CoursMooc

Home > Exams > Cisco > CCNA 1 v7.0 Final Exam

CCNA 1 v7.0 Final Exam Answers – Introduction to Networks

CCNA 1 – Introduction to Networks (Version 7.00) – ITNv7 Course Final Exam. This comprehensive study guide covers the entire ITNv7 curriculum with 60+ questions, detailed explanations, and verified answers. The exam consists of **60 questions**, requiring **70%** to pass, with **1 hour 15 minutes** per attempt.

1. Which two traffic types use the Real-Time Transport Protocol (RTP)? (Choose two.)

A. web

B. file transfer

C. **video**

D. peer to peer

E. **voice**

Explanation: Topic 14.3.4 – RTP is designed for real-time data delivery such as interactive audio and video, prioritizing rapid flow over absolute reliability.

2. Which wireless technology has low-power and data rate requirements making it popular in home automation applications?

A. LoRaWAN

B. 5G

C. Wi-Fi

D. ZigBee

Explanation: Topic 4.6.2 – ZigBee is an IEEE 802.15.4 standard with low power and data rate, ideal for home automation devices.

3. Which layer of the TCP/IP model provides a route to forward messages through an internetwork?

A. application

B. network access

C. internet

D. transport

Explanation: Topic 3.5.3 – The internet layer of TCP/IP corresponds to the OSI network layer and handles addressing and routing messages through an internetwork.

4. Which type of server relies on record types such as A, NS, AAAA, and MX in order to provide services?

A. DNS

B. email

C. file

D. web

Explanation: Topic 15.4.2 – A DNS server stores records: A (IPv4 address), NS (name server), AAAA (IPv6 address), MX (mail exchange).

5. What are proprietary protocols?

A. protocols developed by private organizations to operate on any vendor hardware

B. protocols that can be freely used by any organization or vendor

C. protocols developed by organizations who have control over their definition and operation

D. a collection of protocols known as the TCP/IP protocol suite

Explanation: Topic 3.3.4 – Proprietary protocols have their definition and operation controlled by one company or vendor. Some of them can be used by different organizations with permission from the owner. The TCP/IP protocol suite is an open standard, not a proprietary protocol.

6. What service is provided by DNS?

A. Resolves domain names, such as cisco.com, into IP addresses.

B. A basic set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the web.

C. Allows for data transfers between a client and a file server.

D. Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.

Explanation: Topic 15.4.1 – DNS translates human-readable domain names into numeric IP addresses for network communication.

7. A client packet is received by a server. The packet has a destination port number of 110. What service is the client requesting?

A. DNS

B. DHCP

C. SMTP

D. POP3

Explanation: Topic 14.4.3 – Port 110 is reserved for POP3, used for retrieving email messages.

8. What command can be used on a Windows PC to see the IP configuration of that computer?

A. show ip interface brief

B. ping

C. show interfaces

D. **ipconfig**

Explanation: Topic 17.5.1 – `ipconfig` displays the IP configuration on Windows PCs.

9. A wired laser printer is attached to a home computer. That printer has been shared so that other computers on the home network can also use the printer. What networking model is in use?

A. client-based

B. master-slave

C. point-to-point

D. **peer-to-peer (P2P)**

Explanation: Topic 1.2.2 – Peer-to-peer (P2P) networks have two or more network devices that can share resources such as printers or files without having a dedicated server.

10. What characteristic describes a virus?

A. a network device that filters access and traffic coming into a network

B. the use of stolen credentials to access private data

C. an attack that slows or crashes a device or network service

D. **malicious software or code running on an end device**

Explanation: Topic 16.2.1 – A virus is malware that runs on an end device and propagates by inserting copies into other programs.

11. Three bank employees are using the corporate network. The first employee uses a web browser to view a company web page. The second accesses the corporate database for financial transactions. The third participates in an important live audio conference. If QoS is implemented, what will be the priorities from highest to lowest of the different data types?

A. financial transactions, web page, audio conference

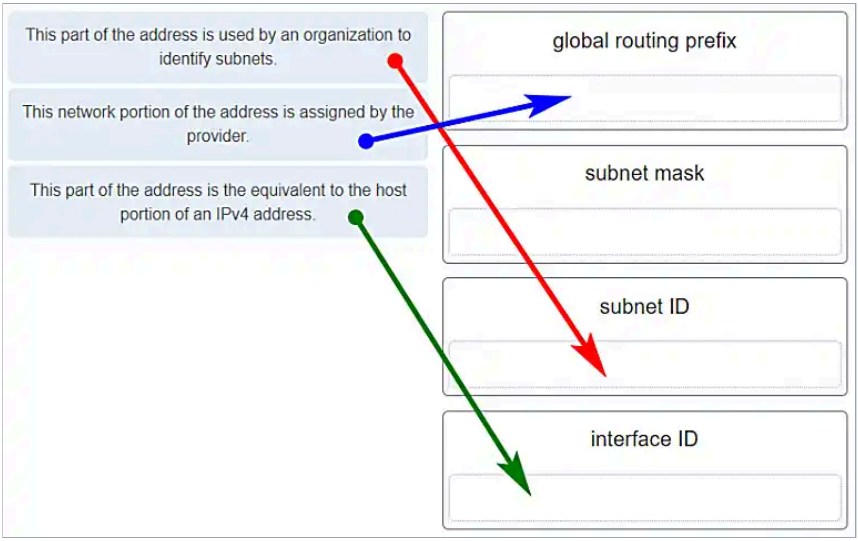
B. **audio conference, financial transactions, web page**

C. financial transactions, audio conference, web page

D. audio conference, web page, financial transactions

Explanation: Topic 1.6.4 – QoS mechanisms enable the establishment of queue management strategies that enforce priorities for different categories of application data. Thus, this queuing enables voice data to have priority over transaction data, which has priority over web data.

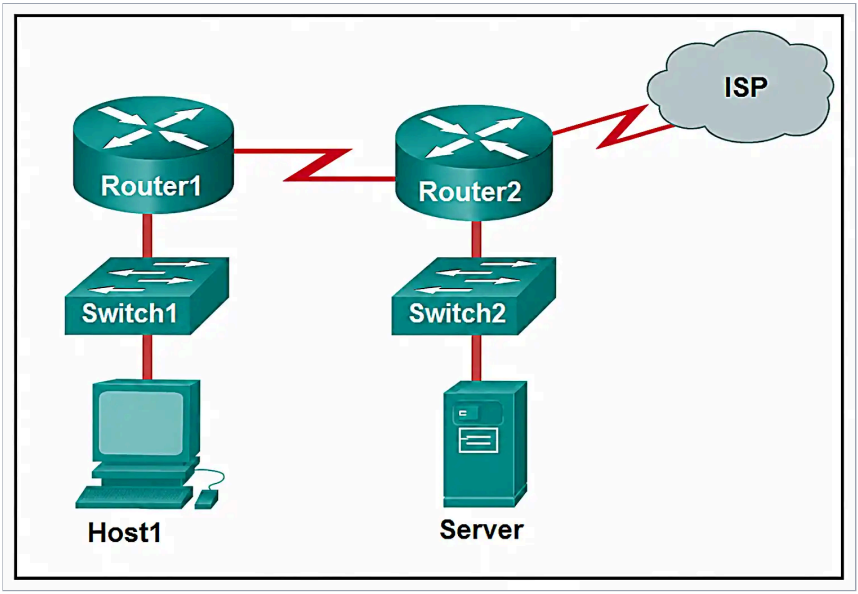
12. Match the description to the IPv6 addressing component. (Not all options are used.)



Explanation: Topic 12.3.6 - Place the options in the following order:

Description	Component
This network portion of the address is assigned by the provider.	global routing
This part of the address is used by an organization to identify subnets.	subnet ID
This part of the address is the equivalent to the host portion of an IPv4 address.	interface ID

13. Refer to the exhibit. If Host1 were to transfer a file to the server, what layers of the TCP/IP model would be used?



A. only application and Internet layers

B. only Internet and network access layers

C. only application, Internet, and network access layers

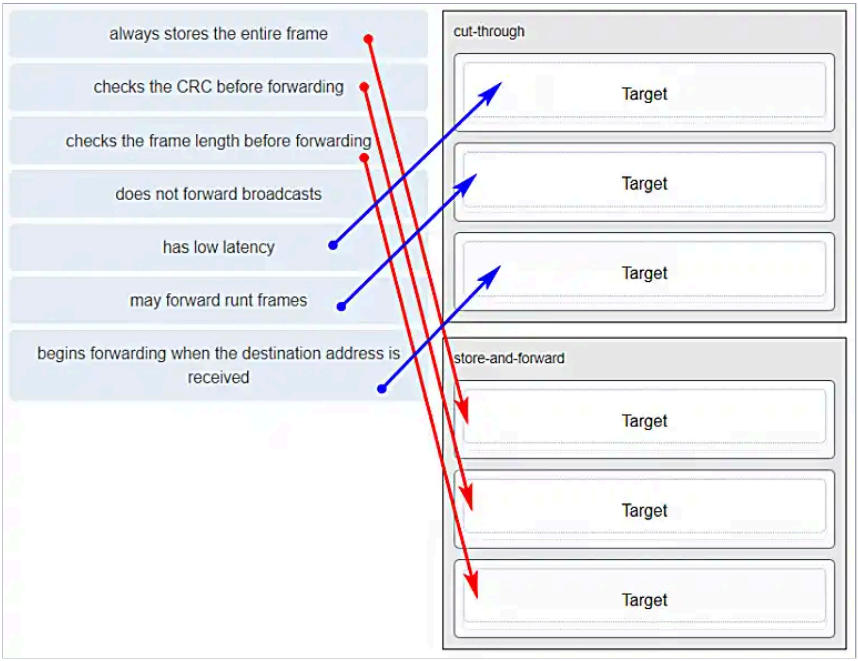
D. **application, transport, Internet, and network access layers**

E. only application, transport, network, data link, and physical layers

F. application, session, transport, network, data link, and physical layers

Explanation: Topic 3.5.3 – The TCP/IP model contains the application, transport, internet, and network access layers. A file transfer uses the FTP application layer protocol. The data would move from the application layer through all of the layers of the model and across the network to the file server.

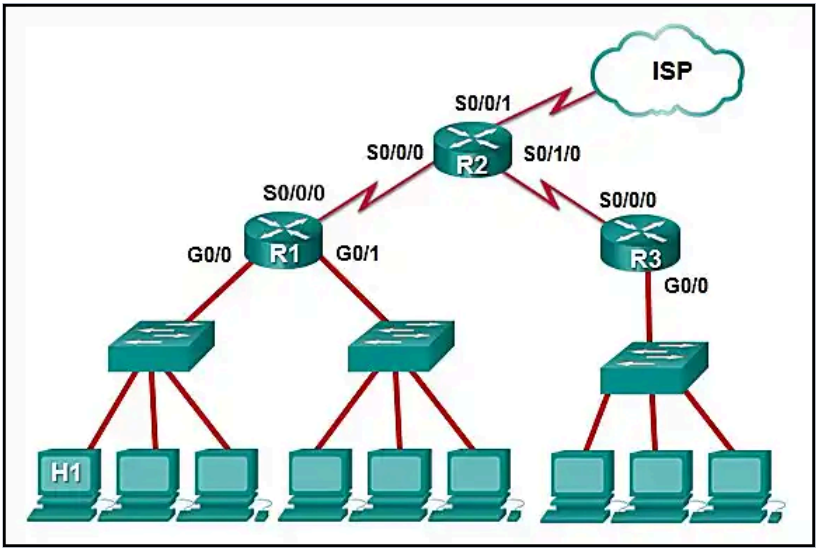
14. Match the characteristic to the forwarding method. (Not all options are used.)



Explanation: Topic 7.4.1 - A store-and-forward switch always stores the entire frame before forwarding, and checks its CRC and frame length. A cut-through switch can forward frames before receiving the destination address field, thus presenting less latency than a store-and-forward switch. Because the frame can begin to be forwarded before it is completely received, the switch may transmit a corrupt or runt frame. All forwarding methods require a Layer 2 switch to forward broadcast frames.

Cut-through	Store-and-forward
low latency	always stores the entire frame
may forward runt frames	checks the CRC before forwarding
begins forwarding when the destination address is received	checks the frame length before forwarding

15. Refer to the exhibit. The IP address of which device interface should be used as the default gateway setting of host H1?



A. R1: S0/0/0

B. R2: S0/0/1

C. **R1: G0/0**

D. R2: S0/0/0

Explanation: Topic 10.3.1 – The default gateway for host H1 is the router interface that is attached to the LAN that H1 is a member of. In this case, that is the G0/0 interface of R1. H1 should be configured with the IP address of that interface in its addressing settings. R1 will provide routing services to packets from H1 that need to be forwarded to remote networks.

16. What service is provided by Internet Messenger?

A. **An application that allows real-time chatting among remote users.**

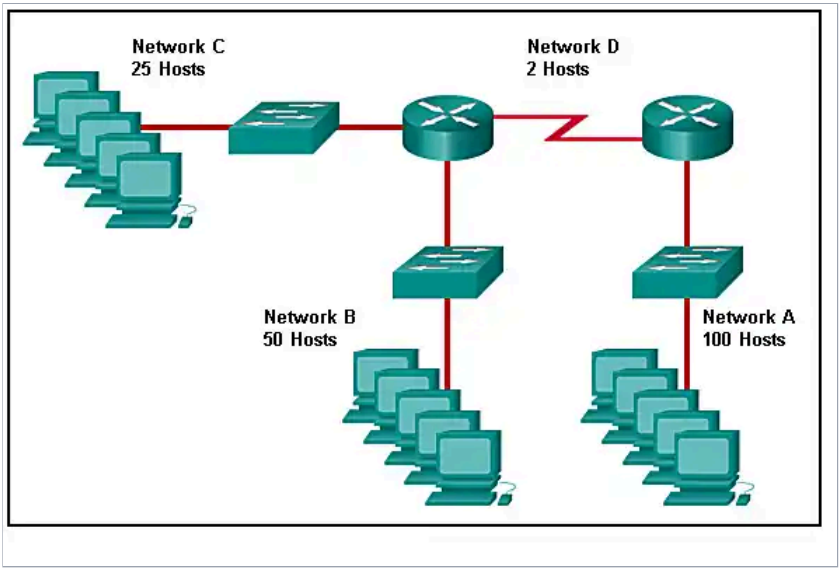
B. Allows remote access to network devices and servers.

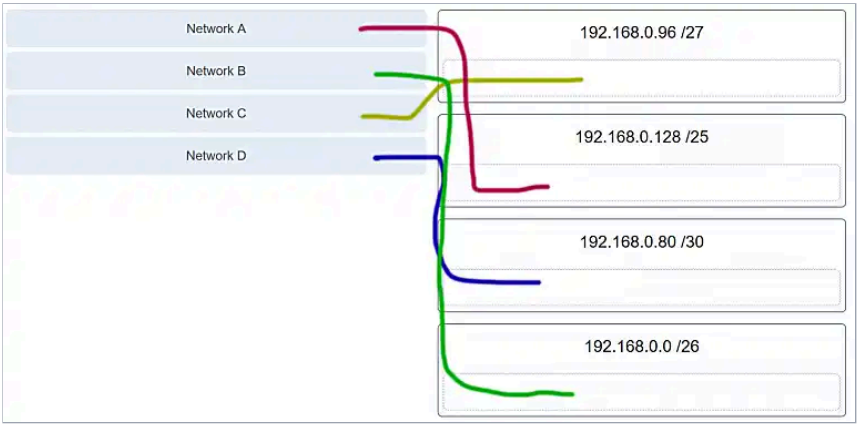
C. Resolves domain names, such as cisco.com, into IP addresses.

D. Uses encryption to provide secure remote access to network devices and servers.

Explanation: Topic 1.2.1 – Internet Messenger facilitates real-time communication between remote users.

17. 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.





Explanation: Topic 11.7.2 - Network A needs to use 192.168.0.128 /25, which yields 128 host addresses. Network B needs to use 192.168.0.0 /26, which yields 64 host addresses. Network C needs to use 192.168.0.96 /27, which yields 32 host addresses. Network D needs to use 192.168.0.80/30, which yields 4 host addresses.

Network	Address/Prefix
Network A	192.168.0.128 /25 (128 hosts)
Network B	192.168.0.0 /26 (64 hosts)

Network C	192.168.0.96 /27 (32 hosts)
Network D	192.168.0.80 /30 (4 hosts)

18. Refer to the exhibit. Which protocol was responsible for building the table that is shown?

```
<output omitted>

Interface: 192.168.1.67 --- 0xa
Internet Address          Physical Address       Type
192.168.1.254             64-0f-29-0d-36-91      dynamic
192.168.1.255             ff-ff-ff-ff-ff-ff      static
224.0.0.22                01-00-5e-00-00-16      static
224.0.0.251               01-00-5e-00-00-fb      static
224.0.0.252               01-00-5e-00-00-fc      static
255.255.255.255           ff-ff-ff-ff-ff-ff      static

Interface: 10.82.253.91 --- 0x10
Internet Address          Physical Address       Type
10.82.253.92              64-0f-29-0d-36-91      dynamic
224.0.0.22                01-00-5e-00-00-16      static
224.0.0.251               01-00-5e-00-00-fb      static
224.0.0.252               01-00-5e-00-00-fc      static
255.255.255.255           ff-ff-ff-ff-ff-ff      static
```

A. DHCP

B. **ARP**

C. DNS

D. ICMP

Explanation: Topic 9.2.7 – The output corresponds to `arp -a`, which displays the ARP table.

19. A network administrator notices that some newly installed Ethernet cabling is carrying corrupt and distorted data signals. The new cabling was installed

close to fluorescent lights and electrical equipment. Which two factors may interfere with the copper cabling and result in signal distortion? (Choose two.)

A. crosstalk

B. extended length of cabling

C. **RFI**

D. **EMI**

E. signal attenuation

Explanation: Topic 4.3.1 – EMI and RFI are external electromagnetic disruptions that corrupt data signals in copper cabling.

20. A host is trying to send a packet to a device on a remote LAN segment, but there are currently no mappings in its ARP cache. How will the device obtain a destination MAC address?

A. It will send the frame and use its own MAC address as the destination.

B. It will send an ARP request for the MAC address of the destination device.

C. It will send the frame with a broadcast MAC address.

D. It will send a request to the DNS server for the destination MAC address.

E. **It will send an ARP request for the MAC address of the default gateway.**

Explanation: Topic 9.2.5 – For a remote destination, the host sends an ARP request for the default gateway's MAC address.

22. A client packet is received by a server. The packet has a destination port number of 53. What service is the client requesting?

A. **DNS**

B. NetBIOS (NetBT)

C. POP3

D. IMAP

Explanation: Topic 14.4.3 – Port 53 is the well-known port for DNS name resolution services.

23. A network administrator is adding a new LAN to a branch office. The new LAN must support 25 connected devices. What is the smallest network mask that the network administrator can use for the new network?

A. 255.255.255.128

B. 255.255.255.192

C. 255.255.255.224

D. 255.255.255.240

Explanation: Topic 11.7.2 – A /27 mask (255.255.255.224) provides 30 usable host addresses (2^5–2), enough for 25 devices.

24. What characteristic describes a Trojan horse?

A. malicious software or code running on an end device

B. an attack that slows or crashes a device or network service

C. the use of stolen credentials to access private data

D. a network device that filters access and traffic coming into a network

Explanation: Topic 16.2.1 – A Trojan horse is malware disguised as legitimate software, relying on user interaction to activate.

25. What service is provided by HTTPS?

A. Uses encryption to provide secure remote access to network devices and servers.

B. Resolves domain names, such as cisco.com, into IP addresses.

C. Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.

D. Allows remote access to network devices and servers.

Explanation: Topic 15.3.2 – HTTPS encrypts web content using SSL/TLS to ensure confidentiality and integrity.

26. A technician with a PC is using multiple applications while connected to the Internet. How is the PC able to keep track of the data flow between multiple application sessions and have each application receive the correct packet flows?

A. The data flow is being tracked based on the destination MAC address of the technician PC.

B. The data flow is being tracked based on the source port number that is used by each application.

C. The data flow is being tracked based on the source IP address that is used by the PC of the technician.

D. The data flow is being tracked based on the destination IP address that is used by the PC of the technician.

Explanation: Topic 14.4.1 – The source port number of an application is randomly generated and used to individually keep track of each session connecting out to the Internet. Each application will use a unique source port number to provide simultaneous communication from multiple applications through the Internet.

27. A network administrator is adding a new LAN to a branch office. The new LAN must support 61 connected devices. What is the smallest network mask that

the network administrator can use for the new network?

A. 255.255.255.240

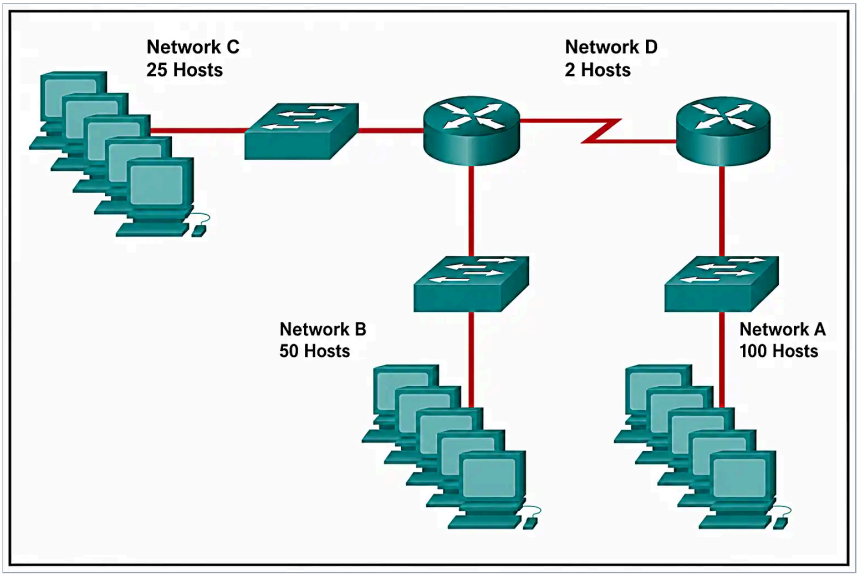
B. 255.255.255.224

C. **255.255.255.192**

D. 255.255.255.128

Explanation: Topic 11.7.2 – A /26 mask (255.255.255.192) provides 62 usable host addresses (2^6–2), enough for 61 devices.

28. 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.)



Explanation: Topic 11.7.2 - 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.

Network	Address/Prefix
Network A	192.168.0.0 /25
Network B	192.168.0.128 /26
Network C	192.168.0.192 /27
Network D	192.168.0.224 /30

29. What characteristic describes a DoS attack?

A. the use of stolen credentials to access private data

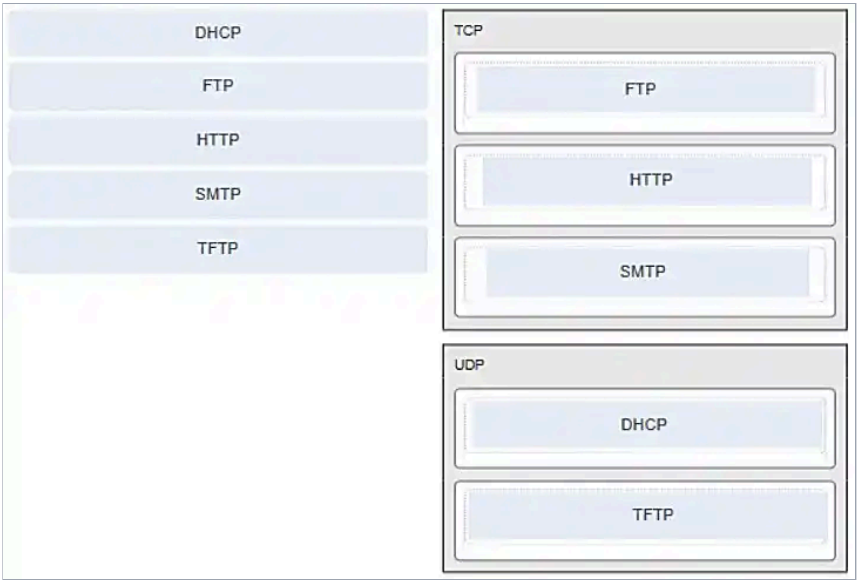
B. a network device that filters access and traffic coming into a network

C. software that is installed on a user device and collects information about the user

D. **an attack that slows or crashes a device or network service**

Explanation: Topic 16.2.4 – A DoS attack is designed to slow or crash network services, disrupting availability.

30. Match the application protocols to the correct transport protocols.



Explanation: Topic 14.4.3 – Match each application protocol to its corresponding transport protocol (TCP or UDP).

31. What service is provided by SMTP?

A. Allows clients to send email to a mail server and the servers to send email to other servers.

B. Allows remote access to network devices and servers.

C. Uses encryption to provide secure remote access to network devices and servers.

D. An application that allows real-time chatting among remote users.

Explanation: Topic 15.3.4 – SMTP handles the outgoing delivery of email messages.

32. Which scenario describes a function provided by the transport layer?

A. A student is using a classroom VoIP phone to call home. The unique identifier burned into the phone is a transport layer address.

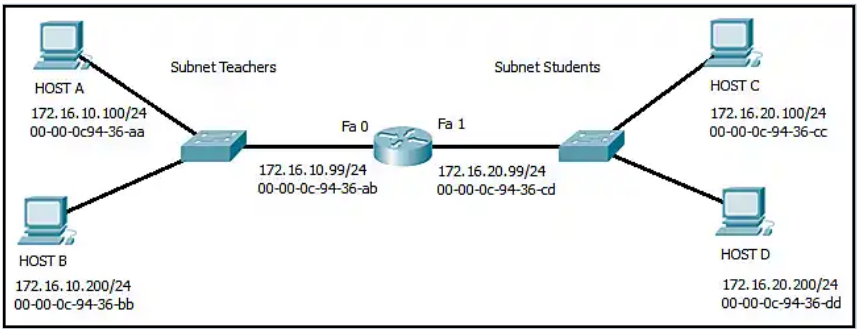
B. A student is playing a short web-based movie with sound. The movie and sound are encoded within the transport layer header.

C. 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.

D. 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.

Explanation: Topic 14.1.2 – The transport layer uses source and destination port numbers to identify the correct application and window.

33. Refer to the exhibit. Host B on subnet Teachers transmits a packet to host D on subnet Students. Which Layer 2 and Layer 3 addresses are contained in the PDUs that are transmitted from host B to the router?



A. Layer 2 destination address = 00-00-0c-94-36-ab
Layer 2 source address = 00-00-0c-94-36-bb
Layer 3 destination address = 172.16.20.200
Layer 3 source address = 172.16.10.200

B. Layer 2 destination address = 00-00-0c-94-36-dd
Layer 2 source address = 00-00-0c-94-36-bb

Layer 3 destination address = 172.16.20.200
Layer 3 source address = 172.16.10.200

C. Layer 2 destination address = 00-00-0c-94-36-cd
Layer 2 source address = 00-00-0c-94-36-bb
Layer 3 destination address = 172.16.20.99
Layer 3 source address = 172.16.10.200

D. Layer 2 destination address = 00-00-0c-94-36-ab
Layer 2 source address = 00-00-0c-94-36-bb
Layer 3 destination address = 172.16.20.200
Layer 3 source address = 172.16.100.200

Explanation: Topic 9.1.2 – The source and destination MAC and IP addresses identify the correct application and window.

34. What does the term "attenuation" mean in data communication?

A. strengthening of a signal by a networking device

B. leakage of signals from one cable pair to another

C. time for a signal to reach its destination

D. loss of signal strength as distance increases

Explanation: Topic 4.3.1 – Data is transmitted on copper cables as electrical pulses. A detector in the network interface of a destination device must receive a signal that can be successfully decoded to match the signal sent. However, the farther the signal travels, the more it deteriorates. This is referred to as signal attenuation.

35. Refer to the exhibit. An administrator is trying to configure the switch but receives the error message that is displayed in the exhibit. What is the problem?

```
Switch1> config t
               ^
% Invalid input detected at '^' marker.
```

A. The entire command, configure terminal, must be used.

B. The administrator is already in global configuration mode.

C. The administrator must first enter privileged EXEC mode before issuing the command.

D. The administrator must connect via the console port to access global configuration mode.

Explanation: Topic 2.2.4 – The administrator is in user EXEC mode (indicated by >), and must use `enable` to enter privileged EXEC mode before using `configure terminal`.

36. Which two protocols operate at the top layer of the TCP/IP protocol suite? (Choose two.)

A. TCP

B. IP

C. UDP

D. POP

E. DNS

F. Ethernet

Explanation: Topic 3.3.4 – DNS and POP operate at the application layer, the top layer of the TCP/IP model.

37. A company has a file server that shares a folder named Public. The network security policy specifies that the Public folder is assigned Read-Only rights to anyone who can log into the server while the Edit rights are assigned only to the network admin group. Which component is addressed in the AAA network service framework?

A. automation

B. accounting

C. authentication

D. **authorization**

Explanation: Topic 16.3.4 – After a user is successfully authenticated (logged into the server), the authorization is the process of determining what network resources the user can access and what operations (such as read or edit) the user can perform.

38. What three requirements are defined by the protocols used in network communications to allow message transmission across a network? (Choose three.)

A. **message size**

B. **message encoding**

C. connector specifications

D. media selection

E. **delivery options**

F. end-device installation

Explanation: Topic 3.1.5 – Protocols define message encoding, message size, and delivery options for successful transmission.

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

A. **does not require a dedicated end-to-end connection**

B. **operates independently of the network media**

C. retransmits packets if errors occur

D. re-assembles out of order packets into the correct order at the receiver end

E. guarantees delivery of packets

Explanation: Topic 8.1.3 – 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.

40. An employee of a large corporation remotely logs into the company using the appropriate username and password. The employee is attending an important video conference with a customer concerning a large sale. It is important for the video quality to be excellent during the meeting. The employee is unaware that after a successful login, the connection to the company ISP failed. The secondary connection, however, activated within seconds. The disruption was not noticed by the employee or other employees. What three network characteristics are described in this scenario? (Choose three.)

A. security

B. scalability

C. powerline networking

D. integrity

E. quality of service

F. fault tolerance

Explanation: Topic 1.6.1 – Usernames and passwords relate to network security. Good quality video, to support video conferencing, relates to prioritizing the video traffic with quality of service (QoS). The fact that a connection to an ISP failed and was then restored but went unnoticed by employees relates to the fault tolerant design of the network.

41. What are two common causes of signal degradation when using UTP cabling? (Choose two.)

A. improper termination

B. low-quality shielding in cable

C. installing cables in conduit

D. low-quality cable or connectors

E. loss of light over long distances

Explanation: Topic 4.4.2 – Improper termination and low-quality cable/connectors cause physical layer degradation.

42. Which subnet would include the address 192.168.1.96 as a usable host address?

A. 192.168.1.64/26

B. 192.168.1.32/27

C. 192.168.1.32/28

D. 192.168.1.64/29

Explanation: Topic 11.5.2 – For the subnet of 192.168.1.64/26, there are 6 bits for host addresses, yielding 64 possible addresses. However, the first and last subnets are the network and broadcast addresses for this subnet. Therefore, the range of host addresses for this subnet is 192.168.1.65 to 192.168.1.126. The other subnets do not contain the address 192.168.1.96 as a valid host address.

43. Refer to the exhibit. On the basis of the output, which two statements about network connectivity are correct? (Choose two.)

```
C:\Windows\system32> tracert 192.168.100.1
Tracing route to 192.168.100.1 over a maximum of 30 hops
1    1 ms    <1 ms    <1 ms    10.10.10.10
2    2 ms     2 ms     1 ms    192.168.1.22
3    2 ms     2 ms     1 ms    192.168.1.62
4    2 ms     2 ms     1 ms    172.16.1.1
5    2 ms     2 ms     1 ms    192.168.100.1
Trace complete.
```

A. This host does not have a default gateway configured.

B. **There are 4 hops between this device and the device at 192.168.100.1.**

C. **There is connectivity between this device and the device at 192.168.100.1.**

D. The connectivity between these two hosts allows for videoconferencing calls.

E. The average transmission time between the two hosts is 2 milliseconds.

Explanation: Topic 17.4.3 – The output displays a successful Layer 3 connection between a host computer and a host at 19.168.100.1. It can be determined that 4 hops exist between them and the average transmission time is 1 milliseconds. Layer 3 connectivity does not necessarily mean that an application can run between the hosts.

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

A. Capture traffic on the weekends when most employees are off work.

B. **Capture traffic during peak utilization times to get a good representation of the different traffic types.**

C. Only capture traffic in the areas of the network that receive most of the traffic such as the data center.

D. **Perform the capture on different network segments.**

E. Only capture WAN traffic because traffic to the web is responsible for the largest amount of traffic on a network.

Explanation: Topic 17.3.2 – 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.

45. What is the consequence of configuring a router with the *ipv6 unicast-routing* global configuration command?

A. All router interfaces will be automatically activated.

B. The IPv6 enabled router interfaces begin sending ICMPv6 Router Advertisement messages.

C. Each router interface will generate an IPv6 link-local address.

D. It statically creates a global unicast address on this router.

Explanation: Topic 12.5.1 – Enabling IPv6 unicast routing causes routers to send ICMPv6 Router Advertisement messages.

46. Which three layers of the OSI model map to the application layer of the TCP/IP model? (Choose three.)

A. application

B. network

C. data link

D. session

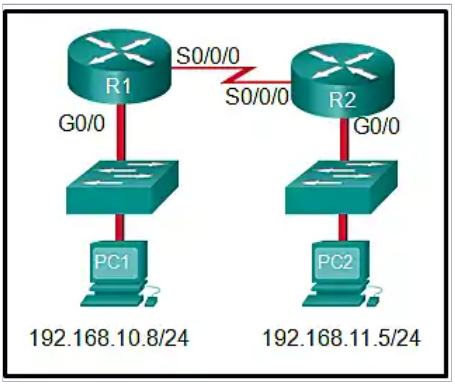
E. presentation

F. transport

Explanation: Topic 15.1.1 – The TCP/IP model consists of four layers: application, transport, internet, and network access. The OSI model consists of seven layers: application, presentation, session, transport, network, data link, and physical. The top

three layers of the OSI model: application, presentation, and session map to the application layer of the TCP/IP model.

47. Refer to the exhibit. If PC1 is sending a packet to PC2 and routing has been configured between the two routers, what will R1 do with the Ethernet frame header attached by PC1?



A. nothing, because the router has a route to the destination network

B. open the header and use it to determine whether the data is to be sent out S0/0/0

C. open the header and replace the destination MAC address with a new one

D. remove the Ethernet header and configure a new Layer 2 header before sending it out S0/0/0

Explanation: Topic 6.1.3 – When PC1 forms the various headers attached to the data one of those headers is the Layer 2 header. Because PC1 connects to an Ethernet network, an Ethernet header is used. The source MAC address will be the MAC address of PC1 and the destination MAC address will be that of G0/0 on R1. When R1 gets that information, the router removes the Layer 2 header and creates a new one for the type of network the data will be placed onto (the serial link).

48. What will happen if the default gateway address is incorrectly configured on a host?

A. The host cannot communicate with other hosts in the local network.

B. The host cannot communicate with hosts in other networks.

C. A ping from the host to 127.0.0.1 would not be successful.

D. The host will have to use ARP to determine the correct address of the default gateway.

E. The switch will not forward packets initiated by the host.

Explanation: Topic 17.7.4 – An incorrect default gateway prevents communication with hosts on other networks.

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

A. When a host is encapsulating a packet into a frame, it refers to the MAC address table to determine the mapping of IP addresses to MAC addresses.

B. An ARP request is sent to all devices on the Ethernet LAN and contains the IP address of the destination host and its multicast MAC address.

C. If a host is ready to send a packet to a local destination device and it has the IP address but not the MAC address of the destination, it generates an ARP broadcast.

D. If no device responds to the ARP request, then the originating node will broadcast the data packet to all devices on the network segment.

E. If a device receiving an ARP request has the destination IPv4 address, it responds with an ARP reply.

Explanation: Topic 9.2.2 – ARP broadcasts requests and hosts with the matching IP address reply with their MAC address.

50. A network administrator is adding a new LAN to a branch office. The new LAN must support 90 connected devices. What is the smallest network mask that the network administrator can use for the new network?

A. 255.255.255.128

B. 255.255.255.240

C. 255.255.255.248

D. 255.255.255.224

Explanation: Topic 11.7.2 – A /25 mask (255.255.255.128) provides 126 usable host addresses, enough for 90 devices.

51. What are two ICMPv6 messages that are not present in ICMP for IPv4? (Choose two.)

A. Neighbor Solicitation

B. Destination Unreachable

C. Host Confirmation

D. Time Exceeded

E. Router Advertisement

F. Route Redirection

Explanation: Topic 13.1.5 – Neighbor Solicitation and Router Advertisement are ICMPv6 messages not present in ICMP for IPv4.

52. A client packet is received by a server. The packet has a destination port number of 80. What service is the client requesting?

A. DHCP

B. SMTP

C. DNS

D. HTTP

Explanation: Topic 14.4.1 – Port 80 is the well-known port for HTTP web services.

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

A. POP only allows the client to store messages in a centralized way, while IMAP allows distributed storage.

B. Messages are kept in the mail servers until they are manually deleted from the email client.

C. 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.

D. IMAP sends and retrieves email, but POP only retrieves email.

Explanation: Topic 15.3.4 – 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.

54. A technician can ping the IP address of the web server of a remote company but cannot successfully ping the URL address of the same web server. Which software utility can the technician use to diagnose the problem?

A. tracert

B. ipconfig

C. netstat

D. nslookup

Explanation: Topic 15.4.4 – Traceroute (tracert) is a utility that generates a list of hops that were successfully reached along the path from source to destination.This list can provide important verification and troubleshooting information. The ipconfig utility is used to display the IP configuration settings on a Windows PC. The Netstat utility is used to identify which active TCP connections are open and running on a networked host. Nslookup is a utility that allows the user to manually query the name servers to resolve a given host name. This utility can also be used to troubleshoot name resolution issues and to verify the current status of the name servers.

55. Which two functions are performed at the LLC sublayer of the OSI Data Link Layer to facilitate Ethernet communication? (Choose two.)

A. implements CSMA/CD over legacy shared half-duplex media

B. enables IPv4 and IPv6 to utilize the same physical medium

C. integrates Layer 2 flows between 10 Gigabit Ethernet over fiber and 1 Gigabit Ethernet over copper

D. implements a process to delimit fields within an Ethernet 2 frame

E. places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame

Explanation: Topic 6.1.2 – The LLC sublayer enables multiple Layer 3 protocols and identifies the protocol in the frame.

56. The global configuration command *ip default-gateway 172.16.100.1* is applied to a switch. What is the effect of this command?

A. The switch can communicate with other hosts on the 172.16.100.0 network.

B. The switch can be remotely managed from a host on another network.

C. The switch is limited to sending and receiving frames to and from the gateway 172.16.100.1.

D. The switch will have a management interface with the address 172.16.100.1.

Explanation: Topic 10.3.2 – The default gateway allows the switch to be managed from a different network.

57. What happens when the *transport input ssh* command is entered on the switch vty lines?

A. The SSH client on the switch is enabled.

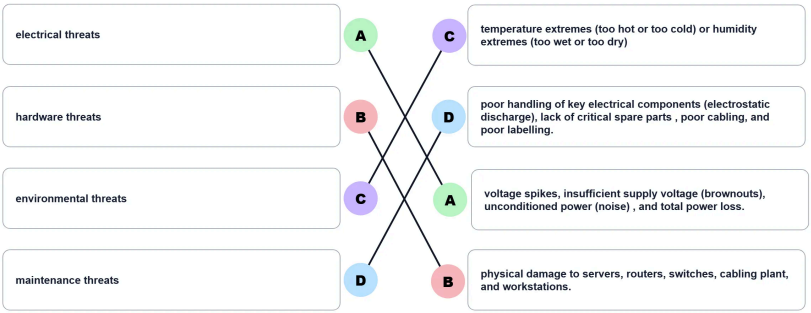
B. The switch requires a username/password combination for remote access.

C. Communication between the switch and remote users is encrypted.

D. The switch requires remote connections via a proprietary client software.

Explanation: Topic 16.4.4 – The transport input ssh command when entered on the switch vty (virtual terminal lines) will encrypt all inbound controlled telnet connections.

58. Match the type of threat with the cause. (Not all options are used.)



Explanation: Topic 16.1.3

Threat Type	Cause
electrical threats	voltage spikes, brownouts, unconditioned power, total power loss
hardware threats	physical damage to servers, routers, switches, cabling, workstations
environmental threats	temperature extremes (too hot or too cold) or humidity extremes
maintenance threats	poor handling of components, lack of spare parts, poor cabling, poor labeling

59. A disgruntled employee is using some free wireless networking tools to determine information about the enterprise wireless networks. This person is

planning on using this information to hack the wireless network. What type of attack is this?

A. DoS

B. access

C. **reconnaissance**

D. Trojan horse

Explanation: Topic 16.2.2 – A reconnaissance attack involves unauthorized discovery and documentation of network systems and vulnerabilities.

60. What service is provided by HTTP?

A. Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.

B. Allows for data transfers between a client and a file server.

C. An application that allows real-time chatting among remote users.

D. **A basic set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the web.**

Explanation: Topic 15.3.1 – HTTP is the foundation for exchanging multimedia files on the web.

61. A client packet is received by a server. The packet has a destination port number of 67. What service is the client requesting?

A. FTP

B. **DHCP**

C. Telnet

D. SSH

Explanation: Topic 14.4.3 – Port 67 is used by DHCP servers for client requests.

62. What are two problems that can be caused by a large number of ARP request and reply messages? (Choose two.)

A. Switches become overloaded because they concentrate all the traffic from the attached subnets.

B. The ARP request is sent as a broadcast, and will flood the entire subnet.

C. The network may become overloaded because ARP reply messages have a very large payload.

D. A large number of ARP request and reply messages may slow down the switching process.

E. All ARP request messages must be processed by all nodes on the local network.

Explanation: Topic 9.2.8 – ARP requests are broadcasts that flood the subnet and must be processed by all nodes.

63. A group of Windows PCs in a new subnet has been added to an Ethernet network. When testing the connectivity, a technician finds that these PCs can access local network resources but not the Internet resources. To troubleshoot the problem, the technician wants to initially confirm the IP address and DNS configurations on the PCs, and also verify connectivity to the local router. Which three Windows CLI commands and utilities will provide the necessary information? (Choose three.)

A. netsh interface ipv6 show neighbor

B. arp -a

C. tracert

D. ping

E. ipconfig

F. nslookup

G. telnet

Explanation: Topic 17.5.1 – `ipconfig` displays IP configuration, `ping` tests connectivity, and `nslookup` verifies DNS resolution.

64. 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?

A. analyze the destination IP address

B. switch the packet to the directly connected interface

C. look up the next-hop address for the packet

D. discard the traffic after consulting the route table

Explanation: Topic 8.5.1 – A router receives a packet on an interface and looks at the destination IP address. It consults its routing table and matches the destination IP address to a routing table entry. The router then discovers that it has to send the packet to the next-hop address or out to a directly connected interface. When the destination address is on a directly connected interface, the packet is switched over to that interface.

65. What characteristic describes antispyware?

A. applications that protect end devices from becoming infected with malicious software

B. a network device that filters access and traffic coming into a network

C. software on a router that filters traffic based on IP addresses or applications

D. a tunneling protocol that provides remote users with secure access into the network of an organization

Explanation: Topic 1.8.2 – Antispyware protects end devices from malware infections.

66. A network administrator needs to keep the user ID, password, and session contents private when establishing remote CLI connectivity with a switch to manage it. Which access method should be chosen?

A. Telnet

B. AUX

C. SSH

D. Console

Explanation: Topic 2.1.4 – SSH encrypts all communication, providing secure remote CLI access.

67. What are the two most effective ways to defend against malware? (Choose two.)

A. Implement a VPN.

B. Implement network firewalls.

C. Implement RAID.

D. Implement strong passwords.

E. Update the operating system and other application software.

F. Install and update antivirus software.

Explanation: Topic 16.3.3 – A cybersecurity specialist must be aware of the technologies and measures that are used as countermeasures to protect the organization from threats and vulnerabilities.

68. Which type of security threat would be responsible if a spreadsheet add-on disables the local software firewall?

A. brute-force attack

B. **Trojan horse**

C. DoS

D. buffer overflow

Explanation: Topic 16.2.1 – A Trojan horse is software that does something harmful, but is hidden in legitimate software code. A denial of service (DoS) attack results in interruption of network services to users, network devices, or applications. A brute-force attack commonly involves trying to access a network device. A buffer overflow occurs when a program attempts to store more data in a memory location than it can hold.

69. Which frame field is created by a source node and used by a destination node to ensure that a transmitted data signal has not been altered by interference, distortion, or signal loss?

A. User Datagram Protocol field

B. transport layer error check field

C. flow control field

D. **frame check sequence field**

E. error correction process field

Explanation: Topic 6.3.2 – The FCS field is used for error detection to verify frame integrity.

70. A network administrator is adding a new LAN to a branch office. The new LAN must support 4 connected devices. What is the smallest network mask that the network administrator can use for the new network?

A. 255.255.255.248

B. 255.255.255.0

C. 255.255.255.128

D. 255.255.255.192

Explanation: Topic 11.5.2 – A /29 mask (255.255.255.248) provides 6 usable host addresses, enough for 4 devices.

71. What service is provided by POP3?

A. Retrieves email from the server by downloading the email to the local mail application of the client.

B. An application that allows real-time chatting among remote users.

C. Allows remote access to network devices and servers.

D. Uses encryption to provide secure remote access to network devices and servers.

Explanation: Topic 15.3.4 – POP3 downloads email from the server to the local client application.

72. What two security solutions are most likely to be used only in a corporate environment? (Choose two.)

A. antispyware

B. **virtual private networks**

C. **intrusion prevention systems**

D. strong passwords

E. antivirus software

Explanation: Topic 1.8.2 – VPNs and intrusion prevention systems are typically deployed in corporate environments.

73. What characteristic describes antivirus software?

A. **applications that protect end devices from becoming infected with malicious software**

B. a network device that filters access and traffic coming into a network

C. a tunneling protocol that provides remote users with secure access into the network of an organization

D. software on a router that filters traffic based on IP addresses or applications

Explanation: Topic 1.8.2 – Antivirus software protects end devices from malicious software.

74. What mechanism is used by a router to prevent a received IPv4 packet from traveling endlessly on a network?

A. It checks the value of the TTL field and if it is 0, it discards the packet and sends a Destination Unreachable message.

B. It checks the value of the TTL field and if it is 100, it discards the packet and sends a Destination Unreachable message.

C. **It decrements the value of the TTL field by 1 and if the result is 0, it discards**

the packet and sends a Time Exceeded message to the source host.

D. It increments the value of the TTL field by 1 and if the result is 100, it discards the packet and sends a Parameter Problem message.

Explanation: Topic 8.2.2 – The router decrements the TTL; if it reaches 0, the packet is discarded and a Time Exceeded message is sent.

75. A client packet is received by a server. The packet has a destination port number of 69. What service is the client requesting?

A. DNS

B. DHCP

C. SMTP

D. TFTP

Explanation: Topic 14.4.3 – Port 69 is the well-known port for TFTP (Trivial File Transfer Protocol).

76. An administrator defined a local user account with a secret password on router R1 for use with SSH. Which three additional steps are required to configure R1 to accept only encrypted SSH connections? (Choose three.)

A. Configure DNS on the router.

B. Generate two-way pre-shared keys.

C. Configure the IP domain name on the router.

D. Generate the SSH keys.

E. Enable inbound vty SSH sessions.

F. Enable inbound vty Telnet sessions.

Explanation: Topic 16.4.4 – SSH requires an IP domain name, generated SSH keys, and enabling SSH on the VTY lines.

77. Which two functions are performed at the MAC sublayer of the OSI Data Link Layer to facilitate Ethernet communication? (Choose two.)

A. handles communication between upper layer networking software and Ethernet NIC hardware

B. implements trailer with frame check sequence for error detection

C. places information in the Ethernet frame that identifies which network layer protocol is being encapsulated

D. implements a process to delimit fields within an Ethernet 2 frame

E. adds Ethernet control information to network protocol data

Explanation: Topic 6.1.2 – The MAC sublayer handles framing, error detection (FCS), and delimiting fields within the Ethernet frame.

78. An IPv6 enabled device sends a data packet with the destination address of FF02::2. What is the target of this packet?

A. all IPv6 enabled devices on the local link

B. all IPv6 DHCP servers

C. all IPv6 enabled devices across the network

D. all IPv6 configured routers on the local link

Explanation: Topic 12.7.2 – FF02::2 is the multicast address for all IPv6 routers on the local link.

79. What are the three parts of an IPv6 global unicast address? (Choose three.)

A. subnet ID

B. subnet mask

C. broadcast address

D. global routing prefix

E. interface ID

Explanation: Topic 12.3.5 – The general format for IPv6 global unicast addresses includes a global routing prefix, a subnet ID, and an interface ID. The global routing prefix is the network portion of the address. A typical global routing prefix is /48 assigned by the Internet provider. The subnet ID portion can be used by an organization to create multiple subnetwork numbers. The interface ID is similar to the host portion of an IPv4 address.

80. A network administrator is designing the layout of a new wireless network. Which three areas of concern should be accounted for when building a wireless network? (Choose three.)

A. extensive cabling

B. mobility options

C. packet collision

D. interference

E. security

F. coverage area

Explanation: Topic 4.6.1 – The three areas of concern for wireless networks focus on the size of the coverage area, any nearby interference, and providing network security. Extensive cabling is not a concern for wireless networks, as a wireless network will require minimal cabling for providing wireless access to hosts. Mobility options are not a component of the areas of concern for wireless networks.

81. A new network administrator has been asked to enter a banner message on a Cisco device. What is the fastest way a network administrator could test whether the banner is properly configured?

A. Enter CTRL-Z at the privileged mode prompt.

B. Exit global configuration mode.

C. Power cycle the device.

D. Reboot the device.

E. Exit privileged EXEC mode and press Enter.

Explanation: Topic 2.4.5 – Exiting privileged EXEC mode displays the banner immediately.

82. What method is used to manage contention-based access on a wireless network?

A. token passing

B. CSMA/CA

C. priority ordering

D. CSMA/CD

Explanation: Topic 6.2.8 – Wireless networks use CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

83. What is a function of the data link layer?

A. provides the formatting of data

B. provides end-to-end delivery of data between hosts

C. provides delivery of data between two applications

D. provides for the exchange of frames over a common local media

Explanation: Topic 6.1.1 – The data link layer facilitates frame exchange over the local media.

84. What is the purpose of the TCP sliding window?

A. to ensure that segments arrive in order at the destination

B. to end communication when data transmission is complete

C. to inform a source to retransmit data from a specific point forward

D. to request that a source decrease the rate at which it transmits data

Explanation: Topic 14.6.5 – The TCP sliding window allows a destination device to inform a source to slow down the rate of transmission. To do this, the destination device reduces the value contained in the window field of the segment. It is acknowledgment numbers that are used to specify retransmission from a specific point forward. It is sequence numbers that are used to ensure segments arrive in order. Finally, it is a FIN control bit that is used to end a communication session.

85. What characteristic describes spyware?

A. a network device that filters access and traffic coming into a network

B. software that is installed on a user device and collects information about the user

C. an attack that slows or crashes a device or network service

D. the use of stolen credentials to access private data

Explanation: Topic 1.8.1 – Spyware collects user information without consent.

86. Which switching method drops frames that fail the FCS check?

A. store-and-forward switching

B. borderless switching

C. ingress port buffering

D. cut-through switching

Explanation: Topic 7.4.1 – Store-and-forward switching drops frames that fail the FCS check.

87. Which range of link-local addresses can be assigned to an IPv6-enabled interface?

A. FEC0::/10

B. FDEE::/7

C. FE80::/10

D. FF00::/8

Explanation: Topic 12.3.7 – Link-local addresses are in the range of FE80::/10 to FEBF::/10. The original IPv6 specification defined site-local addresses and used the prefix range FEC0::/10, but these addresses were deprecated by the IETF in favor of unique local addresses. FDEE::/7 is a unique local address because it is in the range of FC00::/7 to FDFF::/7. IPv6 multicast addresses have the prefix FF00::/8.

88. What service is provided by FTP?

A. A basic set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the web.

B. An application that allows real-time chatting among remote users.

C. Allows for data transfers between a client and a file server.

D. Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.

Explanation: Topic 15.5.1 – FTP enables file transfers between a client and a file server.

89. A user is attempting to access http://www.cisco.com/ without success. Which two configuration values must be set on the host to allow this access? (Choose two.)

A. DNS server

B. source port number

C. HTTP server

D. source MAC address

E. default gateway

Explanation: Topic 11.1.2 – A DNS server and a default gateway are required for web access.

90. Which two statements accurately describe an advantage or a disadvantage when deploying NAT for IPv4 in a network? (Choose two.)

A. NAT adds authentication capability to IPv4.

B. NAT introduces problems for some applications that require end-to-end connectivity.

C. NAT will impact negatively on switch performance.

D. NAT provides a solution to slow down the IPv4 address depletion.

E. NAT improves packet handling.

F. NAT causes routing tables to include more information.

Explanation: Topic 12.1.1 – Network Address Translation (NAT) is a technology that is implemented within IPv4 networks. One application of NAT is to use private IP addresses inside a network and use NAT to share a few public IP addresses for many internal hosts. In this way it provides a solution to slow down the IPv4 address depletion. However, since NAT hides the actual IP addresses that are used by end devices, it may cause problems for some applications that require end-to-end connectivity.

91. What would be the interface ID of an IPv6 enabled interface with a MAC address of 1C-6F-65-C2-BD-F8 when the interface ID is generated by using the EUI-64 process?

A. 0C6F:65FF:FEC2:BDF8

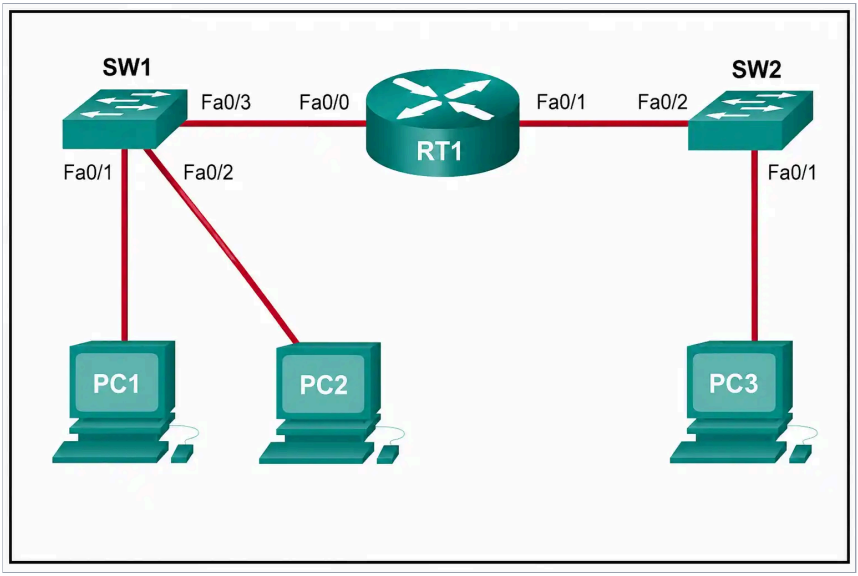
B. **1E6F:65FF:FEC2:BDF8**

C. C16F:65FF:FEC2:BDF8

D. 106F:65FF:FEC2:BDF8

Explanation: Topic 12.5.6 – The EUI-64 process changes the 7th bit (C to E) and inserts FFFE.

92. Refer to the exhibit. PC1 issues an ARP request because it needs to send a packet to PC2. In this scenario, what will happen next?



A. SW1 will send an ARP reply with the SW1 Fa0/1 MAC address.

B. SW1 will send an ARP reply with the PC2 MAC address.

C. **PC2 will send an ARP reply with the PC2 MAC address.**

D. RT1 will send an ARP reply with the RT1 Fa0/0 MAC address.

E. RT1 will send an ARP reply with the PC2 MAC address.

Explanation: Topic 9.2.4 – When a network device wants to communicate with another device on the same network, it sends a broadcast ARP request. In this case, the request will contain the IP address of PC2. The destination device (PC2) sends an ARP reply with its MAC address.

93. What service is provided by BOOTP?

A. Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.

B. Allows for data transfers between a client and a file server.

C. Legacy application that enables a diskless workstation to discover its own IP address and find a BOOTP server on the network.

D. A basic set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the web.

Explanation: Topic 3.3.4 – BOOTP is a legacy protocol for diskless workstations to obtain IP addresses.

94. What characteristic describes adware?

A. a network device that filters access and traffic coming into a network

B. software that is installed on a user device and collects information about the user

C. the use of stolen credentials to access private data

D. an attack that slows or crashes a device or network service

Explanation: Topic 1.8.1 – Adware collects user information and displays unwanted advertisements.

95. When a switch configuration includes a user-defined error threshold on a per-port basis, to which switching method will the switch revert when the error threshold is reached?

A. cut-through

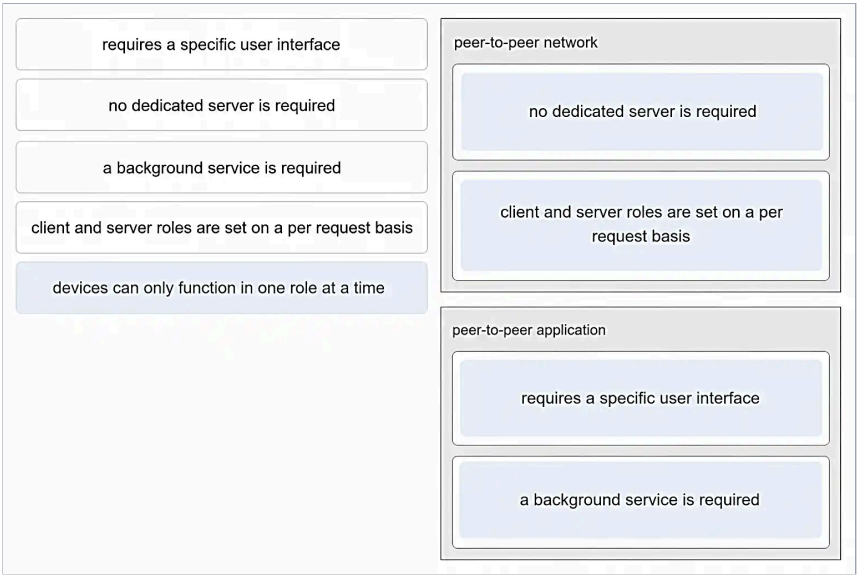
B. store-and-forward

C. fast-forward

D. fragment-free

Explanation: Topic 7.4.2 – When an error threshold is exceeded, the switch reverts to store-and-forward.

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



Explanation: Topic 15.2.2 - 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.

Model	Characteristic
peer-to-peer network	no dedicated server is required
peer-to-peer network	client and server roles are set on a per request basis
peer-to-peer application	requires a specific user interface

peer-to-peer application	a background service is required

97. What are two primary responsibilities of the Ethernet MAC sublayer? (Choose two.)

A. error detection

B. frame delimiting

C. **accessing the media**

D. **data encapsulation**

E. logical addressing

Explanation: Topic 7.1.3 – The MAC sublayer is responsible for media access and data encapsulation.

98. Refer to the exhibit. What three facts can be determined from the viewable output of the show ip interface brief command? (Choose three.)

```
Switch# show ip interface brief
Interface              IP-Address      OK? Method  Status    Protocol
FastEthernet0/1        unassigned      YES manual  up        up
FastEthernet0/2        unassigned      YES manual  down      down
FastEthernet0/3        unassigned      YES manual  down      down
FastEthernet0/5        unassigned      YES manual  down      down
FastEthernet0/6        unassigned      YES manual  down      down

(output omitted)

FastEthernet0/23       unassigned      YES manual  down      down
FastEthernet0/24       unassigned      YES manual  down      down
Vlan1                  192.168.11.3    YES manual  up        up
```

A. Two physical interfaces have been configured.

B. **The switch can be remotely managed.**

C. **One device is attached to a physical interface.**

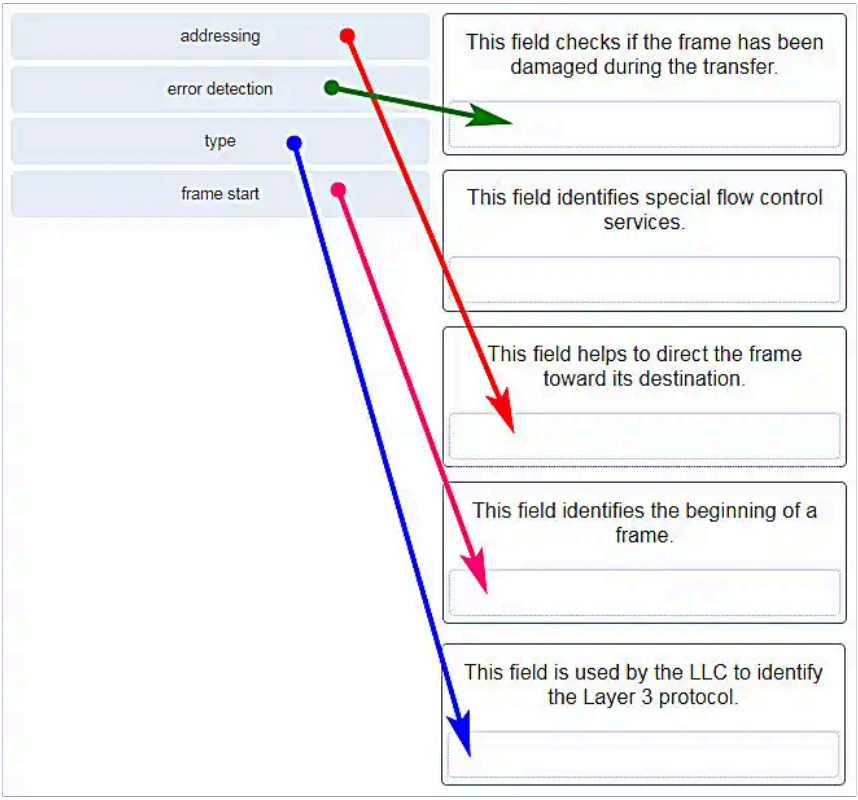
D. Passwords have been configured on the switch.

E. Two devices are attached to the switch.

F. **The default SVI has been configured.**

Explanation: Topic 17.5.7 – Vlan1 is the default SVI. Because an SVI has been configured, the switch can be configured and managed remotely. FastEthernet0/0 is showing up and up, so a device is connected.

99. Match each type of frame field to its function. (Not all options are used.)



Explanation: Topic 6.3.2

Field	Function
addressing	This field helps to direct the frame toward its destination.
error detection	This field checks if the frame has been damaged during the transfer.
type	This field is used by the LLC to identify the Layer 3 protocol.
frame start	This field identifies the beginning of a frame.

100. What is the subnet ID associated with the IPv6 address 2001:DA48:FC5:A4:3D1B::1/64?

A. 2001:DA48::/64

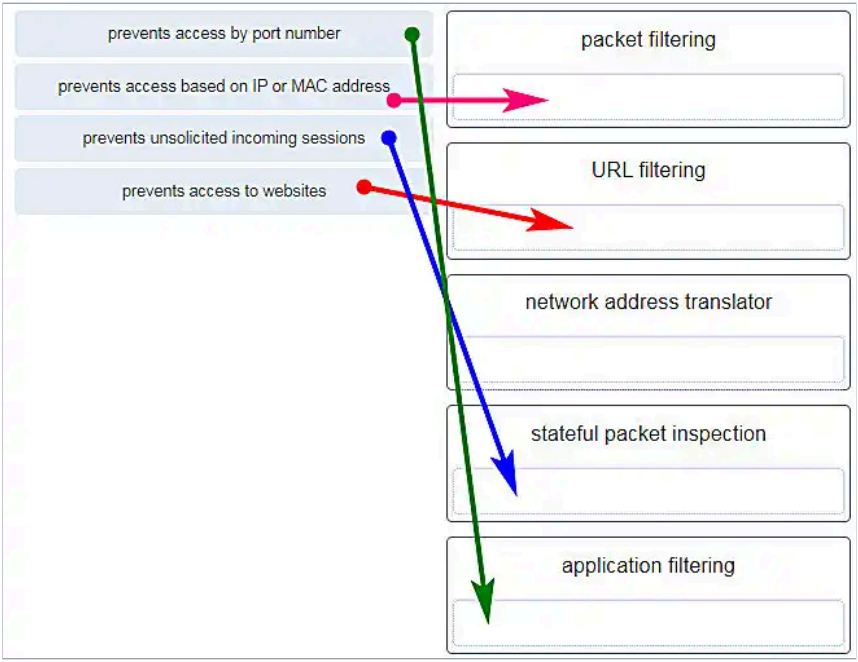
B. 2001:DA48:FC5::A4:/64

C. **2001:DA48:FC5:A4::/64**

D. 2001::/64

Explanation: Topic 12.3.6 – The subnet ID for a /64 prefix includes the first 64 bits of the address.

101. Match the firewall function to the type of threat protection it provides to the network. (Not all options are used.)



Explanation: Topic 16.3.6 - Firewall products come packaged in various forms. These products use different techniques for determining what will be permitted or denied access to a network. They include the following:
+ Packet filtering – Prevents or allows access based on IP or MAC addresses
+ Application filtering – Prevents or allows access by specific application types based on port numbers
+ URL filtering – Prevents or allows access to websites based on specific URLs or keywords
+ Stateful packet inspection (SPI) – Incoming packets must be legitimate responses to requests from internal hosts. Unsolicited packets are blocked unless permitted specifically. SPI can also include the capability to recognize and filter out specific types of attacks, such as denial of service (DoS)

Function	Protection Type
prevents access by port number	application filtering
prevents access based on IP or MAC address	packet filtering
prevents unsolicited incoming sessions	stateful packet inspection
prevents access to websites	URL filtering

102. Users are reporting longer delays in authentication and in accessing network resources during certain time periods of the week. What kind of information should network engineers check to find out if this situation is part of a normal network behavior?

A. syslog records and messages

B. **the network performance baseline**

C. debug output and packet captures

D. network configuration files

Explanation: Topic 17.4.5 – A network performance baseline helps determine if delays are normal or abnormal.

103. How does the service password-encryption command enhance password security on Cisco routers and switches?

A. It requires encrypted passwords to be used when connecting remotely with Telnet.

B. It encrypts passwords that are stored in router or switch configuration files.

C. It requires that a user type encrypted passwords to gain console access.

D. It encrypts passwords as they are sent across the network.

Explanation: Topic 2.4.4 – The service password-encryption command encrypts plaintext passwords in the configuration file so that they cannot be viewed by unauthorized users.

104. Which two statements are correct in a comparison of IPv4 and IPv6 packet headers? (Choose two.)

A. The Source Address field name from IPv4 is kept in IPv6.

B. The Version field from IPv4 is not kept in IPv6.

C. The Destination Address field is new in IPv6.

D. The Header Checksum field name from IPv4 is kept in IPv6.

E. The Time-to-Live field from IPv4 has been replaced by the Hop Limit field in IPv6.

Explanation: Topic 8.3.3 – The IPv6 packet header fields are as follows: Version, Traffic Class, Flow Label, Payload Length, Next Header, Hop Limit, Source Address, and Destination Address. The IPv4 packet header fields include the following: Version, Differentiated Services, Time-to-Live, Protocol, Source IP Address, and Destination IP Address. Both versions have a 4-bit Version field. Both versions have a Source (IP) Address field. IPv4 addresses are 32 bits; IPv6 addresses are 128 bits. The Time-to-Live or TTL field in IPv4 is now called Hop Limit in IPv6, but this field serves the same purpose in both versions. The value in this 8-bit field decrements each time a packet

passes through any router. When this value is 0, the packet is discarded and is not forwarded to any other router.

105. 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?

A. 255.255.255.192

B. 255.255.255.252

C. 255.255.255.240

D. 255.255.255.248

E. 255.255.255.0

F. **255.255.255.224**

Explanation: Topic 11.7.2 – A /27 mask (255.255.255.224) provides 30 usable addresses per subnet, enough for the largest requirement (22 IP phones).

106. What characteristic describes identity theft?

A. **the use of stolen credentials to access private data**

B. software on a router that filters traffic based on IP addresses or applications

C. software that identifies fast-spreading threats

D. a tunneling protocol that provides remote users with secure access

Explanation: Topic 1.8.1 – Identity theft involves using stolen credentials to access private data.

107. A network administrator is adding a new LAN to a branch office. The new LAN must support 200 connected devices. What is the smallest network mask that the network administrator can use for the new network?

A. 255.255.255.240

B. **255.255.255.0**

C. 255.255.255.248

D. 255.255.255.224

Explanation: Topic 11.7.2 – A /24 mask (255.255.255.0) provides 254 usable host addresses, enough for 200 devices.

108. What are three commonly followed standards for constructing and installing cabling? (Choose three.)

A. cost per meter (foot)

B. **cable lengths**

C. connector color

D. **pinouts**

E. **connector types**

F. tensile strength of plastic insulator

Explanation: Topic 4.4.2 – Standards cover cable lengths, pinouts, and connector types.

109. Refer to the exhibit. What is wrong with the displayed termination?

A. The woven copper braid should not have been removed.

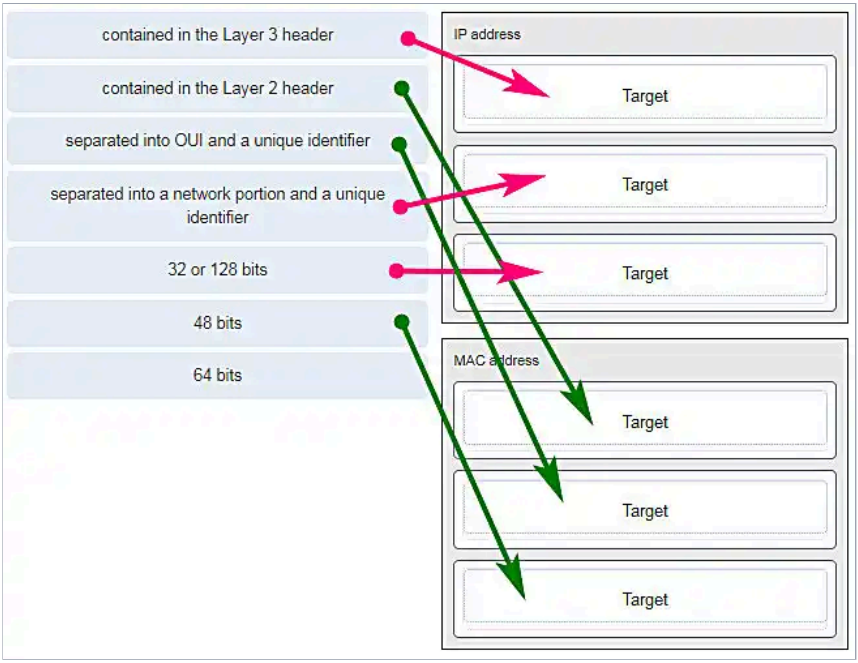
B. The wrong type of connector is being used.

C. **The untwisted length of each wire is too long.**

D. The wires are too thick for the connector that is used.

Explanation: Topic 4.4.2 – The untwisted length must be kept short to avoid crosstalk.

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



Explanation: Topic 9.1.1

IP address	MAC address
contained in the Layer 3 header	contained in the Layer 2 header
separated into a network portion and a unique identifier	separated into OUI and a unique identifier
32 or 128 bits	48 bits

111. A client packet is received by a server. The packet has a destination port number of 143. What service is the client requesting?

A. IMAP

B. FTP

C. SSH

D. Telnet

Explanation: Topic 14.4.3 – Port 143 is the well-known port for IMAP email retrieval.

112. What are two characteristics shared by TCP and UDP? (Choose two.)

A. default window size

B. connectionless communication

C. **port numbering**

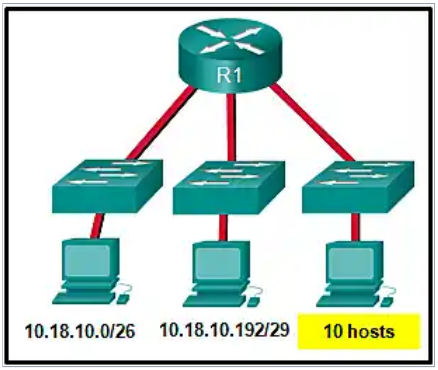
D. 3-way handshake

E. ability to carry digitized voice

F. **use of checksum**

Explanation: Topic 14.1.2 – Both TCP and UDP use source and destination port numbers to distinguish different data streams and to forward the right data segments to the right applications. Error checking the header and data is done by both protocols by using a checksum calculation to determine the integrity of the data that is received. TCP is connection-oriented and uses a 3-way handshake to establish an initial connection. TCP also uses window to regulate the amount of traffic sent before receiving an acknowledgment. UDP is connectionless and is the best protocol for carry digitized VoIP signals.

113. Refer to the exhibit. Which two network addresses can be assigned to the network containing 10 hosts? Your answers should waste the fewest addresses, not reuse addresses that are already assigned, and stay within the 10.18.10.0/24 range of addresses. (Choose two.)



A. 10.18.10.200/28

B. **10.18.10.208/28**

C. 10.18.10.240/27

D. 10.18.10.200/27

E. 10.18.10.224/27

F. **10.18.10.224/28**

Explanation: Topic 11.7.2 – Addresses 10.18.10.0 through 10.18.10.63 are taken for the leftmost network. Addresses 192 through 199 are used by the center network. Because 4 host bits are needed to accommodate 10 hosts, a /28 mask is needed. 10.18.10.200/28 is not a valid network number. Two subnets that can be used are 10.18.10.208/28 and 10.18.10.224/28.

114. A client packet is received by a server. The packet has a destination port number of 21. What service is the client requesting?

A. **FTP**

B. LDAP

C. SLP

D. SNMP

Explanation: Topic 14.4.3 – Port 21 is the well-known port for FTP control.

115. What attribute of a NIC would place it at the data link layer of the OSI model?

A. attached Ethernet cable

B. IP address

C. **MAC address**

D. RJ-45 port

E. TCP/IP protocol stack

Explanation: Topic 7.2.2 – The MAC address is a data link layer attribute.

116. A network administrator is adding a new LAN to a branch office. The new LAN must support 10 connected devices. What is the smallest network mask that the network administrator can use for the new network?

A. 255.255.255.192

B. 255.255.255.248

C. 255.255.255.224

D. **255.255.255.240**

Explanation: Topic 11.5.2 – A /28 mask (255.255.255.240) provides 14 usable host addresses, enough for 10 devices.

117. What technique is used with UTP cable to help protect against signal interference from crosstalk?

A. wrapping a foil shield around the wire pairs

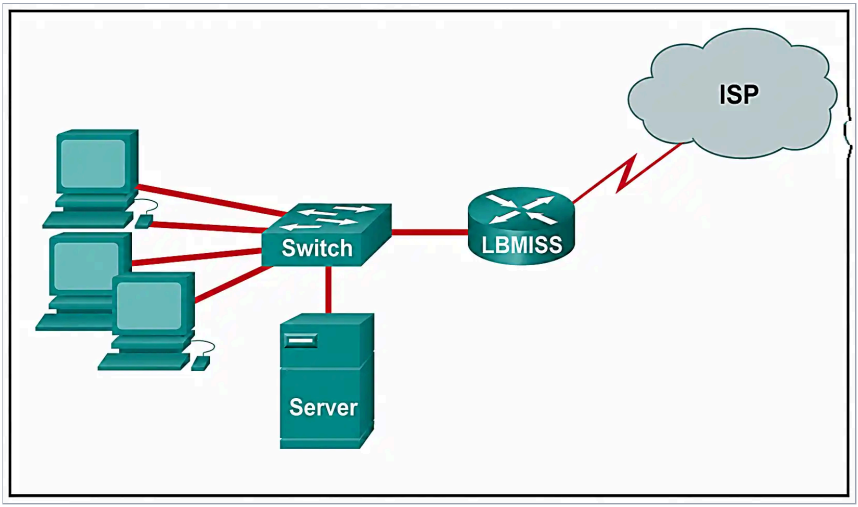
B. **twisting the wires together into pairs**

C. terminating the cable with special grounded connectors

D. encasing the cables within a flexible plastic sheath

Explanation: Topic 4.4.1 – To help prevent the effects of crosstalk, UTP cable wires are twisted together into pairs. Twisting the wires together causes the magnetic fields of each wire to cancel each other out.

118. 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?



A. IP address: 192.168.10.65 subnet mask: 255.255.255.240, default gateway: 192.168.10.76

B. IP address: 192.168.10.38 subnet mask: 255.255.255.240, default gateway: 192.168.10.33

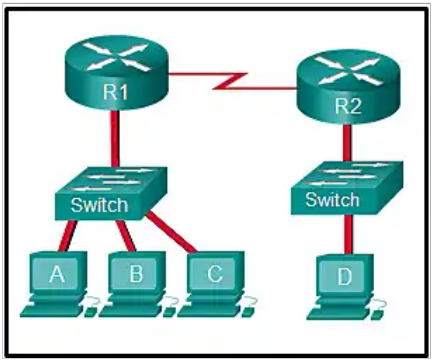
C. IP address: 192.168.10.38 subnet mask: 255.255.255.248, default gateway: 192.168.10.33

D. IP address: 192.168.10.41 subnet mask: 255.255.255.248, default gateway: 192.168.10.46

E. IP address: 192.168.10.254 subnet mask: 255.255.255.0, default gateway: 192.168.10.1

Explanation: Topic 11.5.2 – The fifth subnet (192.168.10.32/29) has a range of 33–38; the router gets 33 and the server gets 38.

119. Refer to the exhibit. The switches are in their default configuration. Host A needs to communicate with host D, but host A does not have the MAC address for its default gateway. Which network hosts will receive the ARP request sent by host A?



A. only host D

B. only router R1

C. only hosts A, B, and C

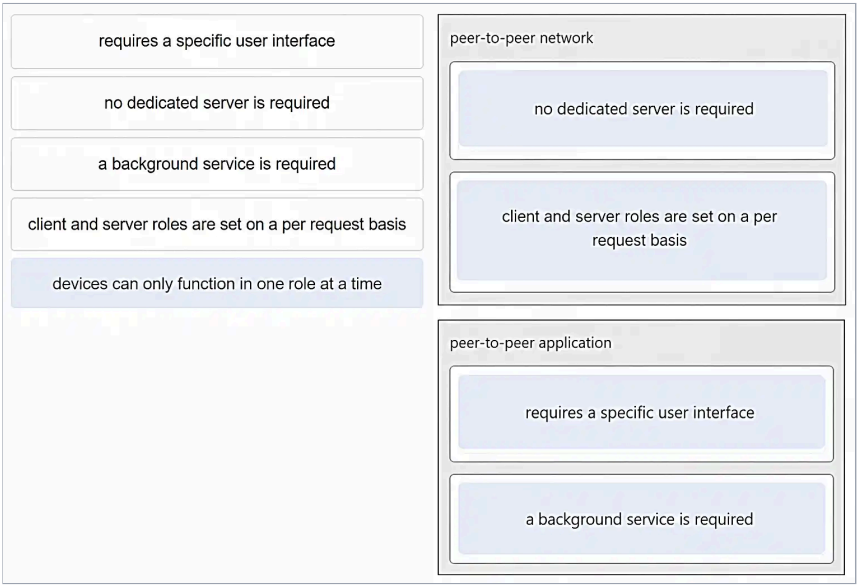
D. only hosts A, B, C, and D

E. only hosts B and C

F. **only hosts B, C, and router R1**

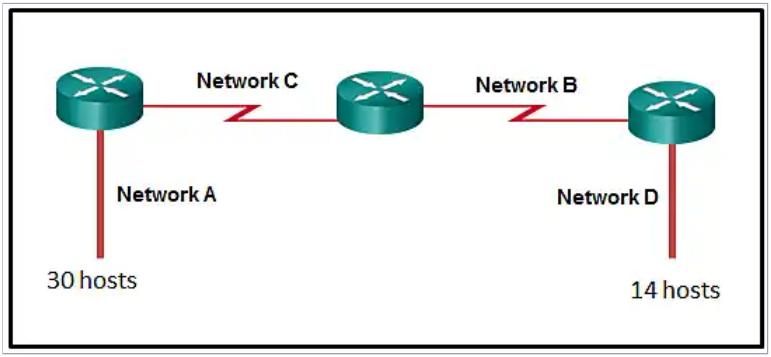
Explanation: Topic 11.4.1 – Since host A does not have the MAC address of the default gateway in its ARP table, host A sends an ARP broadcast. The ARP broadcast would be sent to every device on the local network. Hosts B, C, and router R1 would receive the broadcast. Router R1 would not forward the message.

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



Explanation: Topic 5.2 - 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.

121. Refer to the exhibit. A network engineer has been given the network address of 192.168.99.0 and a subnet mask of 255.255.255.192 to subnet across the four networks shown. How many total host addresses are unused across all four subnets?



A. 88

B. **200**

C. 72

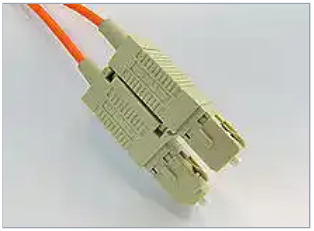
D. 224

E. 158

Explanation: Topic 11.5.2 – Each /26 subnet provides 62 usable addresses; total unused across four subnets is 200.

122. Which connector is used with twisted-pair cabling in an Ethernet LAN?

LC conector



SC conector

BNC

RJ 11

RJ 45 (true answer)

Explanation: Topic 4.4.2 – RJ-45 connectors are used with twisted-pair cabling in Ethernet LANs.
Answer: RJ-45

123. A client packet is received by a server. The packet has a destination port number of 22. What service is the client requesting?

A. SSH

B. SMB/CIFS

C. HTTPS

D. SLP

Explanation: Topic 14.4.3 – Port 22 is the well-known port for SSH.

124. What characteristic describes an IPS?

A. a tunneling protocol that provides remote users with secure access

B. a network device that filters access and traffic coming into a network

C. software that identifies fast-spreading threats

D. software on a router that filters traffic based on IP addresses or applications

Explanation: Topic 1.8.2 – IPS – An intrusion prevention system (IPS) monitors incoming and outgoing traffic looking for malware, network attack signatures, and more. If it recognizes a threat, it can immediately stop it.

125. What service is provided by DHCP?

A. An application that allows real-time chatting among remote users.

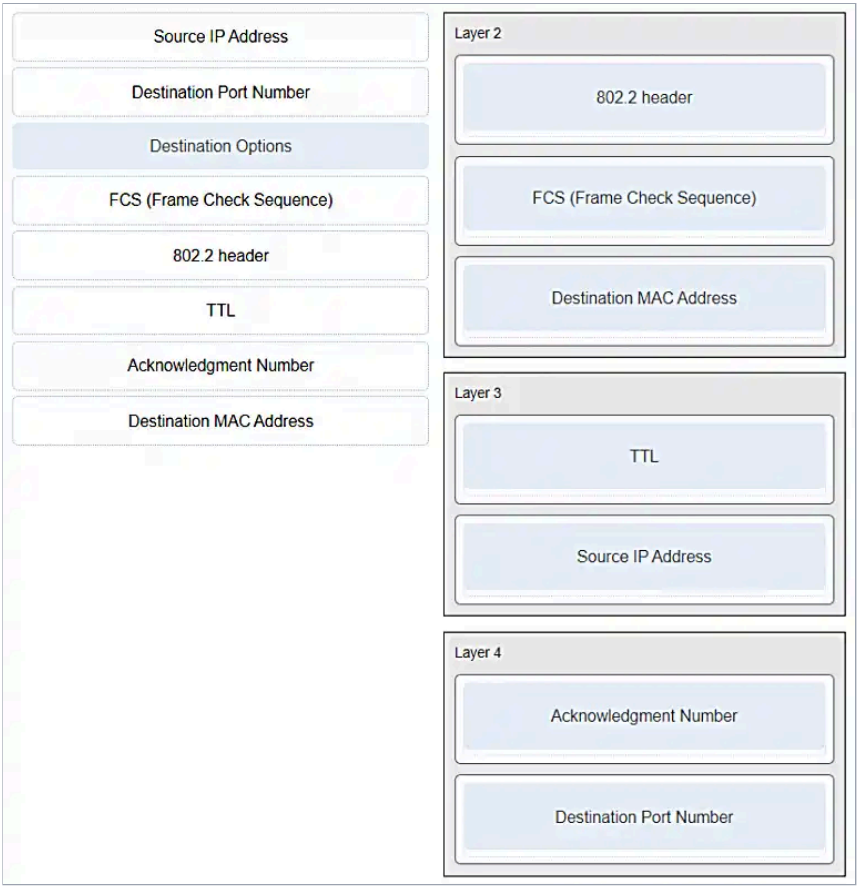
B. Allows remote access to network devices and servers.

C. **Dynamically assigns IP addresses to end and intermediary devices.**

D. Uses encryption to provide secure remote access to network devices and servers.

Explanation: Topic 15.4.6 – DHCP dynamically assigns IP addresses to devices.

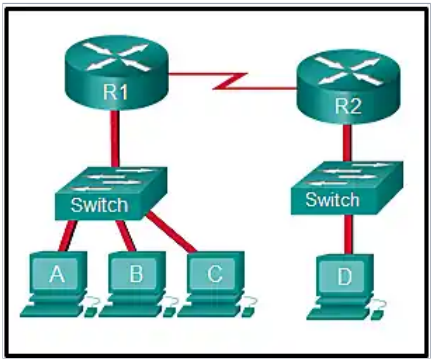
126. Match the header field with the appropriate layer of the OSI model. (Not all options are used.)



Explanation: Topic 3.6.3

Layer 2	Layer 3	Layer 4
802.2 header	source IP address	destination port number
FCS (frame check sequence)	TTL	Acknowledgement number
destination MAC address		

127. Refer to the exhibit. The switches have a default configuration. Host A needs to communicate with host D, but host A does not have the MAC address for the default gateway. Which network devices will receive the ARP request sent by host A?



A. only host D

B. only hosts A, B, C, and D

C. only hosts B and C

D. **only hosts B, C, and router R1**

E. only hosts A, B, and C

F. only router R1

Explanation: Topic 11.4.1 – Because host A does not have the MAC address of the default gateway in the ARP table, host A sends an ARP broadcast. The ARP broadcast would be sent to every device on the local network. Hosts B, C, and router R1 would receive the broadcast. Router R1 would not forward the message.

128. Which wireless technology has low-power and low-data rate requirements making it popular in IoT environments?

A. Bluetooth

B. Zigbee

C. WiMAX

D. Wi-Fi

Explanation: Topic 4.6.2 – Zigbee is a specification used for low-data rate, low-power communications. It is intended for applications that require short-range, low data-rates and long battery life. Zigbee is typically used for industrial and Internet of Things (IoT) environments such as wireless light switches and medical device data collection.

129. What two ICMPv6 message types must be permitted through IPv6 access control lists to allow resolution of Layer 3 addresses to Layer 2 MAC addresses? (Choose two.)

A. neighbor solicitations

B. echo requests

C. neighbor advertisements

D. echo replies

E. router solicitations

F. router advertisements

Explanation: Topic 9.3.3 – Neighbor Solicitation and Neighbor Advertisement messages are used for IPv6 address resolution.

130. A client is using SLAAC to obtain an IPv6 address for its interface. After an address has been generated and applied to the interface, what must the client do before it can begin to use this IPv6 address?

A. It must send a DHCPv6 INFORMATION-REQUEST message to request the address of the DNS server.

B. It must send a DHCPv6 REQUEST message to the DHCPv6 server to request permission to use this address.

C. It must send an ICMPv6 Router Solicitation message to determine what default gateway it should use.

D. It must send an ICMPv6 Neighbor Solicitation message to ensure that the address is not already in use on the network.

Explanation: Topic 12.5.7 – The client performs Duplicate Address Detection (DAD) using Neighbor Solicitation.

131. Two pings were issued from a host on a local network. The first ping was issued to the IP address of the default gateway of the host and it failed. The second ping was issued to the IP address of a host outside the local network and it was successful. What is a possible cause for the failed ping?

A. The default gateway is not operational.

B. The default gateway device is configured with the wrong IP address.

C. Security rules are applied to the default gateway device, preventing it from processing ping requests.

D. The TCP/IP stack on the default gateway is not working properly.

Explanation: Topic 13.2.3 – Security rules may block ICMP ping requests to the gateway.

132. An organization is assigned an IPv6 address block of 2001:db8:0:ca00::/56. How many subnets can be created without using bits in the interface ID space?

A. 256

B. 512

C. 1024

D. 4096

Explanation: Topic 12.8.1 – A /56 prefix provides 8 subnet bits (64-56=8), allowing 2^8=256 subnets.

133. What subnet mask is needed if an IPv4 network has 40 devices that need IP addresses and address space is not to be wasted?

A. 255.255.255.0

B. 255.255.255.240

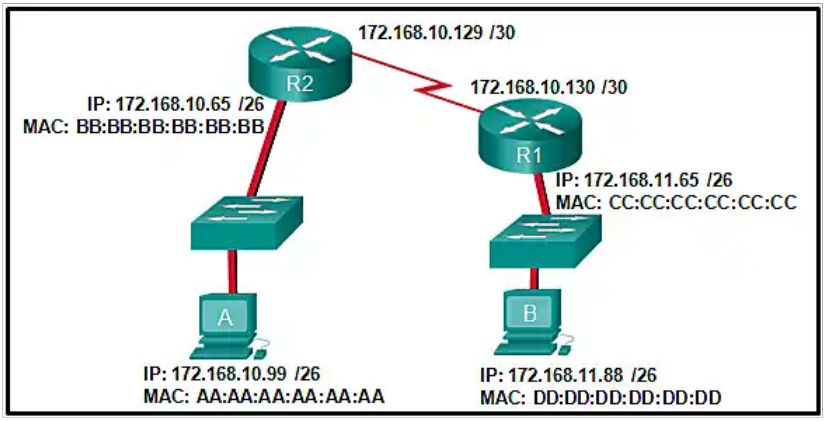
C. 255.255.255.128

D. **255.255.255.192**

E. 255.255.255.224

Explanation: Topic 11.5.2 – In order to accommodate 40 devices, 6 host bits are needed. With 6 bits, 64 addresses are possible, but one address is for the subnet number and one address is for a broadcast. This leaves 62 addresses that can be assigned to network devices. The mask associated with leaving 6 host bits for addressing is 255.255.255.192.

134. Refer to the exhibit. If host A sends an IP packet to host B, what will the destination address be in the frame when it leaves host A?



A. DD:DD:DD:DD:DD:DD

B. 172.168.10.99

C. CC:CC:CC:CC:CC:CC

D. 172.168.10.65

E. **BB:BB:BB:BB:BB:BB**

F. AA:AA:AA:AA:AA:AA

Explanation: Topic 9.1.2 – When a host sends information to a distant network, the Layer 2 frame header will contain a source and destination MAC address. The source address will be the originating host device. The destination address will be the router interface that connects to the same network. In the case of host A sending information to host B, the source address is AA:AA:AA:AA:AA:AA and the destination address is the MAC address assigned to the R2 Ethernet interface, BB:BB:BB:BB:BB:BB.

135. What is a benefit of using cloud computing in networking?

A. Technology is integrated into everyday appliances allowing them to interconnect with other devices, making them more 'smart' or automated.

B. **Network capabilities are extended without requiring investment in new infrastructure, personnel, or software.**

C. End users have the freedom to use personal tools to access information and communicate across a business network.

D. Home networking uses existing electrical wiring to connect devices to the network wherever there is an electrical outlet.

Explanation: Topic 1.7.6 – Cloud computing extends IT's capabilities without requiring investment in new infrastructure, training new personnel, or licensing new software. These services are available on-demand and delivered economically to any device anywhere in the world without compromising security or function. BYOD is about end users having the freedom to use personal tools to access information and communicate across a business or campus network. Smart home technology is integrated into every-day appliances allowing them to interconnect with other devices, making them more 'smart' or automated. Powerline networking is a trend for home networking that uses existing electrical wiring to connect devices to the network wherever there is an electrical outlet, saving the cost of installing data cables.

136. Which two statements are correct about MAC and IP addresses during data transmission if NAT is not involved? (Choose two.)

A. Destination IP addresses in a packet header remain constant along the entire path to a target host.

B. Destination MAC addresses will never change in a frame that goes across seven routers.

C. Every time a frame is encapsulated with a new destination MAC address, a new destination IP address is needed.

D. Destination and source MAC addresses have local significance and change every time a frame goes from one LAN to another.

E. A packet that has crossed four routers has changed the destination IP address four times.

Explanation: Topic 9.1.2 – IP addresses remain constant end-to-end; MAC addresses change at each hop.

137. What is one main characteristic of the data link layer?

A. It generates the electrical or optical signals that represent the 1 and 0 on the media.

B. It converts a stream of data bits into a predefined code.

C. It shields the upper layer protocol from being aware of the physical medium to be used in the communication.

D. It accepts Layer 3 packets and decides the path by which to forward the packet to a remote network.

Explanation: Topic 6.1.1 – The data link layer abstracts the physical medium from upper layers.

138. What are three characteristics of the CSMA/CD process? (Choose three.)

A. The device with the electronic token is the only one that can transmit after a collision.

B. A device listens and waits until the media is not busy before transmitting.

C. After detecting a collision, hosts can attempt to resume transmission after a random time delay has expired.

D. All of the devices on a segment see data that passes on the network medium.

E. A jam signal indicates that the collision has cleared and the media is not busy.

F. Devices can be configured with a higher transmission priority.

Explanation: Topic 6.2.7 – The Carrier Sense Multiple Access/Collision Detection (CSMA/CD) process is a contention-based media access control mechanism used on shared media access networks, such as Ethernet. When a device needs to transmit data, it listens and waits until the media is available (quiet), then it will send data. If two devices transmit at the same time, a collision will occur. Both devices will detect

the collision on the network. When a device detects a collision, it will stop the data transmission process, wait for a random amount of time, then try again.

139. Which information does the show startup-config command display?

A. the IOS image copied into RAM

B. the bootstrap program in the ROM

C. the contents of the current running configuration file in the RAM

D. the contents of the saved configuration file in the NVRAM

Explanation: Topic 2.5.1 – The show startup-config command displays the saved configuration located in NVRAM. The show running-config command displays the contents of the currently running configuration file located in RAM.

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

A. netstat -s

B. route print

C. show ip route

D. netstat -r

E. tracert

Explanation: Topic 8.4.4 – On a Windows host, the route print or netstat -r commands can be used to display the host routing table. Both commands generate the same output. On a router, the show ip route command is used to display the routing table. The netstat –s command is used to display per-protocol statistics. The tracert command is used to display the path that a packet travels to its destination.

141. What are two functions that are provided by the network layer? (Choose two.)

A. directing data packets to destination hosts on other networks

B. placing data on the network medium

C. carrying data between processes that are running on source and destination hosts

D. providing dedicated end-to-end connections

E. providing end devices with a unique network identifier

Explanation: Topic 8.1.1 – The network layer is primarily concerned with passing data from a source to a destination on another network. IP addresses supply unique identifiers for the source and destination. The network layer provides connectionless, best-effort delivery. Devices rely on higher layers to supply services to processes.

142. Which two statements describe features of an IPv4 routing table on a router? (Choose two.)

A. Directly connected interfaces will have two route source codes in the routing table: C and S.

B. If there are two or more possible routes to the same destination, the route associated with the higher metric value is included in the routing table.

C. The netstat -r command can be used to display the routing table of a router.

D. The routing table lists the MAC addresses of each active interface.

E. It stores information about routes derived from the active router interfaces.

F. If a default static route is configured in the router, an entry will be included in the routing table with source code S.

Explanation: Topic 8.5.6 – The routing table stores route information and includes static routes with source code S.

143. What characteristic describes a VPN?

A. software on a router that filters traffic based on IP addresses or applications

B. software that identifies fast-spreading threats

C. a tunneling protocol that provides remote users with secure access into the network of an organization

D. a network device that filters access and traffic coming into a network

Explanation: Topic 1.8.2 – A VPN provides secure remote access to an organization's network.

144. Why would a Layer 2 switch need an IP address?

A. to enable the switch to send broadcast frames to attached PCs

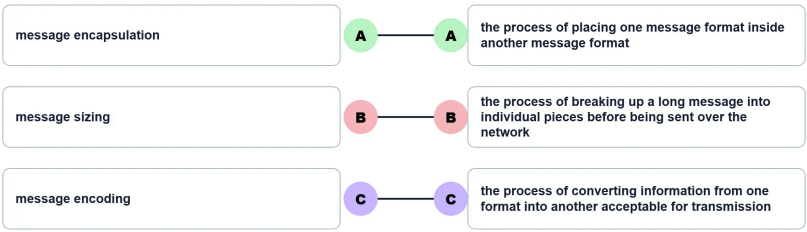
B. to enable the switch to function as a default gateway

C. to enable the switch to be managed remotely

D. to enable the switch to receive frames from attached PCs

Explanation: Topic 10.3.2 – A switch, as a Layer 2 device, does not need an IP address to transmit frames to attached devices. However, when a switch is accessed remotely through the network, it must have a Layer 3 address. The IP address must be applied to a virtual interface rather than to a physical interface. Routers, not switches, function as default gateways.

145. Match each description to its corresponding term. (Not all options are used.)



Explanation: Topic 3.1.5

Term	Description
message encapsulation	the process of placing one message format inside another message format
message sizing	the process of breaking up a long message into individual pieces before being sent over the network
message encoding	the process of converting information from one format into another acceptable for transmission

146. A user sends an HTTP request to a web server on a remote network. During encapsulation for this request, what information is added to the address field of a frame to indicate the destination?

A. the network domain of the destination host

B. the IP address of the default gateway

C. the MAC address of the destination host

D. **the MAC address of the default gateway**

Explanation: Topic 9.1.2 – A frame is encapsulated with source and destination MAC addresses. The source device will not know the MAC address of the remote host. An ARP request will be sent by the source and will be responded to by the router. The router will respond with the MAC address of its interface, the one which is connected to the same network as the source.

147. What is an advantage to using a protocol that is defined by an open standard?

A. A company can monopolize the market.

B. The protocol can only be run on equipment from a specific vendor.

C. An open standard protocol is not controlled or regulated by standards organizations.

D. It encourages competition and promotes choices.

Explanation: Topic 3.4.1 – A monopoly by one company is not a good idea from a user point of view. If a protocol can only be run on one brand, it makes it difficult to have mixed equipment in a network. A proprietary protocol is not free to use. An open standard protocol will in general be implemented by a wide range of vendors.

148. Data is being sent from a source PC to a destination server. Which three statements correctly describe the function of TCP or UDP in this situation? (Choose three.)

A. The source port field identifies the running application or service that will handle data returning to the PC.

B. The TCP process running on the PC randomly selects the destination port when establishing a session with the server.

C. UDP segments are encapsulated within IP packets for transport across the network.

D. The UDP destination port number identifies the application or service on

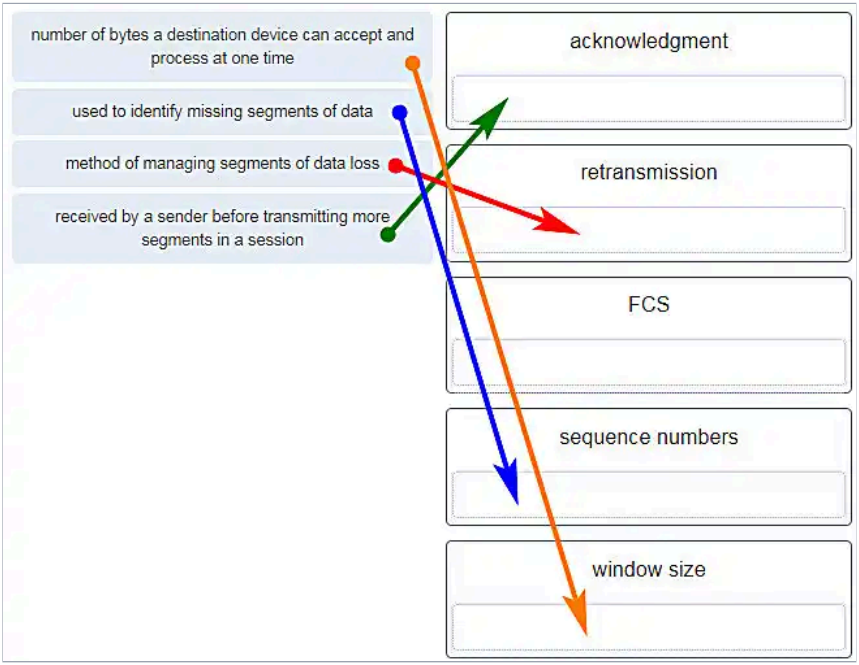
the server which will handle the data.

E. TCP is the preferred protocol when a function requires lower network overhead.

F. The TCP source port number identifies the sending host on the network.

Explanation: Topic 14.4.2 – Layer 4 port numbers identify the application or service which will handle the data. The source port number is added by the sending device and will be the destination port number when the requested information is returned. Layer 4 segments are encapsulated within IP packets. UDP, not TCP, is used when low overhead is needed. A source IP address, not a TCP source port number, identifies the sending host on the network. Destination port numbers are specific ports that a server application or service monitors for requests.

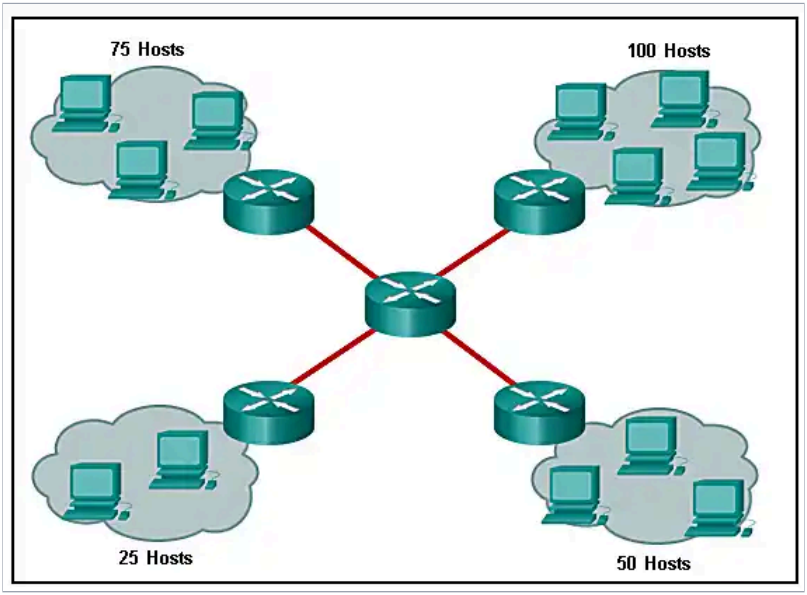
149. Match each description with the corresponding TCP mechanism. (Not all options are used.)



Explanation: Topic 14.6

Description	Mechanism
number of bytes a destination device can accept and process at one time	window size
used to identify missing segments of data	sequence numbers
method of managing segments of data loss	retransmission
received by a sender before transmitting more segments in a session	acknowledgment

150. 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?



A. 255.255.255.192

B. 255.255.255.0

C. **255.255.255.128**

D. 255.255.255.240

E. 255.255.255.224

Explanation: Topic 11.7.2 – 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.

151. A network administrator wants to have the same subnet mask for three subnetworks at a small site. The site has the following networks and numbers of devices:
Subnetwork A: IP phones – 10 addresses,
Subnetwork B: PCs – 8 addresses,
Subnetwork C: Printers – 2 addresses.
What single subnet mask would be appropriate to use for the three subnetworks?

A. 255.255.255.0

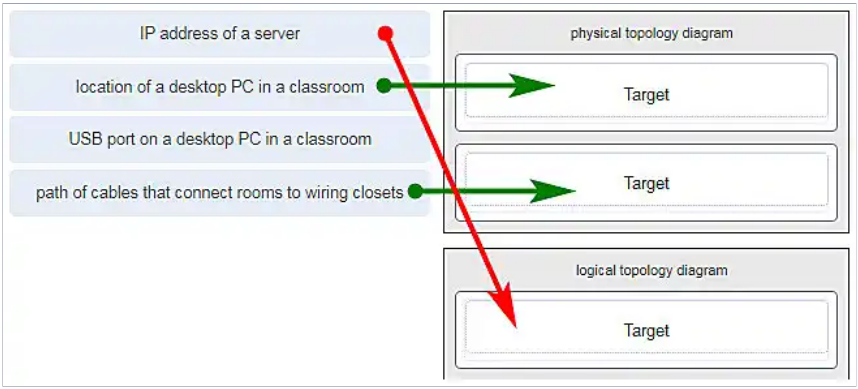
B. **255.255.255.240**

C. 255.255.255.248

D. 255.255.255.252

Explanation: Topic 11.7.2 – If the same mask is to be used, then the network with the most hosts must be examined for number of hosts. Because this is 10 hosts, 4 host bits are needed. The /28 or 255.255.255.240 subnet mask would be appropriate to use for these networks.

152. Match each item to the type of topology diagram on which it is typically identified. (Not all options are used.)



Explanation: Topic 1.3.2 - A logical topology diagram typically depicts the IP addressing scheme and groupings of devices and ports. A physical topology diagram shows how those devices are connected to each other and the network, focusing on the physical locations of intermediary devices, configured ports, and cabling.

physical topology diagram	logical topology diagram
location of a desktop PC in a classroom	IP address of a server
path of cables that connect rooms to wiring closets	

153. What two pieces of information are displayed in the output of the show ip interface brief command? (Choose two.)

A. IP addresses

B. interface descriptions

C. MAC addresses

D. next-hop addresses

E. Layer 1 statuses

F. speed and duplex settings

Explanation: Topic 10.2.3 – The command show ip interface brief shows the IP address of each interface, as well as the operational status of the interfaces at both

Layer 1 and Layer 2. In order to see interface descriptions and speed and duplex settings, use the command show running-config interface. Next-hop addresses are displayed in the routing table with the command show ip route, and the MAC address of an interface can be seen with the command show interfaces.

154. A user is complaining that an external web page is taking longer than normal to load. The web page does eventually load on the user machine. Which tool should the technician use with administrator privileges in order to locate where the issue is in the network?

A. ping

B. nslookup

C. **tracert**

D. ipconfig /displaydns

Explanation: Topic 17.4.3 – `tracert` maps the path and measures transit delays.

155. Which value, that is contained in an IPv4 header field, is decremented by each router that receives a packet?

A. Header Length

B. Differentiated Services

C. **Time-to-Live**

D. Fragment Offset

Explanation: Topic 8.2.2 – When a router receives a packet, the router will decrement the Time-to-Live (TTL) field by one. When the field reaches zero, the receiving router will discard the packet and will send an ICMP Time Exceeded message to the sender.

156. A network technician is researching the use of fiber optic cabling in a new technology center. Which two issues should be considered before implementing fiber optic media? (Choose two.)

A. Fiber optic cabling requires different termination and splicing expertise from what copper cabling requires.

B. Fiber optic cabling requires specific grounding to be immune to EMI.

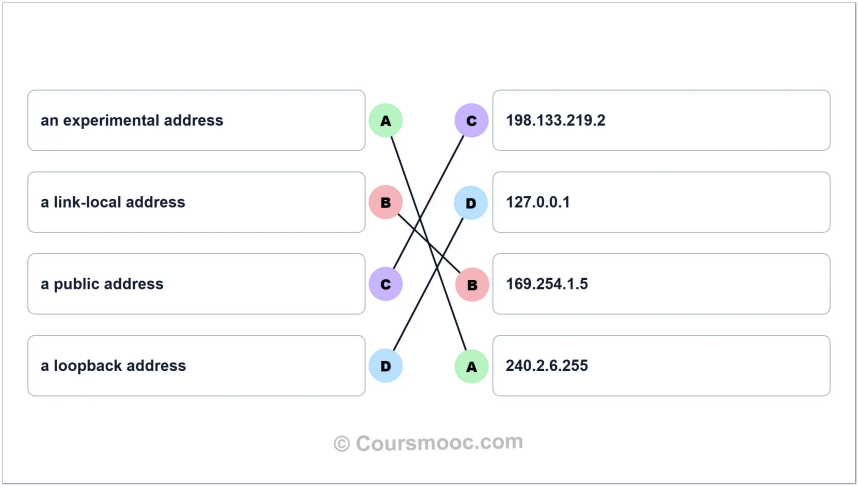
C. Fiber optic cabling is susceptible to loss of signal due to RFI.

D. Fiber optic cable is able to withstand rough handling.

E. Fiber optic provides higher data capacity but is more expensive than copper cabling.

Explanation: Topic 4.5.6 – Fiber optic media is more expensive than copper cabling used over the same distance. Fiber optic cables use light instead of an electrical signal, so EMI and RFI are not issues. However, fiber optic does require different skills to terminate and splice.

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



Explanation: Topic 11.3.4

Description	IP Address
an experimental address	240.2.6.255
a link-local address	169.254.1.5
a public address	198.133.219.2
a loopback address	127.0.0.1

158. 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?

A. when the router receives an ICMP Time Exceeded message

B. when the RTT value reaches zero

C. when the host responds with an ICMP Echo Reply message

D. **when the value in the TTL field reaches zero**

E. when the values of both the Echo Request and Echo Reply messages reach zero

Explanation: Topic 13.1.4 – 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.

159. Users report that the network access is slow. After questioning the employees, the network administrator learned that one employee downloaded a third-party scanning program for the printer. What type of malware might be introduced that causes slow performance of the network?

A. virus

B. **worm**

C. phishing

D. spam

Explanation: Topic 16.2.1 – A cybersecurity specialist needs to be familiar with the characteristics of the different types of malware and attacks that threaten an organization.

CCNA v7.0 Exam Answers

CCNA 1 | CCNA 2 | CCNA 3

- CCNA V7 Introduction
- Modules 1 - 3: Basic Network Connectivity and Communications Exam Answers
- Modules 4 - 7: Ethernet Concepts Exam Answers
- Modules 8 - 10: Communicating Between Networks Exam Answers
- Modules 11 - 13: IP Addressing Exam Answers
- Modules 14 - 15: Network Application Communications Exam Answers
- Modules 16 - 17: Building and Securing a Small Network Exam Answers
- ITN v7 Practice Final Exam
- CCNA 1 v7 Course FINAL Exam Answers →

Popular Exams

- Microsoft exams
- Cisco exams
- All Exams →

Popular Practice Tests

Prev 1 Next

Download PDF

Share this page

Understanding the CCNA 1 v7.0 Final Exam – Introduction to Networks

Passing the CCNA 1 v7.0 Final Exam requires a comprehensive understanding of networking fundamentals, from the OSI and TCP/IP models to Ethernet, IP addressing, routing, and network security. This final exam covers the entire **Introduction to Networks (ITNv7)** curriculum, testing your knowledge on all 17 modules.

Why the Final Exam Matters for Your Networking Career

The CCNA 1 v7.0 Final Exam is the culmination of the Introduction to Networks course. It validates your understanding of **network fundamentals, OSI and TCP/IP models, Ethernet concepts, IP addressing, routing, ARP, and basic network security**. Passing this exam demonstrates that you have the foundational knowledge required for more advanced CCNA courses and real-world networking roles.

Key Topics Covered in the Final Exam

Our verified answers address common exam questions on:

- **Network Fundamentals:** Network models, protocols, and communication rules.
- **Ethernet and Switching:** MAC addresses, frame structure, switching methods, and VLANs.
- **IP Addressing and Subnetting:** IPv4 and IPv6 addressing, subnet masks, CIDR, and VLSM.
- **Routing and ARP:** Router configuration, routing tables, ARP operation, and ICMP.
- **Network Services and Security:** DNS, DHCP, HTTP, FTP, SMTP, and basic security threats.
- **Network Troubleshooting:** Using ping, traceroute, ipconfig, and nslookup.

The exam consists of **60 questions**, requiring **70%** to pass, with a time limit of **1 hour and 15 minutes**. Questions include multiple-choice, drag-and-drop, and simulation-based items.

Common Pitfalls to Avoid

Students often confuse **OSI and TCP/IP model layers** – remember that the TCP/IP application layer maps to the OSI application, presentation, and session layers. Another common mistake is misunderstanding **subnetting** – always calculate the number of host bits needed (2^n–2) to determine the correct subnet mask. Also, pay attention to **well-known port numbers** – know which ports are used by HTTP (80),

HTTPS (443), FTP (21), SSH (22), DNS (53), DHCP (67/68), POP3 (110), and IMAP (143).

When practicing with our answers, avoid memorizing letter choices (A, B, C, D). Cisco often reorders options. Focus on the *concept* behind each correct answer.

Study Strategies That Work

To retain this material long-term, combine our exam answers with hands-on practice. Download Cisco Packet Tracer and build a small network with routers, switches, and PCs. Configure IP addresses, default gateways, and static routes. Use `ping` and `traceroute` to verify connectivity. Observe ARP behavior and examine routing tables. This practical approach cements the theory from all 17 modules.

We also recommend creating flashcards for key terms: **OSI and TCP/IP layers, well-known ports, subnet masks, ARP, TTL, FCS, and the three router boot phases**. Quiz yourself daily until you can define each term without hesitation.

How to Use This Answer Page Effectively

Our goal at CoursMooc.com is to provide **accurate, up-to-date answers for the latest CCNA v7 curriculum**. For each question, we include an explanation—not just the correct choice. Read those explanations carefully. If you find a concept unclear, refer to the official Cisco NetAcad course materials or our additional tutorials linked below.

We regularly update this page to match any changes in the exam. If you notice discrepancies, please let us know through the comments. Your feedback helps other learners succeed.

What's Next After the Final Exam?

After passing the CCNA 1 v7.0 Final Exam, you are ready to move on to **CCNA 2: Switching, Routing, and Wireless Essentials (SRWE)** and **CCNA 3: Enterprise Networking, Security, and Automation (ENSA)**. These courses build on the fundamentals you've mastered here and prepare you for the full CCNA certification exam (200-301).

Final Tips for Exam Day

Before starting the real exam:

- Get a good night's sleep – fatigue leads to misreading questions.
- Read each question twice. Some ask "Which two statements are correct?" – don't just pick one answer.
- Manage your time. You have 75 minutes for 60 questions – about 1.25 minutes per question. Skip difficult ones and return later.
- Look for keywords like "not", "except", or "only". One word changes the entire meaning.
- Trust your first instinct unless you find clear evidence you misread.

Remember: The CCNA v7 curriculum emphasizes **practical troubleshooting**. If you can explain why a packet is dropped or why a certain subnet mask is used, you're ready. Use our answers to verify your thinking, then reinforce with simulation tools. Good luck on your exam – and on your journey to networking expertise.

Social Sciences

Scholarships

- Bachelor Scholarships
- Master Scholarships
- PhD Scholarships
- Post Doctoral Fellowships
- Africa Scholarships
- America Scholarships
- Asia Scholarships
- Australia Scholarships
- Middle East Scholarships
- Europe Scholarships
- Germany Scholarships
- UK Scholarships

Opportunities

- Courses
- Classrooms
- Scholarships
- Exam Preparation
- Practice Tests

Best Articles

- Latest Articles
- How to apply for Scholarships?
- 20+ Free Tech Giants Courses
- How to Pass CCNA Exam Fast