUESTION 23**
Refer to the exhibit.



```
SwitchA# show mac-address-table
< non-essential output omitted >
        Destination Address  Address Type  VLAN  Destination Port
        -------------------  ------------  ----  -------------------
        00b0.d056.fe4d       Dynamic       1     FastEthernet0/3
        00b0.d043.ac2e       Dynamic       1     FastEthernet0/4
        00b0.d0fe.ac32       Dynamic       1     FastEthernet0/5
        00b0.d0da.cb56       Dynamic       1     FastEthernet0/6
```

**Frame received by SwitchA:**

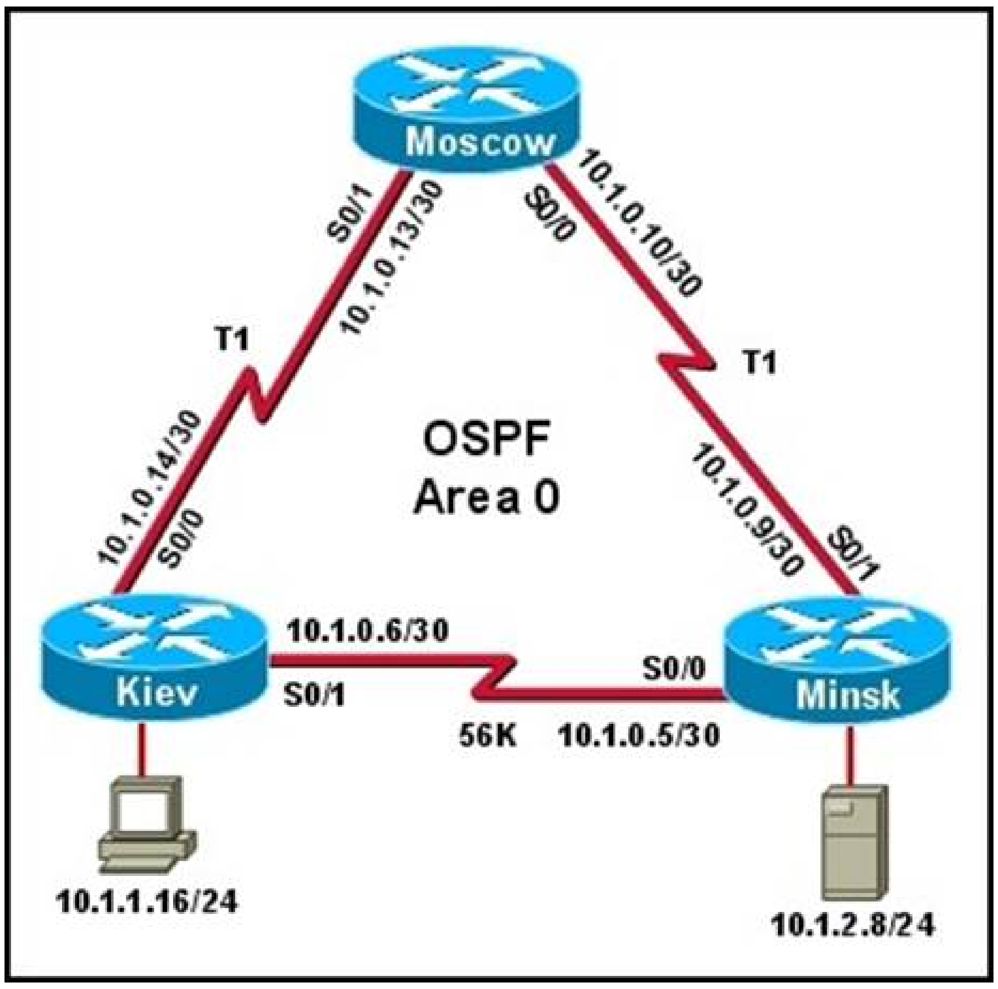
| Source MAC | Destination MAC | Source IP | Destination IP |
|---|---|---|---|
| 00b0.d056.fe4d | 00b0.d0da.895a | 192.168.40.5 | 192.168.40.6 |

Which option describes how SwitchA will handle the frame just received?

A. It will drop the frame.
B. It will forward the frame out of port Fa0/3 only.
C. It will flood the frame out all ports.
D. It will flood the frame out of all the ports except Fa0/3.

**Answer:** D

**NEW QUESTION 25**
Refer to the exhibit.



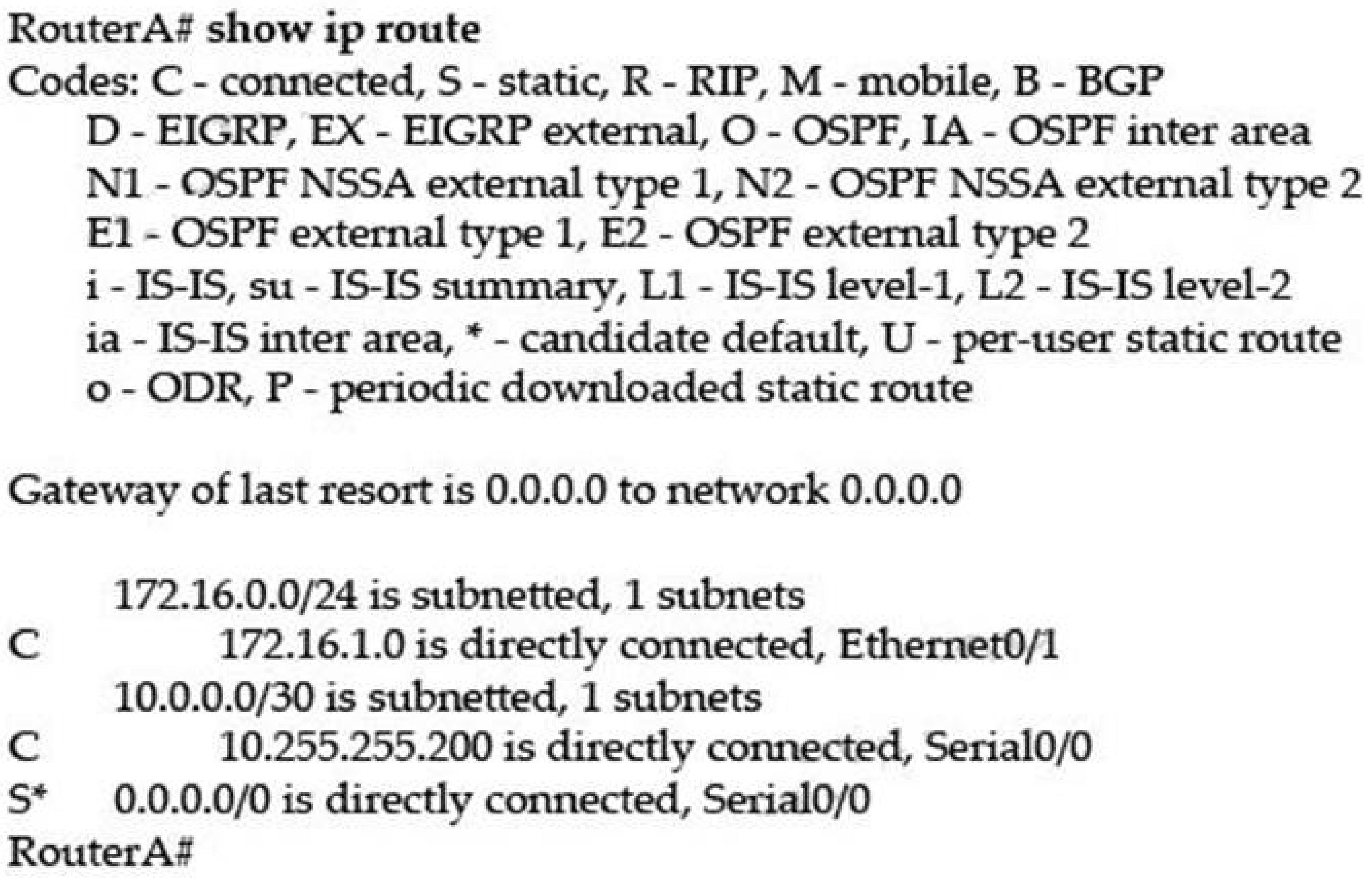
The host in Kiev sends a request for an HTML document to the server in Minsk. What will be the source IP address of the packet as it leaves the Kiev router?

A. 10.1.0.1
B. 10.1.0.5
C. 10.1.0.6
D. 10.1.0.14
E. 10.1.1.16
F. 10.1.2.8

**Answer:** E

**Explanation:** Although the source and destination MAC address will change as a packet traverses a network, the source and destination IP address will not unless network address translation (NAT) is being done, which is not the case here.

**NEW QUESTION 30**
Refer to the exhibit.



```
RouterA# show ip route
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 0.0.0.0 to network 0.0.0.0

        172.16.0.0/24 is subnetted, 1 subnets
C           172.16.1.0 is directly connected, Ethernet0/1
        10.0.0.0/30 is subnetted, 1 subnets
C           10.255.255.200 is directly connected, Serial0/0
S*      0.0.0.0/0 is directly connected, Serial0/0
RouterA#
```

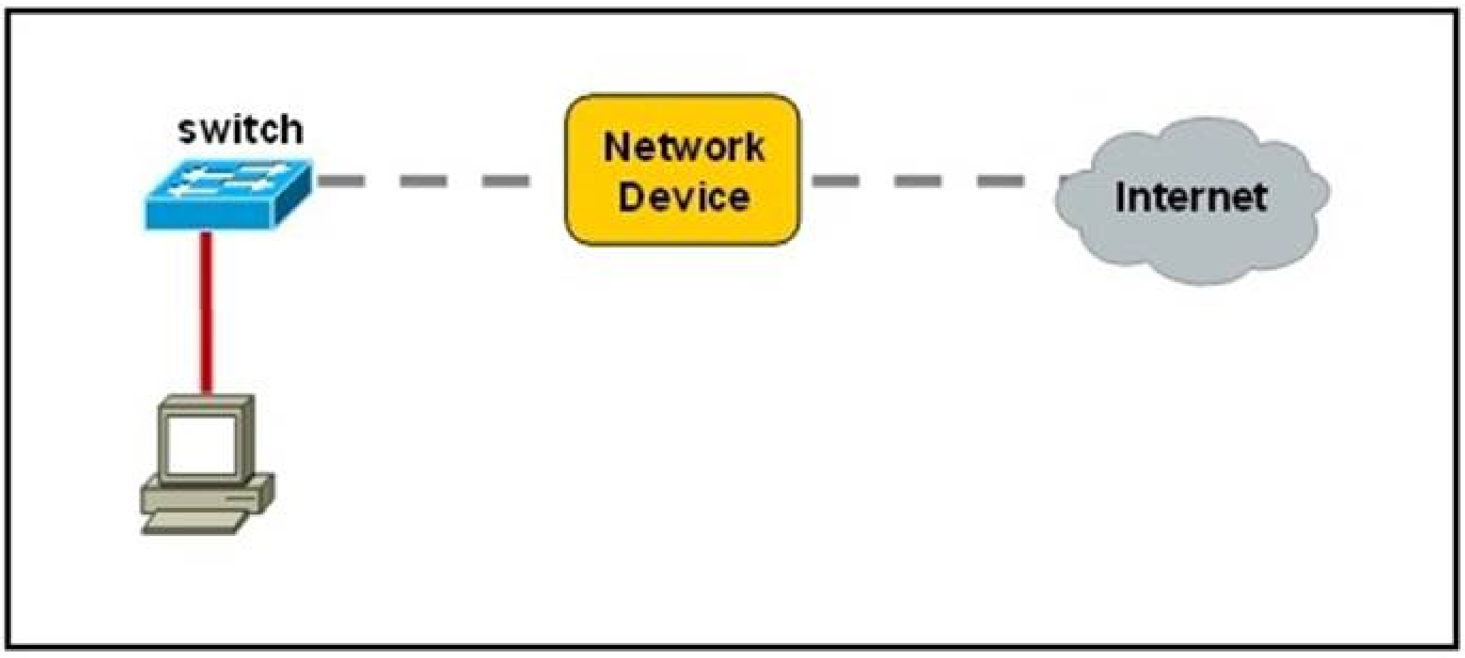
The output is from a router in a large enterprise. From the output, determine the role of the router.

A. ACore router.
B. The HQ Internet gateway router.
C. The WAN router at the central site.
D. Remote stub router at a remote site.

**Answer:** D

**Explanation:** Since the routing table shows only a single default route using the single interface serial 0/0, we know that this is most likely a remote stub site with a single connection to the rest of the network. All the other answer options would mean that this router would have more connections, and would contain more routes.

**NEW QUESTION 34**
Refer to the exhibit.



A network device needs to be installed in the place of the icon labeled Network Device to accommodate a leased line attachment to the Internet. Which network device and interface configuration meets the minimum requirements for this installation?

A. a router with two Ethernet interfaces
B. a switch with two Ethernet interfaces
C. a router with one Ethernet and one serial interface
D. a switch with one Ethernet and one serial interface
E. a router with one Ethernet and one modem interface

**Answer:** C

**Explanation:** Only a router can terminate a leased line attachment access circuit, and only a router can connect two different IP networks. Here, we will need a router with two interfaces, one serial connection for the line attachment and one Ethernet interface to connect to the switch on the LAN.

**NEW QUESTION 39**

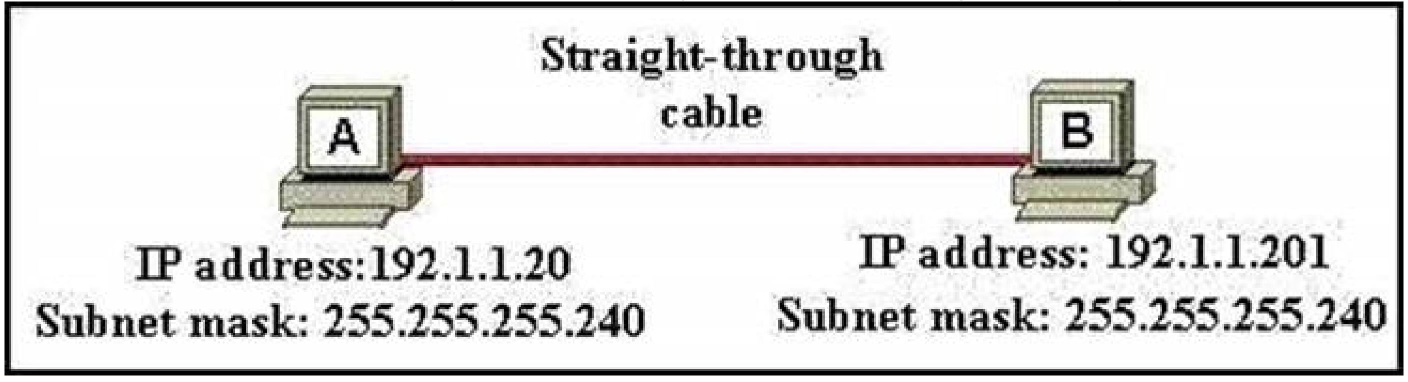
A workstation has just resolved a browser URL to the IP address of a server. What protocol will the workstation now use to determine the destination MAC address to be placed into frames directed toward the server?

A. HTTP
B. DNS
C. DHCP
D. RARP
E. ARP

**Answer:** E

**Explanation:** The RARP protocol is used to translate hardware interface addresses to protocol addresses. The RARP message format is very similar to the ARP format. When the booting computer sends the broadcast ARP request, it places its own hardware address in both the sending and receiving fields in the encapsulated ARP data packet. The RARP server will fill in the correct sending and receiving IP addresses in its response to the message. This way the booting computer will know its IP address when it gets the message from the RARP server

**NEW QUESTION 40**
A network administrator is connecting PC hosts A and B directly through their Ethernet interfaces as shown in the graphic. Ping attempts between the hosts are unsuccessful. What can be done to provide connectivity between the hosts? (Choose two.)



A. A crossover cable should be used in place of the straight-through cable.
B. A rollover cable should be used in place of the straight-through cable.
C. The subnet masks should be set to 255.255.255.192
D. A default gateway needs to be set on each host.
E. The hosts must be reconfigured to use private IP addresses for direct connections of this type.
F. The subnet masks should be set to 255.255.255.0

**Answer:** AF

**Explanation:** If you need to connect two computers but you don't have access to a network and can't set up an ad hoc network, you can use an Ethernet crossover cable to create a direct cable connection.
Generally speaking, a crossover cable is constructed by reversing (or crossing over) the order of the wires inside so that it can connect two computers directly. A crossover cable looks almost exactly like a regular Ethernet cable (a straight-through cable), so make sure you have a crossover cable before following these steps.
Both devices need to be on the same subnet, and since one PC is using 192.1.1.20 and the other is using 192.1.1.201, the subnet mask should be changed to 255.255.255.0.

**NEW QUESTION 43**
How does a switch differ from a hub?

A. A switch does not induce any latency into the frame transfer time.
B. A switch tracks MAC addresses of directly-connected devices.
C. A switch operates at a lower, more efficient layer of the OSI model.
D. A switch decreases the number of broadcast domains.
E. A switch decreases the number of collision domains.

**Answer:** B

**Explanation:** Some of the features and functions of a switch include:
A switch is essentially a fast, multi-port bridge, which can contain dozens of ports. Rather than creating two collision domains, each port creates its own collision domain.
In a network of twenty nodes, twenty collision domains exist if each node is plugged into its own switch port.
If an uplink port is included, one switch creates twenty-one single-node collision domains. A switch dynamically builds and maintains a Content-Addressable Memory (CAM) table, holding all of the necessary MAC information for each port.
For a detailed description of how switches operate, and their key differences to hubs, see
the reference link below.
Reference: http://www.cisco.com/warp/public/473/lan-switch-cisco.shtml

**NEW QUESTION 44**
Which statements are true regarding ICMP packets? (Choose two.)

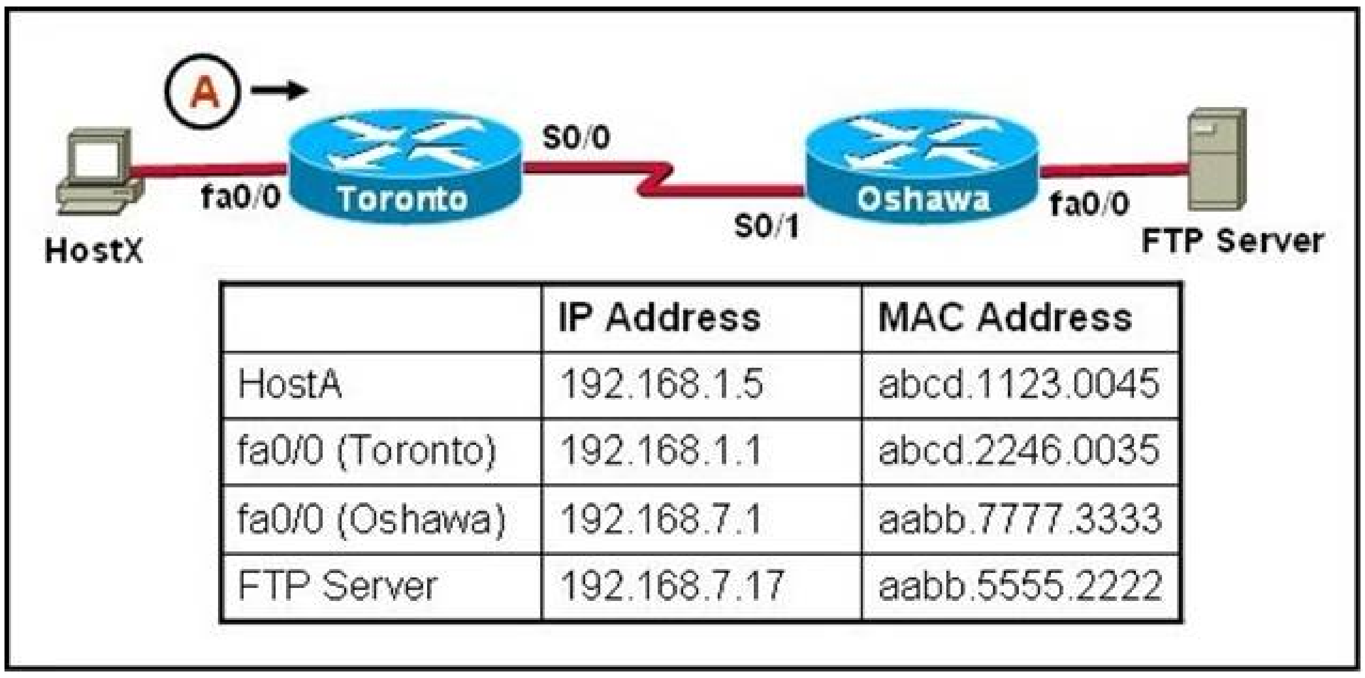
A. They acknowledge receipt of TCP segments.
B. They guarantee datagram delivery.
C. TRACERT uses ICMP packets.
D. They are encapsulated within IP datagrams.

E. They are encapsulated within UDP datagrams.

**Answer:** CD

**Explanation:** Ping may be used to find out whether the local machines are connected to the network or whether a remote site is reachable. This tool is a common network tool for determining the network connectivity, which uses ICMP protocol instead of TCP/IP and UDP/IP. This protocol is usually associated with the network management tools, which provide network information to network administrators, such as ping and traceroute (the later also uses the UDP/IP protocol). ICMP is quite different from the TCP/IP and UDP/IP protocols. No source and destination ports are included in its packets. Therefore, usual packet-filtering rules for TCP/IP and UDP/IP are not applicable. Fortunately, a special "signature" known as the packet's Message type is included for denoting the purposes of the ICMP packet. Most commonly used message types are namely, 0, 3, 4, 5, 8, 11, and 12 which represent echo reply, destination unreachable, source quench, redirect, echo request, time exceeded, and parameter problem respectively.
In the ping service, after receiving the ICMP "echo request" packet from the source location, the destination

**NEW QUESTION 45**
Refer to the exhibit.



| | IP Address | MAC Address |
|---|---|---|
| HostA | 192.168.1.5 | abcd.1123.0045 |
| fa0/0 (Toronto) | 192.168.1.1 | abcd.2246.0035 |
| fa0/0 (Oshawa) | 192.168.7.1 | aabb.7777.3333 |
| FTP Server | 192.168.7.17 | aabb.5555.2222 |

HostX is transferring a file to the FTP server. Point A represents the frame as it goes toward the Toronto router. What will the Layer 2 destination address be at this point?

A. abcd.1123.0045
B. 192.168.7.17
C. aabb.5555.2222
D. 192.168.1.1
E. abcd.2246.0035

**Answer:** E

**Explanation:** For packets destined to a host on another IP network, the destination MAC address will be the LAN interface of the router. Since the FTP server lies on a different network, the host will know to send the frame to its default gateway, which is Toronto.

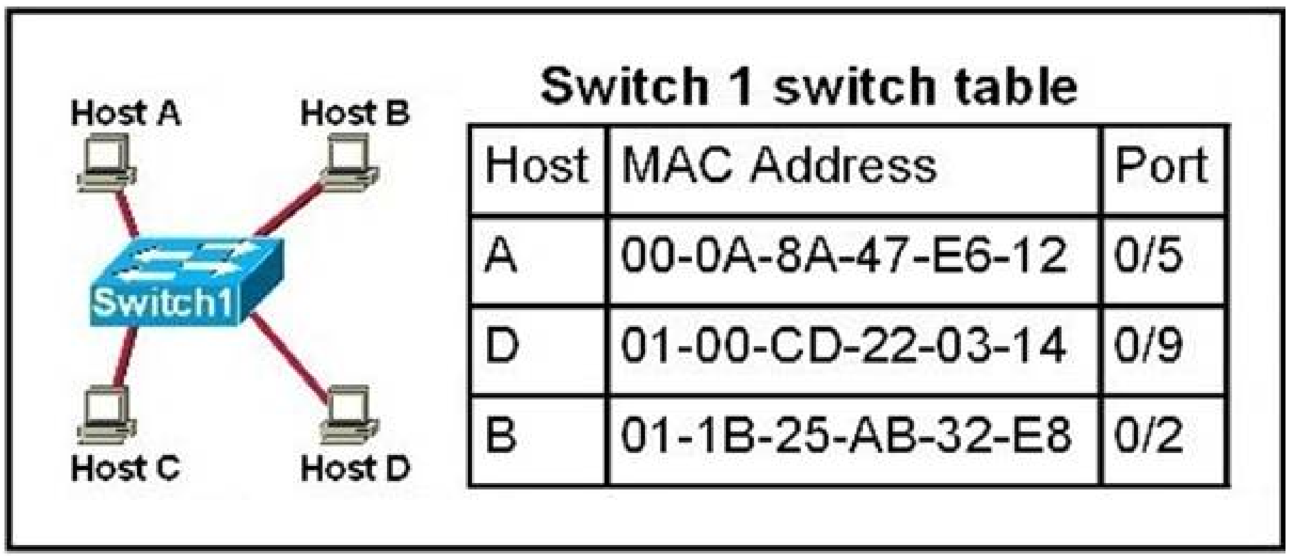
**NEW QUESTION 46**
Which two characteristics describe the access layer of the hierarchical network design model? (Choose two.)

A. layer 3 support
B. port security
C. redundant components
D. VLANs
E. PoE

**Answer:** BD

**Explanation:** Access layer
The main purpose of the access layer is to provide direct connection to devices on the network and controlling which devices are allowed to communicate over it. The access layer interfaces with end devices, such as PCs, printers, and IP phones, to provide access to the rest of the network. The access layer can include routers, switches, bridges, hubs, and wireless access points (AP).
Switch features in the Access layer:
? Port security
? VLANs
? Fast Ethernet/Gigabit Ethernet
? Power over Ethernet (PoE)
? Link aggregation
? Quality of Service (QoS)
References: http://www.ciscopath.com/content/61/ http://www.mcmcse.com/cisco/guides/hierarchical_model.shtml

**NEW QUESTION 48**
Refer to the topology and switching table shown in the graphic.



Switch 1 switch table

| Host | MAC Address | Port |
|---|---|---|
| A | 00-0A-8A-47-E6-12 | 0/5 |
| D | 01-00-CD-22-03-14 | 0/9 |
| B | 01-1B-25-AB-32-E8 | 0/2 |

Host B sends a frame to Host C. What will the switch do with the frame?

A. Drop the frame
B. Send the frame out all ports except port 0/2
C. Return the frame to Host B
D. Send an ARP request for Host C
E. Send an ICMP Host Unreachable message to Host B
F. Record the destination MAC address in the switching table and send the frame directly to Host C

**Answer:** B

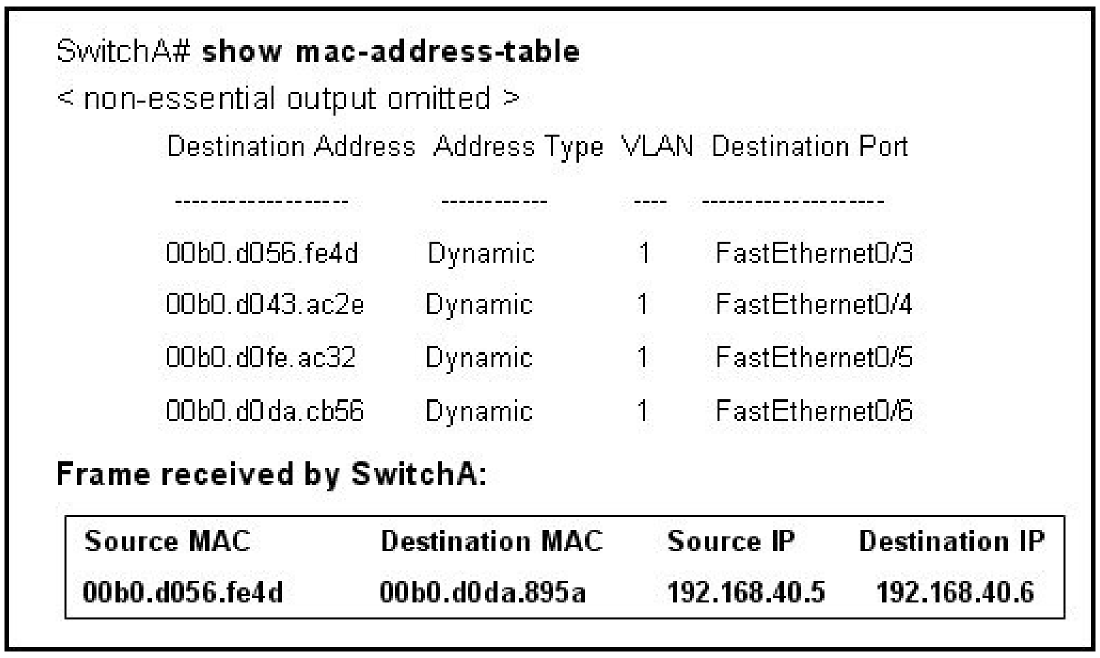
**NEW QUESTION 52**
Which two statements describe the operation of the CSMA/CD access method? (Choose two.)

A. In a CSMA/CD collision domain, multiple stations can successfully transmit data simultaneously.
B. In a CSMA/CD collision domain, stations must wait until the media is not in use before transmitting.
C. The use of hubs to enlarge the size of collision domains is one way to improve the operation of the CSMA/CD access method.
D. After a collision, the station that detected the collision has first priority to resend the lost data.
E. After a collision, all stations run a random backoff algorith
F. When the backoff delay period has expired, all stations have equal priority to transmit data.
G. After a collision, all stations involved run an identical backoff algorithm and then synchronize with each other prior to transmitting data.

**Answer:** BE

**Explanation:** Ethernet networking uses Carrier Sense Multiple Access with Collision Detect (CSMA/CD), a protocol that helps devices share the bandwidth evenly without having two devices transmit at the same time on the network medium. CSMA/CD was created to overcome the problem of those collisions that occur when packets are transmitted simultaneously from different nodes. And trust me, good collision management is crucial, because when a node transmits in a CSMA/CD network, all the other nodes on the network receive and examine that transmission. Only bridges and routers can effectively prevent a transmission from propagating throughout the entire network! So, how does the CSMA/CD protocol work? Like this: when a host wants to transmit over the network, it first checks for the presence of a digital signal on the wire. If all is clear (no other host is transmitting), the host will then proceed with its transmission. But it doesn’t stop there. The transmitting host constantly monitors the wire to make sure no other hosts begin transmitting. If the host detects another signal on the wire, it sends out an extended jam signal that causes all nodes on the segment to stop sending data (think, busy signal). The nodes respond to that jam signal by waiting a while before attempting to transmit again. Backoff algorithms determine when the colliding stations can retransmit. If collisions keep occurring after 15 tries, the nodes attempting to transmit will then time out.

**NEW QUESTION 54**
Refer to the exhibit.



```
SwitchA# show mac-address-table
< non-essential output omitted >
        Destination Address  Address Type  VLAN  Destination Port
        -------------------  ------------  ----  --------------------
        00b0.d056.fe4d       Dynamic       1     FastEthernet0/3
        00b0.d043.ac2e       Dynamic       1     FastEthernet0/4
        00b0.d0fe.ac32       Dynamic       1     FastEthernet0/5
        00b0.d0da.cb56       Dynamic       1     FastEthernet0/6
```

Frame received by SwitchA:

| Source MAC | Destination MAC | Source IP | Destination IP |
|---|---|---|---|
| 00b0.d056.fe4d | 00b0.d0da.895a | 192.168.40.5 | 192.168.40.6 |

SwitchA receives the frame with the addressing shown in the exhibit. According to the command output also shown in the exhibit, how will SwitchA handle this frame?

A. It will drop the frame.
B. It will forward the frame out port Fa0/6 only.
C. It will forward the frame out port Fa0/3 only.
D. It will flood the frame out all ports.
E. It will flood the frame out all ports except Fa0/3.

**Answer:** E

**Explanation:** When frame receives the frame, it checks the source address on MAC table if MAC address found in MAC table it tries to forward if not in MAC table adds the Address on MAC table. After checking the source address, it checks the destination address on MAC table, if MAC address found on MAC table it forwards to proper ports otherwise floods on all ports except the source port.

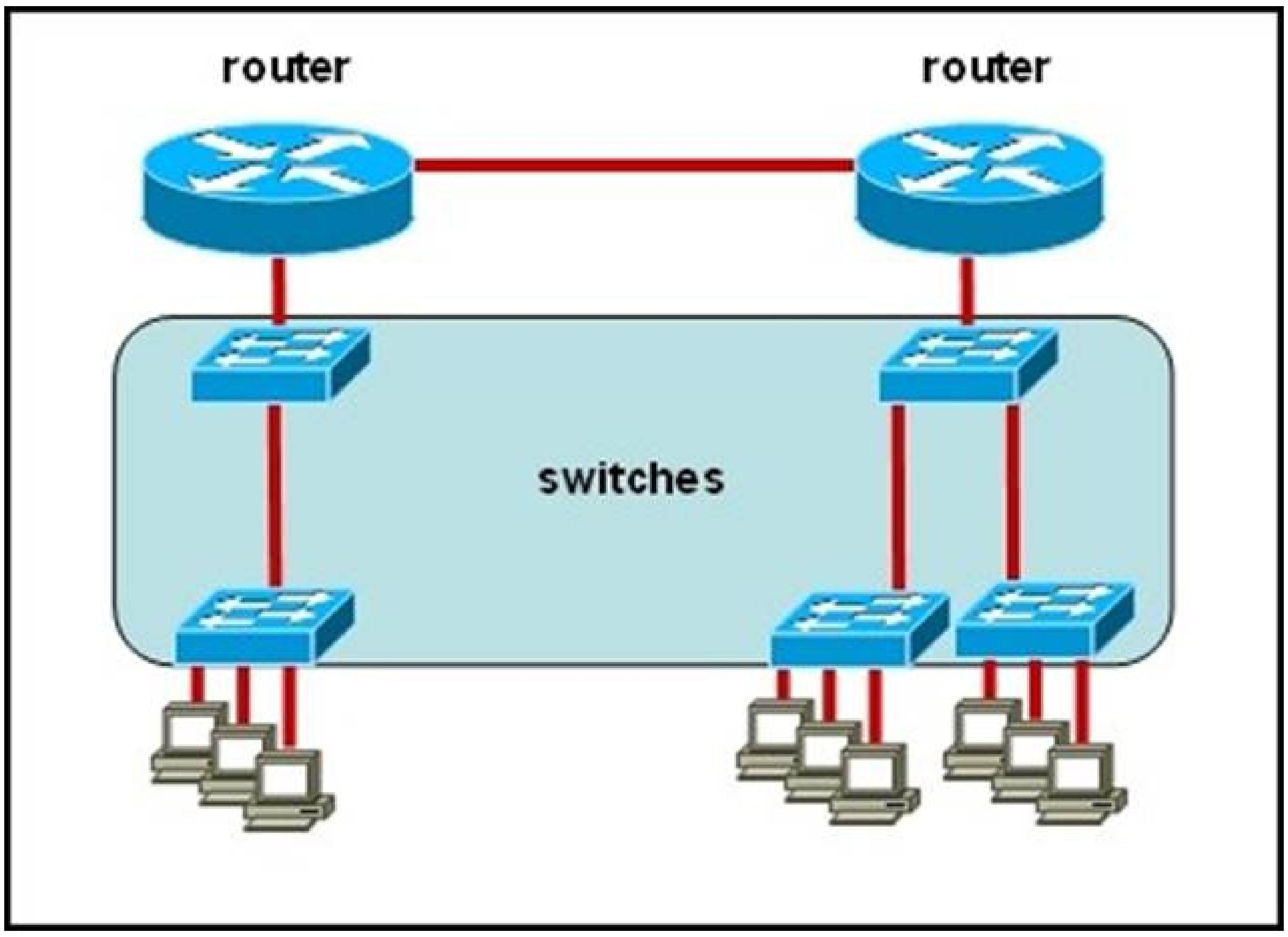
**NEW QUESTION 57**
On a Cisco switch, which protocol determines if an attached VoIP phone is from Cisco or from another vendor?

A. RTP
B. TCP
C. CDP
D. UDP

**Answer:** C

**Explanation:** The Cisco Unified IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Cisco Discovery Protocol (CDP) is a proprietary protocol designed by Cisco to help administrators collect information about both locally attached and remote devices. By using CDP, you can gather hardware and protocol information about neighbor devices, which is useful info for troubleshooting the network.
CDP messages are generated every 60 seconds as multicast messages on each of its active interfaces.
The information shared in a CDP packet about a Cisco device includes the following: Name of the device configured with the hostname command
IOS software version
Hardware capabilities, such as routing, switching, and/or bridging Hardware platform, such as 2600, 2950, or 1900
The layer-3 address(es) of the device
The interface the CDP update was generated on
Reference: http://computernetworkingnotes.com/cisco-devices-administration-and-configuration/cisco-discoveryprotocol.html

**NEW QUESTION 59**
Refer to the exhibit.



All devices attached to the network are shown. How many collision domains are present in this network?

A. 2
B. 3
C. 6
D. 9
E. 15

**Answer:** E

**Explanation:** A switch uses a separate collision domain for each port so there are a total of 9 for each device shown. In addition to this, the switch to switch connections (3) are a separate collision domain. Finally, we add the switch to router connections (2) and the router to router connection (1) for a total of 15.

**NEW QUESTION 61**
A switch receives a frame on one of its ports. There is no entry in the MAC address table for the destination MAC address. What will the switch do with the frame?

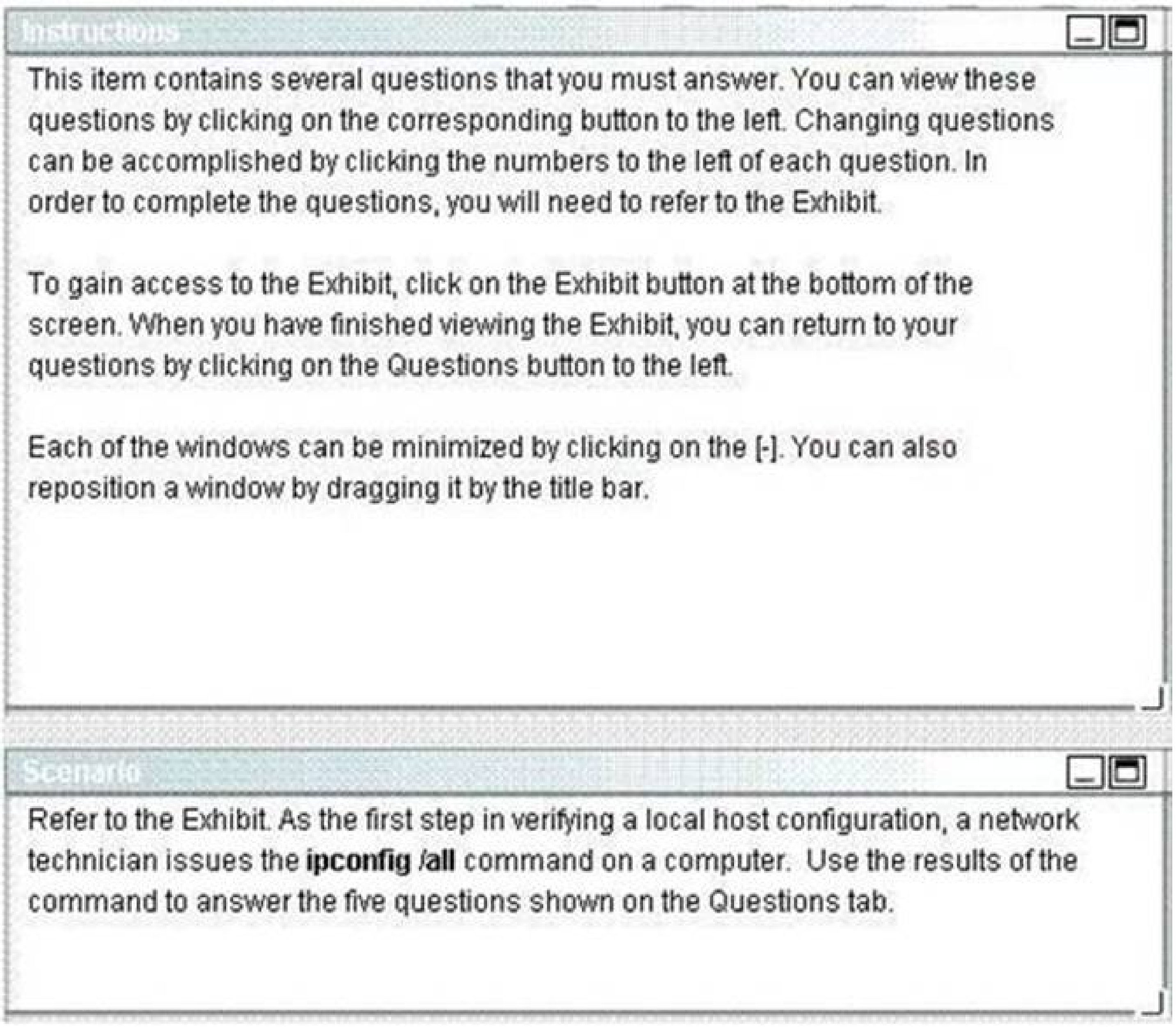
A. drop the frame

B. forward it out of all ports except the one that received it
C. forward it out of all ports
D. store it until it learns the correct port

**Answer:** B

**Explanation:** Understanding this concept is prime for understanding that when switch receives the data frame from the host not having the MAC address already in the MAC table, it will add the MAC address to the source port on the MAC address table and sends the data frame. If the switch already has the MAC address in its table for the destination, it will forward the frame directly to the destination port. If it was not already in its MAC table, then they frame would have been flooded out all ports except for the port that it came from.

**NEW QUESTION 62**
Refer to the exhibit.

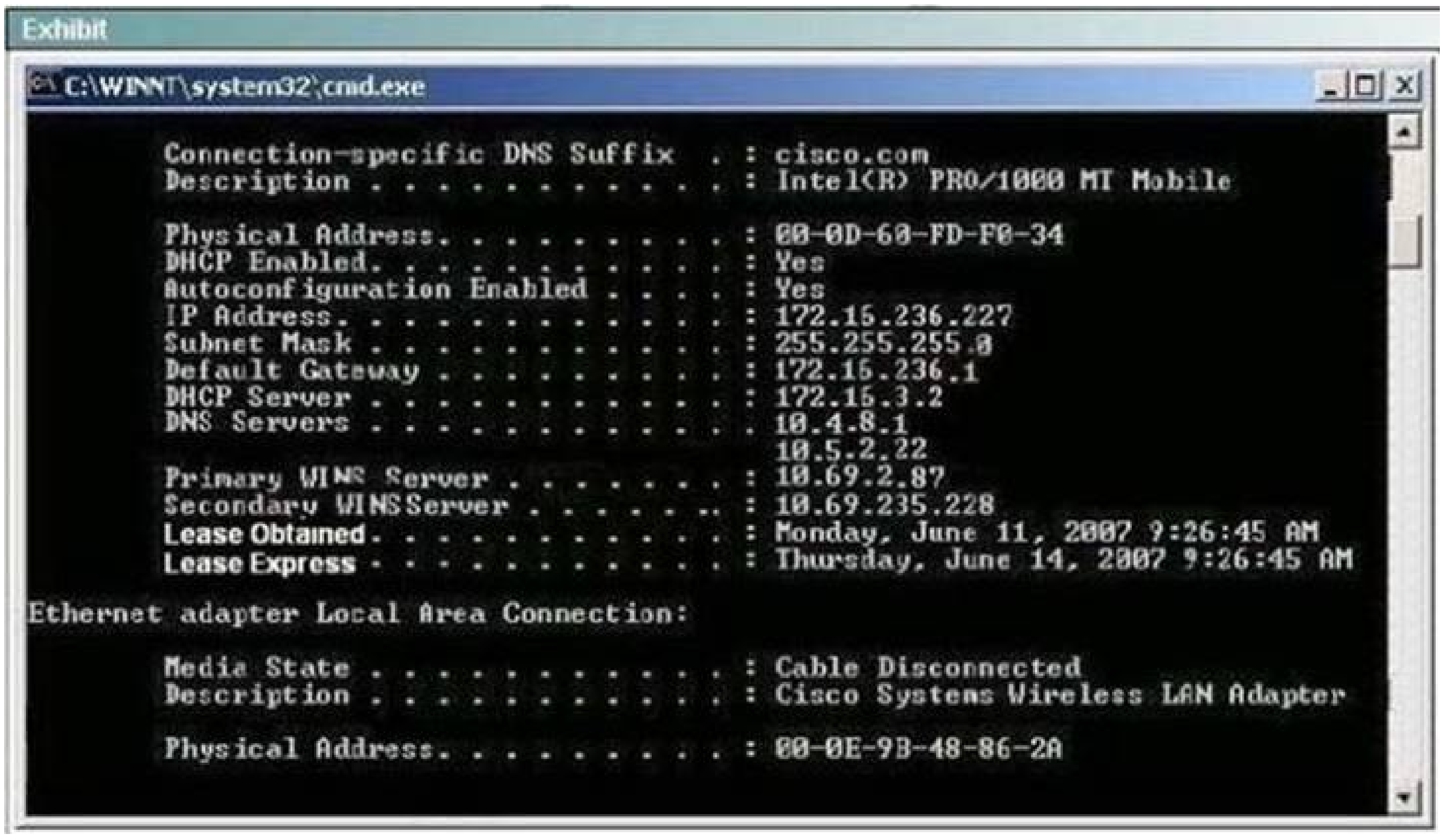


This item contains several questions that you must answer. You can view these questions by clicking on the corresponding button to the left. Changing questions can be accomplished by clicking the numbers to the left of each question. In order to complete the questions, you will need to refer to the Exhibit.

To gain access to the Exhibit, click on the Exhibit button at the bottom of the screen. When you have finished viewing the Exhibit, you can return to your questions by clicking on the Questions button to the left.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

Refer to the Exhibit. As the first step in verifying a local host configuration, a network technician issues the **ipconfig /all** command on a computer. Use the results of the command to answer the five questions shown on the Questions tab.



```
        Connection-specific DNS Suffix  . : cisco.com
        Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Mobile

        Physical Address. . . . . . . . . : 00-0D-60-FD-F0-34
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 172.16.236.227
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.236.1
        DHCP Server . . . . . . . . . . . : 172.16.3.2
        DNS Servers . . . . . . . . . . . . 10.4.8.1
                                            10.5.2.22
        Primary WINS Server . . . . . . . : 10.69.2.87
        Secondary WINSServer . . . . . .. : 10.69.235.228
        Lease Obtained. . . . . . . . . . : Monday, June 11, 2007 9:26:45 AM
        Lease Express - . . . . . . . . . : Thursday, June 14, 2007 9:26:45 AM

Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Cable Disconnected
        Description . . . . . . . . . . . : Cisco Systems Wireless LAN Adapter

        Physical Address. . . . . . . . . : 00-0E-9B-48-86-2A
```

What two things can the technician determine by successfully pinging from this computer to the IP address 172.16.236.1? (Choose two)

A. The network card on the computer is functioning correctly.
B. The default static route on the gateway router is correctly configured.
C. The correct default gateway IP address is configured on the computer.
D. The device with the IP address 172.16.236.1 is reachable over the network.

E. The default gateway at 172.16.236.1 is able to forward packets to the internet.

**Answer:** AD

**Explanation:** The source and destination addresses are on the same network therefore, a default gateway is not necessary for communication between these two addresses.

**NEW QUESTION 64**
Which address type does a switch use to make selective forwarding decisions?

A. Source IP address
B. Destination IP address
C. Source and destination IP address
D. Source MAC address
E. Destination MAC address

**Answer:** E

**Explanation:** Switches analyze the destination MAC to make its forwarding decision since it is a layer 2 device. Routers use the destination IP address to make forwarding decisions.

**NEW QUESTION 69**
What is the purpose of flow control?

A. To ensure data is retransmitted if an acknowledgement is not received.
B. To reassemble segments in the correct order at the destination device.
C. To provide a means for the receiver to govern the amount of data sent by the sender.
D. To regulate the size of each segment.

**Answer:** C

**Explanation:** Flow control is the management of data flow between computers or devices or between nodes in a network so that the data can be handled at an efficient pace. Too much data arriving before a device can handle it causes data overflow, meaning the data is either lost or must be retransmitted. For serial data transmission locally or in a network, the Xon/Xoff protocol can be used. For modem connections, either Xon/Xoff or CTS/RTS (Clear to Send/Ready to Send) commands can be used to control data flow.
In a network, flow control can also be applied by refusing additional device connections until the flow of traffic has subsided.
Reference: http://whatis.techtarget.com/definition/flow-control

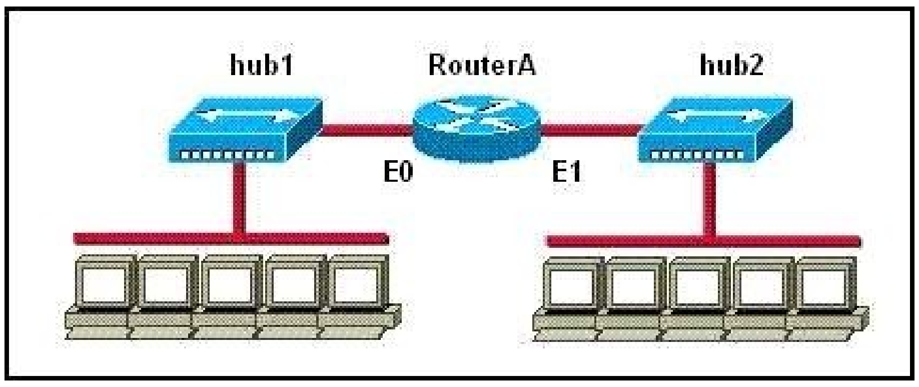
**NEW QUESTION 72**
What does a host on an Ethernet network do when it is creating a frame and it does not have the destination address?

A. Drops the frame
B. Sends out a Layer 3 broadcast message
C. Sends a message to the router requesting the address
D. Sends out an ARP request with the destination IP address

**Answer:** D

**Explanation:** In this case, it will send out an ARP request for MAC address of the destination IP (assuming it doesn't already have it in its table) and then address it to the destination's MAC address.

**NEW QUESTION 75**
Refer to the exhibit.



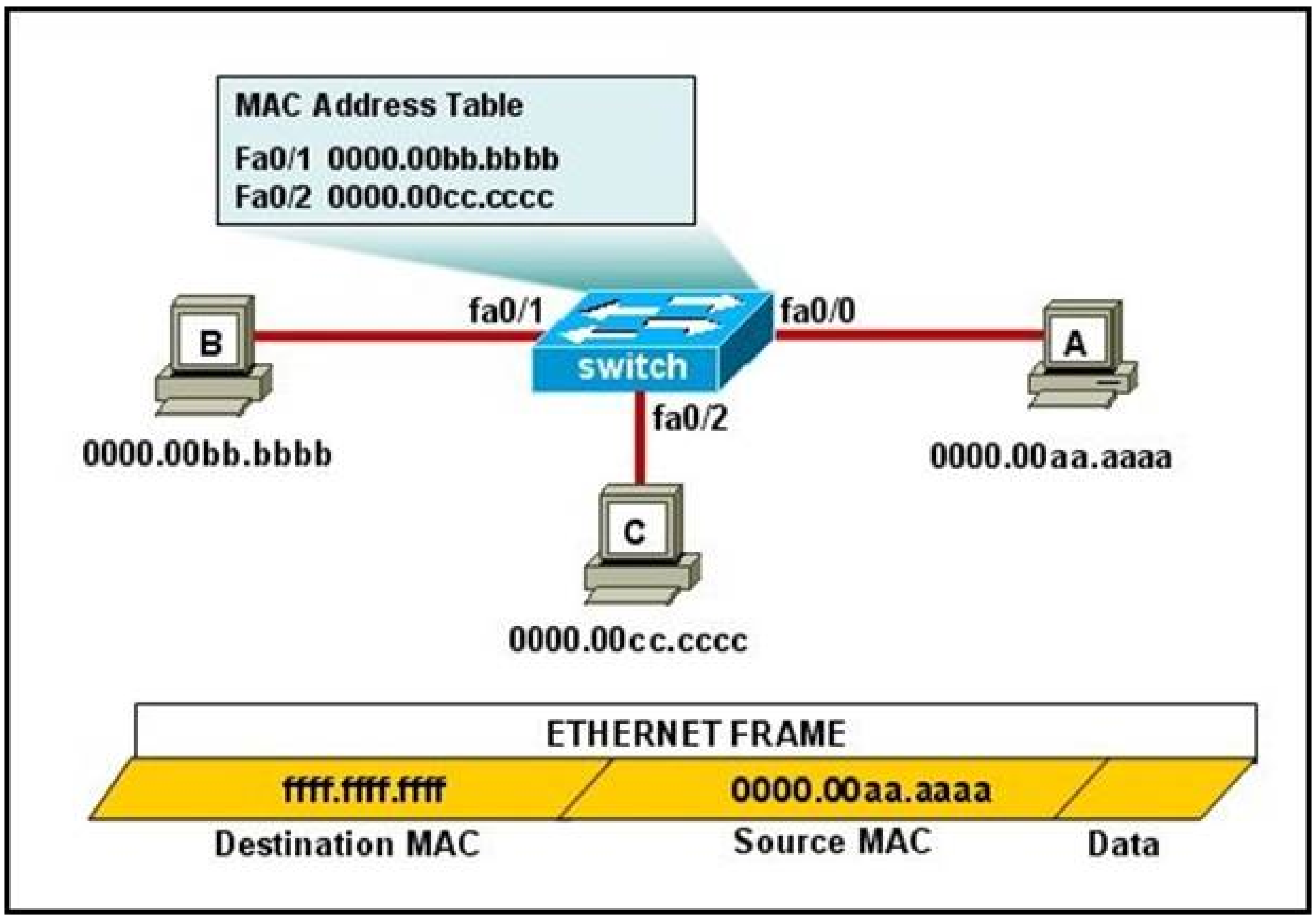
How many collision domains are shown?

A. one
B. two
C. three
D. four
E. six
F. twelve

**Answer:** B

**Explanation:** Hubs create single collision and broadcast domains, so in this case there will be a single collision domain for each of the two hubs.

**NEW QUESTION 77**
Refer to the exhibit.



The MAC address table is shown in its entirety. The Ethernet frame that is shown arrives at the switch.
What two operations will the switch perform when it receives this frame? (Choose two.)

A. The switch will not forward a frame with this destination MAC address.
B. The MAC address of 0000.00aa.aaaa will be added to the MAC Address Table.
C. The MAC address of ffff.ffff.ffff will be added to the MAC address table.
D. The frame will be forwarded out of all the active switch ports except for port fa0/0.
E. The frame will be forwarded out of fa0/0 and fa0/1 only.
F. The frame will be forwarded out of all the ports on the switch.

**Answer:** BD

**Explanation:** If the switch already has the MAC address in its table for the destination, it will forward the frame directly to the destination port. If it was not already in its MAC table, then they frame would have been flooded out all ports except for the port that it came from.

**NEW QUESTION 82**
A switch has 48 ports and 4 VLANs. How many collision and broadcast domains exist on the switch (collision, broadcast)?

A. 4, 48
B. 48, 4
C. 48, 1
D. 1, 48
E. 4, 1

**Answer:** B

**Explanation:** A switch uses a separate collision domain for each port, and each VLAN is a separate broadcast domain.

Topic 3, Routing Fundamentals

**NEW QUESTION 84**
Which IP addresses are valid for hosts belonging to the 10.1.160.0/20 subnet? (Choose three.)

A. 10.1.168.0
B. 10.1.176.1
C. 10.1.174.255
D. 10.1.160.255
E. 10.1.160.0
F. 10.1.175.255

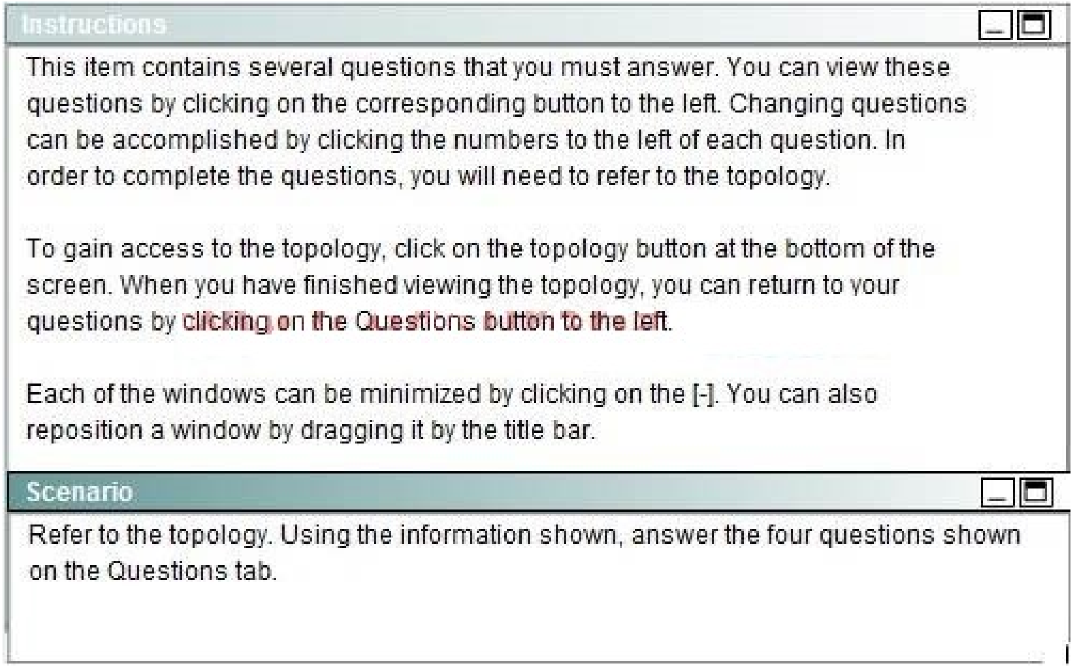
**Answer:** ACD

**Explanation:** All IP address in IP ranges between: 10.1.160.1 and 10.1.175.254 are valid as shown below
Address: 10.1.160.0 00001010.00000001.1010 0000.00000000
Netmask: 255.255.240.0 = 20 11111111.11111111.1111 0000.00000000
Wildcard: 0.0.15.255 00000000.00000000.0000 1111.11111111
Which implies that:

Network: 10.1.160.0/20 00001010.00000001.1010 0000.00000000
HostMin: 10.1.160.1 00001010.00000001.1010 0000.00000001
HostMax: 10.1.175.254 00001010.00000001.1010 1111.11111110
Broadcast: 10.1.175.255 00001010.00000001.1010 1111.11111111

**NEW QUESTION 87**

To allow or prevent load balancing to network 172.16.3.0/24, which of the following commands could be used in R2? (Choose two.)

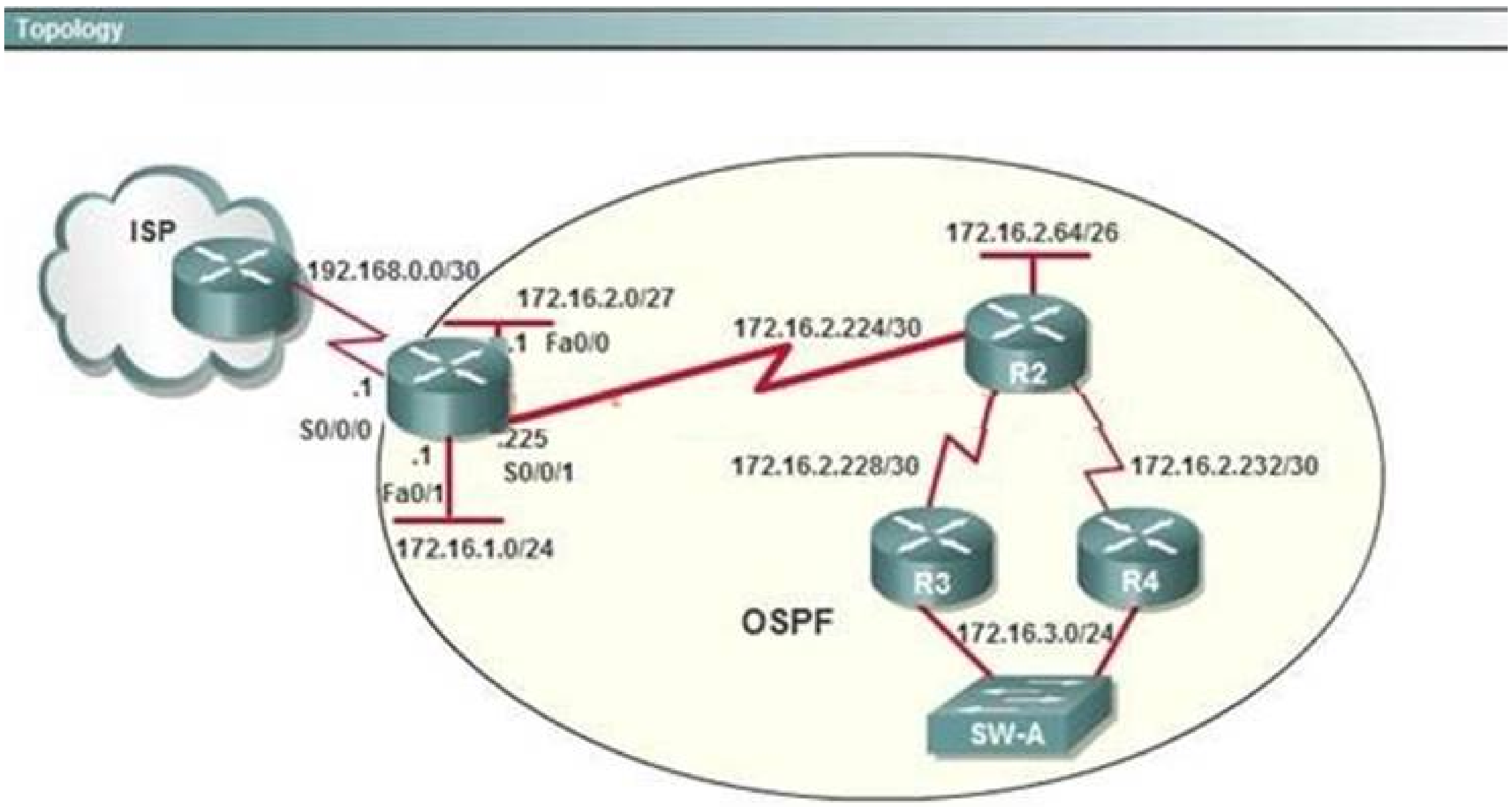


This item contains several questions that you must answer. You can view these questions by clicking on the corresponding button to the left. Changing questions can be accomplished by clicking the numbers to the left of each question. In order to complete the questions, you will need to refer to the topology.

To gain access to the topology, click on the topology button at the bottom of the screen. When you have finished viewing the topology, you can return to your questions by clicking on the Questions button to the left.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

Refer to the topology. Using the information shown, answer the four questions shown on the Questions tab.



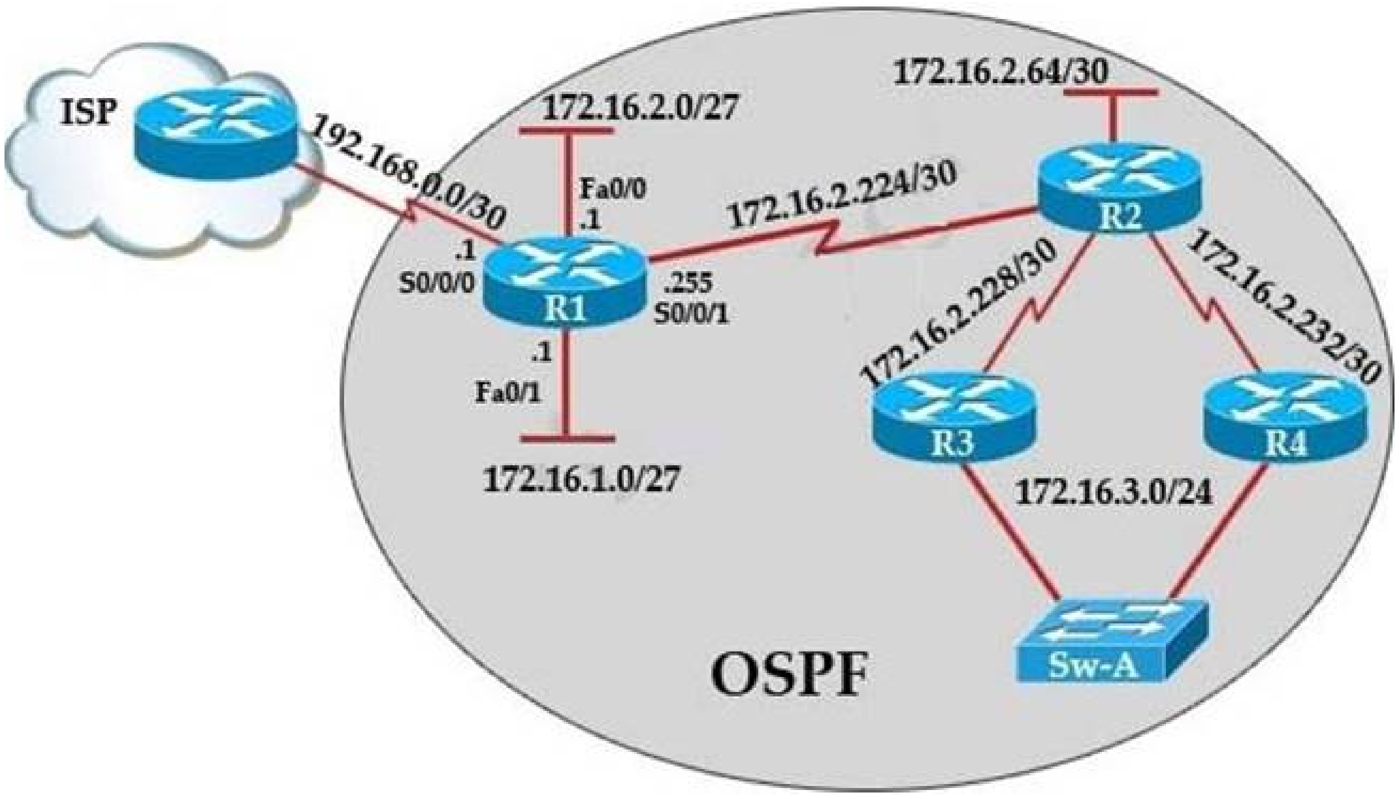
A. R2(config-if)#clock rate
B. R2(config-if)#bandwidth
C. R2(config-if)#ip ospf cost
D. R2(config-if)#ip ospf priority
E. R2(config-router)#distance ospf

**Answer:** BC

**Explanation:** http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.sht ml#t6
The cost (also called metric) of an interface in OSPF is an indication of the overhead required to send packets across a certain interface. The cost of an interface is inversely proportional to the bandwidth of that interface. A higher bandwidth indicates a lower cost. There is more overhead (higher cost) and time delays involved in crossing a 56k serial line than crossing a 10M Ethernet line. The formula used to calculate the cost is:
Cost = 10000 0000/bandwidth in bps
For example, it will cost 10 EXP8/10 EXP7 = 10 to cross a 10M Ethernet line and will cost 10 EXP8/1544000 =64 to cross a T1 line.
By default, the cost of an interface is calculated based on the bandwidth; you can force the cost of an interface with the ip ospf cost <value> interface subconfiguration mode command.

**NEW QUESTION 91**

R1 is configured with the default configuration of OSPF. From the following list of IP addresses configured on R1, which address will the OSPF process select as the router ID?



A. 192.168.0.1
B. 172.16.1.1
C. 172.16.2.1
D. 172.16.2.225

**Answer:** A

**Explanation:** The Router ID (RID) is an IP address used to identify the router and is chosen using the following sequencE.
+ The highest IP address assigned to a loopback (logical) interface. + If a loopback interface is not defined, the highest IP address of all active router's physical interfaces will be chosen.
+ The router ID can be manually assigned
In this case, because a loopback interface is not configured so the highest active IP address 192.168.0.1 is chosen as the router ID.

**NEW QUESTION 92**
What is the purpose of assigning an IP address to a switch?

A. provides local hosts with a default gateway address
B. allows remote management of the switch
C. allows the switch to respond to ARP requests between two hosts
D. ensures that hosts on the same LAN can communicate with each other

**Answer:** B

**Explanation:** A switch is a layer 2 device and doesn’t use network layer for packet forwarding. The IP
address may be used only for administrative purposes such as Telnet access or for network management purposes.

**NEW QUESTION 95**
Which statements describe the routing protocol OSPF? (Choose three.)

A. It supports VLSM.
B. It is used to route between autonomous systems.
C. It confines network instability to one area of the network.
D. It increases routing overhead on the network.
E. It allows extensive control of routing updates.
F. It is simpler to configure than RIP v2.

**Answer:** ACE

**Explanation:** Routing overhead is the amount of information needed to describe the changes in a dynamic network topology.
All routers in an OSPF area have identical copies of the topology database and the topology database of one area is hidden from the rest of the areas to reduce routing overhead because fewer routing updates are sent and smaller routing trees are computed and maintained (allow extensive control of routing updates and confine network instability to one area of the network).

**NEW QUESTION 99**
Which command can you use to manually assign a static IPV6 address to a router interface?

A. ipv6 address PREFIX_1::1/64
B. ipv6 autoconfig 2001:db8:2222:7272::72/64
C. ipv6 autoconfig
D. ipv6 address 2001:db8:2222:7272::72/64

**Answer:** D

**Explanation:** An example of configuring IPv6 on an interface is shown below: Router(config)# interface fastethernet 0/1
Router(config-if)# ipv6 address 3000::2222:1/64

**NEW QUESTION 100**
What is the OSPF default frequency, in seconds, at which a Cisco router sends hello packets on a multi-access network?

A. 10
B. 40
C. 30
D. 20

**Answer:** A

**Explanation:** On broadcast multiacess and point-to-point links, the default is 10 seconds. On NBMA, the default is 30 seconds.

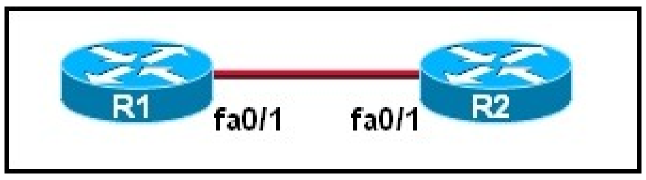
**NEW QUESTION 105**
If an Ethernet port on a router was assigned an IP address of 172.16.112.1/20, what is the maximum number of hosts allowed on this subnet?

A. 1024
B. 2046
C. 4094
D. 4096
E. 8190

**Answer:** C

**Explanation:** Each octet represents eight bits. The bits, in turn, represent (from left to right): 128, 64, 32 , 16 , 8, 4, 2, 1
Add them up and you get 255. Add one for the all zeros option, and the total is 256. Now, take away one of these for the network address (all zeros) and another for the broadcast address (all ones). Each octet represents 254 possible hosts. Or 254 possible
networks. Unless you have subnet zero set on your network gear, in which case you could conceivably have 255.
The CIDR addressing format (/20) tells us that 20 bits are used for the network portion, so the maximum number of networks are 2^20 minus one if you have subnet zero enabled, or minus 2 if not.
You asked about the number of hosts. That will be 32 minus the number of network bits, minus two. So calculate it as (2^(32-20))-2, or (2^12)-2 = 4094

**NEW QUESTION 107**
Refer to the exhibit.



The two routers have had their startup configurations cleared and have been restarted. At a minimum, what must the administrator do to enable CDP to exchange information between R1 and R2?

A. Configure the router with the cdp enable command.
B. Enter no shutdown commands on the R1 and R2 fa0/1 interfaces.
C. Configure IP addressing and no shutdown commands on both the R1 and R2 fa0/1 interfaces.
D. Configure IP addressing and no shutdown commands on either of the R1 or R2 fa0/1 interfaces.

**Answer:** B

**Explanation:** If the no shut down commands are not entered, then CDP can exchange information between the two routers. By default, all Cisco device interfaces and ports are shut down and need to be manually enabled.

**NEW QUESTION 108**
Which address are OSPF hello packets addressed to on point-to-point networks?

A. 224.0.0.5
B. 172.16.0.1
C. 192.168.0.5
D. 223.0.0.1
E. 254.255.255.255

**Answer:** A

**Explanation:** Why does the show ip ospf neighbor Command Reveal Neighbors in the Init State? http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f11.shtml OSPF hello packets have a destination address of 224.0.0.5 (the all ospf routers multicast address).

**NEW QUESTION 112**
Given an IP address of 192.168.1.42 255.255.255.248, what is the subnet address?

A. 192.168.1.8/29

B. 192.168.1.32/27
C. 192.168.1.40/29
D. 192.168.1.16/28
E. 192.168.1.48/29

**Answer:** C

**Explanation:** 248 mask uses 5 bits (1111 1000)
42 IP in binary is (0010 1010)
The base subnet therefore is the lowest binary value that can be written without changing the output of an AND operation of the subnet mask and IP...
1111 1000 AND
0010 1010 equals
0010 1000 - which is .40
/24 is standard class C mask.
Adding the 5 bits from the .248 mask gives /29

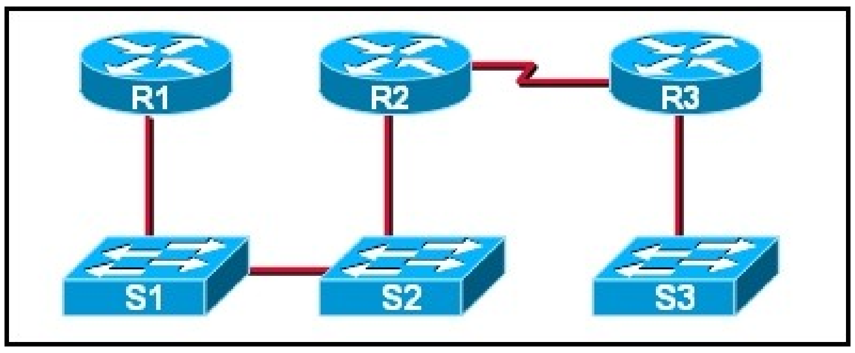
**NEW QUESTION 114**
A network administrator is trying to add a new router into an established OSPF network. The networks attached to the new router do not appear in the routing tables of the other OSPF routers. Given the information in the partial configuration shown below, what configuration error is causing this problem?
Router(config)# router ospf 1
Router(config-router)# network 10.0.0.0 255.0.0.0 area 0

A. The process id is configured improperly.
B. The OSPF area is configured improperly.
C. The network wildcard mask is configured improperly.
D. The network number is configured improperly.
E. The AS is configured improperly.
F. The network subnet mask is configured improperly.

**Answer:** C

**Explanation:** When configuring OSPF, the mask used for the network statement is a wildcard mask similar to an access list. In this specific example, the correct syntax would have been “network 10.0.0.0 0.0.0.255 area 0.”

**NEW QUESTION 117**
Refer to the exhibit.



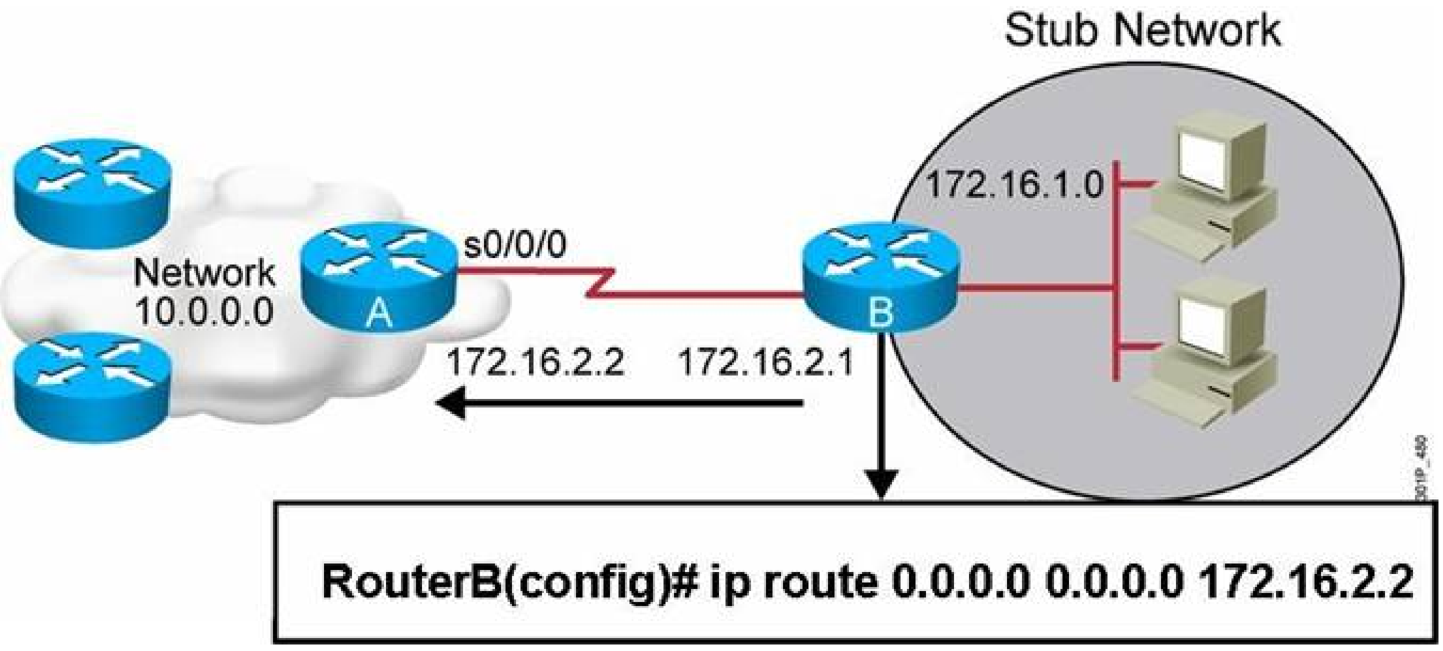
If CDP is enabled on all devices and interfaces, which devices will appear in the output of a show cdp neighbors command issued from R2?

A. R2 and R3
B. R1 and R3
C. R3 and S2
D. R1, S1, S2, and R3
E. R1, S1, S2, R3, and S3

**Answer:** C

**Explanation:** ACisco device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighbors. Since it is a layer two protocol, these packets are not routed. So the devices detected would be immediate connected neighbors.

**NEW QUESTION 118**
Refer to the exhibit.



```
RouterB(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

Which two statements are correct? (Choose two.)

A. This is a default route.
B. Adding the subnet mask is optional for the ip route command.
C. This will allow any host on the 172.16.1.0 network to reach all known destinations beyond RouterA.
D. This command is incorrect, it needs to specify the interface, such as s0/0/0 rather than an IP address.
E. The same command needs to be entered on RouterA so that hosts on the 172.16.1.0 network can reach network 10.0.0.0.

**Answer:** AC

**Explanation:** This is obviously the default route which is set between the routers and since it is entered in such a manner that it ensures connectivity between the stub network and any host lying beyond RouterA.

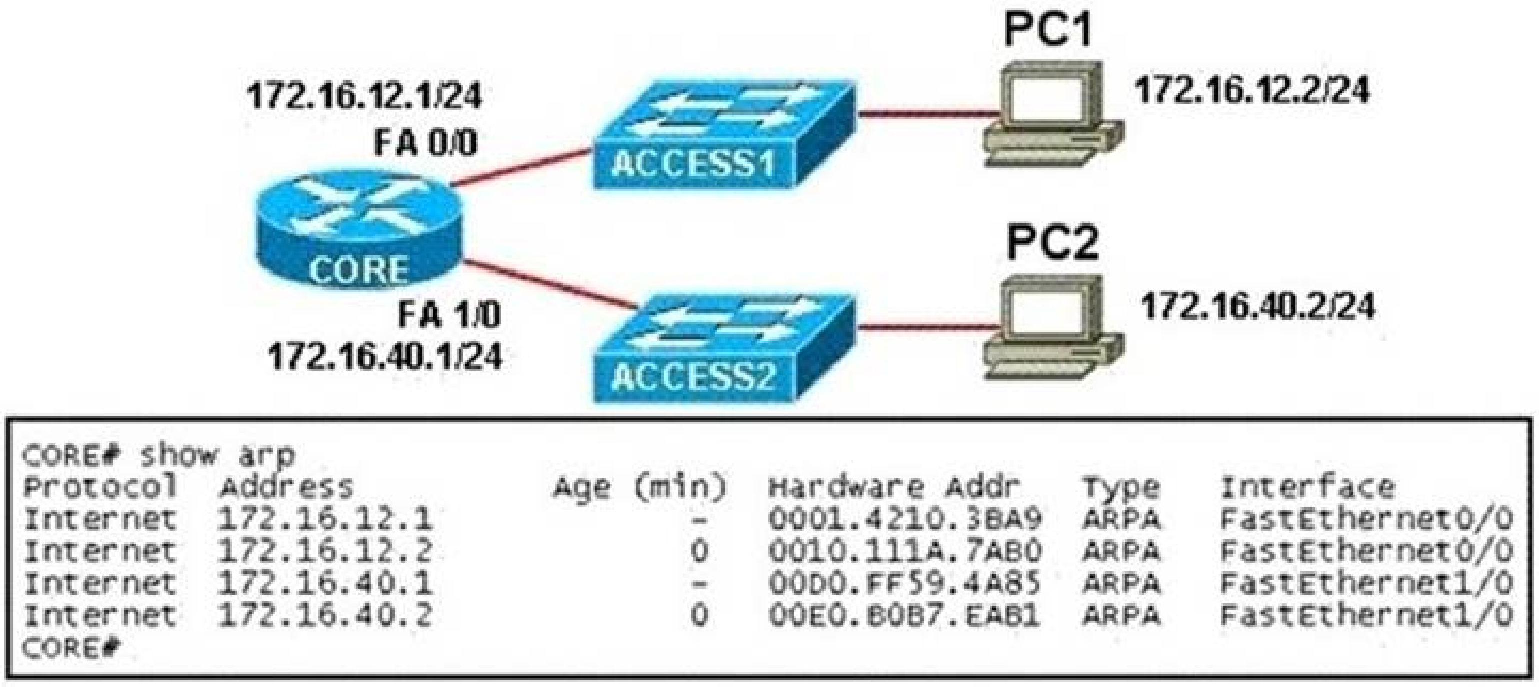
**NEW QUESTION 121**
What OSPF command, when configured, will include all interfaces into area 0?

A. network 0.0.0.0 255.255.255.255 area 0
B. network 0.0.0.0 0.0.0.0 area 0
C. network 255.255.255.255 0.0.0.0 area 0
D. network all-interfaces area 0

**Answer:** A

**Explanation:** Example 3-1 displays OSPF with a process ID of 1 and places all interfaces configured with an IP address in area 0. The network command network 0.0.0.0 255.255.255.255 area 0
dictates that you do not care (255.255.255.255) what the IP address is, but if an IP address is enabled on any interface, place it in area 0.
Example 3-1 Configuring OSPF in a Single Area
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
Reference: http://www.ciscopress.com/articles/article.asp?p=26919&seqNum=3

**NEW QUESTION 123**
Refer to the exhibit.



```
CORE# show arp
Protocol  Address        Age (min)  Hardware Addr   Type   Interface
Internet  172.16.12.1           -   0001.4210.3BA9  ARPA   FastEthernet0/0
Internet  172.16.12.2           0   0010.111A.7AB0  ARPA   FastEthernet0/0
Internet  172.16.40.1           -   00D0.FF59.4A85  ARPA   FastEthernet1/0
Internet  172.16.40.2           0   00E0.B0B7.EAB1  ARPA   FastEthernet1/0
CORE#
```

PC1 pings PC2. What three things will CORE router do with the data that is received from PC1? (Choose three.)

A. The data frames will be forwarded out interface FastEthernet0/1 of CORE router.
B. The data frames will be forwarded out interface FastEthernet1/0 of CORE router.
C. CORE router will replace the destination IP address of the packets with the IP address of PC2.
D. CORE router will replace the MAC address of PC2 in the destination MAC address ofthe frames.
E. CORE router will put the IP address of the forwarding FastEthernet interface in the place of the source IP address in the packets.

F. CORE router will put the MAC address of the forwarding FastEthernet interface in the place of the source MAC address.

**Answer:** BDF

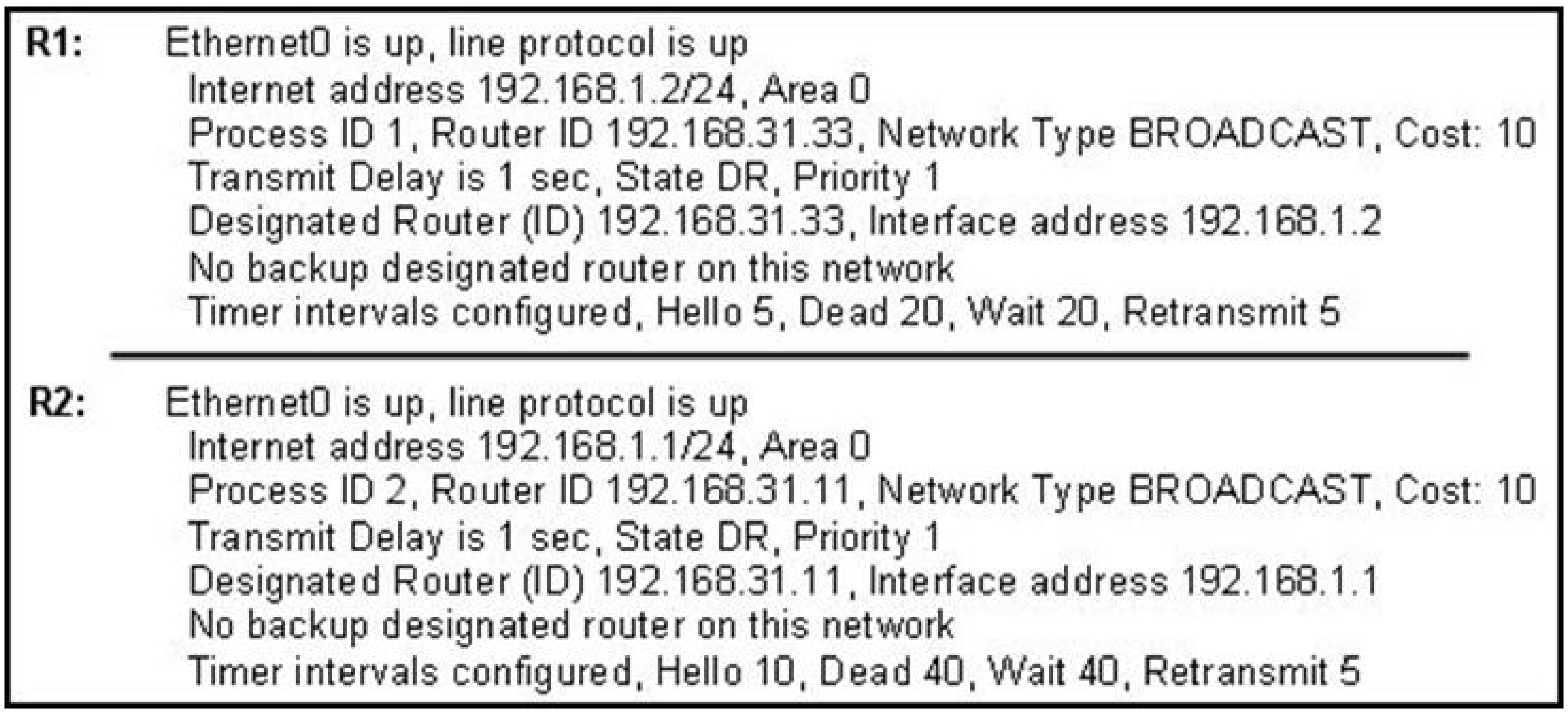
**Explanation:** The router will forward the frames out the interface toward the destination – B is correct. Since the router will has the end station already in it’s MAC table as see by the “show arp” command, it will replace the destination MAC address to that of PC2 – D is correct.
The router will then replace the source IP address to 172.16.40.1 – E is correct.

**NEW QUESTION 126**
Which two statements describe characteristics of IPv6 unicast addressing? (Choose two.)

A. Global addresses start with 2000::/3.
B. Link-local addresses start with FE00:/12.
C. Link-local addresses start with FF00::/10.
D. There is only one loopback address and it is ::1.
E. If a global address is assigned to an interface, then that is the only allowable address for the interface.

**Answer:** AD

**NEW QUESTION 130**
A network administrator is troubleshooting the OSPF configuration of routers R1 and R2. The routers cannot establish an adjacency relationship on their common Ethernet link.



```
R1:    Ethernet0 is up, line protocol is up
        Internet address 192.168.1.2/24, Area 0
        Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost: 10
        Transmit Delay is 1 sec, State DR, Priority 1
        Designated Router (ID) 192.168.31.33, Interface address 192.168.1.2
        No backup designated router on this network
        Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5

R2:    Ethernet0 is up, line protocol is up
        Internet address 192.168.1.1/24, Area 0
        Process ID 2, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 10
        Transmit Delay is 1 sec, State DR, Priority 1
        Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1
        No backup designated router on this network
        Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

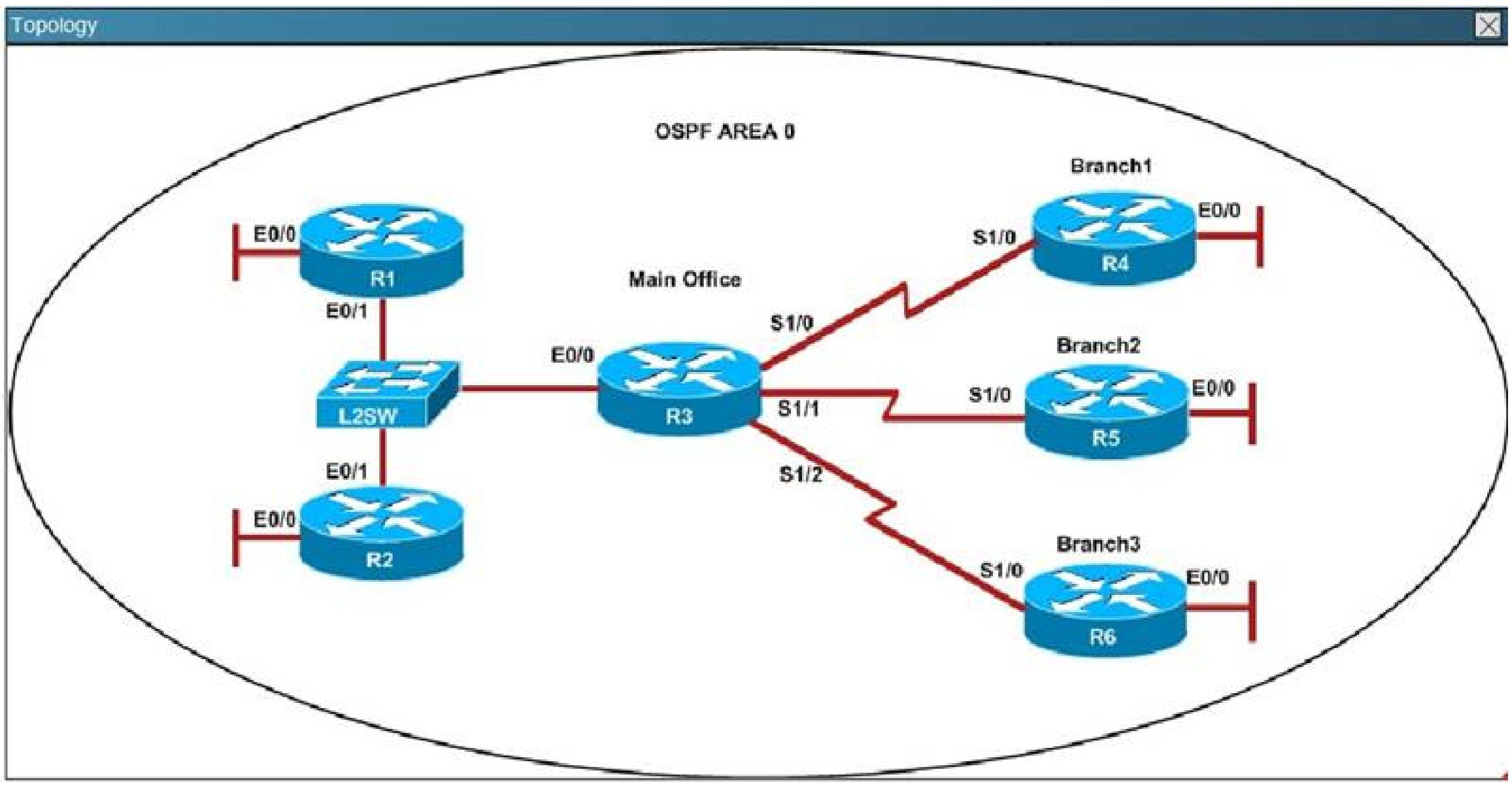
The graphic shows the output of the show ip ospf interface e0 command for routers R1 and R2. Based on the information in the graphic, what is the cause of this problem?

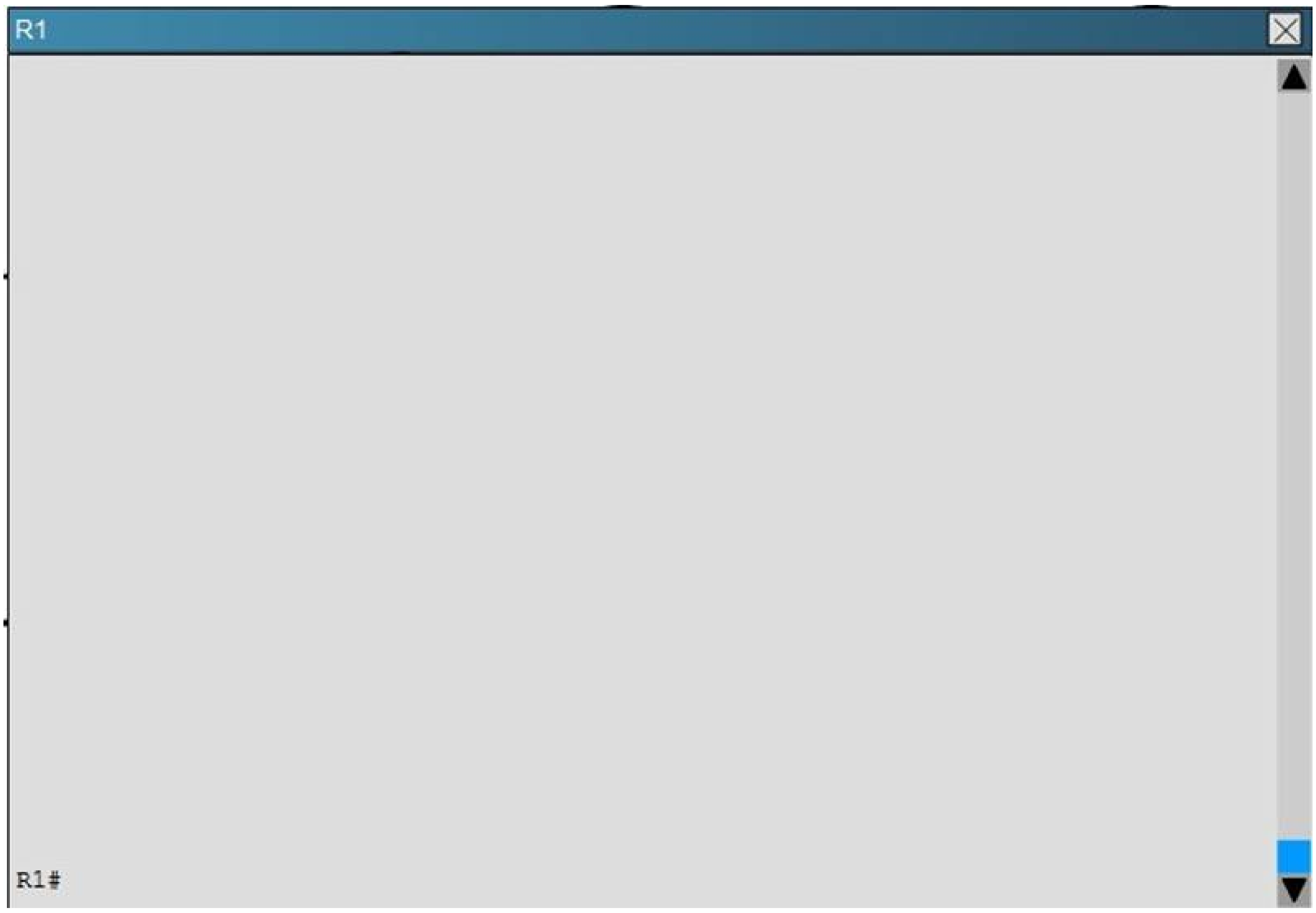
A. The OSPF area is not configured properly.
B. The priority on R1 should be set higher.
C. The cost on R1 should be set higher.
D. The hello and dead timers are not configured properly.
E. A backup designated router needs to be added to the network.
F. The OSPF process ID numbers must match.

**Answer:** D

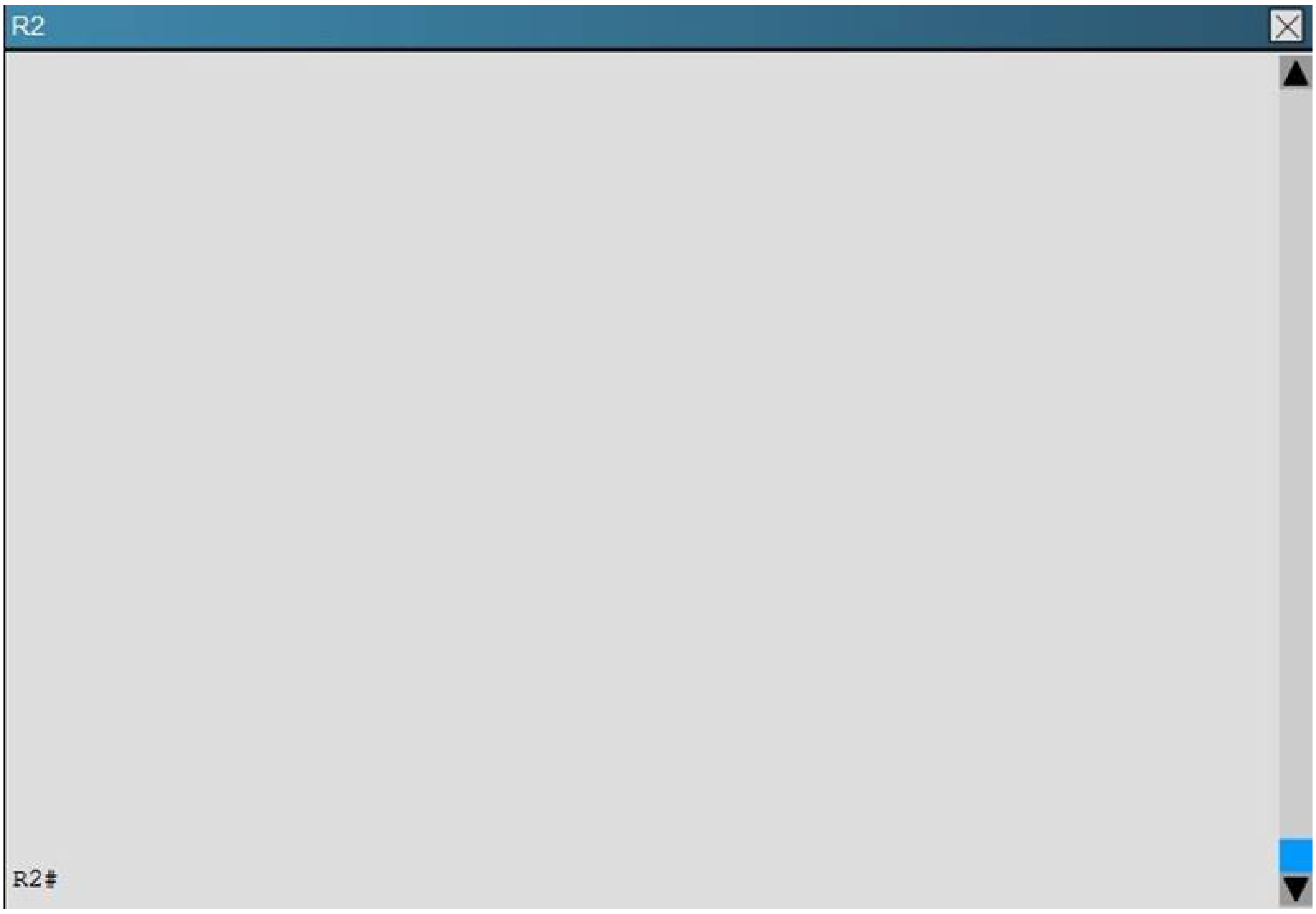
**Explanation:** In OSPF, the hello and dead intervals must match and here we can see the hello interval is set to 5 on R1 and 10 on R2. The dead interval is also set to 20 on R1 but it is 40 on R2.

**NEW QUESTION 132**
Scenario
Refer to the topology. Your company has decided to connect the main office with three other remote branch offices using point-to-point serial links.
You are required to troubleshoot and resolve OSPF neighbor adjacency issues between the main office and the routers located in the remote branch offices.

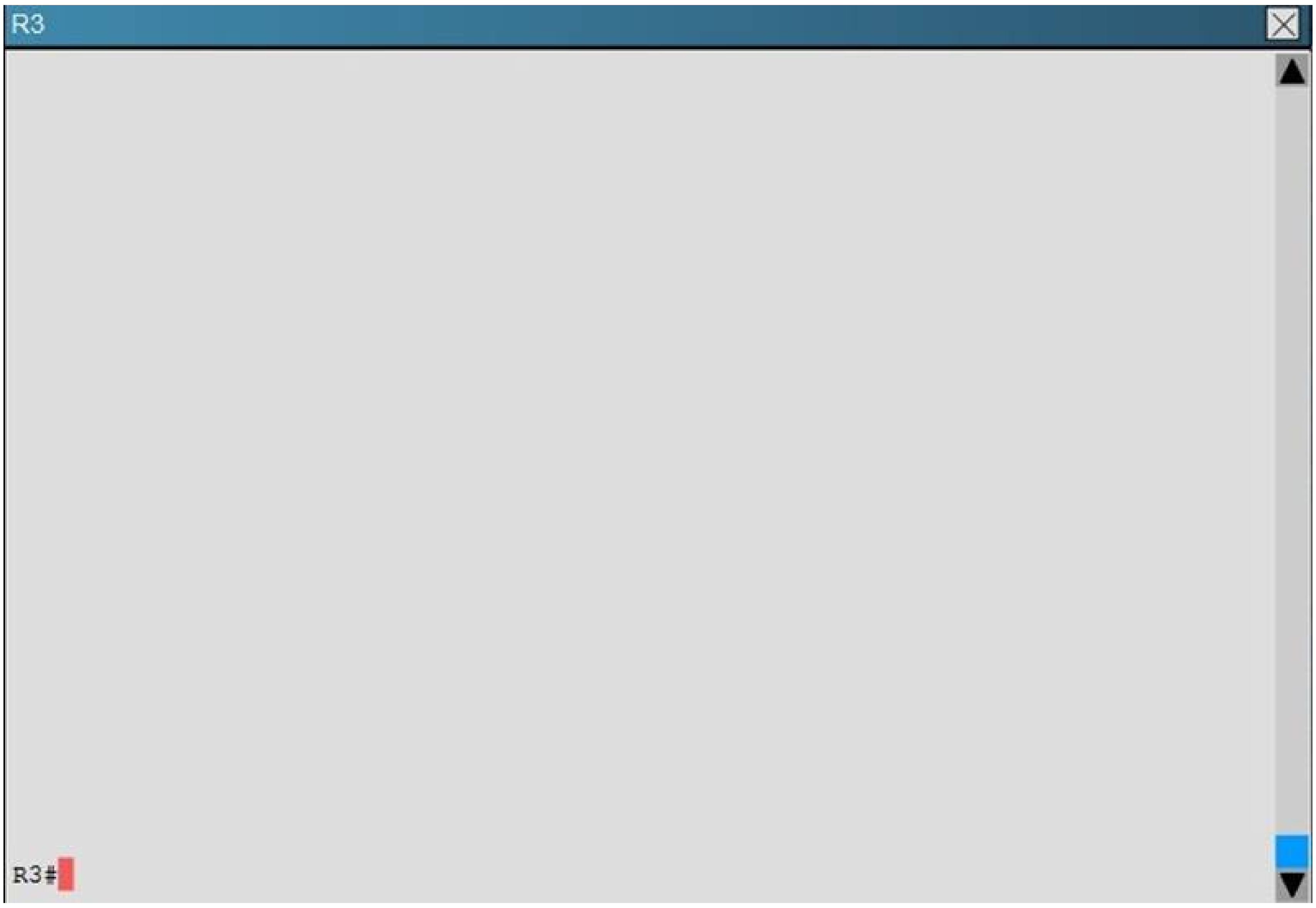

Topology
OSPF AREA 0
Branch1
E0/0
S1/0
R4
E0/0
R1
E0/1
Main Office
S1/0
E0/0
L2SW
R3
S1/1
Branch2
S1/0
E0/0
R5
S1/2
E0/1
E0/0
R2
Branch3
S1/0
E0/0
R6


R1

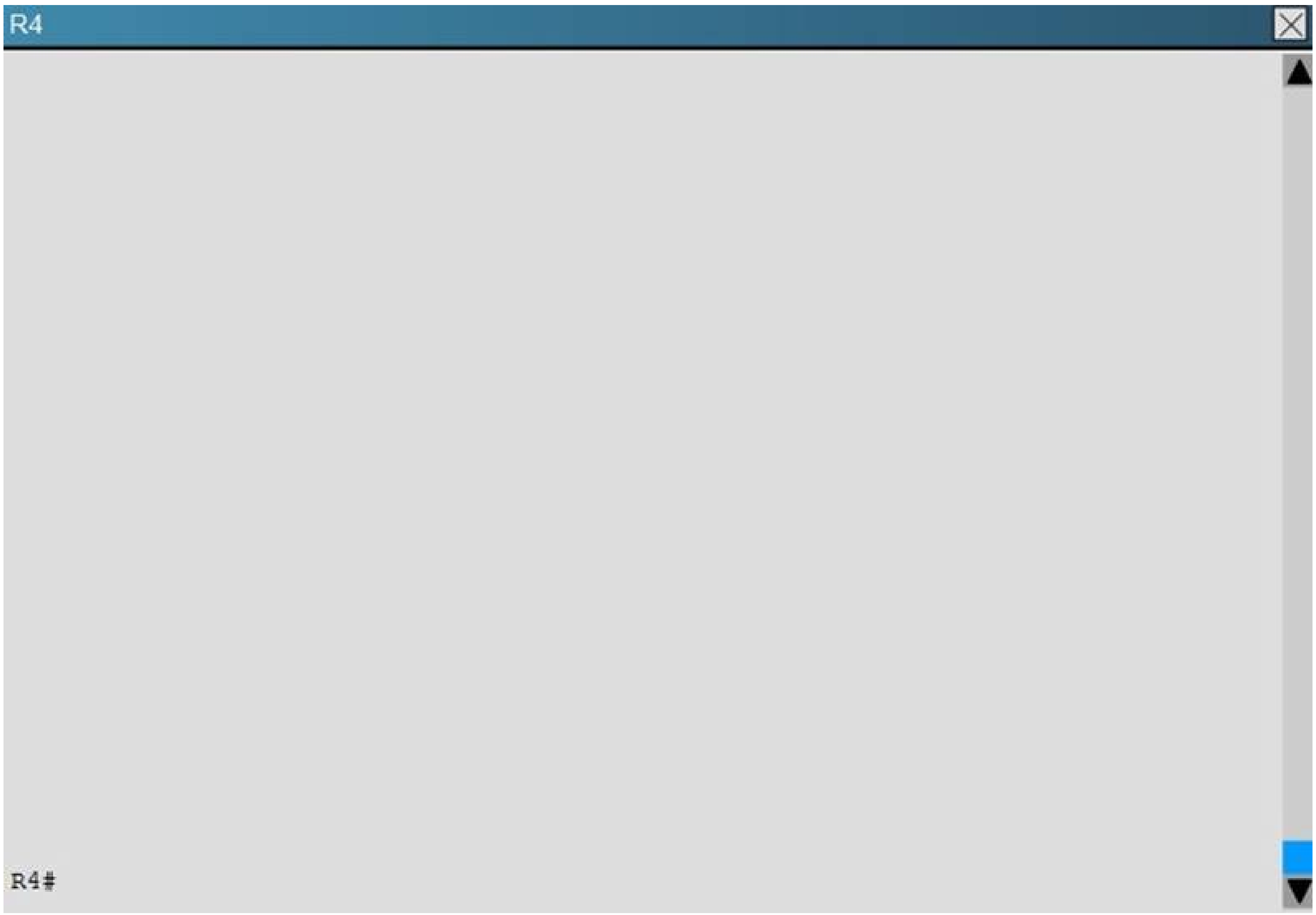
```
R1#
```



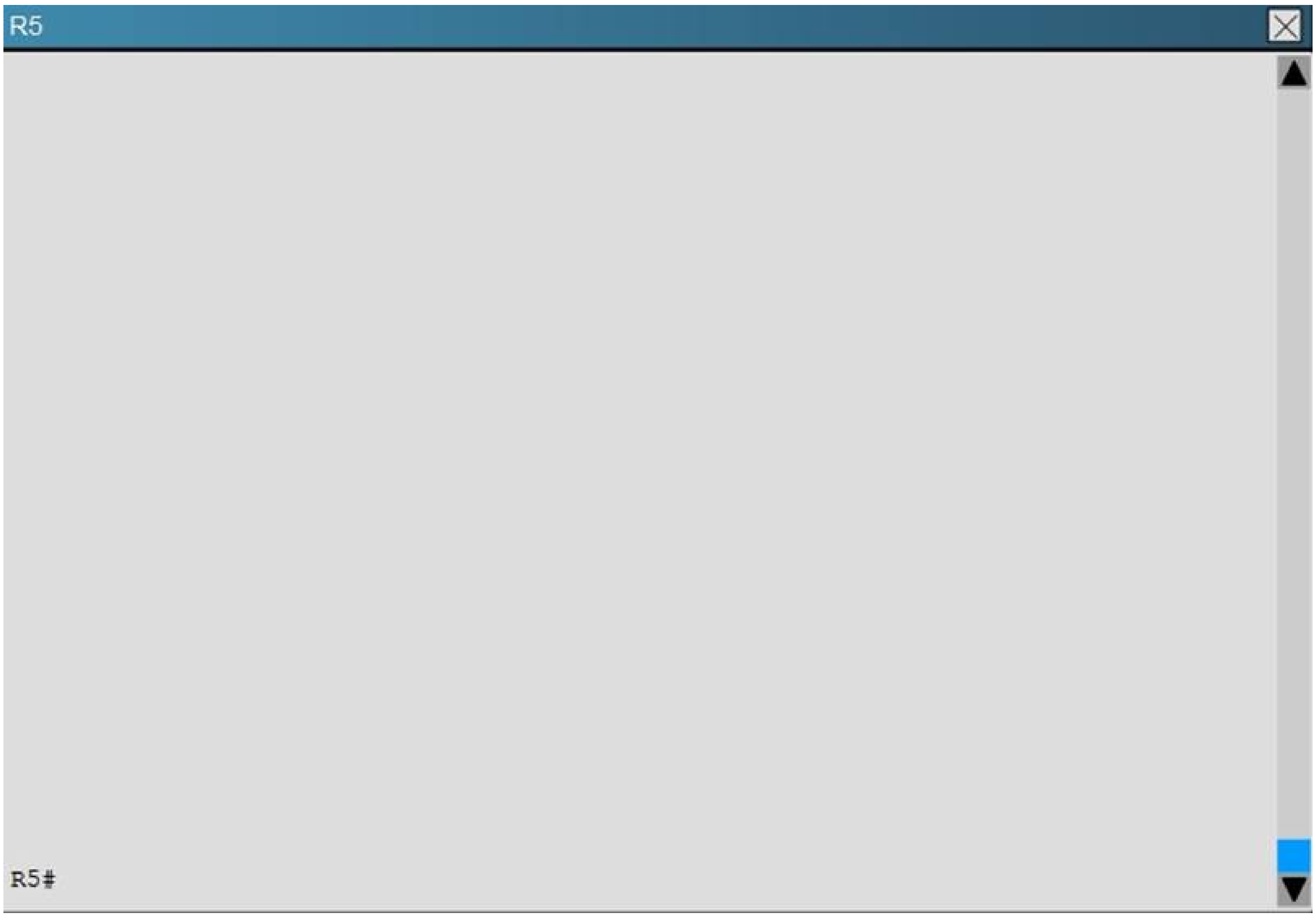
```
R2#
```



```
R3#
```

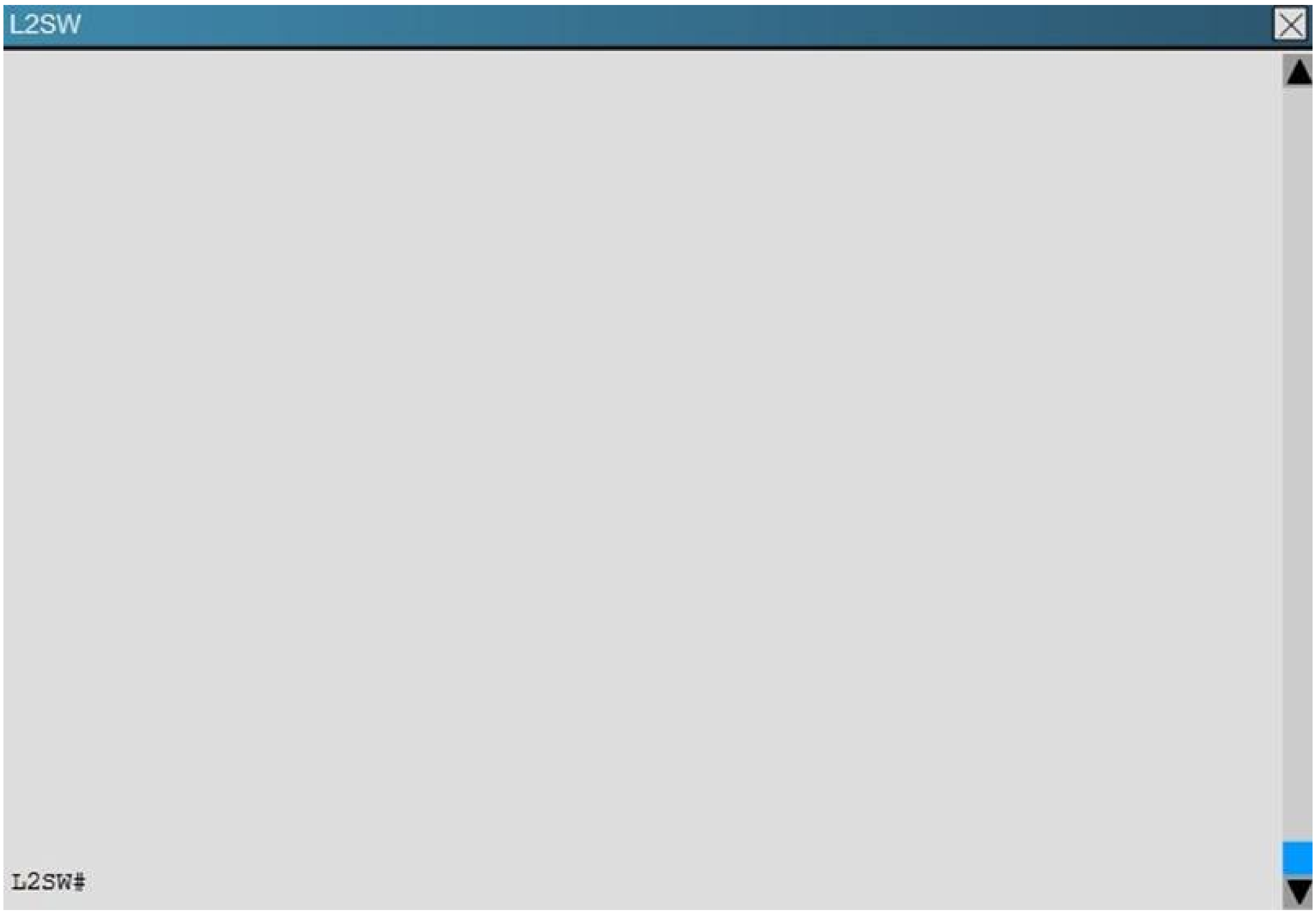


```
R4#
```



```
R5#
```

```
R6#
```



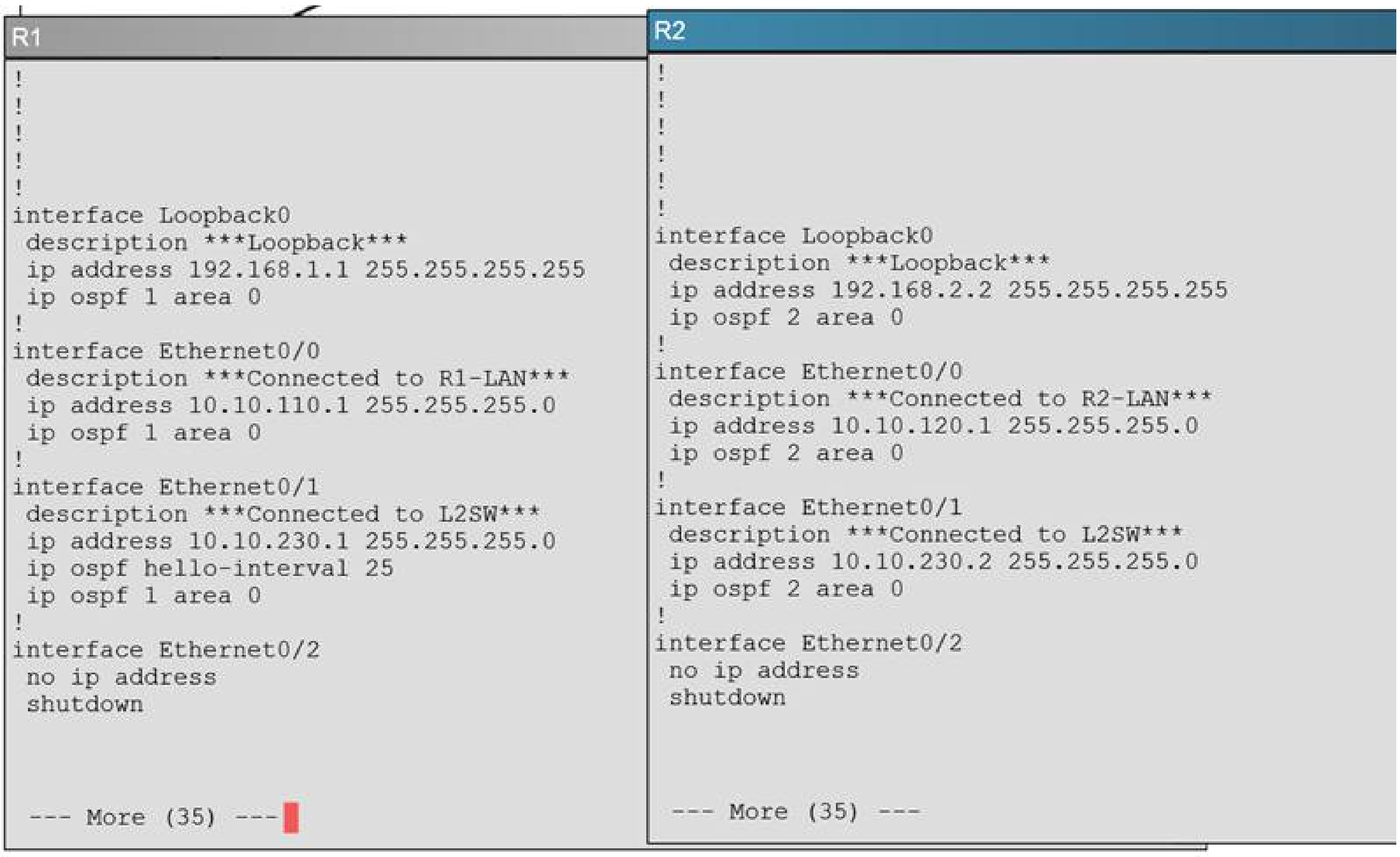
```
L2SW#
```

R1 does not form an OSPF neighbor adjacency with R2. Which option would fix the issue?

A. R1 ethernetO/1 is shutdow
B. Configure no shutdown command.
C. R1 ethernetO/1 configured with a non-default OSPF hello interval of 25: configure no ip ospf hello-interval 25
D. R2 ethernetO/1 and R3 ethernetO/O are configured with a non-default OSPF hello interval of 25; configure no ip ospf hello-interval 25
E. Enable OSPF for R1 ethernetO/1; configure ip ospf 1 area 0 command under ethernetO/1

**Answer:** B

**Explanation:** Looking at the configuration of R1, we see that R1 is configured with a hello interval of 25 on interface Ethernet 0/1 while R2 is left with the default of 10 (not configured).



R1

```
!
!
!
!
!
interface Loopback0
 description ***Loopback***
 ip address 192.168.1.1 255.255.255.255
 ip ospf 1 area 0
!
interface Ethernet0/0
 description ***Connected to R1-LAN***
 ip address 10.10.110.1 255.255.255.0
 ip ospf 1 area 0
!
interface Ethernet0/1
 description ***Connected to L2SW***
 ip address 10.10.230.1 255.255.255.0
 ip ospf hello-interval 25
 ip ospf 1 area 0
!
interface Ethernet0/2
 no ip address
 shutdown


 --- More (35) ---
```

R2

```
!
!
!
!
!
!
interface Loopback0
 description ***Loopback***
 ip address 192.168.2.2 255.255.255.255
 ip ospf 2 area 0
!
interface Ethernet0/0
 description ***Connected to R2-LAN***
 ip address 10.10.120.1 255.255.255.0
 ip ospf 2 area 0
!
interface Ethernet0/1
 description ***Connected to L2SW***
 ip address 10.10.230.2 255.255.255.0
 ip ospf 2 area 0
!
interface Ethernet0/2
 no ip address
 shutdown


 --- More (35) ---
```

**NEW QUESTION 133**
Which two statements describe the process identifier that is used in the command to configure OSPF on a router? (Choose two.)
Router(config)# router ospf 1

A. All OSPF routers in an area must have the same process ID.
B. Only one process number can be used on the same router.
C. Different process identifiers can be used to run multiple OSPF processes
D. The process number can be any number from 1 to 65,535.
E. Hello packets are sent to each neighbor to determine the processor identifier.

**Answer:** CD

**Explanation:** Multiple OSPF processes can be configured on a router using multiple process ID's. The valid process ID's are shown below:
Edge-B(config)#router ospf
<1-65535> Process ID

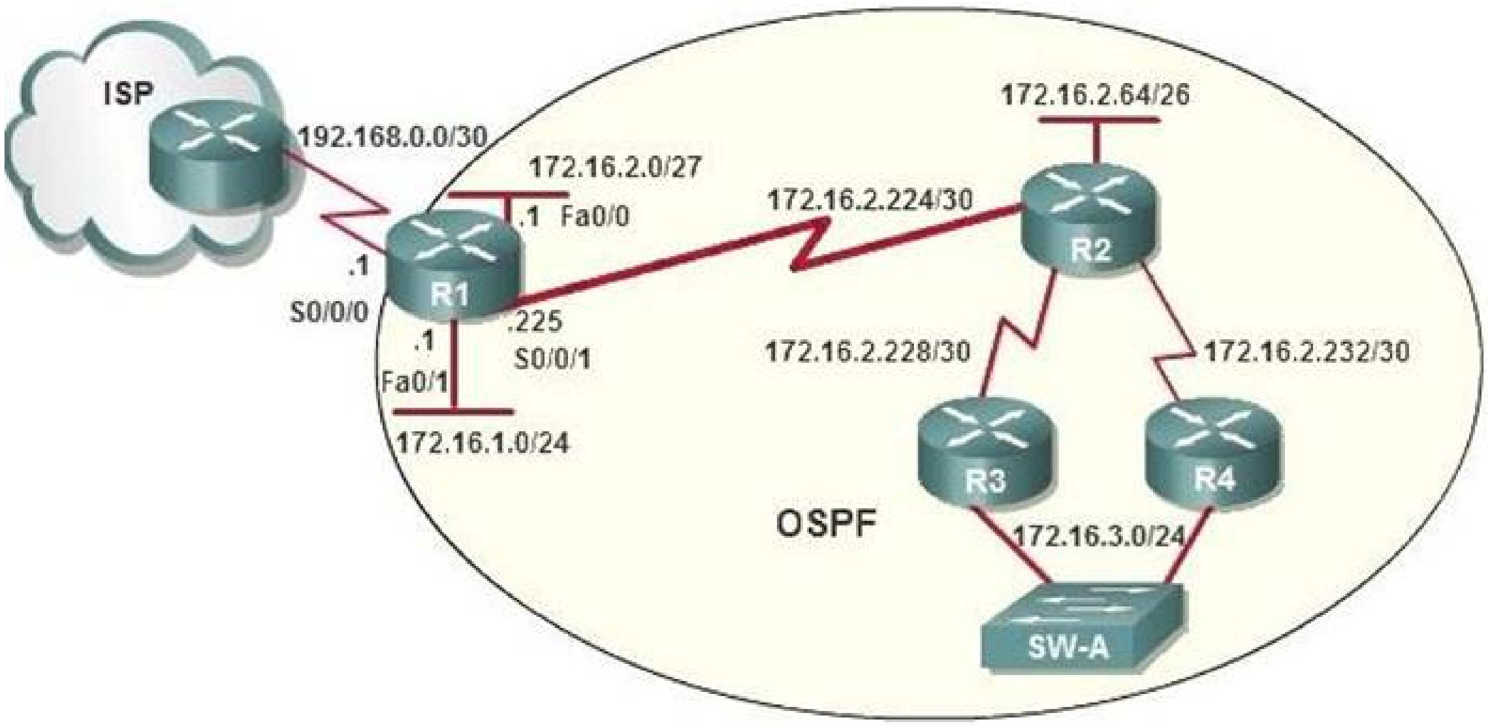
**NEW QUESTION 138**
Given a Class C IP address subnetted with a /30 subnet mask, how many valid host IP addresses are available on each of the subnets?

A. 1
B. 2
C. 4
D. 8
E. 252
F. 254

**Answer:** B

**Explanation:** /30 CIDR corresponds to mask 55.255.255.252 whose binary is 11111100 which means 6 subnet bits and 2 host bits which means 62 subnets and 2 hosts per subnet.

**NEW QUESTION 140**
OSPF is configured using default classful addressing. With all routers and interfaces operational, how many networks will be in the routing table of R1 that are indicated to be learned by OSPF?



A. 2
B. 3
C. 4
D. 5
E. 6
F. 7

**Answer:** C

**Explanation:** Although OSPF is configured using default classful addressing but OSPF is a link-state routing protocol so it will always send the subnet mask of each network in their advertised routes. Therefore R1 will learn the the complete subnets. Four networks list below will be in the routing table of R1:+ 172.16.2.64/30+ 172.16.2.228/30+ 172.16.2.232/30+ 172.16.3.0/24
Note: Other networks will be learned as “Directly connected” networks (marked with letter “C”)

**NEW QUESTION 143**
Which one of the following IP addresses is the last valid host in the subnet using mask 255.255.255.224?

A. 192.168.2.63
B. 192.168.2.62
C. 192.168.2.61
D. 192.168.2.60
E. 192.168.2.32

**Answer:** B

**Explanation:** With the 224 there are 8 networks with increments of 32
One of these is 32 33 62 63 where 63 is broadcast so 62 is last valid host out of given choices.

**NEW QUESTION 147**
What is the network address for the host with IP address 192.168.23.61/28?

A. 192.168.23.0
B. 192.168.23.32
C. 192.168.23.48
D. 192.168.23.56
E. 192.168.23.60

**Answer:** C

**Explanation:** Convert bit-length prefix to quad-dotted decimal representation, then from it find the number of bits used for subnetting you can find previously calculated number of subnets by separating subnets each having value of last bit used for subnet masking Find that your IP address is in which subnet, that subnet's first address is network address and last address is broadcast address.
Based on above steps the answer is option C

**NEW QUESTION 151**
Which of the following describe the process identifier that is used to run OSPF on a router? (Choose two)

A. It is locally significant.
B. It is globally significant.
C. It is needed to identify a unique instance of an OSPF database.
D. It is an optional parameter required only if multiple OSPF processes are running on the router.
E. All routers in the same OSPF area must have the same process ID if they are to exchange routing information.

**Answer:** AC

**Explanation:** https://learningnetwork.cisco.com/thread/6248
They are locally significant only, and have no bearing on the structure of any OSPF packet or LSA update. So you can have a separate process-id on every single router in your network if you so desire.

**NEW QUESTION 154**

```
ROUTER# show ip route
192.168.12.0/24 is variably subnetted, 9 subnets, 3 masks C 192.168.12.64 /28 is directly connected, Loopback1
C 192.168.12.32 /28 is directly connected, Ethernet0 C 192.168.12.48 /28 is directly connected, Loopback0
O 192.168.12.236 /30 [110/128] via 192.168.12.233, 00:35:36, Serial0
C 192.168.12.232 /30 is directly connected, Serial0
O 192.168.12.245 /30 [110/782] via 192.168.12.233, 00:35:36, Serial0
O 192.168.12.240 /30 [110/128] via 192.168.12.233, 00:35:36, Serial0
O 192.168.12.253 /30 [110/782] via 192.168.12.233, 00:35:37, Serial0
O 192.168.12.249 /30 [110/782] via 192.168.12.233, 00:35:37, Serial0
O 192.168.12.240/30 [110/128] via 192.168.12.233, 00:35:36, Serial 0
```

To what does the 128 refer to in the router output above?

A. OSPF cost
B. OSPF priority
C. OSPF hop count
D. OSPF ID number
E. OSPF administrative distance

**Answer:** A

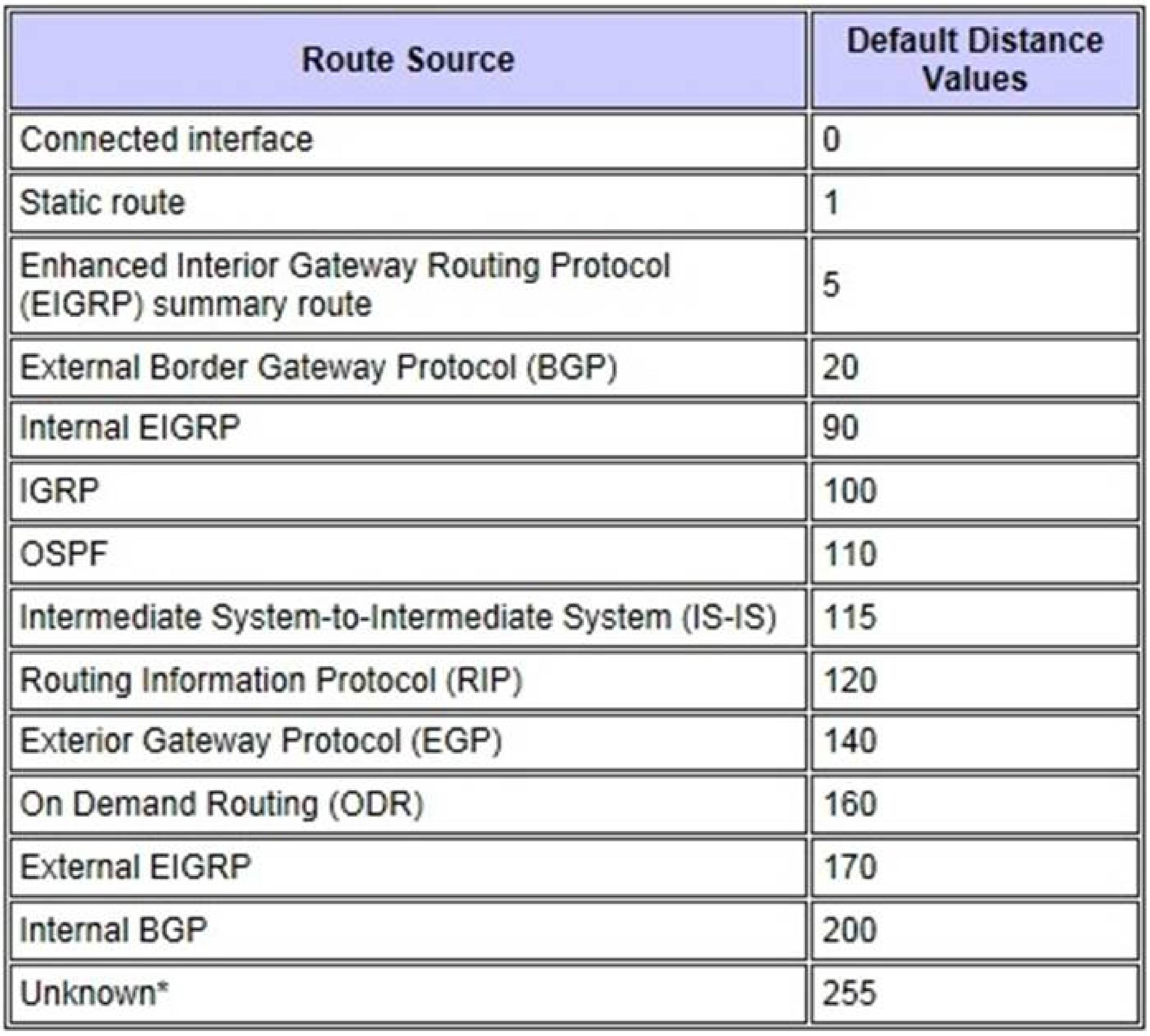
**Explanation:** The first parameter is the Administrative Distance of OSPF (110) while the second parameter is the cost of OSPF.

**NEW QUESTION 157**
What is the default administrative distance of the OSPF routing protocol?

A. 90
B. 100
C. 110
D. 120
E. 130
F. 170

**Answer:** C

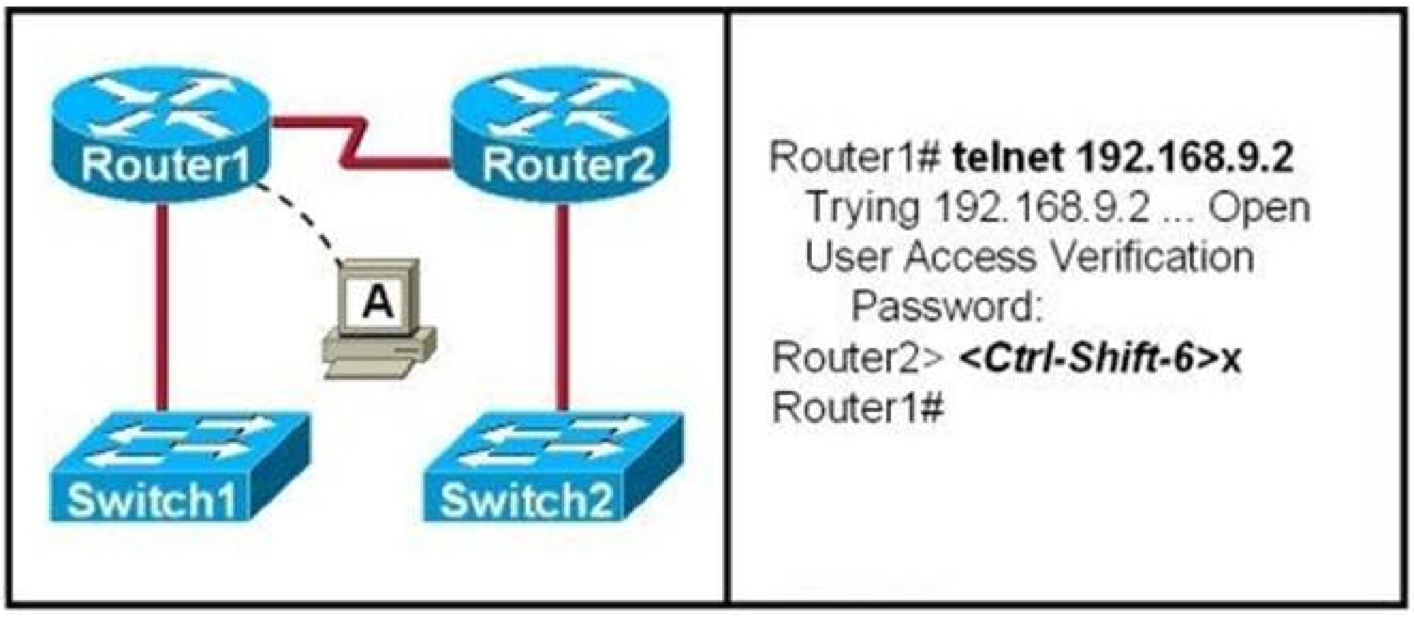
**Explanation:** Default Distance Value Table
This table lists the administrative distance default values of the protocols that Cisco supports:



| Route Source | Default Distance Values |
|---|---|
| Connected interface | 0 |
| Static route | 1 |
| Enhanced Interior Gateway Routing Protocol (EIGRP) summary route | 5 |
| External Border Gateway Protocol (BGP) | 20 |
| Internal EIGRP | 90 |
| IGRP | 100 |
| OSPF | 110 |
| Intermediate System-to-Intermediate System (IS-IS) | 115 |
| Routing Information Protocol (RIP) | 120 |
| Exterior Gateway Protocol (EGP) | 140 |
| On Demand Routing (ODR) | 160 |
| External EIGRP | 170 |
| Internal BGP | 200 |
| Unknown* | 255 |

If the administrative distance is 255, the router does not believe the source of that route and does not install the route in the routing table.

**NEW QUESTION 161**
Refer to the exhibit.



```
Router1# telnet 192.168.9.2
  Trying 192.168.9.2 ... Open
  User Access Verification
      Password:
Router2> <Ctrl-Shift-6>x
Router1#
```

If the resume command is entered after the sequence that is shown in the exhibit, which router prompt will be displayed?

A. Router1>
B. Router1#
C. Router2>
D. Router2#

**Answer:** C

**Explanation:** After resuming the telnet session by using the Enter key after it has been suspended, it will resume back to the telnet session so it will be back to the router2> prompt.

**NEW QUESTION 164**
An administrator must assign static IP addresses to the servers in a network. For network 192.168.20.24/29, the router is assigned the first usable host address while the sales server is given the last usable host address.
Which of the following should be entered into the IP properties box for the sales server?

A. IP address: 192.168.20.14Subnet Mask: 255.255.255.248Default Gateway: 192.168.20.9
B. IP address: 192.168.20.254Subnet Mask: 255.255.255.0Default Gateway: 192.168.20.1

C. IP address: 192.168.20.30Subnet Mask: 255.255.255.248Default Gateway: 192.168.20.25
D. IP address: 192.168.20.30Subnet Mask: 255.255.255.240Default Gateway: 192.168.20.17
E. IP address: 192.168.20.30Subnet Mask: 255.255.255.240Default Gateway: 192.168.20.25

**Answer:** C

**Explanation:** With network 192.168.20.24/29 we have:
Increment: 8 (/29 = 255.255.255.248 = 11111000 for the last octet) Network address: 192.168.20.24 (because 24 = 8 * 3)
Broadcast address: 192.168.20.31 (because 31 = 24 + 8 – 1)
Therefore the first usable IP address is 192.168.20.25 (assigned to the router) and the last usable IP address is 192.168.20.30 (assigned to the sales server). The IP address of the router is also the default gateway of the sales server.

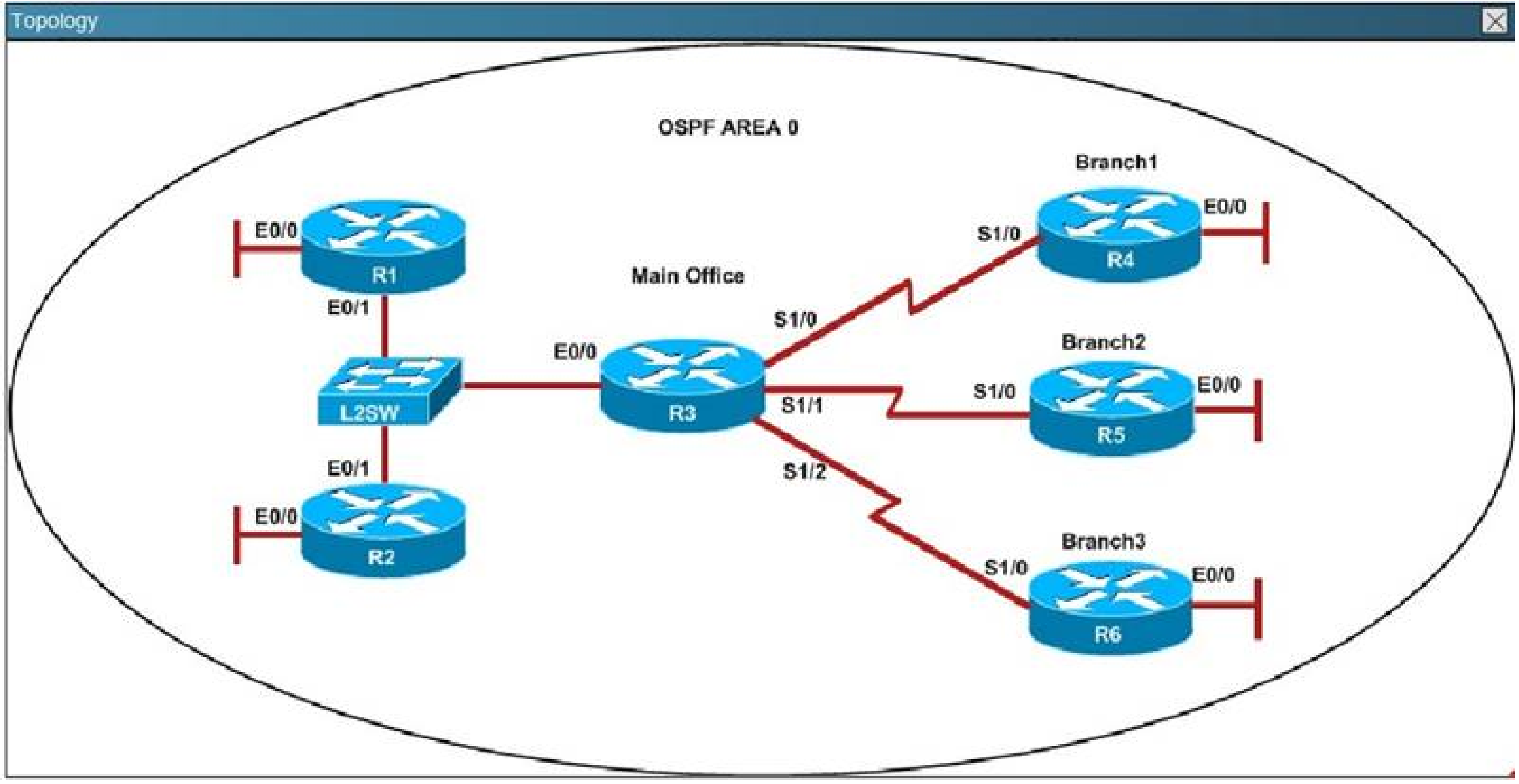
**NEW QUESTION 167**
What does administrative distance refer to?

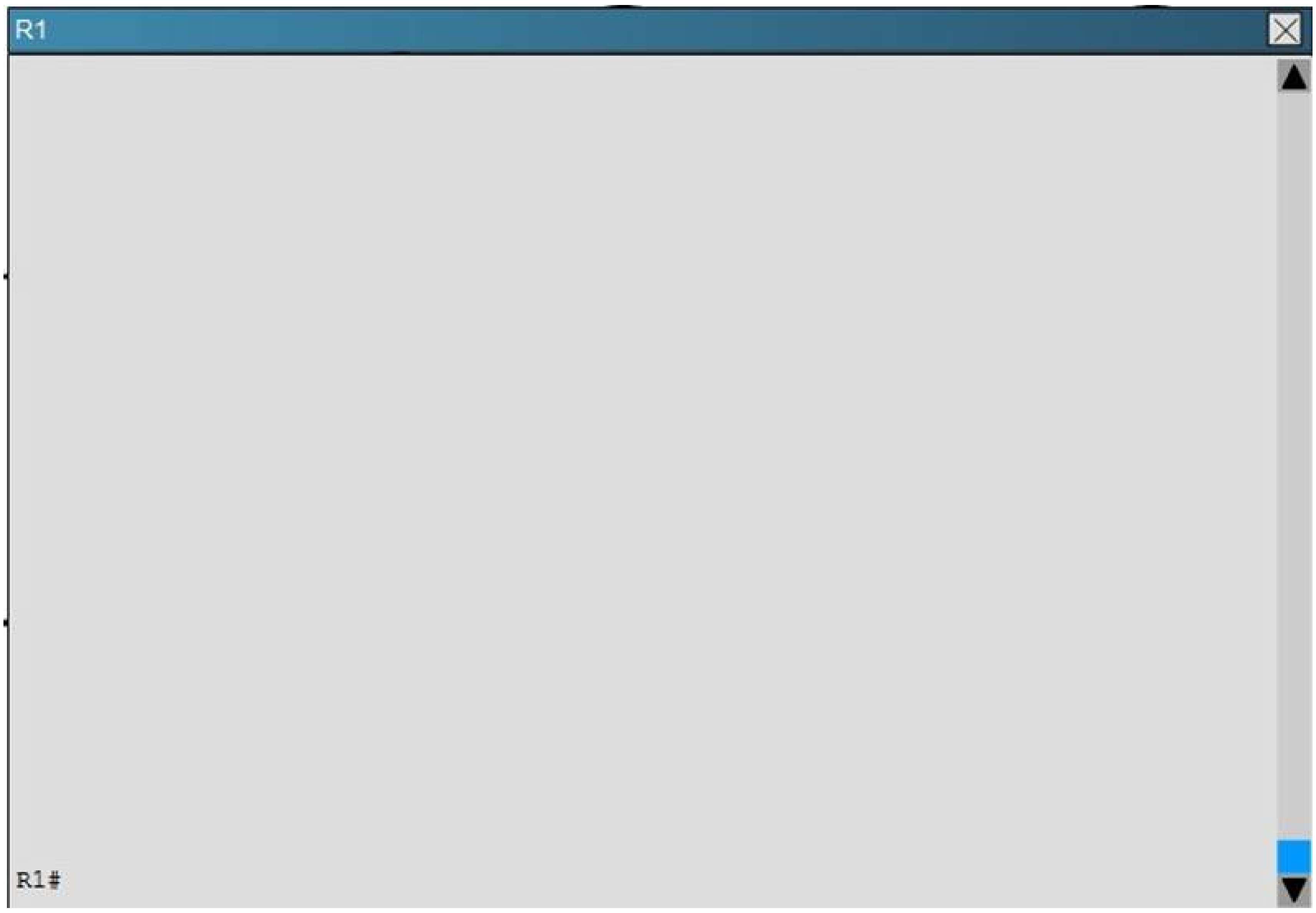
A. the cost of a link between two neighboring routers
B. the advertised cost to reach a network
C. the cost to reach a network that is administratively set
D. a measure of the trustworthiness of a routing information source

**Answer:** D

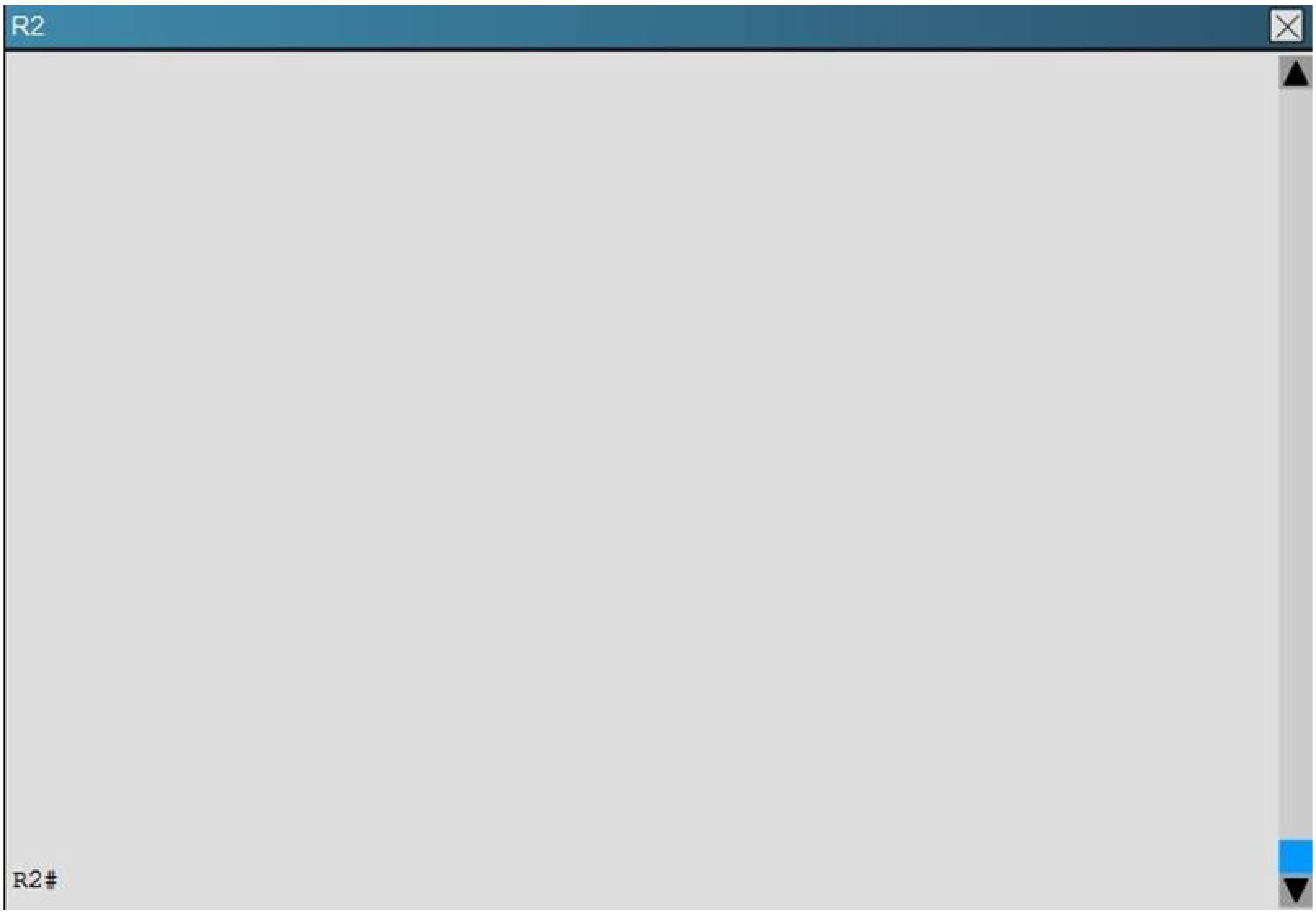
**Explanation:** Reference: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094195.shtml
Administrative distance is the feature that routers use in order to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) with the help of an administrative distance value.
Administrative distance is the first criterion that a router uses to determine which routing protocol to use if two protocols provide route information for the same destination. Administrative distance is a measure of the trustworthiness of the source of the routing information. The smaller the administrative distance value, the more reliable the protocol.

**NEW QUESTION 168**
Scenario
Refer to the topology. Your company has decided to connect the main office with three other remote branch offices using point-to-point serial links.
You are required to troubleshoot and resolve OSPF neighbor adjacency issues between the main office and the routers located in the remote branch offices.

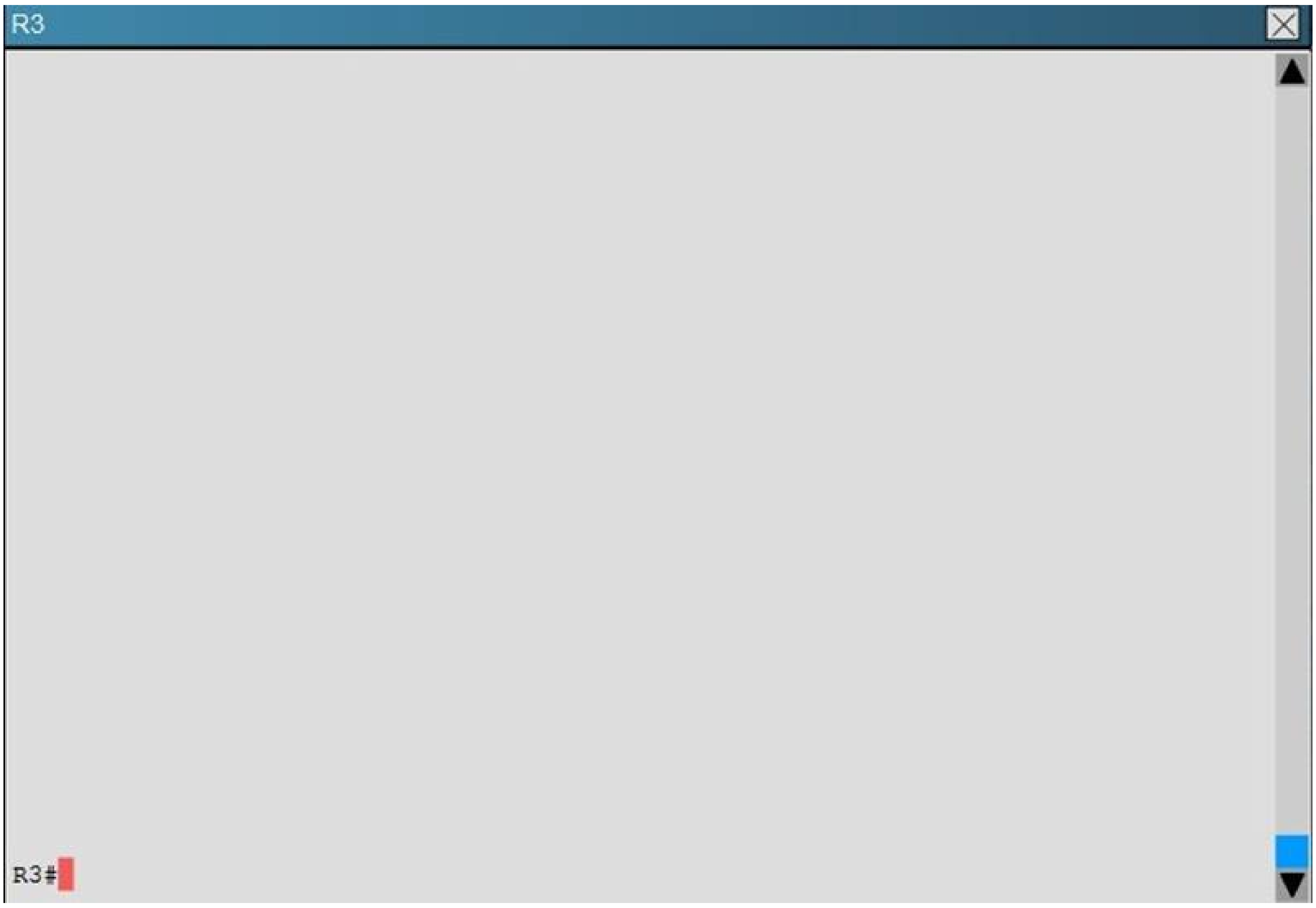




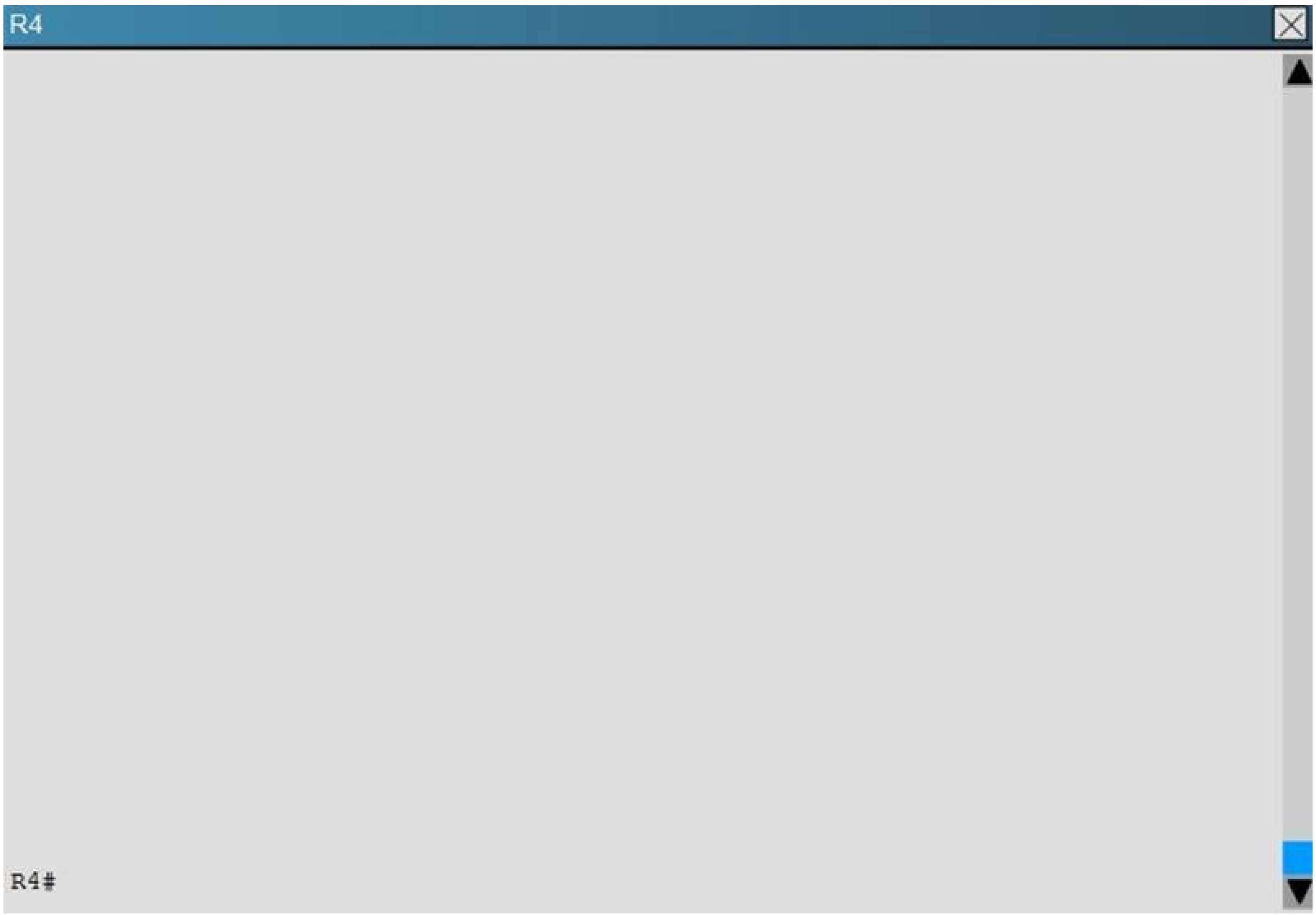
```
R1#
```



```
R2#
```



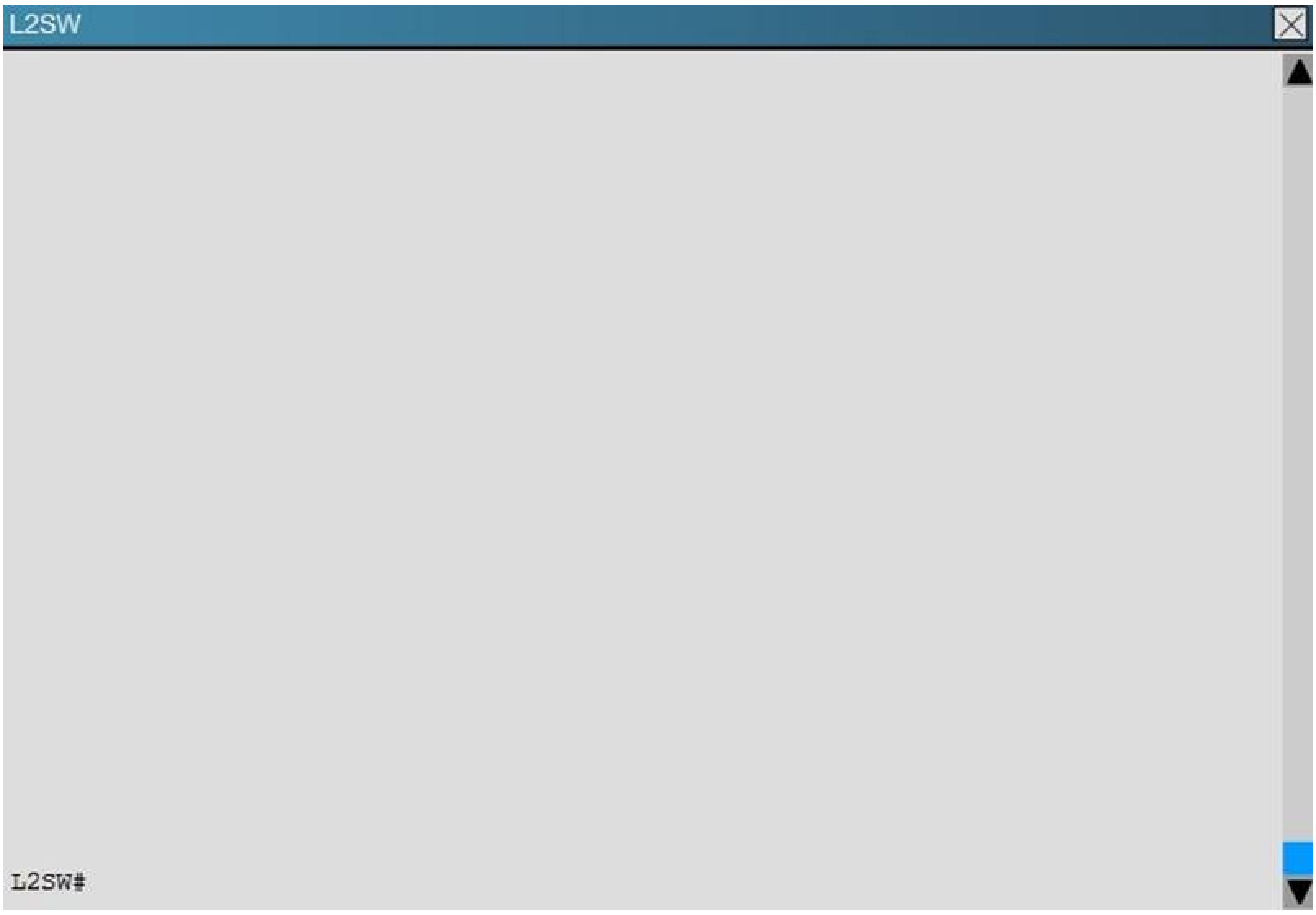
```
R3#
```



```
R4#
```

```
R5#
```

```
R6#
```



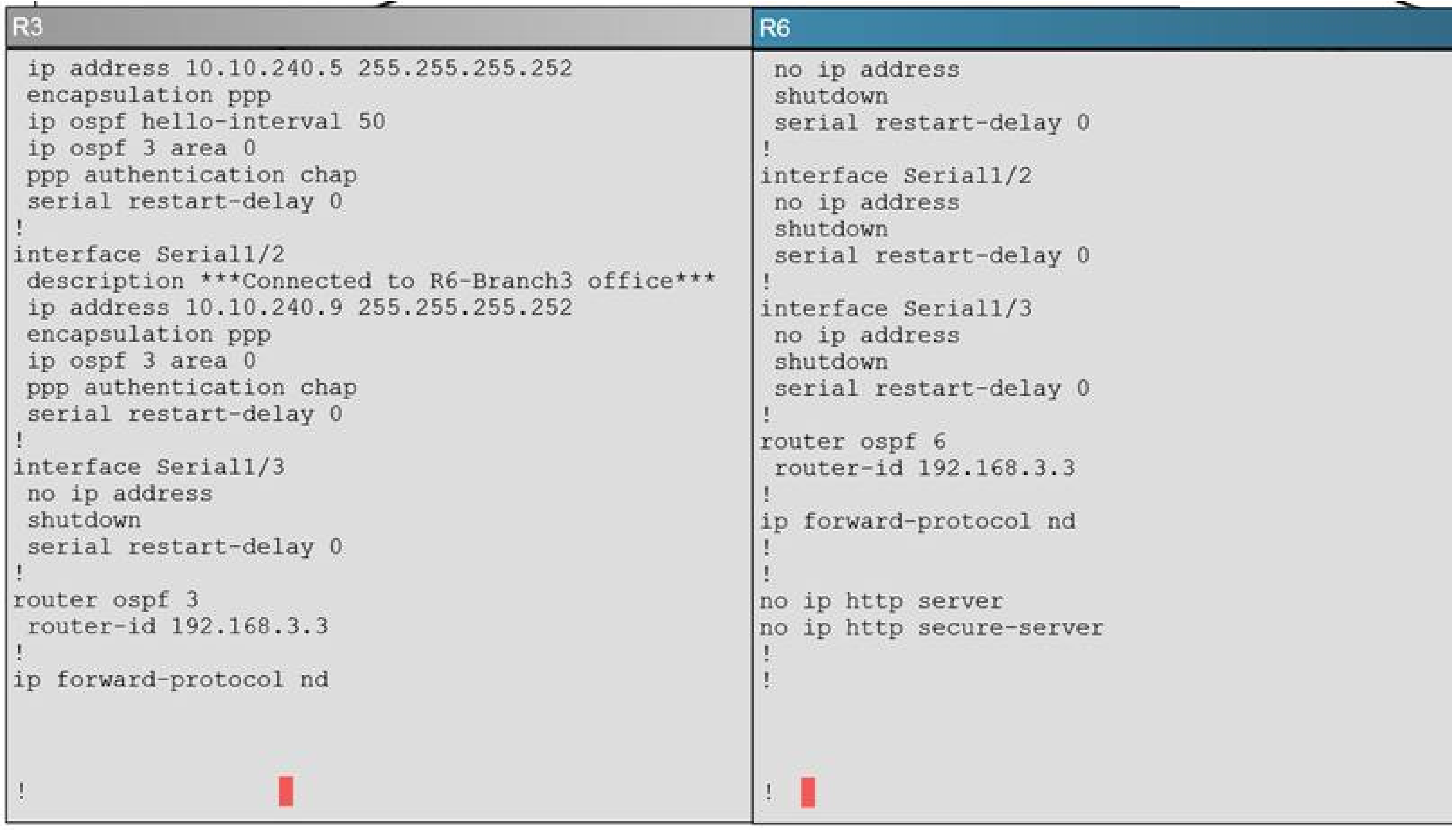
```
L2SW#
```

An OSPF neighbor adjacency is not formed between R3 in the main office and R6 in the Branch3 office. What is causing the problem?

A. There is an area ID mismatch.
B. There is a PPP authentication issue; the username is not configured on R3 and R6.
C. There is an OSPF hello and dead interval mismatch.
D. The R3 router ID is configured on R6.

**Answer:** D

**Explanation:** Using the show running-config command we see that R6 has been incorrectly configured with the same router ID as R3 under the router OSPF process.



```
 ip address 10.10.240.5 255.255.255.252
 encapsulation ppp
 ip ospf hello-interval 50
 ip ospf 3 area 0
 ppp authentication chap
 serial restart-delay 0
!
interface Serial1/2
 description ***Connected to R6-Branch3 office***
 ip address 10.10.240.9 255.255.255.252
 encapsulation ppp
 ip ospf 3 area 0
 ppp authentication chap
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 3
 router-id 192.168.3.3
!
ip forward-protocol nd


!
```

```
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 6
 router-id 192.168.3.3
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!


!
```

**NEW QUESTION 169**
111.111.111 111.111.111.111 755 0x80000005 0x0059CA 2
133.133.133.133 133.133.133.133 775 0x80000005 0x00B5B1 2
Net Link States (Area 0)
Link ID ADV Router Age Seq# Checksum10.1.1.1 111.111.111.111 794 0x80000001 0x001E8B
10.2.2.3 133.133.133.133 812 0x80000001 0x004BA9

10.4.4.1 111.111.111.111 755 0x80000001 0x007F16
10.4.4.3 133.133.133.133 775 0x80000001 0x00C31F

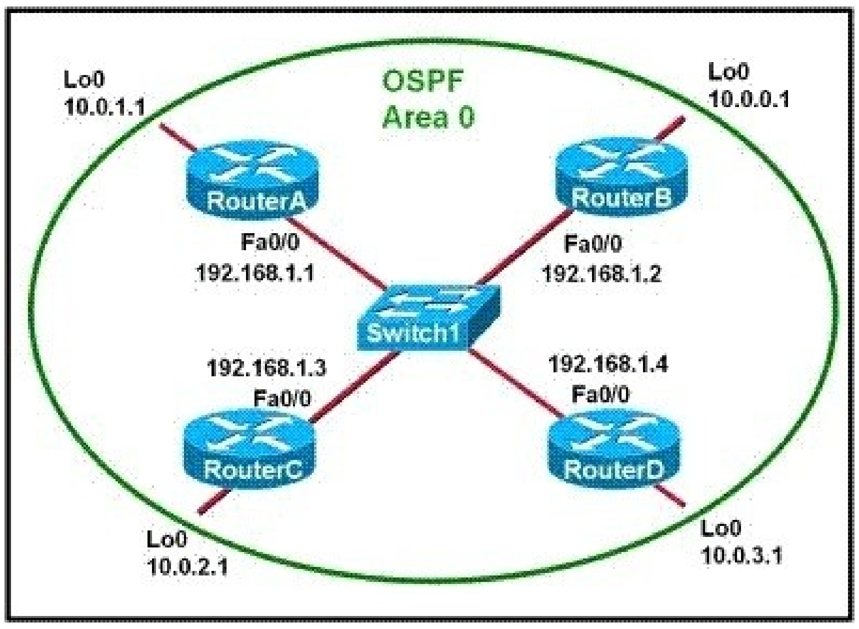
102.
Which statement describes the process ID that is used to run OSPF on a router?

A. It is globally significant and is used to represent the AS number.
B. It is locally significant and is used to identify an instance of the OSPF database.
C. It is globally significant and is used to identify OSPF stub areas.
D. It is locally significant and must be the same throughout an area.

**Answer:** B

**Explanation:** The IP addresses 133.6.5.4 and 190.6.5.4 are both valid Class B addresses when a default mask is in use.
The Class B default mask is 255.255.0.0 and the range of valid addresses is 128.0.0.0- 191.255.255.255.
The IP address 10.6.8.35 is a Class A address. The Class A default mask is 255.0.0.0 and the range of valid addresses is 1.0.0.0 - 127.255.255.255, with the exception of the range

**NEW QUESTION 172**
Refer to the exhibit.



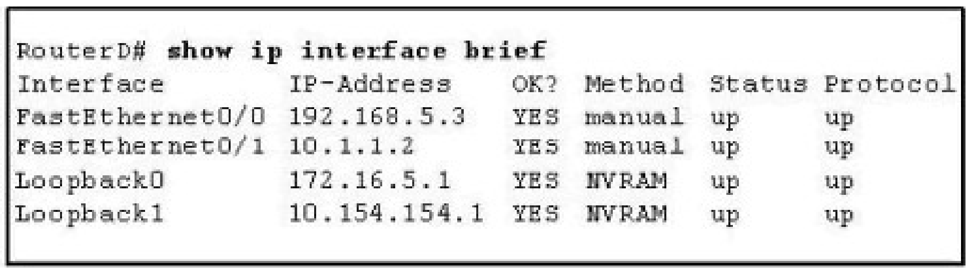
Which two statements are true about the loopback address that is configured on RouterB? (Choose two.)

A. It ensures that data will be forwarded by RouterB.
B. It provides stability for the OSPF process on RouterB.
C. It specifies that the router ID for RouterB should be 10.0.0.1.
D. It decreases the metric for routes that are advertised from RouterB.
E. It indicates that RouterB should be elected the DR for the LAN.

**Answer:** BC

**Explanation:** A loopback interface never comes down even if the link is broken so it provides stability for
the OSPF process (for example we use that loopback interface as the router-id) - The router-ID is chosen in the order below:
+ The highest IP address assigned to a loopback (logical) interface.
+ If a loopback interface is not defined, the highest IP address of all active router's physical interfaces will be chosen.
-> The loopback interface will be chosen as the router ID of RouterB -

**NEW QUESTION 176**
Refer to the exhibit.



```
RouterD# show ip interface brief
Interface        IP-Address     OK? Method Status Protocol
FastEthernet0/0  192.168.5.3    YES manual up     up
FastEthernet0/1  10.1.1.2       YES manual up     up
Loopback0        172.16.5.1     YES NVRAM  up     up
Loopback1        10.154.154.1   YES NVRAM  up     up
```

Given the output for this command, if the router ID has not been manually set, what router ID will OSPF use for this router?

A. 10.1.1.2
B. 10.154.154.1
C. 172.16.5.1
D. 192.168.5.3

**Answer:** C

**Explanation:** The highest IP address of all loopback interfaces will be chosen -> Loopback 0 will be chosen as the router ID.

**NEW QUESTION 180**
Which three approaches can be used while migrating from an IPv4 addressing scheme to an IPv6 scheme? (Choose three)

A. static mapping of IPv4 address to IPv6 addresses
B. configuring IPv4 tunnels between IPv6 islands
C. use DHCPv6 to map IPv4 addresses to IPv6 addresses
D. use proxying and translation (NAT-PT) to translate IPv6 packets into IPv4 packets
E. configure IPv6 directly
F. enable dual-stack routing

**Answer:** BDF

**Explanation:** Connecting IPv6 islands with tunnels
An IPv6 island is a network made of IPv6 links directly connected by IPv6 routers. In the early days of IPv6 deployment, there are many IPv6 islands. IPv6 in IPv4 tunnels are used to connect those islands together. In each island, one (or more) dual stack routers are designated to encapsulate and decapsulate IPv6 packets within IPv4 packets. Different mechanisms have been developed to manage tunnels: automatic tunnels3, configured tunnels3, tunnel brokers3, 6over43, 6to43,...
Reference 2:
http://www.petri.co.il/ipv6-transition.htm
Network Address Translation - Protocol Translation (NAT-PT)
The NAT-PT method enables the ability to either statically or dynamically configure a translation of a IPv4 network address into an IPv6 network address and vice versa. For those familiar with more typically NAT implementations, the operation is very similar but includes a protocol translation function. NAT-PT also ties in an Application Layer Gateway (ALG) functionality that converts Domain Name System (DNS) mappings between protocols.
Dual Stack
The simplest approach when transitioning to IPv6 is to run IPv6 on all of the devices that are currently running IPv4. If this is something that is possible within the organizational network, it is very easy to implement.
However, for many organizations, IPv6 is not supported on all of the IPv4 devices; in these situations other methods must be considered.
Reference: http://www.opus1.com/ipv6/howdoitransitiontoipv6.html

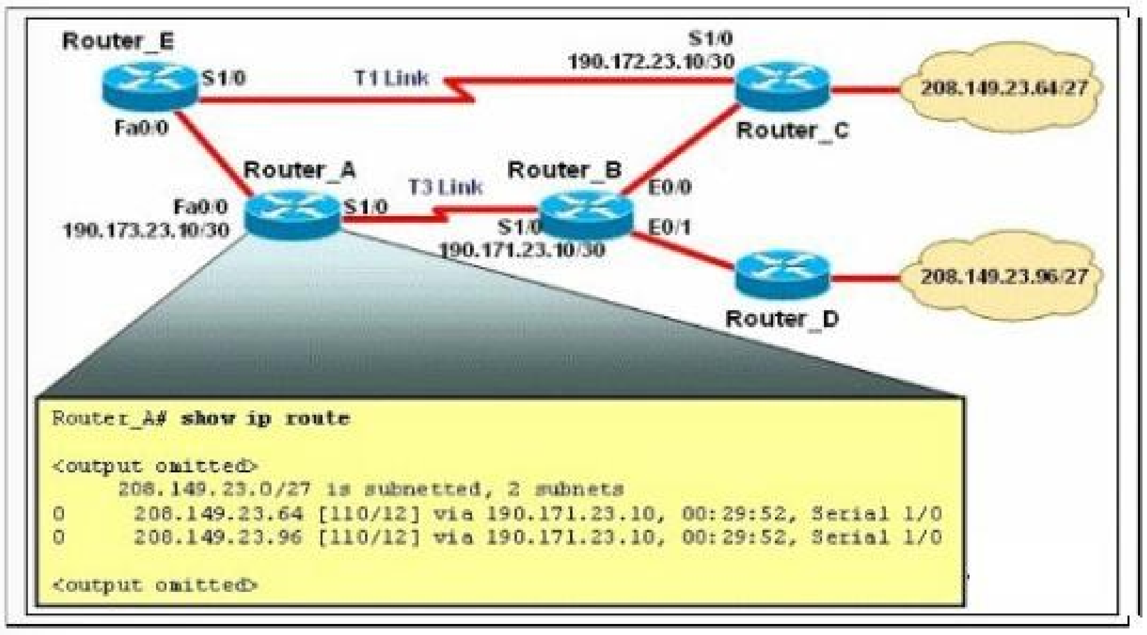
**NEW QUESTION 182**
OSPF routing uses the concept of areas. What are the characteristics of OSPF areas? (Choose Three.)

A. Each OSPF area requires a loopback interface to be configured.
B. Areas may be assigned any number from 0 to 65535.
C. Area 0 is called the backbone area.
D. Hierarchical OSPF networks do not require multiple areas.
E. Multiple OSPF areas must connect to area 0.
F. Single area OSPF networks must be configured in area 1.

**Answer:** BCE

**Explanation:** Definition of OSPF areas: An OSPF network may be structured, or subdivided, into routing areas to simplify administration and optimize traffic and resource utilization. Areas are identified by 32-bit numbers, expressed either simply in decimal, or often in octet-based dot-decimal notation, familiar from IPv4 address notation.
See discussion following Cisco Learning discussion. https://learningnetwork.cisco.com/message/90832

**NEW QUESTION 187**
Refer to the exhibit.



```
Router_A# show ip route

<output omitted>
     208.149.23.0/27 is subnetted, 2 subnets
O      208.149.23.64 [110/12] via 190.171.23.10, 00:29:52, Serial 1/0
O      208.149.23.96 [110/12] via 190.171.23.10, 00:29:52, Serial 1/0

<output omitted>
```

The network is converged.After link-state advertisements are received from Router_A, what information will Router_E contain in its routing table for the subnets 208.149.23.64 and 208.149.23.96?

A. 208.149.23.64[110/13] via 190.173.23.10, 00:00:07, FastEthemet0/0208.149.23.96[110/13] via 190.173.23.10, 00:00:16, FastEthemet0/0
B. 208.149.23.64[110/1] via 190.172.23.10, 00:00:07, Serial1/0208.149.23.96[110/3] via 190.173.23.10, 00:00:16, FastEthemet0/0
C. 208.149.23.64[110/13] via 190.173.23.10, 00:00:07, Serial1/0208.149.23.96[110/13] via 190.173.23.10, 00:00:16, Serial1/0208.149.23.96[110/13] via 190.173.23.10, 00:00:16, FastEthemet0/0
D. 208.149.23.64[110/3] via 190.172.23.10, 00:00:07, Serial1/0208.149.23.96[110/3] via 190.173.23.10, 00:00:16, Serial1/0

**Answer:** A

**Explanation:** Router_E learns two subnets subnets 208.149.23.64 and 208.149.23.96 via Router_A through FastEthernet interface. The interface cost is calculated with the formula 108 / Bandwidth. For FastEthernet it is 108 / 100 Mbps = 108 / 100,000,000 = 1. Therefore the
cost is 12 (learned from Router_A) + 1 = 13 for both subnets ->
The cost through T1 link is much higher than through T3 link (T1 cost = 108 / 1.544 Mbps = 64; T3 cost = 108 / 45 Mbps = 2) so surely OSPF will choose the path through T3 link -> Router_E will choose the path from Router_A through FastEthernet0/0, not Serial1/0.

In fact, we can quickly eliminate answers B, C and D because they contain at least one subnet learned from Serial1/0 -> they are surely incorrect.

**NEW QUESTION 190**
Which command enables IPv6 forwarding on a Cisco router?

A. ipv6 host
B. ipv6 unicast-routing
C. ipv6 local
D. ipv6 neighbor

**Answer:** B

**Explanation:** Enabling IPv6 on Cisco IOS Software Technology http://www.ciscopress.com/articles/article.asp?p=31948&seqNum=4
The first step of enabling IPv6 on a Cisco router is the activation of IPv6 traffic forwarding to forward unicast IPv6 packets between network interfaces. By default, IPv6 traffic forwarding is disabled on Cisco routers.
The ipv6 unicast-routing command is used to enable the forwarding of IPv6 packets between interfaces on the router. The syntax for this command is as follows: Router(config)#ipv6 unicast-routing The ipv6 unicast-routing command is enabled on a global basis.

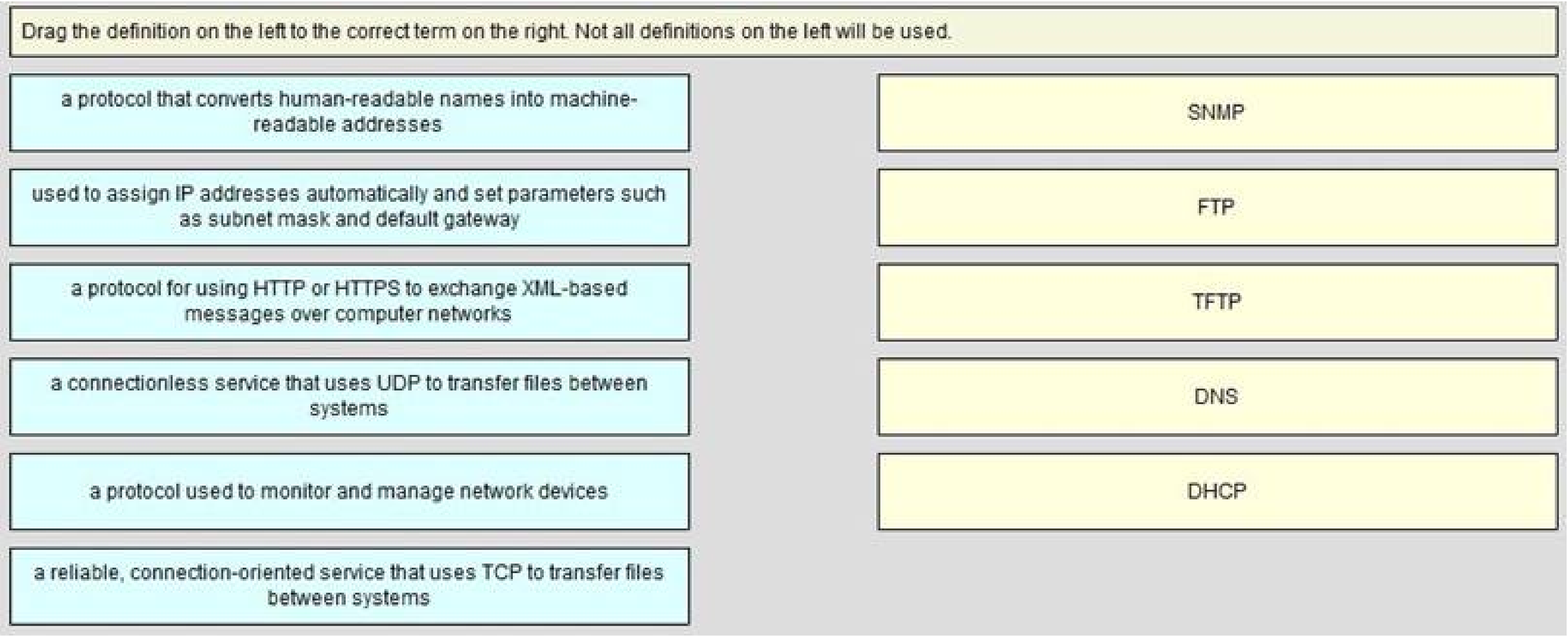
**NEW QUESTION 192**
What is the subnet address of 172.16.159.159/22?

A. 172.16.0.0
B. 172.16.128.0
C. 172.16.156.0
D. 172.16.159.0
E. 172.16.159.128
F. 172.16.192.0

**Answer:** C

**Explanation:** Converting to binary format it comes to 11111111.11111111.11111100.00000000 or 255.255.252.0 Starting with 172.16.0.0 and having increment of 4 we get.

**NEW QUESTION 196**
DRAG DROP
Drag the definition on the left to the correct term on the right. Not all definitions on the left will be used.



Drag the definition on the left to the correct term on the right. Not all definitions on the left will be used.

a protocol that converts human-readable names into machine-readable addresses

used to assign IP addresses automatically and set parameters such as subnet mask and default gateway

a protocol for using HTTP or HTTPS to exchange XML-based messages over computer networks

a connectionless service that uses UDP to transfer files between systems

a protocol used to monitor and manage network devices

a reliable, connection-oriented service that uses TCP to transfer files between systems

SNMP

FTP

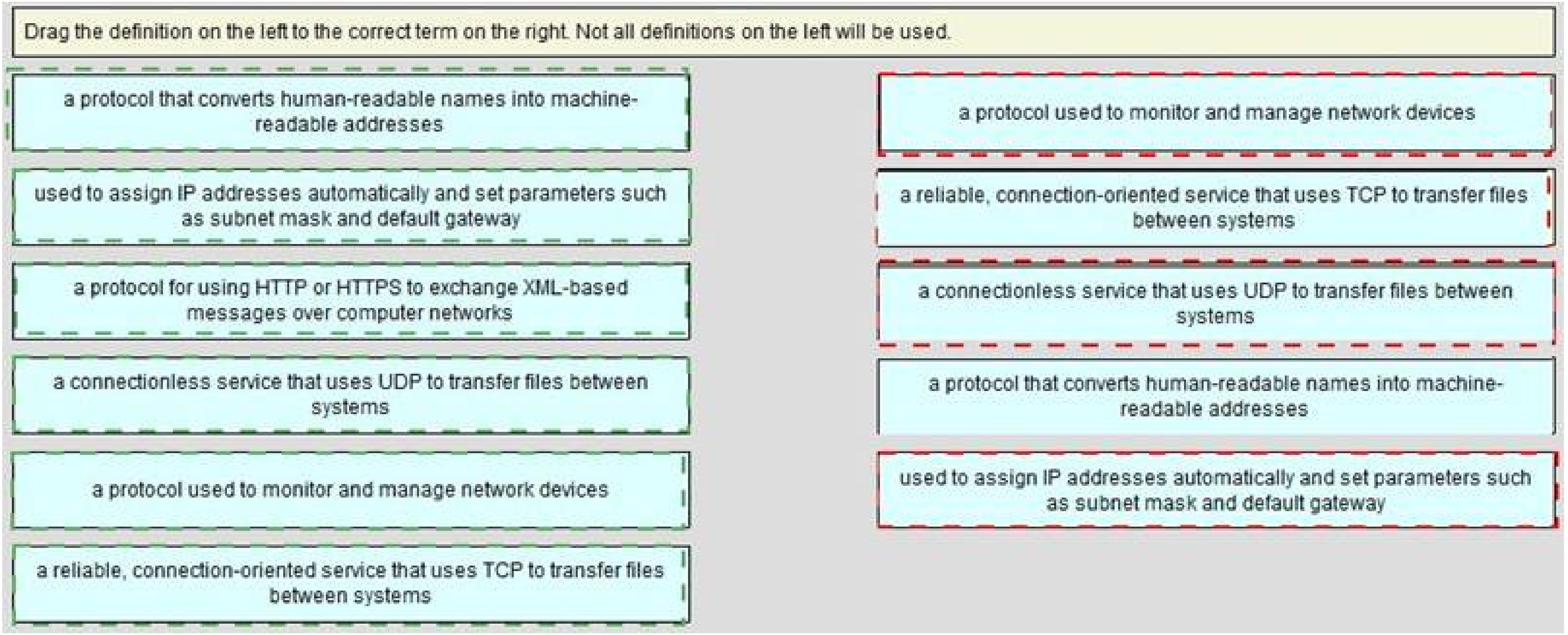
TFTP

DNS

DHCP

**Answer:**

**Explanation:**



Drag the definition on the left to the correct term on the right. Not all definitions on the left will be used.

a protocol that converts human-readable names into machine-readable addresses

used to assign IP addresses automatically and set parameters such as subnet mask and default gateway

a protocol for using HTTP or HTTPS to exchange XML-based messages over computer networks

a connectionless service that uses UDP to transfer files between systems

a protocol used to monitor and manage network devices

a reliable, connection-oriented service that uses TCP to transfer files between systems

a protocol used to monitor and manage network devices

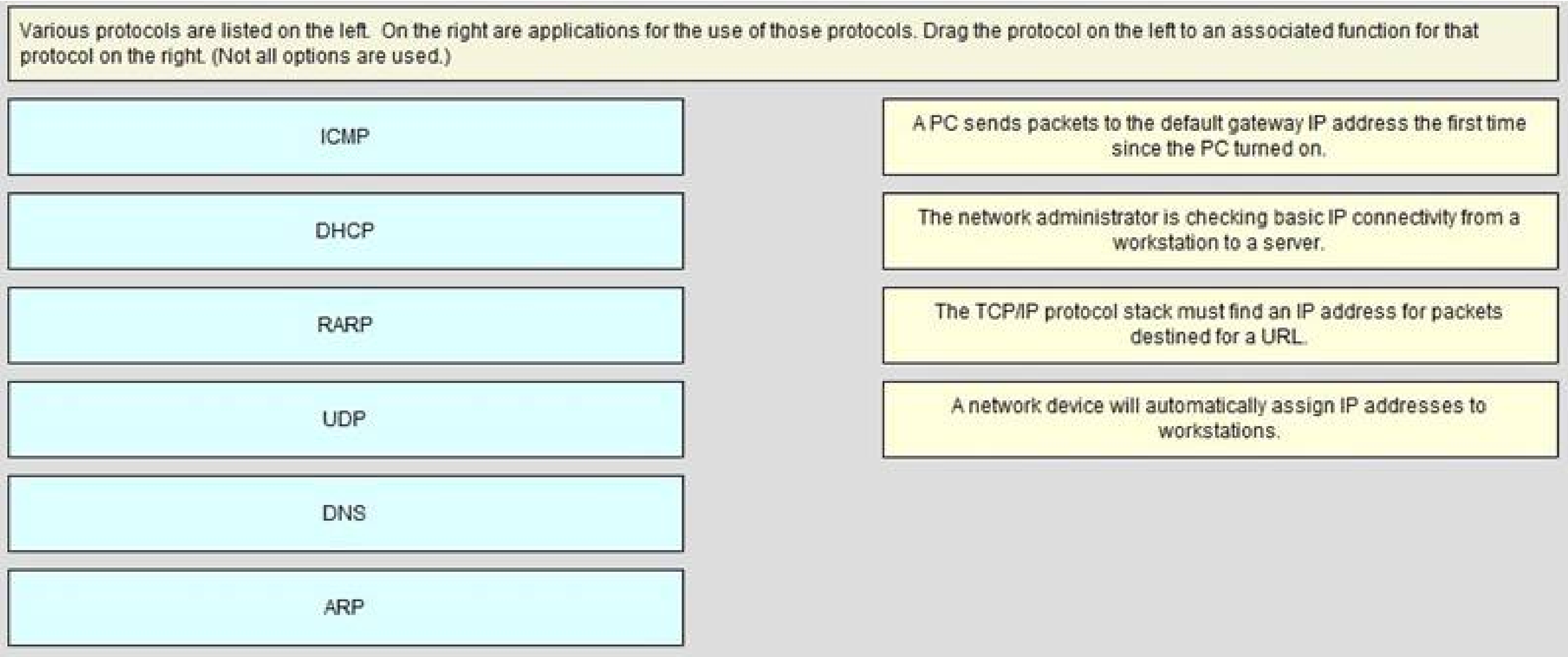
a reliable, connection-oriented service that uses TCP to transfer files between systems

a connectionless service that uses UDP to transfer files between systems

a protocol that converts human-readable names into machine-readable addresses

used to assign IP addresses automatically and set parameters such as subnet mask and default gateway

**NEW QUESTION 197**
DRAG DROP
Various protocols are listed on the left. On the right are applications for the use of those protocols. Drag the protocol on the left to an associated function for that protocol on the right. (Not all options are used.)



Various protocols are listed on the left. On the right are applications for the use of those protocols. Drag the protocol on the left to an associated function for that protocol on the right. (Not all options are used.)

ICMP

DHCP

RARP

UDP

DNS

ARP

A PC sends packets to the default gateway IP address the first time since the PC turned on.

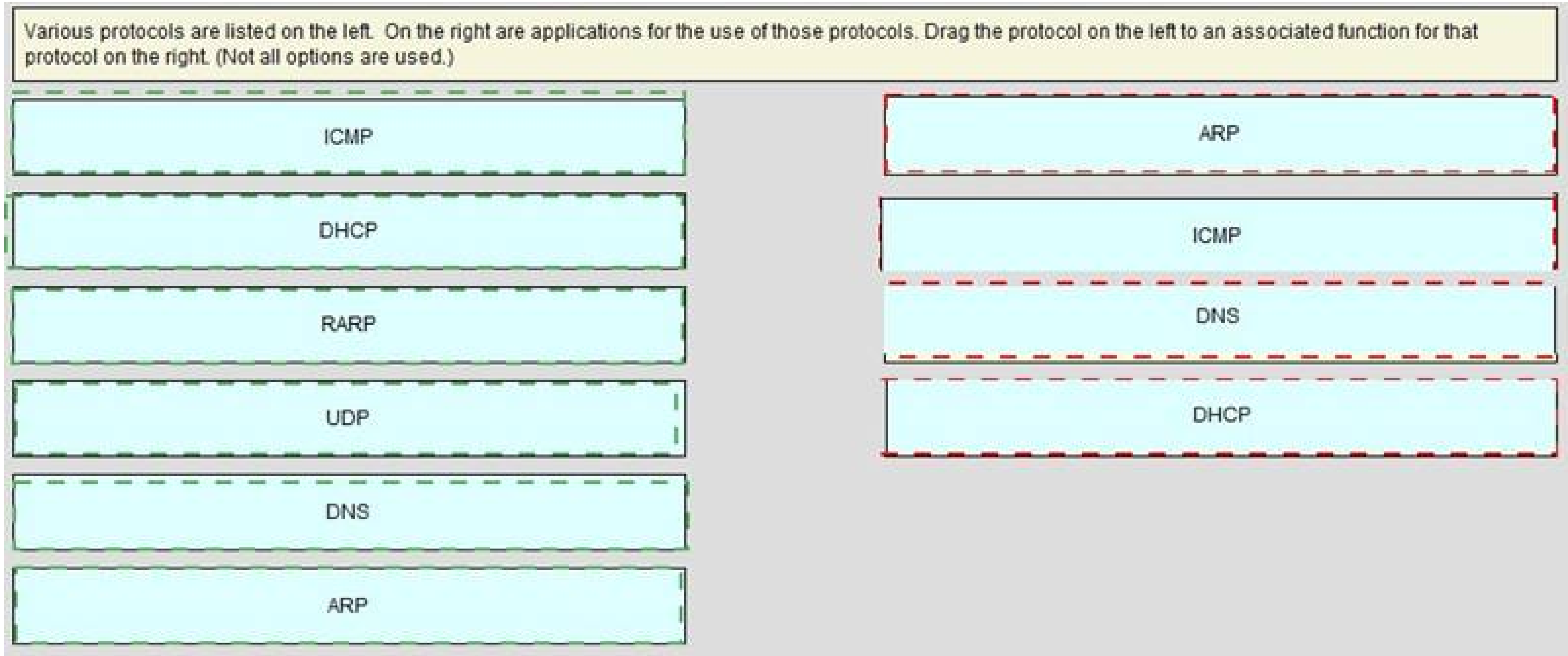
The network administrator is checking basic IP connectivity from a workstation to a server.

The TCP/IP protocol stack must find an IP address for packets destined for a URL.

A network device will automatically assign IP addresses to workstations.

**Answer:**

**Explanation:**



Various protocols are listed on the left. On the right are applications for the use of those protocols. Drag the protocol on the left to an associated function for that protocol on the right. (Not all options are used.)

ICMP

DHCP

RARP

UDP

DNS

ARP

ARP

ICMP

DNS

DHCP

**NEW QUESTION 200**
A network administrator cannot connect to a remote router by using SSH. Part of the show interfaces command is shown.
router#show interfaces
Serial0/1/0 is up, line protocol is down
At which OSI layer should the administrator begin troubleshooting?

A. physical

B. data link
C. network
D. transport

**Answer:** B

**Explanation:** https://learningnetwork.cisco.com/thread/12389
I think the indication here is "Serial 0 is up, line protocol is down". What causes this indication? Correct me if I am wrong. When you have this indication, a cable unplugged is
not a correct answer. If you check the output of your "show interface serial 0" command again, you should notice it as "Serial 0 is down, line protocol is down. Under the "show ip int brief" you should see status = down and protocol = down as opposed to up, down. Because you disconnected the cable, layer 1 will go down, which is indicated by the serial 0 down status. The line protocol status is for layer 2. So, a cable unplugged is not a correct answer to "Serial 0 is up, line protocol is down". Up/down means that the physical layer is OK, but there is a problem with the data link link (line protocol).

**NEW QUESTION 205**
Which of the following statements are TRUE regarding Cisco access lists? (Choose two.)

A. In an inbound access list, packets are filtered as they enter an interface.
B. In an inbound access list, packets are filtered before they exit an interface.
C. Extended access lists are used to filter protocol-specific packets.
D. You must specify a deny statement at the end of each access list to filter unwanted traffic.
E. When a line is added to an existing access list, it is inserted at the beginning of the access list.

**Answer:** AC

**Explanation:** In an inbound access list, packets are filtered as they enter an interface. Extended access lists are used to filter protocol specific packets. Access lists can be used in a variety of situations when the router needs to be given guidelines for decision-making. These situations include:
Filtering traffic as it passes through the router To control access to the VTY lines (Telnet)
To identify "interesting" traffic to invoke Demand Dial Routing (DDR) calls To filter and control routing updates from one router to another
There are two types of access lists, standard and extended. Standard access lists are applied as close to the destination as possible (outbound), and can only base their filtering criteria on the source IP address. The number used while creating an access list specifies the type of access list created. The range used for standard access lists is 1 to 99 and 1300 to 1999. Extended access lists are applied as close to the source as possible (inbound), and can base their filtering criteria on the source or destination IP address, or on the specific protocol being used. The range used for extended access lists is 100 to 199 and 2000 to 2699.
Other features of access lists include:
Inbound access lists are processed before the packet is routed.
Outbound access lists are processed after the packet has been routed to an exit interface. An "implicit deny" is at the bottom of every access list, which means that if a packet has not matched any preceding access list condition, it will be filtered (dropped).
Access lists require at least one permit statement, or all packets will be filtered (dropped). One access list may be configured per direction for each Layer 3 protocol configured on an interface The option stating that in an inbound access list, packets are filtered before they exit an interface is incorrect.
Packets are filtered as they exit an interface when using an outbound access list.
The option stating that a deny statement must be specified at the end of each access list in order to filter unwanted traffic is incorrect. There is an implicit deny at the bottom of every access list.
When a line is added to an existing access list, it is not inserted at the beginning of the access list. It is inserted at the end. This should be taken into consideration. For example, given the following access list, executing the command access-list 110 deny tcp 192.168.5.0 0.0.0.255 any eq www would have NO effect on the packets being filtered because it would be inserted at the end of the list, AFTER the line that allows all traffic.
access-list 110 permit ip host 192.168.5.1 any
access-list 110 deny icmp 192.168.5.0 0.0.0.255 any echo access-list 110 permit any any

**NEW QUESTION 208**
In the configuration of NAT, what does the keyword overload signify?

A. When bandwidth is insufficient, some hosts will not be allowed to access network translation.
B. The pool of IP addresses has been exhausted.
C. Multiple internal hosts will use one IP address to access external network resources.
D. If the number of available IP addresses is exceeded, excess traffic will use the specified address pool.

**Answer:** C

**Explanation:** The keyword overload used in theip nat inside source list 1 pool ovrld overload example command allows NAT to translate multiple inside devices to the single address in the pool.
The types of NAT include:
Static address translation (static NAT)—Allows one-to-one mapping between local and global addresses.
Dynamic address translation (dynamic NAT)—Maps unregistered IP addresses to registered IP addresses from a pool of registered IP addresses.
Overloading—Maps multiple unregistered IP addresses to a single registered IP address (many to one) using different ports. This method is also known as Port Address Translation (PAT). By using overloading, thousands of users can be connected to the Internet by using only one real global IP address.

**NEW QUESTION 209**
What happens when computers on a private network attempt to connect to the Internet through a Cisco router running PAT?

A. The router uses the same IP address but a different TCP source port number for each connection.
B. An IP address is assigned based on the priority of the computer requesting the connection.
C. The router selects an address from a pool of one-to-one address mappings held in the lookup table.
D. The router assigns a unique IP address from a pool of legally registered addresses for the duration of the connection.

**Answer:** A

**Explanation:** Reference: http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/nat_staticpat.html

Static PAT translations allow a specific UDP or TCP port on a global address to be translated to a specific port on a local address. That is, both the address and the port numbers are translated.
Static PAT is the same as static NAT, except that it enables you to specify the protocol (TCP or UDP) and port for the real and mapped addresses. Static PAT enables you to identify the same mapped address across many different static statements, provided that the port is different for each statement. You cannot use the same mapped address for multiple static NAT statements.
Port Address Translation makes the PC connect to the Internet but using different TCP source port.

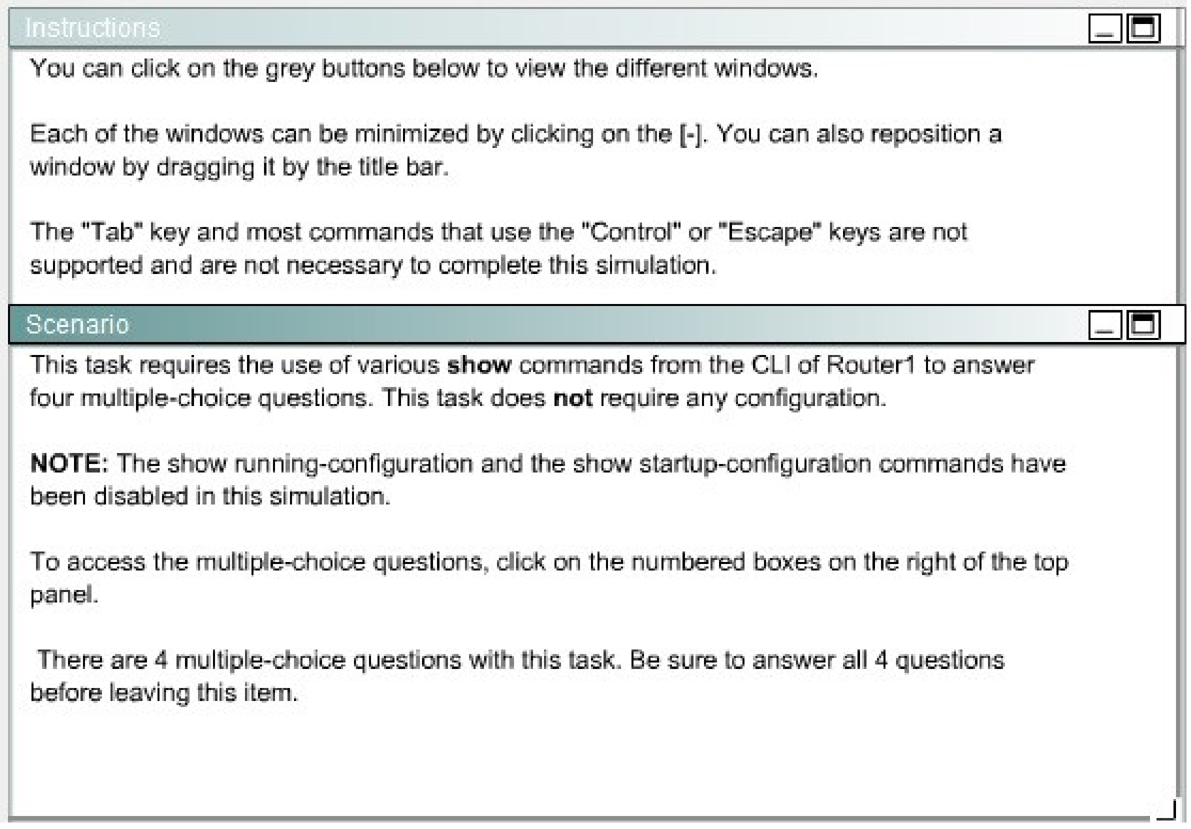
**NEW QUESTION 214**
How many addresses will be available for dynamic NAT translation when a router is configured with the following commands?
Router(config)#ip nat pool TAME 209.165.201.23 209.165.201.30 netmask 255.255.255.224
Router(config)#ip nat inside source list 9 pool TAME

A. 7
B. 8
C. 9
D. 10
E. 24
F. 32

**Answer:** B

**Explanation:** 209.165.201.23 to 209.165.201.30 provides for 8 addresses.

**NEW QUESTION 218**



Instructions

You can click on the grey buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation.

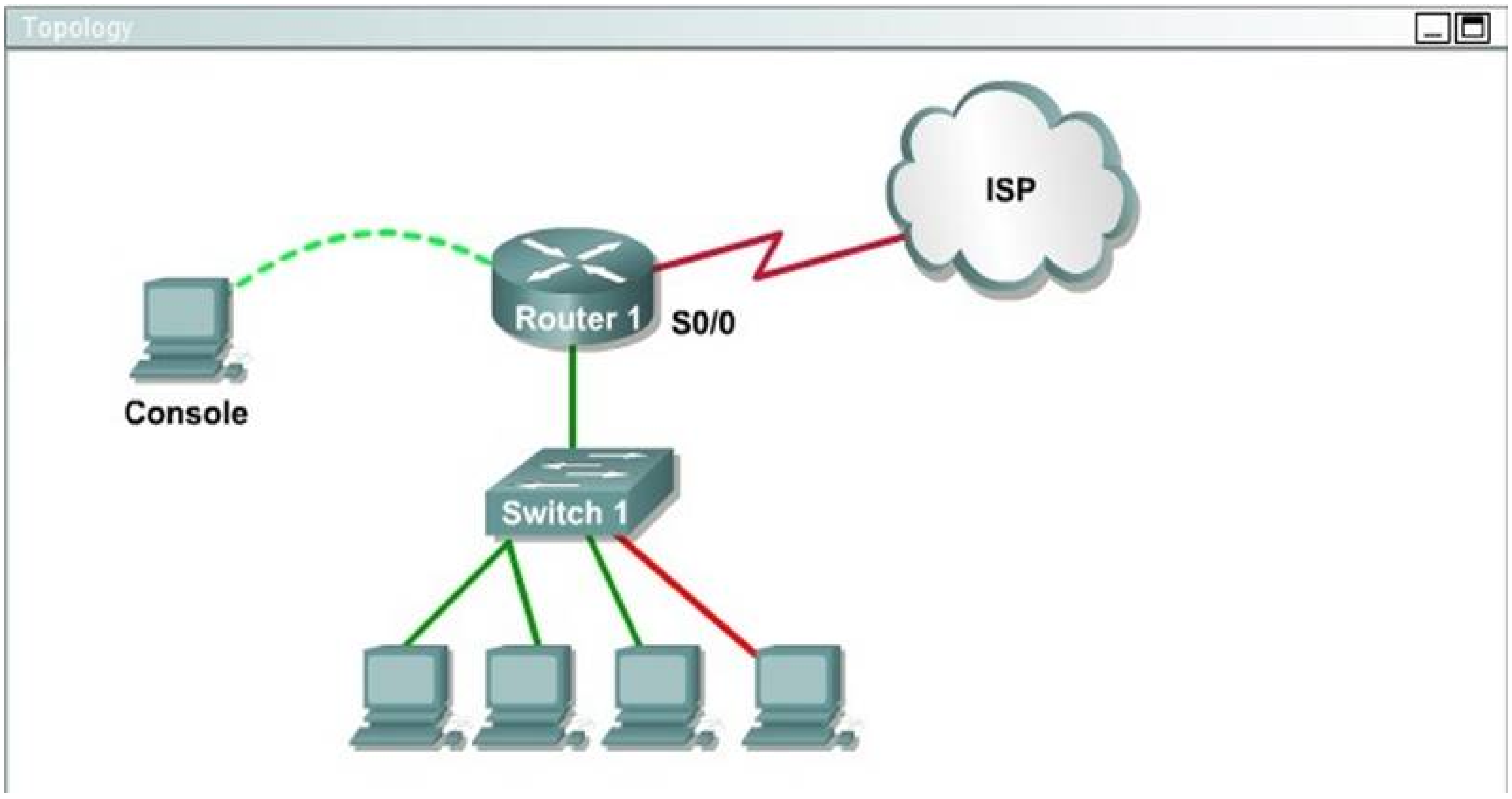
Scenario

This task requires the use of various **show** commands from the CLI of Router1 to answer four multiple-choice questions. This task does **not** require any configuration.

**NOTE:** The show running-configuration and the show startup-configuration commands have been disabled in this simulation.

To access the multiple-choice questions, click on the numbered boxes on the right of the top panel.

There are 4 multiple-choice questions with this task. Be sure to answer all 4 questions before leaving this item.



```
Press RETURN to get started!
Router1>
```

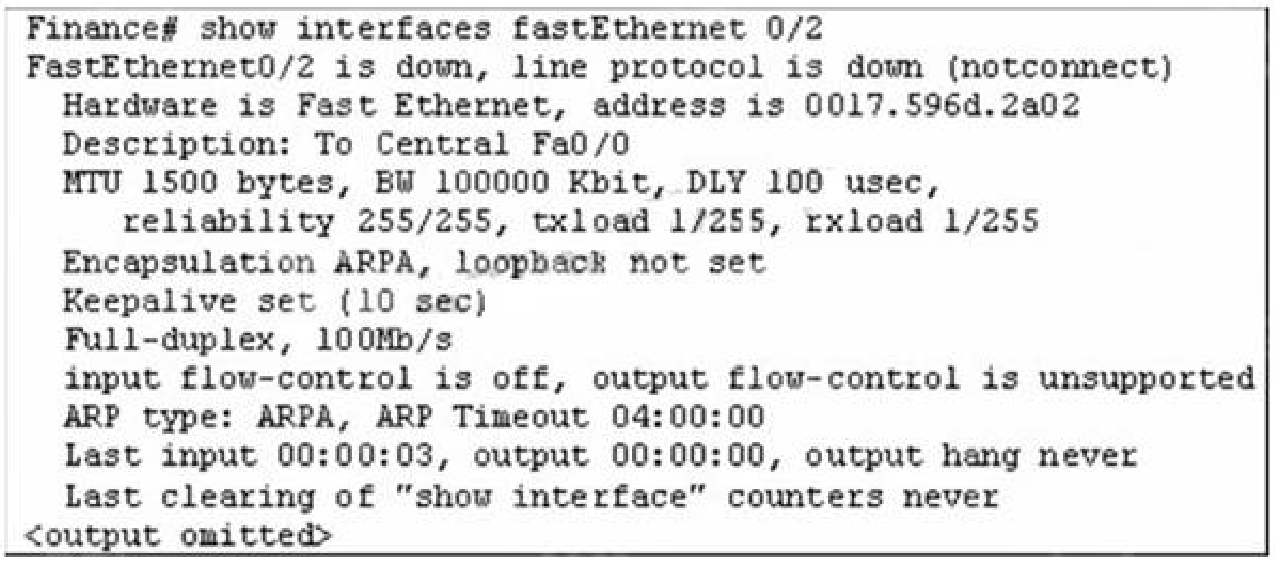
What is the subnet broadcast address of the LAN connected to Router1?

A. 192.168.8.15
B. 192.168.8.31
C. 192.168.8.63
D. 192.168.8.127

**Answer:** A

**Explanation:** The IP address assigned to FA0/1 is 192.168.8.9/29, making 192.168.8.15 the broadcast address.

**NEW QUESTION 222**
Refer to the exhibit.



```
Finance# show interfaces fastEthernet 0/2
FastEthernet0/2 is down, line protocol is down (notconnect)
  Hardware is Fast Ethernet, address is 0017.596d.2a02
  Description: To Central Fa0/0
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:03, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
<output omitted>
```

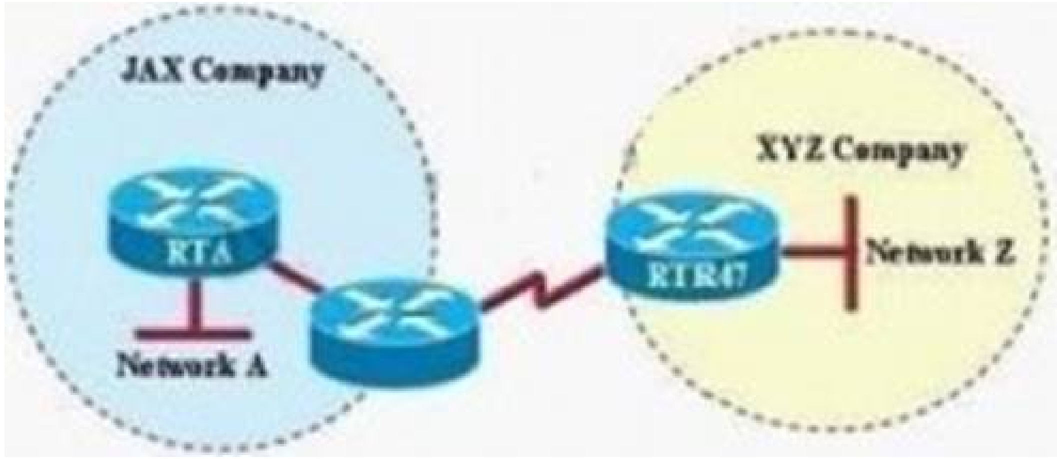
An administrator replaced the 10/100 Mb NIC in a desktop PC with a 1 Gb NIC and now the PC will not connect to the network. The administrator began troubleshooting on the switch. Using the switch output shown, what is the cause of the problem?

A. Speed is set to 100Mb/s.
B. Input flow control is off.
C. Encapsulation is set to ARPA.
D. The port is administratively down.
E. The counters have never been cleared.

**Answer:** A

**Explanation:** For PC to switch connectivity, the speed settings must match. In this case, the 1 Gb NIC will not be able to communicate with a 100Mb fast Ethernet interface, unless the 1Gb NIC can be configured to connect at 100Mb.

**NEW QUESTION 224**
Refer to the exhibit.



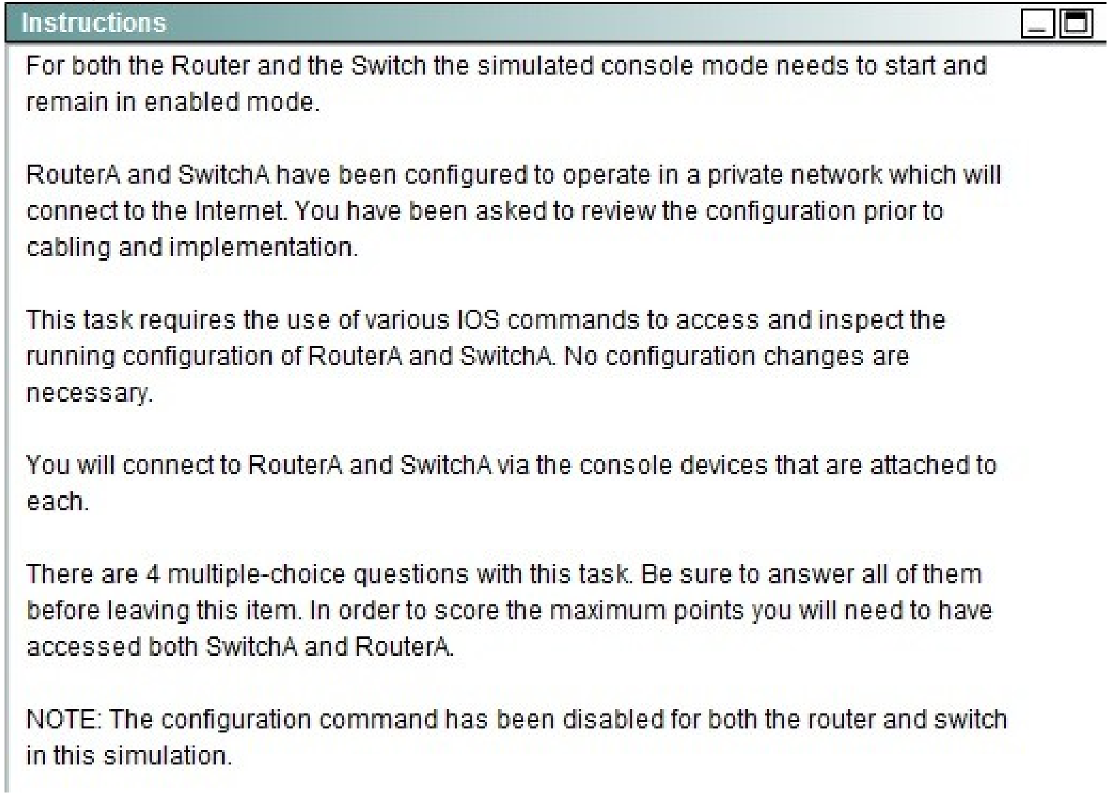
A person is trying to send a file from a host on Network A of the JAX Company to a server on Network Z of the XYZ Company. The file transfer fails. The host on Network A can communicate with other hosts on Network A.
Which command, issued from router RTA, would be the most useful for troubleshooting this problem?

A. show flash:
B. show history
C. show version
D. show interfaces
E. show controllers serial

**Answer:** D

**Explanation:** The most useful thing to check on RTA would be the show interfaces command to see if the interface toward the WAN link is up. The most likely scenario is that the local LAN interface is up, but the other interface toward the XYZ company is down.

**NEW QUESTION 226**



For both the Router and the Switch the simulated console mode needs to start and remain in enabled mode.

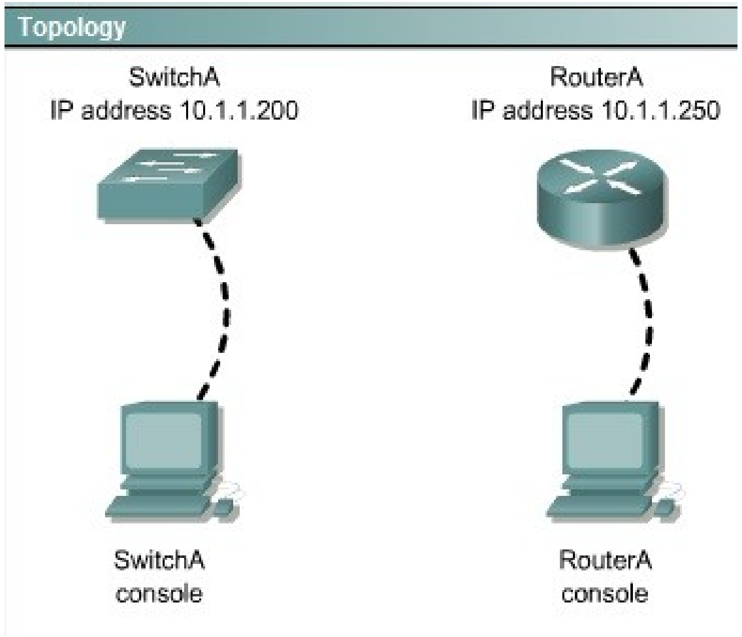
RouterA and SwitchA have been configured to operate in a private network which will connect to the Internet. You have been asked to review the configuration prior to cabling and implementation.

This task requires the use of various IOS commands to access and inspect the running configuration of RouterA and SwitchA. No configuration changes are necessary.

You will connect to RouterA and SwitchA via the console devices that are attached to each.

There are 4 multiple-choice questions with this task. Be sure to answer all of them before leaving this item. In order to score the maximum points you will need to have accessed both SwitchA and RouterA.

NOTE: The configuration command has been disabled for both the router and switch in this simulation.



Select three options which are security issues with the current configuration of SwitchA. (Choose three.)

A. Privilege mode is protected with an unencrypted password
B. Inappropriate wording in banner message
C. Virtual terminal lines are protected only by a password requirement
D. Both the username and password are weak
E. Telnet connections can be used to remotely manage the switch
F. Cisco user will be granted privilege level 15 by default

**Answer:** ABD

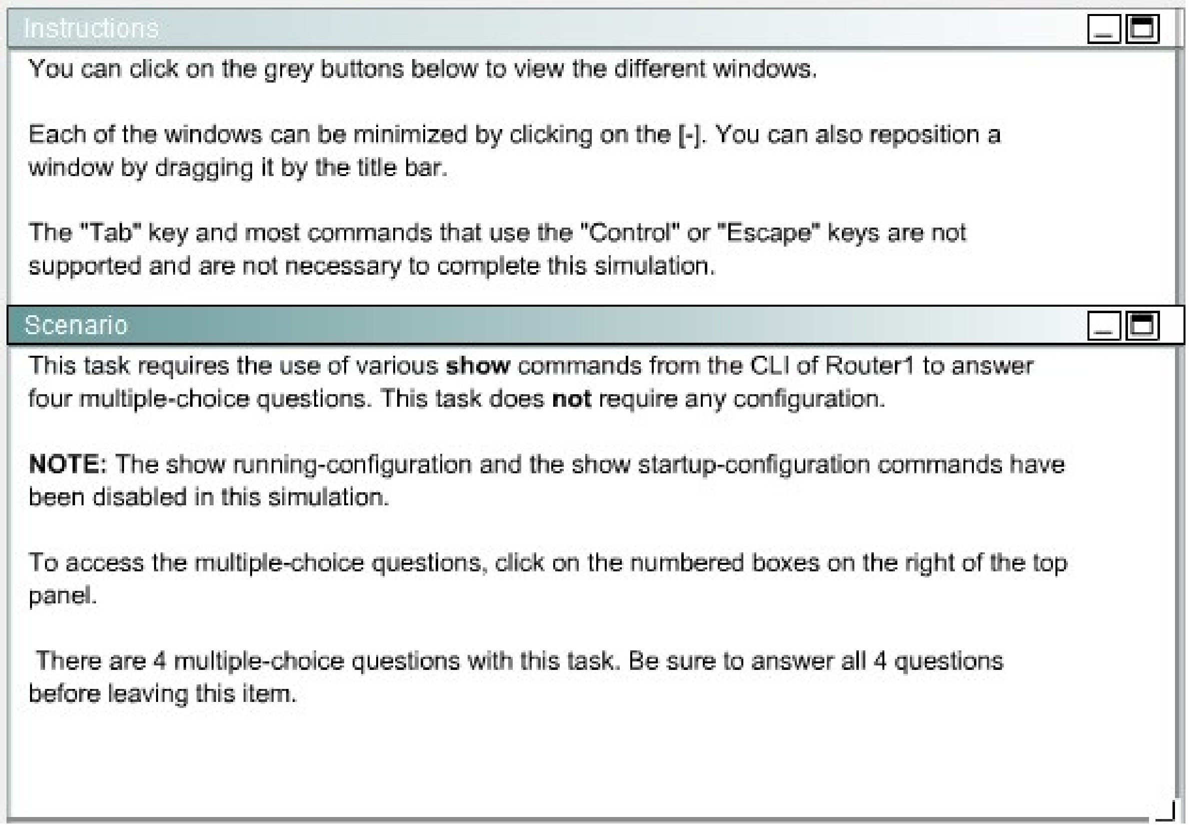
**NEW QUESTION 230**
An administrator has connected devices to a switch and, for security reasons, wants the dynamically learned MAC addresses from the address table added to the running configuration.
What must be done to accomplish this?

A. Enable port security and use the keyword sticky.
B. Set the switchport mode to trunk and save the running configuration.
C. Use the switchport protected command to have the MAC addresses added to the configuration.
D. Use the no switchport port-security command to allow MAC addresses to be added to the configuration.

**Answer:** A

**Explanation:** http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide
/port_sec.pdf
One can configure MAC addresses to be sticky. These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, the interface does not need to dynamically relearn them when the switch restarts, hence enabling security as desired.

**NEW QUESTION 231**



Instructions

You can click on the grey buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation.

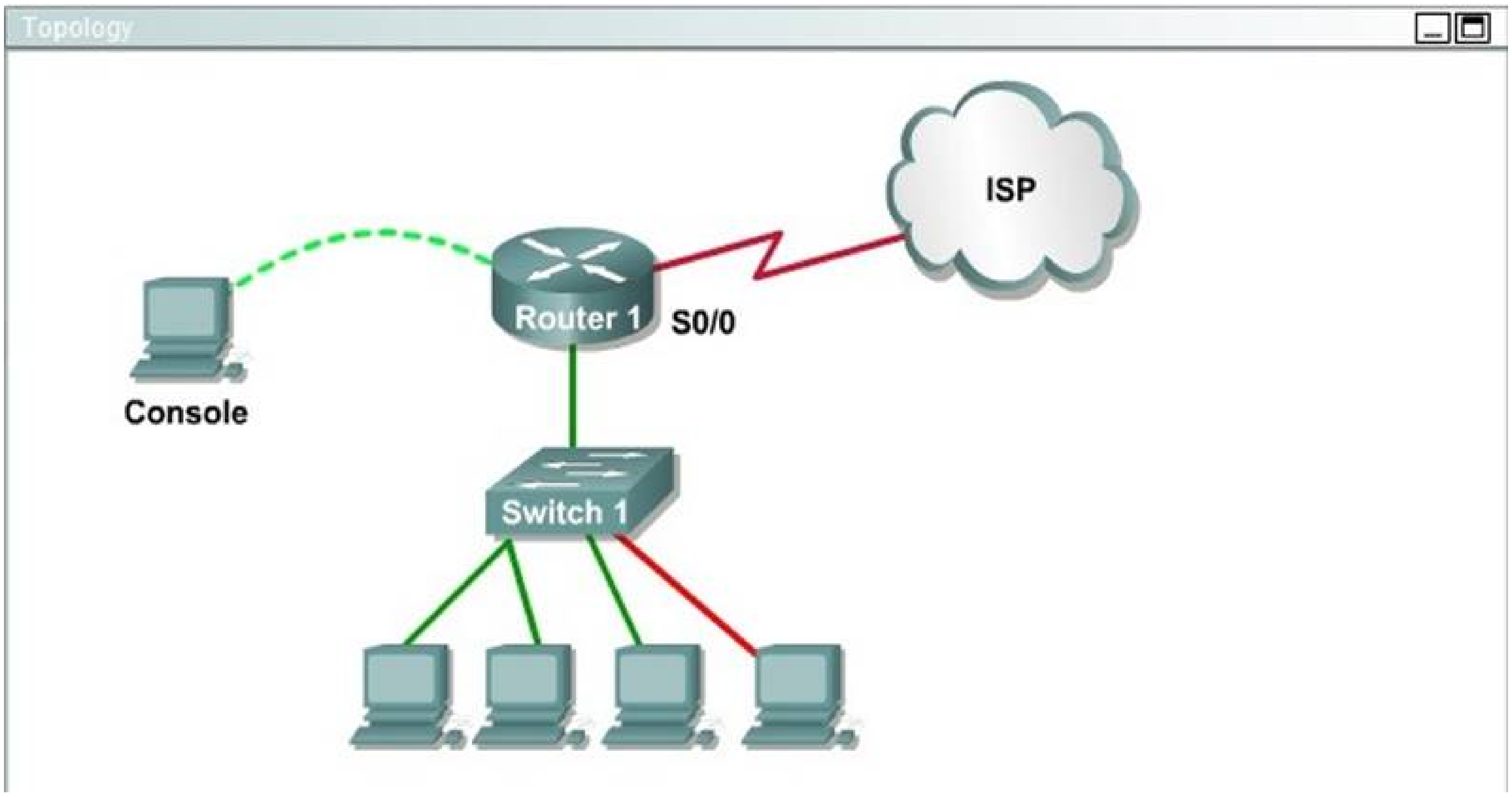
Scenario

This task requires the use of various **show** commands from the CLI of Router1 to answer four multiple-choice questions. This task does **not** require any configuration.

**NOTE:** The show running-configuration and the show startup-configuration commands have been disabled in this simulation.

To access the multiple-choice questions, click on the numbered boxes on the right of the top panel.

There are 4 multiple-choice questions with this task. Be sure to answer all 4 questions before leaving this item.



```
Press RETURN to get started!
Router1>
```

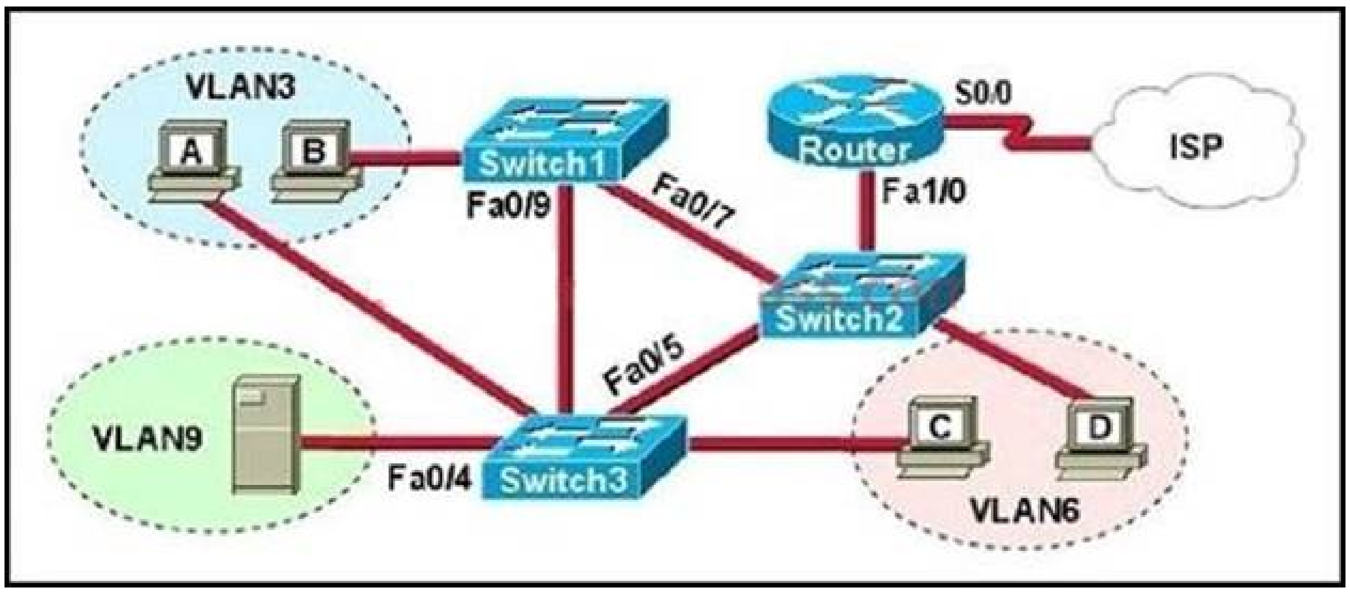
Including the address on the Routed Ethernet interface, how many hosts can have IP addresses on the LAN to which Routed is connected?

A. 6
B. 30
C. 62
D. 126

**Answer:** A

**Explanation:** This is a /29 address, so there are 6 usable IP's on this subnet.

**NEW QUESTION 236**
Refer to the exhibit.



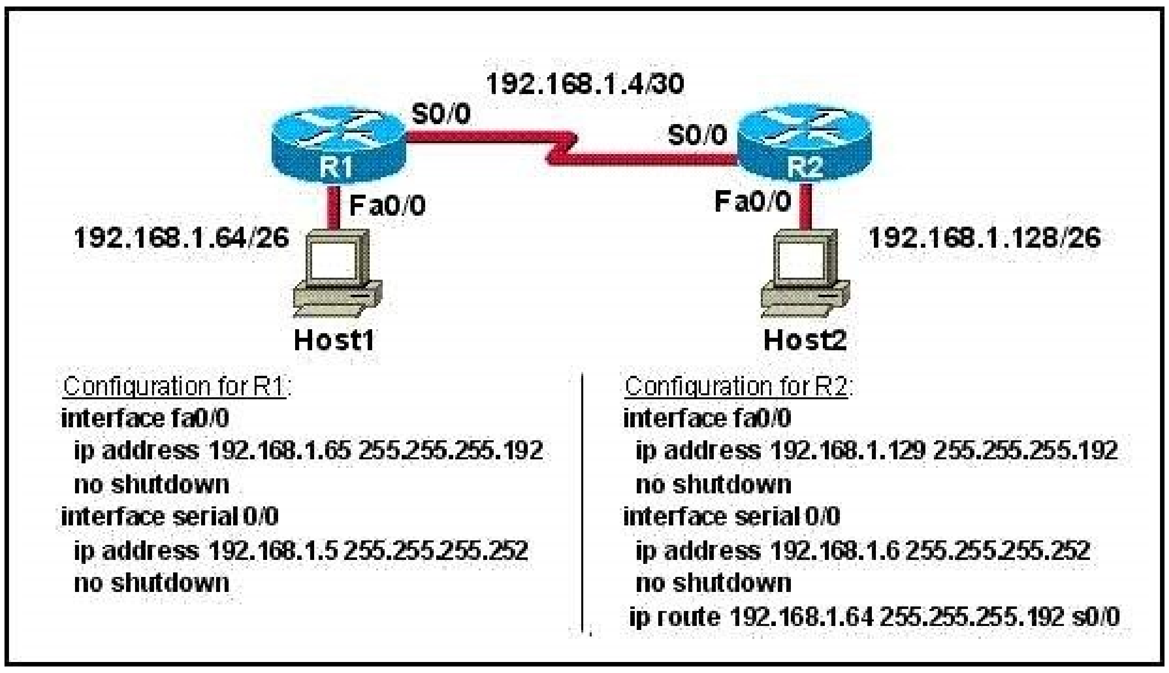
A problem with network connectivity has been observed. It is suspected that the cable connected to switch port Fa0/9 on Switch1 is disconnected. What would be an effect of this cable being disconnected?

A. Host B would not be able to access the server in VLAN9 until the cable is reconnected.
B. Communication between VLAN3 and the other VLANs would be disabled.
C. The transfer of files from Host B to the server in VLAN9 would be significantly slower.
D. For less than a minute, Host B would not be able to access the server in VLAN9. Then normal network function would resume.

**Answer:** D

**Explanation:** Because Switch1 has multiple redundant links in this network, traffic would not work for less than a minute, and then it would get rerouted along the longer path to the host. The 1 minute outage would be the length of time it takes STP to converge.

**NEW QUESTION 238**
Refer to the exhibit.



```
Configuration for R1:
interface fa0/0
 ip address 192.168.1.65 255.255.255.192
 no shutdown
interface serial 0/0
 ip address 192.168.1.5 255.255.255.252
 no shutdown
```

```
Configuration for R2:
interface fa0/0
 ip address 192.168.1.129 255.255.255.192
 no shutdown
interface serial 0/0
 ip address 192.168.1.6 255.255.255.252
 no shutdown
 ip route 192.168.1.64 255.255.255.192 s0/0
```

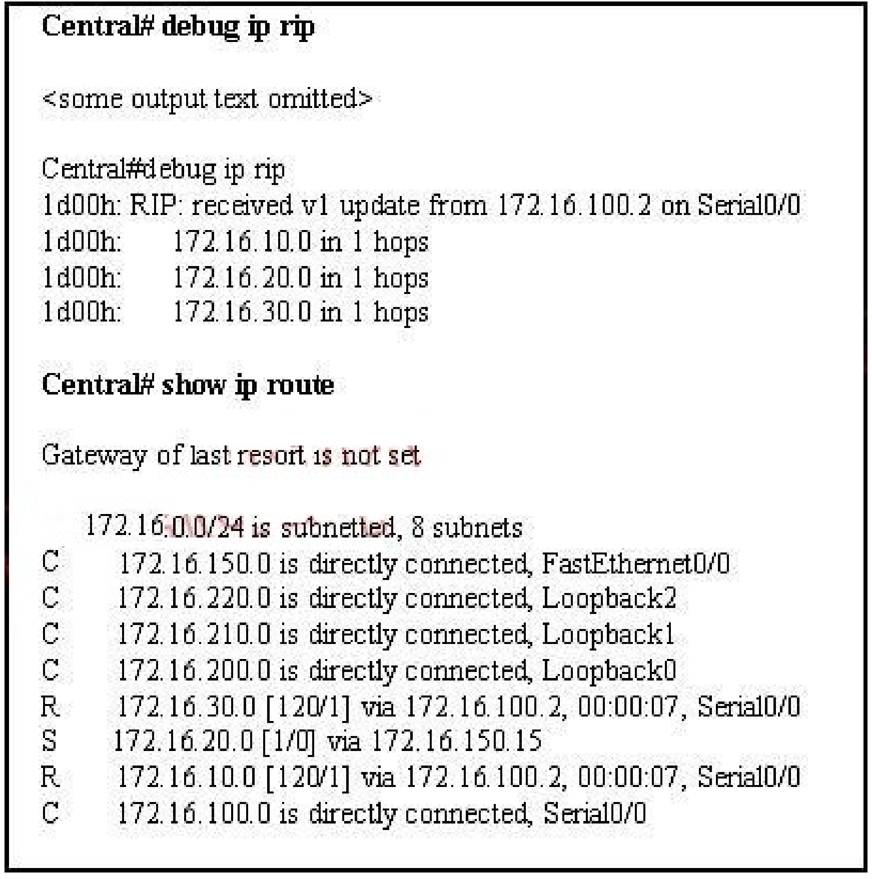
A technician pastes the configurations in the exhibit into the two new routers shown. Otherwise, the routers are configured with their default configurations. A ping from Host1 to Host 2 fails, but the technician is able to ping the S0/0 interface of R2 from Host 1. The configurations of the hosts have been verified as correct. What could be the cause of the problem?

A. The serial cable on R1 needs to be replaced.
B. The interfaces on R2 are not configured properly
C. R1 has no route to the 192.168.1.128 network.
D. The IP addressing scheme has overlapping subnetworks.
E. The ip subnet-zero command must be configured on both routers.

**Answer:** C

**Explanation:** Without a static route pointing to the host 2 network the router R1 is unaware of the path to take to reach that network and reply traffic cannot be sent.

**NEW QUESTION 241**
The network administrator has found the following problem.



```
Central# debug ip rip

<some output text omitted>

Central#debug ip rip
1d00h: RIP: received v1 update from 172.16.100.2 on Serial0/0
1d00h:      172.16.10.0 in 1 hops
1d00h:      172.16.20.0 in 1 hops
1d00h:      172.16.30.0 in 1 hops

Central# show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 8 subnets
C       172.16.150.0 is directly connected, FastEthernet0/0
C       172.16.220.0 is directly connected, Loopback2
C       172.16.210.0 is directly connected, Loopback1
C       172.16.200.0 is directly connected, Loopback0
R       172.16.30.0 [120/1] via 172.16.100.2, 00:00:07, Serial0/0
S      172.16.20.0 [1/0] via 172.16.150.15
R       172.16.10.0 [120/1] via 172.16.100.2, 00:00:07, Serial0/0
C       172.16.100.0 is directly connected, Serial0/0
```

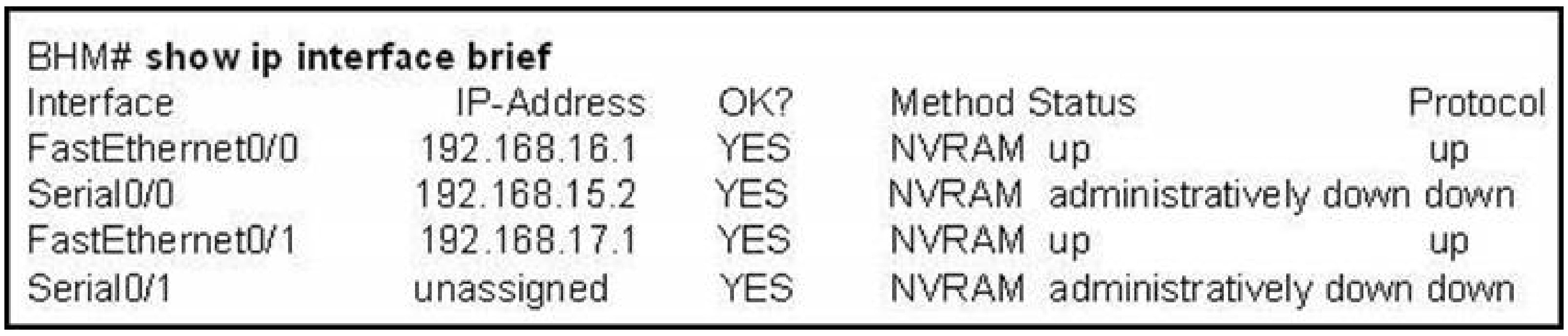
The remote networks 172.16.10.0, 172.16.20.0, and 172.16.30.0 are accessed through the Central router's serial 0/0 interface. No users are able to access 172.16.20.0. After reviewing the command output shown in the graphic, what is the most likely cause of the problem?

A. no gateway of last resort on Central
B. Central router's not receiving 172.16.20.0 update
C. incorrect static route for 172.16.20.0
D. 172.16.20.0 not located in Central's routing table

**Answer:** C

**Explanation:** If we use 172.16.20.0 to route to 172.16.150.15, then the packet will route back. To clear this error we have to use #no ip route 172.16.20.0 255.255.255.0 172.16.150.15
command in configuration mode.

**NEW QUESTION 243**
Refer to the exhibit.



```
BHM# show ip interface brief
Interface          IP-Address    OK?   Method Status                   Protocol
FastEthernet0/0    192.168.16.1  YES   NVRAM  up                       up
Serial0/0          192.168.15.2  YES   NVRAM  administratively down    down
FastEthernet0/1    192.168.17.1  YES   NVRAM  up                       up
Serial0/1          unassigned    YES   NVRAM  administratively down    down
```

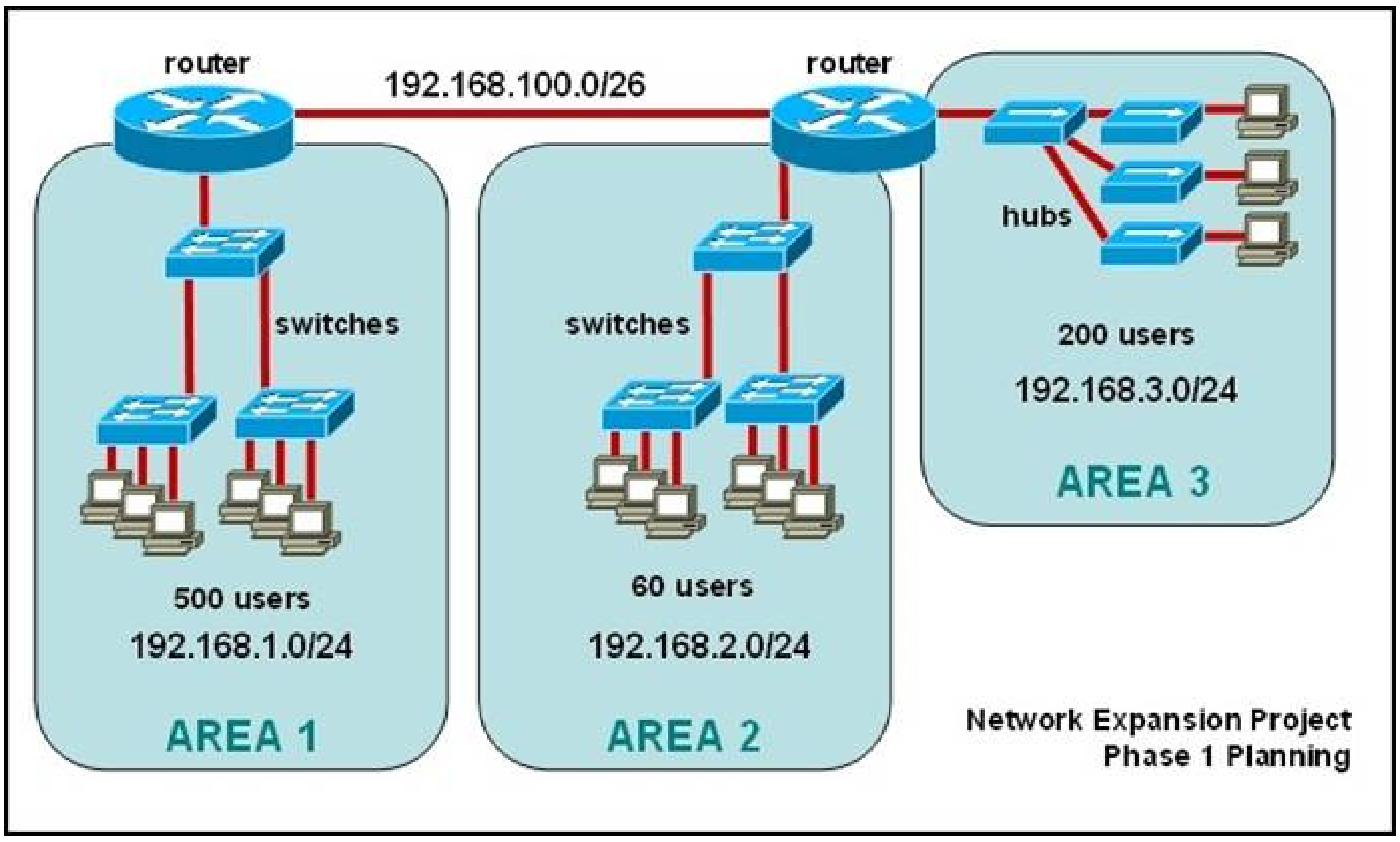
Serial 0/0 does not respond to a ping request from a host on the FastEthernet 0/0 LAN. How can this problem be corrected?

A. Enable the Serial 0/0 interface.
B. Correct the IP address for Serial 0/0.
C. Correct the IP address for FastEthernet 0/0
D. Change the encapsulation type on Serial 0/0
E. Enable autoconfiguration on the Serial 0/0 interface

**Answer:** A

**Explanation:** Serial 0/0 interface is administratively down therefore, you will have to run the "no shutdown" command to enable the interface for data.

**NEW QUESTION 246**
Refer to the exhibit.



The junior network support staff provided the diagram as a recommended configuration for the first phase of a four-phase network expansion project. The entire network expansion will have over 1000 users on 14 network segments and has been allocated this IP address space.

**Answer:**

**NEW QUESTION 251**
168.1.1 through 192.168.5.255
192.168.100.1 through 192.168.100.255
What are three problems with this design? (Choose three.)

A. The AREA 1 IP address space is inadequate for the number of users.
B. The AREA 3 IP address space is inadequate for the number of users.
C. AREA 2 could use a mask of /25 to conserve IP address space.
D. The network address space that is provided requires a single network-wide mask.
E. The router-to-router connection is wasting address space.
F. The broadcast domain in AREA 1 is too large for IP to function.

**Answer:** ACE

**Explanation:** Do a “show ip int brief” and you will see that Fa0/1 has an IP address assigned, but it is shut down.

**NEW QUESTION 256**
What is the purpose of the switchport command?
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security mac-address 0018.DE8B.4BF8

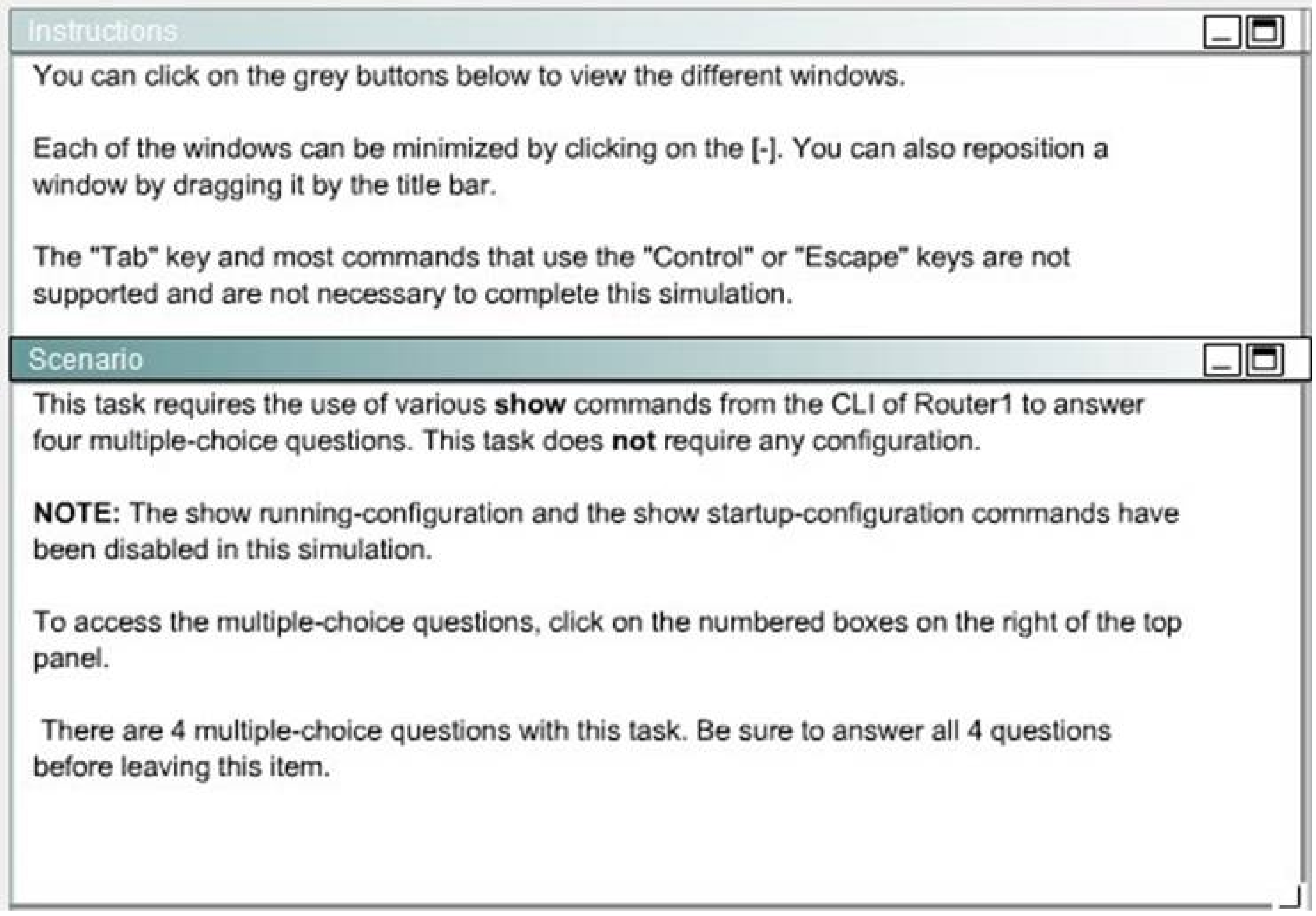
A. It ensures that only the device with the MAC address 0018.DE8B.4BF8 will be able to connect to the port that is being configured.

B. It informs the switch that traffic destined for MAC address 0018.DE8B.4BF8 should only be sent to the port that is being configured.
C. It will act like an access list and the port will filter packets that have a source or destination MAC of 0018.DE8B.4BF8.
D. The switch will shut down the port of any traffic with source MAC address of 0018.DE8B.4BF8.

**Answer:** A

**Explanation:** The first command configurs the maximum number of secure MAC addresses on a port to one. The next command specifies that MAC addresses that are allowed with port security; in this case it is just the one single device MAC. If any other device connects on that port the port will be shut down by the port security feature.

**NEW QUESTION 257**



Instructions

You can click on the grey buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation.

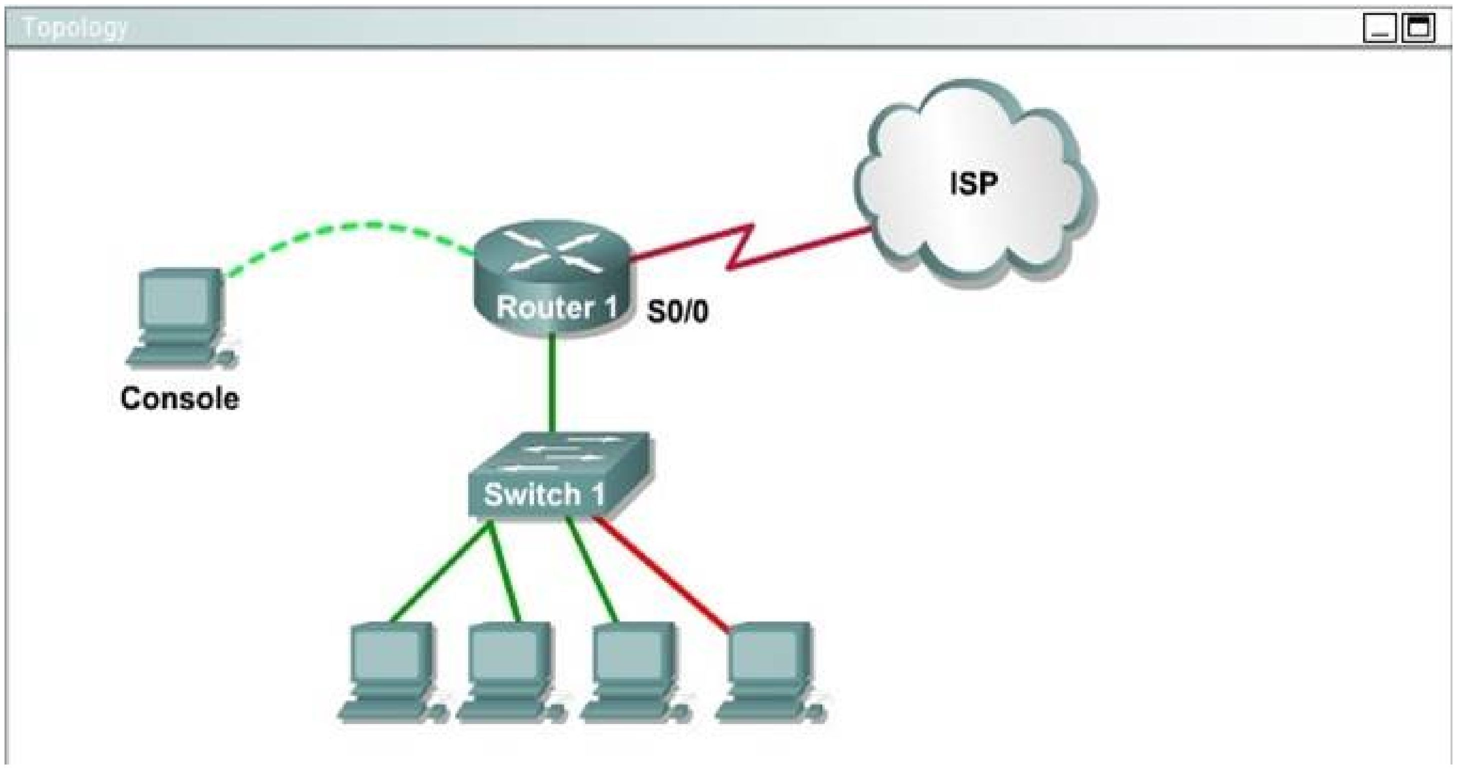
Scenario

This task requires the use of various **show** commands from the CLI of Router1 to answer four multiple-choice questions. This task does **not** require any configuration.

**NOTE:** The show running-configuration and the show startup-configuration commands have been disabled in this simulation.

To access the multiple-choice questions, click on the numbered boxes on the right of the top panel.

There are 4 multiple-choice questions with this task. Be sure to answer all 4 questions before leaving this item.



```
Press RETURN to get started!
Router1>
```

What is the bandwidth on the WAN interface of Router 1?

A. 16 Kbit/sec
B. 32 Kbit/sec
C. 64 Kbit/sec
D. 128 Kbit/sec
E. 512 Kbit/sec
F. 1544 Kbit/sec

**Answer:** A

**Explanation:** Use the “show interface s0/0” to see the bandwidth set at 16 Kbit/sec.
The show interface s0/0 command results will look something like this and the bandwidth will be represented by the "BW" on the fourth line as seen below where BW equals 1544 Kbits/sec.
R2#show interface serial 0/0 Serial0/0 is up, line protocol is down Hardware is GT96K Serial
Internet address is 10.1.1.5/30
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 uses.

**NEW QUESTION 261**
A receiving host has failed to receive all of the segments that it should acknowledge. What can the host do to improve the reliability of this communication session?

A. decrease the window size
B. use a different source port for the session
C. decrease the sequence number
D. obtain a new IP address from the DHCP server
E. start a new session using UDP

**Answer:** A

**Explanation:** The Window bit in the header determines the number of segments that can be sent at a time. This is done to avoid overwhelming the destination. At the start of the session the window in small but it increases over time. The destination host can also decrease the window to slow down the flow. Hence the window is called the sliding window. When the source has sent the number of segments allowed by the window, it cannot send any further segments till an acknowledgement is received from the destination. On networks with high error rates or issues, decreasing the window size can result in more reliable transmission, as the receiver will need to acknowledge fewer segments. With a large window size, the sender will need to resend all the frames if a single one is not received by the receiver.

**NEW QUESTION 266**
From which of the following attacks can Message Authentication Code (MAC) shield your network?

A. DoS
B. DDoS
C. spoofing
D. SYN floods

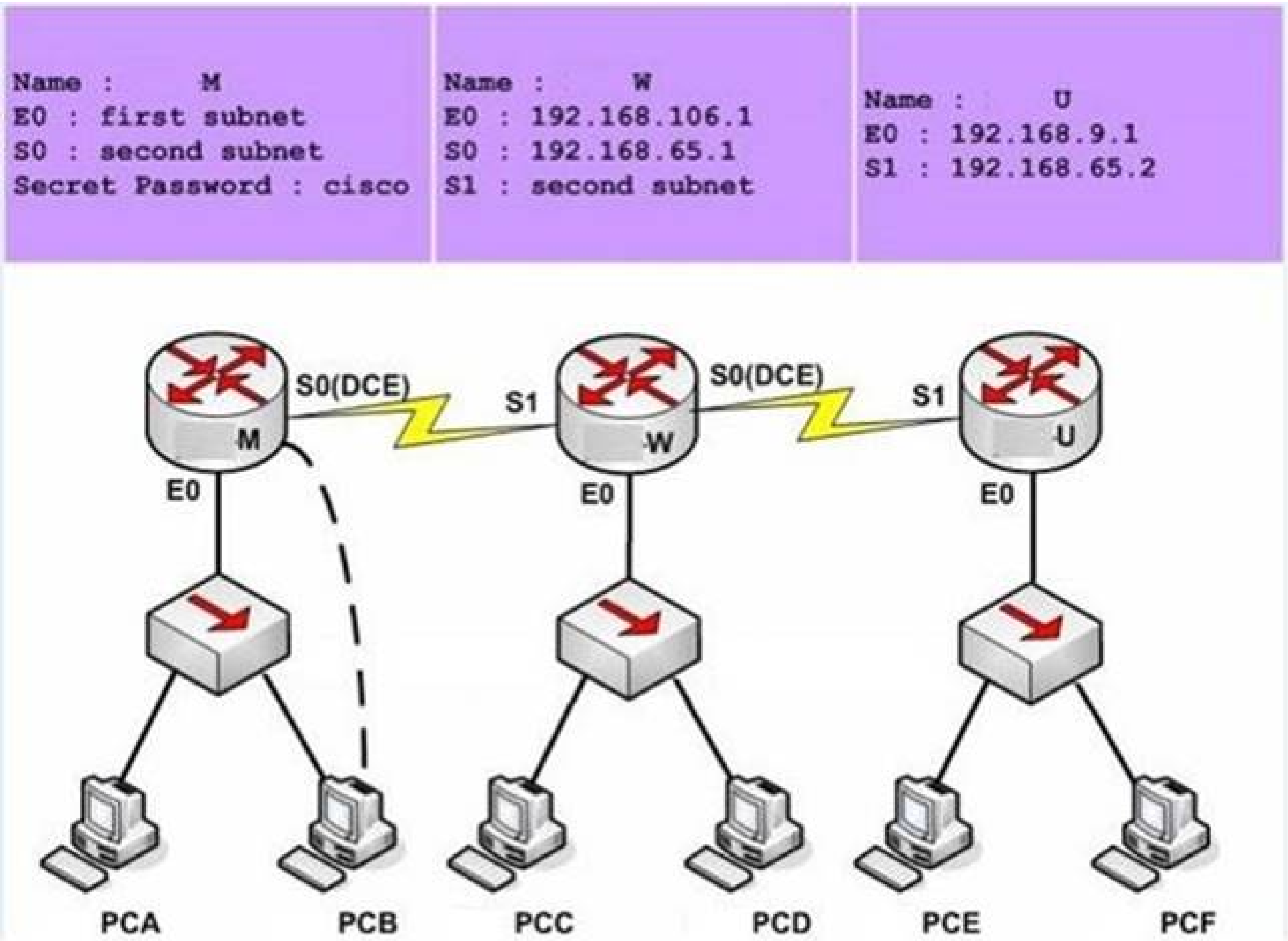
**Answer:** C

**Explanation:** Message Authentication Code (MAC) can shield your network from spoofing attacks. Spoofing, also known as masquerading, is a popular trick in

which an attacker intercepts a network packet, replaces the source address of the packets header with the address of the authorized host, and reinserts fake information which is sent to the receiver. This type of attack involves modifying packet contents. MAC can prevent this type of attack and ensure data integrity by ensuring that no data has changed. MAC also protects against frequency analysis, sequence manipulation, and ciphertext-only attacks.
MAC is a secure message digest that requires a secret key shared by the sender and receiver, making it impossible for sniffers to change both the data and the MAC as the receiver can detect the changes.
A denial-of-service (DoS) attack floods the target system with unwanted requests, causing the loss of service to users. One form of this attack generates a flood of packets requesting a TCP connection with the target, tying up all resources and making the target unable to service other requests. MAC does not prevent DoS attacks. Stateful packet filtering is the most common defense against a DoS attack.
ADistributed Denial of Service attack (DDoS) occurs when multiple systems are used to
flood the network and tax the resources of the target system. Various intrusion detection systems, utilizing stateful packet filtering, can protect against DDoS attacks.
In a SYN flood attack, the attacker floods the target with spoofed IP packets and causes it to either freeze or crash. A SYN flood attack is a type of denial of service attack that exploits the buffers of a device that accept incoming connections and therefore cannot be prevented by MAC. Common defenses against a SYN flood attack include filtering, reducing the SYN-RECEIVED timer, and implementing SYN cache or SYN cookies.

Topic 6, Simulation

**NEW QUESTION 268**
CORRECT TEXT
There are three locations in a school district of a large city: ROUTER -M, ROUTER -W and ROUTER -U. The network connection between two of these locations has already functioned. Configure the ROUTER -M router IP addresses on the E0 and S0 interfaces so that the E0 receives the first usable subnet while the S0 receives the second usable subnet from the network 192.168.160.0/28. Both interfaces would receive the last available ip address on the proper subnet.



```
Name :      M
E0 : first subnet
S0 : second subnet
Secret Password : cisco
```

```
Name :      W
E0 : 192.168.106.1
S0 : 192.168.65.1
S1 : second subnet
```

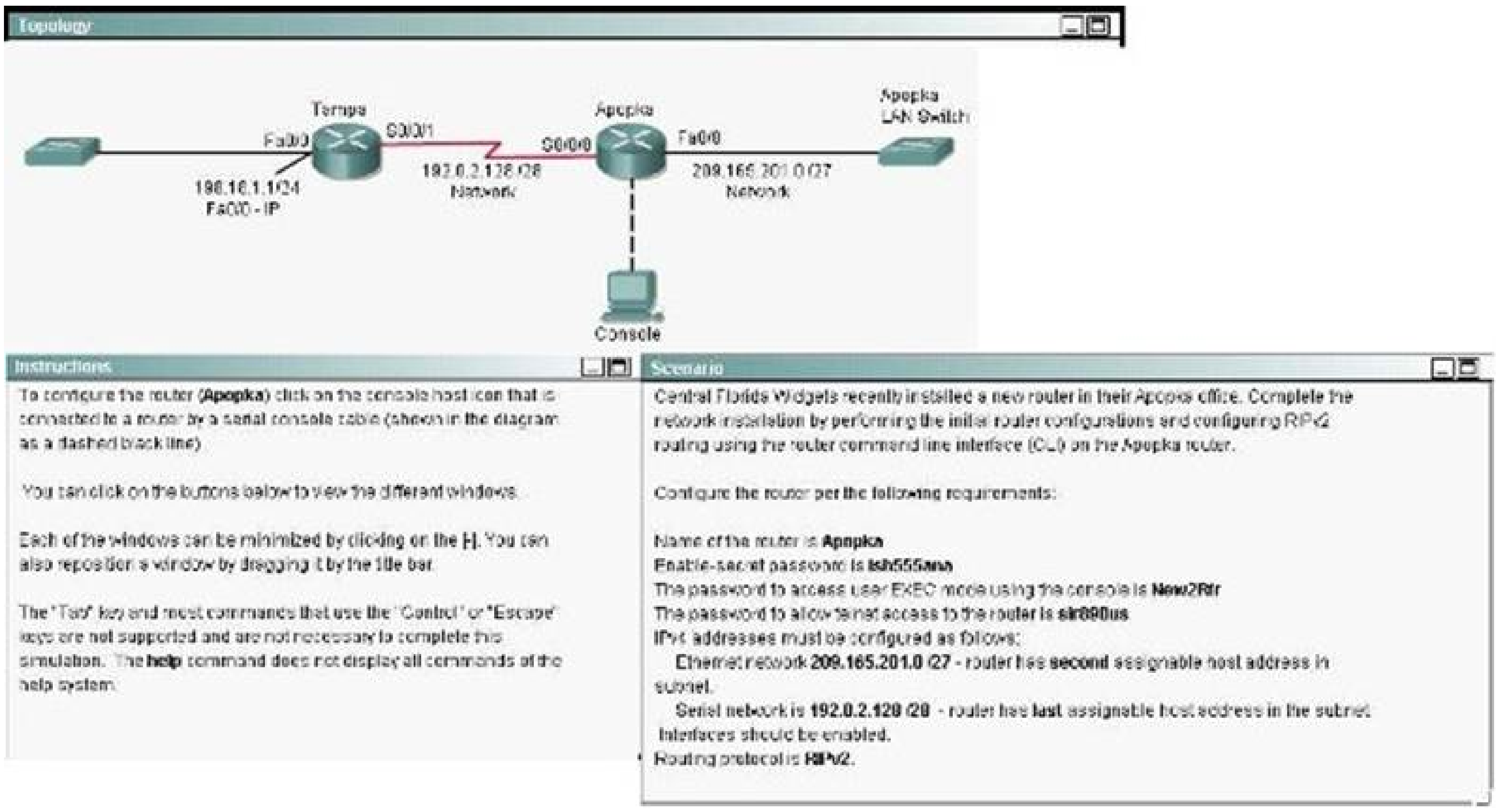
```
Name :      U
E0 : 192.168.9.1
S1 : 192.168.65.2
```

NotE. The OSPF process must be configured to allow interfaces in specific subnets to participate in the routing process.

**Answer:**

**Explanation:** ROUTER-M> enable PassworD. Cisco
ROUTER-M# config t
ROUTER-M(config)# interface e0
ROUTER-M(config-if)# ip address 192.168.160.14 255.255.255.240
ROUTER-M(config-if)# no shutdown
ROUTER -M(config-if)# exit
ROUTER -M(config)# interface s0
ROUTER-M(config-if)# ip address 192.168.160.30 255.255.255.240
ROUTER-M(config-if)# no shutdown
ROUTER-M(config-if)# end
ROUTER-M# copy run start

**NEW QUESTION 270**
CORRECT TEXT



To configure the router (**Apopka**) click on the console host icon that is connected to a router by a serial console cable (shown in the diagram as a dashed black line)

You can click on the buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation. The **help** command does not display all commands of the help system.

Central Florida Widgets recently installed a new router in their Apopka office. Complete the network installation by performing the initial router configurations and configuring RIPv2 routing using the router command line interface (CLI) on the Apopka router.

Configure the router per the following requirements:

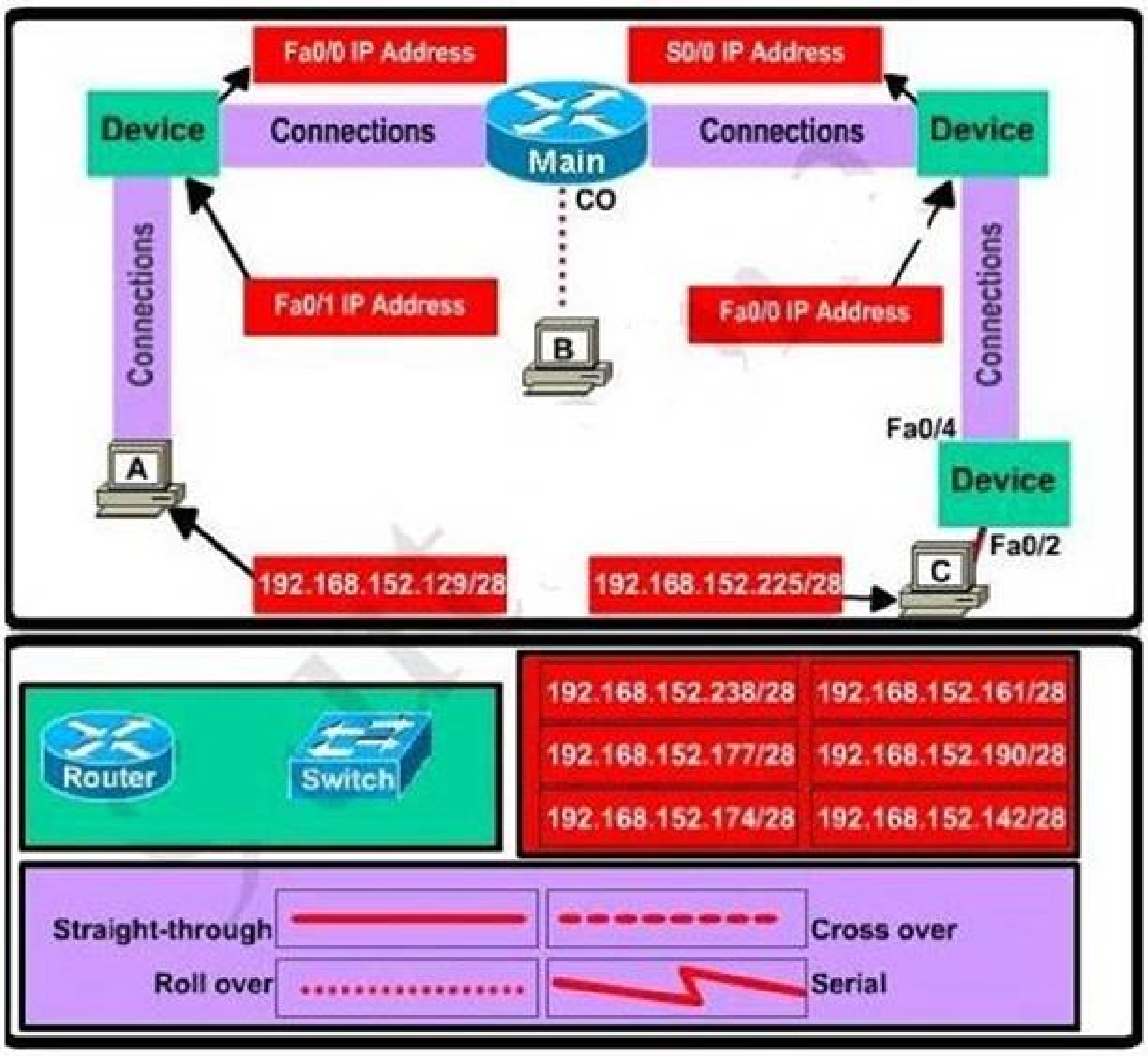
Name of the router is **Apopka**
Enable-secret password is **ish555ana**
The password to access user EXEC mode using the console is **New2Rtr**
The password to allow telnet access to the router is **sir090us**
IPv4 addresses must be configured as follows:
Ethernet network **209.165.201.0 /27** - router has **second** assignable host address in subnet.
Serial network is **192.0.2.128 /28** - router has **last** assignable host address in the subnet.
Interfaces should be enabled.
Routing protocol is **RIPv2.**

**Answer:**

**Explanation:** Router>enable
Router#config terminal
Router(config)#hostname Apopka
2) Enable-secret password (cisco10):
Apopka(config)#enable secret cisco10
3) Set the console password to RouterPass:
Apopka(config)#line console 0
Apopka(config-line)#password RouterPass
Apopka(config-line)#login
Apopka(config-line)#exit
4) Set the Telnet password to scan90:
Apopka(config)#line vty 0 4
Apopka(config-line)#password scan90
Apopka(config-line)#login
Apopka(config-line)#exit
5) Configure Ethernet interface (on the right) of router Apopka:
The subnet mask of the Ethernet network 209.165.201.0 is 27. From this subnet mask, we can find out the increment by converting it into binary form, that is /27 = 1111 1111.1111 1111.1111 1111.1110 0000. Pay more attention to the last bit 1 because it tells us the increment, using the formula:
Increment = 2place of the last bit 1 (starts counting from 0,from right to left), in this case increment = 25 = 32. Therefore:
Increment: 32
Network address: 209.165.201.0
Broadcast address: 209.165.201.31 (because 209.165.201.32 is the second subnetwork, so the previous IP - 209.165.201.31 - is the broadcast address of the first subnet).
-> The second assignable host address of this subnetwork is 209.165.201.2/27 Assign the second assignable host address to Fa0/0 interface of Apopka router:
Apopka(config)#interface Fa0/0
Apopka(config-if)#ip address 209.165.201.2 255.255.255.224 Apopka(config-if)#no shutdown
Apopka(config-if)#exit
6) Configure Serial interface (on the left) of router Apopka:
Using the same method to find out the increment of the Serial network: Serial network 192.0.2.128/28:
Increment: 16 (/28 = 1111 1111.1111 1111.1111 1111.1111 0000)
Network address: 192.0.2.128 (because 8 * 16 = 128 so 192.0.2.128 is also the network address of this subnet)
Broadcast address: 192.0.2.143
-> The last assignable host address in this subnet is 192.0.2.142/28.
Assign the last assignable host address to S0/0/0 interface of Apopka router: Apopka(config)#interface S0/0/0 (or use interface S0/0 if not successful)
Apopka(config-if)#ip address 192.0.2.142 255.255.255.240
Apopka(config-if)#no shutdown Apopka(config-if)#exit
7) Configure RIP v2 routing protocol: Apopka(config)#router rip Apopka(config-router)#version 2
Apopka(config-router)#network 209.165.201.0
Apopka(config-router)#network 192.0.2.128 Apopka(config-router)#end
Save the configuration:
Apopka#copy running-config startup-config
Finally, you should use the ping command to verify all are working properly!

**NEW QUESTION 275**
CORRECT TEXT
This topology contains 3 routers and 1 switch. Complete the topology.
Drag the appropriate device icons to the labeled Device
Drag the appropriate connections to the locations labeled Connections. Drag the appropriate IP addresses to the locations labeled IP address
(Hint: use the given host addresses and Main router information) To remove a device or connection, drag it away from the topology.
Use information gathered from the Main router to complete the configuration of any additional routers.

No passwords are required to access the Main router. The config terminal command has been disabled for the HQ router. The router does not require any configuration.



Configure each additional router with the following:
Configure the interfaces with the correct IP address and enable the interfaces. Set the password to allow console access to consolepw
Set the password to allow telnet access to telnetpw
Set the password to allow privilege mode access to privpw
Not E: Because routes are not being added to the configurations, you will not be able to ping through the internetwork.
All devices have cable autosensing capabilities disabled. All hosts are PC's

**Answer:**

**Explanation:** Specify appropriate devices and drag them on the "Device" boxes
For the device at the bottom-right box, we notice that it has 2 interfaces Fa0/2 and Fa0/4; moreover the link connects the PC on the right with the device on the bottom-right is a straight-through link -> it is a switch
The question stated that this topology contains 3 routers and 1 switch -> two other devices are routers
Place them on appropriate locations as following:
(Host D and host E will be automatically added after placing two routers. Click on them to access neighboring routers)
Specify appropriate connections between these devices:
+ The router on the left is connected with the Main router through FastEthernet interfaces: use a crossover cable
+ The router on the right is connected with the Main router through Serial interfaces: use a serial cable
+ The router on the right and the Switch: use a straight-through cable
+ The router on the left and the computer: use a crossover cable
(To remember which type of cable you should use, follow these tips:
- To connect two serial interfaces of 2 routers we use serial cable
- To specify when we use crossover cable or straight-through cable, we should remember:
Group 1: Router, Host, Server
Group 2: Hub, Switch
One device in group 1 + One device in group 2: use straight-through cable
Two devices in the same group: use crossover cable
For example, we use straight-through cable to connect switch to router, switch to host, hub to host, hub to server... and we use crossover cable to connect switch to switch, switch to hub, router to router, host to host.)
Assign appropriate IP addresses for interfaces:
From Main router, use show running-config command.
(Notice that you may see different IP addresses in the real CCNA exam, the ones shown above are just used for demonstration)
From the output we learned that the ip address of Fa0/0 interface of the Main router is 192.168.152.177/28. This address belongs to a subnetwork which has:
Increment: 16 (/28 = 255.255.255.240 or 1111 1111.1111 1111.1111 1111.1111 0000)
Network address: 192.168.152.176 (because 176 = 16 * 11 and 176 < 177)
Broadcast address: 192.168.152.191 (because 191 = 176 + 16 - 1)
And we can pick up an ip address from the list that belongs to this subnetwork:
192.168.152.190 and assign it to the Fa0/0 interface the router on the left
Use the same method for interface Serial0/0 with an ip address of 192.168.152.161 Increment: 16
Network address: 192.168.152.160 (because 160 = 16 * 10 and 160 < 161)
Broadcast address: 192.168.152.175 (because 176 = 160 + 16 - 1)
-> and we choose 192.168.152.174 for Serial0/0 interface of the router on the right Interface Fa0/1 of the router on the left
IP (of the computer on the left) : 192.168.152.129/28 Increment: 16
Network address: 192.168.152.128 (because 128 = 16 * 8 and 128 < 129)
Broadcast address: 192.168.152.143 (because 143 = 128 + 16 - 1)

-> we choose 192.168.152.142 from the list Interface Fa0/0 of the router on the right
IP (of the computer on the left) : 192.168.152.225/28 Increment: 16
Network address: 192.168.152.224 (because 224 = 16 * 14 and 224 < 225)
Broadcast address: 192.168.152.239 (because 239 = 224 + 16 - 1)
-> we choose 192.168.152.238 from the list
Let's have a look at the picture below to summarize
Configure two routers on the left and right with these commands: Router1 = router on the left
Assign appropriate IP addresses to Fa0/0 & Fa0/1 interfaces: Router1>enable
Router1#configure terminal Router1(config)#interface fa0/0
Router1(config-if)#ip address 192.168.152.190 255.255.255.240 Router1(config-if)#no shutdown
Router1(config-if)#interface fa0/1
Router1(config-if)#ip address 192.168.152.142 255.255.255.240 Router1(config-if)#no shutdown
Set passwords (configure on two routers)
+ Console password: Router1(config-if)#exit Router1(config)#line console 0
Router1(config-line)#password consolepw Router1(config-line)#login
Router1(config-line)#exit
+ Telnet password: Router1(config)#line vty 0 4 Router1(config-line)#password telnetpw Router1(config-line)#login Router1(config-line)#exit
+ Privilege mode password: Router1(config)#enable password privpw Save the configuration: Router1(config)#exit
Router1#copy running-config startup-config
Configure IP addresses of Router2 (router on the right) Router2>enable
Router2#configure terminal Router2(config)#interface fa0/0
Router2(config-if)#ip address 192.168.152.238 255.255.255.240 Router2(config-if)#no shutdown
Router2(config-if)#interface serial0/0
Router2(config-if)#ip address 192.168.152.174 255.255.255.240 Router2(config-if)#no shutdown
Then set the console, telnet and privilege mode passwords for Router2 as we did for Router1, remember to save the configuration when you finished.

Topic 7, Mix Questions A

**NEW QUESTION 276**
Which dynamic routing protocol uses only the hop count to determine the best path to a destination?

A. IGRP
B. RIP
C. EIGRP
D. OSPF

**Answer:** B

**NEW QUESTION 278**
Which statement about a router on a stick is true?

A. Its date plane router traffic for a single VI AN over two or more switches.
B. It uses multiple subinterfaces of a single interface to encapsulate traffic for different VLANs on the same subnet.
C. It requires the native VLAN to be disabled.
D. It uses multiple subinterfaces of a single interface to encapsulate traffic for different VLANs.

**Answer:** D

**Explanation:** https://www.freeccnaworkbook.com/workbooks/ccna/configuring-inter-vlan-routing-router-on-a-stick

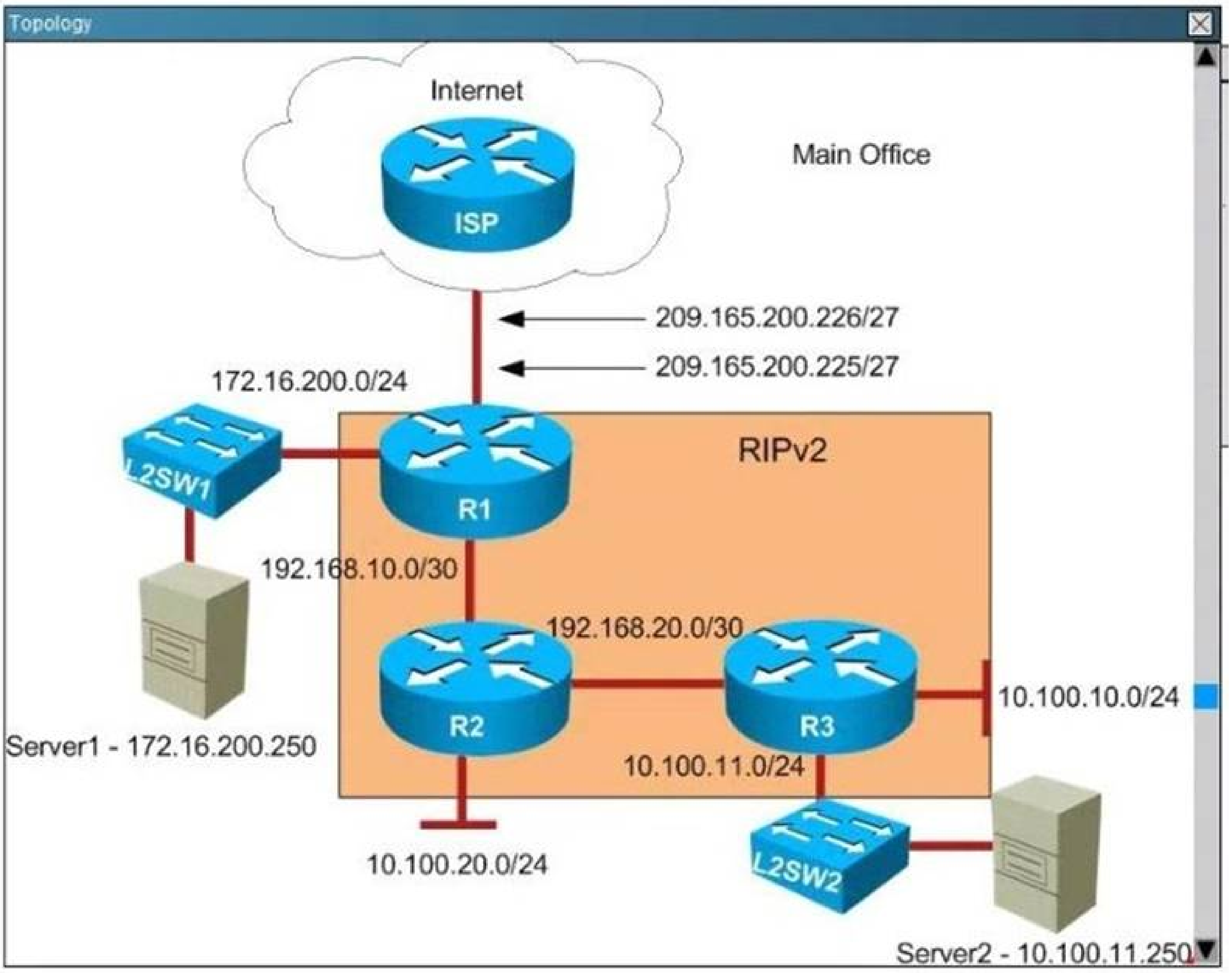
**NEW QUESTION 281**
Which statement about the inside interface configuration in a NAT deployment is true?

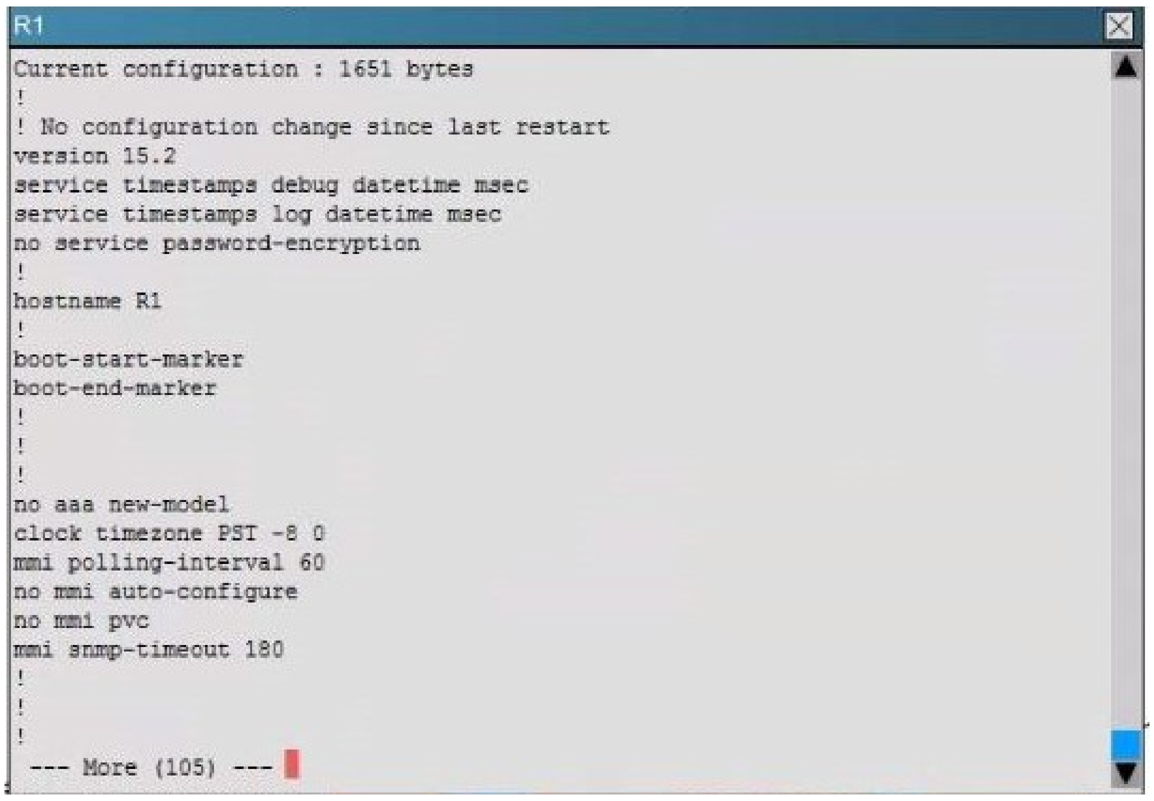
A. It is defined globally
B. It identifies the location of source addresses for outgoing packets to be translated using access or route maps.
C. It must be configured if static NAT is used
D. It identifies the public IP address that traffic will use to reach the internet.

**Answer:** B

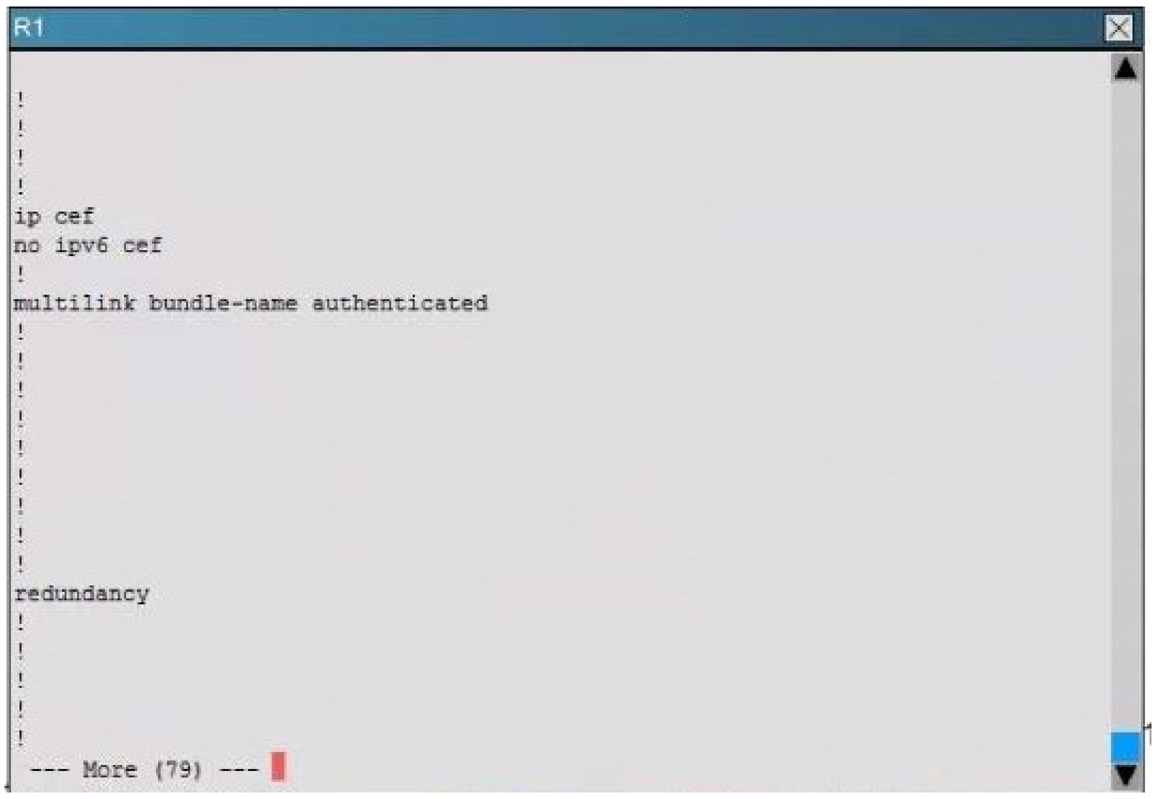
**Explanation:** This module describes how to configure Network Address Translation (NAT) for IP address conservation and how to configure inside and outside source addresses. This module also provides information about the benefits of configuring NAT for IP address conservation.
NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks, and translates the private (not globally unique) addresses in the internal network into legal addresses before packets are forwarded onto another network. NAT can be configured to advertise to the outside world only one address for the entire network. This ability provides additional security by effectively hiding the entire internal network behind that one address.
NAT is also used at the enterprise edge to allow internal users access to the Internet and to allow Internet access to internal devices such as mail servers.

**NEW QUESTION 283**
Scenario:
You are a junior network engineer for a financial company, and the main office network is experiencing network issues. Troubleshoot the network issues.
Router R1 connects the main office to the internet, and routers R2 and R3 are internal routers.
NAT is enabled on router R1.
The routing protocol that is enabled between routers R1, R2 and R3 is RIPv2.
R1 sends the default route into RIPv2 for the internal routers to forward internet traffic to R1.
You have console access on R1, R2 and R3 devices. Use only show commands to troubleshoot the issues.

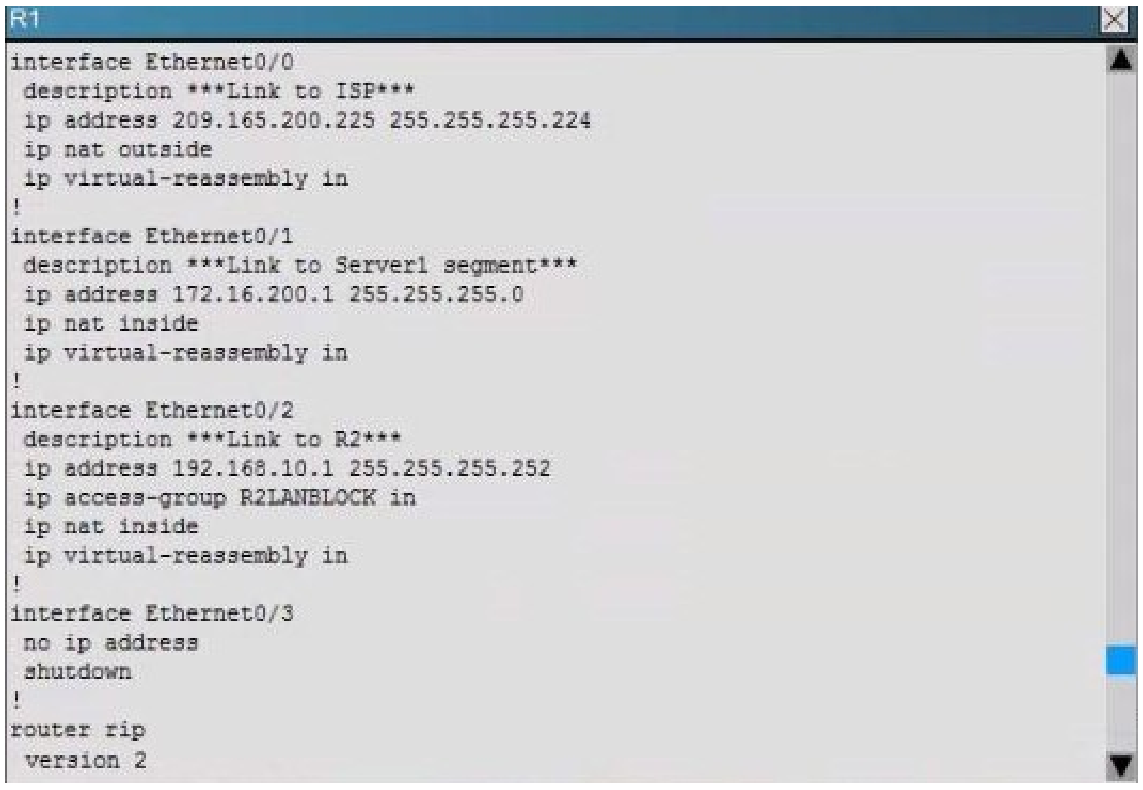




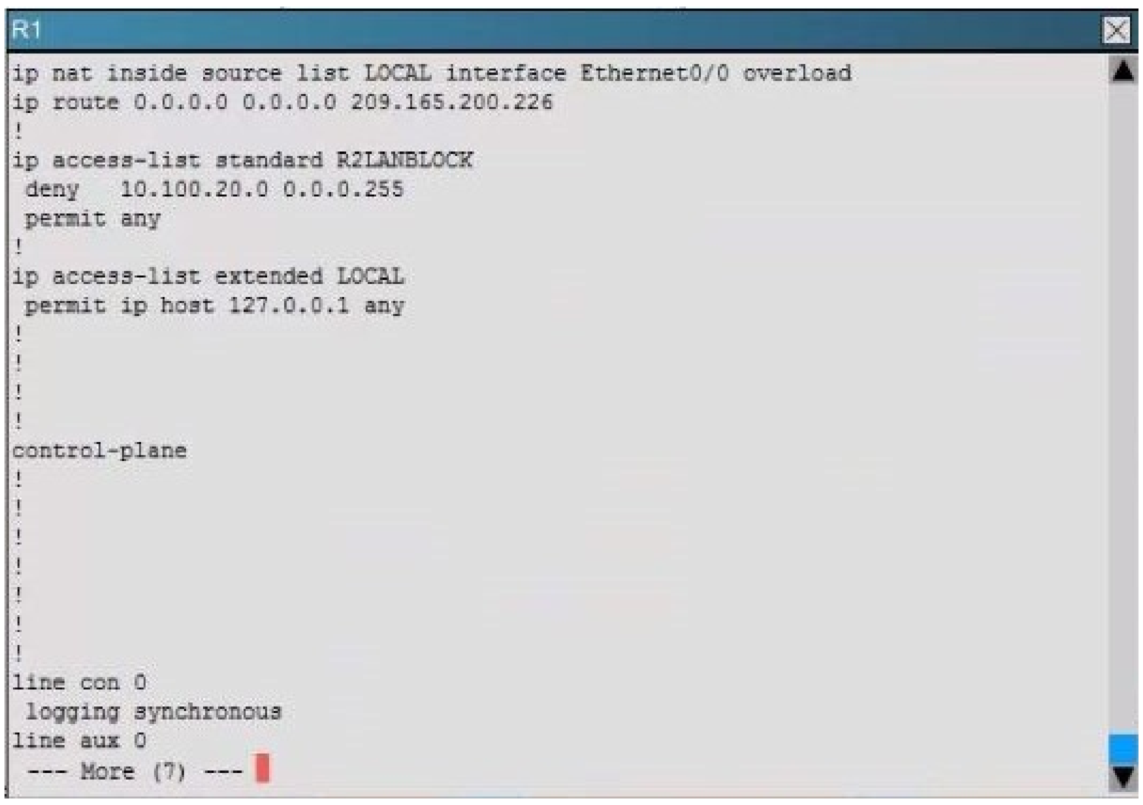
```
Current configuration : 1651 bytes
!
! No configuration change since last restart
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
 --- More (105) ---
```



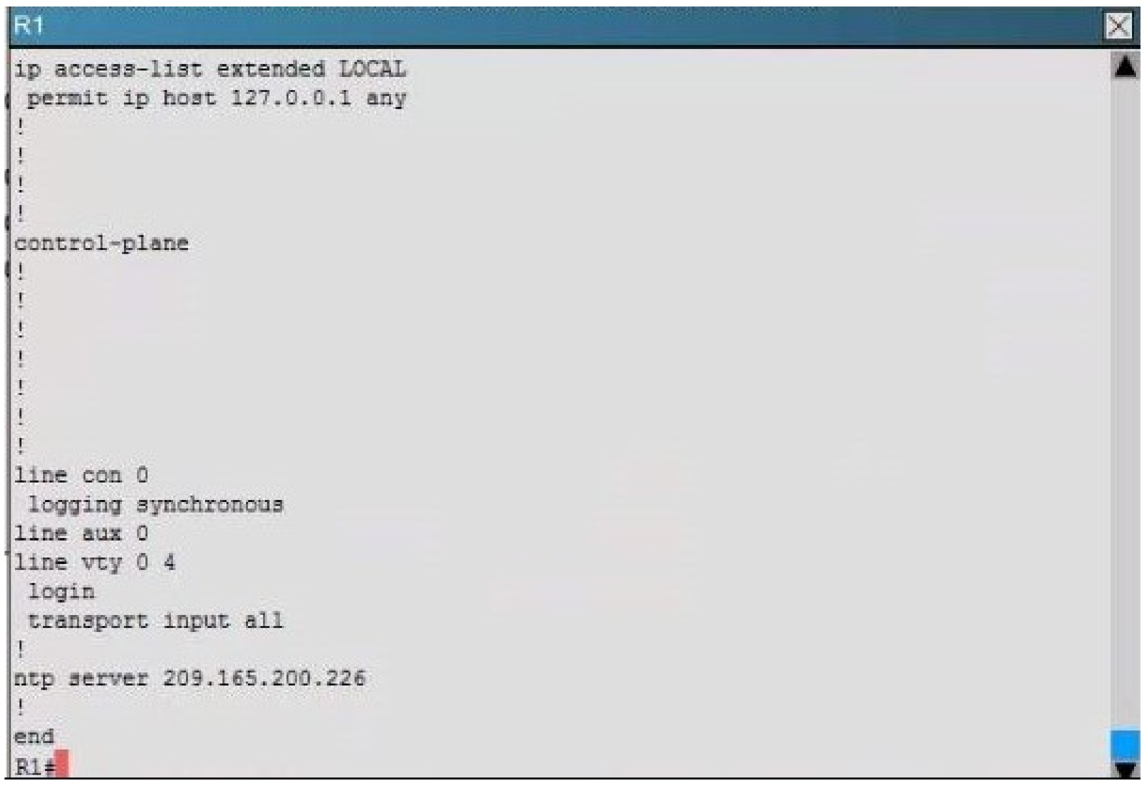
```
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
 --- More (79) ---
```



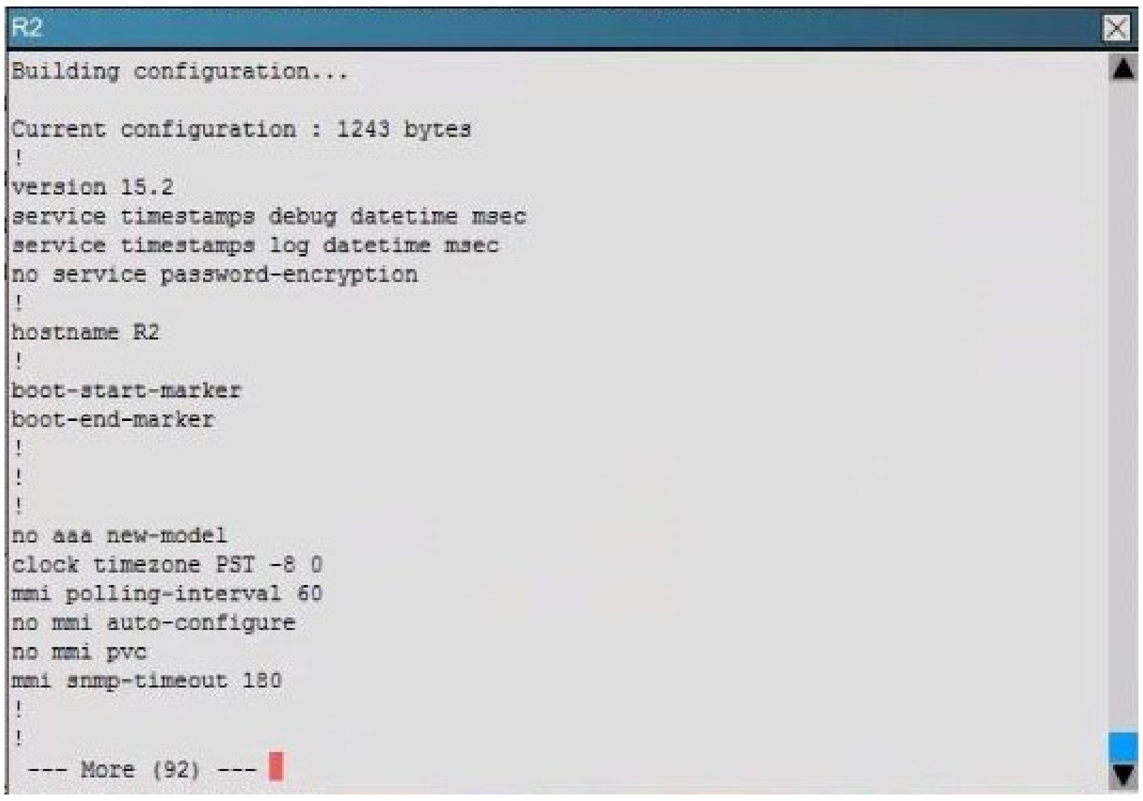
```
interface Ethernet0/0
 description ***Link to ISP***
 ip address 209.165.200.225 255.255.255.224
 ip nat outside
 ip virtual-reassembly in
!
interface Ethernet0/1
 description ***Link to Server1 segment***
 ip address 172.16.200.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/2
 description ***Link to R2***
 ip address 192.168.10.1 255.255.255.252
 ip access-group R2LANBLOCK in
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
```



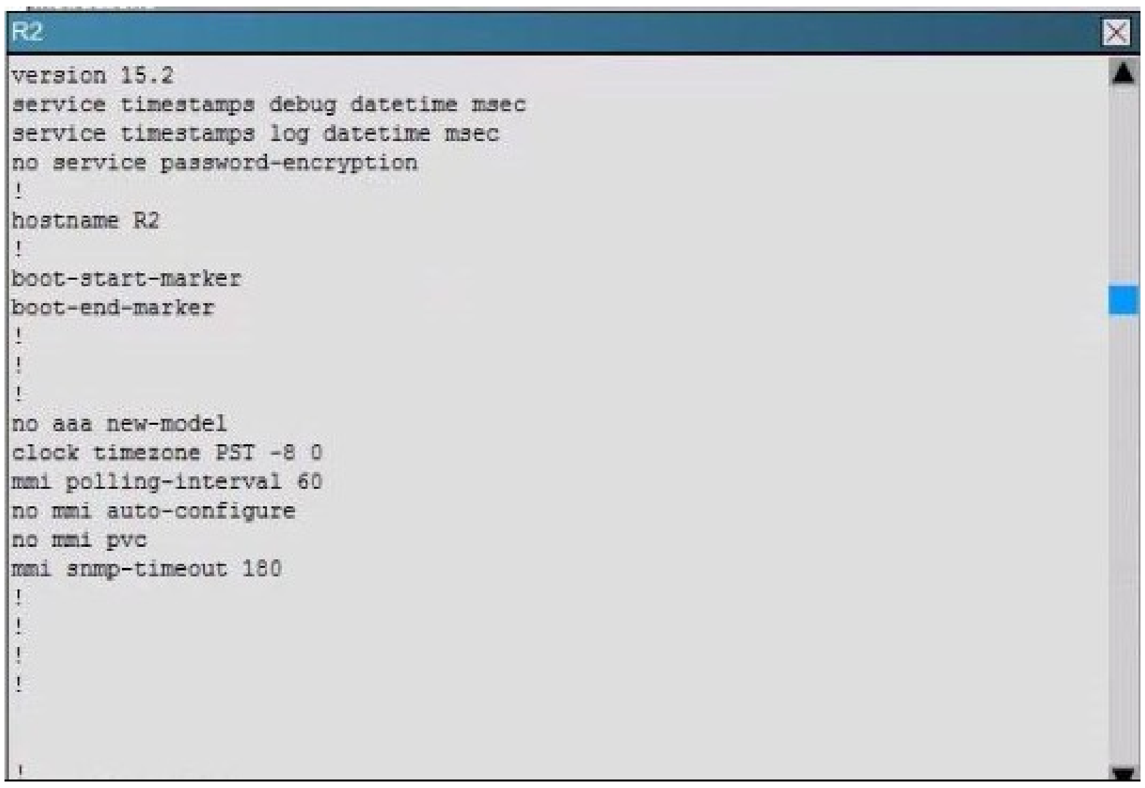
```
ip nat inside source list LOCAL interface Ethernet0/0 overload
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip access-list standard R2LANBLOCK
 deny   10.100.20.0 0.0.0.255
 permit any
!
ip access-list extended LOCAL
 permit ip host 127.0.0.1 any
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
 --- More (7) ---
```



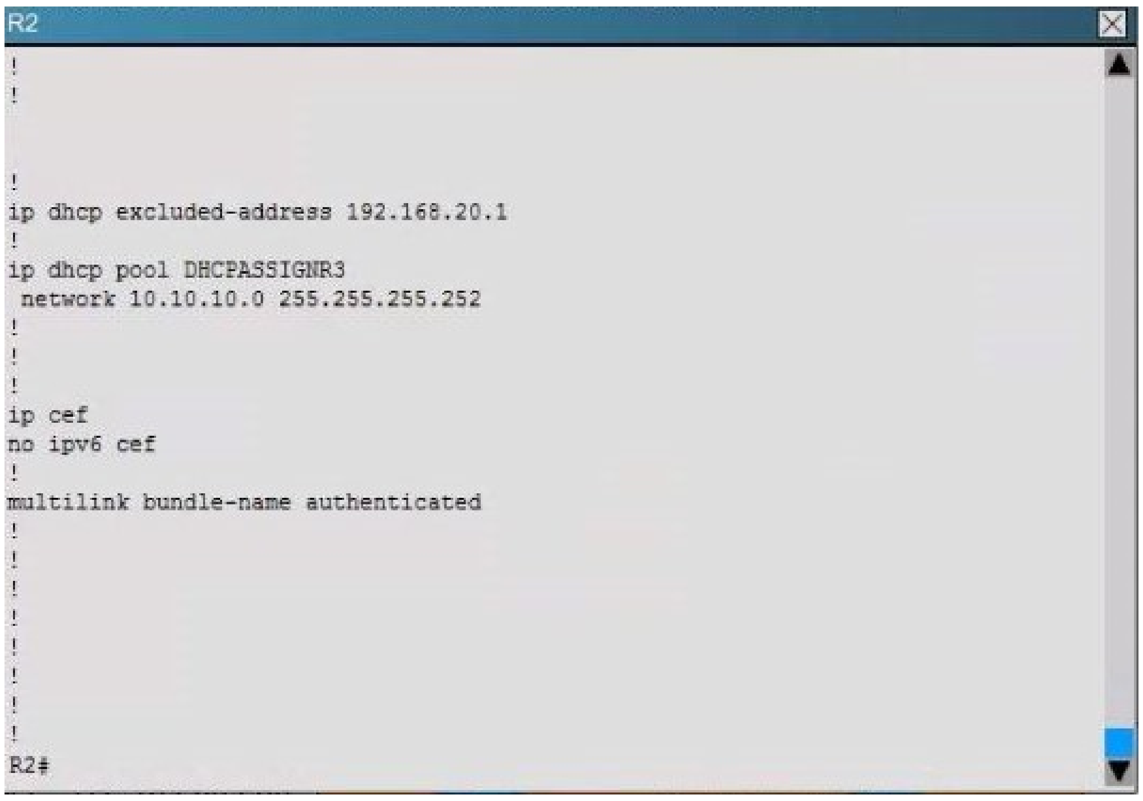
```
ip access-list extended LOCAL
 permit ip host 127.0.0.1 any
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
ntp server 209.165.200.226
!
end
R1#
```



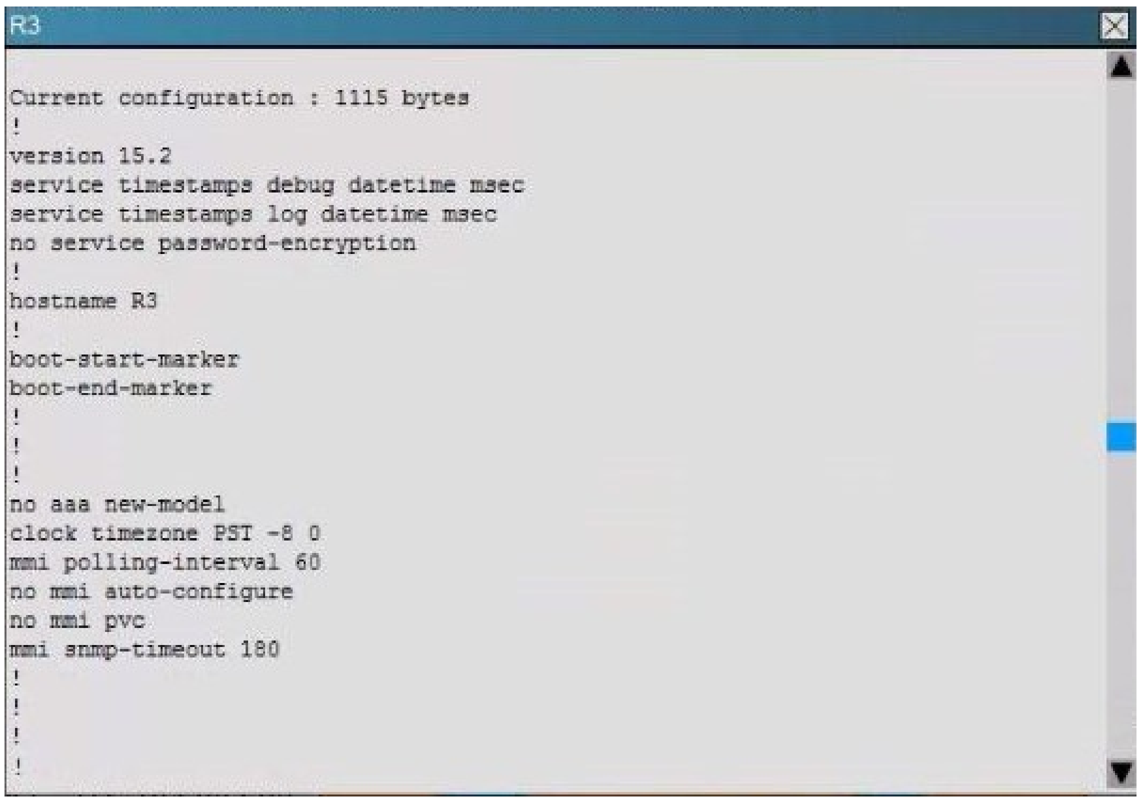
```
Building configuration...

Current configuration : 1243 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
 --- More (92) ---
```



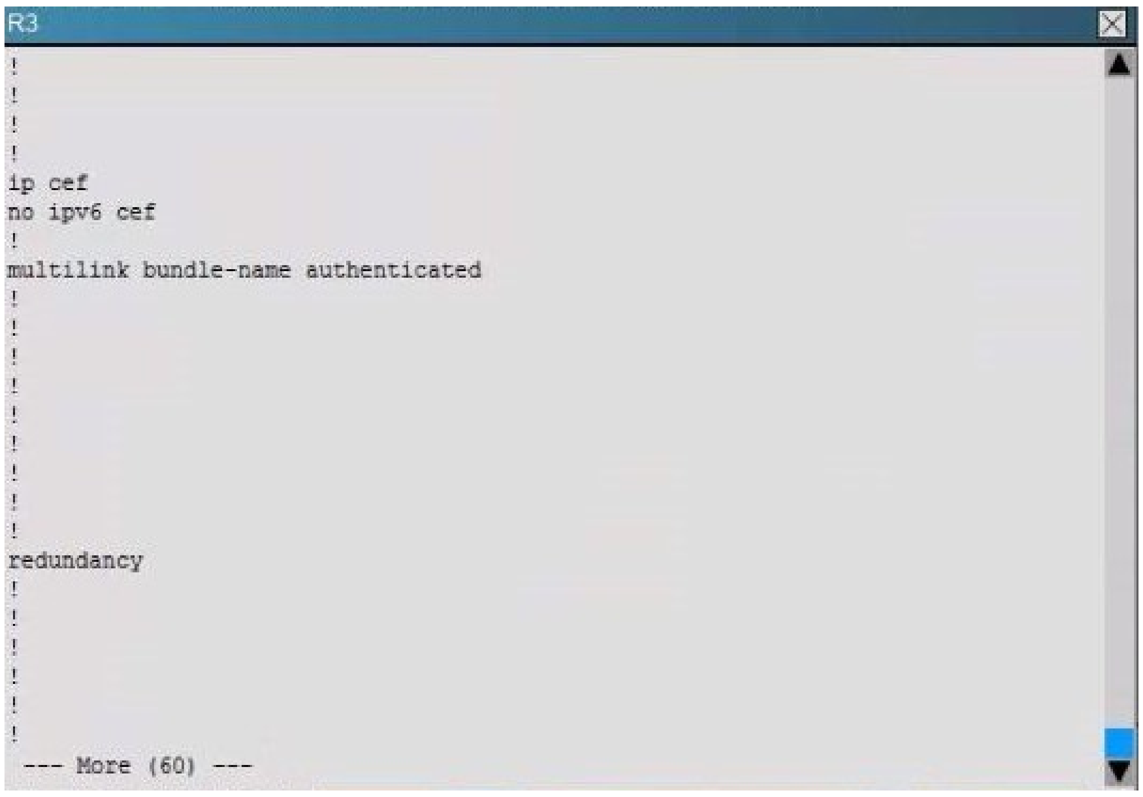
```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!


!
```



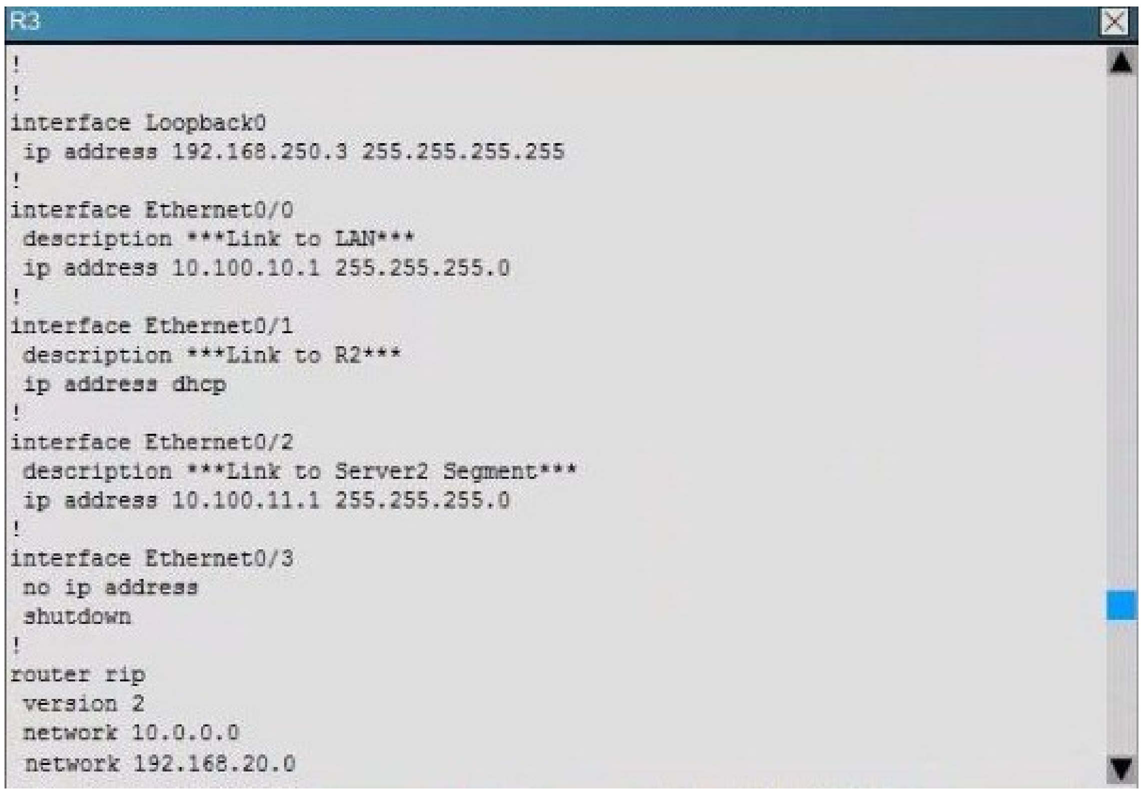
```
!
!


!
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool DHCPASSIGNR3
 network 10.10.10.0 255.255.255.252
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
R2#
```



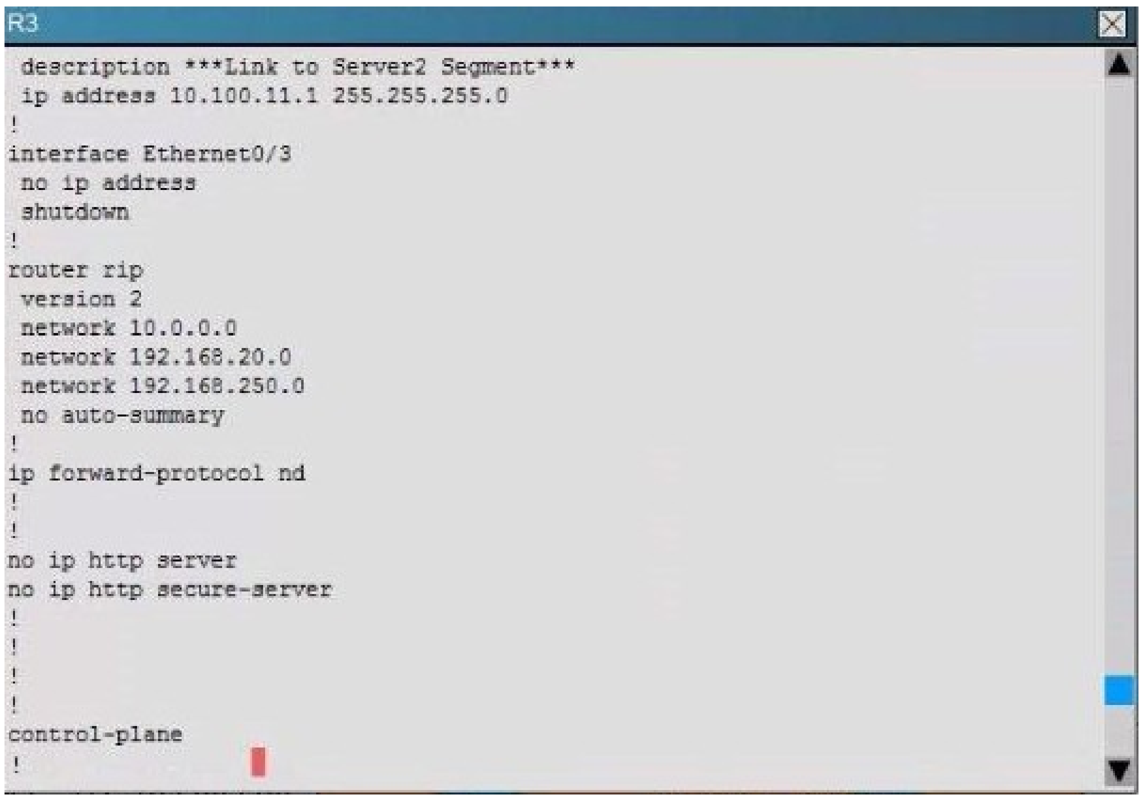
```

Current configuration : 1115 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
```



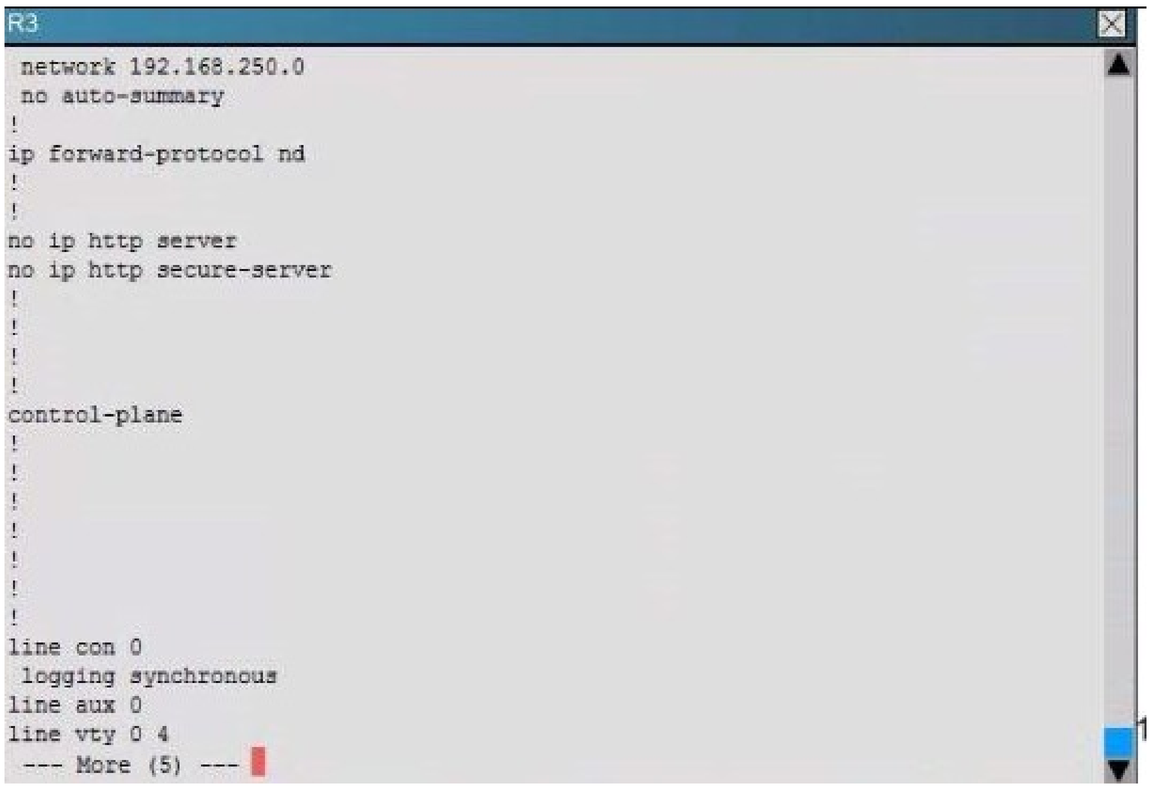
```
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
 --- More (60) ---
```



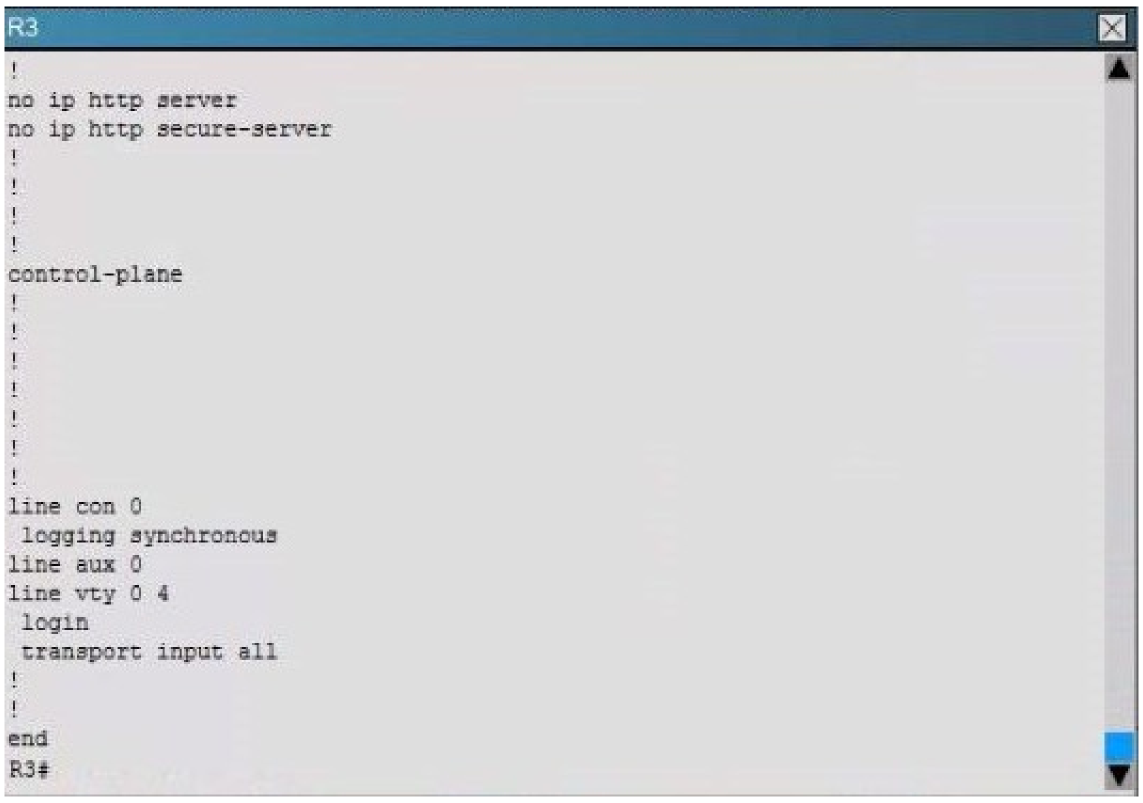
```
!
!
interface Loopback0
 ip address 192.168.250.3 255.255.255.255
!
interface Ethernet0/0
 description ***Link to LAN***
 ip address 10.100.10.1 255.255.255.0
!
interface Ethernet0/1
 description ***Link to R2***
 ip address dhcp
!
interface Ethernet0/2
 description ***Link to Server2 Segment***
 ip address 10.100.11.1 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.20.0
```



```
 description ***Link to Server2 Segment***
 ip address 10.100.11.1 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.20.0
 network 192.168.250.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
```



```
 network 192.168.250.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 --- More (5) ---
```



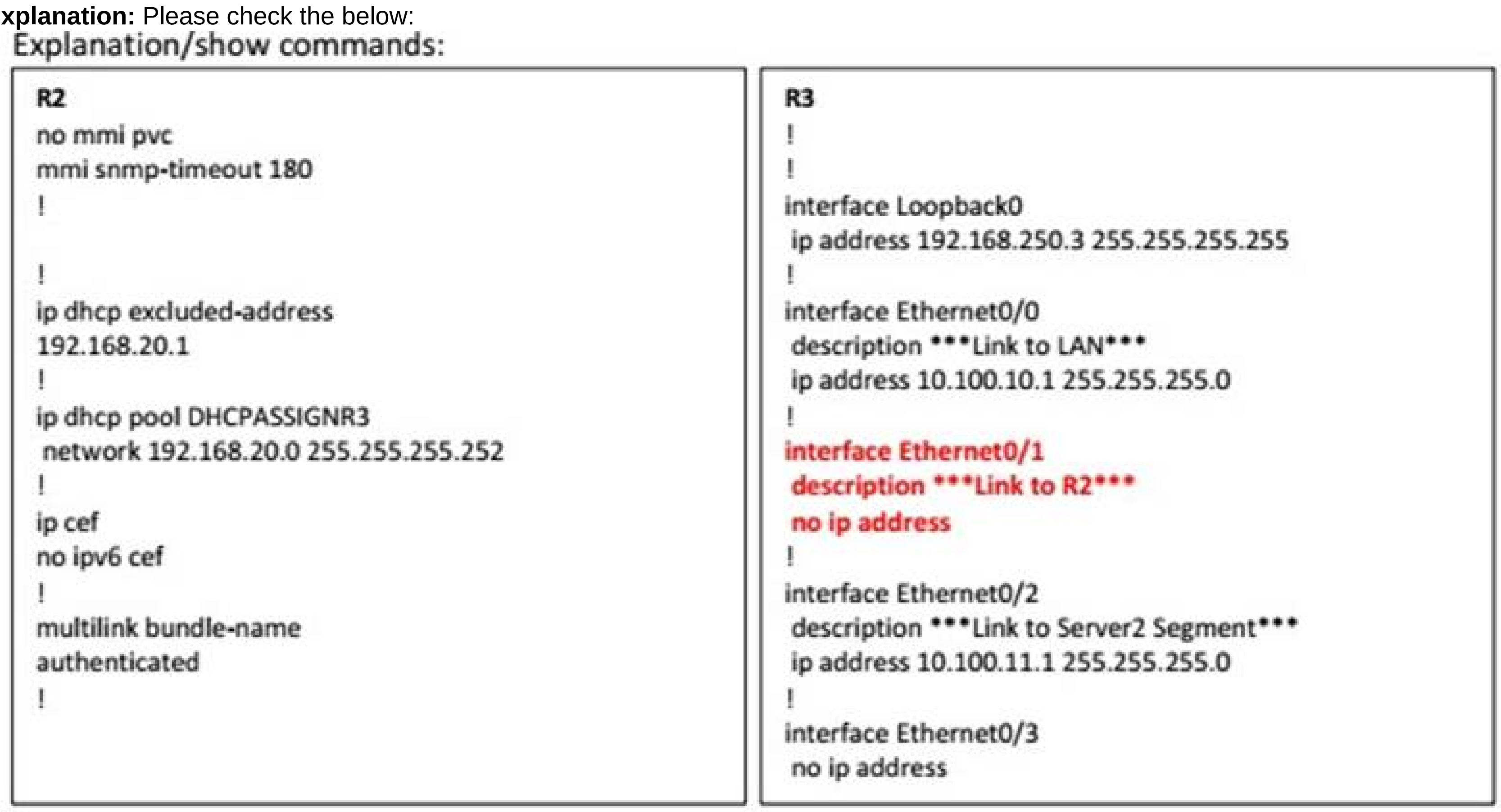
```
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
!
end
R3#
```

Examine the DHCP configuration between R2 and R3; R2 is configured as the DHCP server and R3 as the client. What is the reason R3 is not receiving the IP address via DHCP?

A. On R2. The network statement In the DHCP pool configuration is incorrectly configured.
B. On R3. DHCP is not enabled on the interface that is connected to R2.
C. On R2, the interface that is connected to R3 is in shutdown condition.
D. On R3, the interface that is connected to R2 is in shutdown condition.

**Answer:** B

**Explanation:** Please check the below:



Explanation/show commands:

```
R2
no mmi pvc
mmi snmp-timeout 180
!

!
ip dhcp excluded-address
192.168.20.1
!
ip dhcp pool DHCPASSIGNR3
 network 192.168.20.0 255.255.255.252
!
ip cef
no ipv6 cef
!
multilink bundle-name
authenticated
!
```

```
R3
!
!
interface Loopback0
 ip address 192.168.250.3 255.255.255.255
!
interface Ethernet0/0
 description ***Link to LAN***
 ip address 10.100.10.1 255.255.255.0
!
interface Ethernet0/1
 description ***Link to R2***
 no ip address
!
interface Ethernet0/2
 description ***Link to Server2 Segment***
 ip address 10.100.11.1 255.255.255.0
!
interface Ethernet0/3
 no ip address
```

**NEW QUESTION 284**
Which RFC was created to alleviate the depletion of IPv4 public addresses?

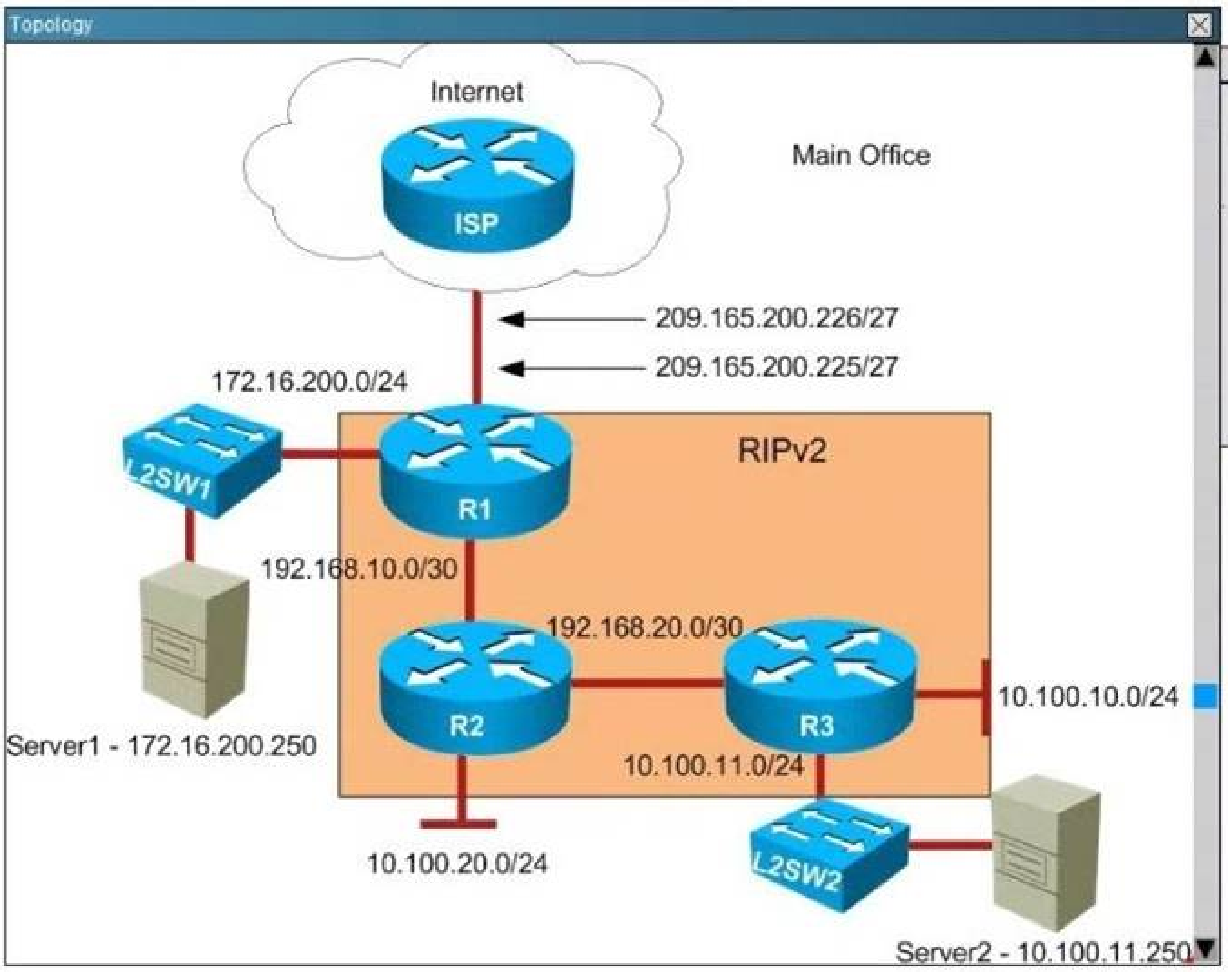
A. RFC 4193
B. RFC 1519
C. RFC 1518
D. RFC 1918

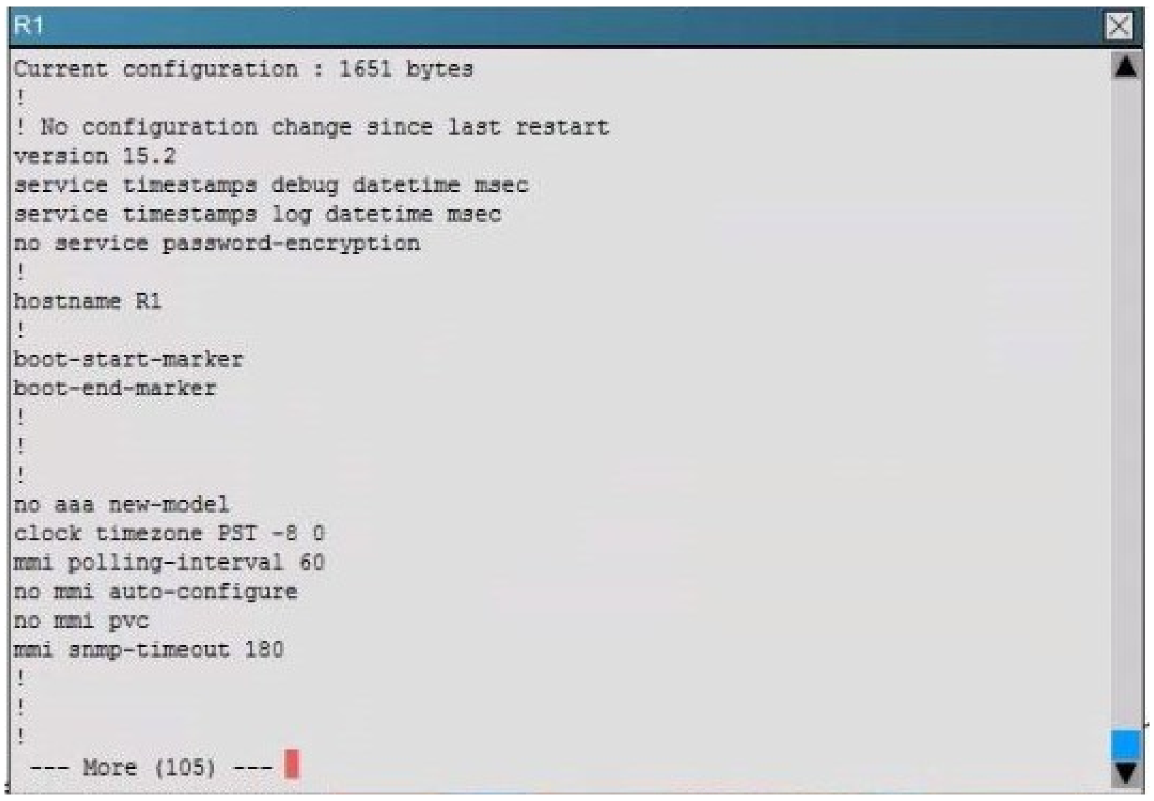
**Answer:** C

**Explanation:** The RFC 1518 is Classless Interdomain Routing (CIDR). CIDR is a mechanism developed to help alleviate the problem of exhaustion of IP addresses and growth of routing tables.
The problems were:
+ With the classful routing system, individual networks were either limited to 254 hosts (/24) or 65,534 hosts (/16). For many network enterprises, 254 hosts were not enough and 65,534 were too large to be used efficiently.
+ Routing information overload. The size and rate of growth of the routing tables in Internet routers is beyond the ability of current software (and people) to effectively manage.
+ Eventual exhaustion of IP network numbers.
To solve these problem, CIDR was selected as the solution in 1992.
In contrast to classful routing, which categorizes addresses into one of three blocks, CIDR allows for blocks of IP addresses to be allocated to Internet service

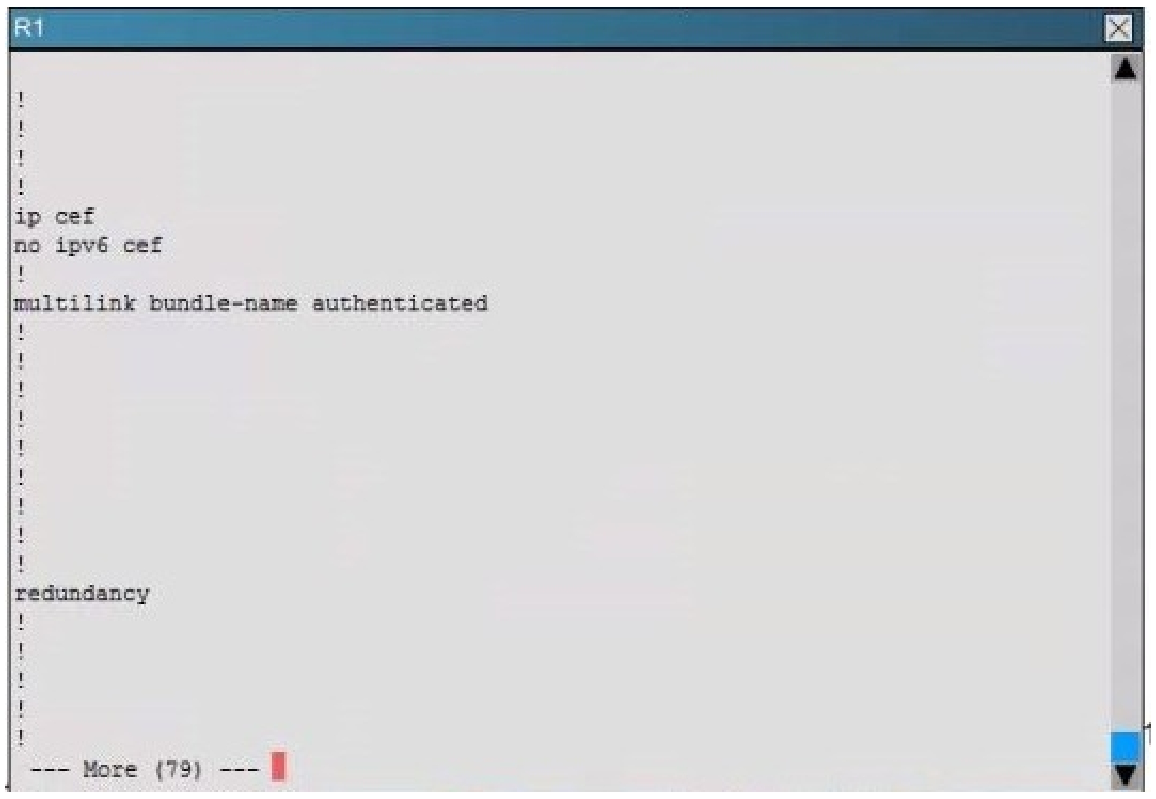
providers. The blocks are then split up and assigned to the provider’s customers.
According to the CIDR standard, the first part of an IP address is a prefix, which identifies the network. The prefix is followed by the host identifier so that information packets can be sent to particular computers within the network. ACIDR address includes the standard 32-bit IP address and also the network prefix. For example, a CIDR address of 200.1.45.2/26, the “/26” indicates the first 26 bits are used to identify the unique network, leaving the remaining bits to identify the specific hosts.
Therefore, instead of assigning the whole block of a class B or C address, now smaller blocks of a class can be assigned. For example, instead of assigning a whole block of 200.1.45.0/24, a smaller block, like 200.1.45.0/27 or 200.1.45.32/27, can be assigned.
In fact, CIDR is specified in RFCs 1518,1519 and 1520 so answer “RFC 1519” is also acceptable.

**NEW QUESTION 289**
Scenario:
You are a junior network engineer for a financial company, and the main office network is experiencing network issues. Troubleshoot the network issues.
Router R1 connects the main office to the internet, and routers R2 and R3 are internal routers. NAT is enabled on router R1.
The routing protocol that is enabled between routers R1, R2 and R3 is RIPv2.
R1 sends the default route into RIPv2 for the internal routers to forward internet traffic to R1.
You have console access on R1, R2 and R3 devices. Use only show commands to troubleshoot the issues.

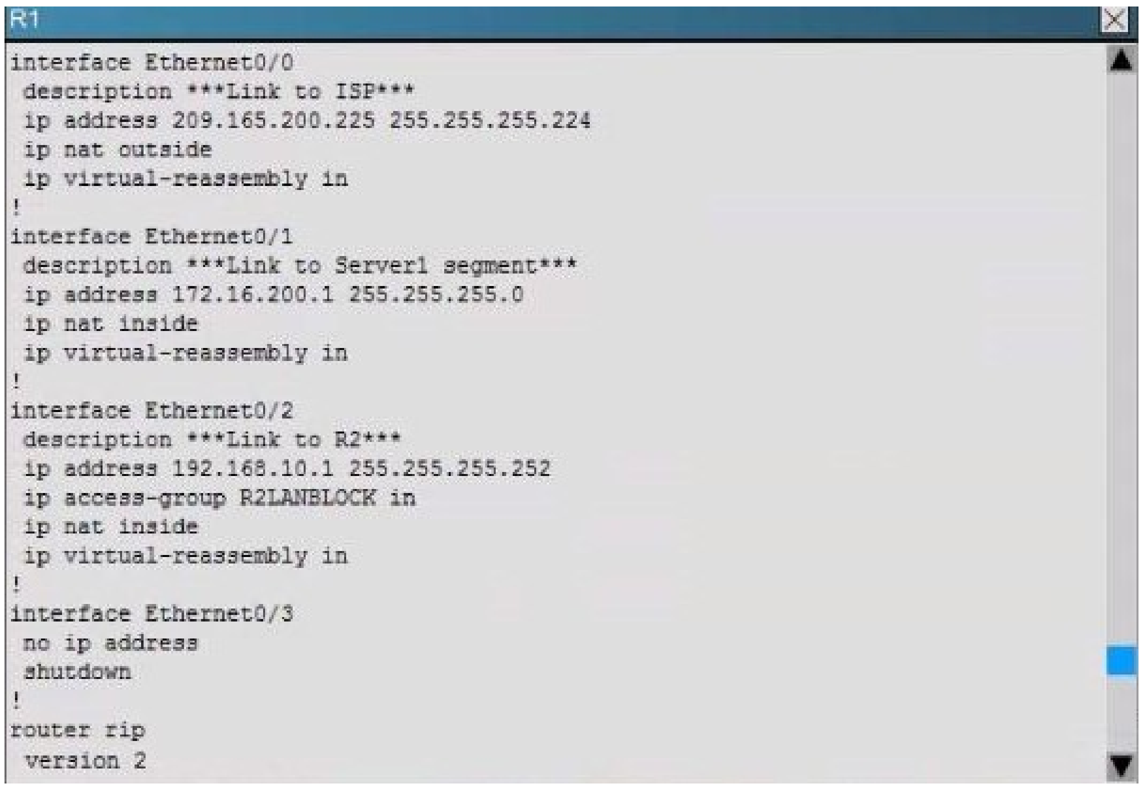




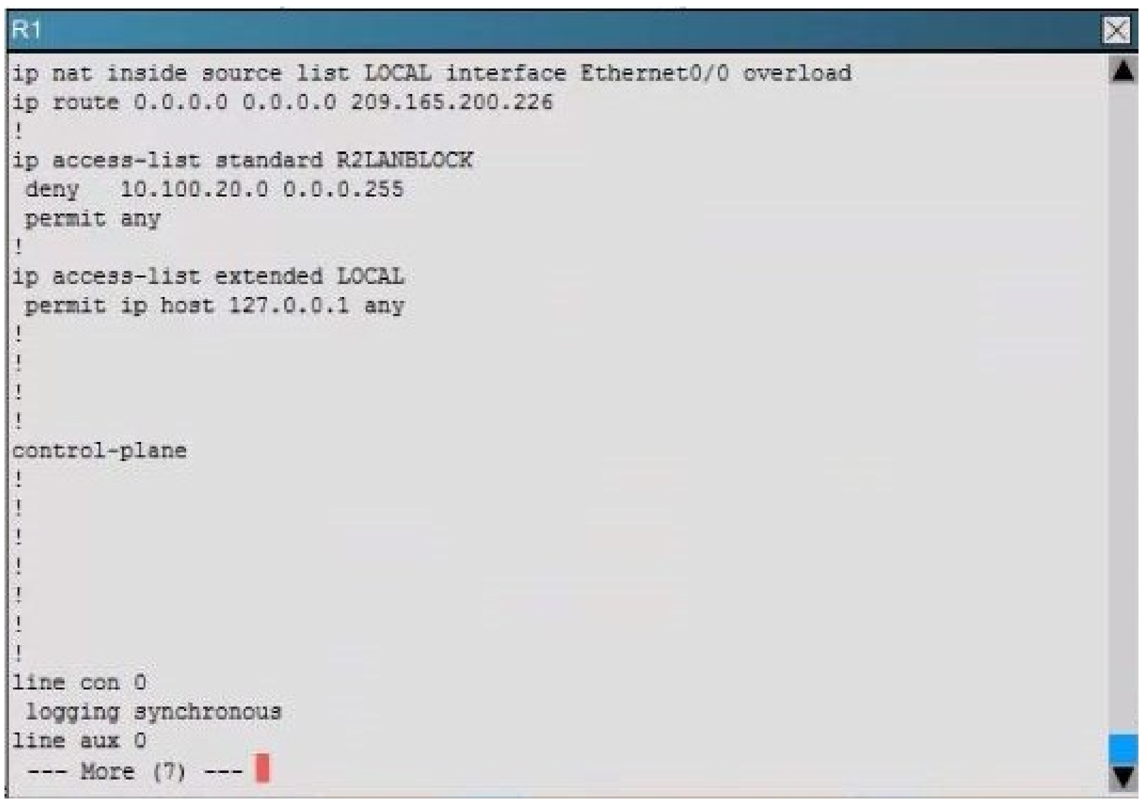
```
Current configuration : 1651 bytes
!
! No configuration change since last restart
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
 --- More (105) ---
```



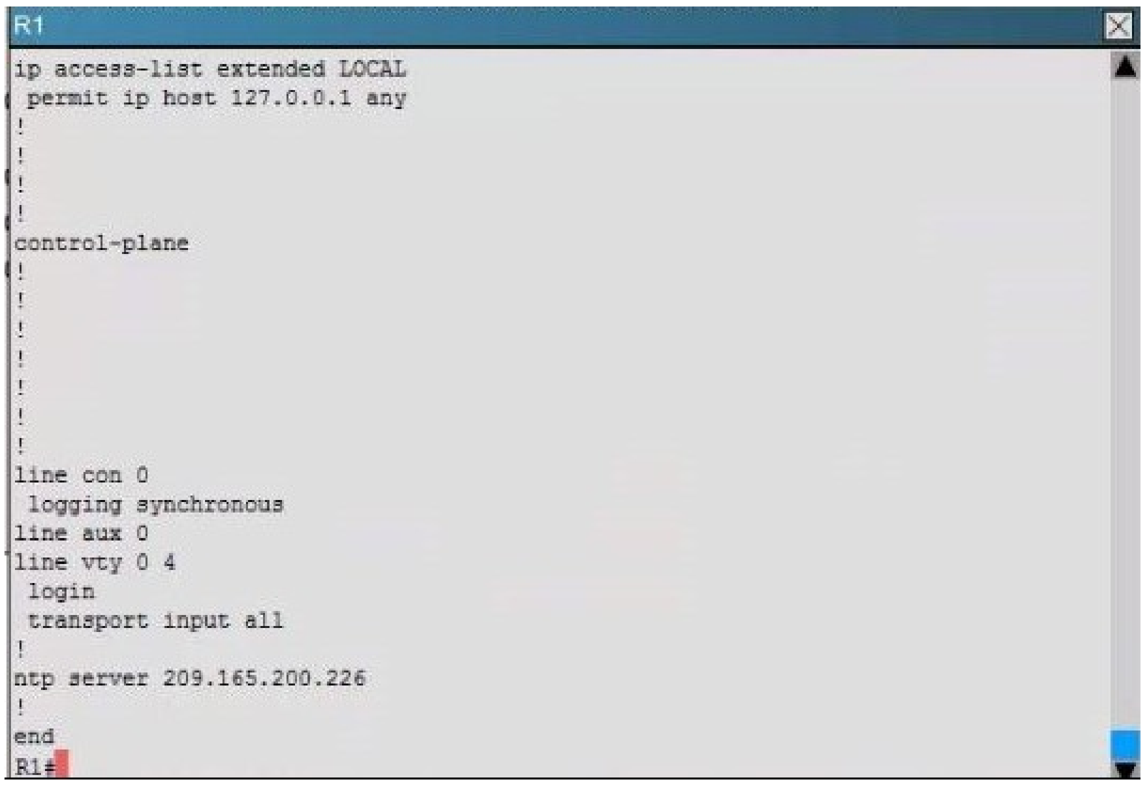
```
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
 --- More (79) ---
```



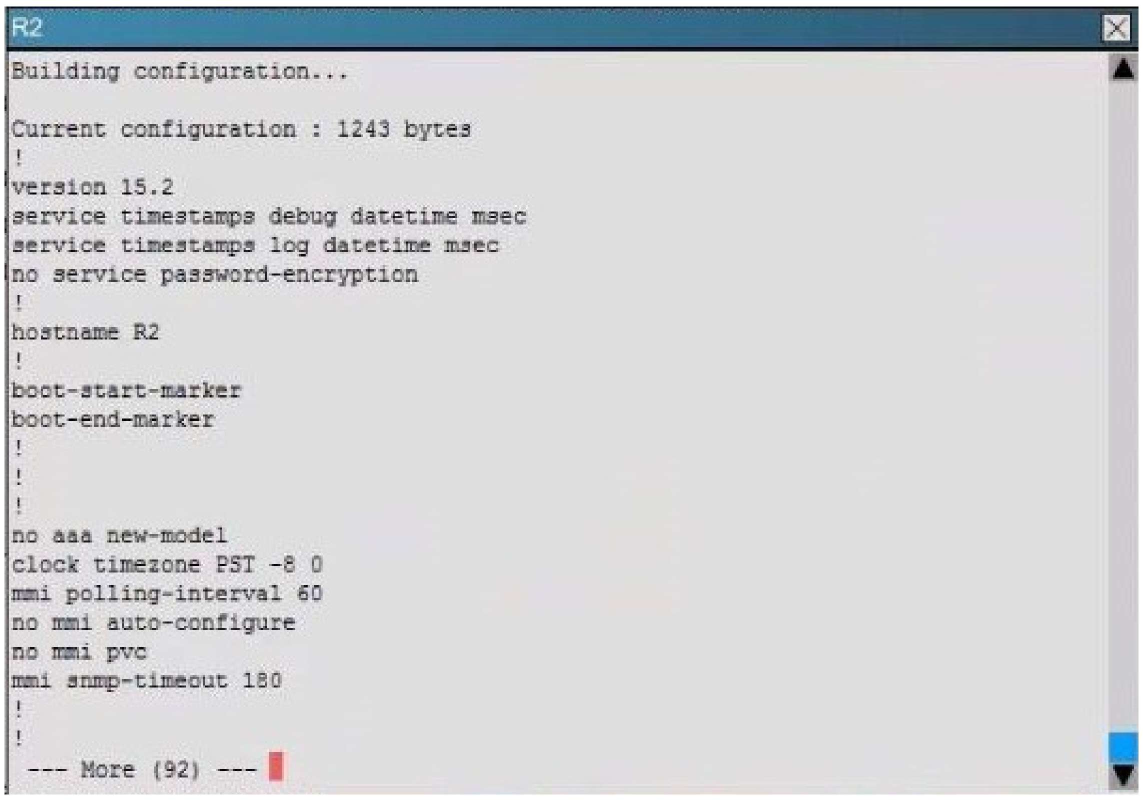
```
interface Ethernet0/0
 description ***Link to ISP***
 ip address 209.165.200.225 255.255.255.224
 ip nat outside
 ip virtual-reassembly in
!
interface Ethernet0/1
 description ***Link to Server1 segment***
 ip address 172.16.200.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/2
 description ***Link to R2***
 ip address 192.168.10.1 255.255.255.252
 ip access-group R2LANBLOCK in
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
```



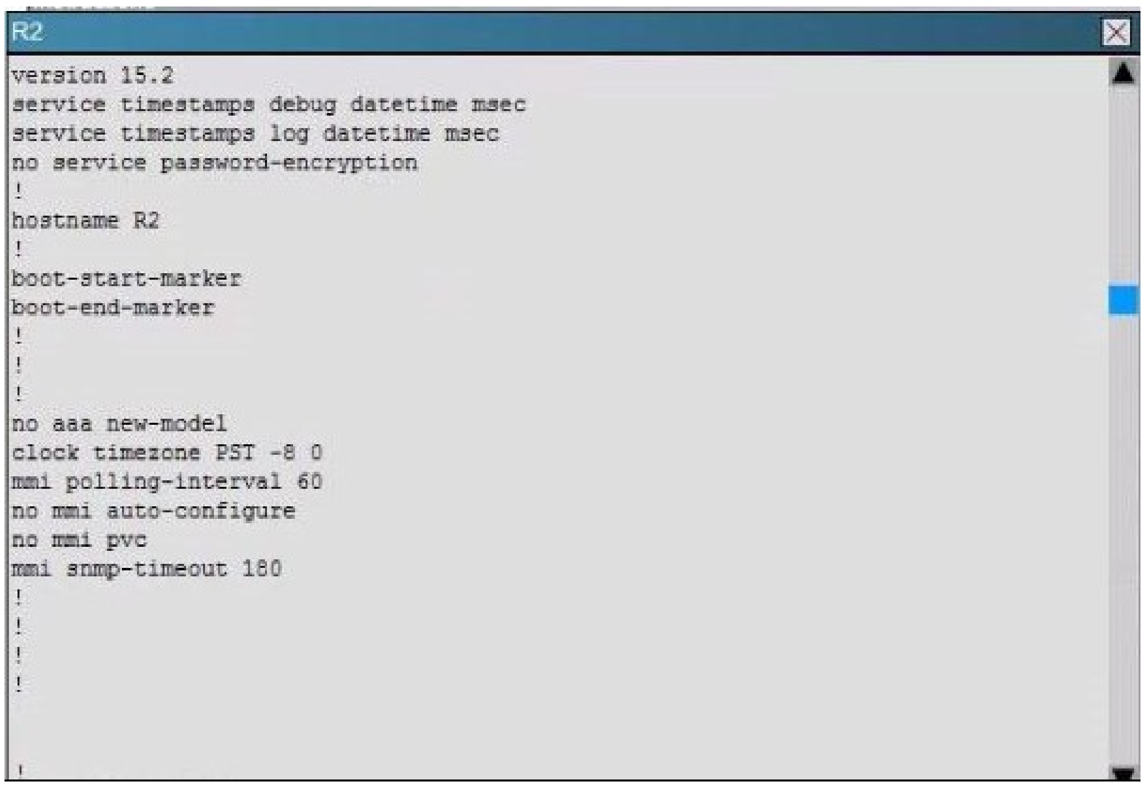
```
ip nat inside source list LOCAL interface Ethernet0/0 overload
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip access-list standard R2LANBLOCK
 deny   10.100.20.0 0.0.0.255
 permit any
!
ip access-list extended LOCAL
 permit ip host 127.0.0.1 any
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
 --- More (7) ---
```



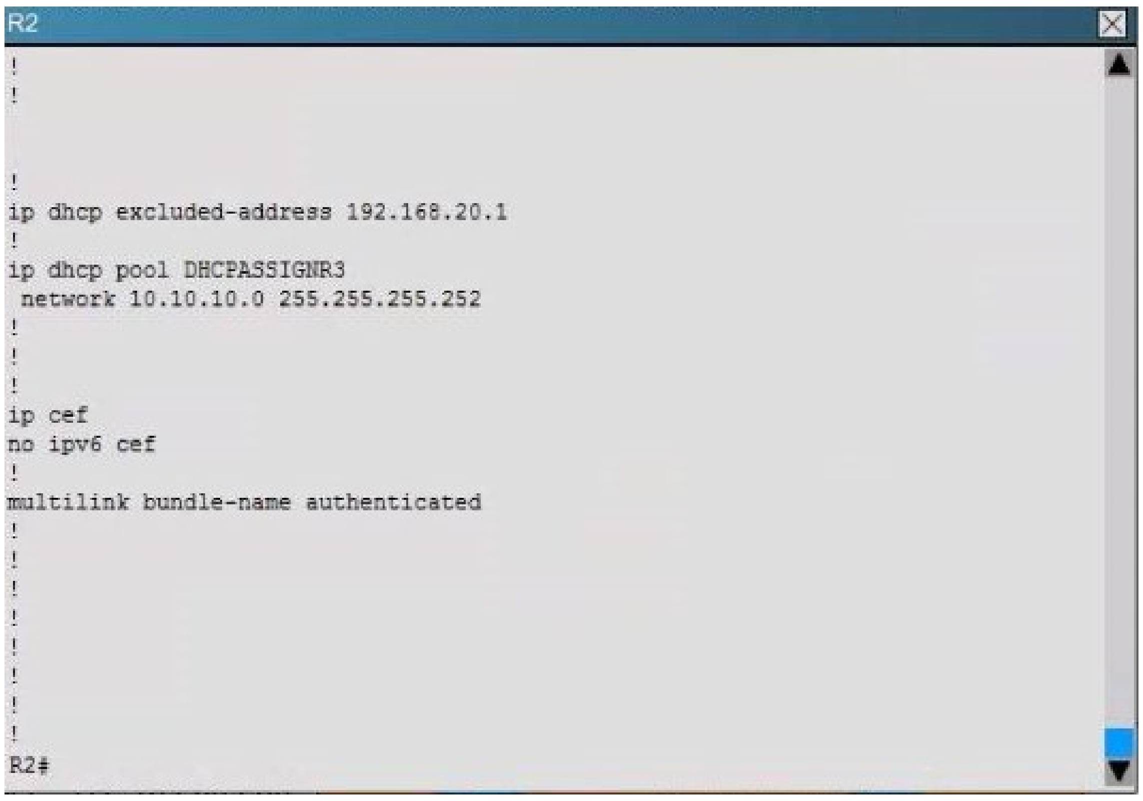
```
ip access-list extended LOCAL
 permit ip host 127.0.0.1 any
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
ntp server 209.165.200.226
!
end
R1#
```



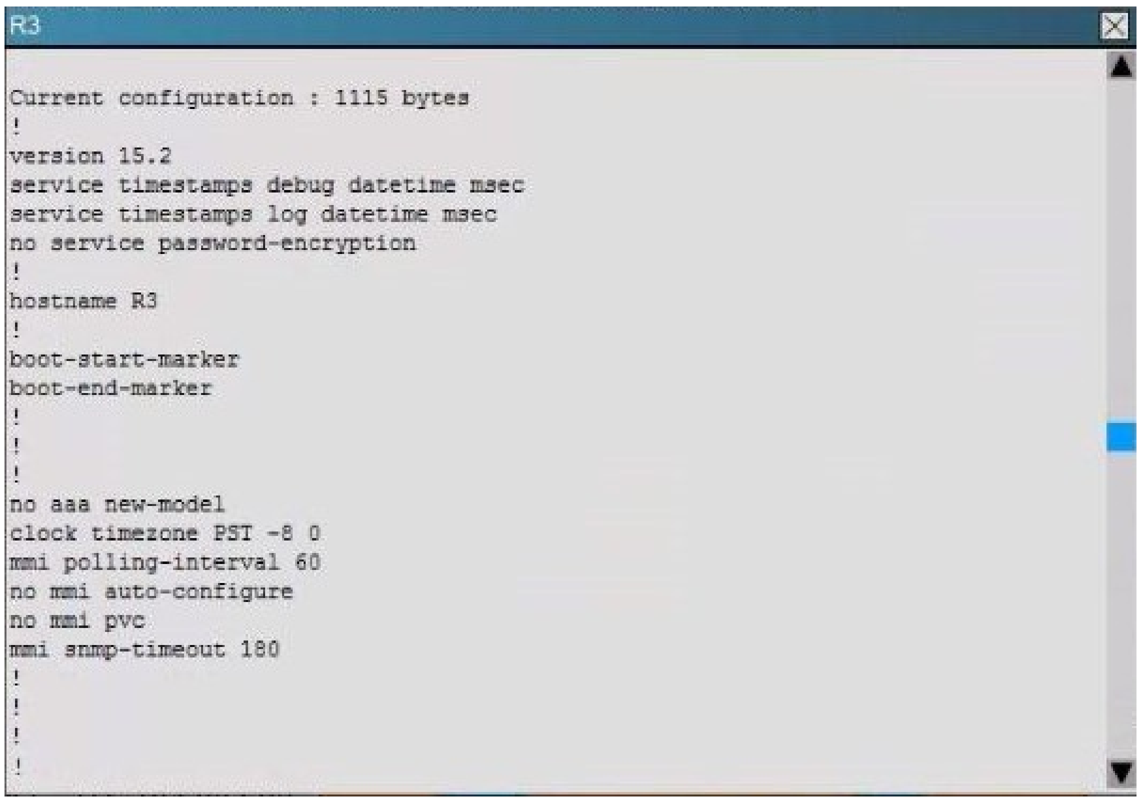
```
Building configuration...

Current configuration : 1243 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
 --- More (92) ---
```



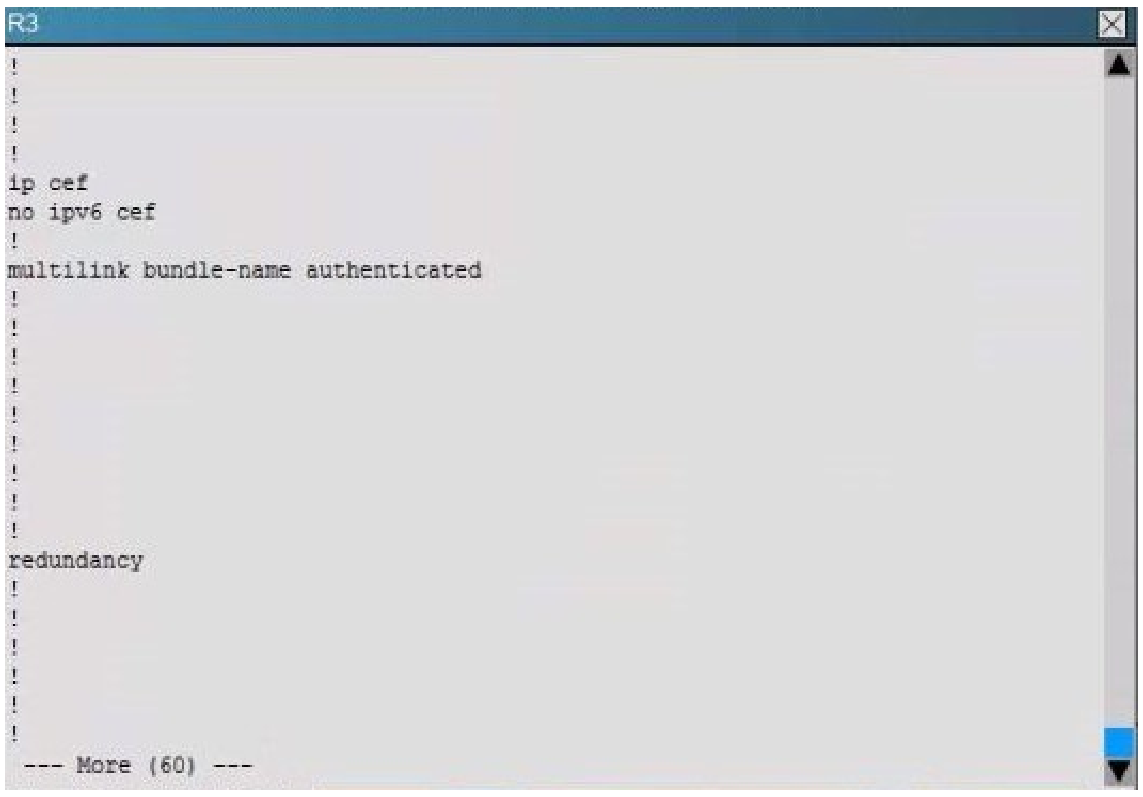
```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!


!
```



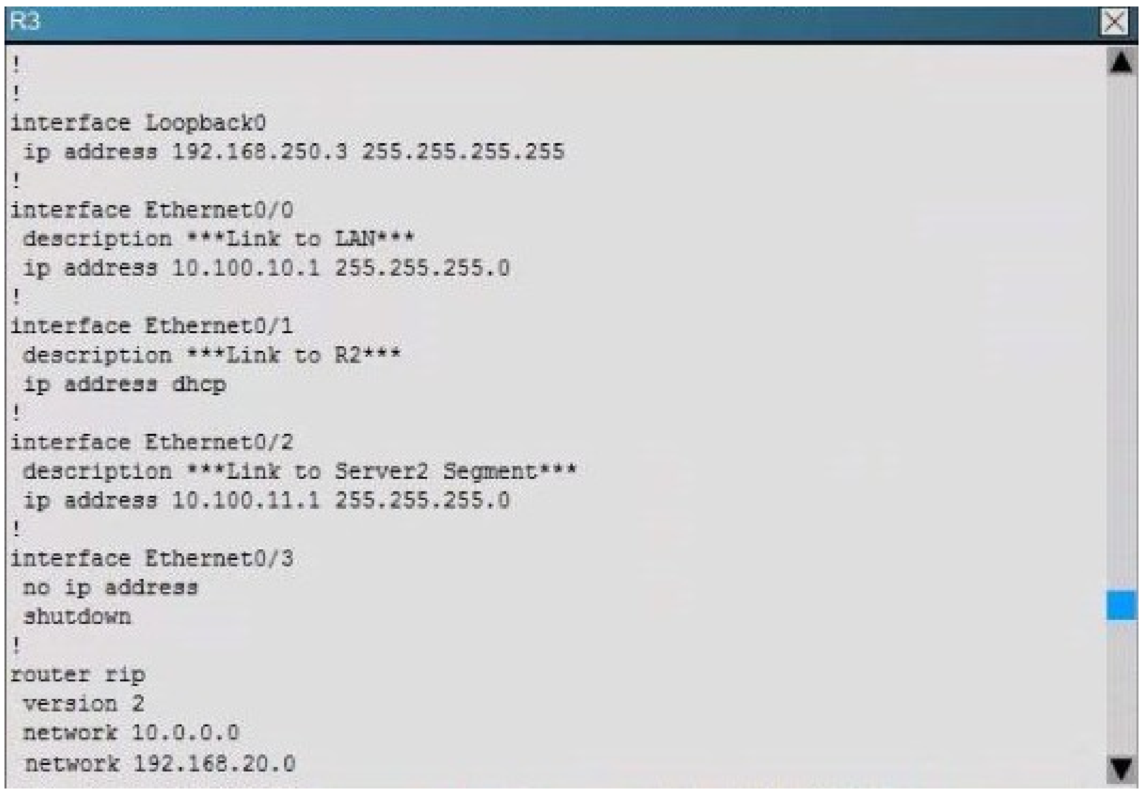
```
!
!


!
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool DHCPASSIGNR3
 network 10.10.10.0 255.255.255.252
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
R2#
```



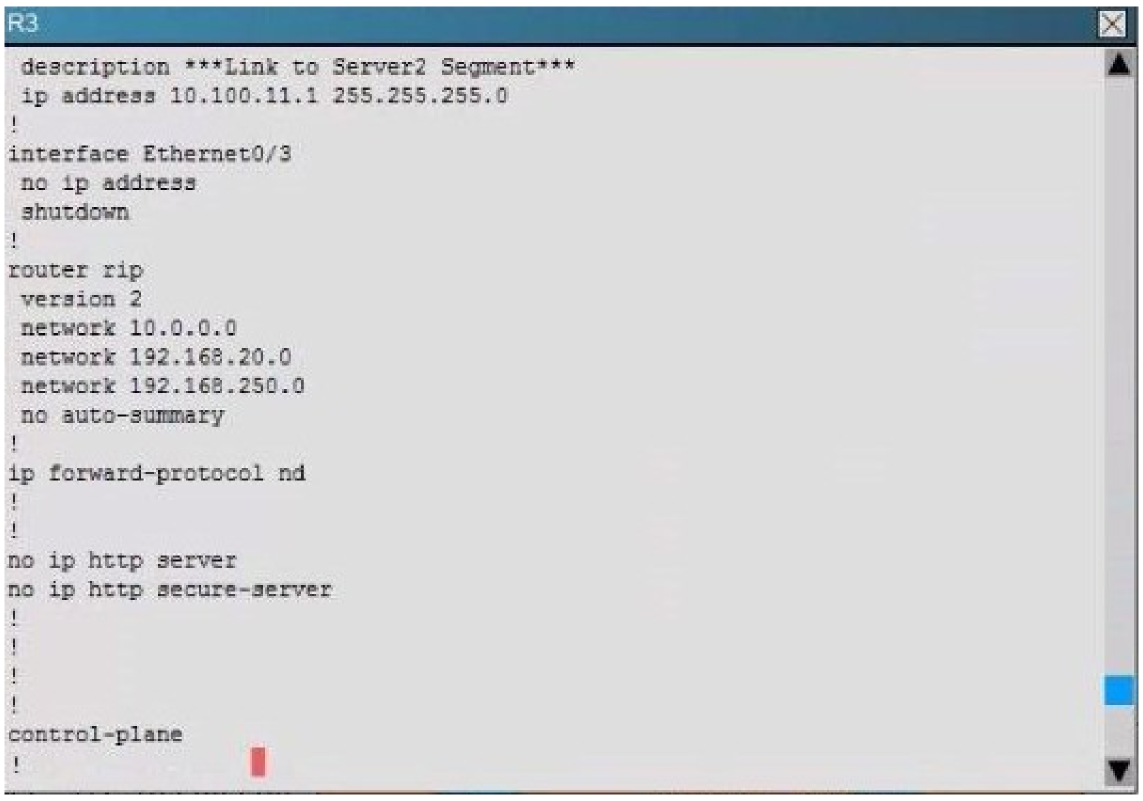
```

Current configuration : 1115 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
```



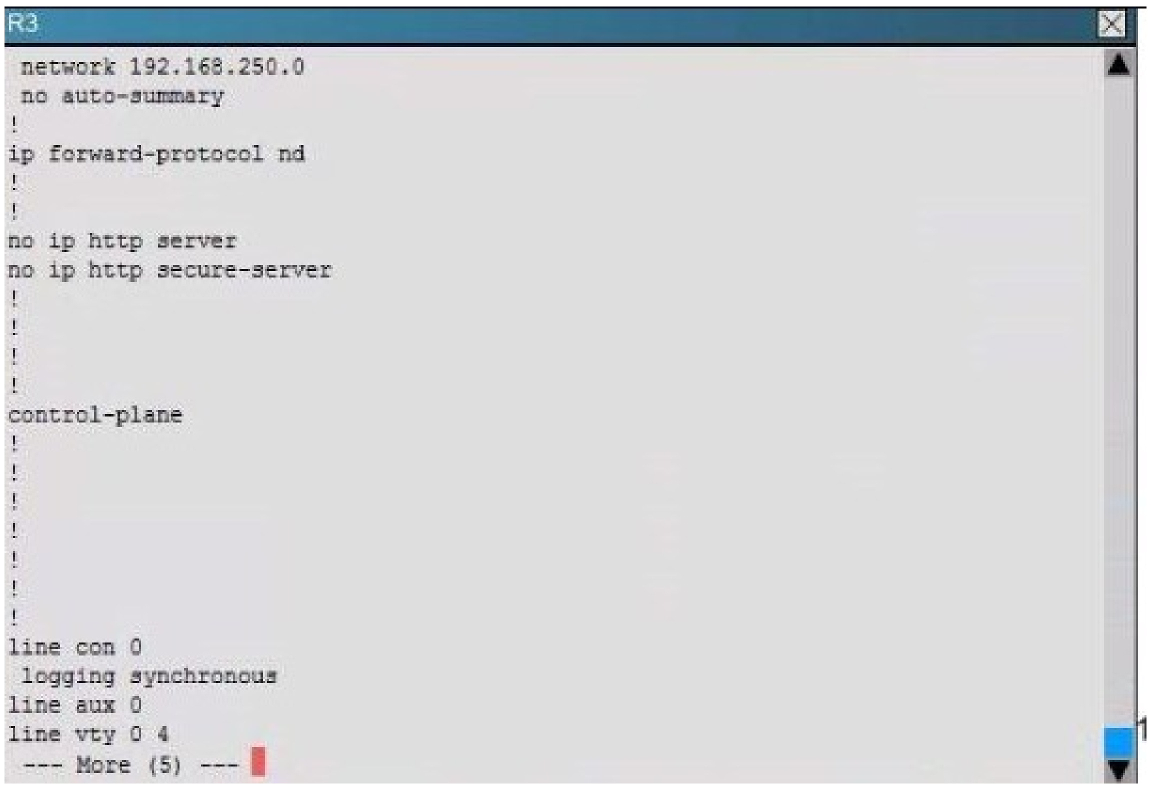
```
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
 --- More (60) ---
```



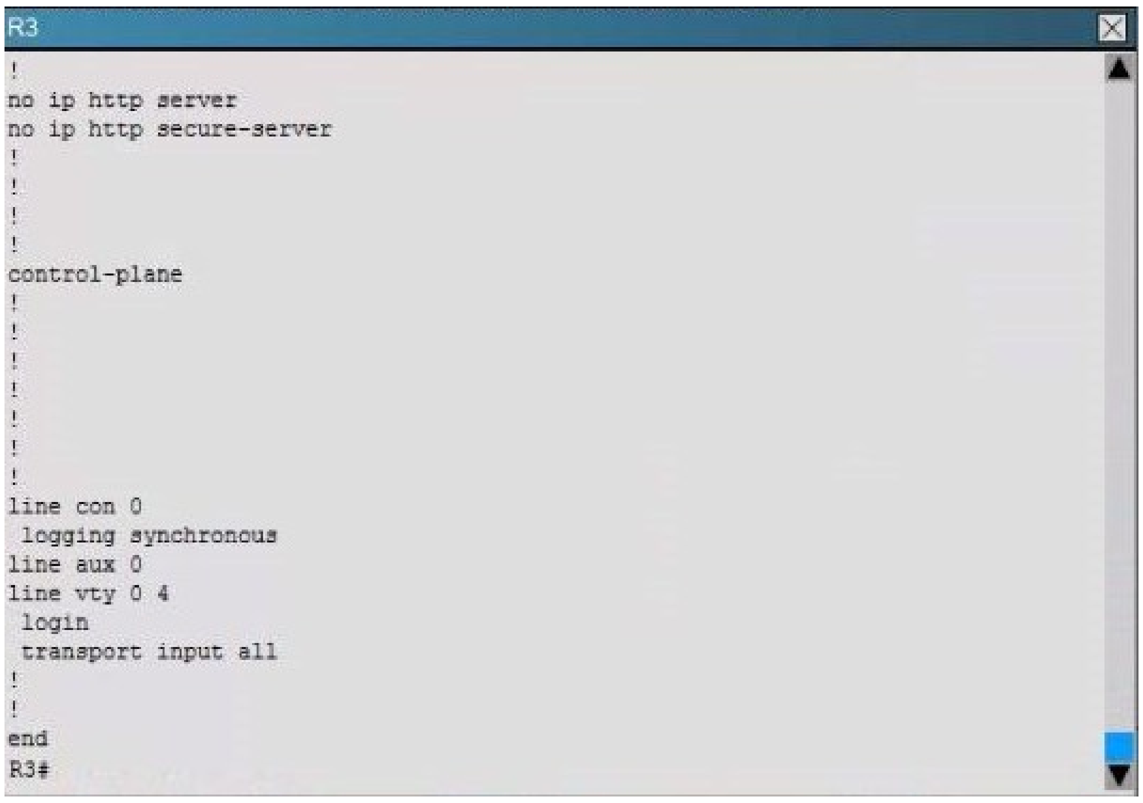
```
!
!
interface Loopback0
 ip address 192.168.250.3 255.255.255.255
!
interface Ethernet0/0
 description ***Link to LAN***
 ip address 10.100.10.1 255.255.255.0
!
interface Ethernet0/1
 description ***Link to R2***
 ip address dhcp
!
interface Ethernet0/2
 description ***Link to Server2 Segment***
 ip address 10.100.11.1 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.20.0
```



```
 description ***Link to Server2 Segment***
 ip address 10.100.11.1 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.20.0
 network 192.168.250.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
```



```
 network 192.168.250.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 --- More (5) ---
```



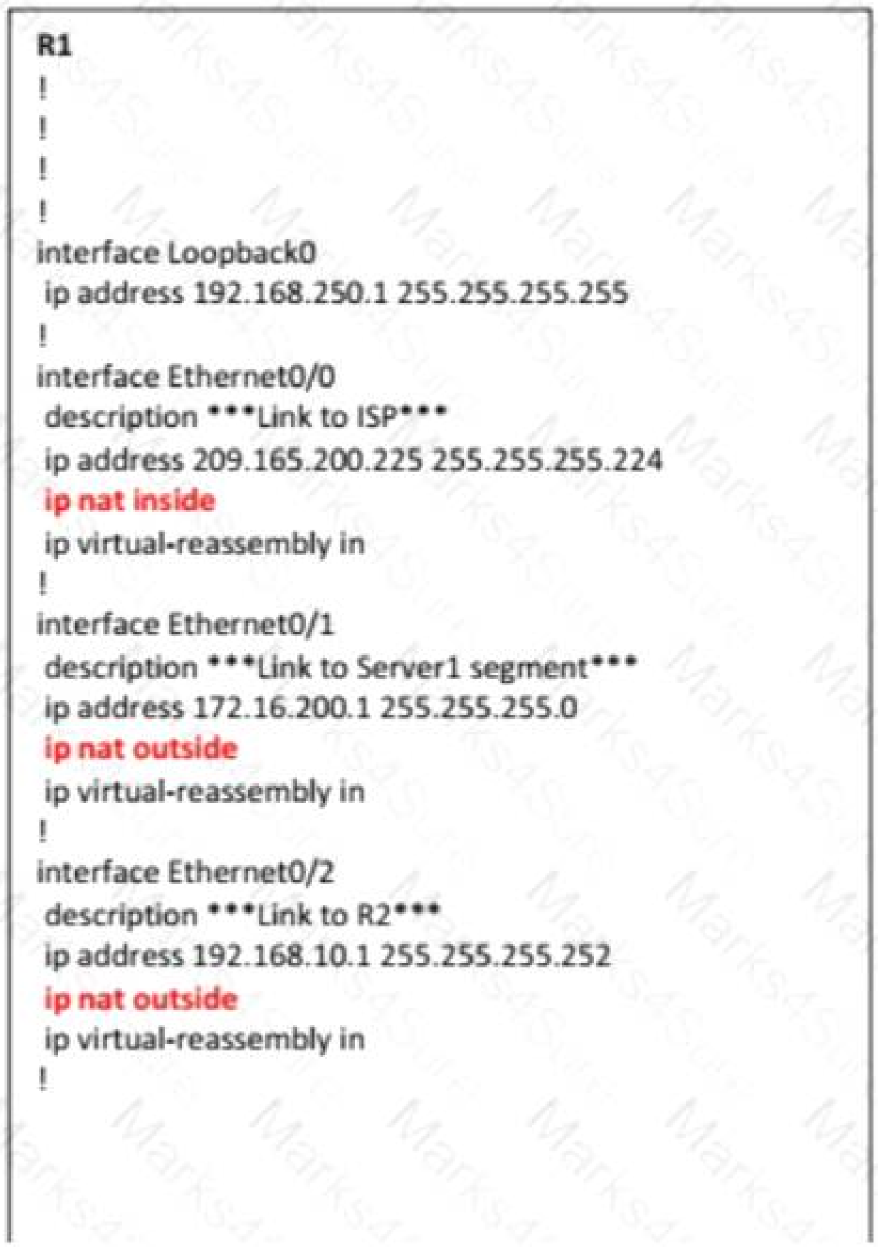
```
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
!
end
R3#
```

Users complain that they are unable to reach internet sites. You are troubleshooting internet connectivity problem at main office. Which statement correctly identifies the problem on Router R1?

A. Interesting traffic for NAT ACL is incorrectly configured.
B. NAT configurations on the interfaces are incorrectly configured
C. NAT translation statement incorrectly configured.
D. Only static NAT translation configured for the server, missing Dynamic NAT or Dynamic NAT overloading for internal networks.

**Answer:** B

**Explanation:**



```
R1
!
!
!
!
interface Loopback0
 ip address 192.168.250.1 255.255.255.255
!
interface Ethernet0/0
 description ***Link to ISP***
 ip address 209.165.200.225 255.255.255.224
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/1
 description ***Link to Server1 segment***
 ip address 172.16.200.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
!
interface Ethernet0/2
 description ***Link to R2***
 ip address 192.168.10.1 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
!
```

**NEW QUESTION 290**
Which entity assigns IPv6 addresses to end users?

A. ICANN
B. APNIC
C. RIR
D. ISPs

**Answer:** C

**NEW QUESTION 295**
By default, how many MAC addresses are permitted to be learned on a switch port with port security enabled?

A. 8
B. 2
C. 1

**Answer:** C

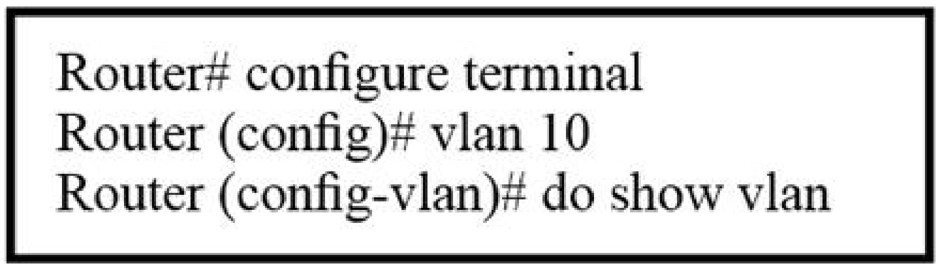
**NEW QUESTION 296**
What is one requirement for interfaces to run IPv6?

A. An IPv6 address must be configured on the interface.
B. An IPv4 address must be configured.
C. Stateless autoconfiguration must be enabled after enabling IPv6 on the interface.
D. IPv6 must be enabled with the ipv6 enable command in global configuration mode.

**Answer:** A

**Explanation:** To use IPv6 on your router, you must, at a minimum, enable the protocol and assign IPv6 addresses to your interfaces.

**NEW QUESTION 299**
Refer to the exhibit.



```
Router# configure terminal
Router (config)# vlan 10
Router (config-vlan)# do show vlan
```

Which statement describes the effect of this configuration?

A. The VLAN 10 VTP configuration is displayed.
B. VLAN 10 spanning-tree output is displayed.
C. The VLAN 10 configuration is saved when the router exits VLAN configuration mode.
D. VLAN 10 is added to the VLAN database.

**Answer:** D

**Explanation:** With the configuration above, when we type “do show vlan” we would not see VLAN 10 in the VLAN database because it has not been created yet. VLAN 10 is only created when we exits VLAN configuration mode (with “exit” command).

**NEW QUESTION 304**
Which destination IP address can a host use to send one message to multiple devices across different subnets?

A. 172.20.1.0
B. 127.0.0.1
C. 192.168.0.119
D. 239.255.0.1

**Answer:** D

**Explanation:** Multicast is a networking protocol where one host can send a message to a special multicast IP address and one or more network devices can listen for and receive those messages.
Multicast works by taking advantage of the existing IPv4 networking infrastructure, and it does so in something of a weird fashion. As you read, keep in mind that things are a little confusing because multicast was "shoe-horned" in to an existing technology.
For the rest of this article, let's use the multicast IP address of 239.255.0.1. We'll not worry about port numbers yet, but make a mental note that they are used in multicast. We'll discuss that later.

**NEW QUESTION 307**
Which MTU size can cause a baby giant error?

A. 1500
B. 9216
C. 1600
D. 1518

**Answer:** D

**Explanation:** http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/29805-175.html

**NEW QUESTION 312**

Scenario:

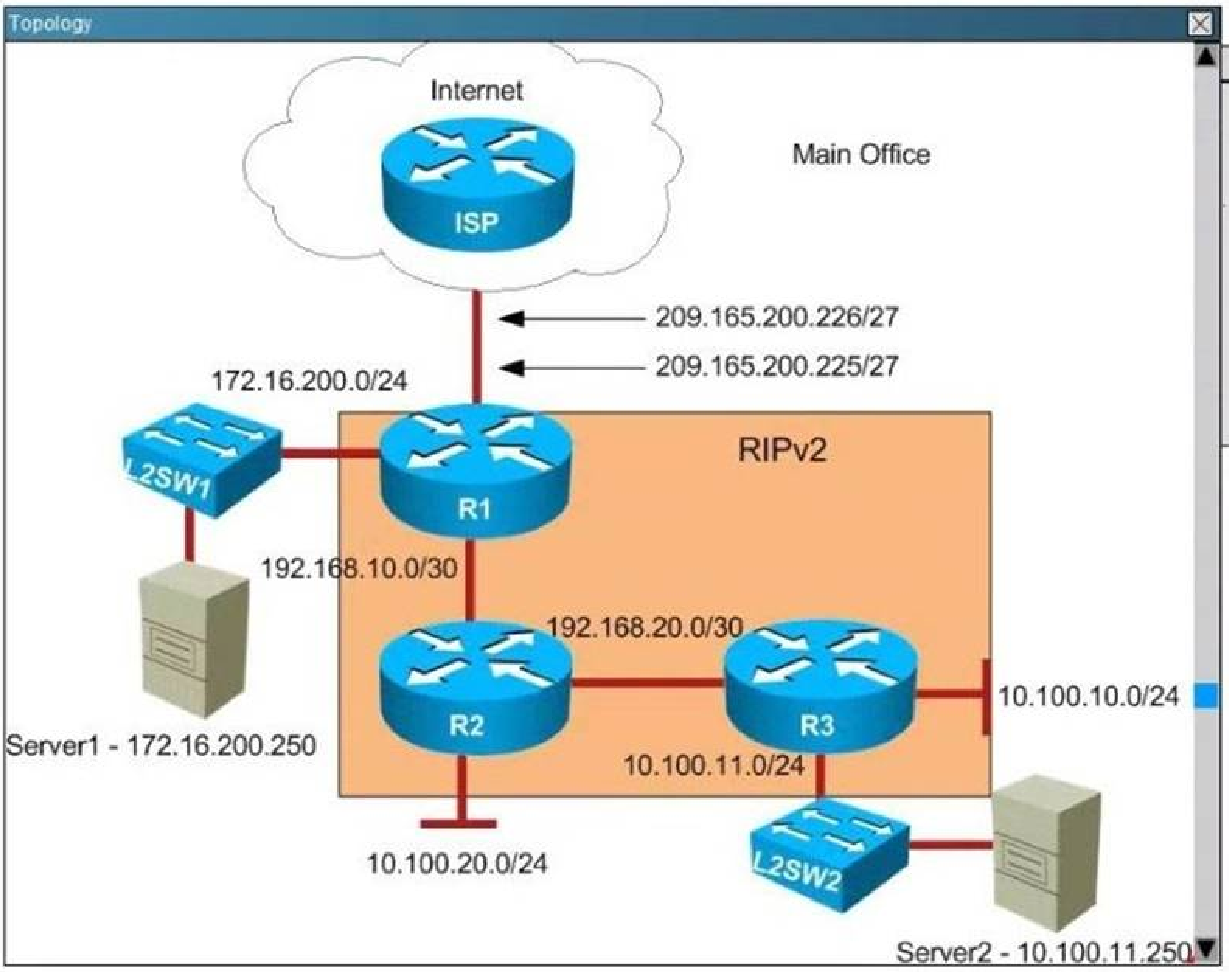
You are a junior network engineer for a financial company, and the main office network is experiencing network issues. Troubleshoot the network issues.

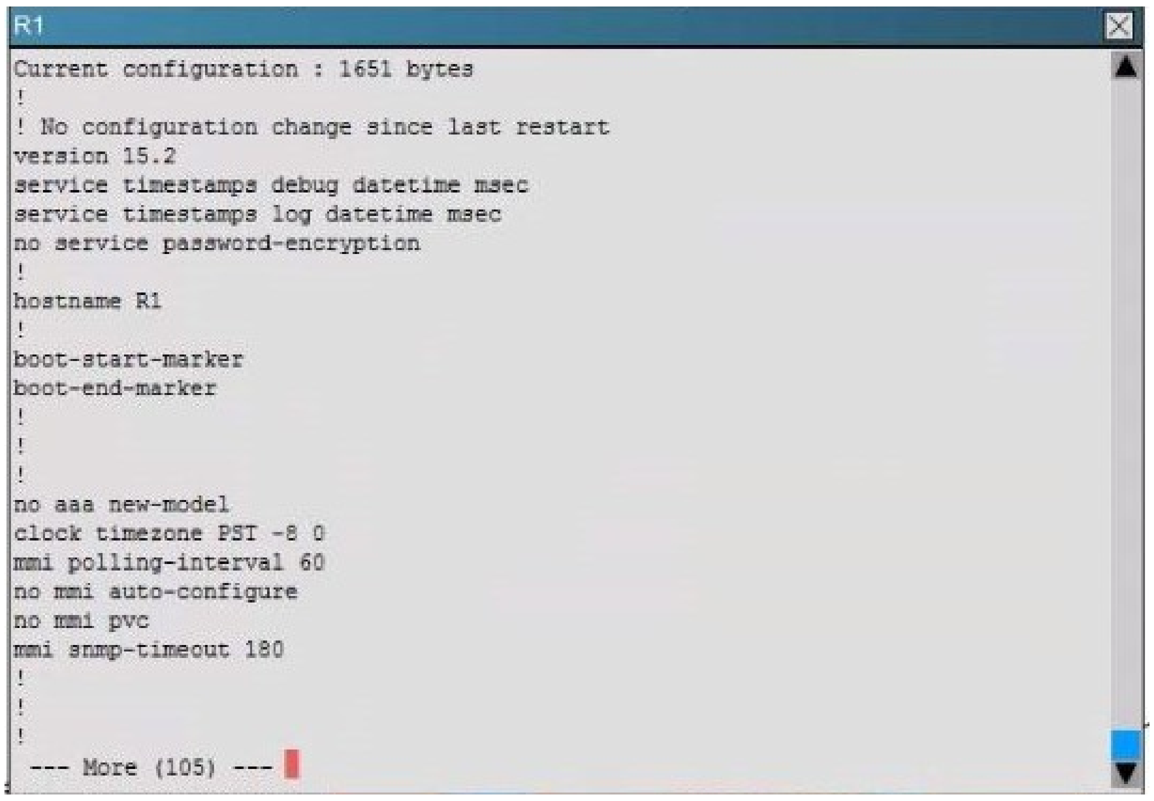
Router R1 connects the main office to the internet, and routers R2 and R3 are internal routers. NAT is enabled on router R1.

The routing protocol that is enabled between routers R1, R2 and R3 is RIPv2.

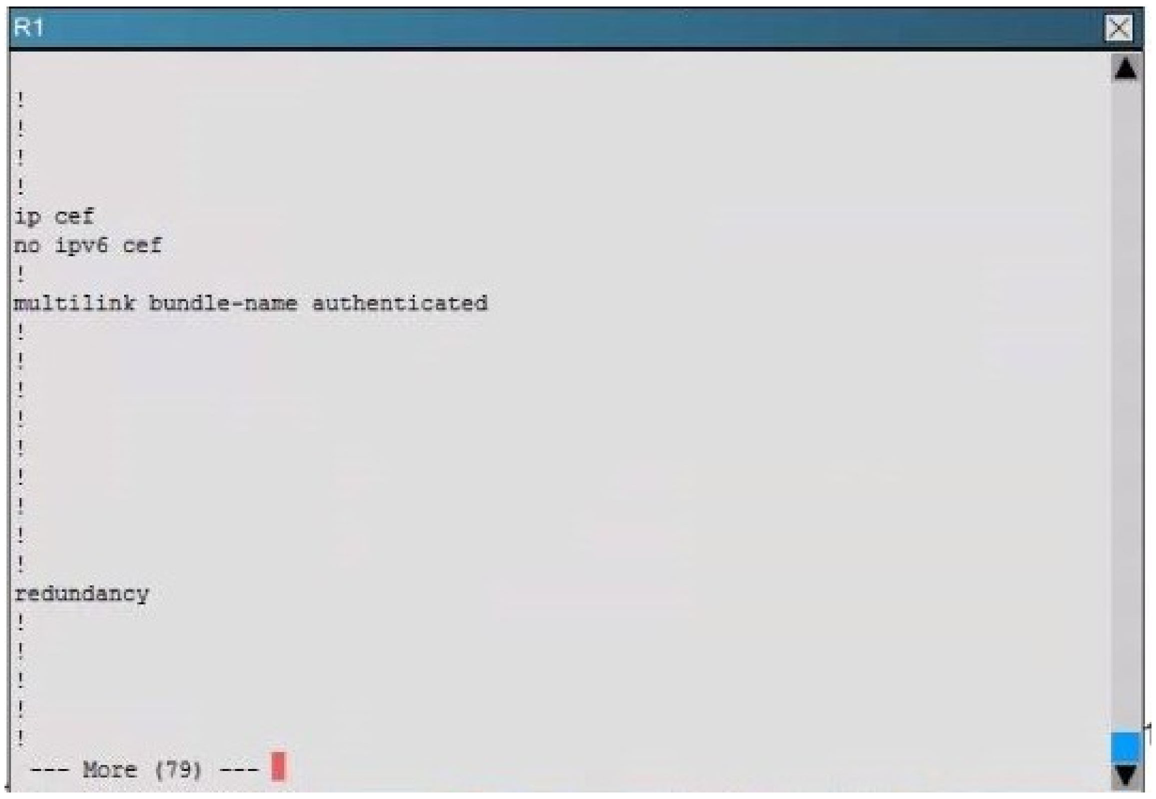
R1 sends the default route into RIPv2 for the internal routers to forward internet traffic to R1.

You have console access on R1, R2 and R3 devices. Use only show commands to troubleshoot the issues.

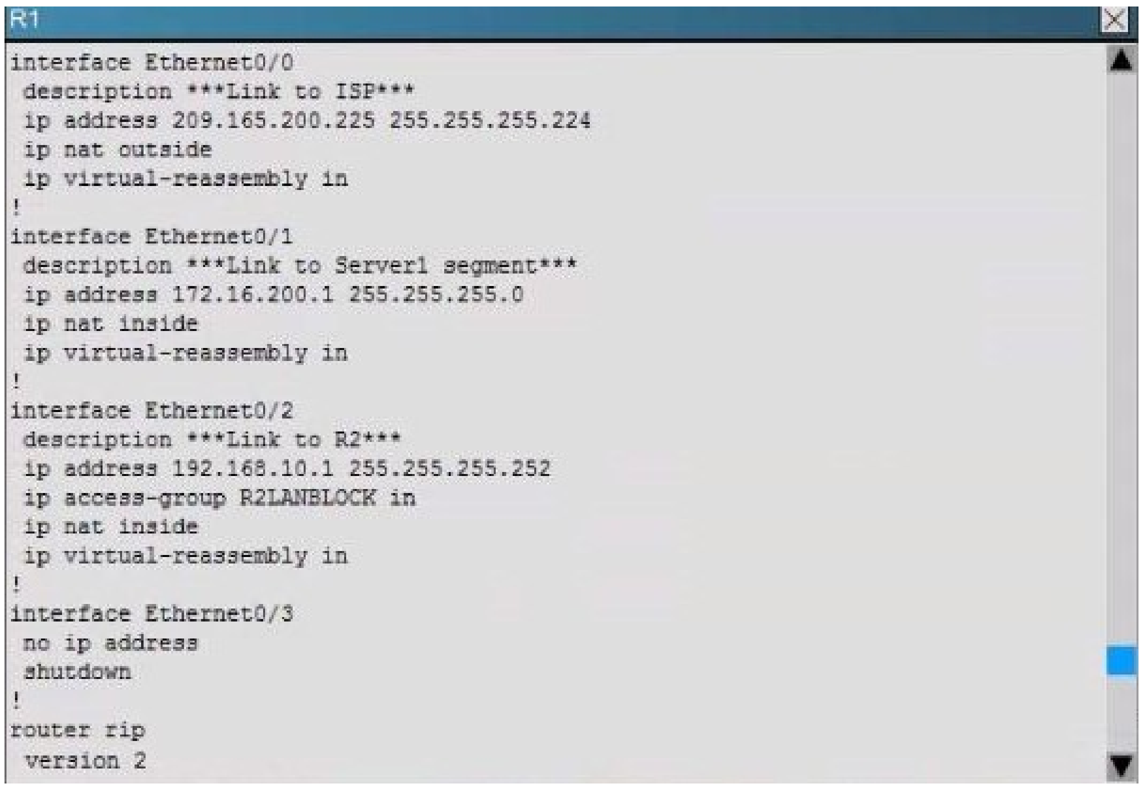




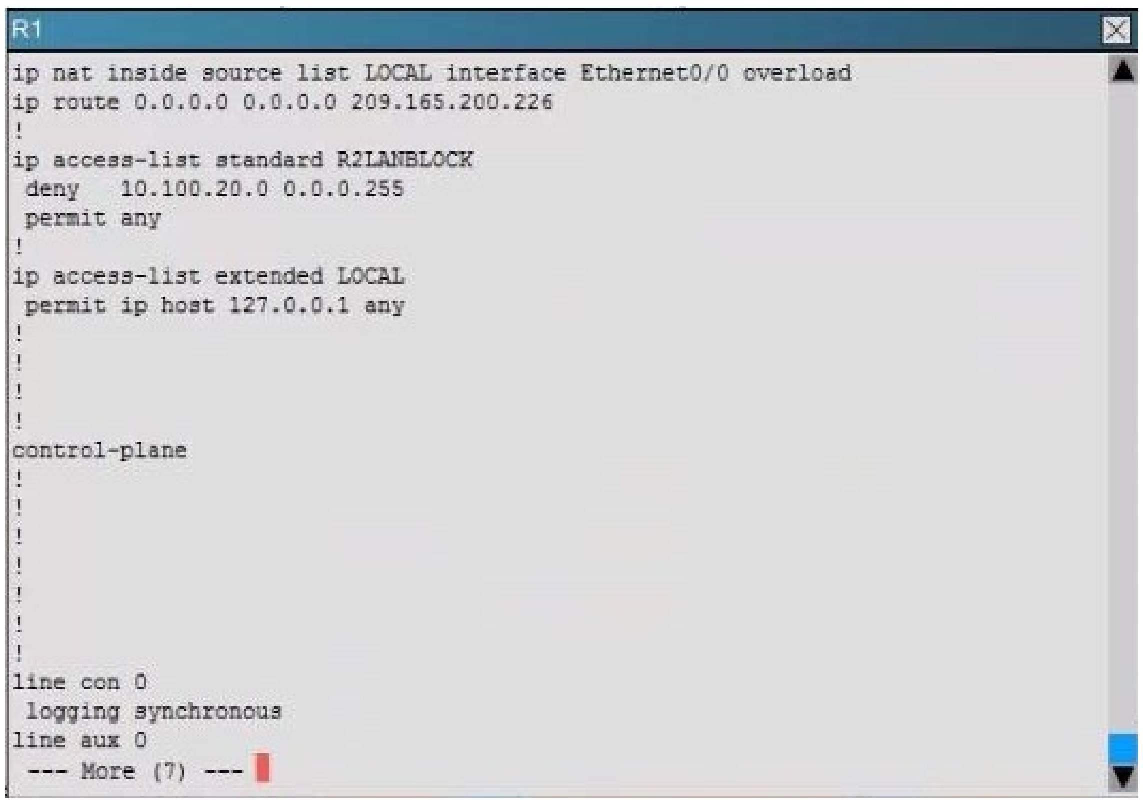
```
Current configuration : 1651 bytes
!
! No configuration change since last restart
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
 --- More (105) ---
```



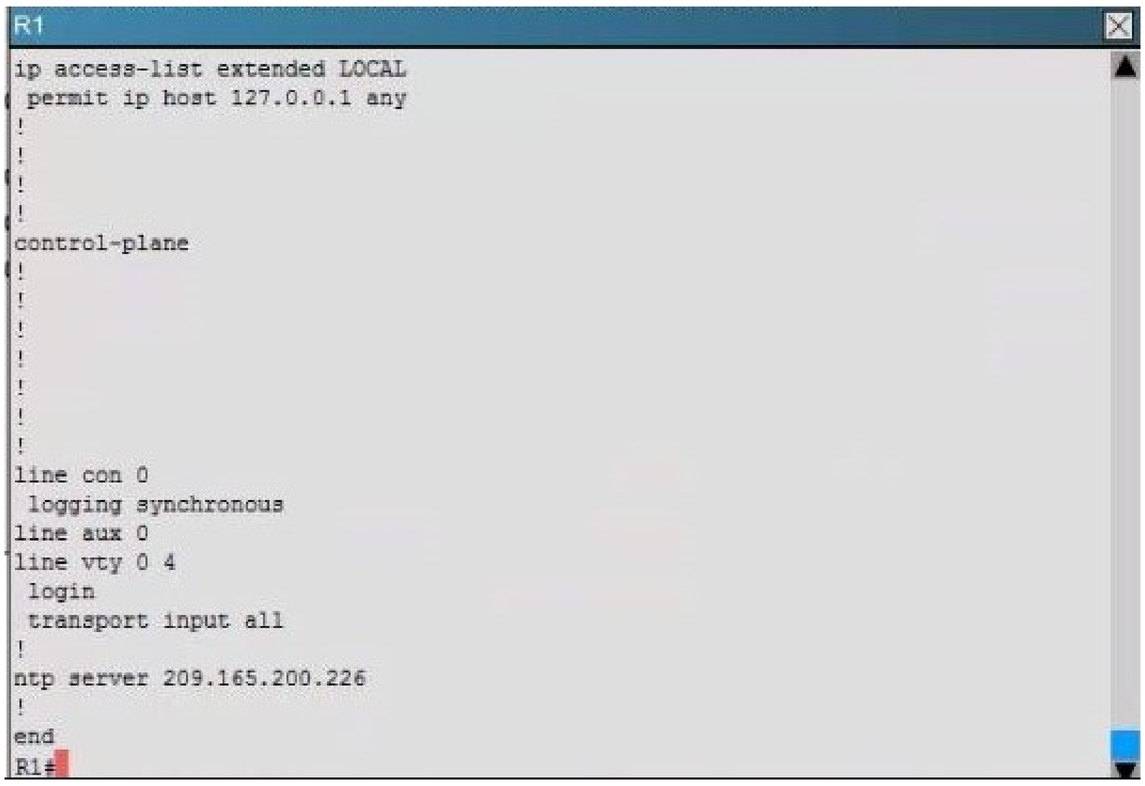
```
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
 --- More (79) ---
```



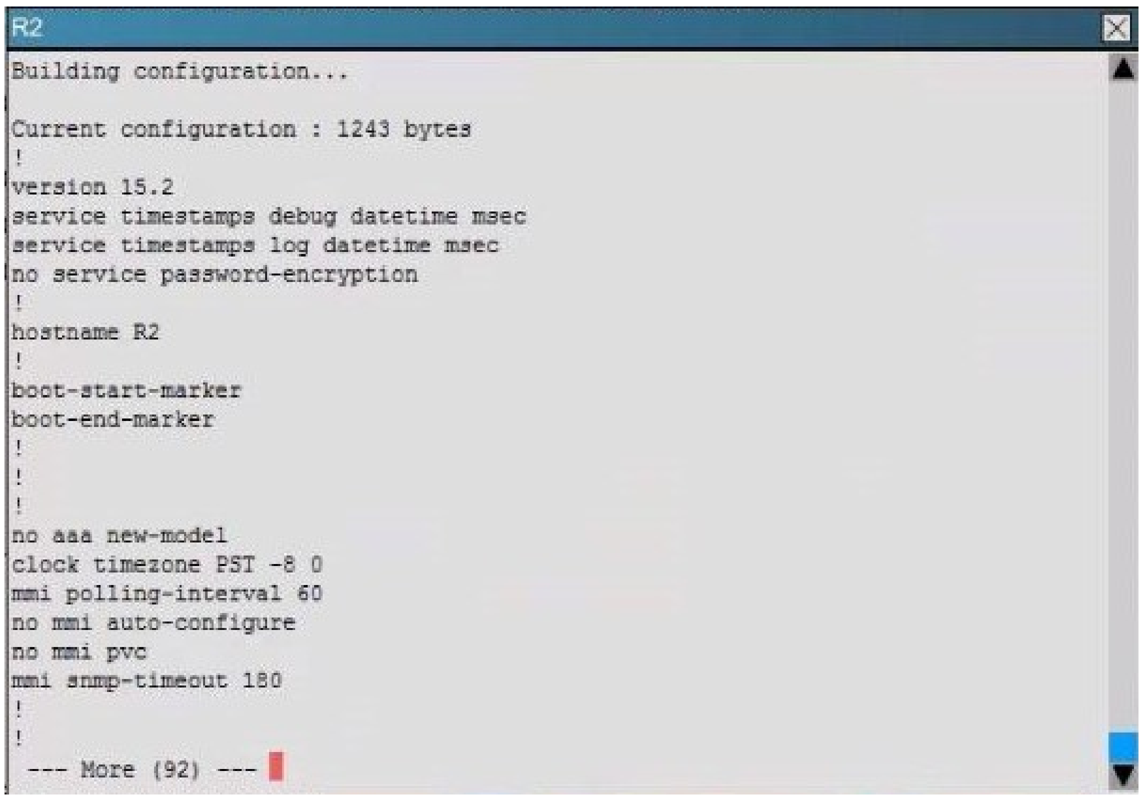
```
interface Ethernet0/0
 description ***Link to ISP***
 ip address 209.165.200.225 255.255.255.224
 ip nat outside
 ip virtual-reassembly in
!
interface Ethernet0/1
 description ***Link to Server1 segment***
 ip address 172.16.200.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/2
 description ***Link to R2***
 ip address 192.168.10.1 255.255.255.252
 ip access-group R2LANBLOCK in
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
```



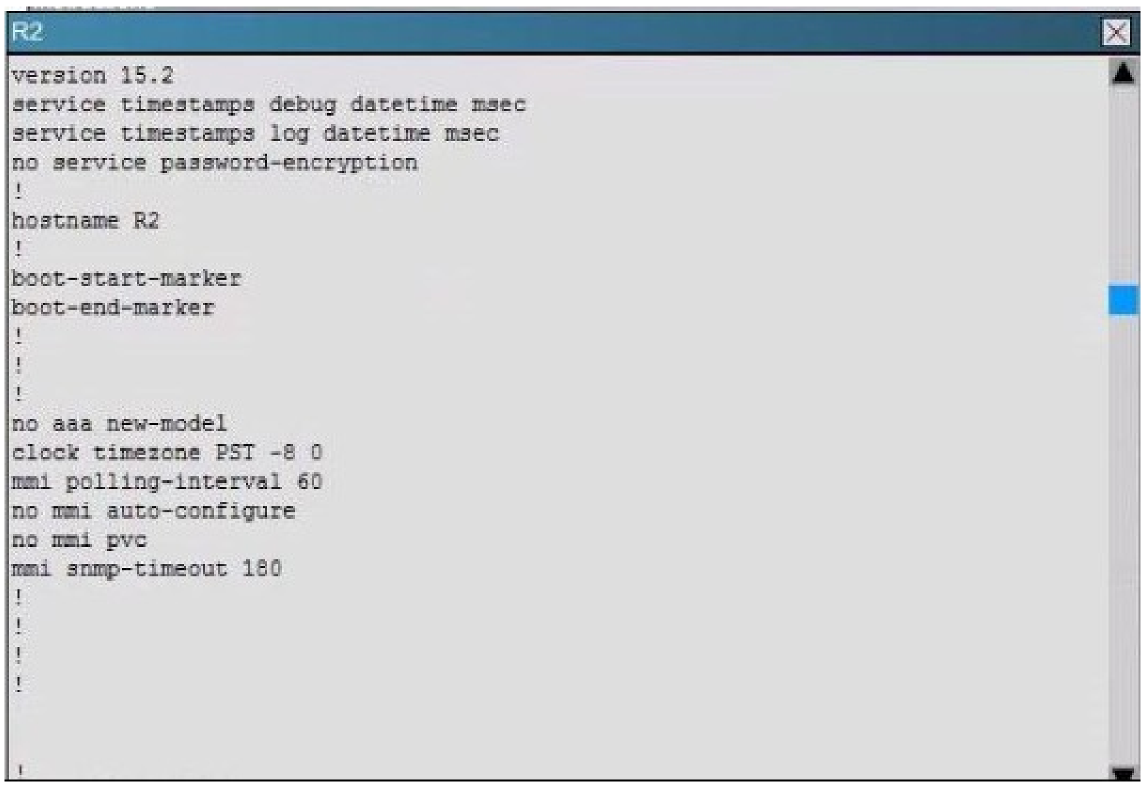
```
ip nat inside source list LOCAL interface Ethernet0/0 overload
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip access-list standard R2LANBLOCK
 deny   10.100.20.0 0.0.0.255
 permit any
!
ip access-list extended LOCAL
 permit ip host 127.0.0.1 any
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
 --- More (7) ---
```



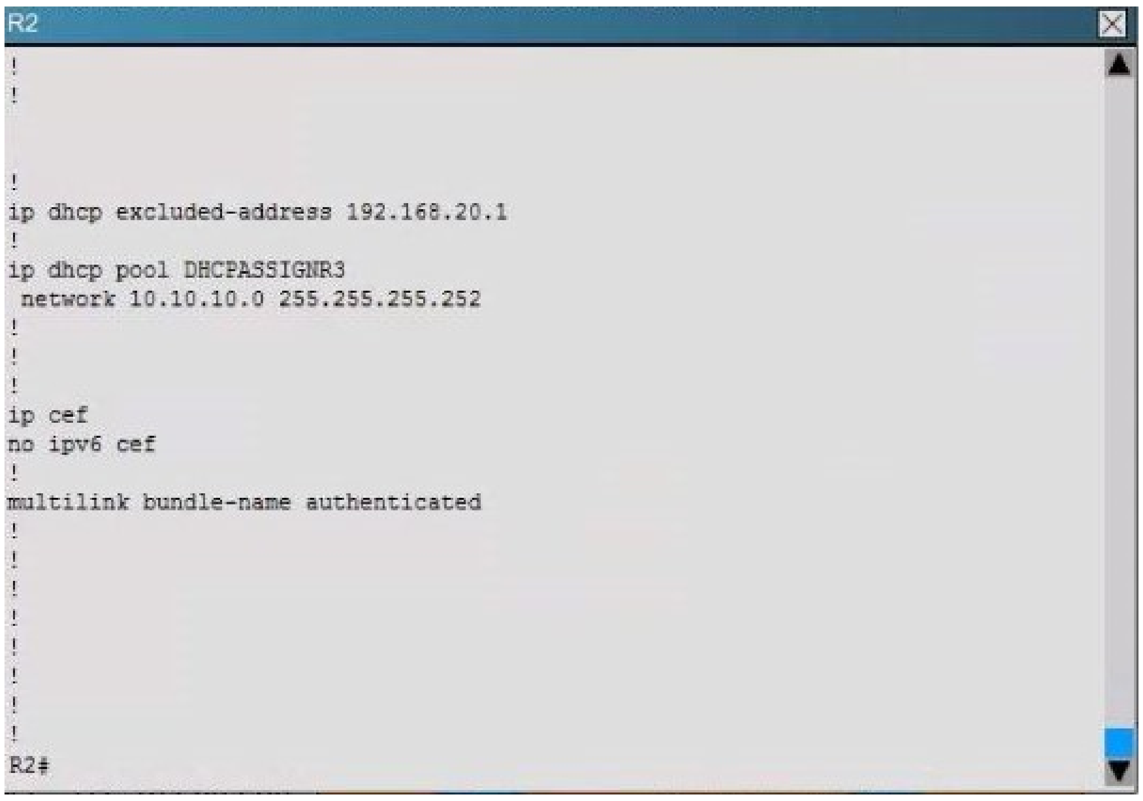
```
ip access-list extended LOCAL
 permit ip host 127.0.0.1 any
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
ntp server 209.165.200.226
!
end
R1#
```



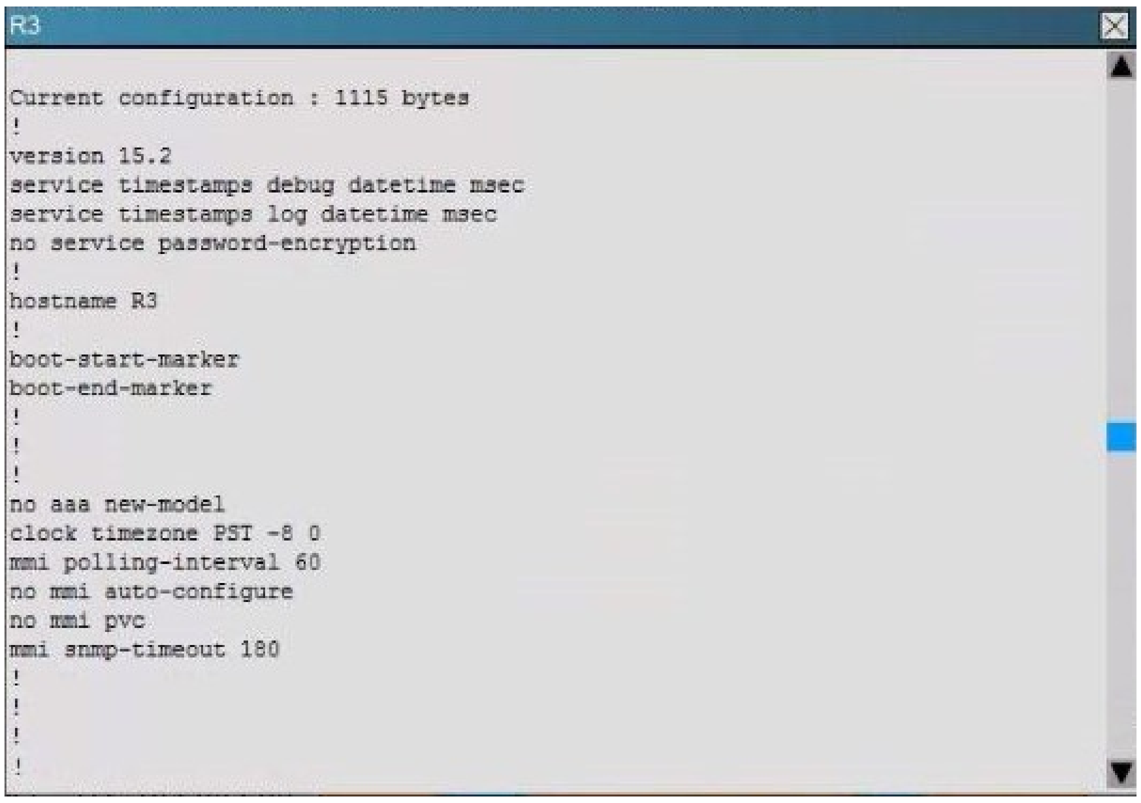
```
Building configuration...

Current configuration : 1243 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
 --- More (92) ---
```



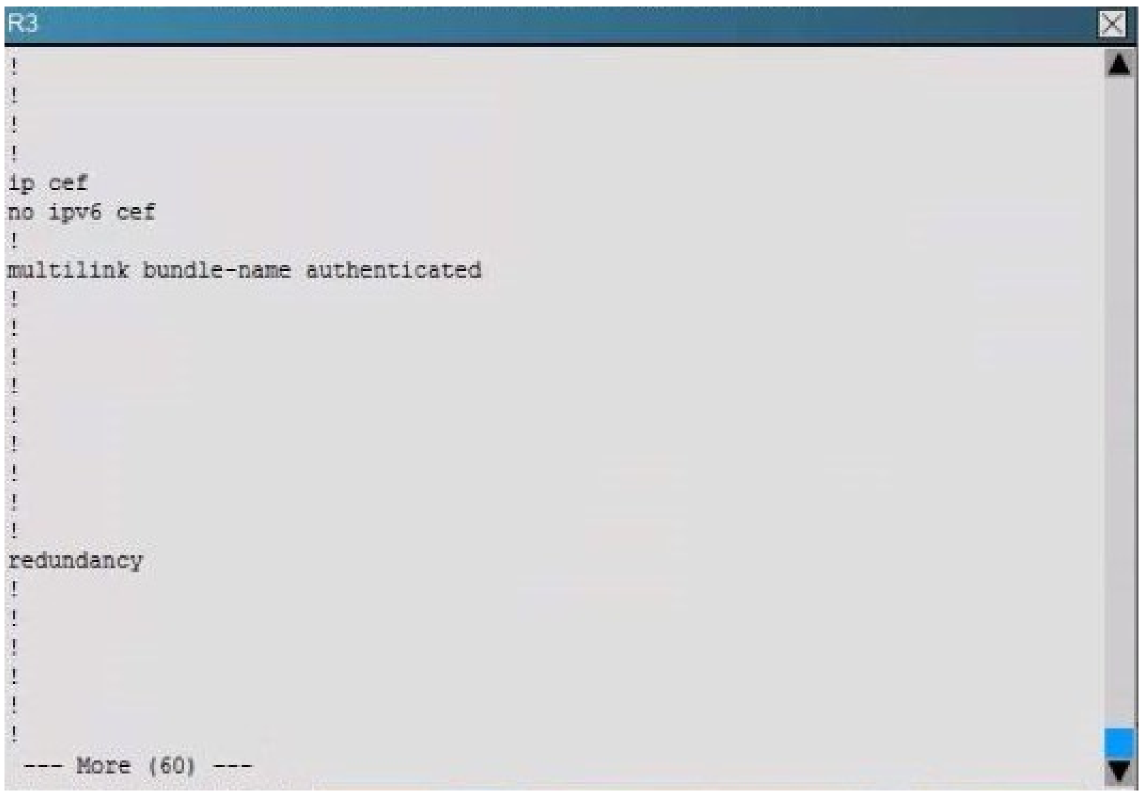
```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!


!
```



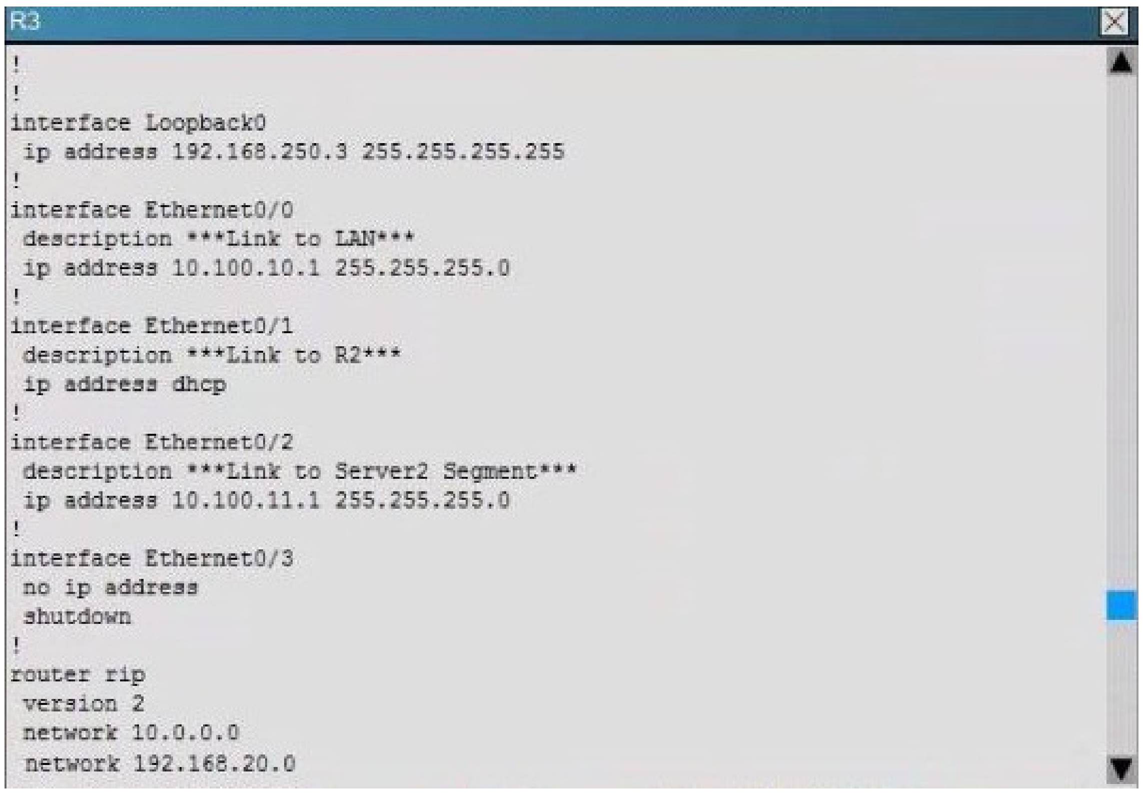
```
!
!


!
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool DHCPASSIGNR3
 network 10.10.10.0 255.255.255.252
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
R2#
```



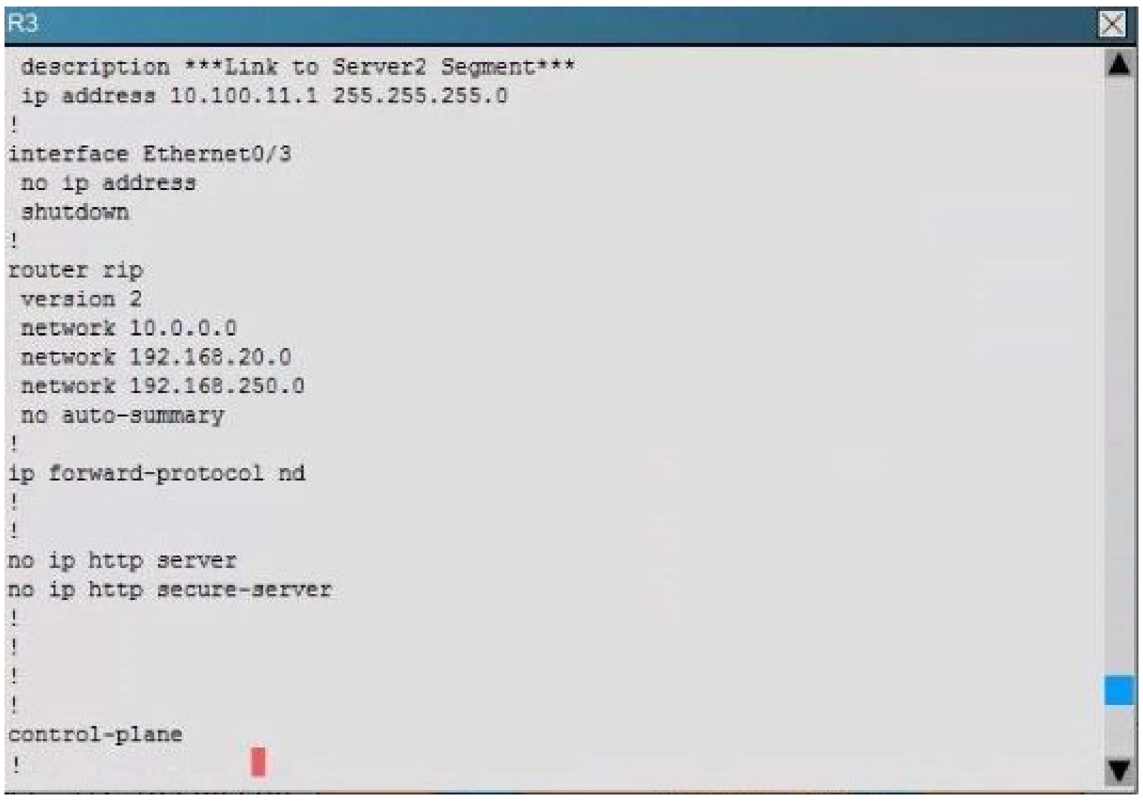
```

Current configuration : 1115 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
```



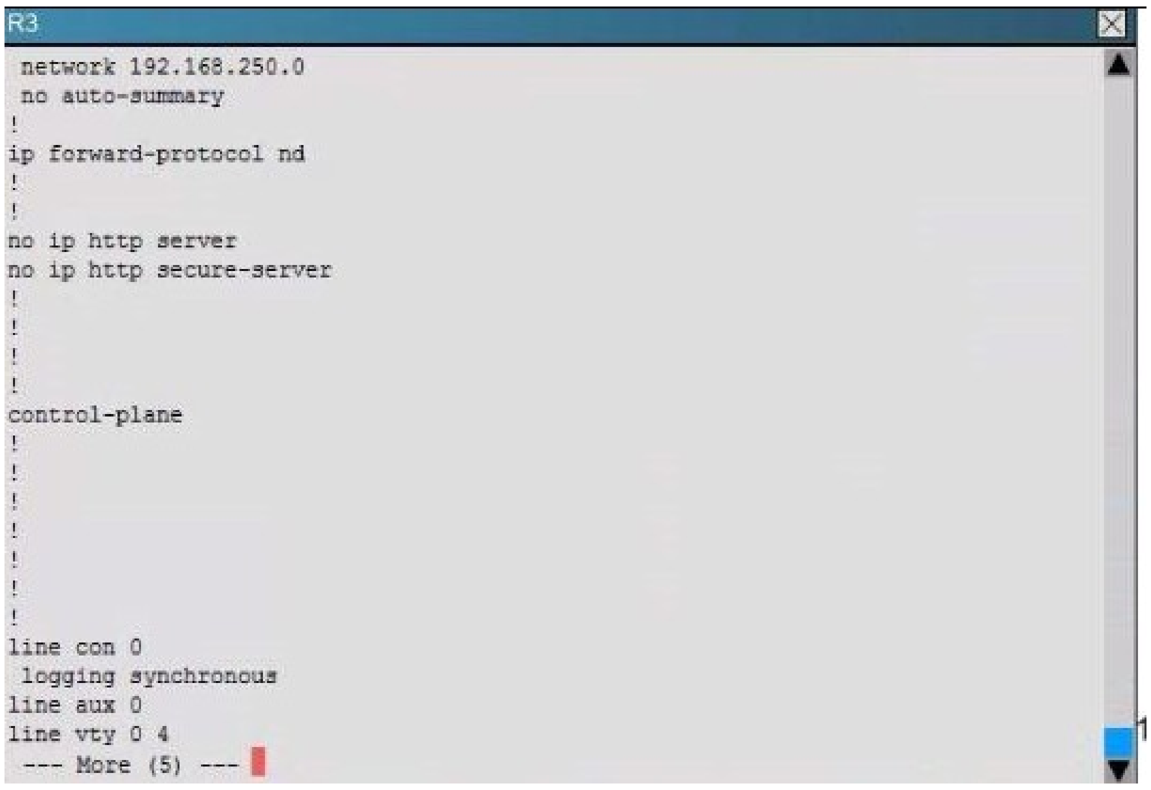
```
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
 --- More (60) ---
```



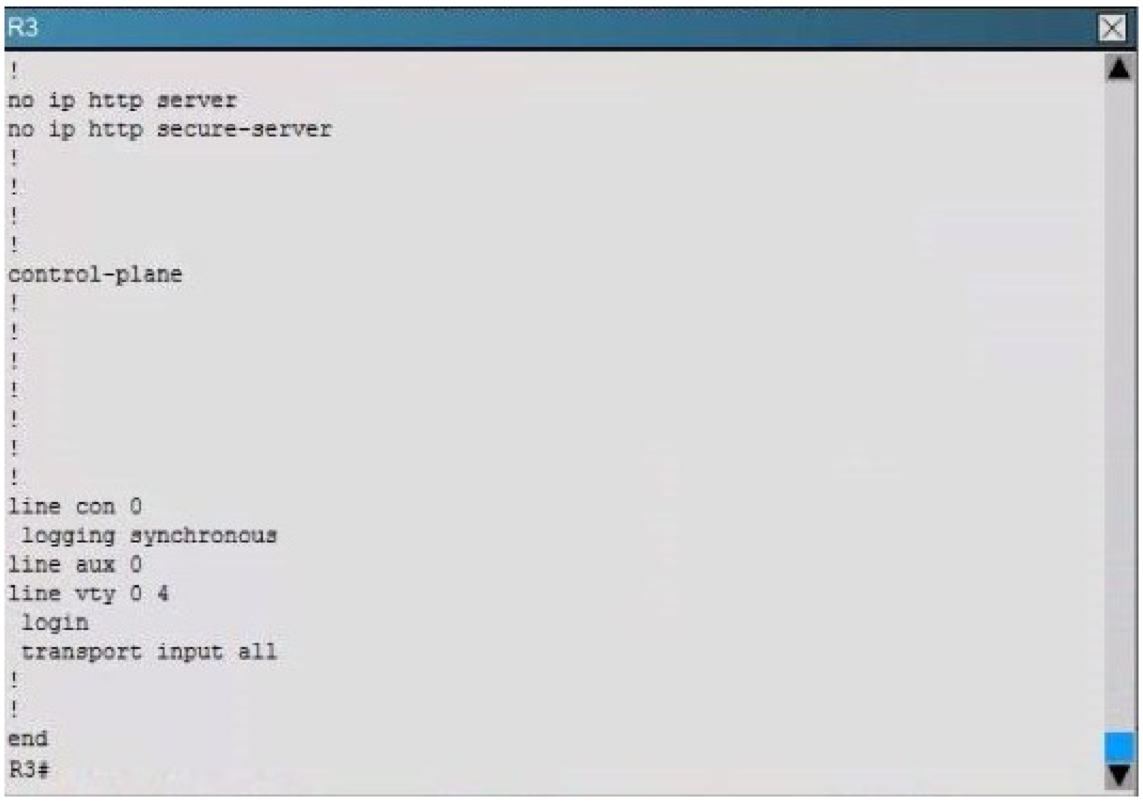
```
!
!
interface Loopback0
 ip address 192.168.250.3 255.255.255.255
!
interface Ethernet0/0
 description ***Link to LAN***
 ip address 10.100.10.1 255.255.255.0
!
interface Ethernet0/1
 description ***Link to R2***
 ip address dhcp
!
interface Ethernet0/2
 description ***Link to Server2 Segment***
 ip address 10.100.11.1 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.20.0
```



```
 description ***Link to Server2 Segment***
 ip address 10.100.11.1 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.20.0
 network 192.168.250.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
```



```
 network 192.168.250.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 --- More (5) ---
```



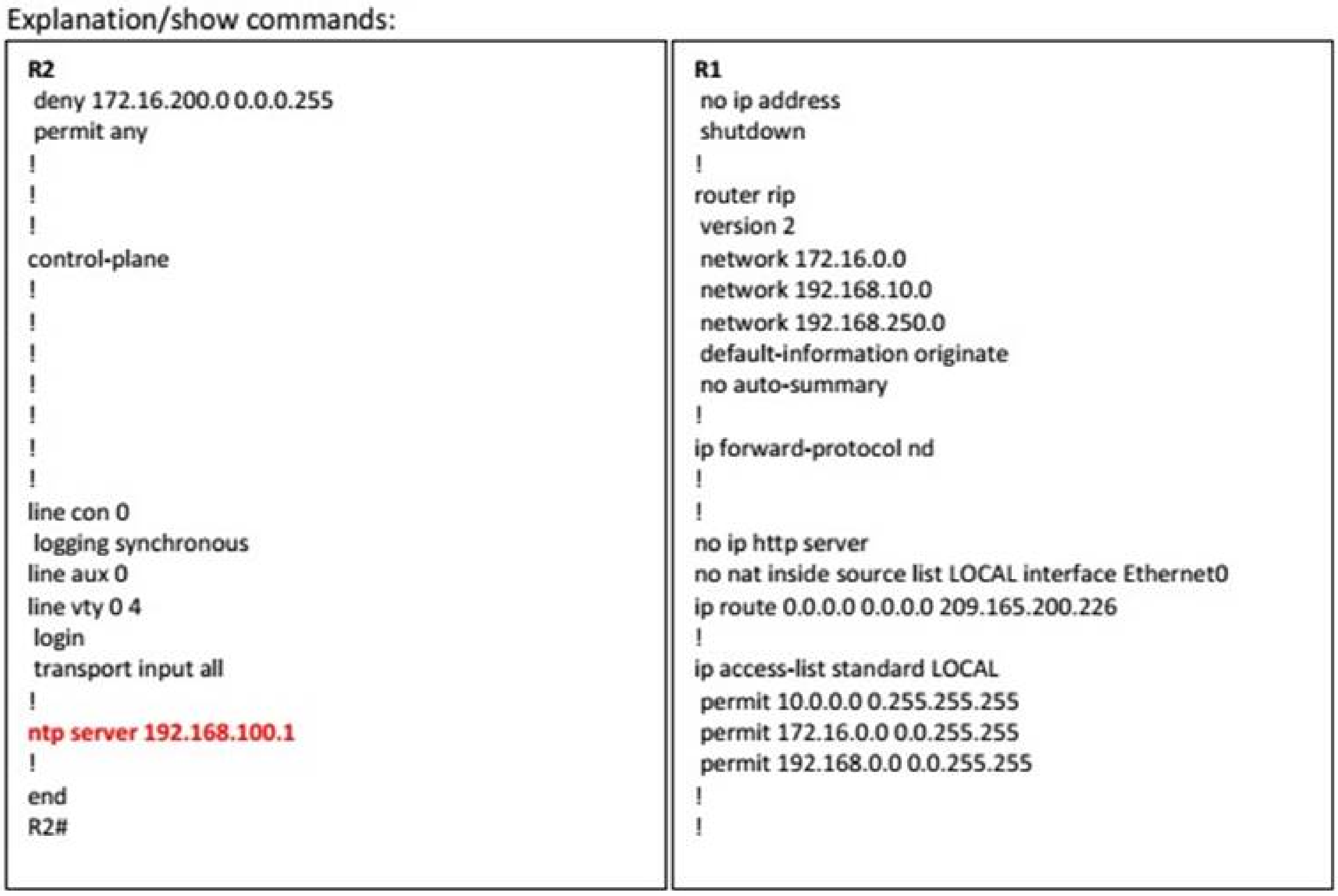
```
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
!
end
R3#
```

R1 router clock is synchronized with ISP router R2 is supposed to receive NTP updates from R1. But you observe that R2 clock is not synchronized with R1. What is the reason R2 is not receiving NTP updates from R1?

A. The IP address that is used in the NTP configuration on R2 router is incorrect.
B. The NTP server command not configured on R2 router.
C. R2 router Ethernet interface that is connected to R1 is placed in shutdown condition.
D. R1 router Ethernet interface that is connected to R2 is placed in shutdown condition.

**Answer:** A

**Explanation:** Check the below configuration for this


Explanation/show commands:

```
R2
 deny 172.16.200.0 0.0.0.255
 permit any
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
ntp server 192.168.100.1
!
end
R2#
```

```
R1
 no ip address
 shutdown
!
router rip
 version 2
 network 172.16.0.0
 network 192.168.10.0
 network 192.168.250.0
 default-information originate
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no nat inside source list LOCAL interface Ethernet0
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip access-list standard LOCAL
 permit 10.0.0.0 0.255.255.255
 permit 172.16.0.0 0.0.255.255
 permit 192.168.0.0 0.0.255.255
!
!
```

**NEW QUESTION 317**
Which option is the default switch port port-security violation mode?

A. shutdown
B. protect
C. shutdown vlan
D. restrict

**Answer:** A

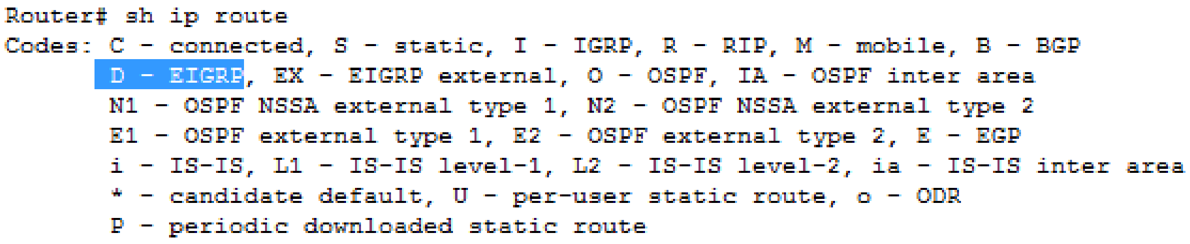
**Explanation:** Shutdown—This mode is the default violation mode; when in this mode, the switch will automatically force the switchport into an error disabled (err-disable) state when a violation occurs. While in this state, the switchport forwards no traffic. The switchport can be brought out of this error disabled state by issuing the errdisable recovery cause CLI command or by disabling and reenabling the switchport.
Shutdown VLAN—This mode mimics the behavior of the shutdown mode but limits the error disabled state the specific violating VLAN.

**NEW QUESTION 322**
Which route source code represents the routing protocol with a default administrative distance of 90 in the routing table?

A. S
B. E
C. D
D. R
E. O

**Answer:** C

**Explanation:** SStatic EEGP DEIGRP RRIP OOSPF
Default Administrative distance of EIGRP protocol is 90 then answer is C



```
Router# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Default Distance Value Table
This table lists the administrative distance default values of the protocols that Cisco supports:
Route Source
Default Distance Values
Connected interface 0
Static route 1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route 5
External Border Gateway Protocol (BGP) 20
Internal EIGRP 90
IGRP 100 OSPF 110
Intermediate System-to-Intermediate System (IS-IS) 115
Routing Information Protocol (RIP) 120
Exterior Gateway Protocol (EGP) 140
On Demand Routing (ODR) 160
External EIGRP 170
Internal BGP 200
Unknown* 255

**NEW QUESTION 327**
Which technology supports the stateless assignment of IPv6 addresses?

A. DNS
B. DHCPv6
C. DHCP
D. autoconfiguration

**Answer:** B

**Explanation:** DHCPv6 Technology Overview
IPv6 Internet Address Assignment Overview
IPv6 has been developed with Internet Address assignment dynamics in mind. Being aware that IPv6 Internet addresses are 128 bits in length and written in hexadecimals makes automation of address-assignment an important aspect within network design. These attributes make it inconvenient for a user to manually assign IPv6 addresses, as the format is not naturally intuitive to the human eye. To facilitate address assignment with little or no human intervention, several methods and technologies have been developed to automate the process of address and configuration parameter assignment to IPv6 hosts.
The various IPv6 address assignment methods are as follows:
1. Manual Assignment
An IPv6 address can be statically configured by a human operator. However, manual assignment is quite open to errors and operational overhead due to the 128 bit length and hexadecimal attributes of the addresses, although for router interfaces and static network elements and resources this can be an appropriate solution.
2. Stateless Address Autoconfiguration (RFC2462)
Stateless Address Autoconfiguration (SLAAC) is one of the most convenient methods to assign Internet addresses to IPv6 nodes. This method does not require any human intervention at all from an IPv6 user. If one wants to use IPv6 SLAAC on an IPv6 node, it is important that this IPv6 node is connected to a network with at least one IPv6 router connected. This router is configured by the network administrator and sends out Router Advertisement announcements onto the link. These announcements can allow the on-link connected IPv6 nodes to configure themselves with IPv6 address and routing parameters, as specified in RFC2462, without further human intervention.
3. Stateful DHCPv6
The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has been standardized by the IETF through RFC3315. DHCPv6 enables DHCP servers to pass configuration parameters, such as IPv6 network addresses, to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration" (RFC 2462), and can be used separately, or in addition to the stateless autoconfiguration to obtain configuration parameters.
4. DHCPv6-PD
DHCPv6 Prefix Delegation (DHCPv6-PD) is an extension to DHCPv6, and is specified in RFC3633. Classical DHCPv6 is typically focused upon parameter assignment from a DHCPv6 server to an IPv6 host running a DHCPv6 protocol stack. A practical example would be the stateful address assignment of "2001:db8::1" from a DHCPv6 server to a DHCPv6 client. DHCPv6-PD however is aimed at assigning complete subnets and other network and interface parameters from a DHCPv6-PD server to a DHCPv6-PD client. This means that instead of a single address assignment, DHCPv6-PD will assign a set of IPv6 "subnets". An example could be the assignment of "2001:db8::/60" from a DHCPv6-PD server to a DHCPv6-PD client. This will allow the DHCPv6-PD client (often a CPE device) to segment the received address IPv6 address space, and assign it dynamically to its IPv6 enabled interfaces.

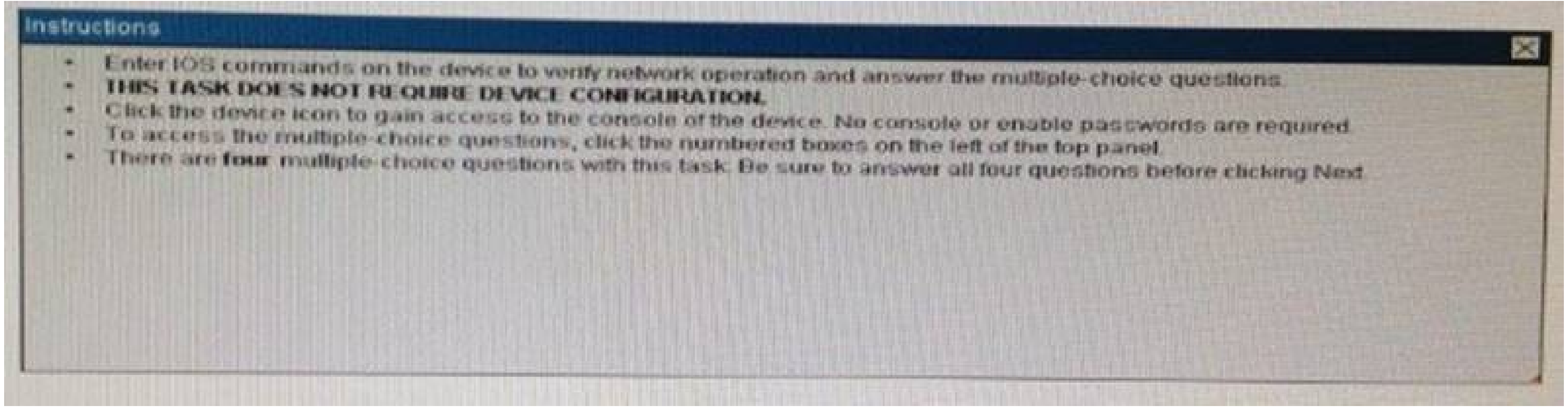
5. Stateless DHCPv6
Stateless DHCPv6 is a combination of "stateless Address Autoconfiguration" and "Dynamic Host Configuration Protocol for IPv6" and is specified by RFC3736. When using stateless-DHCPv6, a device will use Stateless Address Auto-Configuration (SLAAC) to assign one or more IPv6 addresses to an interface, while it utilizes DHCPv6 to receive "additional parameters" which may not be available through SLAAC. For example, additional parameters could include information such as DNS or NTP server addresses, and are provided in a stateless manner by DHCPv6. Using stateless DHCPv6 means that the DHCPv6 server does not need to keep track of any state of assigned IPv6 addresses, and there is no need for state refreshment as result. On network media supporting a large number of hosts associated to a single DHCPv6 server, this could mean a significant reduction in DHCPv6 messages due to the reduced need for address state refreshments.
From Cisco IOS 12.4(15)T onwards the client can also receive timing information, in addition to the "additional parameters" through DHCPv6. This timing information provides an indication to a host when it should refresh its DHCPv6 configuration data. This behavior (RFC4242) is particularly useful in unstable environments where changes are likely to occur.

**NEW QUESTION 329**
Which statement about routing protocols is true?

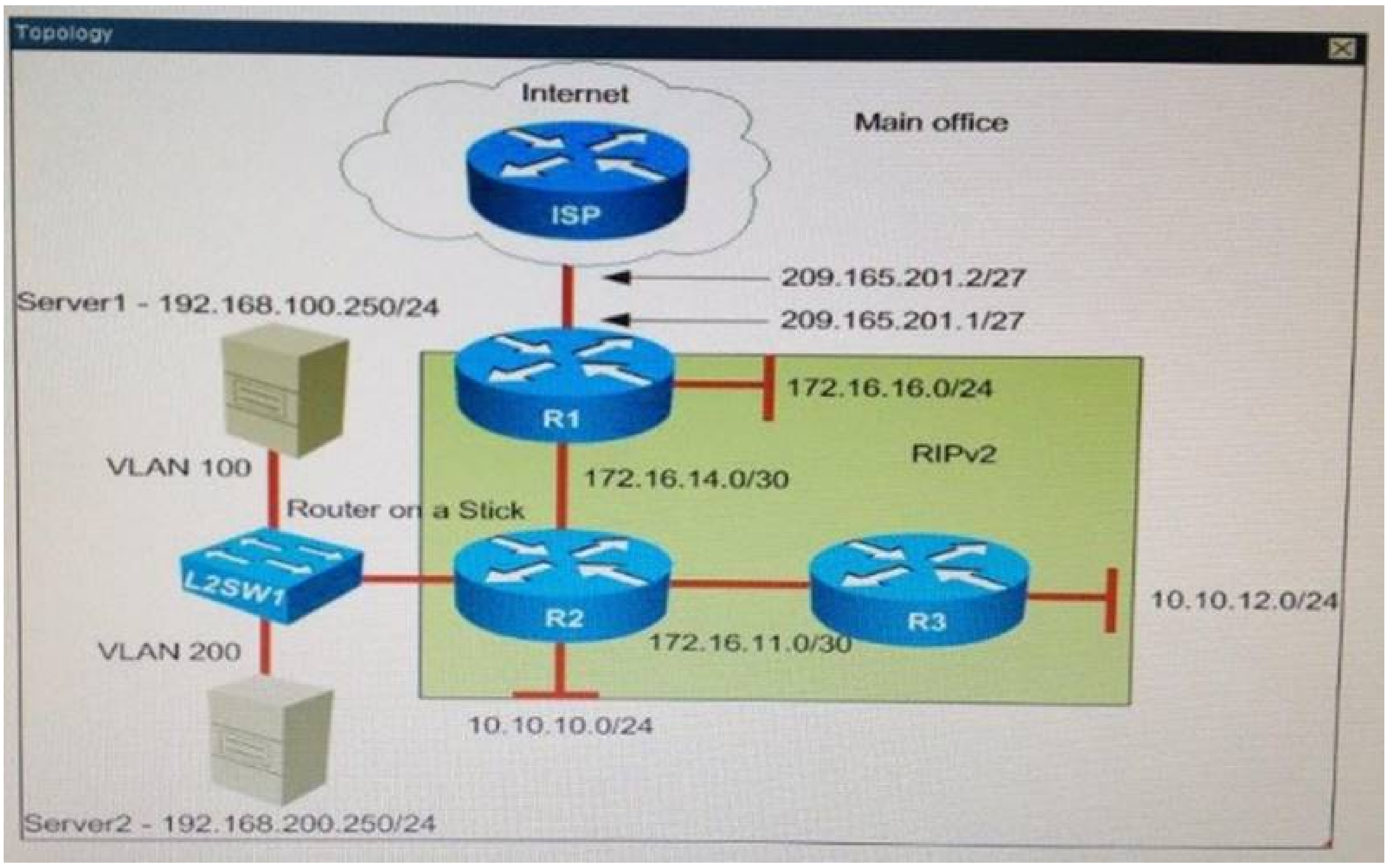
A. Link-state routing protocols choose a path by the number of hops to the destination.
B. OSPF is a link-state routing protocol.
C. Distance-vector routing protocols use the Shortest Path First algorithm.
D. IS-IS is a distance-vector routing protocol.

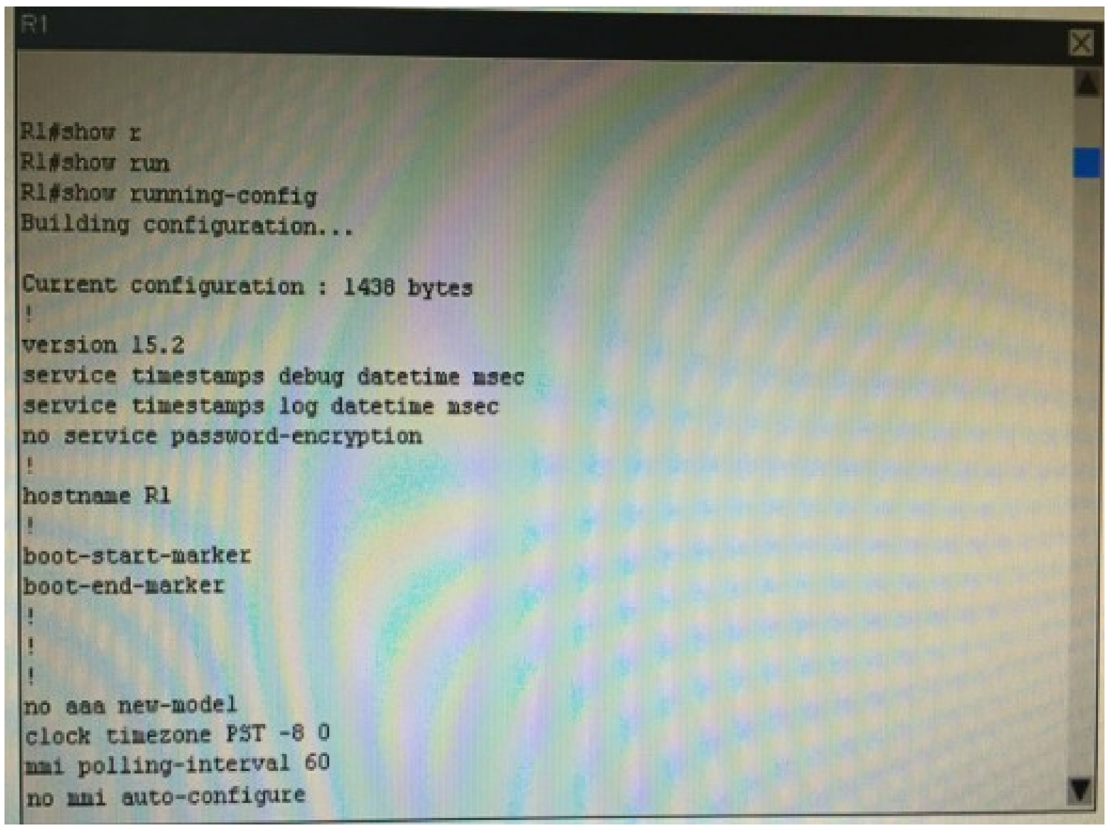
**Answer:** B

**NEW QUESTION 330**
Scenario:
You work for a company that provides managed network services, and of your real estate clients running a small office is experiencing network issues, Troubleshoot the network issues.
Router R1 connects the main office to internet, and routers R2 and R3 are internal routers NAT is enabled on Router R1.
The routing protocol that is enable between routers R1, R2, and R3 is RIPv2.
R1 sends default route into RIPv2 for internal routers to forward internet traffic to R1.
Server1 and Server2 are placed in VLAN 100 and 200 respectively, and dare still running router on stick configuration with router R2.
You have console access on R1, R2, R3, and L2SW1 devices. Use only show commands to troubleshoot the issues.


Instructions

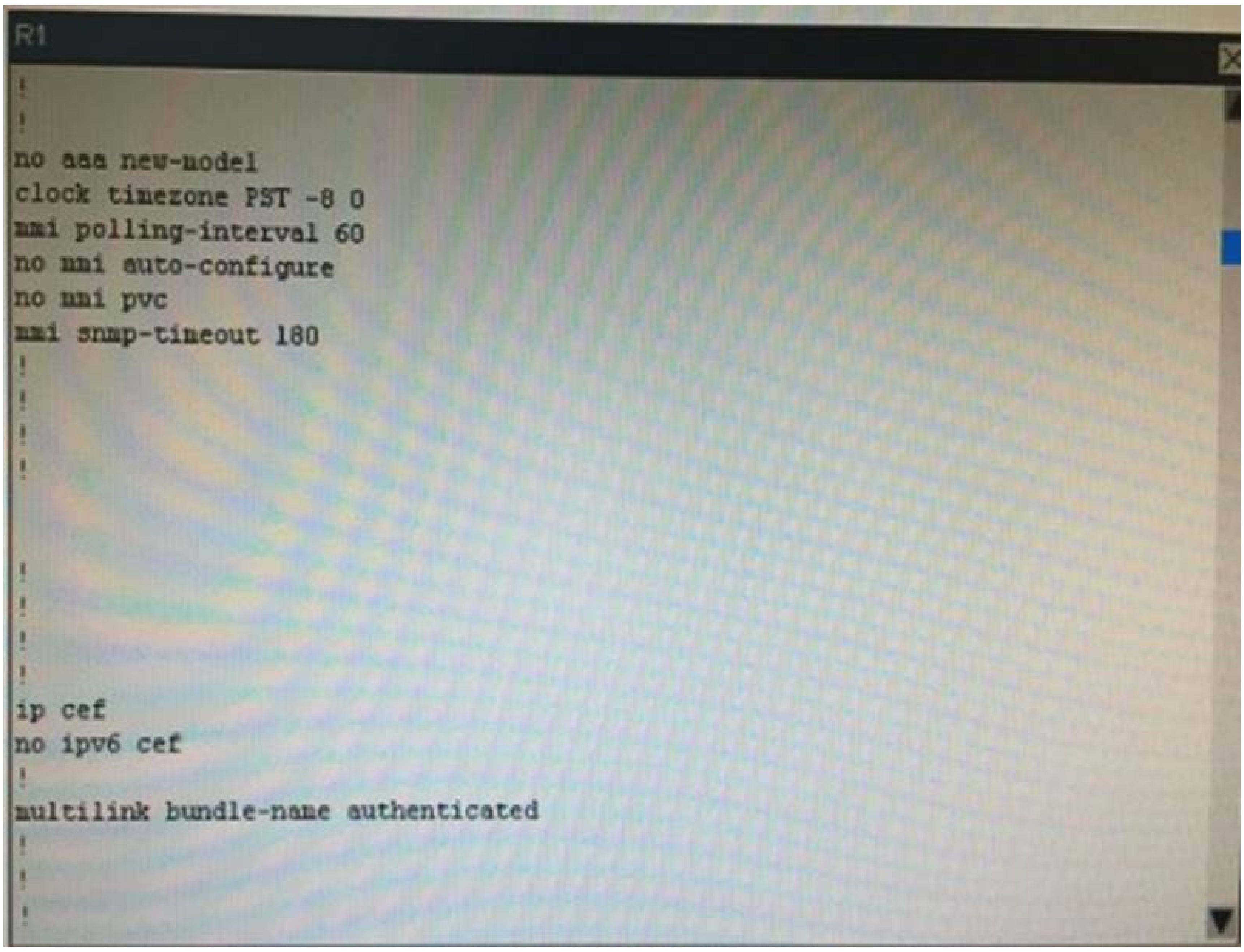
- Enter IOS commands on the device to verify network operation and answer the multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click the device icon to gain access to the console of the device. No console or enable passwords are required.
- To access the multiple-choice questions, click the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before clicking Next.





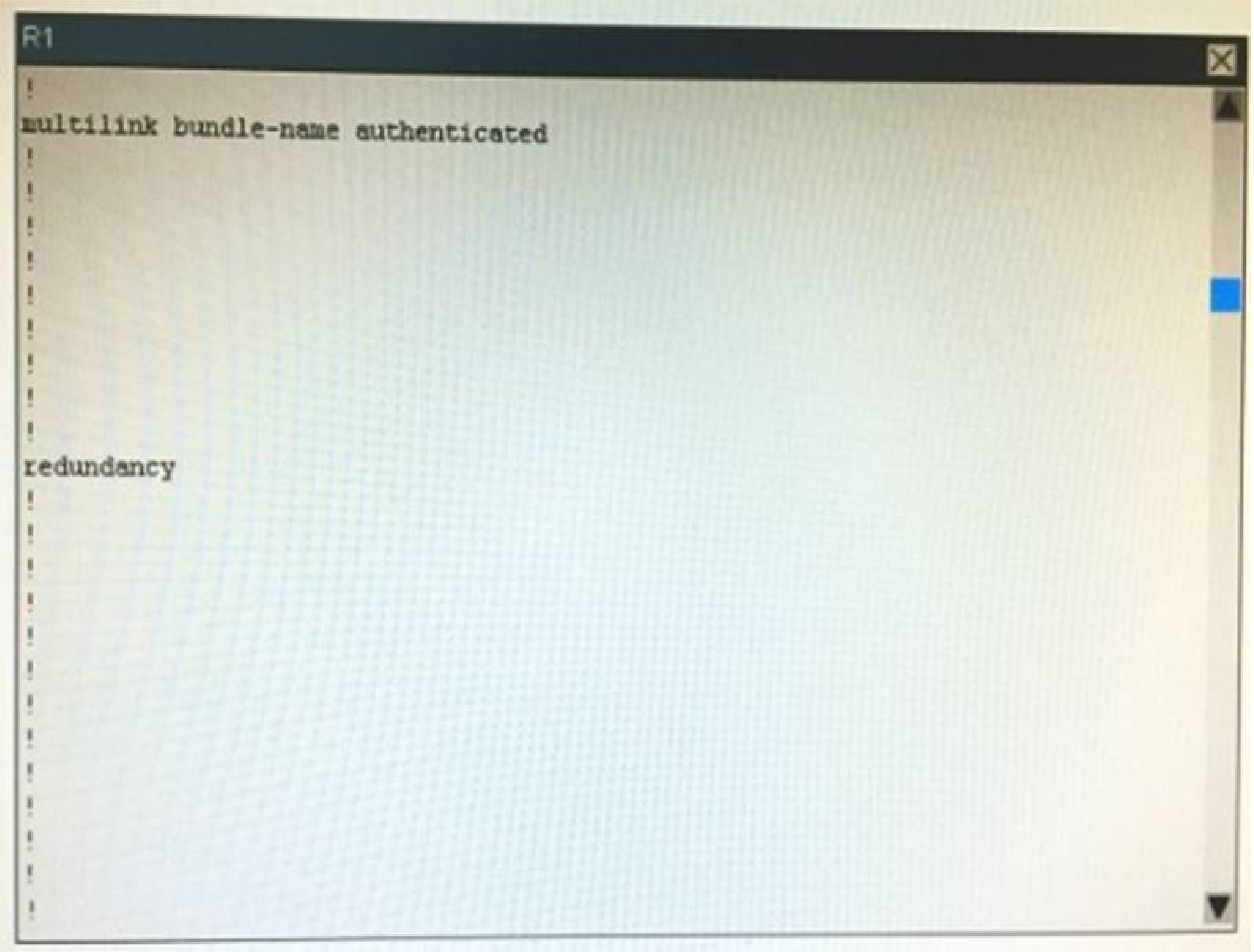
R1

```
R1#show r
R1#show run
R1#show running-config
Building configuration...

Current configuration : 1438 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
```

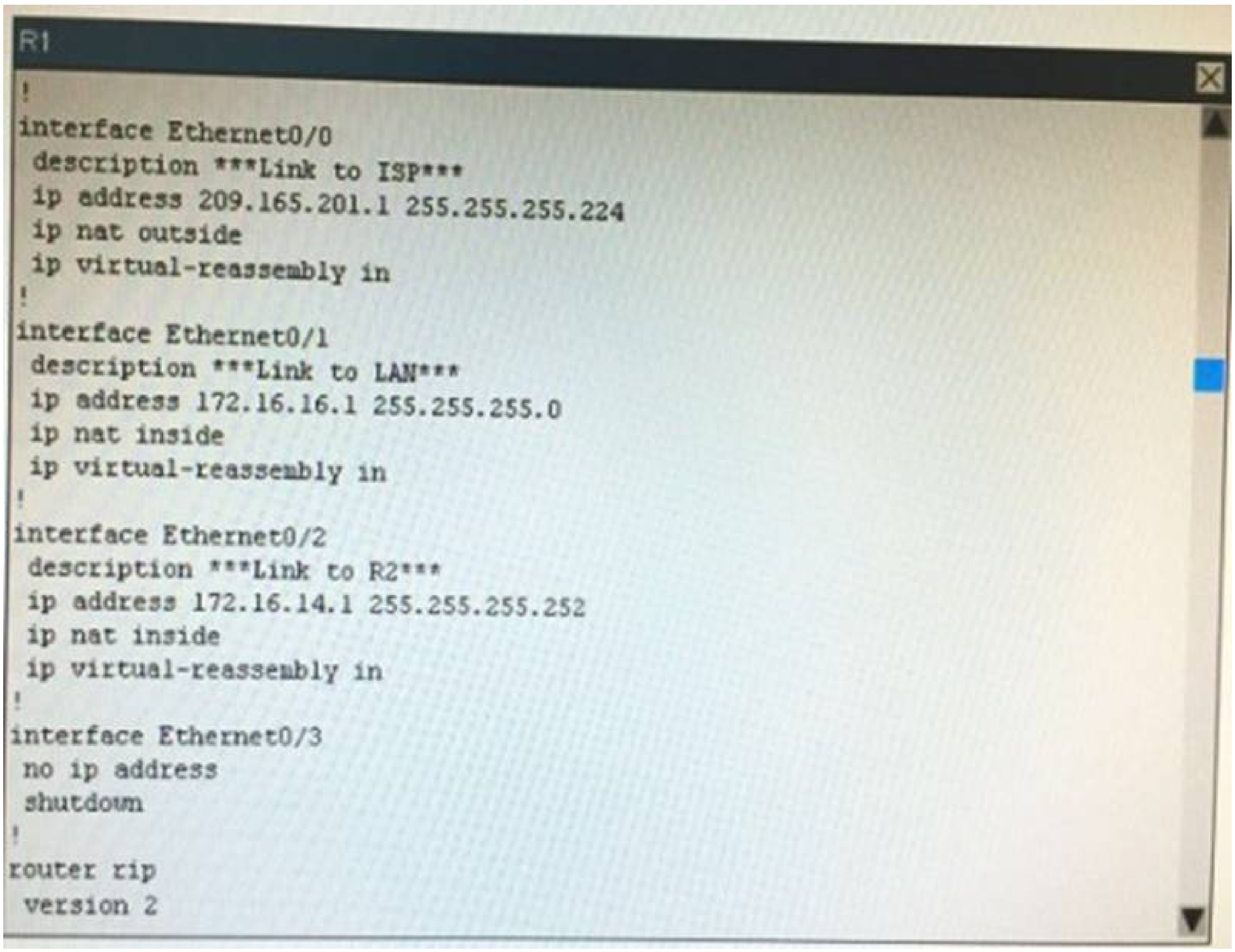


R1

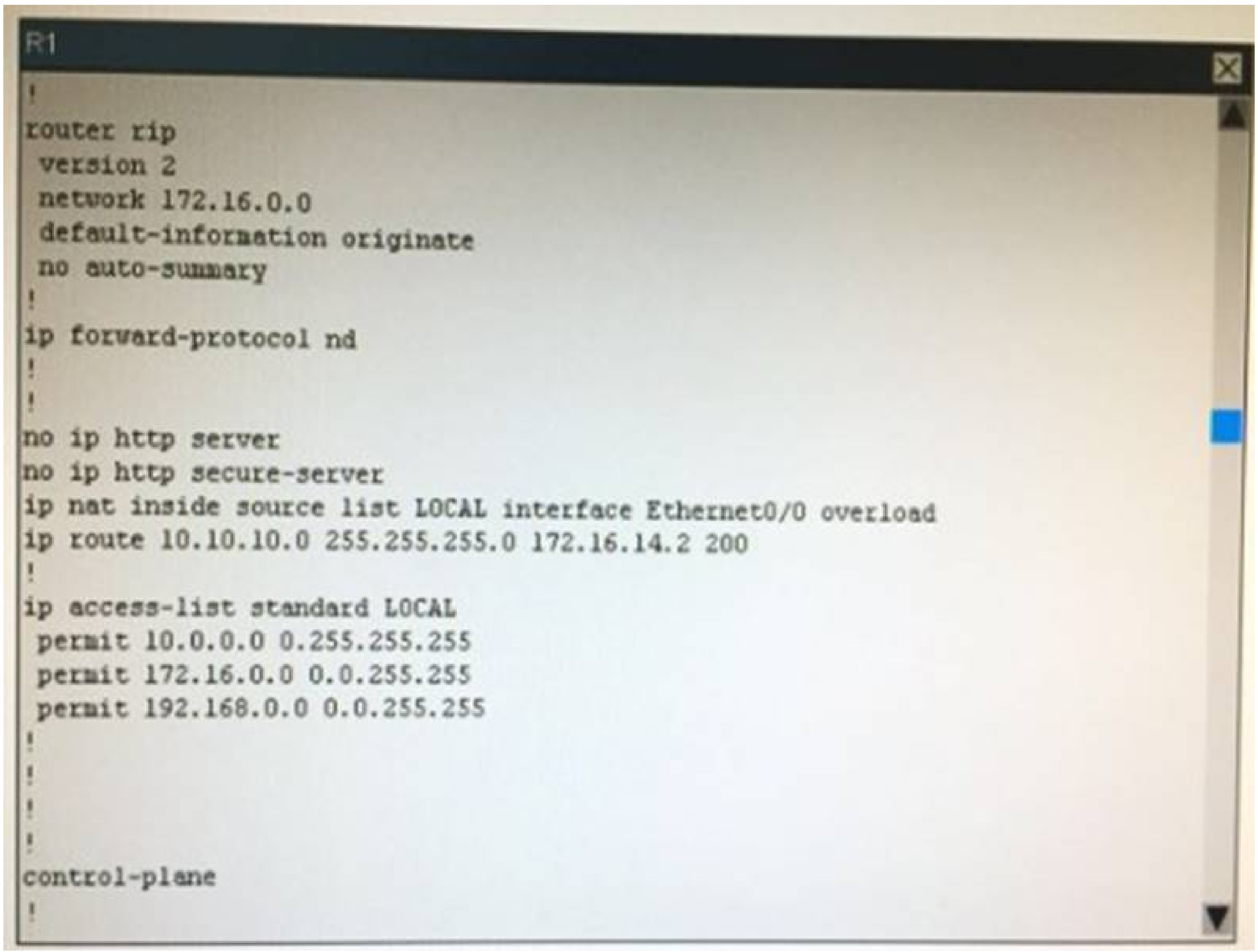
```
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!



!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
```



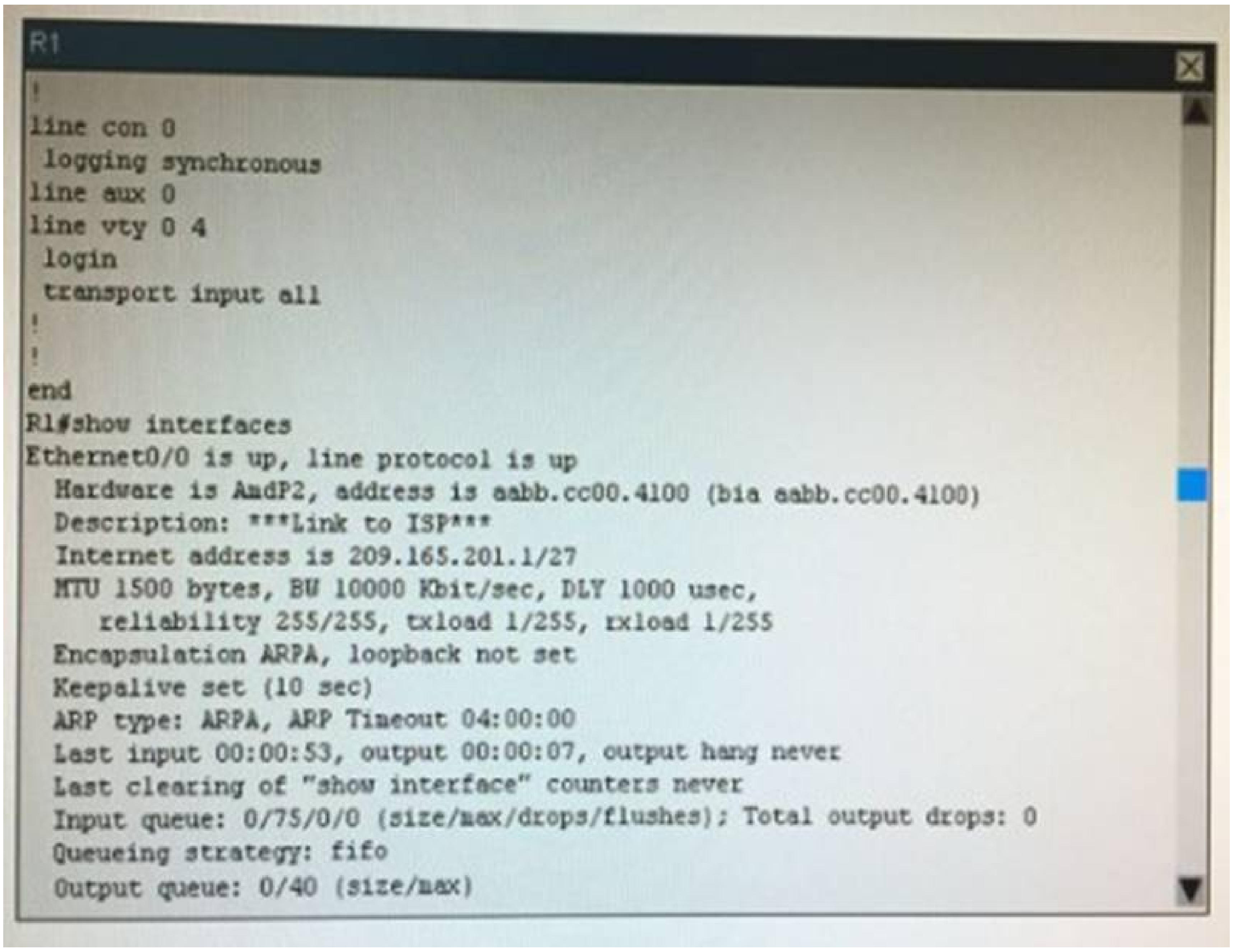
```
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
```



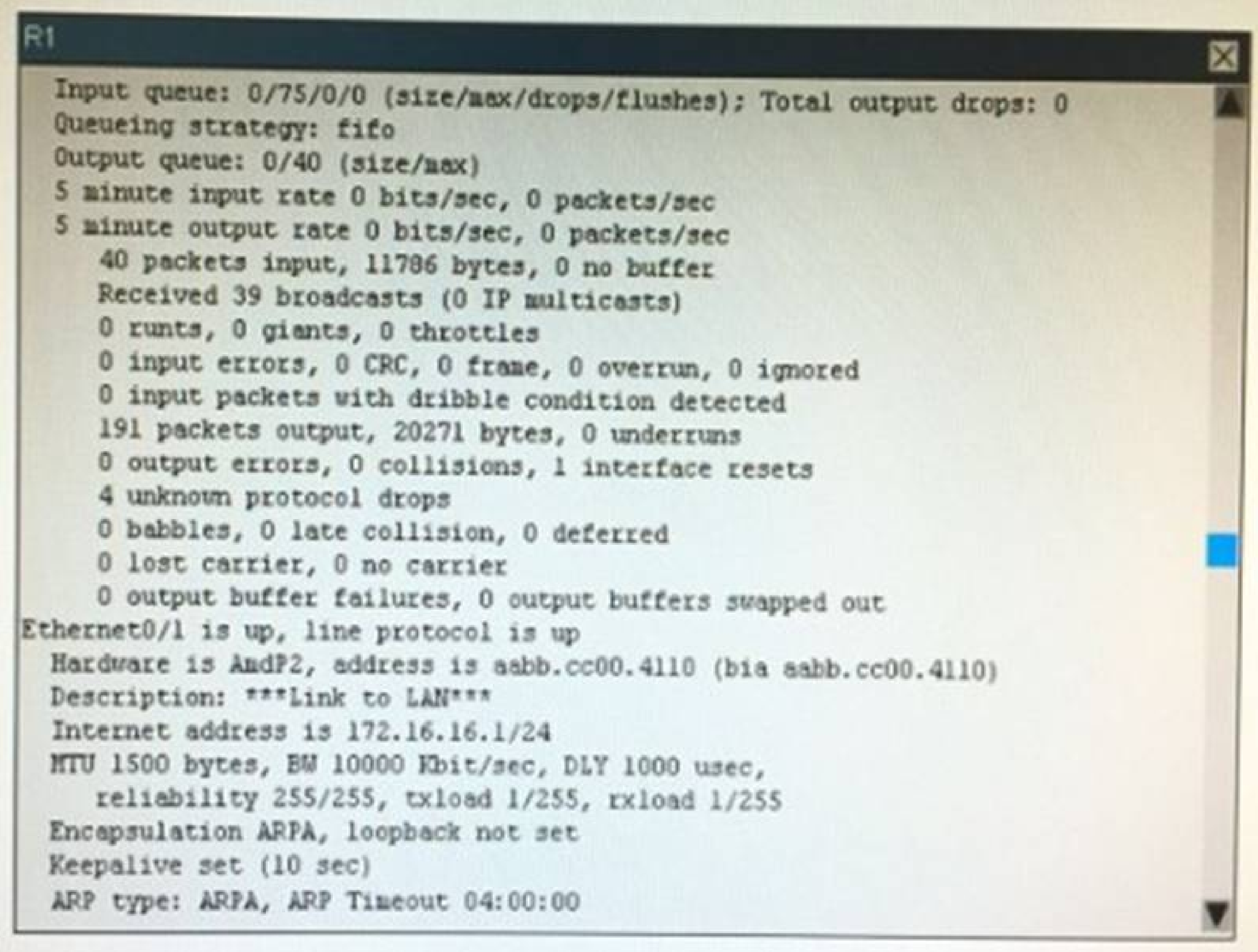
```
!
interface Ethernet0/0
 description ***Link to ISP***
 ip address 209.165.201.1 255.255.255.224
 ip nat outside
 ip virtual-reassembly in
!
interface Ethernet0/1
 description ***Link to LAN***
 ip address 172.16.16.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/2
 description ***Link to R2***
 ip address 172.16.14.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
```



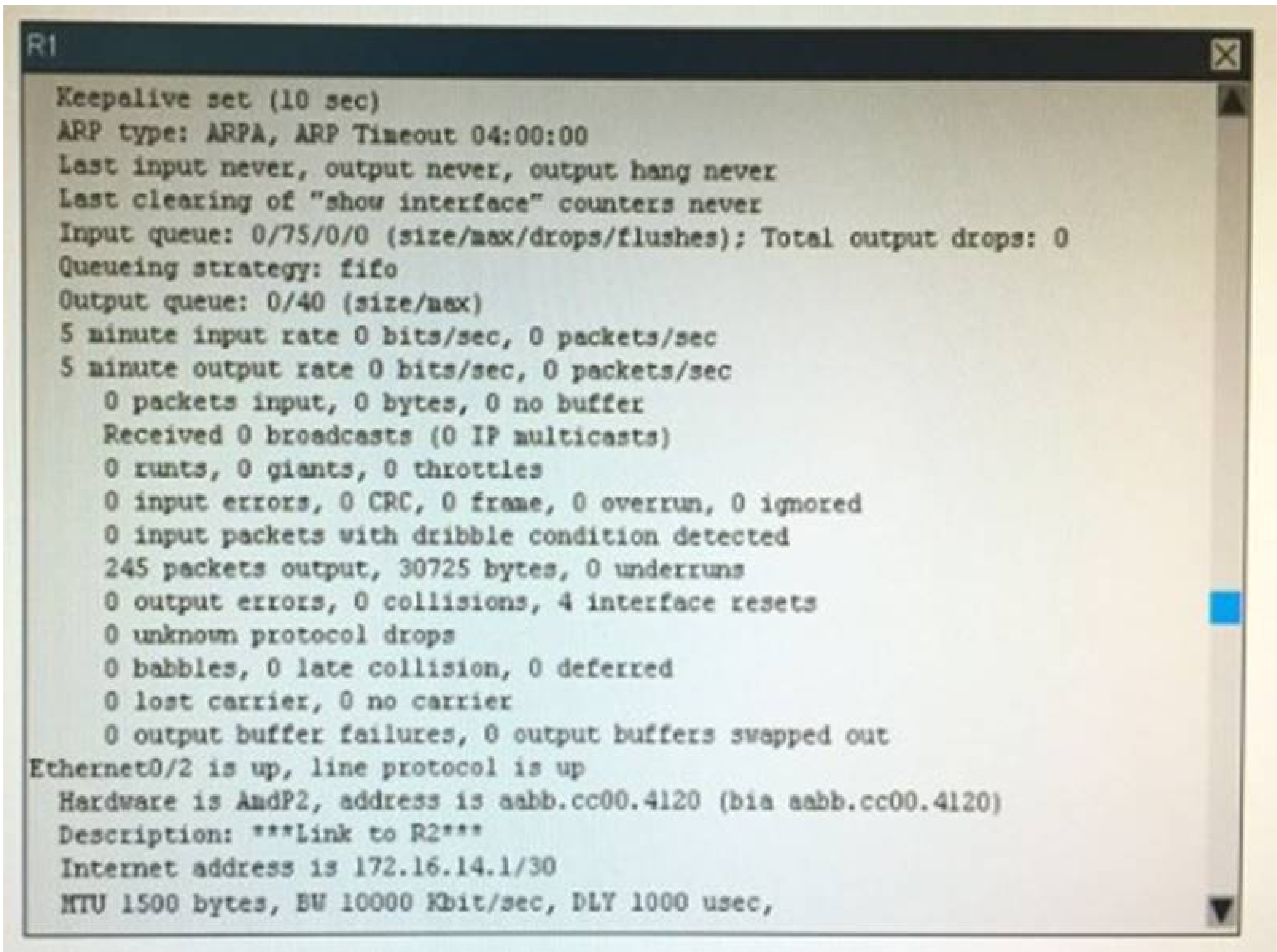
```
!
router rip
 version 2
 network 172.16.0.0
 default-information originate
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip nat inside source list LOCAL interface Ethernet0/0 overload
ip route 10.10.10.0 255.255.255.0 172.16.14.2 200
!
ip access-list standard LOCAL
 permit 10.0.0.0 0.255.255.255
 permit 172.16.0.0 0.0.255.255
 permit 192.168.0.0 0.0.255.255
!
!
!
!
control-plane
!
```



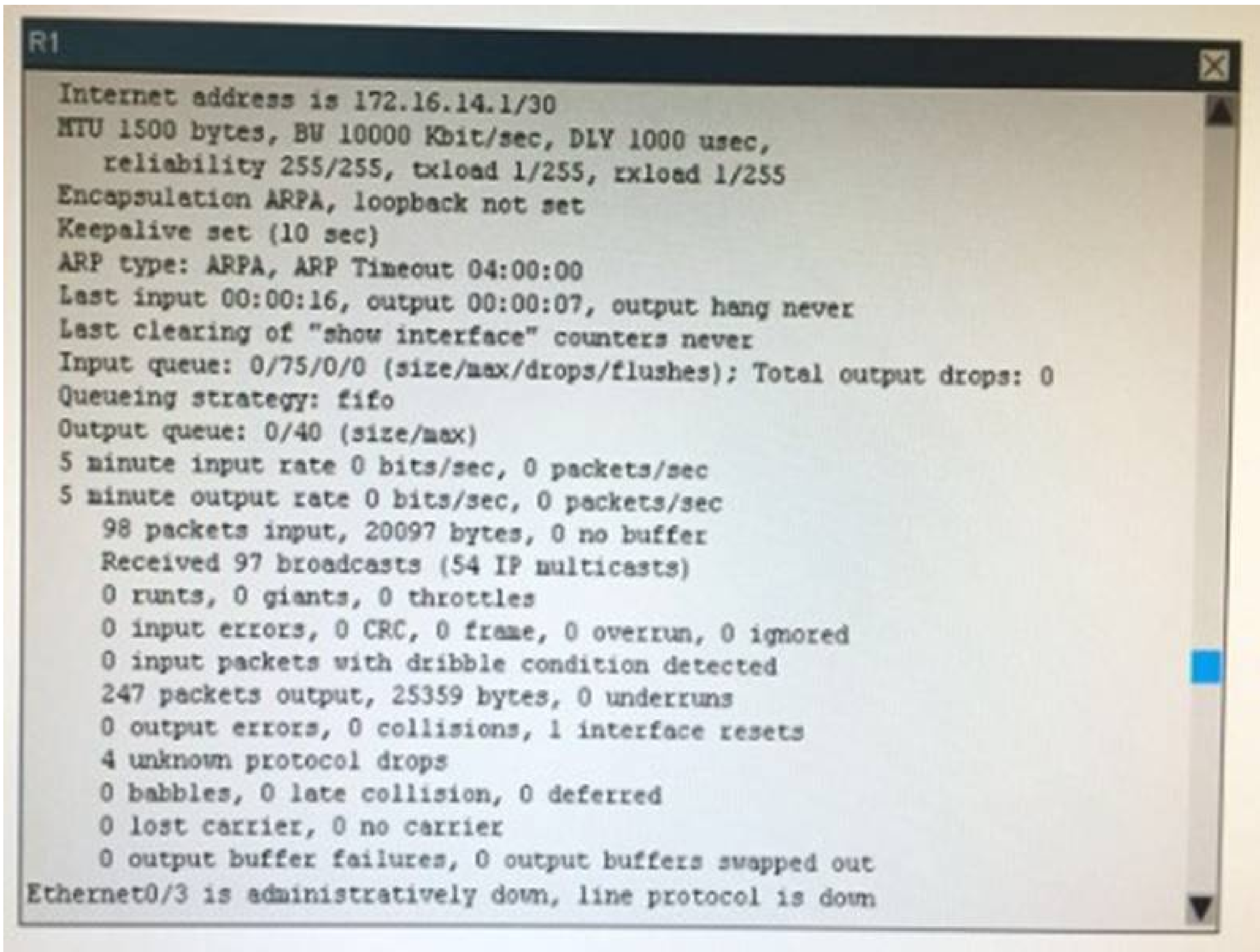
```
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
!
end
R1#show interfaces
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4100 (bia aabb.cc00.4100)
  Description: ***Link to ISP***
  Internet address is 209.165.201.1/27
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:53, output 00:00:07, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
```



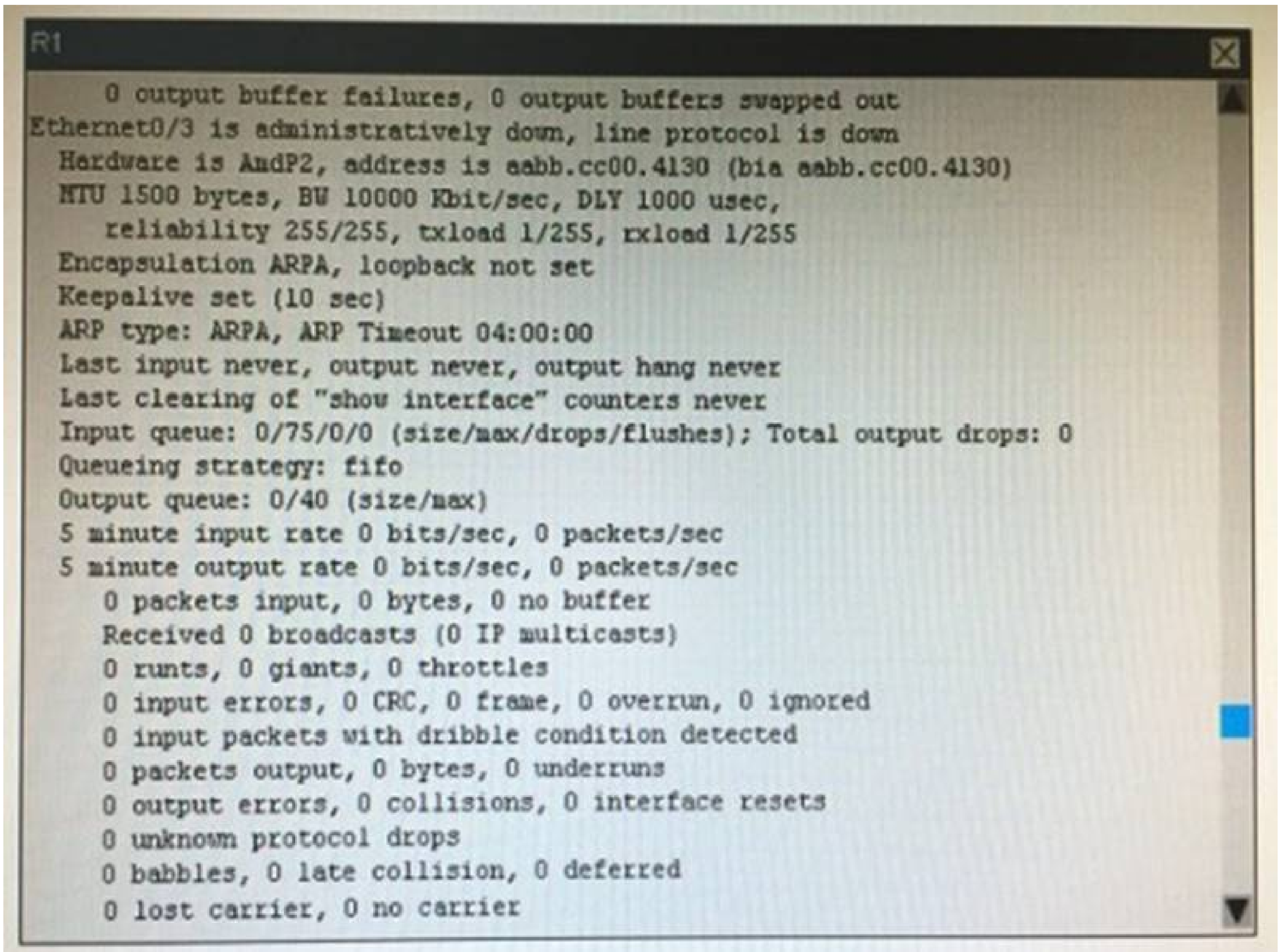
```
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     40 packets input, 11786 bytes, 0 no buffer
     Received 39 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     191 packets output, 20271 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     4 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/1 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4110 (bia aabb.cc00.4110)
  Description: ***Link to LAN***
  Internet address is 172.16.16.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
```



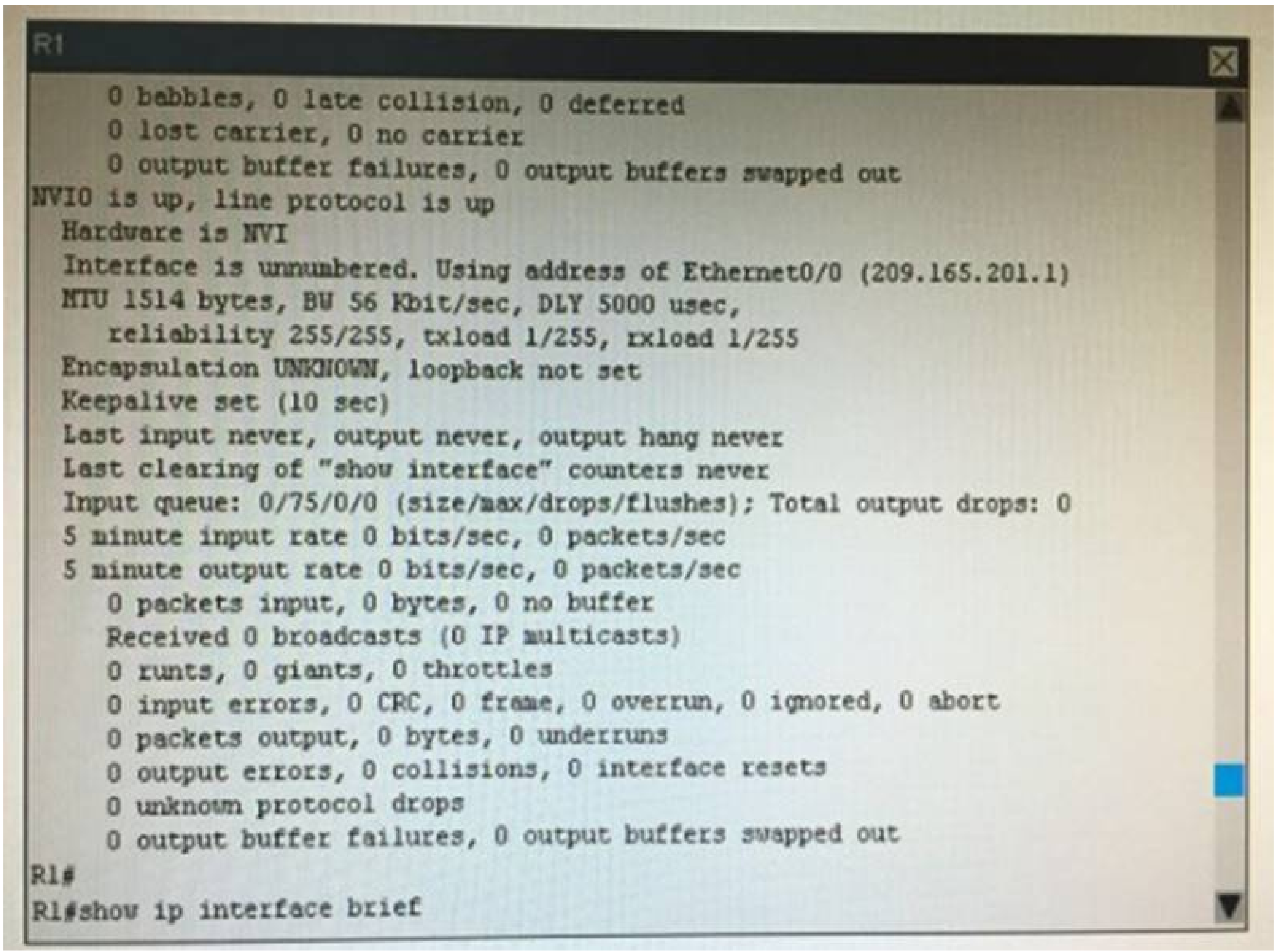
```
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     245 packets output, 30725 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/2 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4120 (bia aabb.cc00.4120)
  Description: ***Link to R2***
  Internet address is 172.16.14.1/30
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
```



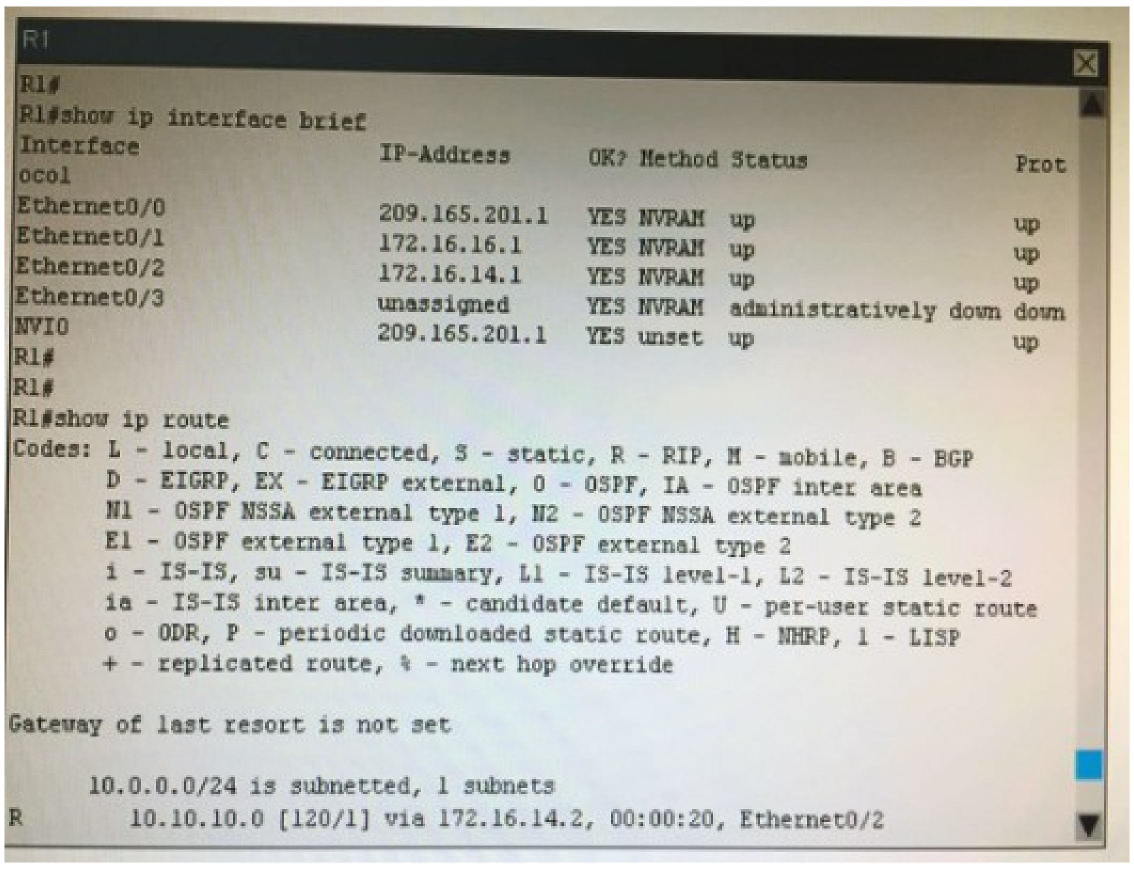
```
  Internet address is 172.16.14.1/30
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:16, output 00:00:07, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     98 packets input, 20097 bytes, 0 no buffer
     Received 97 broadcasts (54 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     247 packets output, 25359 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     4 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/3 is administratively down, line protocol is down
```



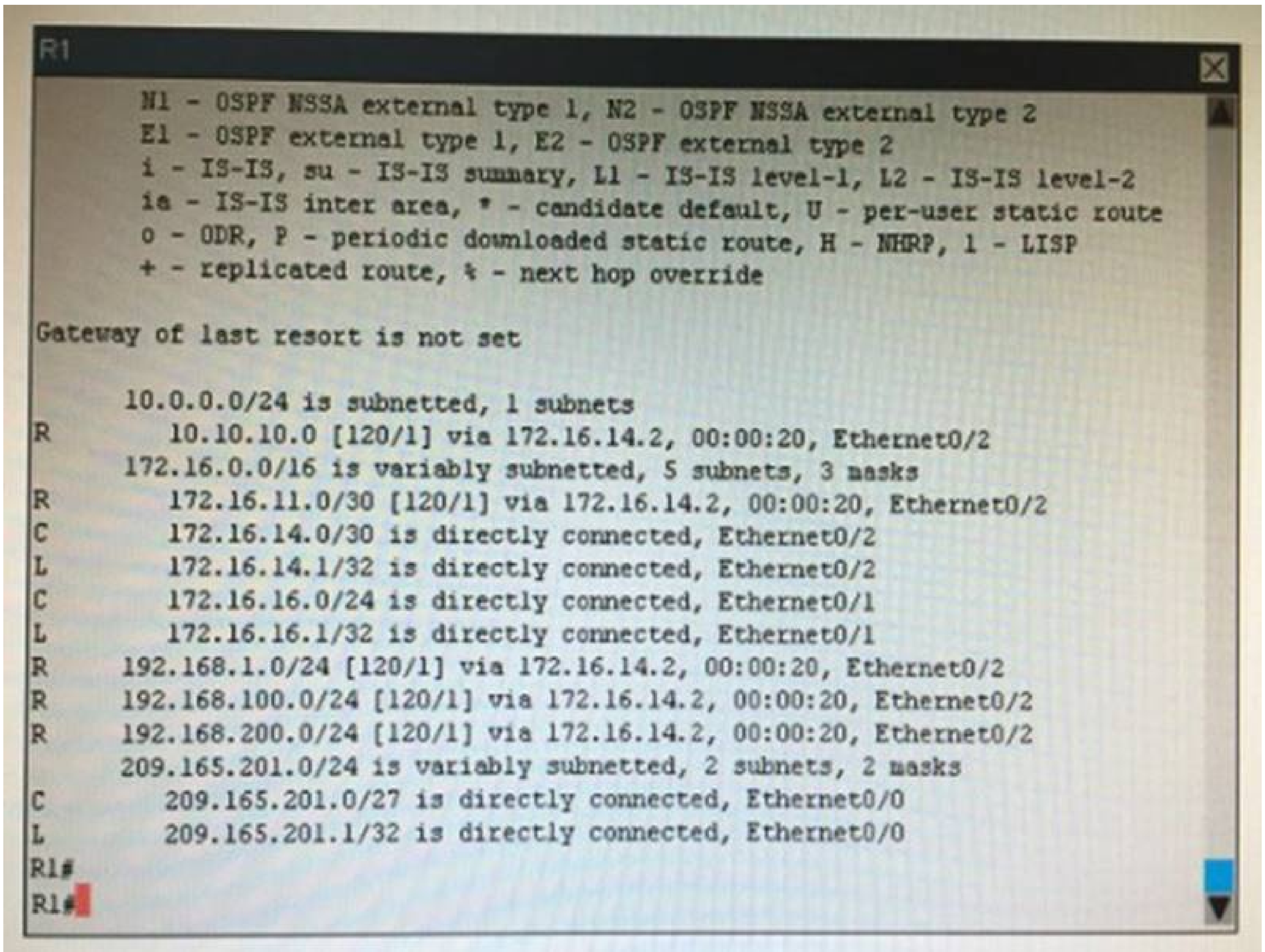
```
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/3 is administratively down, line protocol is down
  Hardware is AmdP2, address is aabb.cc00.4130 (bia aabb.cc00.4130)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
```



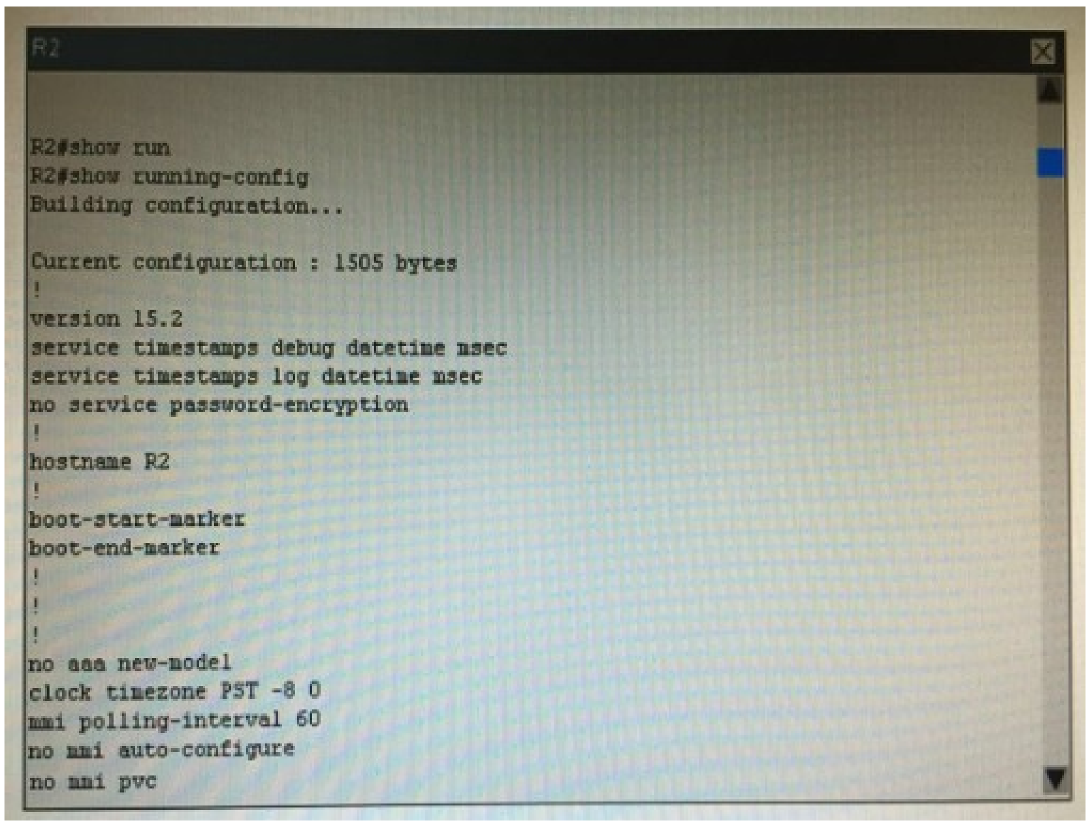
```
R1
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
NVI0 is up, line protocol is up
  Hardware is NVI
  Interface is unnumbered. Using address of Ethernet0/0 (209.165.201.1)
  MTU 1514 bytes, BW 56 Kbit/sec, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation UNKNOWN, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
R1#
R1#show ip interface brief
```



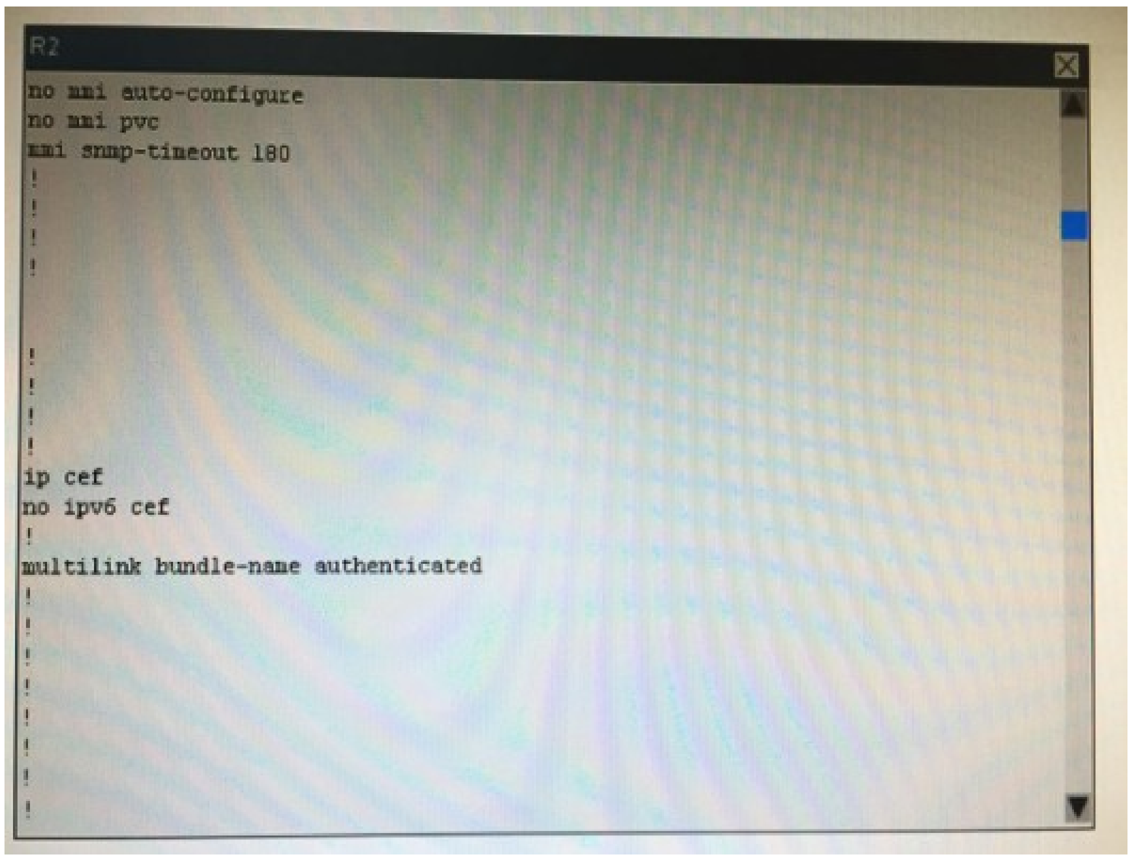
```
R1
R1#
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
Ethernet0/0                209.165.201.1   YES NVRAM  up                    up
Ethernet0/1                172.16.16.1     YES NVRAM  up                    up
Ethernet0/2                172.16.14.1     YES NVRAM  up                    up
Ethernet0/3                unassigned      YES NVRAM  administratively down down
NVI0                       209.165.201.1   YES unset  up                    up
R1#
R1#
R1#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 1 subnets
R        10.10.10.0 [120/1] via 172.16.14.2, 00:00:20, Ethernet0/2
```



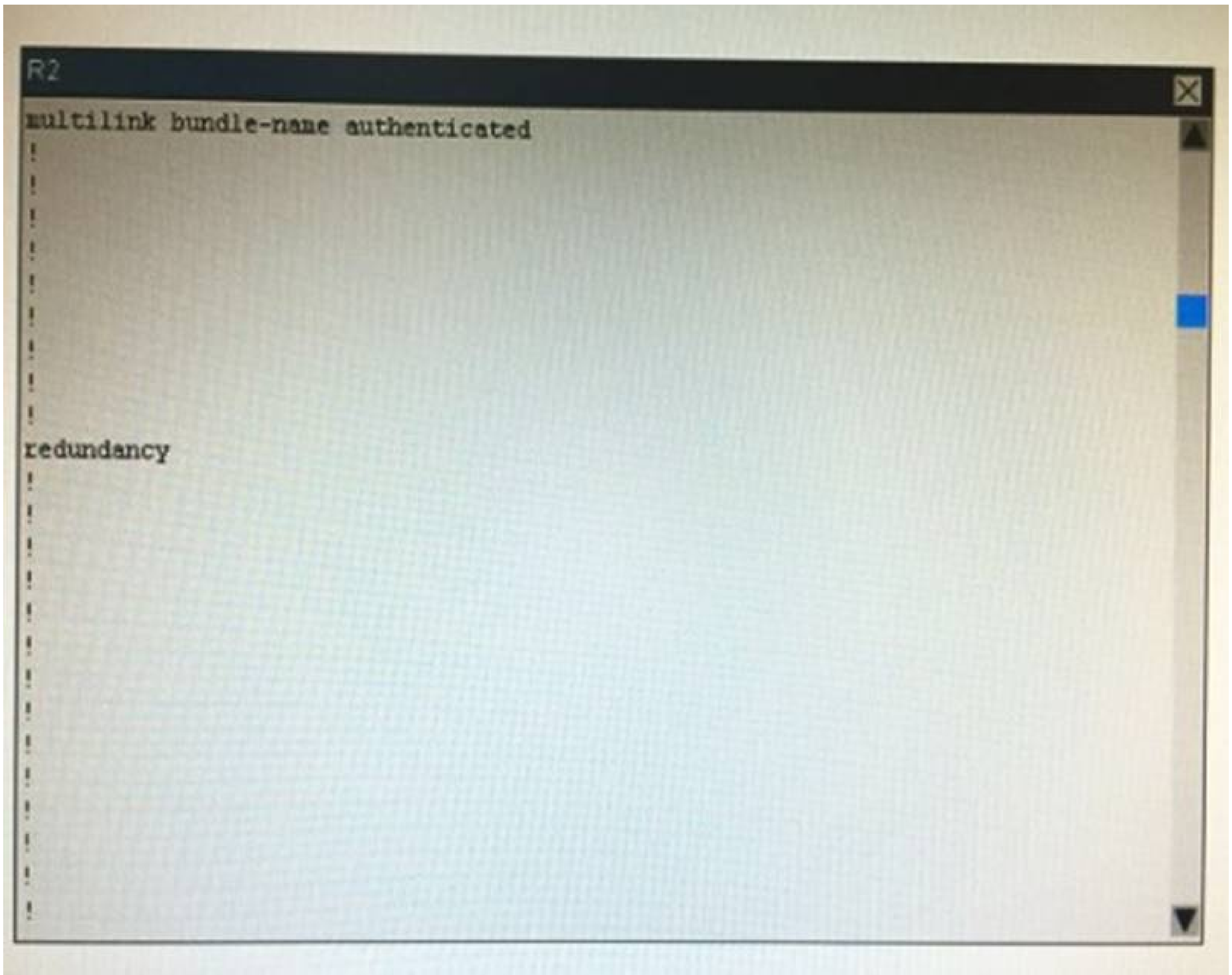
```
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 1 subnets
R        10.10.10.0 [120/1] via 172.16.14.2, 00:00:20, Ethernet0/2
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
R        172.16.11.0/30 [120/1] via 172.16.14.2, 00:00:20, Ethernet0/2
C        172.16.14.0/30 is directly connected, Ethernet0/2
L        172.16.14.1/32 is directly connected, Ethernet0/2
C        172.16.16.0/24 is directly connected, Ethernet0/1
L        172.16.16.1/32 is directly connected, Ethernet0/1
R     192.168.1.0/24 [120/1] via 172.16.14.2, 00:00:20, Ethernet0/2
R     192.168.100.0/24 [120/1] via 172.16.14.2, 00:00:20, Ethernet0/2
R     192.168.200.0/24 [120/1] via 172.16.14.2, 00:00:20, Ethernet0/2
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.201.0/27 is directly connected, Ethernet0/0
L        209.165.201.1/32 is directly connected, Ethernet0/0
R1#
R1#
```



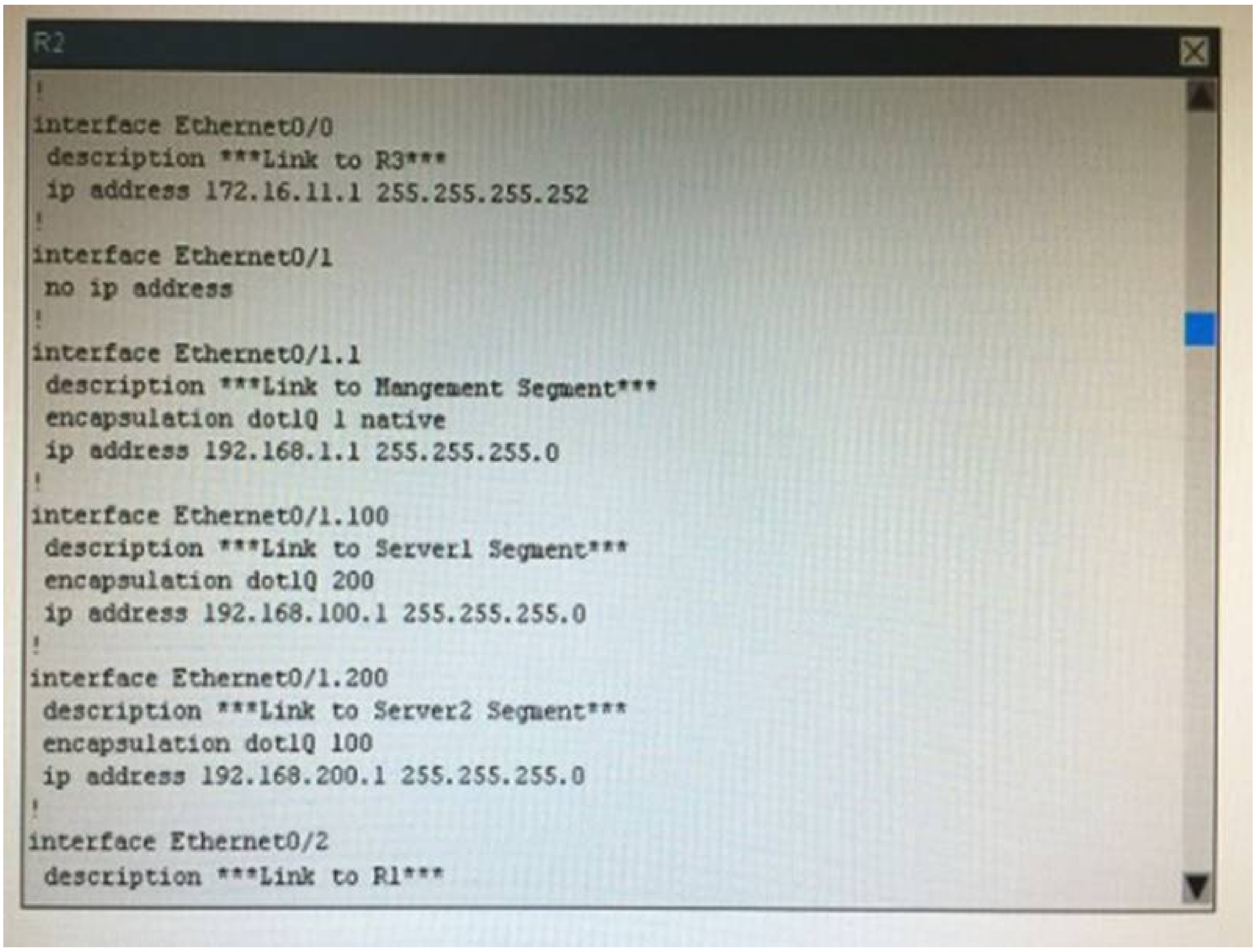
```
R2#show run
R2#show running-config
Building configuration...

Current configuration : 1505 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
```



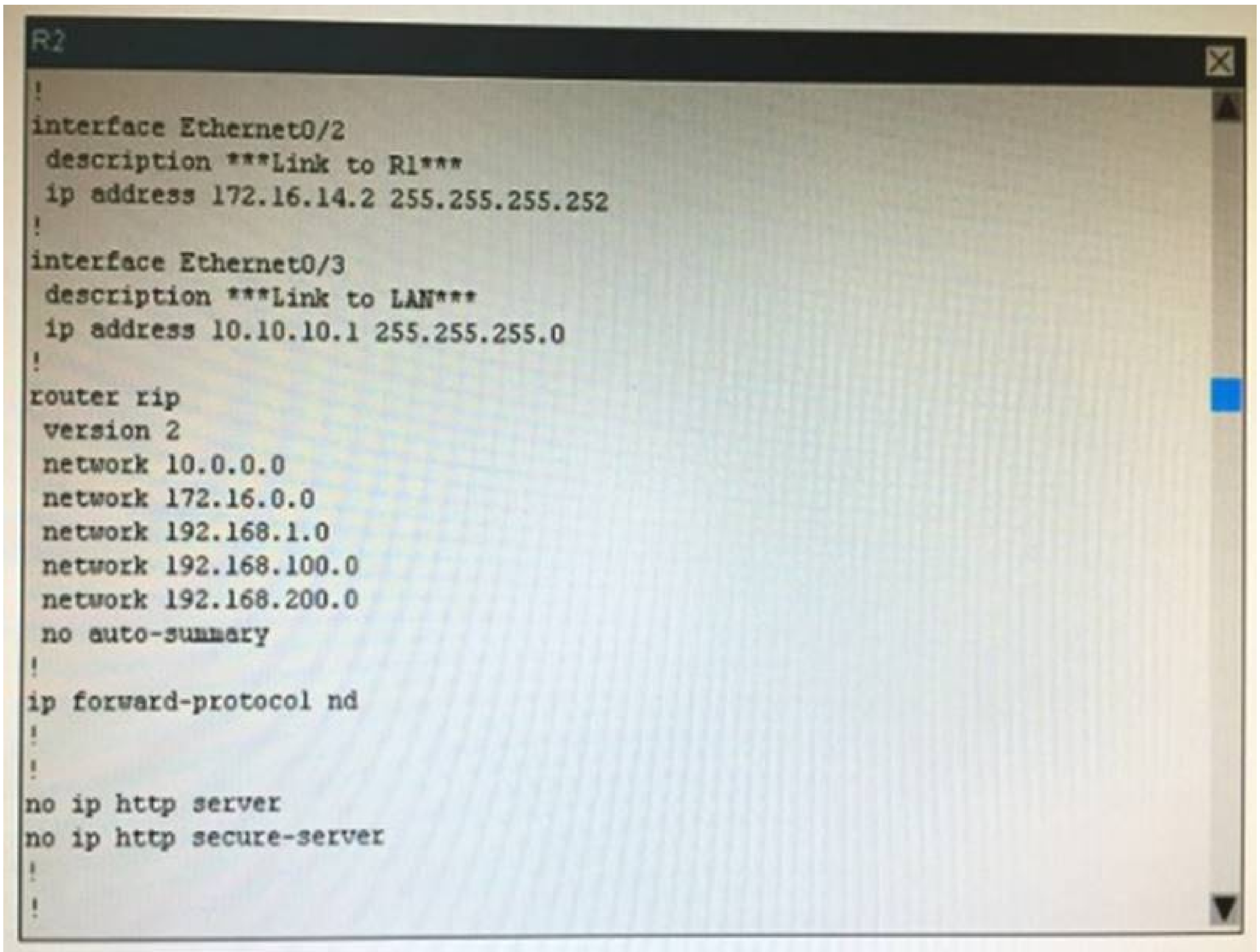
```
R2
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!


!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
```



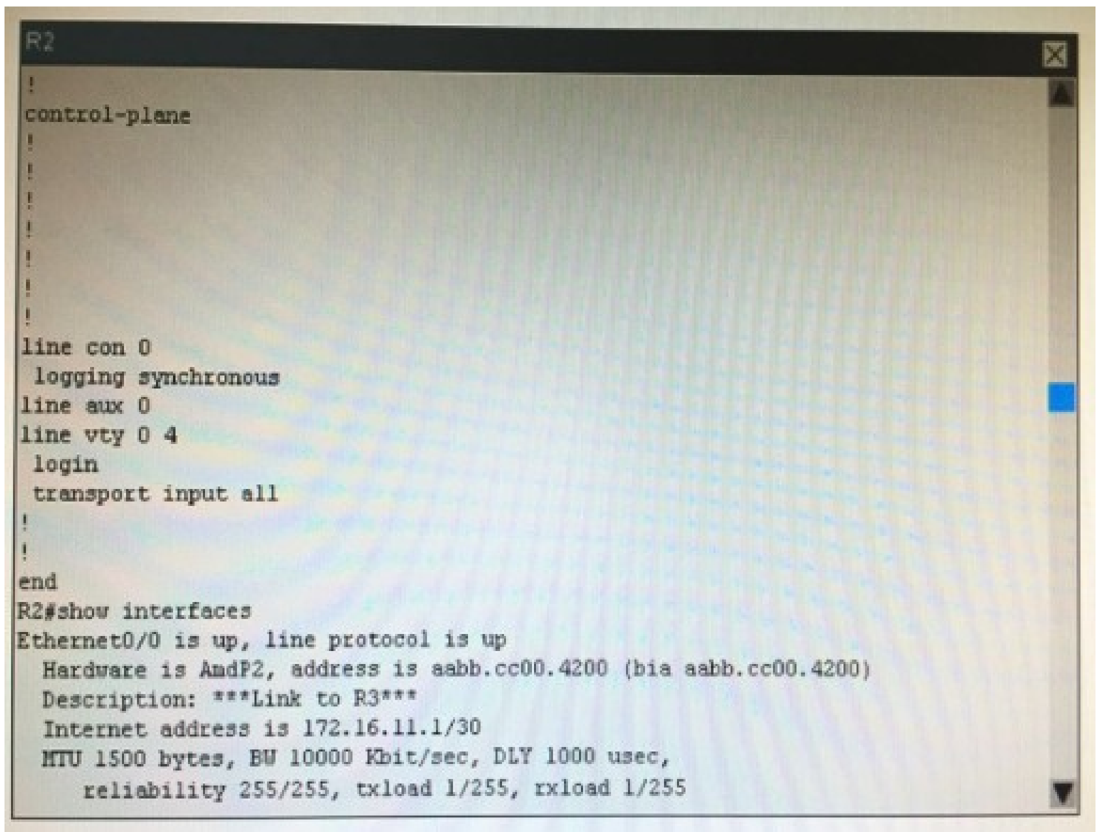
```
R2
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
```



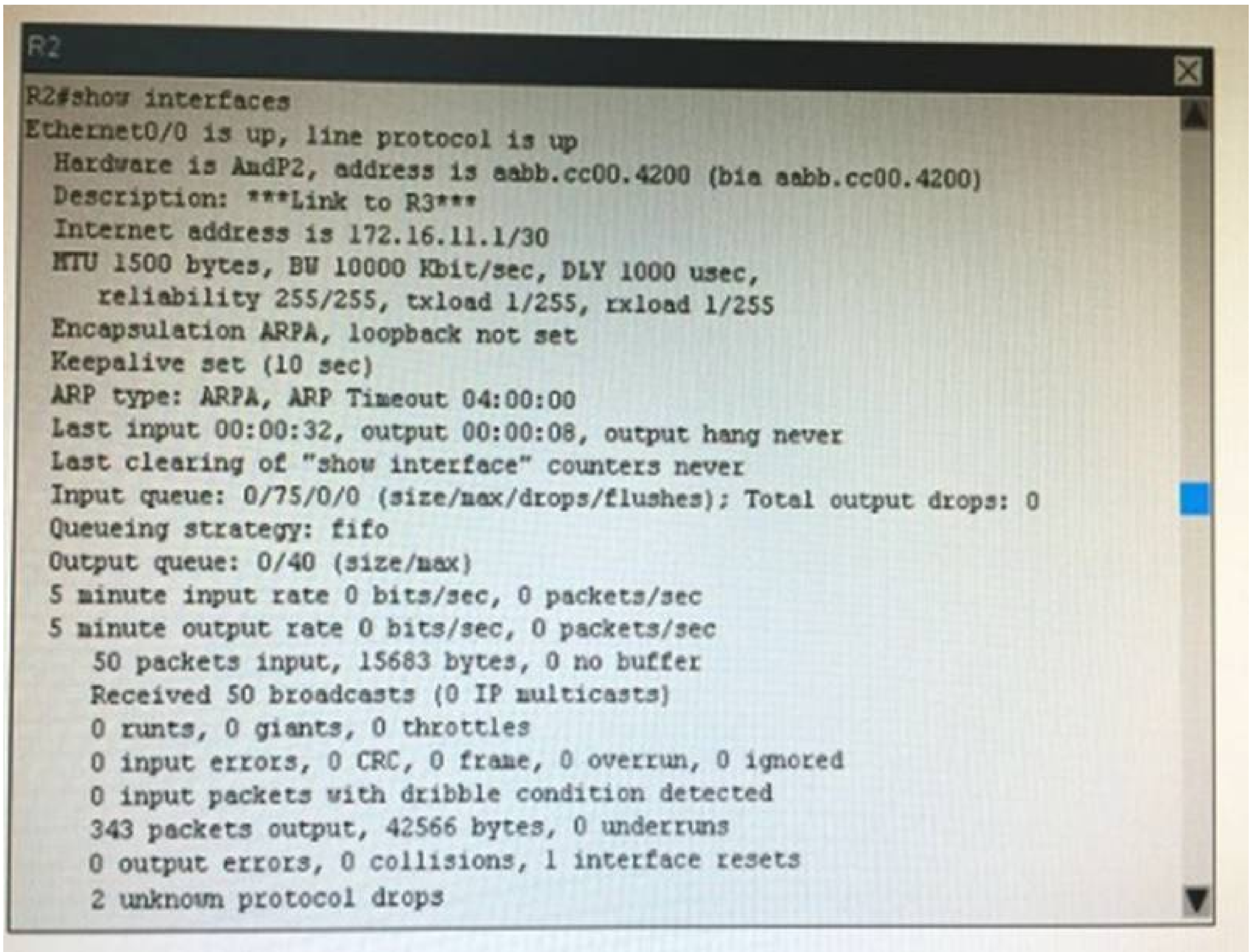
```
!
interface Ethernet0/0
 description ***Link to R3***
 ip address 172.16.11.1 255.255.255.252
!
interface Ethernet0/1
 no ip address
!
interface Ethernet0/1.1
 description ***Link to Mangement Segment***
 encapsulation dot1Q 1 native
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1.100
 description ***Link to Server1 Segment***
 encapsulation dot1Q 200
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/1.200
 description ***Link to Server2 Segment***
 encapsulation dot1Q 100
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet0/2
 description ***Link to R1***
```



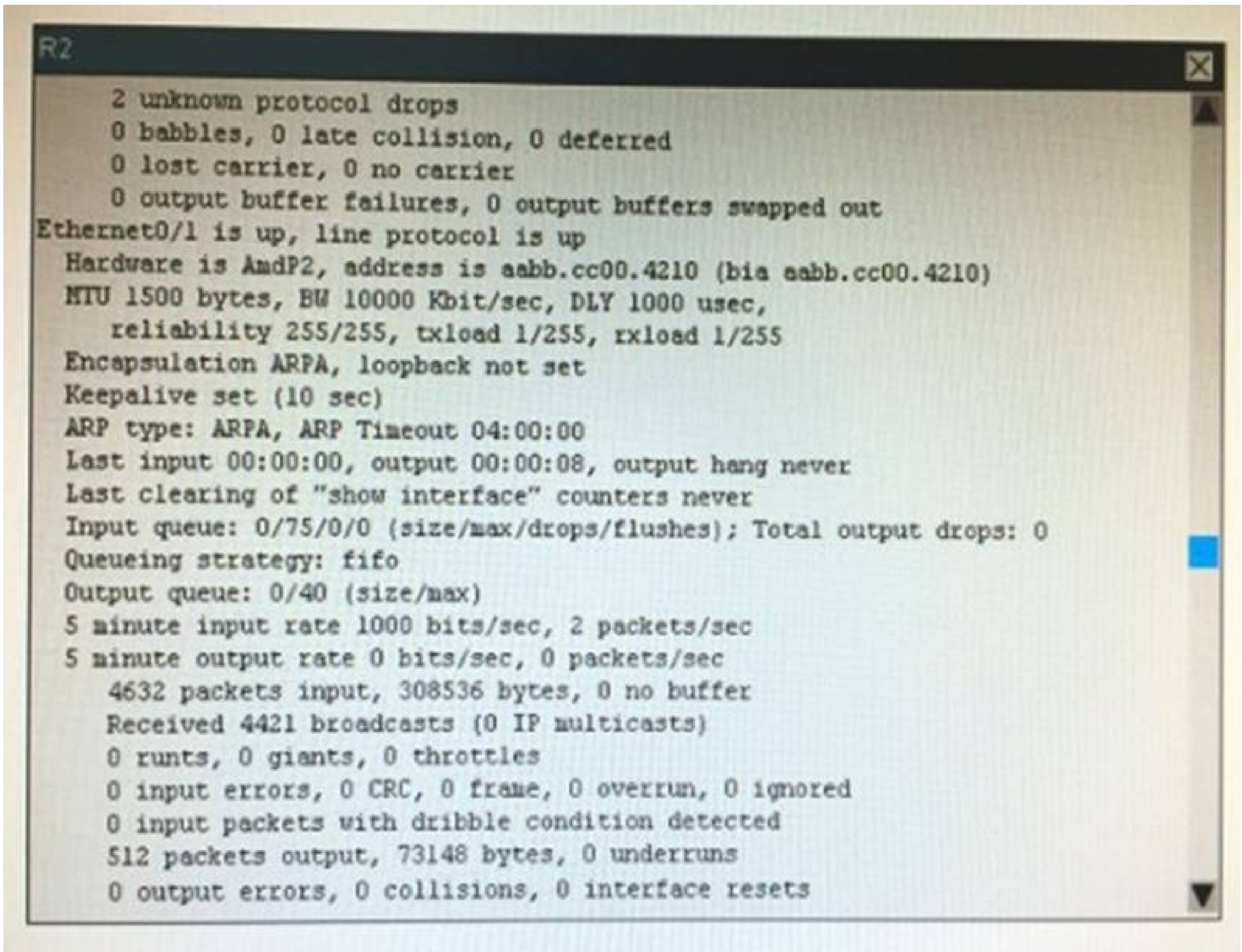
```
!
interface Ethernet0/2
 description ***Link to R1***
 ip address 172.16.14.2 255.255.255.252
!
interface Ethernet0/3
 description ***Link to LAN***
 ip address 10.10.10.1 255.255.255.0
!
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.1.0
 network 192.168.100.0
 network 192.168.200.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
```



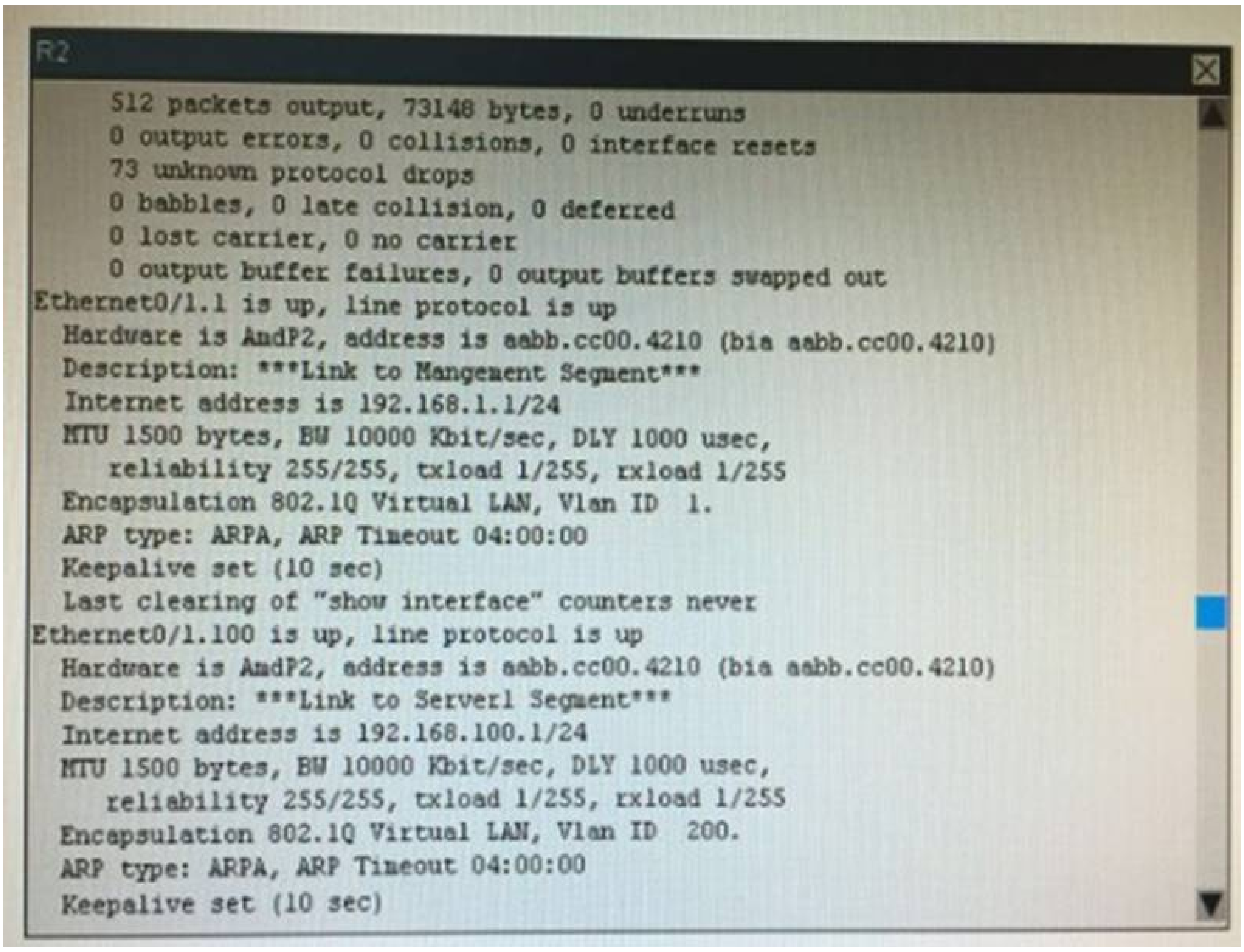
```
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
!
end
R2#show interfaces
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4200 (bia aabb.cc00.4200)
  Description: ***Link to R3***
  Internet address is 172.16.11.1/30
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```



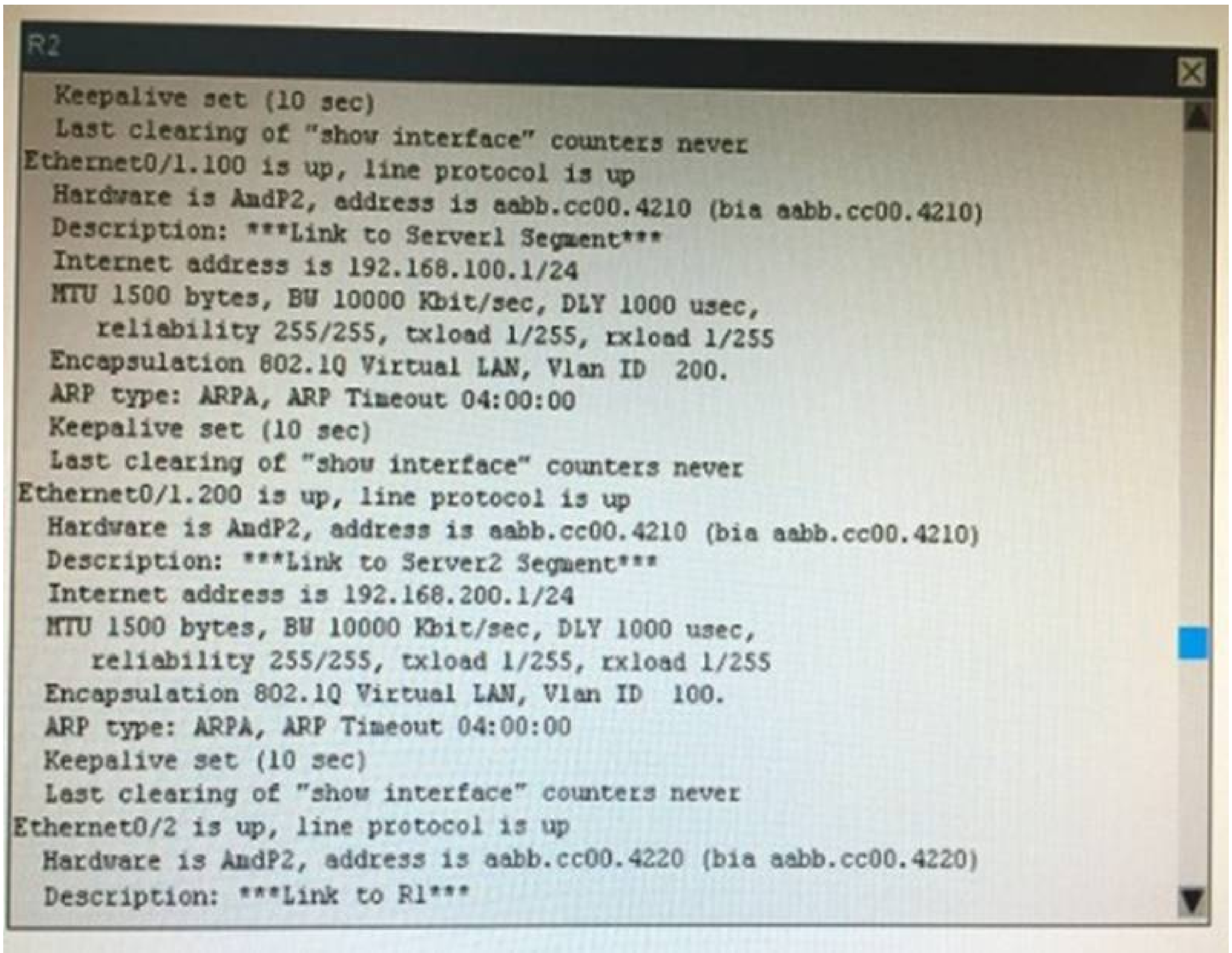
```
R2#show interfaces
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4200 (bia aabb.cc00.4200)
  Description: ***Link to R3***
  Internet address is 172.16.11.1/30
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:32, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     50 packets input, 15683 bytes, 0 no buffer
     Received 50 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     343 packets output, 42566 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     2 unknown protocol drops
```



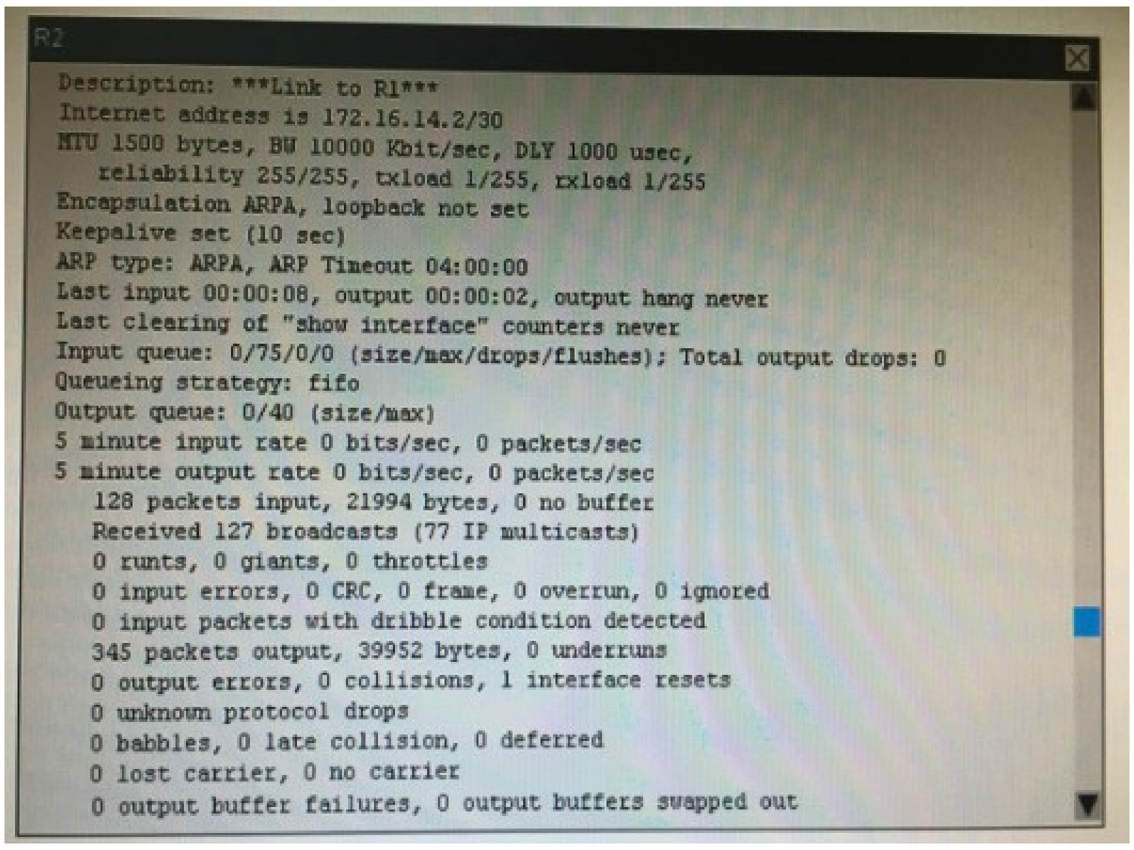
```
     2 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/1 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4210 (bia aabb.cc00.4210)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     4632 packets input, 308536 bytes, 0 no buffer
     Received 4421 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     512 packets output, 73148 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
```



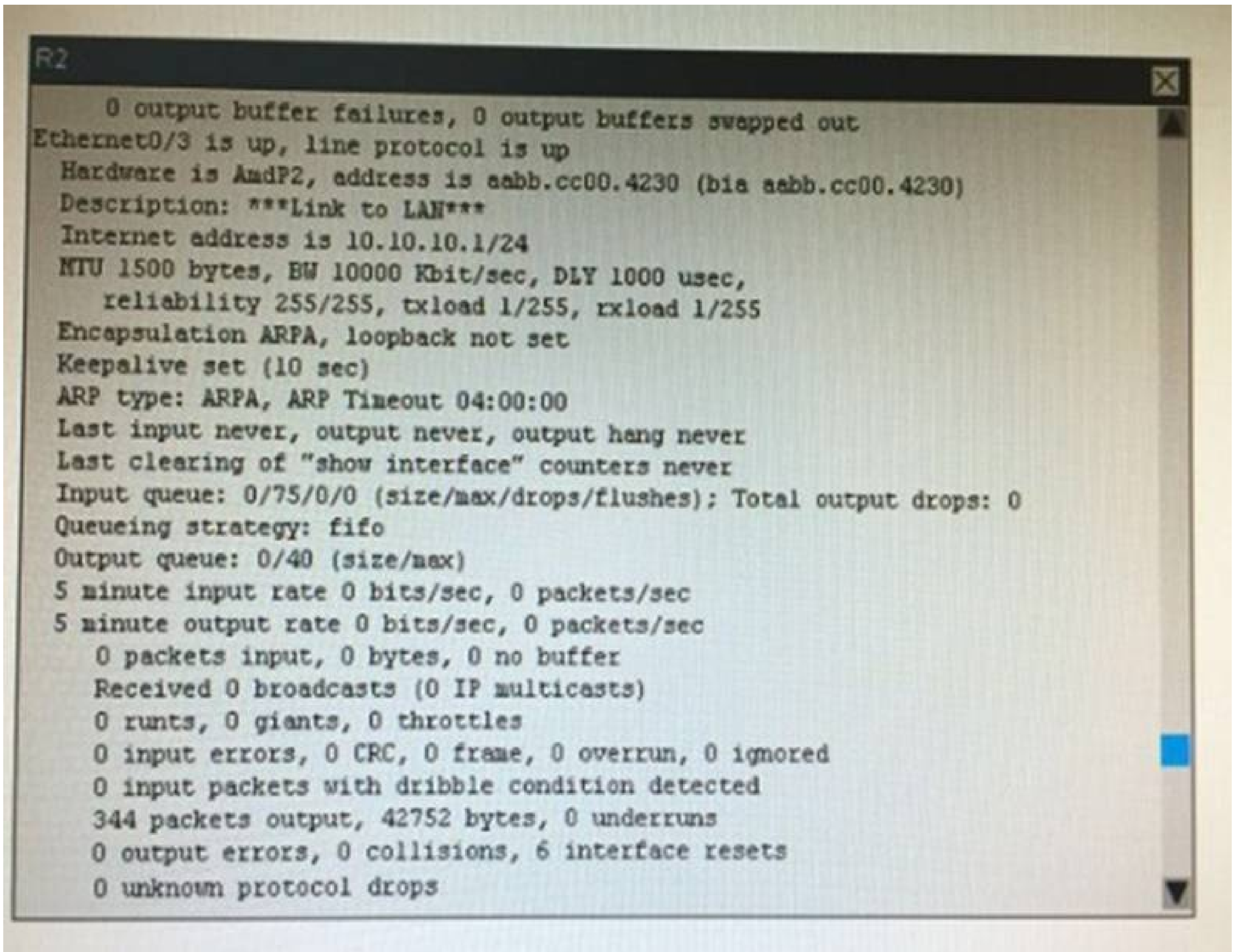
```
     512 packets output, 73148 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     73 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/1.1 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4210 (bia aabb.cc00.4210)
  Description: ***Link to Mangement Segment***
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive set (10 sec)
  Last clearing of "show interface" counters never
Ethernet0/1.100 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4210 (bia aabb.cc00.4210)
  Description: ***Link to Server1 Segment***
  Internet address is 192.168.100.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  200.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive set (10 sec)
```



```
  Keepalive set (10 sec)
  Last clearing of "show interface" counters never
Ethernet0/1.100 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4210 (bia aabb.cc00.4210)
  Description: ***Link to Server1 Segment***
  Internet address is 192.168.100.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  200.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive set (10 sec)
  Last clearing of "show interface" counters never
Ethernet0/1.200 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4210 (bia aabb.cc00.4210)
  Description: ***Link to Server2 Segment***
  Internet address is 192.168.200.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  100.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive set (10 sec)
  Last clearing of "show interface" counters never
Ethernet0/2 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4220 (bia aabb.cc00.4220)
  Description: ***Link to R1***
```

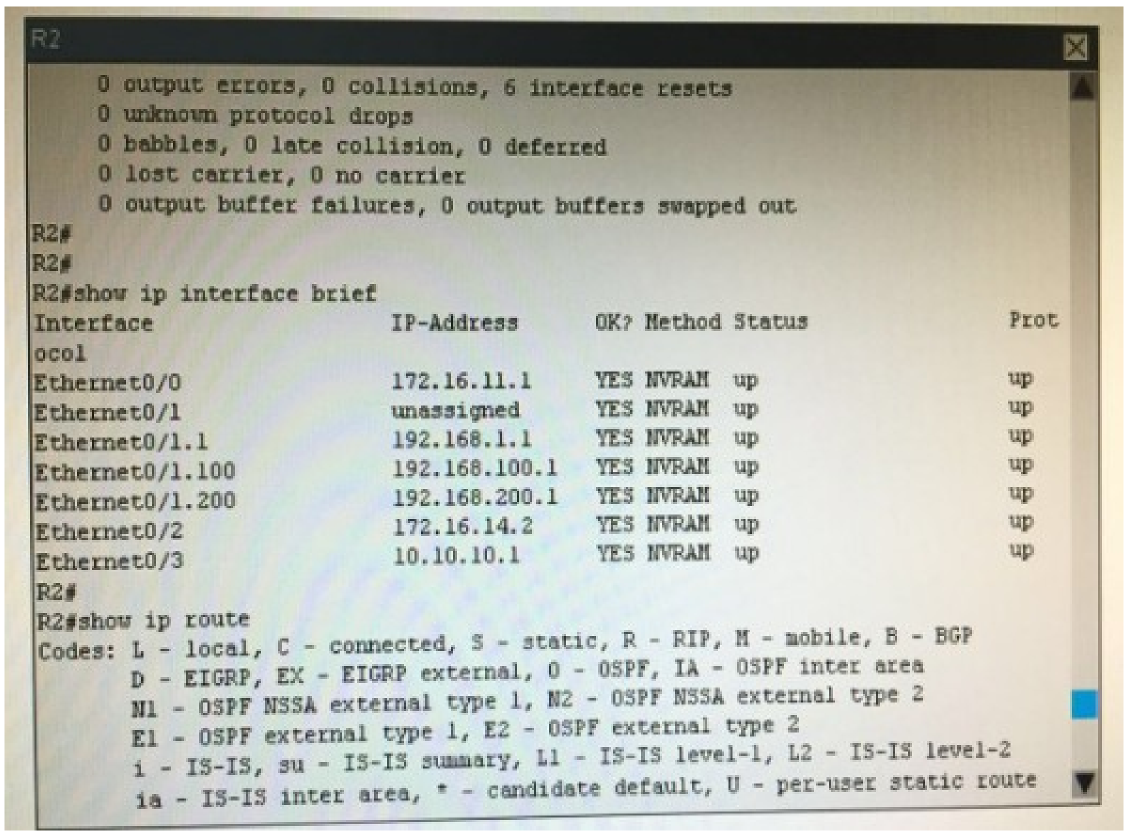


```
  Description: ***Link to R1***
  Internet address is 172.16.14.2/30
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     128 packets input, 21994 bytes, 0 no buffer
     Received 127 broadcasts (77 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     345 packets output, 39952 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```



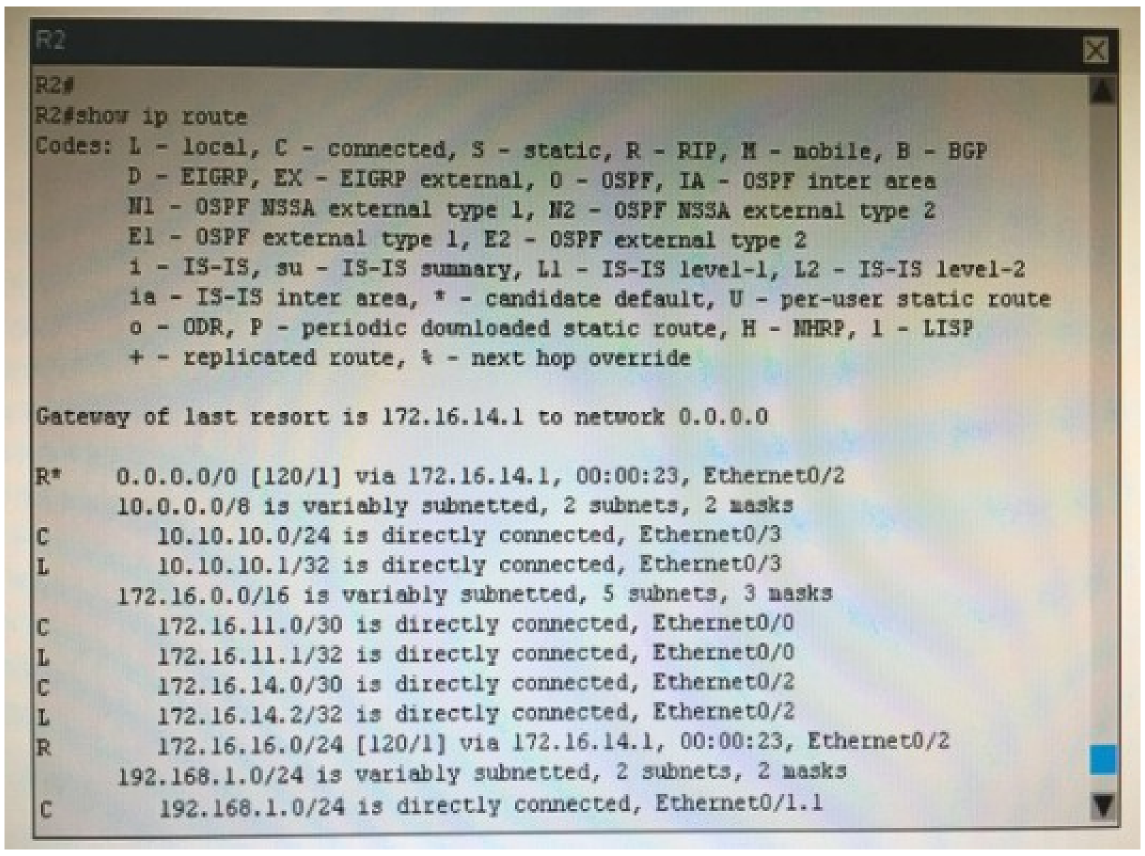
R2

```
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/3 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4230 (bia aabb.cc00.4230)
  Description: ***Link to LAN***
  Internet address is 10.10.10.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     344 packets output, 42752 bytes, 0 underruns
     0 output errors, 0 collisions, 6 interface resets
     0 unknown protocol drops
```

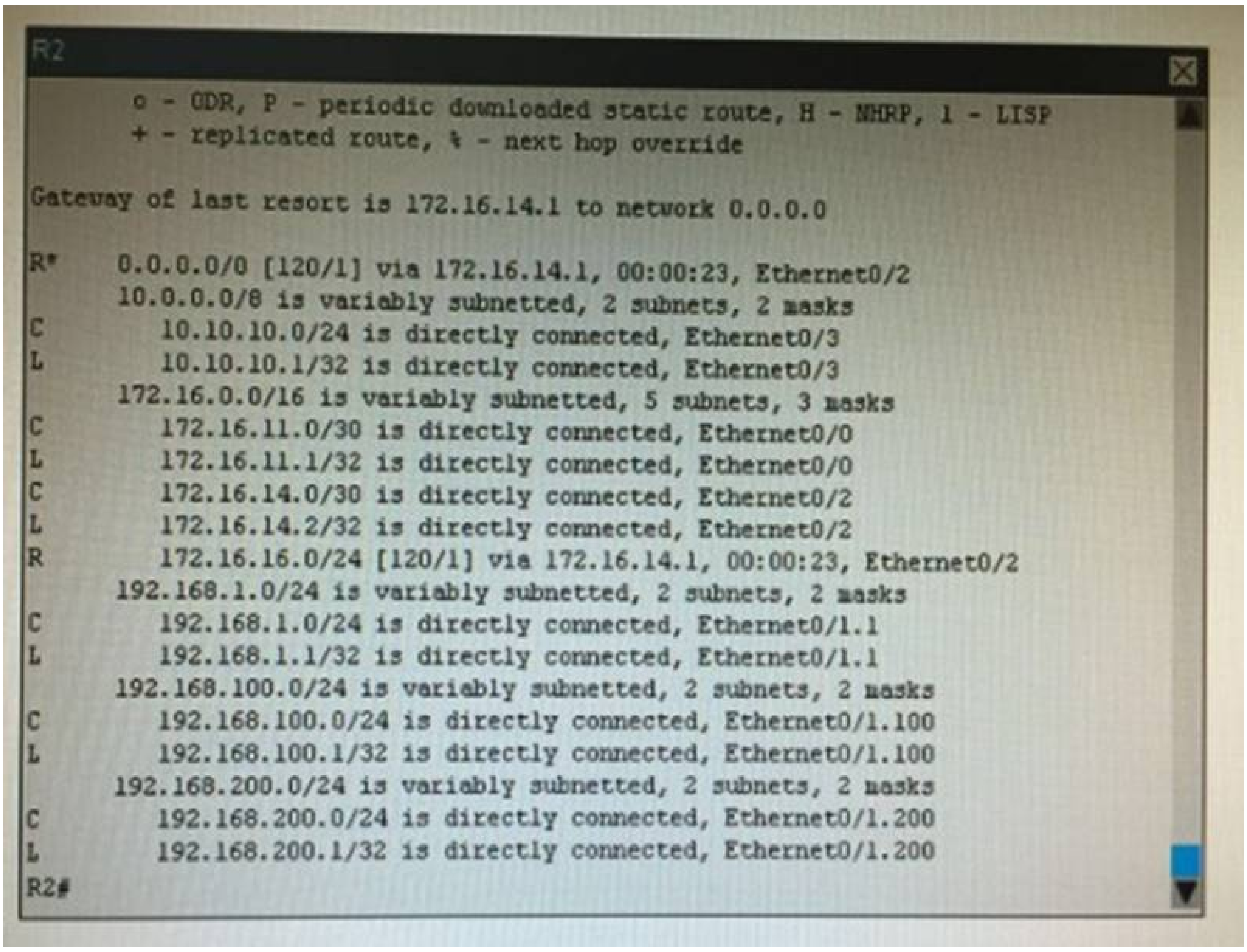


R2

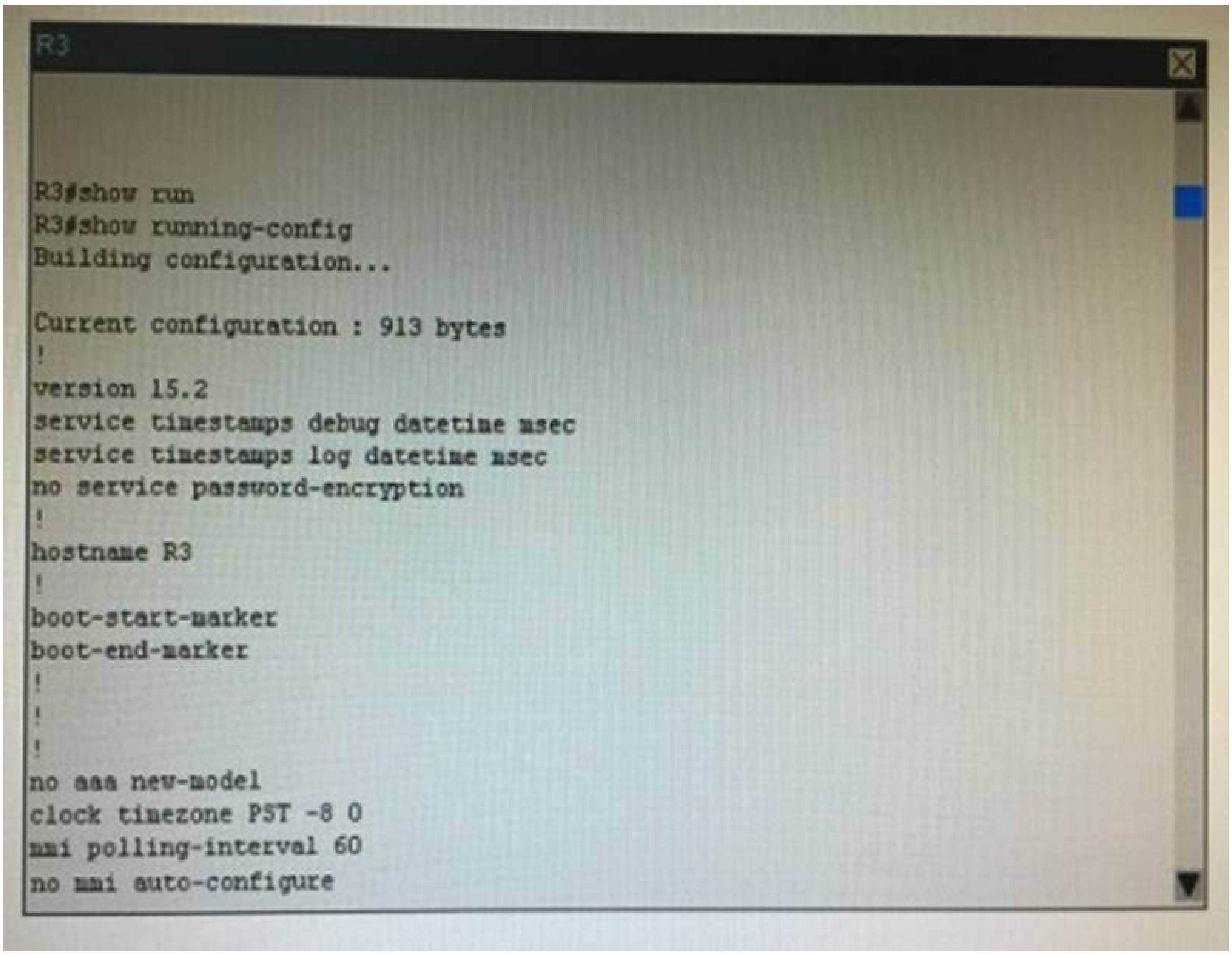
```
     0 output errors, 0 collisions, 6 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R2#
R2#
R2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
Ethernet0/0                172.16.11.1     YES NVRAM  up                    up
Ethernet0/1                unassigned      YES NVRAM  up                    up
Ethernet0/1.1              192.168.1.1     YES NVRAM  up                    up
Ethernet0/1.100            192.168.100.1   YES NVRAM  up                    up
Ethernet0/1.200            192.168.200.1   YES NVRAM  up                    up
Ethernet0/2                172.16.14.2     YES NVRAM  up                    up
Ethernet0/3                10.10.10.1      YES NVRAM  up                    up
R2#
R2#show ip route
Codes: L - local, 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
```



```
R2
R2#
R2#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.14.1 to network 0.0.0.0

R*    0.0.0.0/0 [120/1] via 172.16.14.1, 00:00:23, Ethernet0/2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.10.0/24 is directly connected, Ethernet0/3
L        10.10.10.1/32 is directly connected, Ethernet0/3
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.11.0/30 is directly connected, Ethernet0/0
L        172.16.11.1/32 is directly connected, Ethernet0/0
C        172.16.14.0/30 is directly connected, Ethernet0/2
L        172.16.14.2/32 is directly connected, Ethernet0/2
R        172.16.16.0/24 [120/1] via 172.16.14.1, 00:00:23, Ethernet0/2
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Ethernet0/1.1
```

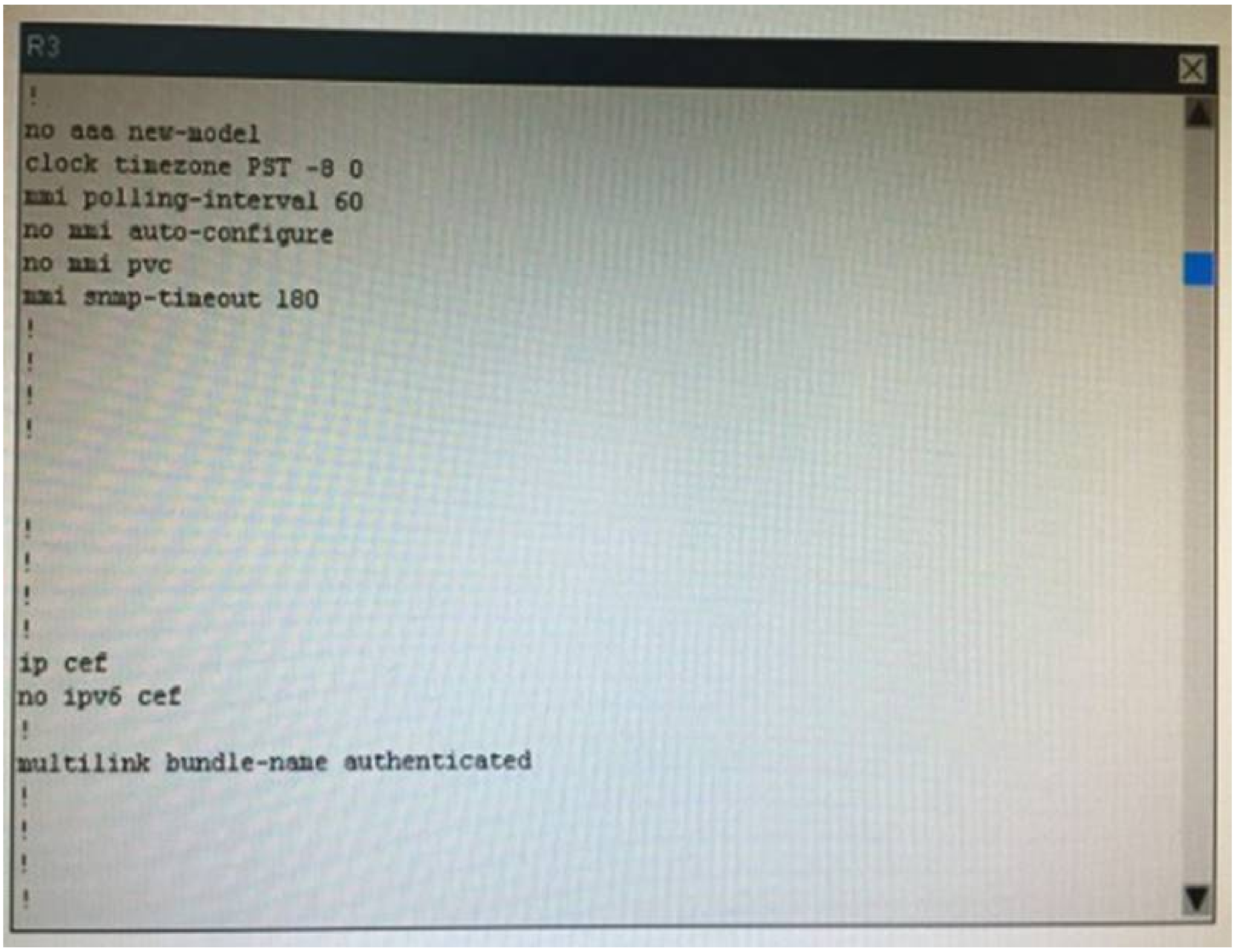


```
R2
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.14.1 to network 0.0.0.0

R*    0.0.0.0/0 [120/1] via 172.16.14.1, 00:00:23, Ethernet0/2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.10.0/24 is directly connected, Ethernet0/3
L        10.10.10.1/32 is directly connected, Ethernet0/3
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.11.0/30 is directly connected, Ethernet0/0
L        172.16.11.1/32 is directly connected, Ethernet0/0
C        172.16.14.0/30 is directly connected, Ethernet0/2
L        172.16.14.2/32 is directly connected, Ethernet0/2
R        172.16.16.0/24 [120/1] via 172.16.14.1, 00:00:23, Ethernet0/2
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Ethernet0/1.1
L        192.168.1.1/32 is directly connected, Ethernet0/1.1
      192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.100.0/24 is directly connected, Ethernet0/1.100
L        192.168.100.1/32 is directly connected, Ethernet0/1.100
      192.168.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.200.0/24 is directly connected, Ethernet0/1.200
L        192.168.200.1/32 is directly connected, Ethernet0/1.200
R2#
```



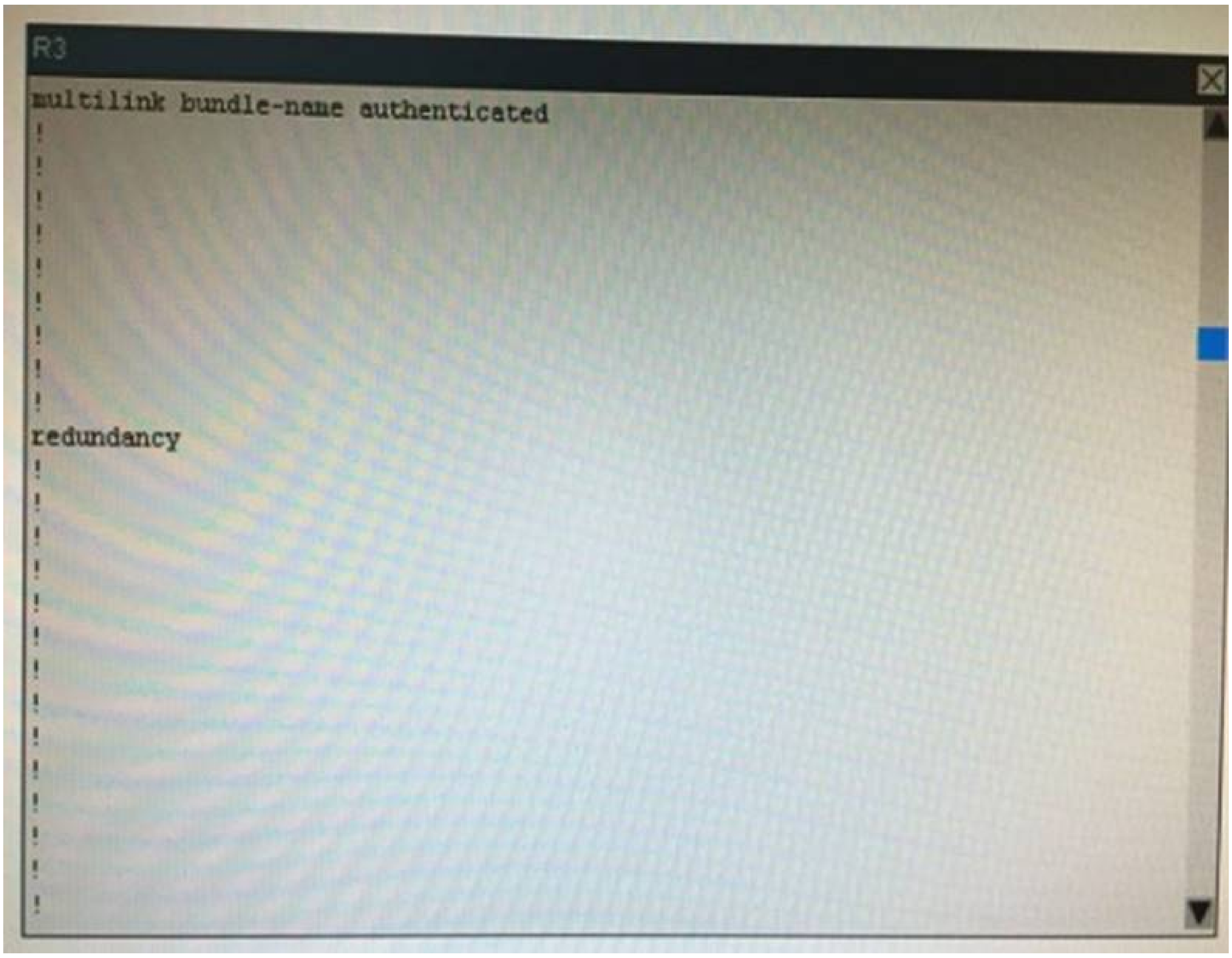
R3

```
R3#show run
R3#show running-config
Building configuration...

Current configuration : 913 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
```

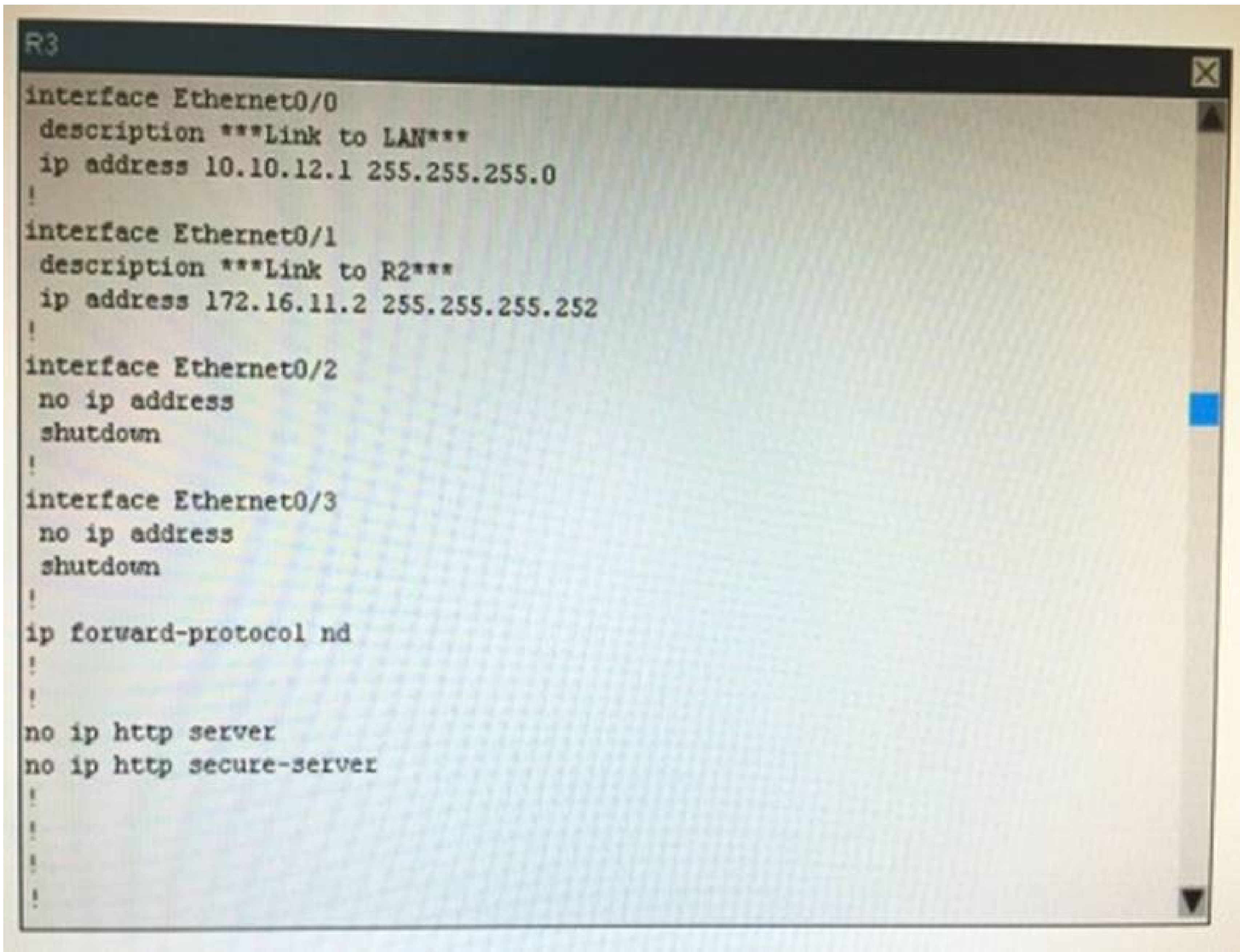


R3

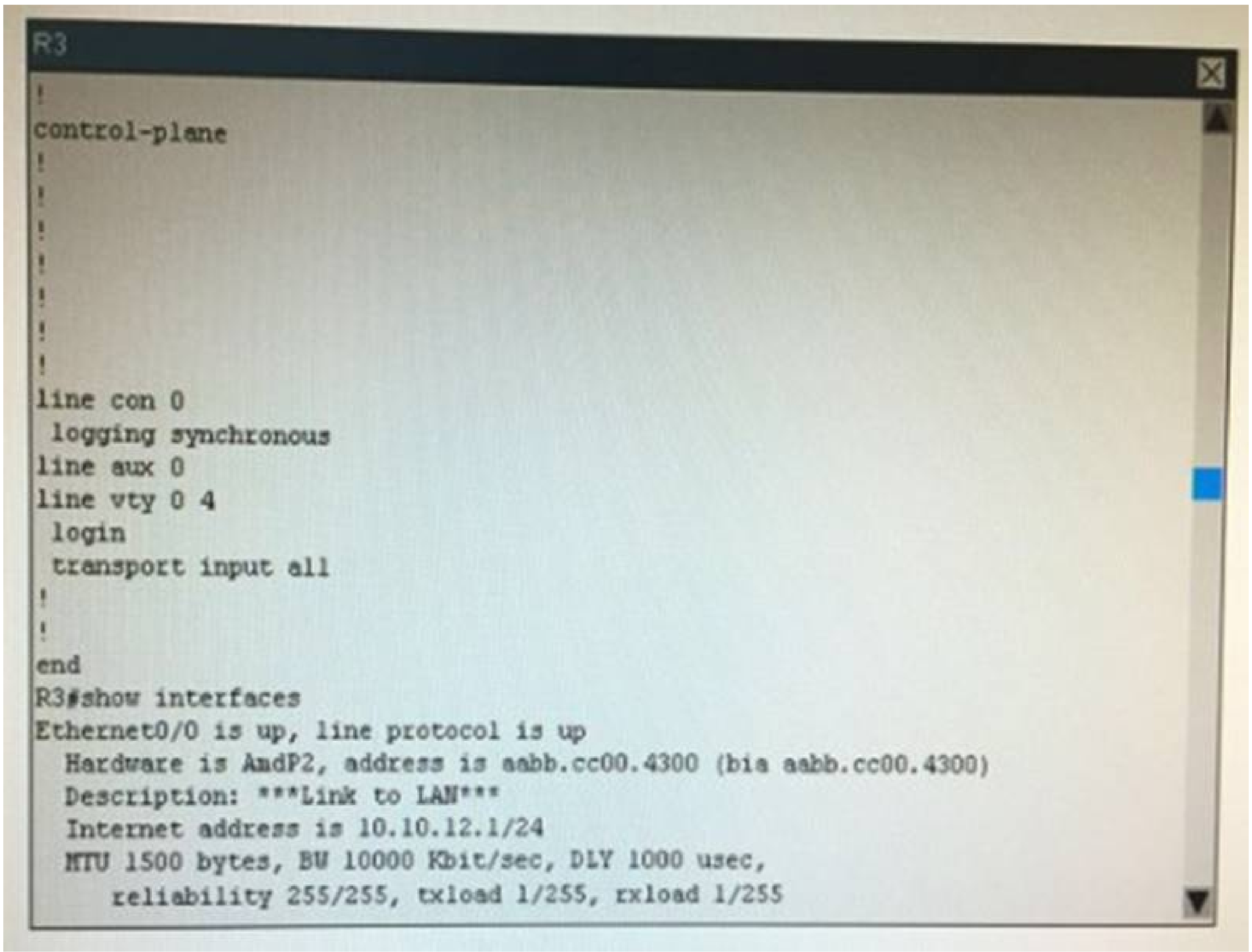
```
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!


!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
```



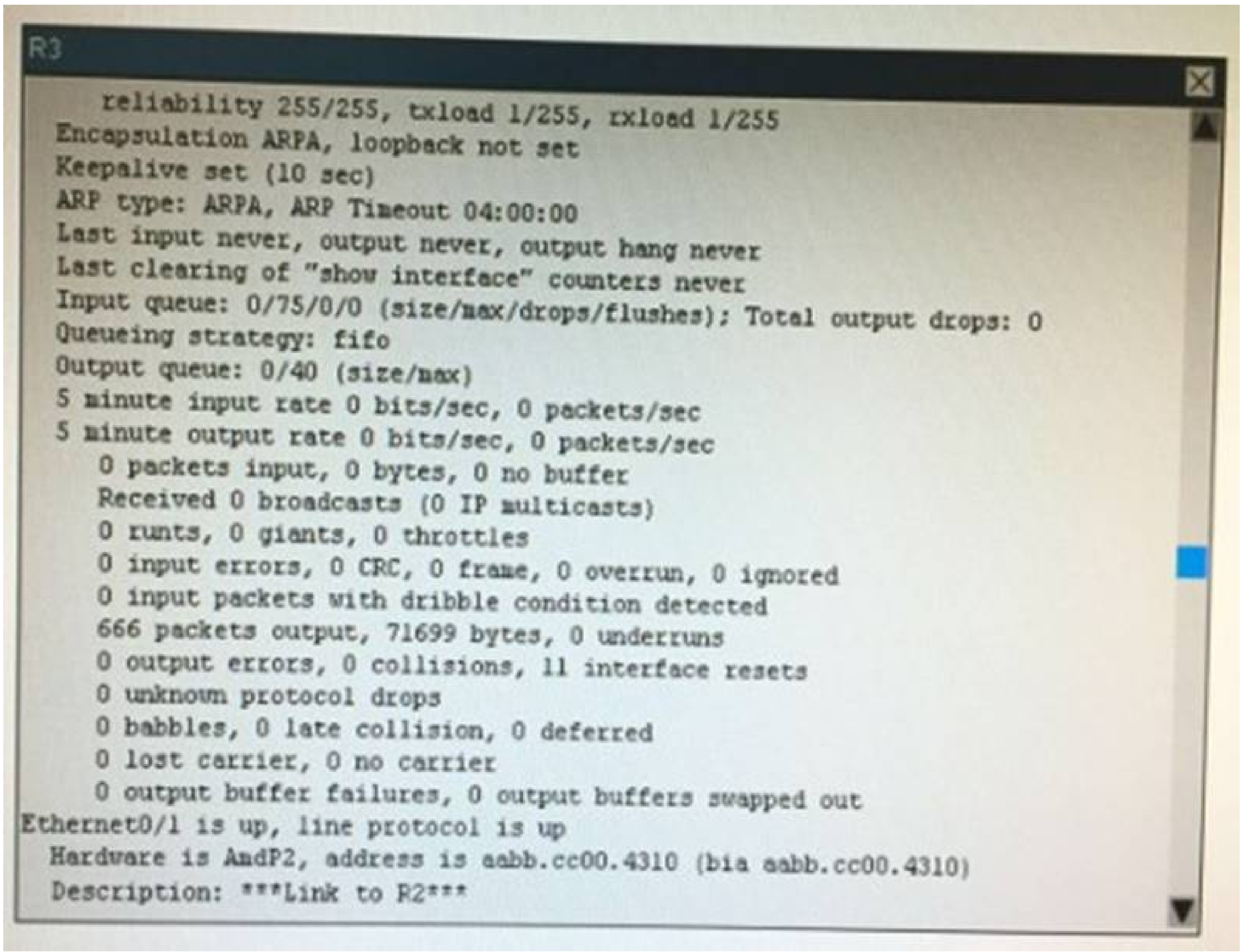
```
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
```



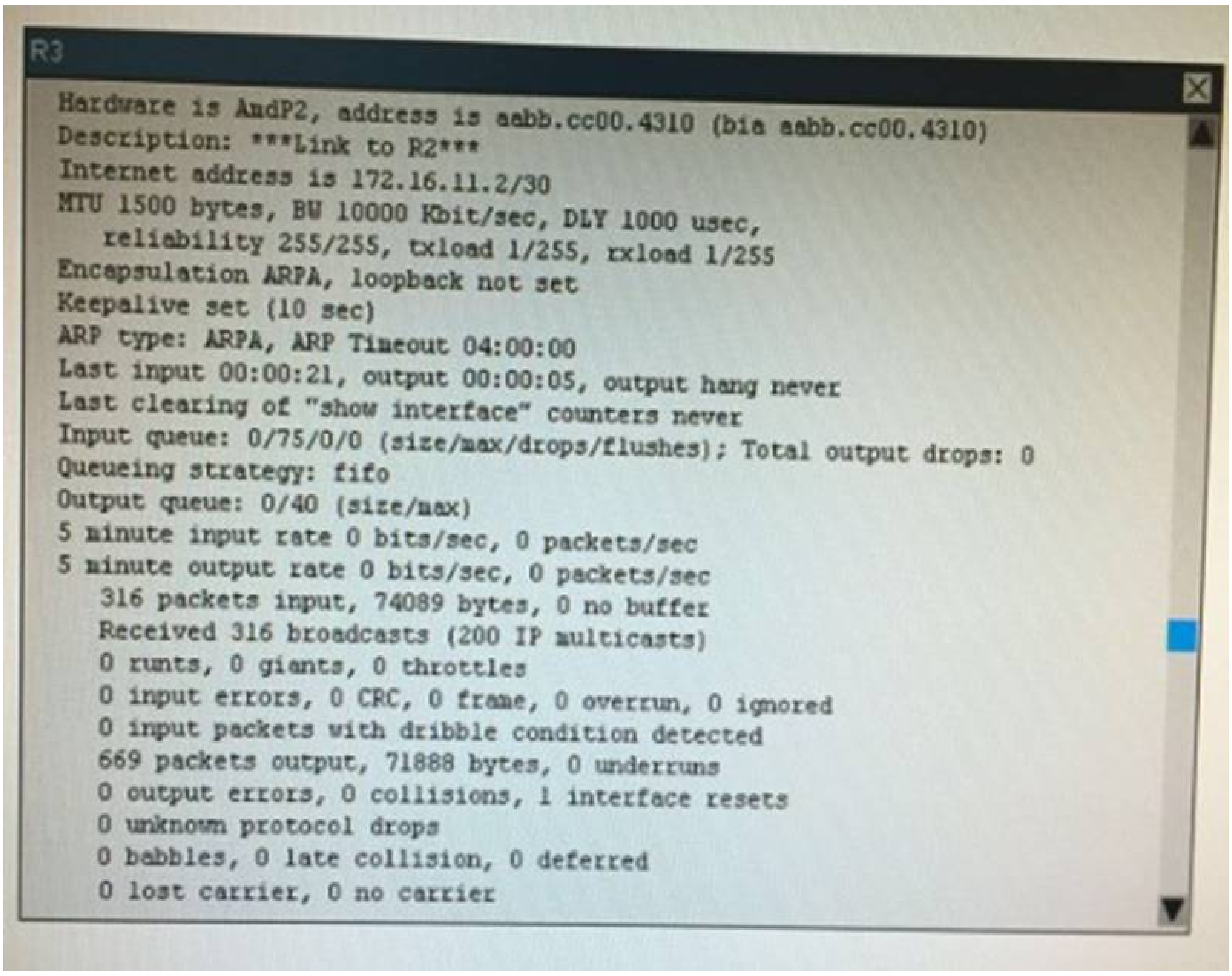
```
interface Ethernet0/0
 description ***Link to LAN***
 ip address 10.10.12.1 255.255.255.0
!
interface Ethernet0/1
 description ***Link to R2***
 ip address 172.16.11.2 255.255.255.252
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
```



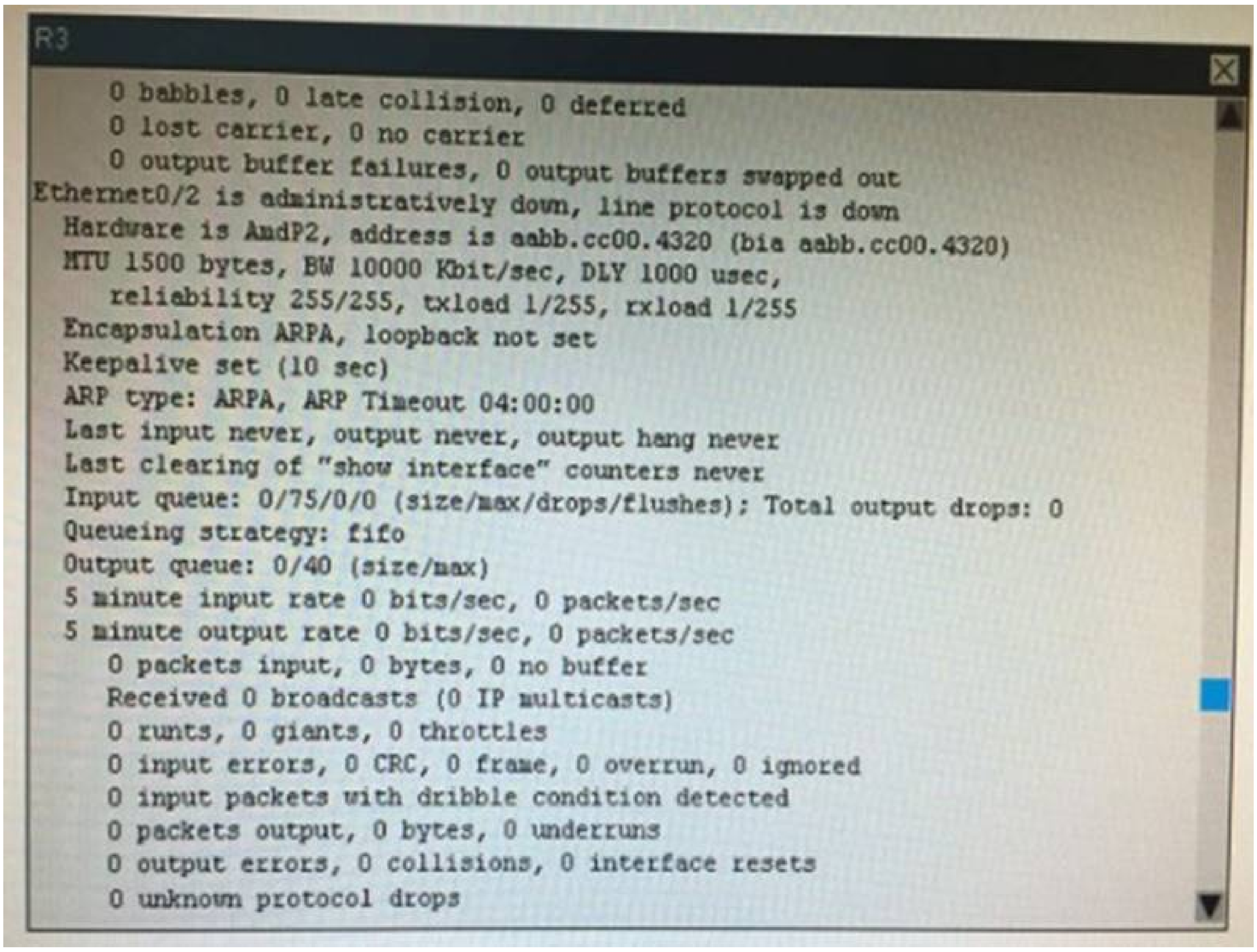
```
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
!
end
R3#show interfaces
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4300 (bia aabb.cc00.4300)
  Description: ***Link to LAN***
  Internet address is 10.10.12.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```



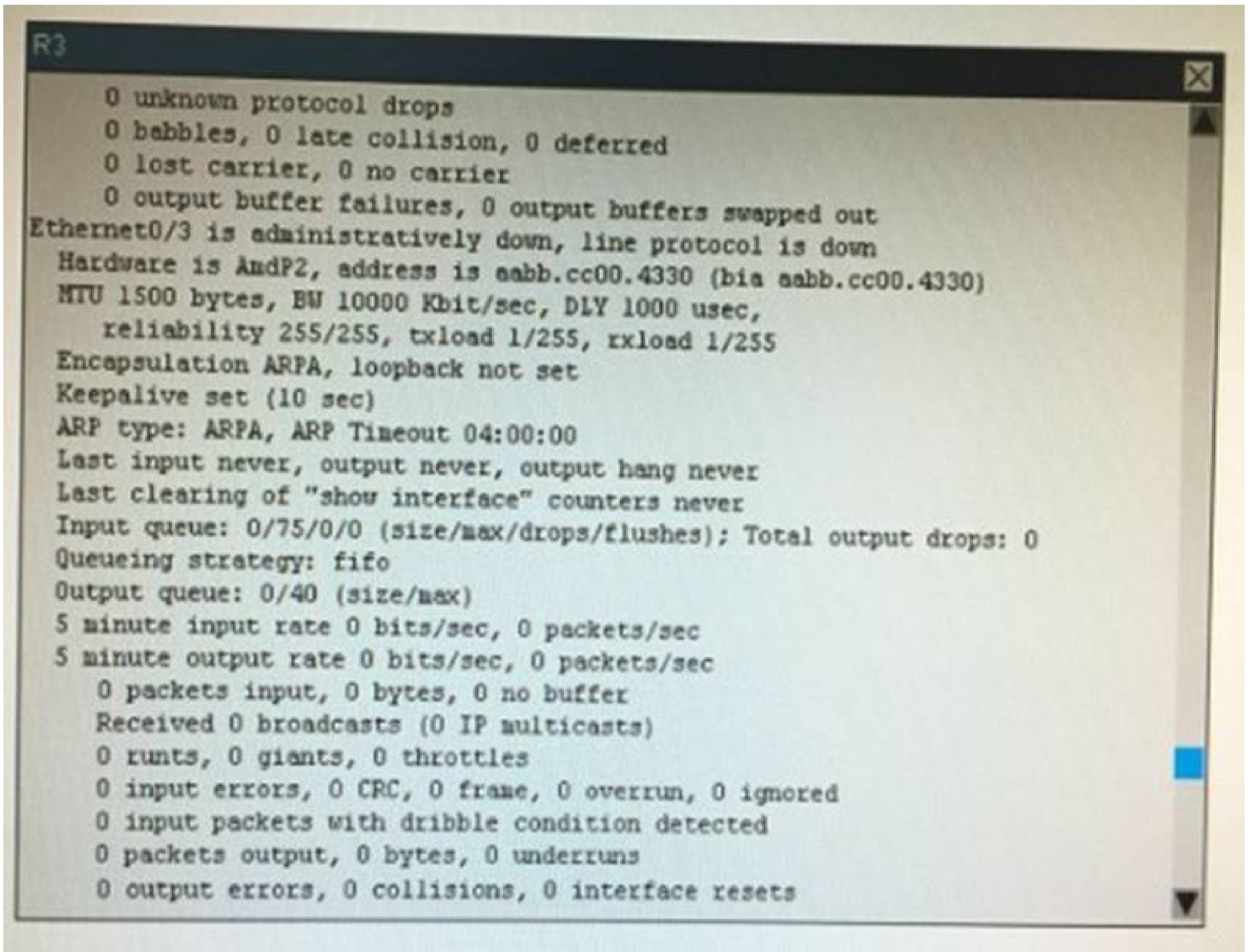
```
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     666 packets output, 71699 bytes, 0 underruns
     0 output errors, 0 collisions, 11 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/1 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4310 (bia aabb.cc00.4310)
  Description: ***Link to R2***
```



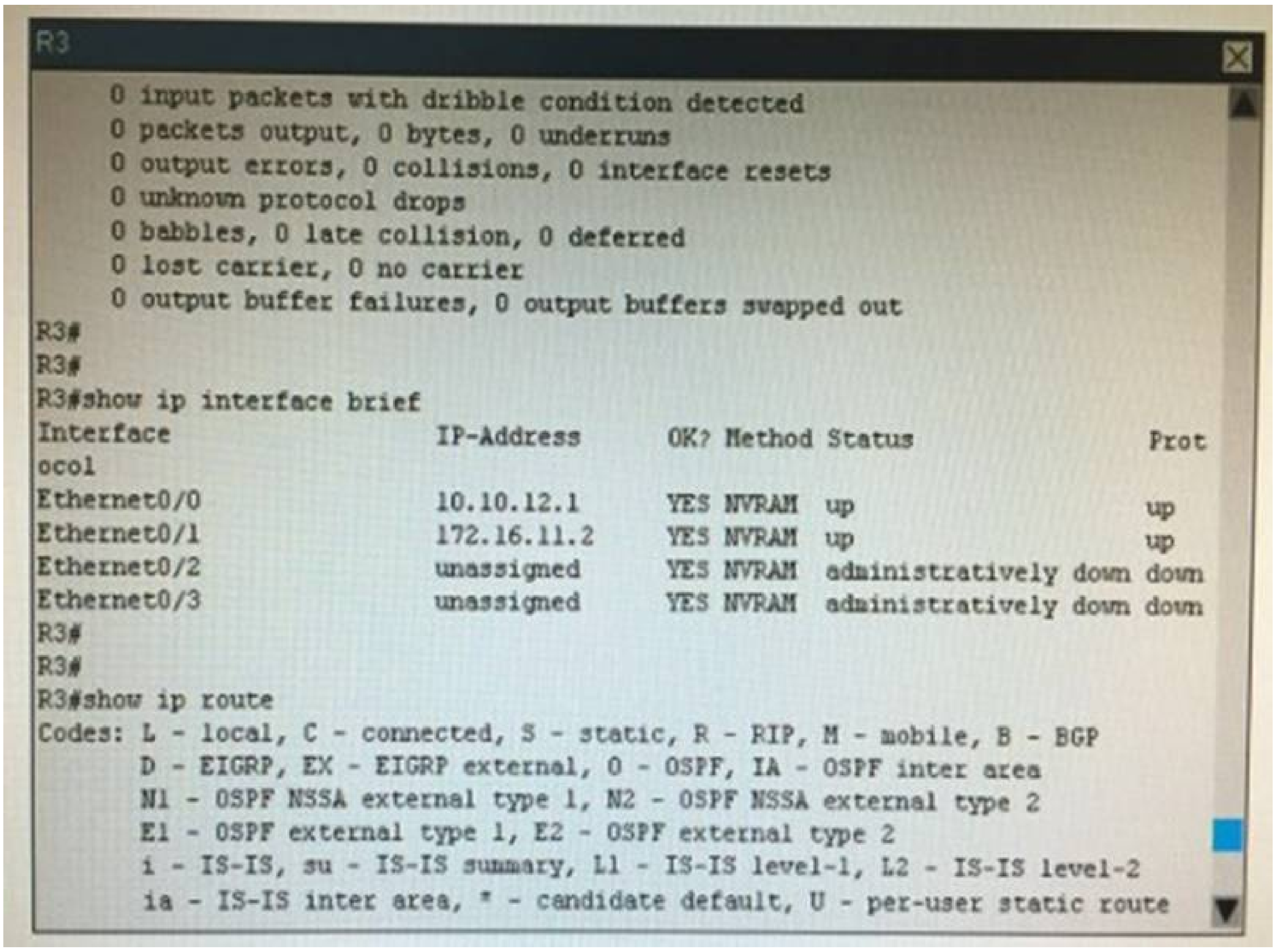
```
 Hardware is AmdP2, address is aabb.cc00.4310 (bia aabb.cc00.4310)
 Description: ***Link to R2***
 Internet address is 172.16.11.2/30
 MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:00:21, output 00:00:05, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
    316 packets input, 74089 bytes, 0 no buffer
    Received 316 broadcasts (200 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    669 packets output, 71888 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
```



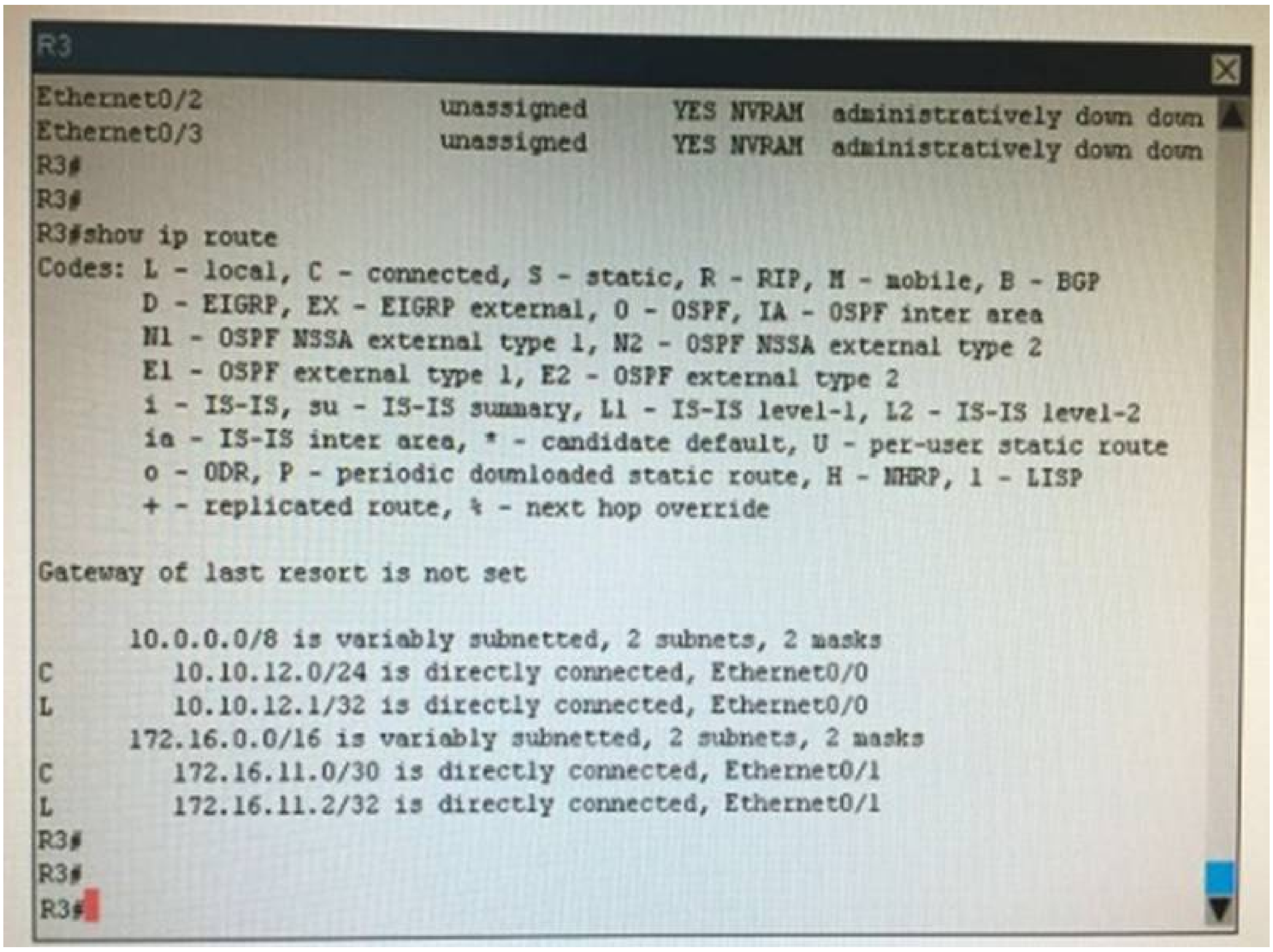
```
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Ethernet0/2 is administratively down, line protocol is down
 Hardware is AmdP2, address is aabb.cc00.4320 (bia aabb.cc00.4320)
 MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input never, output never, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
```



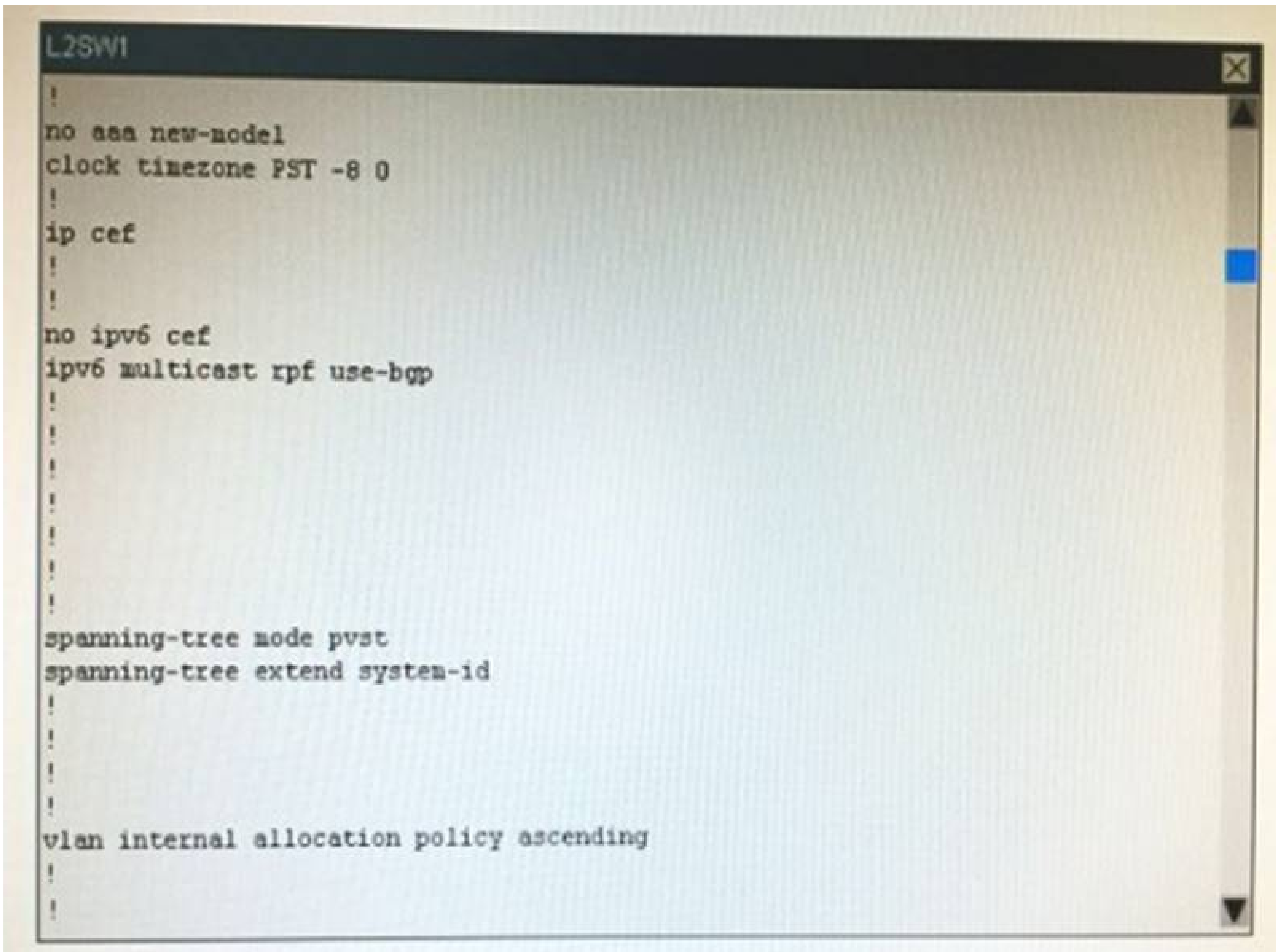
```
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/3 is administratively down, line protocol is down
  Hardware is AmdP2, address is aabb.cc00.4330 (bia aabb.cc00.4330)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
```



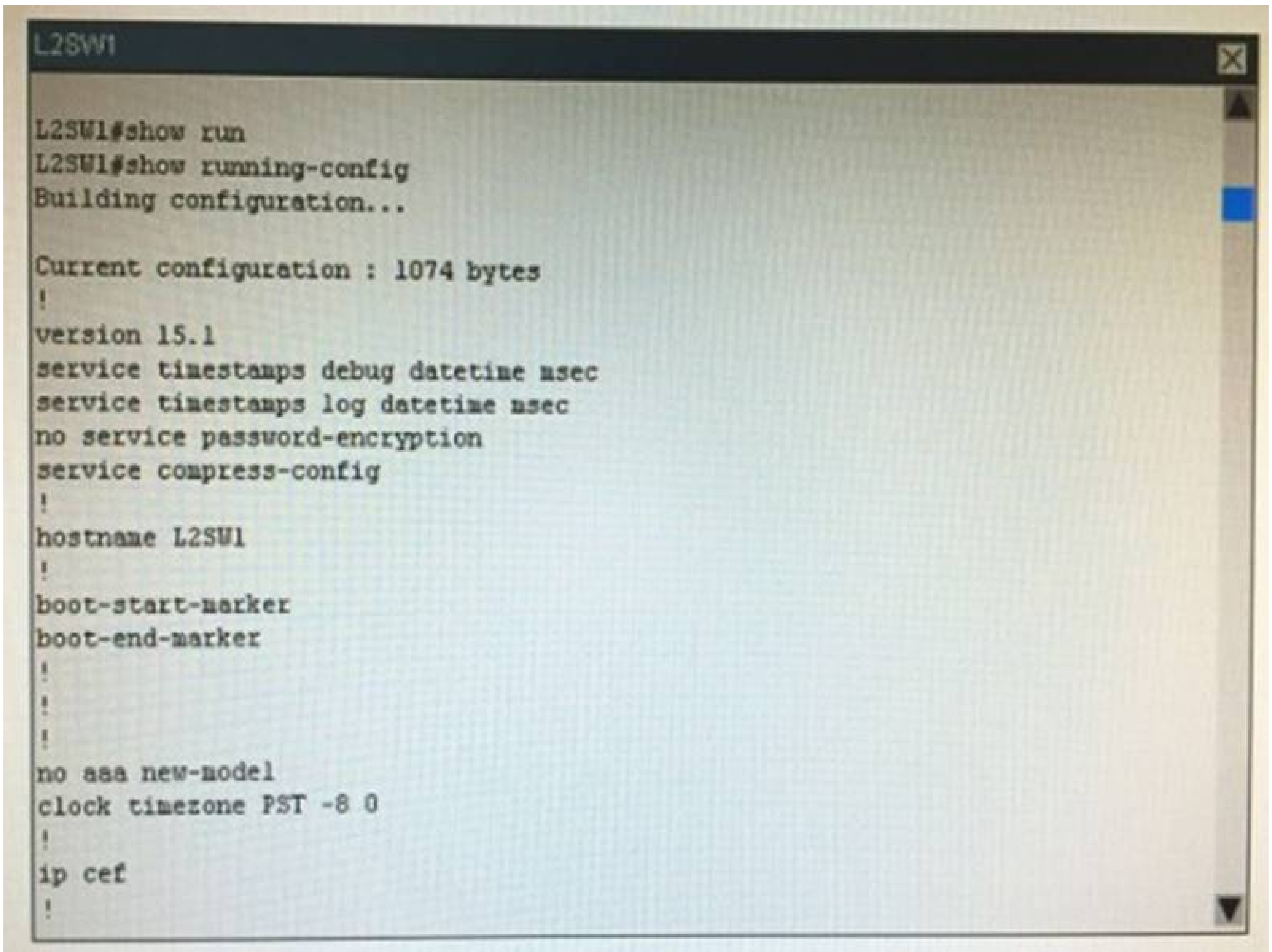
```
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R3#
R3#
R3#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
Ethernet0/0                10.10.12.1      YES NVRAM  up                    up
Ethernet0/1                172.16.11.2     YES NVRAM  up                    up
Ethernet0/2                unassigned      YES NVRAM  administratively down down
Ethernet0/3                unassigned      YES NVRAM  administratively down down
R3#
R3#
R3#show ip route
Codes: L - local, 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
```



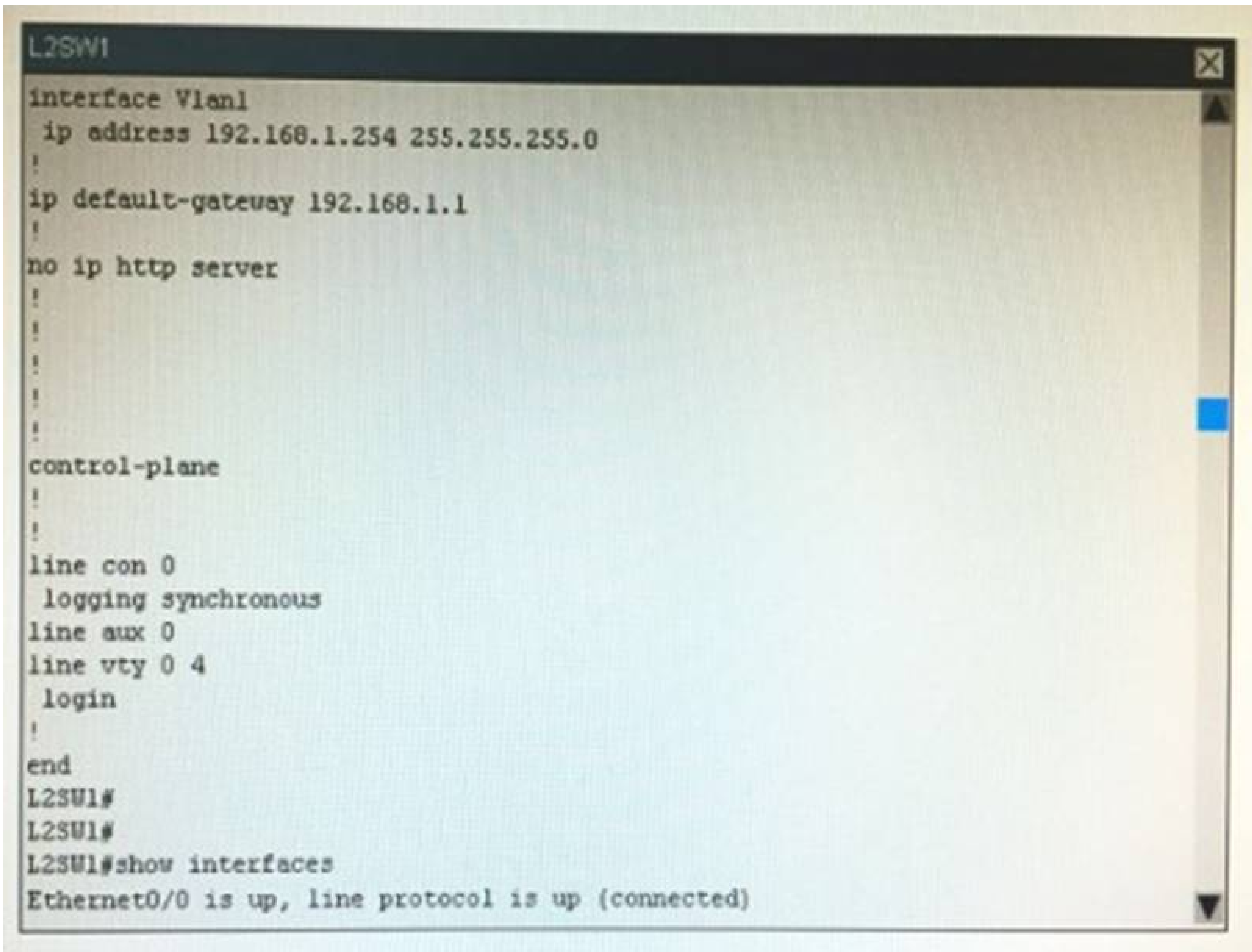
```
Ethernet0/2                 unassigned      YES NVRAM  administratively down down
Ethernet0/3                 unassigned      YES NVRAM  administratively down down
R3#
R3#
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.12.0/24 is directly connected, Ethernet0/0
L        10.10.12.1/32 is directly connected, Ethernet0/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.11.0/30 is directly connected, Ethernet0/1
L        172.16.11.2/32 is directly connected, Ethernet0/1
R3#
R3#
R3#
```



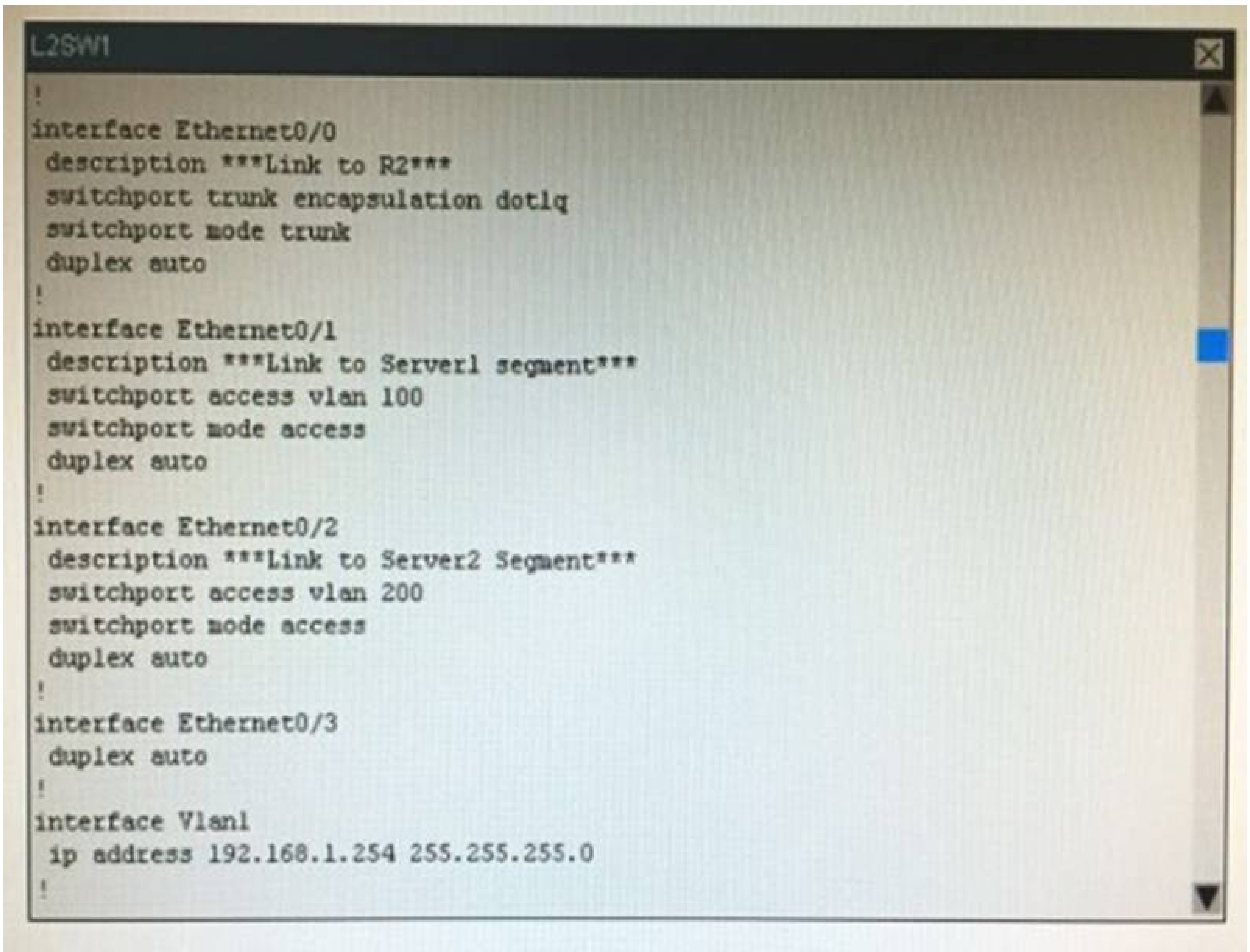
```
!
no aaa new-model
clock timezone PST -8 0
!
ip cef
!
!
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
```



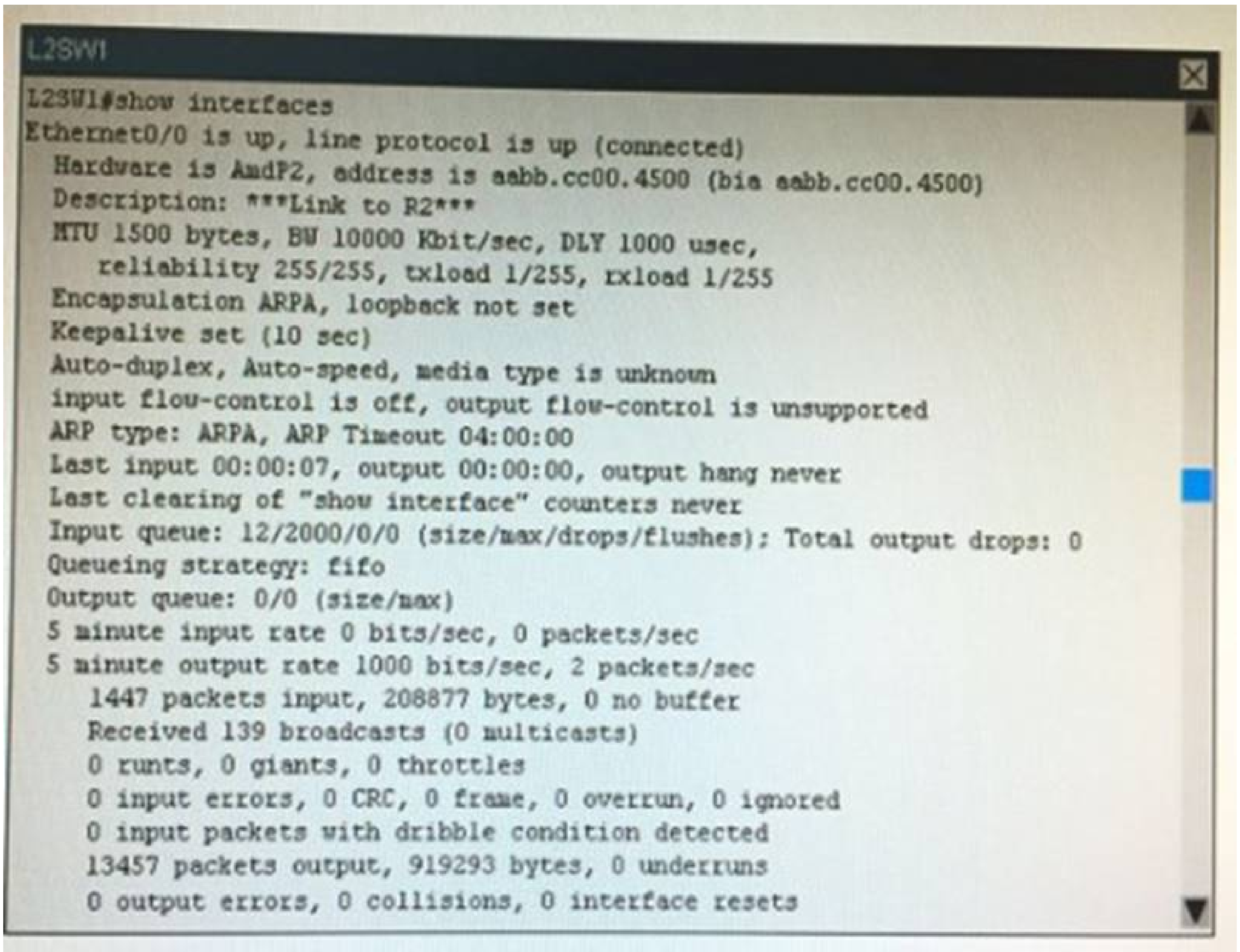
```
L2SW1#show run
L2SW1#show running-config
Building configuration...

Current configuration : 1074 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname L2SW1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
!
ip cef
!
```



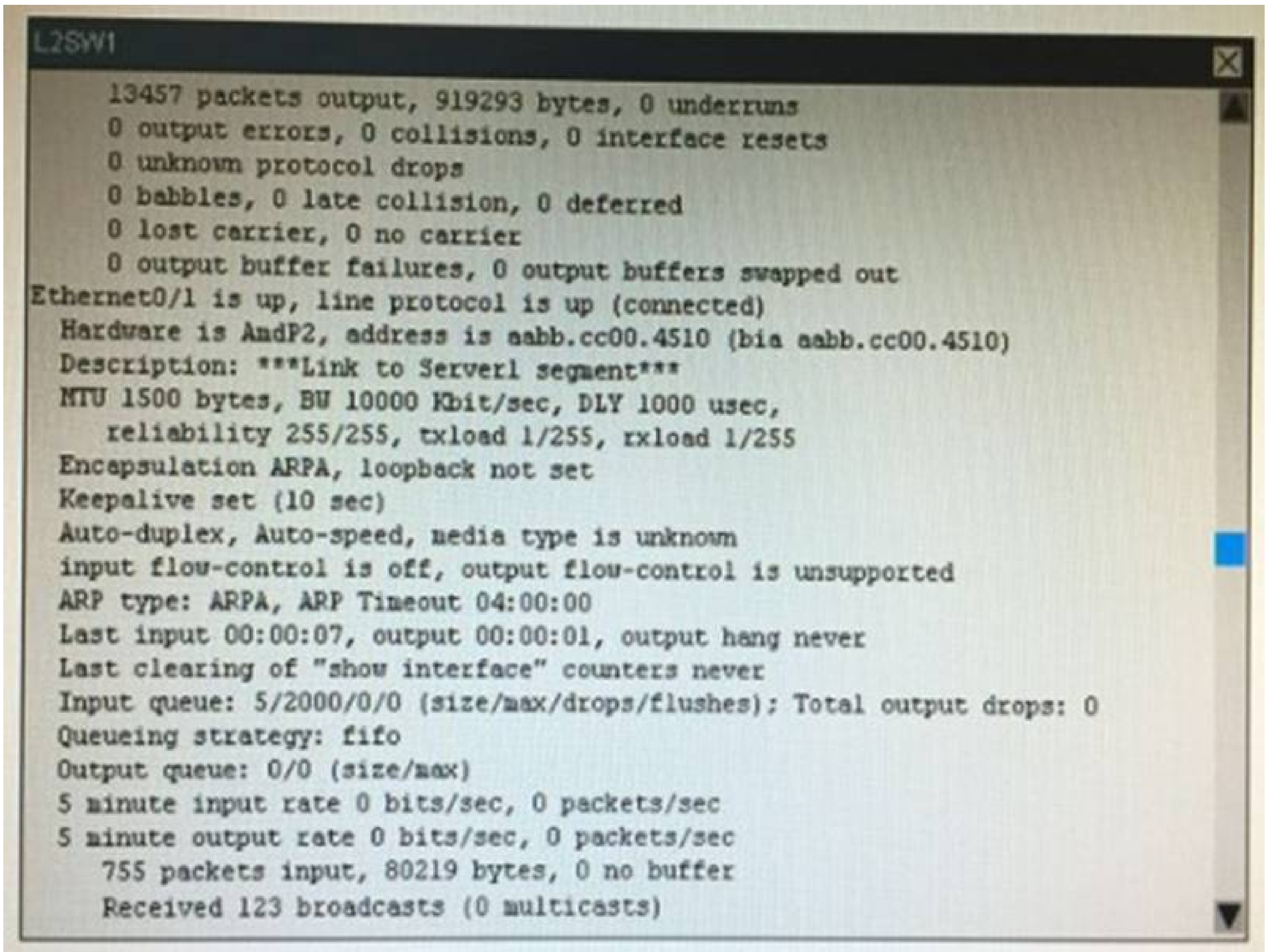
```
interface Vlan1
 ip address 192.168.1.254 255.255.255.0
!
ip default-gateway 192.168.1.1
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
L2SW1#
L2SW1#
L2SW1#show interfaces
Ethernet0/0 is up, line protocol is up (connected)
```



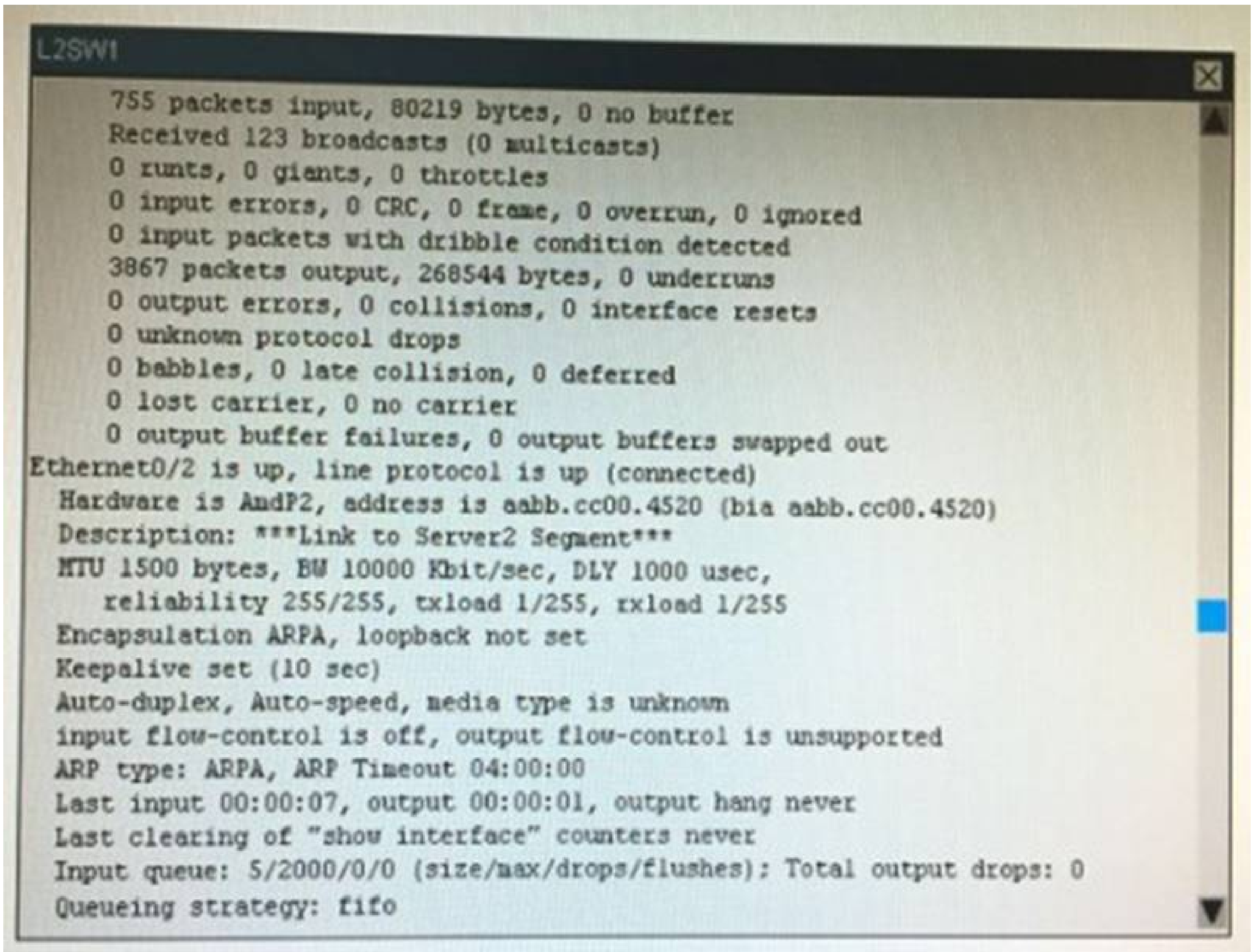
```
!
interface Ethernet0/0
 description ***Link to R2***
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 description ***Link to Server1 segment***
 switchport access vlan 100
 switchport mode access
 duplex auto
!
interface Ethernet0/2
 description ***Link to Server2 Segment***
 switchport access vlan 200
 switchport mode access
 duplex auto
!
interface Ethernet0/3
 duplex auto
!
interface Vlan1
 ip address 192.168.1.254 255.255.255.0
!
```



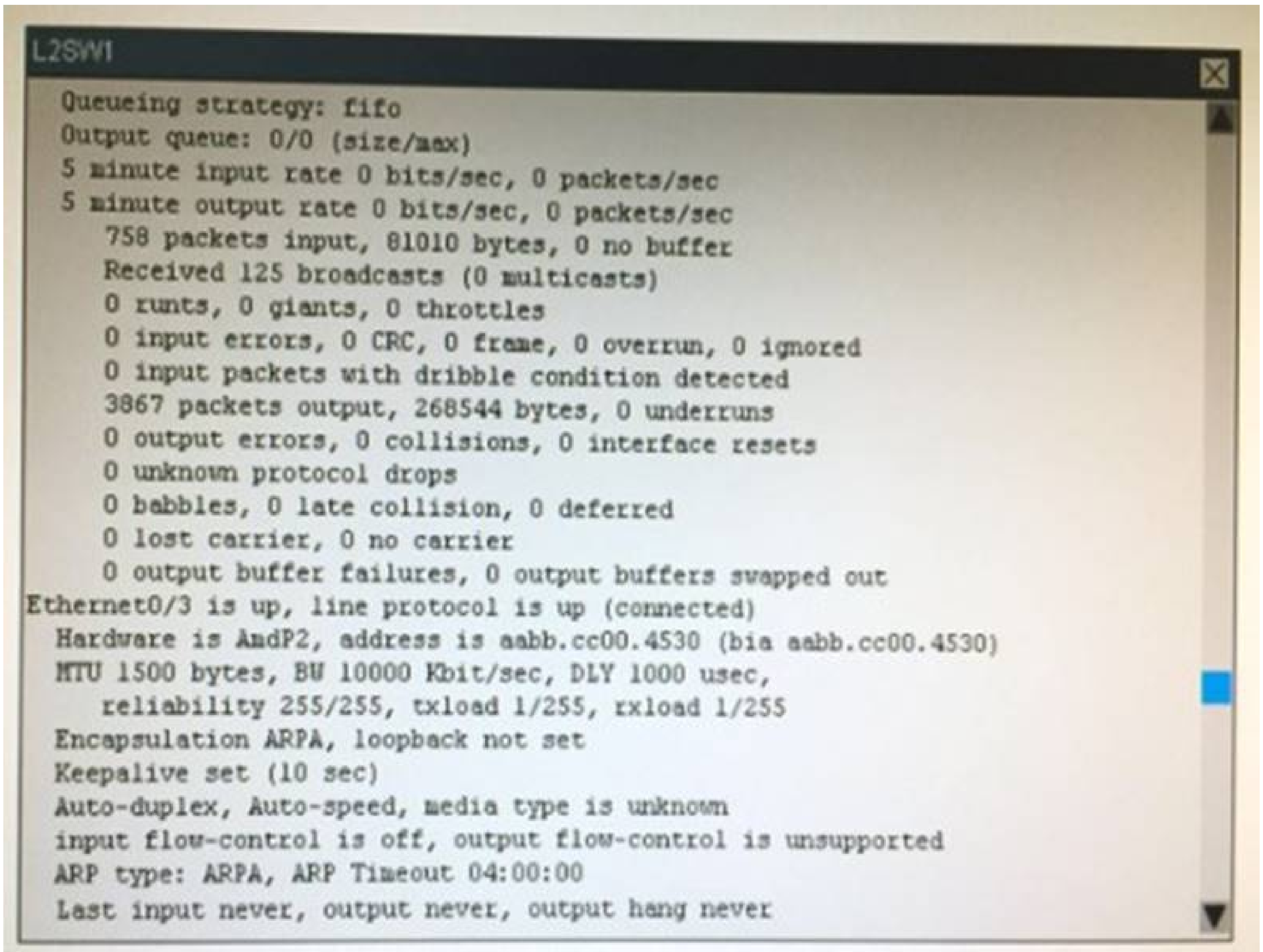
```
L2SW1#show interfaces
Ethernet0/0 is up, line protocol is up (connected)
  Hardware is AmdP2, address is aabb.cc00.4500 (bia aabb.cc00.4500)
  Description: ***Link to R2***
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is unknown
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:07, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 12/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     1447 packets input, 208877 bytes, 0 no buffer
     Received 139 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     13457 packets output, 919293 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
```



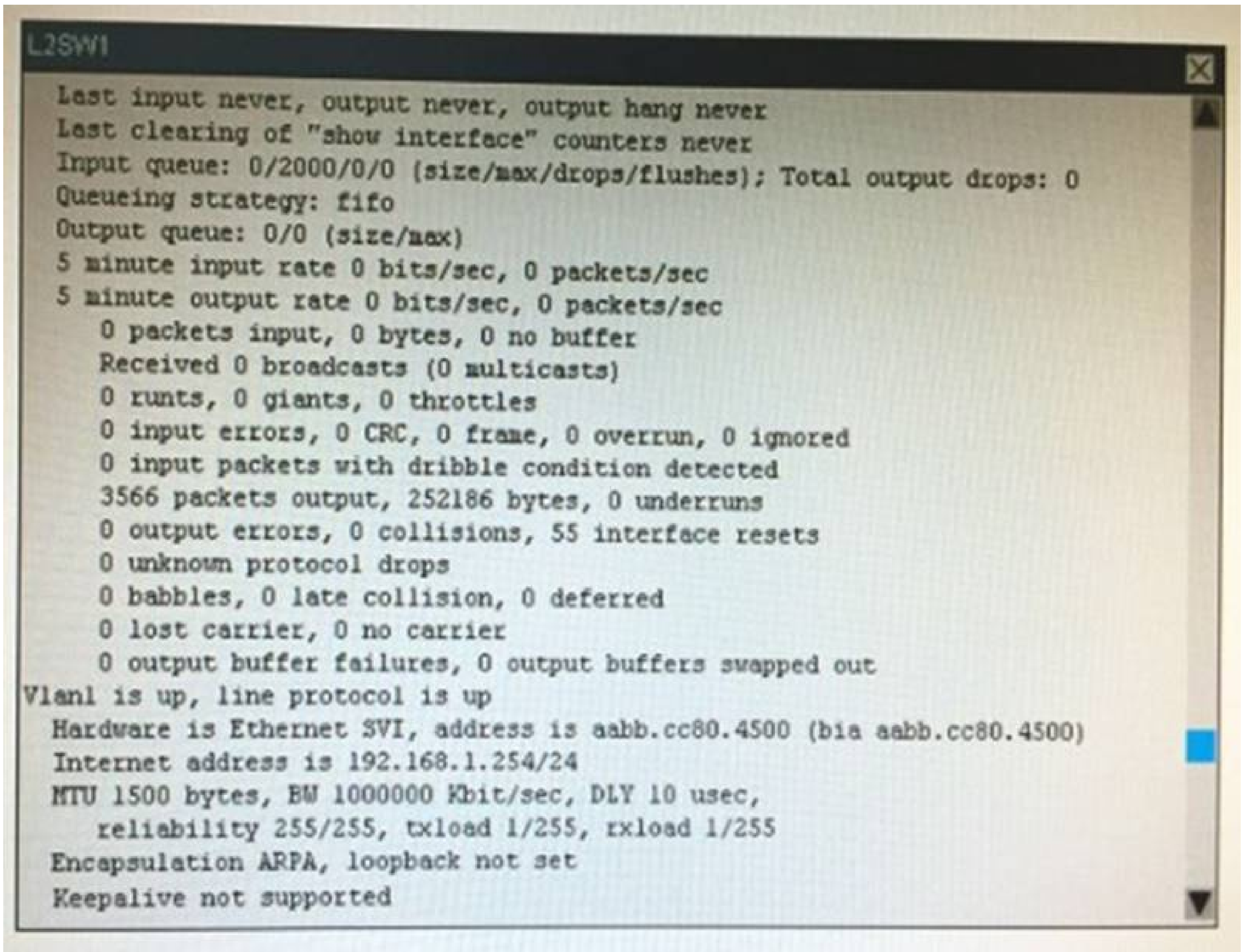
```
     13457 packets output, 919293 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/1 is up, line protocol is up (connected)
  Hardware is AmdP2, address is aabb.cc00.4510 (bia aabb.cc00.4510)
  Description: ***Link to Server1 segment***
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is unknown
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:07, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 5/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     755 packets input, 80219 bytes, 0 no buffer
     Received 123 broadcasts (0 multicasts)
```



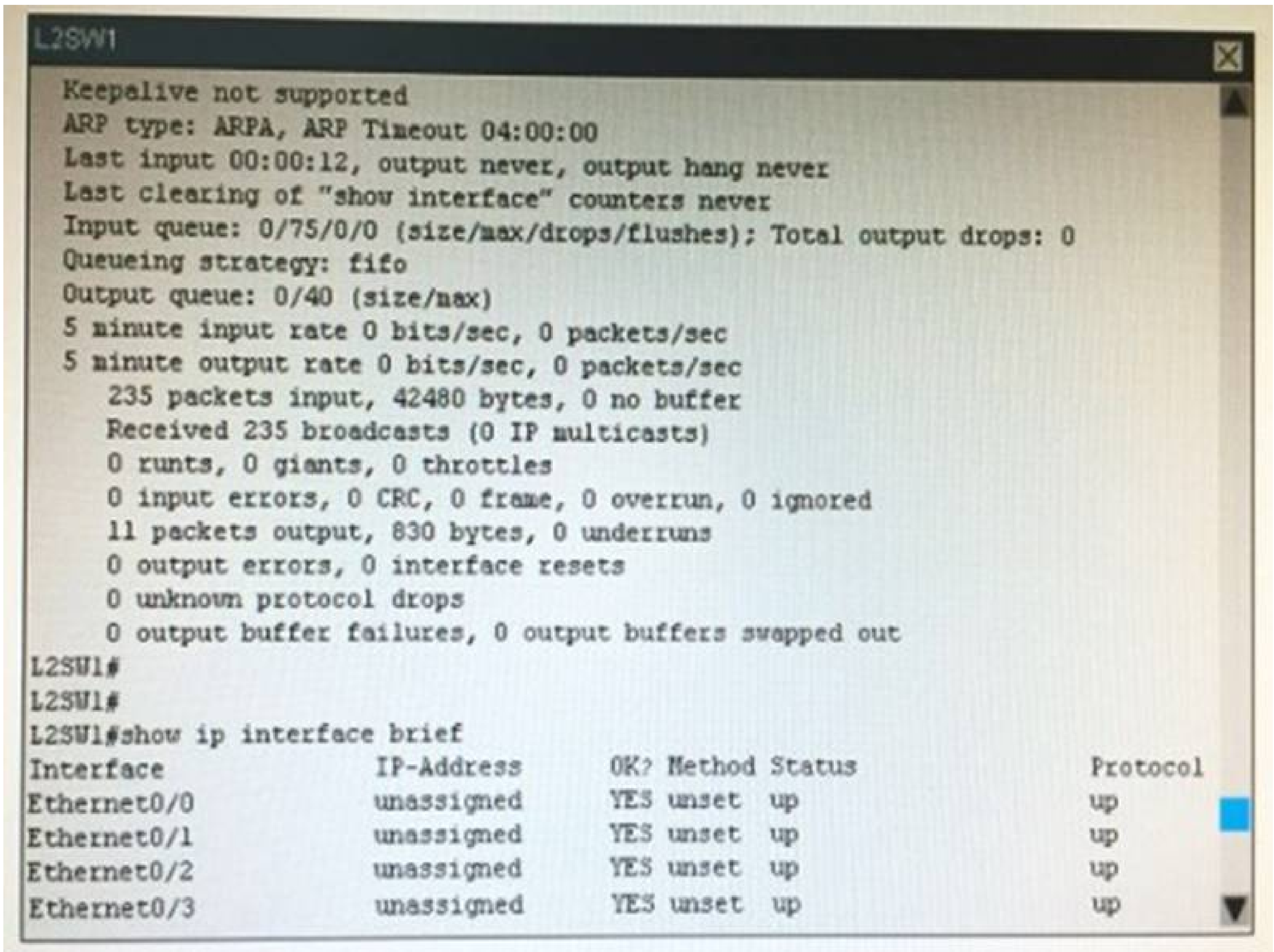
```
     755 packets input, 80219 bytes, 0 no buffer
     Received 123 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     3867 packets output, 268544 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/2 is up, line protocol is up (connected)
  Hardware is AmdP2, address is aabb.cc00.4520 (bia aabb.cc00.4520)
  Description: ***Link to Server2 Segment***
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is unknown
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:07, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 5/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```



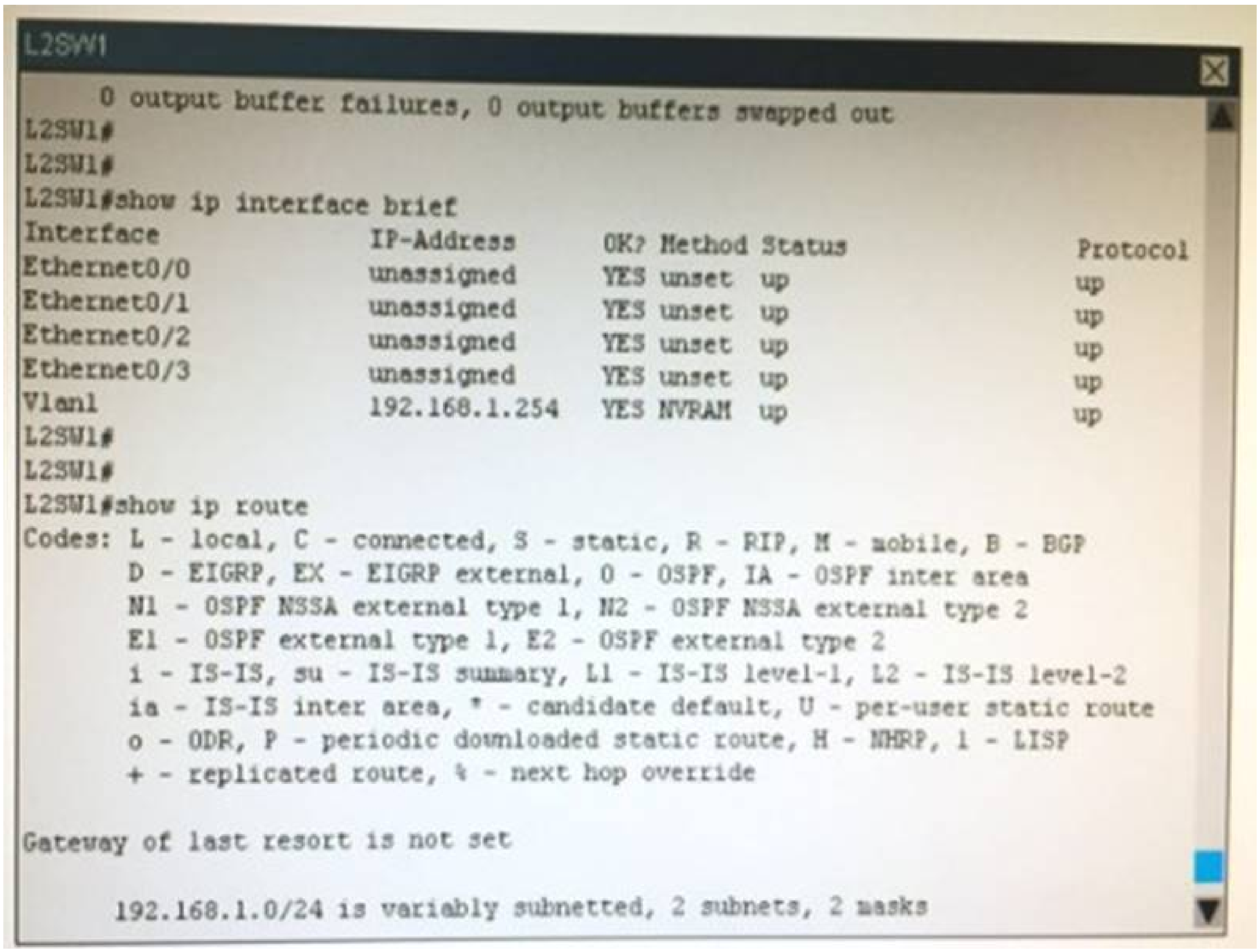
```
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     758 packets input, 81010 bytes, 0 no buffer
     Received 125 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     3867 packets output, 268544 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/3 is up, line protocol is up (connected)
  Hardware is AmdP2, address is aabb.cc00.4530 (bia aabb.cc00.4530)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is unknown
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
```



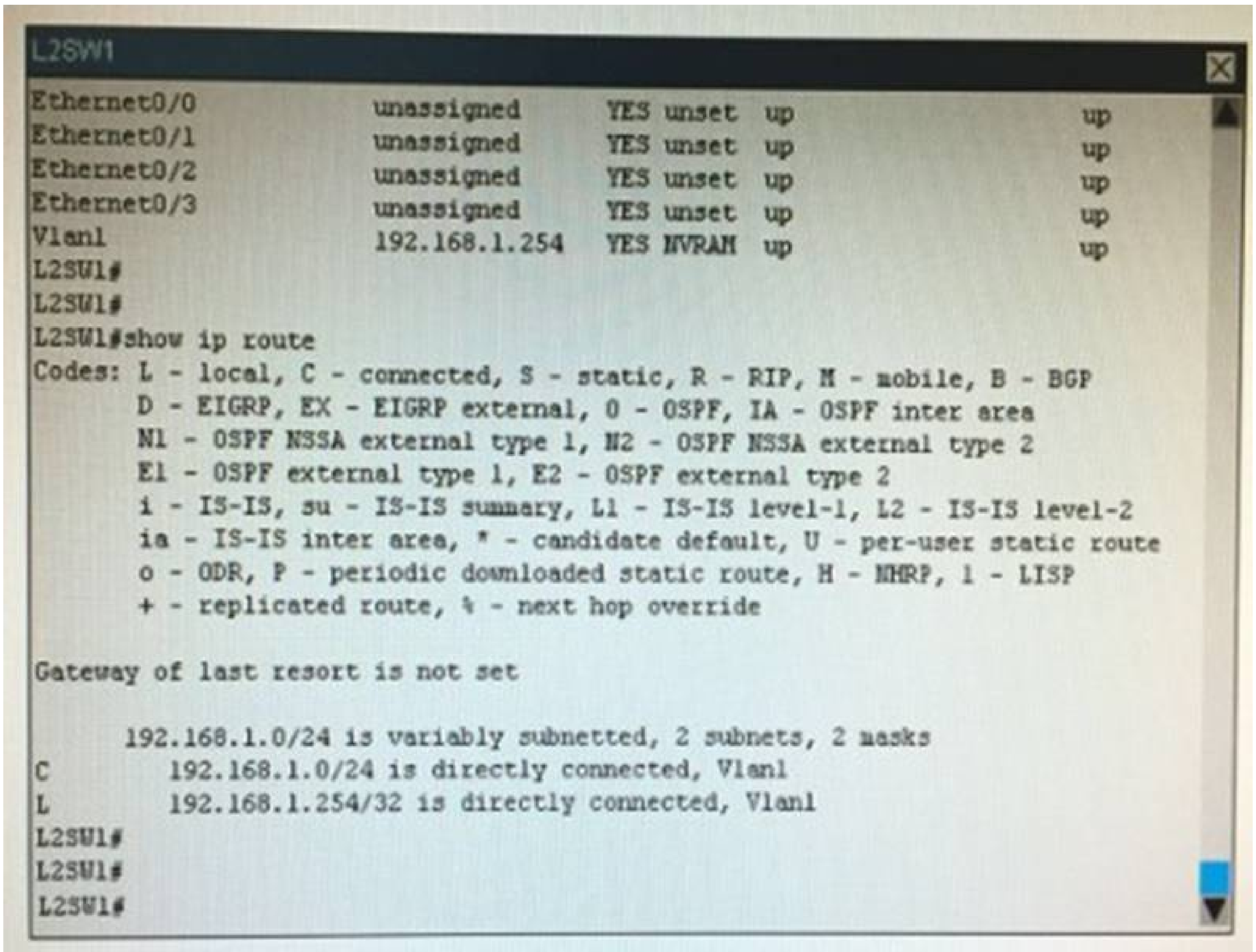
```
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     3566 packets output, 252186 bytes, 0 underruns
     0 output errors, 0 collisions, 55 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Vlan1 is up, line protocol is up
  Hardware is Ethernet SVI, address is aabb.cc80.4500 (bia aabb.cc80.4500)
  Internet address is 192.168.1.254/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
```



```
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:12, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     235 packets input, 42480 bytes, 0 no buffer
     Received 235 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     11 packets output, 830 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
L2SW1#
L2SW1#
L2SW1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
```



```
     0 output buffer failures, 0 output buffers swapped out
L2SW1#
L2SW1#
L2SW1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Vlan1                  192.168.1.254   YES NVRAM  up                    up
L2SW1#
L2SW1#
L2SW1#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
```



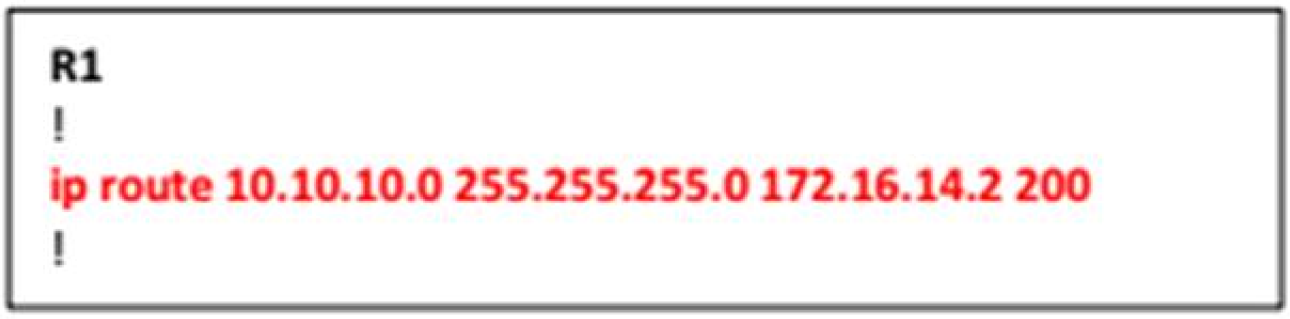
```
Ethernet0/0              unassigned      YES unset  up                    up
Ethernet0/1              unassigned      YES unset  up                    up
Ethernet0/2              unassigned      YES unset  up                    up
Ethernet0/3              unassigned      YES unset  up                    up
Vlan1                    192.168.1.254   YES NVRAM  up                    up
L2SW1#
L2SW1#
L2SW1#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Vlan1
L        192.168.1.254/32 is directly connected, Vlan1
L2SW1#
L2SW1#
L2SW1#
```

What is the correct statement below after examining the R1 routing table?

A. Traffic that is destined to 10.10.10.0/24 from R1 LAN network uses static route instead RIPv2 Because the static route AD that is configured is less than the AD of RIPv2
B. Traffic that is destined to 10.10.10.0/24 from R1 LAN network uses RIPv2 instead static route Because the static route AD that is configured is higher than the AD of RIPv2
C. Traffic that is destined to 10.10.10.0/24 from R1 LAN network uses static route instead RIPv2 But the traffic is forwarded to the ISP instead of the internal network.
D. Traffic that is destined to 10.10.10.0/24 from R1 LAN network uses RIPv2 instead static route Because the static route AD that is configured is 255

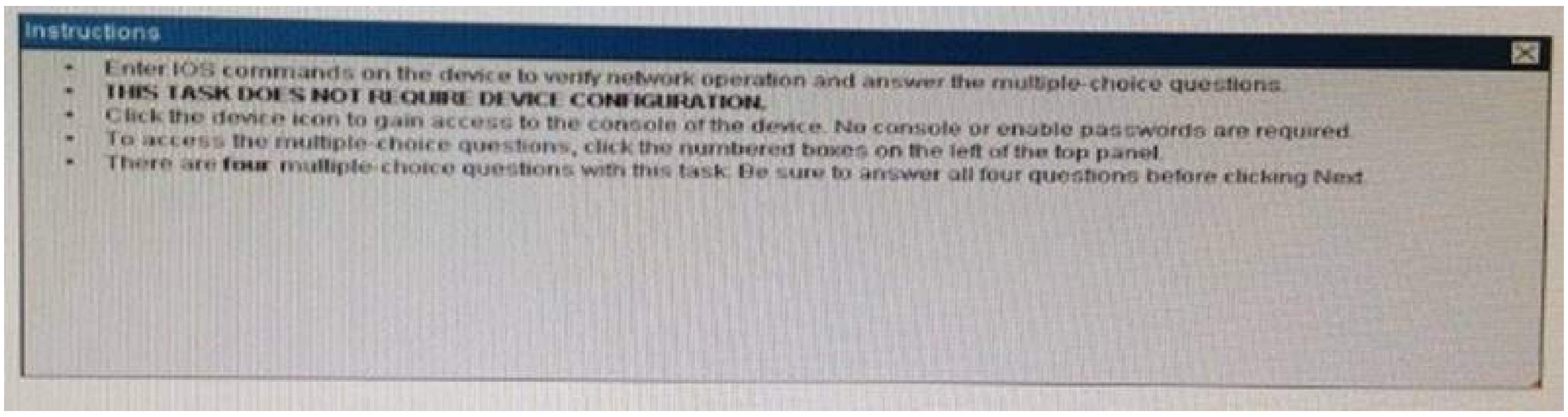
**Answer:** B

**Explanation:** Configuration are below for the answer.



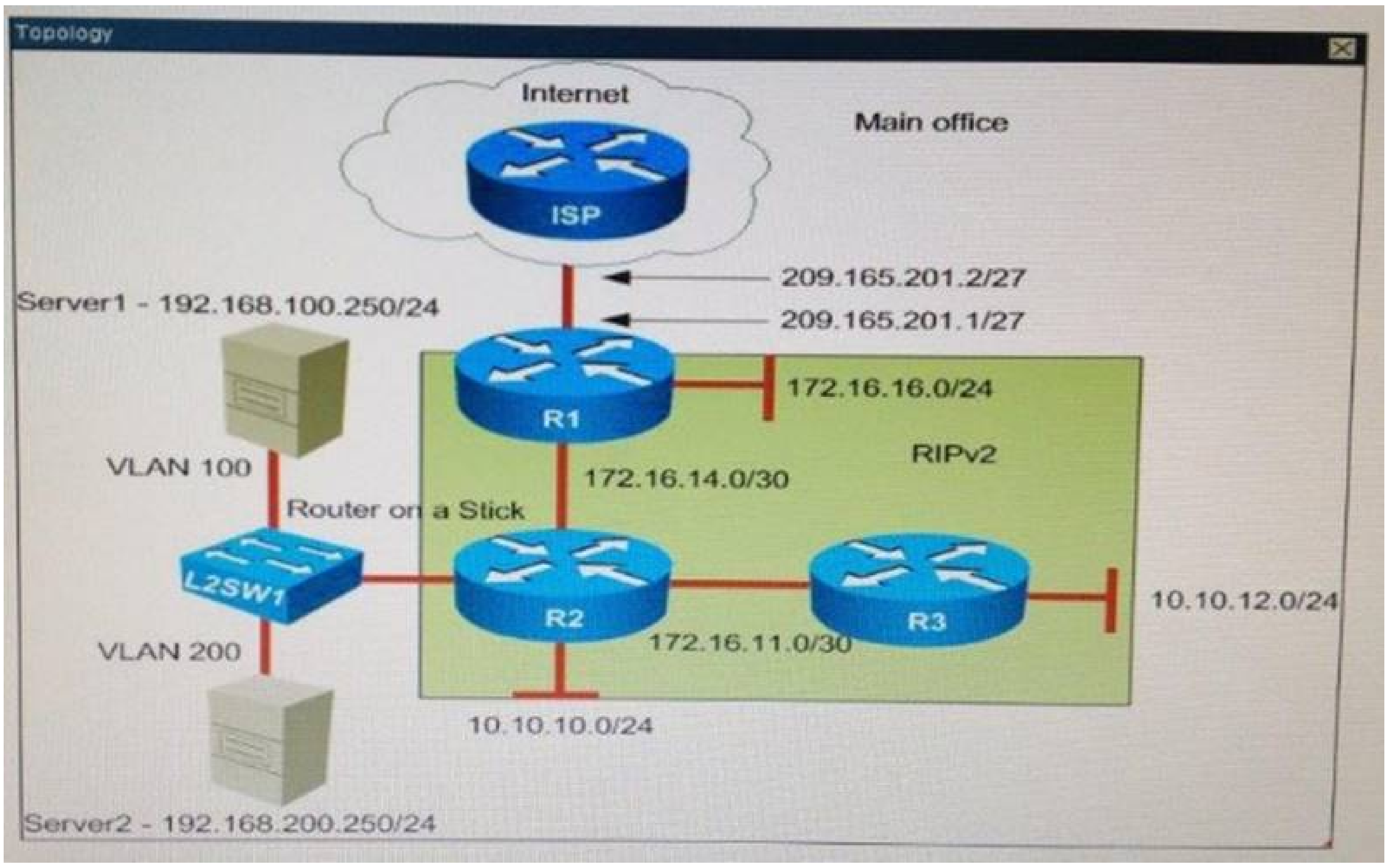
```
R1
!
ip route 10.10.10.0 255.255.255.0 172.16.14.2 200
!
```

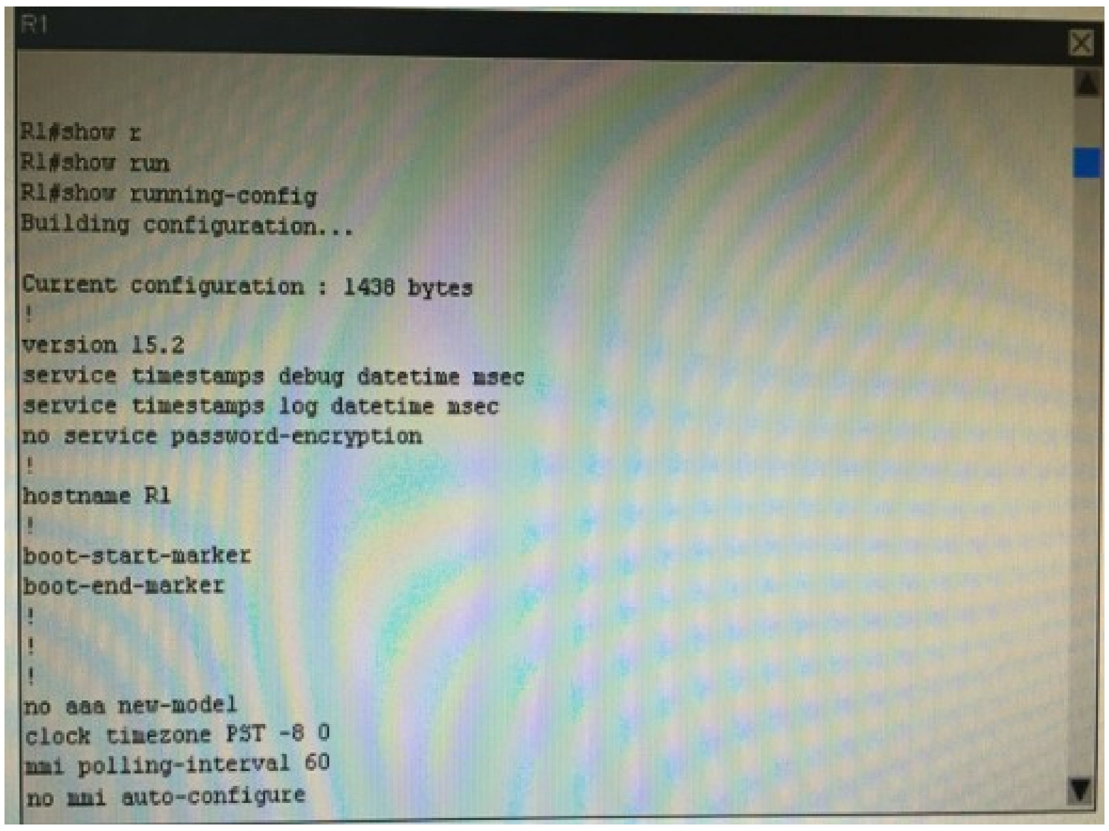
**NEW QUESTION 335**
Scenario:
You work for a company that provides managed network services, and of your real estate clients running a small office is experiencing network issues, Troubleshoot the network issues.
Router R1 connects the main office to internet, and routers R2 and R3 are internal routers NAT is enabled on Router R1.
The routing protocol that is enable between routers R1, R2, and R3 is RIPv2.
R1 sends default route into RIPv2 for internal routers to forward internet traffic to R1.
Server1 and Server2 are placed in VLAN 100 and 200 respectively, and dare still running router on stick configuration with router R2.
You have console access on R1, R2, R3, and L2SW1 devices. Use only show commands to troubleshoot the issues.



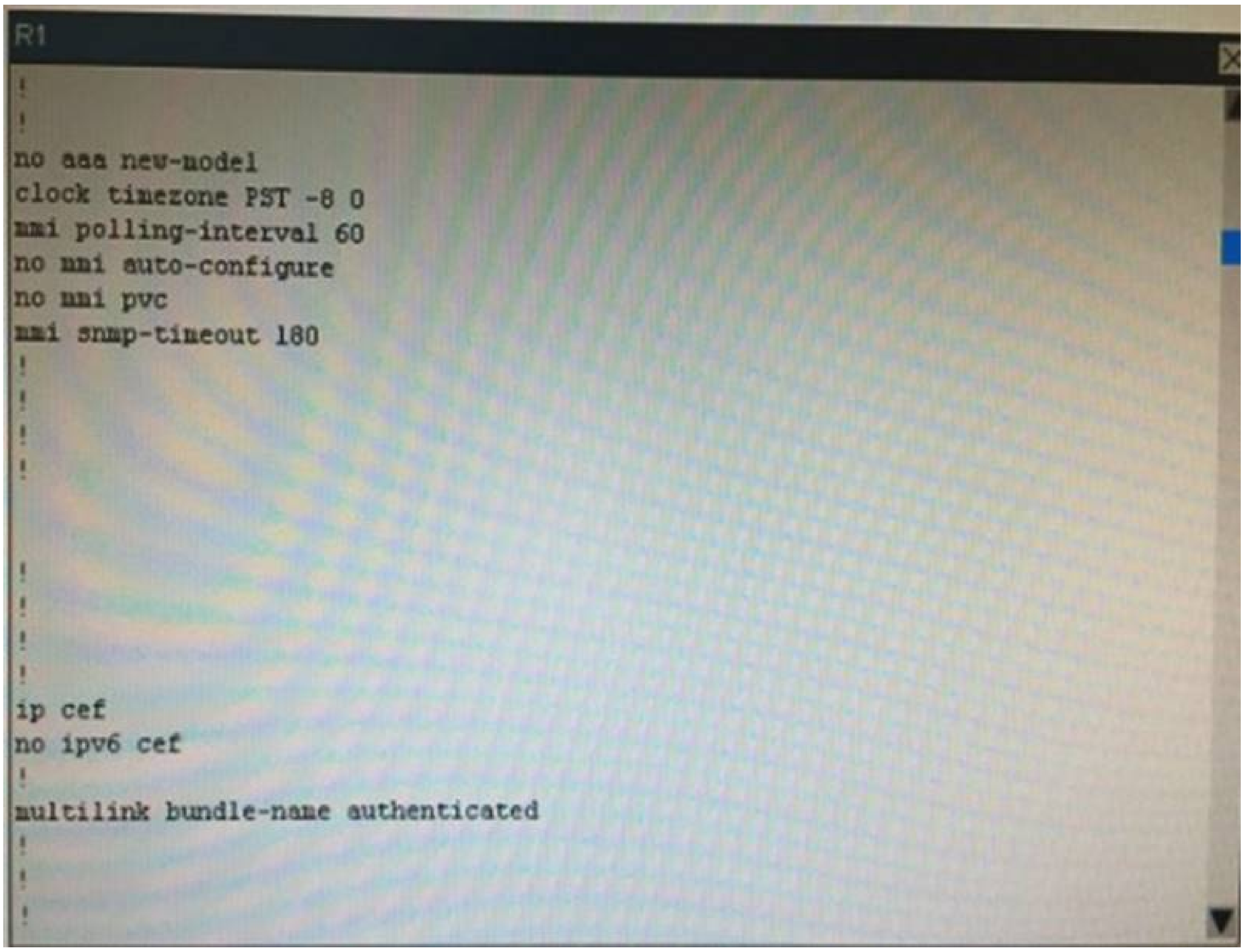
Instructions

- Enter IOS commands on the device to verify network operation and answer the multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click the device icon to gain access to the console of the device. No console or enable passwords are required.
- To access the multiple-choice questions, click the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before clicking Next.

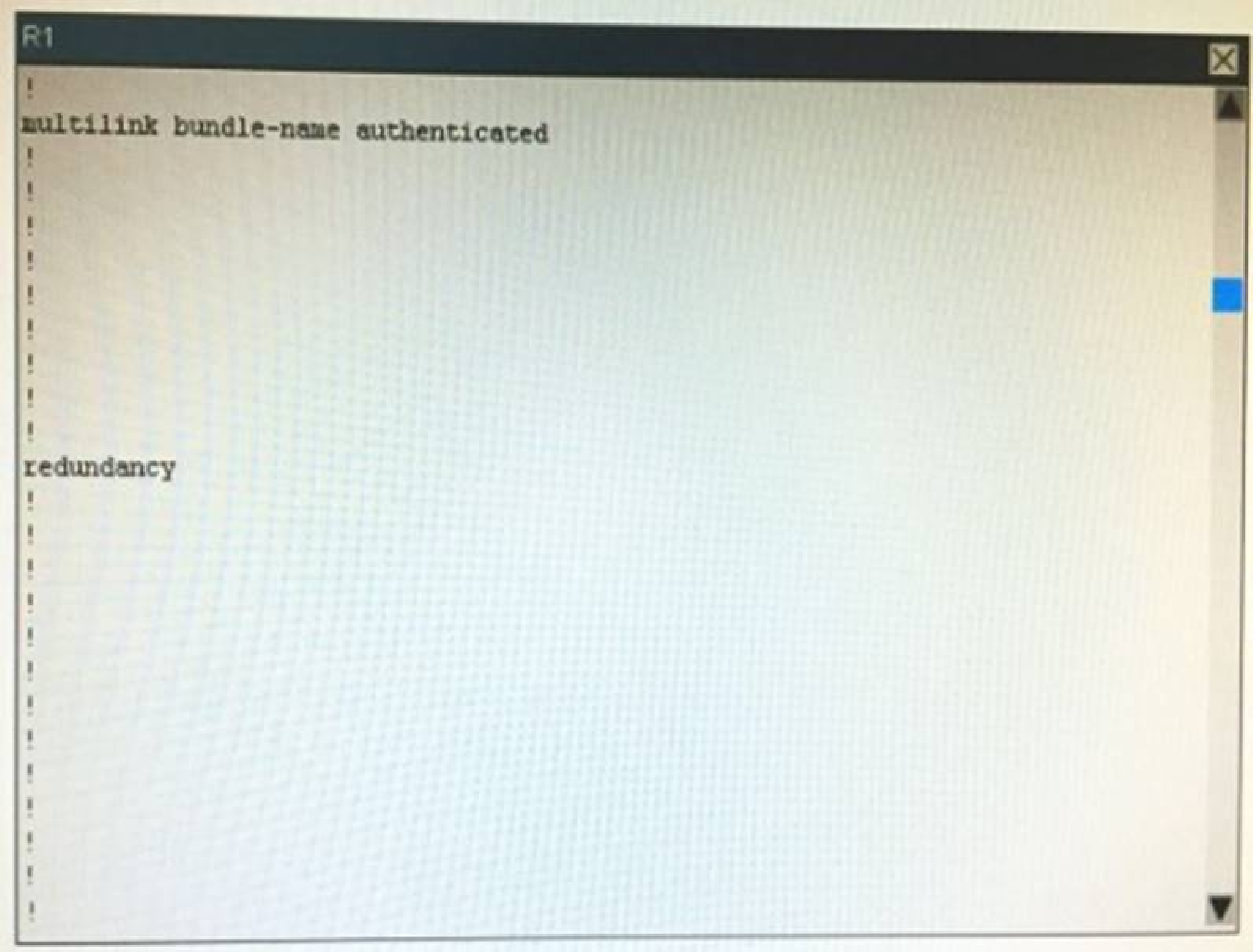




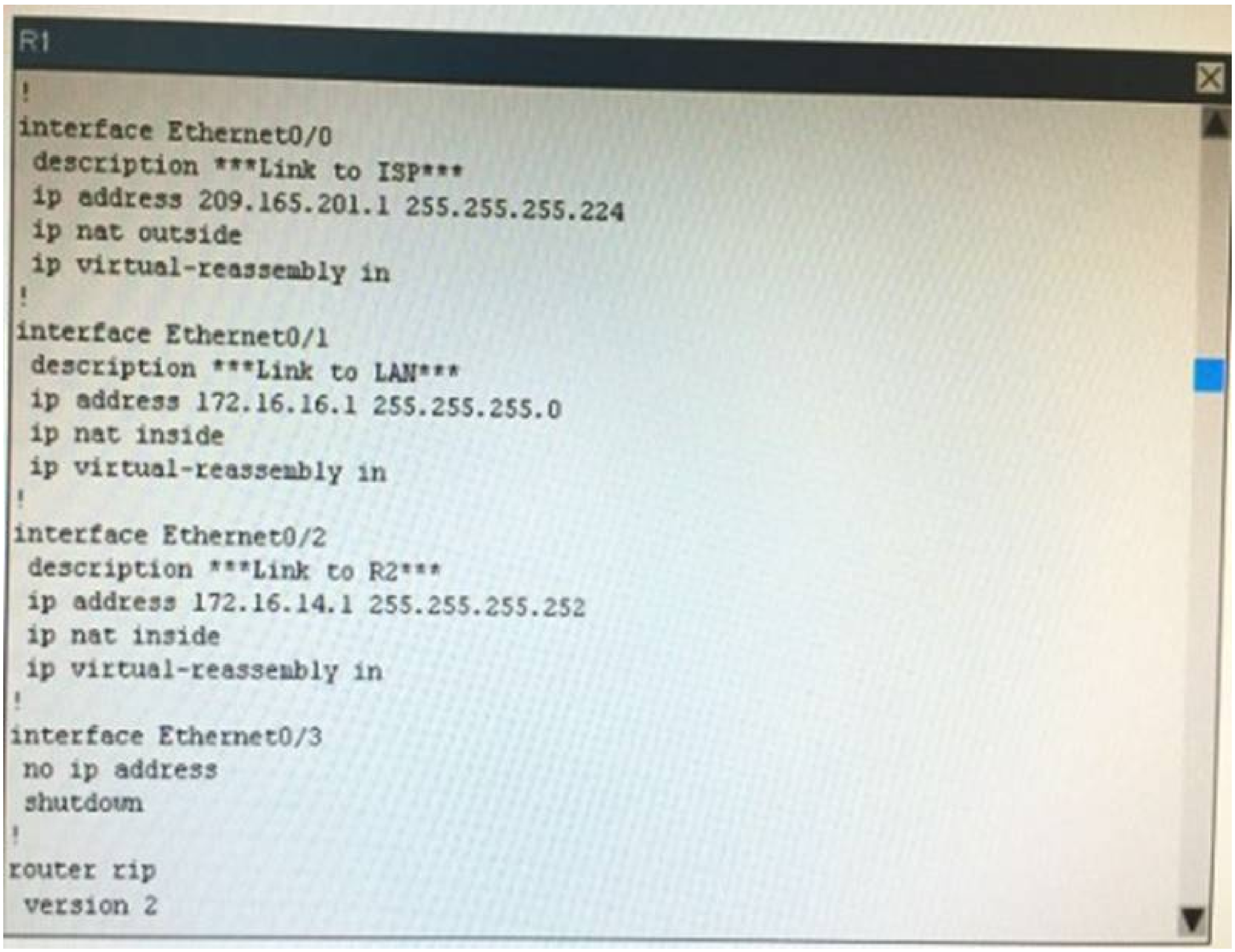
```
R1#show r
R1#show run
R1#show running-config
Building configuration...

Current configuration : 1438 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
```



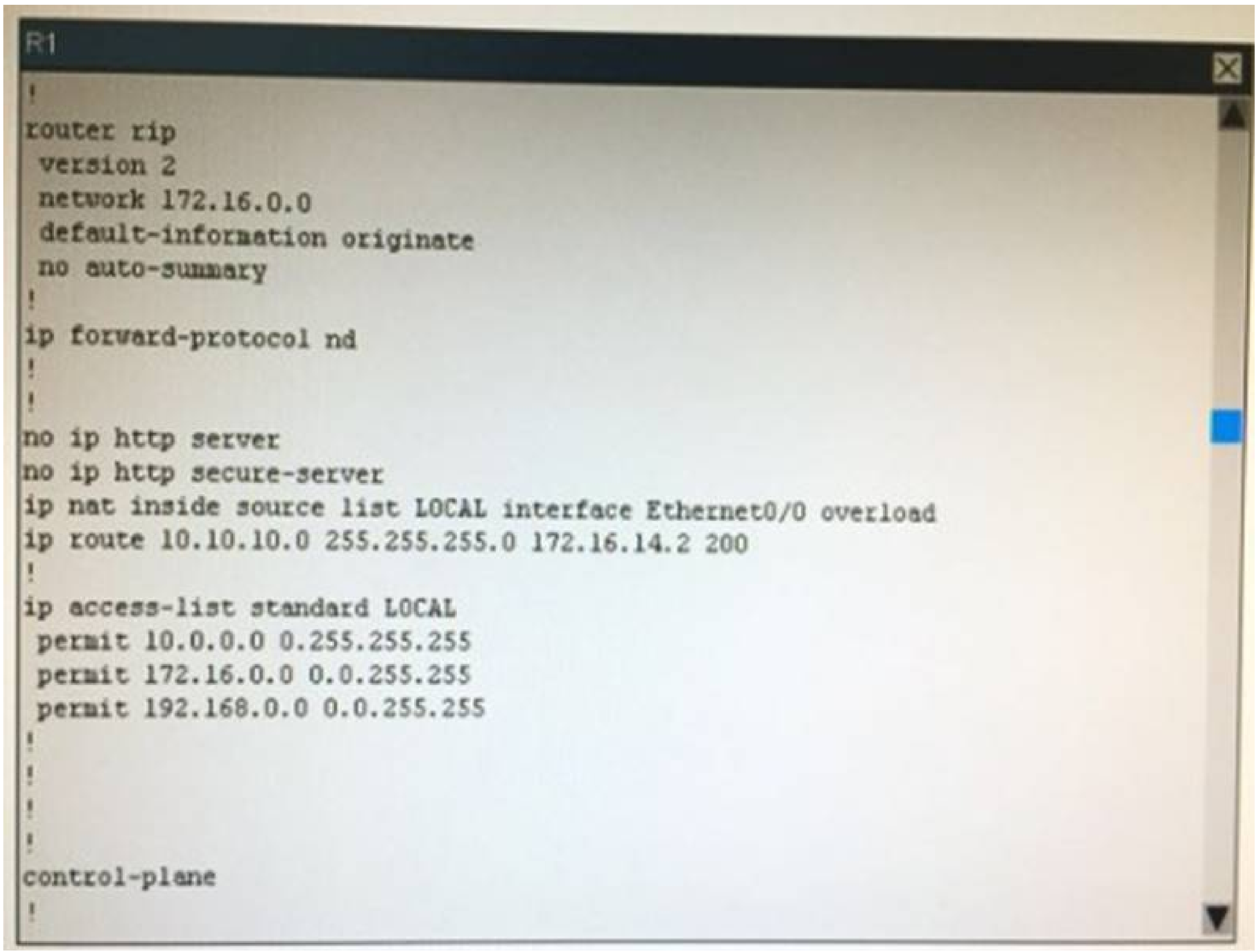
```
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!


!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
```



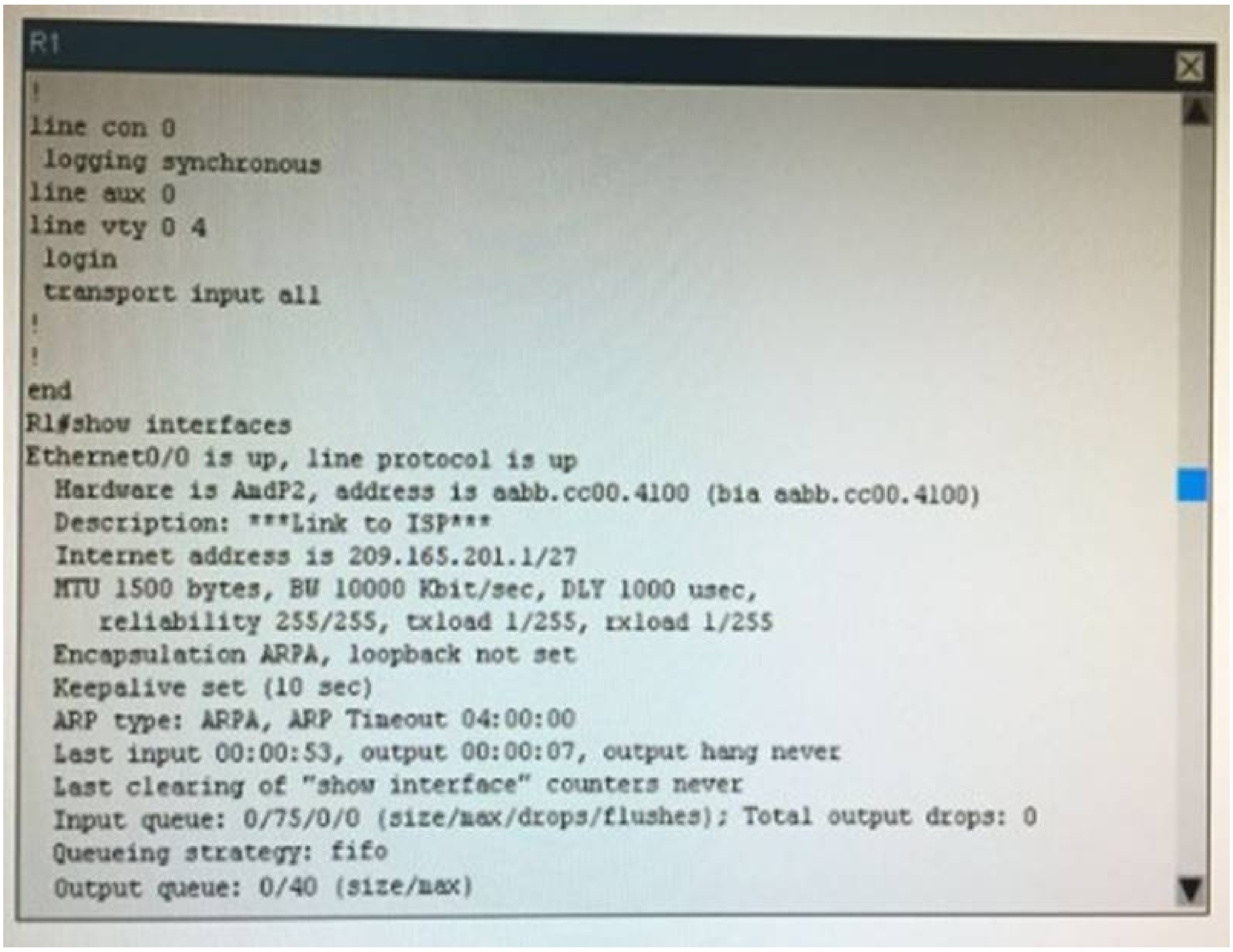
```
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
```



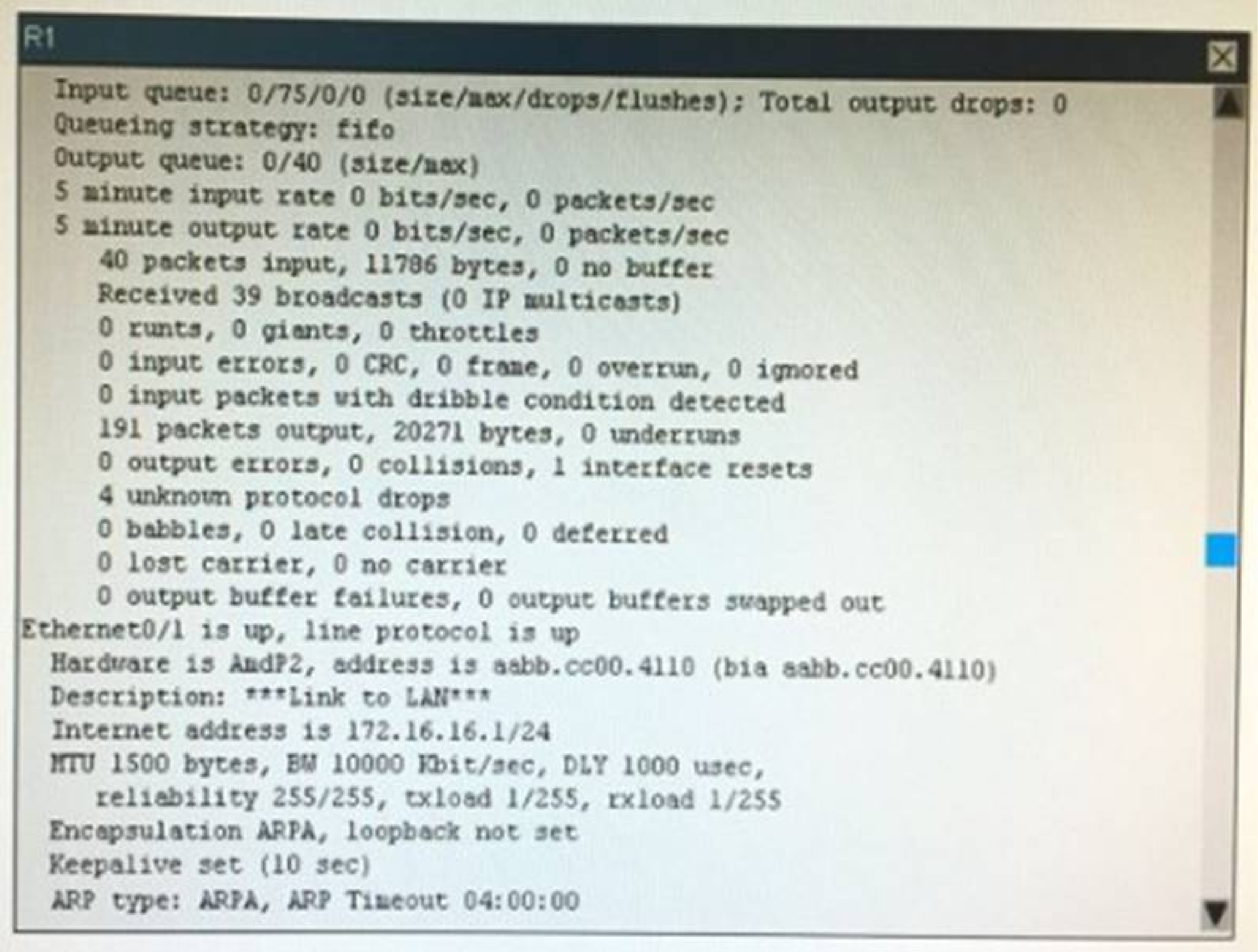
```
!
interface Ethernet0/0
 description ***Link to ISP***
 ip address 209.165.201.1 255.255.255.224
 ip nat outside
 ip virtual-reassembly in
!
interface Ethernet0/1
 description ***Link to LAN***
 ip address 172.16.16.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/2
 description ***Link to R2***
 ip address 172.16.14.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
```



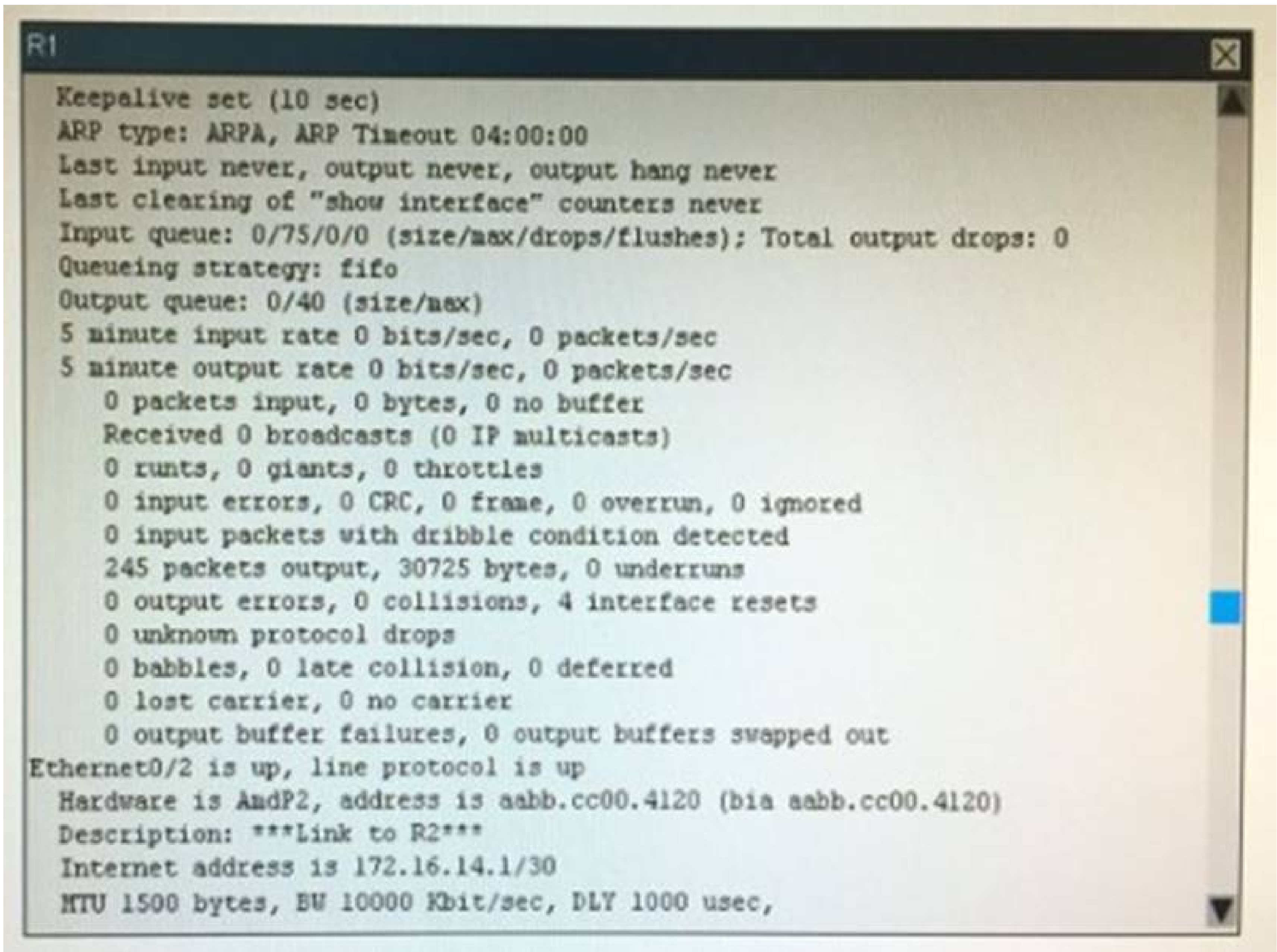
```
!
router rip
 version 2
 network 172.16.0.0
 default-information originate
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip nat inside source list LOCAL interface Ethernet0/0 overload
ip route 10.10.10.0 255.255.255.0 172.16.14.2 200
!
ip access-list standard LOCAL
 permit 10.0.0.0 0.255.255.255
 permit 172.16.0.0 0.0.255.255
 permit 192.168.0.0 0.0.255.255
!
!
!
!
control-plane
!
```



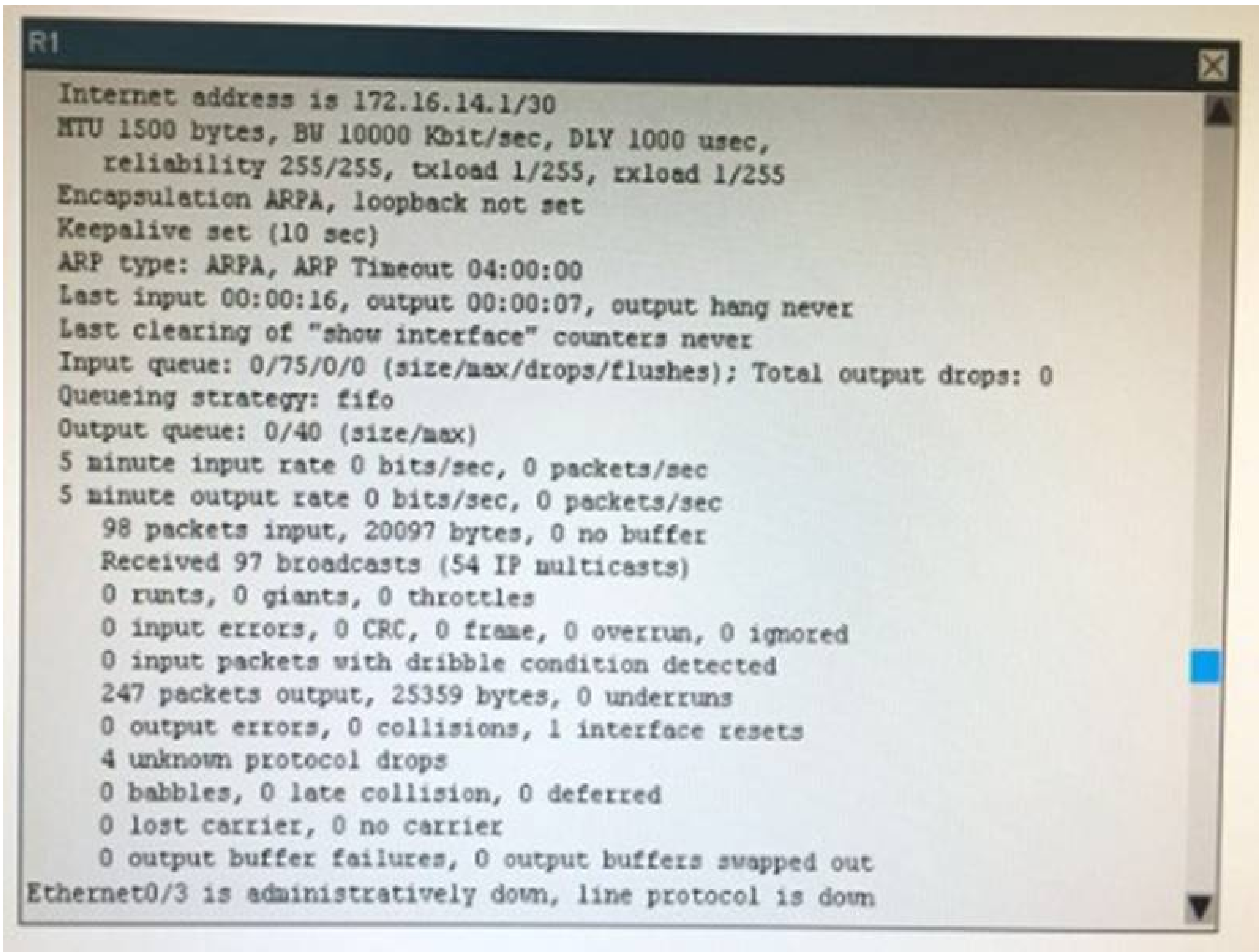
```
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
!
end
R1#show interfaces
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4100 (bia aabb.cc00.4100)
  Description: ***Link to ISP***
  Internet address is 209.165.201.1/27
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:53, output 00:00:07, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
```



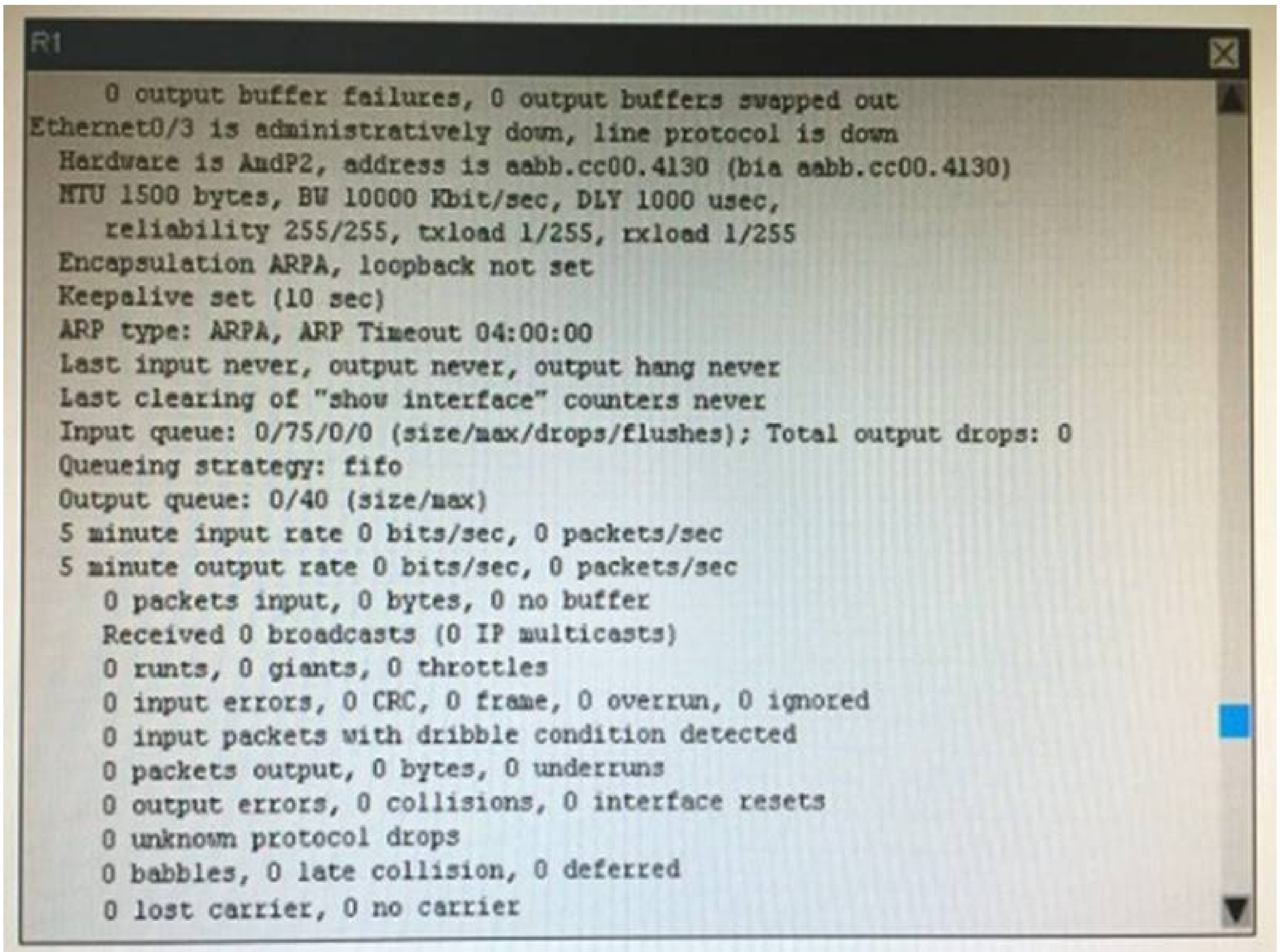
```
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     40 packets input, 11786 bytes, 0 no buffer
     Received 39 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     191 packets output, 20271 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     4 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/1 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4110 (bia aabb.cc00.4110)
  Description: ***Link to LAN***
  Internet address is 172.16.16.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
```



```
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     245 packets output, 30725 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/2 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4120 (bia aabb.cc00.4120)
  Description: ***Link to R2***
  Internet address is 172.16.14.1/30
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
```

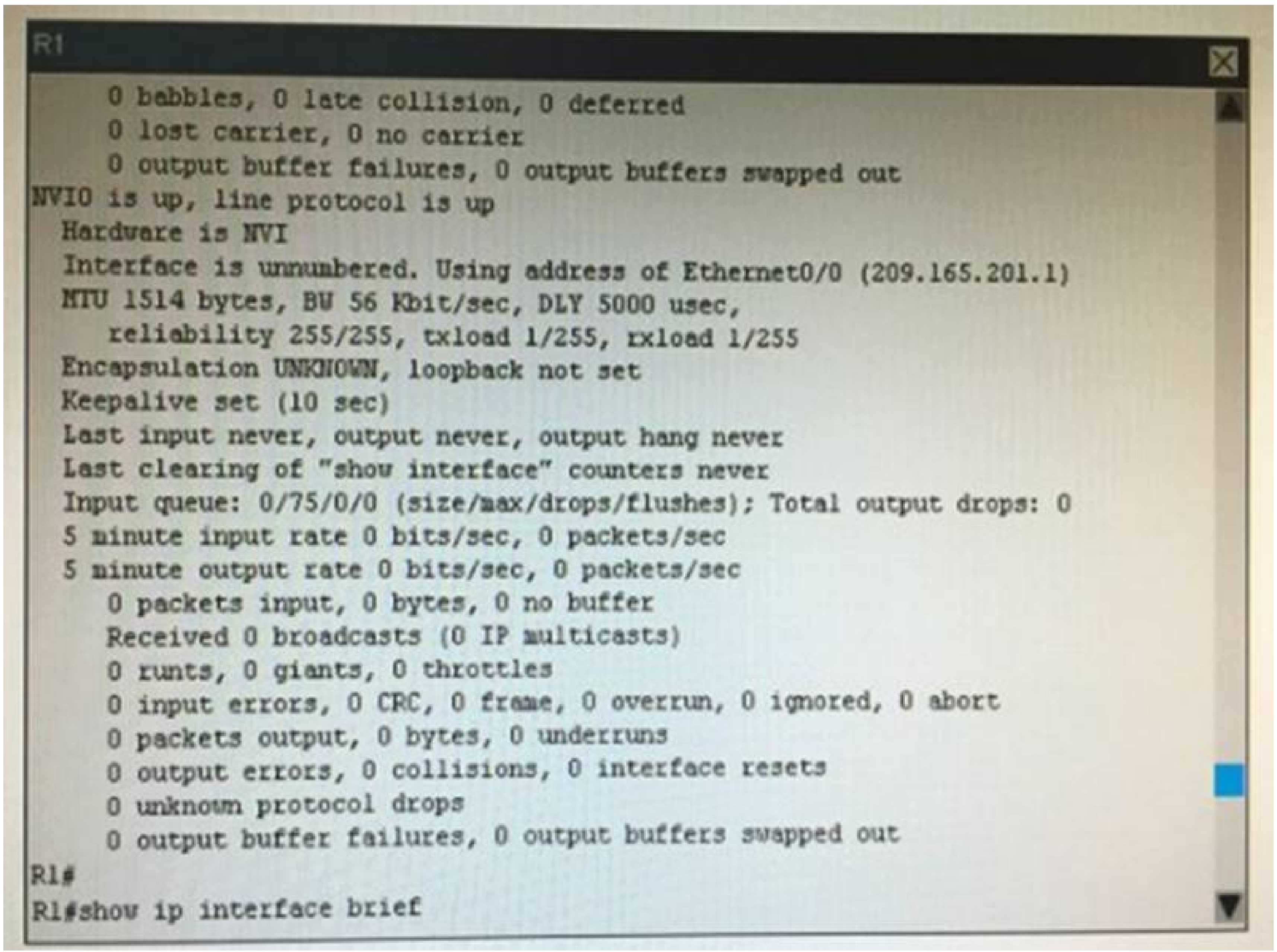


```
  Internet address is 172.16.14.1/30
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:16, output 00:00:07, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     98 packets input, 20097 bytes, 0 no buffer
     Received 97 broadcasts (54 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     247 packets output, 25359 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     4 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/3 is administratively down, line protocol is down
```



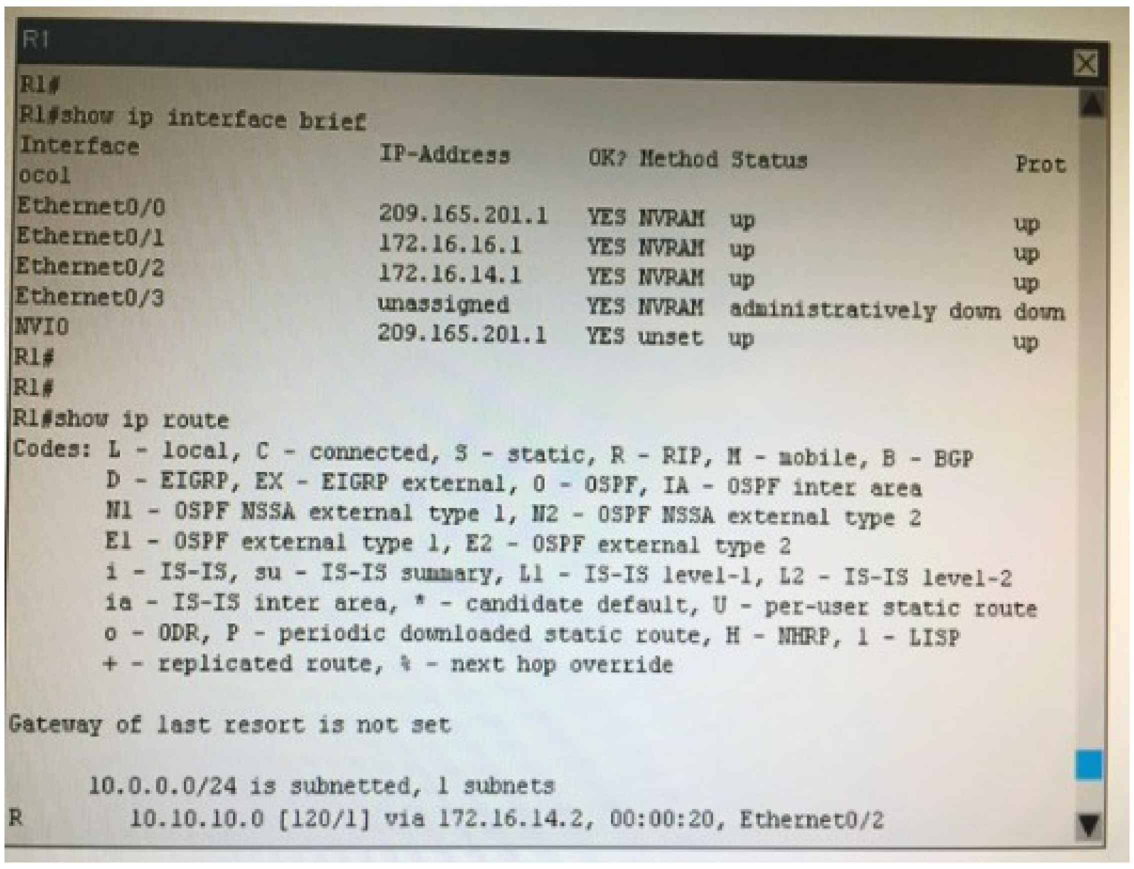
R1

```
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/3 is administratively down, line protocol is down
  Hardware is AmdP2, address is aabb.cc00.4130 (bia aabb.cc00.4130)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
```

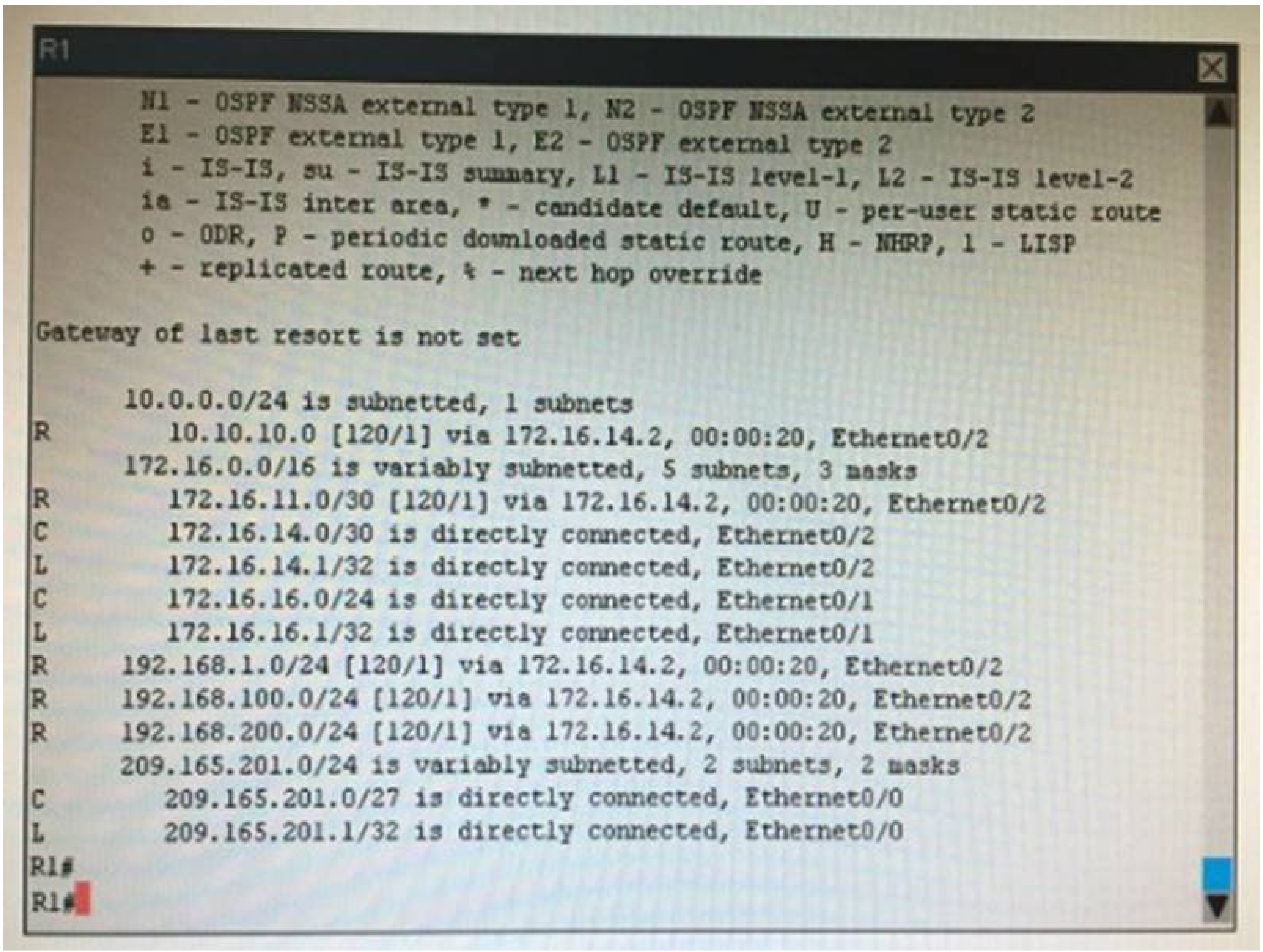


R1

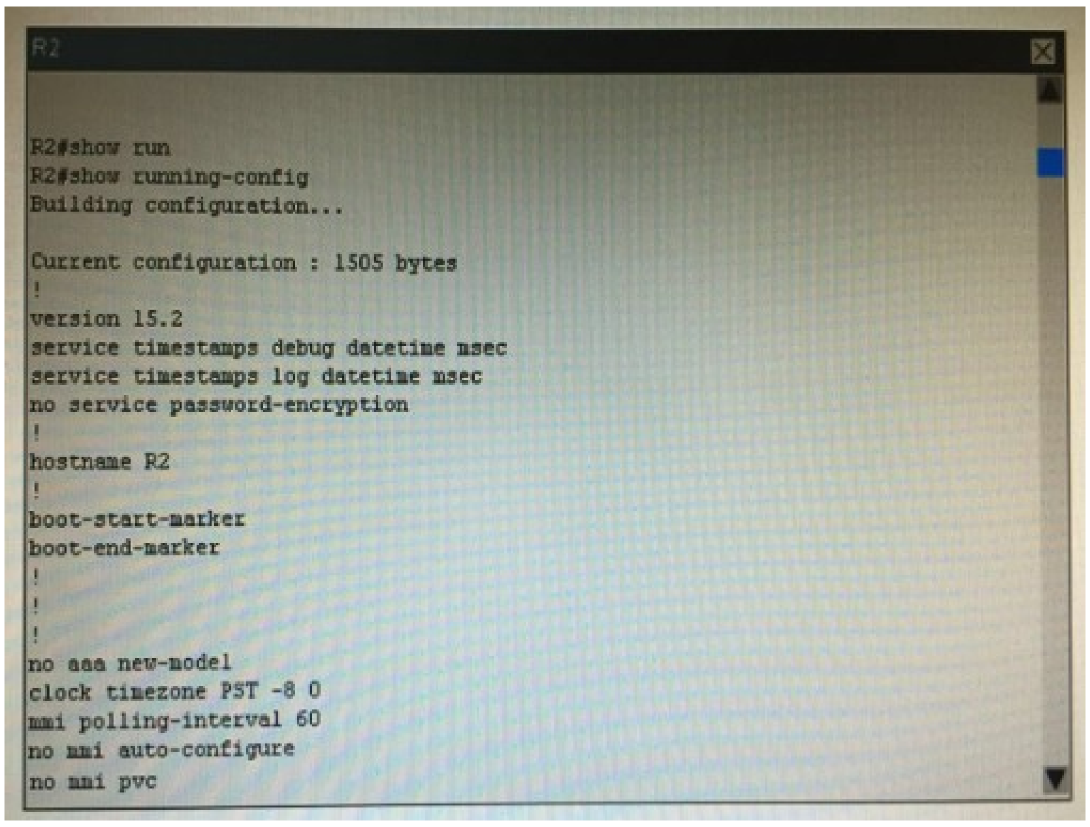
```
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
NVI0 is up, line protocol is up
  Hardware is NVI
  Interface is unnumbered. Using address of Ethernet0/0 (209.165.201.1)
  MTU 1514 bytes, BW 56 Kbit/sec, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation UNKNOWN, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
R1#
R1#show ip interface brief
```



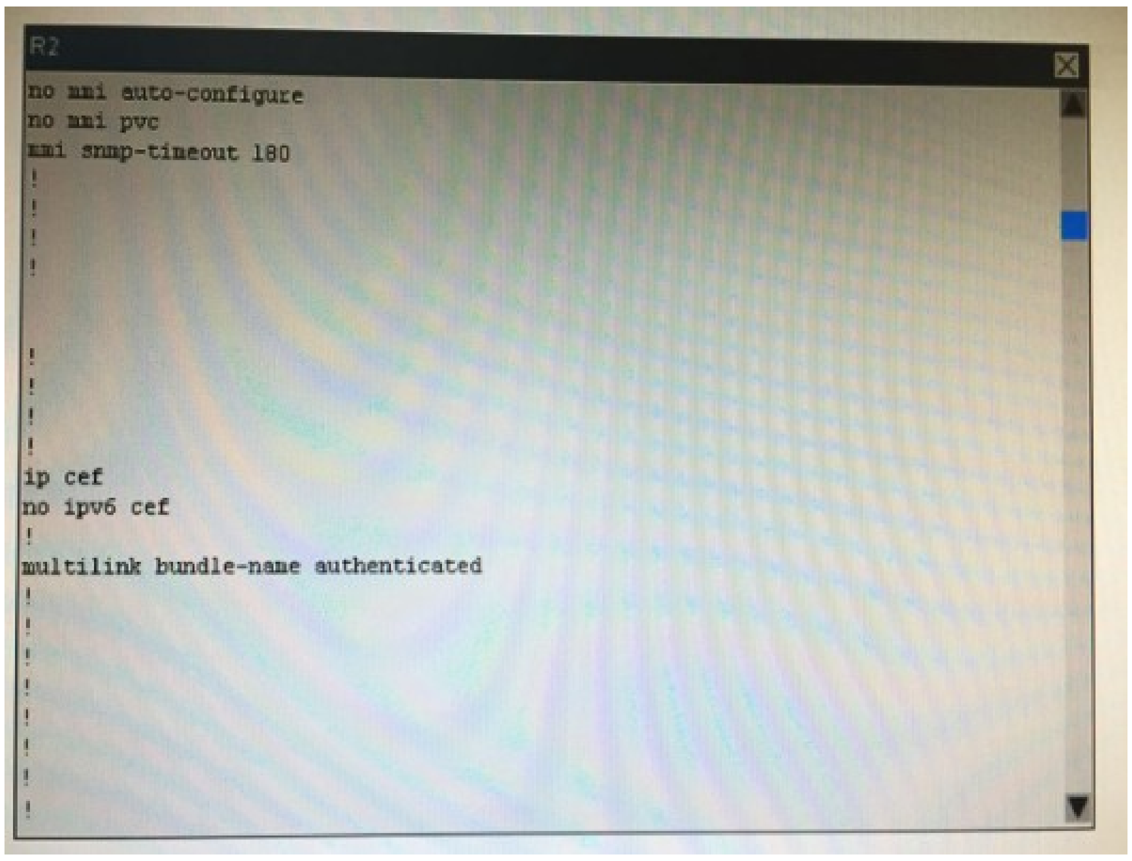
```
R1#
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
Ethernet0/0                209.165.201.1   YES NVRAM  up                    up
Ethernet0/1                172.16.16.1     YES NVRAM  up                    up
Ethernet0/2                172.16.14.1     YES NVRAM  up                    up
Ethernet0/3                unassigned      YES NVRAM  administratively down down
NVI0                       209.165.201.1   YES unset  up                    up
R1#
R1#
R1#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 1 subnets
R        10.10.10.0 [120/1] via 172.16.14.2, 00:00:20, Ethernet0/2
```



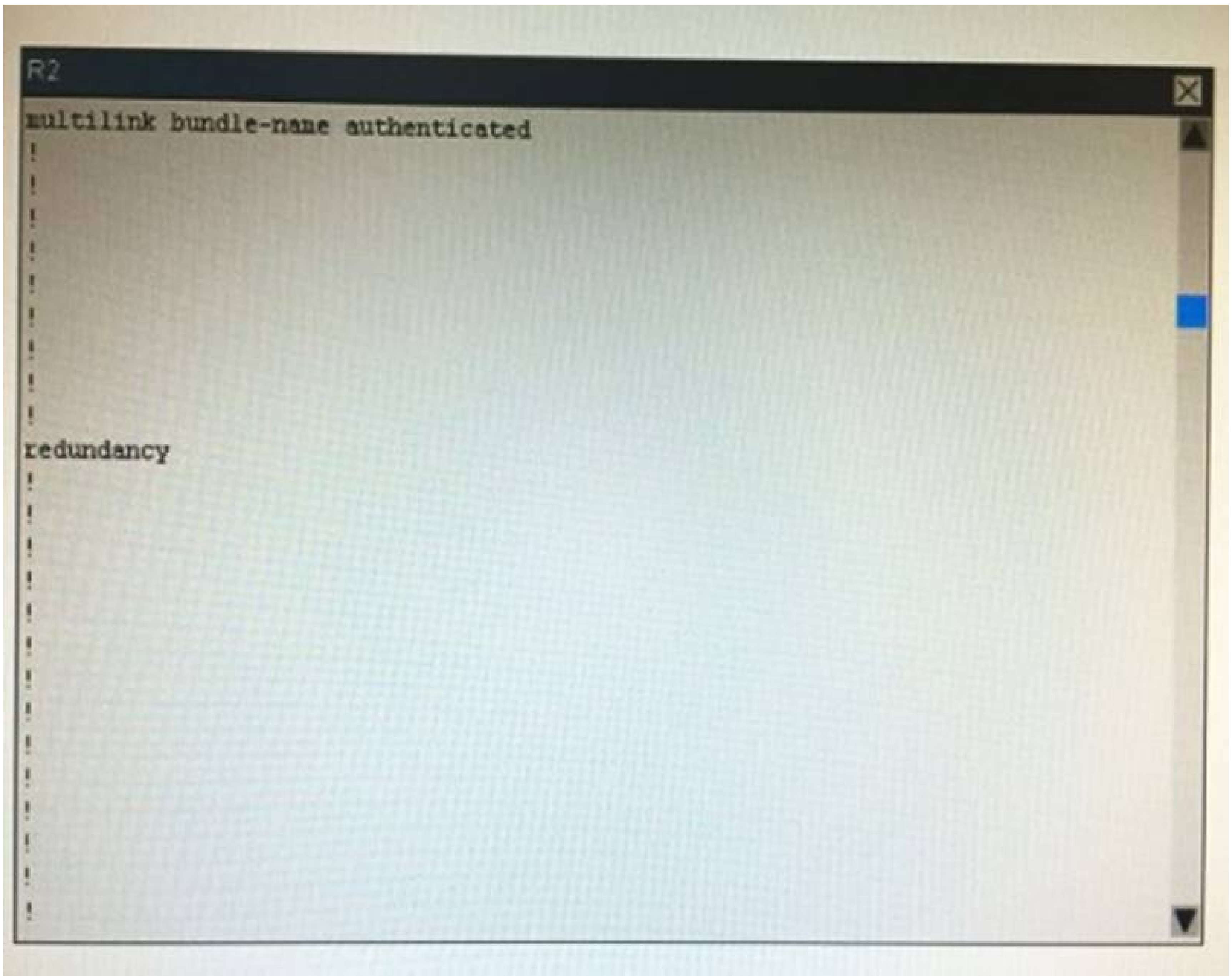
```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 1 subnets
R        10.10.10.0 [120/1] via 172.16.14.2, 00:00:20, Ethernet0/2
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
R        172.16.11.0/30 [120/1] via 172.16.14.2, 00:00:20, Ethernet0/2
C        172.16.14.0/30 is directly connected, Ethernet0/2
L        172.16.14.1/32 is directly connected, Ethernet0/2
C        172.16.16.0/24 is directly connected, Ethernet0/1
L        172.16.16.1/32 is directly connected, Ethernet0/1
R     192.168.1.0/24 [120/1] via 172.16.14.2, 00:00:20, Ethernet0/2
R     192.168.100.0/24 [120/1] via 172.16.14.2, 00:00:20, Ethernet0/2
R     192.168.200.0/24 [120/1] via 172.16.14.2, 00:00:20, Ethernet0/2
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.201.0/27 is directly connected, Ethernet0/0
L        209.165.201.1/32 is directly connected, Ethernet0/0
R1#
R1#
```



```
R2#show run
R2#show running-config
Building configuration...

Current configuration : 1505 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
```

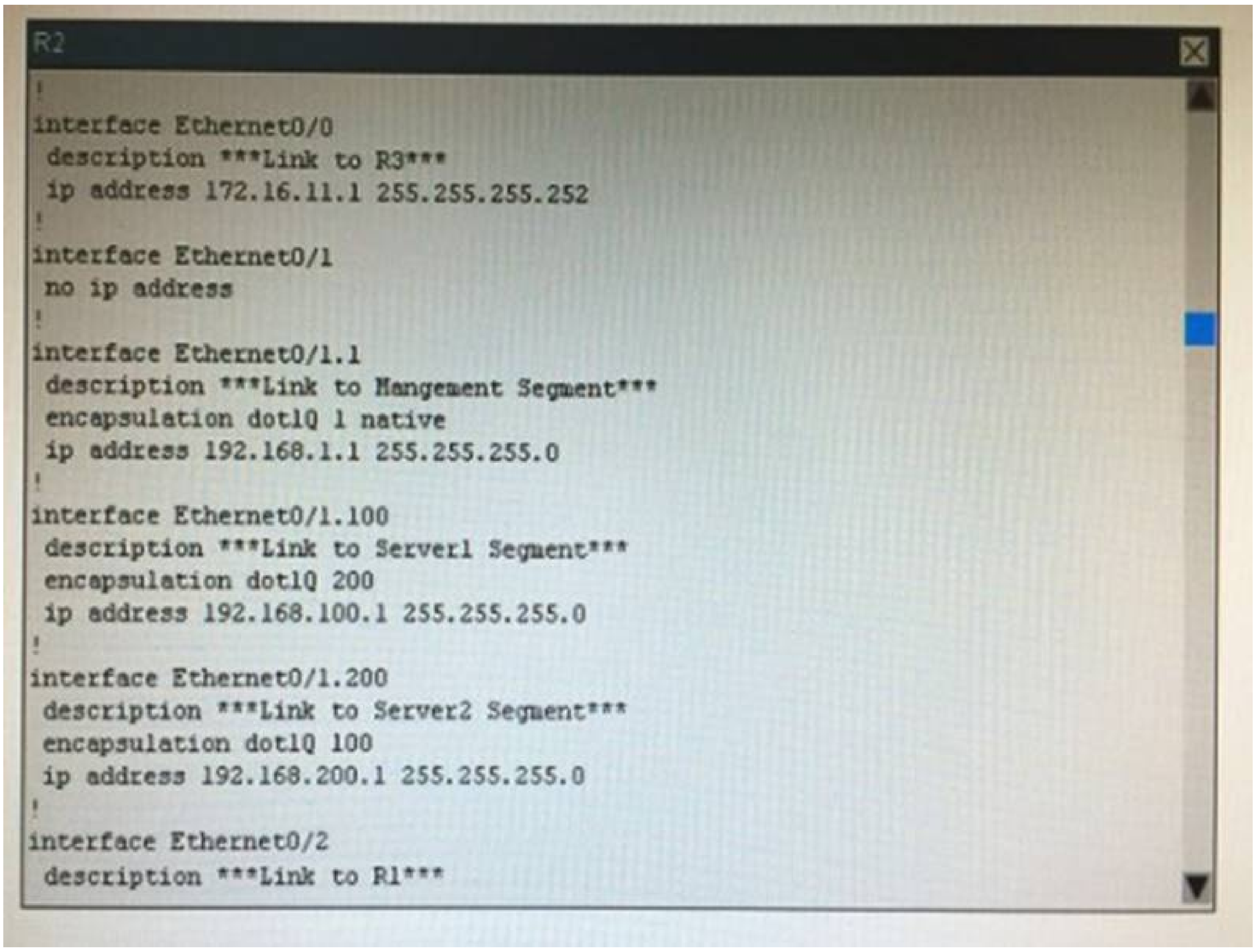


```
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!


!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
```



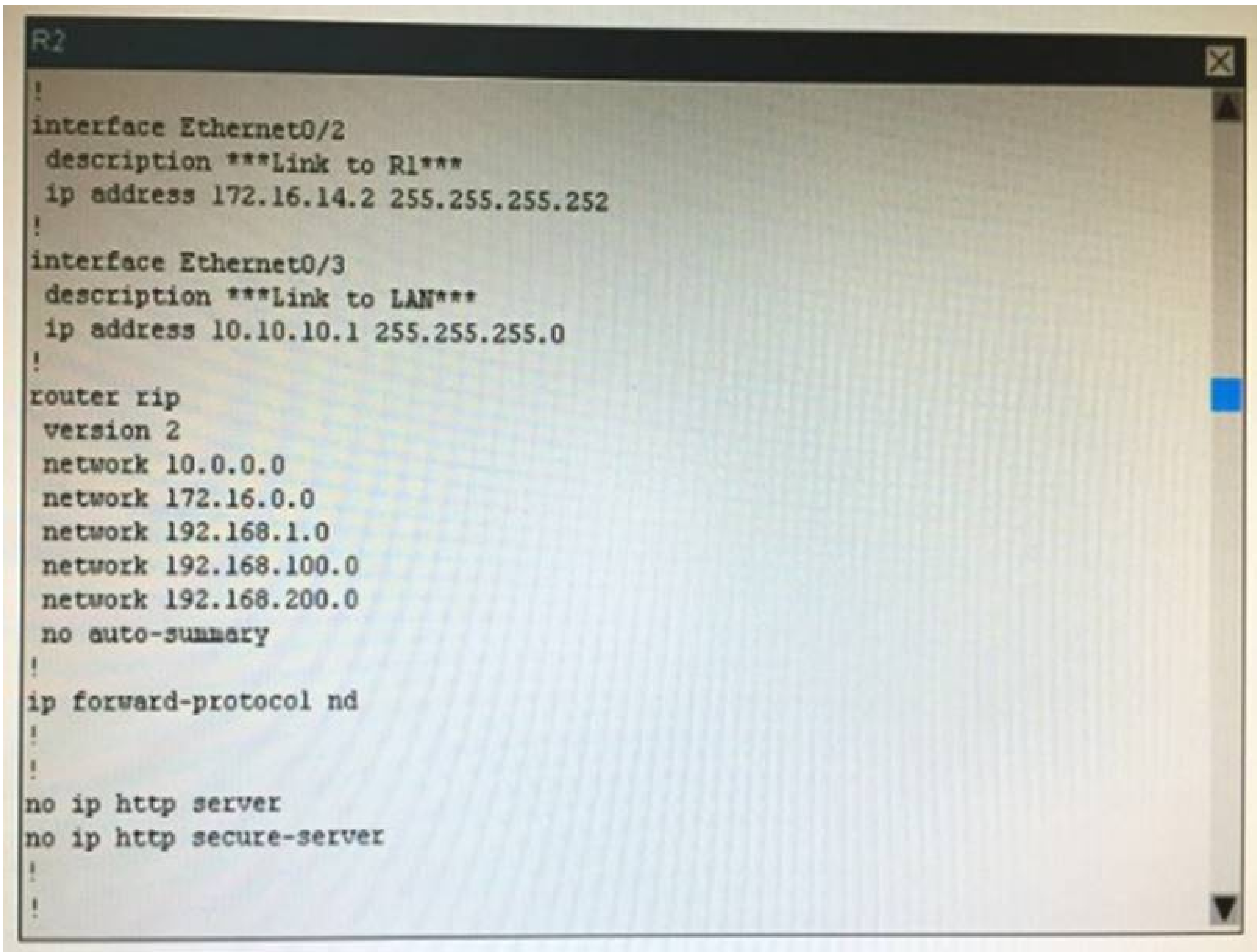
R2

```
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
```

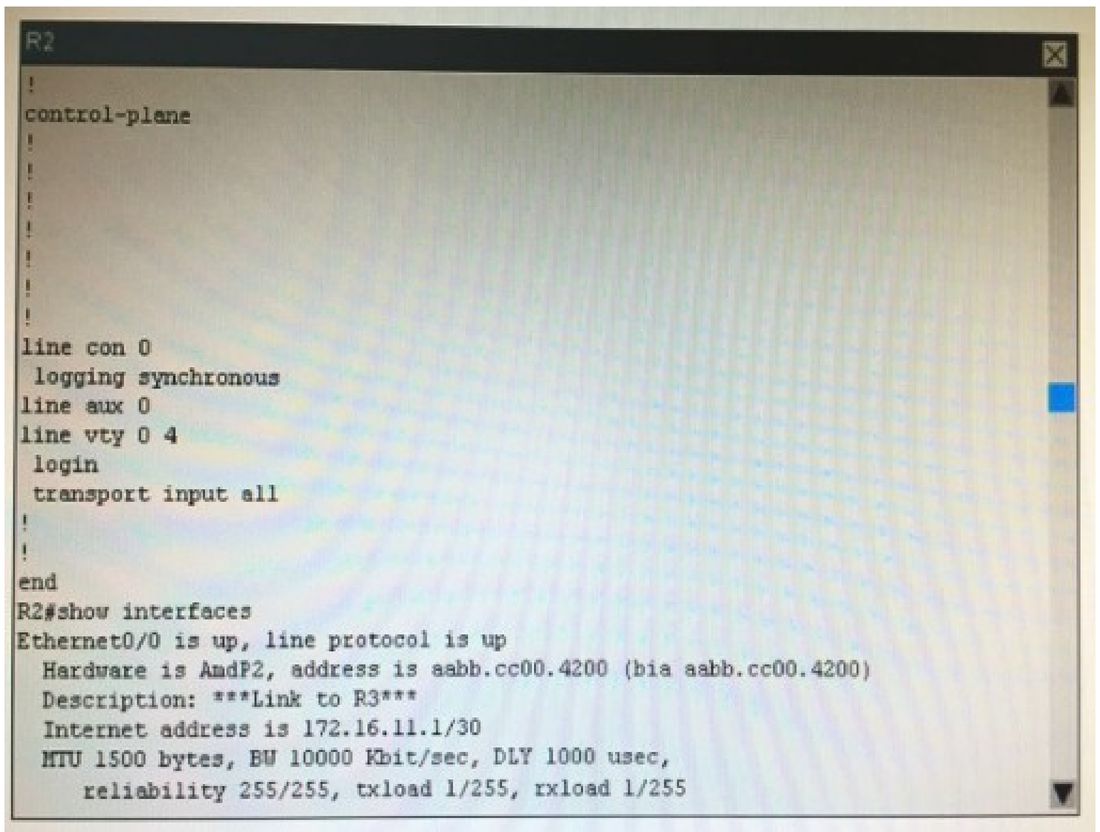


R2

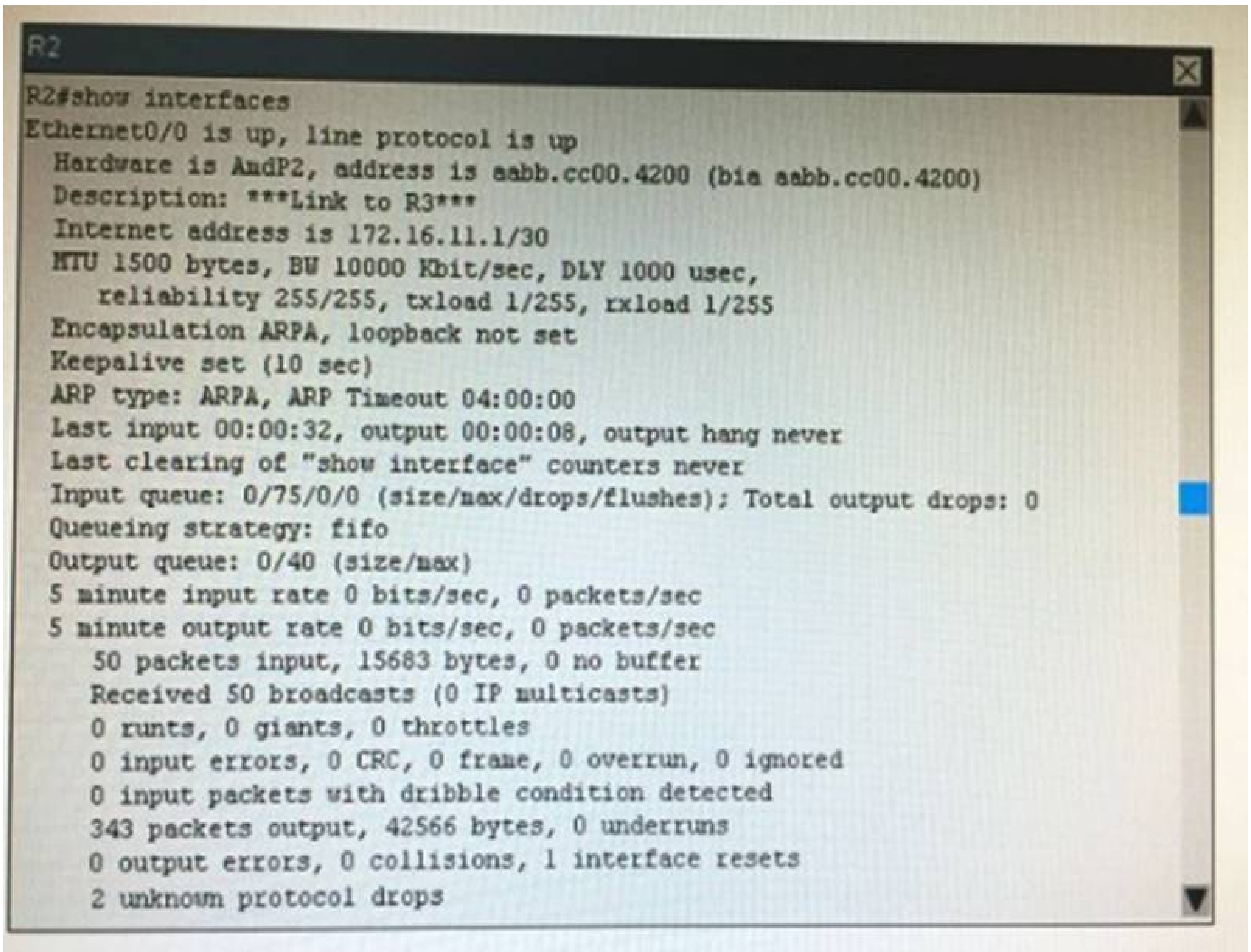
```
!
interface Ethernet0/0
 description ***Link to R3***
 ip address 172.16.11.1 255.255.255.252
!
interface Ethernet0/1
 no ip address
!
interface Ethernet0/1.1
 description ***Link to Mangement Segment***
 encapsulation dot1Q 1 native
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1.100
 description ***Link to Server1 Segment***
 encapsulation dot1Q 200
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/1.200
 description ***Link to Server2 Segment***
 encapsulation dot1Q 100
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet0/2
 description ***Link to R1***
```



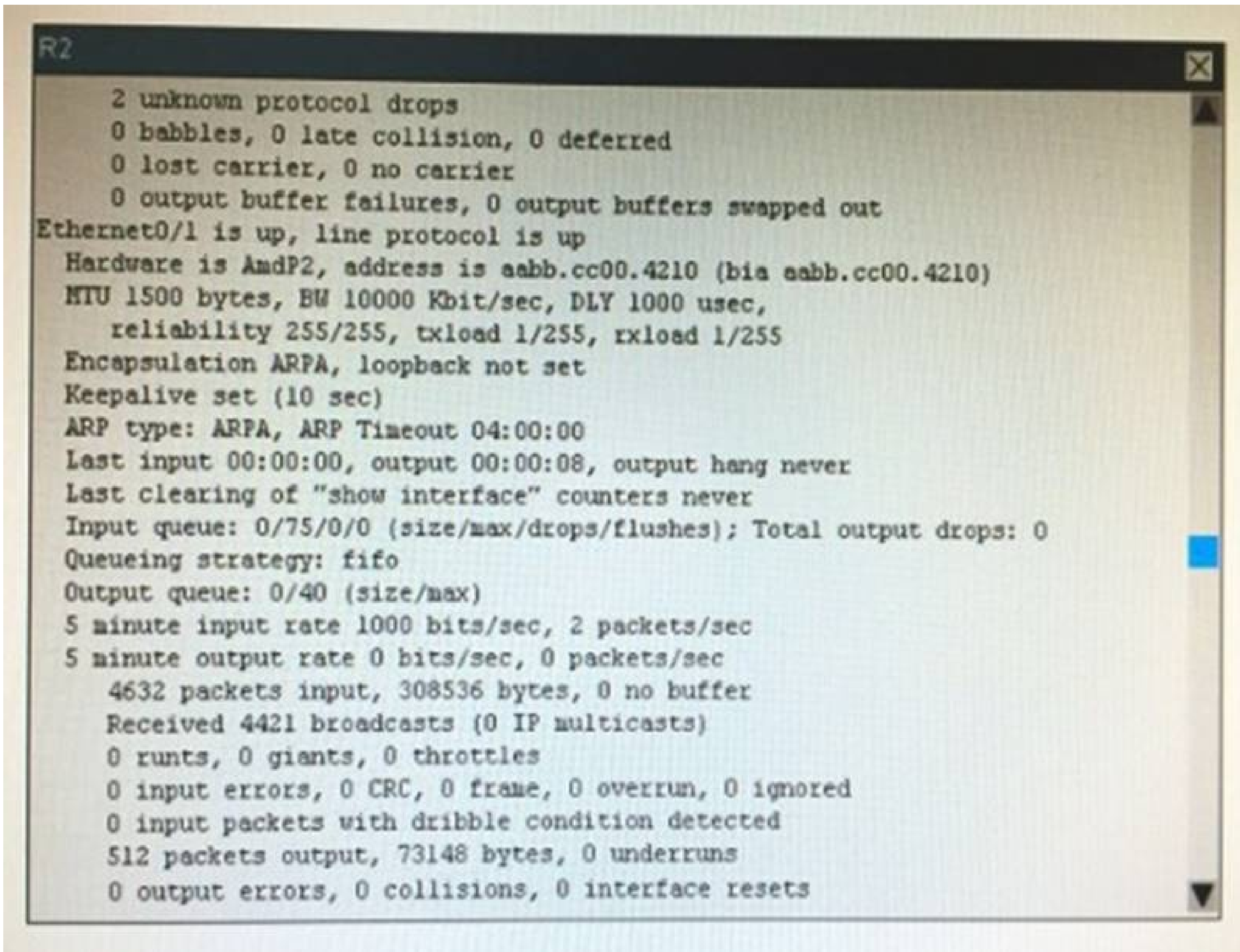
```
!
interface Ethernet0/2
 description ***Link to R1***
 ip address 172.16.14.2 255.255.255.252
!
interface Ethernet0/3
 description ***Link to LAN***
 ip address 10.10.10.1 255.255.255.0
!
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.1.0
 network 192.168.100.0
 network 192.168.200.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
```



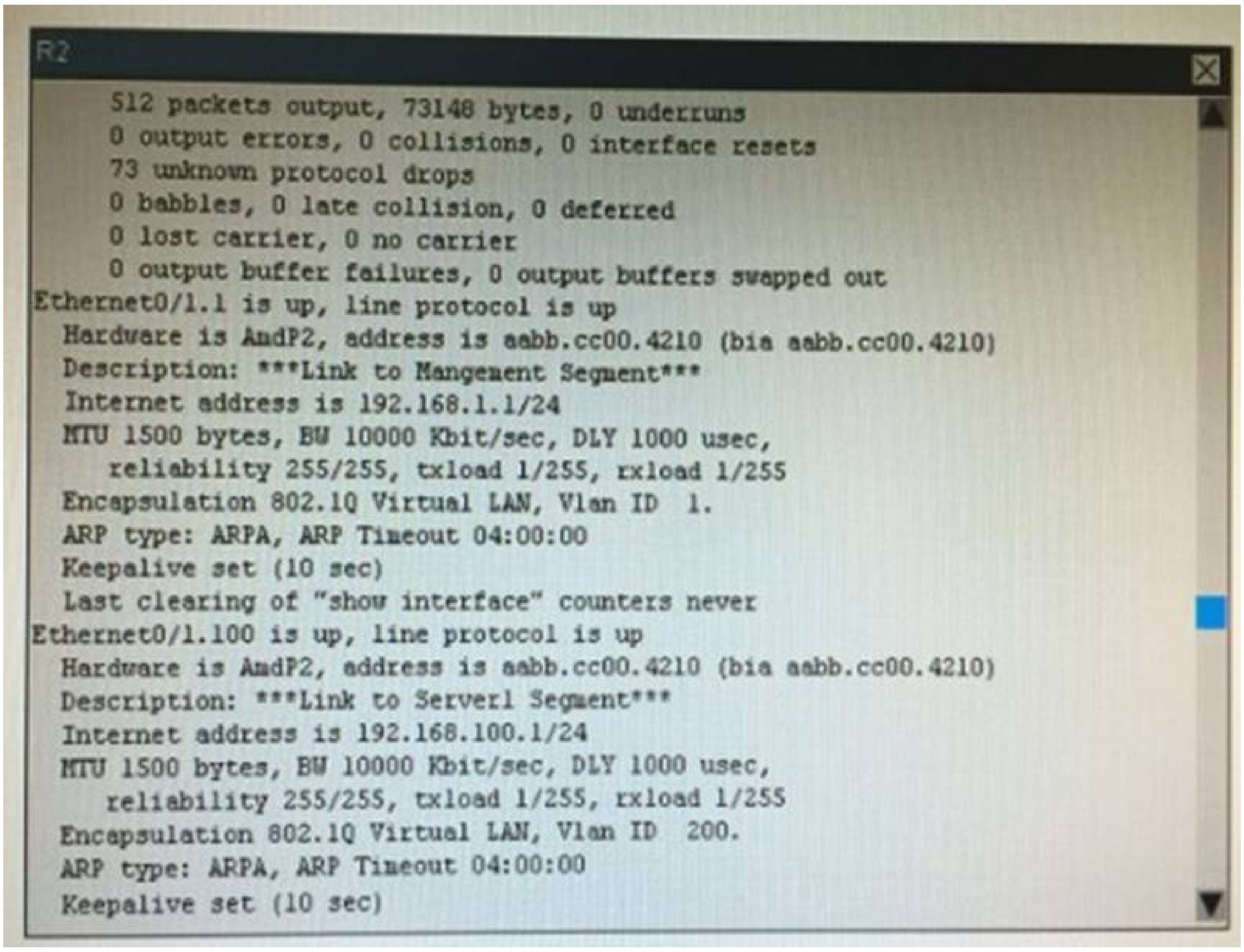
```
!
control-plane
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
!
end
R2#show interfaces
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4200 (bia aabb.cc00.4200)
  Description: ***Link to R3***
  Internet address is 172.16.11.1/30
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```



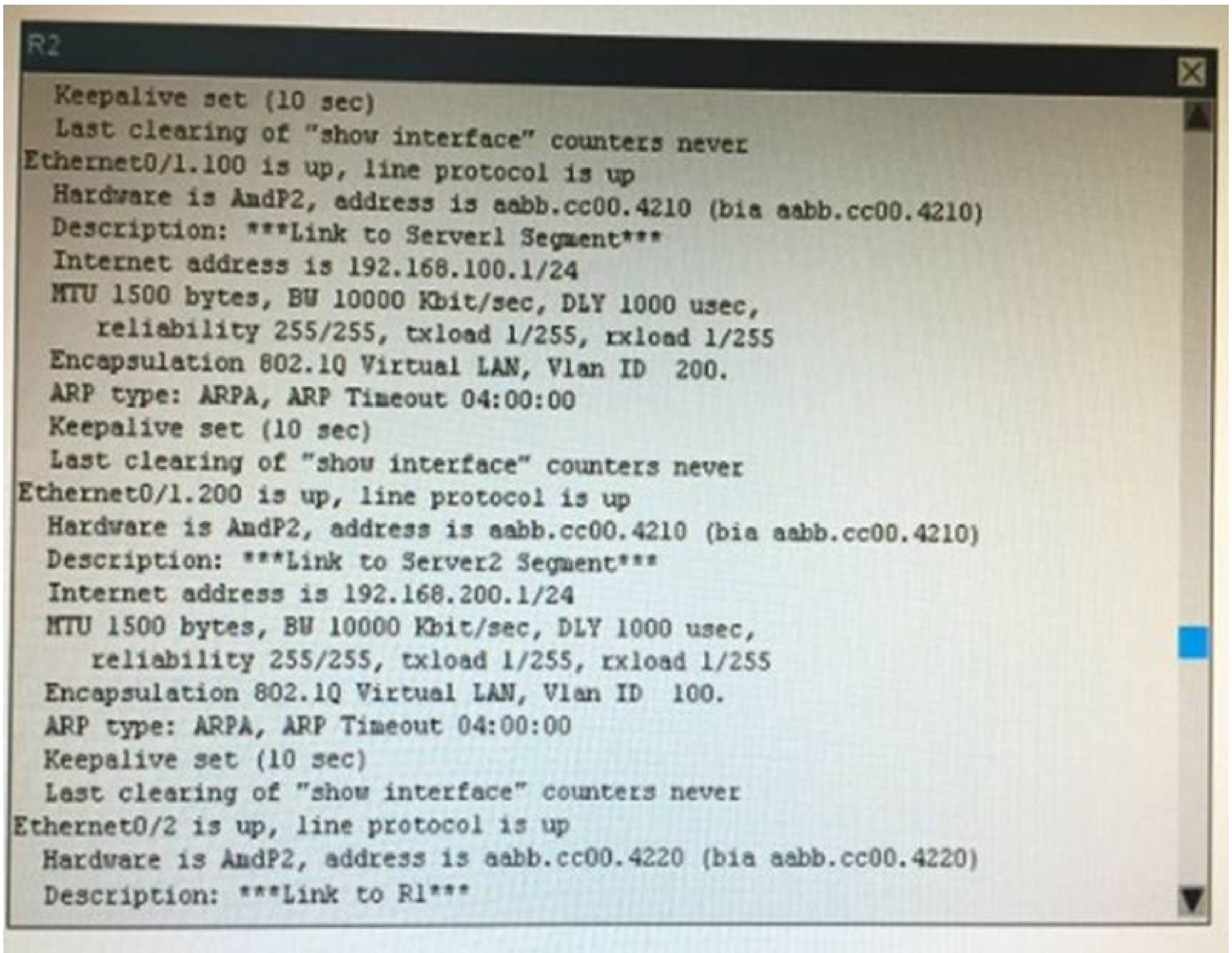
```
R2#show interfaces
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4200 (bia aabb.cc00.4200)
  Description: ***Link to R3***
  Internet address is 172.16.11.1/30
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:32, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     50 packets input, 15683 bytes, 0 no buffer
     Received 50 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     343 packets output, 42566 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     2 unknown protocol drops
```



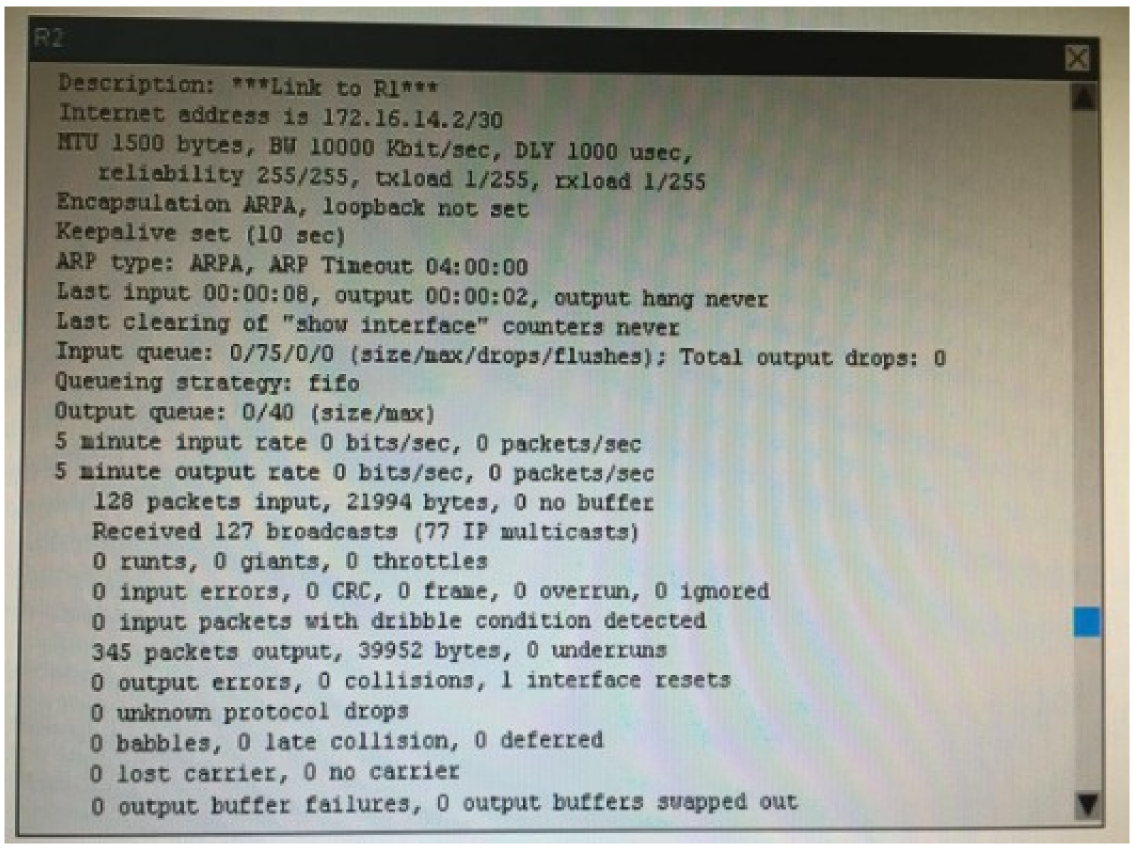
```
     2 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/1 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4210 (bia aabb.cc00.4210)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     4632 packets input, 308536 bytes, 0 no buffer
     Received 4421 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     512 packets output, 73148 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
```



```
     512 packets output, 73148 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     73 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/1.1 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4210 (bia aabb.cc00.4210)
  Description: ***Link to Mangement Segment***
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive set (10 sec)
  Last clearing of "show interface" counters never
Ethernet0/1.100 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4210 (bia aabb.cc00.4210)
  Description: ***Link to Server1 Segment***
  Internet address is 192.168.100.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  200.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive set (10 sec)
```

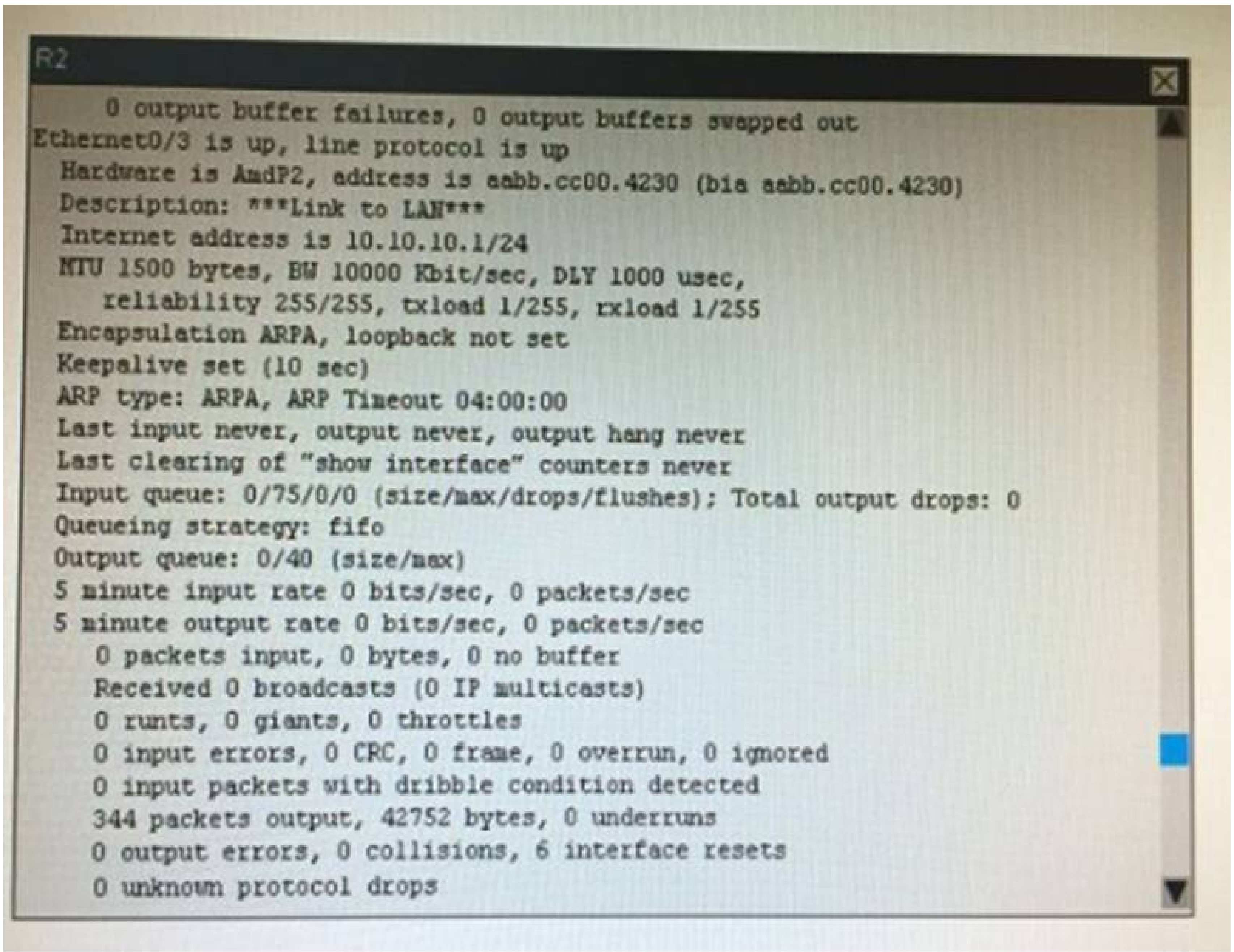


```
  Keepalive set (10 sec)
  Last clearing of "show interface" counters never
Ethernet0/1.100 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4210 (bia aabb.cc00.4210)
  Description: ***Link to Server1 Segment***
  Internet address is 192.168.100.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  200.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive set (10 sec)
  Last clearing of "show interface" counters never
Ethernet0/1.200 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4210 (bia aabb.cc00.4210)
  Description: ***Link to Server2 Segment***
  Internet address is 192.168.200.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  100.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive set (10 sec)
  Last clearing of "show interface" counters never
Ethernet0/2 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4220 (bia aabb.cc00.4220)
  Description: ***Link to R1***
```



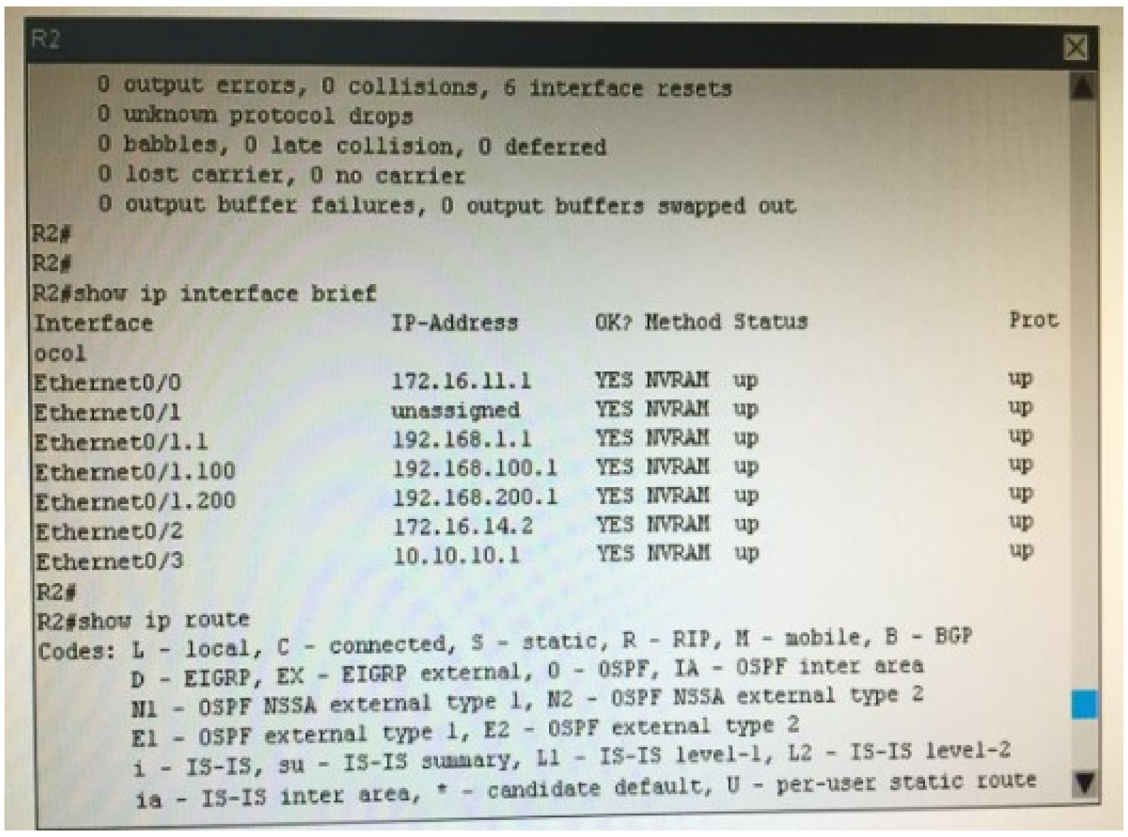
R2

```
Description: ***Link to R1***
Internet address is 172.16.14.2/30
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:02, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   128 packets input, 21994 bytes, 0 no buffer
   Received 127 broadcasts (77 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 input packets with dribble condition detected
   345 packets output, 39952 bytes, 0 underruns
   0 output errors, 0 collisions, 1 interface resets
   0 unknown protocol drops
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier
   0 output buffer failures, 0 output buffers swapped out
```



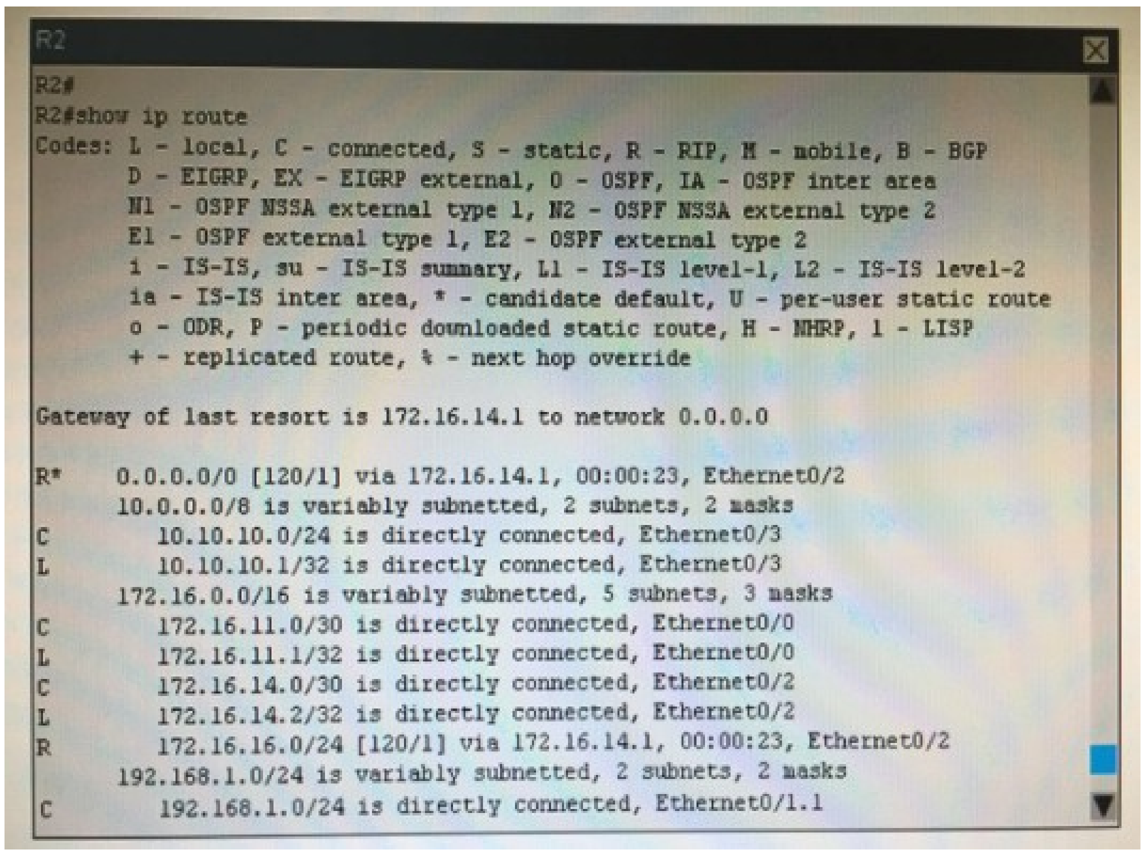
R2

```
    0 output buffer failures, 0 output buffers swapped out
Ethernet0/3 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4230 (bia aabb.cc00.4230)
  Description: ***Link to LAN***
  Internet address is 10.10.10.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     344 packets output, 42752 bytes, 0 underruns
     0 output errors, 0 collisions, 6 interface resets
     0 unknown protocol drops
```



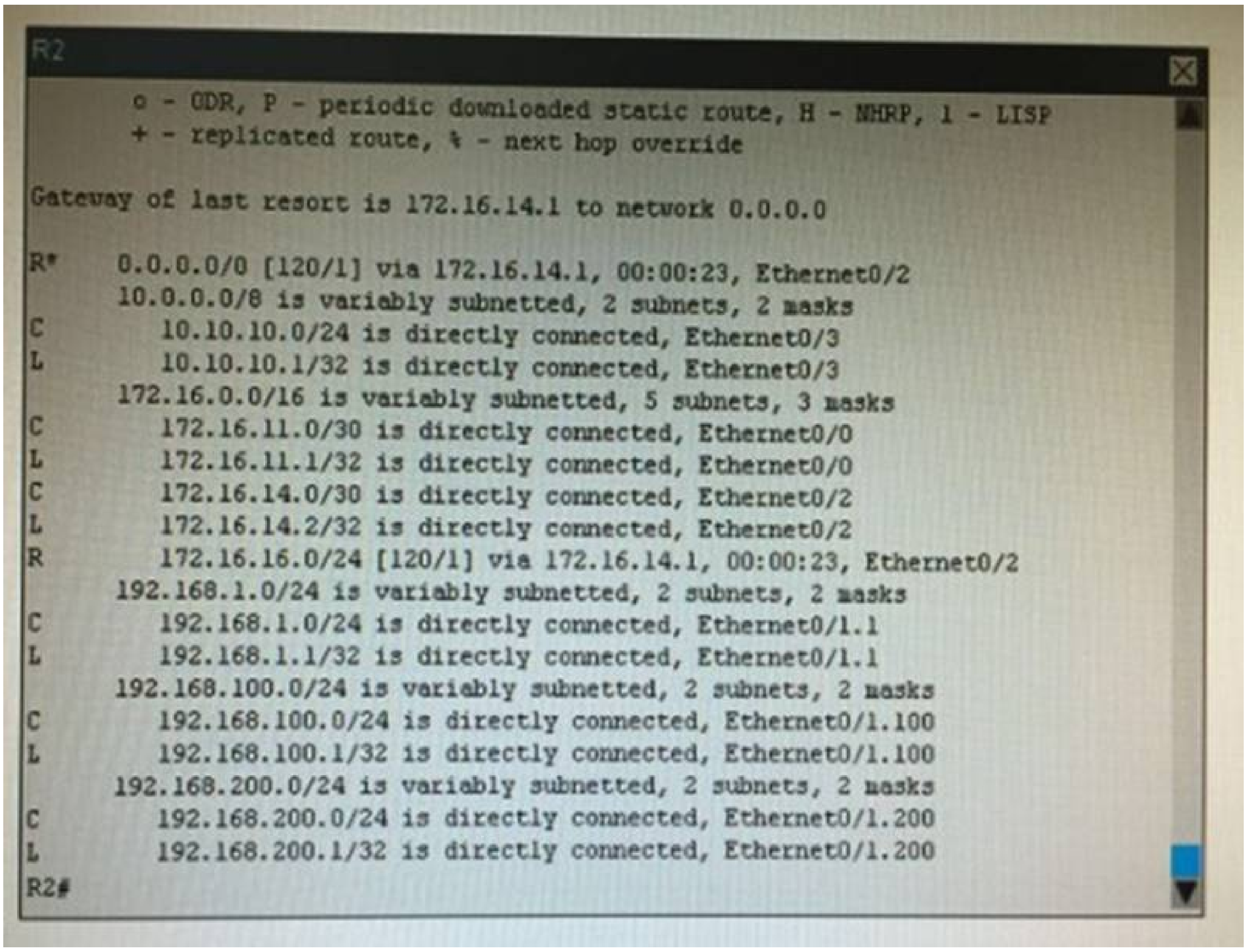
R2

```
     0 output errors, 0 collisions, 6 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R2#
R2#
R2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
Ethernet0/0                172.16.11.1     YES NVRAM  up                    up
Ethernet0/1                unassigned      YES NVRAM  up                    up
Ethernet0/1.1              192.168.1.1     YES NVRAM  up                    up
Ethernet0/1.100            192.168.100.1   YES NVRAM  up                    up
Ethernet0/1.200            192.168.200.1   YES NVRAM  up                    up
Ethernet0/2                172.16.14.2     YES NVRAM  up                    up
Ethernet0/3                10.10.10.1      YES NVRAM  up                    up
R2#
R2#show ip route
Codes: L - local, 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
```

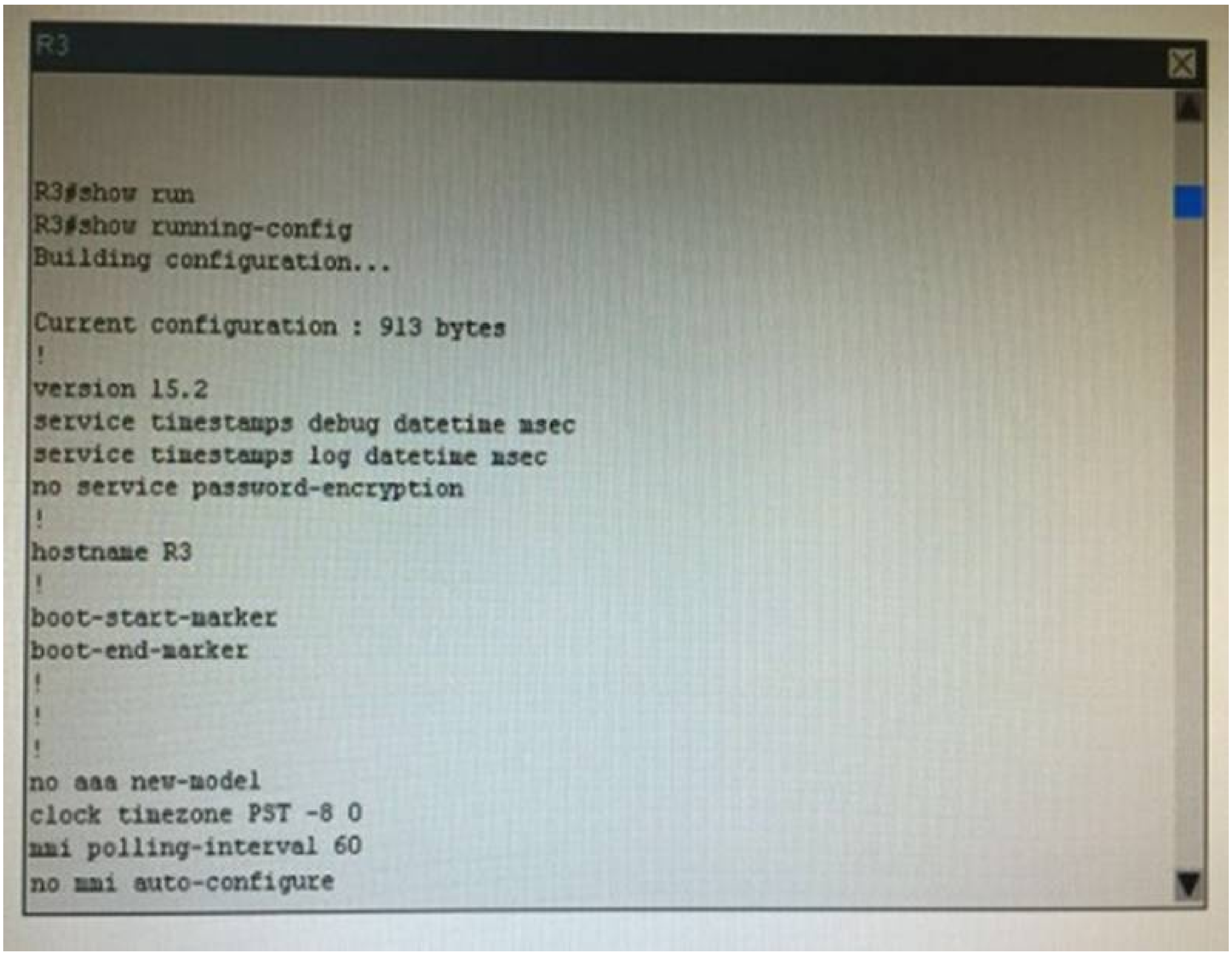


R2

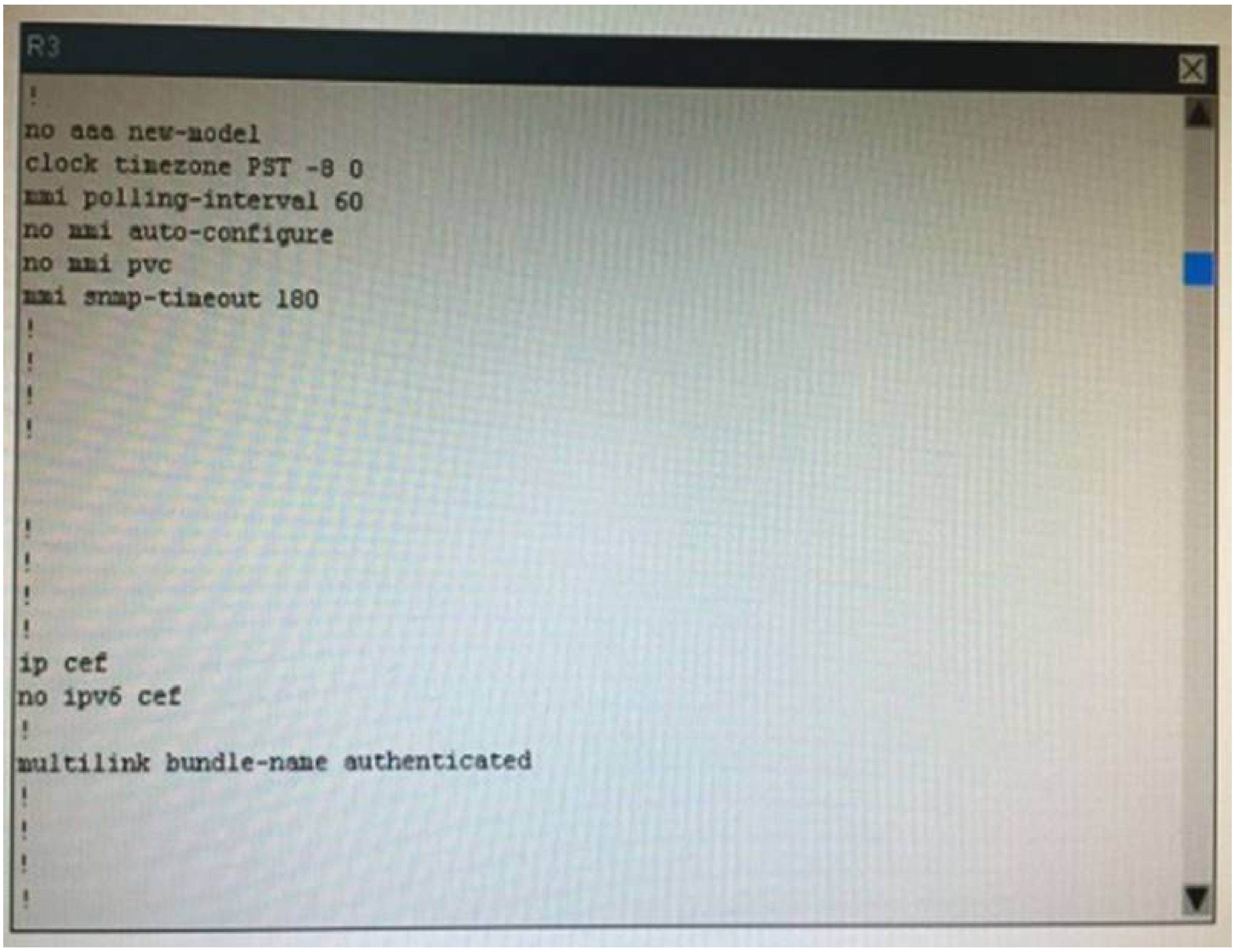
```
R2#
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.14.1 to network 0.0.0.0

R*    0.0.0.0/0 [120/1] via 172.16.14.1, 00:00:23, Ethernet0/2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.10.0/24 is directly connected, Ethernet0/3
L        10.10.10.1/32 is directly connected, Ethernet0/3
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.11.0/30 is directly connected, Ethernet0/0
L        172.16.11.1/32 is directly connected, Ethernet0/0
C        172.16.14.0/30 is directly connected, Ethernet0/2
L        172.16.14.2/32 is directly connected, Ethernet0/2
R        172.16.16.0/24 [120/1] via 172.16.14.1, 00:00:23, Ethernet0/2
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Ethernet0/1.1
```



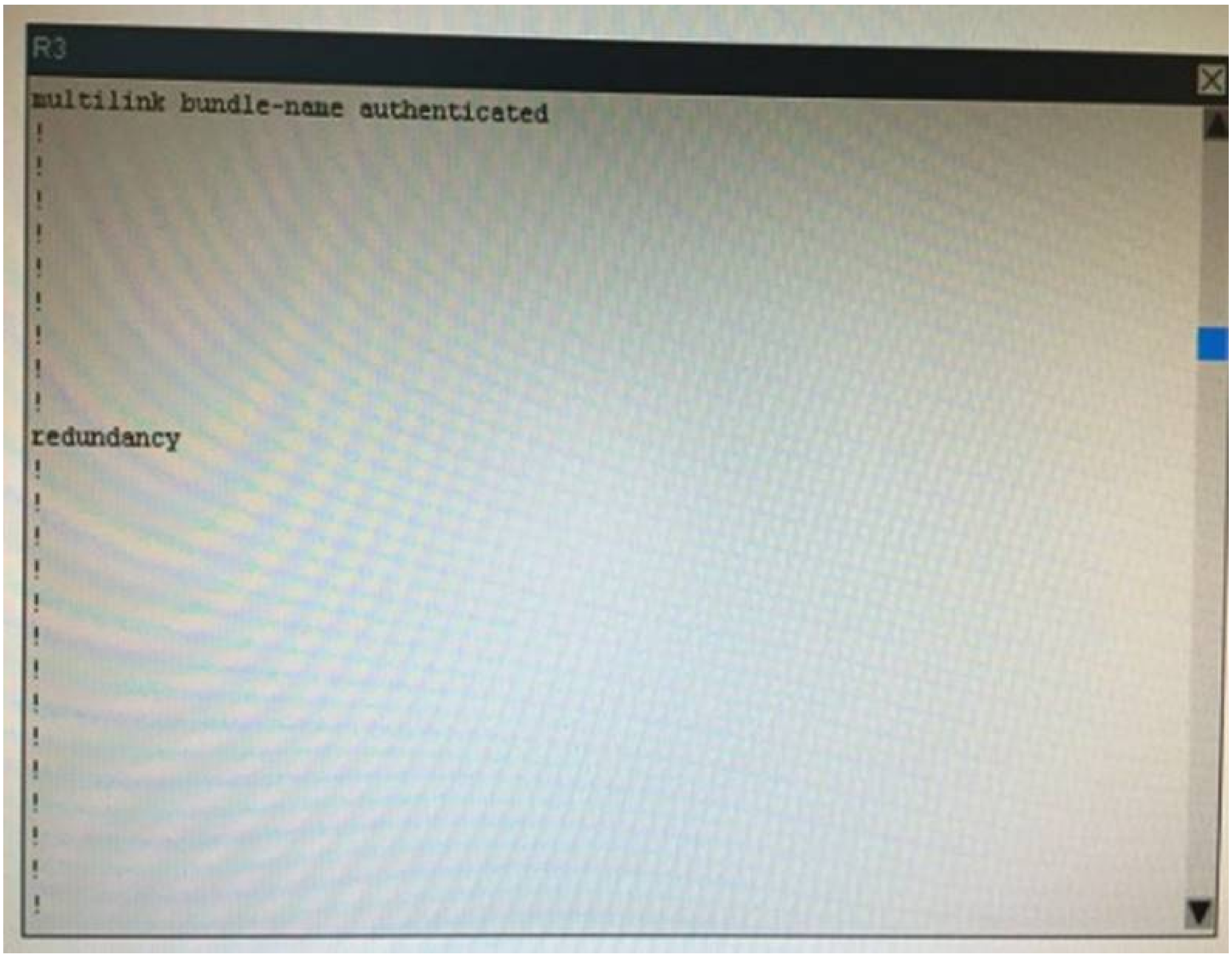
```
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is 172.16.14.1 to network 0.0.0.0

R*    0.0.0.0/0 [120/1] via 172.16.14.1, 00:00:23, Ethernet0/2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.10.0/24 is directly connected, Ethernet0/3
L        10.10.10.1/32 is directly connected, Ethernet0/3
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.11.0/30 is directly connected, Ethernet0/0
L        172.16.11.1/32 is directly connected, Ethernet0/0
C        172.16.14.0/30 is directly connected, Ethernet0/2
L        172.16.14.2/32 is directly connected, Ethernet0/2
R        172.16.16.0/24 [120/1] via 172.16.14.1, 00:00:23, Ethernet0/2
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Ethernet0/1.1
L        192.168.1.1/32 is directly connected, Ethernet0/1.1
      192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.100.0/24 is directly connected, Ethernet0/1.100
L        192.168.100.1/32 is directly connected, Ethernet0/1.100
      192.168.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.200.0/24 is directly connected, Ethernet0/1.200
L        192.168.200.1/32 is directly connected, Ethernet0/1.200
R2#
```



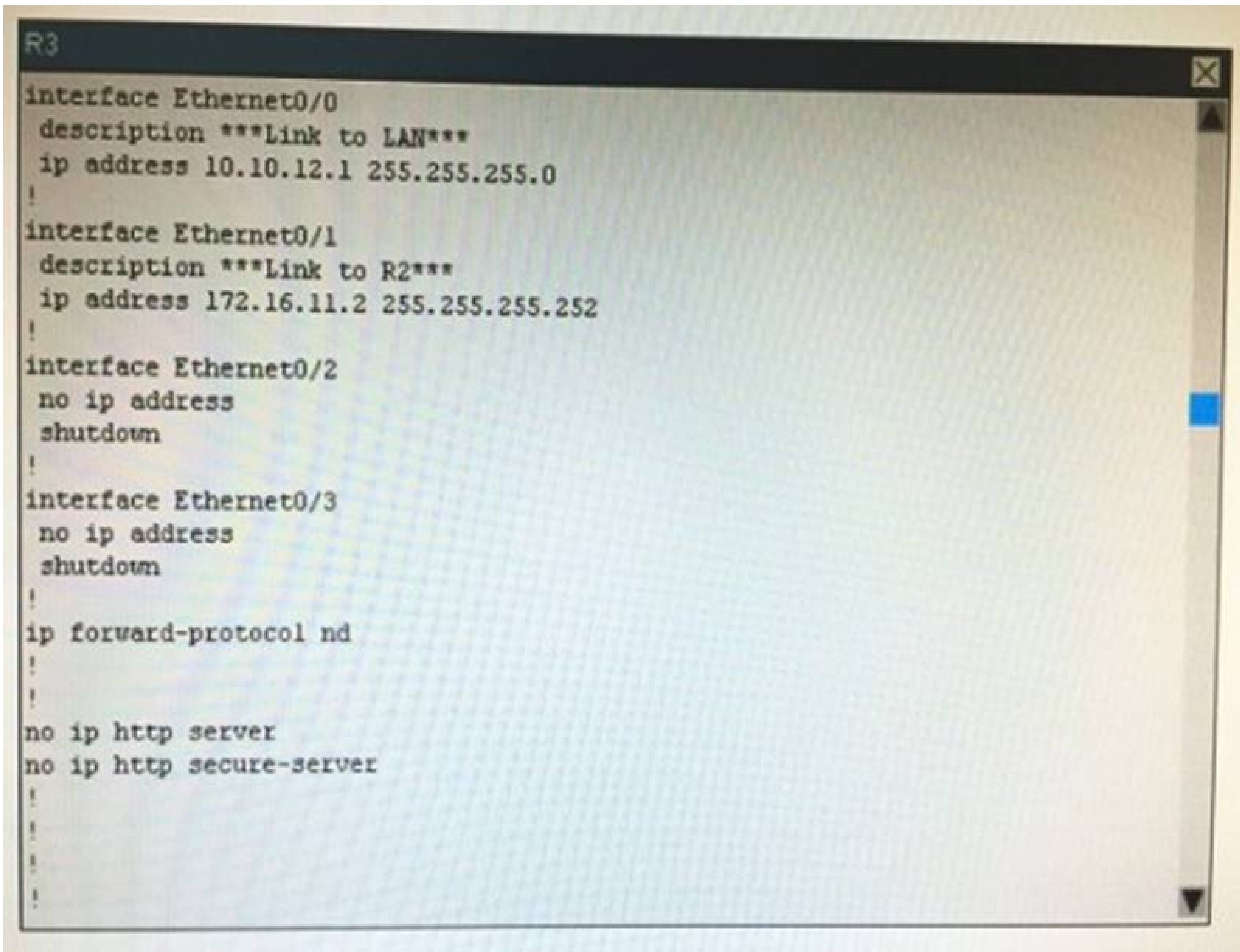
```
R3#show run
R3#show running-config
Building configuration...

Current configuration : 913 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
```



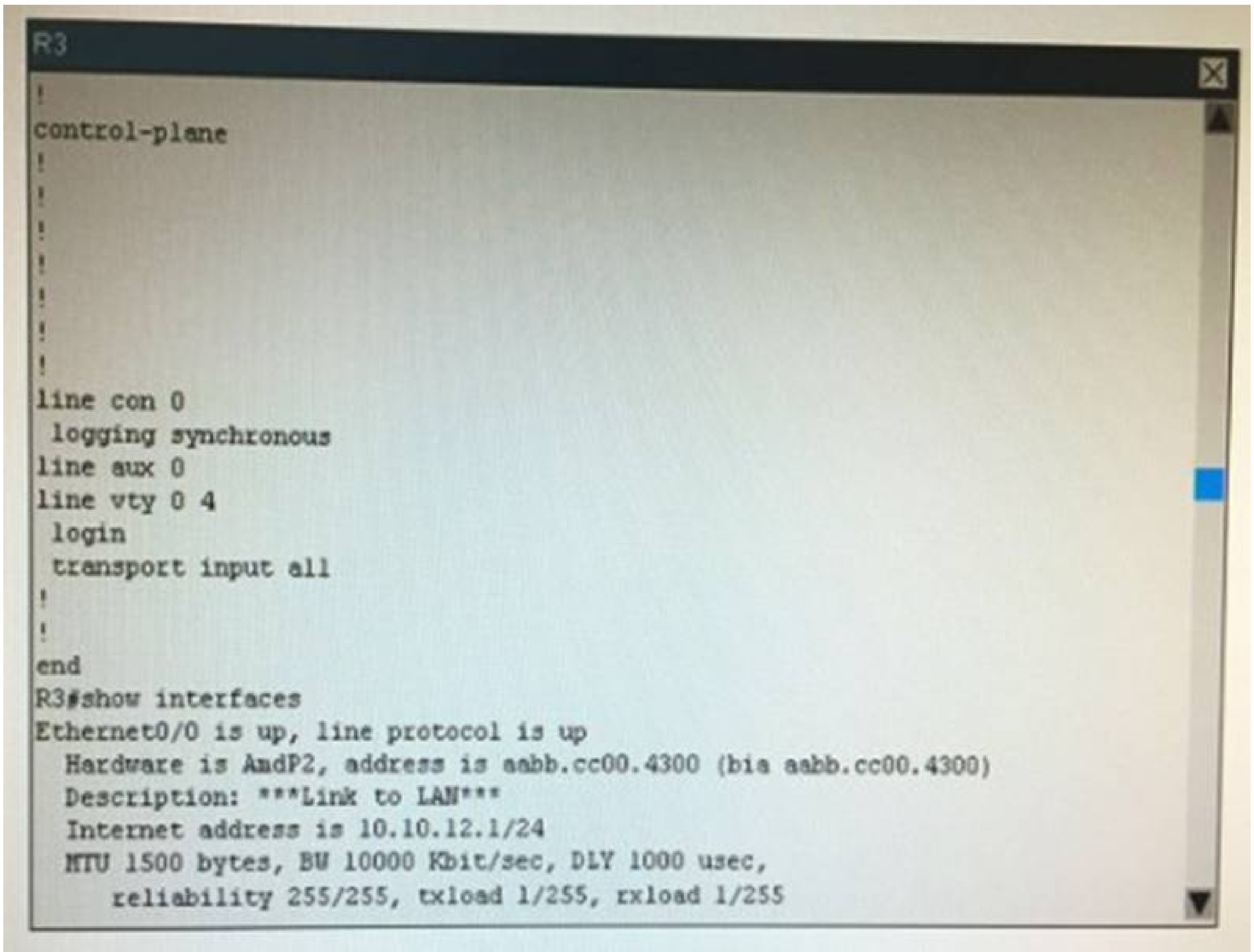
```
R3
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!


!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
```



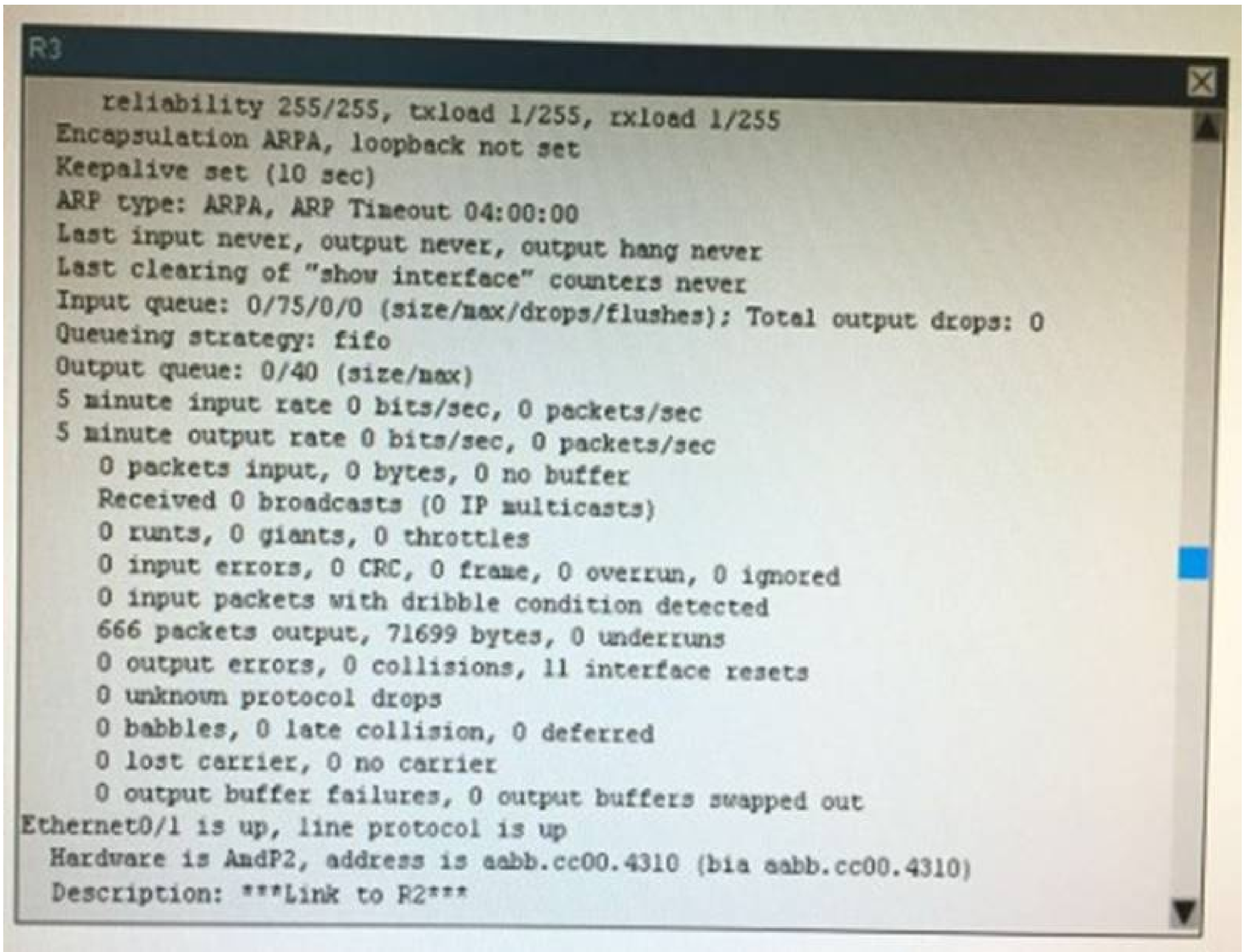
```
R3
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
```



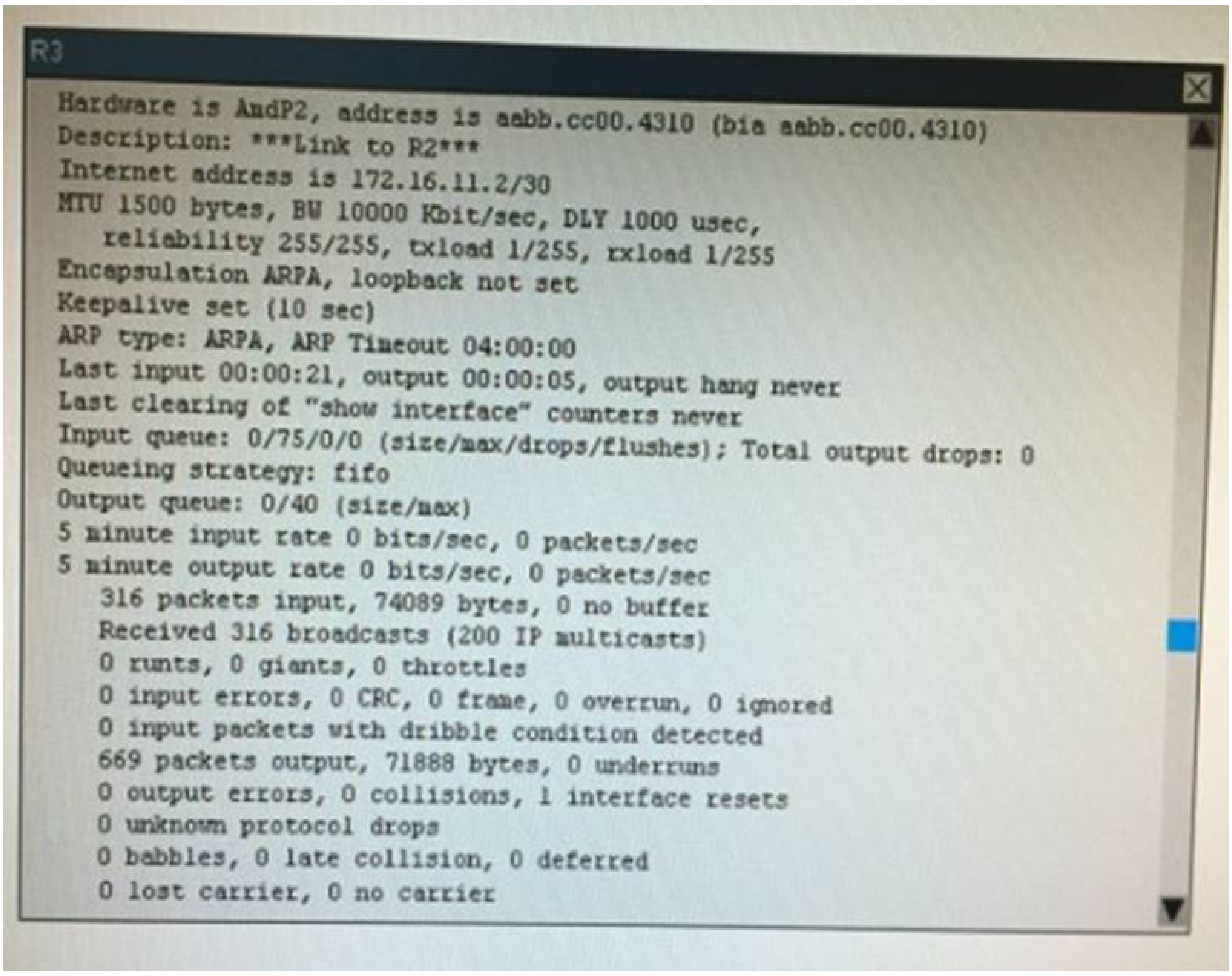
```
interface Ethernet0/0
 description ***Link to LAN***
 ip address 10.10.12.1 255.255.255.0
!
interface Ethernet0/1
 description ***Link to R2***
 ip address 172.16.11.2 255.255.255.252
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
```



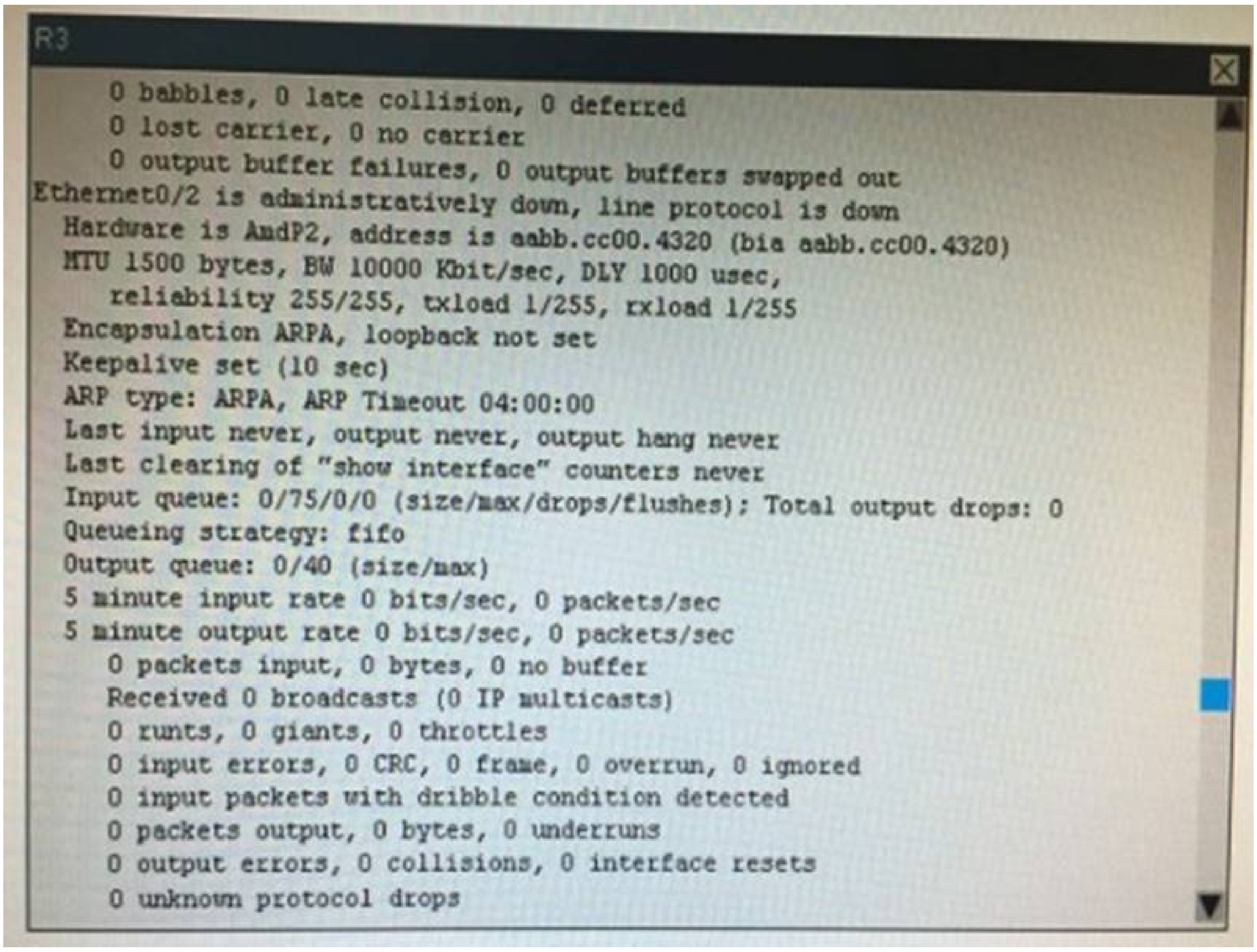
```
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
!
end
R3#show interfaces
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4300 (bia aabb.cc00.4300)
  Description: ***Link to LAN***
  Internet address is 10.10.12.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```



```
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     666 packets output, 71699 bytes, 0 underruns
     0 output errors, 0 collisions, 11 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/1 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.4310 (bia aabb.cc00.4310)
  Description: ***Link to R2***
```

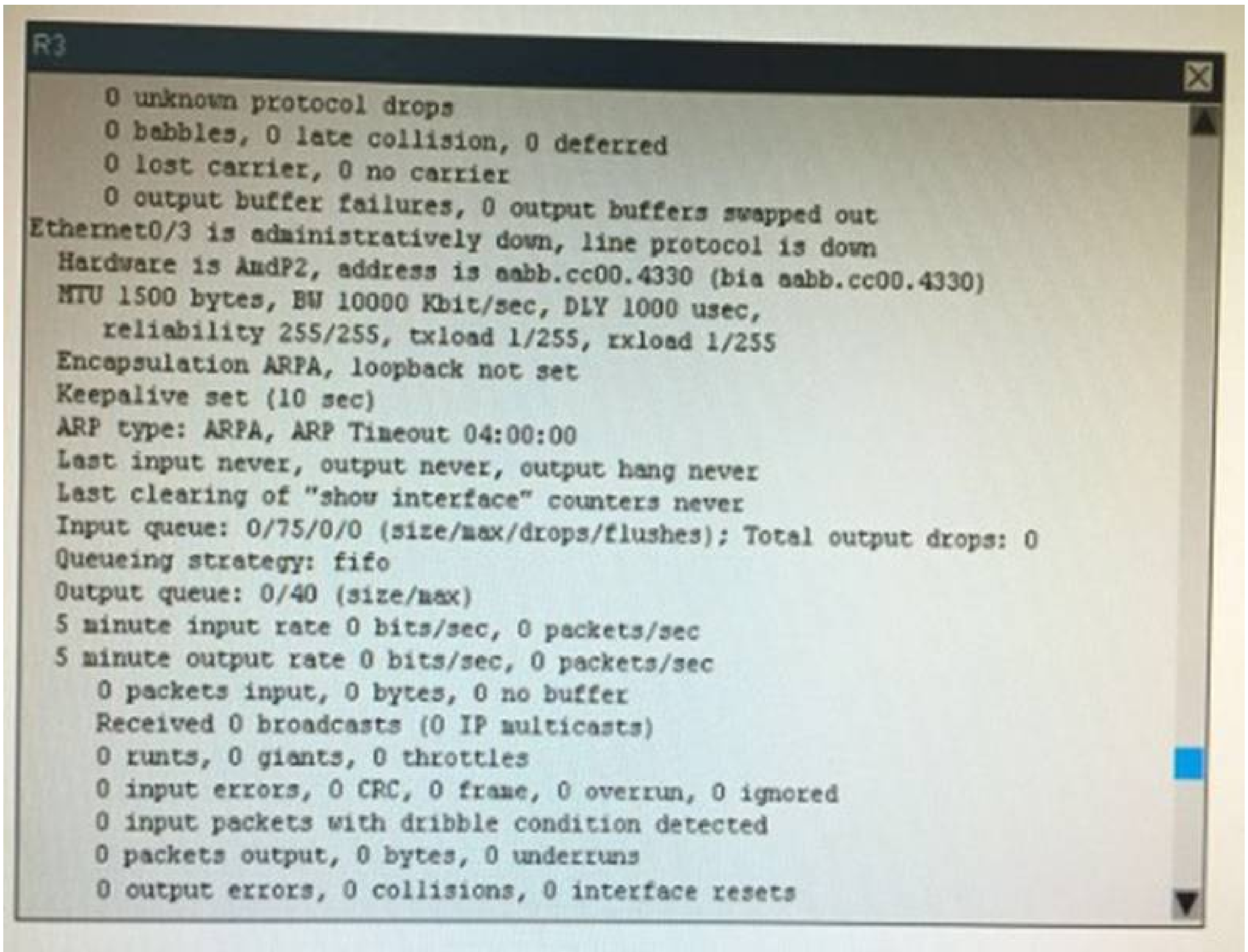


```
  Hardware is AmdP2, address is aabb.cc00.4310 (bia aabb.cc00.4310)
  Description: ***Link to R2***
  Internet address is 172.16.11.2/30
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:21, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     316 packets input, 74089 bytes, 0 no buffer
     Received 316 broadcasts (200 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     669 packets output, 71888 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
```



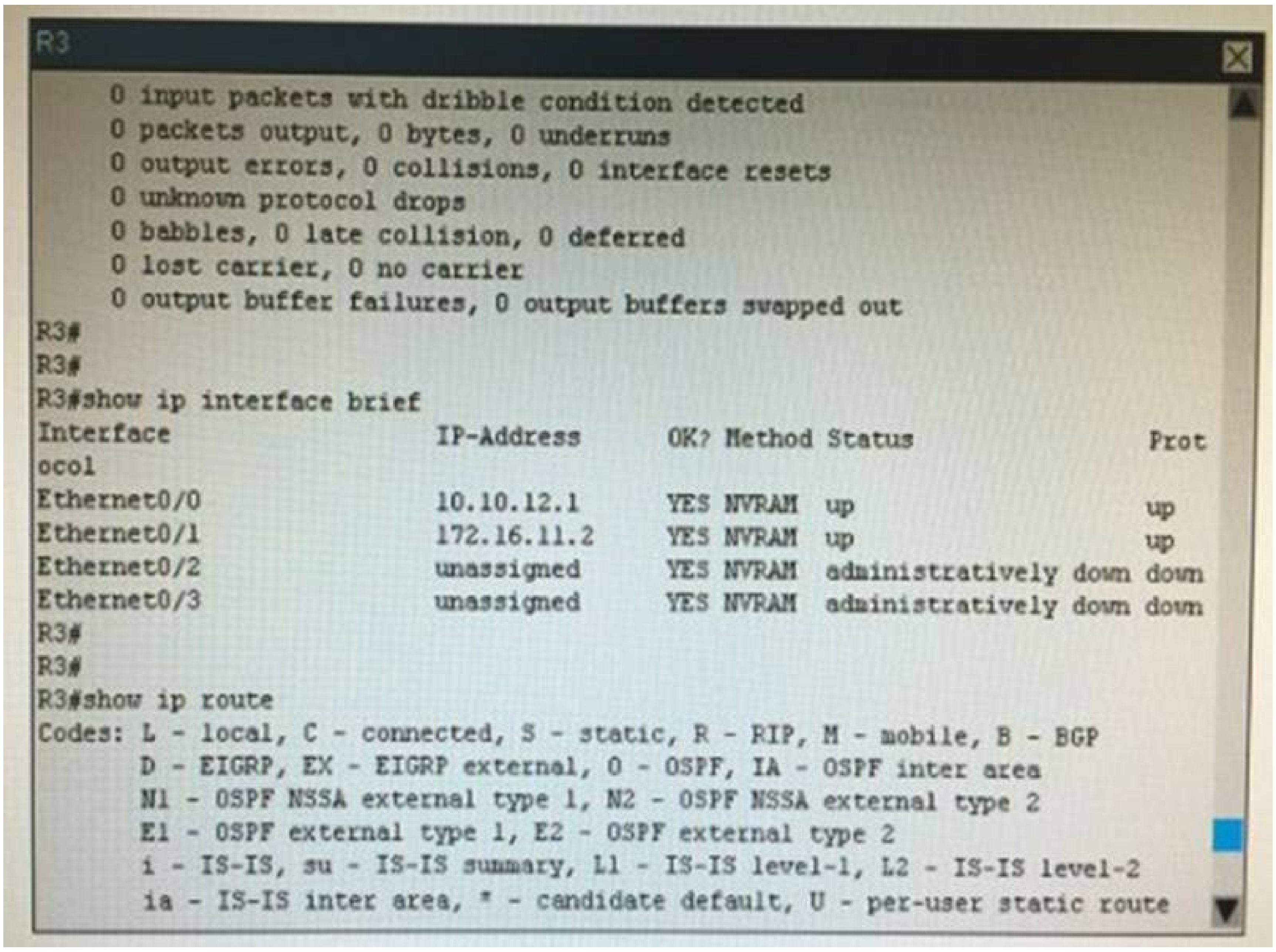
R3

```
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/2 is administratively down, line protocol is down
  Hardware is AmdP2, address is aabb.cc00.4320 (bia aabb.cc00.4320)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
```

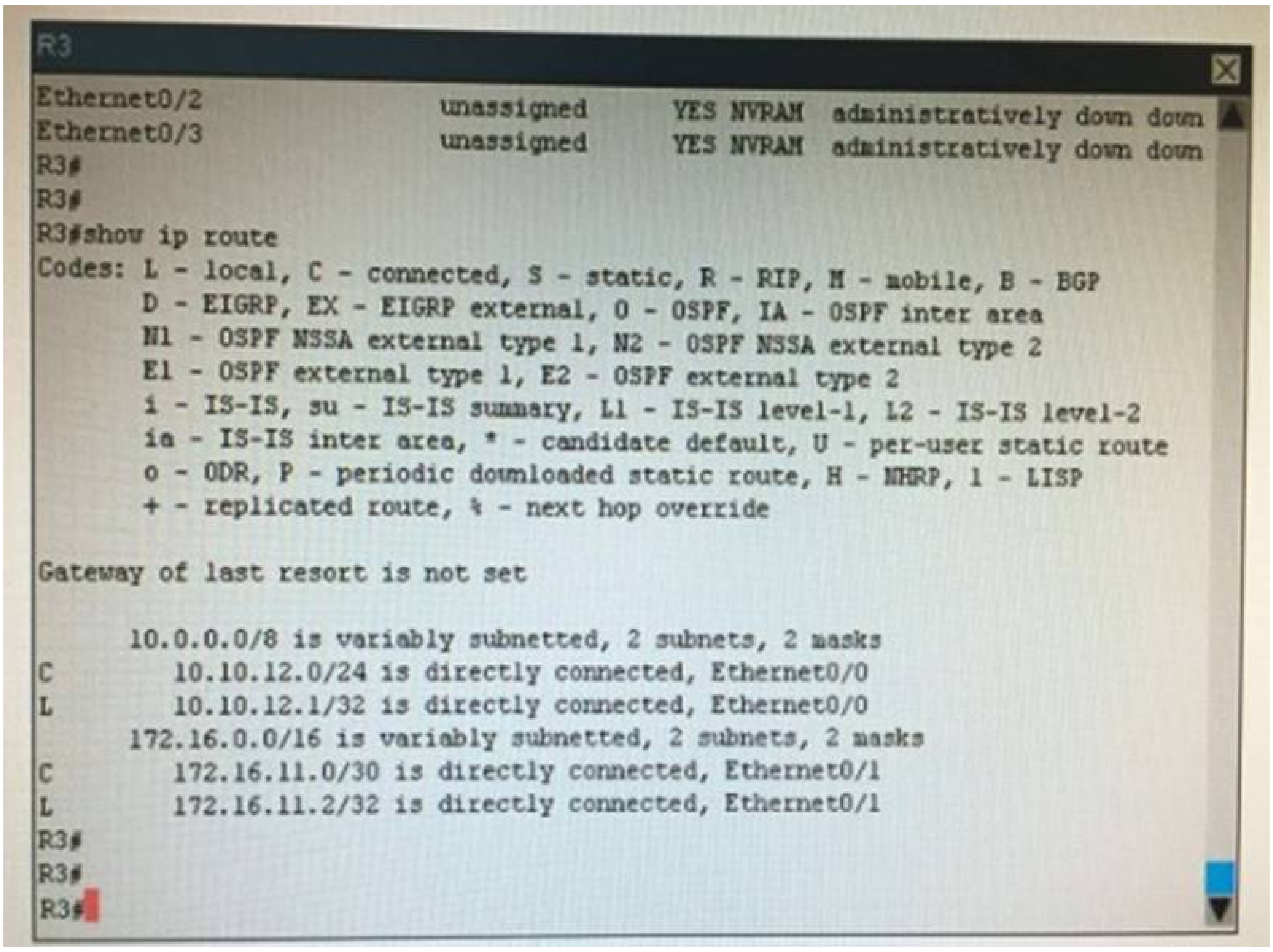


R3

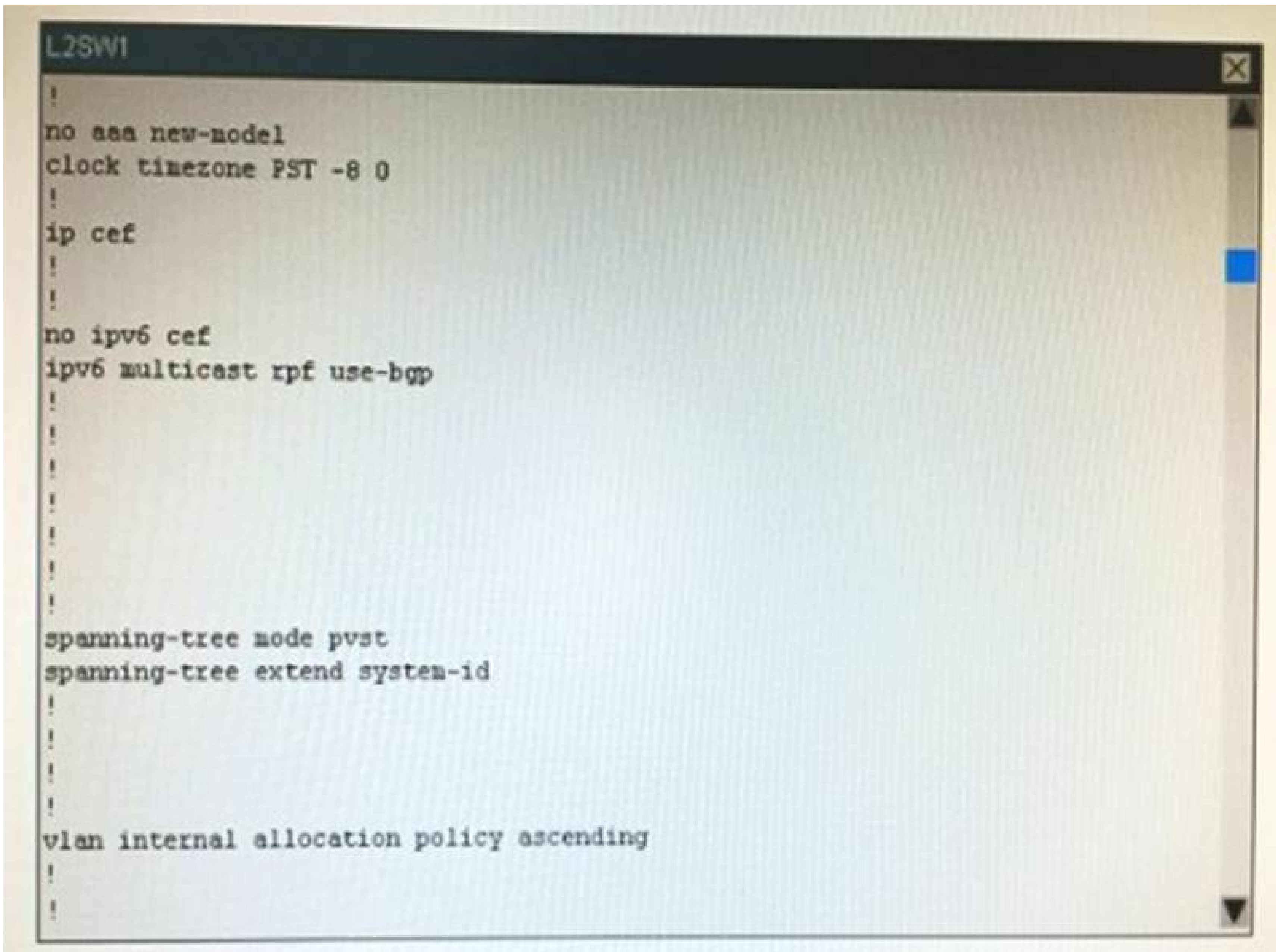
```
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/3 is administratively down, line protocol is down
  Hardware is AmdP2, address is aabb.cc00.4330 (bia aabb.cc00.4330)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
```



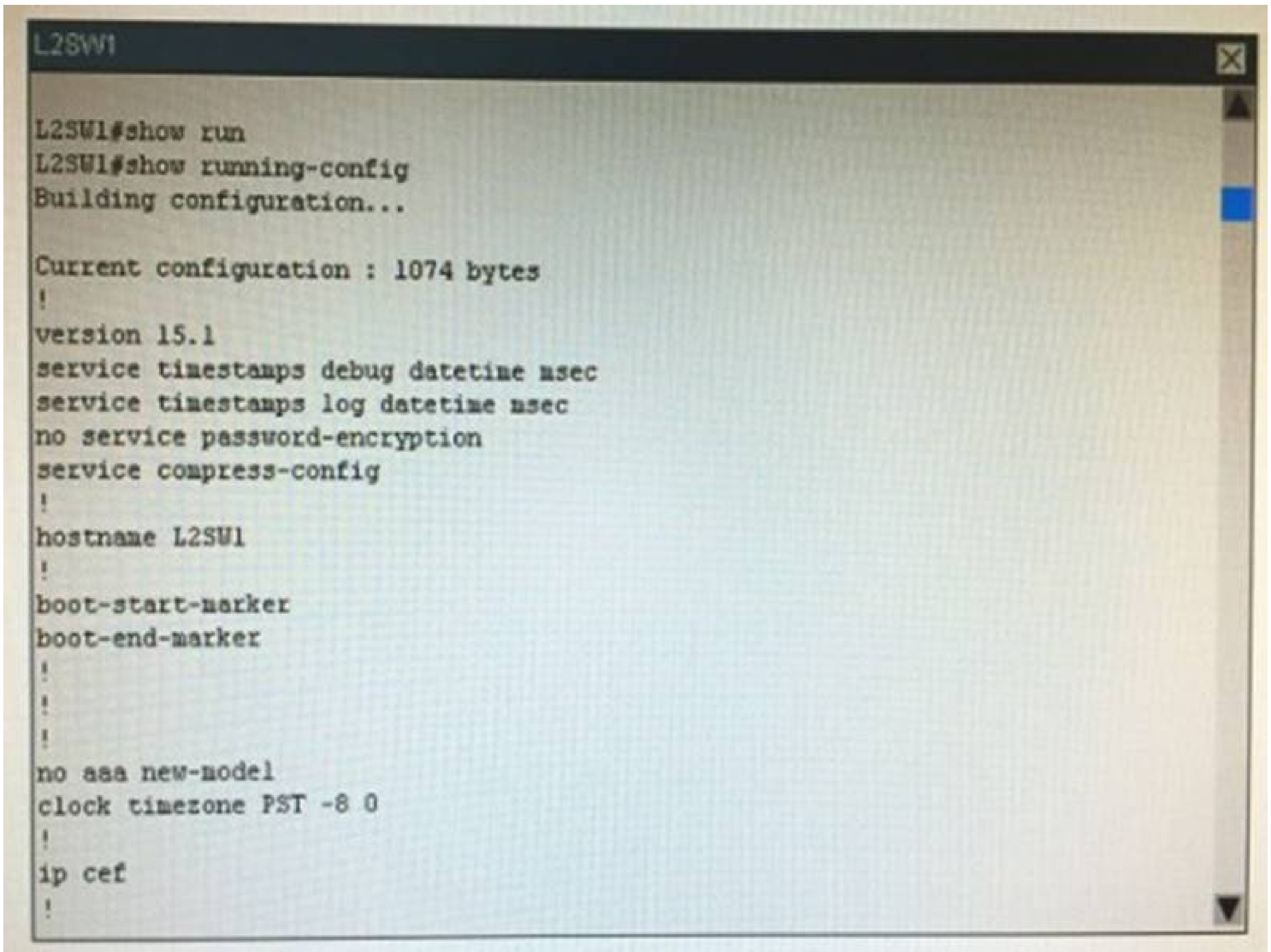
```
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R3#
R3#
R3#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
Ethernet0/0                10.10.12.1      YES NVRAM  up                    up
Ethernet0/1                172.16.11.2     YES NVRAM  up                    up
Ethernet0/2                unassigned      YES NVRAM  administratively down down
Ethernet0/3                unassigned      YES NVRAM  administratively down down
R3#
R3#
R3#show ip route
Codes: L - local, 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
```



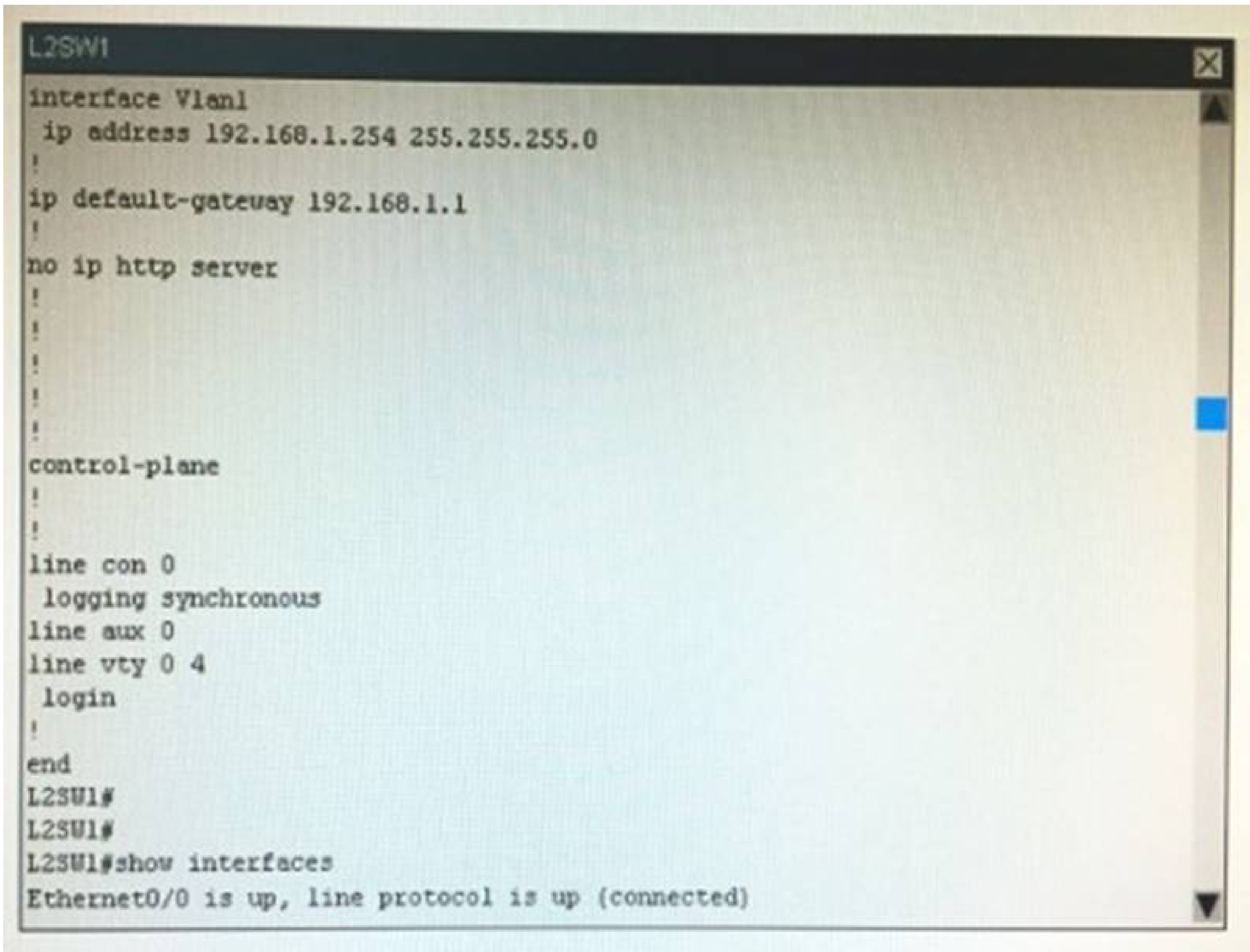
```
Ethernet0/2                unassigned      YES NVRAM  administratively down down
Ethernet0/3                unassigned      YES NVRAM  administratively down down
R3#
R3#
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.12.0/24 is directly connected, Ethernet0/0
L        10.10.12.1/32 is directly connected, Ethernet0/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.11.0/30 is directly connected, Ethernet0/1
L        172.16.11.2/32 is directly connected, Ethernet0/1
R3#
R3#
R3#
```



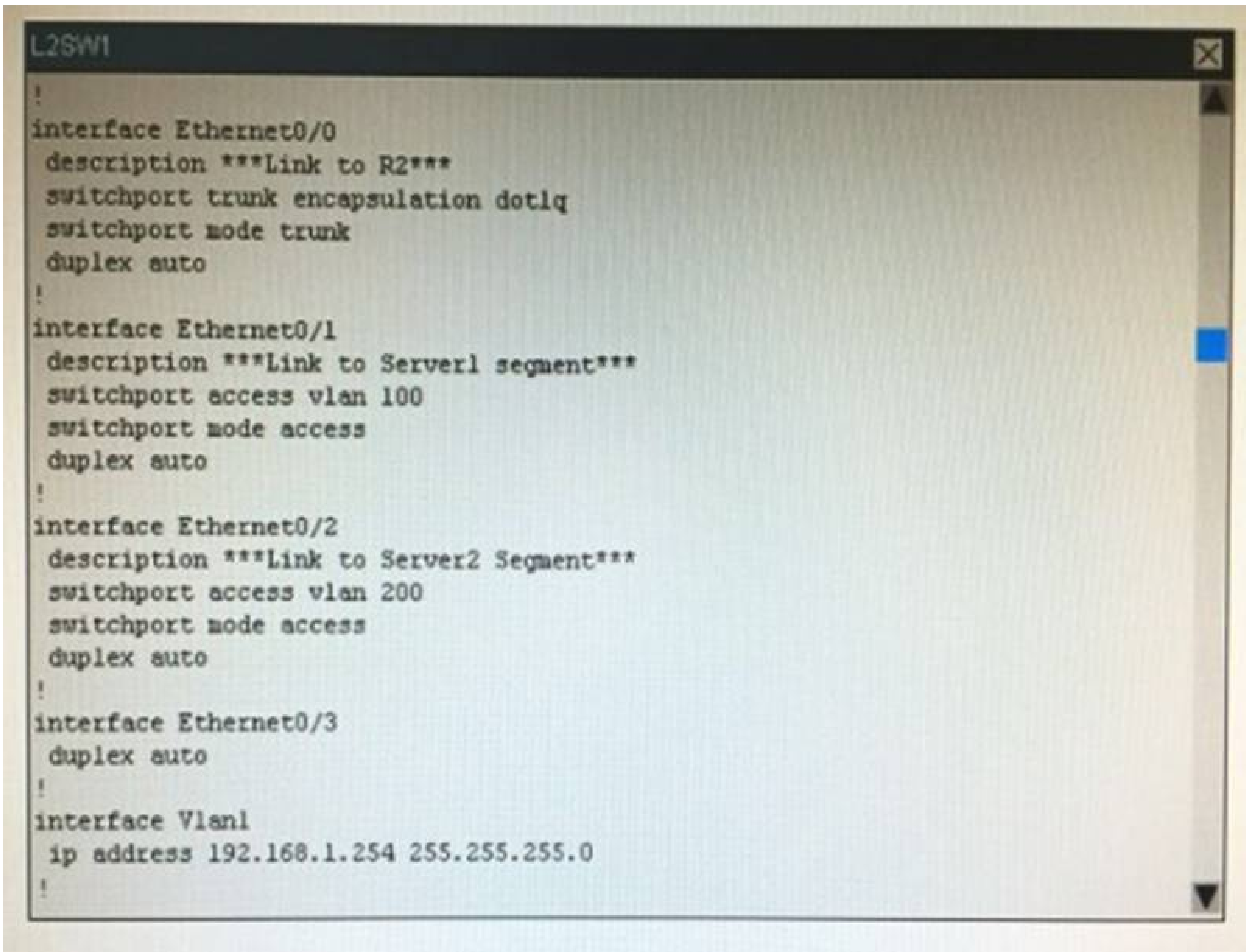
```
!
no aaa new-model
clock timezone PST -8 0
!
ip cef
!
!
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
```



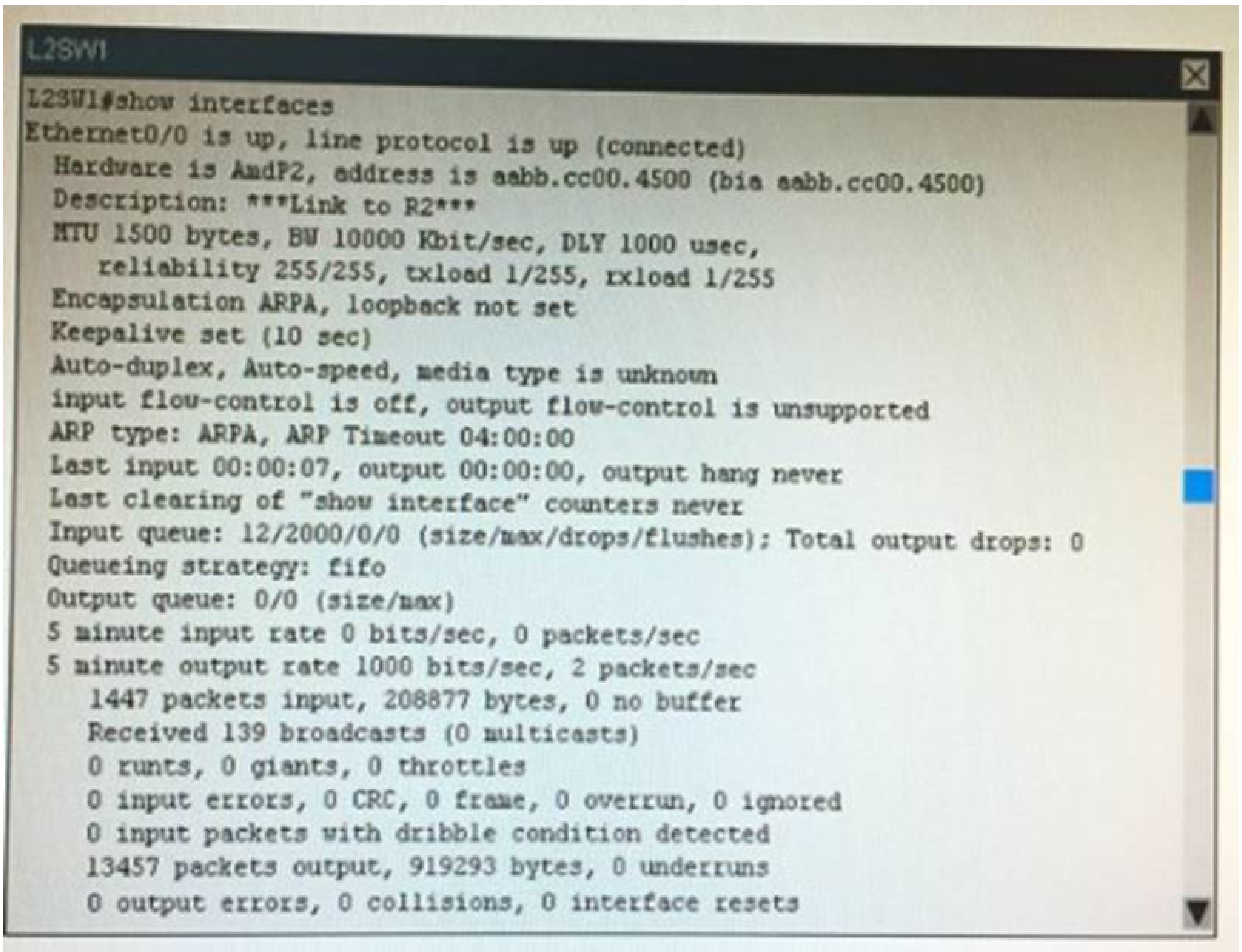
```
L2SW1#show run
L2SW1#show running-config
Building configuration...

Current configuration : 1074 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname L2SW1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
!
ip cef
!
```



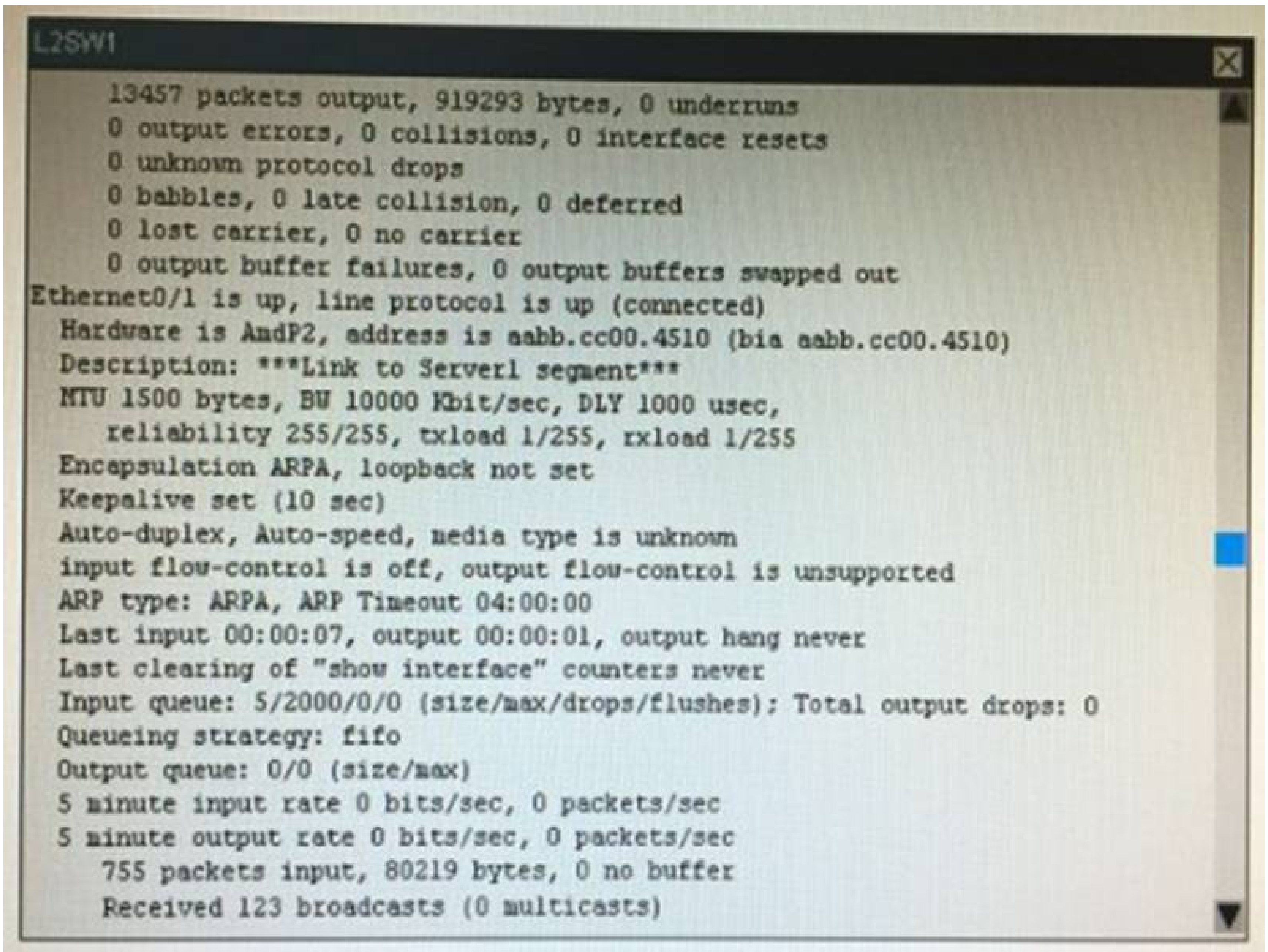
```
interface Vlan1
 ip address 192.168.1.254 255.255.255.0
!
ip default-gateway 192.168.1.1
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
L2SW1#
L2SW1#
L2SW1#show interfaces
Ethernet0/0 is up, line protocol is up (connected)
```



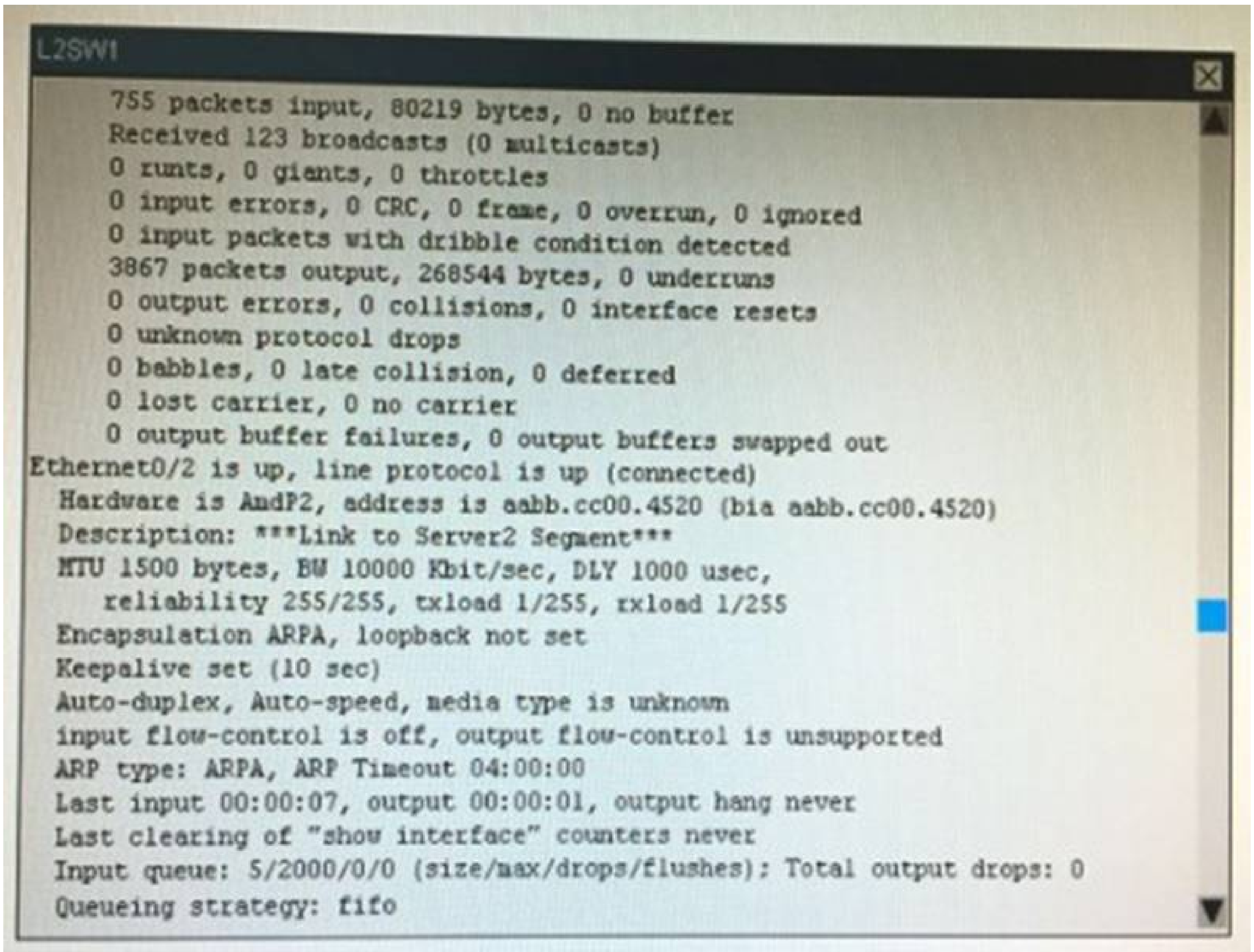
```
!
interface Ethernet0/0
 description ***Link to R2***
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 description ***Link to Server1 segment***
 switchport access vlan 100
 switchport mode access
 duplex auto
!
interface Ethernet0/2
 description ***Link to Server2 Segment***
 switchport access vlan 200
 switchport mode access
 duplex auto
!
interface Ethernet0/3
 duplex auto
!
interface Vlan1
 ip address 192.168.1.254 255.255.255.0
!
```



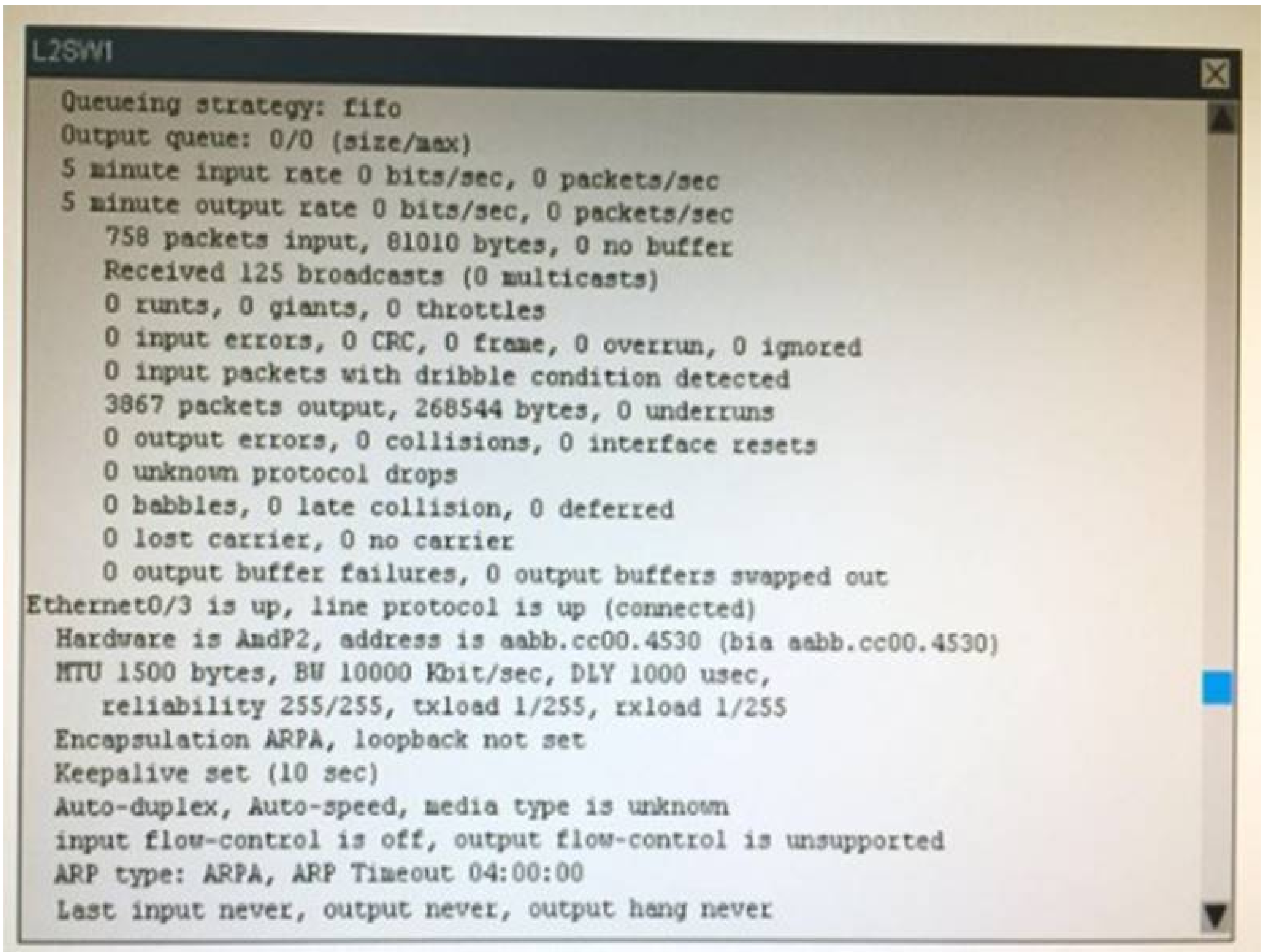
```
L2SW1#show interfaces
Ethernet0/0 is up, line protocol is up (connected)
  Hardware is AmdP2, address is aabb.cc00.4500 (bia aabb.cc00.4500)
  Description: ***Link to R2***
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is unknown
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:07, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 12/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     1447 packets input, 208877 bytes, 0 no buffer
     Received 139 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     13457 packets output, 919293 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
```



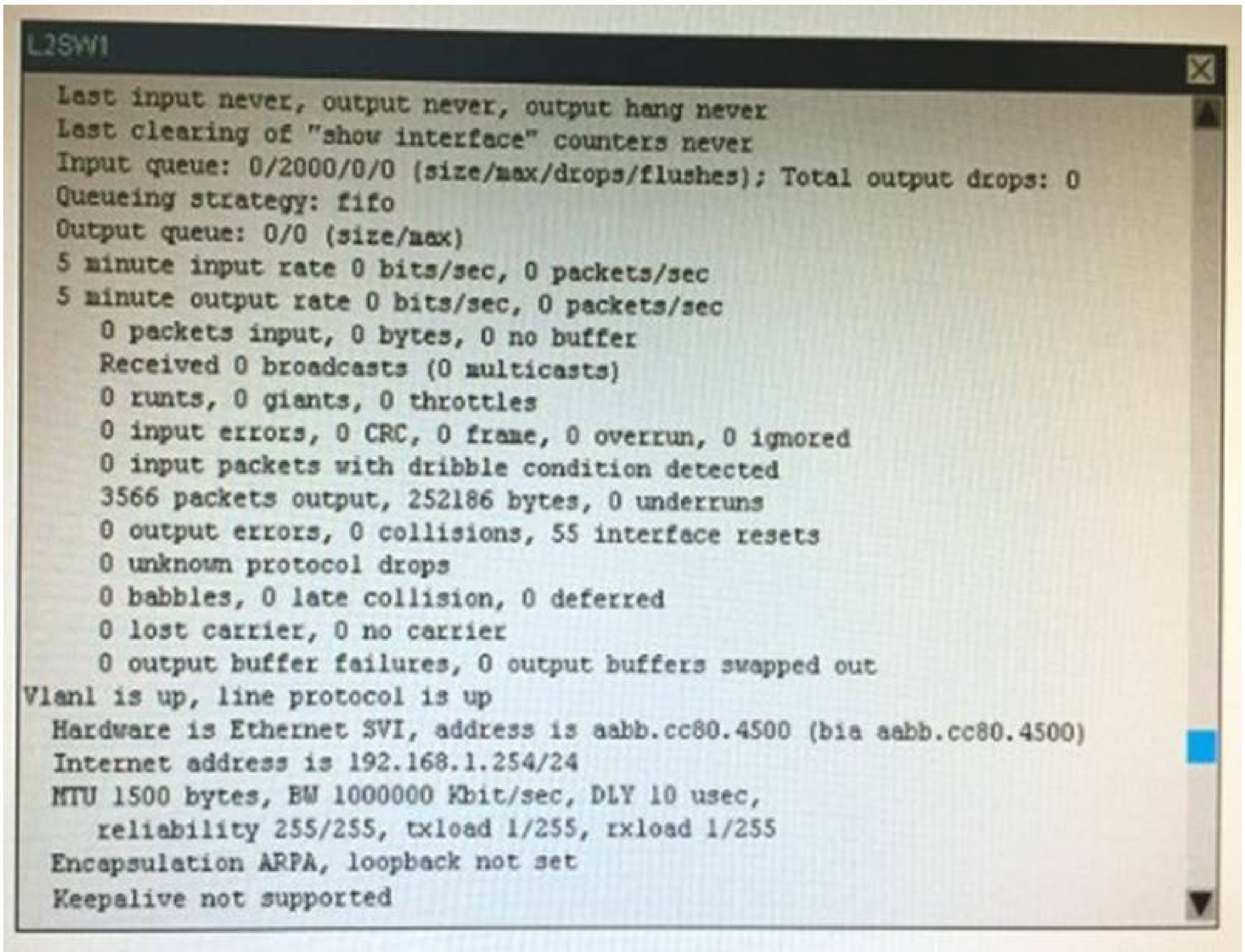
```
     13457 packets output, 919293 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/1 is up, line protocol is up (connected)
  Hardware is AmdP2, address is aabb.cc00.4510 (bia aabb.cc00.4510)
  Description: ***Link to Server1 segment***
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is unknown
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:07, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 5/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     755 packets input, 80219 bytes, 0 no buffer
     Received 123 broadcasts (0 multicasts)
```



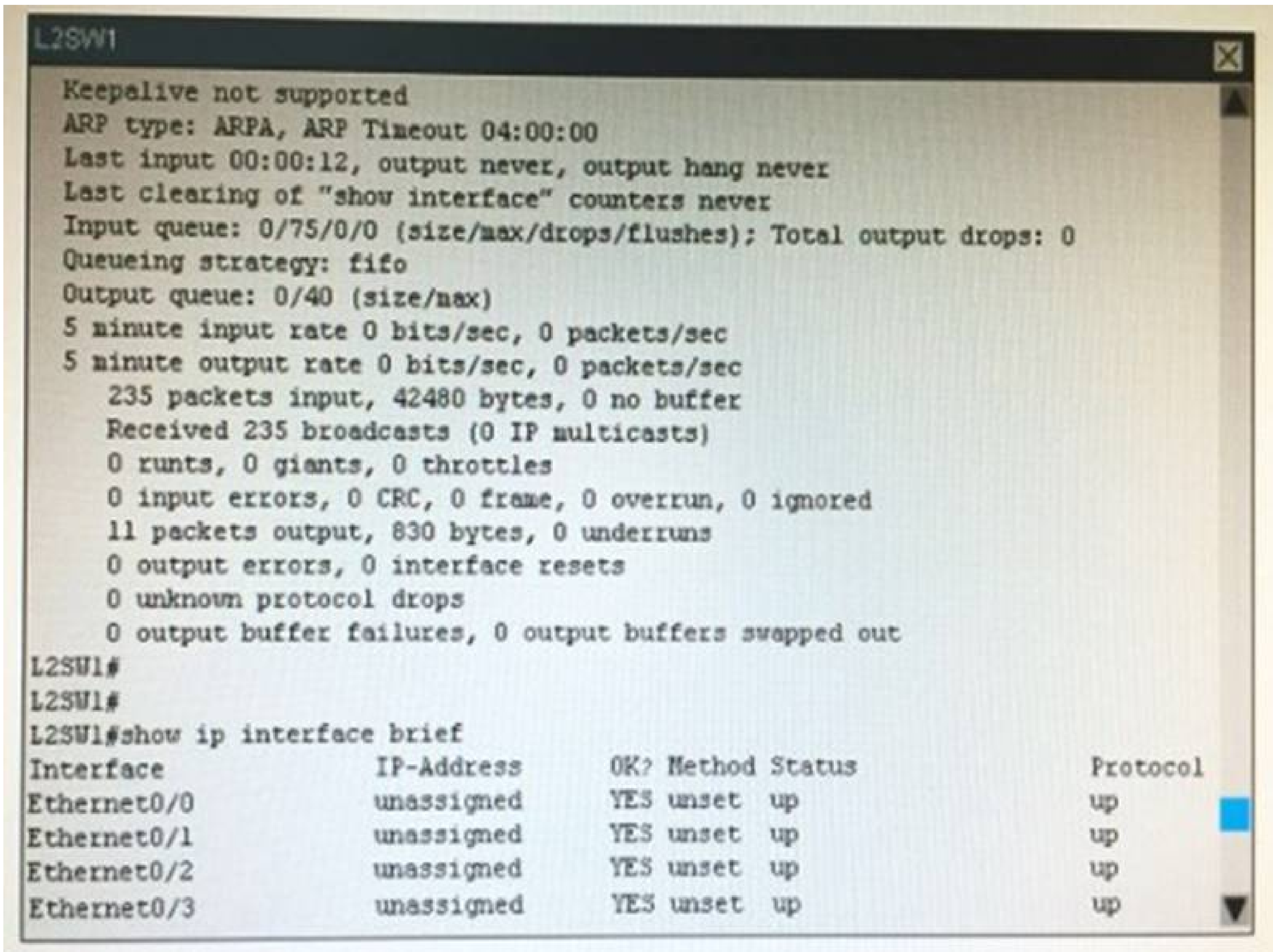
```
     755 packets input, 80219 bytes, 0 no buffer
     Received 123 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     3867 packets output, 268544 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/2 is up, line protocol is up (connected)
  Hardware is AmdP2, address is aabb.cc00.4520 (bia aabb.cc00.4520)
  Description: ***Link to Server2 Segment***
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is unknown
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:07, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 5/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```



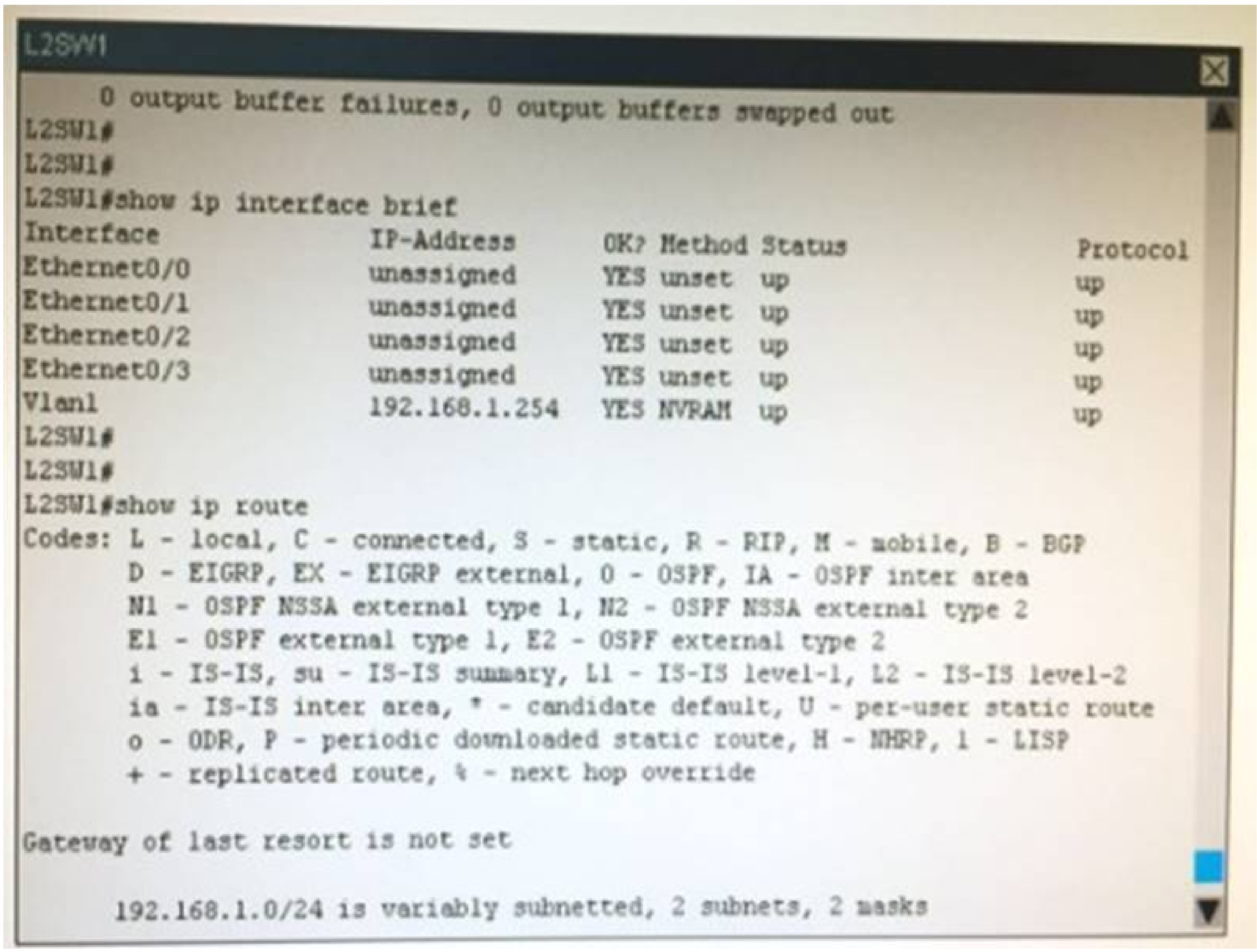
```
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     758 packets input, 81010 bytes, 0 no buffer
     Received 125 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     3867 packets output, 268544 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet0/3 is up, line protocol is up (connected)
  Hardware is AmdP2, address is aabb.cc00.4530 (bia aabb.cc00.4530)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is unknown
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
```



```
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     3566 packets output, 252186 bytes, 0 underruns
     0 output errors, 0 collisions, 55 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Vlan1 is up, line protocol is up
  Hardware is Ethernet SVI, address is aabb.cc80.4500 (bia aabb.cc80.4500)
  Internet address is 192.168.1.254/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
```

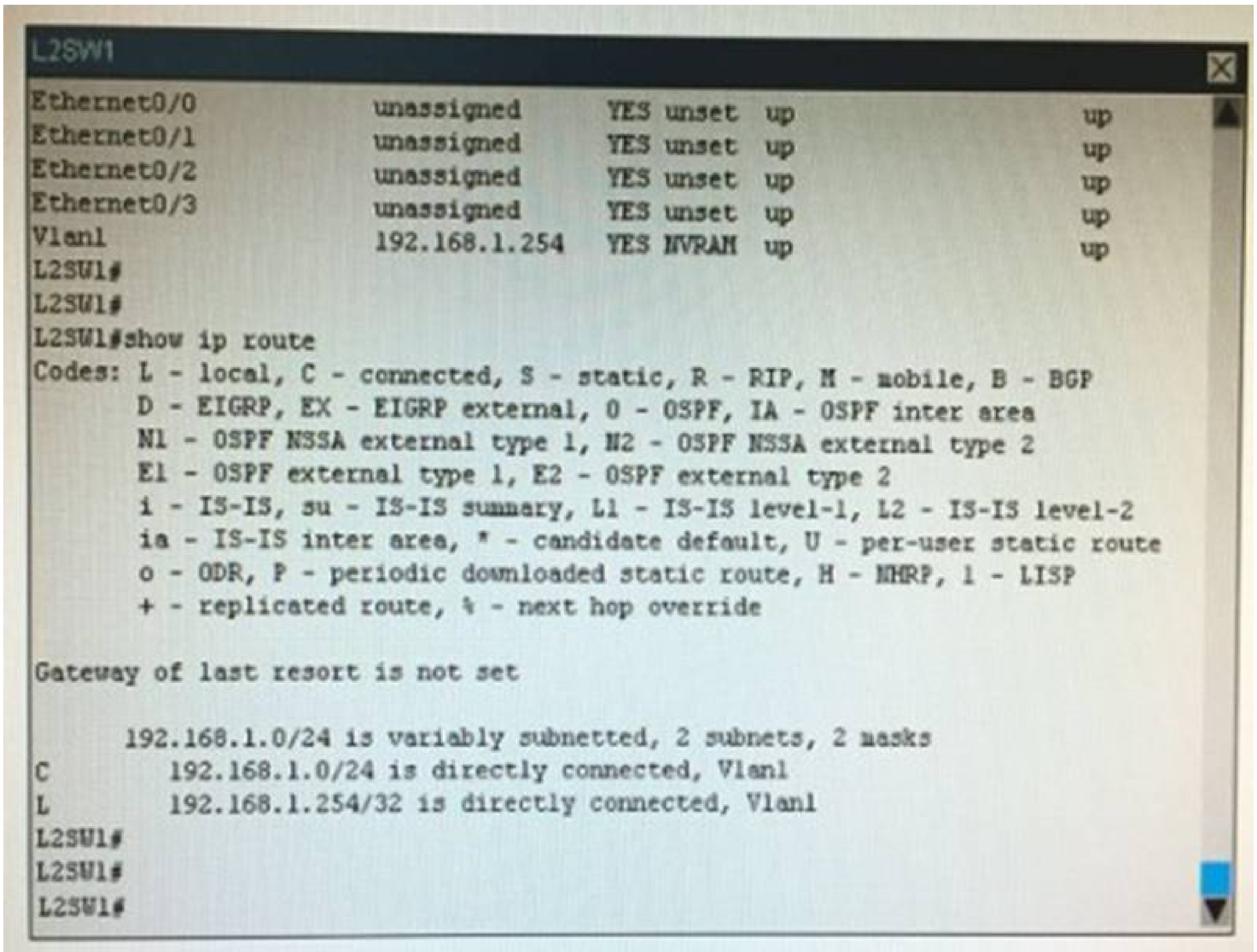


```
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:12, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     235 packets input, 42480 bytes, 0 no buffer
     Received 235 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     11 packets output, 830 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
L2SW1#
L2SW1#
L2SW1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
```



L2SW1

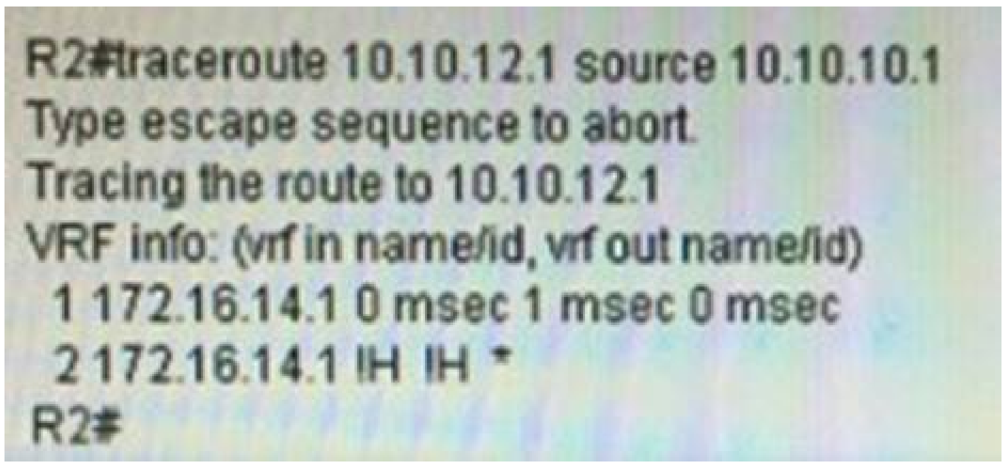
```
    0 output buffer failures, 0 output buffers swapped out
L2SW1#
L2SW1#
L2SW1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Vlan1                  192.168.1.254   YES NVRAM  up                    up
L2SW1#
L2SW1#
L2SW1#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
```



L2SW1

```
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Vlan1                  192.168.1.254   YES NVRAM  up                    up
L2SW1#
L2SW1#
L2SW1#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Vlan1
L        192.168.1.254/32 is directly connected, Vlan1
L2SW1#
L2SW1#
L2SW1#
```

Examine R2 configuration, the traffic that is destined to R3 LAN network sourced from Router R2 is forwarded to R1 instead R3. What could be an issue?

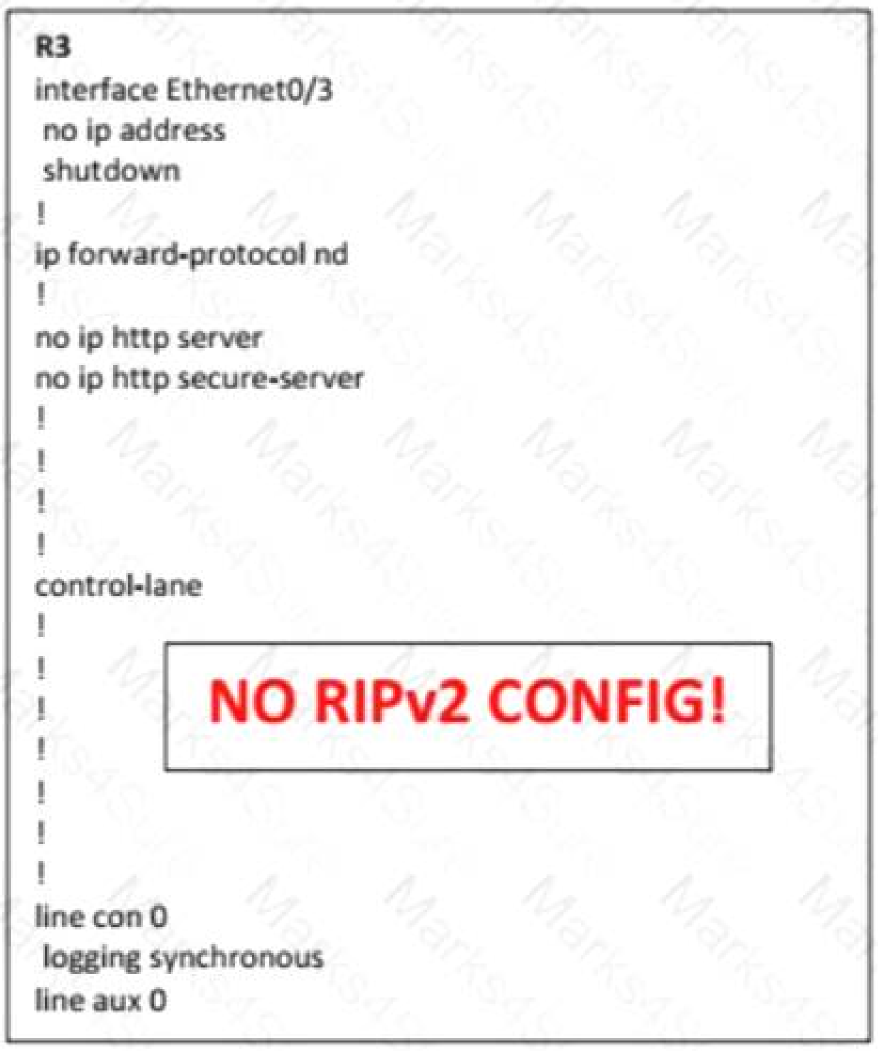


```
R2#traceroute 10.10.12.1 source 10.10.10.1
Type escape sequence to abort.
Tracing the route to 10.10.12.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.14.1 0 msec 1 msec 0 msec
  2 172.16.14.1 !H !H *
R2#
```

A. RIPv2 routing updates are suppressed between R2 and R3 using passive interface feature.
B. RIPv2 enabled on R3, but R3 LAN network that is not advertised into RIPv2 domain.
C. No issue that is identified; this behavior is normal since default route propagated into RIPv2 domain by Router R1.
D. RIPv2 not enabled on R3.

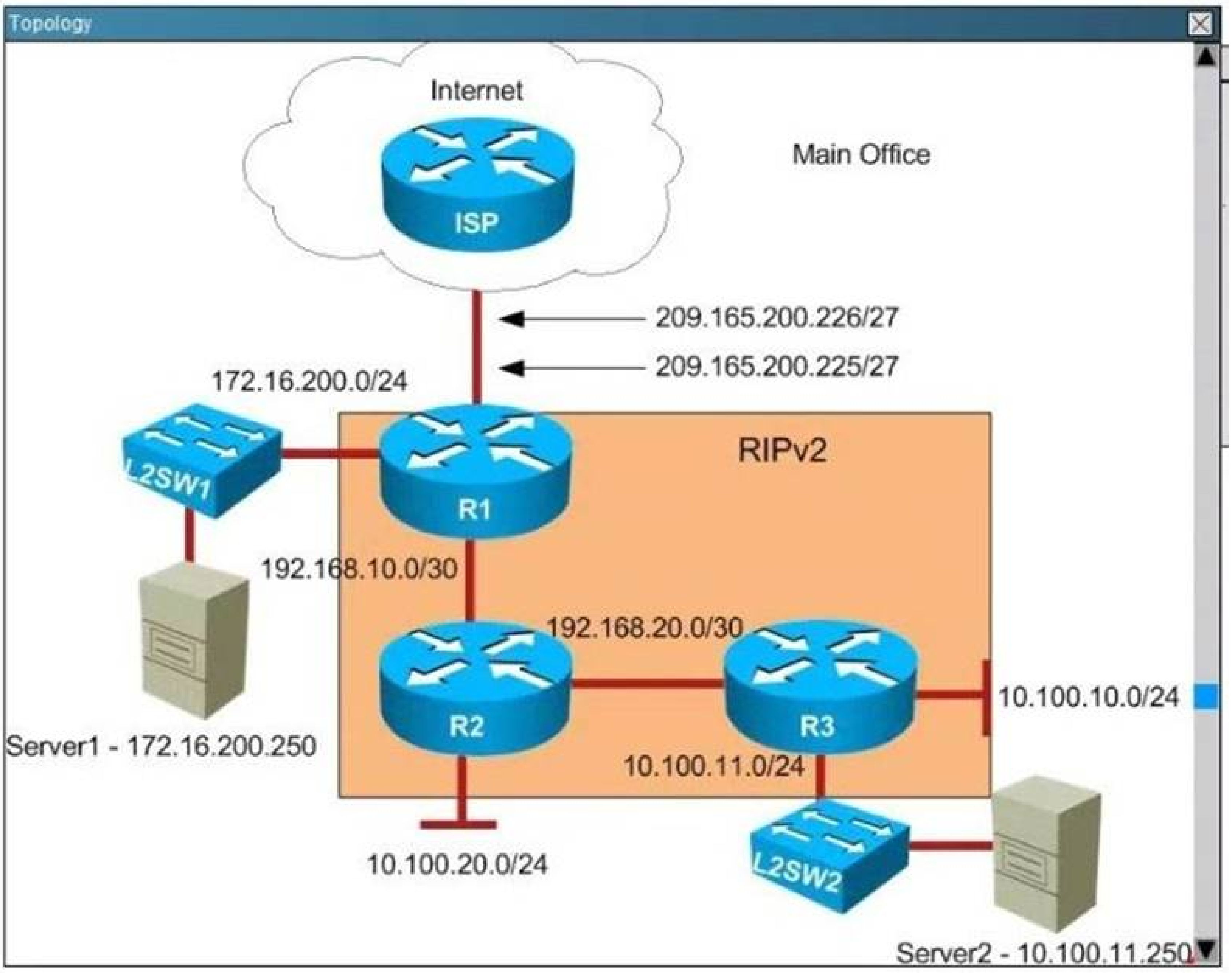
**Answer:** D

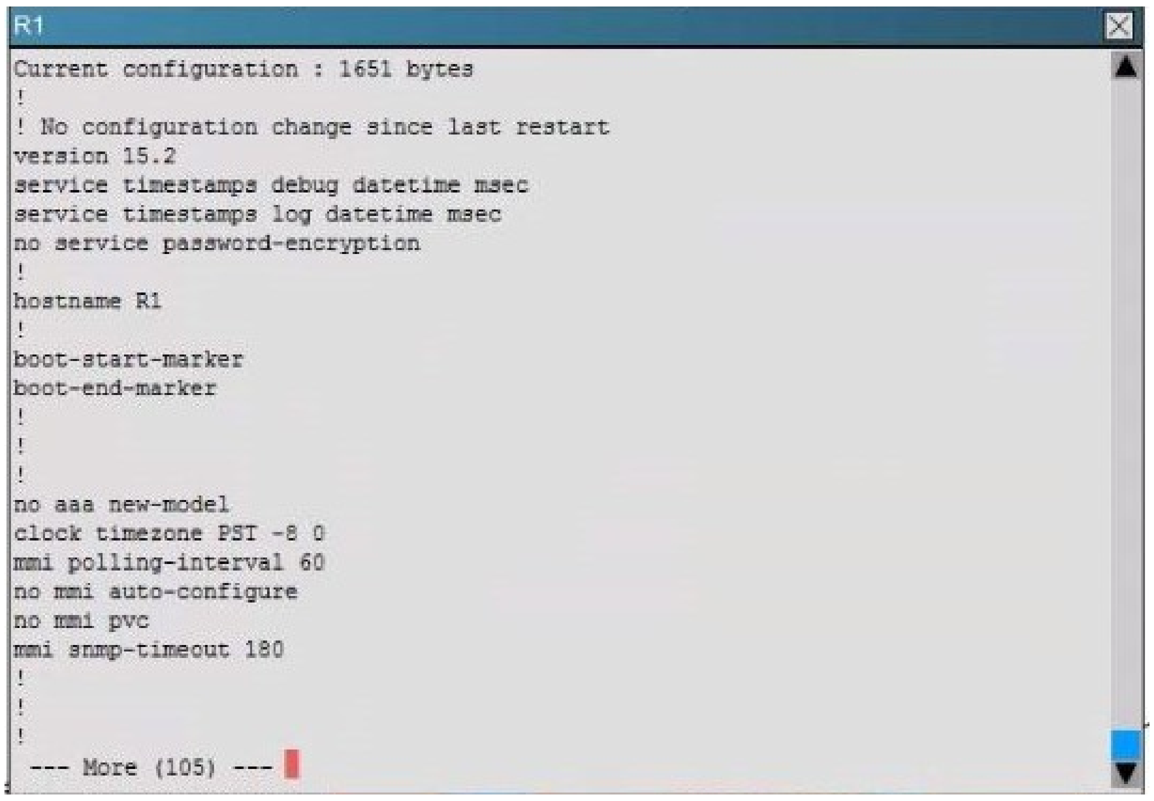
**Explanation:** As per R3



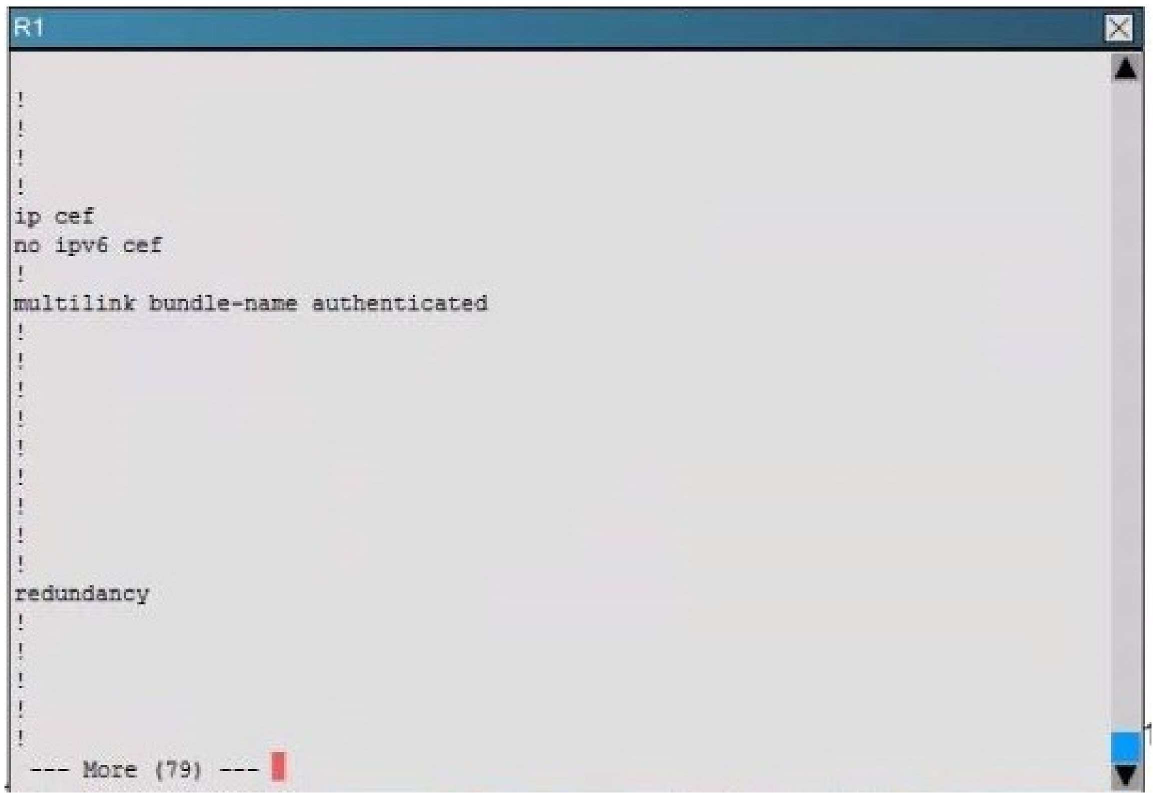
```
R3
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
control-lane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
```

**NEW QUESTION 338**
Scenario:
You are a junior network engineer for a financial company, and the main office network is experiencing network issues. Troubleshoot the network issues.
Router R1 connects the main office to the internet, and routers R2 and R3 are internal routers. NAT is enabled on router R1.
The routing protocol that is enabled between routers R1, R2 and R3 is RIPv2.
R1 sends the default route into RIPv2 for the internal routers to forward internet traffic to R1.
You have console access on R1, R2 and R3 devices. Use only show commands to troubleshoot the issues.

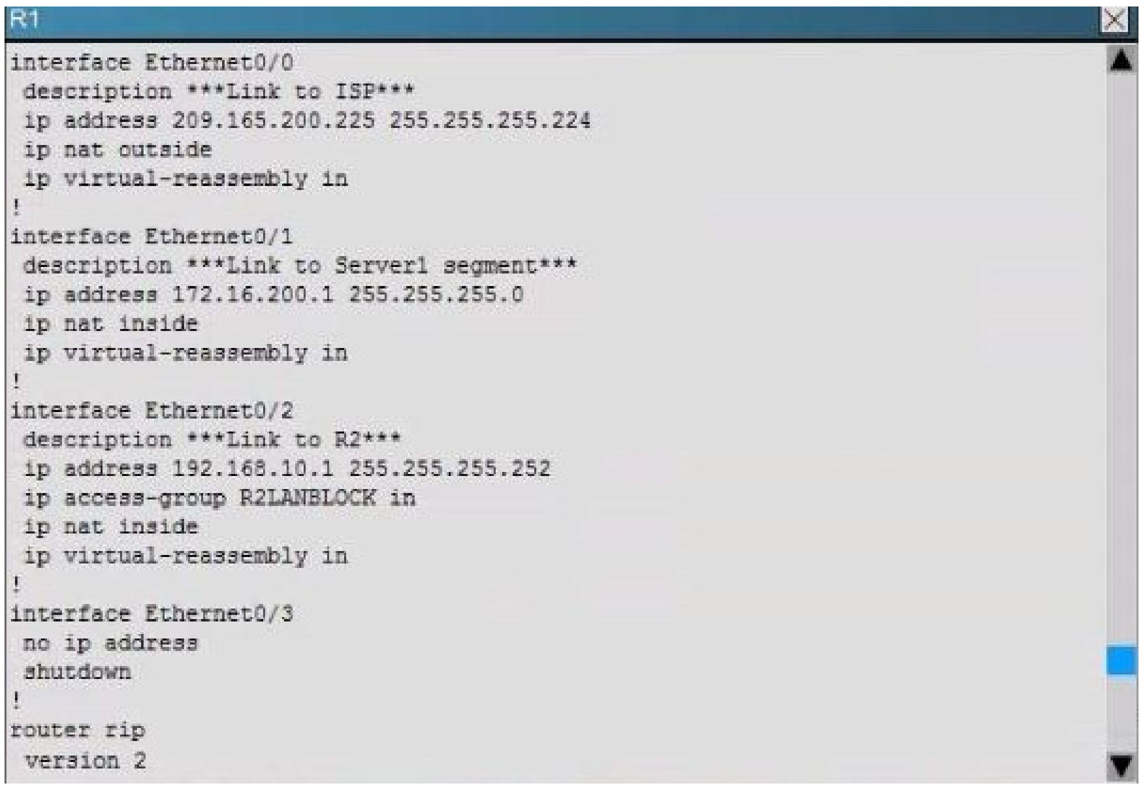




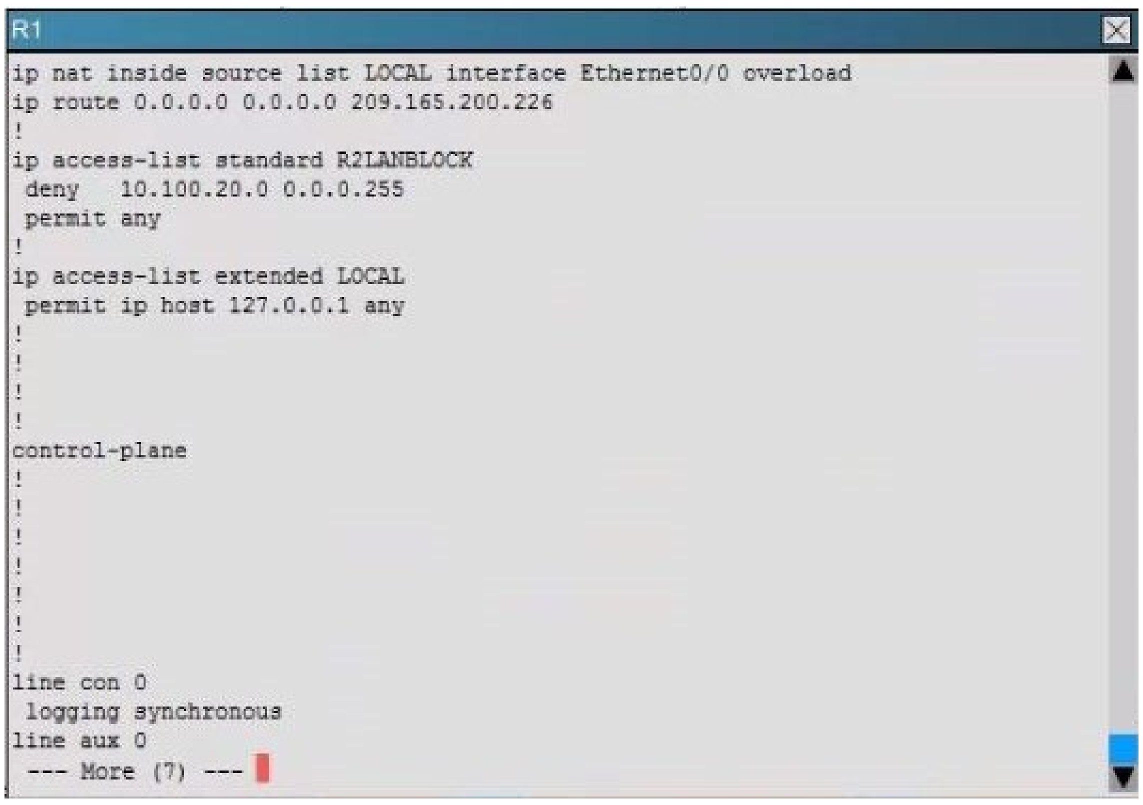
```
Current configuration : 1651 bytes
!
! No configuration change since last restart
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
 --- More (105) ---
```



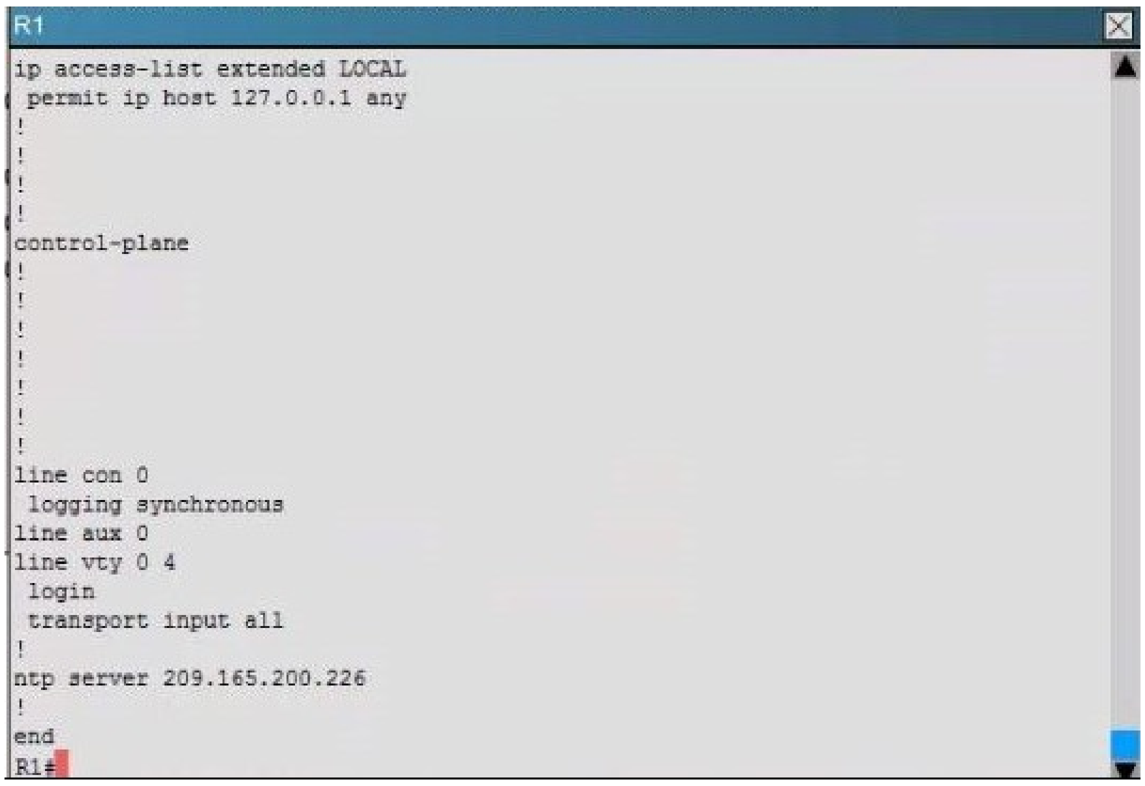
```
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
 --- More (79) ---
```



```
interface Ethernet0/0
 description ***Link to ISP***
 ip address 209.165.200.225 255.255.255.224
 ip nat outside
 ip virtual-reassembly in
!
interface Ethernet0/1
 description ***Link to Server1 segment***
 ip address 172.16.200.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/2
 description ***Link to R2***
 ip address 192.168.10.1 255.255.255.252
 ip access-group R2LANBLOCK in
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
```

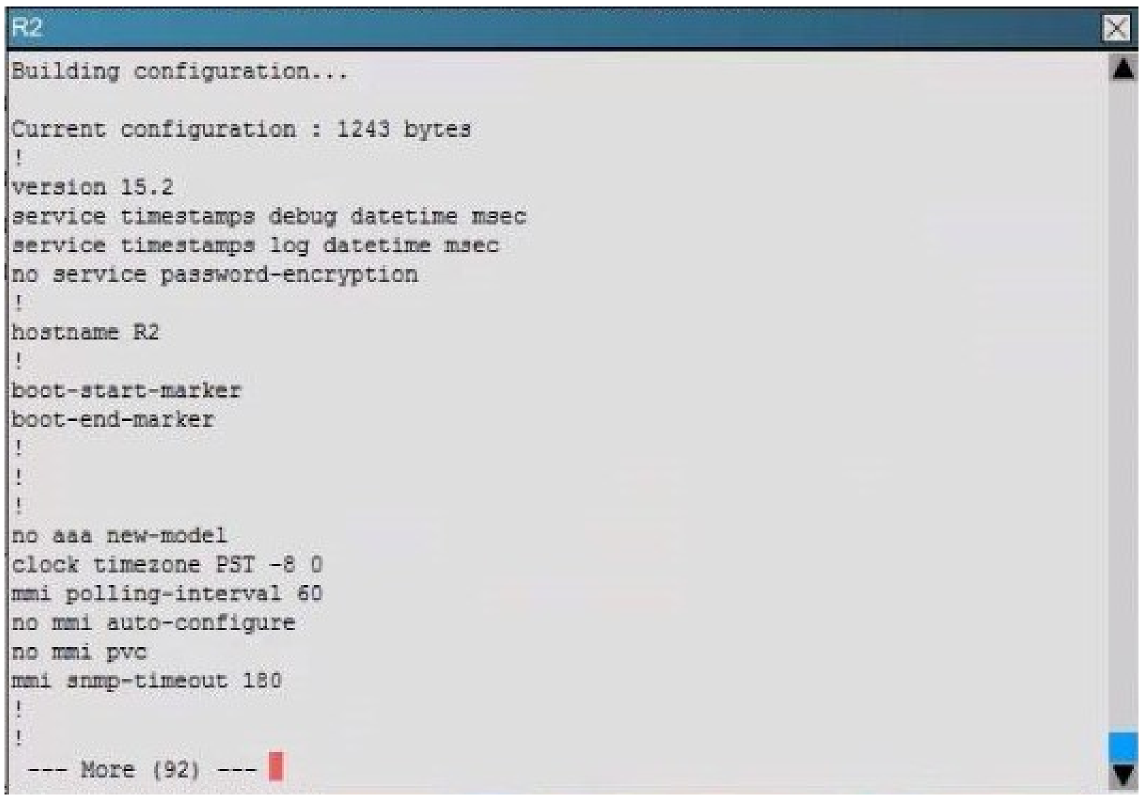


```
ip nat inside source list LOCAL interface Ethernet0/0 overload
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip access-list standard R2LANBLOCK
 deny   10.100.20.0 0.0.0.255
 permit any
!
ip access-list extended LOCAL
 permit ip host 127.0.0.1 any
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
 --- More (7) ---
```



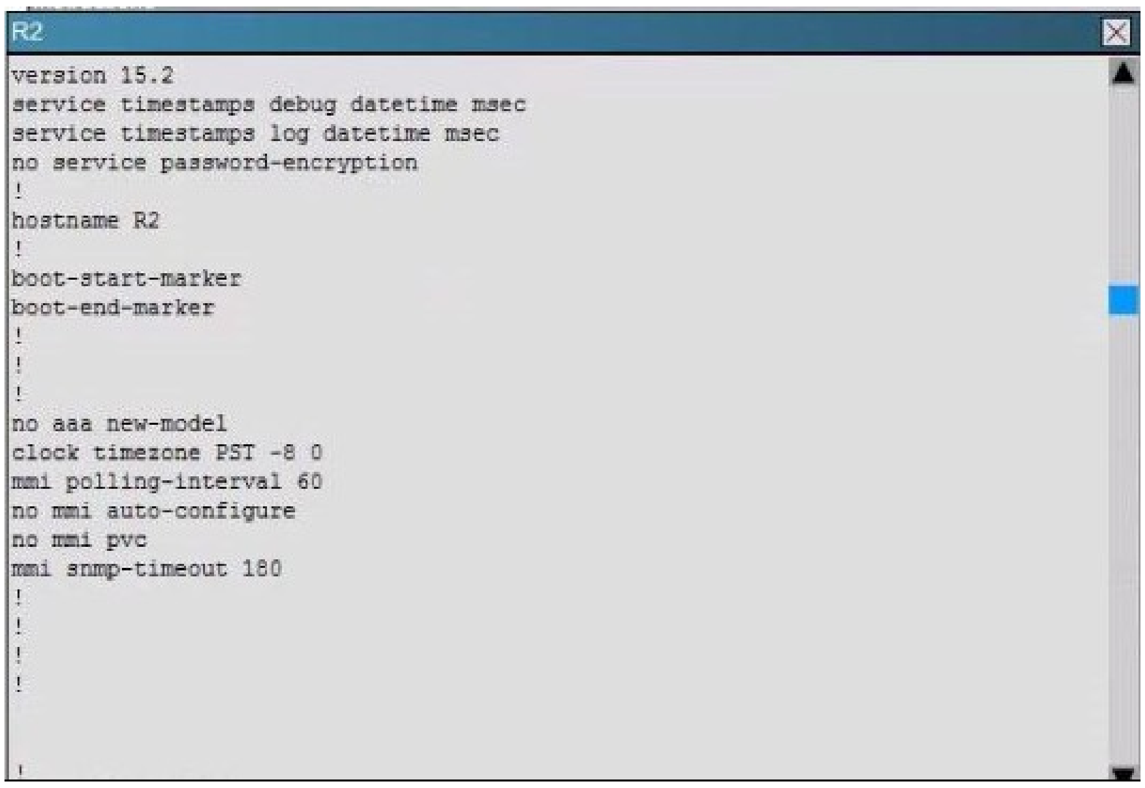
R1

```
ip access-list extended LOCAL
 permit ip host 127.0.0.1 any
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
ntp server 209.165.200.226
!
end
R1#
```



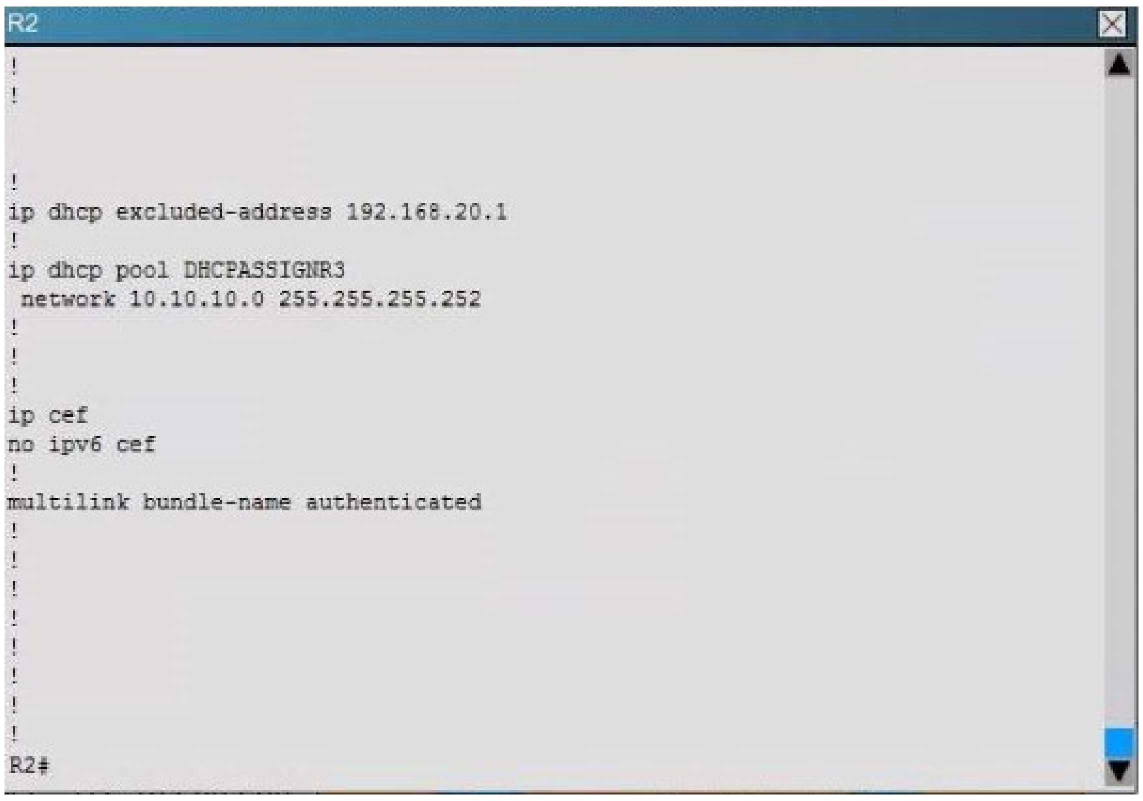
R2

```
Building configuration...

Current configuration : 1243 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
 --- More (92) ---
```

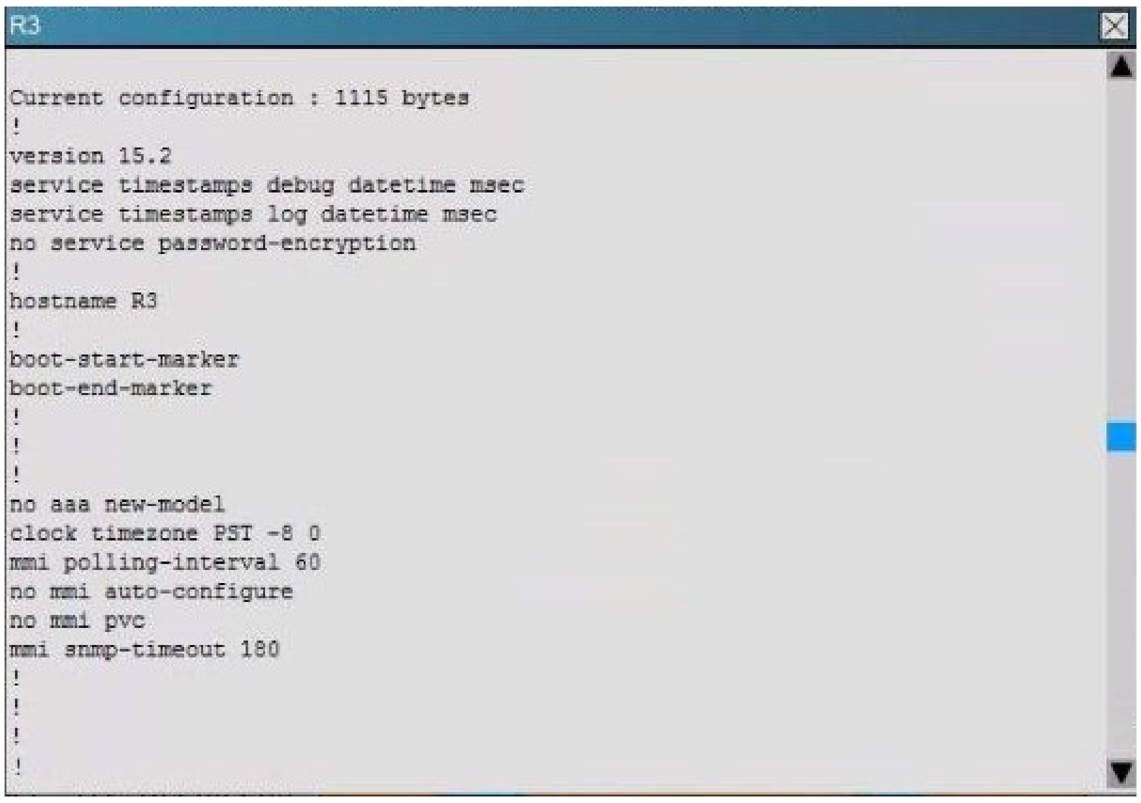


R2

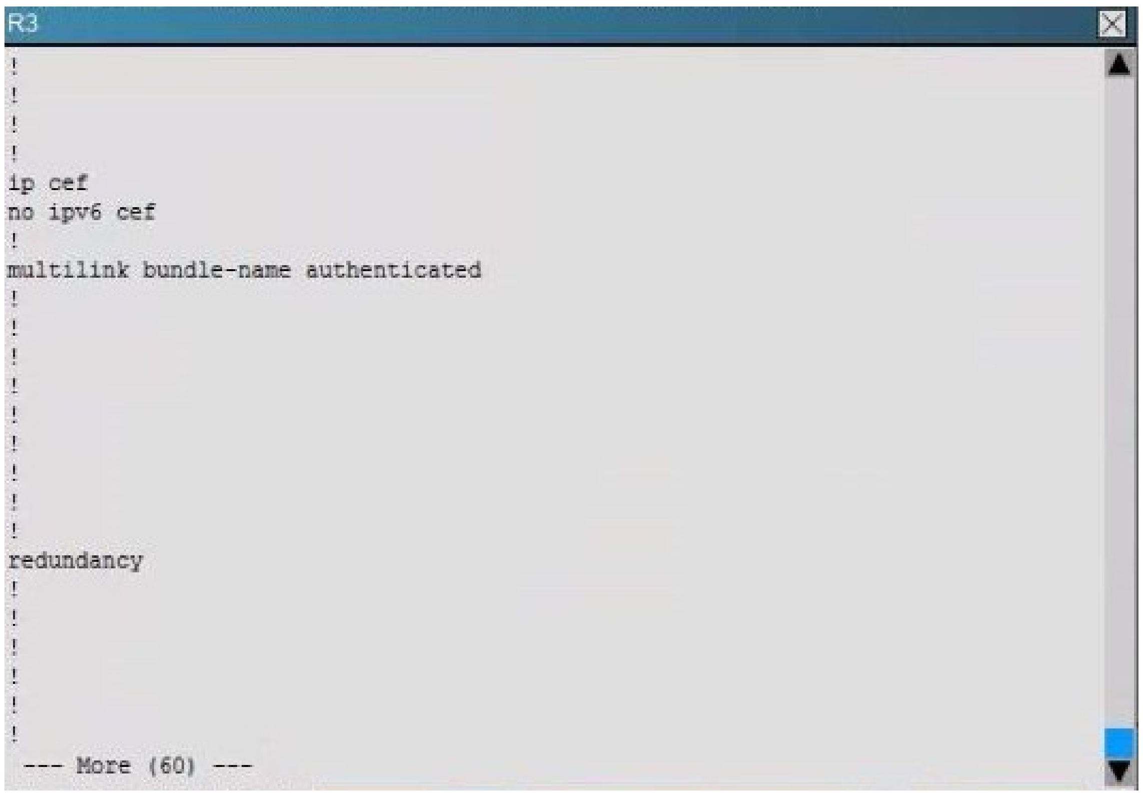
```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!


!
```



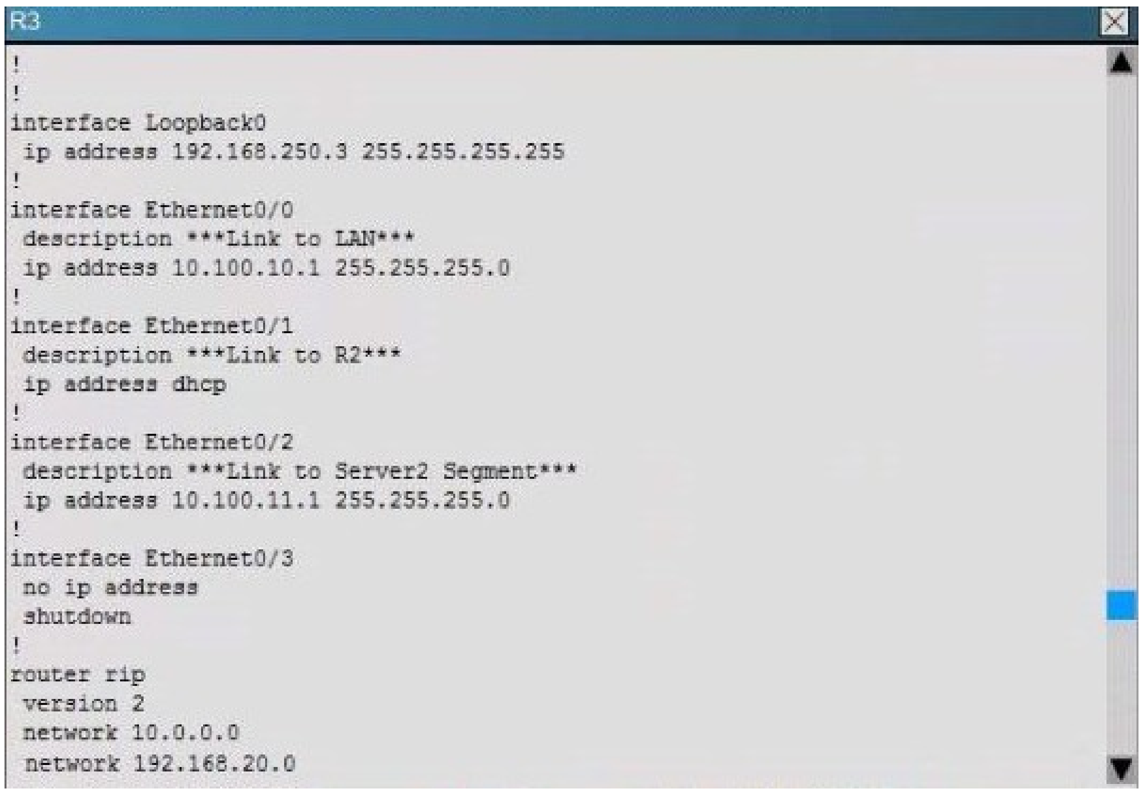
```
!
!


!
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool DHCPASSIGNR3
 network 10.10.10.0 255.255.255.252
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
R2#
```



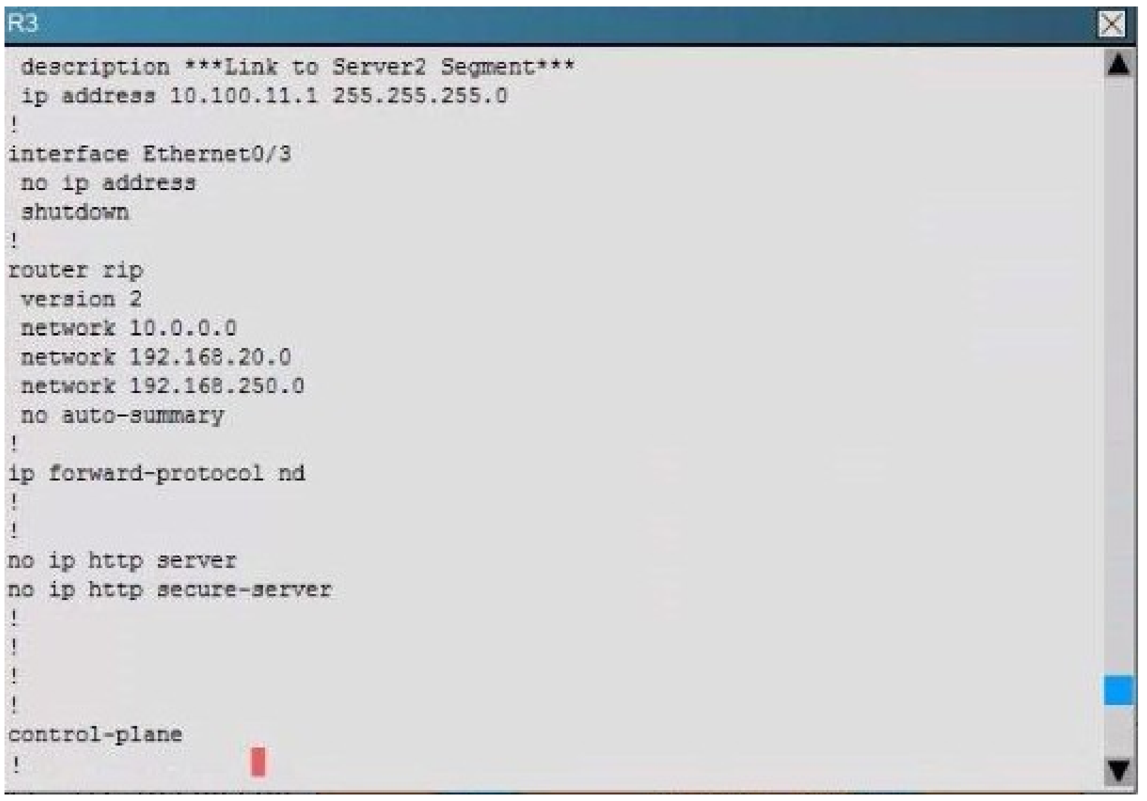
```

Current configuration : 1115 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
```



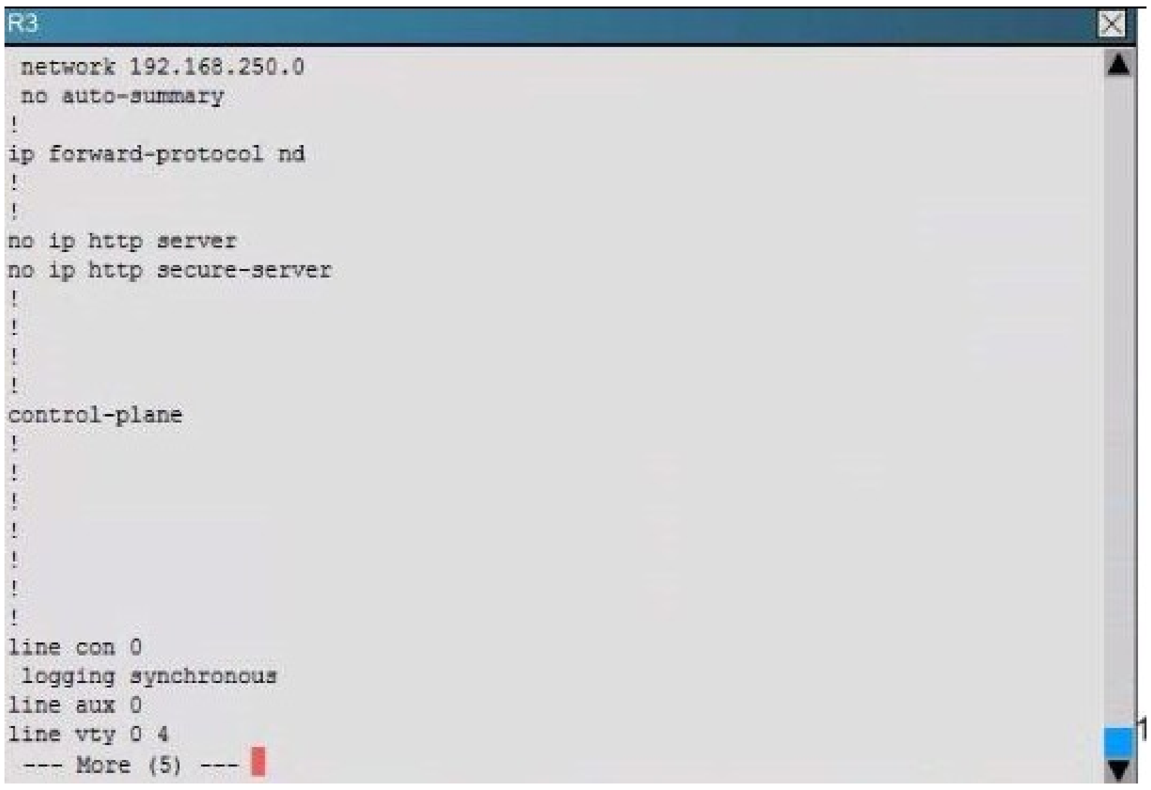
```
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
 --- More (60) ---
```



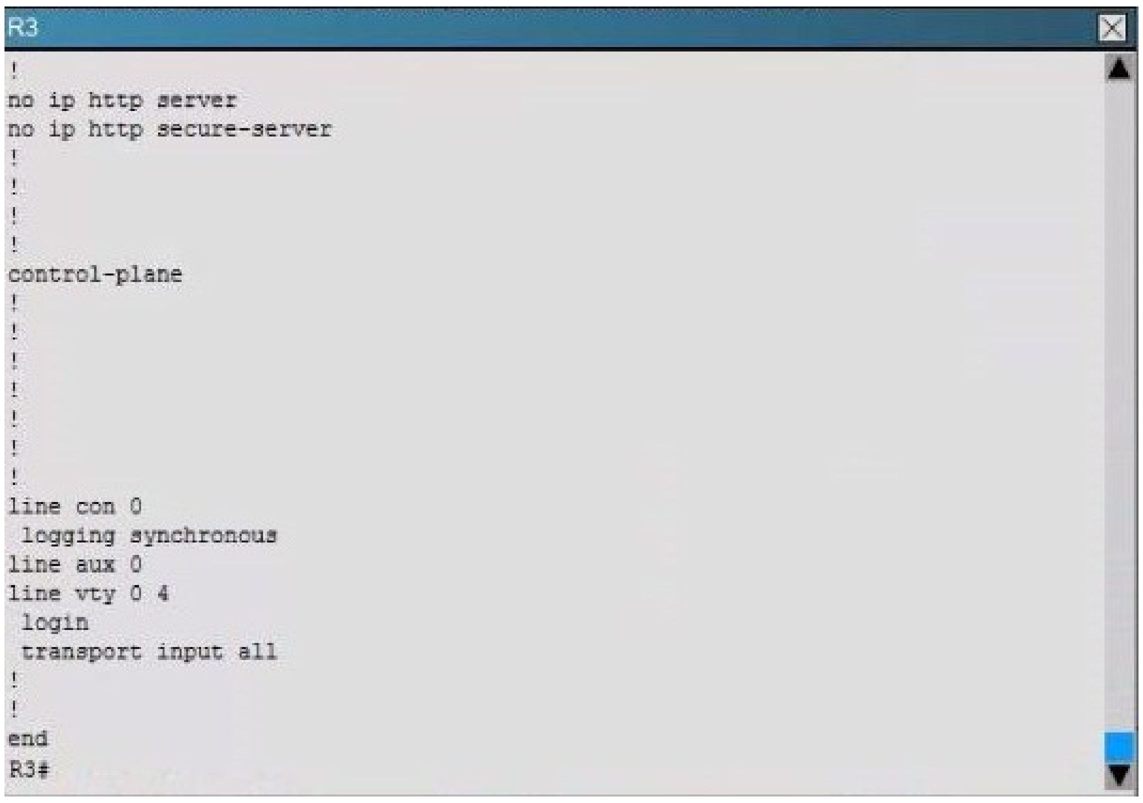
```
!
!
interface Loopback0
 ip address 192.168.250.3 255.255.255.255
!
interface Ethernet0/0
 description ***Link to LAN***
 ip address 10.100.10.1 255.255.255.0
!
interface Ethernet0/1
 description ***Link to R2***
 ip address dhcp
!
interface Ethernet0/2
 description ***Link to Server2 Segment***
 ip address 10.100.11.1 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.20.0
```



```
 description ***Link to Server2 Segment***
 ip address 10.100.11.1 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.20.0
 network 192.168.250.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
```



```
 network 192.168.250.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 --- More (5) ---
```



R3

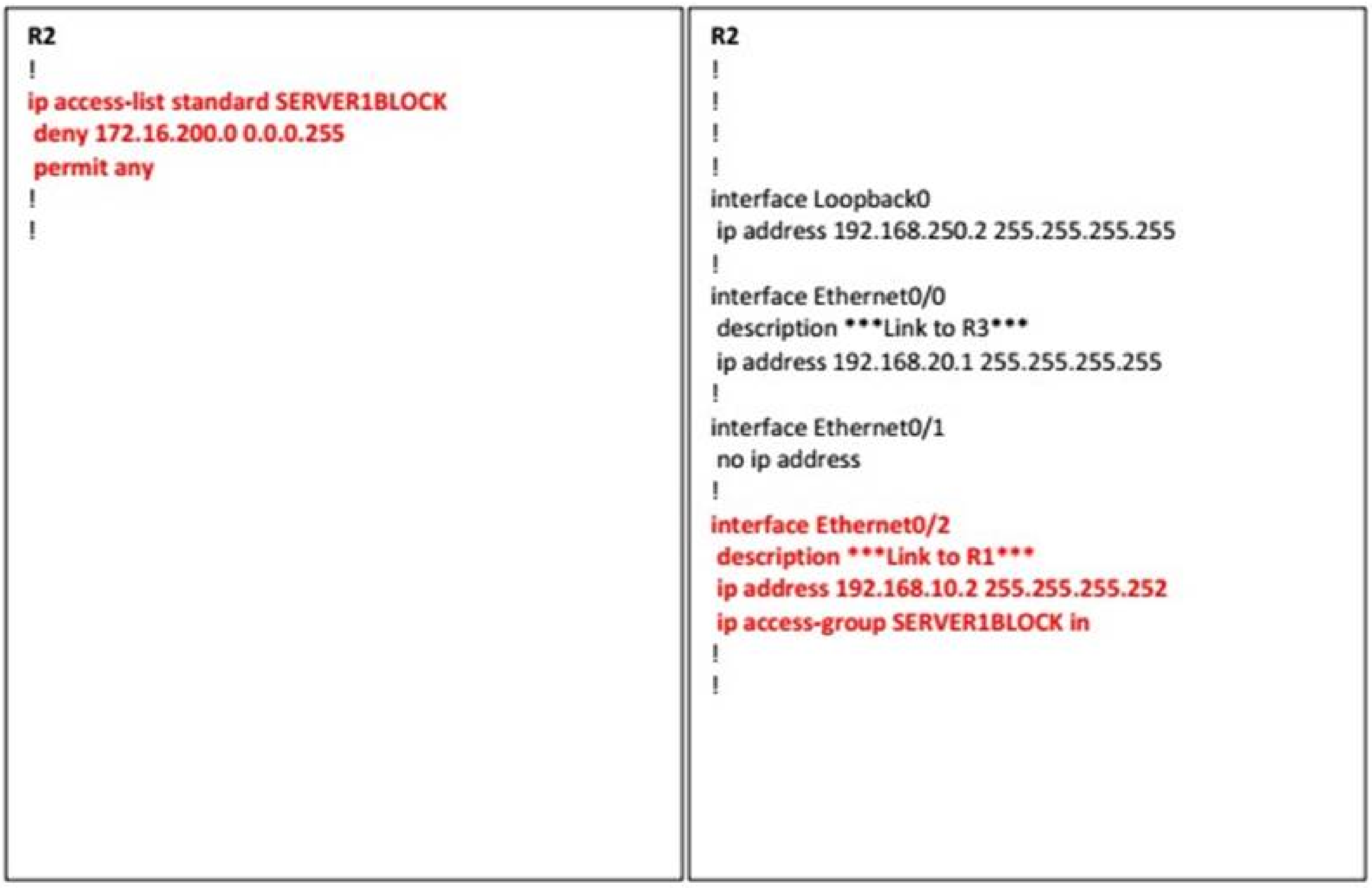
```
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
!
end
R3#
```

Why applications that are installed on PC's in R2 LAN network 10.100.20.0/24 are unable to communicate with server1?

A. A standard ACL statement that is configured on R1 is blocking the traffic sourced from Server1 network.
B. A standard ACL statement that is configured on R2 is blocking the traffic sourced from Setver1 network.
C. A standard ACL statement that is configured on R2 is blocking the traffic sourced from R2 LAN network.
D. A standard ACL statement that is configured on R1 is blocking the traffic sourced from R2 LAM network

**Answer:** B

**Explanation:** Check the below now:



```
R2
!
ip access-list standard SERVER1BLOCK
 deny 172.16.200.0 0.0.0.255
 permit any
!
!
```

```
R2
!
!
!
!
interface Loopback0
 ip address 192.168.250.2 255.255.255.255
!
interface Ethernet0/0
 description ***Link to R3***
 ip address 192.168.20.1 255.255.255.255
!
interface Ethernet0/1
 no ip address
!
interface Ethernet0/2
 description ***Link to R1***
 ip address 192.168.10.2 255.255.255.252
 ip access-group SERVER1BLOCK in
!
!
```

**NEW QUESTION 343**
Which NAT type is used to translate a single inside address to a single outside address?

A. dynamic NAT
B. NAT overload
C. PAT
D. static NAT

**Answer:** D

**Explanation:** Network address translation (NAT) is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device.
There are two different types of NAT:
 NAT
 Static NAT: The simplest type of NAT provides oane-to-one translation of IP addresses.

It is often also referred to as one-to-one NAT. In this type of NAT only the IP addresses, IP header checksum and any higher level checksums that include the IP address need to be changed. The rest of the packet can be left untouched (at least for basic TCP/UDP functionality, some higher level protocols may need further translation). Basic NATs can be used when there is a requirement to interconnect two IP networks with incompatible addressing. With static NAT, translations exist in the NAT translation table as soon as you configure static NAT command(s), and they remain in the translation table until you delete the static NAT command(s).
Dynamic NAT: Dynamic NAT has some similarities and differences compared to static NAT. Like static NAT, the NAT router creates a one-to-one mapping between an inside local and inside global address and changes the IP addresses in packets as they exit and enter the inside network. However, the mapping of an inside local address to an inside global address happens dynamically. Dynamic NAT sets up a pool of possible inside global addresses and defines matching criteria to determine which inside local IP addresses should be translated with NAT. The dynamic entry stays in the table as long as traffic flows occasionally. With dynamic NAT, translations do not exist in the NAT table until the router receives traffic that requires translation. Dynamic translations have a timeout period after which they are purged from the translation table.
PAT
Static PAT: Static PAT translations allow a specific UDP or TCP port on a global address to be translated to a specific port on a local address. Static PAT is the same as static NAT, except that it enables you to specify the protocol (TCP or UDP) and port for the real and mapped addresses. Static PAT enables you to identify the same mapped address across many different static statements, provided that the port is different for each statement. You cannot use the same mapped address for multiple static NAT statements. With static PAT, translations exist in the NAT translation table as soon as you configure static PAT command(s), and they remain in the translation table until you delete the static PAT command(s).
NAT Overload or PAT: It is common to hide an entire IP address space, usually consisting of private IP addresses, behind a single IP address (or in some cases a small group of IP addresses) in another (usually public) address space. This type of NAT is called PAT in overload. The dynamic entry stays in the table as long as traffic flows occasionally. With PAT in overload, translations do not exist in the NAT table until the router receives traffic that requires translation. Translations have a timeout period after which they are purged from the translation table.

**NEW QUESTION 344**
Which statement about static routes is true?

A. The source interface can be configured to make routing decisions.
B. A subnet mask is entered for the next-hop address.
C. The subnet mask is 255.255 255.0 by default
D. The exit interface can be specified to indicate where the packets will be routed.

**Answer:** D

**Explanation:** Static routing can be used to define an exit point from a router when no other routes are available or necessary. This is called a default route.

**NEW QUESTION 347**
Which device allows users to connect to the network using a single or double radio?

A. access point
B. switch
C. wireless controller
D. firewall

**Answer:** A

**NEW QUESTION 348**
When enabled, which feature prevents routing protocols from sending hello messages on an interface'?

A. virtual links
B. passive-interface
C. directed neighbors
D. OSPF areas

**Answer:** B

**Explanation:** You can use the passive-interfacecommand in order to control the advertisement of routing information. The command enables the suppression of routing updates over some interfaces while it allows updates to be exchanged normally over other interfaces.
With most routing protocols, the passive-interface command restricts outgoing advertisements only. But, when used with Enhanced Interior Gateway Routing Protocol (EIGRP), the effect is slightly different. This document demonstrates that use of the passive-interface command in EIGRP suppresses the exchange of hello packets between two routers, which results in the loss of their neighbor relationship. This stops not only routing updates from being advertised, but it also suppresses incoming routing updates. This document also discusses the configuration required in order to allow the suppression of outgoing routing updates, while it also allows incoming routing updates to be learned normally from the neighbor.

**NEW QUESTION 352**
Which statement about native VLAN traffic is true?

A. Cisco Discovery Protocol traffic travels on the native VLAN by default
B. Traffic on the native VLAN is tagged with 1 by default
C. Control plane traffic is blocked on the native VLAN.
D. The native VLAN is typically disabled for security reasons

**Answer:** A

**NEW QUESTION 355**
What is the default lease time for a DHCP binding?

A. 24 hours

B. 12 hours
C. 48 hours
D. 36 hours

**Answer:** A

**Explanation:** By default, each IP address assigned by a DHCP Server comes with a one-day lease, which is the amount of time that the address is valid. To change the lease value for an IP address, use the following command in DHCP pool configuration mode:

**NEW QUESTION 360**
On which type of device is every port in the same collision domain?

A. a router
B. a Layer 2 switch
C. a hub

**Answer:** C

**Explanation:** Collision domain
A collision domain is, as the name implies, a part of a network where packet collisions can occur. A collision occurs when two devices send a packet at the same time on the shared network segment. The packets collide and both devices must send the packets again, which reduces network efficiency. Collisions are often in a hub environment, because each port on a hub is in the same collision domain. By contrast, each port on a bridge, a switch or a router is in a separate collision domain.

**NEW QUESTION 363**
Which value is indicated by the next hop in a routing table?

A. preference of the route source
B. IP address of the remote router for forwarding the packets
C. how the route was learned
D. exit interface IP address for forwarding the packets

**Answer:** D

**Explanation:** The routing table contains network/next hop associations. These associations tell a router that a particular destination can be optimally reached by sending the packet to a specific router that represents the "next hop" on the way to the final destination. The next hop association can also be the outgoing or exit interface to the final destination.

**NEW QUESTION 364**
Which feature allows a device to use a switch port that is configured for half-duplex to access the network?

A. CSMA/CD
B. IGMP
C. port security
D. split horizon

**Answer:** A

**Explanation:** Ethernet began as a local area network technology that provided a half-duplex shared channel for stations connected to coaxial cable segments linked with signal repeaters. In this appendix, we take a detailed look at the half-duplex shared-channel mode of operation, and at the CSMA/CD mechanism that makes it work.
In the original half-duplex mode, the CSMA/CD protocol allows a set of stations to compete for access to a shared Ethernet channel in a fair and equitable manner. The protocol's rules determine the behavior of Ethernet stations, including when they are allowed to transmit a frame onto a shared Ethernet channel, and what to do when a collision occurs.
Today, virtually all devices are connected to Ethernet switch ports over full-duplex media, such as twisted-pair cables. On this type of connection, assuming that both devices can support the full-duplex mode of operation and that Auto-Negotiation (AN) is enabled, the AN protocol will automatically select the highest-performance
mode of operation supported by the devices at each end of the link. That will result in full-duplex mode for the vast majority of Ethernet connections with modern interfaces that support full duplex and AN.

**NEW QUESTION 366**
Which NTP command configures the local device as an NTP reference clock source?

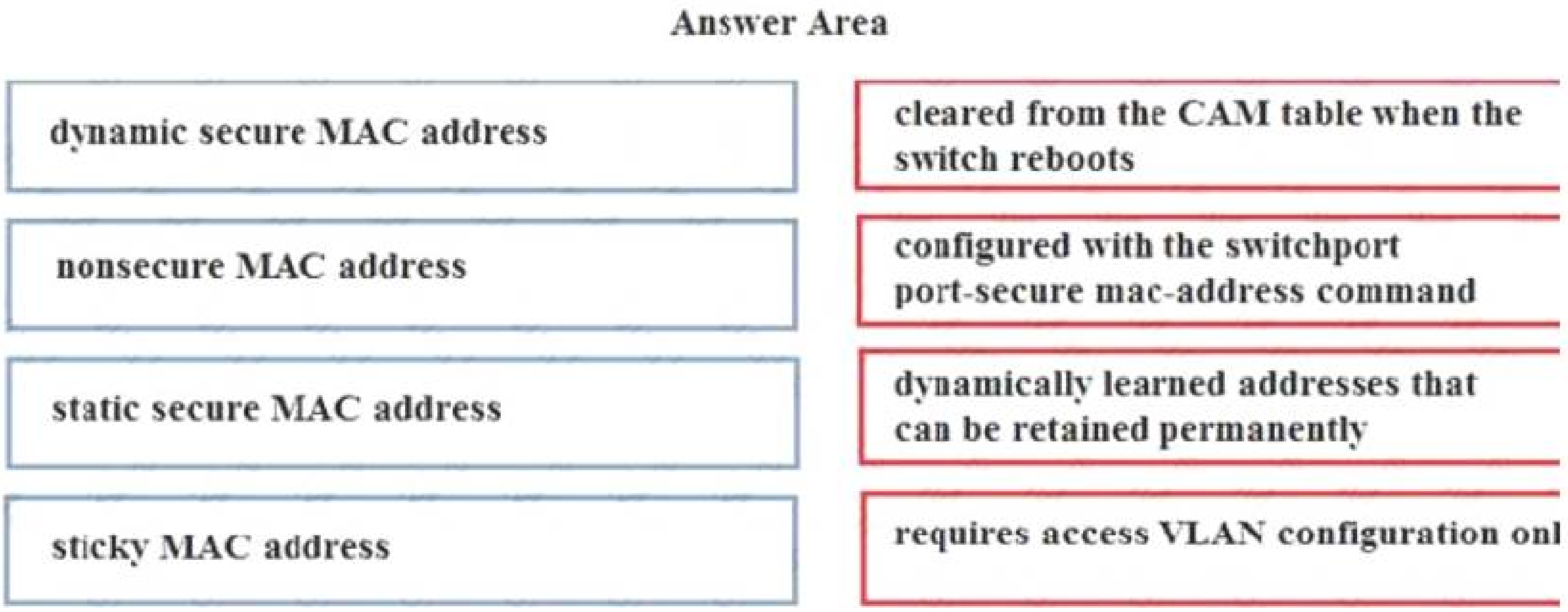
A. ntp peer
B. ntp broadcast
C. ntp master
D. ntp server

**Answer:** D

**Explanation:** Topic 8, NEW QUESTION B

**NEW QUESTION 370**

Drag and drop the MAC address types from the left onto the correct descriptions on the right?
Select and Place:

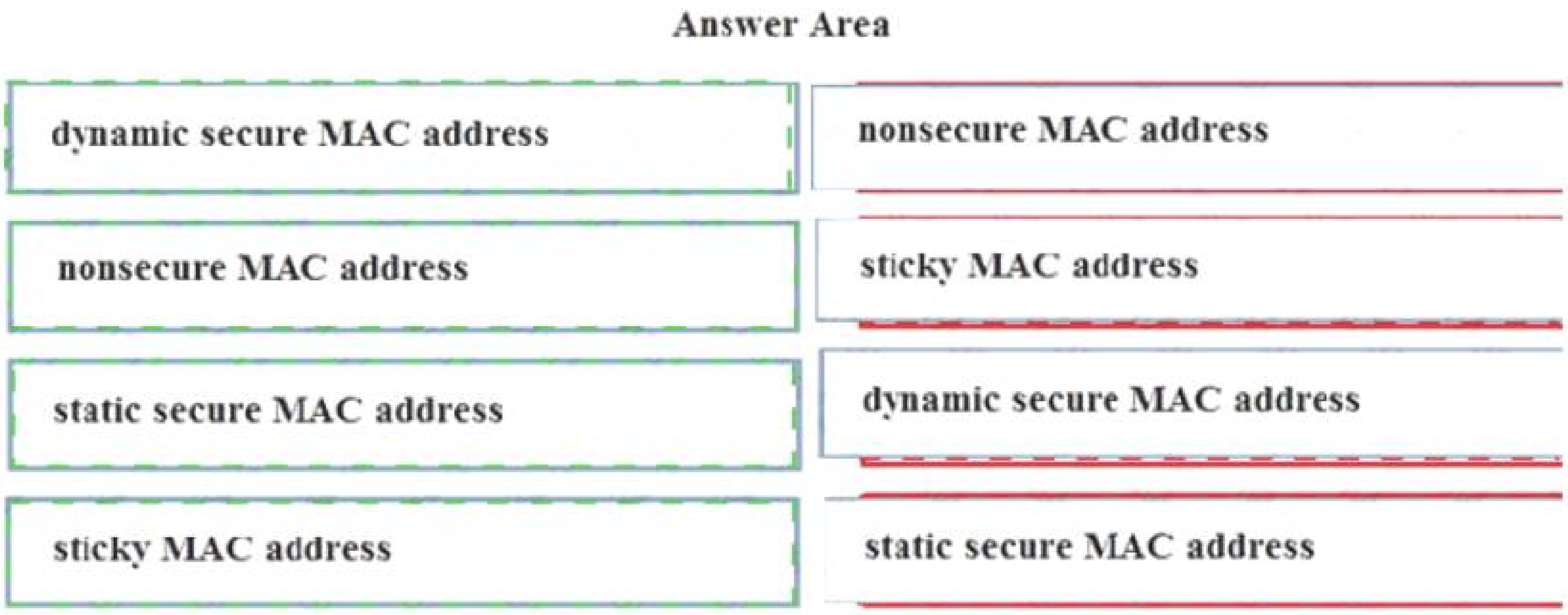


Answer Area

| | |
|---|---|
| dynamic secure MAC address | cleared from the CAM table when the switch reboots |
| nonsecure MAC address | configured with the switchport port-secure mac-address command |
| static secure MAC address | dynamically learned addresses that can be retained permanently |
| sticky MAC address | requires access VLAN configuration onl |

**Answer:**

**Explanation:**



Answer Area

| | |
|---|---|
| dynamic secure MAC address | nonsecure MAC address |
| nonsecure MAC address | sticky MAC address |
| static secure MAC address | dynamic secure MAC address |
| sticky MAC address | static secure MAC address |

**NEW QUESTION 371**
How does a Layer 2 switch differ from a hub?

A. A switch tracks MAC addresses of directly-connected devices.
B. A switch always induces latency into the frame transfer time.
C. A switch operates at a lower, more efficient layer of the OSI model.
D. A switchdecreases the number of collision domains.

**Answer:** A

**NEW QUESTION 374**
How many bits comprise an IPv6 address?

A. 32 bits
B. 64 bits
C. 128 bits
D. 256 bits

**Answer:** C

**NEW QUESTION 378**
Which symptom most commonly indicates that two connecting interfaces are configured with a duplex mismatch?

A. the spanning-tree process shutting down
B. collisions on the interface
C. an interface with a down/down status
D. an interface with an up/down status

**Answer:** B

**NEW QUESTION 382**
You are configuring dynamic NAT on your Cisco IOS router. Which command is used to verify the interfaces that are being used as the outside interface and the inside interface?

A. show interfaces
B. show ip route
C. show ipnat translations
D. show ip interface brief
E. show ip interface
F. show ipnat statistics

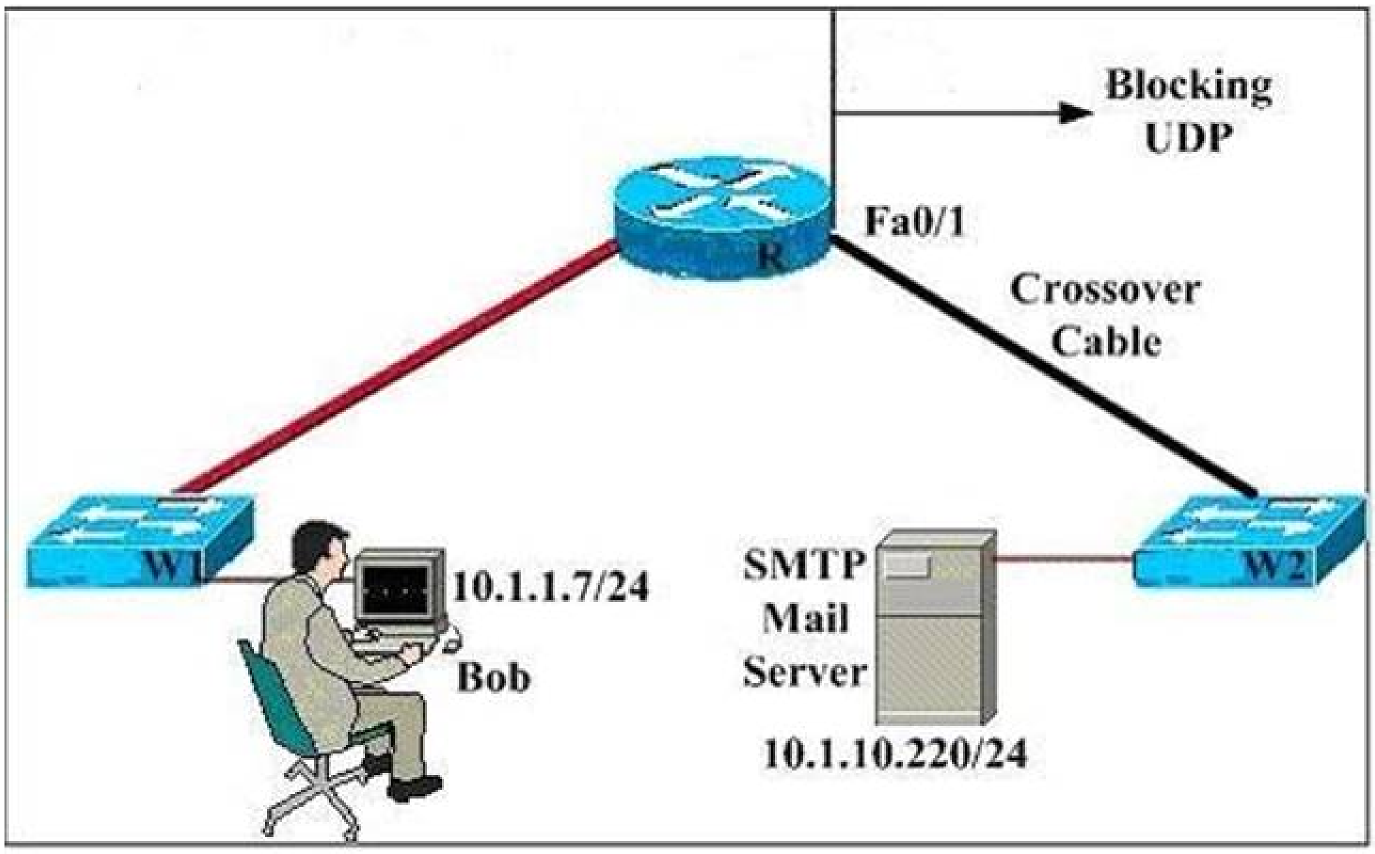
**Answer:** F

**NEW QUESTION 384**
Which two steps must you perform to enable router-on-a-stick on a switch? (Choose two.)

A. Configure an IP route to the VLAN destination network.
B. Connect the Router to a trunk port.
C. Configure full duplex.
D. Configure the subinterface number exactly the same as the matching VLAN.
E. Assign the access port to a VLAN.

**Answer:** BC

**NEW QUESTION 389**
Refer to the exhibit.



Pierre has just installed the mail server and Switch2. For security reasons UDP packets are not permitted outbound on the Fa0/1 router interface. Pierre is now at his workstation testing the new installation and is not able to establish SMTP communication to the mail server.
What is the most likely cause for lack of communication between Pierre's workstation and the mail server?

A. The crossover cable should be a straight-through cable.
B. UDP is blocked coming out of the Fa0/1 interface on the router.
C. The server should be directly connected to the router.
D. The IP addresses are all on the same networ
E. No router is required.

**Answer:** A

**NEW QUESTION 394**
Which two statements about IPv6 address 2002:ab10:beef::/48 are true?(choose two)

A. The embedded IPv4 address can be globally routed.
B. It is used for an ISATAP tunnel
C. The embedded IPv4 address is an RFC 1918 address
D. The MAC address 20:02:b0:10:be:ef is embedded into the IPv6 address
E. It is used for a 6to4 tunnel

**Answer:** AE

**NEW QUESTION 399**
If you want multiple hosts on a network, where do you configure the setting?

A. in the IP protocol
B. in the multicast interface

C. in the serial interface
D. in the global configuration

**Answer:** A

**NEW QUESTION 404**
What is the default configuration register setting on most Cisco routers?

A. 0x2210
B. 0x2104
C. 0x2102
D. 0x2012
E. 0x2142

**Answer:** C

**NEW QUESTION 408**
Which command do you enter on a router running RIP so that it advertises a route on the same interface on which it received the route?

A. no auto-summary
B. no ip split-horizon
C. passive-interface default
D. ip rip v2-broadcast

**Answer:** B

**NEW QUESTION 409**
Which statement about standard access list is true?

A. They have an implicit permit statement at the end to allow all traffic
B. They can use either a wildcard mask or a subnet mask to identify host
C. They can be identified by a number from 1 to 99
D. They must be placed close to the source of traffic

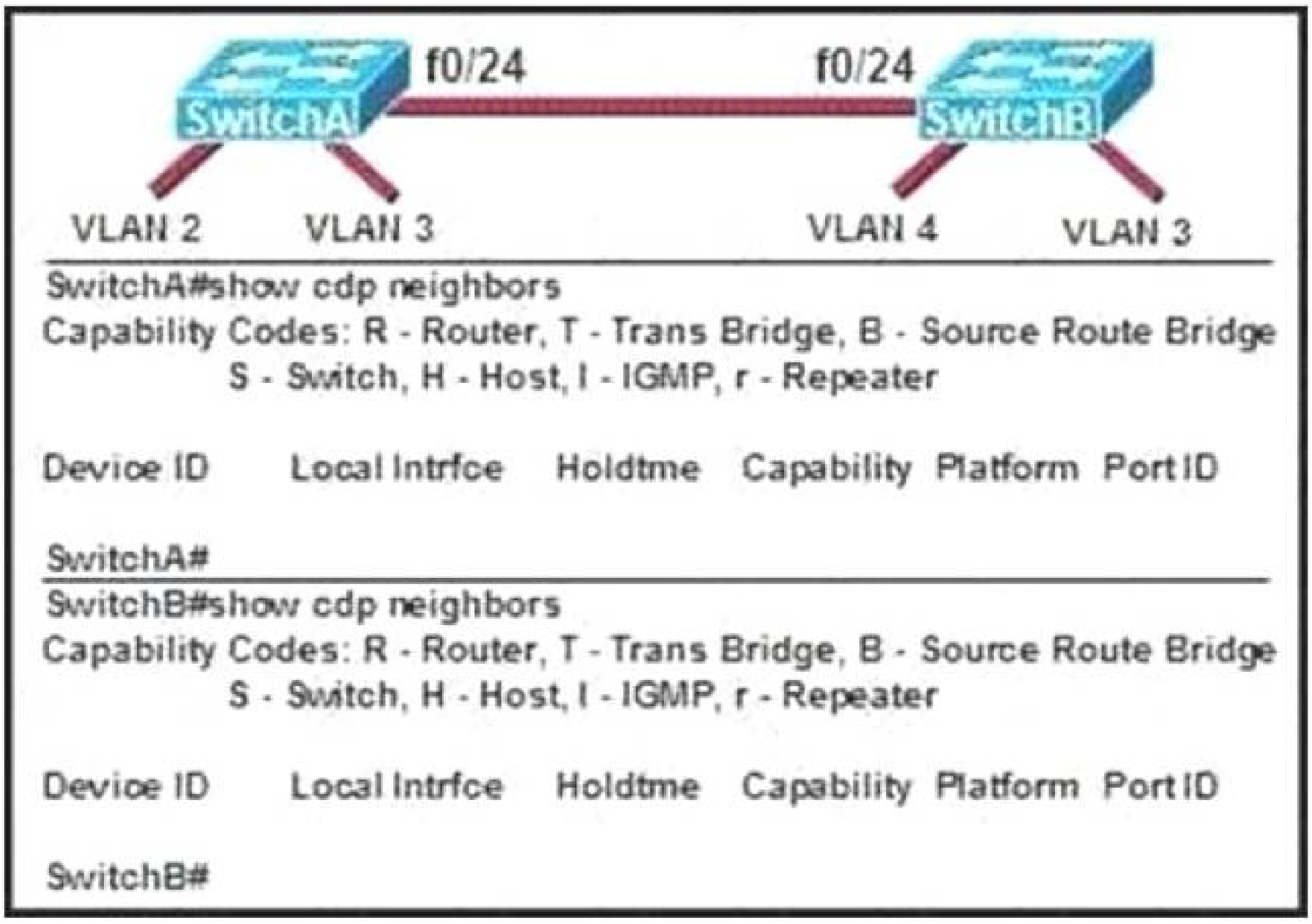
**Answer:** C

**NEW QUESTION 412**
Which forwarding technology stores destination addresses in the cache?

A. MPLS
B. Cisco express forwarding
C. Process switching
D. Fast switching

**Answer:** B

**NEW QUESTION 414**
Refer to the exhibit.



```
SwitchA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID      Local Intrfce     Holdtme    Capability  Platform  Port ID

SwitchA#
```

```
SwitchB#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID      Local Intrfce     Holdtme    Capability  Platform  Port ID

SwitchB#
```

Two 2950 switches connect through ports fa0/24 using a straight-through cable. Based on the output that is shown in the exhibit and the information that is given, what can be concluded about this network?

A. STP can not be configured on a FastEthernet ports.
B. An IP address and default gateway must be configured on each switch.
C. The switches do not share the same VTP domain.
D. Port fa0/24 must be configured as a trunk in order for the switches to share neighbor information.
E. The switches are cabled incorrectly.

**Answer:** E

**NEW QUESTION 418**
A router with a default setting deployed, how will act if it received mistype command?

A. Disable DNS look up
B. Recognizing the command
C. Try to resolve the command to an IP address
D. Try to correct the command
E. Show error message

**Answer:** C

**NEW QUESTION 422**
You have configured the host computers on a campus LAN to receive their DHCP addresses form the local router to be able to browse their corporate site. Which statement about the network environment is true?

A. It supports a DNS server for use by DHCP clients.
B. Two host computers may be assigned the same IP address.
C. The DNS server must be configured manually on each host.
D. The domain name must be configured locally on each host computer.

**Answer:** A

**Explanation:** The local router in this case is called a DHCP server. The main purpose of a DHCP server is to assign IP addresses to the clients. Besides that, a DHCP server can also specify the IP address of the DNS server and specify the domain name for the clients.
For more information about configuring a DHCP server, please read:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/12-4t/dhcp-12-4t-book/config-dhc.html

**NEW QUESTION 424**
Where information about untrusted hosts are stored?

A. CAM table
B. Trunk table
C. MAC table
D. binding database

**Answer:** D

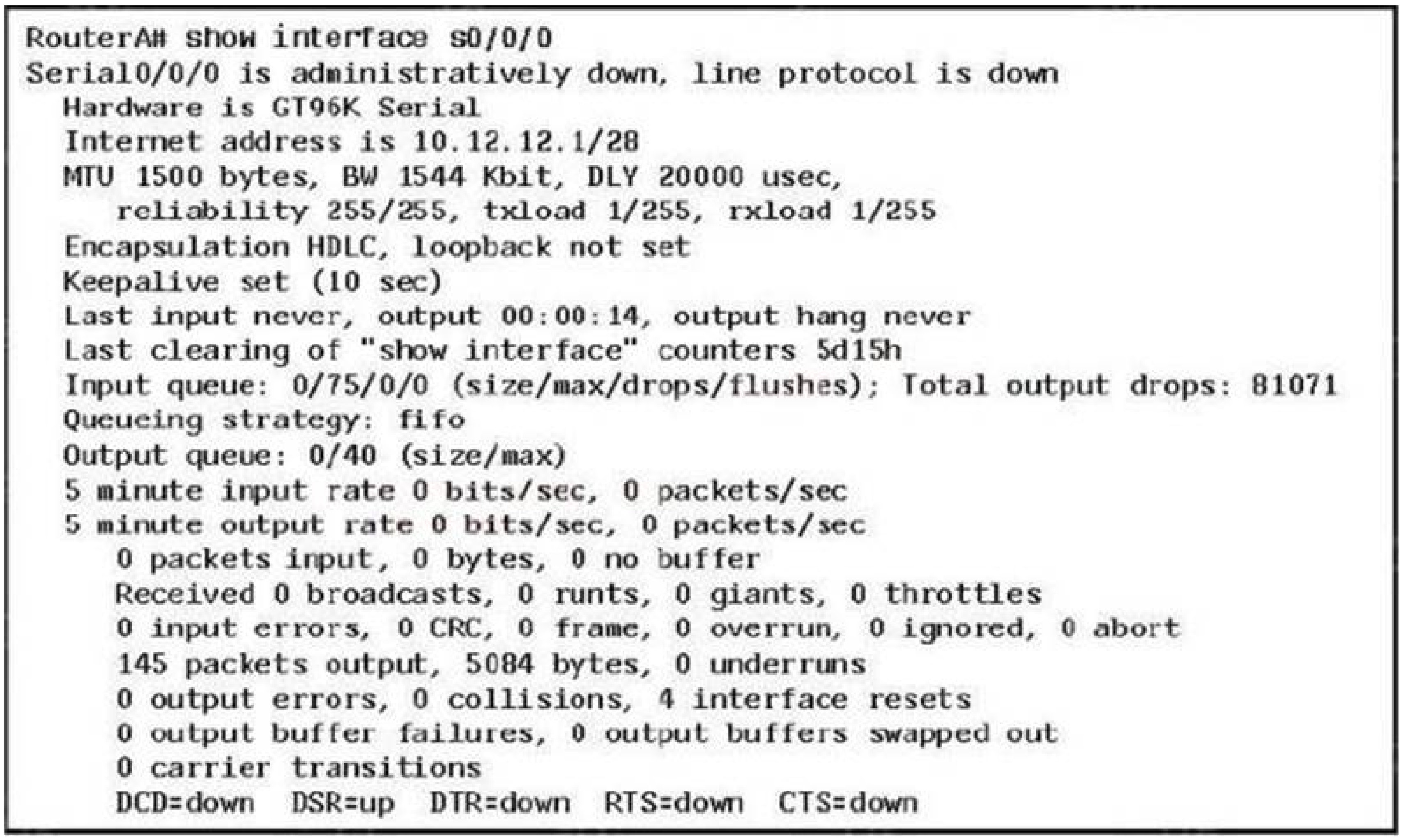
**Explanation:** A switch device builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.

**NEW QUESTION 429**
Which option does the route 0.0.0.0/0 represent?

A. Route with the lowest administrative distance
B. Gateway of last resort
C. Null route
D. Empty routing table

**Answer:** B

**NEW QUESTION 430**
Refer to the exhibit. Which statement is correct regarding the results shown for the show interface s0/0/0 command?



```
RouterA# show interface s0/0/0
Serial0/0/0 is administratively down, line protocol is down
  Hardware is GT96K Serial
  Internet address is 10.12.12.1/28
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input never, output 00:00:14, output hang never
  Last clearing of "show interface" counters 5d15h
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 81071
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     145 packets output, 5084 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=up  DTR=down  RTS=down  CTS=down
```

A. The subnet mask for this interface is 255.255.255.248.
B. The subnet mask for this interface is 255.255.255.252.
C. The IP address that is configured on s0/0/0 is a public address.
D. This interface can be enabled by issuing a no shutdown command.
E. The default encapsulation protocol for a Cisco serial interface is PPP.

**Answer:** D

**NEW QUESTION 433**
Multicast IP addresses can be grouped into which two address-range assignments? (Choose two.)

A. registered
B. dynamic
C. GLOP
D. source-specific multicast
E. private

**Answer:** AB

**NEW QUESTION 435**
Which option is a invalid hostname for a switch?

A. 5witch-Cisco
B. Switch-Cisco!
C. 5witchCisc0
D. SwitchCisc0

**Answer:** B

**Explanation:** The “!” is an invalid letter for a hostname.

**NEW QUESTION 439**
Which equipment is needed to connect hosts between VLAN 10 and VLAN 20?

A. hub
B. switch
C. router
D. firewall
E. APC

**Answer:** C

**NEW QUESTION 441**
Which network configuration can you use to segregate broadcast traffic for two different departments in your organization?

A. Configure two VTP domains and configure the switches in transparent mode.
B. Enable spanning-tree load balancing.

C. Implement switch port security on designated ports.
D. Configure a separate VLAN for each department.

**Answer:** D

**NEW QUESTION 445**
What happens when an 802.11a node broadcasts within the range of an 802.11g access point?

A. The access point transmits, but the node is unable to receive.
B. A connection occurs
C. Both the node and the access point are unable to transmit.
D. The node transmits, but the access point is unable to receive.

**Answer:** D

**NEW QUESTION 448**
Which information is missing from a default syslog message?

A. HOSTNAME
B. SEVERITY
C. MESSAGE
D. TIMESTAMP

**Answer:** A

**Explanation:**
Reference: https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.html

**NEW QUESTION 452**
Assume all the routing protocol have the same length prefix, what would the router prefer?

A. OSPF
B. EIGRP
C. CONNECTED
D. BGP

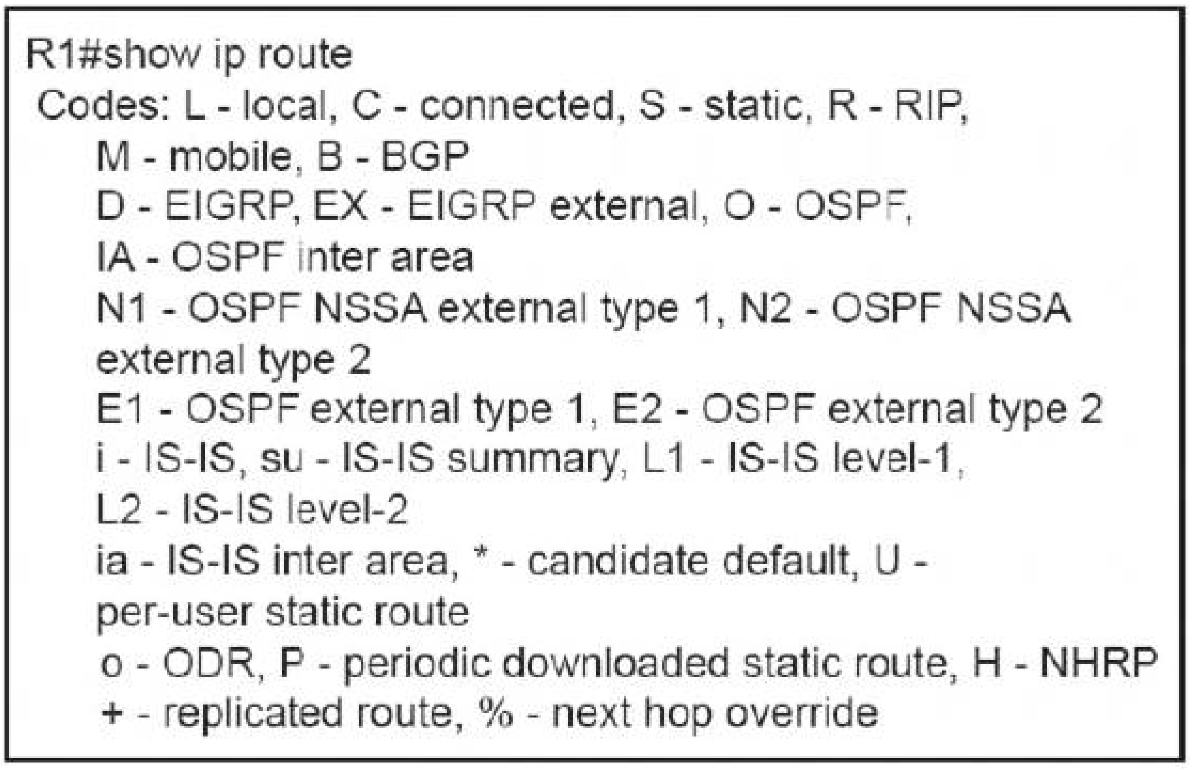
**Answer:** C

**NEW QUESTION 457**
Which hashing algorithm does NTP use for its authentication keys?

A. MD5
B. AES-256
C. 3DES
D. SHA

**Answer:** A

**NEW QUESTION 460**
Refer to the exhibit.



```
R1#show ip route
 Codes: L - local, 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, H - NHRP
      + - replicated route, % - next hop override
```

Which two statements about the route source code in a routing table are true? (Choose two.)

A. It identifies the destination of the route.
B. It identifies the source type of the route.

C. Routes with code C are preferred.
D. It appears after the source network address.
E. Routes with code S are always preferred.

**Answer:** BC

**NEW QUESTION 461**
Which device can be used to extend the LAN without using layer3 device?

A. Access point
B. Switch
C. Wireless controller
D. Firewall

**Answer:** A

**NEW QUESTION 466**
Which of the following is a characteristic of full-duplex communication?

A. It is a CSMA/CD network.
B. It is a CSMA/CA network.
C. It is point-to-point only.
D. Hub communication is done via full duplex.

**Answer:** C

**NEW QUESTION 470**
When you troubleshoot an IPv4 connectivity issue on a router, which three router configuration checks you must perform? (Choose three)

A. Verify that the router interface IP address IP address is correct.
B. Verify that the DNS is configured correctly.
C. Verify that the router and the host use the same subnet mask.
D. Verify that the router firmware is up-to-date.
E. Verify that a default route is configured.
F. Verify that the route appears in the Routing table

**Answer:** ACF

**NEW QUESTION 475**
Which protocol can identify connected devices within a mixed-vendor infrastructure?

A. Virtual terminal protocol
B. Network time protocol
C. Link level discovery protocol
D. Cisco discovery protocol

**Answer:** C

**NEW QUESTION 478**
Which two statements about RIPv2 are true? (Choose two)

A. It must be manually enabled after RIP is configured as the routing protocol
B. It uses multicast address 224.0.0.2 to share routing information between peers
C. its default administrative distances 120
D. It is a link-state routing protocol
E. It is an EGP routing protocol

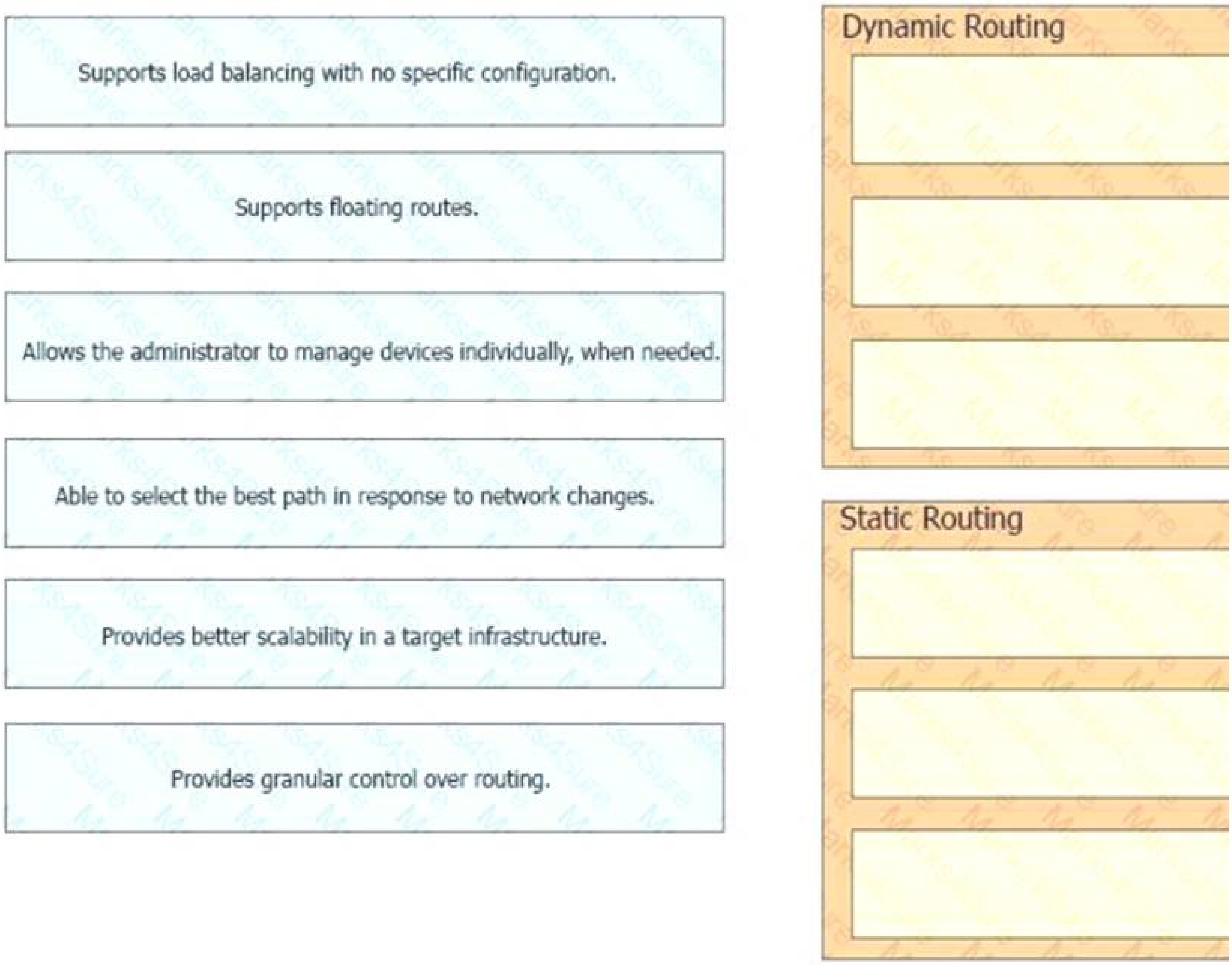
**Answer:** AC

**NEW QUESTION 479**
Which of the following item is used to establish telnet session by having the host name?

A. DNS lookup
B. Ping
C. Syslog
D. ARP

**Answer:** A

**NEW QUESTION 482**
Drag and drop each feature on the left on to the correct routing type on the right.
Select and Place:



Supports load balancing with no specific configuration.

Supports floating routes.

Allows the administrator to manage devices individually, when needed.

Able to select the best path in response to network changes.

Provides better scalability in a target infrastructure.

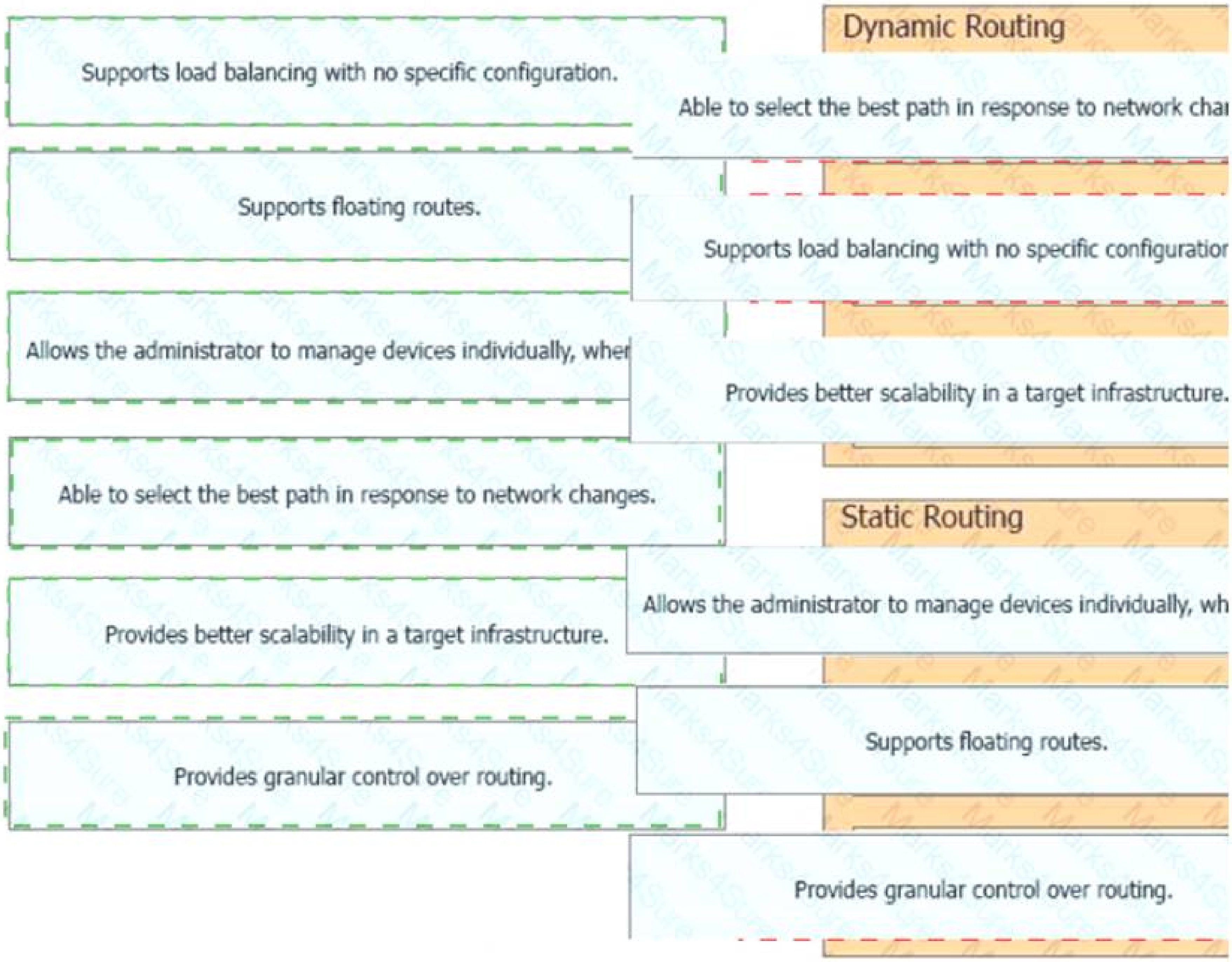
Provides granular control over routing.

Dynamic Routing

Static Routing

**Answer:**

**Explanation:**



Supports load balancing with no specific configuration.

Supports floating routes.

Allows the administrator to manage devices individually, wher

Able to select the best path in response to network changes.

Provides better scalability in a target infrastructure.

Provides granular control over routing.

Dynamic Routing

Able to select the best path in response to network cha

Supports load balancing with no specific configuratio

Provides better scalability in a target infrastructure.

Static Routing

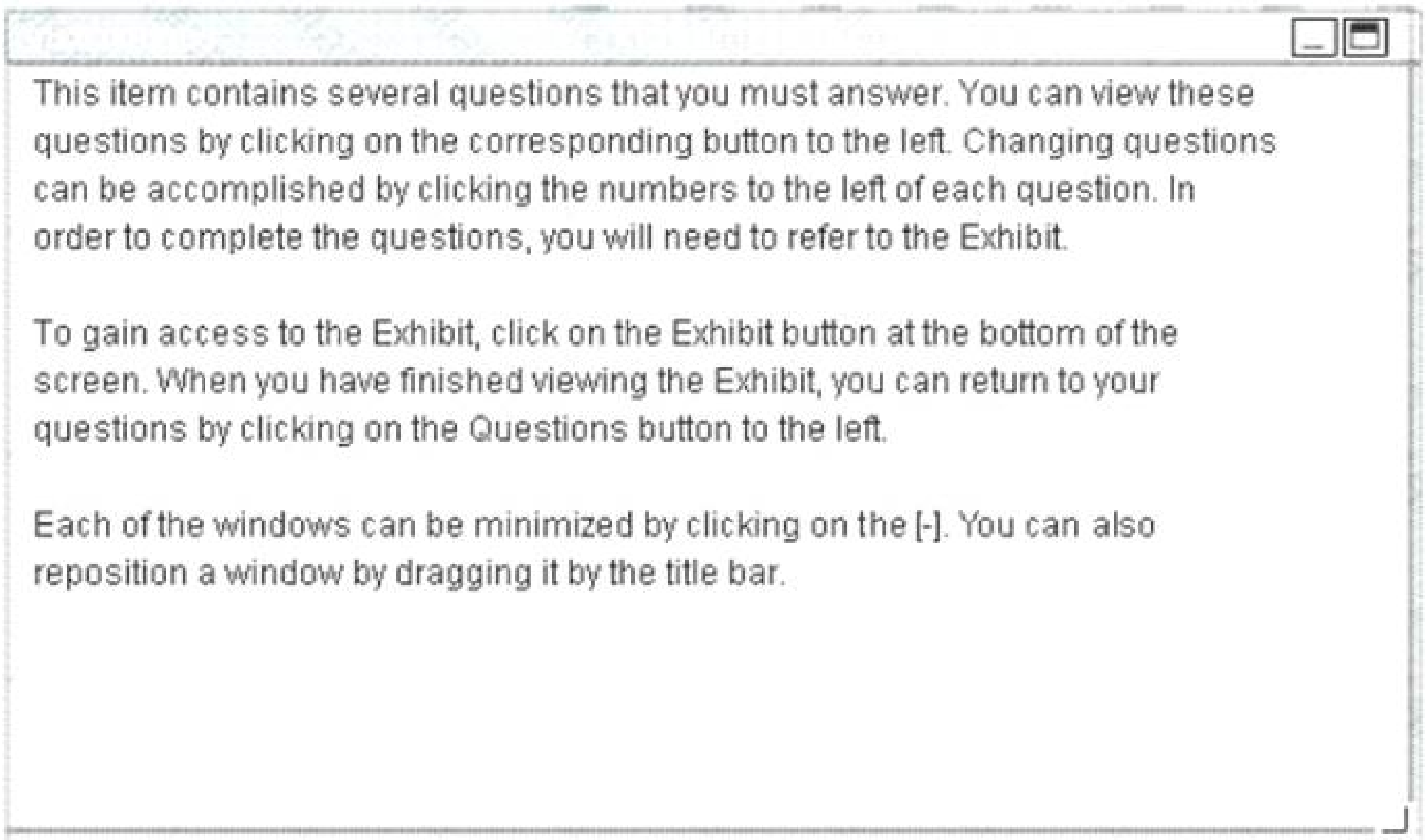
Allows the administrator to manage devices individually, wh

Supports floating routes.

Provides granular control over routing.

**NEW QUESTION 486**

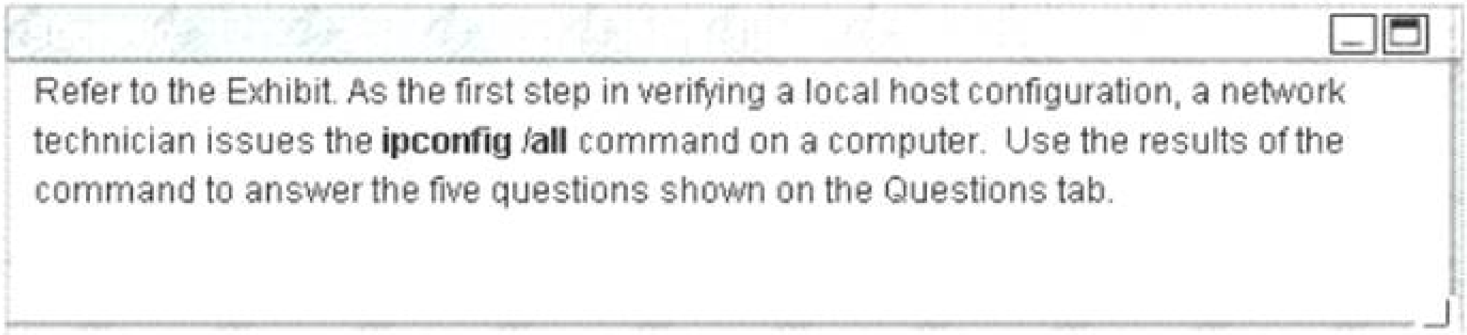
Click on the correct location or locations in the exhibit.



This item contains several questions that you must answer. You can view these questions by clicking on the corresponding button to the left. Changing questions can be accomplished by clicking the numbers to the left of each question. In order to complete the questions, you will need to refer to the Exhibit.

To gain access to the Exhibit, click on the Exhibit button at the bottom of the screen. When you have finished viewing the Exhibit, you can return to your questions by clicking on the Questions button to the left.

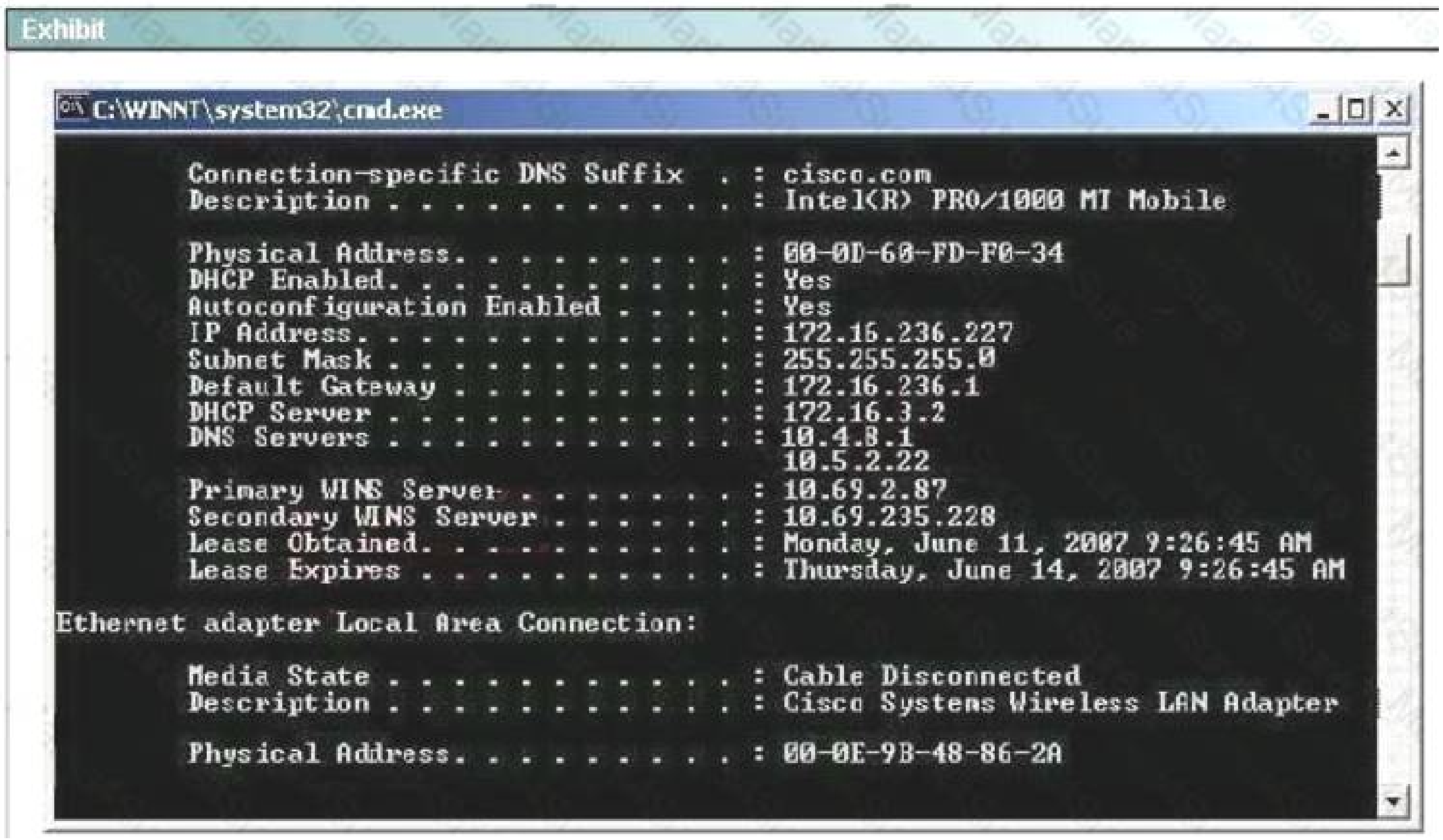
Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.



Refer to the Exhibit. As the first step in verifying a local host configuration, a network technician issues the **ipconfig /all** command on a computer. Use the results of the command to answer the five questions shown on the Questions tab.

Whit statement is true about how the router with the IP address 172.16.236.1 will send a data packet to this computer?

Exhibit



```
        Connection-specific DNS Suffix  . : cisco.com
        Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Mobile

        Physical Address. . . . . . . . . : 00-0D-60-FD-F0-34
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 172.16.236.227
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.236.1
        DHCP Server . . . . . . . . . . . : 172.16.3.2
        DNS Servers . . . . . . . . . . . : 10.4.8.1
                                            10.5.2.22
        Primary WINS Server . . . . . . . : 10.69.2.87
        Secondary WINS Server . . . . . . : 10.69.235.228
        Lease Obtained. . . . . . . . . . : Monday, June 11, 2007 9:26:45 AM
        Lease Expires . . . . . . . . . . : Thursday, June 14, 2007 9:26:45 AM

Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Cable Disconnected
        Description . . . . . . . . . . . : Cisco Systems Wireless LAN Adapter

        Physical Address. . . . . . . . . : 00-0E-9B-48-86-2A
```

A. The router encapsulates the packet in a frame addressed to the MAC address FF-FF-FF-FF-FF-FF and sends it out the interface connected to the 172.16.236.0 network.
B. The router uses an ARP request to obtain the correct MAC address for the compute
C. It then encapsulates the packet in a frame addressed to the MAC address 00-0D-60-FD-F0-34.
D. The router encapsulates the packet in a frame addressed to the MAC address of the next hop router on the path to the computer.
E. The router works at Layer 3 of the OSI model and does not use Layer 2 MAC addresses to send packets to the destination computer.

**Answer:** B

**NEW QUESTION 491**
Which IPV6 feature is supported in IPV4 but is not commonly used?

A. unicast
B. multicast
C. anycast
D. broadcast

**Answer:** C

**NEW QUESTION 495**
What does split horizon prevent?

A. routing loops, link state
B. routing loops, distance vector
C. switching loops, STP
D. switching loops, VTP

**Answer:** B

**NEW QUESTION 500**
Fill in the blank. Which route option can be used to back-up in case of fail?

**Answer:**

**Explanation:** floating route

**NEW QUESTION 505**
Which statement describes the effect of the exec-timeout 30 command?

A. The router maintains a user session indefinitely after it is active for 30 seconds.
B. The router disconnects the user session if it is inactive for 30 minutes.
C. The router maintains a user session indefinitely after it is active for 30 minutes.
D. The router disconnects a user session if it is inactive for 30 seconds.

**Answer:** B

**NEW QUESTION 510**
Which two statements about unique local IPv6 addresses are true? (Choose two)

A. They are identical to IPv4 private addresses.
B. They are defined by RFC 1884.
C. They use the prefix FEC0::/10
D. They use the prefix FC00::/7
E. They can be routed on the IPv6 global internet.

**Answer:** AD

**NEW QUESTION 513**
Which Cisco IOS feature can dynamically assign IP addresses to hosts?

A. DHCP Relay
B. TFTP
C. DNS
D. DHCP

**Answer:** D

**NEW QUESTION 518**
Which three statements about DWDM are true? (Choose three) A. It allows a single strand of fiber to support bidirectional communications

A. It is used for long-distance and submarine cable systems
B. It can multiplex up to 256 channels on a single fiber
C. It supports both the SDH and SONET standards
D. Each channel can carry up to a 1-Gbps signal
E. It supports simplex communications over multiple strands of fiber

**Answer:** CDE

**NEW QUESTION 519**
Which two configuration steps will prevent an unauthorized PC from accessing the corporate network? (Choose two.)

A. set the port security aging time to 0
B. create the port as a protected port and statically assign the MAC address to the address table
C. configure the switch to discover new MAC addresses after a set time of inactivity
D. enable port security on the switch
E. create the port as an access port and statically assign the MAC address to the address table

**Answer:** DE

**NEW QUESTION 524**
What does not belong to Syslog?

A. host name
B. severity
C. timestamp
D. message

**Answer:** A

**NEW QUESTION 528**
Which protocol does ipv6 use to discover other ipv6 nodes on the same segment?

A. CLNS
B. TCPv6
C. NHRP
D. NDP
E. ARP

**Answer:** D

**NEW QUESTION 531**
Which component is part of an Ethernet frame?

A. checksum
B. TTL
C. sequence number
D. frame check sequence

**Answer:** D

**NEW QUESTION 532**

How many VLANs can be carried across an access port?

A. 8
B. 1
C. 4096
D. 1024

**Answer:** B

**NEW QUESTION 533**
From where does a small network get its IP network address?

A. Internet Assigned Numbers Authority (IANA)
B. Internet Architecture Board (IAB)
C. Internet Service Provider (ISP)
D. Internet Domain Name Registry (IDNR)

**Answer:** C

**NEW QUESTION 537**
How can an administrator determine if a router has been configured when it is first powered up?

A. A configured router prompts for a password.
B. A configured router goes to the privileged mode prompt.
C. An unconfigured router goes into the setup dialog.
D. An unconfigured router goes to the enable mode prompt.

**Answer:** C

**NEW QUESTION 540**
Which range represents the standard access list?

A. 99
B. 150
C. 299
D. 2000

**Answer:** A

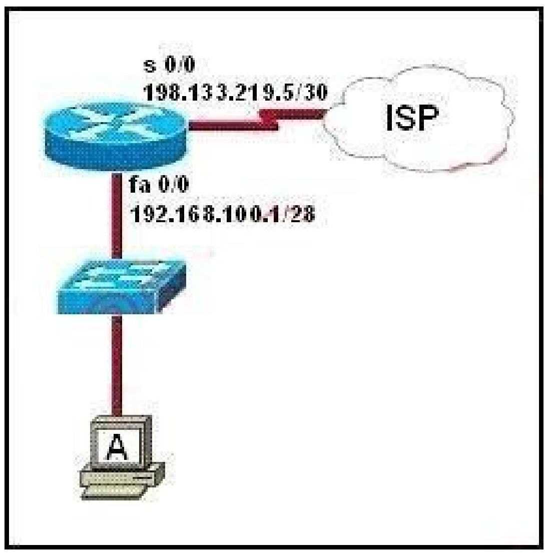
**NEW QUESTION 544**
Which feature automatically disables CEF when it is enabled?

A. RIB
B. ACL logging
C. multicast
D. IP redirects

**Answer:** B

**Explanation:** ACL Logging means to use the "log" or "log-input" parameters at the end of the ACL statements. For example: "access- list 100 deny icmp any any echo reply log-input". In either situation, remember that using either of these two parameters disables CEF switching, which seriously impacts the performance of the router.

**NEW QUESTION 549**
Refer to the exhibit.



A network technician has added host A to the network. Host A cannot communicate on the network. A ping that is issued on the host to address 127.0.0.1 fails.
What is the problem?

A. The router is not forwarding the ping packets to network 127.0.0.0.
B. The remote host at 127.0.0.1 is unreachable.
C. The default gateway is incorrect.

D. The IP address of host A is incorrect.
E. The TCP/IP protocols are not loaded.

**Answer:** E

**NEW QUESTION 553**
In which two situations should you use out-of-band management?

A. when a network device fails to forward packets
B. when you require ROMMON access
C. when management applications need concurrent access to the device
D. when you require administrator access from multiple locations
E. when the control plane fails to respond

**Answer:** AB

**NEW QUESTION 555**
Which configuration must you perform to enable VTP in a switching domain?

A. Configure a switch as a client.
B. Configure a switch with a VTP domain.
C. Configure a switch with VTP mode off to serve as the server switch.
D. Configure a switch in transparent mode.

**Answer:** B

**NEW QUESTION 557**
Which networking Technology is currently recognized as the standard for computer networking?

A. System network architecture
B. Transmission control protocol/Internet protocol
C. Open system Interconnect
D. Open network architecture

**Answer:** B

**NEW QUESTION 562**
Fill in the blank. What would the router use as metrics when having different routing protocol in the routing table?

**Answer:**

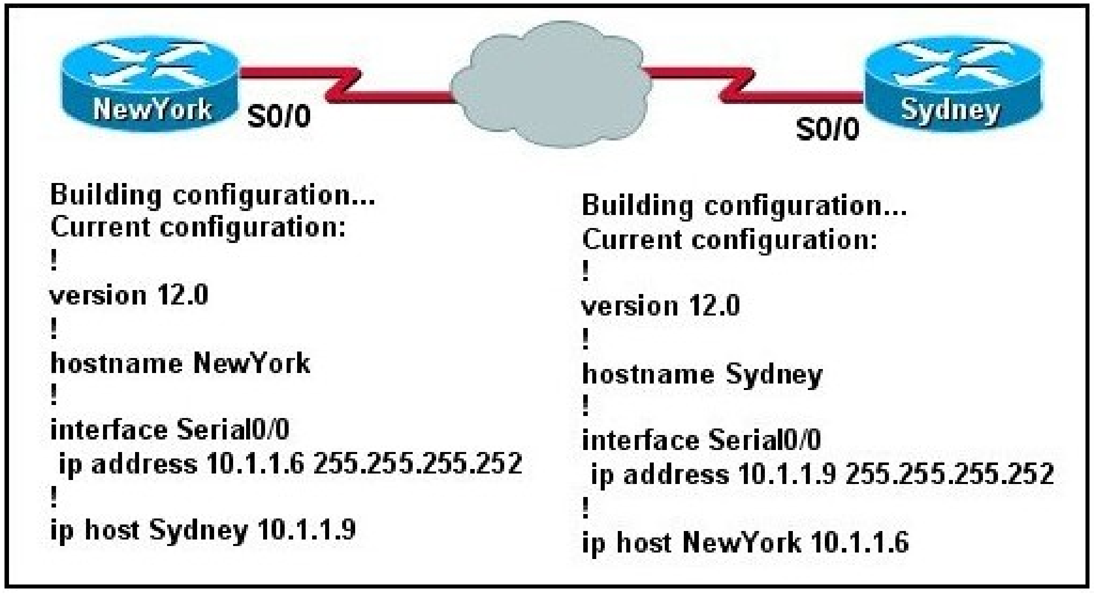
**Explanation:** Prefix length

**NEW QUESTION 563**
Which NTP concept indicates the distance between a device and the reliable time source?

A. clock offset
B. stratum
C. reference
D. dispersion

**Answer:** B

**NEW QUESTION 568**
Refer to the topology and partial configurations shown in the exhibit.



```
Building configuration...
Current configuration:
!
version 12.0
!
hostname NewYork
!
interface Serial0/0
 ip address 10.1.1.6 255.255.255.252
!
ip host Sydney 10.1.1.9
```

```
Building configuration...
Current configuration:
!
version 12.0
!
hostname Sydney
!
interface Serial0/0
 ip address 10.1.1.9 255.255.255.252
!
ip host NewYork 10.1.1.6
```

The network administrator has finished configuring the NewYork and Sydney routers and issues the command ping Sydney from the NewYork router. The ping fails. What command or set of commands should the network administrator issue to correct this problem?

A. Sydney(config)# interface s0/0 Sydney(config-if)#cdp enable
B. Sydney(config)# interface s0/0 Sydney(config-if)# no shut
C. Sydney(config)# line vty 0 4 Sydney(config)# login Sydney(config)# password Sydney
D. Sydney(config)# ip host Sydney 10.1.1.9
E. Sydney(config)# interface s0/0Sydney(config-if)#ip address 10.1.1.5 255.255.255.252 NewYork(config)# ip host Sydney 10.1.1.5

**Answer:** E

**Explanation:** The IP addresses on the two Serial interfaces of two routers are not in the same subnet so they could not recognize each other and the ping failed. Therefore we must correct the IP address of one of the router so that they are in the same subnet.

**NEW QUESTION 572**
Which two statements about 802.1Q are true? (Choose two.)

A. It is an open-standard trunking protocol
B. It is a Cisco-proprietary trunking protocol
C. It inserts a 4-byte identifying tag in the Ethernet frame after the source MAC address field.
D. It encapsulates the original data frame inside a trunking header.
E. It uses a 20-bit label to identify packets within a trunk.

**Answer:** AC

**NEW QUESTION 574**
Which counter indicates the total number of frames that a switch port failed to transmit?

A. frame
B. collisions
C. output errors
D. packet outputs

**Answer:** C

**NEW QUESTION 577**
Which command is used to build DHCP pool?

A. ipdhcp conflict
B. ipdhcp-server pool DHCP
C. ipdhcp pool DHCP
D. ipdhcp-client pool DHCP

**Answer:** C

**NEW QUESTION 581**
Which protocol verifies connectivity between two switches that are configured with IP addresses in the same network?

A. ICMP
B. STP
C. VTP
D. HSRP

**Answer:** A

**NEW QUESTION 586**
When you use the ping command to send ICMP messages across a network, what's the most common request/reply pair you'll see? (Select one answer choice)

A. Echo request and Echo reply
B. ICMP hold and ICMP send
C. ICMP request and ICMP reply
D. Echo off and Echo on

**Answer:** A

**NEW QUESTION 588**
When troubleshooting a LAN interface operating in full duplex mode, which error condition can be immediately ruled out?

A. giants
B. no buffers
C. collisions
D. ignored
E. dribble condition

**Answer:** C

**NEW QUESTION 593**

Which sequence begins a unique local IPv6 address in binary notation?

A. 00000000
B. 1111110
C. 1111100
D. 1111111

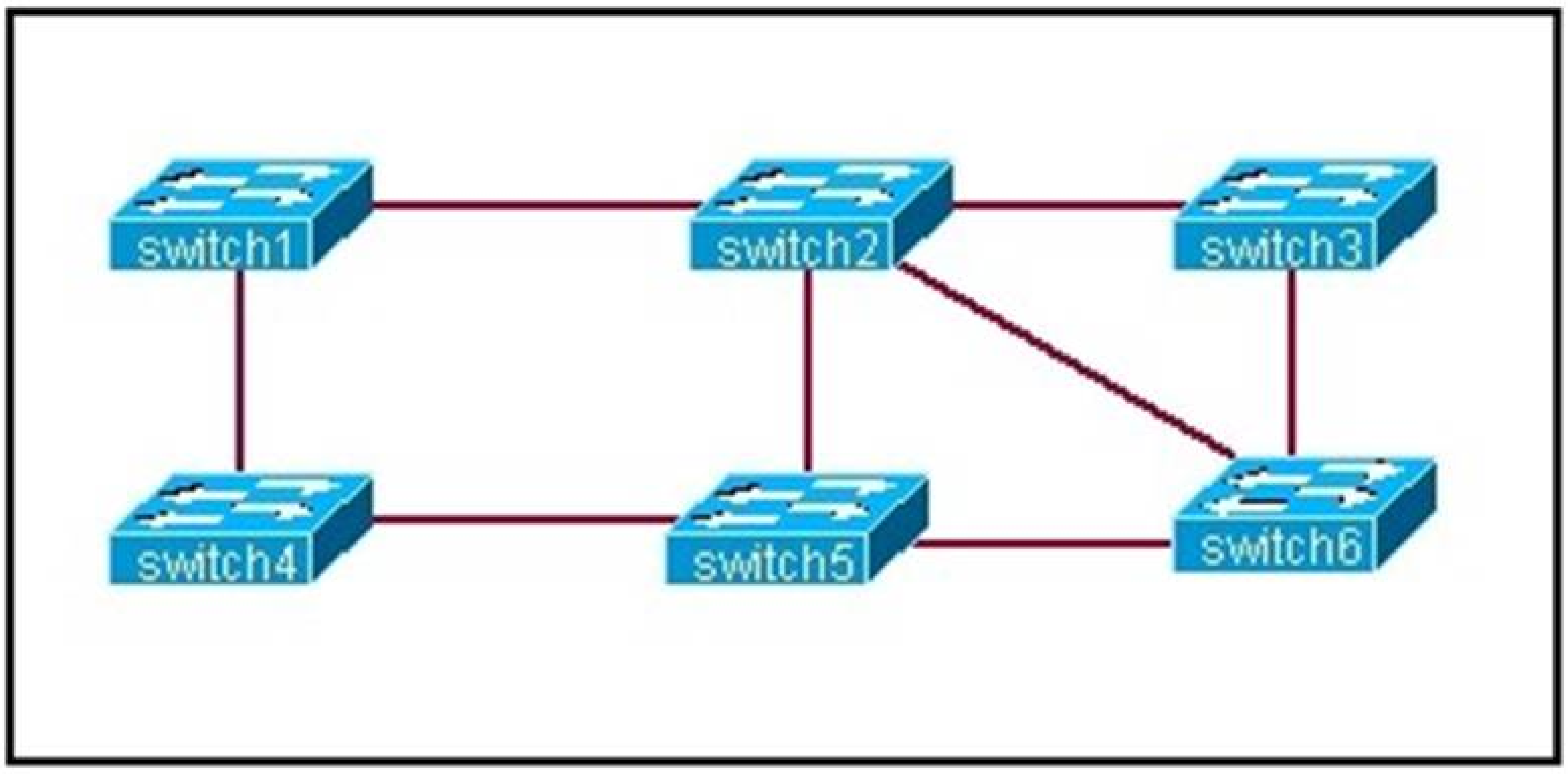
**Answer:** B

**NEW QUESTION 594**
Which commands display information about the Cisco IOS software version currently running on a router? (Choose three)

A. show running-config
B. show stacks
C. show version
D. show flash
E. show protocols
F. show IOS

**Answer:** ACD

**NEW QUESTION 596**
Based on the network shown in the graphic



Which option contains both the potential networking problem and the protocol or setting that should be used to prevent the problem?

A. routing loops, hold down timers
B. Switching loops, split horizon
C. routing loops, split horizon
D. Switching loops, VTP
E. routing loops, STP
F. Switching loops, STP

**Answer:** F

**NEW QUESTION 598**
What is the lowest AD?

A. OSPF
B. EIGRP
C. IS-IS
D. IBGP
E. RIPv2

**Answer:** B

**NEW QUESTION 599**
Which option is one component of an Ethernet frame?

A. sequence number
B. checksum
C. TTL
D. frame check sequence

**Answer:** D

**NEW QUESTION 604**
Where is private IPv4 addressing used?

A. On the endpoints of a VPN tunnel that traverses outside an administrator domain
B. At a remote site that connects over public infrastructure to a hub
C. Within an enterprise
D. Over the internet

**Answer:** C

**NEW QUESTION 606**
Which statement is true about static and dynamic routing?

A. Only static routes are shared between connected interfaces
B. Dynamic routing is more scalable than static routing
C. Only dynamic routes are secure
D. Static routing is easier to maintain in a large network than dynamic routing.

**Answer:** B

**NEW QUESTION 607**
For which important purpose was IPv6 addressing developed?

A. To reduce the number of public IP addresses on the internet
B. To replace network address translation
C. To remove the need for classless inter-domain routing
D. To relieve the shortage of public IP addresses on the internet

**Answer:** D

**NEW QUESTION 610**
What is the default administrative distance of OSPF?

A. 90
B. 100
C. 110
D. 120

**Answer:** C

**NEW QUESTION 612**
Which statement describes the effect of the overload keyword in the ip nat inside source list 90 interface ethernet 0/0 overload command?

A. Addresses that match address list inside are translated to the IP address of the Ethernet 0/0 interface.
B. Hosts that match access inside are translated to an address m the Ethernet 0/0 network.
C. Hosts on the Ethernet 0/0 LAN are translated to the address pool in access list 90.
D. Addresses that match access list 90 are translated through PAT to the IP address of the Ethernet 0/0 interface

**Answer:** D

**NEW QUESTION 616**
What is the maximum number of bits that can be borrowed to create subnets if a Class B network address is being used?

A. 2
B. 6
C. 8
D. 14
E. 16

**Answer:** D

**NEW QUESTION 617**
Which two types of Ethernet networks are compatible with star topologies? (Choose two.)

A. 10BASE-T
B. 100BASE-T
C. 10BASE5
D. 10BASE2

**Answer:** AB

**NEW QUESTION 620**
On which OSI layer does a VLAN operate?

A. Layer 1

B. Layer 2
C. Layer 3
D. Layer 4

**Answer:** B

**NEW QUESTION 621**
Which of the following is true about port security?

A. In stick, port retrain dynamically learned
B. Configure spanning destination
C. The default configuration with max 10
D. Not supported by VLAN

**Answer:** A

**NEW QUESTION 626**
Which of the following true about access points?

A. It used physically to connect network devices
B. It is used as a router
C. Provide full duplex communication
D. It is a layer 2 device used to extend the LAN coverage to wireless devices

**Answer:** D

**NEW QUESTION 628**
What is the default administrative distance for a connected route?

A. 1
B. 5
C. 20

**Answer:** B

**NEW QUESTION 630**
Which two statements about VTP are true? (Choose two.)

A. The VLANs can be configured on a VTP server without a VTP domain name.
B. Each switch sends the VTP password in every summary-advertisement.
C. IOS switches cannot turn off VTP.
D. VTP negotiates a secure channel for VTP advertisements.
E. The switches must be reloaded when you update from VTP version 1 to VTP version 2.

**Answer:** BC

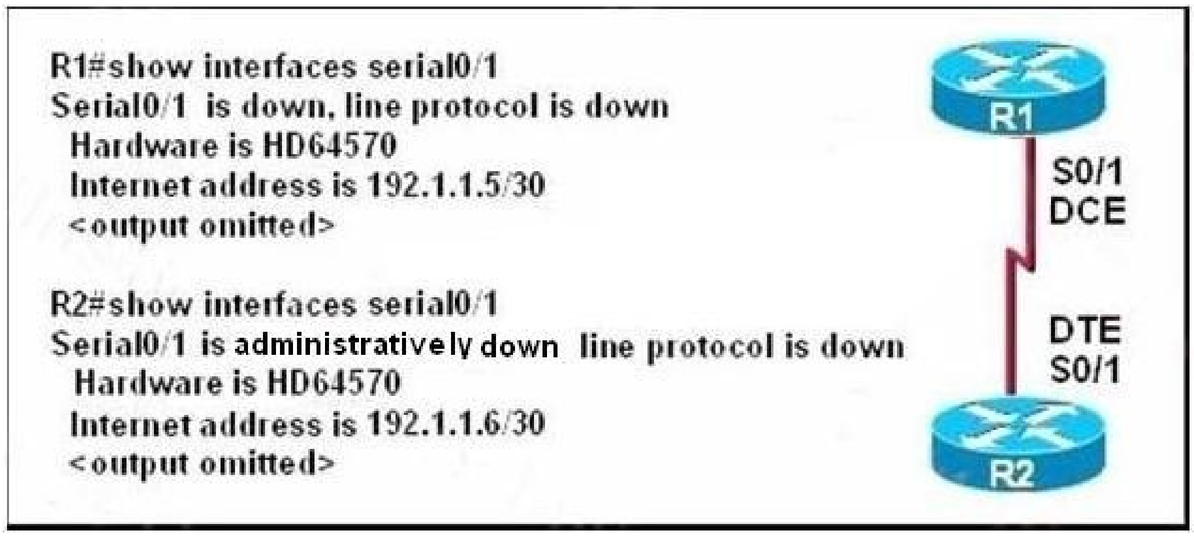
**Explanation:** Reference: https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html#vtp_pw

**NEW QUESTION 632**
Which statement about Cisco Discovery Protocol is true?

A. It is a Cisco-proprietary protocol.
B. It runs on the network layer.
C. It can discover information from routers, firewalls, and switches.
D. It runs on the physical layer and the data link layer.

**Answer:** A

**NEW QUESTION 636**
Refer to the exhibit.



```
R1#show interfaces serial0/1
Serial0/1  is down, line protocol is down
  Hardware is HD64570
  Internet address is 192.1.1.5/30
  <output omitted>

R2#show interfaces serial0/1
Serial0/1 is administratively down  line protocol is down
  Hardware is HD64570
  Internet address is 192.1.1.6/30
  <output omitted>
```

A network technician is unable to ping from R1 to R2. Using the output of the show interfaces serial0/1 command, what should the administrator do to correct the problem?

A. Replace the serial cable between R1 and R2.
B. Reseat the serial connectors on the R1 and R2 routers.
C. Configure the serial0/1 interface on R2 with the no shutdown command.
D. Configure the serial0/1 interface on R1 with the clock rate 56000 command.
E. Configure the serial0/1 interface on R1 with the ip address 192.1.1.7 255.255.255.252 command.

**Answer:** C

**NEW QUESTION 637**
To enable router on a stick on a router subinterface, which two steps must you perform? choose two

A. configure full duplex and speed
B. configure a default to route traffic between subinterfaces
C. configure the subinterface with an ip address
D. configure encapsulation dot1q
E. configure an ip route to the vlan destination network

**Answer:** CD

**NEW QUESTION 639**
Which configuration can be used with PAT to allow multiple inside address to be translated to a single outside address?

A. Dynamic Routing
B. DNS
C. Preempt
D. overload

**Answer:** D

**NEW QUESTION 641**
Which feature facilitates the tagging of frames on a specific VLAN?

A. Routing
B. hairpinning
C. switching
D. encapsulation

**Answer:** D

**NEW QUESTION 642**
Which circumstance causes a security violation on a switch port with port security enabled?

A. The maximum number of secure MAC addresses is reached on a secure port and an unidentified MAC address attempts an ingress connection.
B. A configured MAC address attempts an ingress connection on a different port in a different VLAN.
C. The minimum number of secure MAC addresses is configured on a secure port and an unidentified MAC address attempts an ingress connection.
D. A minimum number of secure MAC addresses has filled the dynamic table.

**Answer:** A

**Explanation:** Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.html

**NEW QUESTION 643**
If you configure syslog messages without specifying the logging trap level, which log messages will the router send?

A. 0-4
B. 0-5
C. 0-6
D. 0-2
E. 0-1

**Answer:** C

**NEW QUESTION 646**
Which feature facilitate the tagging of a specific VLAN?

A. Routing
B. Hairpinning
C. Encapsulation
D. Switching

**Answer:** C

**NEW QUESTION 650**
What is the most efficient subnet mask for a point to point ipv6 connection?

A. /127
B. /128
C. /64
D. /48
E. /32

**Answer:** A

**NEW QUESTION 654**
Which statement about recovering a password on a cisco router is true?

A. it requires physical access to the router
B. the default reset password is cisco
C. a factory reset is required if you forget the password
D. it requires a secure SSL/VPN connection

**Answer:** A

**NEW QUESTION 659**
Which two statements about Ethernet frame formats are true? (Choose two.)

A. The FCS is appended to the VLAN tag.
B. The receiving MAC always recalculates the FCS.
C. The VLAN tag precedes the Length/Type field.
D. The second bit in the Destination Address field indicates whether the address is an individual or group address.
E. The first bit in the Destination Address field determines whether the address is handled globally or locally.
F. The preamble checks the FCS to identify the start and end of a packet.

**Answer:** BC

**NEW QUESTION 661**
In which two ways does TCP differ from UDP? (Choose two.)

A. TCP segments are essentially datagrams.
B. TCP uses broadcast delivery.
C. TCP provides sequence numbering of packets.
D. TCP provides synchronized communication.
E. TCP provides best effort delivery.

**Answer:** CD

**Explanation:** http://www.diffen.com/difference/TCP_vs_UDP
Before two computers can communicate over TCP, they must synchronize their initial sequence numbers (ISN)
TCP uses a sequence number to identify each byte of data. The sequence number identifies the order of the bytes sent from each computer so that the data can be reconstructed in order, regardless of any fragmentation, disordering, or packet loss that may occur during

**NEW QUESTION 664**
Which statement about the enable password is true?

A. The space character is not supported.
B. It is not stored in a secured format.
C. It can be up to 32 characters long.
D. It is stored in a secured format.

**Answer:** B

**Explanation:** Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/fsecur_r/srfpass.html

**NEW QUESTION 666**
Why does a host use a DNS server?

A. To make a DNS client request to server
B. To resolve IP to FQDN
C. To resolve FQDN to IP
D. To assign IP

**Answer:** C

**NEW QUESTION 668**
What is the subnet address of 192.168.1.42 255.255.255.248?

A. 192.168.1.16/28
B. 192.168.1.32/27
C. 192.168.1.40/29
D. 192.168.1.8/29
E. 192.168.1.48/29

**Answer:** C

**Explanation:** 248 mask uses 5 bits (1111 1000) 42 IP in binary is (0010 1010) The base subnet therefore is the lowest binary value that can be written without changing the output of an AND operation of the subnet mask and IP ... 1111 1000 AND 0010 1010 equals 0010 1000 - which is .40 /24 is standard class C mask. adding the 5 bits from the.248 mask gives /29

**NEW QUESTION 669**
Which value must the device send as its username when using CHAP to authenticate with the remote peer site id:17604704 over a PPP link?

A. The automatically generated user name
B. The local host name
C. The user name defined by the administrator
D. The host name of the remote device.

**Answer:** B

**NEW QUESTION 673**
Which technology allows multiple VLANs to be extended across the network without the need for Layer 3 routing?

A. trunk ports
B. MPLS tunnels
C. access ports
D. IPsec tunnels

**Answer:** A

**NEW QUESTION 675**
Which statement describes the effect of the copy run start command on a router in enable mode?

A. The running configuration of the router is saved to NVRAM and used during the boot process.
B. The router reboots and loads the last saved running configuration.
C. A copy of the running configuration of the router is sent by FTP to a designated server.
D. A new running configuration is loaded from flash memory to the router.

**Answer:** A

**NEW QUESTION 678**
Which description refers to administrative distance?

A. the advertised metric to reach a network
B. the cost of a link between two neighboring routers
C. the cost to reach a network that is administratively set
D. a measure of the trustworthiness of a routing information source

**Answer:** D

**NEW QUESTION 683**
If you are in VLAN 10 and it gets a packet from VLAN 2 with 802.1q enabled, what does it do with the packet?

A. Drops the packet
B. forwards it to VLAN 2
C. configures the port to handle traffic from VLAN 2
D. adds it to the VLAN database

**Answer:** A

**NEW QUESTION 687**
Which NTP type designates a router without an external referee clock as an authoritative time source ?

A. Client
B. Server
C. peer
D. master

**Answer:** D

**NEW QUESTION 691**
Which statement about the default Cisco Discovery Protocol configuration is true?

A. CDPv1 is disabled on FastEthernet interfaces.
B. CDPv2 advertisements are unicast.
C. CDPv1 is enabled on Frame Relay subinterfaces.
D. CDPv2 advertisements are broadcast.

**Answer:** D

**NEW QUESTION 694**
Which option is the default time zone used on Cisco devices?

A. CST
B. UTC
C. EST
D. GMT
E. PST

**Answer:** B

**NEW QUESTION 697**
The system LED is amber on a Cisco Catalyst 2950 series switch. What does this indicate?

A. The system is not powered up.
B. The system is powered up and operational.
C. The system is malfunctioning.
D. The system is forwarding traffic.
E. The system is sensing excessive collisions.

**Answer:** C

**Explanation:** The system LED shows whether the system is receiving power and functioning properly. Below lists the LED colors and meanings:
Color
System Status
Off
System is not powered up. Green
System is operating normally. Amber
System is receiving power but is not functioning properly.
(Reference:
http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/hardware/installation/guide/hgovrev.html)

**NEW QUESTION 698**
Which two statements about syslog logging are true? (Choose two.)

A. Messages are stored external to the device.
B. The size of the log file is dependent on the resources of the device.
C. Syslog logging is disabled by default.
D. Messages can be erased when the device reboots.
E. Messages are stored in the internal memory of the device.

**Answer:** AD

**NEW QUESTION 703**
What is the requirement of configuring 6to4 tunnelling on two routers?

A. Both ipv6 and ipv4 must be configured
B. Only IPv6
C. Only IPv4

**Answer:** A

**NEW QUESTION 705**
Which two command can you enter to display the current time sources statistics on devices ? (Choose two.)

A. Show ntp associations.
B. Show clock details
C. Show clock.
D. Show time.
E. Show ntp status

**Answer:** AE

**NEW QUESTION 708**
Which of the following used to identify the immediate destination?

A. Administrative distance
B. Metric
C. Next hop

D. Destination network

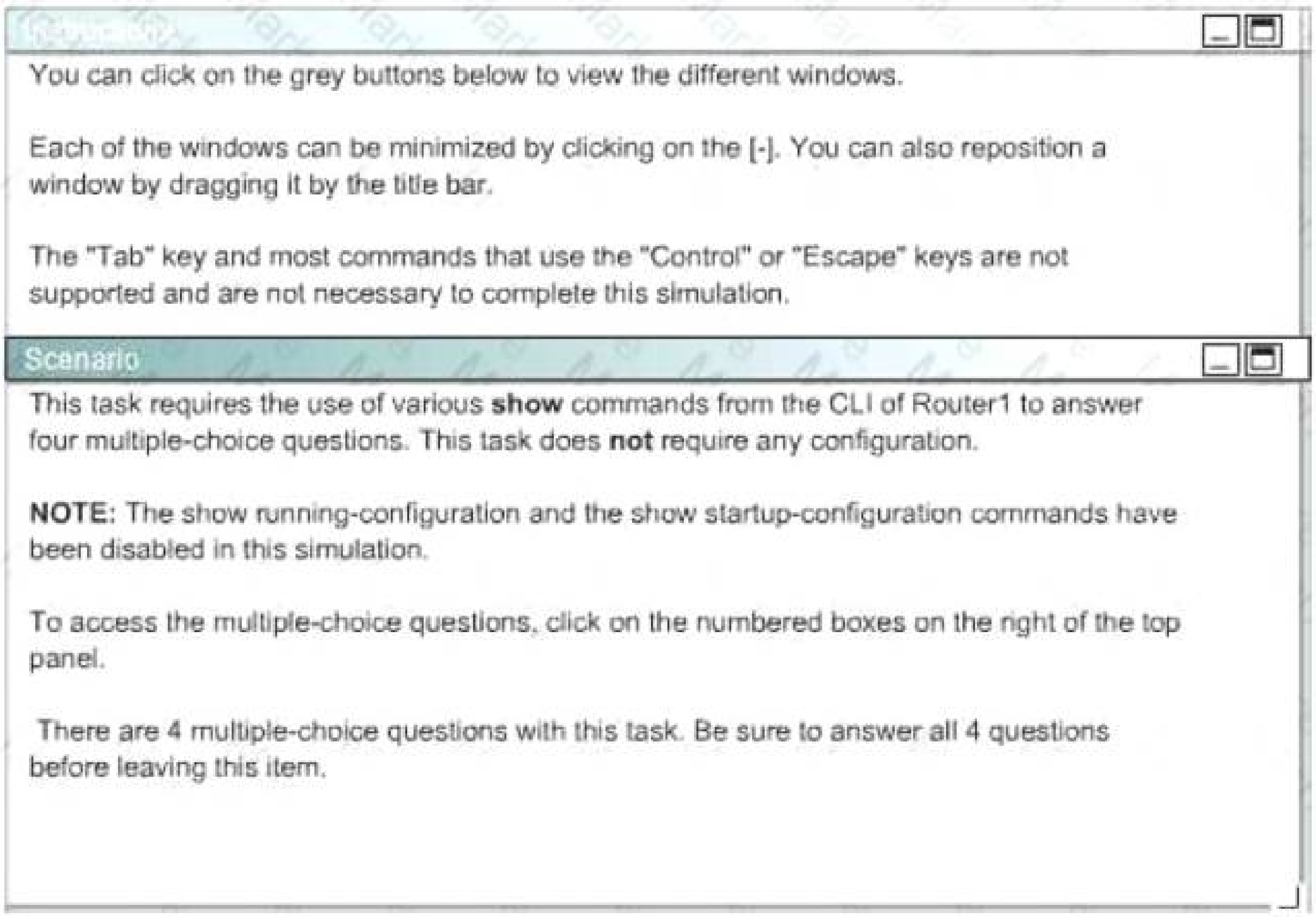
**Answer:** C

**NEW QUESTION 712**
Which subnet mask allows for up to 126 hosts in a single Layer 2 domain?

A. 255.255.128.0
B. 255.255.255.0
C. 255.255.255.128
D. 255.255.255.224

**Answer:** C

**NEW QUESTION 716**
Instruction



You can click on the grey buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation.

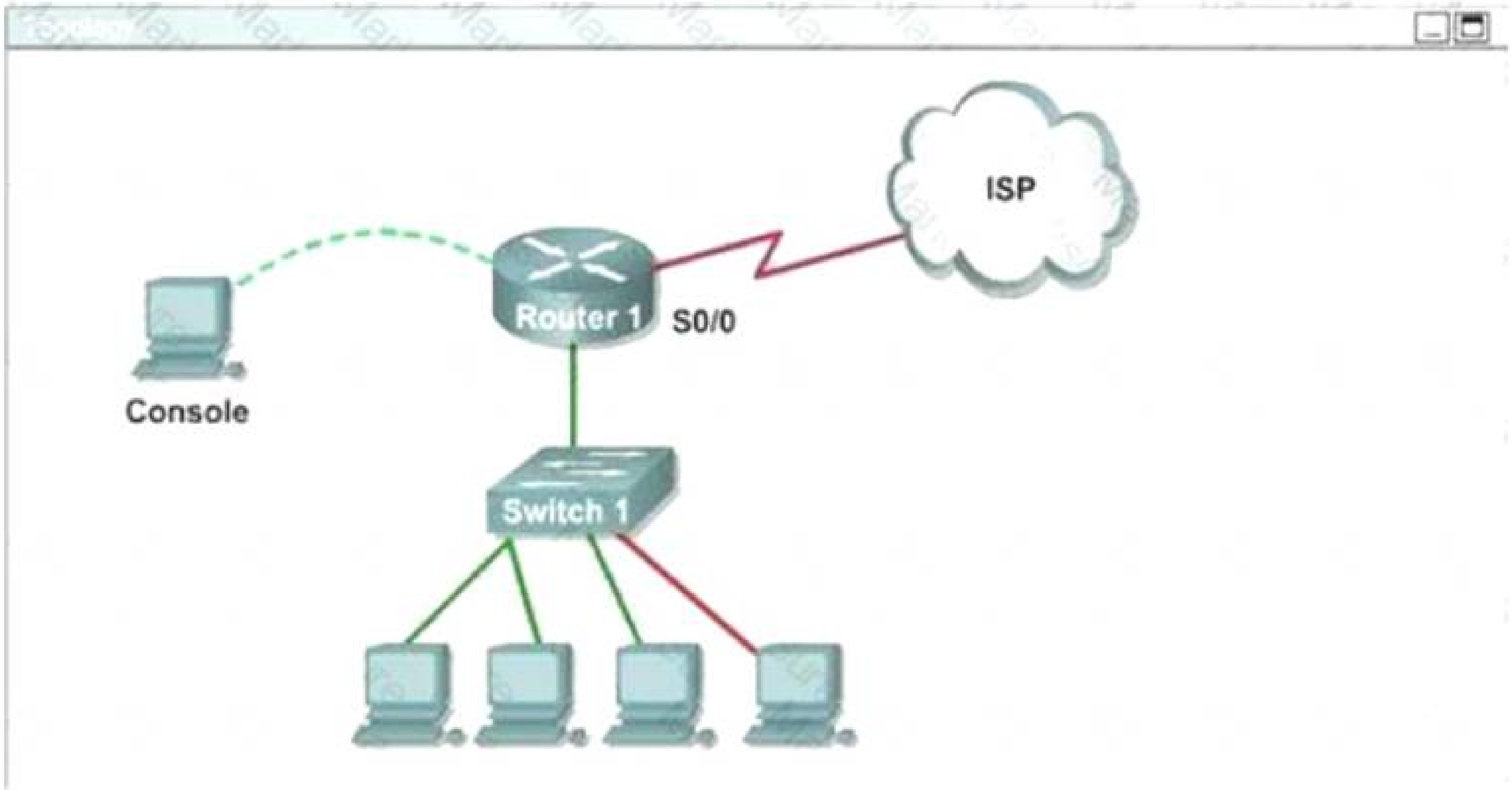
Scenario

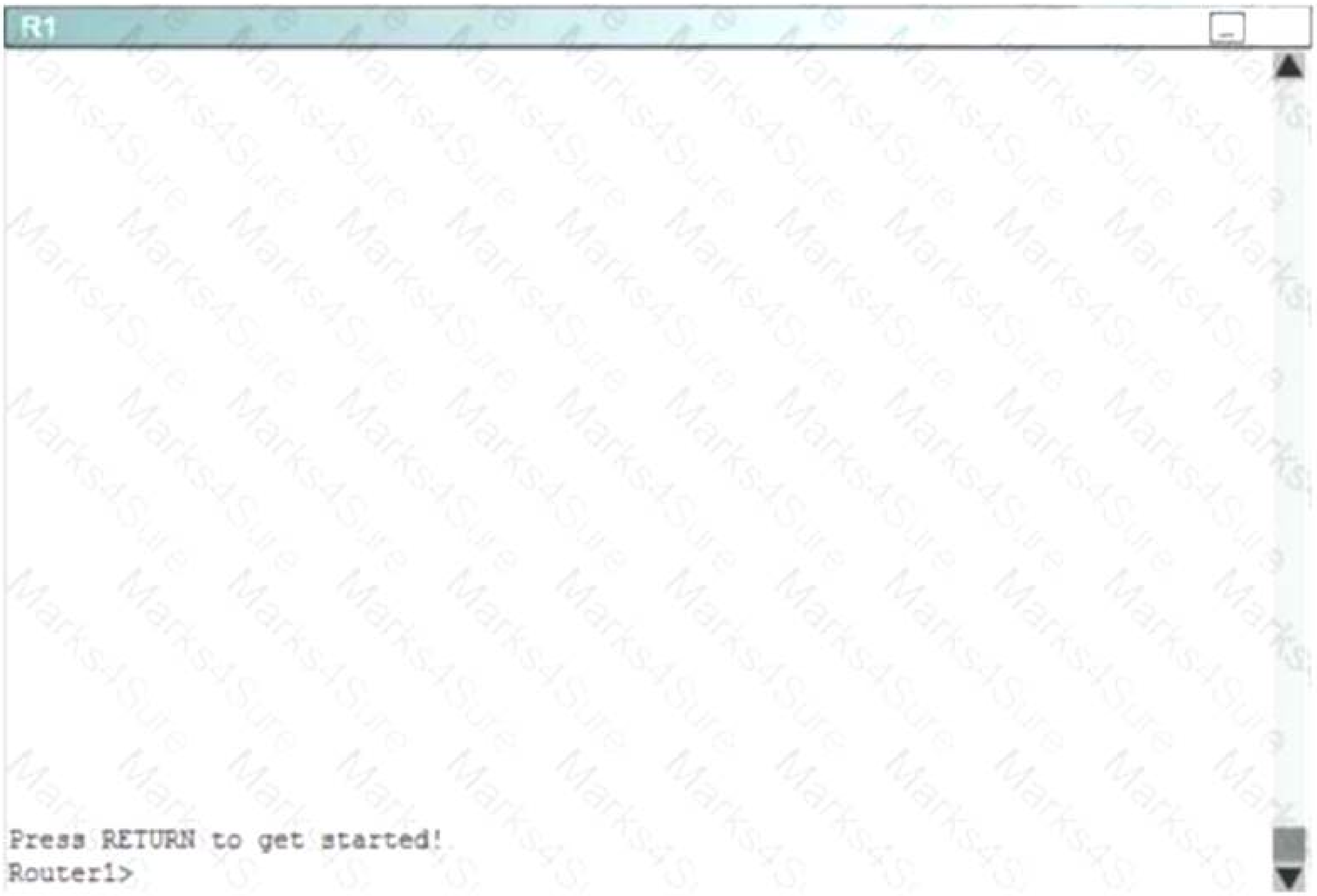
This task requires the use of various **show** commands from the CLI of Router1 to answer four multiple-choice questions. This task does **not** require any configuration.

**NOTE:** The show running-configuration and the show startup-configuration commands have been disabled in this simulation.

To access the multiple-choice questions, click on the numbered boxes on the right of the top panel.

There are 4 multiple-choice questions with this task. Be sure to answer all 4 questions before leaving this item.





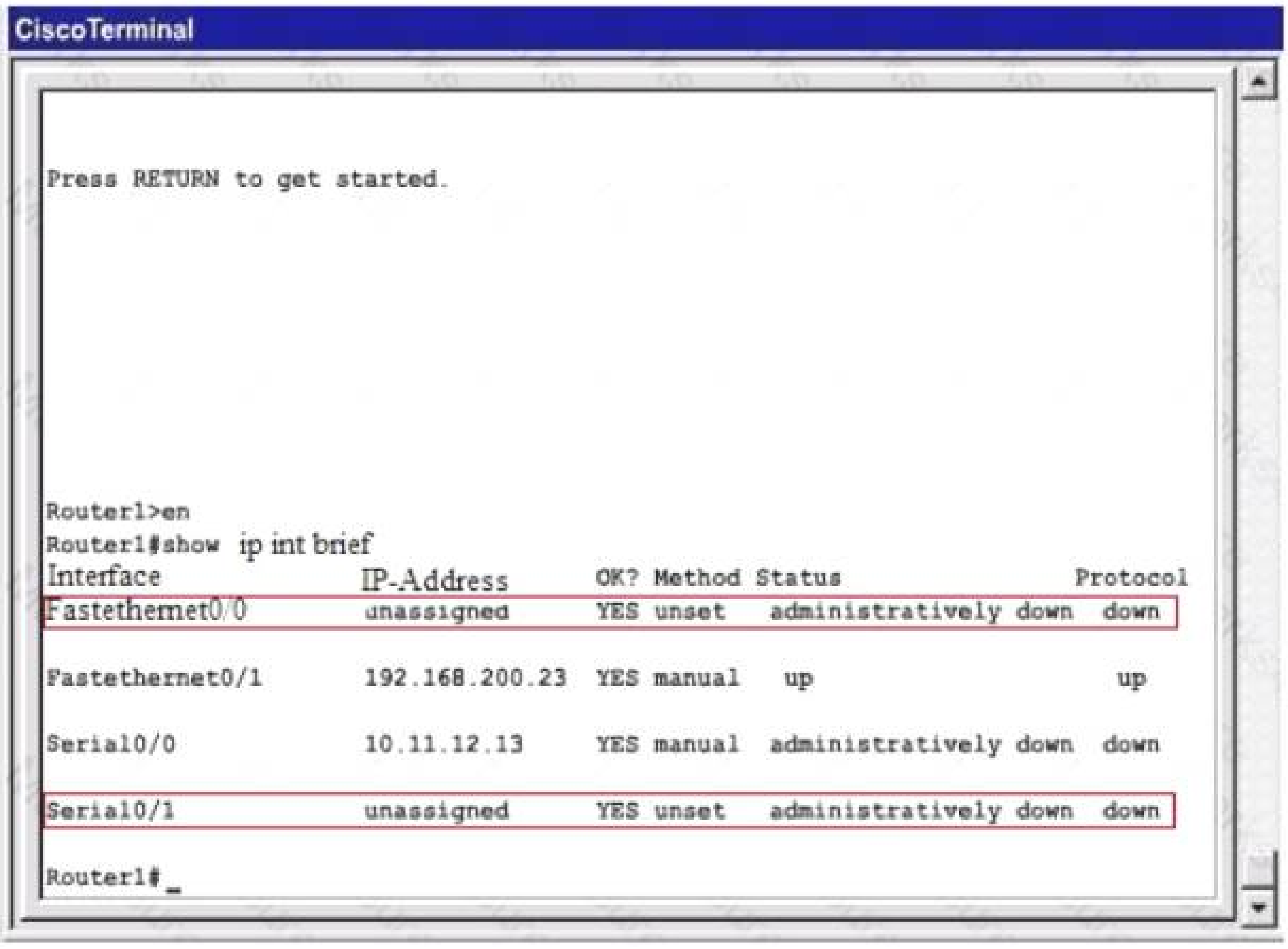
```
Press RETURN to get started!
Router1>
```

What interfaces on Router1 have not had any configurations applied? (Choose two.)

A. Ethernet 0
B. FastEthernet 0/0
C. FastEthernet 0/1
D. Serial 0
E. Serial 0/0
F. Serial 0/1

**Answer:** BF

**Explanation:**



```
Press RETURN to get started.




Router1>en
Router1#show  ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Fastethernet0/0        unassigned      YES unset  administratively down  down

Fastethernet0/1        192.168.200.23  YES manual  up                     up

Serial0/0              10.11.12.13     YES manual  administratively down  down

Serial0/1              unassigned      YES unset  administratively down  down

Router1#_
```

User the "show ip interface brief" command Notice that Router1 does not have Ethernet 0 and Serial 0 interfaces. FastEthernet 0/1 and Serial 0/0 were configured with their IP addresses therefore only FastEthernet 0/0 and Serial0/1 have not had any configurations applied.

**NEW QUESTION 717**
For what reason do you use a standard access list?

A. to filter traffic from identified source addresses
B. to deny traffic to identified destination addresses
C. to load-balance traffic over different interfaces

D. to identify traffic to be label-switched through the network
E. to deny traffic to unidentified destination addresses

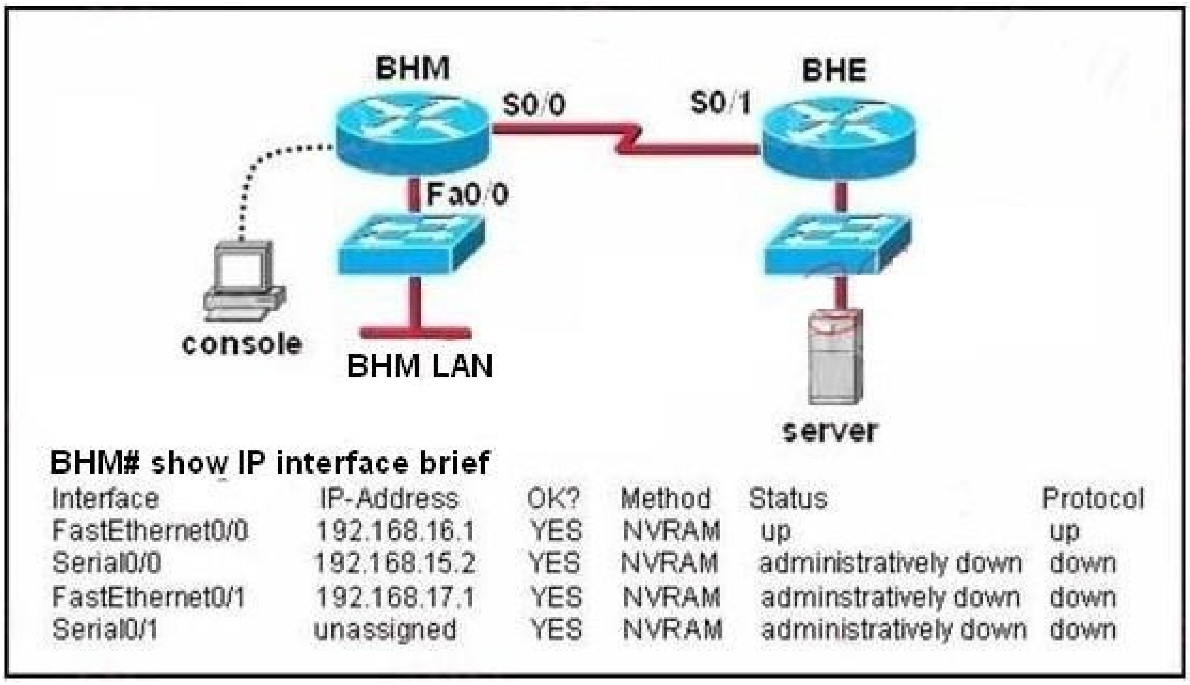
**Answer:** A

**NEW QUESTION 718**
Which two options are fields in an ethernet frame ? (Choose two)

A. destination ip address
B. source ip address
C. type
D. frame check sequence
E. header

**Answer:** CD

**NEW QUESTION 722**
Examine the network diagram and router output shown in the exhibit.



```
BHM# show IP interface brief
Interface          IP-Address    OK?  Method  Status                  Protocol
FastEthernet0/0    192.168.16.1  YES  NVRAM   up                      up
Serial0/0          192.168.15.2  YES  NVRAM   administratively down   down
FastEthernet0/1    192.168.17.1  YES  NVRAM   adminstratively down    down
Serial0/1          unassigned    YES  NVRAM   administratively down   down
```

Users on the BHM LAN are unable to access the server attached to the BHE router. What two things should be done to fix this problem? (Choose two)

A. Enter the configuration mode for interface fastethernet0/0.
B. Enter the configuration mode for interface serial0/0.
C. Enter the configuration mode for interface serial0/1.
D. Issue the run command.
E. Issue the enable command.
F. Issue the no shutdown command.

**Answer:** BF

**NEW QUESTION 726**
Which protocol provides best-effort delivery of user data in a network?

A. TCP
B. MAC
C. IP
D. ARP
E. SMTP

**Answer:** C

**NEW QUESTION 730**
Dhcp client in the back can not communicate with hosts in the outside of their subnet?
***ip dhcp pool my pool******
***network 192.168.10.0/27***
***domain name cisco.com***
****name server some ip***

A. need to activate dhcp pool
B. need to configure default gateway
C. other option
D. other option

**Answer:** B

**NEW QUESTION 734**
For which reason does a DNS client use a DNS server?

A. to assign an IP address

B. to verify network connectivity
C. to resolve an FQDN to an IP address
D. to resolve an IP address to an FQDN

**Answer:** C

**NEW QUESTION 736**
What are types of IPv6 static routes? (Choose Three.)

A. Recursive routes
B. Directly connected routes
C. Fully specified routes
D. Advertised routes
E. Virtual links
F. Redistributed routes

**Answer:** ABC

**NEW QUESTION 739**
Which type of network topology requires each network node to be connected to one another?

A. Ring
B. Star
C. Mesh
D. Bus

**Answer:** C

**NEW QUESTION 742**
What to do when the router password was forgotten?

A. use default password cisco to reset
B. access router physically
C. use ssl/vpn
D. Type confreg 0x2142 at the rommon 1

**Answer:** D

**NEW QUESTION 746**
Which type of route is the most trusted?

A. BGP
B. OSPF
C. static
D. connected

**Answer:** D

**NEW QUESTION 747**
Which type of routing protocol operates by exchanging the entire routing information ?

A. distance vector protocols
B. link state protocols
C. path vector protocols
D. exterior gateway protocols

**Answer:** A

**NEW QUESTION 751**
Which type of secure MAC address must be configured manually?

A. dynamic
B. bia
C. static
D. sticky

**Answer:** C

**NEW QUESTION 754**
Which feature allows the network administrator to view the hardware of a Cisco peer device connected to an interface?

A. RIP
B. CDP
C. VTP
D. STP

**Answer:** B

**NEW QUESTION 756**
Which symbol ping of the following is for unknown packet?

A. .
B. *
C. ?
D. U

**Answer:** C

**NEW QUESTION 759**
Which statement about DHCP address pools is true?

A. A network must be defined before you can configure a manual binding.
B. Only one DNSserver can be identified for an individual DHCP group.
C. You can use a subnet mask of prefix length to define a network.
D. The domain name of the DHCP pool is specified in the global configuration of the router.

**Answer:** C

**NEW QUESTION 762**
Which IPv6 address type is used publicly for hosts?

A. unique local
B. IPv4 mapped
C. global unicast
D. link local

**Answer:** C

**NEW QUESTION 764**
Regarding the extended ping command; which of the statements below are true? (Choose three)

A. The extended ping command is supported from user EXEC mode.
B. The extended ping command is available from privileged EXEC mode.
C. With the extended ping command you can specify the TCP and UDP port to be pinged.
D. With the extended ping command you can specify the timeout value.
E. With the extended ping command you can specify the datagram size.

**Answer:** BDE

**NEW QUESTION 768**
Which of the following command can be used to access all the files in a system?

A. syslog
B. IFS
C. ping
D. NTP

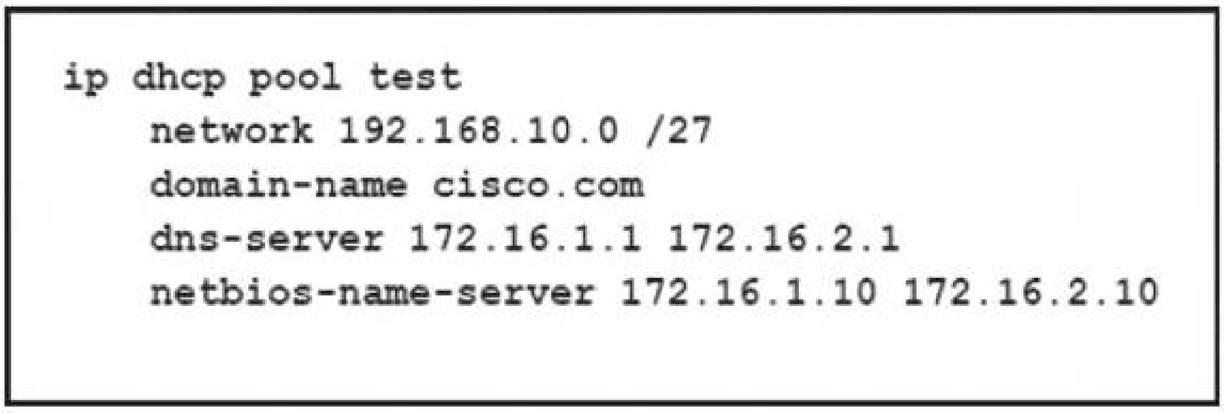
**Answer:** B

**NEW QUESTION 773**
Which major ipv6 address type is supported in ipv4 but rarely used ?

A. Broadcast
B. multicast
C. unicast
D. anycast

**Answer:** D

**NEW QUESTION 774**
Refer to the exhibit.



```
ip dhcp pool test
   network 192.168.10.0 /27
   domain-name cisco.com
   dns-server 172.16.1.1 172.16.2.1
   netbios-name-server 172.16.1.10 172.16.2.10
```

After you apply the given configuration to a router, the DHCP clients behind the device cannot communicate with hosts outside of their subnet. Which action is most likely to correct the problem?

A. Configure the dns server on the same subnet as the clients
B. Activate the dhcp pool
C. Correct the subnet mask
D. configure the default gateway

**Answer:** D

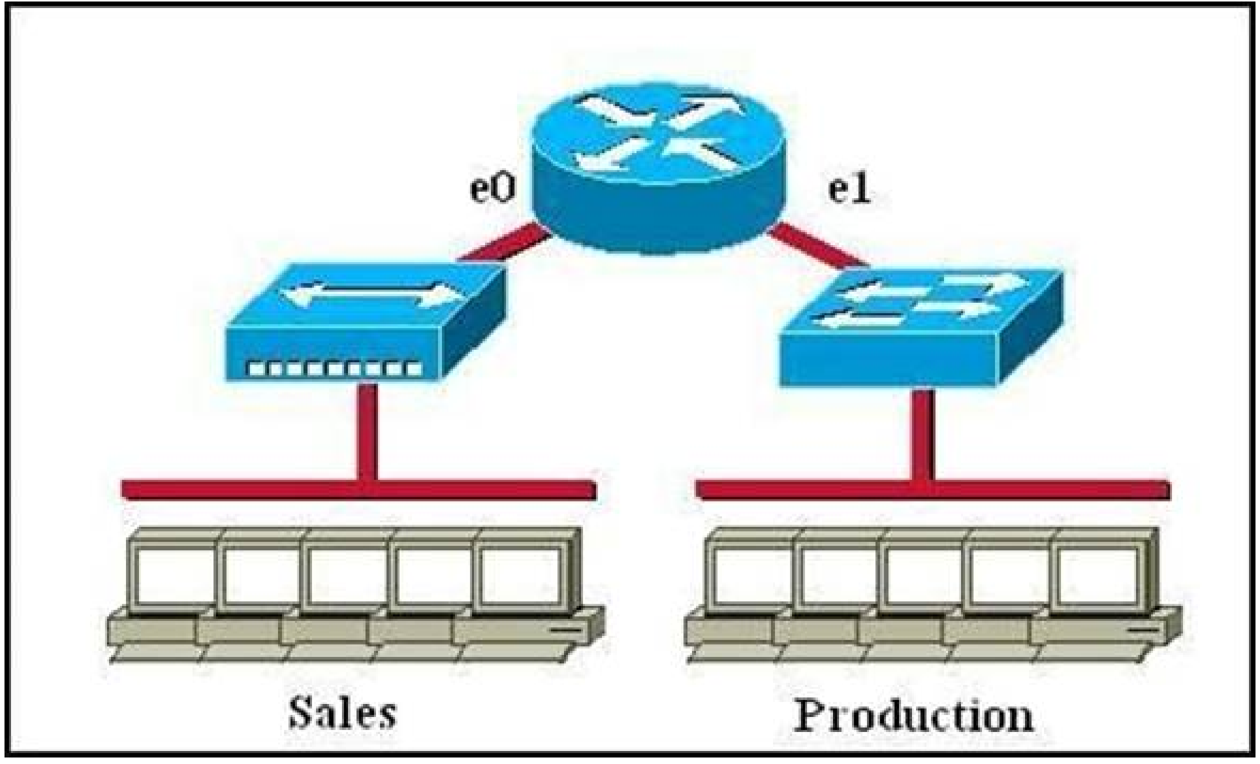
**NEW QUESTION 779**
An administrator is working with the 192.168.4.0 netwrok, which has been subnetted with a /26 mask. Which two addresses can be assigned to hosts within the same subnet? (Choose two.)

A. 192.168.4.67
B. 192.168.4.61
C. 192.168.4.128
D. 192.168.4.132
E. 192.168.4.125
F. 192.168.4.63

**Answer:** AE

**Explanation:** Only the values of host with 67 and 125 fall within the range of /26 CIDR subnet mask, all others lie beyond it.

**NEW QUESTION 780**
Which of the following statements describe the network shown in the graphic? (Choose two.)



A. There are two broadcast domains in the network.
B. There are four broadcast domains in the network.
C. There are six broadcast domains in the network.
D. There are four collision domains in the network.
E. There are five collision domains in the network.
F. There are seven collision domains in the network.

**Answer:** AF

**NEW QUESTION 782**
Which option describes a standard role that a firewall plays in an enterprise network?

A. It can permit unauthorized packets to pass to less secure segments of the network
B. It can decide which packets can traverse from a less secure segment of the network to a more secure
C. It can forward packets based on rules that are predetermined by IEEE standards

D. It can deny all packets from entering an administrative domain.

**Answer:** B

**NEW QUESTION 785**
After you configure a default route to the Internet on a router, the route is missing from the routing table.
Which option describes a possible reason for the problem?

A. The next-hop address is unreachable.
B. The default route was configured on a passive interface.
C. Dynamic routing is disabled.
D. Cisco Discovery Protocol is disabled on the interface used to reach the next hop.

**Answer:** A

**NEW QUESTION 786**
Which type of routing protocol operates by using first information from each device peers?

A. link-state protocols
B. distance-vector protocols
C. path-vector protocols
D. exterior gateway protocols

**Answer:** A

**NEW QUESTION 791**
Which statement is true about port-security violations is true?

A. When a violation occurs on a switch port in restrict mode, the switch port continues to accept traffic from unknown MAC address until the administrator manually disables it.
B. When a violation occurs on a switch port in protect mode, it sends a syslog notification message.
C. A port in the err-disabled state must be re-enabled manually, if recovery is disabled.
D. When a switch port is in protect mode, it allows traffic from unknown MAC address until it has learned the maximum allowable number of MAC addresses.

**Answer:** C

**NEW QUESTION 795**
Which technique can you use to route IPv6 traffic over an IPv4 infrastructure?

A. NAT
B. 6to4 tunneling
C. L2TPv3
D. dual-stack

**Answer:** B

**NEW QUESTION 796**
Which feature automatically disables Cisco Express Forwarding when it is enabled?

A. multicast
B. IP redirects
C. RIB
D. ACL logging

**Answer:** D

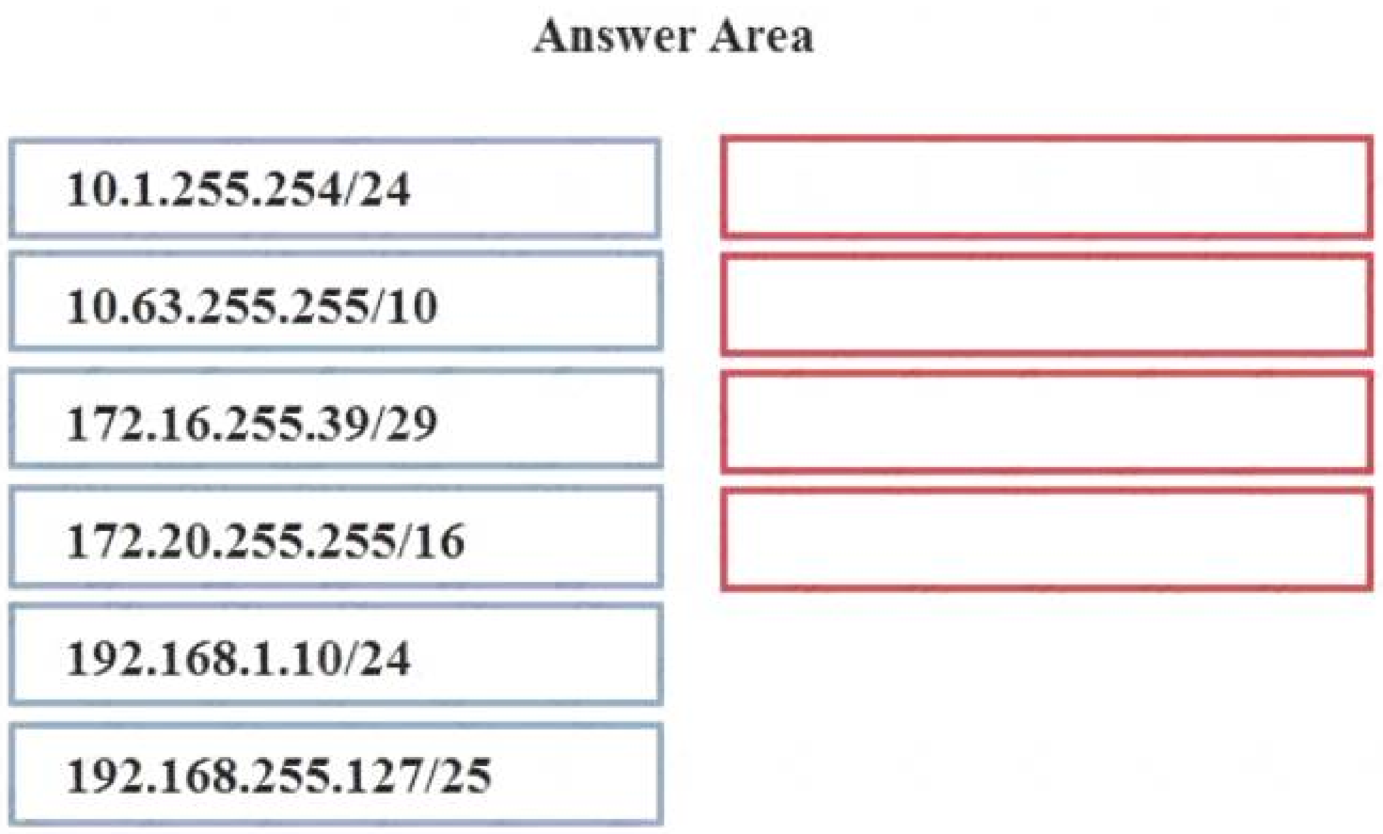
**Explanation:** If you enable CiscoExpress Forwarding and then create an access list that uses the logkeyword, the packets that match the access list are not Cisco Express Forwarding switched. They are process switched. Logging disables Cisco Express Forwarding.

**NEW QUESTION 800**
Which statement is a Cisco best practice for switch port security?

A. Vacant switch ports must be shut down.
B. Empty ports must be enabled in VLAN 1.
C. VLAN 1 must be configured as the native VLAN.
D. Err-disabled ports must be configured to automatically re-enable.

**Answer:** A

**NEW QUESTION 804**
Drag and drop each broadcast IP address on the left to the Broadcast Address column on the right. Not all options are used.
Select and Place:



Answer Area

10.1.255.254/24

10.63.255.255/10

172.16.255.39/29

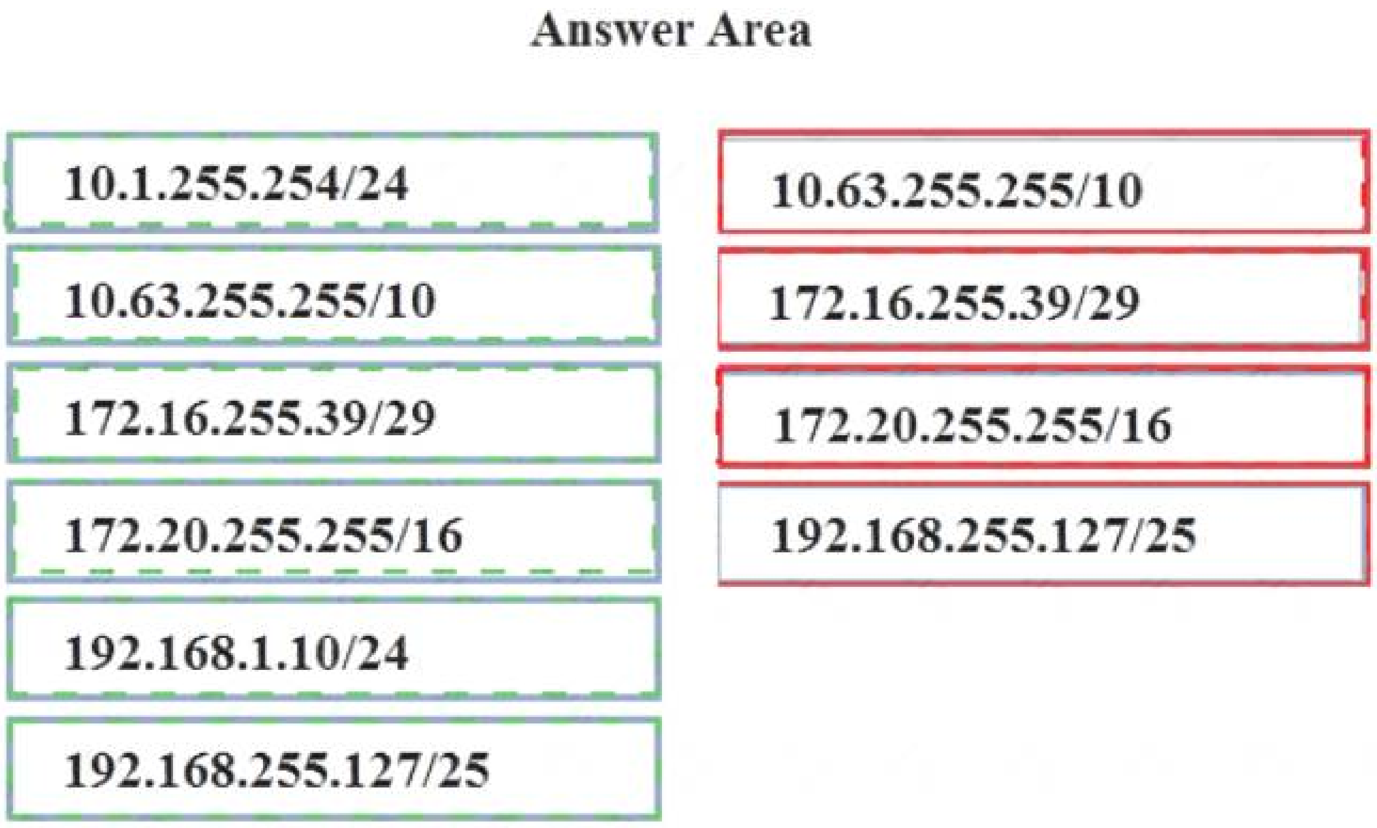
172.20.255.255/16

192.168.1.10/24

192.168.255.127/25

**Answer:**

**Explanation:**

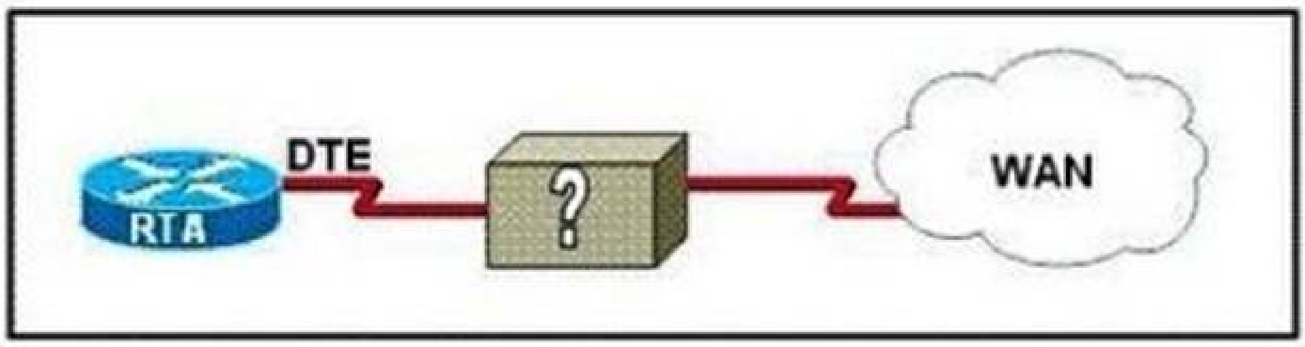


Answer Area

| | |
|---|---|
| 10.1.255.254/24 | 10.63.255.255/10 |
| 10.63.255.255/10 | 172.16.255.39/29 |
| 172.16.255.39/29 | 172.20.255.255/16 |
| 172.20.255.255/16 | 192.168.255.127/25 |
| 192.168.1.10/24 | |
| 192.168.255.127/25 | |

**NEW QUESTION 806**

Refer to the exhibit. The network administrator must complete the connection between the RTA of the XYZ Company and the service provider. To accomplish this task, which two devices could be installed at the customer site to provide a connection through the local loop to the central office of the provider? (Choose two.)



A. WAN switch
B. PVC
C. ATM switch
D. multiplexer
E. CSU/DSU
F. modem

**Answer:** EF

**NEW QUESTION 808**

......