CCNA Cyber Ops (Version 1.1) – Chapter 4 Exam Answers Full

May 13, 2019

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. Which message does an IPv4 host use to reply when it receives a DHCPOFFER message from a DHCP server?

- DHCPACK
- **DHCPREQUEST**
- DHCPDISCOVER
- DHCPOFFER

B. When the client receives the DHCPOFFER from the server, it sends back a DHCPREQUEST broadcast message. On receiving the DHCPREQUESTmessage, the server replies with a unicast DHCPACK message.

2. What OSI layer is responsible for establishing a temporary communication session between two applications and ensuring that transmitted data can be reassembled in proper sequence?

- Session
- **Transport**
- Network
- Data link

B. The transport layer of the OSI model has several responsibilities. One of the primary responsibilities is to segment data into blocks that can be reassembled in proper sequence at the destination device.

3. PC1 and PC3 are on different networks separated by a router, RT1. PC1 issues an ARP request because it needs to send a packet to PC3. In this scenario, what will happen next?

- RT1 will forward the ARP request to PC3.
- RT1 will drop the ARP request.
- **RT1 will send an ARP reply with its own MAC address.**
- RT1 will send an ARP reply with the PC3 MAC address.

C. When a network device has to communicate with a device on another network, it broadcasts an ARP request asking for the default gateway MAC address. The default gateway (RT1) unicasts an ARP reply with its MAC address.

4. What addresses are mapped by ARP?

- Destination IPv4 address to the source MAC address
- Destination IPv4 address to the destination hostname
- Destination MAC address to the source IPv4 address
- **Destination MAC address to a destination IPv4 address**

D. ARP, or the Address Resolution Protocol, works by mapping a destination MAC address to a destination IPv4 address. The host knows the destination IPv4 address and uses ARP to resolve the corresponding destination MAC address.

5. Which statement is true about FTP?

- **The client can download data from or upload data to the server.**
- The client can choose if FTP is going to establish one or two connections with the server.
- FTP is a peer-to-peer application.
- FTP does not provide reliability during data transmission.

A. FTP is a client/server protocol. FTP requires two connections between the client and the server and uses TCP to provide reliable connections. With FTP, data transfer can happen in either direction. The client can download (pull) data from the server or upload (push) data to the server.

6. Which two OSI model layers have the same functionality as two layers of the TCP/IP model? (Choose two.)

- Session
- **Transport**
- **Network**
- Data link
- Physical

B, C. The OSI transport layer is functionally equivalent to the TCP/IP transport layer, and the OSI network layer is equivalent to the TCP/IP Internet layer. The OSI data link and physical layers together are equivalent to the TCP/IP network access layer. The OSI session layer

(with the presentation layer) is included within the TCP/IP application layer.

7. Which statement is true about the TCP/IP and OSI models?

- **The TCP/IP transport layer and OSI Layer 4 provide similar services and functions.**
- The TCP/IP network access layer has similar functions to the OSI network layer.
- The OSI Layer 7 and the TCP/IP application layer provide identical functions.
- The first three OSI layers describe general services that are also provided by the TCP/IP Internet layer.

A. The TCP/IP Internet layer provides the same function as the OSI network layer. The transport layer of both the TCP/IP and OSI models provides the same function. The TCP/IP application layer includes the same functions as OSI Layers 5, 6, and 7.

8. What is the most compressed representation of the IPv6 address 2001:0000:0000:abcd:0000:0000:0000:0001?

- 2001::abcd::1
- 2001:0:abcd::1
- 2001::abcd:0:1
- **2001:0:0:abcd::1**
- 2001:0000:abcd::1

D. The IPv6 address 2001:0000:0000:abcd:0000:0000:0000:0001 in its most compressed format would be 2001:0:0:abcd::1. The first two hextets of zeros would each compress to a single zero. The three consecutive hextets of zeros can be compressed to a double colon ::. The three leading zeros in the last hextet can be removed. The double colon :: can only be used once in an address.

9. What three application layer protocols are part of the TCP/IP protocol suite? (Choose three.)

- ARP
- **DHCP**
- **DNS**
- **FTP**
- NAT
- PPP

B, C, D. DNS, DHCP, and FTP are all application layer protocols in the TCP/IP protocol suite. ARP and PPP are network access layer protocols, and NAT is an Internet layer protocol in the TCP/IP protocol suite.

10. If the default gateway is configured incorrectly on the host, what is the impact on communications?

- The host is unable to communicate on the local network.
- There is no impact on communications.
- The host can communicate with other hosts on remote networks, but is unable to communicate with hosts on the local network.
- **The host can communicate with other hosts on the local network, but is unable to communicate with hosts on remote networks.**

D. A default gateway is only required to communicate with devices onanother network. The absence of a default gateway does not affect connectivity between devices on the same local network

11. Which message delivery option is used when all devices need to receive the same message simultaneously?

- Duplex
- Unicast
- Multicast
- **Broadcast**

D. When all devices need to receive the same message simultaneously, the message would be delivered as a broadcast. Unicast delivery occurs when one source host sends a message to one destination host. The sending of the same message from a host to a group of destination hosts is multicast delivery. Duplex communications refers to the ability of the medium to carry messages in both directions.

12. How is a DHCPDISCOVER transmitted on a network to reach a DHCP server?

- A DHCPDISCOVER message is sent with a multicast IP address that all DHCP servers listen to as the destination address.
- **A DHCPDISCOVER message is sent with the broadcast IP address as the destination address.**
- A DHCPDISCOVER message is sent with the IP address of the default gateway as the destination address.
- A DHCPDISCOVER message is sent with the IP address of the DHCP server as the destination address.

The DHCPDISCOVER message is sent by a DHCPv4 client and targets a broadcast IP along with the destination port 67. The DHCPv4 server or servers respond to the DHCPv4 clients by targeting port 68.

13. A high school in New York (school A) is using videoconferencing technology to establish student interactions with another high school (school B) in Russia. The videoconferencing is conducted between two end devices through the Internet. The network administrator of school A configures the end device with the IP address 209.165.201.10. The administrator sends a request for the IP address for the end device in school B and the response is 192.168.25.10. Neither school is using a VPN. The administrator knows immediately that this IP will not work. Why?

- This is a link-local address.
- This is a loopback address.
- There is an IP address conflict.
- **This is a private IP address.**

The IP address 192.168.25.10 is an IPv4 private address. This address will not be routed over the Internet, so school A will not be able to reach school B. Because the address is a private one, it can be used freely on an internal network. As long as no two devices on the internal network are assigned the same private IP, there is no IP conflict issue. Devices that are assigned a private IP will need to use NAT in order to communicate over the Internet.

14. What is a socket?

- the combination of the source and destination sequence numbers and port numbers
- **the combination of a source IP address and port number or a destination IP address and port number**
- the combination of the source and destination sequence and acknowledgment numbers
- the combination of the source and destination IP address and source and destination Ethernet address

A socket is a combination of the source IP address and source port or the destination IP address and the destination port number.

15. What part of the URL, http://www.cisco.com/index.html, represents the top-level DNS domain?

- www
- http
- index
- **com**

The components of the URL http://www.cisco.com/index.htm are as follows:
http = protocol
www = part of the server name

cisco = part of the domain name
index = file name
com = the top-level domain

16. The graphic shows a network diagram as follows:
**PC A connects to switch S1, which connects to the G0/0 interface of router R1.**
PC B connects to switch S2, which connects to the G0/1 interface of router R1. A
network analyst is connected to switch S2. The address of each device is as
follows:
PC A: 192.168.1.212 and FE80::1243:FEFE:8A43:2122 and 01-90-C0-E4-55-BB
PC B: 192.168.2.101 and FE80::FBB2:E77A:D143 and 08-CB-8A-5C-D5-8A
R1 G0/0:192.168.1.1 and FE80::1 and 00-D0-D3-BE-79-26
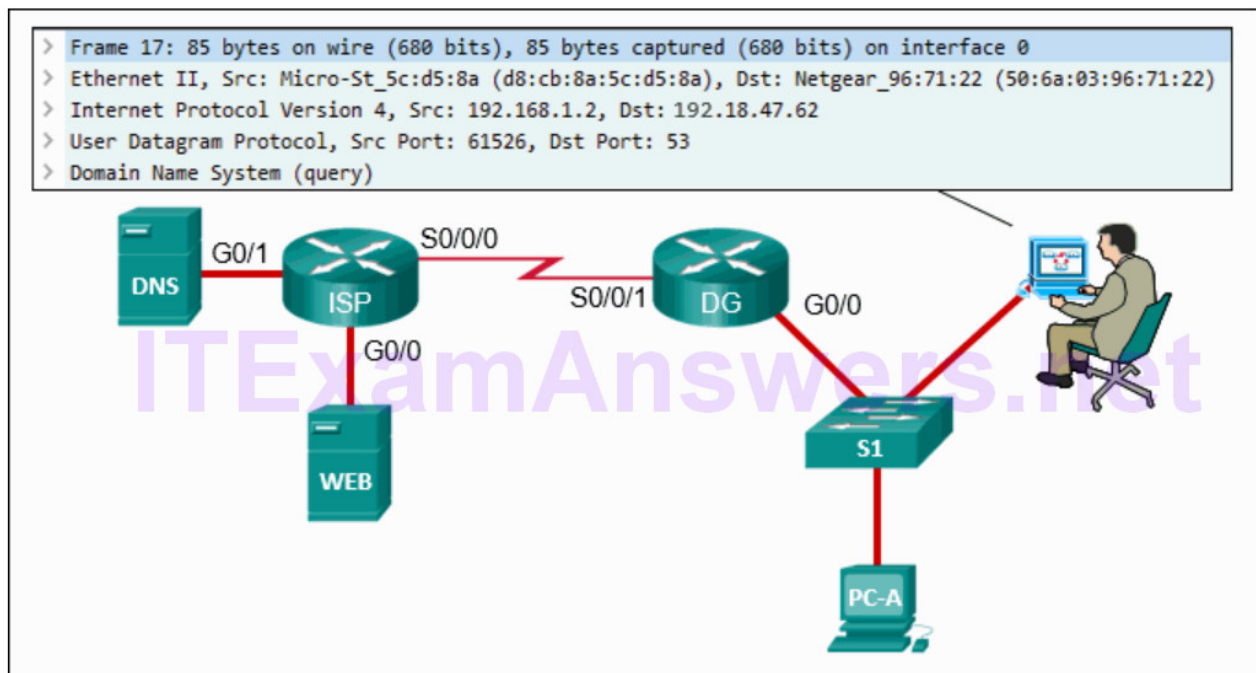**R1 G0/1: 192.168.2.1 and FE80::1 and 00-60-0F-B1-D1-11**
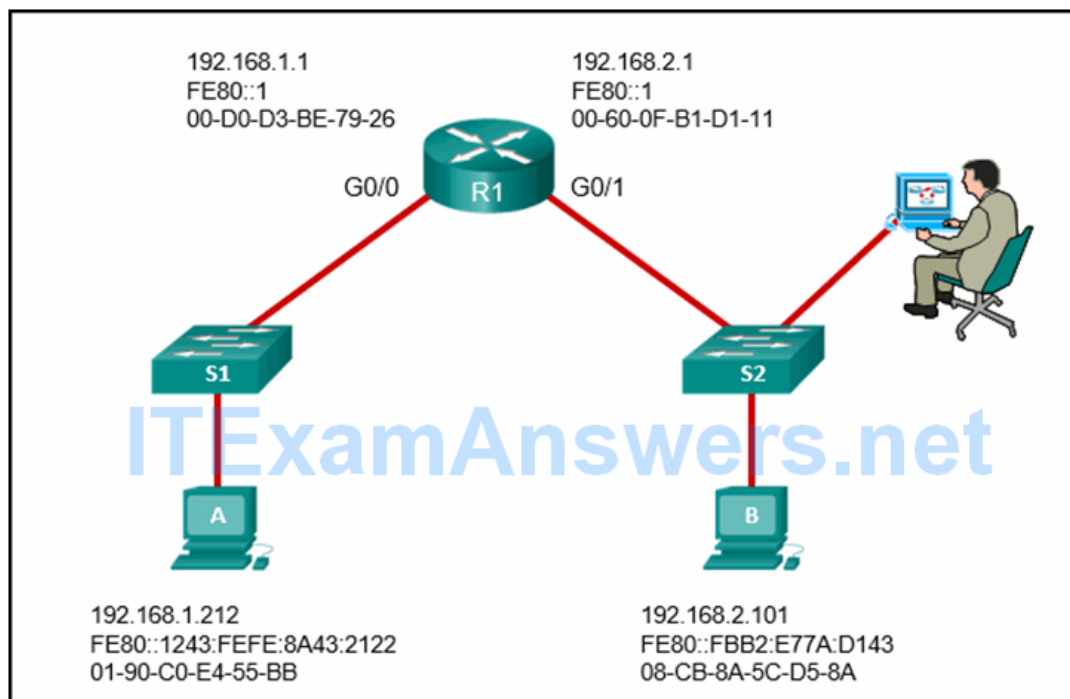
Refer to the exhibit. A cybersecurity analyst is viewing captured ICMP echo
request packets sent from host A to host B on switch S2. What is the source MAC
address of Ethernet frames carrying the ICMP echo request packets?

- 08-CB-8A-5C-D5-BA
- 00-D0-D3-BE-79-26
- **00-60-0F-B1-D1-11**
- 01-90-C0-E4-55-BB

When router R1 receives the ICMP echo requests from host A it will forward the packets out
interface G0/1 towards host B. However, before forwarding the packets, R1 will encapsulate
them in a new Ethernet frame using the MAC address of interface G0/1 as the source and the

MAC address of host B as the destination.

17. Refer to the exhibit. A cybersecurity analyst is viewing captured packets forwarded on switch S1. Which device has the MAC address 50:6a:03:96:71:22?


```
> Frame 17: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
> Ethernet II, Src: Micro-St_5c:d5:8a (d8:cb:8a:5c:d5:8a), Dst: Netgear_96:71:22 (50:6a:03:96:71:22)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.18.47.62
> User Datagram Protocol, Src Port: 61526, Dst Port: 53
> Domain Name System (query)
```

- PC-A
- **router DG**
- DSN server
- router ISP
- web server

The Wireshark capture is of a DNS query from PC-A to the DNS server. Because the DNS server is on a remote network, the PC will send the query to the default gateway router, router DG, using the MAC address of the router G0/0 interface on the router.

18. Which term is used to describe the process of placing one message format inside another message format?

- encoding
- multiplexing
- **encapsulation**
- segmentation

The encapsulation process is performed at each OSI layer and is the process of placing one message format inside another message format.

19. Which PDU format is used when bits are received from the network medium by the NIC of a host?

- **frame**
- file
- packet
- segment

When received at the physical layer of a host, the bits are formatted into a frame at the data link layer. A packet is the PDU at the network layer. A segment is the PDU at the transport layer. A file is a data structure that may be used at the application layer.

20. What are two features of ARP? (Choose two.)

- An ARP request is sent to all devices on the Ethernet LAN and contains the IP address of the destination host and its multicast MAC address.
- If no device responds to the ARP request, then the originating node will broadcast the data packet to all devices on the network segment.
- When a host is encapsulating a packet into a frame, it refers to the MAC address table to determine the mapping of IP addresses to MAC addresses.
- **If a host is ready to send a packet to a local destination device and it has the IP address but not the MAC address of the destination, it generates an ARP broadcast.**
- **If a device receiving an ARP request has the destination IPv4 address, it responds with an ARP reply.**

When a node encapsulates a data packet into a frame, it needs the destination MAC address. First it determines if the destination device is on the local network or on a remote network. Then it checks the ARP table (not the MAC table) to see if a pair of IP address and MAC address exists for either the destination IP address (if the destination host is on the local network) or the default gateway IP address (if the destination host is on a remote network). If the match does not exist, it generates an ARP broadcast to seek the IP address to MAC address resolution. Because the destination MAC address is unknown, the ARP request is broadcast with the MAC address FFFF.FFFF.FFFF. Either the destination device or the default gateway will respond with its MAC address, which enables the sending node to assemble the frame. If no device responds to the ARP request, then the originating node will discard the packet because a frame cannot be created.

21. In NAT translation for internal hosts, what address would be used by external users to reach internal hosts?

- outside global
- outside local
- inside local
- **inside global**

From the perspective of a NAT device, inside global addresses are used by external users to reach internal hosts. Inside local addresses are the addresses assigned to internal hosts. Outside global addresses are the addresses of destinations on the external network. Outside local addresses are the actual private addresses of destination hosts behind other NAT devices.

22. The exhibit shows a network topology. PC1 and PC2 are connected to the Fa0/1 and Fa0/2 ports of the SW1 switch, respectively. SW1 is connected through its Fa0/3 port to the Fa0/0 interface of the RT1 router. RT1 is connected through its Fa0/1 to the Fa0/2 port of SW2 switch. SW2 is connected through its Fa0/1 port to the PC3.
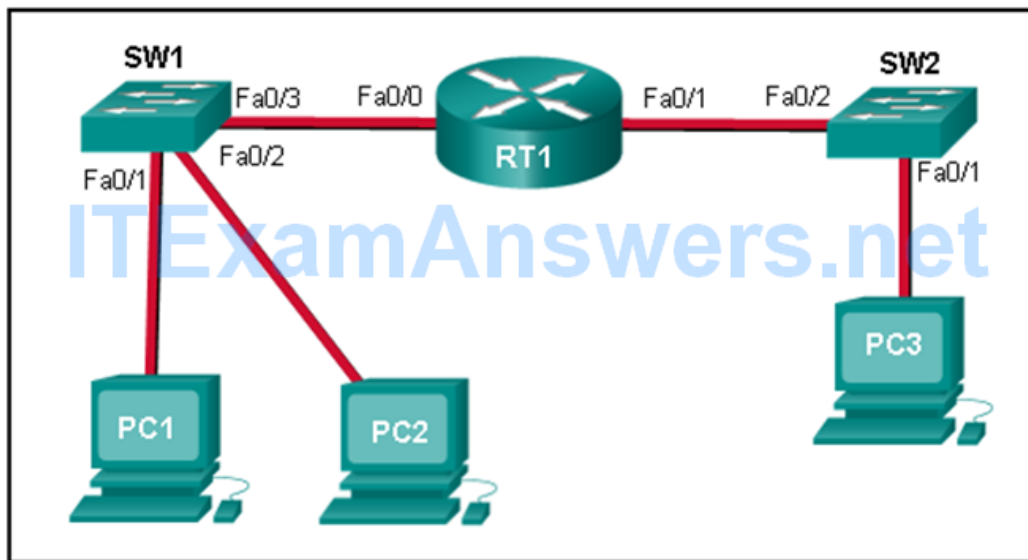
Refer to the exhibit. PC1 issues an ARP request because it needs to send a packet to PC2. In this scenario, what will happen next?

- SW1 will send an ARP reply with the PC2 MAC address.
- **PC2 will send an ARP reply with its MAC address.**
- RT1 will send an ARP reply with its Fa0/0 MAC address.
- RT1 will send an ARP reply with the PC2 MAC address.
- SW1 will send an ARP reply with its Fa0/1 MAC address.

When a network device wants to communicate with another device on the same network, it sends a broadcast ARP request. In this case, the request will contain the IP address of PC2. The destination device (PC2) sends an ARP reply with its MAC address.

23. Which two characteristics are associated with UDP sessions? (Choose two.)

- Unacknowledged data packets are retransmitted.
- **Destination devices receive traffic with minimal delay.**
- Destination devices reassemble messages and pass them to an application.

- Transmitted data segments are tracked.
- **Received data is unacknowledged.**

TCP:
• Provides tracking of transmitted data segments
• Destination devices will acknowledge received data.
• Source devices will retransmit unacknowledged data.

UDP
• Destination devices will not acknowledge received data
• Headers use very little overhead and cause minimal delay.

24. Refer to the exhibit. What is the global IPv6 address of the host in uncompressed format?

- **2001:0DB8:0000:0000:0BAF:0000:3F57:FE94**
- 2001:0DB8:0000:0BAF:0000:0000:3F57:FE94
- 2001:DB80:0000:0000:BAF0:0000:3F57:FE94
- 2001:0DB8:0000:0000:0000:0BAF:3F57:FE94

In the compressed format, the :: represents two contiguous hextets of all zeros. Leading zeros in the second, fifth, and sixth hextets have also been removed.

25. What is the purpose of the routing process?

- to provide secure Internet file transfer
- to convert a URL name into an IP address
- to forward traffic on the basis of MAC addresses
- to encapsulate data that is used to communicate across a network
- **to select the paths that are used to direct traffic to destination networks**

26. Which application layer protocol uses message types such as GET, PUT, and POST?

- SMTP
- POP3

- DHCP
- **HTTP**
- DNS

The GET command is a client request for data from a web server. A PUT command uploads resources and content, such as images, to a web server. A POST command uploads data files to a web server.

27. Which transport layer feature is used to guarantee session establishment?

- UDP sequence number
- **TCP 3-way handshake**
- TCP port number
- UDP ACK flag

TCP uses the 3-way handshake. UDP does not use this feature. The 3-way handshake ensures there is connectivity between the source and destination devices before transmission occurs.

28. What is the prefix length notation for the subnet mask 255.255.255.224?

- /26
- **/27**
- /28
- /25

The binary format for 255.255.255.224 is 11111111.11111111.11111111.11100000. The prefix length is the number of consecutive 1s in the subnet mask. Therefore, the prefix length is /27.

29. What are two potential network problems that can result from ARP operation? (Choose two.)

- Multiple ARP replies result in the switch MAC address table containing entries that match the MAC addresses of hosts that are connected to the relevant switch port.
- **Network attackers could manipulate MAC address and IP address mappings in ARP messages with the intent of intercepting network traffic.**
- **On large networks with low bandwidth, multiple ARP broadcasts could cause data communication delays.**
- Manually configuring static ARP associations could facilitate ARP poisoning or MAC address spoofing.
- Large numbers of ARP request broadcasts could cause the host MAC address table to overflow and prevent the host from communicating on the network.

Large numbers of ARP broadcast messages could cause momentary data communications delays. Network attackers could manipulate MAC address and IP address mappings in ARP messages with the intent to intercept network traffic. ARP requests and replies cause entries

to be made into the ARP table, not the MAC address table. ARP table overflows are very unlikely. Manually configuring static ARP associations is a way to prevent, not facilitate, ARP poisoning and MAC address spoofing. Multiple ARP replies resulting in the switch MAC address table containing entries that match the MAC addresses of connected nodes and are associated with the relevant switch port are required for normal switch frame forwarding operations. It is not an ARP caused network problem.

30. Which TCP mechanism is used to identify missing segments?

- **sequence numbers**
- FCS
- acknowledgments
- window size

TCP segments are acknowledged by the receiver as they arrive. The receiver keeps track of the sequence number of received segments and uses the sequence number to reorder the segments and to identify any missing segments that need to be retransmitted.

31. What is the purpose of ICMP messages?

- **to provide feedback of IP packet transmissions**
- to monitor the process of a domain name to IP address resolution
- to inform routers about network topology changes
- to ensure the delivery of an IP packet

The purpose of ICMP messages is to provide feedback about issues that are related to the processing of IP packets.

32. What happens if part of an FTP message is not delivered to the destination?

- The message is lost because FTP does not use a reliable delivery method.
- **The part of the FTP message that was lost is re-sent.**
- The FTP source host sends a query to the destination host.
- The entire FTP message is re-sent.

Because FTP uses TCP as its transport layer protocol, sequence and acknowledgment numbers will identify the missing segments, which will be re-sent to complete the message.

33. What is the primary purpose of NAT?

- **conserve IPv4 addresses**
- allow peer-to-peer file sharing
- enhance network performance
- increase network security

NAT was developed to conserve IPv4 addresses. A side benefit is that NAT adds a small level of security by hiding the internal network addressing scheme. However, there are some drawbacks of using NAT. It does not allow true peer-to-peer communication and it adds latency to outbound connections.

34. Why does a Layer 3 device perform the ANDing process on a destination IP address and subnet mask?

- **to identify the network address of the destination network**
- to identify the host address of the destination host
- to identify the broadcast address of the destination network
- to identify faulty frames

ANDing allows us to identify the network address from the IP address and the network mask.

35. Refer to the exhibit. Using the network in the exhibit, what would be the default gateway address for host A in the 192.133.219.0 network?
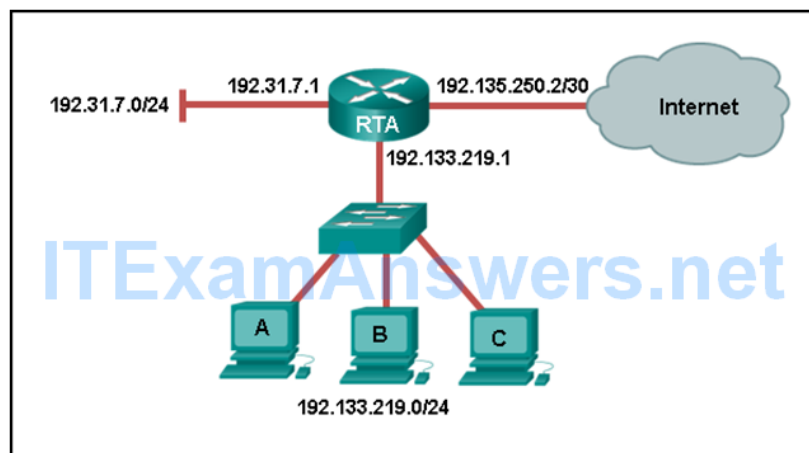
- 192.135.250.1
- 192.133.219.0
- **192.133.219.1**
- 192.31.7.1

36. Which three IP addresses are private ? (Choose three.)

- 192.167.10.10
- **10.1.1.1**
- **192.168.5.5**
- **172.16.4.4**
- 172.32.5.2
- 224.6.6.6

The private IP addresses are within these three ranges:
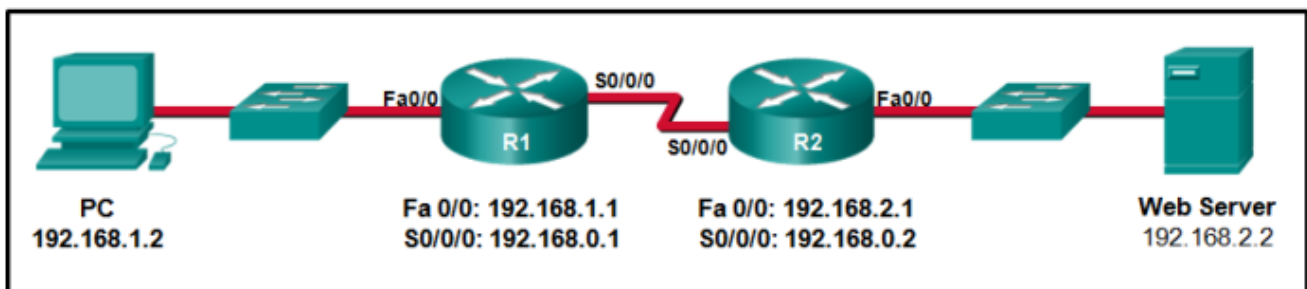10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

37. Match the TCP/IP model layer with the function.

application
transport
internet
network access

supports communication between applications
transport

represents data to the user
application

controls the media
network access

determines best path
internet

38. Refer to the exhibit. Consider a datagram that originates on the PC and that is destined for the web server. Match the IP addresses and port numbers that are in that datagram to the description. (Not all options are used.)

PC
192.168.1.2

Fa 0/0: 192.168.1.1
S0/0/0: 192.168.0.1

Fa 0/0: 192.168.2.1
S0/0/0: 192.168.0.2

Web Server
192.168.2.2

destination IP address	192.168.1.1
destination port number	
source IP address	192.168.1.2
source port number	
	192.168.2.2
	25
	2578
	80

A TCP/IP segment that originated on the PC has 192.168.1.2 as the IP source address. 2578 is the only possible option for the source port number because the PC port number must be in the range of registered ports 1024 to 49151. The destination is the web server, which has the IP address 192.168.2.2, and the destination port number is 80 according to the HTTP protocol standard.

39. Match the compressed IPv6 address representation with the full IPv6 address. (Not all options are used.)

2001:DB8:10:11::10

2001:DB8::10:11:101

2001:DB8:10::11:101

2001:DB8::10:0:11:101

2001:0DB8:0010:0000:0000:0000:0011:0101

2001:0DB8:0000:0000:0010:0000:0011:0101

2001:0DB8:0010:0000:0011:0000:0000:0101

2001:0DB8:0010:0011:0000:0000:0000:0010

2001:0DB8:0000:0000:0000:0010:0011:0101