CCNA 1 (v5.1 + v6.0) Chapter 6 Exam Answers 2019 – 100% Full

itexamanswers.net/ccna-1-v5-1-v6-0-chapter-6-exam-answers-100-full.html

March 7, 2016

4.5 / **5** (**235** votes)
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. Which characteristic of the network layer in the OSI model allows carrying packets for multiple types of communications among many hosts?

- the de-encapsulation of headers from lower layers
- the selection of paths for and direct packets toward the destination
- **the ability to operate without regard to the data that is carried in each packet***
- the ability to manage the data transport between processes running on hosts

Explain:
The function of the network layer protocols specifies the packet structure and processing used to carry the data from one host to another host. The actual communication data is encapsulated in the network layer PDU. The feature of its operation without regard to the data carried in each packet allows the network layer to carry packets for multiple types of communications.

2. What are two characteristics of IP? (Choose two.)

- **does not require a dedicated end-to-end connection ***
- **operates independently of the network media***
- retransmits packets if errors occur
- re-assembles out of order packets into the correct order at the receiver end
- guarantees delivery of packets

Explain:
The Internet Protocol (IP) is a connectionless, best effort protocol. This means that IP requires no end-to-end connection nor does it guarantee delivery of packets. IP is also media independent, which means it operates independently of the network media carrying the packets.

3. When a connectionless protocol is in use at a lower layer of the OSI model, how is missing data detected and retransmitted if necessary?

- Connectionless acknowledgements are used to request retransmission.
- **Upper-layer connection-oriented protocols keep track of the data received and can request retransmission from the upper-level protocols on the sending host.***
- Network layer IP protocols manage the communication sessions if connection-oriented transport services are not available.
- The best-effort delivery process guarantees that all packets that are sent are received.

Explain:
When connectionless protocols are in use at a lower layer of the OSI model, upper-level protocols may need to work together on the sending and receiving hosts to account for and retransmit lost data. In some cases, this is not necessary, because for some applications a certain amount of data loss is tolerable.

4. Which field in the IPv4 header is used to prevent a packet from traversing a network endlessly?

- **Time-to-Live***
- Sequence Number
- Acknowledgment Number
- Differentiated Services

Explain:
The value of the Time-to-Live (TTL) field in the IPv4 header is used to limit the lifetime of a packet. The sending host sets the initial TTL value; which is decreased by one each time the packet is processed by a router. If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address. The Differentiated Services (DS) field is used to determine the priority of each packet. Sequence Number and Acknowledgment Number are two fields in the TCP header.

5. What IPv4 header field identifies the upper layer protocol carried in the packet?

- **Protocol***
- Identification
- Version
- Differentiated Services

Explain:
It is the Protocol field in the IP header that identifies the upper-layer protocol the packet is carrying. The Version field identifies the IP version. The Differential Services field is used for setting packet priority. The Identification field is used to reorder fragmented packets.

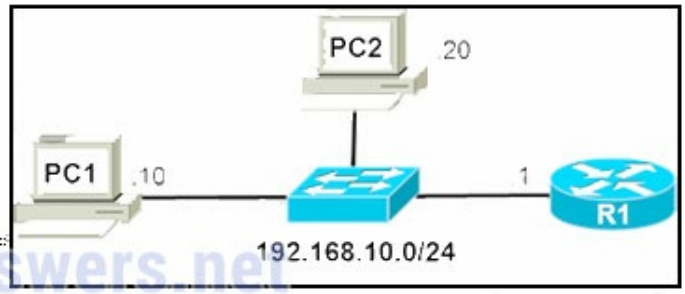
6. What is one advantage that the IPv6 simplified header offers over IPv4?

- smaller-sized header
- little requirement for processing checksums
- smaller-sized source and destination IP addresses
- **efficient packet handling***

Explain:
The IPv6 simplified header offers several advantages over IPv4:
· Better routing efficiency and efficient packet handling for performance and forwarding-rate scalability
· No requirement for processing checksums
· Simplified and more efficient extension header mechanisms (as opposed to the IPv4 Options field)
· A Flow Label field for per-flow processing with no need to open the transport inner packet to identify the various traffic flows

7. Refer to the exhibit. Which route from the PC1 routing table will be used to reach PC2?

```
C:\Users\PC1> netstat -r

<Output omitted>

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10      25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     306
    192.168.10.0    255.255.255.0         On-link    192.168.10.10     281
   192.168.10.10  255.255.255.255         On-link    192.168.10.10     281
  192.168.10.255  255.255.255.255         On-link    192.168.10.10     281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10     281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10     281
===========================================================================
```



- A. The graphic contains a table that has five columns. The column headings and values are as follows. The column one heading is Network Destination and the value is 192.168.10.0. The column two heading is Netmask and the value is 255.255.255.0. The column three heading is Gateway and the value is On-link. The column four heading is Interface and the value is 192.168.10.10. The column five heading is Metric and the value is 281.

Network Destination	Netmask	Gateway	Interface	Metric
192.168.10.0	255.255.255.0	On-link	192.168.10.10	281

- B. The graphic contains a table that has five columns. The column headings and values are as follows. The column one heading is Network Destination and the value is 192.168.10.10. The column two heading is Netmask and the value is 255.255.255.255. The column three heading is Gateway and the value is On-link. The column four heading is Interface and the value is 192.168.10.10. The column five heading is Metric and the value is 281.

Network Destination	Netmask	Gateway	Interface	Metric
192.168.10.10	255.255.255.255	On-link	192.168.10.10	281

- C. The graphic contains a table that has five columns. The column headings and values are as follows. The column one heading is Network Destination and the value is 127.0.0.1. The column two heading is Netmask and the value is 255.255.255.255. The column three heading is Gateway and the value is On-link. The column four heading is Interface and the value is 127.0.0.1. The column five heading is Metric and the value is 306.

Network Destination	Netmask	Gateway	Interface	Metric
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306

- D. The graphic contains a table that has five columns. The column headings and values are as follows. The column one heading is Network Destination and the value is 0.0.0.0. The column two heading is Netmask and the value is 0.0.0.0. The column three heading is Gateway and the value is 192.168.10.1. The column four heading is Interface and the value is 192.168.10.10. The column five heading is Metric and the value is 25.

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.10	25

Correct answer: A

Explain:
PC1 and PC2 are both on network 192.168.10.0 with mask 255.255.255.0, so there is no need to access the default gateway (entry 0.0.0.0 0.0.0.0). Entry 127.0.0.1 255.255.255.255 is the loopback interface and entry 192.168.10.10 255.255.255.255 identifies the PC1 address interface.

8. Refer to the exhibit. R1 receives a packet destined for the IP address 192.168.2.10. Out which interface will R1 forward the packet?

```
R1# show ip route
<output omitted>

 172.16.0.0/24 is subnetted, 3 subnets
D       172.16.10.0 [90/2297856] via 172.16.1.2, 00:06:49, <output omitted>
C       172.16.11.0 is directly connected, FastEthernet0/1
C       172.16.1.0 is directly connected, Serial0/0/1
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.10.1.0/24 is directly connected, FastEthernet0/1
C       10.3.3.0/24 is directly connected, FastEthernet0/0
C       10.1.0.0/16 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/2681856] via 172.16.1.2, 00:07:42, <output omitted>
                    [90/2681856] via 10.1.1.2, 00:07:42, <output omitted>
D    192.168.2.0/24 [90/2297856] via 172.16.1.2, 00:06:34, <output omitted>
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```


- FastEthernet0/0
- FastEthernet0/1
- Serial0/0/0
- **Serial0/0/1***

Explain:
If a route in the routing table points to a next hop address, the router will perform a second lookup to determine out which interface the next hop is located.

9. What type of route is indicated by the code C in an IPv4 routing table on a Cisco router?

- static route
- default route
- **directly connected route***
- dynamic route that is learned through EIGRP

Explain:
Some of the IPv4 routing table codes include the following:
C – directly connected
S – static
D – EIGRP
* – candidate default

10. What routing table entry has a next hop address associated with a destination network?

- directly-connected routes
- local routes
- **remote routes***
- C and L source routes

Explain:
Routing table entries for remote routes will have a next hop IP address. The next hop IP address is the address of the router interface of the next device to be used to reach the destination network. Directly-connected and local routes have no next hop, because they do not require going through another router to be reached.

11. Which statement describes a hardware feature of a Cisco 1941 router that has the default hardware configuration?

- It does not have an AUX port.
- It has three FastEthernet interfaces for LAN access.
- **It has two types of ports that can be used to access the console.***
- It does not require a CPU because it relies on Compact Flash to run the IOS.

Explain:
The connections in a Cisco 1941 router include two types of ports that are used for initial configuration and command-line interface management access. The two ports are the regular RJ-45 port and a new USB Type-B (mini-B USB) connector. In addition, the router has an AUX port for remote management access, and two Gigabit Ethernet interfaces for LAN access. Compact Flash can be used increase device storage, but it does not perform the functions of the CPU, which is required for operation of the device.

12. Following default settings, what is the next step in the router boot sequence after the IOS loads from flash?

- Perform the POST routine.
- **Locate and load the startup-config file from NVRAM.***
- Load the bootstrap program from ROM.
- Load the running-config file from RAM.

Explain:
There are three major steps to the router boot sequence:
Perform Power-On-Self-Test (POST)
Load the IOS from Flash or TFTP server
Load the startup configuration file from NVRAM

13. What are two types of router interfaces? (Choose two.)

- SVI

- **LAN***
- DHCP
- Telnet
- **WAN***

Explain:
Router interfaces can be grouped into two categories:
· LAN interfaces – Used for connecting cables that terminate with LAN devices, such as computers and switches. This interface can also be used to connect routers to each other.
· WAN interfaces – Used for connecting routers to external networks, usually over a larger geographical distance.

14. Which two pieces of information are in the RAM of a Cisco router during normal operation? (Choose two.)

- **Cisco IOS***
- backup IOS file
- **IP routing table***
- basic diagnostic software
- startup configuration file

Explain:
The Cisco IOS file is stored in flash memory and copied into RAM during the boot up. The IP routing table is also stored in RAM. The basic diagnostic software is stored in ROM and the startup configuration file is stored in NVRAM.

15. A router boots and enters setup mode. What is the reason for this?

- The IOS image is corrupt.
- Cisco IOS is missing from flash memory.
- **The configuration file is missing from NVRAM.***
- The POST process has detected hardware failure.

16. What is the purpose of the startup configuration file on a Cisco router?

- to facilitate the basic operation of the hardware components of a device
- **to contain the commands that are used to initially configure a router on startup***
- to contain the configuration commands that the router IOS is currently using
- to provide a limited backup version of the IOS, in case the router cannot load the full featured IOS

Explain:
The startup configuration file is stored in NVRAM and contains the commands needed to initially configure a router. It also creates the running configuration file that is stored in in RAM.

17. Which three commands are used to set up secure access to a router through a connection to the console interface? (Choose three.)

- interface fastethernet 0/0
- line vty 0 4
- **line console 0***
- enable secret cisco
- **login ***
- **password cisco ***

Explain:
The three commands needed to password protect the console port are as follows:
line console 0
password cisco
login
Theinterface fastethernet 0/0 command is commonly used to access the configuration mode used to apply specific parameters such as the IP address to the Fa0/0 port. The line vty 0 4 command is used to access the configuration mode for Telnet. The0and 4 parameters specify ports 0 through 4, or a maximum of five simultaneous Telnet connections. The enable secret command is used to apply a password used on the router to access the privileged mode.

18. Which characteristic describes an IPv6 enhancement over IPv4?

- IPv6 addresses are based on 128-bit flat addressing as opposed to IPv4 which is based on 32-bit hierarchical addressing.
- **The IPv6 header is simpler than the IPv4 header is, which improves packet handling.***
- Both IPv4 and IPv6 support authentication, but only IPv6 supports privacy capabilities.
- The IPv6 address space is four times bigger than the IPv4 address space.

Explain:
IPv6 addresses are based on 128-bit hierarchical addressing, and the IPv6 header has been simplified with fewer fields, improving packet handling. IPv6 natively supports authentication and privacy capabilities as opposed to IPv4 that needs additional features to support those. The IPv6 address space is many times bigger than IPv4 address space.

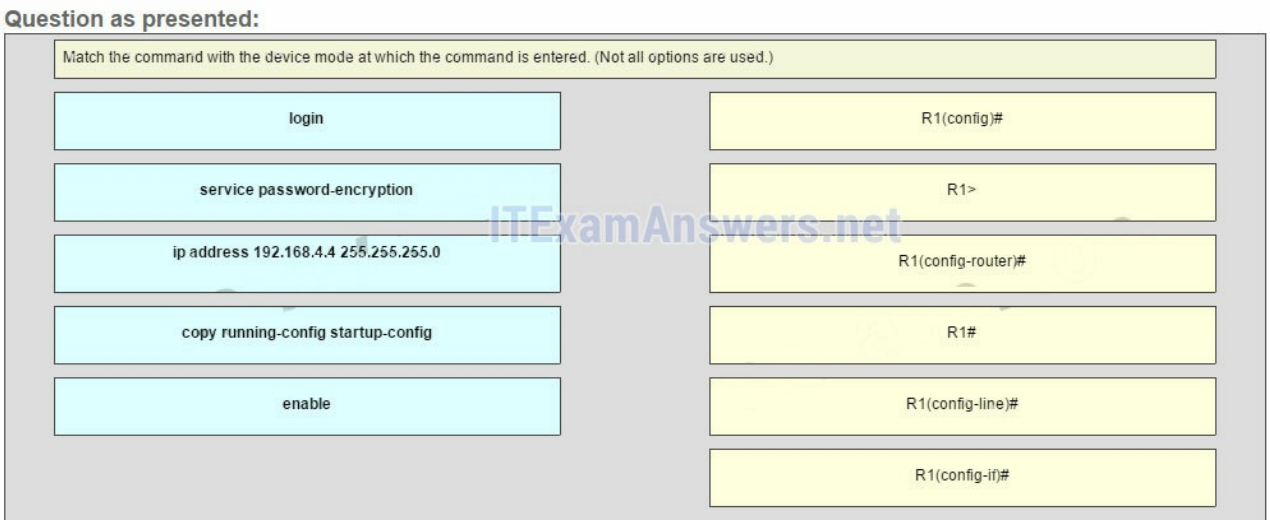
19. Open the PT Activity. The enable password on all devices is cisco.
Perform the tasks in the activity instructions and then answer the question.
For what reason is the failure occurring?

- PC1 has an incorrect default gateway configured.
- **SW1 does not have a default gateway configured.***
- The IP address of SW1 is configured in a wrong subnet.
- PC2 has an incorrect default gateway configured.

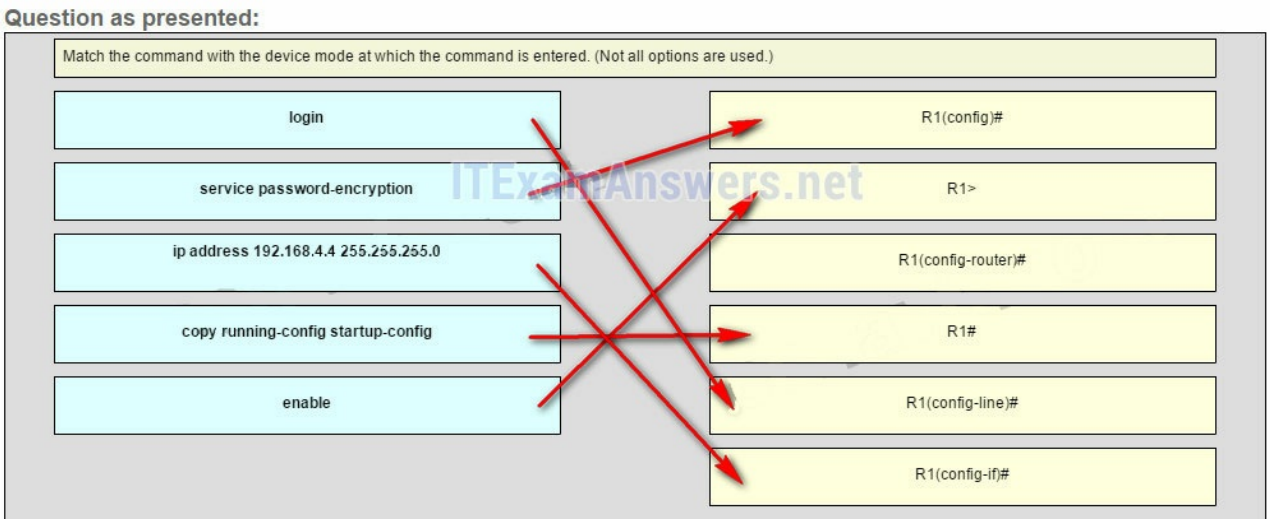
Explain:
The ip default-gateway command is missing on the SW1 configuration. Packets from PC2 are able to successfully reach SW1, but SW1 is unable to forward reply packets beyond the local network without the ip default-gateway command issued.

20. Match the command with the device mode at which the command is entered. (Not all options are used.)

Question



Answer



Explain:
The enable command is entered in R1> mode. The login command is entered in R1(config-line)# mode. The copy running-config startup-config command is entered in R1# mode. The ip address 192.168.4.4 255.255.255.0 command is entered in R1(config-if)# mode. The service password-encryption command is entered in global configuration mode.

Other Questions

21. When connectionless protocols are implemented at the lower layers of the OSI model, what are usually used to acknowledge the data receipt and request the retransmission of missing data?

- connectionless acknowledgements
- **upper-layer connection-oriented protocols***
- Network layer IP protocols
- Transport layer UDP protocols

22. Which IPv4 header field is responsible for defining the priority of the packet?

- flow label
- flags
- **differentiated services***
- traffic class

23. Why is NAT not needed in IPv6?

- Because IPv6 has integrated security, there is no need to hide the IPv6 addresses of internal networks.?
- **Any host or user can get a public IPv6 network address because the number of available IPv6 addresses is extremely large.?***
- The problems that are induced by NAT applications are solved because the IPv6 header improves packet handling by intermediate routers.?
- The end-to-end connectivity problems that are caused by NAT are solved because the number of routes increases with the number of nodes that are connected to the Internet.

24. What is a service provided by the Flow Label field of the IPv6 header?

- It limits the lifetime of a packet.
- It identifies the total length of the IPv6 packet.
- It classifies packets for traffic congestion control.
- **It informs network devices to maintain the same path for real-time application packets.***

25. How do hosts ensure that their packets are directed to the correct network destination?

- **They have to keep their own local routing table that contains a route to the loopback interface, a local network route, and a remote default route.?***
- They always direct their packets to the default gateway, which will be responsible for the packet delivery.
- They search in their own local routing table for a route to the network destination address and pass this information to the default gateway.
- They send a query packet to the default gateway asking for the best route.

26. Which two commands can be used on a Windows host to display the routing table? (Choose two.)

- netstat -s
- **route print***
- show ip route
- **netstat -r***
- tracert

27. During the process of forwarding traffic, what will the router do immediately after matching the destination IP address to a network on a directly connected routing table entry?

- discard the traffic after consulting the route table
- look up the next-hop address for the packet
- **switch the packet to the directly connected interface***
- analyze the destination IP address

28. A technician is configuring a router that is actively running on the network. Suddenly, power to the router is lost. If the technician has not saved the configuration, which two types of information will be lost? (Choose two.)

- Cisco IOS image file
- **routing table***
- bootstrap file
- **ARP cache***
- startup configuration

29. Which two interfaces will allow access via the VTY lines to configure the router? (Choose two.)

- aux interfaces
- **LAN interfaces ***
- **WAN interfaces***
- console interfaces
- USB interfaces

30. Which two files, if found, are copied into RAM as a router with the default configuration register setting boots up? (Choose two.)

- running configuration
- **IOS image file ***
- **startup configuration***
- POST diagnostics

31. When would the Cisco IOS image held in ROM be used to boot the router?

- during a file transfer operation
- during a normal boot process
- **when the full IOS cannot be found***
- when the running configuration directs the router to do this

32. After troubleshooting a router, the network administrator wants to save the router configuration so that it will be used automatically the next time that the router reboots. What command should be issued?

- copy running-config flash
- copy startup-config flash
- **copy running-config startup-config ***
- reload
- copy startup-config running-config

33. Which three commands are used to set up a password for a person who attaches a cable to a new router so that an initial configuration can be performed? (Choose three.)

- interface fastethernet 0/0
- line vty 0 4
- **line console 0***
- enable secret cisco
- **login ***
- **password cisco***

34. Which statement about router interfaces is true?

- Router LAN interfaces are not activated by default, but router WAN interfaces are.
- **Once the no shutdown command is given, a router interface is active and operational.***
- Commands that apply an IP address and subnet mask to an interface are entered in global configuration mode.
- **A configured and activated router interface must be connected to another device in order to operate.***

35. Which command displays a summary chart of all router interfaces, their IP addresses, and their current operational status?

- show ip route
- show version
- show interfaces
- **show ip interface brief***

36. A technician is manually configuring a computer with the necessary IP parameters to communicate over the corporate network. The computer already has an IP address, a subnet mask, and a DNS server. What else has to be

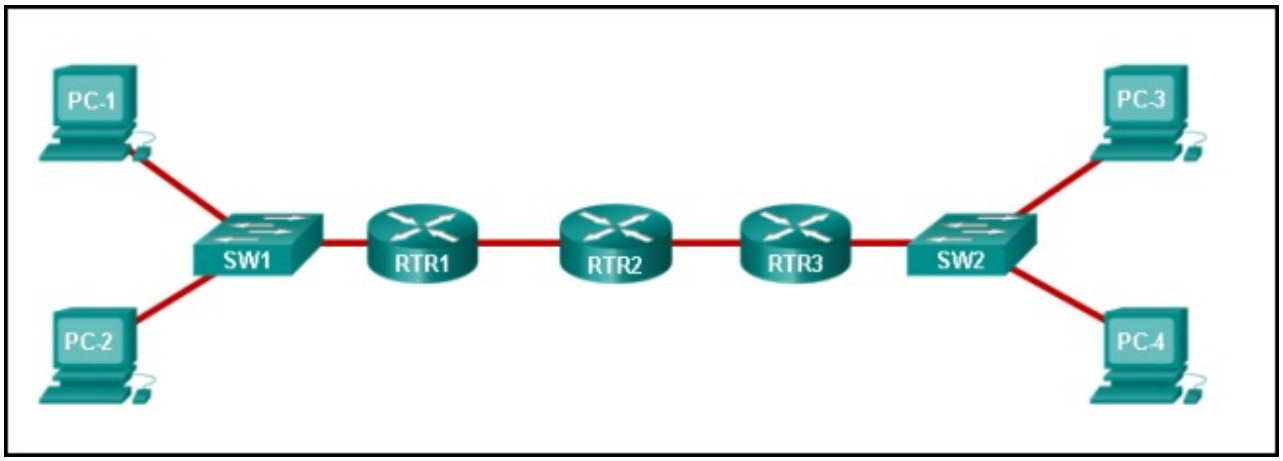
configured for Internet access?

- the WINS server address
- **the default gateway address***
- the MAC address
- the domain name of the organization

37. A computer has to send a packet to a destination host in the same LAN. How will the packet be sent?

- The packet will be sent to the default gateway first, and then, depending on the response from the gateway, it may be sent to the destination host.
- **The packet will be sent directly to the destination host.***
- The packet will first be sent to the default gateway, and then from the default gateway it will be sent directly to the destination host.
- The packet will be sent only to the default gateway.

38. Refer to the exhibit. Fill in the blank.

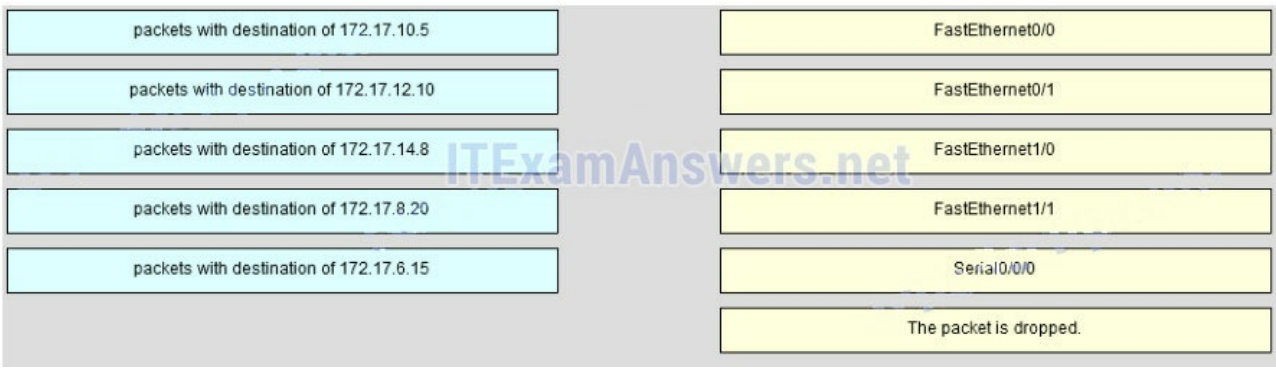


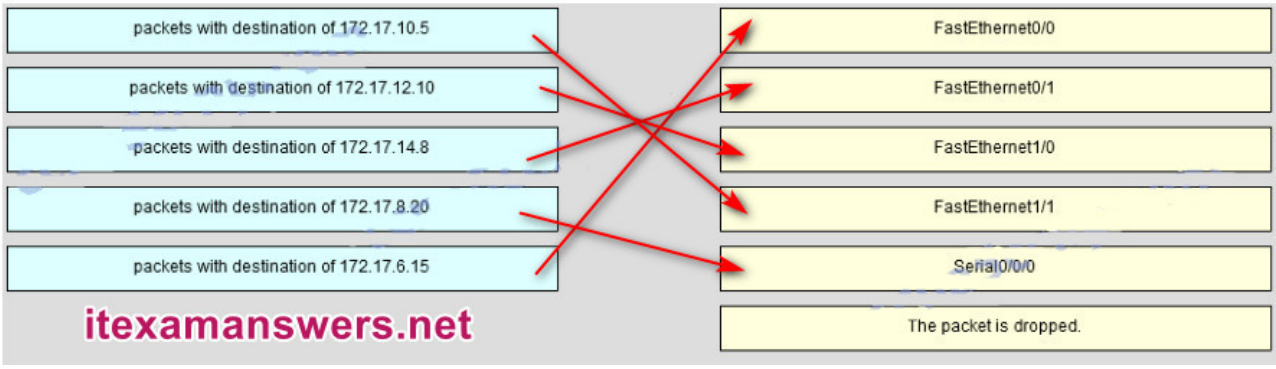
A packet leaving PC-1 has to traverse 3 hops to reach PC-4.?

39. Fill in the blank. In a router, ROM is the nonvolatile memory where the diagnostic software, the bootup instructions, and a limited IOS are stored.

40. Refer to the exhibit. Match the packets with their destination IP address to the exiting interfaces on the router. (Not all targets are used.)

```
<output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.0.0 is directly connected, Serial0/0/0
     172.17.0.0/24 is subnetted, 4 subnets
O       172.17.6.0 [110/2] via 192.168.3.4, 00:10:41, FastEthernet0/0
O       172.17.10.0 [110/2] via 192.168.5.2, 00:09:52, FastEthernet1/1
O       172.17.12.0 [110/2] via 192.168.4.2, 00:12:23, FastEthernet1/0
C       172.17.14.0 is directly connected, FastEthernet0/1
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet1/0
C    192.168.5.0/24 is directly connected, FastEthernet1/1
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

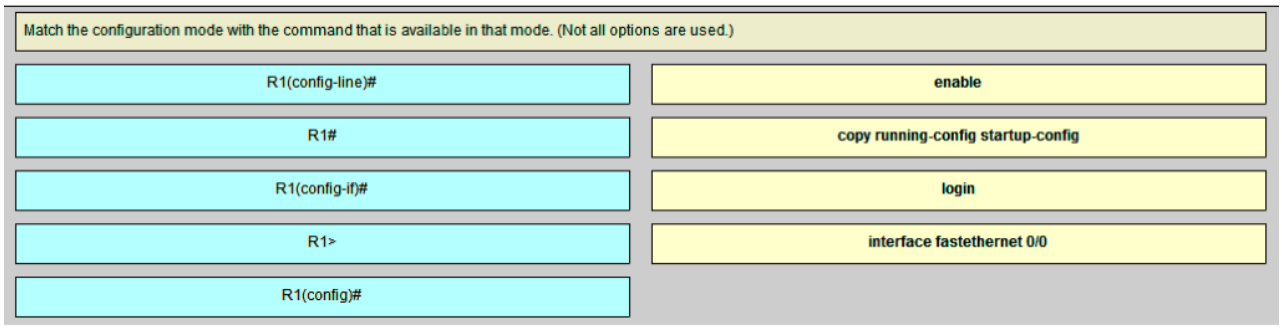


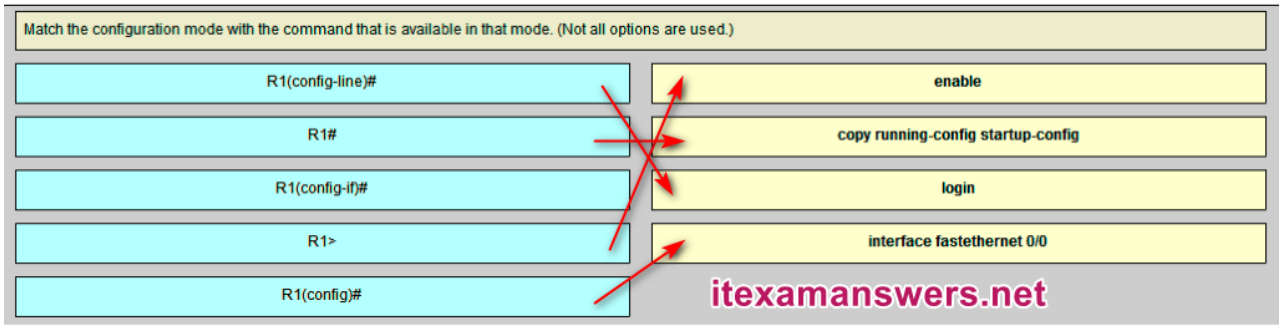


41. Open the PT Activity. Perform the tasks in the activity instructions and then answer the question or complete the task. Does the router have enough RAM and flash memory to support the new IOS?

- **The router has enough RAM and flash memory for the IOS upgrade.***
- The router has enough RAM, but needs more flash memory for the IOS upgrade.
- The router has enough flash memory, but needs more RAM for the IOS upgrade.
- The router needs more RAM and more flash memory for the IOS upgrade.

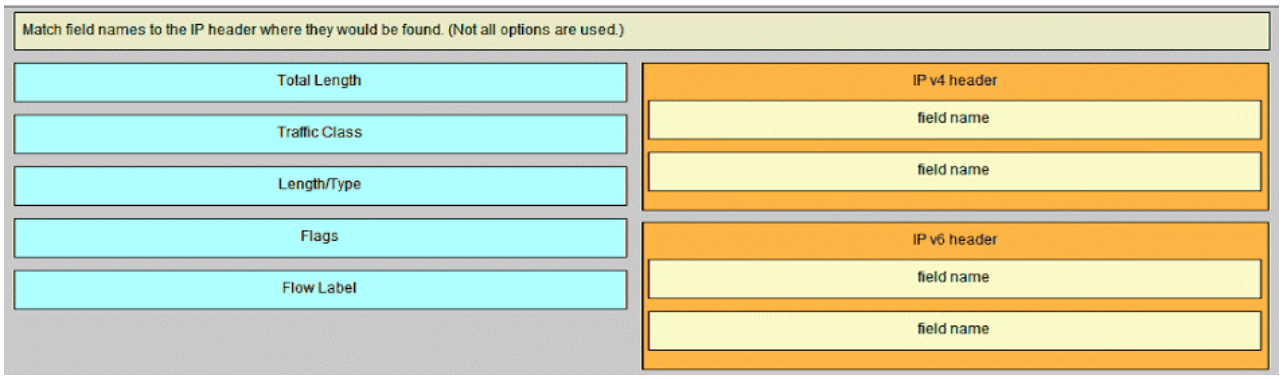
42. Match the configuration mode with the command that is available in that mode. (Not all options are used.)

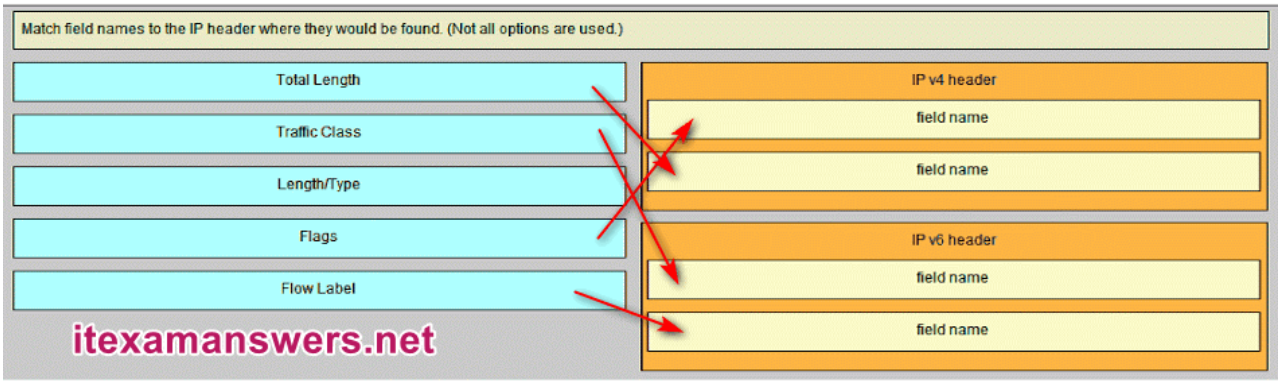




Sort elements
enable -> R1>
copy running-config startup-config -> R1#
login -> R1(config-line)#
interface fastethernet 0/0 -> R1(config)#

43. Match field names to the IP header where they would be found. (Not all options are used)





Sort elements
IP v4 Header (A) -> Flags (A)
IP v4 Header (B) -> Total Length (B)
IP v6 Header (C) ->Traffic Class (C)
IP v6 Header (D) -> Flow Label (D)

44. Which type of static route that is configured on a router uses only the exit interface?

- fully specified static route
- default static route
- **directly connected static route***
- recursive static route

Download PDF File below:

ITexamanswers.net – CCNA 1 (v5.1 + v6.0) Chapter 6 Exam Answers Full.pdf

1 file(s) 1.60 MB

Download

This content is locked!
Please support us, use one of the buttons below to unlock the content.

like
tweet
share

follow us
error
share
or wait 106s

CCNA 1 (v5.1 + v6.0) Chapter 7 Exam Answers 2019 – 100% Full

itexamanswers.net/ccna-1-v5-1-v6-0-chapter-7-exam-answers-100-full.html

March 7, 2016

4.6 / **5** (**353** votes)
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.

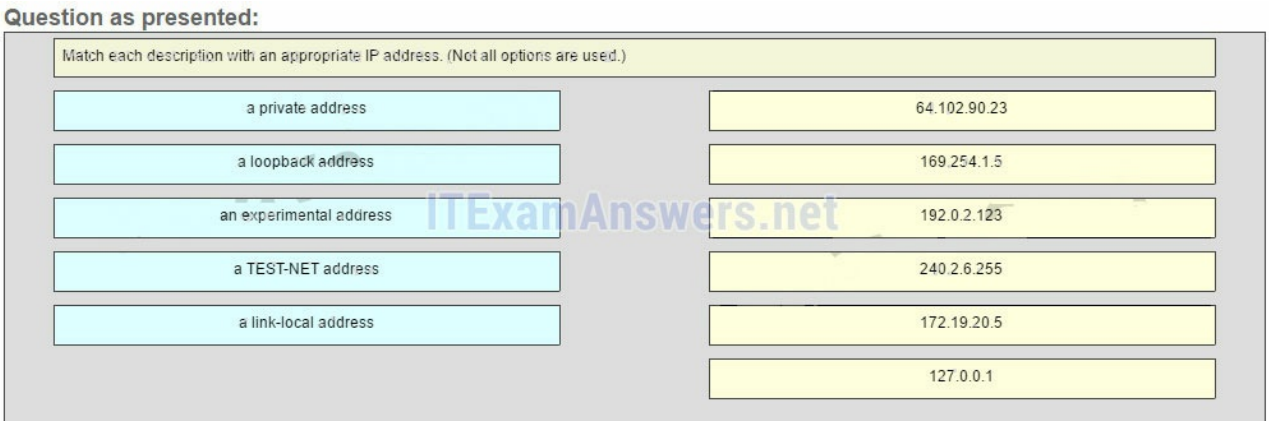
24. Fill in the blank.
The binary equivalent of the decimal number 232 is **11101000**

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.

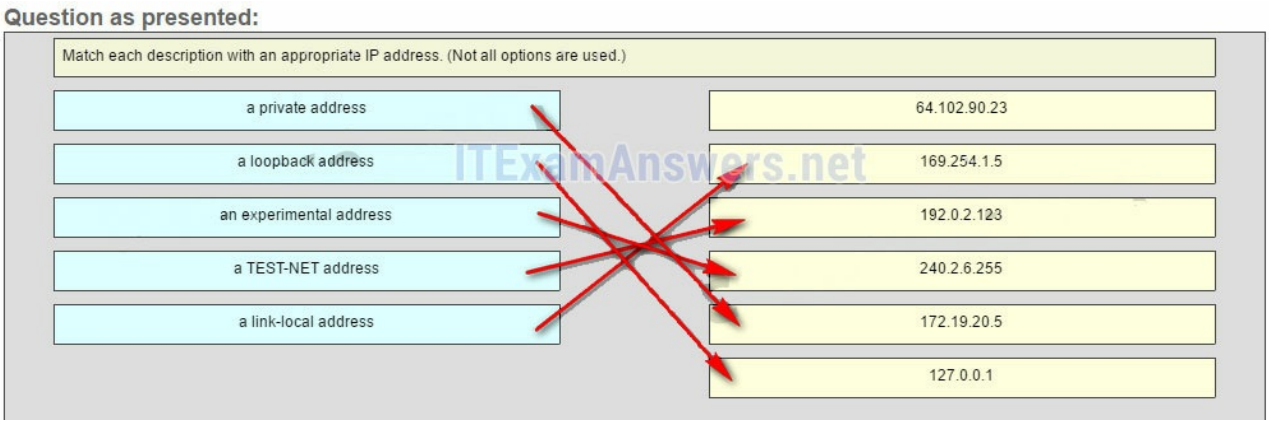
25. Fill in the blank.
What is the decimal equivalent of the hex number 0x3F? **63**

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



Answer



169.254.1.5 -> a link-local address
192.0.2.123 -> a TEST-NET address
240.2.6.255 -> an experimental address
172.19.20.5 -> a private address
127.0.0.1 -> a loopback address

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?

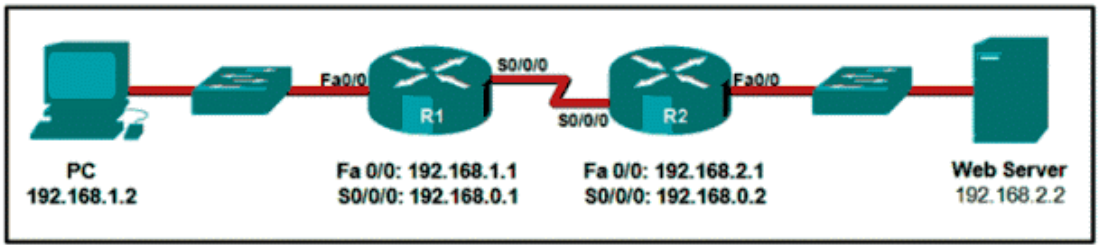
- The file is segmented and then reassembled in the correct order by TCP.
- **The file is segmented and then reassembled in the correct order at the destination, if necessary, by the upper-layer protocol.**

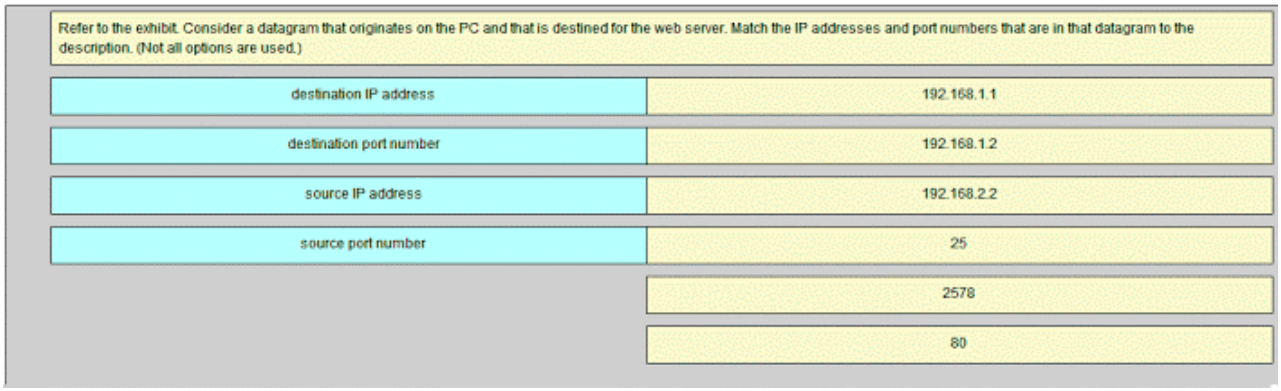
- The file is not segmented, because UDP is the transport layer protocol that is used by TFTP.
- Large files must be sent by FTP not TFTP.

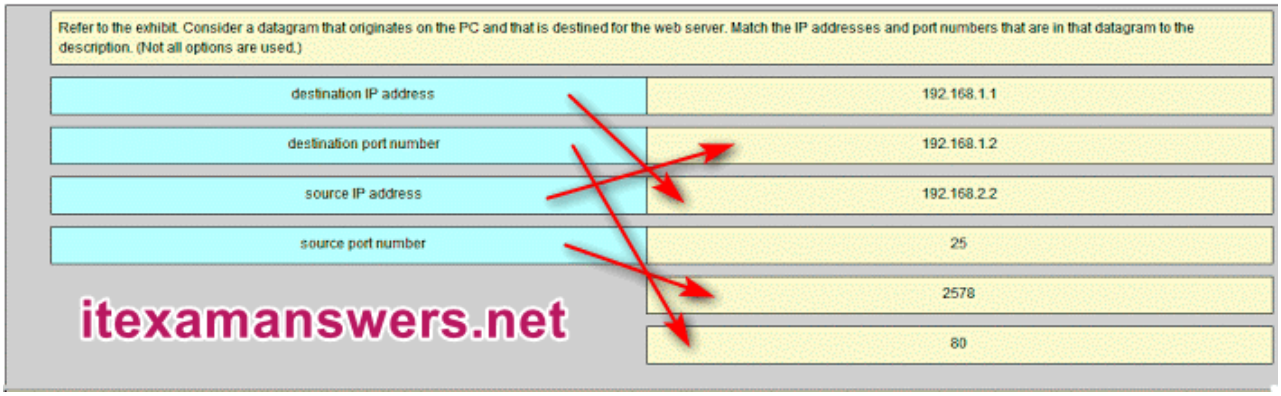
44. Fill in the blank.
During a TCP session, the **SYN** flag is used by the client to request communication with the server.

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.)



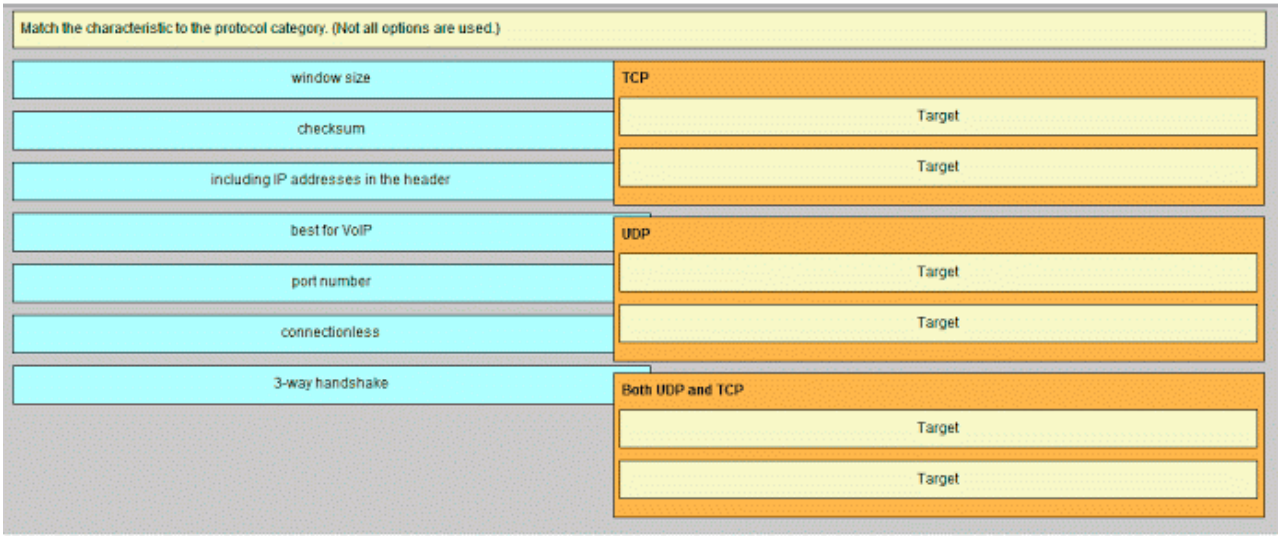


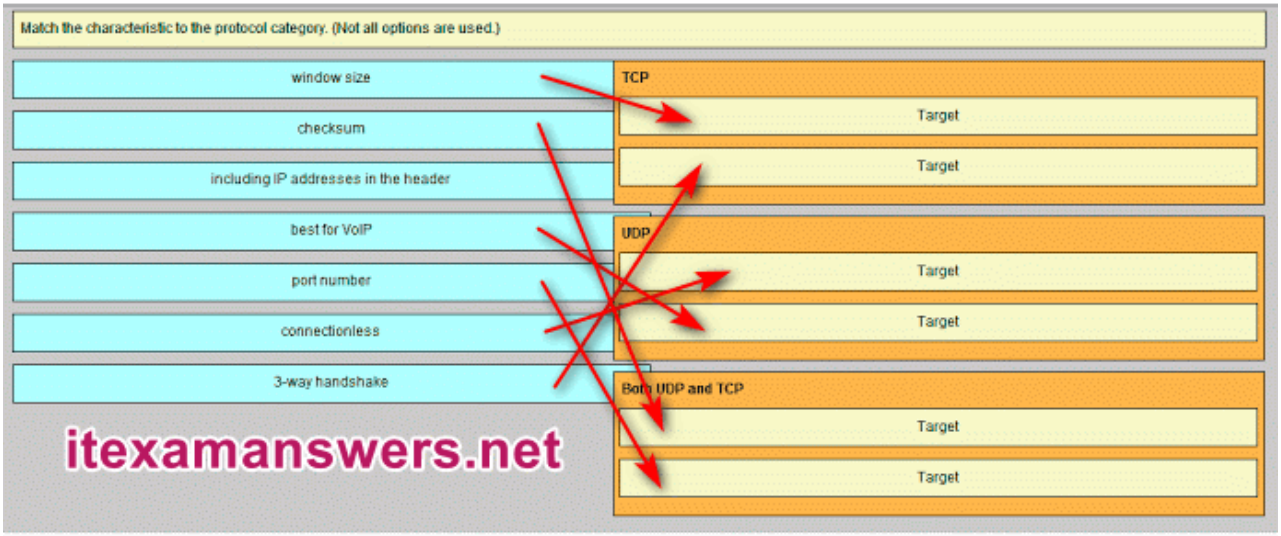


192.168.1.2 -> source IP address
192.168.2.2 -> destination IP address

2578 -> source port number
80 -> destination port number

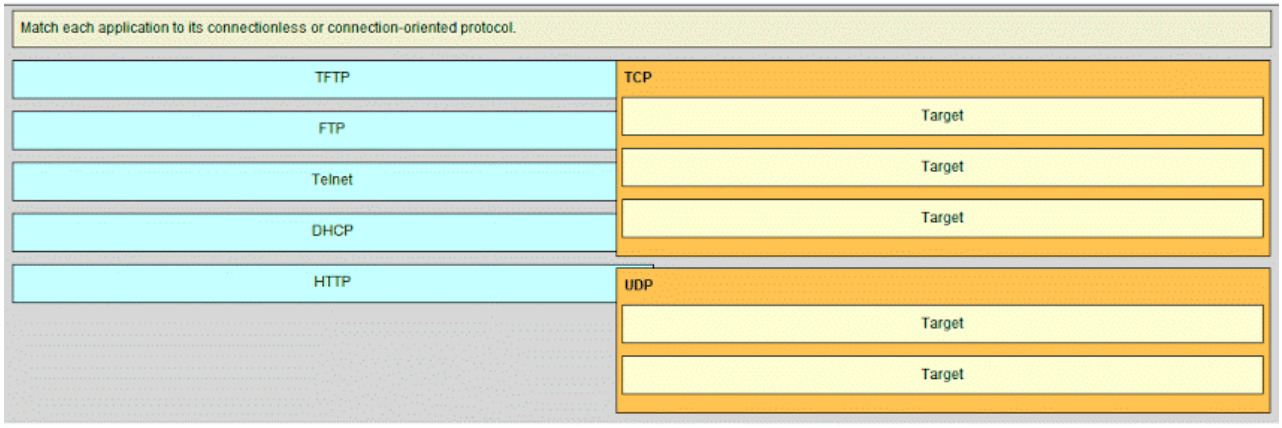
47. Match the characteristic to the protocol category. (Not all options are used.)

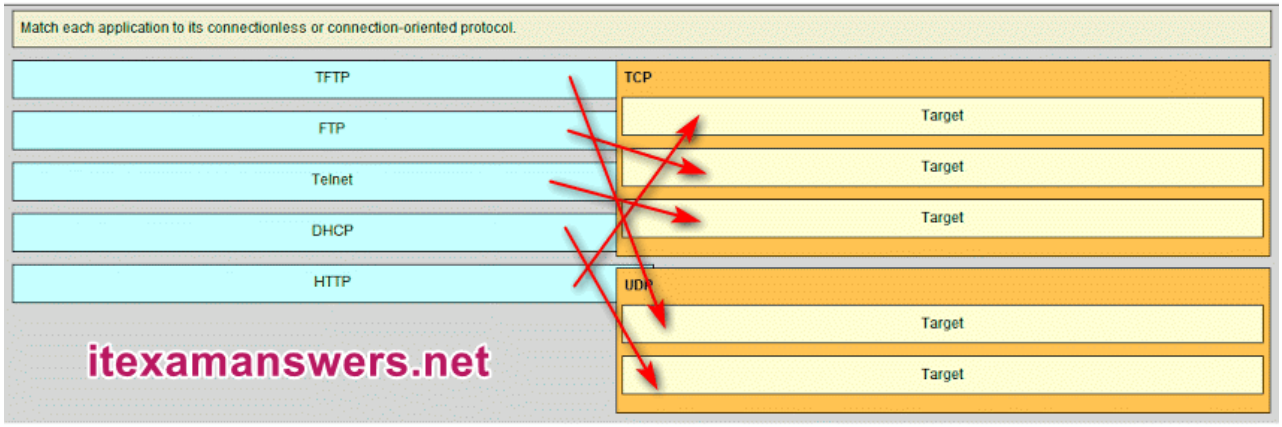




TCP -> window size
TCP -> 3-way handshake
UDP -> connectionless
UDP -> best for VoIP
Both UDP and TCP -> checksum
Both UDP and TCP -> port number

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





TCP -> HTTP
TCP -> FTP
TCP -> TELNET
UDP -> TFTP
UDP -> DHCP

Download PDF File below:

ITexamanswers.net – CCNA 1 (v5.1 + v6.0) Chapter 7 Exam Answers Full.pdf

1 file(s) 1.10 MB

Download

This content is locked!
Please support us, use one of the buttons below to unlock the content.

like
tweet
share
follow us

error
share
or wait 0s

CCNA 1 (v5.1 + v6.0) Chapter 8 Exam Answers 2019 – 100% Full

itexamanswers.net/ccna-1-v5-1-v6-0-chapter-8-exam-answers-100-full.html

March 7, 2016

4.6 / **5** (**118** votes)
How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer.

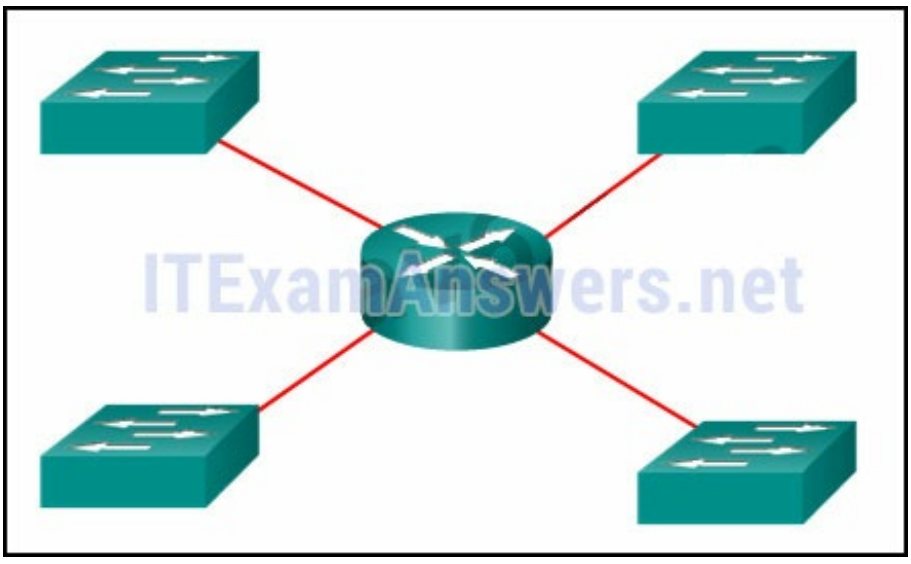
NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. What is a result of connecting two or more switches together?

- The number of broadcast domains is increased.
- **The size of the broadcast domain is increased.***
- The number of collision domains is reduced.
- The size of the collision domain is increased.

Explain:
When two or more switches are connected together, the size of the broadcast domain is increased and so is the number of collision domains. The number of broadcast domains is increased only when routers are added.

2. Refer to the exhibit. How many broadcast domains are there?



- 1
- 2
- 3
- **4***

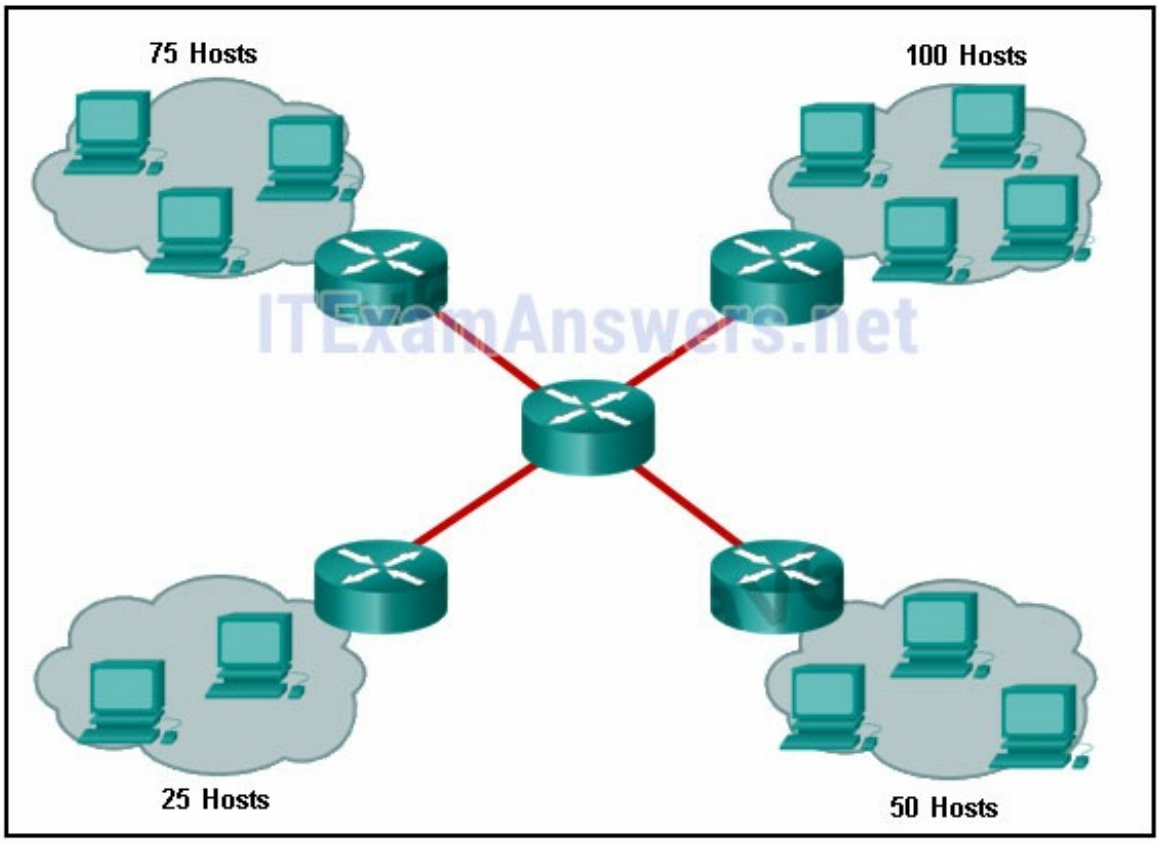
Explain:
A router is used to route traffic between different networks. Broadcast traffic is not permitted to cross the router and therefore will be contained within the respective subnets where it originated.

3. What are two reasons a network administrator might want to create subnets? (Choose two.)

- simplifies network design
- **improves network performance ***
- **easier to implement security policies***
- reduction in number of routers needed
- reduction in number of switches needed

Explain:
Two reasons for creating subnets include reduction of overall network traffic and improvement of network performance. Subnets also allow an administrator to implement subnet-based security policies. The number of routers or switches is not affected. Subnets do not simplify network design.

4. Refer to the exhibit. A company uses the address block of 128.107.0.0/16 for its network. What subnet mask would provide the maximum number of equal size subnets while providing enough host addresses for each subnet in the exhibit?

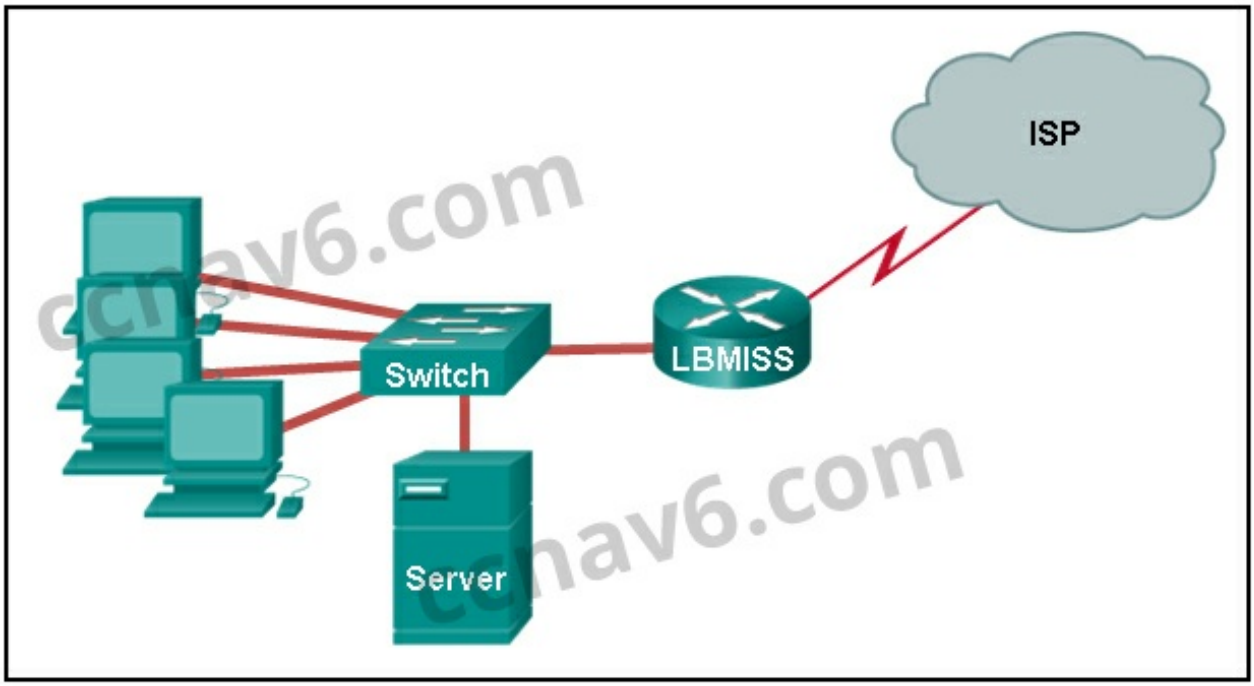


- 255.255.255.0
- **255.255.255.128***

- 255.255.255.192
- 255.255.255.224
- 255.255.255.240

Explain:
The largest subnet in the topology has 100 hosts in it so the subnet mask must have at least 7 host bits in it (27-2=126). 255.255.255.0 has 8 hosts bits, but this does not meet the requirement of providing the maximum number of subnets.

5. Refer to the exhibit. The network administrator has assigned the LAN of LBMISS an address range of 192.168.10.0. This address range has been subnetted using a /29 prefix. In order to accommodate a new building, the technician has decided to use the fifth subnet for configuring the new network (subnet zero is the first subnet). By company policies, the router interface is always assigned the first usable host address and the workgroup server is given the last usable host address. Which configuration should be entered into the properties of the workgroup server to allow connectivity to the Internet?



- IP address: 192.168.10.65 subnet mask: 255.255.255.240, default gateway: 192.168.10.76
- IP address: 192.168.10.38 subnet mask: 255.255.255.240, default gateway: 192.168.10.33
- **IP address: 192.168.10.38 subnet mask: 255.255.255.248, default gateway: 192.168.10.33***
- IP address: 192.168.10.41 subnet mask: 255.255.255.248, default gateway: 192.168.10.46
- IP address: 192.168.10.254 subnet mask: 255.255.255.0, default gateway: 192.168.10.1

Explain:
Using a /29 prefix to subnet 192.168.10.0 results in subnets that increment by 8:
192.168.10.0 (1)
192.168.10.8 (2)
192.168.10.16 (3)
192.168.10.24 (4)
192.168.10.32 (5)

6. If a network device has a mask of /28, how many IP addresses are available for hosts on this network?

- 256
- 254
- 62
- 32
- 16
- **14***

Explain:
A /28 mask is the same as 255.255.255.240. This leaves 4 host bits. With 4 host bits, 16 IP addresses are possible, but one address represents the subnet number and one address represents the broadcast address. 14 addresses can then be used to assign to network devices.

7. Which subnet mask would be used if 5 host bits are available?

- 255.255.255.0
- 255.255.255.128
- **255.255.255.224***
- 255.255.255.240

Explain:
The subnet mask of 255.255.255.0 has 8 host bits. The mask of 255.255.255.128 results in 7 host bits. The mask of 255.255.255.224 has 5 host bits. Finally, 255.255.255.240 represents 4 host bits.

8. How many host addresses are available on the network 172.16.128.0 with a subnet mask of 255.255.252.0?

- 510
- 512
- **1022***
- 1024
- 2046
- 2048

Explain:
A mask of 255.255.252.0 is equal to a prefix of /22. A /22 prefix provides 22 bits for the network portion and leaves 10 bits for the host portion. The 10 bits in the host portion will provide 1022 usable IP addresses (2^10 – 2 = 1022).

9. How many bits must be borrowed from the host portion of an address to accommodate a router with five connected networks?

- two
- **three***
- four
- five

Explain:
Each network that is directly connected to an interface on a router requires its own subnet. The formula 2n, where n is the number of bits borrowed, is used to calculate the available number of subnets when borrowing a specific number of bits.

10. A network administrator wants to have the same network mask for all networks at a particular small site. The site has the following networks and number of devices:
IP phones – 22 addresses
PCs – 20 addresses needed
Printers – 2 addresses needed
Scanners – 2 addresses needed
The network administrator has deemed that 192.168.10.0/24 is to be the network used at this site. Which single subnet mask would make the most efficient use of the available addresses to use for the four subnetworks?

- 255.255.255.0
- 255.255.255.192
- **255.255.255.224***
- 255.255.255.240
- 255.255.255.248
- 255.255.255.252

Explain:
If the same mask is to be used, then the network with the most hosts must be examined for the number of hosts, which in this case is 22 hosts. Thus, 5 host bits are needed. The /27 or 255.255.255.224 subnet mask would be appropriate to use for these networks.

11. A company has a network address of 192.168.1.64 with a subnet mask of 255.255.255.192. The company wants to create two subnetworks that would contain 10 hosts and 18 hosts respectively. Which two networks would achieve that? (Choose two.)

- 192.168.1.16/28
- **192.168.1.64/27***
- 192.168.1.128/27
- **192.168.1.96/28***
- 192.168.1.192/28

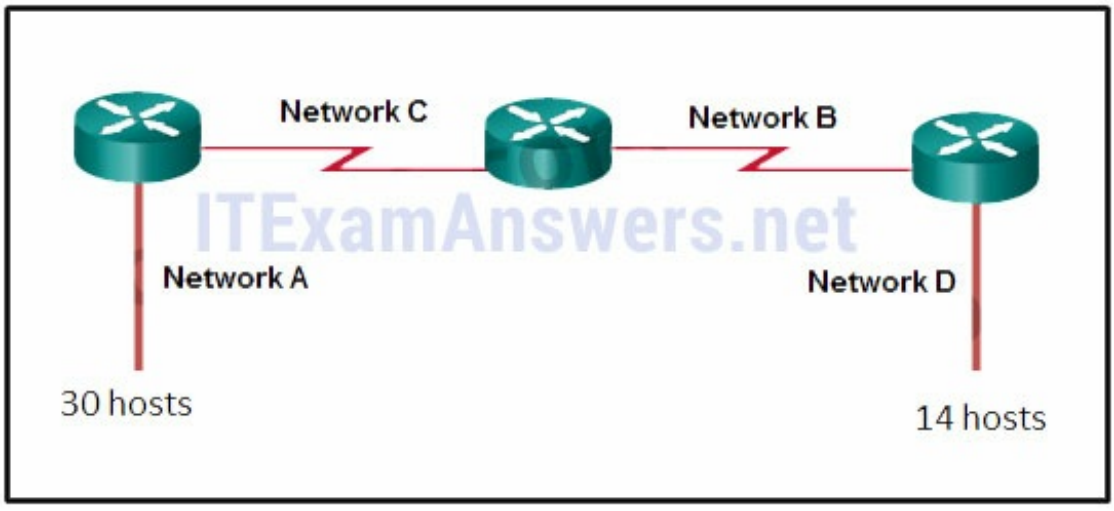
Explain:
Subnet 192.168.1.64 /27 has 5 bits that are allocated for host addresses and therefore will be able to support 32 addresses, but only 30 valid host IP addresses. Subnet 192.168.1.96/28 has 4 bits for host addresses and will be able to support 16 addresses, but only 14 valid host IP addresses

12. A network administrator is variably subnetting a network. The smallest subnet has a mask of 255.255.255.248. How many usable host addresses will this subnet provide?

- 4
- **6***
- 8
- 10
- 12

Explain:
The mask 255.255.255.248 is equivalent to the /29 prefix. This leaves 3 bits for hosts, providing a total of 6 usable IP addresses (23 = 8 – 2 = 6).

13. Refer to the exhibit. Given the network address of 192.168.5.0 and a subnet mask of 255.255.255.224, how many total host addresses are unused in the assigned subnets?

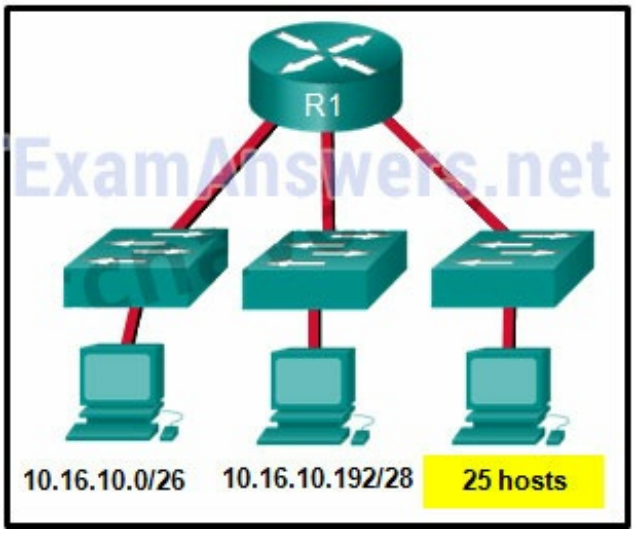


- 56
- 60
- 64
- 68

- **72***

Explain:
The network IP address 192.168.5.0 with a subnet mask of 255.255.255.224 provides 30 usable IP addresses for each subnet. Subnet A needs 30 host addresses. There are no addresses wasted. Subnet B uses 2 of the 30 available IP addresses, because it is a serial link. Consequently, it wastes 28 addresses. Likewise, subnet C wastes 28 addresses. Subnet D needs 14 addresses, so it wastes 16 addresses. The total wasted addresses are 0+28+28+16=72 addresses.

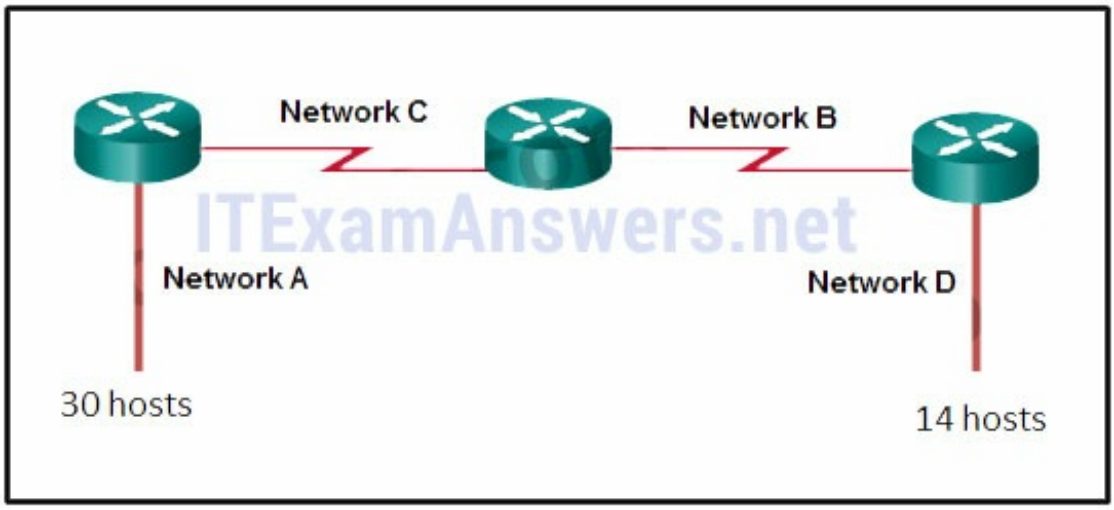
14. Refer to the exhibit. Considering the addresses already used and having to remain within the 10.16.10.0/24 network range, which subnet address could be assigned to the network containing 25 hosts?



- 10.16.10.160/26
- 10.16.10.128/28
- **10.16.10.64/27***
- 10.16.10.224/26
- 10.16.10.240/27
- 10.16.10.240/28

Explain:
Addresses 10.16.10.0 through 10.16.10.63 are taken for the leftmost network. Addresses 10.16.10.192 through 10.16.10.207 are used by the center network.The address space from 208-255 assumes a /28 mask, which does not allow enough host bits to accommodate 25 host addresses.The address ranges that are available include 10.16.10.64/26 and10.16.10.128/26. To accommodate 25 hosts, 5 host bits are needed, so a /27 mask is necessary. Four possible /27 subnets could be created from the available addresses between 10.16.10.64 and 10.16.10.191:
10.16.10.64/27
10.16.10.96/27
10.16.10.128/27
10.16.10.160/27

15. Refer to the exhibit. Given the network address of 192.168.5.0 and a subnet mask of 255.255.255.224 for all subnets, how many total host addresses are unused in the assigned subnets?



- 64
- 56
- 68
- 60
- **72***

16. A network administrator needs to monitor network traffic to and from servers in a data center. Which features of an IP addressing scheme should be applied to these devices?

- random static addresses to improve security
- addresses from different subnets for redundancy
- **predictable static IP addresses for easier identification***
- dynamic addresses to reduce the probability of duplicate addresses

Explain:
When monitoring servers, a network administrator needs to be able to quickly identify them. Using a predictable static addressing scheme for these devices makes them easier to identify. Server security, redundancy, and duplication of addresses are not features of an IP addressing scheme.

17. Which two reasons generally make DHCP the preferred method of assigning IP addresses to hosts on large networks? (Choose two.)

- **It eliminates most address configuration errors.***
- It ensures that addresses are only applied to devices that require a permanent address.
- It guarantees that every device that needs an address will get one.
- It provides an address only to devices that are authorized to be connected to the network.
- **It reduces the burden on network support staff.***

Explain:
DHCP is generally the preferred method of assigning IP addresses to hosts on large networks because it reduces the burden on network support staff and virtually eliminates entry errors. However, DHCP itself does not discriminate between authorized and unauthorized devices and will assign configuration parameters to all requesting devices. DHCP servers are usually configured to assign addresses from a subnet range, so there is no guarantee that every device that needs an address will get one.

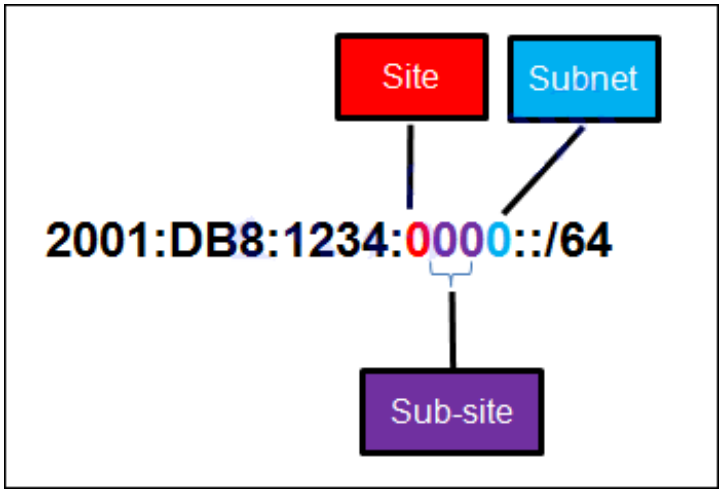
18. A DHCP server is used to assign IP addresses dynamically to the hosts on a network. The address pool is configured with 192.168.10.0/24. There are 3 printers on this network that need to use reserved static IP addresses from the pool. How many IP addresses in the pool are left to be assigned to other hosts?

- 254
- **251***
- 252
- 253

Explain:
If the block of addresses allocated to the pool is 192.168.10.0/24, there are 254 IP addresses to be assigned to hosts on the network. As there are 3 printers which need to have their addresses assigned statically, then there are 251 IP addresses left for assignment.

19. Refer to the exhibit. A company is deploying an IPv6 addressing scheme for its network. The company design document indicates that the subnet portion of the IPv6 addresses is used for the new hierarchical network design, with the site subsection to represent multiple geographical sites of the company, the sub-site section to represent multiple campuses at each site, and the subnet section to indicate each network segment separated by routers. With such a scheme, what is the maximum number of subnets achieved per sub-site?

- 0
- 4
- **16***
- 256



Explain:
Because only one hexadecimal character is used to represent the subnet, that one character can represent 16 different values 0 through F.

20. What is the prefix for the host address 2001:DB8:BC15:A:12AB::1/64?

- 2001:DB8:BC15
- **2001:DB8:BC15:A***
- 2001:DB8:BC15:A:1
- 2001:DB8:BC15:A:12

Explain:
The network portion, or prefix, of an IPv6 address is identified through the prefix length. A /64 prefix length indicates that the first 64 bits of the IPv6 address is the network portion. Hence the prefix is 2001:DB8:BC15:A.

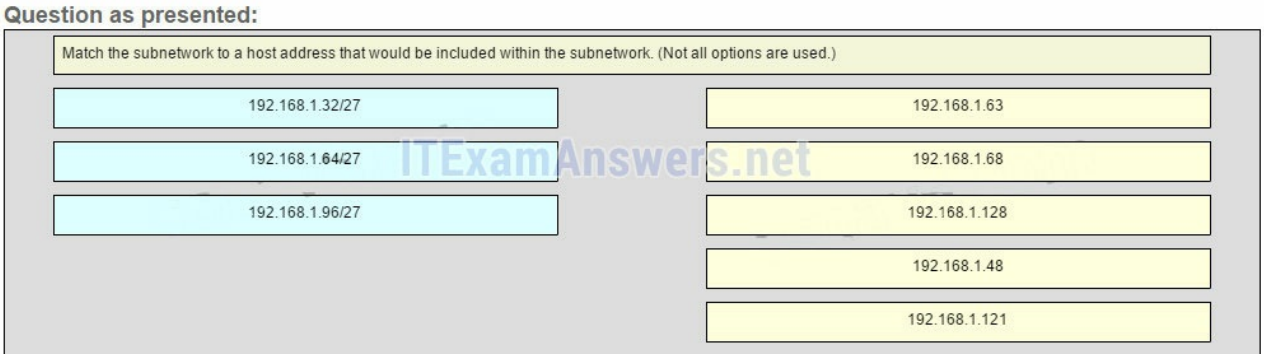
21. Consider the following range of addresses:

2001:0DB8:BC15:00A0:0000::
2001:0DB8:BC15:00A1:0000::
2001:0DB8:BC15:00A2:0000::
...
2001:0DB8:BC15:00AF:0000::

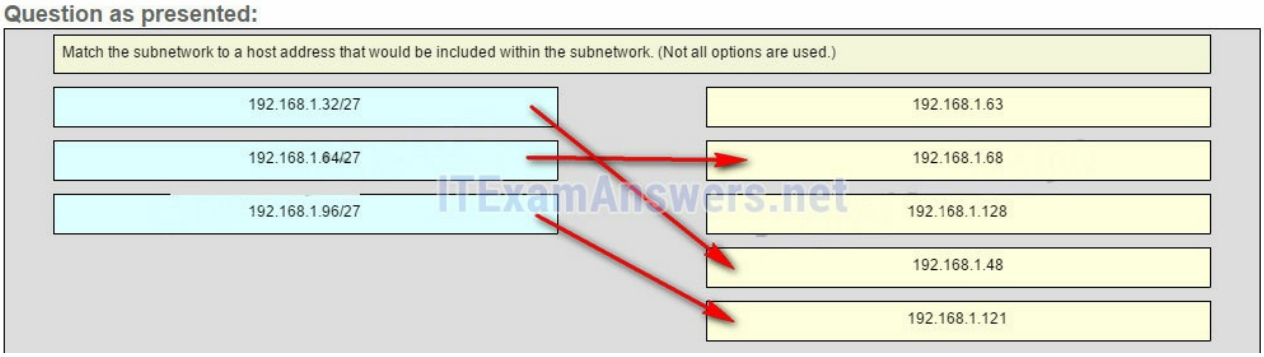
The prefix-length for the range of addresses is **/60**

Explain:
All the addresses have the part 2001:0DB8:BC15:00A in common. Each number or letter in the address represents 4 bits, so the prefix-length is /60.

22. Match the subnetwork to a host address that would be included within the subnetwork. (Not all options are used.)
Question

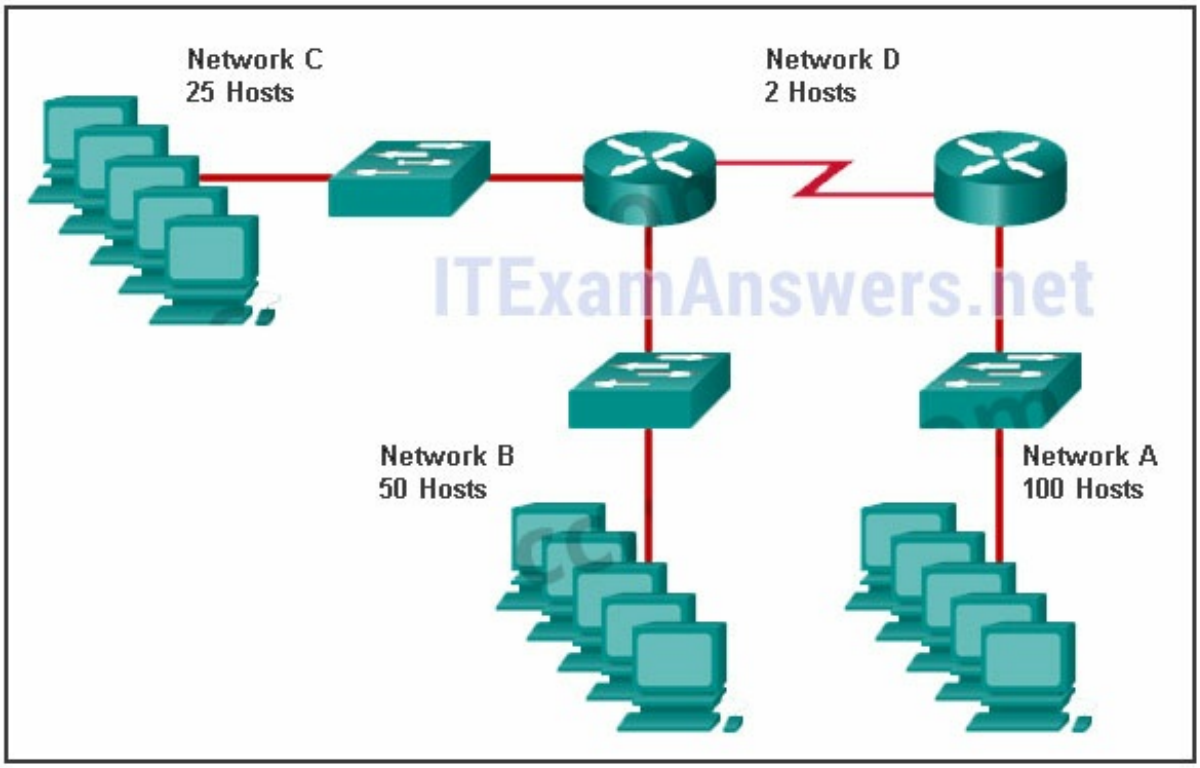


Answer



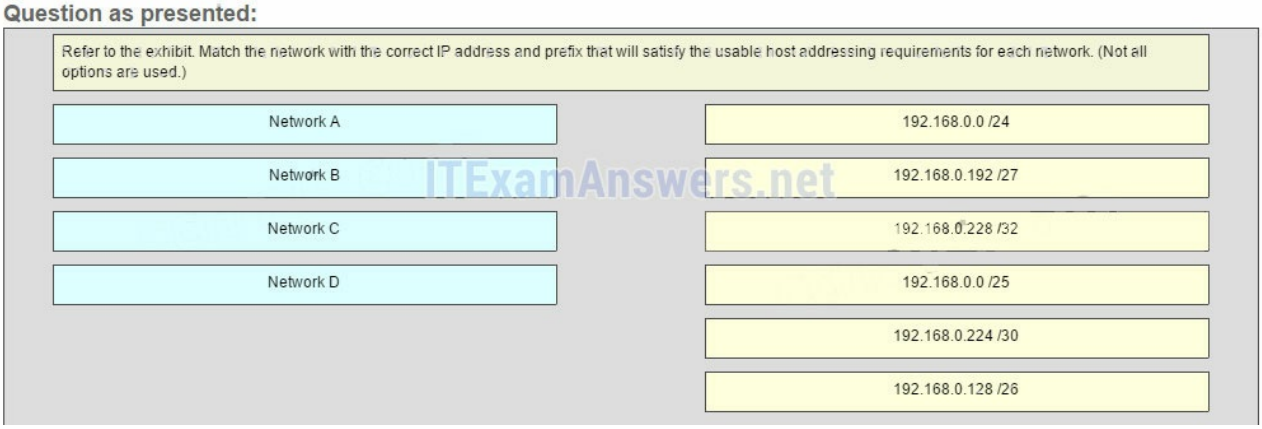
Explain:
Subnet 192.168.1.32/27 will have a valid host range from 192.168.1.33 – 192.168.1.62 with the broadcast address as 192.168.1.63
Subnet 192.168.1.64/27 will have a valid host range from 192.168.1.65 – 192.168.1.94 with the broadcast address as 192.168.1.95
Subnet 192.168.1.96/27 will have a valid host range from 192.168.1.97 – 192.168.1.126 with the broadcast address as 192.168.1.127

23. Refer to the exhibit. Match the network with the correct IP address and prefix that will satisfy the usable host addressing requirements for each network. (Not all options are used.) From right to left, network A has 100 hosts connected to the router on the right. The router on the right is connected via a serial link to the router on the left. The serial link represents network D with 2 hosts. The left router connects network B with 50 hosts and network C with 25 hosts.



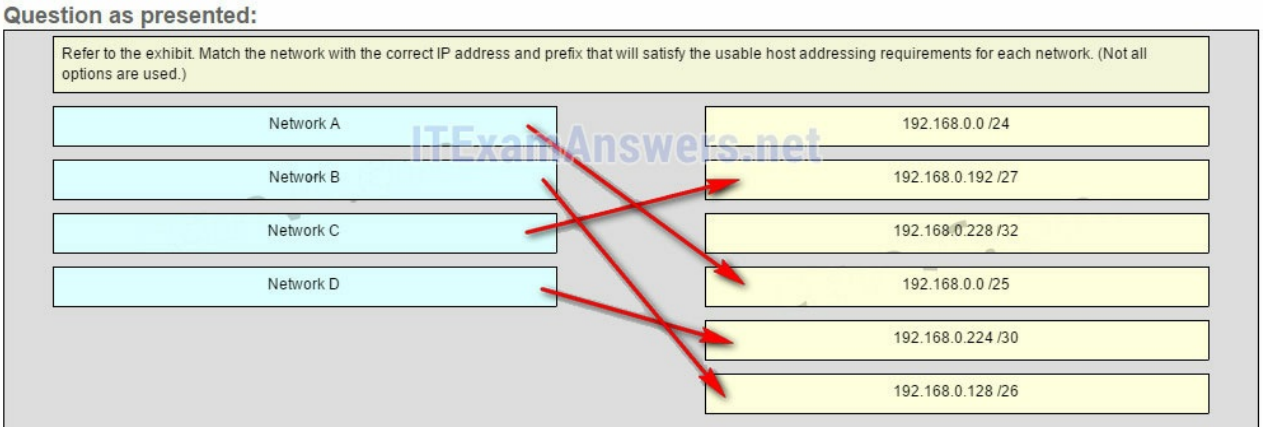
Question

Question as presented:



Answer

Question as presented:



Explain:
Network A needs to use 192.168.0.0 /25 which yields 128 host addresses.
Network B needs to use 192.168.0.128 /26 which yields 64 host addresses.
Network C needs to use 192.168.0.192 /27 which yields 32 host addresses.
Network D needs to use 192.168.0.224 /30 which yields 4 host addresses.

Older Version

24. How many bits are in an IPv4 address?

- **32***
- 64
- 128
- 256

25. Which two parts are components of an IPv4 address? (Choose two.)

- subnet portion
- **network portion***
- logical portion
- **host portion***
- physical portion
- broadcast portion

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

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

27. A message is sent to all hosts on a remote network. Which type of message is it?

- limited broadcast
- multicast
- **directed broadcast***
- unicast

28. What two statements describe characteristics of Layer 3 broadcasts? (Choose two.)

- Broadcasts are a threat and users must avoid using protocols that implement them.
- **Routers create broadcast domains. ***
- Some IPv6 protocols use broadcasts.
- There is a broadcast domain on each switch interface.
- **A limited broadcast packet has a destination IP address of 255.255.255.255.***
- A router will not forward any type of Layer 3 broadcast packet.

29. Which network migration technique encapsulates IPv6 packets inside IPv4 packets to carry them over IPv4 network infrastructures?

- encapsulation
- translation
- dual-stack
- **tunneling***

30. Which two statements are correct about IPv4 and IPv6 addresses? (Choose two.)

- **IPv6 addresses are represented by hexadecimal numbers.***
- IPv4 addresses are represented by hexadecimal numbers.
- IPv6 addresses are 32 bits in length.
- **IPv4 addresses are 32 bits in length.***
- IPv4 addresses are 128 bits in length.
- IPv6 addresses are 64 bits in length.

31. Which IPv6 address is most compressed for the full FE80:0:0:0:2AA:FF:FE9A:4CA3 address?

- FE8::2AA:FF:FE9A:4CA3?

- **FE80::2AA:FF:FE9A:4CA3***
- FE80::0:2AA:FF:FE9A:4CA3?
- FE80:::0:2AA:FF:FE9A:4CA3?

32. What are two types of IPv6 unicast addresses? (Choose two.)

- multicast
- **loopback ***
- **link-local***
- anycast
- broadcast

33. 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***

34. An IPv6 enabled device sends a data packet with the destination address of FF02::1. What is the target of this packet?

- all IPv6 DHCP servers *
- **all IPv6 enabled nodes on the local link** *
- all IPv6 configured routers on the local link *
- all IPv6 configured routers across the network *

35. When a Cisco router is being moved from an IPv4 network to a complete IPv6 environment, which series of commands would correctly enable IPv6 forwarding and interface addressing?

- Router# configure terminal
  Router(config)# interface fastethernet 0/0
  Router(config-if)# ip address 192.168.1.254 255.255.255.0
  Router(config-if)# no shutdown
  Router(config-if)# exit
  Router(config)# ipv6 unicast-routing

- **Router# configure terminal**
  Router(config)# interface fastethernet 0/0
  Router(config-if)# ipv6 address 2001:db8:bced:1::9/64
  Router(config-if)# no shutdown
  Router(config-if)# exit
  Router(config)# ipv6 unicast-routing*
- Router# configure terminal
  Router(config)# interface fastethernet 0/0
  Router(config-if)# ipv6 address 2001:db8:bced:1::9/64
  Router(config-if)# no shutdown
- Router# configure terminal
  Router(config)# interface fastethernet 0/0
  Router(config-if)# ip address 2001:db8:bced:1::9/64
  Router(config-if)# ip address 192.168.1.254 255.255.255.0
  Router(config-if)# no shutdown

36. Which two ICMP messages are used by both IPv4 and IPv6 protocols? (Choose two.)?

- router solicitation
- **route redirection***
- neighbor solicitation
- **protocol unreachable***
- router advertisement

37. When an IPv6 enabled host needs to discover the MAC address of an intended IPv6 destination, which destination address is used by the source host in the NS message?

- all-node multicast address
- **solicited-node multicast address***
- link-local address of the receiver
- global unicast address of the receiver

38. When will a router drop a traceroute 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

39. 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.***

40. 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 ***
- **whether or not the destination device is reachable through the network***
- the average time it takes each router in the path between source and destination to respond

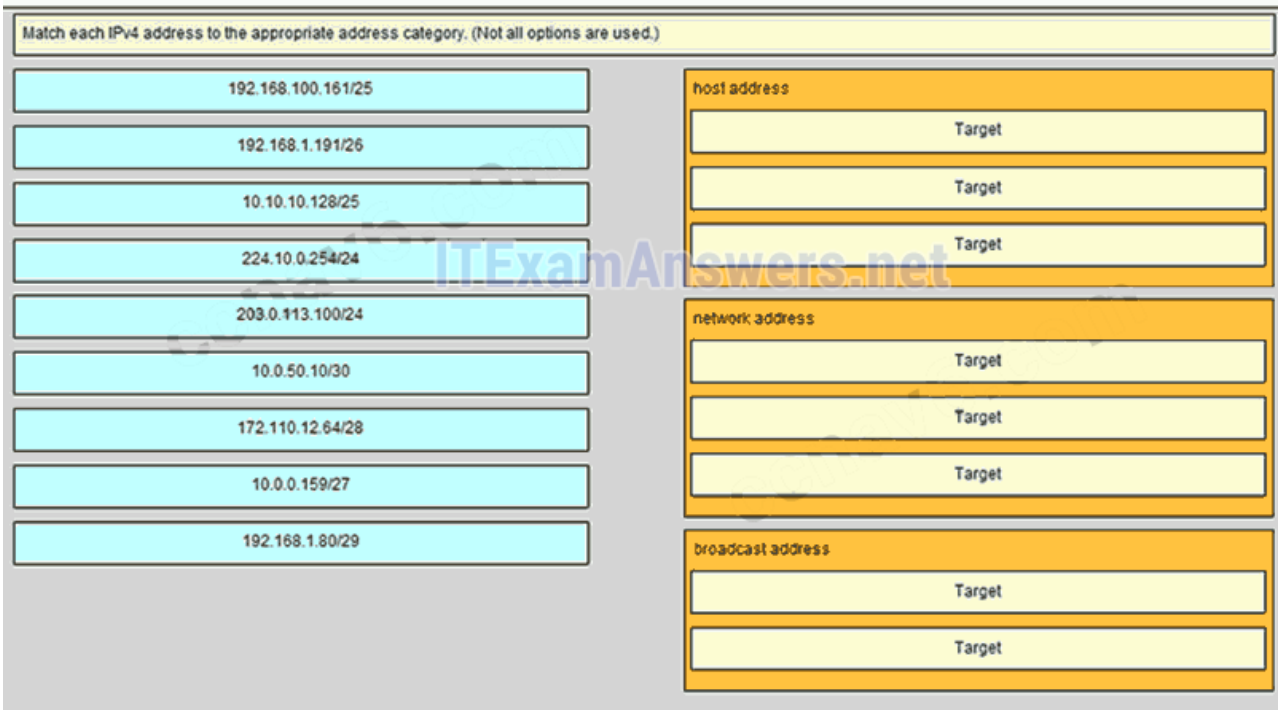
41. Fill in the blank.
The decimal equivalent of the binary number 10010101 is **149**

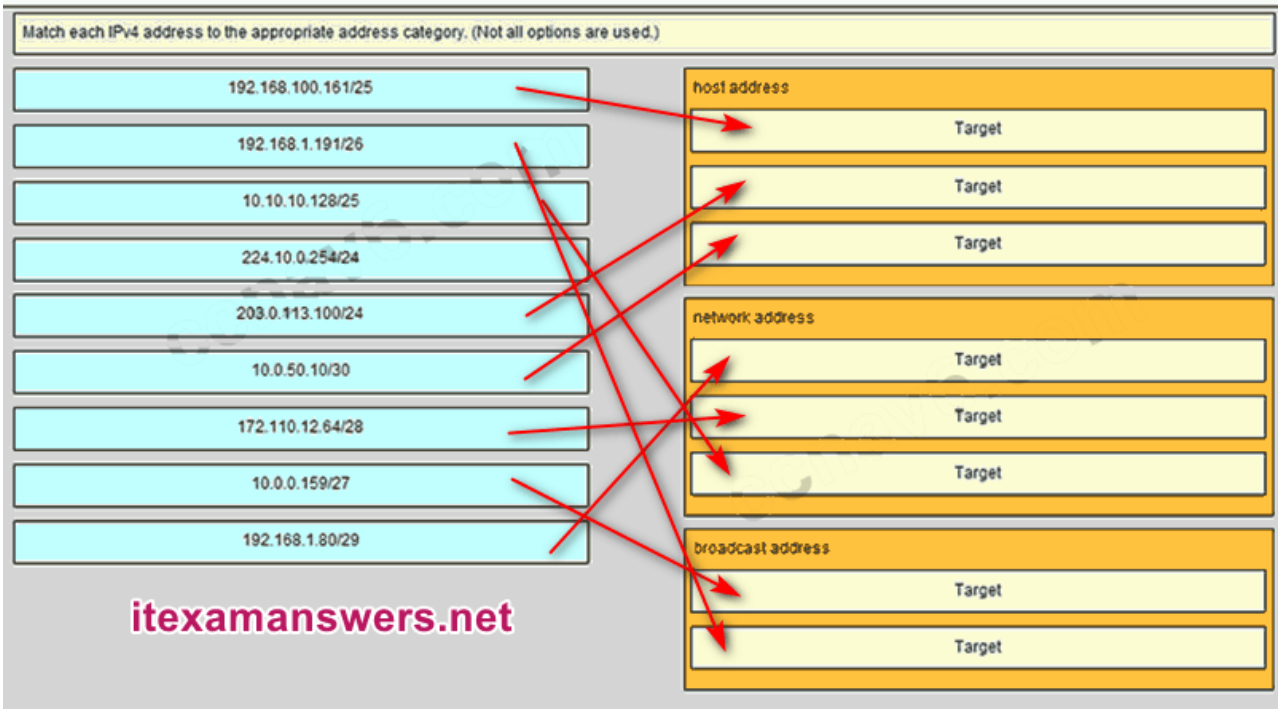
42. Fill in the blank.
What is the decimal equivalent of the hex number 0x3F? **63***

43. Open the PT Activity. Perform the tasks in the activity instructions and then answer the question. Which message is displayed on the web server?

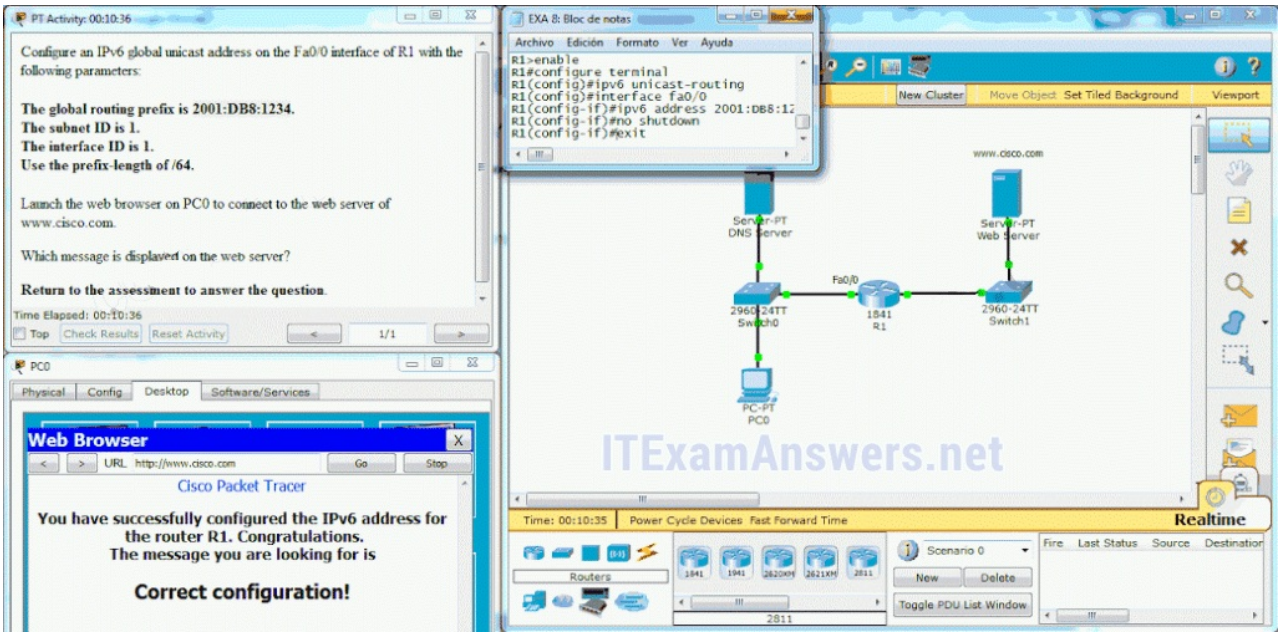
- You did it right!
- **Correct configuration!***
- IPv6 address configured!
- Successful configuration!

44. Match each IPv4 address to the appropriate address category. (Not all options are used.)

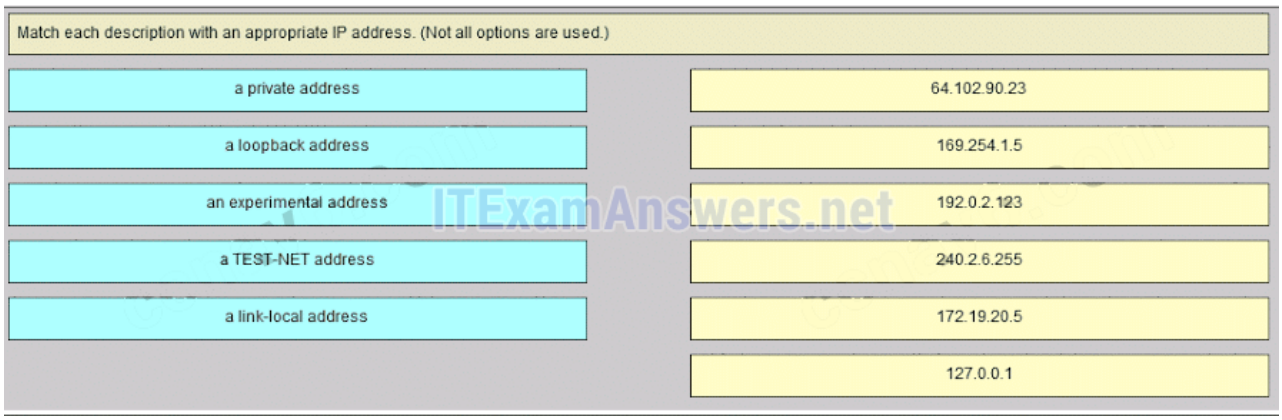


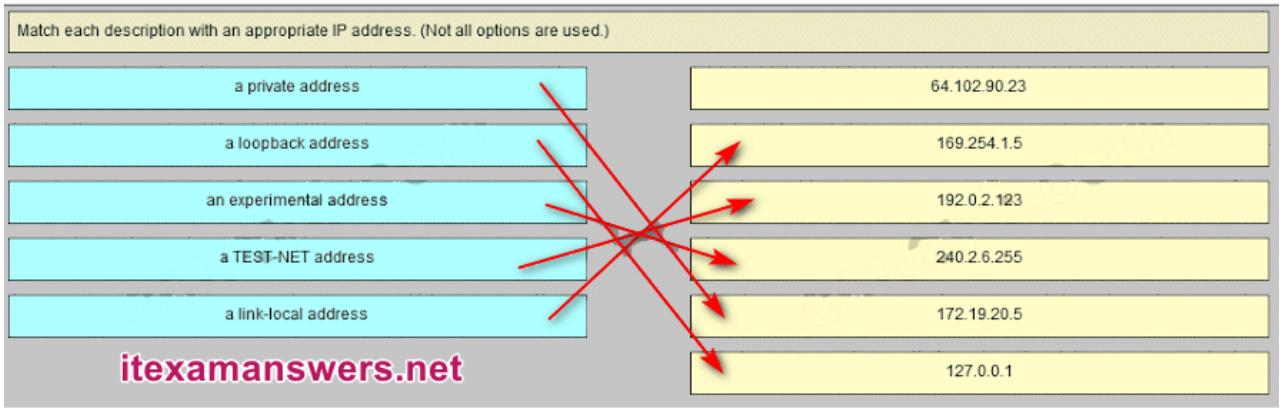


Place the options in the following order:
Host address [A] 192.168.100.161/25 [A]
Host address [B] 203.0.113.100/24 [B]
Host address [C] 10.0.50.10/30 [C]
Network address [D] 192.168.1.80/29 [D]
Network address [E] 172.110.12.64/28 [E]
Network address [F] 10.10.10.128/25 [F]
Broadcast address [G] 10.0.0.159/27 [G]
Broadcast address [H] 192.168.1.191/26 [H]



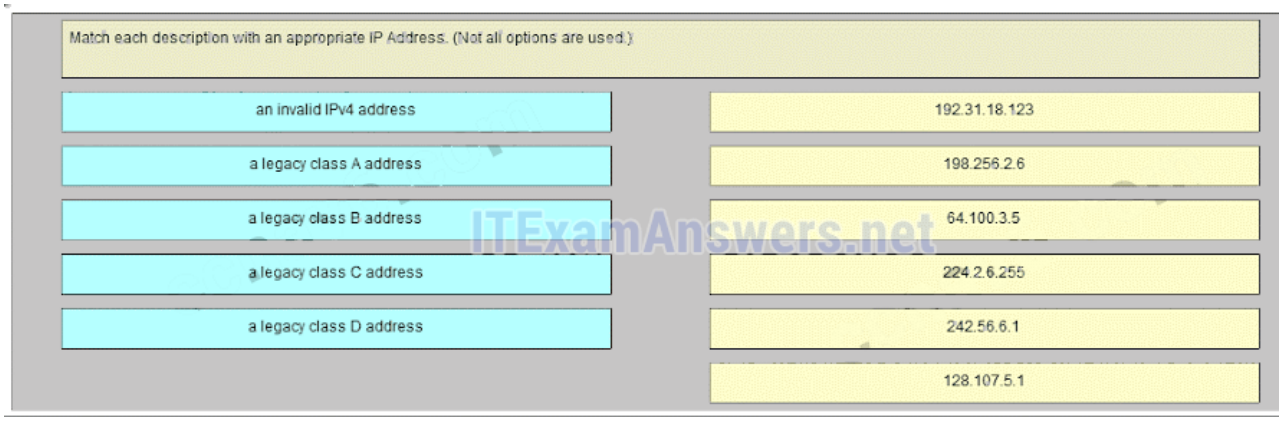
45. Match each description with an appropriate IP address. (Not all options are used)

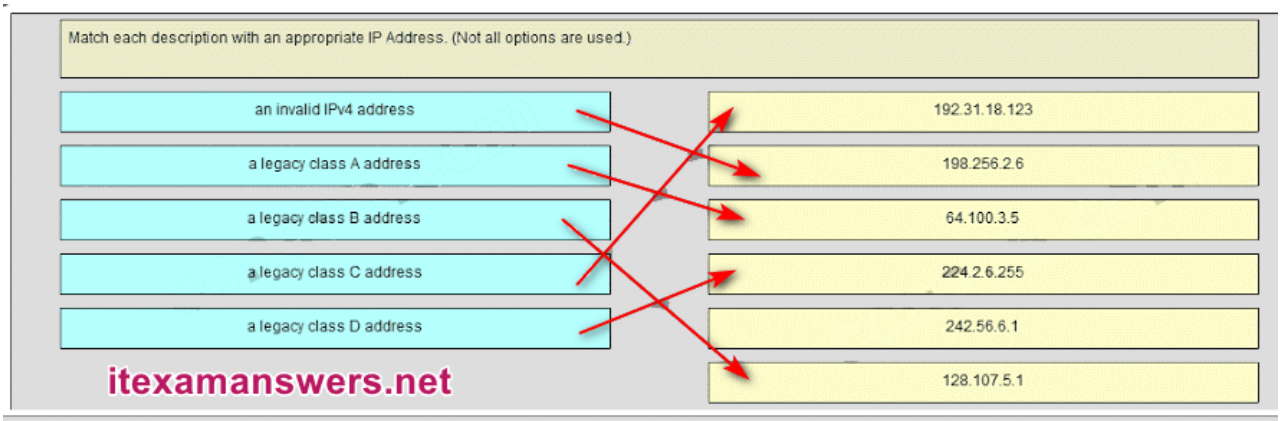




169.254.1.5 -> a link-local address
192.0.2.153 -> a TEST-NET address
240.2.6.255 -> an experimental address
172.19.20.5 -> a private address
127.0.0.1 -> a loopback address

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





192.31.18.123 -> a legacy class C address
198.256.2.6 -> an invalid IPv4 address
64.100.3.5 -> a legacy class A address
224.2.6.255 -> a legacy class D address
128.107.5.1 -> a legacy class B address

47. Which three addresses could be used as the destination address for OSPFv3 messages? (Choose three.)

- FF02::A
- FF02::1:2
- 2001:db8:cafe::1
- **FE80::1***
- **FF02::5***
- **FF02::6***

48. What is the result of connecting multiple switches to each other?

- The number of broadcast domains is increasing.
- The number of collision domains decreases.
- **The size of the broadcast domain is increasing.***
- The size of the collision domain decreases.

49. Which wildcard mask would be used to advertise the 192.168.5.96/27 network as part of an OSPF configuration?

- 255.255.255.224
- 0.0.0.32
- 255.255.255.223
- **0.0.0.31***

Download PDF File below:

ITexamanswers.net – CCNA 1 (v5.1 + v6.0) Chapter 8 Exam Answers Full.pdf

1 file(s) 1.52 MB

Download

CCNA 1 (v5.1 + v6.0) Chapter 9 Exam Answers 2019 – 100% Full

itexamanswers.net/ccna-1-v5-1-v6-0-chapter-9-exam-answers-100-full.html

March 7, 2016

4.5 / **5** (**22** votes)
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. Which two characteristics are associated with UDP sessions? (Choose two.)

- **Destination devices receive traffic with minimal delay.***
- Transmitted data segments are tracked.
- Destination devices reassemble messages and pass them to an application.
- **Received data is unacknowledged.***
- Unacknowledged data packets are retransmitted.

Explain:
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.

2. 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 FTP source host sends a query to the destination host.
- **The part of the FTP message that was lost is re-sent.***
- The entire FTP message is re-sent.

Explain:
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.

3. 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

Explain:
Multiplexing is useful for interleaving multiple communication streams. Window size is used to slow down the rate of data communication. Port numbers are used to pass data streams to their proper applications. Acknowledgments are used to notify a sending device that a stream of data packets has or has not been received.

4. What kind of port must be requested from IANA in order to be used with a specific application?

- **registered port***
- private port
- dynamic port
- source port

Explain:
Registered ports (numbers 1024 to 49151) are assigned by IANA to a requesting entity to use with specific processes or applications. These processes are primarily individual applications that a user has chosen to install, rather than common applications that would receive a well-known port number. For example, Cisco has registered port 1985 for its Hot Standby Routing Protocol (HSRP) process.

5. What type of information is included in the transport header?

- destination and source logical addresses
- destination and source physical addresses
- **destination and source port numbers***
- encoded application data

Explain:
In a segment, the transport layer header will include the source and destination process, or port numbers. Destination and source physical addressing is included in the frame header. Destination and source logical addressing is included in the network header. Application data is encoded in the upper layers of the protocol stack.

6. 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

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

7. What is the complete range of TCP and UDP well-known ports?

- 0 to 255
- **0 to 1023***
- 256 – 1023
- 1024 – 49151

Explain:
There are three ranges of TCP and UDP ports. The well-know range of port numbers is from 0 – 1023.

8. Which flag in the TCP header is used in response to a received FIN in order to terminate connectivity between two network devices?

- FIN
- **ACK***
- SYN
- RST

Explain:
In a TCP session, when a device has no more data to send, it will send a segment with the FIN flag set. The connected device that receives the segment will respond with an ACK to acknowledge that segment. The device that sent the ACK will then send a FIN message to close the connection it has with the other device. The sending of the FIN should be followed with the receipt of an ACK from the other device.

9. What is a characteristic of a TCP server process?

- Every application process running on the server has to be configured to use a dynamic port number.
- **There can be many ports open simultaneously on a server, one for each active server application.***
- An individual server can have two services assigned to the same port number within the same transport layer services.

- A host running two different applications can have both configured to use the same server port.

Explain:
Each application process running on the server is configured to use a port number, either by default or manually, by a system administrator. An individual server cannot have two services assigned to the same port number within the same transport layer services. A host running a web server application and a file transfer application cannot have both configured to use the same server port. There can be many ports open simultaneously on a server, one for each active server application.

10. 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

Explain:
TCP uses the SYN and ACK flags in order to establish connectivity between two network devices.

11. 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

Explain:
With a window of 1000 bytes, the destination host accepts segments until all 1000 bytes of data have been received. Then the destination host sends an acknowledgment.

12. 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

Explain:
Window is the number of bytes that the sender will send prior to expecting an acknowledgement from the destination device. The initial window is agreed upon during the session startup via the three-way handshake between source and destination. It is determined by how much data the destination device of a TCP session is able to accept and process at one time.

13. 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

14. What information is used by TCP to reassemble and reorder received segments?

- port numbers
- **sequence numbers***
- acknowledgment numbers
- fragment numbers

Explain:
At the transport layer, TCP uses the sequence numbers in the header of each TCP segment to reassemble the segments into the correct order.

15. What does TCP do if the sending source detects network congestion on the path to the destination?

- The source host will send a request for more frequent acknowledgments to the destination.
- **The source will decrease the amount of data that it sends before it must receive acknowledgements from the destination.***
- The destination will request retransmission of the entire message.
- The source will acknowledge the last segment that is sent and include a request for a smaller window size in the message.

Explain:
If the source determines that TCP segments are either not being acknowledged or not acknowledged in a timely manner, then it can reduce the number of bytes it sends before receiving an acknowledgment. Notice that it is the source that is reducing the number of unacknowledged bytes it sends. This does not involve changing the window size in the segment header.

16. What is a characteristic of UDP?

- UDP datagrams take the same path and arrive in the correct order at the destination.
- Applications that use UDP are always considered unreliable.
- **UDP reassembles the received datagrams in the order they were received.***
- UDP only passes data to the network when the destination is ready to receive the data.

Explain:
UDP has no way to reorder the datagrams into their transmission order, so UDP simply reassembles the data in the order it was received and forwards it to the application.

17. 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.

Explain:
When a client has UDP datagrams to send, it just sends the datagrams.

18. 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.

Explain:
The TFTP protocol uses UDP for queries, so the TFTP application must implement the reliability, if needed.

19. A host device is receiving live streaming video. How does the device account for video data that is lost during transmission?

- The device will immediately request a retransmission of the missing data.
- The device will use sequence numbers to pause the video stream until the correct data arrives.
- The device will delay the streaming video until the entire video stream is received.
- **The device will continue receiving the streaming video, but there may be a momentary disruption.***

Explain:
When TCP is used as the transport protocol, data must be received in a specific sequence or all data must be fully received in order for it to be used. TCP will use sequence numbers, acknowledgments and retransmission to accomplish this. However, when UDP

is used as the transport protocol, data that arrives out of order or with missing segments may cause a momentary disruption, but the destination device may still be able to use the data that it has received. This technology results in the least amount of network delay by providing minimal reliability. Since live streaming video applications use UDP as the transport protocol, the receiver will continue showing the video although there may be a slight delay or reduction in quality.

20. Why does HTTP use TCP as the transport layer protocol?

- to ensure the fastest possible download speed
- because HTTP is a best-effort protocol
- because transmission errors can be tolerated easily
- **because HTTP requires reliable delivery***

Explain:
When a host requests a web page, transmission reliability and completeness must be guaranteed. Therefore, HTTP uses TCP as its transport layer protocol.

21. When is UDP preferred to TCP?

- when a client sends a segment to a server
- when all the data must be fully received before any part of it is considered useful
- **when an application can tolerate some loss of data during transmission***
- when segments must arrive in a very specific sequence to be processed successfully

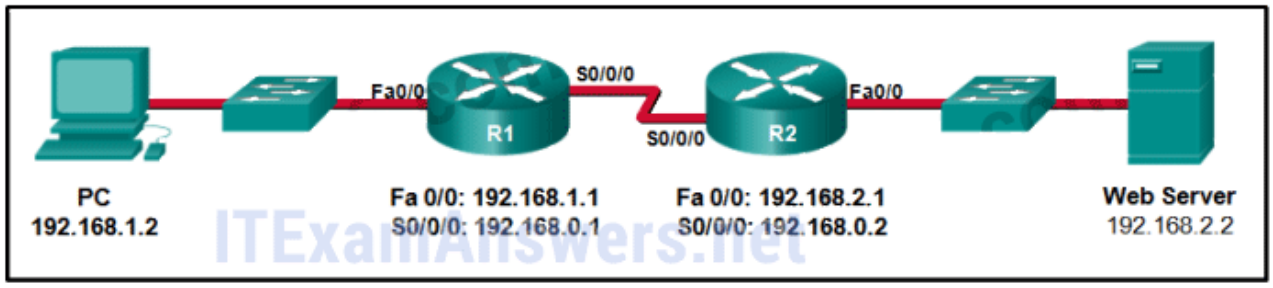
Explain:
UDP can be used when an application can tolerate some data loss. UDP is the preferred protocol for applications that provide voice or video that cannot tolerate delay.

22. Which three application layer protocols use TCP? (Choose three.)

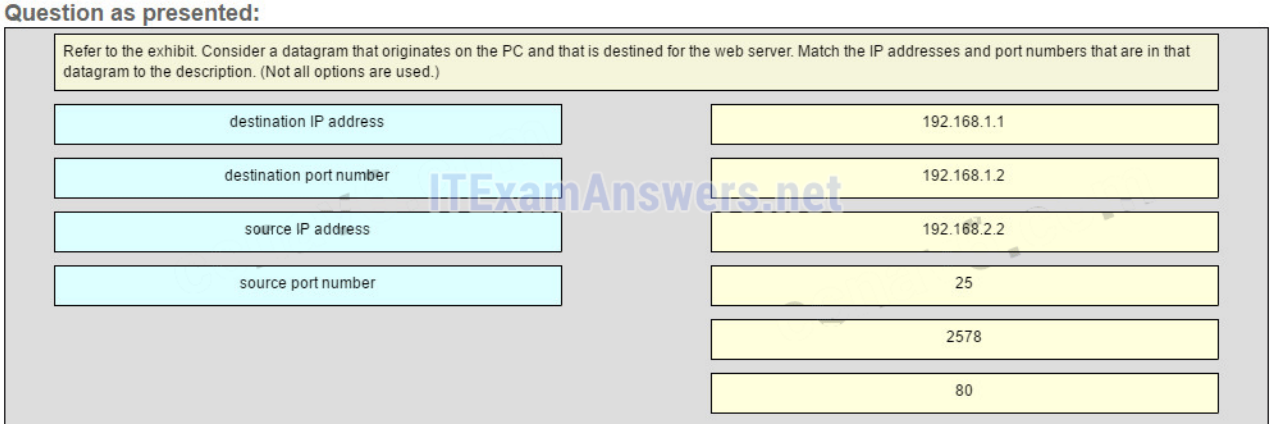
- **SMTP***
- **FTP***
- SNMP
- **HTTP***
- TFTP
- DHCP

Explain:
Some protocols require the reliable data transport that is provided by TCP. In addition, these protocols do not have real time communication requirements and can tolerate some data loss while minimizing protocol overhead. Examples of these protocols are SMTP, FTP, and HTTP.

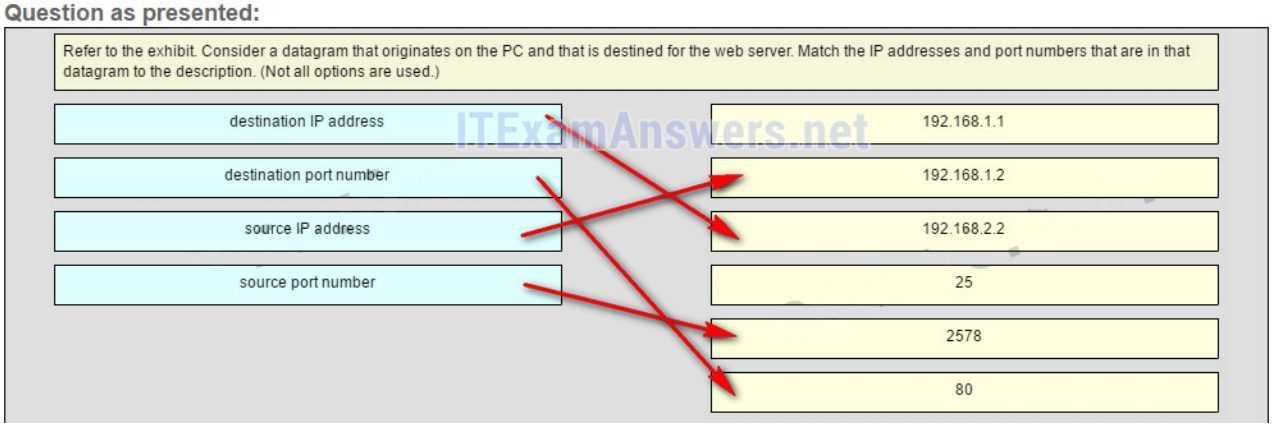
23. Refer to the exhibit. Consider a datagram that originates on the PC and that is destined for the web server. Match the IP addresses and port numbers that are in that datagram to the description. (Not all options are used.)



Question as presented:



Question as presented:



destination IP address -> 192.168.2.2
destination port number -> 80
source IP address -> 192.168.1.2
source port number -> 2578

Explain:
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

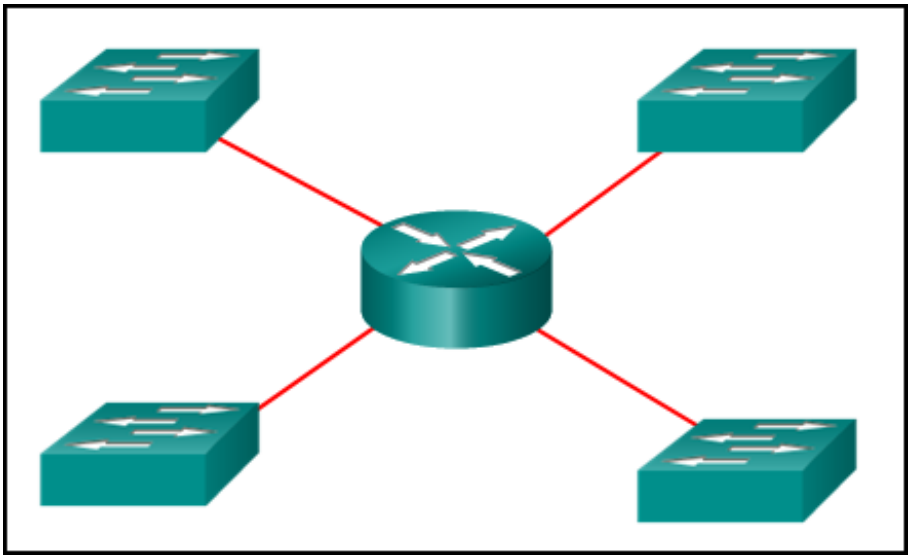
must be in the range of registered ports 1024 to 49151. The destination is the web server, which has the IP address 192.168.2.2, and the destination port number is 80 according to the HTTP protocol standard.

24. What information is used by TCP to reassemble and reorder received segments?

- **sequence numbers***
- acknowledgment numbers
- fragment numbers
- port numbers

Older Version

25. Refer to the exhibit. How many broadcast domains are there?



- 1
- 2
- 3
- **4***

26. How many usable host addresses are there in the subnet 192.168.1.32/27?

- 32
- **30***
- 64
- 16
- 62

27. How many host addresses are available on the network 172.16.128.0 with a subnet mask of 255.255.252.0?

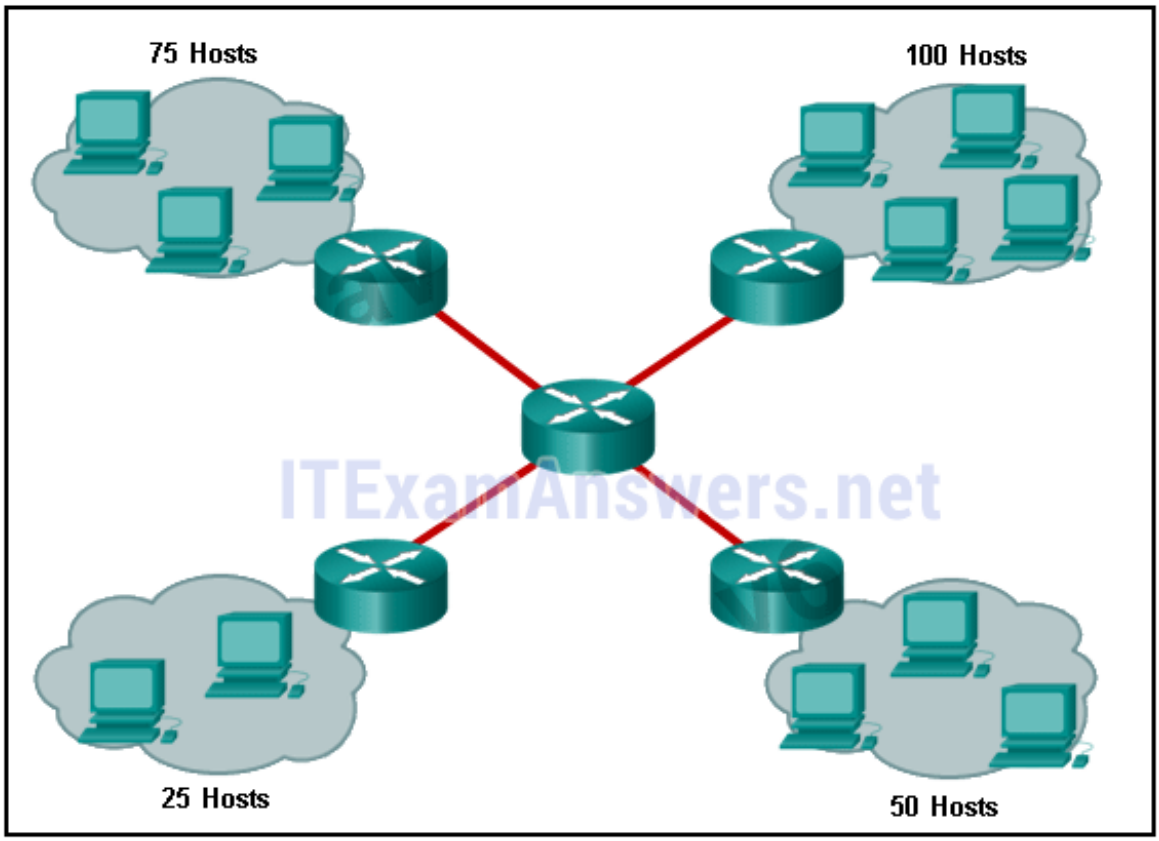
- 510

- 512
- **1022***
- 1024
- 2046
- 2048

28. A network administrator is variably subnetting a network. The smallest subnet has a mask of 255.255.255.248. How many host addresses will this subnet provide??

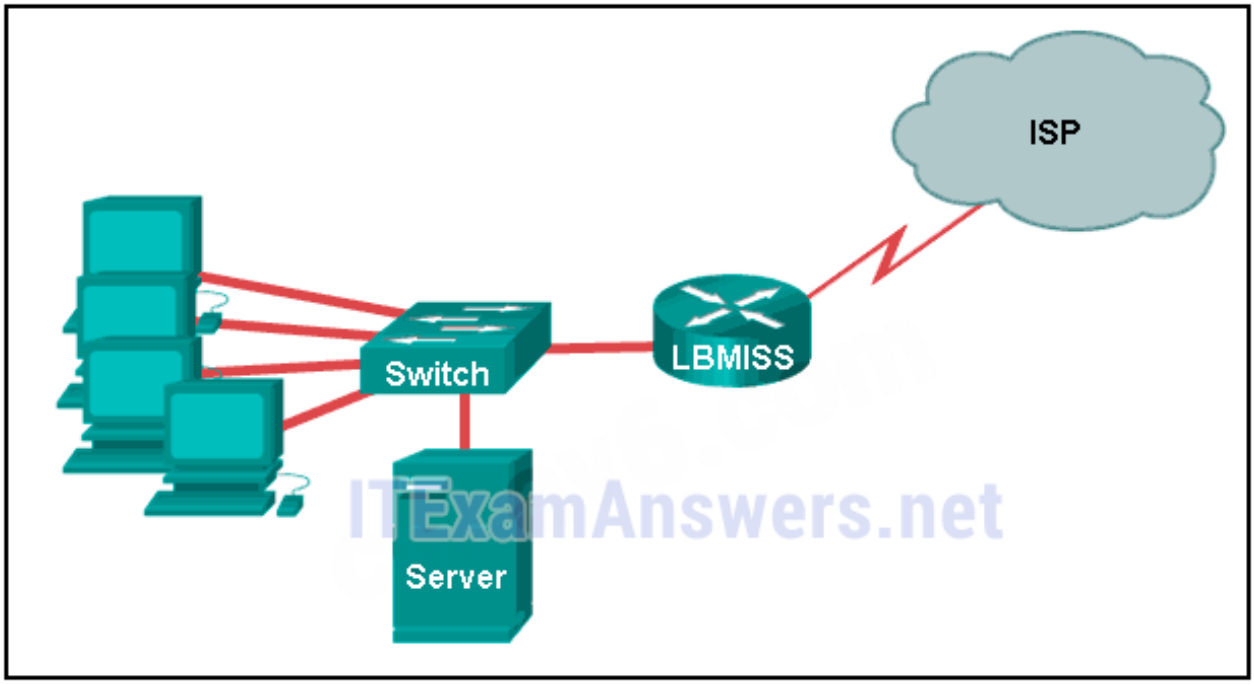
- 4
- **6***
- 8
- 10
- 12

29. Refer to the exhibit. A company uses the address block of 128.107.0.0/16 for its network. What subnet mask would provide the maximum number of equal size subnets while providing enough host addresses for each subnet in the exhibit?



- 255.255.255.0
- **255.255.255.128***
- 255.255.255.192
- 255.255.255.224
- 255.255.255.240

30. Refer to the exhibit. The network administrator has assigned the LAN of LBMISS an address range of 192.168.10.0. This address range has been subnetted using a /29 prefix. In order to accommodate a new building, the technician has decided to use the fifth subnet for configuring the new network (subnet zero is the first subnet). By company policies, the router interface is always assigned the first usable host address and the workgroup server is given the last usable host address. Which configuration should be entered into the properties of the workgroup server to allow connectivity to the Internet?



- IP address: 192.168.10.65 subnet mask: 255.255.255.240, default gateway: 192.168.10.76
- IP address: 192.168.10.38 subnet mask: 255.255.255.240, default gateway: 192.168.10.33
- **IP address: 192.168.10.38 subnet mask: 255.255.255.248, default gateway: 192.168.10.33***
- IP address: 192.168.10.41 subnet mask: 255.255.255.248, default gateway: 192.168.10.46
- IP address: 192.168.10.254 subnet mask: 255.255.255.0, default gateway: 192.168.10.1

31. How many bits must be borrowed from the host portion of an address to accommodate a router with five connected networks?

- two
- **three***
- four
- five

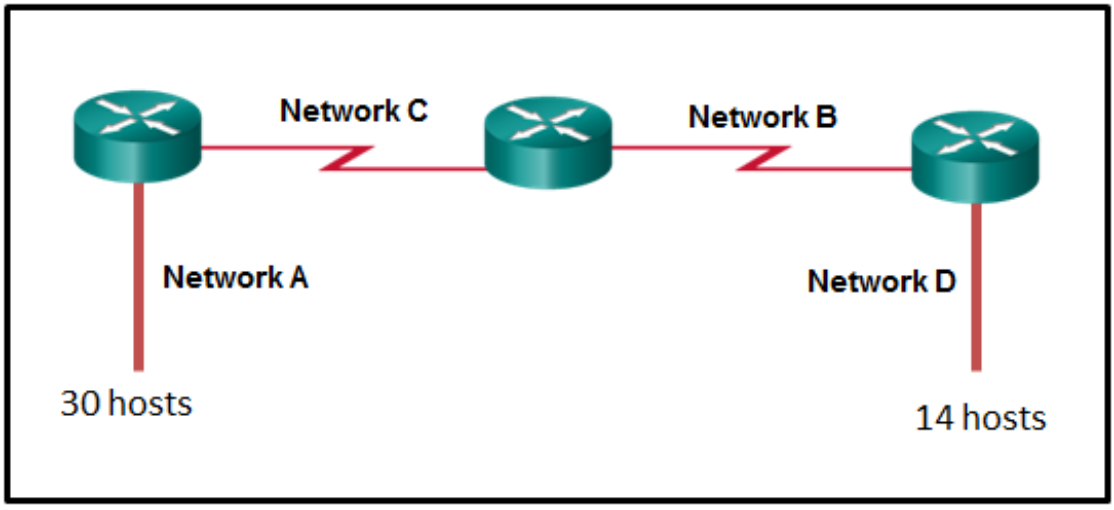
32. A company has a network address of 192.168.1.64 with a subnet mask of 255.255.255.192. The company wants to create two subnetworks that would contain 10 hosts and 18 hosts respectively. Which two networks would achieve that? (Choose two.)

- 192.168.1.16/28
- **192.168.1.64/27***
- 192.168.1.128/27
- **192.168.1.96/28***
- 192.168.1.192/28

33. In a network that uses IPv4, what prefix would best fit a subnet containing 100 hosts?

- /23
- /24
- **/25***
- /26

34. Refer to the exhibit.
Given the network address of 192.168.5.0 and a subnet mask of 255.255.255.224, how many total host addresses are unused in the assigned subnets?



- 56
- 60
- 64
- 68
- **72***

35. When developing an IP addressing scheme for an enterprise network, which devices are recommended to be grouped into their own subnet or logical addressing group?

- end-user clients

- workstation clients
- mobile and laptop hosts
- **hosts accessible from the Internet***

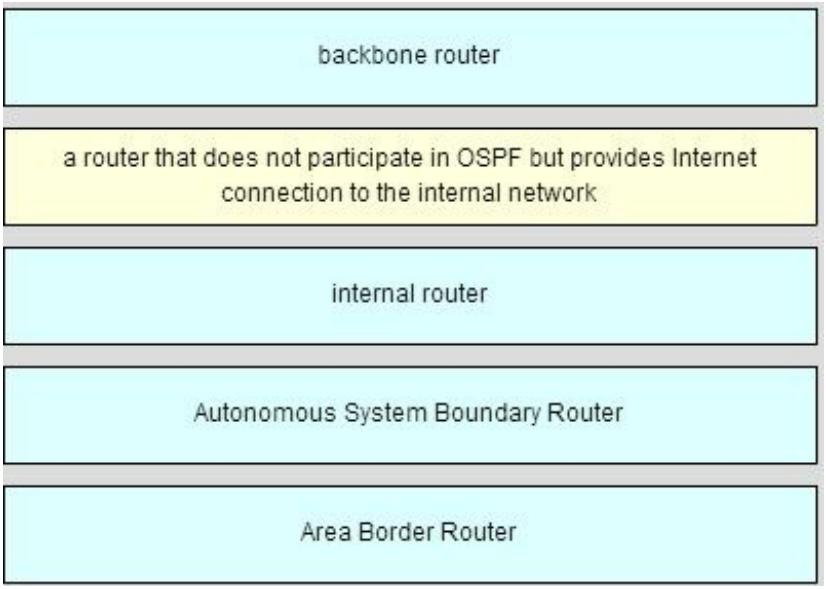
36. A network administrator needs to monitor network traffic to and from servers in a data center. Which features of an IP addressing scheme should be applied to these devices?

- random static addresses to improve security
- addresses from different subnets for redundancy
- **predictable static IP addresses for easier identification***
- dynamic addresses to reduce the probability of duplicate addresses

37. Which two reasons generally make DHCP the preferred method of assigning IP addresses to hosts on large networks? (Choose two.)

- **It eliminates most address configuration errors.***
- It ensures that addresses are only applied to devices that require a permanent address.
- It guarantees that every device that needs an address will get one.
- It provides an address only to devices that are authorized to be connected to the network.
- **It reduces the burden on network support staff.***

38. Refer to the exhibit. A computer that is configured with the IPv6 address as shown in the exhibit is unable to access the internet. What is the problem?



- The DNS address is wrong.
- There should not be an alternative DNS address.
- **The gateway address is in the wrong subnet.***
- The settings were not validated.

39. When subnetting a /64 IPv6 network prefix, which is the preferred new prefix

length?

- /66
- /70
- **/72***
- /74

40. What is the subnet address for the address 2001:DB8:BC15:A:12AB::1/64?

- 2001:DB8:BC15::0
- **2001:DB8:BC15:A::0***
- 2001:DB8:BC15:A:1::1
- 2001:DB8:BC15:A:12::0

41. Which two notations are useable nibble boundaries when subnetting in IPv6? (Choose two.)

- /62
- **/64***
- /66
- **/68***
- /70

42. Fill in the blank.
In dotted decimal notation, the IP address **172.25.0.126** is the last host address for the network 172.25.0.64/26.

43. Fill in the blank.
In dotted decimal notation, the subnet mask **255.255.254.0** will accommodate 500 hosts per subnet.
Consider the following range of addresses:
2001:0DB8:BC15:00A0:0000::
2001:0DB8:BC15:00A1:0000::
2001:0DB8:BC15:00A2:0000::
…
2001:0DB8:BC15:00AF:0000::
The prefix-length for the range of addresses is **/60**

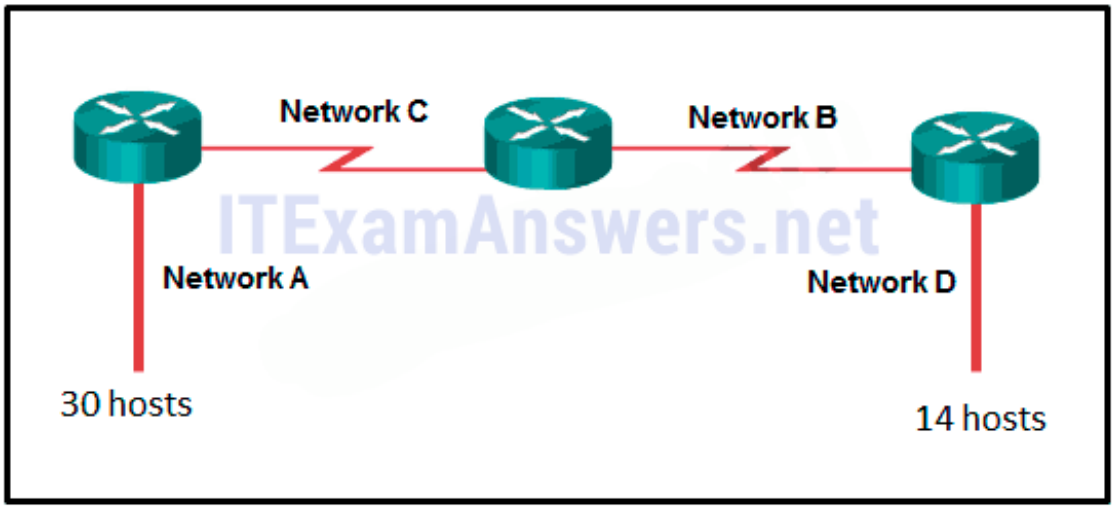
44. Fill in the blank.
A nibble consists of **4** bits.

45. Open the PT Activity. Perform the tasks in the activity instructions and then answer the question. What issue is causing Host A to be unable to communicate with Host B?

- The subnet mask of host A is incorrect.
- Host A has an incorrect default gateway.

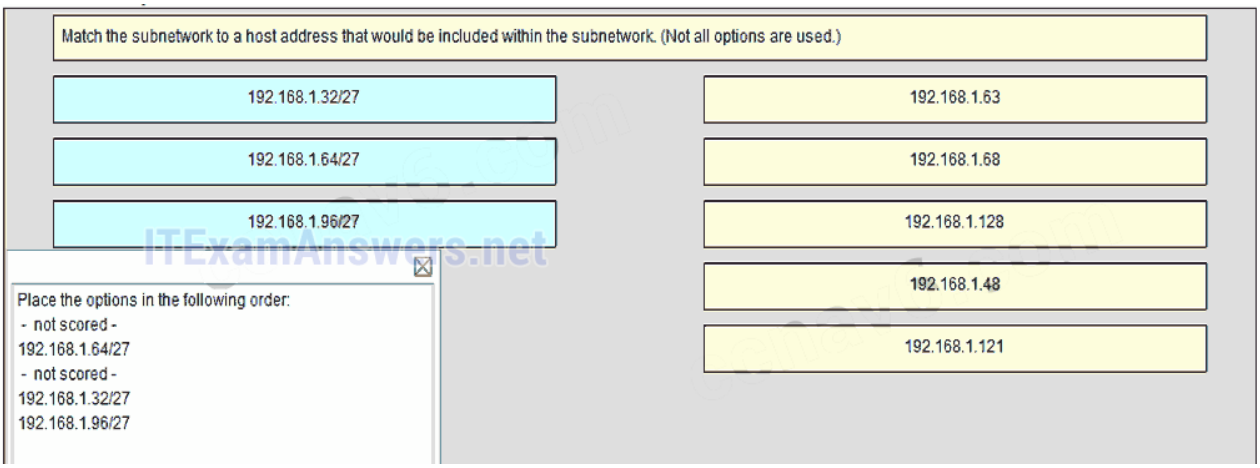
- **Host A and host B are on overlapping subnets.***
- The IP address of host B is not in the same subnet as the default gateway is on.

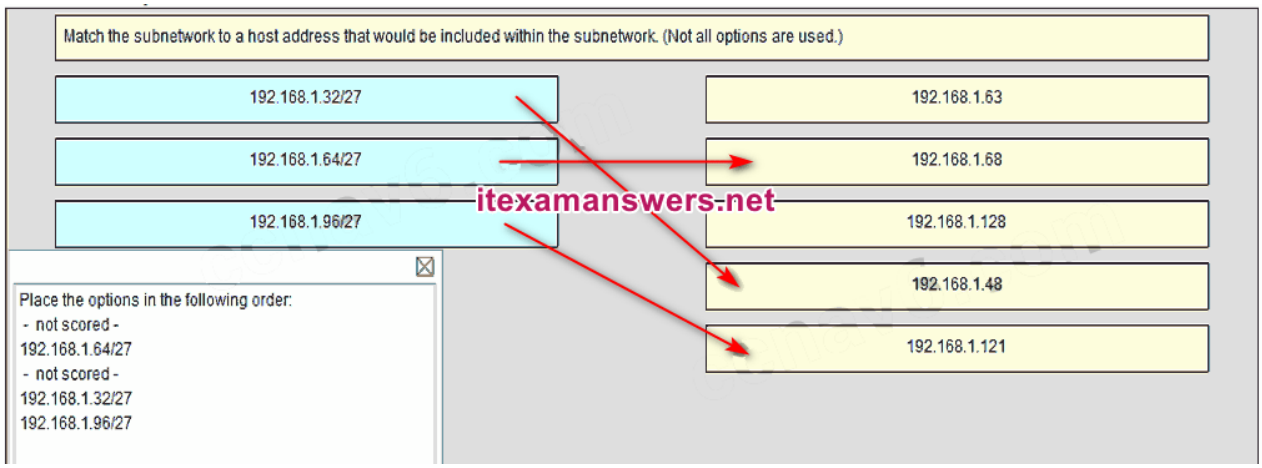
46. Refer to the exhibit. Given the network address of 192.168.5.0 and a subnet mask of 255.255.255.224, how many addresses are wasted in total by subnetting each network with a subnet mask of 255.255.255.224?



- 56
- 60
- 64
- 68
- **72***

47. Match the subnetwork to a host address that would be included within the subnetwork. (Not all option are used.)

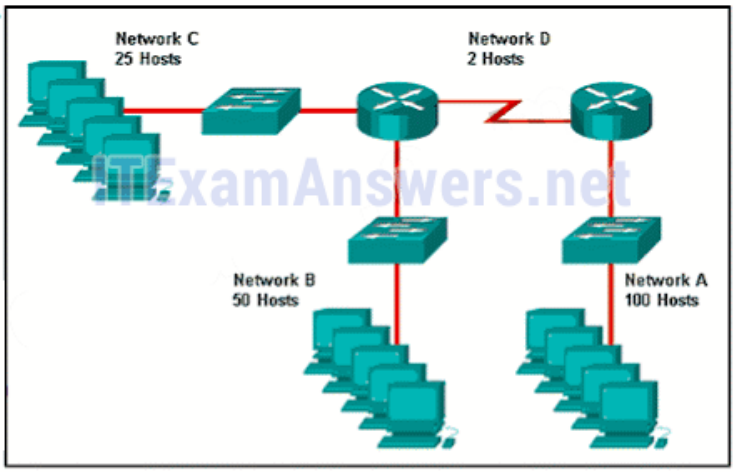




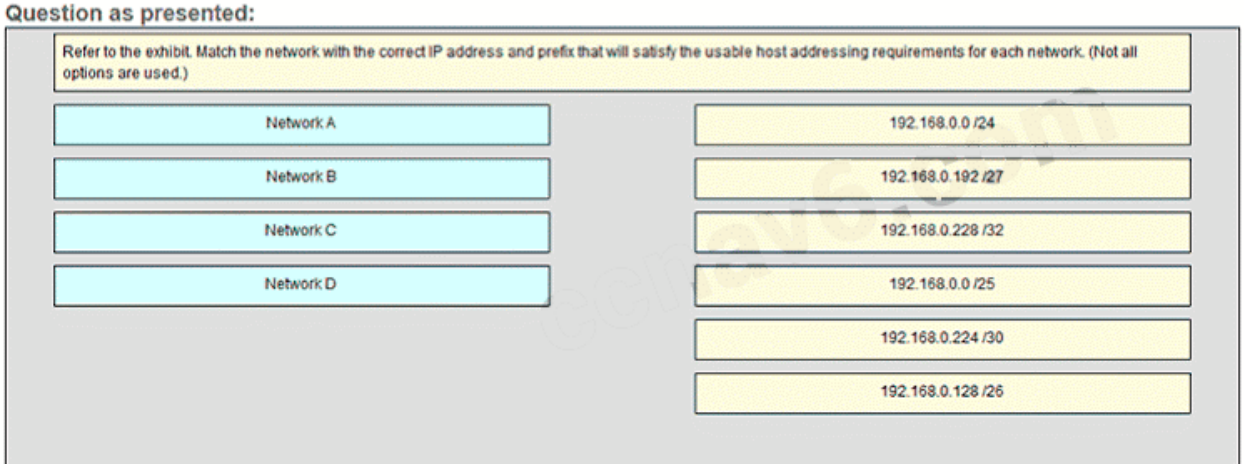
Place the options in the following order:

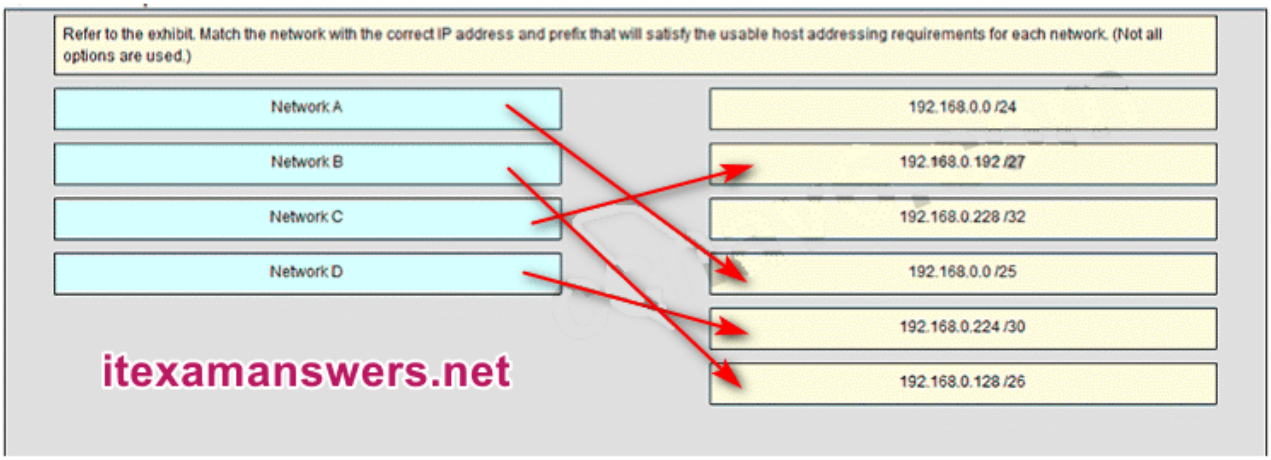
– not scored –
192.168.1.64/27
– not scored –
192.168.1.32/27
192.168.1.96/27

48. Refer to the exhibit. Match the network with the correct IP address and prefix that will satisfy the usable host addressing requirements for each network. (Not all options are used.)



Question as presented:





Place the options in the following order:
– not scored –
Network C
– not scored –
Network A
Network D
Network B

Download PDF File below:

ITexamanswers.net – CCNA 1 (v5.1 + v6.0) Chapter 9 Exam Answers Full.pdf

1 file(s) 1.31 MB

Download

share
or wait 117s

CCNA 1 (v5.1 + v6.0) Chapter 10 Exam Answers 2019 – 100% Full

itexamanswers.net/ccna-1-v5-1-v6-0-chapter-10-exam-answers-100-full.html

March 7, 2016

4.5 / **5** (**1344** votes)
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. Which two definitions accurately describe the associated application layer protocol? (Choose two.)

- SMTP – transfers web pages from web servers to clients
- **Telnet – provides remote access to servers and networking devices***
- **DNS – resolves Internet names to IP addresses***
- FTP – transfers email messages and attachments
- HTTP – enables devices on a network to obtain IP addresses

Explain:
The Domain Name Service (DNS) protocol resolves Internet names to IP addresses. Hypertext Transfer Protocol (HTTP) transfers files that make up the web pages of the World Wide Web. The Simple Mail Transfer Protocol (SMTP) transfers mail messages and attachments. Telnet, a terminal emulation protocol, provides remote access to servers and networking devices. The File Transfer Protocol (FTP) transfers files between systems.

2. The application layer of the TCP/IP model performs the functions of what three layers of the OSI model? (Choose three.)

- physical
- **session***
- network
- **presentation***
- data link
- transport
- **application***

Explain:
The network access layer of the TCP/IP model performs the same functions as the physical and data link layers of the OSI model. The internetwork layer equates to the

network layer of the OSI model. The transport layers are the same in both models. The application layer of the TCP/IP model represents the session, presentation, and application layers of the OSI model.

3. Which layer in the TCP/IP model is used for formatting, compressing, and encrypting data?

- internetwork
- session
- presentation
- **application***
- network access

Explain:
The application layer of the TCP/IP model performs the functions of three layers of the OSI model – application, presentation, and session. The application layer of the TCP/IP model is the layer that provides the interface between the applications, is responsible for formatting, compressing, and encrypting data, and is used to create and maintain dialogs between source and destination applications.

4. What are two characteristics of the application layer of the TCP/IP model? (Choose two.)

- responsibility for logical addressing
- responsibility for physical addressing
- **the creation and maintenance of dialogue between source and destination applications ***
- **closest to the end user***
- the establishing of window size

Explain:
The application layer of the TCP/IP model is the layer that is closest to the end user, providing the interface between the applications. It is responsible for formatting, compressing, and encrypting data, and is used to create and maintain dialog between source and destination applications.

5. A manufacturing company subscribes to certain hosted services from its ISP. The services that are required include hosted world wide web, file transfer, and e-mail. Which protocols represent these three key applications? (Choose three.)

- **FTP***
- **HTTP***
- DNS
- SNMP
- DHCP
- **SMTP***

Explain:
The ISP uses the HTTP protocol in conjunction with hosting web pages, the FTP protocol with file transfers, and SMTP with e-mail. DNS is used to translate domain names to IP addresses. SNMP is used for network management traffic. DHCP ic commonly used to manage IP addressing.

6. What is an example of network communication that uses the client-server model?

- A user uses eMule to download a file that is shared by a friend after the file location is determined.
- A workstation initiates an ARP to find the MAC address of a receiving host.
- A user prints a document by using a printer that is attached to a workstation of a coworker.
- **A workstation initiates a DNS request when the user types www.cisco.com in the address bar of a web browser.***

Explain:
When a user types a domain name of a website into the address bar of a web browser, a workstation needs to send a DNS request to the DNS server for the name resolution process. This request is a client/server model application. The eMule application is P2P. Sharing a printer on a workstation is a peer-to-peer network. Using ARP is just a broadcast message sent by a host.

7. Two students are working on a network design project. One student is doing the drawing, while the other student is writing the proposal. The drawing is finished and the student wants to share the folder that contains the drawing so that the other student can access the file and copy it to a USB drive. Which networking model is being used?

- **peer-to-peer***
- client-based
- master-slave
- point-to-point

Explain:
In a peer-to-peer (P2P) networking model, data is exchanged between two network devices without the use of a dedicated server.

8. What do the client/server and peer-to-peer network models have in common?

- Both models have dedicated servers.
- **Both models support devices in server and client roles.***
- Both models require the use of TCP/IP-based protocols.
- Both models are used only in the wired network environment.

Explain:
In both the client/server and peer-to-peer network models, clients and servers exist. In peer-to-peer networks, no dedicated server exists, but a device can assume the server role to provide information to a device serving in the client role.

9. What is an advantage for small organizations of adopting IMAP instead of POP?

- **Messages are kept in the mail servers until they are manually deleted from the email client.***
- When the user connects to a POP server, copies of the messages are kept in the mail server for a short time, but IMAP keeps them for a long time.
- IMAP sends and retrieves email, but POP only retrieves email.
- POP only allows the client to store messages in a centralized way, while IMAP allows distributed storage.

Explain:
IMAP and POP are protocols that are used to retrieve email messages. The advantage of using IMAP instead of POP is that when the user connects to an IMAP-capable server, copies of the messages are downloaded to the client application. IMAP then stores the email messages on the server until the user manually deletes those messages.

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

- DNS
- DHCP
- SMTP
- **HTTP***
- POP3

Explain:
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.

11. When retrieving email messages, which protocol allows for easy, centralized storage and backup of emails that would be desirable for a small- to medium-sized business?

- **IMAP***
- POP
- SMTP
- HTTPS

Explain:
IMAP is preferred for small-to medium-sized businesses as IMAP allows centralized storage and backup of emails, with copies of the emails being forwarded to clients. POP

delivers the emails to the clients and deletes them on the email server. SMTP is used to send emails and not to receive them. HTTPS is not used for secure web browsing.

12. What is the function of the Nslookup utility?

- **to manually query the name servers to resolve a given host name***
- to view the network settings on a host
- to manually force a client to send a DHCP request
- to display all cached DNS entries on a host

Explain: Nslookup is a command-line utility that is used to send a query to DNS servers to resolve a specific host name to an IP address.

13. What message type is used by an HTTP client to request data from a web server?

- POST
- ACK
- **GET***
- PUT

Explain:HTTP clients send GET messages to request data from web servers.

14. Which protocol is used by a client to communicate securely with a web server?

- SMB
- **HTTPS***
- SMTP
- IMAP

Explain:HTTPS is a secure form of HTTP used to access web content hosted by a web server.

15. Which three statements describe a DHCP Discover message? (Choose three.)

- The source MAC address is 48 ones (FF-FF-FF-FF-FF-FF).
- **The destination IP address is 255.255.255.255.***
- The message comes from a server offering an IP address.
- **The message comes from a client seeking an IP address.***
- **All hosts receive the message, but only a DHCP server replies.***
- Only the DHCP server receives the message.

Explain:
When a host configured to use DHCP powers up on a network it sends a DHCPDISCOVER message. FF-FF-FF-FF-FF-FF is the L2 broadcast address. A DHCP server replies with a unicast DHCPOFFER message back to the host.

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

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

Explain:
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

17. Which two tasks can be performed by a local DNS server? (Choose two.)

- providing IP addresses to local hosts
- allowing data transfer between two network devices
- **mapping name-to-IP addresses for internal hosts***
- **forwarding name resolution requests between servers***
- retrieving email messages

Explain:
Two important functions of DNS are to (1) provide IP addresses for domain names such as www.cisco.com, and (2) forward requests that cannot be resolved to other servers in order to provide domain name to IP address translation. DHCP provides IP addressing information to local devices. A file transfer protocol such as FTP, SFTP, or TFTP provides file sharing services. IMAP or POP can be used to retrieve an email message from a server.

18. Which phrase describes an FTP daemon?

- a diagnostic FTP program
- **a program that is running on an FTP server***
- a program that is running on an FTP client
- an application that is used to request data from an FTP server

Explain:
An FTP server runs an FTP daemon, which is a program that provides FTP services. End users who request services must run an FTP client program.

19. Which statement is true about FTP?

- The client can choose if FTP is going to establish one or two connections with the server.

- **The client can download data from or upload data to the server.***
- FTP is a peer-to-peer application.
- FTP does not provide reliability during data transmission.

Explain:
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.

20. What is true about the Server Message Block protocol?

- Different SMB message types have a different format.
- **Clients establish a long term connection to servers.***
- SMB messages cannot authenticate a session.
- SMB uses the FTP protocol for communication.

Explain:
The Server Message Block protocol is a protocol for file, printer, and directory sharing. Clients establish a long term connection to servers and when the connection is active, the resources can be accessed. Every SMB message has the same format. The use of SMB differs from FTP mainly in the length of the sessions. SMB messages can authenticate sessions.

21. Which application layer protocol is used to provide file-sharing and print services to Microsoft applications?

- **HTTP**
- **SMTP**
- **DHCP**
- **SMB***

Explain:
SMB is used in Microsoft networking for file-sharing and print services. The Linux operating system provides a method of sharing resources with Microsoft networks by using a version of SMB called SAMBA.

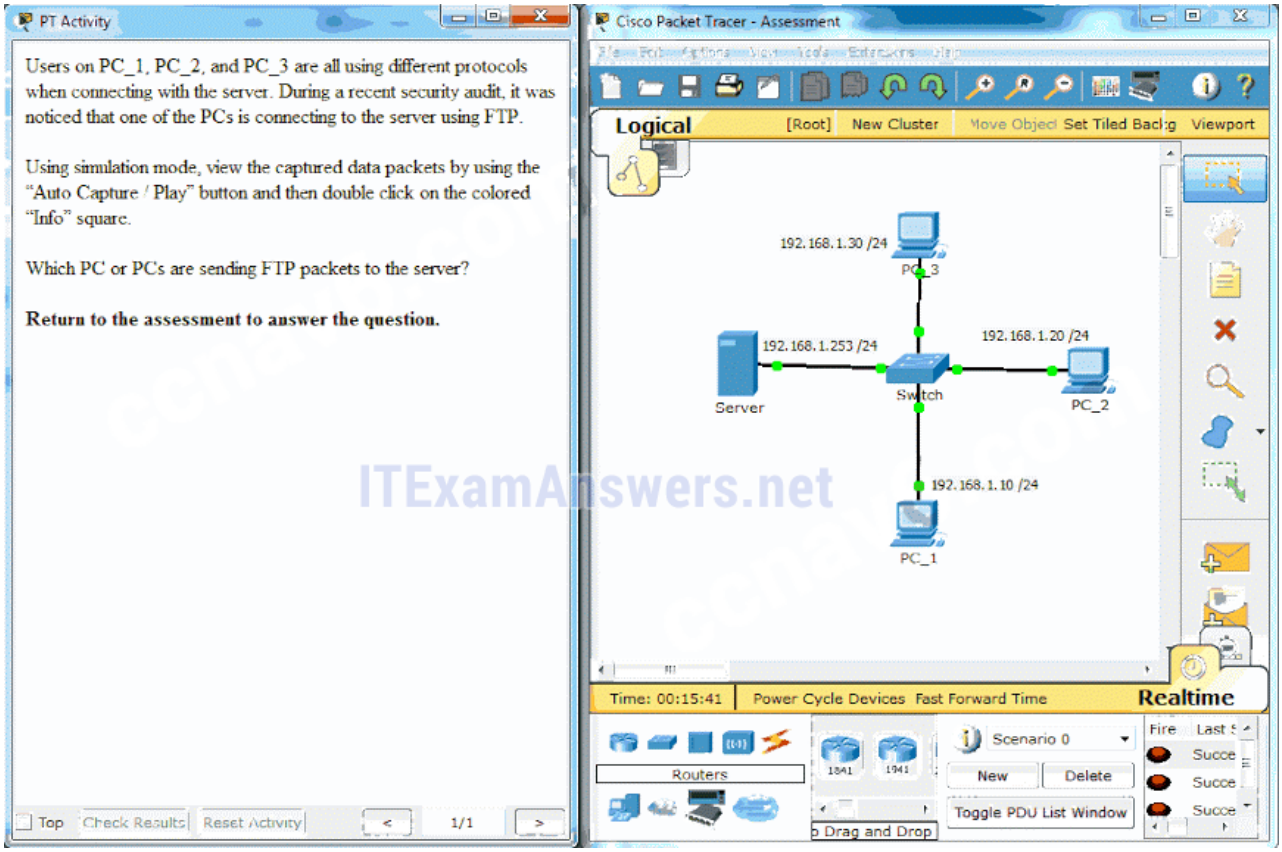
22. Fill in the blank.
What is the acronym for the protocol that is used when securely communicating with a web server? HTTPS

Explain:
Hypertext Transfer Protocol Secure (HTTPS) is the protocol that is used for accessing or posting web server information using a secure communication channel.

23. Fill in the blank.
The HTTP message type used by the client to request data from the web server is the GET message.

Explain:
GET is one of the message types used by HTTP. A client (web browser) sends the GET message to the web server to request HTML pages.

24. Open the PT Activity.



Perform the tasks in the activity instructions and then answer the question.Which PC or PCs are sending FTP packets to the server?

- **PC_3**
- **PC_1**
- **PC_2***
- **PC_1 and PC_3**

Explain:
After you view the details of the packets that are being transferred between each PC and the server, you will see that the PC that is using a destination port number of 20 or 21 is the PC using the FTP service. PC_2 has an outbound port number of 21 to create an FTP control session with the server at 192.168.1.253.

25. Fill in the blank.

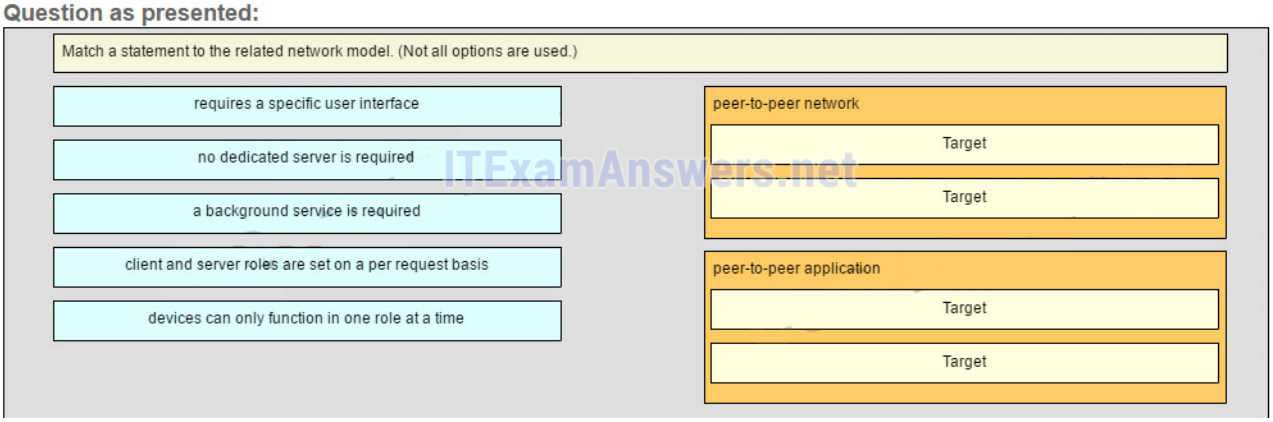
Refer to the exhibit. What command was used to resolve a given host name by querying the name servers?
nslookup

```
<output omitted>

> cisco.netacad.net
Server:  Unknown
Address:  192.168.0.1

Non-authoritative answer:
Name:    cisco.netacad.net
Address:  72.163.6.223

<output omitted>
```

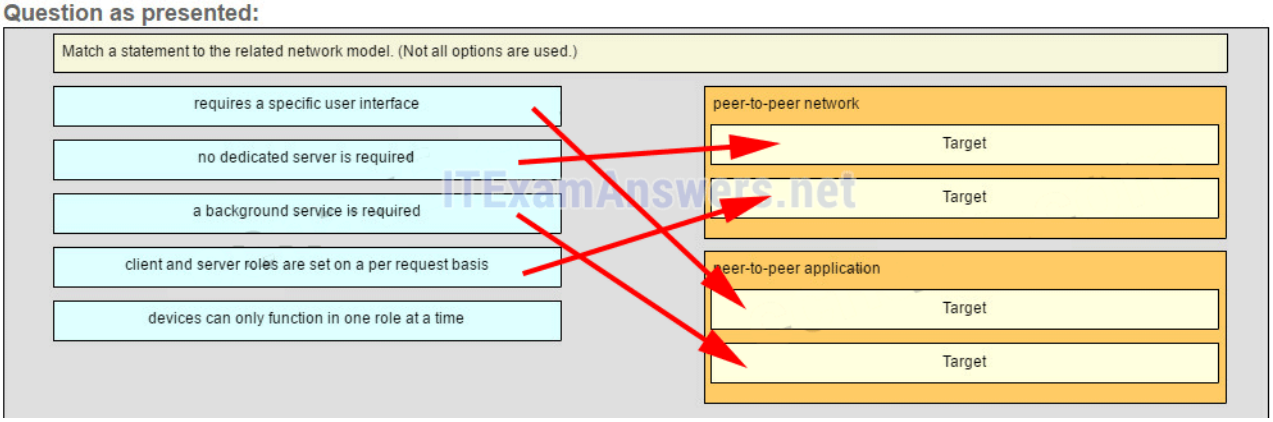
Explain:
A user can manually query the name servers to resolve a given host name using the nslookup command. Nslookup is both a command and a utility.

26. Match a statement to the related network model. (Not all options are used.)

Question as presented:



Question as presented:

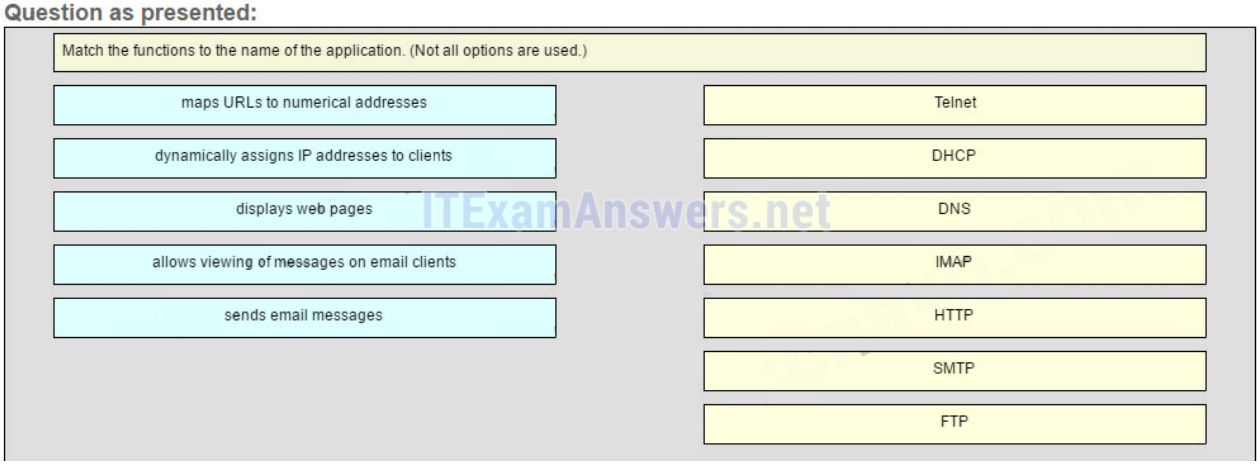


Place the options in the following order:peer-to-peer network
[+] no dedicated server is required
[+] client and server roles are set on a per request basis
peer-to-peer aplication
[#] requires a specific user interface
[#] a background service is required

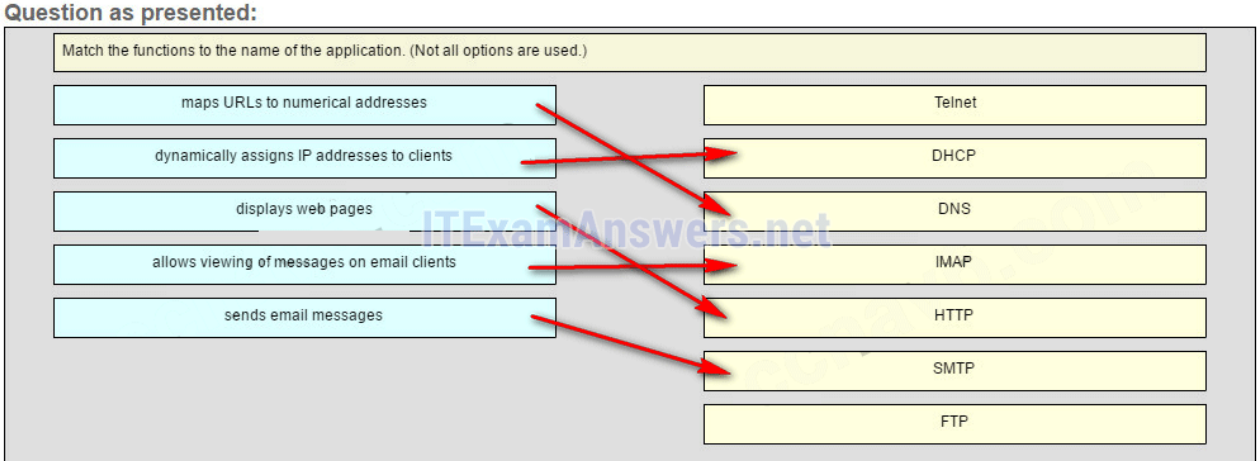
Explain:
Peer-to-peer networks do not require the use of a dedicated server, and devices can assume both client and server roles simultaneously on a per request basis. Because they do not require formalized accounts or permissions, they are best used in limited situations. Peer-to-peer applications require a user interface and background service to be running, and can be used in more diverse situations.

27. Match the functions to the name of the application. (Not all options are used.)

Question as presented:



Question as presented:



Place the options in the following order:
— not scored —
DHCP -> dynamically assigns IP address to clients
DNS -> maps URLs to numerical addresses
IMAP -> allows viewing of messages on email clients
HTTP -> displays web pages
SMTP -> sends email messages
— not scored —

Older Version

28. Which three layers of the OSI model provide similar network services to those provided by the application layer of the TCP/IP model? (Choose three.)

- physical layer
- **session layer***
- transport layer
- **application layer***
- **presentation layer***
- data link layer

29. Which two tasks are functions of the presentation layer? (Choose two.)

- **compression***
- addressing
- **encryption***
- session control
- authentication

30. Select three protocols that operate at the Application Layer of the OSI model. (Choose three.)

- ARP
- TCP
- DSL
- **FTP ***
- **POP3 ***
- **DHCP***

31. A manufacturing company subscribes to certain hosted services from their ISP. The services required include hosted world wide web, file transfer, and e-mail. Which protocols represent these three key applications? (Choose three.)

- **FTP ***
- **HTTP***
- DNS
- SNMP
- DHCP
- **SMTP***

32. What are two characteristics of peer-to-peer networks? (Choose two.)

- scalable
- one way data flow
- **decentralized resources***
- centralized user accounts
- **resource sharing without a dedicated server***

33. Which two actions are taken by SMTP if the destination email server is busy when email messages are sent? (Choose two.)

- SMTP sends an error message back to the sender and closes the connection.
- **SMTP tries to send the messages at a later time.***
- SMTP will discard the message if it is still not delivered after a predetermined expiration time.
- **SMTP periodically checks the queue for messages and attempts to send them again.***
- SMTP sends the messages to another mail server for delivery.

34. A DHCP-enabled client PC has just booted. During which two steps will the client PC use broadcast messages when communicating with a DHCP server? (Choose two.)

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

35. A user accessed the game site www.nogamename.com last week. The night before the user accesses the game site again, the site administrator changes the site IP address. What will be the consequence of that action for the user?

- The user will not be able to access the site.
- **The user will access the site without problems.***
- The user will have to modify the DNS server address on the local PC in order to access the site.
- The user will have to issue a ping to this new IP address to be sure that the domain name remained the same.

36. Which DNS server in the DNS hierarchy would be considered authoritative for the domain name records of a company named netacad?

- .com
- **netacad.com***
- mx.netacad.com
- www.netacad.com

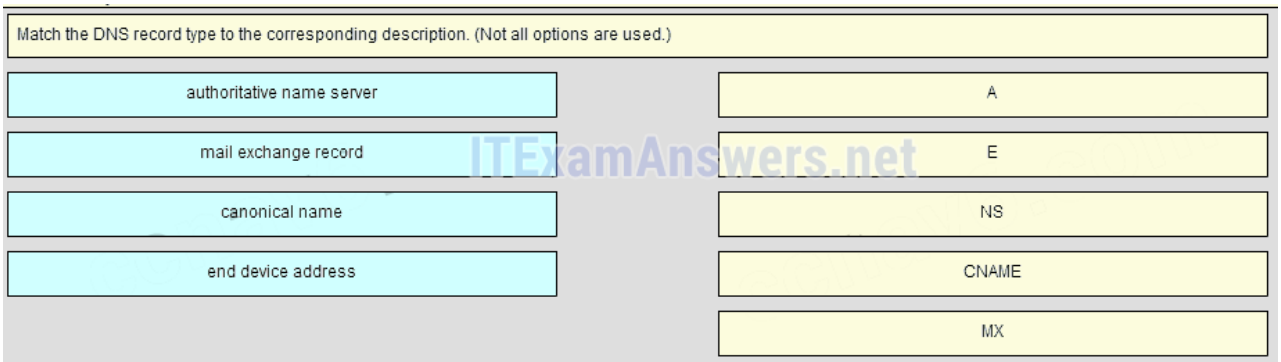
37. When would it be more efficient to use SMB to transfer files instead of FTP?

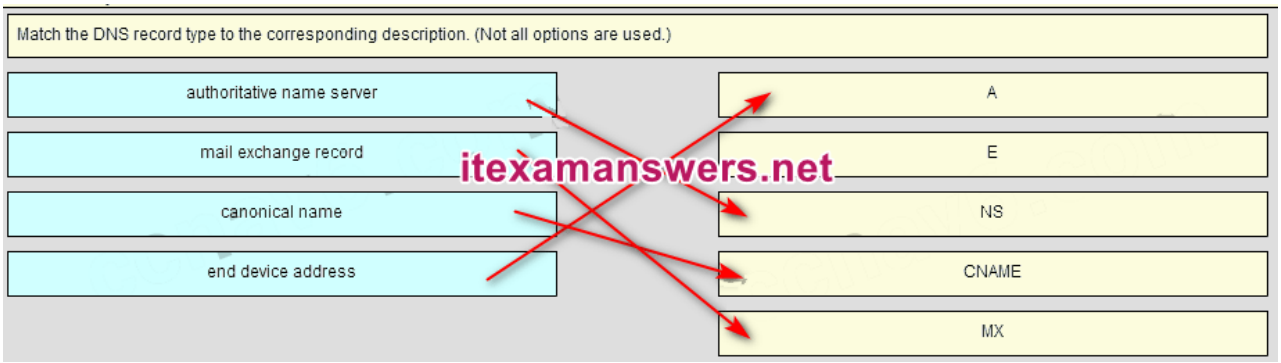
- when downloading large files with a variety of formats from different servers
- when a peer-to-peer application is required
- when the host devices on the network use the Windows operating system
- **when downloading large numbers of files from the same server***
- when uploading the same file to multiple remote servers

38. Fill in the blank.
What is the acronym for the protocol that is used when securely communicating with a web server? HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is the protocol that is used for accessing or posting web server information using a secure communication channel.

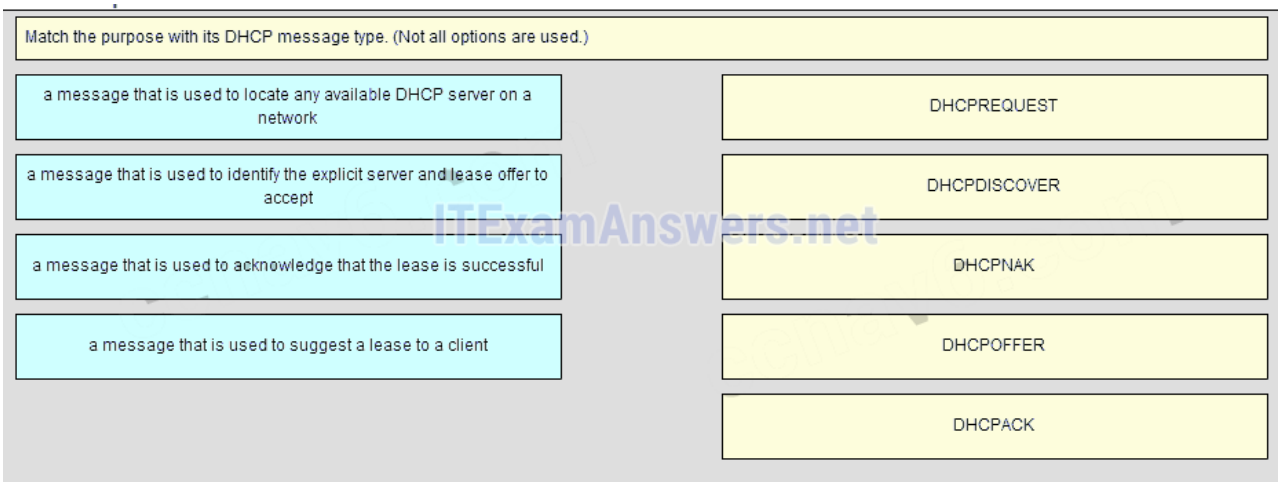
39. Match the DNS record type to the corresponding description. (Not all options are used.)

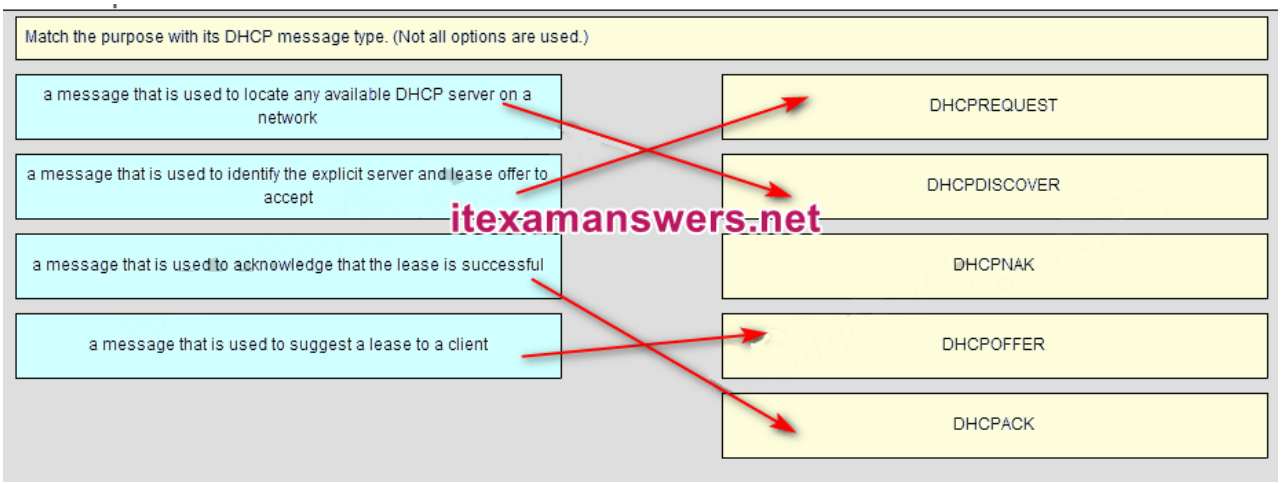




Place the options in the following order:
end device address
– not scored –
authoritative name server
canonical name
mail exchange record

40. Match the purpose with its DHCP message type. (Not all options are used.)





Place the options in the following order:
a message that is used to identify the explicit server and lease offer to accept
a message that is used to locate any available DHCP server on a network
– not scored –
a message that is used to suggest a lease to a client
a message that is used to acknowledge that the lease is successful

Download PDF File below:

ITexamanswers.net – CCNA 1 (v5.1 + v6.0) Chapter 10 Exam Answers Full.pdf

1 file(s) 1.37 MB

Download

This content is locked!
Please support us, use one of the buttons below to unlock the content.

like
tweet
share
follow us
error
share
or wait 200s

CCNA 1 (v5.1 + v6.0) Chapter 11 Exam Answers 2019 – 100% Full

itexamanswers.net/ccna-1-v5-1-v6-0-chapter-11-exam-answers-100-full.html

March 7, 2016

1.5 / **5** (**1212** votes)
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. A newly hired network technician is given the task of ordering new hardware for a small business with a large growth forecast. Which primary factor should the technician be concerned with when choosing the new devices?

- devices with a fixed number and type of interfaces
- devices that have support for network monitoring
- redundant devices
- **devices with support for modularity***

Explain:
In a small business with a large growth forecast, the primary influencing factor would be the ability of devices to support modularity. Devices with a fixed type/number of interfaces would not support growth. Redundancy is an important factor, but typically found in large enterprises. Network monitoring is also an important consideration, but not as important as modularity.

2. Which network design consideration would be more important to a large corporation than to a small business?

- Internet router
- firewall
- low port density switch
- **redundancy***

Explain:
Small businesses today do need Internet access and use an Internet router to provide this need. A switch is required to connect the two host devices and any IP phones or network devices such as a printer or a scanner. The switch may be integrated into the router. A firewall is needed to protect the business computing assets. Redundancy is not normally found in very small companies, but slightly larger small companies might use port density redundancy or have redundant Internet providers/links.

3. Which two traffic types require delay sensitive delivery? (Choose two.)

- email
- web
- FTP
- **voice***
- **video***

Explain:
Voice and video traffic have delay sensitive characteristics and must be given priority over other traffic types such as web, email, and file transfer traffic.

4. A network administrator for a small company is contemplating how to scale the network over the next three years to accommodate projected growth. Which three types of information should be used to plan for network growth? (Choose three.)

- human resource policies and procedures for all employees in the company
- **documentation of the current physical and logical topologies ***
- **analysis of the network traffic based on protocols, applications, and services used on the network***
- history and mission statement of the company
- **inventory of the devices that are currently used on the network***
- listing of the current employees and their role in the company

Explain:
Several elements that are needed to scale a network include documentation of the physical and logical topology, a list of devices that are used on the network, and an analysis of the traffic on the network.

5. Which two statements describe how to assess traffic flow patterns and network traffic types using a protocol analyzer? (Choose two.)

- Capture traffic on the weekends when most employees are off work.
- Only capture traffic in the areas of the network that receive most of the traffic such as the data center.
- **Capture traffic during peak utilization times to get a good representation of the different traffic types. ***
- **Perform the capture on different network segments.***
- Only capture WAN traffic because traffic to the web is responsible for the largest amount of traffic on a network.

Explain:
Traffic flow patterns should be gathered during peak utilization times to get a good representation of the different traffic types. The capture should also be performed on different network segments because some traffic will be local to a particular segment.

6. Some routers and switches in a wiring closet malfunctioned after an air conditioning unit failed. What type of threat does this situation describe?

- configuration
- **environmental***
- electrical
- maintenance

Explain:
The four classes of threats are as follows:
Hardware threats – physical damage to servers, routers, switches, cabling plant, and workstations
Environmental threats – temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry)
Electrical threats – voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss
Maintenance threats – poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labeling

7. Which type of network threat is intended to prevent authorized users from accessing resources?

- **DoS attacks***
- access attacks
- reconnaissance attacks
- trust exploitation

Explain:
Network reconnaissance attacks involve the unauthorized discovery and mapping of the network and network systems. Access attacks and trust exploitation involve unauthorized manipulation of data and access to systems or user privileges. DoS, or Denial of Service attacks, are intended to prevent legitimate users and devices from accessing network resources.

8. Which two actions can be taken to prevent a successful network attack on an email server account? (Choose two.)

- **Never send the password through the network in a clear text.***
- Never use passwords that need the Shift key.
- Use servers from different vendors.
- Distribute servers throughout the building, placing them close to the stakeholders.
- **Limit the number of unsuccessful attempts to log in to the server.***

Explain:
One of the most common types of access attack uses a packet sniffer to yield user accounts and passwords that are transmitted as clear text. Repeated attempts to log in to a server to gain unauthorized access constitute another type of access attack. Limiting

the number of attempts to log in to the server and using encrypted passwords will help prevent successful logins through these types of access attack.

9. Which firewall feature is used to ensure that packets coming into a network are legitimate responses initiated from internal hosts?

- application filtering
- **stateful packet inspection***
- URL filtering
- packet filtering

Explain:
Stateful packet inspection on a firewall checks that incoming packets are actually legitimate responses to requests originating from hosts inside the network. Packet filtering can be used to permit or deny access to resources based on IP or MAC address. Application filtering can permit or deny access based on port number. URL filtering is used to permit or deny access based on URL or on keywords.

10. What is the purpose of the network security authentication function?

- **to require users to prove who they are***
- to determine which resources a user can access
- to keep track of the actions of a user
- to provide challenge and response questions

Explain:
Authentication, authorization, and accounting are network services collectively known as AAA. Authentication requires users to prove who they are. Authorization determines which resources the user can access. Accounting keeps track of the actions of the user.

11. A network administrator is issuing the login block-for 180 attempts 2 within 30 command on a router. Which threat is the network administrator trying to prevent?

- **a user who is trying to guess a password to access the router***
- a worm that is attempting to access another part of the network
- an unidentified individual who is trying to access the network equipment room
- a device that is trying to inspect the traffic on a link

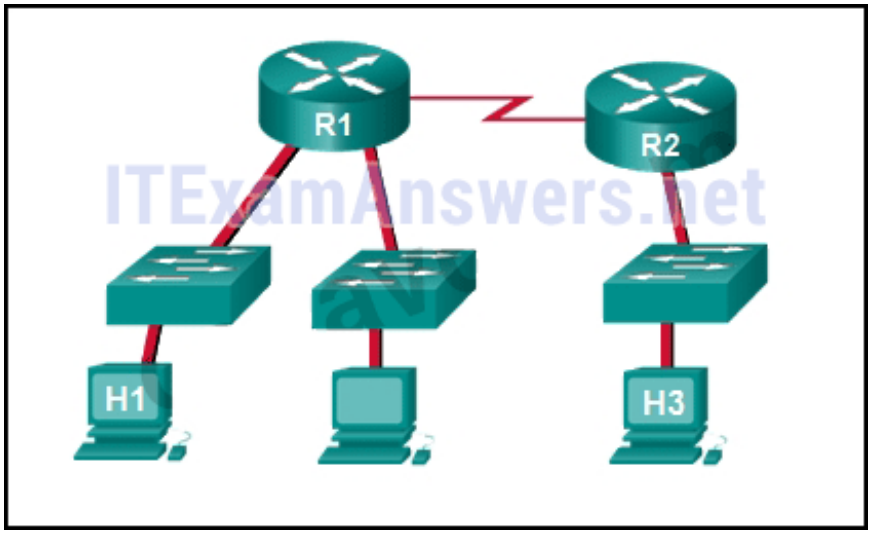
Explain:
The login block-for 180 attempts 2 within 30 command will cause the device to block authentication after 2 unsuccessful attempts within 30 seconds for a duration of 180 seconds. A device inspecting the traffic on a link has nothing to do with the router. The router configuration cannot prevent unauthorized access to the equipment room. A worm would not attempt to access the router to propagate to another part of the network.

12. Which two steps are required before SSH can be enabled on a Cisco router? (Choose two.)

- **Give the router a host name and domain name.***
- Create a banner that will be displayed to users when they connect.
- **Generate a set of secret keys to be used for encryption and decryption.***
- Set up an authentication server to handle incoming connection requests.
- Enable SSH on the physical interfaces where the incoming connection requests will be received.

Explain:
There are four steps to configure SSH on a Cisco router. First, set the host name and domain name. Second, generate a set of RSA keys to be used for encrypting and decrypting the traffic. Third, create the user IDs and passwords of the users who will be connecting. Lastly, enable SSH on the vty lines on the router. SSH does not need to be set up on any physical interfaces, nor does an external authentication server need to be used. While it is a good idea to configure a banner to display legal information for connecting users, it is not required to enable SSH.

13. Refer to the exhibit. Baseline documentation for a small company had ping round trip time statistics of 36/97/132 between hosts H1 and H3. Today the network administrator checked connectivity by pinging between hosts H1 and H3 that resulted in a round trip time of 1458/2390/6066. What does this indicate to the network administrator?



- Connectivity between H1 and H3 is fine.
- H3 is not connected properly to the network.
- Something is causing interference between H1 and R1.
- Performance between the networks is within expected parameters.
- **Something is causing a time delay between the networks.***

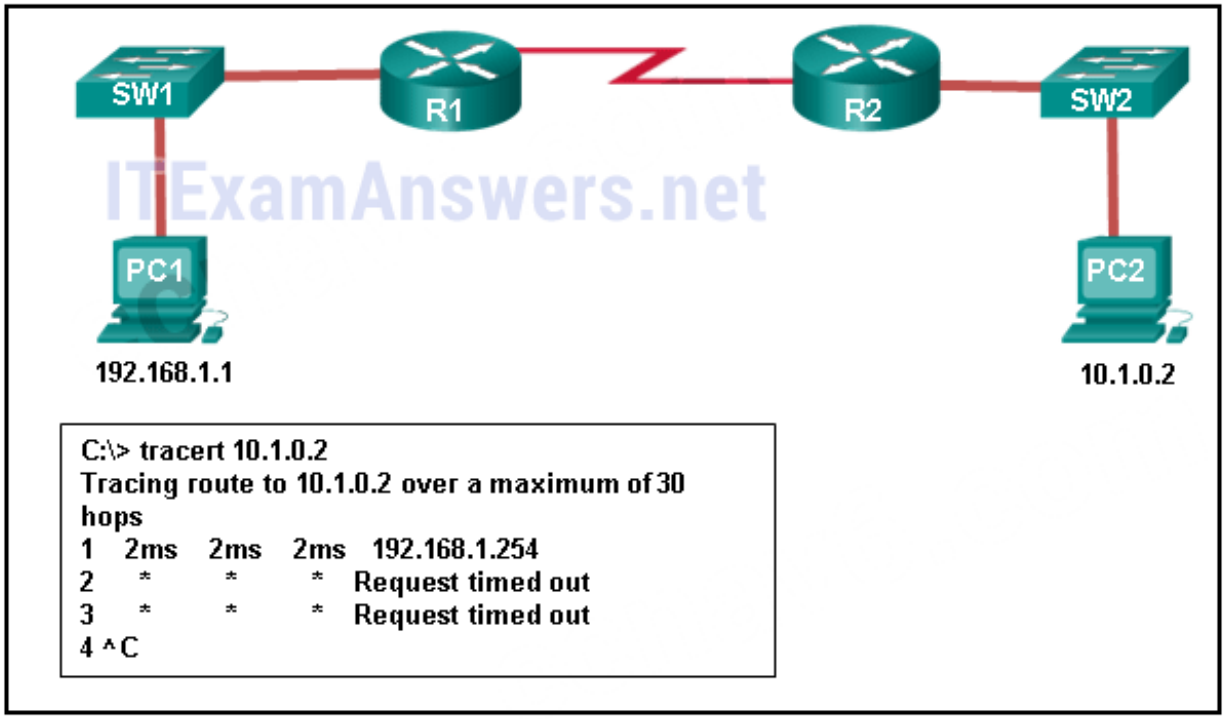
Explain:
Ping round trip time statistics are shown in milliseconds. The larger the number the more delay. A baseline is critical in times of slow performance. By looking at the documentation for the performance when the network is performing fine and comparing it to information when there is a problem, a network administrator can resolve problems faster.

14. When should an administrator establish a network baseline?

- when the traffic is at peak in the network
- when there is a sudden drop in traffic
- at the lowest point of traffic in the network
- **at regular intervals over a period of time***

Explain:
An effective network baseline can be established by monitoring the traffic at regular intervals. This allows the administrator to take note when any deviance from the established norm occurs in the network.

15. Refer to the exhibit. An administrator is trying to troubleshoot connectivity between PC1 and PC2 and uses the tracert command from PC1 to do it. Based on the displayed output, where should the administrator begin troubleshooting?



- PC2
- **R1***
- SW2
- R2
- SW1

Explain:
Tracert is used to trace the path a packet takes. The only successful response was from the first device along the path on the same LAN as the sending host. The first device is the default gateway on router R1. The administrator should therefore start troubleshooting at R1.

16. Which statement is true about CDP on a Cisco device?

- The show cdp neighbor detail command will reveal the IP address of a neighbor only if there is Layer 3 connectivity.
- To disable CDP globally, the no cdp enable command in interface configuration mode must be used.
- **CDP can be disabled globally or on a specific interface.***
- Because it runs at the data link layer, the CDP protocol can only be implemented in switches.

Explain:
CDP is a Cisco-proprietary protocol that can be disabled globally by using the no cdp run global configuration command, or disabled on a specific interface, by using the no cdp enable interface configuration command. Because CDP operates at the data link layer, two or more Cisco network devices, such as routers can learn about each other even if Layer 3 connectivity does not exist. The show cdp neighbors detail command reveals the IP address of a neighboring device regardless of whether you can ping the neighbor.

17. A network administrator for a small campus network has issued the show ip interface brief command on a switch. What is the administrator verifying with this command?

- **the status of the switch interfaces and the address configured on interface vlan 1***
- that a specific host on another network can be reached
- the path that is used to reach a specific host on another network
- the default gateway that is used by the switch

Explain:
The show ip interface brief command is used to verify the status and IP address configuration of the physical and switch virtual interfaces (SVI).

18. A network technician issues the arp -d * command on a PC after the router that is connected to the LAN is reconfigured. What is the result after this command is issued?

- **The ARP cache is cleared.***
- The current content of the ARP cache is displayed.
- The detailed information of the ARP cache is displayed.
- The ARP cache is synchronized with the router interface.

Explain:
Issuing the arp –d * command on a PC will clear the ARP cache content. This is helpful when a network technician wants to ensure the cache is populated with updated information.

19. Fill in the blank.
VoIP defines the protocols and technologies that implement the transmission of voice data over an IP network

20. Fill in the blank. Do not use abbreviations.
The show **file systems** command provides information about the amount of free nvram and flash memory with the permissions for reading or writing data.

21. Fill in the blank. Do not use abbreviations.
The **show version** command that is issued on a router is used to verify the value of the software configuration register.

Explain:
The show version command that is issued on a router displays the value of the configuration register, the Cisco IOS version being used, and the amount of flash memory on the device, among other information.

22. What service defines the protocols and technologies that implement the transmission of voice packets over an IP network?

- **VoIP***
- NAT
- DHCP
- QoS

23. What is the purpose of using SSH to connect to a router?

- **It allows a secure remote connection to the router command line interface.***
- It allows a router to be configured using a graphical interface.
- It allows the router to be monitored through a network management application.
- It allows secure transfer of the IOS software image from an unsecure workstation or server.

24. What information about a Cisco router can be verified using the show version command?

- **the value of the configuration register***
- the administrative distance used to reach networks
- the operational status of serial interfaces
- the routing protocol version that is enabled

25. A network technician issues the C:\> tracert -6 www.cisco.com command on a Windows PC. What is the purpose of the -6 command option?

- **It forces the trace to use IPv6.***
- It limits the trace to only 6 hops.
- It sets a 6 milliseconds timeout for each replay.
- It sends 6 probes within each TTL time period.

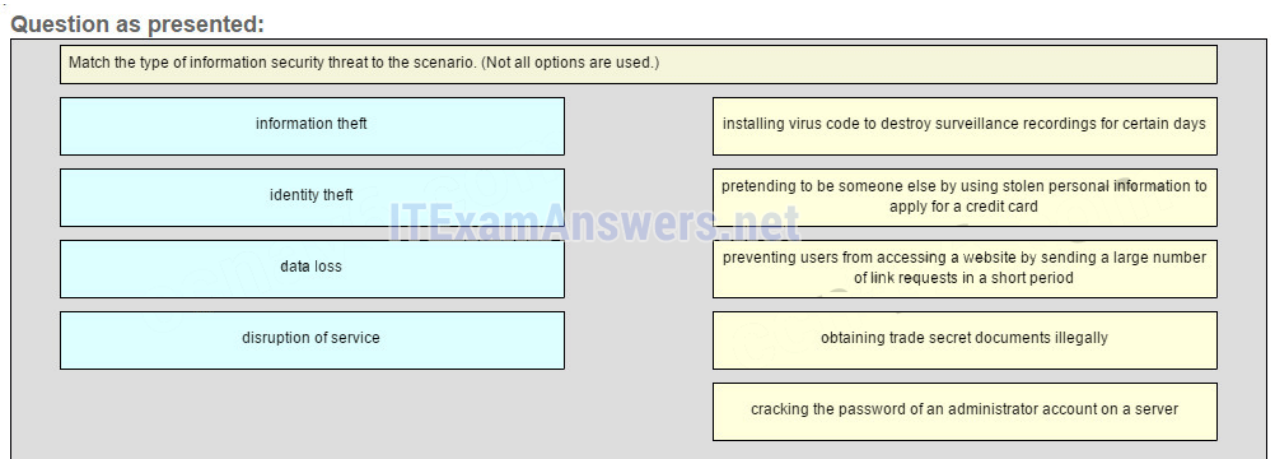
Explain:
The -6 option in the command C:\> tracert -6 www.cisco.com is used to force the trace to use IPv6.

26. Which command should be used on a Cisco router or switch to allow log messages to be displayed on remotely connected sessions using Telnet or SSH?

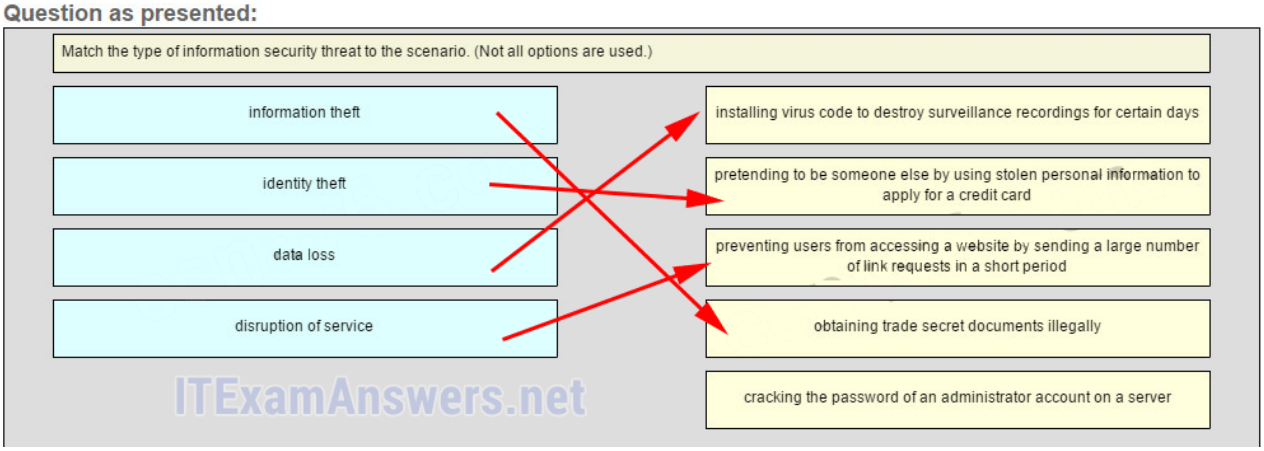
- debug all
- logging synchronous
- show running-config
- **terminal monitor***

Explain:
The terminal monitor command is very important to use when log messages appear. Log messages appear by default when a user is directly consoled into a Cisco device, but require the terminal monitor command to be entered when a user is accessing a network device remotely.

27. Match the type of information security threat to the scenario. (Not all options are used.)



Question as presented:



Place the options in the following order.
installing virus code to destroy surveillance recordings for certain days -> data loss
pretending to be someone else by using stolen personal information to apply for a credit card ->identity theft
preventing userd from accessing a website by sending a large number of link requests in a short period -> disruption of service
obtaining trade secret documents illegally -> information theft
— not scored —

Explain:
After an intruder gains access to a network, common network threats are as follows:
Information theft
Identity theft
Data loss or manipulation
Disruption of service
Cracking the password for a known username is a type of access attack.

Older Version

28. What is the purpose of issuing the commands cd nvram: then dir at the privilege exec mode of a router?

- to clear the content of the NVRAM
- to direct all new files to the NVRAM
- **to list the content of the NVRAM***
- to copy the directories from the NVRAM

29. Which command will backup the configuration that is stored in NVRAM to a TFTP server?

- copy running-config tftp
- copy tftp running-config
- **copy startup-config tftp***
- copy tftp startup-config

30. Which protocol supports rapid delivery of streaming media?

- SNMP
- TCP
- PoE
- **RTP***

31. How should traffic flow be captured in order to best understand traffic patterns in a network?

- during low utilization times
- **during peak utilization times***
- when it is on the main network segment only
- when it is from a subset of users

32. A network administrator checks the security log and notices there was unauthorized access to an internal file server over the weekend. Upon further investigation of the file system log, the administrator notices several important documents were copied to a host located outside of the company. What kind of threat is represented in this scenario?

- data loss
- identity theft
- **information theft***
- disruption of service

33. Which two actions can be taken to prevent a successful attack on an email server account? (Choose two.)

- **Never send the password through the network in a clear text.***
- Never use passwords that need the Shift key.
- Never allow physical access to the server console.
- Only permit authorized access to the server room.
- **Limit the number of unsuccessful attempts to log in to the server.***

34. Which type of network attack involves the disabling or corruption of networks, systems, or services?

- reconnaissance attacks
- access attacks
- **denial of service attacks***
- malicious code attacks

35. A network administrator has determined that various computers on the network are infected with a worm. Which sequence of steps should be followed to mitigate the worm attack?

- inoculation, containment, quarantine, and treatment
- containment, quarantine, treatment, and inoculation
- treatment, quarantine, inoculation, and containment
- **containment, inoculation, quarantine, and treatment ***

36. What is a security feature of using NAT on a network?

- allows external IP addresses to be concealed from internal users
- **allows internal IP addresses to be concealed from external users***
- denies all packets that originate from private IP addresses
- denies all internal hosts from communicating outside their own network

37. A ping fails when performed from router R1 to directly connected router R2. The network administrator then proceeds to issue the show cdp neighbors command. Why would the network administrator issue this command if the ping failed between the two routers?

- The network administrator suspects a virus because the ping command did not work.
- **The network administrator wants to verify Layer 2 connectivity.***
- The network administrator wants to verify the IP address configured on router R2.
- The network administrator wants to determine if connectivity can be established from a non-directly connected network.

38. If a configuration file is saved to a USB flash drive attached to a router, what must be done by the network administrator before the file can be used on the router?

- Convert the file system from FAT32 to FAT16.
- **Edit the configuration file with a text editor.***
- Change the permission on the file from ro to rw.
- Use the dir command from the router to remove the Windows automatic alphabetization of the files on the flash drive.

39. Which two statements about a service set identifier (SSID) are true? (Choose two.)

- **tells a wireless device to which WLAN it belongs***
- consists of a 32-character string and is not case sensitive
- responsible for determining the signal strength
- **all wireless devices on the same WLAN must have the same SSID***
- used to encrypt data sent across the wireless network

40. What do WLANs that conform to IEEE 802.11 standards allow wireless users to do?

- use wireless mice and keyboards

- create a one-to-many local network using infrared technology
- use cell phones to access remote services over very large areas
- **connect wireless hosts to hosts or services on a wired Ethernet network ***

41. Which WLAN security protocol generates a new dynamic key each time a client establishes a connection with the AP?

- EAP
- PSK
- WEP
- **WPA***

42. Which two statements characterize wireless network security? (Choose two.)

- Wireless networks offer the same security features as wired networks.
- Some RF channels provide automatic encryption of wireless data.
- **With SSID broadcast disabled, an attacker must know the SSID to connect.***
- **Using the default IP address on an access point makes hacking easier.***
- An attacker needs physical access to at least one network device to launch an attack.

43. Open the PT Activity. Perform the tasks in the activity instructions and then answer the question. How long will a user be blocked if the user exceeds the maximum allowed number of unsuccessful login attempts?

- 1 minute
- 2 minutes
- **3 minutes***
- 4 minutes

Download PDF File below:

ITexamanswers.net – CCNA 1 (v5.1 + v6.0) Chapter 11 Exam Answers Full.pdf

1 file(s) 1.12 MB

Download

This content is locked!

Please support us, use one of the buttons below to unlock the content.

like
tweet
share
follow us
error
share
or wait 213s