[Updated Constantly]

HERE

CCNA 1 (v5.1 + v6.0) Chapter 7 Exam Answers Full

How to find: Press "Ctrl + F" in the browser and fill in whatever wording is in the question to find that question/answer.

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. **How many bits are in an IPv4 address?**
   - **32***
   - 64
   - 128
   - 256

   Explain:
   An IPv4 address is comprised of 4 octets of binary digits, each containing 8 bits, resulting in a 32-bit address.

2. **Which two parts are components of an IPv4 address? (Choose two.)**
   - subnet portion
   - **network portion***
   - logical portion
   - **host portion***
   - physical portion
   - broadcast portion

   Explain:
   An IPv4 address is divided into two parts: a network portion – to identify the specific network on which a host resides, and a host portion – to identify specific hosts on a network. A subnet mask is used to identify the length of each portion.

3. **What does the IP address 172.17.4.250/24 represent?**
   - network address
   - multicast address
   - **host address***
   - broadcast address

Explain:
The /24 shows that the network address is 172.17.4.0. The broadcast address for this network would be 172.17.4.255. Useable host addresses for this network are 172.17.4.1 through 172.17.4.254.

4. **What is the purpose of the subnet mask in conjunction with an IP address?**
   - to uniquely identify a host on a network
   - to identify whether the address is public or private
   - **to determine the subnet to which the host belongs***
   - to mask the IP address to outsiders

Explain:
With the IPv4 address, a subnet mask is also necessary. A subnet mask is a special type of IPv4 address that coupled with the IP address determines the subnet of which the device is a member.

5. **What subnet mask is represented by the slash notation /20?**
   - 255.255.255.248
   - 255.255.224.0
   - **255.255.240.0***
   - 255.255.255.0
   - 255.255.255.192

Explain:
The slash notation /20 represents a subnet mask with 20 1s. This would translate to: 11111111.11111111.11110000.0000, which in turn would convert into 255.255.240.0.

6. **A message is sent to all hosts on a remote network. Which type of message is it?**
   - limited broadcast
   - multicast
   - **directed broadcast***
   - unicast

Explain:
A directed broadcast is a message sent to all hosts on a specific network. It is useful for sending a broadcast to all hosts on a nonlocal network. A multicast message is a message sent to a selected group of hosts that are part of a subscribing multicast group. A limited broadcast is used for a communication that is limited to the hosts on the local network. A unicast message is a message sent from one host to another.

7. **What are three characteristics of multicast transmission? (Choose three.)**

- The source address of a multicast transmission is in the range of 224.0.0.0 to 224.0.0.255.
- **A single packet can be sent to a group of hosts. ***
- **Multicast transmission can be used by routers to exchange routing information. ***
- **The range of 224.0.0.0 to 224.0.0.255 is reserved to reach multicast groups on a local network.***
- Computers use multicast transmission to request IPv4 addresses.
- Multicast messages map lower layer addresses to upper layer addresses.

Explain:

Broadcast messages consist of single packets that are sent to all hosts on a network segment. These types of messages are used to request IPv4 addresses, and map upper layer addresses to lower layer addresses. A multicast transmission is a single packet sent to a group of hosts and is used by routing protocols, such as OSPF and RIPv2, to exchange routes. The address range 224.0.0.0 to 224.0.0.255 is reserved for link-local addresses to reach multicast groups on a local network.

8. **Which three IP addresses are private ? (Choose three.)**
   - **10.1.1.1***
   - 172.32.5.2
   - 192.167.10.10
   - **172.16.4.4 ***
   - **192.168.5.5***
   - 224.6.6.6

Explain:

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

9. **Which two IPv4 to IPv6 transition techniques manage the interconnection of IPv6 domains? (Choose two.)**
   - trunking
   - **dual stack***
   - encapsulation
   - **tunneling***
   - multiplexing

Explain:

There are three techniques to allow IPv4 and IPv6 to co-exist on a network. Dual stack allows

IPv4 and IPv6 to coexist on the same network segment. Dual stack devices run both IPv4 and IPv6 protocol stacks simultaneously. Tunneling is a method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet, similar to other types of data. Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4

10. **Which of these addresses is the shortest abbreviation for the IP address: 3FFE:1044:0000:0000:00AB:0000:0000:0057?**
    - 3FFE:1044::AB::57
    - 3FFE:1044::00AB::0057
    - **3FFE:1044:0:0:AB::57***
    - 3FFE:1044:0:0:00AB::0057
    - 3FFE:1044:0000:0000:00AB::57
    - 3FFE:1044:0000:0000:00AB::0057
11. **What type of address is automatically assigned to an interface when IPv6 is enabled on that interface?**
    - global unicast
    - **link-local***
    - loopback
    - unique local

    Explain:
    When IPv6 is enabled on any interface, that interface will automatically generate an IPv6 link-local address.
12. **What are two types of IPv6 unicast addresses? (Choose two.)**
    - multicast
    - **loopback***
    - **link-local***
    - anycast
    - broadcast

    Explain:
    Multicast, anycast, and unicast are types of IPv6 addresses. There is no broadcast address in IPv6. Loopback and link-local are specific types of unicast addresses.
13. **What are three parts of an IPv6 global unicast address? (Choose three.)**
    - an interface ID that is used to identify the local network for a particular host

- **a global routing prefix that is used to identify the network portion of the address that has been provided by an ISP ***
- **a subnet ID that is used to identify networks inside of the local enterprise site***
- a global routing prefix that is used to identify the portion of the network address provided by a local administrator
- **an interface ID that is used to identify the local host on the network***

Explain:
There are three elements that make up an IPv6 global unicast address. A global routing prefix which is provided by an ISP, a subnet ID which is determined by the organization, and an interface ID which uniquely identifies the interface interface of a host.

14. **An administrator wants to configure hosts to automatically assign IPv6 addresses to themselves by the use of Router Advertisement messages, but also to obtain the DNS server address from a DHCPv6 server. Which address assignment method should be configured?**
    - SLAAC
    - **stateless DHCPv6***
    - stateful DHCPv6
    - RA and EUI-64

    Explain:
    Stateless DHCPv6 allows clients to use ICMPv6 Router Advertisement (RA) messages to automatically assign IPv6 addresses to themselves, but then allows these clients to contact a DHCPv6 server to obtain additional information such as the domain name and address of DNS servers. SLAAC does not allow the client to obtain additional information through DHCPv6, and stateful DHCPv6 requires that the client receive its interface address directly from a DHCPv6 server. RA messages, when combined with an EUI-64 interface identifier, are used to automatically create an interface IPv6 address, and are part of both SLAAC and stateless DHCPv6.

15. **Which protocol supports Stateless Address Autoconfiguration (SLAAC) for dynamic assignment of IPv6 addresses to a host?**
    - ARPv6
    - DHCPv6
    - **ICMPv6***
    - UDP

    Explain:
    SLAAC uses ICMPv6 messages when dynamically assigning an IPv6 address to a host.

DHCPv6 is an alternate method of assigning an IPv6 addresses to a host. ARPv6 does not exist. Neighbor Discovery Protocol (NDP) provides the functionality of ARP for IPv6 networks. UDP is the transport layer protocol used by DHCPv6.

16. **Which two things can be determined by using the ping command? (Choose two.)**
    - the number of routers between the source and destination device
    - the IP address of the router nearest the destination device
    - **the average time it takes a packet to reach the destination and for the response to return to the source ***
    - **the destination device is reachable through the network***
    - the average time it takes each router in the path between source and destination to respond

Explain:
A ping command provides feedback on the time between when an echo request was sent to a remote host and when the echo reply was received. This can be a measure of network performance. A successful ping also indicates that the destination host was reachable through the network.

17. **What is the purpose of ICMP messages?**
    - to inform routers about network topology changes
    - to ensure the delivery of an IP packet
    - **to provide feedback of IP packet transmissions***
    - to monitor the process of a domain name to IP address resolution

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

18. **What is indicated by a successful ping to the ::1 IPv6 address?**
    - The host is cabled properly.
    - The default gateway address is correctly configured.
    - All hosts on the local link are available.
    - The link-local address is correctly configured.
    - **IP is properly installed on the host.***

Explain:
The IPv6 address ::1 is the loopback address. A successful ping to this address means that the TCP/IP stack is correctly installed. It does not mean that any addresses are correctly configured.

19. **A user is executing a tracert to a remote device. At what point would a router, which is in the path to the destination device, stop forwarding the packet?**
    - when the router receives an ICMP Time Exceeded message
    - when the RTT value reaches zero
    - when the host responds with an ICMP Echo Reply message
    - **when the value in the TTL field reaches zero***
    - when the values of both the Echo Request and Echo Reply messages reach zero

    Explain:
    When a router receives a traceroute packet, the value in the TTL field is decremented by 1. When the value in the field reaches zero, the receiving router will not forward the packet, and will send an ICMP Time Exceeded message back to the source.

20. **What is the binary equivalent of the decimal number 232?**
    - **11101000***
    - 11000110
    - 10011000
    - 11110010

21. **What is the decimal equivalent of the binary number 10010101?**
    - **149**
    - 157
    - 168
    - 192

22. **What field content is used by ICMPv6 to determine that a packet has expired?**
    - TTL field
    - CRC field
    - **Hop Limit field***
    - Time Exceeded field

    Explain:
    ICMPv6 sends a Time Exceeded message if the router cannot forward an IPv6 packet because the packet expired. The router uses a hop limit field to determine if the packet has expired, and does not have a TTL field.

23. **Fill in the blank.**

    The decimal equivalent of the binary number 10010101 is **149**

    Explain:
    To convert a binary number to the decimal equivalent, add the value of the position where any binary 1 is present.

24. **Fill in the blank.**

The binary equivalent of the decimal number 232 is **11101000**

Explain:

To convert a decimal number to binary, first determine if the decimal number is equal to or greater than 128. In this case, because 232 is larger than 128, a 1 is placed in the bit position for decimal value 128 and the value of 128 is then subtracted from 232. This results in the value of 104. We then compare this value to 64. As 104 is larger than 64, a 1 is placed in the bit position for the decimal value 64 and the value of 64 is subtracted from 104. The remaining value is then 40. The process should be continued for all the remaining bit positions.

25. **Fill in the blank.**

What is the decimal equivalent of the hex number 0x3F? **63**

Explain:

To convert from hexadecimal to decimal, multiply each digit by the place value that is associated with the position of the digit and add the results.

26. **Match each description with an appropriate IP address. (Not all options are used.)**

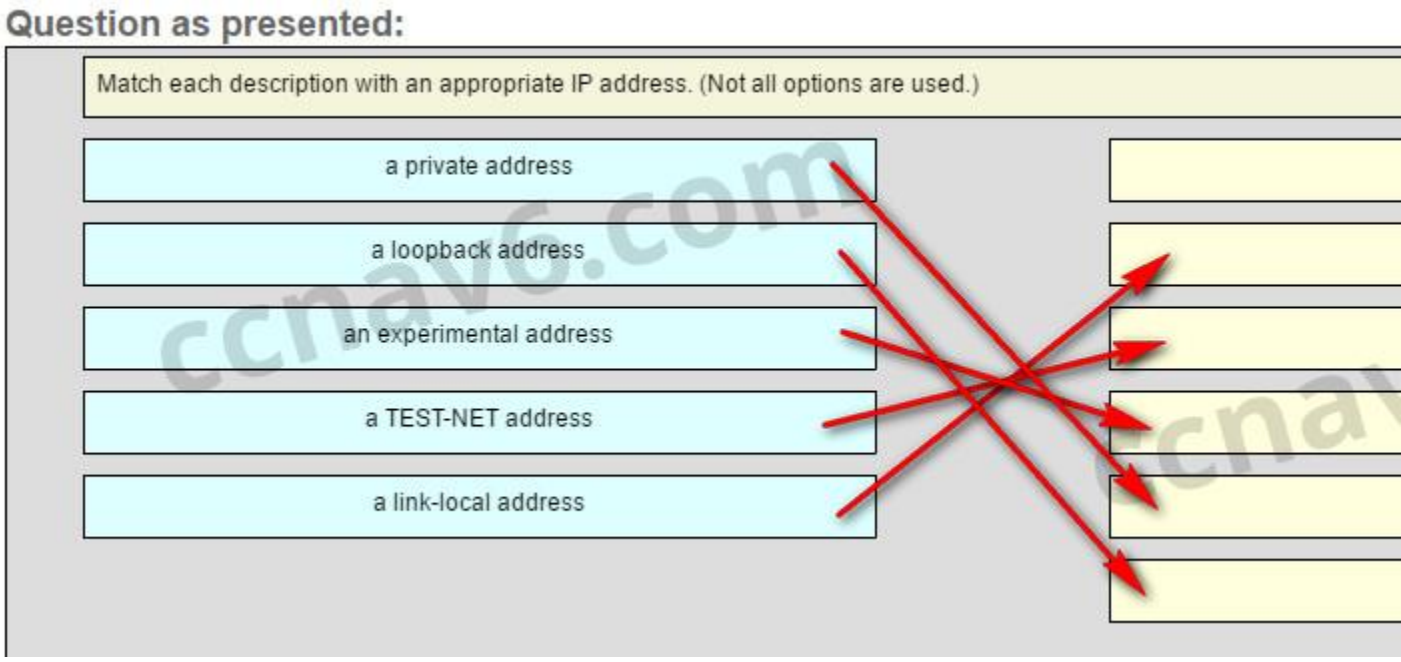
Question

Question as presented:

Match each description with an appropriate IP address. (Not all options are used.)

- a private address
- a loopback address
- an experimental address
- a TEST-NET address
- a link-local address

Answer



Explain:

Link-Local addresses are assigned automatically by the OS environment and are located in the block 169.254.0.0/16. The private addresses ranges are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. TEST-NET addresses belong to the range 192.0.2.0/24. The addresses in the block 240.0.0.0 to 255.255.255.254 are reserved as experimental addresses. Loopback addresses belong to the block 127.0.0.0/8.

Older Versions

27. **What is a socket?**
    - the combination of the source and destination IP address and source and destination Ethernet address
    - **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 sequence numbers and port numbers
28. **A host device needs to send a large video file across the network while providing data communication to other users. Which feature will allow different communication streams to occur at the same time, without having a single data stream using all available bandwidth?**
    - window size
    - **multiplexing***

- port numbers
- acknowledgments

29. **A host device sends a data packet to a web server via the HTTP protocol. What is used by the transport layer to pass the data stream to the proper application on the server?**
    - sequence number
    - acknowledgment
    - source port number
    - **destination port number***
30. **What is a beneficial feature of the UDP transport protocol?**
    - acknowledgment of received data
    - **fewer delays in transmission***
    - tracking of data segments using sequence numbers
    - the ability to retransmit lost data
31. **Which scenario describes a function provided by the transport layer?**
    - A student is using a classroom VoIP phone to call home. The unique identifier burned into the phone is a transport layer address used to contact another network device on the same network.
    - A student is playing a short web-based movie with sound. The movie and sound are encoded within the transport layer header.
    - **A student has two web browser windows open in order to access two web sites. The transport layer ensures the correct web page is delivered to the correct browser window.***
    - A corporate worker is accessing a web server located on a corporate network. The transport layer formats the screen so the web page appears properly no matter what device is being used to view the web site.
32. **What is the complete range of TCP and UDP well-known ports?**
    - 0 to 255
    - **0 to 1023***
    - 256 – 1023
    - 1024 – 49151
33. **What does a client application select for a TCP or UDP source port number?**
    - a random value in the well-known port range
    - **a random value in the range of the registered ports***
    - a predefined value in the well-known port range
    - a predefined value in the range of the registered ports

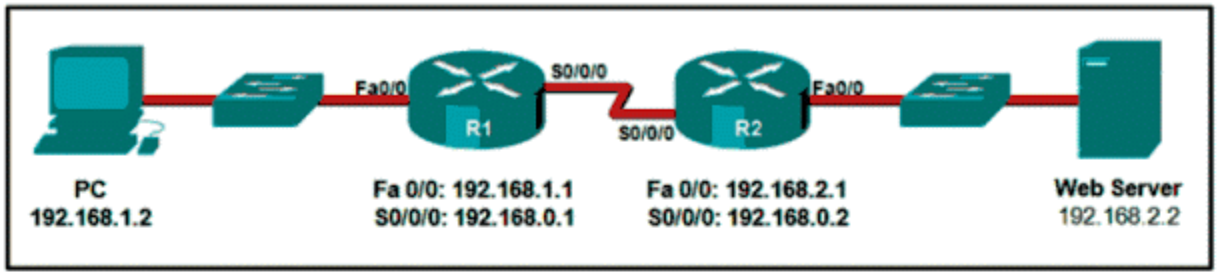
34. **Compared to UDP, what factor causes additional network overhead for TCP communication?**
    - **network traffic that is caused by retransmissions***
    - the identification of applications based on destination port numbers
    - the encapsulation into IP packets
    - the checksum error detection
35. **Which transport layer feature is used to guarantee session establishment?**
    - UDP ACK flag
    - **TCP 3-way handshake***
    - UDP sequence number
    - TCP port number
36. **Which two flags in the TCP header are used in a TCP three-way handshake to establish connectivity between two network devices? (Choose two.)**
    - **ACK***
    - FIN
    - PSH
    - RST
    - **SYN***
    - URG
37. **Which factor determines TCP window size?**
    - the amount of data to be transmitted
    - the number of services included in the TCP segment
    - **the amount of data the destination can process at one time***
    - the amount of data the source is capable of sending at one time
38. **During a TCP session, a destination device sends an acknowledgment number to the source device. What does the acknowledgment number represent?**
    - the total number of bytes that have been received
    - one number more than the sequence number
    - **the next byte that the destination expects to receive***
    - the last sequence number that was sent by the source
39. **A PC is downloading a large file from a server. The TCP window is 1000 bytes. The server is sending the file using 100-byte segments. How many segments will the server send before it requires an acknowledgment from the PC?**
    - 1 segment
    - **10 segments***
    - 100 segments

- 1000 segments

40. **Which two TCP header fields are used to confirm receipt of data?**
    - FIN flag
    - SYN flag
    - checksum
    - **sequence number ***
    - **acknowledgment number***
41. **What happens if the first packet of a TFTP transfer is lost?**
    - The client will wait indefinitely for the reply.
    - **The TFTP application will retry the request if a reply is not received.***
    - The next-hop router or the default gateway will provide a reply with an error code.
    - The transport layer will retry the query if a reply is not received.
42. **What does a client do when it has UDP datagrams to send?**
    - **It just sends the datagrams.***
    - It queries the server to see if it is ready to receive data.
    - It sends a simplified three-way handshake to the server.
    - It sends to the server a segment with the SYN flag set to synchronize the conversation.
43. **A technician wishes to use TFTP to transfer a large file from a file server to a remote router. Which statement is correct about this scenario?**
    - The file is segmented and then reassembled in the correct order by TCP.
    - **The file is segmented and then reassembled in the correct order at the destination, if necessary, by the upper-layer protocol.**
    - The file is not segmented, because UDP is the transport layer protocol that is used by TFTP.
    - Large files must be sent by FTP not TFTP.
44. **Fill in the blank.**

    During a TCP session, the **SYN** flag is used by the client to request communication with the server.
45. **Fill in the blank using a number.**

    A total of **4** messages are exchanged during the TCP session termination process between the client and the server.
46. **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.)**



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.)

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

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 a description. (Not all options are used.)

192.168.1.1
source IP address
destination IP address
25
source port number
destination port number

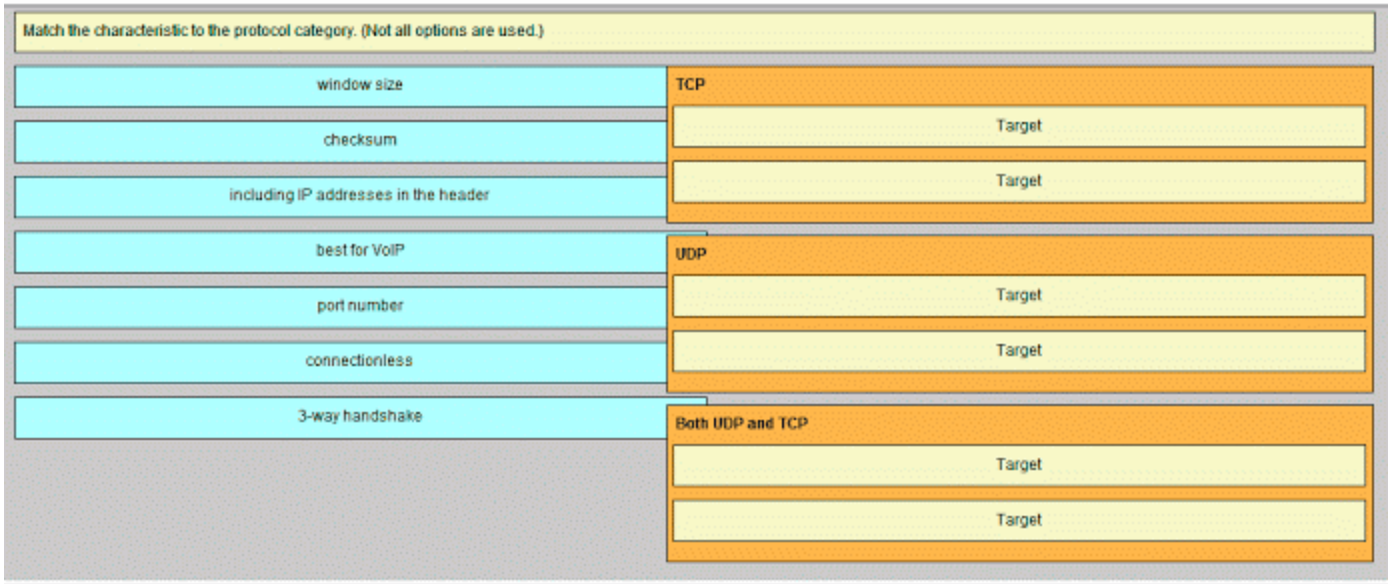
192.168.1.2 -> source IP address

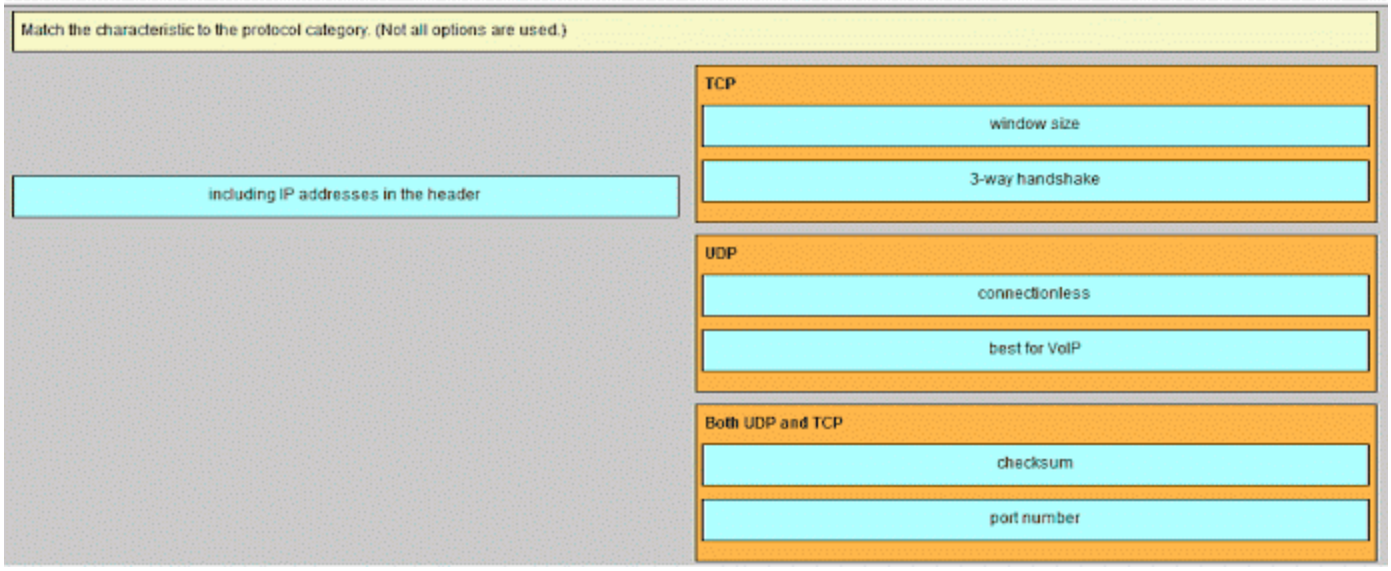
192.168.2.2 -> destination IP address

2578 -> source port number

80 -> destination port number

47. **Match the characteristic to the protocol category. (Not all options are used.)**





TCP -> window size

TCP -> 3-way handshake

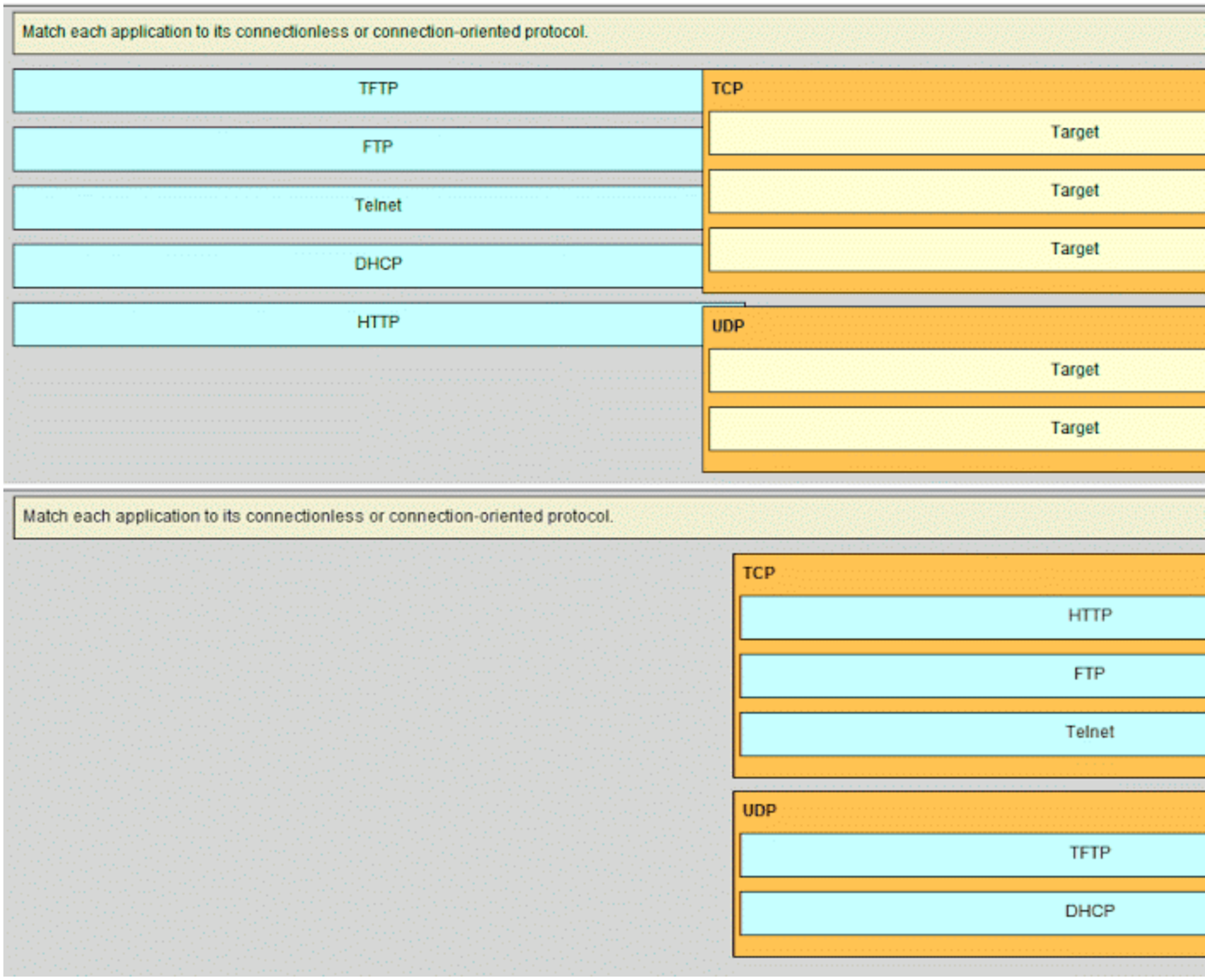
UDP -> connectionless

UDP -> best for VoIP

Both UDP and TCP -> checksum

Both UDP and TCP -> port number

48. **Match each application to its connectionless or connection-oriented protocol.**



TCP -> HTTP

TCP -> FTP

TCP -> TELNET

UDP -> TFTP

UDP -> DHCP