**<https://itexamanswers.net/ccna-1-introduction-to-networks-v5-1-v6-0-exams-answers>**

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

**1. A company is contemplating whether to use a client/server or a peer-to-peer network. What are three characteristics of a peer-to-peer network? (Choose three.)**

* better security
* **easy to create\***
* better device performance when acting as both client and server
* **lacks centralized administration \***
* **less cost to implement\***
* scalable

**Explain:**  
Because network devices and dedicated servers are not required, peer-to-peer networks are easy to create, less complex, and have lower costs. Peer-to-peer networks also have no centralized administration. They are less secure, not scalable, and those devices acting as both client and server may perform slower.

**2. Which device performs the function of determining the path that messages should take through internetworks?**

* **a router\***
* a firewall
* a web server
* a DSL modem

**Explain:**  
A router is used to determine the path that the messages should take through the network. A firewall is used to filter incoming and outgoing traffic. A DSL modem is used to provide Internet connection for a home or an organization.

**3. What two criteria are used to help select a network medium from various network media? (Choose two.)**

* the types of data that need to be prioritized
* the cost of the end devices utilized in the network
* **the distance the selected medium can successfully carry a signal\***
* the number of intermediary devices installed in the network
* **the environment where the selected medium is to be installed\***

**Explain:**  
Criteria for choosing a network medium are the distance the selected medium can successfully carry a signal, the environment in which the selected medium is to be installed, the amount of data and the speed at which the data must be transmitted, and the cost of the medium and its installation.

**4. Which two statements describe intermediary devices? (Choose two.)**

* Intermediary devices generate data content.
* Intermediary devices alter data content.
* **Intermediary devices direct the path of the data. \***
* **Intermediary devices connect individual hosts to the network.\***
* Intermediary devices initiate the encapsulation process.

**Explain:**  
Applications on end devices generate data, alter data content, and are responsible for initiating the encapsulation process.

**5. What are two functions of end devices on a network? (Choose two.)**

* **They originate the data that flows through the network.\***
* They direct data over alternate paths in the event of link failures.
* They filter the flow of data to enhance security.
* **They are the interface between humans and the communication network.\***
* They provide the channel over which the network message travels.

**Explain:**  
End devices originate the data that flows through the network. Intermediary devices direct data over alternate paths in the event of link failures and filter the flow of data to enhance security. Network media provide the channel through which network messages travel.

**6. Which area of the network would a college IT staff most likely have to redesign as a direct result of many students bringing their own tablets and smartphones to school to access school resources?**

* extranet
* intranet
* wired LAN
* **wireless LAN\***
* wireless WAN

**Explain:**  
An extranet is a network area where people or corporate partners external to the company access data. An intranet simply describes the network area that is normally accessed only by internal personnel. The wired LAN is affected by BYODs (bring your own devices) when the devices attach to the wired network. A college wireless LAN is most likely used by the tablet and smartphone. A wireless WAN would more likely be used by college students to access their cell provider network.

**7. An employee at a branch office is creating a quote for a customer. In order to do this, the employee needs to access confidential pricing information from internal servers at the Head Office. What type of network would the employee access?**

* **an intranet\***
* the Internet
* an extranet
* a local area network

**Explain:**  
Intranet is a term used to refer to a private connection of LANs and WANs that belongs to an organization. An intranet is designed to be accessible only by the organization’s members, employees, or others with authorization.

**8. Which two connection options provide an always-on, high-bandwidth Internet connection to computers in a home office? (Choose two.)**

* cellular
* **DSL\***
* satellite
* **cable\***
* dial-up telephone

**Explain:**  
Cable and DSL both provide high bandwidth, an always on connection, and an Ethernet connection to a host computer or LAN.

**9. Which two Internet connection options do not require that physical cables be run to the building? (Choose two.)**

* DSL
* **cellular\***
* **satellite\***
* dialup
* dedicated leased line

**Explain:**  
Cellular connectivity requires the use of the cell phone network. Satellite connectivity is often used where physical cabling is not available outside the home or business.

**10. Which term describes the state of a network when the demand on the network resources exceeds the available capacity?**

* convergence
* **congestion\***
* optimization
* synchronization

**Explain:**  
When the demand on the network resources exceeds the available capacity, the network becomes congested. A converged network is designed to deliver multiple communication types, such as data, video and voice services, using the same network infrastructure.

**11. Which expression accurately defines the term bandwidth?**

* a method of limiting the impact of a hardware or software failure on the network
* **a measure of the data carrying capacity of the media\***
* a state where the demand on the network resources exceeds the available capacity
* a set of techniques to manage the utilization of network resources

**Explain:**  
A method of limiting the impact of a hardware or software failure is fault tolerance. A measure of the data carrying capacity is bandwidth. A set of techniques to manage the utilization of network resources is QoS. A state where the demand on the network resources exceeds the available capacity is called congestion.

**12. Which networking trend involves the use of personal tools and devices for accessing resources on a business or campus network?**

* video conferencing
* cloud computing
* **BYOD\***
* powerline networking

**Explain:**  
BYOD, or bring your own device, is a trend in networking where users are allowed to use personal devices and tools on business and campus networks

**13. What is a characteristic of a converged network?**

* it provides only one path between the source and destination of a message
* it limits the impact of a failure by minimizing the number of devices affected
* **it delivers data, voice, and video over the same network infrastructure\***
* A converged network requires a separate network infrastructure for each type of communication technology

**Explain:**  
A converged network is one in which multiple technologies such as data, telephone, and video are all delivered on the same network infrastructure.

**14. Which statement describes a characteristic of cloud computing?**

* A business can connect directly to the Internet without the use of an ISP.
* **Applications can be accessed over the Internet by individual users or businesses using any device, anywhere in the world.\***
* Devices can connect to the Internet through existing electrical wiring.
* Investment in new infrastructure is required in order to access the cloud.

**Explain:**  
Cloud computing allows users to access applications, back up and store files, and perform tasks without needing additional software or servers. Cloud users access resources through subscription-based or pay-per-use services, in real time, using nothing more than a web browser.

**15. Which statement describes the use of powerline networking technology?**

* New “smart” electrical cabling is used to extend an existing home LAN.
* A home LAN is installed without the use of physical cabling.
* **A device connects to an existing home LAN using an adapter and an existing electrical outlet.\***
* Wireless access points use powerline adapters to distribute data through the home LAN.

**Explain:**  
Powerline networking adds the ability to connect a device to the network using an adapter wherever there is an electrical outlet.​ The network uses existing electrical wiring to send data. It is not a replacement for physical cabling, but it can add functionality in places where wireless access points cannot be used or cannot reach devices.​

**16. What security violation would cause the most amount of damage to the life of a home user?**

* denial of service to your email server
* replication of worms and viruses in your computer
* **capturing of personal data that leads to identity theft\***
* spyware that leads to spam emails

**Explain:**  
On a personal PC, denial of service to servers, worms and viruses, and spyware producing spam emails can be annoying, invasive, and frustrating. However, identity theft can be devastating and life altering. Security solutions should be in place on all personal devices to protect against this type of threat.

**17. A user is implementing security on a small office network. Which two actions would provide the minimum security requirements for this network? (Choose two.)**

* **implementing a firewall\***
* installing a wireless network
* **installing antivirus software\***
* implementing an intrusion detection system
* adding a dedicated intrusion prevention device

**Explain:**  
Technically complex security measures such as intrusion prevention and intrusion prevention systems are usually associated with business networks rather than home networks. Installing antivirus software, antimalware software, and implementing a firewall will usually be the minimum requirements for home networks. Installing a home wireless network will not improve network security, and will require further security actions to be taken.

**18. Fill in the blank.**  
A **converged** network is capable of delivering voice, video, text, and graphics over the same communication channels.

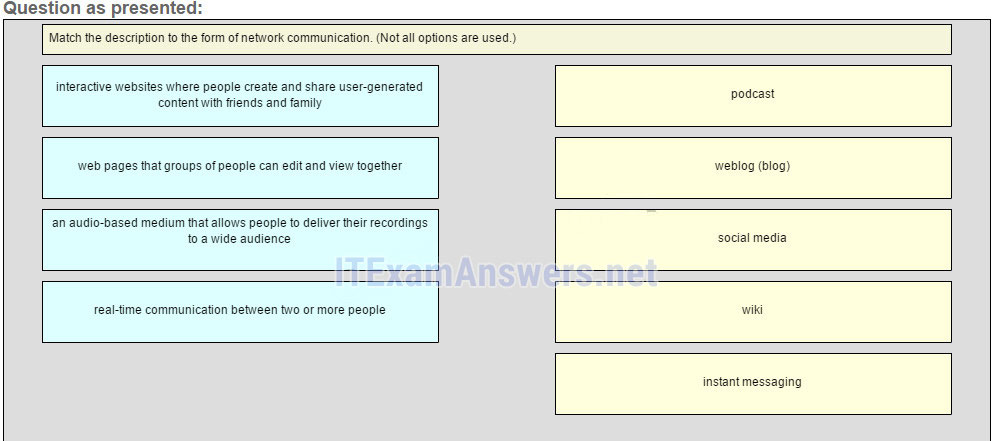
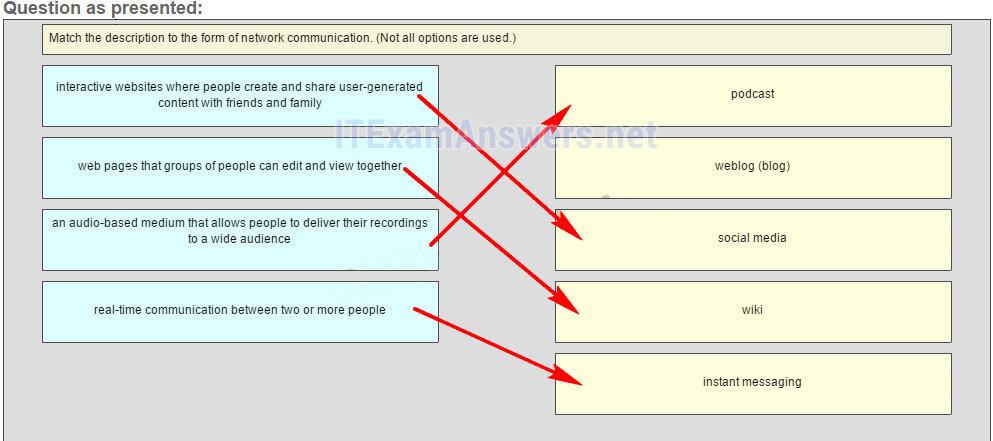
**Explain:**  
When one network is used for all types of communication such as voice, video, text, and graphics, the network is referred to as a converged network.

**19. Fill in the blank.**

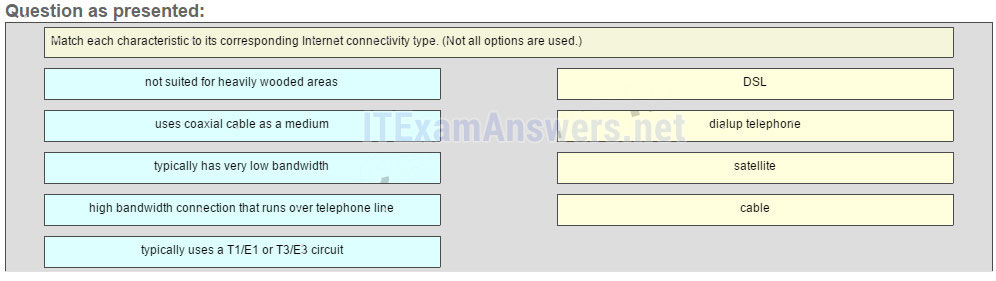
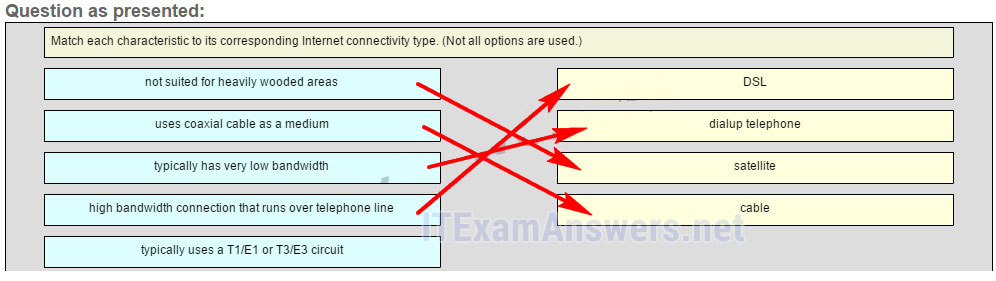
The acronym **byod** refers to the policy that allows employees to use their personal devices in the business office to access the network and other resources.

**20. What are two functions of intermediary devices on a network? (Choose two.)**

* They are the primary source and providers of information and services to end devices.
* They run applications that support collaboration for business.
* They form the interface between the human network and the underlying communication network.
* **They direct data along alternate pathways when there is a link failure. \***
* **They filter the flow of data, based on security settings.\***

**21. Match the description to the form of network communication. (Not all options are used.**  
  


**Place the options in the following order:**  
**an audio-based medium that allows people to deliver their recordings to a wide audience** **–> podcast**  
**interactive websites where people create and share user-generated content with friends and family** **–> social media**  
**web pages that groups of people can edit and view together** **–> wiki**  
**real-time communication between two or more people** **–> instant messaging**

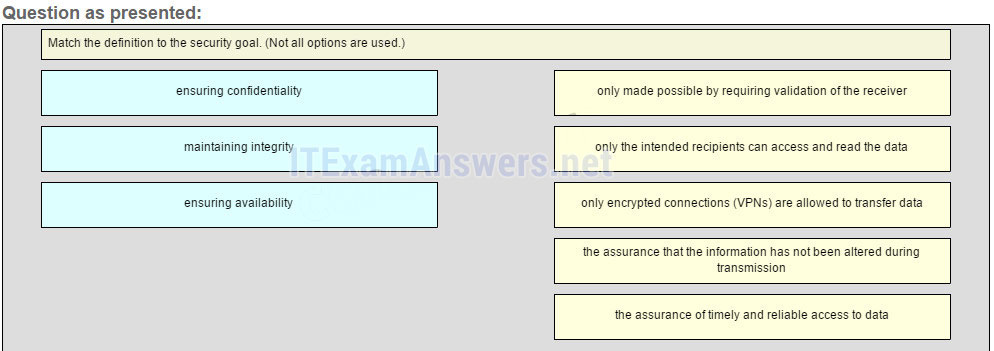
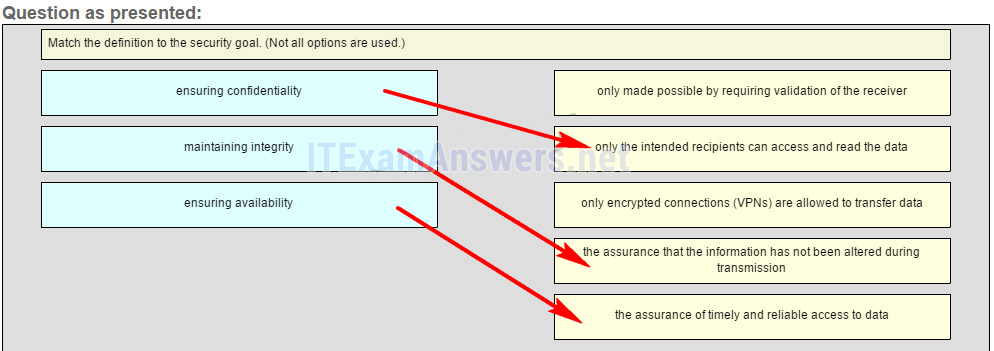
**22. Match each characteristic to its corresponding internet conectivity type. (Not all options are used)**  
  
  
**Place the options in the following order:**  
**high bandwidth connection that runs over telephone line -> 1**  
**typically has very low bandwidth -> 2**  
**not suited for heavily wooded areas -> 3**  
**uses coaxial cable as a medium -> 4**

**Explain:**  
DSL is an always-on, high bandwidth connection that runs over telephone lines. Cable uses the same coaxial cable that carries television signals into the home to provide Internet access. Dialup telephone is much slower than either DSL or cable, but is the least expensive option for home users because it can use any telephone line and a simple modem. Satellite requires a clear line of sight and is affected by trees and other obstructions. None of these typical home options use dedicated leased lines such as T1/E1 and T3/E3.

**23. What is the Internet?**

* It is a network based on Ethernet technology.
* It provides network access for mobile devices.
* **It provides connections through interconnected global networks.\***
* It is a private network for an organization with LAN and WAN connections.

**Explain:**  
The Internet provides global connections that enable networked devices (workstations and mobile devices) with different network technologies, such as Ethernet, DSL/cable, and serial connections, to communicate. A private network for an organization with LAN and WAN connections is an intranet.

**24. Match the definition to the security goal. (Not all options are used.)**  
  


**ensuring confidentiality** -> only the intended recipients can access and read the data  
**maintaining integrity** -> the assurance that the information has not been altered during transmission  
**ensuring availability** -> the assurance of timely and reliable access to data

**Explain:**  
Data integrity verifies that the data has not been altered on the trip between the sender and the receiver. A field calculated by the sender is recalculated and verified to be the same by the receiver. Passwords and authorization maintain control over who has access to personal data. Redundant devices and links attempt to provide 99.999% availability to users. Integrity is made possible by requiring validation of the sender, not the destination. VPNs are not the only secure method by which data can be transferred confidentially.

**25. What type of network must a home user access in order to do online shopping?**

* an intranet
* **the Internet\***
* an extranet
* a local area network

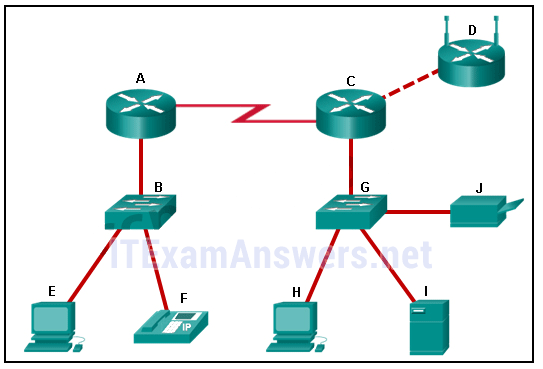
**26. What type of network traffic requires QoS?**

* email
* on-line purchasing
* **video conferencing\***
* wiki

**27. A network administrator is implementing a policy that requires strong, complex passwords. Which data protection goal does this policy support?**

* data integrity
* data quality
* **data confidentiality\***
* data redundancy

### Older Version

**28. Refer to the exhibit. Which set of devices contains only intermediary devices?Error! Filename not specified.**

* **A, B, D, G\***
* A, B, E, F
* C, D, G, I
* G, H, I, J

**29. Which two statements about the relationship between LANs and WANs are true? (Choose two.)**

* Both LANs and WANs connect end devices.
* **WANs connect LANs at slower speed bandwidth than LANs connect their internal end devices.\***
* LANs connect multiple WANs together.
* WANs must be publicly-owned, but LANs can be owned by either public or private entities.
* **WANs are typically operated through multiple ISPs, but LANs are typically operated by single organizations or individuals.\***

**30. Which two Internet solutions provide an always-on, high-bandwidth connection to computers on a LAN? (Choose two.) Which two Internet solutions provide an always-on, high-bandwidth connection to computers on a LAN? (Choose two.)**

* cellular
* **DSL\***
* satellite
* **cable\***
* dial-up telephone

**31. Which description correctly defines a converged network?**

* **a single network channel capable of delivering multiple communication forms\***
* a network that allows users to interact directly with each other over multiple channels
* a dedicated network with separate channels for video and voice services
* a network that is limited to exchanging character-based information

**32. Which statement describes a network that supports QoS?**

* The fewest possible devices are affected by a failure.
* The network should be able to expand to keep up with user demand.
* **The network provides predictable levels of service to different types of traffic.\***
* Data sent over the network is not altered in transmission.

**33. What is a characteristic of circuit-switched networks?**

* **If all circuits are busy, a new call cannot be placed.\***
* If a circuit fails, the call will be forwarded on a new path.
* Circuit-switched networks can dynamically learn and use redundant circuits.
* A single message can be broken into multiple message blocks that are transmitted through multiple circuits simultaneously.

**34. Which expression accurately defines the term congestion?**

* a method of limiting the impact of a hardware or software failure on the network
* a measure of the data carrying capacity of the network
* **a state where the demand on the network resources exceeds the available capacity\***
* a set of techniques to manage the utilization of network resources

**35. Which tool provides real-time video and audio communication over the Internet so that businesses can conduct corporate meetings with participants from several remote locations?**

* wiki
* weblog
* **TelePresence\***
* instant messaging

**36. Requiring strong, complex passwords is a practice that supports which network security goal?**

* maintaining communication integrity
* ensuring reliability of access
* **ensuring data confidentiality\***
* ensuring redundancy

**37. Which three network tools provide the minimum required security protection for home users? (Choose three.)**

* an intrusion prevention system
* **antivirus software \***
* **antispyware software\***
* access control lists
* **a firewall\***
* powerline networking

**38. Which two Internet solutions provide an always-on, high-bandwidth connection to computers on a LAN? (Choose two.)**

* cellular
* **DSL\***
* satellite
* **cable\***
* dial-up telephone

**39. What two criteria are used to help select network media? (Choose two.)**

* **the distance the media can successfully carry a signal\***
* **the environment where the media is to be installed\***
* the cost of the end devices utilized in the network
* the number of intermediary devices installed in the network
* the types of data that need to be prioritized

**40. Fill in the blank.**

The acronym **byod** refers to the trend of end users being able to use their personal devices to access the business network and resources.

**41. A college is building a new dormitory on its campus. Workers are digging in the ground to install a new water pipe for the dormitory. A worker accidentally damages a fiber optic cable that connects two of the existing dormitories to the campus data center. Although the cable has been cut, students in the dormitories only experience a very short interruption of network services. What characteristic of the network is shown here?**

* quality of service (QoS)
* scalability
* security
* **fault tolerance \***
* integrity

# CCNA 1 (v5.1 + v6.0) Chapter 2 Exam Answers 2019 – 100% Full

**1. What is the function of the kernel of an operating software?**

* It provides a user interface that allows users to request a specific task.
* The kernel links the hardware drivers with the underlying electronics of a computer.
* It is an application that allows the initial configuration of a Cisco device.
* **The kernel provisions hardware resources to meet software requirements.\***

**Explain:**  
Operating systems function with a shell, a kernel, and the hardware. The shell interfaces with the users, allowing them to request specific tasks from the device. The kernel provisions resources from the hardware to meet software requirements. The hardware functions by using drivers and their underlying electronics. The hardware represents the physical components of the device.

**2. 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?**

* Telnet
* Console
* AUX
* **SSH\***

**Explain:**  
To be truly private a technician would use a Console connection however if remote management is required SSH provides a secure method.

**3. Which procedure is used to access a Cisco 2960 switch when performing an initial configuration in a secure environment?**

* Use Telnet to remotely access the switch through the network.
* **Use the console port to locally access the switch from a serial or USB interface of the PC.\***
* Use Secure Shell to remotely access the switch through the network.
* Use the AUX port to locally access the switch from a serial or USB interface of the PC.

**Explain:**  
Telnet and SSH require active networking services to be configured on a Cisco device before they become functional. Cisco switches do not contain AUX ports.

**4. Which command or key combination allows a user to return to the previous level in the command hierarchy?**

* end
* **exit\***
* Ctrl-Z
* Ctrl-C

**Explain:**  
End and CTRL-Z return the user to the privileged EXEC mode. Ctrl-C ends a command in process. The exit command returns the user to the previous level.

**5. A router has a valid operating system and a configuration file stored in NVRAM. The configuration file contains an enable secret password but no console password. When the router boots up, which mode will display?**

* global configuration mode
* setup mode
* privileged EXEC mode
* **user EXEC mode \***

**Explain:**  
If a Cisco IOS device has a valid IOS and a valid configuration file, it will boot into user EXEC mode. A password will be required to enter privileged EXEC mode.

**6. Which two functions are provided to users by the context-sensitive help feature of the Cisco IOS CLI? (Choose two.)**

* providing an error message when a wrong command is submitted
* **displaying a list of all available commands within the current mode\***
* allowing the user to complete the remainder of an abbreviated command with the TAB key
* **determining which option, keyword, or argument is available for the entered command\***
* selecting the best command to accomplish a task

**Explain:**  
Context-sensitive help provides the user with a list of commands and the arguments associated with those commands within the current mode of a networking device. A syntax checker provides error checks on submitted commands and the TAB key can be used for command completion if a partial command is entered.

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

* the IOS image copied into RAM
* the bootstrap program in the ROM
* the contents of the current running configuration file in the RAM
* **the contents of the saved configuration file in the NVRAM \***

**Explain:**  
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.​

**8. Why is it important to configure a hostname on a device?**

* a Cisco router or switch only begins to operate when its hostname is set
* a hostname must be configured before any other parameters
* **to identify the device during remote access (SSH or telnet)\***
* to allow local access to the device through the console port

**Explain:**  
It is important to configure a hostname because various authentication processes use the device hostname. Hostnames are helpful for documentation, and they identify the device during remote access.

**9. Which two host names follow the guidelines for naming conventions on Cisco IOS devices? (Choose two.)**

* Branch2!
* **RM-3-Switch-2A4\***
* Floor(15)
* HO Floor 17
* **SwBranch799\***

**Explain:**  
Some guidelines for naming conventions are that names should:  
Start with a letter  
Contain no spaces  
End with a letter or digit  
Use only letters, digits, and dashes  
Be less than 64 characters in length

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

* It encrypts passwords as they are sent across the network.
* **It encrypts passwords that are stored in router or switch configuration files.\***
* It requires that a user type encrypted passwords to gain console access to a router or switch.
* It requires encrypted passwords to be used when connecting remotely to a router or switch with Telnet.

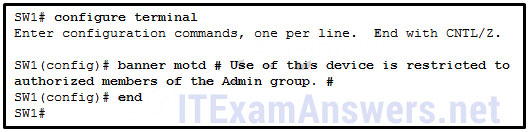
**Explain:**  
The service password-encryption command encrypts plaintext passwords in the configuration file so that they cannot be viewed by unauthorized users.

**11. In your opinion (this has no bearing on your grade), please indicate how enthusiastic you are about the content of this course and the things you’re learning (or have learned):**

* Not At All Enthusiastic
* Slightly Enthusiastic
* **Enthusiastic\***
* Very Enthusiastic
* Completely Enthusiastic

**12. In your opinion (this has no bearing on your grade), please indicate your interest in this course:**

* Not At All Interested
* Slightly Interested
* **Interested\***
* Very Interested
* Completely Interested

**13. Refer to the exhibit. A network administrator is configuring the MOTD on switch SW1. What is the purpose of this command?**  


* **to display a message when a user accesses the switch\***
* to configure switch SW1 so that only the users in the Admin group can telnet into SW1
* to force users of the Admin group to enter a password for authentication
* to configure switch SW1 so that the message will display when a user enters the enable command

**Explain:**  
A banner message can be an important part of the legal process in the event that someone is prosecuted for breaking into a device. A banner message should make it clear that only authorized personnel should attempt to access the device. However, the banner command does not prevent unauthorized entry.

**14. While trying to solve a network issue, a technician made multiple changes to the current router configuration file. The changes did not solve the problem and were not saved. What action can the technician take to discard the changes and work with the file in NVRAM?**

* **Issue the reload command without saving the running configuration.\***
* Delete the vlan.dat file and reboot the device.
* Close and reopen the terminal emulation software.
* Issue the copy startup-config running-config command.

**Explain:**  
The technician does not want to make any mistakes trying to remove all the changes that were done to the running configuration file. The solution is to reboot the router without saving the running configuration. The copy startup-config running-config command does not overwrite the running configuration file with the configuration file stored in NVRAM, but rather it just has an additive effect.

**15. What is the function of the kernel of an operating system?**

* It provides a user interface that allows users to request a specific task.
* The kernel links the hardware drivers with the underlying electronics of a computer.
* It is an application that allows the initial configuration of a Cisco device.
* **The kernel provisions hardware resources to meet software requirements.\***

**Explain:**  
Operating systems function with a shell, a kernel, and the hardware. The shell interfaces with the users, allowing them to request specific tasks from the device. The kernel provisions resources from the hardware to meet software requirements. The hardware functions by using drivers and their underlying electronics. The hardware represents the physical components of the device.

**16. A router with a valid operating system contains a configuration file stored in NVRAM. The configuration file has an enable secret password but no console password. When the router boots up, which mode will display?**

* privileged EXEC mode
* setup mode
* **user EXEC mode\***
* global configuration mode

**Explain:**If a Cisco IOS device has a valid IOS and a valid configuration file, it will boot into user EXEC mode. A password will be required to enter privileged EXEC mode.

**17. In your opinion (this has no bearing on your grade), please rate your motivation to do well in this course:**

* Not At All Motivated
* Slightly Motivated
* Motivated
* **Very Motivated\***
* Completely Motivated

**18. Which statement is true about the running configuration file in a Cisco IOS device?**

* **It affects the operation of the device immediately when modified.\***
* It is stored in NVRAM.
* It should be deleted using the erase running-config command.
* It is automatically saved when the router reboots.

**Explain:**  
As soon as configuration commands are entered into a router, they modify the device immediately. Running configuration files can not be deleted nor are they saved automatically.

**19. What are two characteristics of RAM on a Cisco device? (Choose two.)**

* RAM provides nonvolatile storage.
* **The configuration that is actively running on the device is stored in RAM. \***
* **The contents of RAM are lost during a power cycle. \***
* RAM is a component in Cisco switches but not in Cisco routers.
* RAM is able to store multiple versions of IOS and configuration files.

**Explain:**  
RAM stores data that is used by the device to support network operations. The running configuration is stored in RAM. This type of memory is considered volatile memory because data is lost during a power cycle. Flash memory stores the IOS and delivers a copy of the IOS into RAM when a device is powered on. Flash memory is nonvolatile since it retains stored contents during a loss of power.

**20. Which interface allows remote management of a Layer 2 switch?**

* the AUX interface
* the console port interface
* **the switch virtual interface\***
* the first Ethernet port interface

**Explain:**  
In a Layer 2 switch, there is a switch virtual interface (SVI) that provides a means for remotely managing the device.

**21. Which interface is the default SVI on a Cisco switch?**

* FastEthernet 0/1
* GigabitEthernet 0/1
* **VLAN 1\***
* VLAN 99

**Explain:**  
An SVI is a virtual interface and VLAN 1 is enabled by default on Cisco switches. VLAN 99 must be configured to be used. FastEthernet 0/1 and GigabitEthernet 0/1 are physical interfaces.

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

* to enable the switch to send broadcast frames to attached PCs
* to enable the switch to function as a default gateway
* **to enable the switch to be managed remotely\***
* to enable the switch to receive frames from attached PCs

**Explain:**  
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.

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

* ping
* **ipconfig\***
* show interfaces
* show ip interface brief

**Explain:**  
On a Windows PC, the ipconfig command can be used to verify the current IP configuration. The ping command can be used to verify connectivity to other network devices. The show interfaces and show ip interface brief commands are both Cisco IOS commands that are used to see the status of router and switch interfaces.

**24. A technician is adding a new PC to a LAN. After unpacking the components and making all the connections, the technician starts the PC. After the OS loads, the technician opens a browser, and verifies that the PC can reach the Internet. Why was the PC able to connect to the network with no additional configuration?**

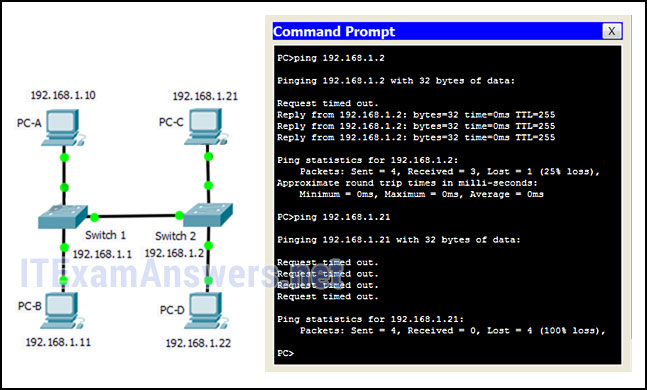
* The PC does not require any additional information to function on the network.
* The PC came preconfigured with IP addressing information from the factory.
* **The PC was preconfigured to use DHCP.\***
* The PC used DNS to automatically receive IP addressing information from a server.
* The PC virtual interface is compatible with any network.

**Explain:**  
The new PC was preconfigured to use DHCP. When the PC is connected to a network that uses DHCP, it gets the IP address settings from the DHCP server that will allow it to function on the network. All devices require at least an IP address and subnet mask to function on a LAN. DNS does not automatically configure addresses on hosts. PC virtual interfaces are not universally compatible with LANs and do not necessarily provide a host with an IP address. At this place in the course, virtual interfaces are used on network switches.

**25. What is a user trying to determine when issuing a ping 10.1.1.1 command on a PC?**

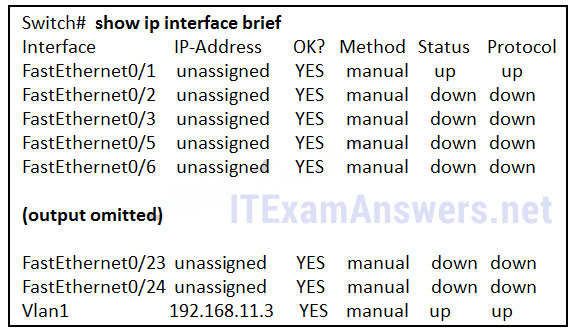
* if the TCP/IP stack is functioning on the PC without putting traffic on the wire
* **if there is connectivity with the destination device\***
* the path that traffic will take to reach the destination
* what type of device is at the destination

**Explain:**  
The ping destination command can be used to test connectivity.

**26. Refer to the exhibit. A network technician is testing connectivity in a new network. Based on the test results shown in the exhibit, which device does the technician have connectivity with and which device does the technician not have connectivity with? (Choose two.)**  


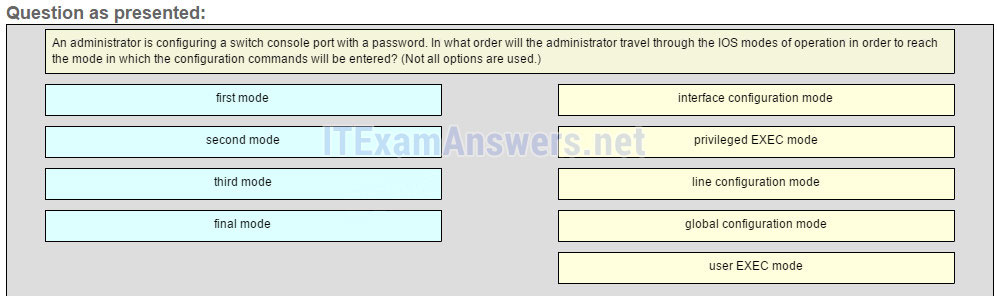
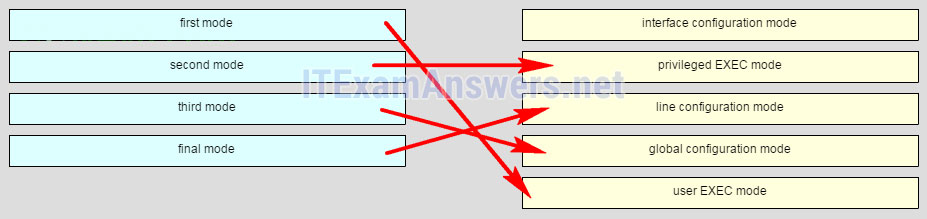
* **connectivity: switch 2\***
* connectivity: PC-D
* connectivity: PC-B
* no connectivity: switch 1
* no connectivity: switch 2
* **no connectivity: PC-C\***

**Explain:**  
The exhibit shows ping tests to two devices. One device has the IP address of 192.168.1.2, which is switch 2. The other test is to the IP address of 192.168.1.21, which is host PC-C. For the first test, to switch 2, the results are successful, with four reply messages received. This means that connectivity exists to switch 2. For the second test, all four messages timed out. This indicates that connectivity does not exist to PC-C.

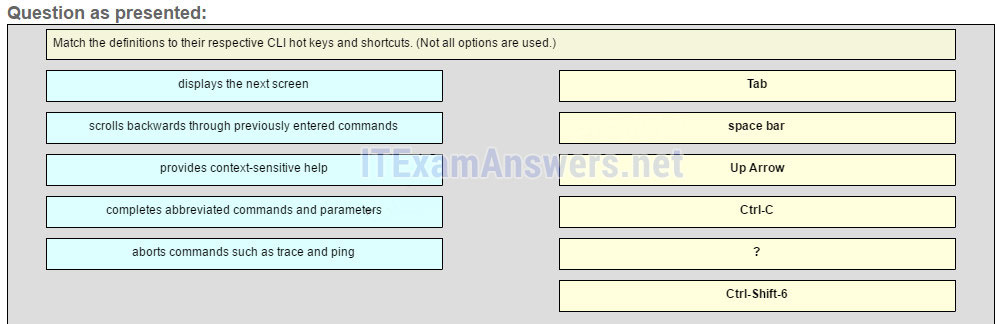
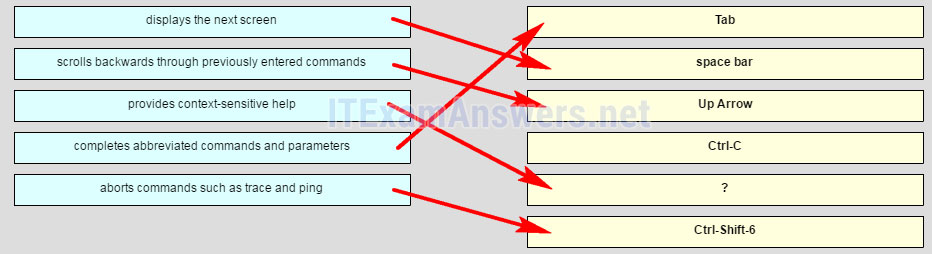
**27. Refer to the exhibit.**  
  
**Refer to the exhibit. What three facts can be determined from the viewable output of the show ip interface brief command? (Choose three.)**

* Two physical interfaces have been configured.
* **The switch can be remotely managed.\***
* **One device is attached to a physical interface.\***
* Passwords have been configured on the switch.
* Two devices are attached to the switch.
* **The default SVI has been configured.\***

**Explain:**  
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.

**28. An administrator is configuring a switch console port with a password. In what order will the administrator travel through the IOS modes of operation in order to reach the mode in which the configuration commands will be entered? (Not all options are used.)**  
  
  
**Place the options in the following order:**  
– not scored –  
second mode  
final mode  
third mode  
first mode

**Explain:**  
The configuration mode that the administrator first encounters is user EXEC mode. After the enable command is entered, the next mode is privileged EXEC mode. From there, the configure terminal command is entered to move to global configuration mode. Finally, the administrator enters the line console 0 command to enter the mode in which the configuration will be entered.

**29. Match the definitions to their respective CLI hot keys and shortcuts. (Not all options are used.)**  
**Question**  
  
**Answer**  
  
**Place the options in the following order:**   
completes abbreviated commands and parameters  
displays the next screen  
scrolls backwards through previously entered commands  
– not scored –  
provides context-sensitive help  
aborts commands such as trace and ping

**Explain:**  
The shortcuts with their functions are as follows:  
– Tab – Completes the remainder of a partially typed command or keyword  
– Space bar – displays the next screen  
– ? – provides context-sensitive help  
– Up Arrow – Allows user to scroll backward through former commands  
– Ctrl-C – cancels any command currently being entered and returns directly to privileged EXEC mode  
– Ctrl-Shift-6 – Allows the user to interrupt an IOS process such as ping or traceroute

### Other Questions

**30. A network administrator is planning an IOS upgrade on several of the head office routers and switches. Which three questions must be answered before continuing with the IOS selection and upgrade? (Choose three.)**

* Are the devices on the same LAN?
* Do the devices have enough NVRAM to store the IOS image?
* **What models of routers and switches require upgrades?\***
* What ports are installed on the routers and switches?
* **Do the routers and switches have enough RAM and flash memory for the proposed IOS versions? \***
* **What features are required for the devices?\***

**31. A router has a valid operating system and a configuration stored in NVRAM. When the router boots up, which mode will display?**

* global configuration mode
* setup mode
* ROM monitor mode
* **user EXEC mode\***

**32. Which two characters are allowed as part of the hostname of a Cisco device? (Choose two.)**

* **numbers\***
* question mark
* space
* tab
* **dash\***

**33. What is a result of using the service password-encryption command on a Cisco network device?**

* The command encrypts the banner message.
* The command encrypts the enable mode password.
* **All passwords in the configuration are not shown in clear text when viewing the configuration.\***
* A network administrator who later logs into the device will be required to enter an administrator password in order to gain access to the Cisco device.

**34. 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?**

* Reboot the device.
* Enter CTRL-Z at the privileged mode prompt.
* Exit global configuration mode.
* Power cycle the device.
* **Exit privileged EXEC mode and press Enter.\***

**35. Passwords can be used to restrict access to all or parts of the Cisco IOS. Select the modes and interfaces that can be protected with passwords. (Choose three.)**

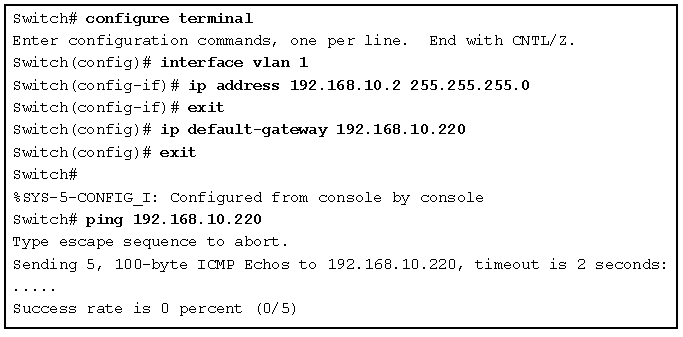
* **VTY interface \***
* **console interface\***
* Ethernet interface
* boot IOS mode
* **privileged EXEC mode\***
* router configuration mode

**36. What benefit does DHCP provide to a network?**

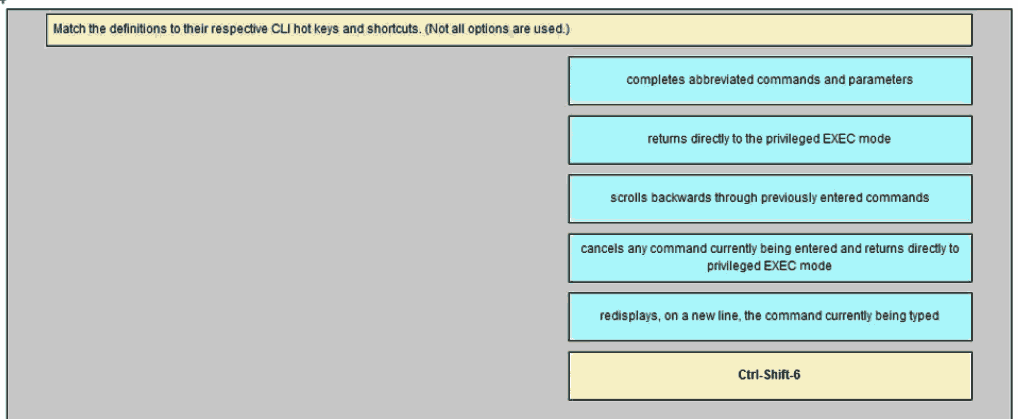
* Hosts always have the same IP address and are therefore always reachable.
* DHCP allows users to refer to locations by a name rather than an IP address.
* **Hosts can connect to the network and get an IP address without manual configuration.\***
* Duplicate addresses cannot occur on a network that issues dynamic addresses using DHCP and has static assignments.

**37. What criterion must be followed in the design of an IPv4 addressing scheme for end devices?**

* Each IP address must match the address that is assigned to the host by DNS.
* **Each IP address must be unique within the local network.\***
* Each IP address needs to be compatible with the MAC address.
* Each local host should be assigned an IP address with a unique network component.

**38. Refer to the exhibit. A switch was configured as shown. A ping to the default gateway was issued, but the ping was not successful. Other switches in the same network can ping this gateway. What is a possible reason for this?**  


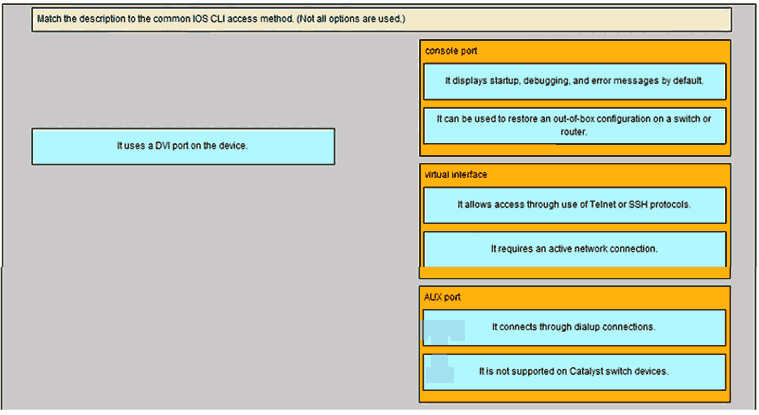
* The VLAN IP address and the default gateway IP address are not in the same network.
* The local DNS server is not functioning correctly.
* **The no shutdown command was not issued for VLAN 1.\***
* The ip default-gateway command has to be issued in the VLAN interface configuration mode.
* The default gateway address must be 192.168.10.1.

**39. Match the difinitions to their respective CLI hot keys and shortcuts.**  
  
Tab -> **Completes abbreviated commands and parameters**  
Ctrl-R -> **returns directly to the privileged EXEC mode**  
Up Arrow -> **scrolls backwards through previously entered commands**  
Ctrl-Z -> **cancels any command currently being entered and returns directly to privileged EXEC mode**  
Ctrl-C -> **Redisplays, on a new line, the command currently being typed**

**40. Which two features are characteristics of flash memory? (Choose two.)**

Flash receives a copy of the IOS from RAM when a device is powered on.  
**Flash provides nonvolatile storage.\***  
**The contents of flash may be overwritten.\***  
Flash is a component in Cisco switches but not in Cisco routers.  
The contents of flash may be lost during a power cycle.

**41. Match the description to the common IOS CLI access method.**

  
**Console port**  
**It displays startup, debugging, and error messages by default.\***  
**It can be used to restore an out-of-box configuration on a switch or router.\***  
**Virtual interface**  
**It allows access throught use of Telnet or SSH protocols.\***  
**It requires an active network connection.\***  
**AUX port**  
**It connects throught dialup connections\***  
**It is not supported on Catalyst switch devices\***

# CCNA 1 (v5.1 + v6.0) Chapter 3 Exam Answers 2019 – 100% Full

**1. What method can be used by two computers to ensure that packets are not dropped because too much data is being sent too quickly?**

* encapsulation
* **flow control\***
* access method
* response timeout

**Explain:**  
In order for two computers to be able to communicate effectively, there must be a mechanism that allows both the source and destination to set the timing of the transmission and receipt of data. Flow control allows for this by ensuring that data is not sent too fast for it to be received properly.

**2. What type of communication will send a message to all devices on a local area network?**

* **broadcast\***
* multicast
* unicast
* allcast

**Explain:**Broadcast communication is a one-to-all communication. A unicast communication is a one-to-one communication. Multicast is a one-to-many communication where the message is delivered to a specific group of hosts. Allcast is not a standard term to describe message delivery.

**3. What process is used to place one message inside another message for transfer from the source to the destination?**

* access control
* decoding
* **encapsulation\***
* flow control

**Explain:**Encapsulation is the process of placing one message format into another message format. An example is how a packet is placed in its entirety into the data field as it is encapsulated into a frame.

**4. A web client is sending a request for a webpage to a web server. From the perspective of the client, what is the correct order of the protocol stack that is used to prepare the request for transmission?**

* HTTP, IP, TCP, Ethernet
* **HTTP, TCP, IP, Ethernet\***
* Ethernet, TCP, IP, HTTP
* Ethernet, IP, TCP, HTTP

**Explain:**  
1. HTTP governs the way that a web server and client interact.  
2. TCP manages individual conversations between web servers and clients.  
3. IP is responsible for delivery across the best path to the destination.  
4. Ethernet takes the packet from IP and formats it for transmission.

**5. Which statement is correct about network protocols?**

* Network protocols define the type of hardware that is used and how it is mounted in racks.
* **They define how messages are exchanged between the source and the destination.\***
* They all function in the network access layer of TCP/IP.
* They are only required for exchange of messages between devices on remote networks.

**Explain:**  
Network protocols are implemented in hardware, or software, or both. They interact with each other within different layers of a protocol stack. Protocols have nothing to do with the installation of the network equipment. Network protocols are required to exchange information between source and destination devices in both local and remote networks.

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

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

**Explain:**  
he TCP/IP internet layer provides the same function as the OSI network layer. The transport layer of both the TCP/IP and OSI models provides the same function. The TCP/IP application layer includes the same functions as OSI Layers 5, 6, and 7.

**7. What is an advantage of using standards to develop and implement protocols?**

* A particular protocol can only be implemented by one manufacturer.
* **Products from different manufacturers can interoperate successfully.\***
* Different manufacturers are free to apply different requirements when implementing a protocol.
* Standards provide flexibility for manufacturers to create devices that comply with unique requirements.

**Explain:**  
Standards-based protocols enable products from different manufacturers to interoperate successfully. Standards-based protocols enable many manufacturers to implement that protocol. If different manufacturers implement different requirements within the same protocol, then their products will not be interoperable.

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

* ARP
* **DHCP \***
* **DNS \***
* **FTP\***
* NAT
* PPP

**Explain:**  
DNS, DHCP, and FTP are all application layer protocols in the TCP/IP protocol suite. ARP and PPP are network access layer protocols, and NAT is an internet layer protocol in the TCP/IP protocol suite.

**9. What are proprietary protocols?**

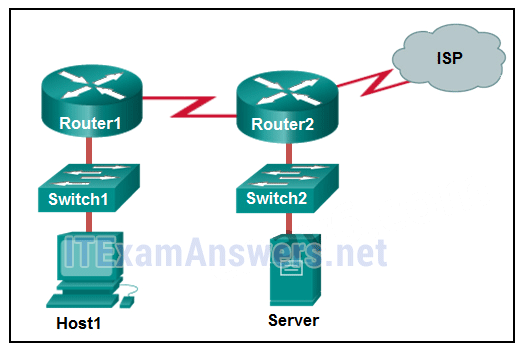
* protocols developed by private organizations to operate on any vendor hardware
* protocols that can be freely used by any organization or vendor
* **protocols developed by organizations who have control over their definition and operation\***
* a collection of protocols known as the TCP/IP protocol suite

**Explain:**  
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.

**10. What is an advantage of network devices using open standard protocols?**

* Network communications is confined to data transfers between devices from the same vendor.
* **A client host and a server running different operating systems can successfully exchange data.\***
* Internet access can be controlled by a single ISP in each market.
* Competition and innovation are limited to specific types of products.

**Explain:**  
An advantage of network devices implementing open standard protocols, such as from the TCP/IP suite, is that clients and servers running different operating systems can communicate with each other. Open standard protocols facilitate innovation and competition between vendors and across markets, and can reduce the occurrence of monopolies in networking markets.

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


* only application and Internet layers
* only Internet and network access layers
* only application, Internet, and network access layers
* **application, transport, Internet, and network access layers\***
* only application, transport, network, data link, and physical layers
* application, session, transport, network, data link, and physical layers

**Explain:**  
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.

**12. Which three layers of the OSI model are comparable in function to the application layer of the TCP/IP model? (Choose three.)**

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

**Explain:**  
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.

**13. At which layer of the OSI model would a logical address be encapsulated?**

* physical layer
* data link layer
* **network layer\***
* transport layer

**Explain:**  
Logical addresses, also known as IP addresses, are encapsulated at the network layer. Physical addresses are encapsulated at the data link layer. Port addresses are encapsulated at the transport layer. No addresses are encapsulated at the physical layer.

**14. At which layer of the OSI model would a logical address be added during encapsulation??**

* physical layer
* data link layer
* **network layer\***
* transport layer

**Explain:**  
Logical addresses, also known as IP addresses, are encapsulated at the network layer. Physical addresses are encapsulated at the data link layer. Port addresses are encapsulated at the transport layer. No addresses are encapsulated at the physical layer.

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

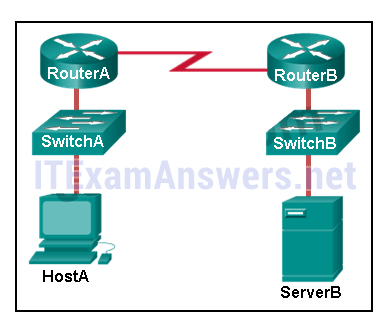
* file
* **frame\***
* packet
* segment

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

**16. Which PDU is processed when a host computer is de-encapsulating a message at the transport layer of the TCP/IP model?**

* bits
* frame
* packet
* **segment\***

**Explain:**  
At the transport layer, a host computer will de-encapsulate a segment to reassemble data to an acceptable format by the application layer protocol of the TCP/IP model.

**17. Refer to the exhibit. HostA is attempting to contact ServerB. Which two statements correctly describe the addressing that HostA will generate in the process? (Choose two.)**  


* A packet with the destination IP address of RouterB.
* A frame with the destination MAC address of SwitchA.
* A packet with the destination IP address of RouterA.
* **A frame with the destination MAC address of RouterA.\***
* **A packet with the destination IP address of ServerB.\***
* A frame with the destination MAC address of ServerB.

**Explain:**  
In order to send data to ServerB, HostA will generate a packet that contains the IP address of the destination device on the remote network and a frame that contains the MAC address of the default gateway device on the local network.

**18. Which address does a NIC use when deciding whether to accept a frame?**

* source IP address
* source MAC address
* destination IP address
* **destination MAC address\***
* source Ethernet address

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

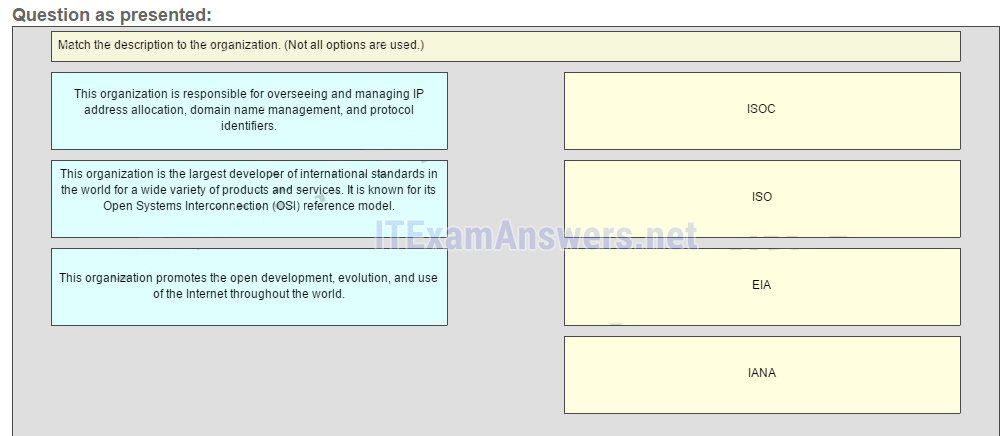
* The host cannot communicate with other hosts in the local network.
* The switch will not forward packets initiated by the host.
* The host will have to use ARP to determine the correct address of the default gateway.
* **The host cannot communicate with hosts in other networks.\***
* A ping from the host to 127.0.0.1 would not be successful.

**Explain:**  
When a host needs to send a message to another host located on the same network, it can forward the message directly. However, when a host needs to send a message to a remote network, it must use the router, also known as the default gateway. This is because the data link frame address of the remote destination host cannot be used directly. Instead, the IP packet has to be sent to the router (default gateway) and the router will forward the packet toward its destination. Therefore, if the default gateway is incorrectly configured, the host can communicate with other hosts on the same network, but not with hosts on remote networks.

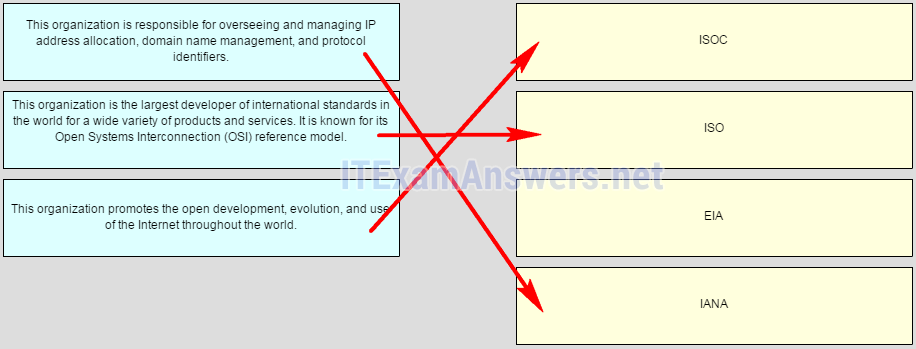
**20. Which characteristic describes the default gateway of a host computer?**

* **the logical address of the router interface on the same network as the host computer\***
* the physical address of the switch interface connected to the host computer
* the physical address of the router interface on the same network as the host computer
* the logical address assigned to the switch interface connected to the router

**Explain:**  
The default gateway is the IP address of an interface on the router on the same network as the sending host.

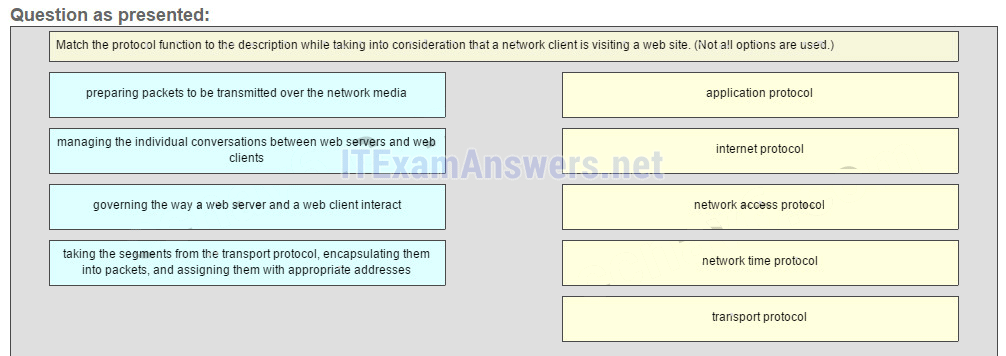
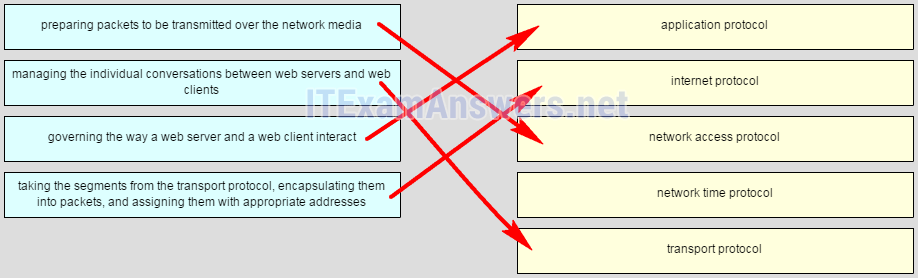


**21. Match the description to the organization. (Not all options are used.)**



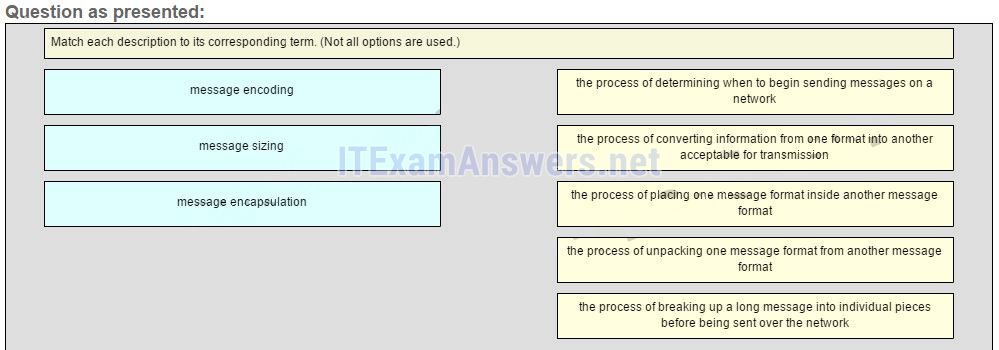
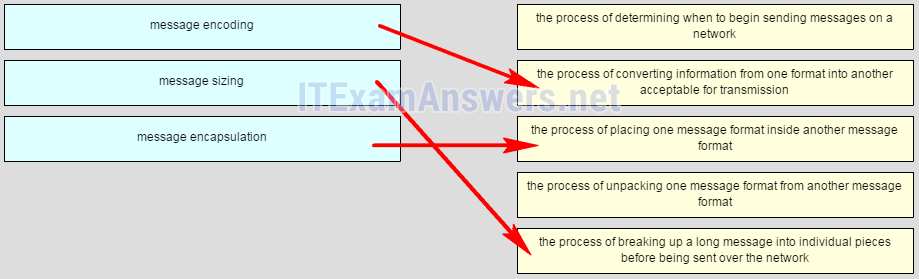
**ISOC ->** **The organization promotes the open development, evolution, and use of the internet throughout the world**  
**ISO ->** **This organization is the largest developer of international standars in the world for a wide variety of products and services. It is know for its Open System Interconection (OSI) reference model.**  
**IANA ->** **This organization is responsible for overseeing and managing IP address allocation, domain name management, and protocol identifiers**

**Explain:**  
The EIA is an international standards and trade organization for electronics organizations. It is best known for its standards related to electrical wiring, connectors, and the 19-inch racks used to mount networking equipment.

**22. Match the protocol function to the description while taking into consideration that a network client is visiting a web site. (Not all options are used.)**  
  


**Place the options in the following order:**   
**governing the way a web server and a web client interact** –> application protocol  
**taking the segments from transport protocol, encapsulating them into packets, and assigning them with appropriate addresses** –> internet protocol  
**preparing packets to be transmitted over the network media** –> network access protocol  
– not scored –  
**managing the individual conversations between web servers and web clients** –> transport protocol

**Explain:**  
When a web client visits a web server, several network communication protocols are involved. These different protocols work together to ensure that the messages are received and understood by both parties. These protocols include the following:  
Application Protocol – governing the way a web server and a web client interact  
Transport Protocol – managing the individual conversations between web servers and web clients  
Internet Protocol – taking the formatted segments from the transport protocol, encapsulating them into packets, assigning them the appropriate addresses, and delivering them across the best path to the destination host  
Network Access Protocol – preparing packets to be transmitted over the network media  
Network Time Protocol is used to synchronize clocks between computer systems. It is not involved in this case.

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


**Place the options in the following order:**   
– not scored –  
**message encoding** -> the process of converting information from one format into another acceptable for transmission  
**message encapsulation** -> the process of placing one message format inside another message format  
– not scored –  
**message sizing** -> the process of breaking up a long message into individual pieces before being sent over the network

## Other Quetions

**24. A computer in a given network is communicating with a specific group of computers. What type of communication is this?**

* broadcast
* **multicast\***
* unicast
* ARP
* HTTP

**25. Which protocol is responsible for controlling the size and rate of the HTTP messages exchanged between server and client?**

* HTTP
* ARP
* **TCP\***
* DHCP

**26. A user is viewing an HTML document located on a web server. What protocol segments the messages and manages the segments in the individual conversation between the web server and the web client?**

* DHCP
* **TCP\***
* HTTP
* ARP

**27. Which IEEE standard enables a wireless NIC to connect to a wireless AP that is made by a different manufacturer?**

* 802.1
* **802.11\***
* 802.3
* 802.2

**28. What is a function of Layer 4 of the OSI model?**

* to specify the packet type to be used by the communications
* to apply framing information to the packet, based on the attached media
* to represent data to the user, including encoding and dialog control
* **to describe the ordered and reliable delivery of data between source and destination\***

**29. What is a benefit of using a layered model for network communications?**

* **fostering competition among device and software vendors by enforcing the compatibility of their products\***
* enhancing network transmission performance by defining targets for each layer
* avoiding possible incompatibility issues by using a common set of developing tools
* simplifying protocol development by limiting every layer to one function

**30. What is the general term that is used to describe a piece of data at any layer of a networking model?**

* frame
* packet
* **protocol data unit\***
* segment

**31. Which statement accurately describes a TCP/IP encapsulation process when a PC is sending data to the network?**

* Data is sent from the internet layer to the network access layer.
* Packets are sent from the network access layer to the transport layer.
* **Segments are sent from the transport layer to the internet layer.\***
* Frames are sent from the network access layer to the internet layer.

**32. What statement describes the function of the Address Resolution Protocol?**

* ARP is used to discover the IP address of any host on a different network.
* ARP is used to discover the IP address of any host on the local network.
* ARP is used to discover the MAC address of any host on a different network.
* **ARP is used to discover the MAC address of any host on the local network.\***

**33. Which address provides a unique host address for data communications at the internet layer?**

* data-link address
* **logical address\***
* Layer 2 address
* physical address

**34. Which protocol is used by a computer to find the MAC address of the default gateway on an Ethernet network?**

* **ARP\***
* TCP
* UDP
* DHCP

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

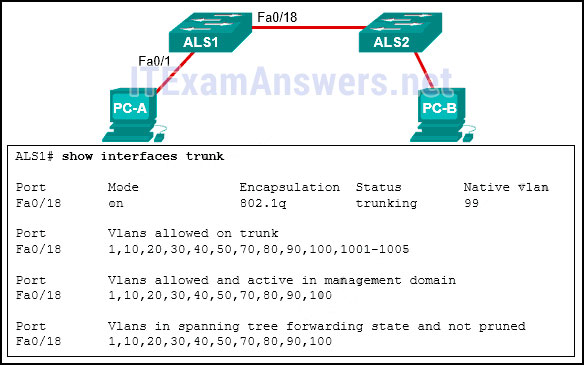
* The host is unable to communicate on the local network.
* **The host can communicate with other hosts on the local network, but is unable to communicate with hosts on remote networks.\***
* The host can communicate with other hosts on remote networks, but is unable to communicate with hosts on the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

**36. Open the PT Activity. Perform the tasks in the activity instructions and then answer the question. Based on the configured network, what IP address would PC1 and PC2 use as their default gateway?**

* 192.168.1.2
* 10.1.1.1
* 172.16.1.1
* **192.168.1.1\***
* 192.168.1.10

**37. 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?**

* **the MAC address of the default gateway\***
* the IP address of the destination host
* the MAC address of the destination host
* the IP address of the default gateway

**38. Refer to the exhibit. PC-A and PC-B are both in VLAN 60. PC-A is unable to communicate with PC-B. What is the problem?**  


* The native VLAN is being pruned from the link.
* The trunk has been configured with the switchport nonegotiate command.
* The native VLAN should be VLAN 60.
* **The VLAN that is used by PC-A is not in the list of allowed VLANs on the trunk.\***

**39. Which command is used to remove only VLAN 20 from a switch?**

* no switchport access vlan 20
* **no vlan 20\***
* delete vlan.dat
* delete flash:vlan.dat

# CCNA 1 (v5.1 + v6.0) Chapter 4 Exam Answers 2019 – 100% Full

**1. What are two reasons for physical layer protocols to use frame encoding techniques? (Choose two.)**

* to reduce the number of collisions on the media
* **to distinguish data bits from control bits\***
* to provide better media error correction
* **to identify where the frame starts and ends\***
* to increase the media throughput
* to distinguish data from control information

**Explain:**  
An encoding technique converts a stream of data bits in a predefined code that can be recognized by both the transmitter and the receiver. Using predefined patterns helps to differentiate data bits from control bits and provide better media error detection.

**2. What is indicated by the term throughput?**

* the guaranteed data transfer rate offered by an ISP
* the capacity of a particular medium to carry data
* the measure of the usable data transferred across the media
* **the measure of the bits transferred across the media over a given period of time\***
* the time it takes for a message to get from sender to receiver

**Explain:**  
Throughput is the measure of the transfer of bits across the media over a given period of time. Throughput is affected by a number of factors such as, EMI and latency, so it rarely matches the specified bandwidth for a network medium. The throughput measurement includes user data bits and other data bits, such as overhead, acknowledging, and encapsulation. The measure of the usable data transferred across the media is called goodput.

**3. A network administrator notices that some newly installed Ethernet cabling is carrying corrupt and distorted data signals. The new cabling was installed in the ceiling close to fluorescent lights and electrical equipment. Which two factors may interfere with the copper cabling and result in signal distortion and data corruption? (Choose two.)**

* **EMI\***
* crosstalk
* **RFI\***
* signal attenuation
* extended length of cabling

**Explain:**  
EMI and RFI signals can distort and corrupt data signals that are carried by copper media. These distortions usually come from radio waves and electromagnetic devices such as motors and florescent lights. Crosstalk is a disturbance that is caused by adjacent wires bundled too close together with the magnetic field of one wire affecting another. Signal attenuation is caused when an electrical signal begins to deteriorate over the length of a copper cable.

**4. Which characteristic describes crosstalk?**

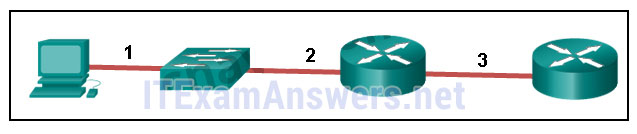
* the distortion of the network signal from fluorescent lighting
* **the distortion of the transmitted messages from signals carried in adjacent wires\***
* the weakening of the network signal over long cable lengths
* the loss of wireless signal over excessive distance from the access point

**Explain:**  
EMI and RFI can distort network signals because of interference from fluorescent lights or electric motors. Attenuation results in deterioration of the network signal as it travels along copper cabling. Wireless devices can experience loss of signals because of excessive distances from a access point, but this is not crosstalk. Crosstalk is the disturbance caused by the electric or magnetic fields of the signal carried on an adjacent wire within the same cable.

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

* **twisting the wires together into pairs\***
* wrapping a foil shield around the wire pairs
* encasing the cables within a flexible plastic sheath
* terminating the cable with special grounded connectors

**Explain:**  
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.

**6. Refer to the exhibit. The PC is connected to the console port of the switch. All the other connections are made through FastEthernet links. Which types of UTP cables can be used to connect the devices?**  


* 1 – rollover, 2 – crossover, 3 – straight-through
* **1 – rollover, 2 – straight-through, 3 – crossover\***
* 1 – crossover, 2 – straight-through, 3 – rollover
* 1 – crossover, 2 – rollover, 3 – straight-through

**Explain:**  
A straight-through cable is commonly used to interconnect a host to a switch and a switch to a router. A crossover cable is used to interconnect similar devices together like switch to a switch, a host to a host, or a router to a router. If a switch has the MDIX capability, a crossover could be used to connect the switch to the router; however, that option is not available. A rollover cable is used to connect to a router or switch console port.

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


* The woven copper braid should not have been removed.
* The wrong type of connector is being used.
* **The untwisted length of each wire is too long.\***
* The wires are too thick for the connector that is used.

**Explain:**  
When a cable to an RJ-45 connector is terminated, it is important to ensure that the untwisted wires are not too long and that the flexible plastic sheath surrounding the wires is crimped down and not the bare wires. None of the colored wires should be visible from the bottom of the jack.

**8. Which type of connector does a network interface card use?**

* DIN
* PS-2
* RJ-11
* **RJ-45\***

**9. What is one advantage of using fiber optic cabling rather than copper cabling?**

* It is usually cheaper than copper cabling.
* It is able to be installed around sharp bends.
* It is easier to terminate and install than copper cabling.
* **It is able to carry signals much farther than copper cabling.\***

**Explain:**  
Copper cabling is usually cheaper and easier to install than fiber optic cabling. However, fiber cables generally have a much greater signaling range than copper.

**10. Why are two strands of fiber used for a single fiber optic connection?**

* The two strands allow the data to travel for longer distances without degrading.
* They prevent crosstalk from causing interference on the connection.
* They increase the speed at which the data can travel.
* **They allow for full-duplex connectivity.\***

**Explain:**  
Light can only travel in one direction down a single strand of fiber. In order to allow for full-duplex communication two strands of fiber must be connected between each device.

**11. 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.)**

* mobility options
* **security \***
* **interference \***
* **coverage area\***
* extensive cabling
* packet collision

**Explain:**  
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.

**12. Which layer of the OSI model is responsible for specifying the encapsulation method used for specific types of media?**

* application
* transport
* **data link\***
* physical

**Explain:**  
Encapsulation is a function of the data link layer. Different media types require different data link layer encapsulation.

**13. What are two services performed by the data link layer of the OSI model? (Choose two.)**

* It encrypts data packets.
* It determines the path to forward packets.
* **It accepts Layer 3 packets and encapsulates them into frames. \***
* **It provides media access control and performs error detection.\***
* It monitors the Layer 2 communication by building a MAC address table.

**Explain:**  
The data link layer is responsible for the exchange of frames between nodes over a physical network media. Specifically the data link layer performs two basic services:  
It accepts Layer 3 packets and encapsulates them into frames.  
It provides media access control and performs error detection.  
Path determination is a service provided at Layer 3. A Layer 2 switch builds a MAC address table as part of its operation, but path determination is not the service that is provided by the data link layer.

**14. What is true concerning physical and logical topologies?**

* The logical topology is always the same as the physical topology.
* Physical topologies are concerned with how a network transfers frames.
* Physical topologies display the IP addressing scheme of each network.
* **Logical topologies refer to how a network transfers data between devices.\***

**Explain:**  
Physical topologies show the physical interconnection of devices. Logical topologies show the way the network will transfer data between connected nodes.

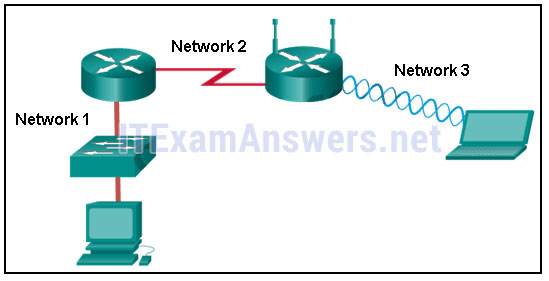
**15. Which method of data transfer allows information to be sent and received at the same time?**

* **full duplex\***
* half duplex
* multiplex
* simplex

**16. Which statement describes an extended star topology?**

* **End devices connect to a central intermediate device, which in turn connects to other central intermediate devices.\***
* End devices are connected together by a bus and each bus connects to a central intermediate device.
* Each end system is connected to its respective neighbor via an intermediate device.
* All end and intermediate devices are connected in a chain to each other.

**Explain:**  
In an extended star topology, central intermediate devices interconnect other star topologies.

**17. Refer to the exhibit. Which statement describes the media access control methods that are used by the networks in the exhibit?**  


* All three networks use CSMA/CA
* None of the networks require media access control.
* **Network 1 uses CSMA/CD and Network 3 uses CSMA/CA.\***
* Network 1 uses CSMA/CA and Network 2 uses CSMA/CD.
* Network 2 uses CSMA/CA and Network 3 uses CSMA/CD.

**Explain:**  
Network 1 represents an Ethernet LAN. Data on the wired LAN accesses the media using CSMA/CD. Network 2 represents a point-to-point WAN connection so no media access method is required. Network 3 represents a WLAN and data accesses the network using CSMA/CA.

**18. What is contained in the trailer of a data-link frame?**

* logical address
* physical address
* data
* **error detection\***

**Explain:**  
The trailer in a data-link frame contains error detection information that is pertinent to the frame included in the FCS field. The header contains control information, such as the addressing, while the area that is indicated by the word “data” includes the data, transport layer PDU, and the IP header.

**19. As data travels on the media in a stream of 1s and 0s how does a receiving node identify the beginning and end of a frame?**

* **The transmitting node inserts start and stop bits into the frame.\***
* The transmitting node sends a beacon to notify that a data frame is attached.
* The receiving node identifies the beginning of a frame by seeing a physical address.
* The transmitting node sends an out-of-band signal to the receiver about the beginning of the frame.

**Explain:**  
When data travels on the media, it is converted into a stream of 1s and 0s. The framing process inserts into the frame start and stop indicator flags so that the destination can detect the beginning and end of the frame.

**20. What is a role of the Logical Link Control sublayer?**

* to provide data link layer addressing
* to provide access to various Layer 1 network technologies
* to define the media access processes performed by network hardware
* **to mark frames to identify the network layer protocol being carried\***

**Explain:**There are two data link sublayers, MAC and LLC. The LLC sublayer is responsible for communicating with the network layer and for tagging frames to identify what Layer 3 protocol is encapsulated.

**21. What is the definition of bandwidth?**

* the measure of usable data transferred over a given period of time
* the speed at which bits travel on the network
* the measure of the transfer of bits across the media over a given period of time
* **the amount of data that can flow from one place to another in a given amount of time\***

**Explain:**Bandwidth is the measure of the capacity of a network medium to carry data. It is the amount of data that can move between two points on the network over a specific period of time, typically one second.

**22. What is the function of the CRC value that is found in the FCS field of a frame?**

* **to verify the integrity of the received frame\***
* to verify the physical address in the frame
* to verify the logical address in the frame
* to compute the checksum header for the data field in the frame

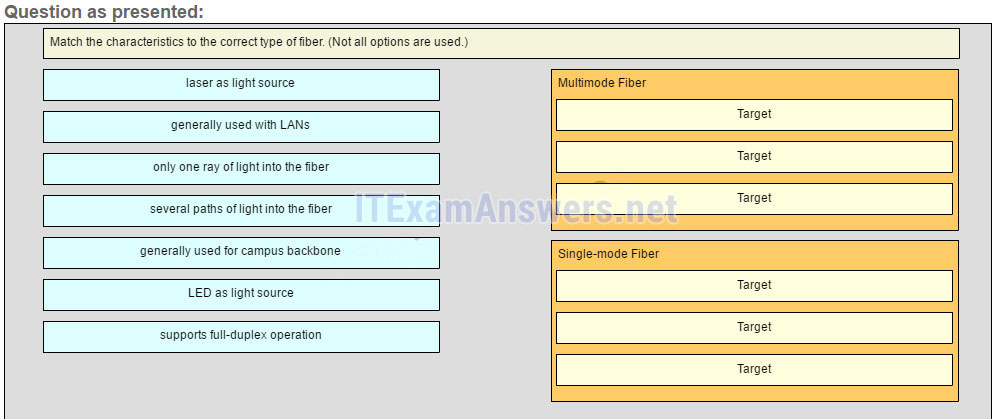
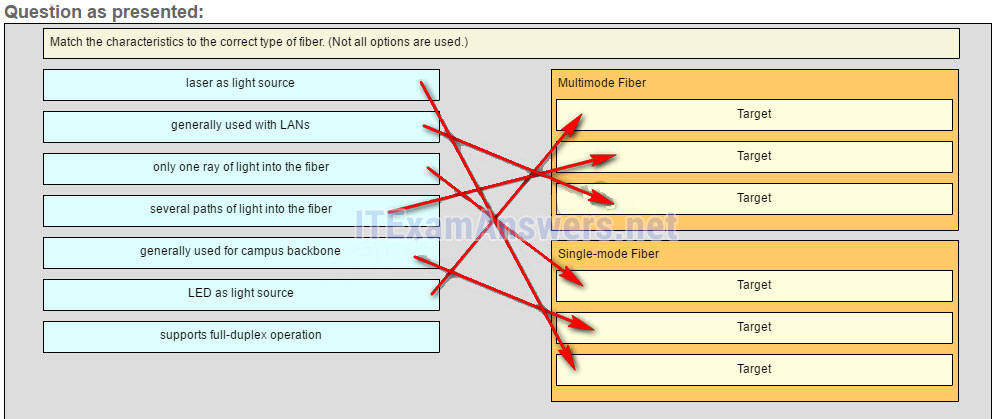
**Explain:**  
The CRC value in the FCS field of the received frame is compared to the computed CRC value of that frame, in order to verify the integrity of the frame. If the two values do not match, then the frame is discarded.

**23. Fill in the blank.**  
The term **bandwidth** indicates the capacity of a medium to carry data and it is typically measured in kilobits per second (kb/s) or megabits per second (Mb/s).

**Explain:**  
Bandwidth is the capacity of a medium to carry data in a given amount of time. It is typically measured in kilobits per second (kb/s) or megabits per second (Mb/s).​

**24. Fill in the blank.**  
What acronym is used to reference the data link sublayer that identifies the network layer protocol encapsulated in the frame? **LLC**

**Explain:**  
Logical Link Control (LLC) is the data link sublayer that defines the software processes that provide services to the network layer protocols. LLC places information in the frame and that information identifies the network layer protocol that is encapsulated in the frame.

**25. Match the characteristics to the correct type of fiber. (Not all options are used.)**  
  
  
**Multimode Fiber**  
**LED as light source\***  
**several paths of light into the fiber\***  
**generally used with LANs\***  
**Single-mode Fiber**  
**only one ray of light into the fiber\***  
**generally used for campus backbone\***  
**laser as light source\***

**Explain:**  
Single-mode fiber uses a laser as the light source. Its small core produces a single straight path for light and it is commonly used with campus backbones. Multimode fiber uses LEDs as the light source. Its larger core allows for multiple paths for the light. It is commonly used with LANs.

**26. Fill in the blank.**  
A physical topology that is a variation or combination of a point-to-point, hub and spoke, or mesh topology is commonly known as a **hybrid** topology.

**Explain:**  
A hybrid topology is a variation or combination of a point-to-point, hub and spoke, or mesh topology. This may include a partial mesh or extended star topology.

**27. What are two examples of hybrid topologies? (Choose two.)**

* point-to-point
* **partial mesh\***
* **extended star\***
* hub and spoke
* full mesh

**Explain:**A hybrid topology is one that is a variation or a combination of other topologies. Both partial mesh and the extended star are examples of hybrid topologies.

## Other Quetions

**28. Which statement describes signaling at the physical layer?**

* **Sending the signals asynchronously means that they are transmitted without a clock signal.\***
* In signaling, a 1 always represents voltage and a 0 always represents the absence of voltage.
* Wireless encoding includes sending a series of clicks to delimit the frames.
* Signaling is a method of converting a stream of data into a predefined code

**29. The throughput of a FastEthernet network is 80 Mb/s. The traffic overhead for establishing sessions, acknowledgments, and encapsulation is 15 Mb/s for the same time period. What is the goodput for this network?**

* 15 Mb/s
* 95 Mb/s
* 55 Mb/s
* **65 Mb/s\***
* 80 Mb/s

**30. How is the magnetic field cancellation effect enhanced in UTP cables?**

* by increasing the thickness of the PVC sheath that encases all the wires
* **by increasing and varying the number of twists in each wire pair\***
* by increasing the thickness of the copper wires
* by decreasing the number of wires that are used to carry data

**31. Which statement is correct about multimode fiber?**

* Multimode fiber cables carry signals from multiple connected sending devices.
* Multimode fiber commonly uses a laser as a light source.
* **SC-SC patch cords are used with multimode fiber cables.\***
* Multimode fiber has a thinner core than single-mode fiber..

**32. A network administrator is required to upgrade wireless access to end users in a building. To provide data rates up to 1.3 Gb/s and still be backward compatible with older devices, which wireless standard should be implemented?**

* 802.11n
* **802.11ac\***
* 802.11g
* 802.11b

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

* It generates the electrical or optical signals that represent the 1 and 0 on the media.
* It converts a stream of data bits into a predefined code.
* **It shields the upper layer protocol from being aware of the physical medium to be used in the communication.\***
* It accepts Layer 3 packets and decides the path by which to forward a frame to a host on a remote network.

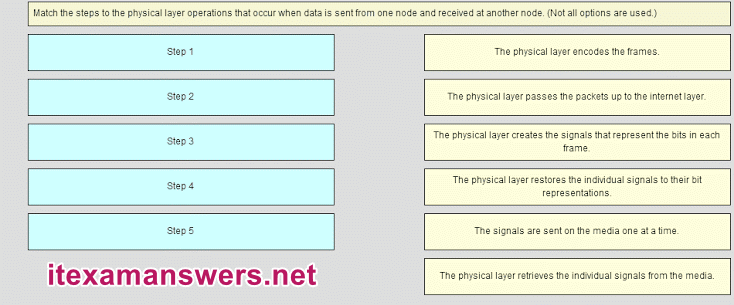
**34. What are two characteristics of 802.11 wireless networks? (Choose two.)**

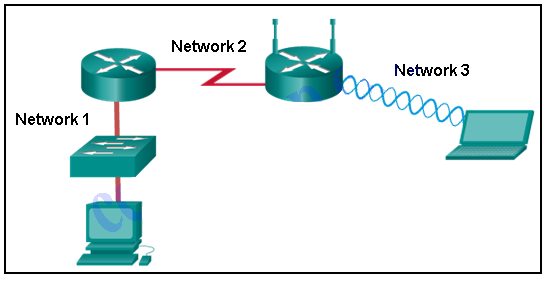
* **They use CSMA/CA technology.\***
* They use CSMA/CD technology.
* They are collision-free networks.
* Stations can transmit at any time.
* **Collisions can exist in the networks.\***

**35. What is the purpose of the FCS field in a frame?**

* to obtain the MAC address of the sending node
* to verify the logical address of the sending node
* to compute the CRC header for the data field
* **to determine if errors occurred in the transmission and reception\***

**36. Fill in the blank with a number.**  
10,000,000,000 b/s can also be written as 10 Gb/s.

**37. Match the steps to the physical layer operations that occur when data is sent from one node and received at another node.**  
  
**Sort elements**  
**The physical layer encodes the frames** -> **Step 1\***  
**The physical layer creates the signals that represent the bits in each frame** -> **Step 2\***  
**The signals are sent on the media one at a time.** -> **Step 3**   
**The physical layer retrieves the individual signals from the media** -> **Step 4**   
**The physical layer restores the individual signals to their bit representations** -> **Step 5\***

**38. Refer to the exhibit.**  
  
**Which statement describes the media access control methods that are used by the networks in the exhibit?**  
All three networks use CSMA/CA  
None of the networks require media access control.  
**Network 1 uses CSMA/CD and Network 3 uses CSMA/CA.\*\***  
Network 1 uses CSMA/CA and Network 2 uses CSMA/CD.  
Network 2 uses CSMA/CA and Network 3 uses CSMA/CD.

# CCNA 1 (v5.1 + v6.0) Chapter 5 Exam Answers 2019 – 100% Full

**1. What happens to runt frames received by a Cisco Ethernet switch?**

* **The frame is dropped.\***
* The frame is returned to the originating network device.
* The frame is broadcast to all other devices on the same network.
* The frame is sent to the default gateway.

**Explain:**  
In an attempt to conserve bandwidth and not forward useless frames, Ethernet devices drop frames that are considered to be runt (less than 64 bytes) or jumbo (greater than 1500 bytes) frames.

**2. What are the two sizes (minimum and maximum) of an Ethernet frame? (Choose two.)**

* 56 bytes
* **64 bytes\***
* 128 bytes
* 1024 bytes
* **1518 bytes\***

**Explain:**  
The minimum Ethernet frame is 64 bytes. The maximum Ethernet frame is 1518 bytes. A network technician must know the minimum and maximum frame size in order to recognize runt and jumbo frames.

**3. What statement describes Ethernet?**

* **It defines the most common LAN type in the world.\***
* It is the required Layer 1 and 2 standard for Internet communication.
* It defines a standard model used to describe how networking works.
* It connects multiple sites such as routers located in different countries.

**Explain:**  
Ethernet is the most common LAN protocol in the world. It operates at Layer 1 and 2, but is not required for Internet communication. The OSI model is used to describe how networks operate. A WAN connects multiple sites located in different countries.

**4. Which two statements describe features or functions of the logical link control sublayer in Ethernet standards? (Choose two.)**

* **Logical link control is implemented in software.\***
* Logical link control is specified in the IEEE 802.3 standard.
* The LLC sublayer adds a header and a trailer to the data.
* **The data link layer uses LLC to communicate with the upper layers of the protocol suite.\***
* The LLC sublayer is responsible for the placement and retrieval of frames on and off the media.

**Explain:**  
Logical link control is implemented in software and enables the data link layer to communicate with the upper layers of the protocol suite. Logical link control is specified in the IEEE 802.2 standard. IEEE 802.3 is a suite of standards that define the different Ethernet types. The MAC (Media Access Control) sublayer is responsible for the placement and retrieval of frames on and off the media. The MAC sublayer is also responsible for adding a header and a trailer to the network layer protocol data unit (PDU).

**5. What statement describes a characteristic of MAC addresses?**

* **They must be globally unique.\***
* They are only routable within the private network.
* They are added as part of a Layer 3 PDU.
* They have a 32-bit binary value.

**Explain:**  
Any vendor selling Ethernet devices must register with the IEEE to ensure the vendor is assigned a unique 24-bit code, which becomes the first 24 bits of the MAC address. The last 24 bits of the MAC address are generated per hardware device. This helps to ensure globally unique addresses for each Ethernet device.

**6. Which statement is true about MAC addresses?**

* MAC addresses are implemented by software.
* A NIC only needs a MAC address if connected to a WAN.
* **The first three bytes are used by the vendor assigned OUI.\***
* The ISO is responsible for MAC addresses regulations.

**Explain:**  
A MAC address is composed of 6 bytes. The first 3 bytes are used for vendor identification and the last 3 bytes must be assigned a unique value within the same OUI. MAC addresses are implemented in hardware. A NIC needs a MAC address to communicate over the LAN. The IEEE regulates the MAC addresses.

**7. Which destination address is used in an ARP request frame?**

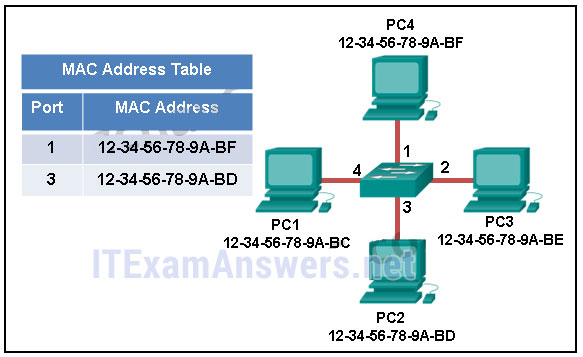
* 0.0.0.0
* 255.255.255.255
* **FFFF.FFFF.FFFF\***
* 127.0.0.1
* 01-00-5E-00-AA-23

**Explain:**  
The purpose of an ARP request is to find the MAC address of the destination host on an Ethernet LAN. The ARP process sends a Layer 2 broadcast to all devices on the Ethernet LAN. The frame contains the IP address of the destination and the broadcast MAC address, FFFF.FFFF.FFFF.

**8. What addressing information is recorded by a switch to build its MAC address table?**

* the destination Layer 3 address of incoming packets
* the destination Layer 2 address of outgoing frames
* the source Layer 3 address of outgoing packets
* **the source Layer 2 address of incoming frames\***

**Explain:**  
A switch builds a MAC address table by inspecting incoming Layer 2 frames and recording the source MAC address found in the frame header. The discovered and recorded MAC address is then associated with the port used to receive the frame.

**9. Refer to the exhibit. The exhibit shows a small switched network and the contents of the MAC address table of the switch. PC1 has sent a frame addressed to PC3. What will the switch do with the frame?**  


* The switch will discard the frame.
* The switch will forward the frame only to port 2.
* **The switch will forward the frame to all ports except port 4.\***
* The switch will forward the frame to all ports.
* The switch will forward the frame only to ports 1 and 3.

**Explain:**  
The MAC address of PC3 is not present in the MAC table of the switch. Because the switch does not know where to send the frame that is addressed to PC3, it will forward the frame to all the switch ports, except for port 4, which is the incoming port.

**10. Which switching method uses the CRC value in a frame?**

* cut-through
* fast-forward
* fragment-free
* **store-and-forward\***

**Explain:**  
When the store-and-forward switching method is used, the switch receives the complete frame before forwarding it on to the destination. The cyclic redundancy check (CRC) part of the trailer is used to determine if the frame has been modified during transit.​​ In contrast, a cut-through switch forwards the frame once the destination Layer 2 address is read. Two types of cut-through switching methods are fast-forward and fragment-free.

**11. What is auto-MDIX?**

* a type of Cisco switch
* an Ethernet connector type
* a type of port on a Cisco switch
* **a feature that detects Ethernet cable type\***

**Explain:**  
Auto-MDIX is a feature that is enabled on the latest Cisco switches and that allows the switch to detect and use whatever type of cable is attached to a specific port.​​

**12. 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?**  


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

**Explain:**  
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.

**13. What is the aim of an ARP spoofing attack?**

* **to associate IP addresses to the wrong MAC address\***
* to overwhelm network hosts with ARP requests
* to flood the network with ARP reply broadcasts
* to fill switch MAC address tables with bogus addresses

**14. What is a characteristic of port-based memory buffering?**

* Frames in the memory buffer are dynamically linked to destination ports.
* All frames are stored in a common memory buffer.
* **Frames are buffered in queues linked to specific ports.\***
* All ports on a switch share a single memory buffer.

**Explain:**Buffering is a technique used by Ethernet switches to store frames until they can be transmitted. With port-based buffering, frames are stored in queues that are linked to specific incoming and outgoing ports.

**15. What is the minimum Ethernet frame size that will not be discarded by the receiver as a runt frame?**

* **64 bytes\***
* 512 bytes
* 1024 bytes
* 1500 bytes

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

 Manually configuring static ARP associations could facilitate ARP poisoning or MAC address spoofing.

 **On large networks with low bandwidth, multiple ARP broadcasts could cause data communication delays. \***

 **Network attackers could manipulate MAC address and IP address mappings in ARP messages with the intent of intercepting network traffic.\***

 Large numbers of ARP request broadcasts could cause the host MAC address table to overflow and prevent the host from communicating on the network.

 Multiple ARP replies result in the switch MAC address table containing entries that match the MAC addresses of hosts that are connected to the relevant switch port.

**Explain:**  
Large numbers of ARP broadcast messages could cause momentary data communications delays. Network attackers could manipulate MAC address and IP address mappings in ARP messages with the intent to intercept network traffic. ARP requests and replies cause entries to be made into the ARP table, not the MAC address table. ARP table overflows are very unlikely. Manually configuring static ARP associations is a way to prevent, not facilitate, ARP poisoning and MAC address spoofing. Multiple ARP replies resulting in the switch MAC address table containing entries that match the MAC addresses of connected nodes and are associated with the relevant switch port are required for normal switch frame forwarding operations. It is not an ARP caused network problem.

**17. Fill in the blank.**  
A collision fragment, also known as a **RUNT** frame, is a frame of fewer than 64 bytes in length.

**Explain:**  
A runt frame is a frame of fewer than 64 bytes, usually generated by a collision or a network interface failure.

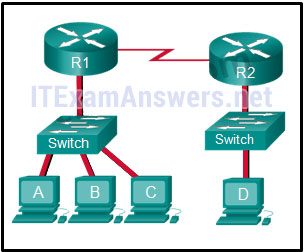
**18. Fill in the blank.**  
On a Cisco switch, **port-based** memory buffering is used to buffer frames in queues linked to specific incoming and outgoing ports.

**19. Fill in the blank.**  
ARP **spoofing** is a technique that is used to send fake ARP messages to other hosts in the LAN. The aim is to associate IP addresses to the wrong MAC addresses.

**Explain:**  
ARP spoofing or ARP poisoning is a technique used by an attacker to reply to an ARP request for an IPv4 address belonging to another device, such as the default gateway.

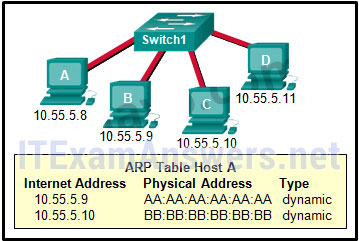
**20. Which statement describes the treatment of ARP requests on the local link?**

* They must be forwarded by all routers on the local network.
* **They are received and processed by every device on the local network.\***
* They are dropped by all switches on the local network.
* They are received and processed only by the target device.

**21. 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?**  


* only host D
* only router R1
* only hosts A, B, and C
* only hosts A, B, C, and D
* only hosts B and C
* **only hosts B, C, and router R1\***

**Explain:**  
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.

**22. Refer to the exhibit. A switch with a default configuration connects four hosts. The ARP table for host A is shown. What happens when host A wants to send an IP packet to host D?**  


* Host A sends an ARP request to the MAC address of host D.
* Host D sends an ARP request to host A.
* Host A sends out the packet to the switch. The switch sends the packet only to the host D, which in turn responds.
* **Host A sends out a broadcast of FF:FF:FF:FF:FF:FF. Every other host connected to the switch receives the broadcast and host D responds with its MAC address.\***

**Explain:**  
Whenever the destination MAC address is not contained within the ARP table of the originating host, the host (host A in this example) will send a Layer 2 broadcast that has a destination MAC address of FF:FF:FF:FF:FF:FF. All devices on the same network receive this broadcast. Host D will respond to this broadcast.

**23. True or False?**  
**When a device is sending data to another device on a remote network, the Ethernet frame is sent to the MAC address of the default gateway.**

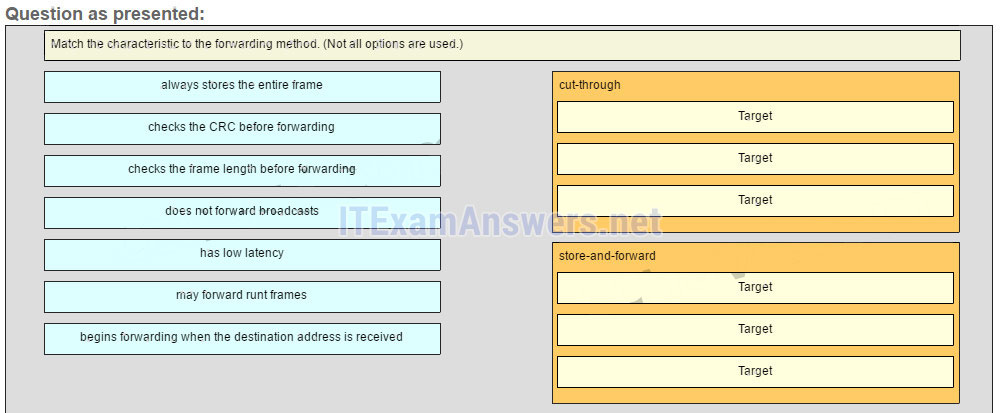
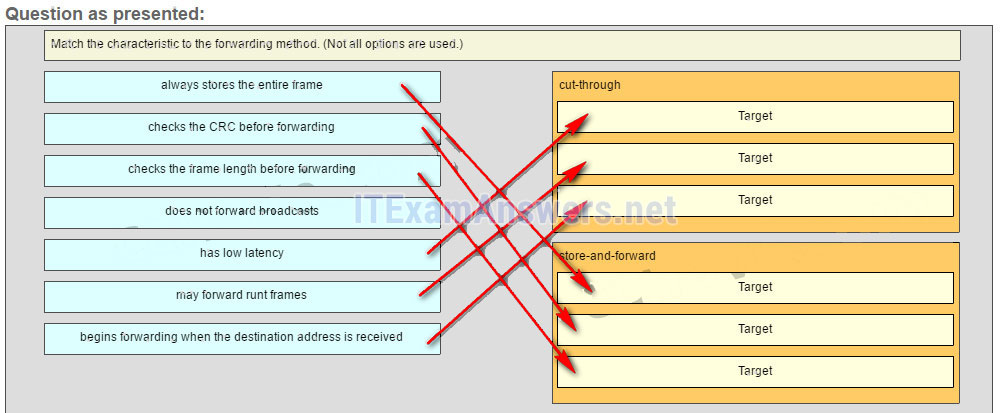
* **true\***
* false

**Explain:**  
A MAC address is only useful on the local Ethernet network. When data is destined for a remote network of any type, the data is sent to the default gateway device, the Layer 3 device that routes for the local network.

**24. The ARP table in a switch maps which two types of address together?**

* **Layer 3 address to a Layer 2 address\***
* Layer 3 address to a Layer 4 address
* Layer 4 address to a Layer 2 address
* Layer 2 address to a Layer 4 address

**Explain:**  
The switch ARP table keeps a mapping of Layer 2 MAC addresses to Layer 3 IP addresses. These mappings can be learned by the switch dynamically through ARP or statically through manual configuration.

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


**Sort elements**  
**cut-through (A) -> low latency (A)\***  
**cut-through (B) -> may forward runt frames (B)\***  
**cut-through (C) -> begins forwarding when the destination address is received (C)\***  
**store-and-forward (D) -> always stores the entire frame (D)\***  
**store-and-forward (E) -> checks the CRC before forwarding (E)\***  
**store-and-forward (F) -> checks the frame length before forwarding (F)**

**Explain:**  
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.

## Other Questions

**26. What is a characteristic of a contention-based access method?**

* It processes more overhead than the controlled access methods do.
* It has mechanisms to track the turns to access the media.
* **It is a nondeterministic method.\***
* It scales very well under heavy media use.

**27. What is the purpose of the preamble in an Ethernet frame?**

* is used as a padding for data
* **is used for timing synchronization\***
* is used to identify the source address
* is used to identify the destination address

**28. What is the Layer 2 multicast MAC address that corresponds to the Layer 3 IPv4 multicast address 224.139.34.56?**

* 00-00-00-0B-22-38
* **01-00-5E-0B-22-38\***
* 01-5E-00-0B-22-38
* FE-80-00-0B-22-38
* FF-FF-FF-0B-22-38

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

* A packet that has crossed four routers has changed the destination IP address four times.
* Destination MAC addresses will never change in a frame that goes across seven routers.
* **Destination and source MAC addresses have local significance and change every time a frame goes from one LAN to another. \***
* **Destination IP addresses in a packet header remain constant along the entire path to a target host.\***
* Every time a frame is encapsulated with a new destination MAC address, a new destination IP address is needed.

**30. What are two features of ARP? (Choose two.)**

* **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.\***
* 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.
* When a host is encapsulating a packet into a frame, it refers to the MAC address table to determine the mapping of IP addresses to MAC addresses.
* If no device responds to the ARP request, then the originating node will broadcast the data packet to all devices on the network segment.
* **If a device receiving an ARP request has the destination IPv4 address, it responds with an ARP reply.\***

**31. 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?**

* It will send an ARP request for the MAC address of the destination device.
* **It will send an ARP request for the MAC address of the default gateway. \***
* **It will send the frame and use its own MAC address as the destination. \***
* It will send the frame with a broadcast MAC address.
* It will send a request to the DNS server for the destination MAC address.

**32. A network administrator is connecting two modern switches using a straight-through cable. The switches are new and have never been configured. Which three statements are correct about the final result of the connection? (Choose three.)**

* **The link between the switches will work at the fastest speed that is supported by both switches. \***
* **The link between switches will work as full-duplex.\***
* If both switches support different speeds, they will each work at their own fastest speed.
* **The auto-MDIX feature will configure the interfaces eliminating the need for a crossover cable.\***
* The connection will not be possible unless the administrator changes the cable to a crossover cable.
* The duplex capability has to be manually configured because it cannot be negotiated.

**33. A Layer 2 switch is used to switch incoming frames from a 1000BASE-T port to a port connected to a 100Base-T network. Which method of memory buffering would work best for this task?**

* port-based buffering
* level 1 cache buffering
* **shared memory buffering\***
* fixed configuration buffering

**34. When would a switch record multiple entries for a single switch port in its MAC address table?**

* when a router is connected to the switch port
* when multiple ARP broadcasts have been forwarded
* **when another switch is connected to the switch port\***
* when the switch is configured for Layer 3 switching

**35. Which two statements describe a fixed configuration Ethernet switch? (Choose two.)**

* The switch cannot be configured with multiple VLANs.
* An SVI cannot be configured on the switch.
* **A fixed configuration switch may be stackable. \***
* **The number of ports on the switch cannot be increased.\***
* The port density of the switch is determined by the Cisco IOS.

**36. How does adding an Ethernet line card affect the form factor of a switch?**

* by increasing the back plane switching speed
* **by expanding the port density\***
* by making the switch stackable
* by expanding the NVRAM capacity

**37. Which address or combination of addresses does a Layer 3 switch use to make forwarding decisions?**

* IP address only
* port address only
* MAC address only
* MAC and port addresses
* **MAC and IP addresses\***

**38. What statement illustrates a drawback of the CSMA/CD access method?**

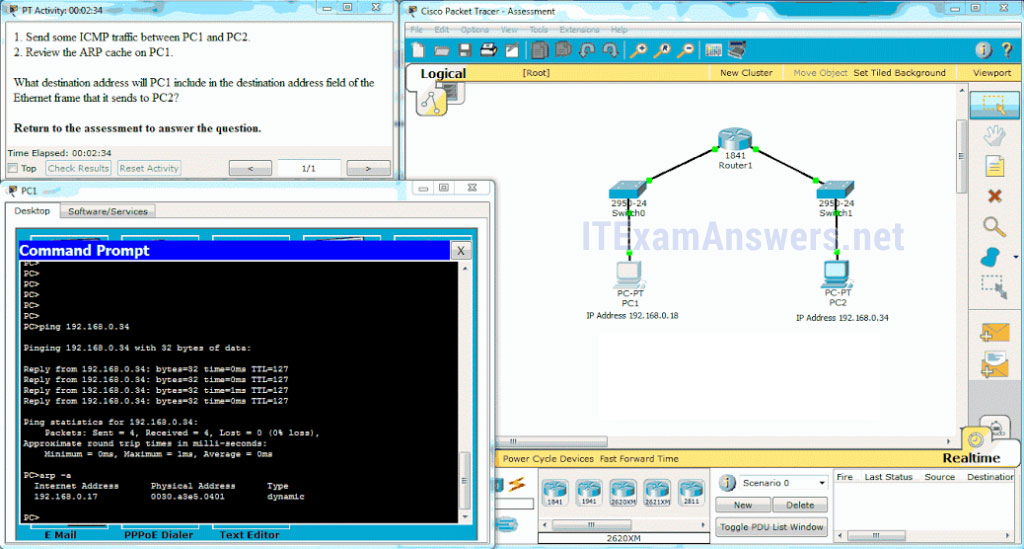
* Deterministic media access protocols slow network performance.
* It is more complex than non-deterministic protocols.
* **Collisions can decrease network performance.\***
* CSMA/CD LAN technologies are only available at slower speeds than other LAN technologies.

**39. Open the PT Activity. Perform the tasks in the activity instruction and then answer the question.**  
**What destination address will PC1 include in the destination address field of the Ethernet frame that it sends to PC2?**

* 192.168.0.17
* 192.168.0.34
* **0030.a3e5.0401\***
* 00e0.b0be.8014
* 0007.ec35.a5c6

**40. Which address or combination of addresses does a Layer 3 switch use to make forwarding decisions?**

* **MAC and IP addresses\***
* MAC address only
* MAC and port addresses
* port address only
* IP address only

**41. Launch PT. Hide and Save PT**  
  
**Open the PT Activity. Perform the tasks in the activity instruction and then answer the question. What destination address will PC1 include in the destination address field of the Ethernet frame that it sends to PC2?**

* 00e0.b0be.8014
* **0030.a3e5.0401\***
* 192.168.0.34
* 192.168.0.17
* 0007.ec35.a5c6

**42. How does adding an Ethernet line card affect the form factor of a switch?**

* by increasing the back plane switching speed
* **by expanding the port density\***
* by expanding the NVRAM capacity
* by making the switch stackable

**43. What statement illustrates a drawback of the CSMA/CD access method?**

* **Collisions can decrease network performance.\***
* Deterministic media access protocols slow network performance.
* CSMA/CD LAN technologies are only available at slower speeds than other LAN technologies.
* It is more complex than non-deterministic protocols.

**44. A network administrator issues the following commands on a Layer 3 switch:**

DLS1(config)# interface f0/3

DLS1(config-if)# no switchport

DLS1(config-if)# ip address 172.16.0.1 255.255.255.0

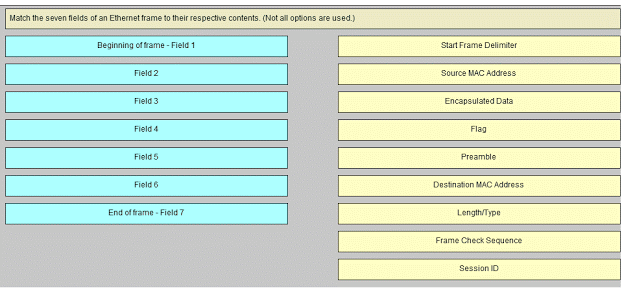
DLS1(config-if)# no shutdown

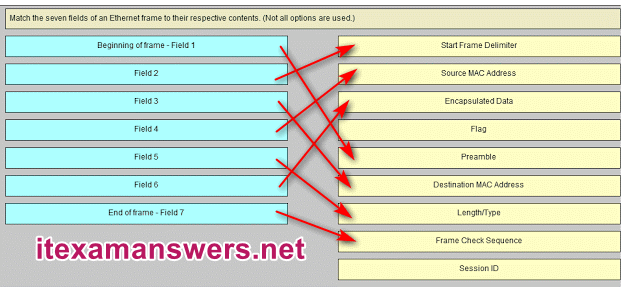
DLS1(config-if)# end

**What is the administrator configuring?**

* a Cisco Express Forwarding instance
* **a routed port\***
* a trunk interface
* a switched virtual interface

**45. The binary number 0000 1010 can be expressed as “A” in hexadecimal.  
Match the seven fields of an Ethernet frame to their respective contents. (Not all options are used.)**





**Sort elements**  
**Start Frame Delimiter -> Field 2\***  
**Source MAC Address -> Field 4\***  
**Encapsulated Data -> Field 6\***  
**Preamble -> Beginning of frame – Field 1\***  
**Destination MAC Address -> Field 3\***  
**Length/Type -> Field 5\***  
**Frame Check Sequence -> End of frame – Field 7**

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

**1. Which characteristic of the network layer in the OSI model allows carrying packets for multiple types of communications among many hosts?**

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

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

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

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

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

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

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

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

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

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

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

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

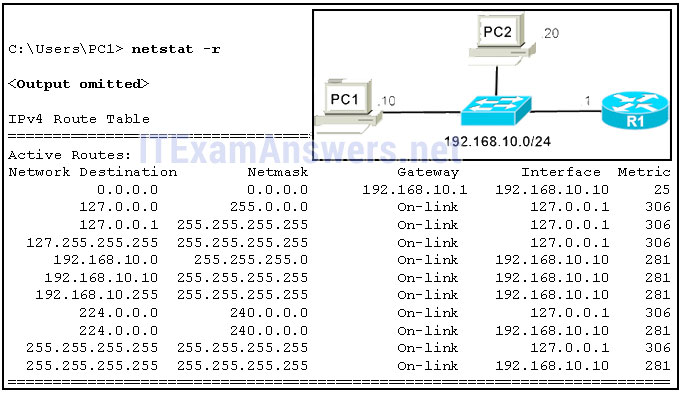
* **Protocol\***
* Identification
* Version
* Differentiated Services

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

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

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

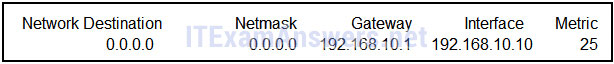
**Explain:**  
The IPv6 simplified header offers several advantages over IPv4:  
· Better routing efficiency and efficient packet handling for performance and forwarding-rate scalability  
· No requirement for processing checksums  
· Simplified and more efficient extension header mechanisms (as opposed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

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


A. 

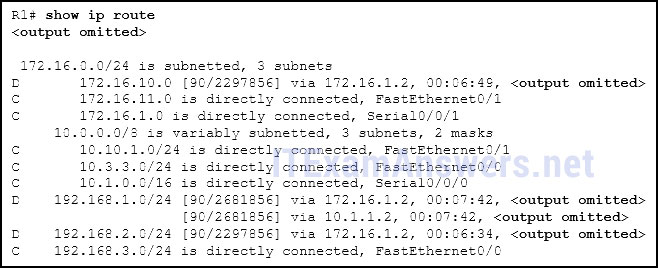
B. 

C. 

D. 

**Correct answer: A**

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

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


* FastEthernet0/0
* FastEthernet0/1
* Serial0/0/0
* **Serial0/0/1\***

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

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

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

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

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

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

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

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

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

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

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

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

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

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

* SVI
* **LAN\***
* DHCP
* Telnet
* **WAN\***

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

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

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

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

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

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

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

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

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

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

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

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

**18. Which characteristic describes an IPv6 enhancement over IPv4?**

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

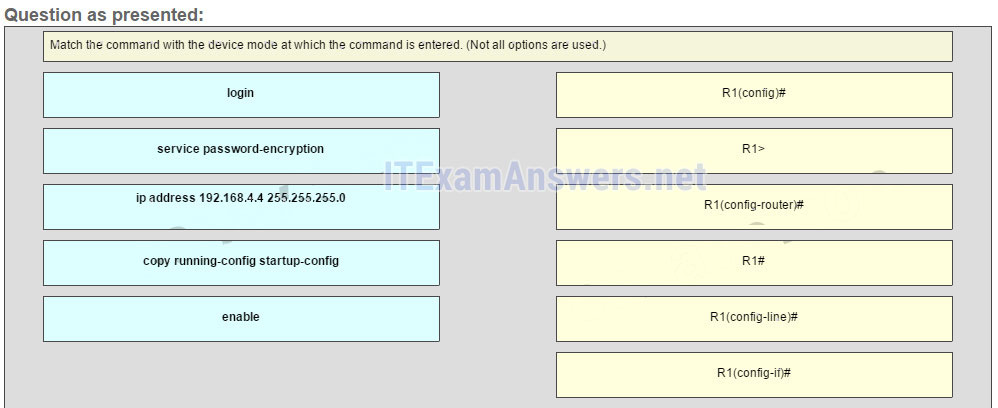
**Explain:**  
IPv6 addresses are based on 128-bit hierarchical addressing, and the IPv6 header has been simplified with fewer fields, improving packet handling. IPv6 natively supports authentication and privacy capabilities as opposed to IPv4 that needs additional features to support those. The IPv6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

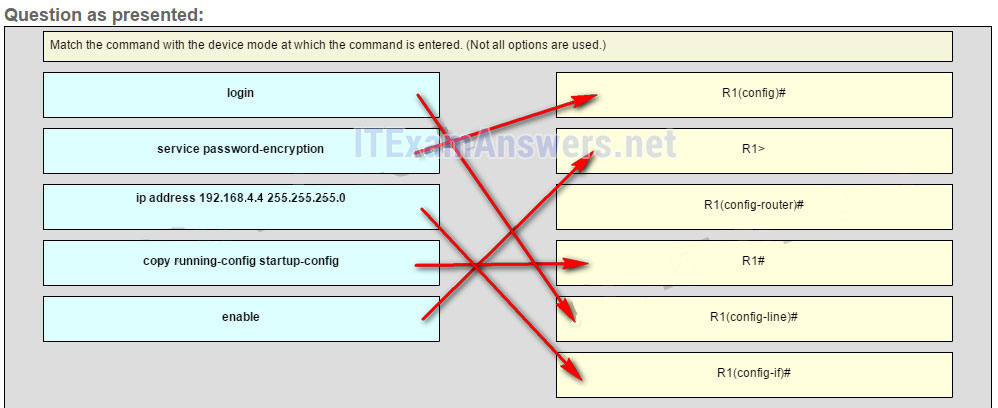
**19. Open the PT Activity. The enable password on all devices is cisco.  
Perform the tasks in the activity instructions and then answer the question.**  
**For what reason is the failure occurring?**

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

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

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

Question  


Answer  


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

## Other Questions

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

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

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

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

**23. Why is NAT not needed in IPv6?**

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

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

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

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

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

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

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

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

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

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

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

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

* aux interfaces
* **LAN interfaces \***
* **WAN interfaces\***
* console interfaces
* USB interfaces

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

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

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

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

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

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

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

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

**34. Which statement about router interfaces is true?**

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

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

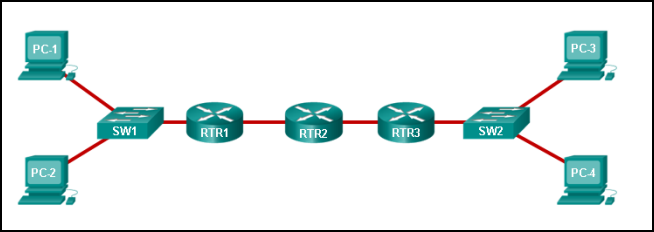
* show ip route
* show version
* show interfaces
* **show ip interface brief\***

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

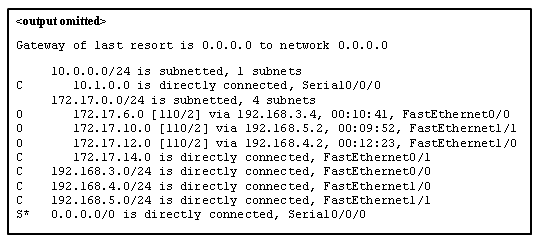
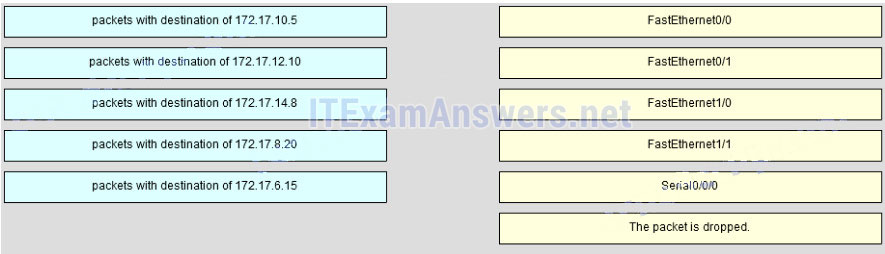
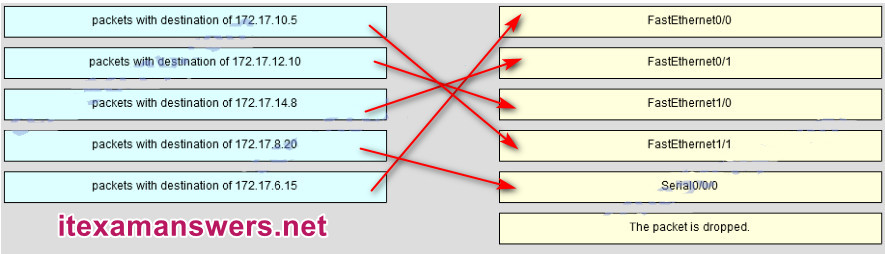
* the WINS server address
* **the default gateway address\***
* the MAC address
* the domain name of the organization

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

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

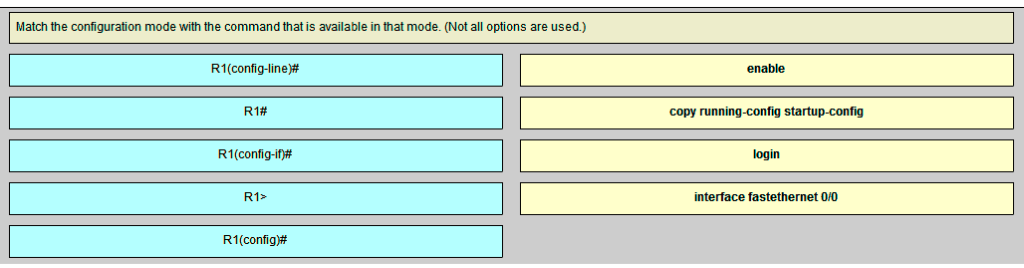
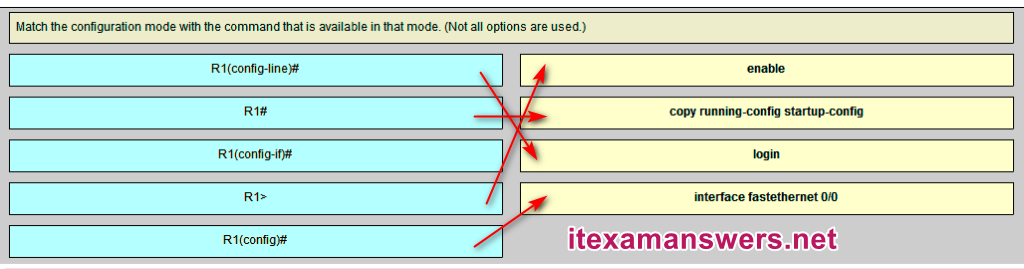
**38. Refer to the exhibit. Fill in the blank.**  
  
**A packet leaving PC-1 has to traverse 3 hops to reach PC-4.?**

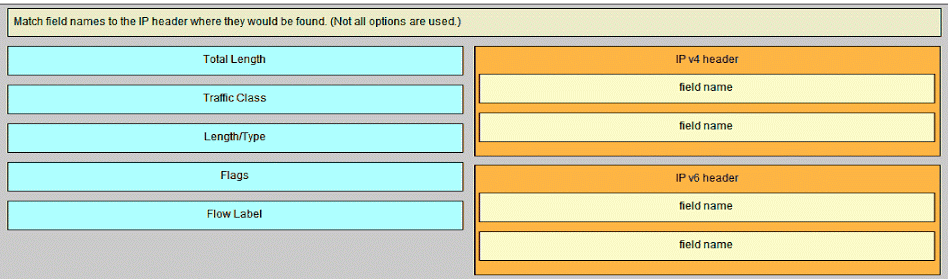
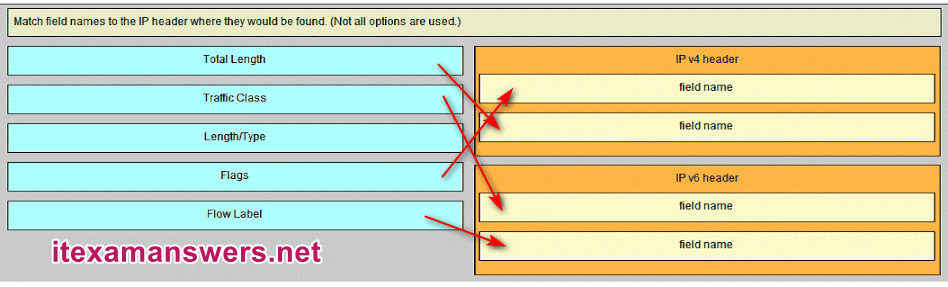
**39. Fill in the blank. In a router, ROM is the nonvolatile memory where the diagnostic software, the bootup instructions, and a limited IOS are stored.**

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


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

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

**42. Match the configuration mode with the command that is available in that mode. (Not all options are used.)**  
  
  
**Sort elements**  
**enable -> R1>**  
**copy running-config startup-config -> R1#**  
**login -> R1(config-line)#**  
**interface fastethernet 0/0 -> R1(config)#**

**43. Match field names to the IP header where they would be found. (Not all options are used)**  
  
  
**Sort elements**  
**IP v4 Header (A) -> Flags (A)**  
**IP v4 Header (B) -> Total Length (B)**  
**IP v6 Header (C) ->Traffic Class (C)**  
**IP v6 Header (D) -> Flow Label (D)**

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

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

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

**1. How many bits are in an IPv4 address?**

* **32\***
* 64
* 128
* 256

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

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

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

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

**3. What does the IP address 172.17.4.250/24 represent?**

* network address
* multicast address
* **host address\***
* broadcast address

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

**4. What is the purpose of the subnet mask in conjunction with an IP address?**

* to uniquely identify a host on a network
* to identify whether the address is public or private
* **to determine the subnet to which the host belongs\***
* to mask the IP address to outsiders

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

**5. What subnet mask is represented by the slash notation /20?**

* 255.255.255.248
* 255.255.224.0
* **255.255.240.0\***
* 255.255.255.0
* 255.255.255.192

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

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

* limited broadcast
* multicast
* **directed broadcast\***
* unicast

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

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

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

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

**8. Which three IP addresses are private ? (Choose three.)**

* **10.1.1.1\***
* 172.32.5.2
* 192.167.10.10
* **172.16.4.4 \***
* **192.168.5.5\***
* 224.6.6.6

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

**9. Which two IPv4 to IPv6 transition techniques manage the interconnection of IPv6 domains? (Choose two.)**

* trunking
* **dual stack\***
* encapsulation
* **tunneling\***
* multiplexing

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

**10. Which of these addresses is the shortest abbreviation for the IP address:  
3FFE:1044:0000:0000:00AB:0000:0000:0057?**

* 3FFE:1044::AB::57
* 3FFE:1044::00AB::0057
* **3FFE:1044:0:0:AB::57\***
* 3FFE:1044:0:0:00AB::0057
* 3FFE:1044:0000:0000:00AB::57
* 3FFE:1044:0000:0000:00AB::0057

**11. What type of address is automatically assigned to an interface when IPv6 is enabled on that interface?**

* global unicast
* **link-local\***
* loopback
* unique local

**Explain:**  
When IPv6 is enabled on any interface, that interface will automatically generate an IPv6 link-local address.

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

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

**Explain:**  
Multicast, anycast, and unicast are types of IPv6 addresses. There is no broadcast address in IPv6. Loopback and link-local are specific types of unicast addresses.

**13. What are three parts of an IPv6 global unicast address? (Choose three.)**

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

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

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

* SLAAC
* **stateless DHCPv6\***
* stateful DHCPv6
* RA and EUI-64

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

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

* ARPv6
* DHCPv6
* **ICMPv6\***
* UDP

**Explain:**  
SLAAC uses ICMPv6 messages when dynamically assigning an IPv6 address to a host. DHCPv6 is an alternate method of assigning an IPv6 addresses to a host. ARPv6 does not exist. Neighbor Discovery Protocol (NDP) provides the functionality of ARP for IPv6 networks. UDP is the transport layer protocol used by DHCPv6.

**16. Which two things can be determined by using the ping command? (Choose two.)**

* the number of routers between the source and destination device
* the IP address of the router nearest the destination device
* **the average time it takes a packet to reach the destination and for the response to return to the source \***
* **the destination device is reachable through the network\***
* the average time it takes each router in the path between source and destination to respond

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

**17. What is the purpose of ICMP messages?**

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

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

**18. What is indicated by a successful ping to the ::1 IPv6 address?**

* The host is cabled properly.
* The default gateway address is correctly configured.
* All hosts on the local link are available.
* The link-local address is correctly configured.
* **IP is properly installed on the host.\***

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

**19. A user is executing a tracert to a remote device. At what point would a router, which is in the path to the destination device, stop forwarding the packet?**

* when the router receives an ICMP Time Exceeded message
* when the RTT value reaches zero
* when the host responds with an ICMP Echo Reply message
* **when the value in the TTL field reaches zero\***
* when the values of both the Echo Request and Echo Reply messages reach zero

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

**20. What is the binary equivalent of the decimal number 232?**

* **11101000\***
* 11000110
* 10011000
* 11110010

**21. What is the decimal equivalent of the binary number 10010101?**

* **149**
* 157
* 168
* 192

**22. What field content is used by ICMPv6 to determine that a packet has expired?**

* TTL field
* CRC field
* **Hop Limit field\***
* Time Exceeded field

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

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

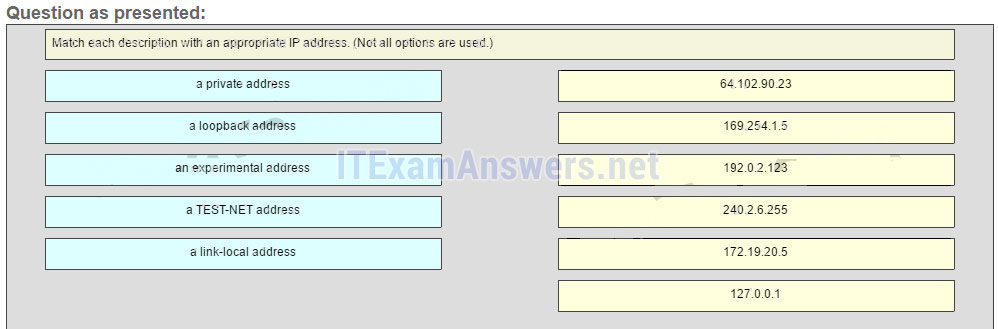
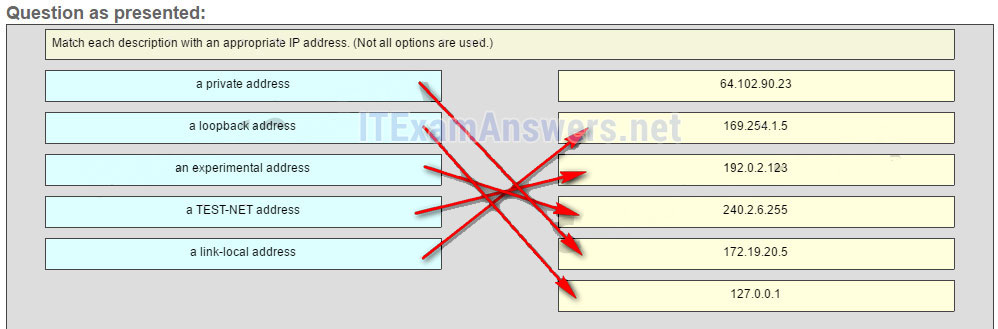
**Explain:**  
To convert a binary number to the decimal equivalent, add the value of the position where any binary 1 is present.

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

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

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

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

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


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

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

## Older Versions

**27. What is a socket?**

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

**28. A host device needs to send a large video file across the network while providing data communication to other users. Which feature will allow different communication streams to occur at the same time, without having a single data stream using all available bandwidth?**

* window size
* **multiplexing\***
* port numbers
* acknowledgments

**29. A host device sends a data packet to a web server via the HTTP protocol. What is used by the transport layer to pass the data stream to the proper application on the server?**

* sequence number
* acknowledgment
* source port number
* **destination port number\***

**30. What is a beneficial feature of the UDP transport protocol?**

* acknowledgment of received data
* **fewer delays in transmission\***
* tracking of data segments using sequence numbers
* the ability to retransmit lost data

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

* A student is using a classroom VoIP phone to call home. The unique identifier burned into the phone is a transport layer address used to contact another network device on the same network.
* A student is playing a short web-based movie with sound. The movie and sound are encoded within the transport layer header.
* **A student has two web browser windows open in order to access two web sites. The transport layer ensures the correct web page is delivered to the correct browser window.\***
* A corporate worker is accessing a web server located on a corporate network. The transport layer formats the screen so the web page appears properly no matter what device is being used to view the web site.

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

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

**33. What does a client application select for a TCP or UDP source port number?**

* a random value in the well-known port range
* **a random value in the range of the registered ports\***
* a predefined value in the well-known port range
* a predefined value in the range of the registered ports

**34. Compared to UDP, what factor causes additional network overhead for TCP communication?**

* **network traffic that is caused by retransmissions\***
* the identification of applications based on destination port numbers
* the encapsulation into IP packets
* the checksum error detection

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

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

**36. Which two flags in the TCP header are used in a TCP three-way handshake to establish connectivity between two network devices? (Choose two.)**

* **ACK\***
* FIN
* PSH
* RST
* **SYN\***
* URG

**37. Which factor determines TCP window size?**

* the amount of data to be transmitted
* the number of services included in the TCP segment
* **the amount of data the destination can process at one time\***
* the amount of data the source is capable of sending at one time

**38. During a TCP session, a destination device sends an acknowledgment number to the source device. What does the acknowledgment number represent?**

* the total number of bytes that have been received
* one number more than the sequence number
* **the next byte that the destination expects to receive\***
* the last sequence number that was sent by the source

**39. A PC is downloading a large file from a server. The TCP window is 1000 bytes. The server is sending the file using 100-byte segments. How many segments will the server send before it requires an acknowledgment from the PC?**

* 1 segment
* **10 segments\***
* 100 segments
* 1000 segments

**40. Which two TCP header fields are used to confirm receipt of data?**

* FIN flag
* SYN flag
* checksum
* **sequence number \***
* **acknowledgment number\***

**41. What happens if the first packet of a TFTP transfer is lost?**

* The client will wait indefinitely for the reply.
* **The TFTP application will retry the request if a reply is not received.\***
* The next-hop router or the default gateway will provide a reply with an error code.
* The transport layer will retry the query if a reply is not received.

**42. What does a client do when it has UDP datagrams to send?**

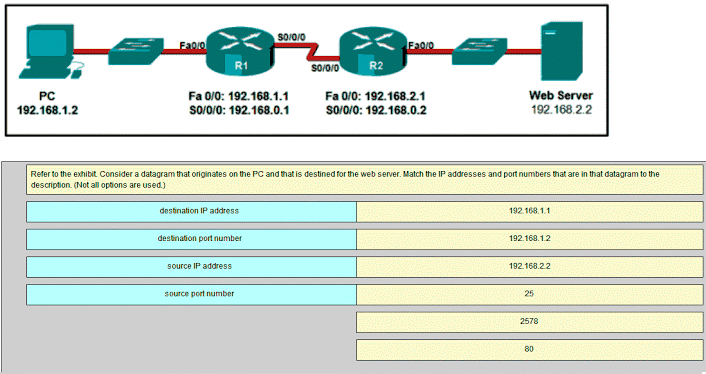
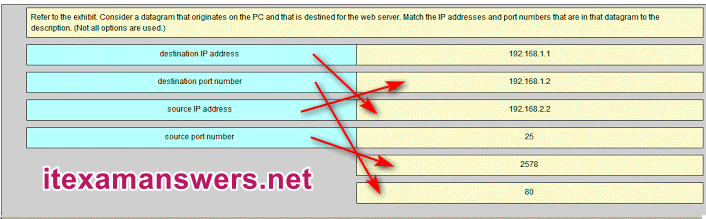
* **It just sends the datagrams.\***
* It queries the server to see if it is ready to receive data.
* It sends a simplified three-way handshake to the server.
* It sends to the server a segment with the SYN flag set to synchronize the conversation.

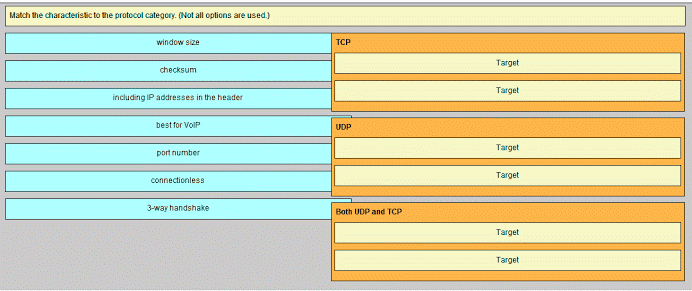
**43. A technician wishes to use TFTP to transfer a large file from a file server to a remote router. Which statement is correct about this scenario?**

* The file is segmented and then reassembled in the correct order by TCP.
* **The file is segmented and then reassembled in the correct order at the destination, if necessary, by the upper-layer protocol.**
* The file is not segmented, because UDP is the transport layer protocol that is used by TFTP.
* Large files must be sent by FTP not TFTP.

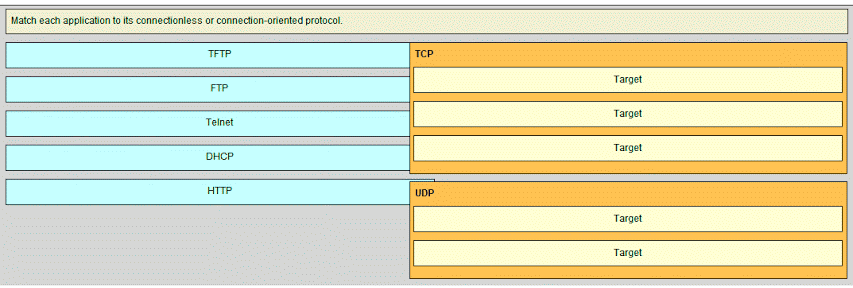
**44. Fill in the blank.**  
During a TCP session, the **SYN** flag is used by the client to request communication with the server.

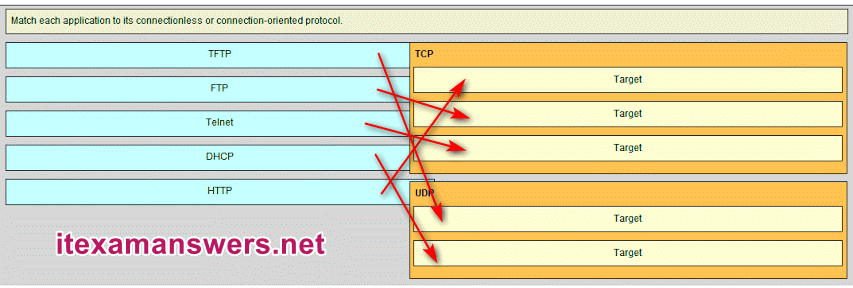
**45. Fill in the blank using a number.**  
A total of **4** messages are exchanged during the TCP session termination process between the client and the server.

**46. Refer to the exhibit. Consider a datagram that originates on the PC and that is destined for the web server. Match the IP addresses and port numbers that are in that datagram to the description. (Not all options are used.)**  
  
  
**192.168.1.2 -> source IP address**  
**192.168.2.2 -> destination IP address**  
**2578 -> source port number**  
**80 -> destination port number**

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


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

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


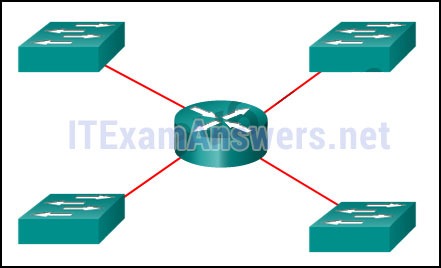
  
**TCP -> HTTP**   
**TCP -> FTP**   
**TCP -> TELNET**  
**UDP -> TFTP**  
**UDP -> DHCP**

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

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

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

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

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


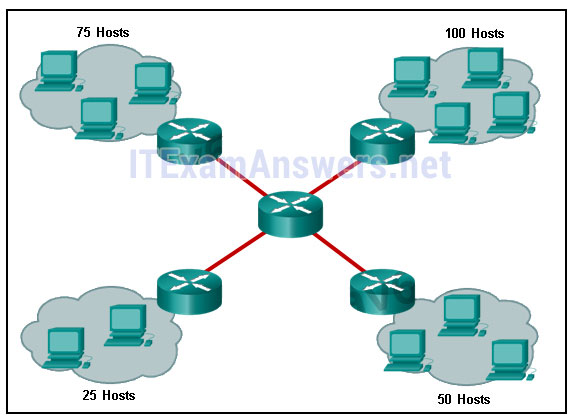
* 1
* 2
* 3
* **4\***

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

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

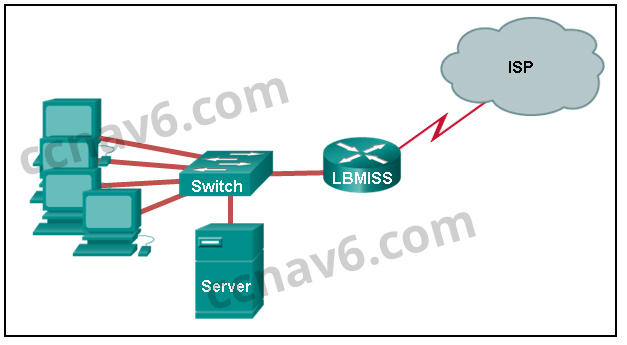
* simplifies network design
* **improves network performance \***
* **easier to implement security policies\***
* reduction in number of routers needed
* reduction in number of switches needed

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

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


* 255.255.255.0
* **255.255.255.128\***
* 255.255.255.192
* 255.255.255.224
* 255.255.255.240

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

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


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

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

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

* 256
* 254
* 62
* 32
* 16
* **14\***

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

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

* 255.255.255.0
* 255.255.255.128
* **255.255.255.224\***
* 255.255.255.240

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

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

* 510
* 512
* **1022\***
* 1024
* 2046
* 2048

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

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

* two
* **three\***
* four
* five

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

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

* 255.255.255.0
* 255.255.255.192
* **255.255.255.224\***
* 255.255.255.240
* 255.255.255.248
* 255.255.255.252

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

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

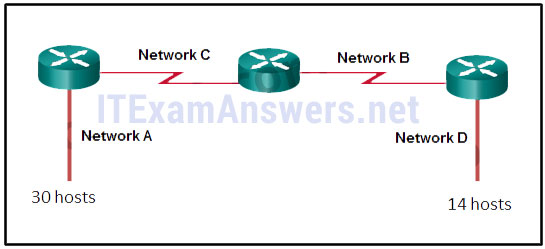
* 192.168.1.16/28
* **192.168.1.64/27\***
* 192.168.1.128/27
* **192.168.1.96/28\***
* 192.168.1.192/28

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

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

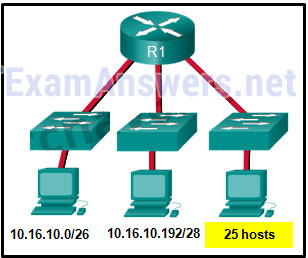
* 4
* **6\***
* 8
* 10
* 12

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

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


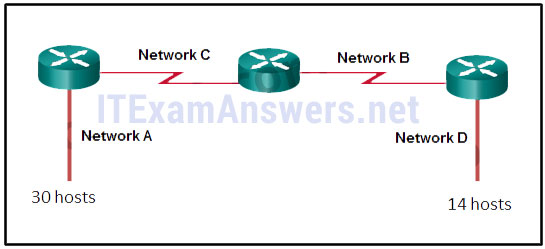
* 56
* 60
* 64
* 68
* **72\***

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

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


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

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

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


* 64
* 56
* 68
* 60
* **72\***

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

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

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

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

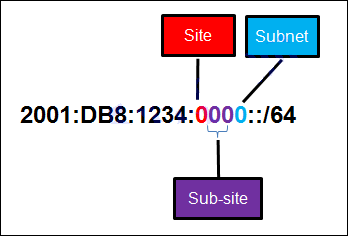
* **It eliminates most address configuration errors.\***
* It ensures that addresses are only applied to devices that require a permanent address.
* It guarantees that every device that needs an address will get one.
* It provides an address only to devices that are authorized to be connected to the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

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

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

* 254
* **251\***
* 252
* 253

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

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


* 0
* 4
* **16\***
* 256

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

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

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

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

**21. Consider the following range of addresses:**

2001:0DB8:BC15:00A0:0000::

2001:0DB8:BC15:00A1:0000::

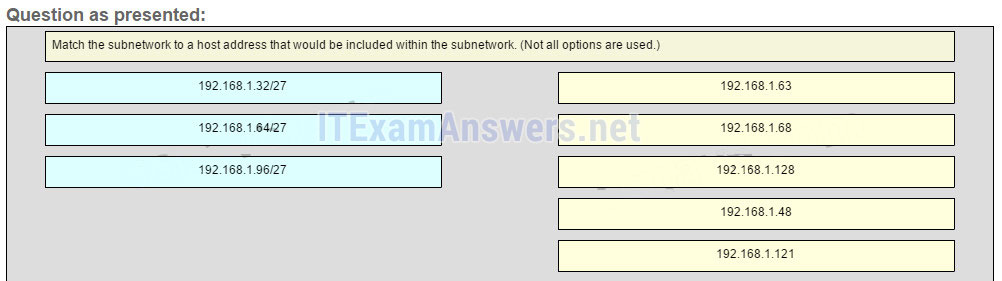
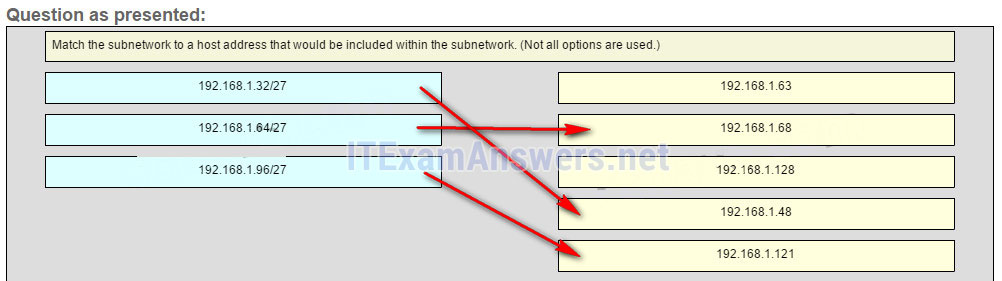
2001:0DB8:BC15:00A2:0000::

…

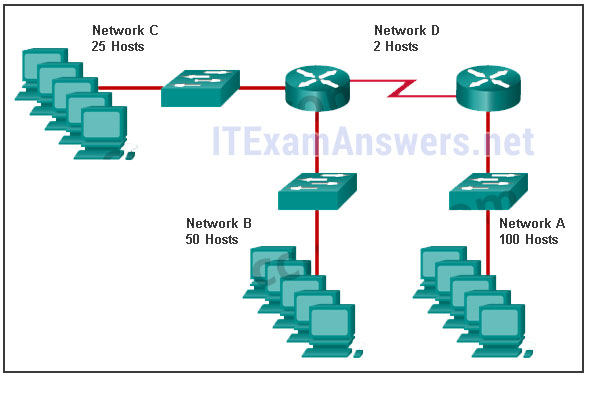
2001:0DB8:BC15:00AF:0000::

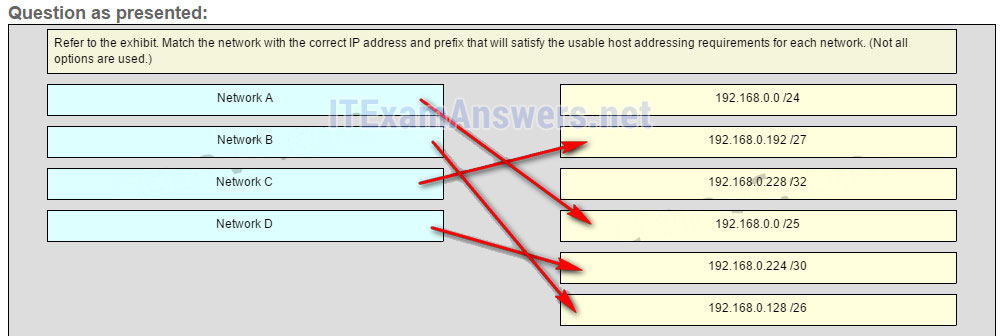
The prefix-length for the range of addresses is **/60**

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

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


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

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


**Answer**  


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

## Older Version

**24. How many bits are in an IPv4 address?**

* **32\***
* 64
* 128
* 256

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

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

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

* /25
* /26
* **/27\***

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

* limited broadcast
* multicast
* **directed broadcast\***
* unicast

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

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

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

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

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

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

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

* FE8::2AA:FF:FE9A:4CA3?
* **FE80::2AA:FF:FE9A:4CA3\***
* FE80::0:2AA:FF:FE9A:4CA3?
* FE80:::0:2AA:FF:FE9A:4CA3?

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

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

**33. What are three parts of an IPv6 global unicast address? (Choose three.)**

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

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

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

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

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

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

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

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

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

**38. When will a router drop a traceroute packet?**

* when the router receives an ICMP Time Exceeded message
* when the RTT value reaches zero
* when the host responds with an ICMP Echo Reply message
* **when the value in the TTL field reaches zero\***
* when the values of both the Echo Request and Echo Reply messages reach zero

**39. What is indicated by a successful ping to the ::1 IPv6 address?**

* The host is cabled properly.
* The default gateway address is correctly configured.
* All hosts on the local link are available.
* The link-local address is correctly configured.
* **IP is properly installed on the host.\***

**40. Which two things can be determined by using the ping command? (Choose two.)**

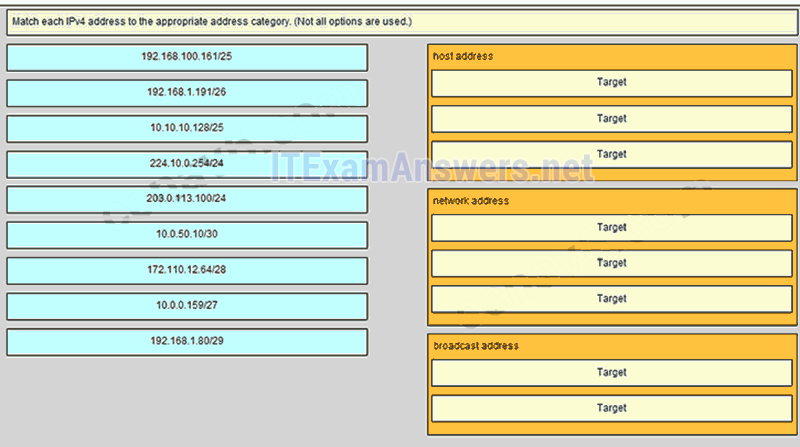
* the number of routers between the source and destination device
* the IP address of the router nearest the destination device
* **the average time it takes a packet to reach the destination and for the response to return to the source \***
* **whether or not the destination device is reachable through the network\***
* the average time it takes each router in the path between source and destination to respond

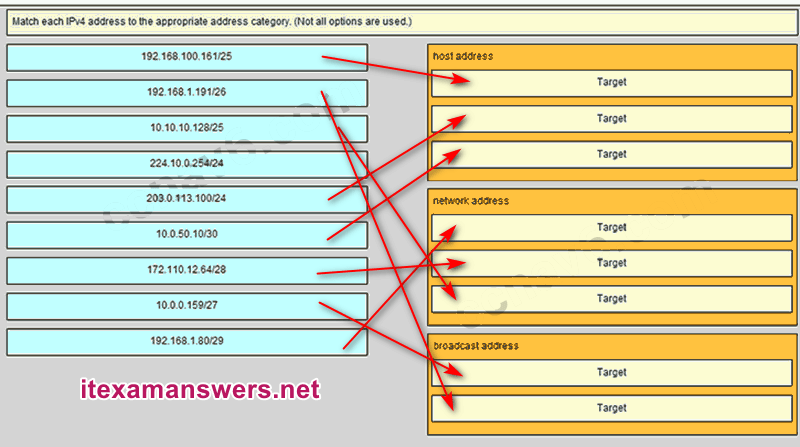
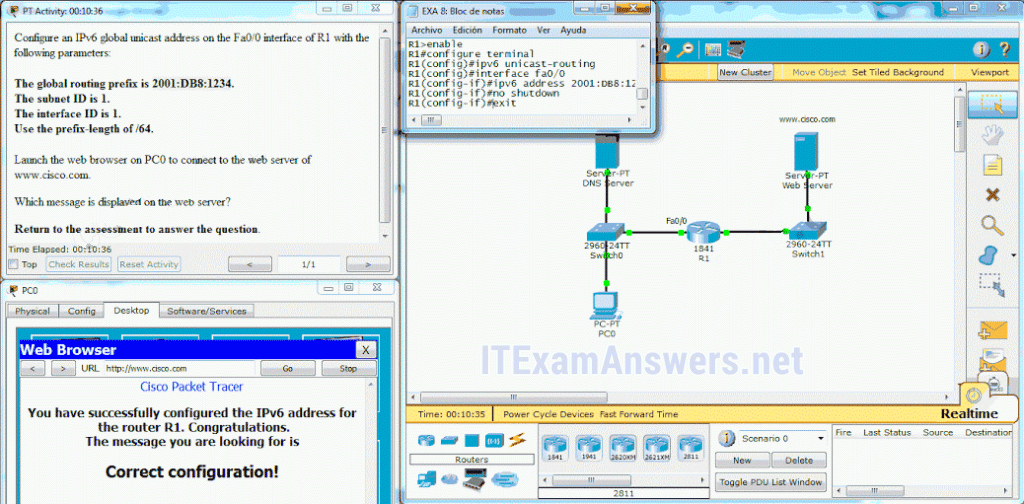
**41. Fill in the blank.**  
The decimal equivalent of the binary number 10010101 is **149**

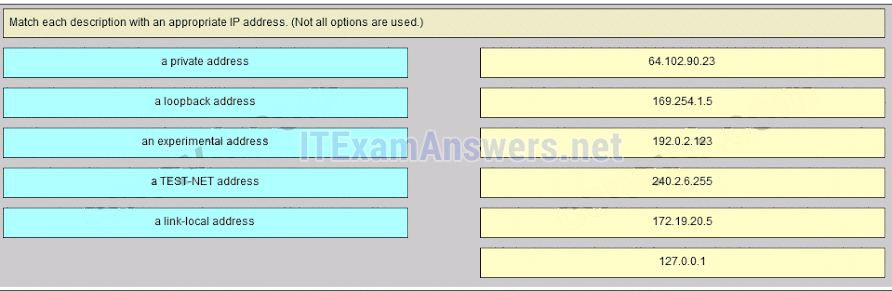
**42. Fill in the blank.**  
What is the decimal equivalent of the hex number 0x3F? **63\***

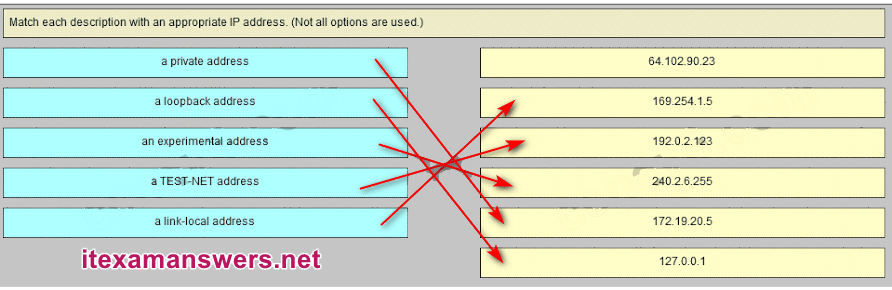
**43. Open the PT Activity. Perform the tasks in the activity instructions and then answer the question. Which message is displayed on the web server?**

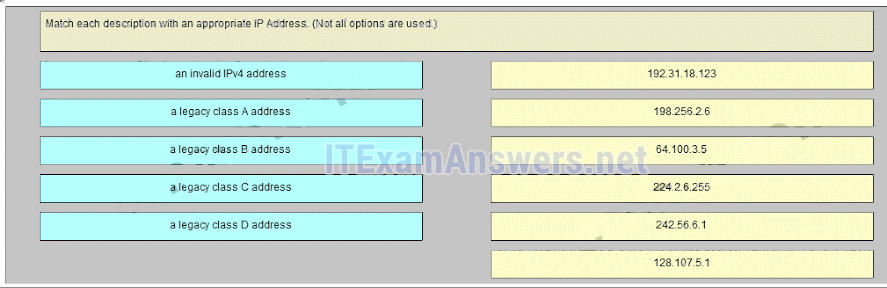
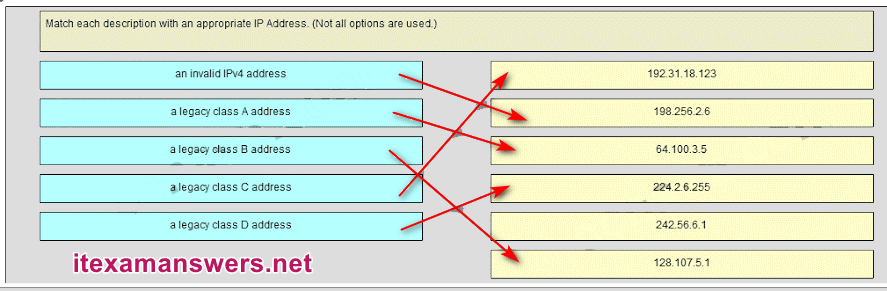
* You did it right!
* **Correct configuration!\***
* IPv6 address configured!
* Successful configuration!

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


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


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


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

**46. Match each description with an appropriate IP address. (Not all options are used.)**  
  
  
**192.31.18.123 -> a legacy class C address**  
**198.256.2.6 -> an invalid IPv4 address**  
**64.100.3.5 -> a legacy class A address**  
**224.2.6.255 -> a legacy class D address**  
**128.107.5.1 -> a legacy class B address**

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

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

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

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

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

* 255.255.255.224
* 0.0.0.32
* 255.255.255.223
* **0.0.0.31\***

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

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

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

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

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

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

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

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

**3. A host device needs to send a large video file across the network while providing data communication to other users. Which feature will allow different communication streams to occur at the same time, without having a single data stream using all available bandwidth?**

* window size
* **multiplexing\***
* port numbers
* acknowledgments

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

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

* **registered port\***
* private port
* dynamic port
* source port

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

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

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

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

**6. What is a socket?**

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

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

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

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

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

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

* FIN
* **ACK\***
* SYN
* RST

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

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

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

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

**10. Which two flags in the TCP header are used in a TCP three-way handshake to establish connectivity between two network devices? (Choose two.)**

* **ACK\***
* FIN
* PSH
* RST
* **SYN\***
* URG

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

**11. A PC is downloading a large file from a server. The TCP window is 1000 bytes. The server is sending the file using 100-byte segments. How many segments will the server send before it requires an acknowledgment from the PC?**

* 1 segment
* **10 segments\***
* 100 segments
* 1000 segments

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

**12. Which factor determines TCP window size?**

* the amount of data to be transmitted
* the number of services included in the TCP segment
* **the amount of data the destination can process at one time\***
* the amount of data the source is capable of sending at one time

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

**13. During a TCP session, a destination device sends an acknowledgment number to the source device. What does the acknowledgment number represent?**

* the total number of bytes that have been received
* one number more than the sequence number
* **the next byte that the destination expects to receive\***
* the last sequence number that was sent by the source

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

* port numbers
* **sequence numbers\***
* acknowledgment numbers
* fragment numbers

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

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

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

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

**16. What is a characteristic of UDP?**

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

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

**17. What does a client do when it has UDP datagrams to send?**

* **It just sends the datagrams.\***
* It queries the server to see if it is ready to receive data.
* It sends a simplified three-way handshake to the server.
* It sends to the server a segment with the SYN flag set to synchronize the conversation.

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

**18. What happens if the first packet of a TFTP transfer is lost?**

* The client will wait indefinitely for the reply.
* **The TFTP application will retry the request if a reply is not received.\***
* The next-hop router or the default gateway will provide a reply with an error code.
* The transport layer will retry the query if a reply is not received.

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

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

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

**Explain:**  
When TCP is used as the transport protocol, data must be received in a specific sequence or all data must be fully received in order for it to be used. TCP will use sequence numbers, acknowledgments and retransmission to accomplish this. However, when UDP is used as the transport protocol, data that arrives out of order or with missing segments may cause a momentary disruption, but the destination device may still be able to use the data that it has received. This technology results in the least amount of network delay by providing minimal reliability. Since live streaming video applications use UDP as the transport protocol, the receiver will continue showing the video although there may be a slight delay or reduction in quality.

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

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

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

**21. When is UDP preferred to TCP?**

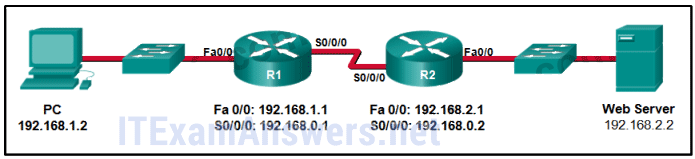
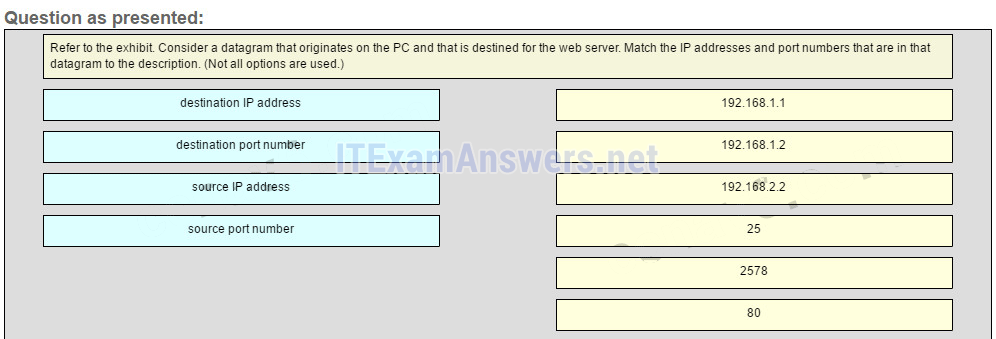
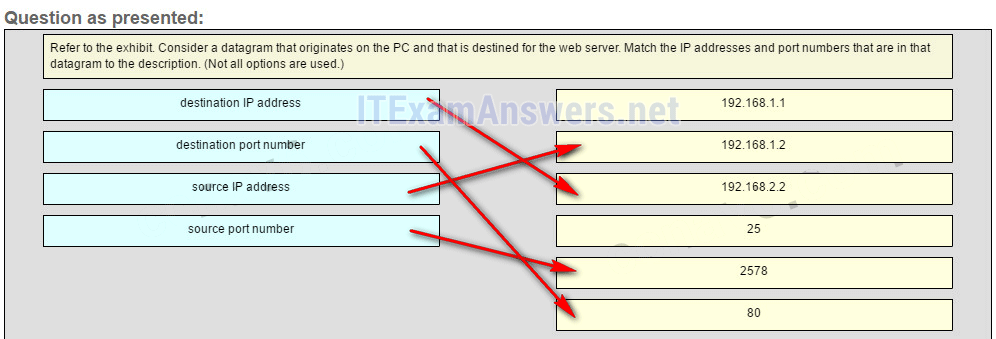
* when a client sends a segment to a server
* when all the data must be fully received before any part of it is considered useful
* **when an application can tolerate some loss of data during transmission\***
* when segments must arrive in a very specific sequence to be processed successfully

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

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

* **SMTP\***
* **FTP\***
* SNMP
* **HTTP\***
* TFTP
* DHCP

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

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


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

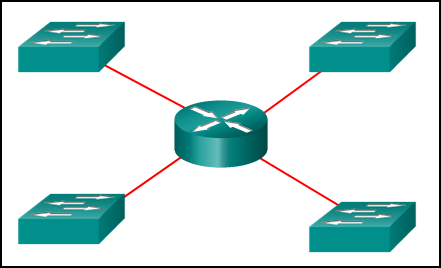
**Explain:**  
A TCP/IP segment that originated on the PC has 192.168.1.2 as the IP source address. 2578 is the only possible option for the source port number because the PC port number must be in the range of registered ports 1024 to 49151. The destination is the web server, which has the IP address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

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

* **sequence numbers\***
* acknowledgment numbers
* fragment numbers
* port numbers

## Older Version

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



* 1
* 2
* 3
* **4\***

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

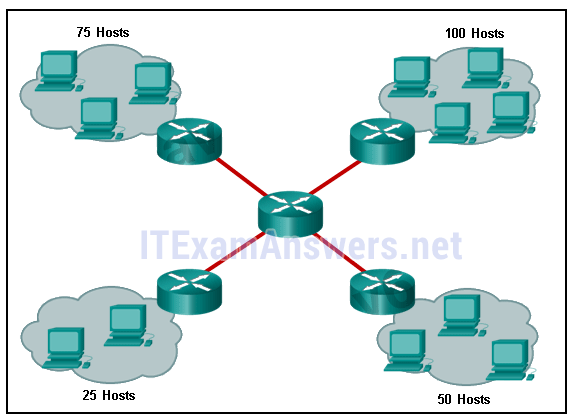
* 32
* **30\***
* 64
* 16
* 62

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

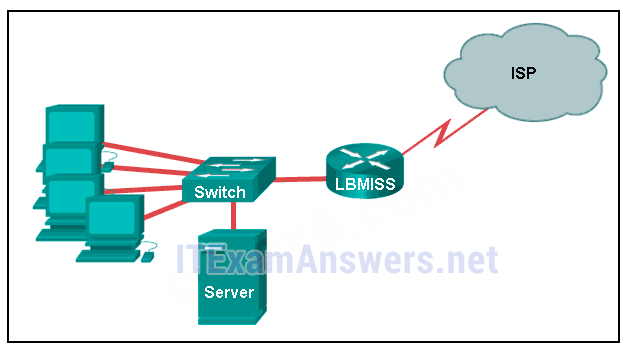
* 510
* 512
* **1022\***
* 1024
* 2046
* 2048

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

* 4
* **6\***
* 8
* 10
* 12

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


* 255.255.255.0
* **255.255.255.128\***
* 255.255.255.192
* 255.255.255.224
* 255.255.255.240

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


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

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

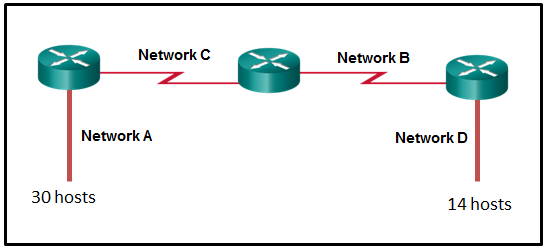
* two
* **three\***
* four
* five

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

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

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

* /23
* /24
* **/25\***
* /26

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


* 56
* 60
* 64
* 68
* **72\***

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

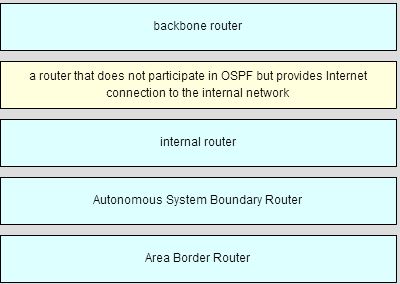
* end-user clients
* workstation clients
* mobile and laptop hosts
* **hosts accessible from the Internet\***

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

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

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

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

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


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

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

* /66
* /70
* **/72\***
* /74

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

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

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

* /62
* **/64\***
* /66
* **/68\***
* /70

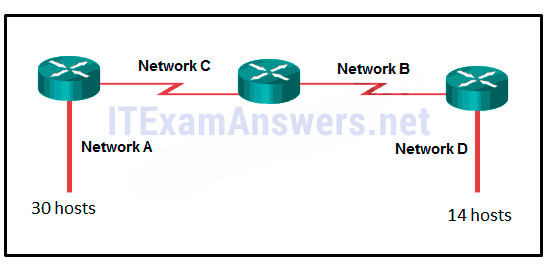
**42. Fill in the blank.**  
In dotted decimal notation, the IP address **172.25.0.126** is the last host address for the network 172.25.0.64/26.

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

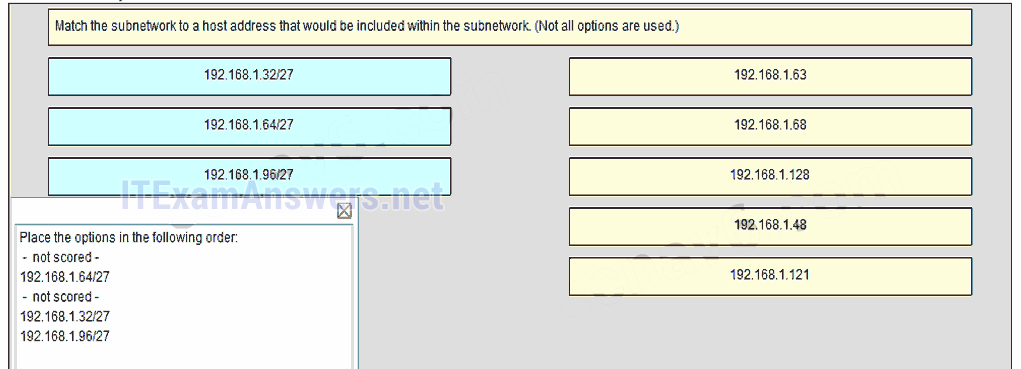
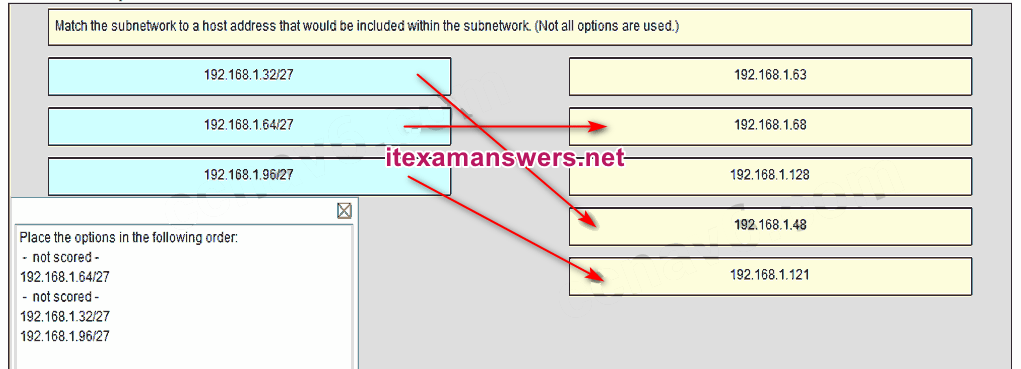
**44. Fill in the blank.**  
A nibble consists of **4** bits.

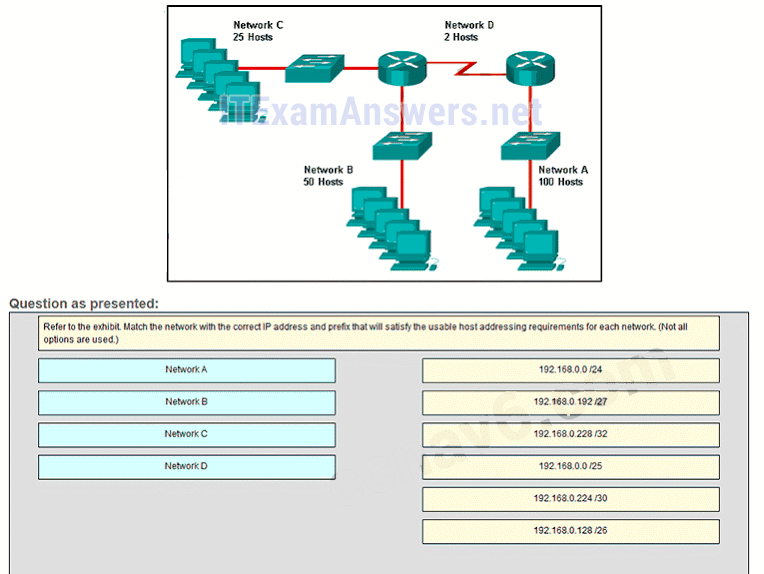
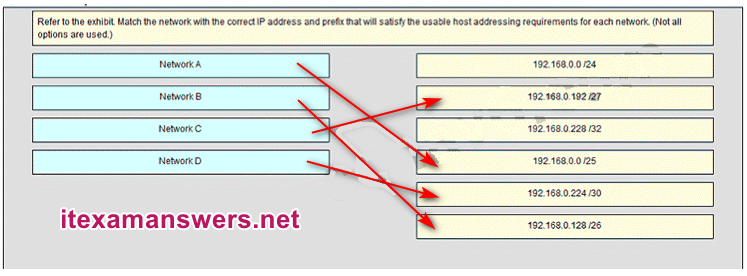
**45. Open the PT Activity. Perform the tasks in the activity instructions and then answer the question. What issue is causing Host A to be unable to communicate with Host B?**

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

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


* 56
* 60
* 64
* 68
* **72\***

**47. Match the subnetwork to a host address that would be included within the subnetwork. (Not all option are used.)**  
  
  
Place the options in the following order:  
 **– not scored –  
192.168.1.64/27  
– not scored –  
192.168.1.32/27  
192.168.1.96/27**

**48. Refer to the exhibit. Match the network with the correct IP address and prefix that will satisfy the usable host addressing requirements for each network. (Not all options are used.)**  
  
  
**Place the options in the following order:**  
**– not scored –  
Network C  
– not scored –  
Network A  
Network D  
Network B**

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

**1. Which two definitions accurately describe the associated application layer protocol? (Choose two.)**

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

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

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

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

**Explain:**  
The network access layer of the TCP/IP model performs the same functions as the physical and data link layers of the OSI model. The internetwork layer equates to the network layer of the OSI model. The transport layers are the same in both models. The application layer of the TCP/IP model represents the session, presentation, and application layers of the OSI model.​

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

* internetwork
* session
* presentation
* **application\***
* network access

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

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

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

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

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

* **FTP\***
* **HTTP\***
* DNS
* SNMP
* DHCP
* **SMTP\***

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

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

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

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

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

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

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

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

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

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

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

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

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

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

* DNS
* DHCP
* SMTP
* **HTTP\***
* POP3

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

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

* **IMAP\***
* POP
* SMTP
* HTTPS

**Explain:**  
IMAP is preferred for small-to medium-sized businesses as IMAP allows centralized storage and backup of emails, with copies of the emails being forwarded to clients. POP delivers the emails to the clients and deletes them on the email server. SMTP is used to send emails and not to receive them. HTTPS is not used for secure web browsing.

**12. What is the function of the Nslookup utility?**

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

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

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

* POST
* ACK
* **GET\***
* PUT

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

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

* SMB
* **HTTPS\***
* SMTP
* IMAP

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

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

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

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

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

* **.com\***
* www
* http
* index

**Explain:**  
The components of the URL http://www.cisco.com/index.htm are as follows:  
http = protocol  
www = part of the server name  
cisco = part of the domain name  
index = file name  
com = the top-level domain

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

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

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

**18. Which phrase describes an FTP daemon?**

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

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

**19. Which statement is true about FTP?**

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

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

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

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

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

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

* **HTTP**
* **SMTP**
* **DHCP**
* **SMB\***

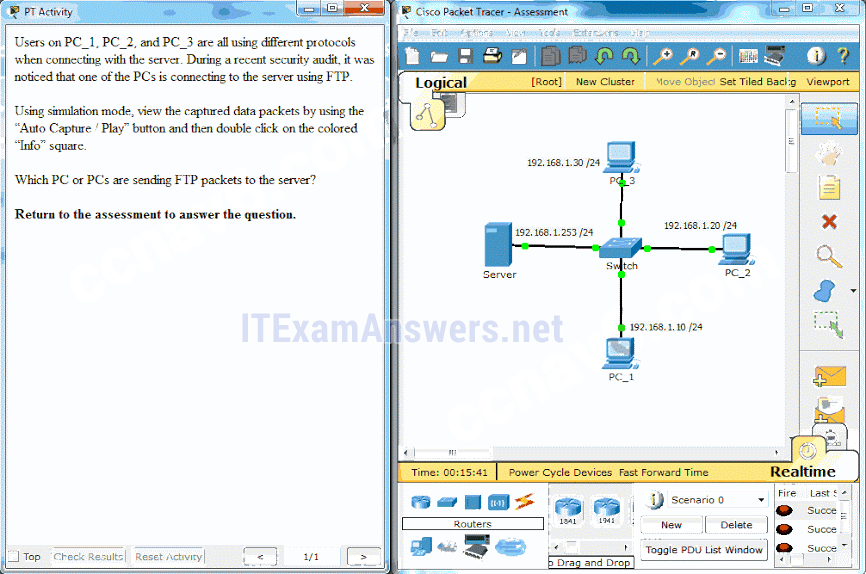
**Explain:  
SMB is used in Microsoft networking for file-sharing and print services. The Linux operating system provides a method of sharing resources with Microsoft networks by using a version of SMB called SAMBA.**

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

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

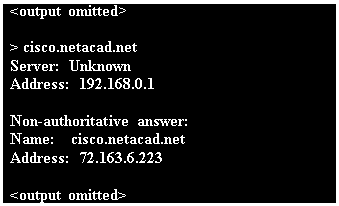
**23. Fill in the blank.  
The HTTP message type used by the client to request data from the web server is the GET message.**

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

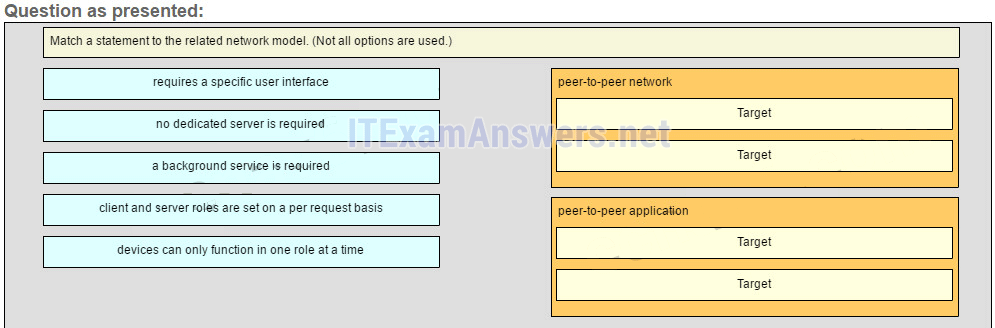
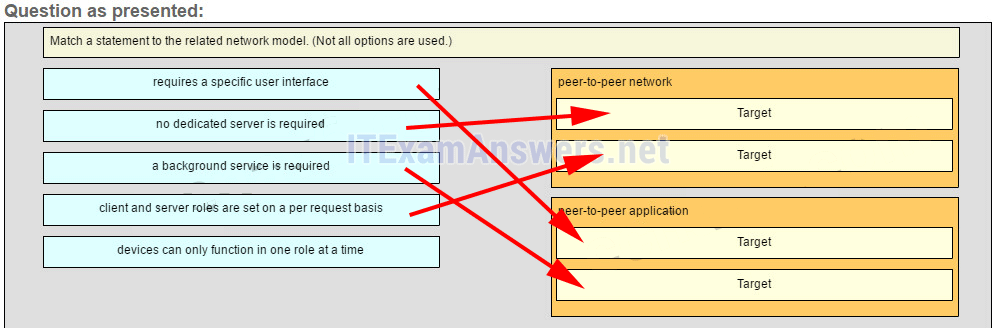
**24. Open the PT Activity.  
  
Perform the tasks in the activity instructions and then answer the question.Which PC or PCs are sending FTP packets to the server?**

* **PC\_3**
* **PC\_1**
* **PC\_2\***
* **PC\_1 and PC\_3**

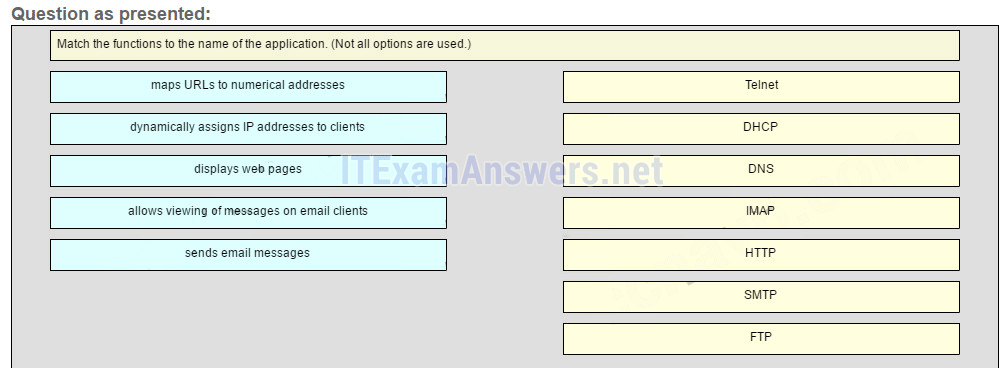
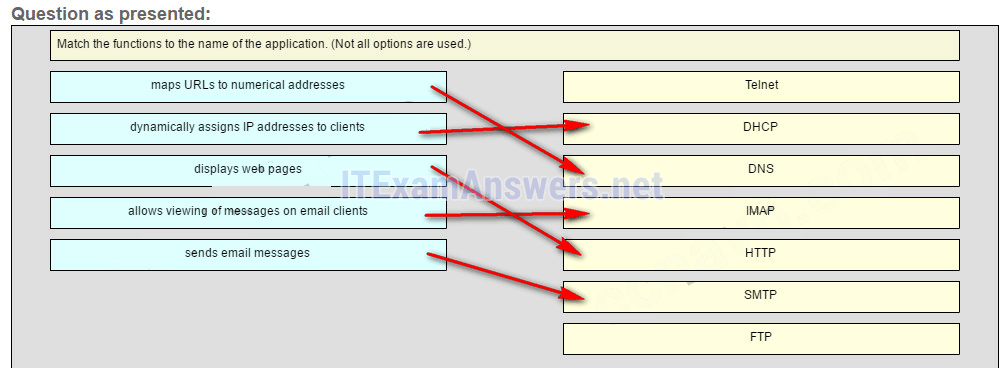
**Explain:  
After you view the details of the packets that are being transferred between each PC and the server, you will see that the PC that is using a destination port number of 20 or 21 is the PC using the FTP service. PC\_2 has an outbound port number of 21 to create an FTP control session with the server at 192.168.1.253.**

**25. Fill in the blank.  
  
Refer to the exhibit. What command was used to resolve a given host name by querying the name servers?  
nslookup**

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

**26. Match a statement to the related network model. (Not all options are used.)  
  
  
Place the options in the following order:peer-to-peer network  
[+] no dedicated server is required   
[+] client and server roles are set on a per request basis  
peer-to-peer aplication  
[#] requires a specific user interface   
[#] a background service is required**

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

**27. Match the functions to the name of the application. (Not all options are used.)  
  
  
Place the options in the following order:  
— not scored —  
DHCP -> dynamically assigns IP address to clients  
DNS -> maps URLs to numerical addresses  
IMAP -> allows viewing of messages on email clients  
HTTP -> displays web pages  
SMTP -> sends email messages  
— not scored —**

## Older Version

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

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

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

* **compression\***
* **addressing**
* **encryption\***
* **session control**
* **authentication**

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

* **ARP**
* **TCP**
* **DSL**
* **FTP \***
* **POP3 \***
* **DHCP\***

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

* **FTP \***
* **HTTP\***
* **DNS**
* **SNMP**
* **DHCP**
* **SMTP\***

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

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

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

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

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

* **DHCPDISCOVER\***
* **DHCPACK**
* **DHCPOFFER**
* **DHCPREQUEST\***
* **DHCPNAK**

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

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

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

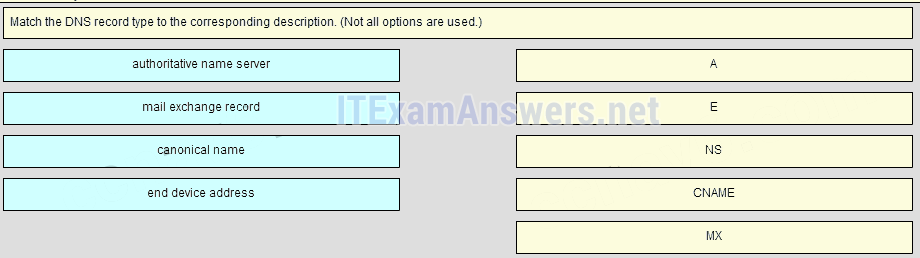
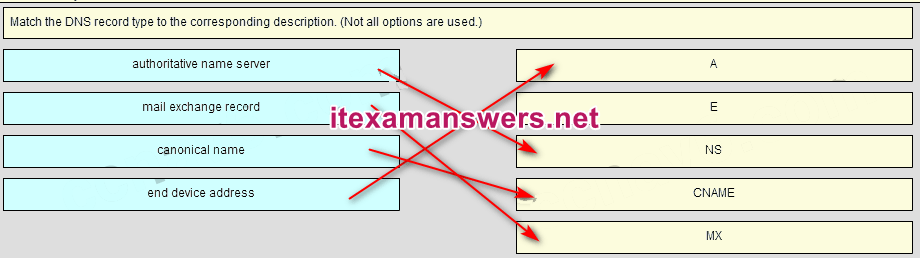
* **.com**
* **netacad.com\***
* **mx.netacad.com**
* **www.netacad.com**

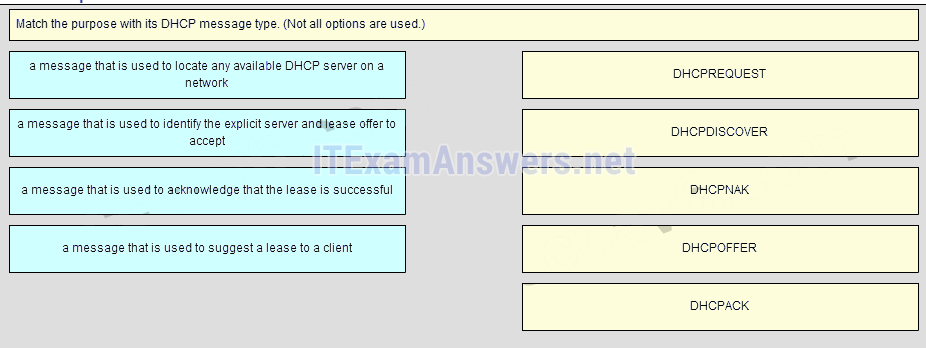
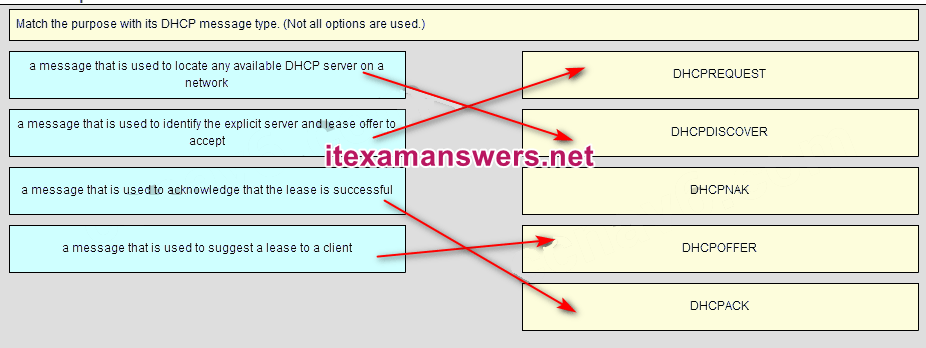
**37. When would it be more efficient to use SMB to transfer files instead of FTP?**

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

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

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

**39. Match the DNS record type to the corresponding description. (Not all options are used.)  
  
  
Place the options in the following order:  
end device address   
– not scored –  
authoritative name server  
canonical name  
mail exchange record**

**40. Match the purpose with its DHCP message type. (Not all options are used.)  
  
  
Place the options in the following order:  
a message that is used to identify the explicit server and lease offer to accept  
a message that is used to locate any available DHCP server on a network  
– not scored –  
a message that is used to suggest a lease to a client  
a message that is used to acknowledge that the lease is successful**

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

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

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

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

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

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

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

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

* email
* web
* FTP
* **voice\***
* **video\***

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

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

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

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

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

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

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

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

* configuration
* **environmental\***
* electrical
* maintenance

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

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

* **DoS attacks\***
* access attacks
* reconnaissance attacks
* trust exploitation

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

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

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

**Explain:**  
One of the most common types of access attack uses a packet sniffer to yield user accounts and passwords that are transmitted as clear text. Repeated attempts to log in to a server to gain unauthorized access constitute another type of access attack. Limiting the number of attempts to log in to the server and using encrypted passwords will help prevent successful logins through these types of access attack.

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

* application filtering
* **stateful packet inspection\***
* URL filtering
* packet filtering

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

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

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

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

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

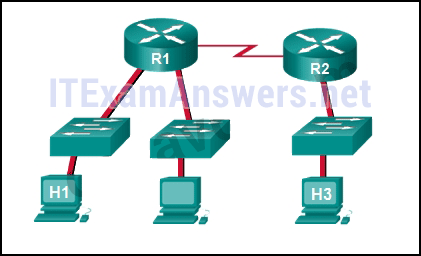
* **a user who is trying to guess a password to access the router\***
* a worm that is attempting to access another part of the network
* an unidentified individual who is trying to access the network equipment room
* a device that is trying to inspect the traffic on a link

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

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

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

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

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


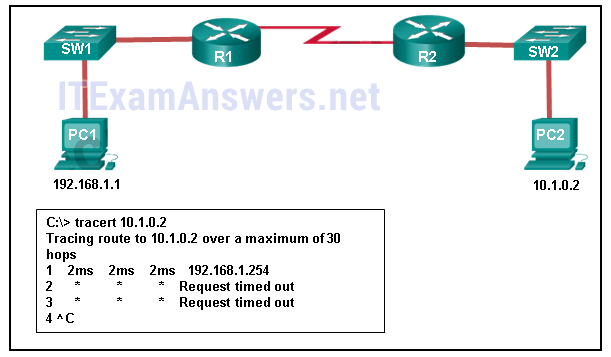
* Connectivity between H1 and H3 is fine.
* H3 is not connected properly to the network.
* Something is causing interference between H1 and R1.
* Performance between the networks is within expected parameters.
* **Something is causing a time delay between the networks.\***

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

**14. When should an administrator establish a network baseline?**

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

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

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


* PC2
* **R1\***
* SW2
* R2
* SW1

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

* **VoIP\***
* NAT
* DHCP
* QoS

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

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

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

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

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

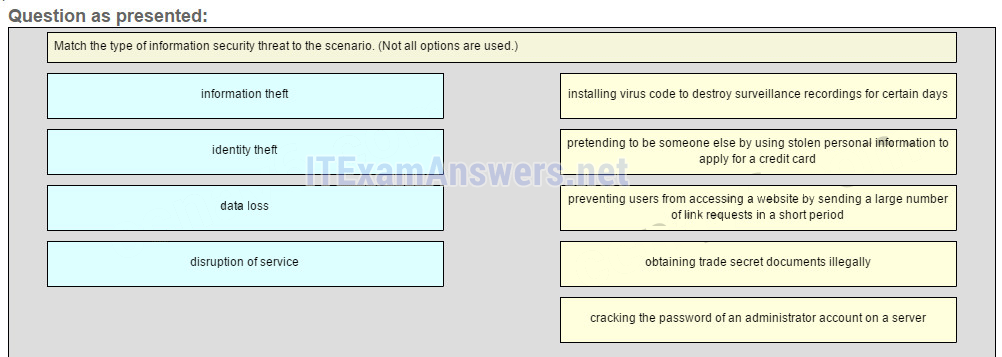
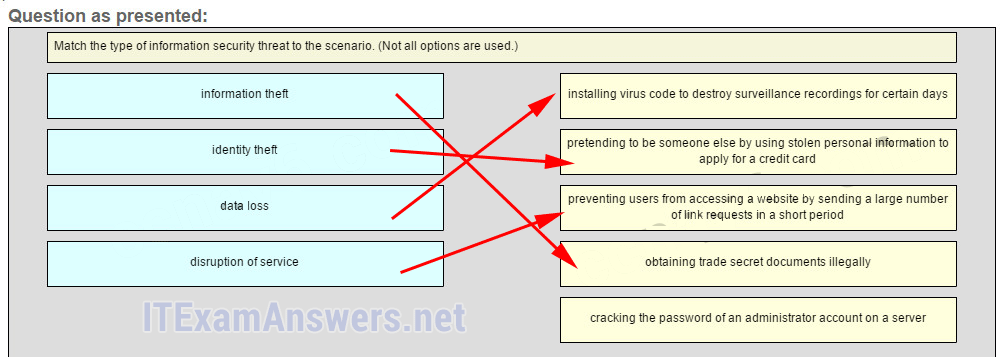
* **It forces the trace to use IPv6.\***
* It limits the trace to only 6 hops.
* It sets a 6 milliseconds timeout for each replay.
* It sends 6 probes within each TTL time period.

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

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

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

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

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

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

## Older Version

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

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

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

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

**30. Which protocol supports rapid delivery of streaming media?**

* SNMP
* TCP
* PoE
* **RTP\***

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

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

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

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

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

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

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

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

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

* inoculation, containment, quarantine, and treatment
* containment, quarantine, treatment, and inoculation
* treatment, quarantine, inoculation, and containment
* **containment, inoculation, quarantine, and treatment \***

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

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

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

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

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

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

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

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

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

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

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

* EAP
* PSK
* WEP
* **WPA\***

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

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

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

* 1 minute
* 2 minutes
* **3 minutes\***
* 4 minutes

https://netacad.com

# Required: Pre-Assessment 1

Question 1

1 / 1 pts

1. What terms represent the maximum and actual speed that can be utilized by a device to transfer data?

bandwidth; goodput

throughput; bandwidth

throughput; goodput

I don't know

**bandwidth; throughput**

Question 2

1 / 1 pts

2. What is the delay in the amount of time for data to travel between two points on a network?

throughput

goodput

**latency**

I don't know

bandwidth

Question 3

1 / 1 pts

3. What is the purpose of an IP address?

**It identifies the source and destination of data packets on a network.**

It identifies the physical location of a data center.

I don't know

It identifies a return address for replying to email messages.

It identifies a location in memory from which a program runs.

Question 4

1 / 1 pts

4. Which network device is used to translate a domain name to the associated IP address?

DHCP server

default gateway

I don't know

**DNS server**

router

Question 5

1 / 1 pts

5. A wireless network was recently installed in a coffee shop and customer mobile devices are not receiving network configuration information. What should be done to correct the problem?

**Make sure the DHCP server is functional.**

Provide peripheral devices to customers.

Ensure that the default gateway device is working properly.

Check the connection of the DNS server to the Internet.

I don't know

# Required: Pre-Assessment 2

Question 1

1 / 1 pts

1. Which IP configuration parameter provides the IP address of a network device that a computer would use to access the Internet?

host IP address

subnet mask

I don't know

**default gateway**

DNS server

Question 2

1 / 1 pts

2. What address type does a switch use to make selective forwarding decisions?

**destination MAC**

source IP

destination IP

I don't know

source MAC

Question 3

1 / 1 pts

3. What role does a router play on a network?

connecting smaller networks into a single broadcast domain

**selecting the path to destination networks**

I don't know

forwarding Layer 2 broadcasts

forwarding frames based on a MAC address

Question 4

1 / 1 pts

4. What type of information is contained in an ARP table?

I don't know

**IP address to MAC address mappings**

domain name to IP address mappings

routes to reach destination networks

switch ports associated with destination MAC addresses

Question 5

1 / 1 pts

5. What is the primary motivation for development of IPv6?

**expanded addressing capabilities**

security

I don't know

header format simplification

addressing the need for simplification

# Chapter 1 Quiz

Question 1

2 / 2 pts

When an appropriate switch form factor for a network is being determined, what should be selected when fault tolerance and bandwidth availability are desired but the budget is limited?

**stackable switch**

non-stackable switch

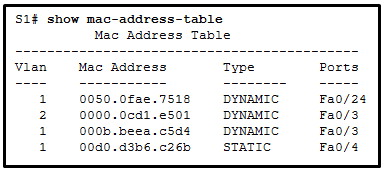
fixed configuration switch

modular switch

Refer to curriculum topic: 1.1.2  
Stackable switches provide fault tolerance and bandwidth availability by using special cables between switches and are less costly to implement than modular switches. A non-stackable switch does not provide these features. A fixed configuration switch is a single switch that does not support features beyond those that originally came with it. A modular switch usually provides fault tolerance and features for bandwidth availability but is rather costly to implement.

Question 2

1 / 2 pts



Refer to the exhibit. A switch receives a Layer 2 frame that contains a source MAC address of 000b.a023.c501 and a destination MAC address of 0050.0fae.75aa. Place the switch steps in the order they occur. (Not all options are used.)

occurs first

**occurs second**

-> Because the destination is not known, the switch forwards the frame out all ports except the port through which the frame arrived.

Refer to curriculum topic: 1.2.1  
The first step a switch does when processing a frame is to see if the source MAC address is in the MAC address table. If the address is not there, the switch adds it. The switch then examines the destination MAC address and compares it to the MAC address table. If the address is in the table, the switch forwards the frame out the corresponding port. If the address is missing from the table, the switch will forward the frame to all ports except the port through which the frame arrived.

Question 3

2 / 2 pts

Which function is supplied by the access layer in a three-layer network design?

high-speed connectivity

routing

application of policies

**network access**

backbone connectivity

Refer to curriculum topic: 1.1.1  
The main purpose of devices in the access layer is to supply network access to end users. Distribution layer devices provide services such as routing and policy functions. The core layer provides high-speed backbone connectivity.

Question 4

2 / 2 pts

Which statement is true about broadcast and collision domains?

Adding a router to a network will increase the size of the collision domain.

The size of the collision domain can be reduced by adding hubs to a network.

The more interfaces a router has the larger the resulting broadcast domain.

**Adding a switch to a network will increase the size of the broadcast domain.**

Refer to curriculum topic: 1.2.2  
A switch that receives a broadcast frame will forward the frame out all other interfaces, including interfaces that connect to other switches. These switches will also perform the same forwarding action. By adding more switches to the network, the of the broadcast domain increases.

Question 5

2 / 2 pts

Which switching method describes a switch that transfers a frame as soon as the destination MAC address is read?

fragment-free

**cut-through**

store-and-forward

latency forwarding

Refer to curriculum topic: 1.2.1

Question 6

2 / 2 pts

Which cost-effective physical network topology design is recommended when building a three-tier campus network that connects three buildings?​

bus

mesh

**extended star**

dual ring

Refer to curriculum topic: 1.1.1  
For efficiency, scalability, and cost-effectiveness, building an extended star topology from a centralized site to all other campus sites is recommended. A mesh topology is much more expensive, and bus and dual ring topologies are more difficult to troubleshoot and maintain.

Question 7

2 / 2 pts

Which option correctly describes a switching method?

cut-through: makes a forwarding decision after receiving the entire frame

store-and-forward: forwards the frame immediately after examining its destination MAC address

cut-through: provides the flexibility to support any mix of Ethernet speeds

**store-and-forward: ensures that the frame is free of physical and data-link errors**

Refer to curriculum topic: 1.2.1  
Store-and-forward switching performs an error check on an incoming frame after receiving the entire frame on the ingress port. Switches which use this method have the flexibility to support any mix of Ethernet speeds. The cut-through method begins the forwarding process after the destination MAC address of an incoming frame is looked up and the egress port has been determined.

Question 8

2 / 2 pts

When the appropriate switch form factor for a network is being determined, what type of switch should be selected when future expansion is important and cost is not a limiting factor?

stackable switch

1 rack unit switch

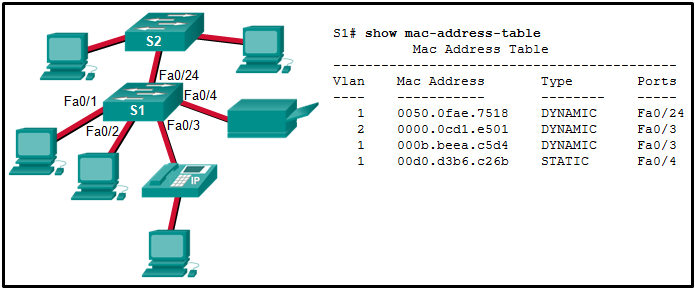
fixed configuration switch

**modular switch**

Refer to curriculum topic: 1.1.2  
A modular switch provides fault tolerance and features for bandwidth availability and future expansion by using line cards but is rather costly to implement. Stackable switches provide fault tolerance and bandwidth availability by using special cables between the switches and are less costly to implement than modular switches. A nonstackable switch does not provide these features. A fixed configuration switch is a single switch that does not support features beyond those that originally came with it.

Question 9

2 / 2 pts



Refer to the exhibit. The PC that is attached to port Fa0/1 is sending a packet that has the destination MAC address of 0050.0fae.299c. Based on the current S1 MAC address table, what will S1 do first when the packet arrives at the switch?

forward the data to S2

broadcast an ARP request to all S1 ports except port Fa0/1

**add the MAC address of the PC that is attached to Fa0/1 to the MAC address table**

broadcast the data to all S1 ports and all S2 ports that have attached end devices

broadcast the data to all S1 ports that have attached end devices, except the Fa0/1 port

Refer to curriculum topic: 1.2.1  
The first step a switch does when processing a frame is to see if the source MAC address is in the MAC address table. If the address is not there, the switch adds it. The switch then examines the destination MAC address and compares it to the MAC address table. If the address is in the table, the switch forwards the frame out the corresponding port. If the address is missing from the table, the switch will broadcast the frame to all ports except the port through which the frame arrived.

Question 10

2 / 2 pts

Which service is provided by an automated attendant feature on a converged network?

point-to-point video

**call routing**

IT management interface

video conferencing

Refer to curriculum topic: 1.1.1  
The automated attendant feature increases the speed of voice services by routing calls directly to individuals or departments. Point-to-point video and video conferencing describe video services on a converged network. An IT management interface is part of a converged network solution that allows IT personnel to facilitate moves, adds, and changes through a centralized application.

Question 11

2 / 2 pts

Which two statements about Layer 2 Ethernet switches are true? (Choose two.)

Layer 2 switches prevent broadcasts.

**Layer 2 switches have multiple collision domains.**

Layer 2 switches route traffic between different networks.

Layer 2 switches decrease the number of broadcast domains.

**Layer 2 switches can send traffic based on the destination MAC address.**

Refer to curriculum topic: 1.2.2

Question 12

2 / 2 pts

Which two characteristics describe a converged network? (Choose two.)

decreased service calls

**support of voice and video both using the same switch**

separate wiring infrastructure for voice and video traffic

**affordability for small and medium businesses**

cheaper equipment cost

Refer to curriculum topic: 1.1.1  
Converged networks have traditional user traffic as well as digitized voice and video traffic that once required separate networks. Now, instead of separate groups managing separate networks, one group of personnel can manage the network.

Question 13

2 / 2 pts

What are the three layers of the switch hierarchical design model? (Choose three.)

**access**

data link

**core**

network access

enterprise

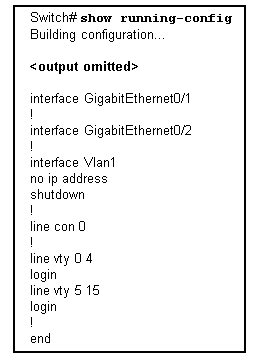
**distribution**

Refer to curriculum topic: 1.1.1  
The access layer is the lowest layer and it provides network access to users. The distribution layer has many functions, but it aggregates data from the access layer, provides filtering, policy control, and sets Layer 3 routing boundaries. The core layer provides high speed connectivity.

# Chapter 2 Quiz

Question 1

2 / 2 pts



Refer to the exhibit. What can be determined from the partial output of the **show running-config** command?

Because the default gateway is not configured, connected hosts will have no connectivity to the Internet.

Remote management of the switch can occur on VLAN 1.

The switch was unable to find and load the complete IOS.

**This appears to be the default configuration of the switch.**

Refer to curriculum topic: 2.1.1  
If the switch was unable to find and load the IOS, the prompt would be switch:. A Layer 2 switch does not provide the default gateway for connected hosts. The default gateway is provided by a Layer 3 device. The switch cannot be managed remotely until a management VLAN and a default gateway have been configured.

Question 2

2 / 2 pts

An attacker has bypassed physical security and was able to connect a laptop to a Ethernet interface on a switch. If all the switch ports are configured with port security and the violation mode is set to factory-default, which action is taken against the attacker?

Packets with unknown source addresses are dropped and there is no notification that a security violation has occurred.

Packets with unknown source addresses are dropped and there is a notification that a security violation has occurred.

**Packets with unknown source addresses are dropped and the interface becomes error-disabled and turns off the port LED.**

Packets with unknown source addresses are forwarded and there is a notification to the syslog server.​

Refer to curriculum topic: 2.2.4  
The default violation mode is shutdown. In this mode, a port security violation causes the interface to immediately become error-disabled and turns off the port LED. It also sends an SNMP trap, logs a syslog message, and increments the violation counter.

Question 3

2 / 2 pts

A network technician wants to implement SSH as the means by which a router may be managed remotely. What are two procedures that the technician should use to successfully complete this task? (Choose two.)

Configure the login banner.

**Configure authentication.**

**Define the asymmetrical keys.**

Configure the console password.

Enter the **service password-encryption** command.

Refer to curriculum topic: 2.2.1

Question 4

2 / 2 pts

How can DHCP packets be used to threaten a switched LAN?

A rogue DHCP packet that contains a virus is accepted by a host.

**Numerous DHCP requests are sent to the DHCP server from spoofed hosts, causing the DHCP address pool to become depleted.**

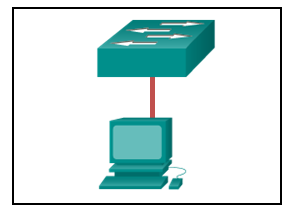
ICMP ping packets are disguised as legitimate DHCP packets. These packets are numerous and deny bandwidth to critical network infrastructure devices.

A DHCP request packet is disguised as a Telnet or SSH packet. While the device is denying access to the SSH or Telnet port, a rogue device posing as a DHCP server sends fake DHCP response packets.

Refer to curriculum topic: 2.2.2  
This type of attack is known as DHCP starvation. After the attack has occurred, legitimate hosts are unable to get an address from the DHCP server because all of the addresses in the pool have been assigned.

Question 5

2 / 2 pts



Refer to the exhibit. The switch and workstation are administratively configured for full-duplex operation. Which statement accurately reflects the operation of this link?

**No collisions will occur on this link.**

Only one of the devices can transmit at a time.

The switch will have priority for transmitting data.

The devices will default back to half duplex if excessive collisions occur.

Refer to curriculum topic: 2.1.2

Question 6

2 / 2 pts

Which configuration must be in place for the auto-MDIX feature to function on a switch interface?

The interface must be in access mode.

The interface must be assigned to VLAN 1.

**The speed and duplex of the interface must be configured for auto detect.**

The interface must be manually configured for full-duplex mode.

Refer to curriculum topic: 2.1.2  
The auto-MIDX feature only functions on Cisco devices when the speed and duplex of the connected interfaces are set to auto detect.

Question 7

2 / 2 pts

What is the first action in the boot sequence when a switch is powered on?

load the default Cisco IOS software

load boot loader software

low-level CPU initialization

**load a power-on self-test program**

Refer to curriculum topic: 2.1.1  
The first action to take place when a switch is powered on is the POST or power-on self-test. POST performs tests on the CPU, memory, and flash in preparation for loading the boot loader.

Question 8

2 / 2 pts

What are two ways to make a switch less vulnerable to attacks like MAC address flooding, CDP attacks, and Telnet attacks? (Choose two.)

Enable CDP on the switch.

**Change passwords regularly.**

**Turn off unnecessary services.**

Enable the HTTP server on the switch.

Use the enable password rather than the enable secret password.

Refer to curriculum topic: 2.2.4

Question 9

2 / 2 pts

A network administrator plugs a new PC into a switch port. The LED for that port changes to solid green. What statement best describes the current status of the port?

There is a duplex mismatch error.

There is a link fault error. This port is unable to forward frames.

**The port is operational and ready to transmit packets.**

This port has been disabled by management and is unable to forward frames.

The flash memory is busy.

Refer to curriculum topic: 2.1.1

Question 10

2 / 2 pts

Fill in the blank.  
The initialism refers to a protocol that provides an encrypted connection. The protocol replaces the clear text Telnet protocol for Cisco device management.

**Answer 1:**

**ssh**

Refer to curriculum topic: 2.2.1  
SSH is the initialism for Secure Shell, a secure protocol for remote access.

Question 11

2 / 2 pts

What is the result of issuing the **no switchport port-security mac-address sticky** command on an interface with port security configured?​​

The sticky secure MAC addresses are removed from the address table and from the running configuration.

**The sticky secure MAC addresses remain part of the address table but are removed from the running configuration.**

The static secure MAC addresses are removed from the address table and from the running configuration.

The static secure MAC addresses remain part of the address table but are removed from the running configuration.

Refer to curriculum topic: 2.2.4  
Sticky learning is disabled by using the **no switchport port-security mac-address sticky** command. Any sticky secure MAC addresses remain as part of the mac-address table but are removed from the running configuration.

Question 12

2 / 2 pts

What would be an ideal environment to carry out penetration tests?

on the production network during nonpeak times

under controlled conditions during business hours ​on the production network

**on an off-line test bed network that mimics the actual production network**

on a network environment simulated by software

Refer to curriculum topic: 2.2.3  
An off-line test bed network that mimics the actual production network is the ideal environment for the network staff to conduct these tests.

Question 13

2 / 2 pts

A network administrator has configured ​VLAN 99 as the management VLAN and has configured it with an IP address and subnet mask. The administrator issues the **show interface vlan 99** command and notices that the line protocol is down. Which action can change the state of the line protocol to up?

**Connect a host to an interface associated with VLAN 99.**

Configure a default gateway.

Remove all access ports from VLAN 99.

Configure a transport input method on the vty lines.

Refer to curriculum topic: 2.1.1  
Once an SVI is configured with an IP address and subnet mask, it can be used for remote management. An SVI interface will be active when the SVI VLAN has an active port associated with it.

Question 14

2 / 2 pts

Fill in the blank.  
In an Ethernet network, frames smaller than 64 bytes are called .

**Answer 1:**

**runt**

Refer to curriculum topic: 2.1.2  
Giants are Ethernet frames that are larger than the maximum allowed. Runts are Ethernet frames that are smaller than the minimum allowed.

# Chapter 2 Quiz - Securing Network Devices

Question 1

2 / 2 pts

What security function does Cisco ACS provide?

It creates a DMZ for public access to servers.

It provides protection from DoS attacks that involve power loss to equipment.

It secures backup copies of router operating systems and configuration files.

**It provides centralized TACACS+ and RADIUS authentication.**

Refer to curriculum topic: 2.1.2  
Cisco ACS, or Access Control Server, is used to centrally and securely store administrative usernames and passwords for TACACS+ and RADIUS authentication.

Question 2

2 / 2 pts

What tool is available through the Cisco IOS CLI to initiate security audits and to make recommended configuration changes with or without administrator input?

Cisco ACS

One-Step Lockdown

**Cisco AutoSecure**

Security Audit Wizard

Refer to curriculum topic: 2.4.1  
Security Audit Wizard and One-Step Lockdown are both features provided through the Cisco Configuration Professional. Cisco ACS is an access control server. Cisco AutoSecure is available through the CLI and can initiate security audits and make configuration changes.

Question 3

2 / 2 pts

A network administrator needs to protect a router against brute force login attempts. What is the correct **login-block-for** command syntax to disable login for 3 minutes if more than 3 failed attempts are made within a 2 minute period?

login block-for 180 attempts 120 within 3

login block-for 3 attempts 120 within 3

login block-for 3 attempts 3 within 2

**login block-for 180 attempts 3 within 120**

Refer to curriculum topic: 2.1.3  
The correct syntax for the command is **login block-for** *seconds* **attempts** *tries* **within** *seconds*. So for a 3 minute login delay, 180 seconds are needed. The failed attempts are 3 within 2 minutes which is 120 seconds:**login block-for 180 attempts 3 within 120**.

Question 4

2 / 2 pts

What three configuration steps must be performed to implement SSH access to a router? (Choose three.)

a password on the console line

**an IP domain name**

**a user account**

an enable mode password

**a unique hostname**

an encrypted password

Refer to curriculum topic: 2.1.4  
To implement SSH on a router the following steps need to be performed:

* Configure a unique hostname.
* Configure the domain name of the network.
* Configure a user account to use AAA or local database for authentication.
* Generate RSA keys.
* Enable VTY SSH sessions.

Question 5

2 / 2 pts

What is the default privilege level of user accounts created on Cisco routers?

0

1

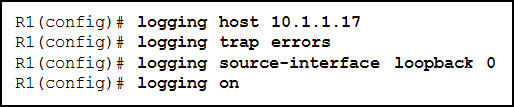
**15**

16

Refer to curriculum topic: 2.2.1  
There are 16 privilege levels that can be configured as part of the **username** command, ranging from 0 to 15. By default, if no level is specified, the account will have privilege level 15, which is the highest level.

Question 6

2 / 2 pts



Refer to the exhibit. An administrator has entered the commands that are shown on router R1. At what trap level is the logging function set?

2

**3**

5

6

Refer to curriculum topic: 2.3.3  
The key word **errors** in the **logging trap** command maps to a syslog level of 3.

Question 7

2 / 2 pts

Which two tasks are associated with router hardening? (Choose two.)

installing the maximum amount of memory possible

placing the router in a secure room

using uninterruptible power supplies

**disabling unused ports and interfaces**

**securing administrative access**

Refer to curriculum topic: 2.1.1  
A critical step in securing a router is to harden it against attack. Two tasks that can be done to harden a router are disabling unused ports and interfaces and securing administrative access to the router. Installing maximum memory in a router will help protect the operating system from DoS attacks but is not a hardening task. Placing the router in a secure room with an uninterruptible power supply provides physical security but is not hardening the router.

Question 8

2 / 2 pts

What must be done before any role-based CLI views can be created?

**Issue the aaa new-model command.**

Assign multiple privilege levels.

Create the secret password for the root user.

Configure usernames and passwords.

Refer to curriculum topic: 2.2.2  
There are five steps involved to create a view on a Cisco router.  
1) AAA must be enabled.  
2) The view must be created.  
3) A secret password must be assigned to the view.  
4) Commands must be assigned to the view.  
5) View configuration mode must be exited.

Question 9

2 / 2 pts

What are two SNMP messages types that are sent by SNMP managers to SNMP agents? (Choose two.)

**set**

**get**

trap

notification

MIB

Refer to curriculum topic: 2.3.4  
Get messages are used by SNMP managers to get information from SNMP agents. Set messages are used by SNMP managers to initiate actions within the agent device. Traps and notifications are used by SNMP agents to notify SNMP managers of significant events. MIBs are information databases that are maintained on SNMP agents about device operations.

Question 10

2 / 2 pts

An administrator has been asked to configure basic access security on a router, including creating secure passwords and disabling unattended connections. Which three actions accomplish this and use recommended security practices to do so? (Choose three.)

Create passwords with only alphanumeric characters.

**Set the minimum password length to 10 characters.**

Set the executive timeout parameters on the console port to 120 and 0.

**Set the executive timeout parameters on the vty lines to 3 and 0.**

**Enable the password encryption service for the router.**

Enable login using the Aux port with the executive timeout set to 0 and 0.

Refer to curriculum topic: 2.1.2  
To make passwords secure, a minimum length of 10 characters is recommended. When setting the timeout timers of the router vty lines, a recommended timeout period is three minutes or less. All current and future passwords configured on the router should also be encrypted.

Question 11

2 / 2 pts

What are the two types of community strings available for authenticating SNMP messages? (Choose two.)

write-only

**read-only**

**read-write**

full-control

write-copy

Refer to curriculum topic: 2.3.4  
Community strings are used by the SNMP server and agent to authenticate SNMP messages. There are two types of community strings: (1) read-only for read access to the MIB, and (2) read-write for read and write access to the MIB.

Question 12

2 / 2 pts

How can an administrator disable access to ROMMON mode on a Cisco router to prevent unauthorized password recovery?

**Issue the no service password-recovery command.**

Configure a secure boot image.

Issue the **secure boot-config restore** command.

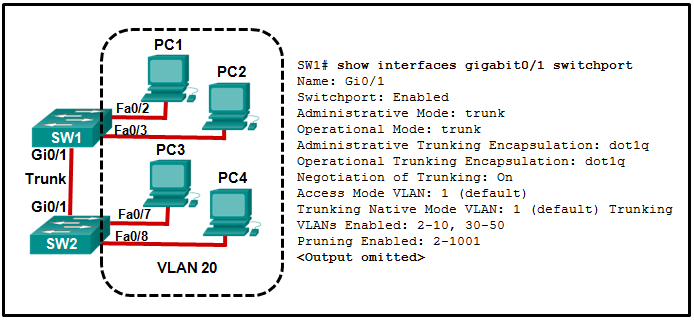
Set the configuration register to 0x2102.

Refer to curriculum topic: 2.3.1  
If the **no password-recovery** global configuration command is entered, the Cisco router will disable all access to ROMMON mode and password recovery is unable to be performed.

# Chapter 3 Quiz

Question 1

2 / 2 pts



Refer to the exhibit. All workstations are configured correctly in VLAN 20. Workstations that are connected to switch SW1 are not able to send traffic to workstations on SW2. What could be done to remedy the problem?

**Allow VLAN 20 on the trunk link.**

Enable DTP on both ends of the trunk.

Configure all workstations on SW1 to be part of the default VLAN.

Configure all workstations on SW2 to be part of the native VLAN.

Refer to curriculum topic: 3.2.4  
Enabling DTP on both switches simply allows negotiation of trunking. The "Negotiation of Trunking" line in the graphic shows that DTP is already enabled. The graphic also shows how the native VLAN is 1, and the default VLAN for any Cisco switch is 1. The graphic shows the PCs are to be in VLAN 20.

Question 2

2 / 2 pts

What is the purpose of the switch command **switchport access vlan 99**?

to enable port security

to make the port operational

**to assign the port to a particular VLAN**

to designate the VLAN that does not get tagged

to assign the port to the default native VLAN (VLAN 99)

Refer to curriculum topic: 3.2.1

Question 3

2 / 2 pts

If an organization is changing to include Cisco IP phones in its network, what design feature must be considered to ensure voice quality?

Voice traffic needs to be tagged with the native VLAN.

**A separate VLAN is needed for voice traffic.**

Additional switch ports that are dedicated to Cisco IP phones are required.

Voice traffic and data traffic require separate trunk links between switches.

Refer to curriculum topic: 3.1.1  
A PC commonly connects to an IP phone and the IP phone, in turn, connects to a switch. The phone does not require a separate port. Because voice traffic cannot tolerate much packet delay, it needs to be in a separate VLAN.  The voice VLAN can be configured to provide quality of service (QoS), which will ensure that the voice traffic has a higher priority than data traffic.

Question 4

2 / 2 pts

Here is a link to the [PT Activity](https://150566673.netacad.com/assessment_questions/22627354/files/16602124/download?verifier=9jw3qsrqEDbRNnM0xNiJCTshVtH1IltGe6DqzN7y&wrap=1).

Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.  
  
What security issue is of concern regarding the VLAN configuration of the switches?

All interfaces are in the same user VLAN.

The management VLAN is using the same VLAN ID as a user VLAN is using.

The "black hole" VLAN is not configured.

**The native VLAN has not been changed from the default setting.**

Refer to curriculum topic: 3.3.2  
As a best practice, the native VLAN should be something other than VLAN 1. It should be isolated with no other user traffic.

* Use the command **show interface** *interface-id* **switchport** will display information including the VLAN on which the native VLAN is configured.
* Use the **show interface trunk** command to display the native VLAN and VLANs that are allowed over the trunk.
* Use the **show vlan** command to display user VLANs - this will show that all unused ports are assigned to the "black hole" VLAN.

Question 5

2 / 2 pts

An administrator is investigating a failure on a trunk link between a Cisco switch and a switch from another vendor. After a few **show** commands, the administrator notices that the the switches are not negotiating a trunk. What is a probable cause for this issue?

Both switches are in trunk mode.

Both switches are in nonegotiate mode.

**Switches from other vendors do not support DTP.**

DTP frames are flooding the entire network.

Refer to curriculum topic: 3.2.3  
DTP is a Cisco proprietary protocol. Non-Cisco switches do not support DTP.

Question 6

2 / 2 pts

In which location are the normal range VLANs stored on a Cisco switch by default?

**flash memory**

startup-config

running-config

RAM

Refer to curriculum topic: 3.2.1  
Normal range VLANs are stored in a file called vlan.dat and located in the flash memory.

Question 7

2 / 2 pts

For what reason would a network administrator use the **show interfaces trunk** command on a switch?

**to view the native VLAN**

to examine DTP negotiation as it occurs

to verify port association with a particular VLAN

to display an IP address for any existing VLAN

Refer to curriculum topic: 3.2.4  
The **show interfaces trunk** command displays the ports that are trunk ports, the trunking mode, the encapsulation type, the trunk status, the native VLAN, and the allowed VLANs on the link.

Question 8

1.33 / 2 pts

Match the action to the corresponding command. (Not all options are used.)

**assigns VLAN 10 for untagged traffic**

**activates the current interface as trunk**

**switchport trunk allowed vlan remove 10**

Refer to curriculum topic: 3.2.2

Question 9

2 / 2 pts

A switch receives a frame on a trunk port, but the frame is tagged with the same VLAN ID as the native VLAN of the trunk link. What happens to that frame?

The frame is broadcast.

The frame is flooded.

The frame is forwarded.

**The frame is dropped.**

Refer to curriculum topic: 3.1.2  
Traffic on a trunk port is not supposed to be tagged for the native VLAN. The switch will recognize this traffic and will drop it.

Question 10

2 / 2 pts

Which two statements accurately describe DTP? (Choose two.)

**DTP is a Cisco proprietary protocol.**

**DTP supports IEEE 802.1Q.**

Cisco switches require DTP to establish trunks.

DTP must be enabled on only one side of the trunk link.

Trunk ports that are configured for dynamic auto will request to enter the trunking state.

Refer to curriculum topic: 3.2.3  
Dynamic Trunking Protocol (DTP) manages trunk negotiation, and IEEE 802.1Q is the industry standard for trunking. DTP is found on Cisco devices. DTP can be disabled on a port by using the **switchport nonegotiate** command.

Question 11

2 / 2 pts

Which step should be performed first when deleting a VLAN that has member switch ports?

Reload the switch.

Implement the command **delete vlan.dat**.

**Reassign all VLAN member ports to a different VLAN.**

Backup the running-config.

Refer to curriculum topic: 3.2.1  
Before deleting an active VLAN, it is recommended that all ports currently assigned as a member of that VLAN be reassigned. Any port that is a member of a VLAN that is deleted will become unusable.

Question 12

2 / 2 pts

Which distinct type of VLAN is used by an administrator to access and configure a switch?

default VLAN

native VLAN

data VLAN

**management VLAN**

Refer to curriculum topic: 3.1.1  
A management VLAN is used to remotely access and configure a switch. Data VLANs are used to separate a network into groups of users or devices. The default VLAN is the initial VLAN all switch ports are placed in when loading the default configuration on a switch. The 802.1Q trunk port places untagged traffic on the native VLAN.

Question 13

2 / 2 pts

What is one way to prevent the VLAN hopping attack?

**Disable DTP negotiation on all ports.**

Change the native VLAN to an unused VLAN.

Designate a different default VLAN.

Remove all user VLANs from the trunk.

Refer to curriculum topic: 3.3.1  
Turn trunking off on all ports that are used to connect to hosts and disable DTP negotiation on all trunking ports to prevent the VLAN hopping attack. This type of attack can be attempted through switch spoofing or double tagging.

Question 14

2 / 2 pts

Which two statements describe the benefits of VLANs? (Choose two.)

VLANs improve network performance by regulating flow control and window size.

VLANs enable switches to route packets to remote networks via VLAN ID filtering.

VLANs reduce network cost by reducing the number of physical ports required on switches.

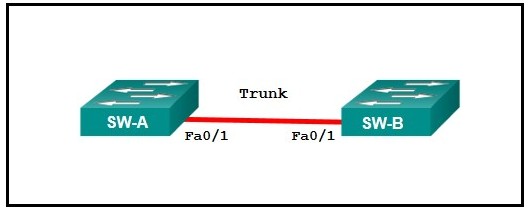
**VLANs improve network security by isolating users that have access to sensitive data and applications.**

**VLANs divide a network into smaller logical networks, resulting in lower susceptibility to broadcast storms.**

Refer to curriculum topic: 3.1.1

Question 15

2 / 2 pts



Refer to the exhibit. What protocol should be configured on SW-A FastEthernet 0/1 if it is to send traffic from multiple VLANs to switch SW-B?

Spanning Tree

RIP v2

**IEEE 802.1Q**

ARP

Rapid Spanning Tree

Refer to curriculum topic: 3.1.2

# Chapter 3 Quiz

Question 1

2 / 2 pts

What is the purpose of protocols in data communications?

specifying the bandwidth of the channel or medium for each type of communication

specifying the device operating systems that will support the communication

**providing the rules required for a specific type of communication to occur**

dictating the content of the message sent during communication

Refer to curriculum topic: 3.1.1  
Protocols provide rules that define how a message is transmitted across a network. Implementation requirements such as electronic and bandwidth details for data communication are specified by standards. Operating systems are not specified by protocols, but will implement protocols. Protocols determine how and when to send a message but they do not control the contents of a message.

Question 2

2 / 2 pts

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

connector specifications

**message encoding**

media selection

**message size**

**delivery options**

end-device installation

Refer to curriculum topic: 3.1.1  
The protocols used in network communications define the details of how a message is transmitted, including requirements for message delivery options, message timing, message encoding, formatting and encapsulation, and message size.

Question 3

2 / 2 pts

What layer of the TCP/IP protocol model determines the best path through the network?

application

transport

**internet**

network access

Refer to curriculum topic: 3.2.4  
The TCP/IP model consists of four layers: application, transport, internet, and network access. The internet layer determines the best path through the network.

Question 4

2 / 2 pts

What type of delivery uses data link layer addresses?

remote delivery

local and remote delivery

**local delivery**

remote delivery using routers

Refer to curriculum topic: 3.3.2  
If a device is sending frames to another device on the same local network, it uses ARP to determine the MAC address of the receiving device. The sending device then uses the Layer 2 addresses to send the frames.

Question 5

2 / 2 pts

Which layer of the OSI model defines services to segment and reassemble data for individual communications between end devices?

application

presentation

session

**transport**

network

Refer to curriculum topic: 3.2.4  
The OSI model consists of seven layers: application, presentation, session, transport, network, data link, and physical. The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices.

Question 6

2 / 2 pts

Which three acronyms/initialisms represent standards organizations? (Choose three.)

**IANA**

TCP/IP

**IEEE**

**IETF**

OSI

MAC

Refer to curriculum topic: 3.2.3  
TCP/IP is a protocol stack that contains a lot of other protocols such as HTTP, FTP, and DNS. The TCP/IP protocol stack is required to be used when communicating on the Internet. A MAC address is an address that is burned into an Ethernet network card. OSI is the 7 layer model that is used to explain how networking works.

Question 7

2 / 2 pts

Why are open standards important in the data communications industry?

They are required for devices to gain access to the Internet.

They eliminate the threat of security breaches.

**They enable interoperability between software and hardware from different vendors.**

They encourage network organizations to develop proprietary software to retain their competitive edge.

Refer to curriculum topic: 3.2.3  
Open standard protocols facilitate interoperability between software and hardware made by different manufactures. For example, open standards allow a client with a Linux operating system to connect to a server running a Microsoft Windows operating system. They would also be able to successfully exchange data. If all software, hardware, and protocols were proprietary, this would not be possible.

Question 8

2 / 2 pts

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

The host is unable to communicate on the local network.

**The host can communicate with other hosts on the local network, but is unable to communicate with hosts on remote networks.**

The host can communicate with other hosts on remote networks, but is unable to communicate with hosts on the local network.

There is no impact on communications.

Refer to curriculum topic: 3.3.2  
A default gateway is only required to communicate with devices on another network. The absence of a default gateway does not affect connectivity between devices on the same local network.

Question 9

2 / 2 pts

What is the general term that is used to describe a piece of data at any layer of a networking model?

frame

packet

**protocol data unit**

segment

Refer to curriculum topic: 3.3.1  
The term protocol data unit (PDU) is used to describe a piece of data at any layer of a networking model. A packet is the PDU at the network layer. A frame is the data link layer PDU. A segment is the PDU at the transport layer.

Question 10

2 / 2 pts

Fill in the blank.  
The MAC address of a PC does not change when the PC is moved to a different network because the MAC address is embedded in the of the PC.

**Answer 1:**

**NIC**

Refer to curriculum topic: 3.3.2  
The MAC address is also known as the physical or Ethernet address. Because it is encoded on hardware, on the Ethernet NIC, it will stay the same no matter where the NIC is geographically located.

Question 11

2 / 2 pts

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

duplex

unicast

multicast

broadcast

Refer to curriculum topic: 3.1.1  
When all devices need to receive the same message simultaneously, the message would be delivered as a broadcast. Unicast delivery occurs when one source host sends a message to one destination host. The sending of the same message from a host to a group of destination hosts is multicast delivery. Duplex communications refers to the ability of the medium to carry messages in both directions.

Question 12

2 / 2 pts

Which logical address is used for delivery of data to a remote network?

destination MAC address

**destination IP address**

destination port number

source MAC address

source IP address

Refer to curriculum topic: 3.3.2  
The destination IP address is used for end-to-end delivery of data to a remote network. The destination MAC address is used for delivery on a local network. The destination port number identifies the application that should process the data at the destination. Source addresses identify the sender of the data.

Question 13

2 / 2 pts

What type of message is sent to a specific group of hosts?

static

unicast

dynamic

**multicast**

broadcast

Refer to curriculum topic: 3.1.1  
A communication that has a single source going to a single destination is called a unicast. A communication from a single source to a group of destinations is called a multicast. A communication from a single source to all destinations on the same local network is called a broadcast.

Question 14

2 / 2 pts

At which layer of the OSI model would a physical address be encapsulated?

physical layer

**data link layer**

network layer

transport layer

Refer to curriculum topic: 3.3.2  
Physical addresses are encapsulated at the data link layer. Logical addresses, also known as IP addresses, are encapsulated at the network layer. Port addresses are encapsulated at the transport layer. No addresses are encapsulated at the physical layer.

# Chapter 3 Quiz - Authentication, Authorization, and Accounting

Question 1

2 / 2 pts

What is the purpose of the **none** keyword in an AAA authentication configuration?

It completely disables AAA authentication on the device.

It prevents users from logging in to the device remotely.

It only allows users with privilege level 15 to log in to the device.

**It allows users to log into the device without credentials if all other authentication methods fail.**

Refer to curriculum topic: 3.2.1  
The **none** keyword allows a user to log in without credentials, and provides a backup in case all other authentication methods fail. A failure occurs if the authentication method is not working, for example if a server is unreachable, or a local database has not been configured.

Question 2

2 / 2 pts

Which server-based authentication protocol would be best for an organization that wants to apply authorization policies on a per-group basis?

ACS

SSH

RADIUS

**TACACS+**

Refer to curriculum topic: 3.3.2  
TACACS+ is considered to be more secure than RADIUS because all TACACS+ traffic is encrypted instead of just the user password when using RADIUS.

Question 3

2 / 2 pts

Which scenario represents an AAA client that would be configured in the Cisco Secure ACS application?

**a router that allows users to connect remotely**

a user who logs in remotely to various devices

a user who connects to a network via a VPN tunnel

a PC that is used to connect remotely to network devices

Refer to curriculum topic: 3.3.4  
AAA clients are the devices that use the services of the Cisco Secure ACS application for AAA. This includes routers, switches, firewalls, and VPN concentrators. Although users and hosts are sometimes referred to as "clients" in other contexts, they are not AAA clients in the Cisco Secure ACS application.

Question 4

2 / 2 pts

What is the purpose of the **start-stop** parameter when AAA accounting is being configured?

It disables AAA accounting services on the line.

**It generates a log entry at the beginning and end of a process.**

It ensures that users cannot start or stop the AAA process on the router.

It causes the AAA process to be in the stopped state whenever the router first starts.

Refer to curriculum topic: 3.5.2  
There are three triggers that define when AAA generates a log entry: start-stop, stop-only, and none. Start-stop generates a log entry when a process both starts and stops. The stop-only generates a log entry only when a process completes. None prevents accounting messages from being sent at all.

Question 5

2 / 2 pts

Which statement describes a characteristic of authorization in an AAA solution?

**It works similarly to privilege levels and role-based CLI.**

It only applies to packet mode AAA and not character mode AAA.

It requires users to perform an additional step after authentication.

It accepts usernames and passwords to determine if users are who they say they are.

Refer to curriculum topic: 3.1.2  
The authorization process is similar to CLI privilege levels and role-based CLI. It happens automatically after a user authenticates, and does not require the user to perform any additional steps.

Question 6

2 / 2 pts



Refer to the exhibit. What configuration would need to be applied to the vty lines in order to use this AAA policy?

login authentication admin

login authentication radius

login authentication local

**No configuration is necessary.**

Refer to curriculum topic: 3.2.1  
The special named list "default" is enabled automatically on all interfaces and lines. No extra configuration is necessary to make the configuration work. If the default list is replaced with another list on the vty line, it can be put back again with the **login authentication default** command.

Question 7

2 / 2 pts

What is a drawback of the local database method of securing device access that can be solved by using AAA with centralized servers?

There is no ability to provide accountability.

It is very susceptible to brute-force attacks because there is no username.

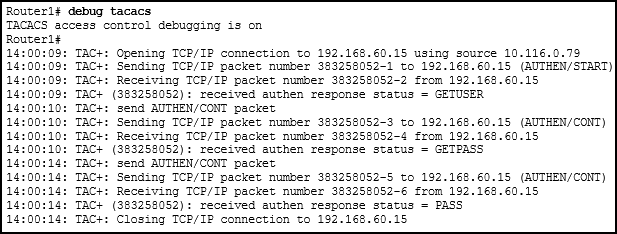
The passwords can only be stored in plain text in the running configuration.

**Because the user accounts must be configured locally on each device, AAA with centralized servers is not scalable.**

Refer to curriculum topic: 3.1.1  
The local database method of securing device access utilizes usernames and passwords that are configured locally on the router. This allows administrators to keep track of who logged in to the device and when. The passwords can also be encrypted in the configuration. However, the account information must be configured on each device where that account should have access, making this solution very difficult to scale.

Question 8

2 / 2 pts



Refer to the exhibit. Which statement describes the output of the debug?

An incorrect password was used.

**A user was successfully authenticated.**

A proper username was not provided to the TACACS+ server.

The secret key used by the router to authenticate to the TACACS+ server is incorrect.

Refer to curriculum topic: 3.4.3  
The "authen response status = PASS" line in the debug output indicates that the login attempt was successful.

Question 9

2 / 2 pts

What is the primary function of the **aaa authorization** command?

permit AAA server access to AAA client services

**limit authenticated user access to AAA client services**

permit authenticated user access to AAA client services

limit AAA server access to AAA client services

Refer to curriculum topic: 3.5.1  
Authorization is concerned with allowing and disallowing authenticated users access to certain areas and programs on the network as well as specific services. Controlling access to configuration commands greatly simplifies the infrastructure security in large enterprise networks.

Question 10

2 / 2 pts

Match each functional component of AAA with its description. (Not all options are used.)

**authentication**

**proving that users are who they say they are**

**authorization**

**determining what resources users can access or the operations they are allowed to perform**

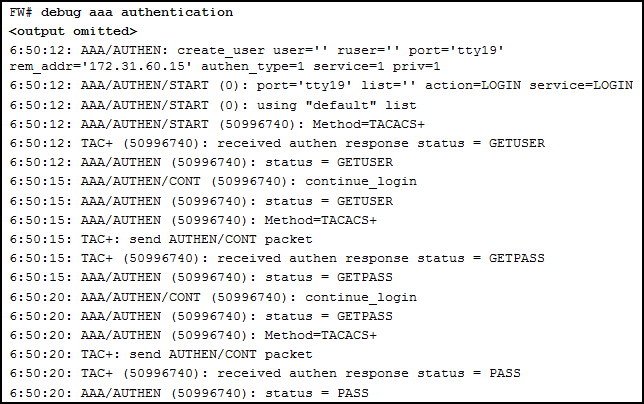
**accounting**

**recording what users do and what they access**

Refer to curriculum topic: 3.1.1

Question 11

2 / 2 pts

6:50:12: AAA/AUTHEN/START (50996740): Method=TACACS+  
6:50:12: TAC+ (50996740): received authen response status = GETUSER  
6:50:12: AAA/AUTHEN (50996740): status = GETUSER  
6:50:15: AAA/AUTHEN/CONT (50996740): continue\_login  
6:50:15: AAA/AUTHEN (50996740): status = GETUSER  
6:50:15: AAA/AUTHEN (50996740): Method=TACACS+  
6:50:15: TAC+: send AUTHEN/CONT packet  
6:50:15: TAC+ (50996740): received authen response status = GETPASS  
6:50:15: AAA/AUTHEN (50996740): status = GETPASS  
6:50:20: AAA/AUTHEN/CONT (50996740): continue\_login  
6:50:20: AAA/AUTHEN (50996740): status = GETPASS  
6:50:20: AAA/AUTHEN (50996740): Method=TACACS+  
6:50:20: TAC+: send AUTHEN/CONT packet  
6:50:20: TAC+ (50996740): received authen response status = PASS  
6:50:20: AAA/AUTHEN (50996740): status = PASS">

Refer to the exhibit. What part of the AAA status message helps a network administrator determine which method list is being referenced?

**GETUSER**

AAA/AUTHEN/START

create\_user

received authen response status

Refer to curriculum topic: 3.2.3  
The GETUSER and GETPASS are useful status messages to look for in the output in order to quickly identify which method list is being used.

Question 12

2 / 2 pts

Which statement describes a difference between RADIUS and TACACS+?

RADIUS uses TCP whereas TACACS+ uses UDP.

RADIUS is supported by the Cisco Secure ACS software whereas TACACS+ is not.

**RADIUS encrypts only the password whereas TACACS+ encrypts all communication.**

RADIUS separates authentication and authorization whereas TACACS+ combines them as one process.

Refer to curriculum topic: 3.3.2  
TACACS+ uses TCP, encrypts the entire packet (not just the password), and separates authentication and authorization into two distinct processes. Both protocols are supported by the Cisco Secure ACS software.

# Chapter 4 Quiz

Question 1

2 / 2 pts

What code is used in the routing table to identify routes learned through EIGRP?

C

**D**

L

O

S

Refer to curriculum topic: 4.3.4  
Each route in a routing table has a code that identifies how the route was learned by the router. The code letter D is used to identify routes that are learned through EIGRP.

Question 2

2 / 2 pts

Which two statements describe characteristics of load balancing? (Choose two.)

Load balancing occurs when a router sends the same packet to different destination networks.

Load balancing occurs when the same number of packets are sent over static and dynamic routes.

**Load balancing allows a router to forward packets over multiple paths to the same destination network.**

**Unequal cost load balancing is supported by EIGRP.**

If multiple paths with different metrics to a destinations exist, the router cannot support load balancing.

Refer to curriculum topic: 4.2.2

Question 3

2 / 2 pts

When a router learns that multiple paths are available to a destination network from the same routing protocol, which factor is considered by a router to choose the best path to forward a packet?

**the lowest metric**

the order of paths on the routing table

the fastest bandwidth of exiting interfaces

the reliability value of the neighboring routers

Refer to curriculum topic: 4.2.2  
When a router learns that multiple paths are available to a destination network from the same routing protocol, the route with the lowest metric is put into the routing table to forward packets toward that network.

Question 4

2 / 2 pts

Which two statements correctly describe the components of a router? (Choose two.)

RAM permanently stores the configuration file used during the boot sequence.

**ROM contains diagnostics executed on hardware modules.**

NVRAM stores a backup copy of the IOS used during the boot sequence.

**Flash memory does not lose its contents during a reboot.**

ROM contains the most current and most complete version of the IOS.

Flash contains boot system commands to identify the location of the IOS.

Refer to curriculum topic: 4.1.1

Question 5

2 / 2 pts

What is a gateway of last resort?

**the IP address of another router**

the IP address of the Internet provider

a term to describe a default gateway on a host device

where dropped packets are sent

Refer to curriculum topic: 4.1.2  
Even though a gateway of last resort could be an IP address of an ISP router, this does not have to be the case. A gateway of last resort, as seen in a Cisco routing table, is simply the IP address that is used to route packets addressed to networks not explicitly listed in the routing table. A Windows-based computer uses the term default gateway, not gateway of last resort.

Question 6

2 / 2 pts

Which three statements describe features of Cisco devices that perform routing? (Choose three.)

**The IP address of a LAN interface on a Layer 3 device provides the default gateway for hosts connected to that LAN.**

A routing protocol must be enabled in order for a Layer 3 device to build a routing table.

**A routing table is automatically created for directly connected, active LAN and WAN interfaces.**

**Routing tables are volatile. When power is removed from a Layer 3 device, the routing table ceases to exist.**

Routing is enabled on a switch via the **interface vlan *x*** command and the assignment of an IP address.

A directly connected Layer 3 interface must be manually added to the routing table in order for routing to be enabled on that interface.

Refer to curriculum topic: 4.3.1  
A routing table entry for a directly connected IPv4 or IPv6 network is automatically added to the routing table when the corresponding interface is up. The **interface vlan** and **ip address** commands are used on a switch to assign an IP address to the device. As seen in the chapter content and lab activities, addressing and activating LAN and WAN interfaces automatically trigger the building of a routing table in a Layer 3 device.

Question 7

2 / 2 pts

The output of the **show ip route** command contains the following entry:  
  
S 10.2.0.0 [1/0] via 172.16.2.2.  
  
What value is indicated by the 1 in the [1/0] portion of the output?

metric

number of hops

**administrative distance**

interface ID through which the network can be reached

Refer to curriculum topic: 6.2.1  
In the routing table entry, S 10.2.0.0 [1/0] via 172.16.2.2, the numbers inside the bracket indicate the administrative distance and metric respectively.

Question 8

2 / 2 pts

Here is a link to the [PT Activity](https://150566673.netacad.com/assessment_questions/22567826/files/16568887/download?verifier=Soq9XyqLAmRRbBlkmg3Y9DnrwhTHiAlQQHYEnSfr&wrap=1).

Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.  
  
When PC0 pings the web server, which MAC address is the source MAC address in the frame from R2 to the web server?

0001.43EA.3E03

0001.9756.6278

0001.C972.4201

**0001.C972.4202**

0002.16D6.A601

Refer to curriculum topic: 4.2.1  
In the segment between R2 and the Web Server, when R2 encapsulates a frame to be sent to the web server, R2 uses the MAC address of its interface that is directly connected to the segment, Fa0/1, as the source MAC.

Question 9

2 / 2 pts

Why are routers needed in networking?

to connect devices to a LAN

to guarantee delivery of packets

to provide a status on packet delivery

**to forward network traffic to remote networks**

to route information and accept acknowledgments of data delivery

Refer to curriculum topic: 4.1.1  
One of the basic functions of a router is to connect different networks. Each interface on a router belongs to a different network. LAN devices can be connected through switches. Packet delivery, packet delivery status, and acknowledgments are functions of the transport layer.

Question 10

2 / 2 pts

What is the purpose of a routing protocol?

It is used to build and maintain ARP tables.

It provides a method for segmenting and reassembling data packets.

It allows an administrator to devise an addressing scheme for the network.

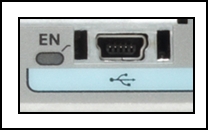
**It allows a router to share information about known networks with other routers.**

It provides a procedure for encoding and decoding data into bits for packet forwarding.

Refer to curriculum topic: 4.3.4

Question 11

2 / 2 pts



Refer to the exhibit. What is the purpose of the router port that is shown?

to backup the IOS

**to configure the router**

to run an IOS from an alternate location

to connect to a port on a switch

Refer to curriculum topic: 4.1.2  
The exhibited port is a USB port that is found on some Cisco router models. This USB port provides console access to the router, which allows access to the CLI for configuration purposes. The pale blue background behind the icon is also the standard color that is used on Cisco devices to indicate a console connection.

Question 12

2 / 2 pts

A new junior network intern connects a laptop to an access layer switch in the wiring closet. After configuring a terminal emulation program, the intern presses the Enter key, and the S1\_ATC\_E2> prompt appears. What could have been done to better protect the switch?

Create a banner message.

**Create a console password.**

Use the **enable secret** command.

Use the **service password-encryption** command.

Refer to curriculum topic: 4.1.3  
Configuring the console line with a password requires the password to be entered before the switch prompt can be accessed. A banner is only a warning message. The **enable secret** command encrypts the enable password. The **service password-encryption** command protects all passwords from being seen when the **show running-configuration** command is used.

Question 13

2 / 2 pts

During the process of encapsulation, how does the PC determine if the packet is destined for a host on a remote network?

by checking the ARP cache for the destination host MAC address

by querying the DNS server for the information of the destination host

by sending a broadcast to the local LAN segment to see if there is any response

**by performing the AND operation on the destination IP address and its own subnet mask**

Refer to curriculum topic: 4.2.1  
When a PC needs to encapsulate a frame to send a data packet, it first performs an AND operation with its own IP and subnet mask, which yields the network address. Then it performs another AND operation using the destination IP and the same subnet mask. By comparing the two AND operations results, the PC knows if the destination is on the local LAN or on a remote network.

Question 14

2 / 2 pts

Which two statements describe static routes? (Choose two.)

They are created in interface configuration mode.

**They require manual reconfiguration to accommodate network changes.**

They automatically become the default gateway of the router.

**They are identified in the routing table with the prefix *S.***

They are automatically updated whenever an interface is reconfigured or shutdown.

Refer to curriculum topic: 6.1.1

Question 15

2 / 2 pts

Which packet-forwarding method does a router use to make switching decisions when it is using a forwarding information base and an adjacency table?

fast switching

**Cisco Express Forwarding**

process switching

flow process

Refer to curriculum topic: 4.1.1  
Cisco Express Forwarding (CEF) is the fastest and preferred switching method. It uses a FIB and an adjacency table to perform the task of packet switching. These data structures change with the topology.

Question 16

2 / 2 pts

What address and prefix length is used when configuring an IPv6 default static route?

**::/0**

::1/128

0.0.0.0/0

FF02::1/8

Refer to curriculum topic: 4.3.3  
The IPv6 address and prefix for a default static route is ::/0. This represents all zeros in the address and a prefix length of zero.

# Chapter 5 Quiz

Question 1

2 / 2 pts

Fill in the blank. Do not use abbreviated commands.  
The parameter can be added to the **show interfaces** *interface\_id* command to display the administrative and operational switch interface mode.​

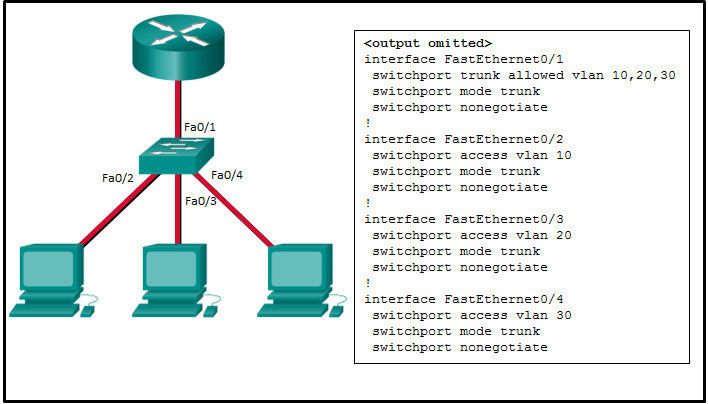
**Answer 1:**

**switchport**

Refer to curriculum topic: 5.2.1  
The output of the show interface 0/1 switchport command displays the administrative and operational mode as shown below:  
Switch0# **show interfaces FastEthernet 0/1 switchport**  
Name: Fa0/1  
Switchport: Enabled  
Administrative Mode: trunk  
Operational Mode: trunk  
Administrative Trunking Encapsulation: dot1q  
  
**(The rest of the output has been omitted.)**

Question 2

2 / 2 pts



Refer to the exhibit. Inter-VLAN communication between VLAN 10, VLAN 20, and VLAN 30 is not successful. What is the problem?​

The access interfaces do not have IP addresses and each should be configured with an IP address.

**The FastEthernet0/2, FastEthernet0/3, and FastEthernet0/4 interfaces are configured as trunk.**

The switch interface FastEthernet0/1 is configured to not negotiate and should be configured to negotiate.​

The switch interfaces FastEthernet0/2, FastEthernet0/3, and FastEthernet0/4 are configured to not negotiate and should be configured to negotiate.​

Refer to curriculum topic: 5.2.1  
The FastEthernet0/2, FastEthernet0/3, and FastEthernet0/4 access interfaces are configured as trunk by the **switchport mode trunk** command. They should be configured as access interfaces. The administrator must issue the **switchport mode access** command.

Question 3

2 / 2 pts

Which option should be used after the **sdm prefer** configuration command to enable static routing on Cisco Catalyst 2960 switches?

Switch(config)# **sdm prefer qos**

Switch(config)# **sdm prefer default**

**Switch(config)# sdm prefer lanbase-routing**

Switch(config)# **sdm prefer dual-ipv4-and-ipv6**

Refer to curriculum topic: 5.3.1  
The Cisco Switch Database Manager (SDM) provides multiple templates for the 2960 switch. The SDM lanbase-routing template can be enabled to allow the switch to route between VLANs and to support static routing. The other options provide templates for other roles that the 2960 switch can take.

Question 4

2 / 2 pts

A network administrator enters the following command sequence on a Cisco 3560 switch. What is the purpose of these commands?  
  
Switch(config)# **interface gigabitethernet 0/1**  
Switch(config-if)# **no switchport**

to shut down the Gi0/1 port

**to make the Gi0/1 port a routed port**

to enable the Gi0/1 port as a switch virtual interface

to enable the Gi0/1 port as a bridge virtual interface

Refer to curriculum topic: 5.3.1  
By default, the physical ports on a 3560 switch are Layer 2 interfaces. To make them routed ports, the interface command **no switchport** should be used. The other options do not describe the purpose of this command.

Question 5

0 / 2 pts

Here is a link to the [PT Activity](https://150566673.netacad.com/assessment_questions/22627364/files/16602129/download?verifier=TqgE5jbXBzmqHkcnTR4yXff6bogwZ33BiE2GkWUc&wrap=1).

Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.  
Which **ping** command from PC0 to PC1 completes successfully?

ping 192.168.2.2

**ping 192.168.2.3**

ping 192.168.2.4

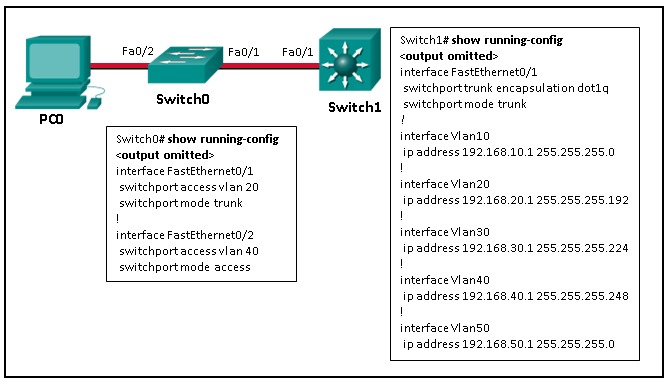
ping 192.168.2.5

ping 192.168.2.6

Refer to curriculum topic: 5.1.3  
Configure Router0 as follows:  
**interface FastEthernet0/0**  
**no shutdown**  
**interface FastEthernet0/0.10**  
**encapsulation dot1Q 10**  
**ip address 192.168.1.1 255.255.255.0**  
**interface FastEthernet0/0.20**  
**encapsulation dot1Q 20**  
**ip address 192.168.2.1 255.255.255.0**

Question 6

2 / 2 pts



Refer to the exhibit. Fill in the blank. Use dot notation.  
PC0 has been assigned the last valid host address in the subnet. The IPv4 address for PC0 will be .

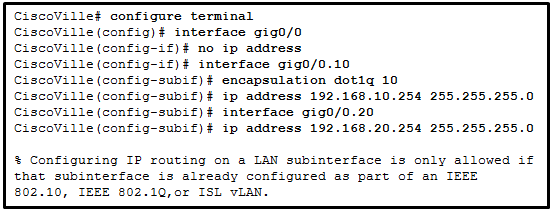
**Answer 1:**

**192.168.40.6.**

Refer to curriculum topic: 5.3.2  
The Fa0/2 port of Switch0 is assigned to VLAN40, so the PC0 must be in the same subnet of the virtual interface VLAN40 of the Layer 3 switch Switch1. This means that VLAN40 has IP addresses in the range of 192.168.40.2 to 192.168.40.6.​

Question 7

2 / 2 pts



Refer to the exhibit. What is the cause of the error that is displayed in the configuration of inter-VLAN routing on router CiscoVille?

The gig0/0 interface does not support inter-VLAN routing.

The **no shutdown** command has not been configured.

The IP address on CiscoVille is incorrect.

**The encapsulation dot1Q 20 command has not been configured.​**

Refer to curriculum topic: 5.1.3  
The steps to configure inter-VLAN routing must be completed in a specific order. Before configuring an IP address on a subinterface, the **encapsulation dot1q VLAN\_id** command must be specified first.

Question 8

2 / 2 pts

Which scalable method must be implemented in order to provide inter-VLAN routing on a switched network with more than 1000 VLANs?

configuring static routes on a Layer 2 switch device

**routing traffic internally to a Layer 3 switch device**

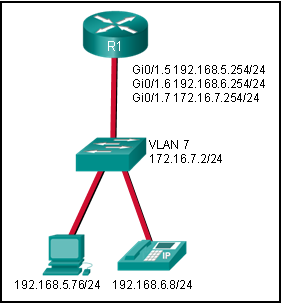
connecting each physical router interface to a different physical switch port, with each switch port assigned to a different VLAN

connecting a router interface to a switch port that is configured in trunk mode to route packets between VLANs, with each VLAN assigned to a router subinterface​

Refer to curriculum topic: 5.1.1  
Layer 2 switches are able to perform static routing, but this method is inefficient with a large number of VLANs. Multilayer switching is more scalable than any other inter-VLAN routing implementation, with traffic being routed internally to the switch device. In router-on-a-stick inter-VLAN routing, where a single physical interface routes traffic among multiple VLANs on a network, there is no practical scalability. The legacy inter-VLAN routing is very inefficient and is no longer used in switched networks, because each VLAN requires a physical router interface that is connected to a different physical switch port.

Question 9

2 / 2 pts



Refer to the exhibit. Which implementation of inter-VLAN routing does this topology use?

interdomain

**router on a stick**

multiple physical interfaces

routing via a multilayer switch

Refer to curriculum topic: 5.1.1  
With router on a stick, subinterfaces are used on one physical router interface. One subinterface per VLAN is used in this design. When multiple interfaces are used on a router, each physical interface such as Gi0/0 and Gi0/1 is assigned one IP address. Each VLAN would require a physical interface. When routing via a multilayer switch, one SVI is assigned an IP address for each VLAN. Interdomain routing does not affect inter-VLAN communication.

Question 10

2 / 2 pts

What is the meaning of the number 10 in the **encapsulation dot1Q 10 native** router subinterface command?​

the interface number

the subinterface number​

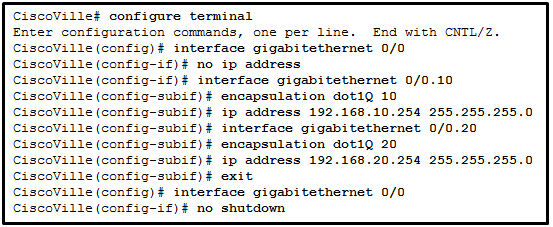
the subnet number

**the VLAN ID**

Refer to curriculum topic: 5.1.3  
The administrator can use the encapsulation command to specify the encapsulation type (IEEE 802.1Q or ISL), the VLAN ID, and optionally the native VLAN.

Question 11

2 / 2 pts



Refer to the exhibit. A network administrator has configured router CiscoVille with the above commands to provide inter-VLAN routing. What type of port will be required on a switch that is connected to Gi0/0 on router CiscoVille to allow inter-VLAN routing?

routed port

access port

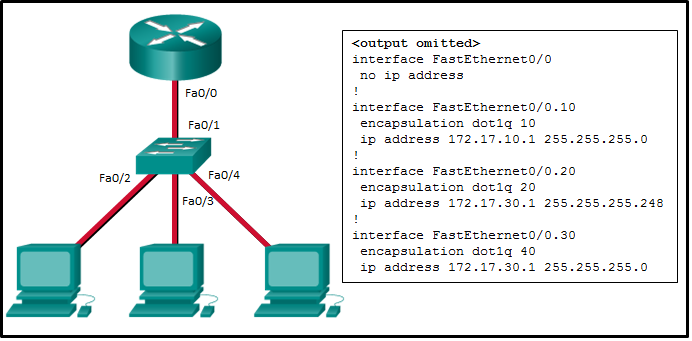
**trunk port**

SVI

Refer to curriculum topic: 5.1.3  
To allow a router-on-a-stick configuration to function, a switch must be connected to the router via a trunk port to carry the VLANs to be routed. An SVI would be used on a multilayer switch where the switch is performing inter-VLAN routing.

Question 12

2 / 2 pts



Refer to the exhibit. An administrator is troubleshooting a router-on-a-stick network that should have the following requirements:   
  
VLAN ID Network Subnet mask Subinterface Default Gateway  
10 172.17.10.0 255.255.255.0 Fa 0/0.10 172.17.10.1  
20 172.17.20.0 255.255.255.0 Fa 0/0.20 172.17.20.1  
30 172.17.30.0 255.255.255.0 Fa 0/0.30 172.17.30.1  
  
Which two errors can be identified from the **show running-config** command output from the router? (Choose two.)

There is no IP address that is configured for the router physical interface.

**The VLAN ID for VLAN 30 is wrongly configured.​**

A command to configure the router physical interface as a trunk is missing.

**The IP address and subnet mask are wrongly configured for VLAN 20.​**

The **no shutdown** command was not issued on subinterfaces.

Refer to curriculum topic: 5.2.2  
The errors in the configuration are: 1) The IP address and subnet mask for VLAN 20 are wrong. They have to be respectively 172.17.20.1 and 255.255.255.0. 2) The VLAN that is assigned to subinterface Fa0/0.30 is incorrect. The **encapsulation dot1q 40** command should be **encapsulation dot1q 30**. There is not a single command to be issued on a router physical interface to configure trunking. The **no shutdown** command has to be issued on the physical interface, not on the subinterfaces. In this case it was issued, because only the **shutdown** command is displayed on the **show running-config** command output.

Question 13

2 / 2 pts

A PC is to access a web server on another network. Which inter-VLAN method will provide the highest bandwidth at Layer 3 and also provide a default gateway for the PC?

router on a stick

**multilayer switch with routing enabled**

trunked interface between the router and the switch

multiple physical interfaces on the router, all connected to a Layer 2 switch

Refer to curriculum topic: 5.1.1  
A router-on-a-stick design is the same as having a trunked interface between the router and the switch. This design works, but does not scale well because all VLANs must traverse the one connection between the router and the switch. Multiple physical interfaces on the router would be faster than the router-on-a-stick design, but a router has a limited number of physical interfaces. Layer 3 switches with routing enabled have more Ethernet ports as well as the ability to route.

# Chapter 6 Quiz

Question 1

2 / 2 pts

What are two reasons why an administrator might choose to use static routing rather than dynamic routing? (Choose two.)

Static routing is easier to maintain in large networks.

**Static routing is more secure.**

Static routing is more scalable.

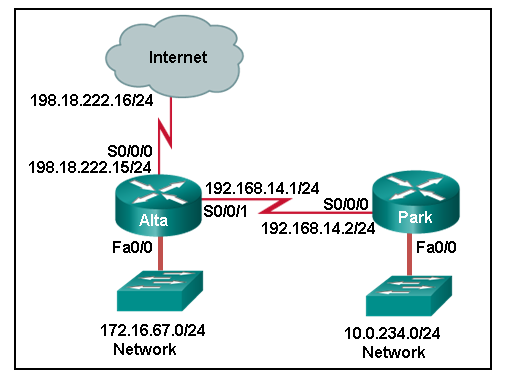
**Static routing uses less router processing and memory.**

Static routing does not require complete knowledge of the whole network.

Refer to curriculum topic: 6.1.1  
Because static routes must be created and changed manually, they require a larger investment of administrative time and do not scale easily. Static routes do not require additional CPU cycles to calculate and advertise routes, and they provide more security because they are not advertised over the network. Proper implementation of static routes requires the administrator to have a complete understanding of the network topology.

Question 2

2 / 2 pts



Refer to the exhibit. Which set of commands will configure static routes that will allow the Park and the Alta routers to a) forward packets to each LAN and b) direct all other traffic to the Internet?

**Park(config)# ip route 0.0.0.0 0.0.0.0 192.168.14.1  
Alta(config)# ip route 10.0.234.0 255.255.255.0 192.168.14.2  
Alta(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0**

Park(config)# **ip route 0.0.0.0 0.0.0.0 192.168.14.1**  
Alta(config)# **ip route 10.0.234.0 255.255.255.0 192.168.14.2**  
Alta(config)# **ip route 198.18.222.0 255.255.255.255 s0/0/0**

Park(config)# **ip route 172.16.67.0 255.255.255.0 192.168.14.1**  
Park(config)# **ip route 0.0.0.0 0.0.0.0 192.168.14.1**  
Alta(config)# **ip route 10.0.234.0 255.255.255.0 192.168.14.2**

Park(config)# **ip route 172.16.67.0 255.255.255.0 192.168.14.1**  
Alta(config)# **ip route 10.0.234.0 255.255.255.0 192.168.14.2**  
Alta(config)# **ip route 0.0.0.0 0.0.0.0 s0/0/1**

Refer to curriculum topic: 6.2.2

Question 3

2 / 2 pts

Which two conditions must exist in order to summarize IPv6 routes into a single static IPv6 route? (Choose two.)

**The destination networks are contiguous and can be summarized into a single network address.**

The multiple static routes all use different exit-interface or next-hop IPv6 address.

The destination networks are not contiguous.

**The multiple static routes all use the same exit-interface or next-hop IPv6 address.**

The administrative distance is greater than the administrative distance of another static route or dynamic routes.

Refer to curriculum topic: 6.4.2  
Static IPv6 routes can be summarized into a single static IPv6 route if the destination networks are contiguous and can be summarized into a single network address. Moreover, all static routes have to use the same exit-interface or next-hop IPv6 address. Floating static routes are static routes that have an administrative distance greater than the administrative distance of another static or dynamic route.

Question 4

2 / 2 pts

Fill in the blank.  
  
A network is a network that is accessed by a single route.

**Answer 1:**

**stub**

Refer to curriculum topic: 6.1.1

Question 5

2 / 2 pts

What type of static route is created when the next-hop IP address and exit interface are specified?

recursive static route

directly connected static route

**fully specified static route**

floating static route

Refer to curriculum topic: 6.2.1  
A fully specified static route has the next-hop IP address and exit interface specified. A recursive static route has only the next-hop IP address specified. A directly attached static route has only the router exit interface specified. A floating static route has a higher metric than the dynamic routes and serves as a backup route.

Question 6

2 / 2 pts

Here is a link to the [PT Activity](https://150566673.netacad.com/assessment_questions/22567740/files/16568867/download?verifier=W06tI2uh8k9LLF4kKpwF9HTB9dxOFNSGw7MOow9Q&wrap=1).

Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.  
  
Why are the pings from PC0 to Server0 not successful?

The static route to network 192.168.1.0 is misconfigured on Router1.

The static route to network 192.168.1.0 is misconfigured on Router2.​

**The static route to network 192.168.2.0 is misconfigured on Router1.​**

The static route to network 192.168.2.0 is misconfigured on Router2.​

Refer to curriculum topic: 6.5.2  
Static routes should specify either a local interface or a next-hop IP address.

Question 7

2 / 2 pts

What is a supernet?

the network for a default route

a network that contains both private and public addresses

a set of discontiguous networks that are controlled by an ISP

**a summarization of serveral IP classful networks into one IP address range**

Refer to curriculum topic: 6.3.2

Question 8

2 / 2 pts

Fill in the blank.  
A static route can be used to provide a backup route to a dynamically learned route.

**Answer 1:**

**floating**

Refer to curriculum topic: 6.1.2  
An example of a floating static route used in conjunction with the EIGRP routing protocol would be as follows.  
(config)# **ip route 192.168.10.0 255.255.255.0 95**  
Notice the extra number at the end of the static route. This route only appears in the routing table if the EIGRP-learned route with an administrative distance of 90 went down. That floating static route cannot appear in the routing table when a route with a better administrative distance exists.

Question 9

2 / 2 pts

Which is a valid summary route for networks 192.168.8.0/22, 192.168.12.0/22, and 192.168.16.0/22?

192.168.0.0/18

**192.168.0.0/19**

192.168.0.0/20

192.168.8.0/21

Refer to curriculum topic: 6.4.1  
The third octet of the network addresses represented in binary are:  
00001000  
00001100  
00010000  
The common leftmost bits are 000 in all three octets. Thus, the summary route will be 192.168.0.0/19.

Question 10

2 / 2 pts

A network administrator enters the following command into Router1: **ip route 192.168.0.0 255.255.255.0 S0/1/0**. Router1 then receives a packet that is destined for 192.168.0.22/24. After finding the recently configured static route in the routing table, what does Router1 do next to process the packet?

drops the packet because the destination host is not listed in the routing table

looks up the MAC address of the S0/1/0 interface to determine the destination MAC address of the new frame

performs a recursive lookup for the IP address of the S0/1/0 interface before forwarding the packet

**encapsulates the packet into a frame for the WAN link and forwards the packet out the S0/1/0 interface**

Refer to curriculum topic: 6.2.1

Question 11

2 / 2 pts

Which command would create a valid IPv6 default route?

**ipv6 route ::/0 fe80::1**

**ipv6 route 2001:db8:acad:1::/64 ::1**

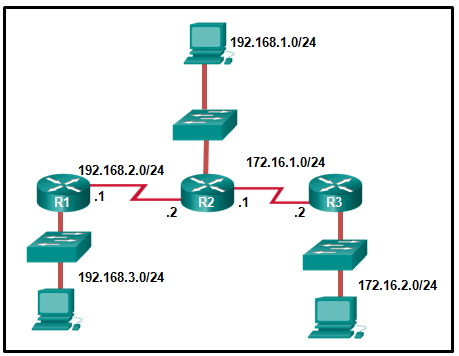
**ipv6 route ::/0 2001:db8:acad:2::a**

**ipv6 route ::/128 2001:db8:acad:1::1**

Refer to curriculum topic: 6.2.4  
The correct prefix and prefix length for a default route is ::/0, which matches any address. ::/128 matches only the specific address of all zeros. When creating a static route that uses a link-local address as the next hop, an exit interface must also be specified for the route to be valid.

Question 12

2 / 2 pts



Fill in the blank. Refer to the exhibit.  
  
On R1, the command to configure a static route to network 172.16.2.0 by specifying the next-hop IP address is **ip route 172.16.2.0 255.255.255.0** .​

**Answer 1:**

**192.168.2.2**

Refer to curriculum topic: 6.2.1  
When a static route is to be configured via the next-hop IP address, the IP address of the interface of the next router in the path to the destination is used.

Question 13

2 / 2 pts

Which static route statement shows a recursive IPv6 static route?

ipv6 route 0::/0 S0/0/0

ipv6 route 0::/0 S0/0/0 254

ipv6 route 2001:db8:cafe:1::/56 S0/0/0

**ipv6 route 2001:db8:cafe:1::/56 2001:db8:1000:10::1**

ipv6 route 2001:db8:cafe:1::/56 S0/0/0 2001:db8:1000:10::1

Refer to curriculum topic: 6.2.3  
In a recursive static route, only the next-hop IPv6 address is specified. As a consequence, the router must perform a recursive route table lookup to find an exit interface associated with the network of the IPv6 address.

Question 14

2 / 2 pts

What command, or set of commands, would be used to determine if the following configuration on router HQ works as designed?  
  
**ip route 0.0.0.0 0.0.0.0 serial 0/0/0 10  
ip route 0.0.0.0 0.0.0.0 serial 0/1/0**

**HQ(config)# interface serial 0/1/0  
HQ(config-if)# shutdown  
HQ(config-if)# end  
HQ# show ip route**

HQ# **traceroute 128.107.0.99**

HQ# **show ip interface brief**

HQ# **ping 128.107.0.99**  
HQ# **ping 64.100.0.5**

HQ# **show ip route**

Refer to curriculum topic: 6.5.2  
To test a floating static route, take down the main route/link in order to see whether the backup link appears in the routing table. The **show ip route** command simply shows the routing table. Only one of the static routes would be shown at any one time.

Question 15

2 / 2 pts

Why would a summarized static route be configured on a router?

to reduce the number of public IP addresses required by an organization

to provide a better route than a particular routing protocol

to provide a default gateway for a router that connects to an ISP

**to reduce the size of the routing table**

to reduce the size of the routing protocol update to a neighboring router

Refer to curriculum topic: 6.3.2  
A summary route represents multiple networks. A summarized static route does not necessarily provide a better route than a routing protocol does. A default static route would provide a default gateway for a router that is connected to an ISP. Routing protocol updates may not necessarily be reduced in size if static route routes are also used.

# Chapter 7 Quiz

Question 1

2 / 2 pts

The network portion of the address 172.16.30.5/16 is .

**Answer 1:**

**172.16**

Refer to curriculum topic: 8.1.2  
A prefix of /16 means that 16 bits are used for the network part of the address. The network portion of the address is therefore 172.16.

Question 2

2 / 2 pts

Fill in the blank.  
The shortest compressed format of the IPv6 address 2001:0DB8:0000:1470:0000:0000:0000:0200 is

**Answer 1:**

**2001:DB8:0:1470::200**

Refer to curriculum topic: 7.2.2  
A double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hextets) consisting of all 0s, and can only be used once per IPv6 address. Any leading 0s (zeros) in any 16-bit section or hextet can be omitted.

Question 3

2 / 2 pts

Match the IPv6 address with the IPv6 address type. (Not all options are used.)

**2001:DB8::BAF:3F57:FE94**

Other Incorrect Match Options:

* unique local
* link-local

Refer to curriculum topic: 7.2.5  
FF02::1:FFAE:F85F is a solicited node multicast address.  
2001:DB8::BAF:3F57:FE94 is a global unicast address.  
FF02::1 is the all node multicast address. Packets sent to this address will be received by all IPv6 hosts on the local link.  
::1 is the IPv6 loopback address.  
There are no examples of link local or unique local addresses provided.

Question 4

2 / 2 pts

Fill in the blank.  
The last host address on the 10.15.25.0/24 network is .

**Answer 1:**

**10.15.25.254**

Refer to curriculum topic: 8.1.3  
The host portion of the last host address will contain all 1 bits with a 0 bit for the lowest order or rightmost bit. This address is always one less than the broadcast address. The range of addresses for the network 10.15.25.0/24 is 10.15.25.0 (network address) through 10.15.25.255 (broadcast address). So the last host address for this network is 10.15.25.254.

Question 5

2 / 2 pts

Which two types of devices are typically assigned static IP addresses? (Choose two.)

workstations

**web servers**

**printers**

hubs

laptops

Refer to curriculum topic: 8.2.1  
Servers and peripherals are often accessed by an IP address, so these devices need predictable IP addresses. End-user devices often have dynamic addresses that are assigned. Hubs do not require IPv4 addresses to operate as intermediary devices.

Question 6

2 / 2 pts

In which alternative to DHCPv6 does a router dynamically provide IPv6 configuration information to hosts?

ARP

EUI-64

ICMPv6

**SLAAC**

Refer to curriculum topic: 7.2.4  
Stateless Address Autoconfiguration (SLAAC) can be used as an alternative to DHCPv6. In this approach, a router provides global routing prefix, prefix length, default gateway, and DNS server information to a host. The host is not provided with a global unicast address by SLAAC. Instead, SLAAC suggests that the host create its own global unicast address based on the supplied global routing prefix. ARP is not used in IPv6. ICMPv6 messages are used by SLAAC to provide addressing and other configuration information. EUI-64 is a process in which a host will create an Interface ID from its 48-bit MAC address.

Question 7

2 / 2 pts

A user who is unable to connect to the file server contacts the help desk. The helpdesk technician asks the user to ping the IP address of the default gateway that is configured on the workstation. What is the purpose for this **ping** command?

to obtain a dynamic IP address from the server

to request that gateway forward the connection request to the file server

**to test that the host has the capability to reach hosts on other networks**

to resolve the domain name of the file server to its IP address

Refer to curriculum topic: 7.3.2  
The **ping** command is used to test connectivity between hosts. The other options describe tasks not performed by **ping**. Pinging the default gateway will test whether the host has the capability to reach hosts on its own network and on other networks.

Question 8

2 / 2 pts

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

encapsulation

translation

dual-stack

**tunneling**

Refer to curriculum topic: 7.2.1  
The tunneling migration technique encapsulates an IPv6 packet inside an IPv4 packet. Encapsulation assembles a message and adds information to each layer in order to transmit the data over the network. Translation is a migration technique that allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. The dual-stack migration technique allows IPv4 and IPv6 protocol stacks to coexist on the same network simultaneously.

Question 9

2 / 2 pts

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

**This part of the address is used by an organization to identify subnets.**

**This network portion of the address is assigned by the provider.**

**This part of the address is the equivalent to the host portion of an IPv4 address.**

Other Incorrect Match Options:

* subnet mask

Refer to curriculum topic: 7.2.4  
A global IPv6 unicast address contains three parts. The Global Routing Prefix of an IPv6 is the prefix or network portion of the address assigned by the provider, such as an ISP, to a customer or site. The Subnet ID Field is used by an organization to identify a subnet within its site. The interface ID field of the IPv6 Interface ID is equivalent to the host portion of an IPv4 address.

Question 10

2 / 2 pts

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

/25

/26

**/27**

/28

Refer to curriculum topic: 7.1.2  
The binary format for 255.255.255.224 is 11111111.11111111.11111111.11100000. The prefix length is the number of consecutive 1s in the subnet mask. Therefore, the prefix length is /27.

Question 11

2 / 2 pts

Fill in the blank.  
The 8-digit binary value of the last octet of the IPv4 address 172.17.10.7 is .

**Answer 1:**

**00000111**

Refer to curriculum topic: 7.1.1  
7 = 4 + 2 + 1 = 00000111

Question 12

2 / 2 pts

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

the one IPv6 device on the link that has been uniquely configured with this address

**all IPv6 enabled devices on the local link​ or network**

only IPv6 DHCP servers​

only IPv6 configured routers

Refer to curriculum topic: 7.2.5  
This address is one of the assigned IPv6 multicast addresses. Packets addressed to FF02::1 are for all IPv6 enabled devices on the link or network. FF02::2 is for all IPv6 routers that exist on the network.

Question 13

2 / 2 pts

Which type of IPv6 address is not routable and used only for communication on a single subnet?

global unicast address

**link-local address**

loopback address

unique local address

unspecified address

Refer to curriculum topic: 7.2.3  
Link-local addresses have relevance only on the local link. Routers will not forward packets that include a link-local address as either the source or destination address.

Question 14

2 / 2 pts

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

**a link-local address**

**169.254.1.5**

**a public address**

**198.133.219.2**

**an experimental address**

**240.2.6.255**

**a loopback address**

**127.0.0.1**

Refer to curriculum topic: 7.1.4  
Link-Local addresses are assigned automatically by the OS and are located in the block 169.254.0.0/16. The private address ranges are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. The addresses in the block 240.0.0.0 to 255.255.255.254 are reserved as experimental addresses. Loopback addresses belong to the block 127.0.0.0/8.

# Chapter 7 Quiz

Question 1

2 / 2 pts

Match the steps that are taken by a router in the route look up process when it receives a packet, there is no match, and the packet is eventually dropped. (Not all options are used.)

**step 1**

**examining level 1 network routes for the best match**

**step 2**

**examining child routes of the parent route for the best match**

**step 3**

**searching level 1 supernet routes for the best match**

**step 4**

**determining if a default route exists**

**step 5**

**dropping the packet**

Question 2

2 / 2 pts

A network administrator has examined the routing table of a router and noted that the entry for the destination network 172.16.4.0/24 begins with the letter **D**. What does this letter signify?

The route to network 172.16.4.0/24 is directly connected.

**The route source was learned dynamically.**

That is the direct route for packets to that network.

The route to this network is configured statically on the router.

Refer to curriculum topic: 7.5.1  
Routing table entries that begin with the letter **D** are learned dynamically using the EIGRP routing protocol. Static route entries on the routing table are identified with **S**. Directly connected route entries are denoted by the letter **C**.

Question 3

0 / 2 pts

Which classless routing protocol supports VLSM and CIDR, bounded and triggered updates, and uses the multicast address of 224.0.0.10?

RIPv1

RIPv2

OSPF

**EIGRP**

Refer to curriculum topic: 7.2.2  
RIPv1 uses broadcast, not multicast. RIPv2 uses the multicast address 224.0.0.9.

Question 4

2 / 2 pts

Which algorithm is used by the OSPF routing process to construct the SPF tree on a router?

DUAL algorithm

Bellman-Ford algorithm

**Dijkstra's algorithm**

path vector protocol

Refer to curriculum topic: 7.4.1  
OSPF routing process uses Dijkstra's algorithm to construct the SPF tree. DUAL algorithm is used by the EIGRP routing protocol. Bellman-Ford algorithm is used by RIP routing protocol. Path vector protocol is the protocol used by BGP.

Question 5

2 / 2 pts

Here is a link to the [PT Activity](https://150566673.netacad.com/assessment_questions/22627341/files/16602123/download?verifier=fgWTPkakiijhO6tzXBOt9ZyJQjgM5Nxf4kkwtvEy&wrap=1).

Open the PT activity. Perform the tasks in the activity instructions and then answer the question.  
Which two networks are two hops away from Router2? (Choose two.)​

2001:DB8::

2001:DB8:1::

**2001:DB8:2::**

2001:DB8:5::

**2001:DB8:6::**

2001:DB8:8::​

Refer to curriculum topic: 7.5.4  
To configure RIPng, the following steps must be completed:  
1. Activate ipv6 routing.  
2. Enable the RIP-ID process on interface Fa0/0.  
3. Enable the RIP-ID process on interface Fa0/1.  
View the ipv6 routing table and determine which networks have metrics of 2.

Question 6

2 / 2 pts

Which factor directly affects the time to convergence?

the data link layer protocol used

number of hosts

**size of the network**

type of applications used

Refer to curriculum topic: 7.1.3  
The factors that directly affect the time to convergence are the speed of the links, the type of protocol used, and the size of the network. The number of hosts, the applications, and the Layer 2 protocol that is used have no direct impact on the time to reach convergence.

Question 7

2 / 2 pts

What is the difference between interior and exterior routing protocols?

Exterior routing protocols are only used by large ISPs. Interior routing protocols are used by small ISPs.

Interior routing protocols are used to route on the Internet. Exterior routing protocols are used inside organizations.

Exterior routing protocols are used to administer a single autonomous system. Interior routing protocols are used to administer several domains.

**Interior routing protocols are used to communicate within a single autonomous system. Exterior routing protocols are used to communicate between multiple autonomous systems.**

Refer to curriculum topic: 7.1.4

Question 8

0 / 2 pts

Which classless routing protocol supports VLSM and CIDR, supports manual route summarization, and uses the multicast address 224.0.0.9?

RIPv1

**RIPv2**

OSPF

EIGRP

Refer to curriculum topic: 7.2.2  
A router using RIPv1 sends out a broadcast, not multicast, message to communicate with an adjacent RIPv1 router. OSPF and EIGRP use multicast addresses for updates between routers.

Question 9

2 / 2 pts

What is an advantage of OSPF compared to RIP?

**fast convergence**

less complexity

less CPU processing

low memory requirements

Refer to curriculum topic: 7.4.3  
Link-state routing protocols require more CPU processing and memory to compute the routes using the Dijkstra algorithm. They are more complex but converge much faster than distance vector protocols like RIP.

Question 10

2 / 2 pts

Which two statements are true for OSPF Hello packets? (Choose two.)

They are used to negotiate correct parameters among neighboring interfaces.

**They are used to maintain neighbor relationships.**

They are used to determine the complete network topology.

**They are used for dynamic neighbor discovery.**

They are used to flood link-state information to all neighbors.

Refer to curriculum topic: 7.4.2  
Hello packets are small packets used to find neighbors and maintain neighbor relationships. As long as hello packets are received periodically from neighbors, they are deemed to be still alive and functioning.

Question 11

2 / 2 pts

What is the purpose of classifying Cisco IP routing table entries as ultimate route, level 1 route, level 1 parent route, and level 2 child routes?

to enable the implementation of dynamic routing protocols

to explain the operation of the routing table as a flat database

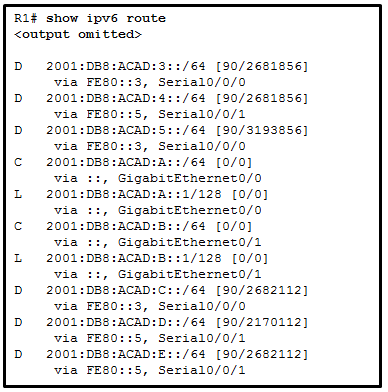
to enable Cisco routers to implement both IPv4 and IPv6 routing

**to explain the operation of the hierarchical structure of the routing table**

Refer to curriculum topic: 7.5.2  
The Cisco IP routing table is not a flat database. It has a hierarchical structure that is used to expedite the lookup process when locating routes and forwarding packets. The terms ultimate route, level 1 route, level 1 parent route, and level 2 child routes describe the operation and the hierarchical nature of the routing table contents.

Question 12

2 / 2 pts



Refer to the exhibit. What is the metric to forward a data packet with the IPv6 destination address 2001:DB8:ACAD:E:240:BFF:FED4:9DD2?

90

128

2170112

2681856

**2682112**

3193856

Refer to curriculum topic: 7.5.4  
The IPv6 destination address 2001:DB8:ACAD:E:240:BFF:FED4:9DD2 belongs to the network of 2001:DB8:ACAD:E::/64. In the routing table, the route to forward the packet has Serial 0/0/1 as an exit interface and 2682112 as the cost.

Question 13

2 / 2 pts

What are two functions of dynamic routing protocols? (Choose two.)

**to maintain routing tables**

to assure low router overhead

to avoid exposing network information

**to discover the network**

to choose the path that is specified by the administrator

Refer to curriculum topic: 7.1.1  
Dynamic routing protocols exist to discover the network, maintain routing tables, and calculate the best path. Having low levels of routing overhead, using the path specified by the administrator, and avoiding the exposure of network information are functions of static routing.

Question 14

2 / 2 pts

What are two characteristics of link-state protocols compared to distance vector protocols? (Choose two.)

**They require a lot of hardware resources.**

They know of the network topology from the perspective of their neighbors.

**They compute their own knowledge of the network topology.**

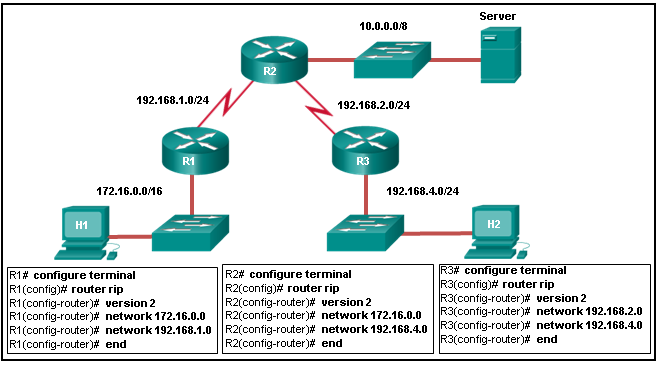
They use hop counts to compute the network topology.

They flood the routing table to all hosts periodically.

Refer to curriculum topic: 7.1.4  
OSPF is an example of a link-state protocol. It uses the Dijkstra algorithm to calculate the best path route. This is a complex algorithm and is used to compute the network topology based on all the link-state packets it receives from all the routers in the area. It thus computes the network topology from its own perspective and not from the perspective of its neighbors.

Question 15

2 / 2 pts



Refer to the exhibit. All hosts and router interfaces are configured correctly. Pings to the server from both H1 and H2 and pings between H1 and H2 are not successful. What is causing this problem?

RIPv2 does not support VLSM.

RIPv2 is misconfigured on router R1.

**RIPv2 is misconfigured on router R2.**

RIPv2 is misconfigured on router R3.

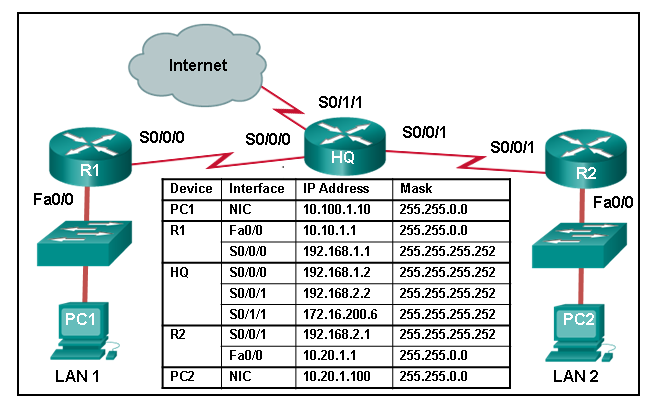
RIPv2 does not support discontiguous networks.

Refer to curriculum topic: 7.3.1  
RIP configuration on a router should contain network statements for connected networks only. Remote networks are learned from routing updates from other routers.

# Section 7.1 Quiz

Question 1

2 / 2 pts



Refer to the exhibit. A network engineer is configuring IPv6 routing on the network. Which command issued on router HQ will configure a default route to the Internet to forward packets to an IPv6 destination network that is not listed in the routing table?​

ipv6 route ::/0 serial 0/0/0

ip route 0.0.0.0 0.0.0.0 serial 0/1/1

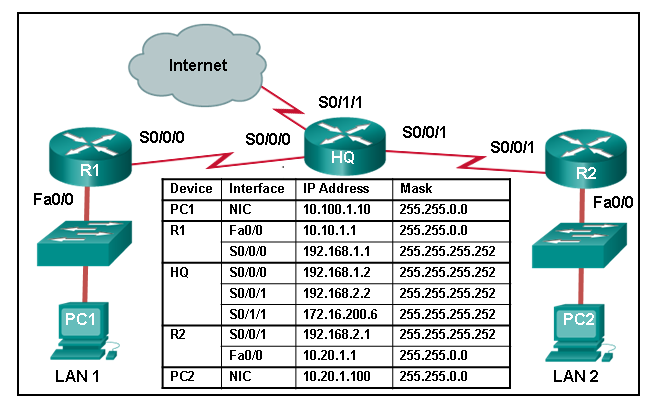
ipv6 route ::1/0 serial 0/1/1

**ipv6 route ::/0 serial 0/1/1**

Refer to curriculum topic: 2.2.4  
Commands that begin with **ip** relate to IPv4 processes. IPv6 specific commands begin with **ipv6**. The address ::1 is the IPv6 loopback address.

Question 2

2 / 2 pts



Refer to the exhibit. A network engineer is troubleshooting why PC1 cannot communicate with hosts in other networks. What is the problem?

A default route has not been configured on router R1.

A default gateway IP address of 10.20.1.1 needs to be configured on PC1.

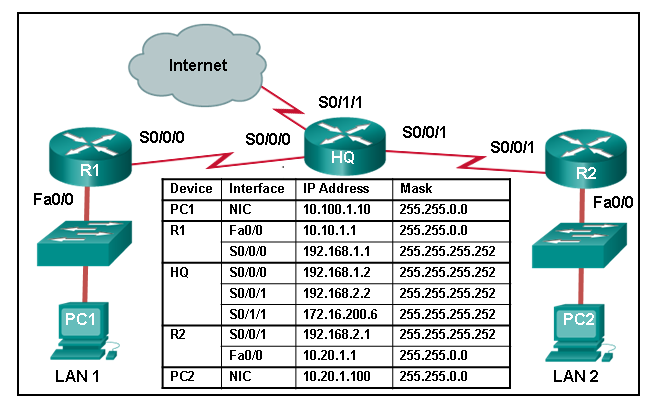
**The IP address that is configured on PC1 is in a different network than the gateway address on router R1.**

The subnet mask that is configured on PC1 is the same as the mask that is configured on the router R1 interface.

Refer to curriculum topic: 1.1.2  
For PC1 to be able to communicate with hosts on the other networks, it needs to have an IP address in the same network as the gateway to which it is connected. Its current address of 10.100.1.10/16 is not within the 10.10.0.0/16 network of the gateway interface on R1 (address 10.10.1.1/16).

Question 3

2 / 2 pts



Refer to the exhibit. Given that HQ is correctly configured, what is the next hop address of a packet that HQ is forwarding to LAN 1?

10.10.1.1

10.100.1.10

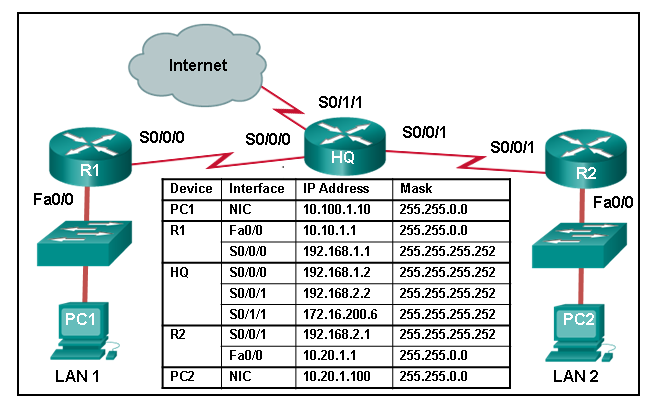
192.168.1.2

**192.168.1.1**

Refer to curriculum topic: 1.2.1  
The final destination address of a packet that is sent to LAN 1 is the 10.10.0.0/16 network, but HQ will send the packet to the next-hop interface on router, R1, which has the address of 192.168.1.1.

Question 4

2 / 2 pts



Refer to the exhibit. What is the IP address of the gateway for LAN 2?

10.10.1.1

**10.20.1.1**

192.168.2.2

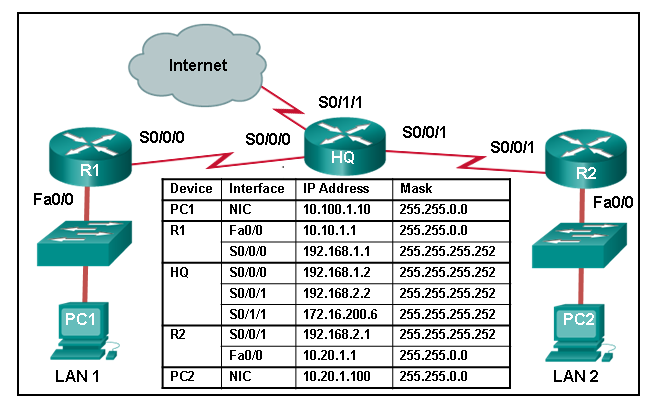
10.20.1.100

192.168.2.1

Refer to curriculum topic: 1.1.2  
The gateway for a network is the router interface to which the network is directly connected.

Question 5

2 / 2 pts



Refer to the exhibit. Which command that is issued on R1 will ensure that a packet from LAN 1 and destined for LAN 2 will be forwarded correctly?

ip route 10.20.0.0 255.255.0.0 192.168.1.1

ip route 10.10.0.0 255.255.0.0 192.168.1.2

**ip route 10.20.0.0 255.255.0.0 serial 0/0/0**

ip route 10.20.0.0 255.255.0.0 fastethernet 0/0

Refer to curriculum topic: 2.2.1  
To configure a static route the command **ip route** *prefix* *mask* {*ip-address* | *interface-type* *interface-number* [*ip-address*]} is used. The correct commands in this case would be:  
**ip route 10.20.0.0 255.255.0.0 serial 0/0/0**  
or  
**ip route 10.20.0.0 255.255.0.0 192.168.1.2**  
or  
**ip route 10.20.0.0 255.255.0.0 serial 0/0/0 192.168.1.2**

Question 6

2 / 2 pts



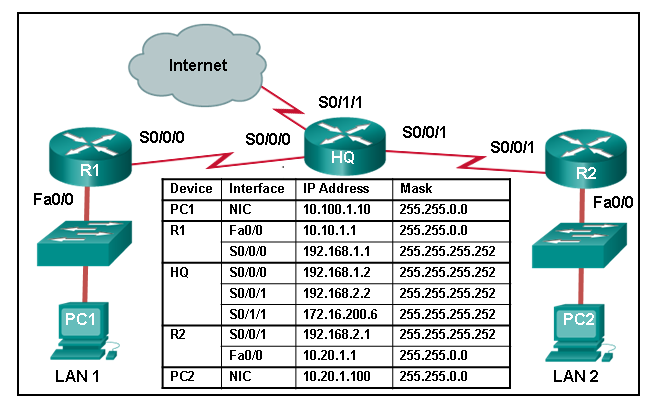
Refer to the exhibit. Fill in the blank.  
A route to network /16 is required in the routing table of HQ to forward a packet from LAN 1 to LAN 2.

**Answer 1:**

**10.20.0.0**

Question 7

2 / 2 pts



Refer to the exhibit. A network engineer is replacing the static routing on the network with dynamic routing. If all shown interfaces are active, what is the first step that a configured dynamic routing protocol will perform on router HQ?

Router HQ will add the remote 10.10.0.0/16 and 10.20.0.0/16 networks to its routing table.

**Router HQ will attempt to send information about the 192.168.1.0/30, 192.168.2.0/30, and 172.16.200.4/30 networks to routers R1 and R2.**

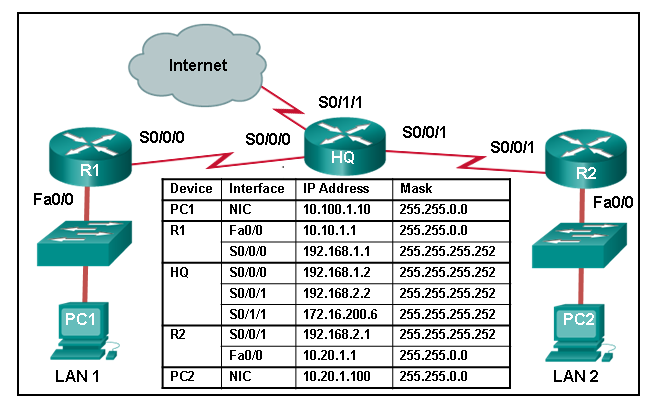
Router HQ will add the 192.168.1.0/30, 192.168.2.0/30, and 172.16.200.4/30 networks to its routing table.

Router HQ will initially send information about network 172.16.200.4/30 to routers R1 and R2.

Refer to curriculum topic: 3.1.3  
When the routing protocol is first configured, router HQ will attempt to communicate with routers R1 and R2 by sending details of all its active directly connected networks. A router will add directly connected active networks and subnet masks to its routing table when it first starts up whether or not a dynamic routing protocol is configured. The remote 10.10.0.0/16 and 10.20.0.0/16 networks will only be added to the routing table on HQ after HQ has received that information from R1 and R2.

Question 8

2 / 2 pts



Refer to the exhibit. In addition to static routes directing traffic to networks 10.10.0.0/16 and 10.20.0.0/16, Router HQ is also configured with the following command:  
  
**ip route 0.0.0.0 0.0.0.0 serial 0/1/1**  
  
What is the purpose of this command?

Packets that are destined for networks that are not in the routing table of HQ will be dropped.

**Packets with a destination network that is not 10.10.0.0/16 or is not 10.20.0.0/16 or is not a directly connected network will be forwarded to the Internet.**

Packets that are received from the Internet will be forwarded to one of the LANs connected to R1 or R2.

Packets from the 10.10.0.0/16 network will be forwarded to network 10.20.0.0/16, and packets from the 10.20.0.0/16 network will be forwarded to network 10.10.0.0/16.

Refer to curriculum topic: 2.2.2  
The command **ip route 0.0.0.0 0.0.0.0 serial 0/1/1** configures a default route on router HQ that will cause packets with a destination network address that is not an entry on the routing table to be forwarded to the Internet out interface serial 0/1/1.

# Chapter 8 Quiz

Question 1

2 / 2 pts

A network administrator configures a loopback interface as the OSPF router ID with the IP address of 192.168.1.1/30. What could be the consequence of using this 30-bit mask for the loopback interface?

Older routers do not recognize the **router-id** command.

The interface is not enabled for OSPF.

OSPF routers must also be configured with a router priority value.

**This loopback interface may be advertised as a reachable network.**

Refer to curriculum topic: 8.2.1  
A loopback interface used as an OSPF router ID normally uses a 32-bit mask that creates a host route. This route is not advertised as a route to other routers unless a network statement including this interface is added.

Question 2

2 / 2 pts

Which statement is correct about multiarea OSPF?

OSPF can consolidate a fragmented OSPF area into one large area.

All routers are in one area called the backbone area (area 0).

**Arranging routers into areas partitions a large autonomous system in order to lighten the load on routers.**

OSPF multiarea increases the frequency of SPF calculation.

Refer to curriculum topic: 8.1.1  
A company with one large autonomous system or AS can be divided into smaller areas. When this occurs and the OSPF routing protocol is implemented, the design is called multiarea OSPF. Multiarea OSPF decreases the frequency of the SPF calculation, thus lightening the load on the router. In a single area OSPF design, all the routers are located in area 0 or the backbone area.

Question 3

2 / 2 pts

Which statement describes a difference or similarity between OSPFv2 and OSPFv3?

OSPFv2 requires the DR/BDR election to occur on multiaccess networks only, whereas OSPv3 requires DR/BDR elections for all network types.

Both OSPFv2 and OSPFv3 use the router configuration **network** command to advertise networks.

**Both OSPFv2 and OSPFv3 use multicast destination addresses for link-state packets.**

OSPFv2 uses a 32 bit router ID and OSPFv3 uses a 128 bit router ID.

Refer to curriculum topic: 8.3.1  
OSPFv2 uses the router configuration **network** command to advertise networks. OSPFv3 uses the **ipv6 ospf** *process-id* **area** *area-id* interface configuration command. Both OSPFv2 and OSPFv3 use a 32 bit router ID. Both OSPFv2 and OSPFv3 require the DR/BDR election to occur on multiaccess networks. Neither protocol requires a DR/BDR election for point-to-point networks.

Question 4

2 / 2 pts

Which OSPF wildcard mask would be appropriate to use for the given network prefix?

/30 and 0.0.0.2

**/13 and 0.7.255.255**

/23 and 0.0.2.255

/18 and 0.0.64.255

Refer to curriculum topic: 8.2.2  
To calculate wildcard masks, follow these steps:  
1.  Change the subnet mask into dotted-decimal format.  
2.  Subtract the resulting mask from 255.255.255.255.  
3.  The result is the wildcard mask.  
Example: A mask of  /18 equals 255.255.192.0. A mask of 255.255.192.0 subtracted from 255.255.255.255 yields a wildcard mask of 0.0.63.255.

Question 5

2 / 2 pts

Match each OSPF packet type to how it is used by a router. (Not all options are used.)

**link-state update packet**

**advertise new information**

**database description packet**

**compare local topology to that sent by another router**

**hello packet**

**establish and maintain adjacencies**

**link-state request packet**

**query another router for additional information**

Refer to curriculum topic: 8.1.2

Question 6

2 / 2 pts

What are three entries that are displayed by the **show ip ospf neighbor** command? (Choose three.)

the route metric and neighbor next hop address

**the router ID of the neighboring routers**

**the OSPF state of each interface**

the OSPF process ID used to establish the adjacency

the OSPF area number shared by the neighbor routers

**the IP address of the neighbor router interface to which this router is directly connected**

Refer to curriculum topic: 8.2.4  
The route metric and neighbor next hop address are routing table entries that are displayed by the **show ip route** command. The **show ip ospf neighbor** command does not display the OSPF process ID or the OSPF area number.

Question 7

2 / 2 pts

Fill in the blank. Do not use abbreviations.  
The command **clear ip ospf** forces a router with a new or changed router ID to form new adjacencies.

**Answer 1:**

**process**

Refer to curriculum topic: 8.2.1  
An active OSPF router will not allow the router ID to be changed until it is reloaded or the OSPF process is cleared. Clearing the current process forces the router to renegotiate adjacencies and advertise its new information.

Question 8

2 / 2 pts

A network technician issues the following commands when configuring a router:  
R1(config)# **router ospf 11**   
R1(config-router)# **network 10.10.10.0 0.0.0.255 area 0**   
  
What does the number 11 represent?

the autonomous system number to which R1 belongs

the area number where R1 is located

the cost of the link to R1

**the OSPF process ID on R1**

the administrative distance that is manually assigned to R1

Refer to curriculum topic: 8.2.1  
There is no autonomous system number to configure on OSPF. The area number is located at the end of the network statement. The cost of a link can be modified in the interface configuration mode. The process ID is local to the router.

Question 9

2 / 2 pts

Which two statements are correct about the OSPF **passive-interface** command? (Choose two.)

**The OSPF network will benefit from more efficient use of bandwidth and resources.**

The router will not advertise the network of the passive interface to its neighbors.

OSPF link-state information is still sent and received through the passive interface.

**The router will not establish any OSPF neighbor relationships with routers on that link.**

Refer to curriculum topic: 8.2.2  
The **passive-interface** router configuration mode command prevents routing messages from being transmitted through a router interface but it will still allow that network to be advertised to other routers through other participating interfaces. Stopping the unnecessary forwarding of routing protocol messages through a LAN interface saves bandwidth and provides more efficient use of resources on LAN devices.

Question 10

2 / 2 pts

Fill in the blank.  
The wildcard mask that is used to advertise exactly the network 192.168.160.0 with subnet mask 255.255.240.0 is

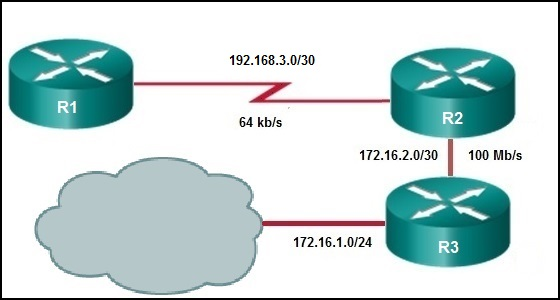
**Answer 1:**

**0.0.15.255**

Refer to curriculum topic: 8.2.2  
The easiest method for calculating a wildcard mask is to subtract the network subnet mask from 255.255.255.255. In this case we have 255.255.255.255 - 255.255.240.0.

Question 11

2 / 2 pts



Fill in the blank.  
Refer to the exhibit. With the default metric settings, the OSPF cost for R1 to reach the network 172.16.1.0 is

**Answer 1:**

**1564**

Refer to curriculum topic: 8.2.3  
The OSPF cost metric is the accumulated value from R1 to network 172.16.1.0. The cost for the first link is 100,000,000/64,000 (1562). The cost for the second link is 100,000,000/100,000,000 (1). The cost for the third link is 100,000,000/100,000,000 (1). The OSPF cost metric from R1 to 172.16.1.0 is therefore 1564.

Question 12

2 / 2 pts

At which OSPF state are neighbor routers converged and able to exchange routing updates?

Two-Way

ExStart

Exchange

**Full**

Refer to curriculum topic: 8.1.3  
OSPF neighbors that reach the Full state are converged and can exchange routing information.

Question 13

2 / 2 pts

The OSPF hello timer has been set to 15 seconds on a router in a point-to-point network. By default, what is the dead interval on this router?

15 seconds

30 seconds

45 seconds

**60 seconds**

Refer to curriculum topic: 8.1.2  
By default, the dead interval is calculated as 4 times the hello interval.

Question 14

2 / 2 pts

What will an OSPF router prefer to use first as a router ID?

**any IP address that is configured using the router-id command**

a loopback interface that is configured with the highest IP address on the router

the highest active interface IP that is configured on the router

the highest active interface that participates in the routing process because of a specifically configured **network** statement

Refer to curriculum topic: 8.2.1  
The first preference for an OSPF router ID is an explicitly configured 32-bit address. This address is not included in the routing table and is not defined by the **network** command. If a router ID that is configured through the **router-id** command is not available, OSPF routers next use the highest IP address available on a loopback interface, as loopbacks used as router IDs are also not routable addresses. Lacking either of these alternatives, an OSPF router will use the highest IP address from its active physical interfaces.

# Chapter 8 Quiz - Implementing Virtual Private Networks

Question 1

2 / 2 pts

What three protocols must be permitted through the company firewall for establishment of IPsec site-to-site VPNs? (Choose three.)

**ESP**

NTP

HTTPS

**AH**

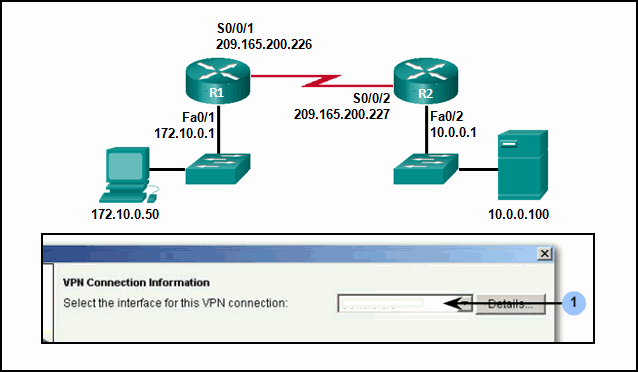
**ISAKMP**

SSH

Refer to curriculum topic: 8.4.2  
ESP, AH, and ISAKMP must all be permitted through the perimeter routers and firewalls in order for IPsec site-to-site VPNs to be established. NTP and HTTPS are application protocols and are not required for IPsec.

Question 2

2 / 2 pts



Refer to the exhibit. Router R1 is being configured for a site-to-site VPN via the CCP Step by Step wizard from the LAN host at IP address 172.10.0.50. What interface ID will be displayed in the box marked 1 when the VPN is configured correctly?

FastEthernet 0/1

FastEthernet 0/2

**Serial 0/0/1**

Serial 0/0/2

Refer to curriculum topic: 8.5.3  
The Step by Step wizard will display the interfaces available on the router that is being configured. In this case there will be two interfaces to choose from, FastEthernet 0/1 and Serial 0/0/1. The correct interface is the outside interface connected to the IPsec peer over the untrusted network, Serial 0/0/1.

Question 3

2 / 2 pts

Which method of Internet connectivity is typically used for remote-access VPNs by telecommuters?

an ATM connection

**a broadband connection**

a Frame Relay connection

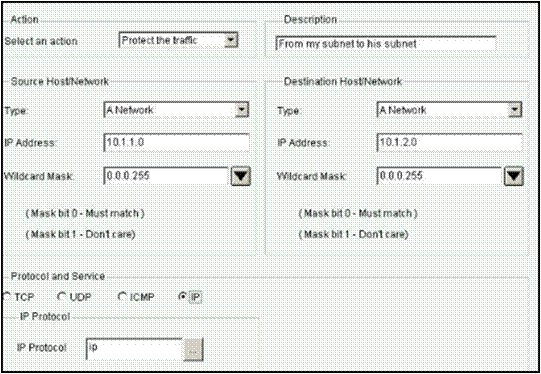
a GRE tunnel

a leased line

Refer to curriculum topic: 8.1.2  
Remote-access VPNs typically use a broadband connection for Internet connectivity because that is what a person would be using from a home network or from a hotel if the person is traveling. Site-to-site VPNs commonly consist of Frame Relay, ATM, and leased line or GRE tunnel connectivity.

Question 4

2 / 2 pts



Refer to the exhibit. What action will the router configured with the shown access rule take on traffic that is sourced from the 10.1.1.0/24 network and destined to the 10.1.2.0/24 network?

**It will forward the traffic encrypted over the VPN.**

It will block the traffic.

It will drop the traffic.

It will forward the traffic in plain text over the VPN.

Refer to curriculum topic: 8.5.3  
The access rule as shown in the wizard will create an access-list which will define interesting traffic as any IP traffic that originates from the 10.1.1.0 network and is destined to the 10.1.2.0 network. The interesting traffic will be encrypted and forwarded to the VPN peer.

Question 5

2 / 2 pts

Which statement describes the effect of key length in deterring an attacker from hacking through an encryption key?

The length of a key will not vary between encryption algorithms.

The length of a key does not affect the degree of security.

The shorter the key, the harder it is to break.

**The longer the key, the more key possibilities exist.**

Refer to curriculum topic: 8.3.1  
While preventing brute-force attacks and other forced decryption concerns, the longer the key length, the harder it is to break. A 64-bit key can take one year to break with a sophisticated computer, while a 128-bit key may take 1019years to decrypt. Different encryption algorithms will provide varying key lengths for implementation.

Question 6

2 / 2 pts

What Cisco VPN solution provides users with remote-access connectivity using only a web browser and requires no pre-installed client software?

Cisco Easy VPN

Cisco VPN wizard

**Cisco SSL VPN**

Cisco VPN client

Refer to curriculum topic: 8.6.3  
The Cisco SSL VPN solution provides remote-access connectivity for users from almost any Internet-enabled location using only an SSL-capable web browser.

Question 7

2 / 2 pts

Which IPsec framework protocol provides data integrity and data authentication, but does not provide data confidentiality?

**AH**

IP protocol 50

ESP

DH

Refer to curriculum topic: 8.3.2  
Authentication Header (AH) is IP protocol 51 and does not provide data confidentiality. The data payload is not encrypted. Encapsulating Security Payload (ESP) is IP protocol 50 and provides data confidentiality, integrity, and authentication. The DH algorithm is used in IPsec to negotiate a shared secret key for the peers.

Question 8

2 / 2 pts

Which IPsec security function provides assurance that the data received via a VPN has not been modified in transit?

confidentiality

**integrity**

authentication

secure key exchange

Refer to curriculum topic: 8.3.1  
Integrity is a function of IPsec and ensures data arrives unchanged at the destination through the use of a hash algorithm. Confidentiality is a function of IPsec and utilizes encryption to protect data transfers with a key. Authentication is a function of IPsec and provides specific access to users and devices with valid authentication factors. Secure key exchange is a function of IPsec and allows two peers to maintain their private key confidentiality while sharing their public key.

Question 9

2 / 2 pts

Which type of VPN may require the Cisco VPN Client software?

**remote access VPN**

SSL VPN

site-to-site VPN

MPLS VPN

Refer to curriculum topic: 8.1.2  
With a remote-access VPN, the client peer may need special VPN client software installed.

Question 10

2 / 2 pts

Which two statements accurately describe characteristics of IPsec? (Choose two.)

IPsec works at the application layer and protects all application data.

IPsec works at the transport layer and protects data at the network layer.

**IPsec works at the network layer and operates over all Layer 2 protocols.**

IPsec is a framework of proprietary standards that depend on Cisco specific algorithms.

IPsec is a framework of standards developed by Cisco that relies on OSI algorithms.

**IPsec is a framework of open standards that relies on existing algorithms.**

Refer to curriculum topic: 8.3.1  
IPsec can secure a path between two network devices. IPsec can provide the following security functions:

* **Confidentiality** - IPsec ensures confidentiality by using encryption.
* **Integrity** - IPsec ensures that data arrives unchanged at the destination using a hash algorithm, such as MD5 or SHA.
* **Authentication** - IPsec uses Internet Key Exchange (IKE) to authenticate users and devices that can carry out communication independently. IKE uses several types of authentication, including username and password, one-time password, biometrics, pre-shared keys (PSKs), and digital certificates.
* **Secure key exchange** - IPsec uses the Diffie-Hellman (DH) algorithm to provide a public key exchange method for two peers to establish a shared secret key.

Question 11

2 / 2 pts

Which Cisco VPN product line is available for purchase, provides enterprise-class security, and incorporates firewall, IPS, and VPN functionality for large networks?

Cisco VPN 3000 Series Concentrators

Cisco ISR routers

Cisco PIX 500 Series Security Appliances

**Cisco Adaptive Security Appliances**

Refer to curriculum topic: 8.1.3  
Cisco ASA appliances deliver enterprise-class security and IPsec VPN technology to small, medium, and large enterprise networks. Cisco PIX, and VPN 3000 concentrators are designated end-of-sale and end-of-life. The Cisco ISR routers provide small to medium-sized business functionality.

Question 12

2 / 2 pts

Which UDP port must be permitted on any IP interface used to exchange IKE information between security gateways?

400

**500**

600

700

Refer to curriculum topic: 8.3.3  
Because IKE uses UDP port 500, this port must be permitted on the interfaces over which IKE information travels.

# Chapter 8 Quiz

Question 1

2 / 2 pts

What are two benefits of subnetting networks? (Choose two.)

combining multiple smaller networks into larger networks

**reducing the size of broadcast domains**

decreasing the number of broadcast domains

**grouping devices to improve management and security**

increasing the size of collision domains

Refer to curriculum topic: 8.1.1  
When a single network is subnetted into multiple networks the following occurs:

* A new broadcast domain is created for every network that is created through subnetting.
* The amount of network traffic that crosses the entire network decreases.
* Devices can be grouped together to improve network management and security.
* More IP addresses are usable because each network will have a network address and broadcast address.

Question 2

2 / 2 pts

The network portion of the address 172.16.30.5/16 is .

**Answer 1:**

**172.16**

Refer to curriculum topic: 8.1.2  
A prefix of /16 means that 16 bits are used for the network part of the address. The network portion of the address is therefore 172.16.

Question 3

2 / 2 pts

A college has five campuses. Each campus has IP phones installed. Each campus has an assigned IP address range. For example, one campus has IP addresses that start with 10.1.x.x. On another campus the address range is 10.2.x.x. The college has standardized that IP phones are assigned IP addresses that have the number 4X in the third octet. For example, at one campus the address ranges used with phones include 10.1.40.x, 10.1.41.x, 10.1.42.x, etc. Which two groupings were used to create this IP addressing scheme? (Choose two.)

**geographic location**

**device type**

department

personnel type

support model

Refer to curriculum topic: 8.1.1  
The IP address design being used is by geographic location (for example, one campus is 10.1, another campus 10.2, another campus 10.3). The other design criterion is that the next octet number designates IP phones, or a specific device type, with numbers starting with 4, but which can include other numbers. Other devices that might get a designation inside this octet could be printers, PCs, and access points.

Question 4

2 / 2 pts

Three methods allow IPv6 and IPv4 to co-exist. Match each method with its description. (Not all options are used.)

**The IPv4 packets and IPv6 packets coexist in the same network.**

**The IPv6 packet is transported inside an IPv4 packet.**

**IPv6 packets are converted into IPv4 packets, and vice versa.**

Other Incorrect Match Options:

* DHCP

Refer to curriculum topic: 7.2.1  
The term for the method that allows for the coexistence of the two types of packets on a single network is dual-stack. Tunneling allows for the IPv6 packet to be transported inside IPv4 packets. An IP packet can also be converted from version 6 to version 4 and vice versa. DHCP is a protocol that is used for allocating  network parameters to hosts on an IP network.

Question 5

2 / 2 pts

Fill in the blank.  
The last host address on the 10.15.25.0/24 network is .

**Answer 1:**

**10.15.25.254/24**

Refer to curriculum topic: 8.1.3  
The host portion of the last host address will contain all 1 bits with a 0 bit for the lowest order or rightmost bit. This address is always one less than the broadcast address. The range of addresses for the network 10.15.25.0/24 is 10.15.25.0 (network address) through 10.15.25.255 (broadcast address). So the last host address for this network is 10.15.25.254.

Question 6

2 / 2 pts

What does the IP address 192.168.1.15/29 represent?

subnetwork address

multicast address

unicast address

**broadcast address**

Refer to curriculum topic: 8.1.2  
A broadcast address is the last address of any given network. This address cannot be assigned to a host, and it is used to communicate with all hosts on that network.

Question 7

2 / 2 pts

A network administrator has received the IPv6 prefix 2001:DB8::/48 for subnetting. Assuming the administrator does not subnet into the interface ID portion of the address space, how many subnets can the administrator create from the /48 prefix?

16

256

4096

**65536**

Refer to curriculum topic: 8.3.1  
With a network prefix of 48, there will be 16 bits available for subnetting because the interface ID starts at bit 64. Sixteen bits will yield 65536 subnets.

Question 8

2 / 2 pts

What is the subnet address for the IPv6 address 2001:D12:AA04:B5::1/64?

2001::/64

2001:D12::/64​

2001:D12:AA04::/64​

**2001:D12:AA04:B5::/64​**

Refer to curriculum topic: 8.3.1  
The /64 represents the network and subnet IPv6 fields which are the first four groups of hexadecimal digits. The first address within that range is the subnetwork address of 2001: D12:AA04:B5::/64.​

Question 9

2 / 2 pts

An administrator wants to create four subnetworks from the network address 192.168.1.0/24. What is the network address and subnet mask of the second useable subnet?

**subnetwork 192.168.1.64  
subnet mask 255.255.255.192**

subnetwork 192.168.1.32  
subnet mask 255.255.255.240

subnetwork 192.168.1.64  
subnet mask 255.255.255.240

subnetwork 192.168.1.128  
subnet mask 255.255.255.192

subnetwork 192.168.1.8  
subnet mask 255.255.255.224

Refer to curriculum topic: 8.1.4  
The number of bits that are borrowed would be two, thus giving a total of 4 useable subnets:  
192.168.1.0  
192.168.1.64  
192.168.1.128  
192.168.1.192  
Because 2 bits are borrowed, the new subnet mask would be /26 or 255.255.255.192

Question 10

2 / 2 pts

Three devices are on three different subnets. Match the network address and the broadcast address with each subnet where these devices are located. (Not all options are used.)

Device 1: IP address 192.168.10.77/28 on subnet 1

Device 2: IP address192.168.10.17/30 on subnet 2

Device 3: IP address 192.168.10.35/29 on subnet 3

**Subnet 1 network number**

**192.168.10.64**

**Subnet 1 broadcast address**

**192.168.10.79**

**Subnet 2 network number**

**192.168.10.16**

**Subnet 2 broadcast address**

**192.168.10.19**

**Subnet 3 network number**

**192.168.10.32**

**Subnet 3 broadcast address**

**192.168.10.39**

Refer to curriculum topic: 8.1.5  
To calculate any of these addresses, write the device IP address in binary. Draw a line showing where the subnet mask 1s end. For example, with Device 1, the final octet (77) is 01001101. The line would be drawn between the 0100 and the 1101 because the subnet mask is /28. Change all the bits to the right of the line to 0s to determine the network number (01000000 or 64). Change all the bits to the right of the line to 1s to determine the broadcast address (01001111 or 79).

Question 11

2 / 2 pts

A network administrator subnets the 192.168.10.0/24 network into subnets with /26 masks. How many equal-sized subnets are created?

1

2

**4**

8

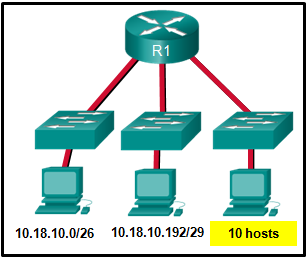
16

64

Refer to curriculum topic: 8.1.2  
The normal mask for 192.168.10.0 is /24. A /26 mask indicates 2 bits have been borrowed for subnetting. With 2 bits, four subnets of equal size could be created.​

Question 12

2 / 2 pts



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.)

10.18.10.200/28

**10.18.10.208/28**

**10.18.10.224/28**

10.18.10.200/27

10.18.10.224/27

10.18.10.240/27

Refer to curriculum topic: 8.1.5  
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.

Question 13

2 / 2 pts

How many host addresses are available on the 192.168.10.128/26 network?

30

32

60

**62**

64

Refer to curriculum topic: 8.1.2  
A /26 prefix gives 6 host bits, which provides a total of 64 addresses, because 26 = 64. Subtracting the network and broadcast addresses leaves 62 usable host addresses.

Question 14

2 / 2 pts

A network engineer is subnetting the 10.0.240.0/20 network into smaller subnets. Each new subnet will contain between a minimum of 20 hosts and a maximum of 30 hosts. Which subnet mask will meet these requirements?

255.255.224.0

255.255.240.0

**255.255.255.224**

255.255.255.240

Refer to curriculum topic: 8.1.4  
For each new subnet to contain between 20 and 30 hosts, 5 host bits are required. When 5 host bits are being used, 27 network bits are remaining. A /27 prefix provides the subnet mask of 255.255.255.224.

# Chapter 9 Quiz

Question 1

2 / 2 pts

Which series of commands will cause access list 15 to restrict Telnet access on a router?

**R1(config)# line vty 0 4  
R1(config​-line)# access-class 15 in**

R1(config)#**line vty 0 4**  
R1(config​-line)# **ip access-group 15 in**

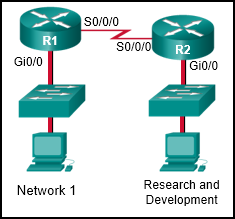
R1(config)#**int gi0/0**  
R1(config​-if)# **access-class 15 in**

R1(config)#**int gi0/0**  
R1(config​-if)# **ip access-group 15 in**

Refer to curriculum topic: 9.2.3  
Once an access list to restrict Telnet or SSH access has been created, it is applied to the vty lines with the **access-class** command. This will restrict Telnet or SSH access.

Question 2

2 / 2 pts



Refer to the exhibit. A network administrator wants to create a standard ACL to prevent network 1 traffic from being transmitted to the Research and Development network. On which router interface and in which direction should the standard ACL be applied?

R1 Gi0/0 inbound

R1 Gi0/0 outbound

R1 S0/0/0 outbound

R2 S0/0/0 inbound

**R2 Gi0/0 outbound**

R2 Gi0/0 inbound

Refer to curriculum topic: 9.1.5  
Standard ACLs can only specify source addresses, so the standard ACL would contain the network 1 address and appropriate wildcard mask. Also, because standard ACLs can only contain source addresses, the ACL should be placed as close to the destination as possible. The destination is the Research and Development LAN. The R2 Gi0/0 interface is that destination. By tracing the path that the packets will take starting with network 1 and traveling to the Research and Development network, a student can determine that the packets would be coming out of the R2 Gi0/0 interface.

Question 3

2 / 2 pts

Which command is used to activate an IPv6 ACL named ENG\_ACL on an interface so that the router filters traffic prior to accessing the routing table?

ipv6 access-class ENG\_ACL in

ipv6 access-class ENG\_ACL out

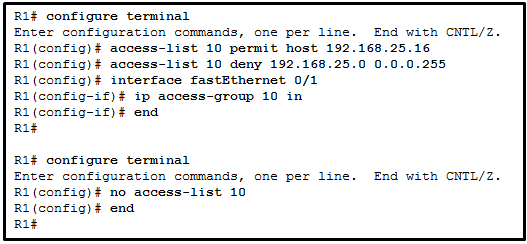
**ipv6 traffic-filter ENG\_ACL in**

ipv6 traffic-filter ENG\_ACL out

Refer to curriculum topic: 9.5.2  
For the purpose of applying an access list to a particular interface, the **ipv6 traffic-filter** IPv6 command is equivalent to the **access-group** IPv4 command. The direction in which the traffic is examined (in orout) is also required.

Question 4

2 / 2 pts



Refer to the exhibit. A network administrator is configuring a standard IPv4 ACL. What is the effect after the command **no access-list 10** is entered?

ACL 10 is disabled on Fa0/1.

**ACL 10 is removed from the running configuration.**

ACL 10 will be disabled and removed after R1 restarts.

ACL 10 is removed from both the running configuration and the interface Fa0/1.

Refer to curriculum topic: 9.2.1  
The R1(config)# **no access-list** access-list number> command removes the ACL from the running-config immediately. However, to disable an ACL on an interface, the command R1(config-if)# **no ip access-group** should be entered.

Question 5

2 / 2 pts

Which set of access control entries would allow all users on the 192.168.10.0/24 network to access a web server that is located at 172.17.80.1, but would not allow them to use Telnet?

access-list 103 deny tcp host 192.168.10.0 any eq 23  
access-list 103 permit tcp host 192.168.10.1 eq 80

access-list 103 permit 192.168.10.0 0.0.0.255 host 172.17.80.1  
access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq telnet​​

**access-list 103 permit tcp 192.168.10.0 0.0.0.255 host 172.17.80.1 eq 80  
access-list 103 deny tcp ​192.168.10.0 0.0.0.255 any eq 23**

access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80  
access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq 23

Refer to curriculum topic: 9.3.2  
For an extended ACL to meet these requirements the following need to be included in the access control entries:

* identification number in the range 100-199 or 2000-2699
* permit or deny parameter
* protocol
* source address and wildcard
* destination address and wildcard
* port number or name

Question 6

2 / 2 pts

Which range represents all the IP addresses that are affected when network 10.120.160.0 with a wildcard mask of 0.0.7.255 is used in an ACE?

10.120.160.0 to 10.127.255.255

**10.120.160.0 to 10.120.167.255**

10.120.160.0 to 10.120.168.0

10.120.160.0 to 10.120.191.255

Refer to curriculum topic: 9.1.3  
A wildcard mask of 0.0.7.255 means that the first 5 bits of the 3rd octet must remain the same but the last 3 bits can have values from 000 to 111. The last octet has a value of 255, which means the last octet can have values from all zeros to all 1s.

Question 7

2 / 2 pts

What is the effect of the **established** parameter in an extended ACL?

blocks all incoming traffic from reaching a network

**allows external traffic into a network only if it is part of an existing connection with an internal host**

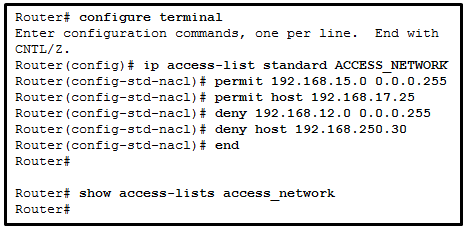
allows external sources to send unsolicited requests for information to source IP addresses in the network

allows traffic from a permitted source address to go to any destination outside the network

Refer to curriculum topic: 9.3.2  
The **established** parameter adds a level of security to network operations by requiring that the specified protocol traffic be initiated by an internal host. This is accomplished by checking for the presence of the ACK or RST bits in incoming TCP segments, which indicate the packets belong to an existing connection. For instance, adding **established** to an ACL permitting network hosts to use HTTP to reach a specified web server limits the traffic coming from that server to responses to requests. Unsolicited traffic will be blocked because the ACK or RST bits in the TCP header will not be set.

Question 8

2 / 2 pts



Refer to the exhibit. A network administrator configures a named ACL on the router. Why is there no output displayed when the **show** command is issued?

The ACL is not activated.

**The ACL name is case sensitive.**

The ACL has not been applied to an interface.

No packets have matched the ACL statements yet.

Refer to curriculum topic: 9.2.1  
The name in a named ACL is alphanumeric, case sensitive and unique. Thus, the router treats access\_network and ACCESS\_NETWORK as if they are two separate ACLs.

Question 9

2 / 2 pts

In the creation of an IPv6 ACL, what is the purpose of the implicit final command entries, **permit icmp any any nd-na** and **permit icmp any any nd-ns**?

**to allow IPv6 to MAC address resolution**

to allow forwarding of IPv6 multicast packets

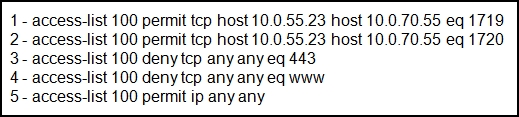
to allow automatic address configuration

to allow forwarding of ICMPv6 packets

Refer to curriculum topic: 9.5.1  
IPv6 address to MAC address resolution is performed through the exchange of ICMPv6 neighbor discovery packets comprised of neighbor solicitation and neighbor advertisement packets. Unless these packets are permitted on a router interface, the interface will not be able to perform MAC address resolution.

Question 10

2 / 2 pts



Refer to the exhibit. This ACL is applied on traffic outbound from the router on the interface that directly connects to the 10.0.70.5 server. A request for information from a secure web page is sent from host 10.0.55.23 and is destined for the 10.0.70.5 server. Which line of the access list will cause the router to take action (forward the packet onward or drop the packet)?

1

2

**3**

4

5

the deny ip any any that is at the end of every ACL

Refer to curriculum topic: 9.4.1  
The first two lines of the ACL allow traffic from a particular application from the IP address 10.0.55.23 destined for 10.0.70.55. Because neither of these lines meets the criterion of request for information from a secure web page (port 443 is HTTPS) from 10.0.55.23 to the web server located at 10.0.70.5, no action is taken by the router. The third line is a match and because the "permission" is to deny the packet, the packet is dropped. No further examination is done by the router.

Question 11

2 / 2 pts

Which two statements are correct about extended ACLs? (Choose two)

Extended ACLs use a number range from 1-99.

Extended ACLs end with an implicit permit statement.

**Extended ACLs evaluate the source and destination addresses.**

**Port numbers can be used to add greater definition to an ACL.**

Multiple ACLs can be placed on the same interface as long as they are in the same direction.

Refer to curriculum topic: 9.1.2

Question 12

2 / 2 pts

In applying an ACL to a router interface, which traffic is designated as outbound?

traffic that is coming from the source IP address into the router

**traffic that is leaving the router and going toward the destination host**

traffic that is going from the destination IP address into the router

traffic for which the router can find no routing table entry

Refer to curriculum topic: 9.3.2  
Inbound and outbound are interpreted from the point of view of the router. Traffic that is designated in an inbound ACL will be denied or permitted when coming into that router interface from a source. Traffic that is designated in an outbound ACL will be denied or permitted when going out the interface to the destination.

Question 13

2 / 2 pts

ACLs are used primarily to filter traffic. What are two additional uses of ACLs? (Choose two.)

specifying source addresses for authentication

**specifying internal hosts for NAT**

**identifying traffic for QoS**

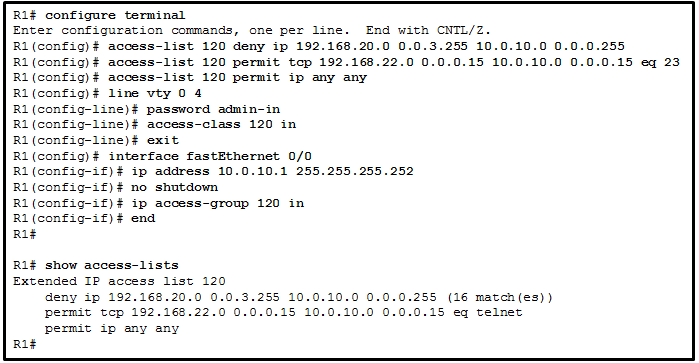
reorganizing traffic into VLANs

filtering VTP packets

Refer to curriculum topic: 9.1.1

Question 14

2 / 2 pts



Refer to the exhibit. A network administrator is configuring an ACL to limit the connection to R1 vty lines to only the IT group workstations in the network 192.168.22.0/28. The administrator verifies the successful Telnet connections from a workstation with IP 192.168.22.5 to R1 before the ACL is applied. However, after the ACL is applied to the interface Fa0/0, Telnet connections are denied. What is the cause of the connection failure?

The permit ACE specifies a wrong port number.

The enable secret password is not configured on R1.

The **login** command has not been entered for vty lines.

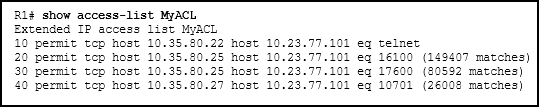
**The IT group network is included in the deny statement.**

The permit ACE should specify protocol ip instead of tcp.

Refer to curriculum topic: 9.4.2  
The source IP range in the deny ACE is 192.168.20.0 0.0.3.255, which covers IP addresses from 192.168.20.0 to 192.168.23.255. The IT group network 192.168.22.0/28 is included in the 192.168.20/22 network. Therefore, the connection is denied. To fix it, the order of the deny and permit ACE should be switched.

Question 15

2 / 2 pts



Refer to the exhibit. What can be determined from this output?

The ACL is missing the deny ip any any ACE.

Because there are no matches for line 10, the ACL is not working.

The ACL is only monitoring traffic destined for 10.23.77.101 from three specific hosts.

**The router has not had any Telnet packets from 10.35.80.22 that are destined for 10.23.77.101.**

Refer to curriculum topic: 9.4.1  
ACL entry 10 in MyACL matches any Telnet packets between host 10.35.80.22 and 10.23.77.101. No matches have occurred on this ACE as evidenced by the lack of a "(xxx matches)" ACE. The deny ip any any ACE is not required because there is an implicit deny ACE added to every access control list. When no matches exist for an ACL, it only means that no traffic has matched the conditions that exist for that particular line. The ACL is monitoring traffic that matches three specific hosts going to very specific destination devices. All other traffic is not permitted by the implicit deny ip any any ACE.

# Chapter 9 Quiz - Implementing the Cisco Adaptive Security Appliance

Question 1

2 / 2 pts

What two tools are available in ASDM to configure clientless SSL VPNs on a Cisco ASA? (Choose two.)

X-Windows

**ASDM Assistant**

Cisco AnyConnect VPN client

Cisco VPN client

**VPN wizard**

Refer to curriculum topic: 9.3.3  
The Cisco ASDM has two tools that can be used for configuring an SSL VPN on an ASA:

1. the ASDM assistant, which will guide an administrator through the SSL VPN configuration
2. the VPN wizard, which simplifies the SSL VPN configuration

Question 2

2 / 2 pts

Which statement is true about ASA CLI and IOS CLI commands?

The **show ip interface brief** command is valid for both CLIs.​

The ASA CLI does not recognize the **write erase** command, but the IOS CLI does.

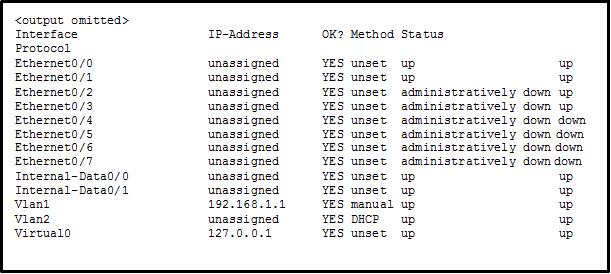
Only the ASA CLI requires the use of Ctrl-C to interrupt **show**commands.

**Both CLIs recognizes the Tab key to complete a partial command.**

Refer to curriculum topic: 9.2.1  
The ASA CLI recognizes the **write erase** command, not the **erase startup-config** command. The **show ip interface brief** command is valid only for the IOS CLI. The ASA CLI recognizes the **show interface ip brief** command. The ASA CLI requires the use of Q to interrupt **show** commands.

Question 3

2 / 2 pts



Refer to the exhibit. A network administrator is verifying the security configuration of an ASA. Which command produces the exhibited output?

show switch vlan

**show interface ip brief**

show vlan

show ip interface brief

Refer to curriculum topic: 9.2.2  
Use the **show interface ip brief** command to verify IP address assignment and interface status on an ASA.

Question 4

2 / 2 pts

Which condition must be met for a network administrator to remotely manage multiple ASAs with Cisco ASDM?

All the ASAs are the same model.

All the ASAs are in the same network.

**All the ASAs are running the same ASDM version.**

All the ASAs are configured with the same security policy.

Refer to curriculum topic: 9.2.3  
Cisco ASDM is a Java-based GUI tool that facilitates the management of Cisco ASAs. Cisco ASDM can be used to manage multiple ASAs that run the same ASDM version. As long as the condition is met, multiple ASAs can be managed through one ASDM, and they can be deployed in different local networks and running different security configurations.

Question 5

2 / 2 pts

In what three ways do the 5505 and 5510 Adaptive Security Appliances differ? (Choose three.)

in the method by which they can be configured using either CLI or ASDM

in their compatibility with Cisco SecureX technology

**in the maximum traffic throughput supported**

**in the number of interfaces**

in operating system version support

**in types of interfaces**

Refer to curriculum topic: 9.1.1 The Cisco ASA 5505 is an entry-level, full-featured security appliance for small businesses, branch offices, and enterprise teleworker environments. The ASA 5505 is commonly used as an edge security device that connects a small business to an ISP device for access to the Internet. It provides an 8 port 10/100 Fast Ethernet switch. The 5510 is a higher-end ASA model that is designed to deliver advanced security services for medium-d businesses and enterprise branch offices. The ASA 5510 supports 300 Mb/s throughput and a capacity of 9,000 firewall connections per second. The 5510 has 5 possible FastEthernet interfaces with expansion slots to provide gigabit support. The expansion slots also allows the capability of AIP-SSM and CSC-SSM that provides advanced IPD and threat protection.

Question 6

2 / 2 pts

A network engineer is using a Cisco ASA as a proxy device to provide remote secure access to a company web server. What technology is being used?

Cisco AnyConnect Secure Mobility Client with SSL

**Cisco Secure Mobility Clientless SSL VPN**

Cisco VPN Client

generic routing encapsulation tunnel using IPsec

Refer to curriculum topic: 9.0.0  
The clientless SSL VPN deployment model enables corporations to provide access to corporate resources even when the remote device is not corporately-managed. In this deployment model, the Cisco ASA is used as a proxy device to network resources. It provides a web portal interface for remote devices to navigate the network using port-forwarding capabilities. Cisco AnyConnect Secure Mobility Client will require installation of Cisco VPN client or AnyConnect client software on the end-user computer. Using a GRE tunnel with IPsec would create a site-to-site VPN, when a remote-access VPN would be better suited to this scenario.

Question 7

2 / 2 pts

Which protocol requires Layer 7 inspection by an ASA device?​

TFTP

**SNMP**

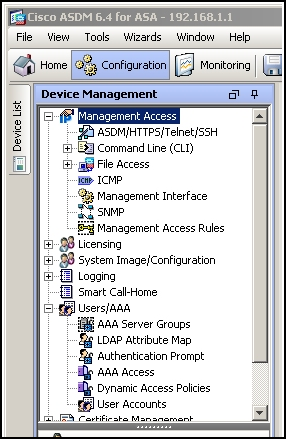
SMTP

Telnet

Refer to curriculum topic: 9.1.1  
Some packets require Layer 7 inspection by the ASA. This inspection is required for protocols that have two or more channels: a data channel and a control channel. Protocols that require Layer 7 inspection include FTP, H.323, and SNMP.

Question 8

2 / 2 pts



Refer to the exhibit. Which ASDM menu sequence would be required to configure Telnet or SSH AAA authentication using a TACACS server first or the local device user database if the TACACS server authentication is unavailable?

Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH

Configuration > Device Management > Management Access > Management Interface

**Configuration > Device Management > Users/AAA > AAA Access**

Configuration > Device Management > Users/AAA > AAA Server Group

Configuration > Device Management > Users/AAA > User Accounts

Refer to curriculum topic: 9.2.8

Question 9

2 / 2 pts

An administrator has successfully configured a site-to-site VPN on an ASA 5505. Which ASDM menu sequence displays the number of packets encrypted, decrypted, and security association requests?

Configuration > Site-to-Site VPN > Advanced

Configuration > Site-to-Site VPN > Connection Profiles

Configuration > Site-to-Site VPN > Group Policies

**Monitoring > VPN > VPN Statistics > Crypto Statistics**

Monitoring > VPN > VPN Statistics > Encryption Statistics

Monitoring > VPN > VPN Statistics > Sessions

Refer to curriculum topic: 9.3.3

Question 10

2 / 2 pts

Which statement describes a feature of ACLs on an ASA device?

Standard ACLs are not supported in an ASA.

An ACL is only required on the outside interface to filter traffic from the Internet.

**An ASA will provide access control and traffic inspection when no ACL is configured.**

Separate ACLs for network addresses and protocols are required when implementing ACLs in an ASA.

Refer to curriculum topic: 9.2.6  
Similar to IOS ACLs, ASA ACLs can use both standard and extended ACLs and only one ACL can be applied per interface, per protocol, and per direction. ASA devices will inspect and filter traffic based on the interface security levels. This is done without an ACL configured.

Question 11

2 / 2 pts

What is one of the drawbacks to using transparent mode operation on an ASA device?​

no support for IP addressing

no support for using an ASA as a Layer 2 switch​

no support for management

**no support for QoS**

Refer to curriculum topic: 9.1.1  
In transparent mode the ASA functions like a Layer 2 device. An ASA device can have an IP address assigned on the local network for management purposes. The drawbacks to using transparent mode include no support for dynamic routing protocols, VPNs, QoS, or DHCP Relay.

Question 12

2 / 2 pts

The ASA device can be configured using either the or the command-line interface.

**Answer 1:**

**ASDM**

Refer to curriculum topic: 9.2.1  
There are two ways to configure and manage the ASA device: the command-line interface (CLI) and the Adaptive Security Device Manager (ASDM).

# Section 9.1 Quiz

Question 1

2 / 2 pts

Fill in the blanks. Use dotted decimal format.  
The wildcard mask that is associated with the network 192.168.12.0/24 is .

**Answer 1:**

**0.0.0.255**

Refer to curriculum topic: 9.1.3  
The wildcard mask can be found by subtracting the subnet mask from 255.255.255.255.  
Mask 255.255.255.255  
Subnet mask - 255.255.255.0  
Wild card mask 0 . 0 . 0. 255

Question 2

2 / 2 pts

What range of IP addresses is represented by the network and wildcard mask 192.168.70.0 0.0.1.255?

**192.168.70.0 to 192.168.71.255**

192.168.70.0 to 192.168.70.255

192.168.70.0 to 192.168.73.255

192.168.70.0 to 192.168.76.255

Refer to curriculum topic: 9.1.3  
The number of 1s in the wildcard mask represents the number of 0s in the subnet mask.  
The subnet mask in this case is therefore 255.255.254.0. The range of IP addresses for this network would be 192.168.70.0 – 192.168.71.255 with 192.168.71.255 being the broadcast address.

Question 3

0 / 2 pts

Fill in the blanks. Use dotted decimal format.  
The wildcard mask that is associated with 192.168.12.96/27 is .

**Answer 1:**

**0.0.0.31**

Refer to curriculum topic: 9.1.3  
The wildcard mask can be found by subtracting the subnet mask from 255.255.255.255.

Question 4

2 / 2 pts

Fill in the blanks. Use dotted decimal format.  
The wildcard mask that is associated with 152.115.128.0/17 is .

**Answer 1:**

**0.0.127.255**

Refer to curriculum topic: 9.1.3  
The wildcard mask can be found by subtracting the subnet mask from 255.255.255.255.

Question 5

2 / 2 pts

Fill in the blanks. Use dotted decimal format.  
The wildcard mask that is associated with 128.165.216.0/23 is .

**Answer 1:**

**0.0.1.255**

Refer to curriculum topic: 9.1.3  
The wildcard mask can be found by subtracting the subnet mask from 255.255.255.255.

Question 6

2 / 2 pts

What range of IP addresses is represented by the network and wildcard mask 192.168.70.0 0.0.0.127?

**192.168.70.0 to 192.168.70.127**

192.168.70.0 to 192.168.70.255

192.168.70.0 to 192.168.70.63

192.168.70.0 to 192.168.71.255

Refer to curriculum topic: 9.1.3  
The number of 1s in the wildcard mask represents the number of 0s in the subnet mask.  
The range of IP addresses for this network would be 192.168.70.0 – 192.168.70.127 with 192.168.70.127 being the broadcast address.

Question 7

2 / 2 pts

What range of IP addresses is represented by the network and wildcard mask 172.16.32.0 0.0.15.255?

**172.16.32.0 to 172.16.47.255**

172.16.32.0 to 172.16.34.255

172.16.32.0 to 172.16.63.255

172.16.32.0 to 172.16.240.255

Refer to curriculum topic: 9.1.3  
The wildcard mask 0.0.15.255 would filter addresses smilar to the subnet 255.255.240.0, This wildcard mask would therefore represent addresses from the network address range 172.16.32.0/20 – 172.16.47.255,  with 172.16.32.0 being the network address and 172.16.47.255 being the broadcast address.

# Chapter 10 Quiz

Question 1

2 / 2 pts

In which alternative to DHCPv6 does a router dynamically provide IPv6 configuration information to hosts?

ARP

EUI-64

ICMPv6

**SLAAC**

Refer to curriculum topic: 10.2.1  
Stateless Address Autoconfiguration (SLAAC) can be used as an alternative to DHCPv6. In this approach, a router provides global routing prefix, prefix length, default gateway, and DNS server information to a host. The host is not provided with a global unicast address by SLAAC. Instead, SLAAC suggests that the host create its own global unicast address based on the supplied global routing prefix. ARP is not used in IPv6. ICMPv6 messages are used by SLAAC to provide addressing and other configuration information. EUI-64 is a process in which a host will create an Interface ID from its 48-bit MAC address.

Question 2

2 / 2 pts

An administrator has configured a DHCPv4 relay router and issued these commands:  
  
Router(config)# **interface g0/0**  
Router(config-if)# **ip address 10.0.1.1 255.255.255.0**  
Router(config-if)# **no shutdown**  
Router(config-if)# **exit**  
Router(config)# **ip dhcp pool RELAY**  
Router(dhcp-config)# **end**  
  
The clients are not receiving IP parameters from the DHCPv4 server. What is a possible cause?

The pool cannot be named 'RELAY'.

The router is configured as a DHCPv4 client.

The IP address is incorrect for the subnet mask that is used.

**The ip helper-address command is missing.**

Refer to curriculum topic: 10.1.2  
This router should be configured with the **ip helper-address** command, followed with the IP address of the DHCPv4 server, because the router is meant to be used as a relay agent. The **ip dhcp pool RELAY** command just names the DHCPv4 pool, and it does not enable the relay function.

Question 3

2 / 2 pts

Here is a link to the [PT Activity](https://150566673.netacad.com/assessment_questions/22627384/files/16602136/download?verifier=74eqP9ixmQWgaznRH8Mb1ssEN5joflgdYpiu4H9o&wrap=1).

Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.  
  
What is the keyword that is displayed on www.netacad.com?

DHCP

IPv6

Cisco

**Router**

switch

networking

Refer to curriculum topic: 10.2.4  
In order for the host to receive the address of the DNS server, the host must use stateless DHCPv6. The router is configured with the correct DHCPv6 pool, but is missing the command **ipv6 nd other-config-flag** that signals to the host that it should use DHCPv6 to get additional address information. This command should be added to the interface Gigabit0/0 configuration on the router.

Question 4

2 / 2 pts

When a client is requesting an initial address lease from a DHCP server, why is the DHCPREQUEST message sent as a broadcast?

The client does not yet know the IP address of the DHCP server that sent the offer.

The DHCP server may be on a different subnet, so the request must be sent as a broadcast.

The client does not have a MAC address assigned yet, so it cannot send a unicast message at Layer 2.

**The client may have received offers from multiple servers, and the broadcast serves to implicitly decline those other offers.**

Refer to curriculum topic: 10.1.1  
During the initial DHCP exchange between a client and server, the client broadcasts a DHCPDISCOVER message looking for DHCP servers. Multiple servers may be configured to respond to this request with DHCPOFFER messages. The client will choose the lease from one of the servers by sending a DHCPREQUEST message. It sends this message as a broadcast so that the other DHCP servers that sent offers will know that their offers were declined and the corresponding address can go back into the pool.

Question 5

2 / 2 pts

Which command should be configured on a router interface to set the router as a stateful DHCPv6 client?

ipv6 enable

**ipv6 address dhcp**

ipv6 address autoconfigure

ipv6 dhcp server stateful

Refer to curriculum topic: 10.2.3  
When the **ipv6 address dhcp** command is configured on a router interface, it enables the router as a DHCPv6 client on this interface. The **ipv6 enable** command enables IPv6 on an interface and allows the router to configure its link-local address. The **ipv6 address autoconfigure** command tells the router to use either SLAAC or stateless DHCPv6 to configure its global unicast address. The **ipv6 dhcp server** command is used on a router that is running a DHCPv6 server to indicate what address information should be served to clients.

Question 6

2 / 2 pts

After booting, a client receives an ICMPv6 RA message with the M flag set to 0 and the O flag set to 1. What does this indicate?

The client should request an IPv6 address directly from a DHCPv6 server.

The client should automatically configure an IPv6 address without contacting a DHCPv6 server.

**The client should automatically configure an IPv6 address and then contact a DHCPv6 server for more information.**

The client should be statically configured with an IPv6 address because the local router does not support autoconfiguration.

Refer to curriculum topic: 10.2.1  
The Managed Address Configuration (M) flag and the Other Configuration (O) flag in ICMPv6 RA messages are used to indicate to an IPv6 client how it should configure its IPv6 addresses. If the M flag is set to 0 it means that the host should automatically configure its own IPv6 interface address rather than asking for one from a DHCPv6 server. If the O flag is set to 1, it means that the client can find additional addressing information, such as a DNS server address, by contacting a DHCPv6 server after it has automatically configured its own address.

Question 7

2 / 2 pts

Match the DHCP message types to the order of the stateful DHCPv6 process when a client first connects to an IPv6 network. (Not all options are used.)

**Step 1**

**DHCPv6 SOLICIT**

**Step 2**

**DHCPv6 ADVERTISE**

**Step 3**

**DHCPv6 REQUEST**

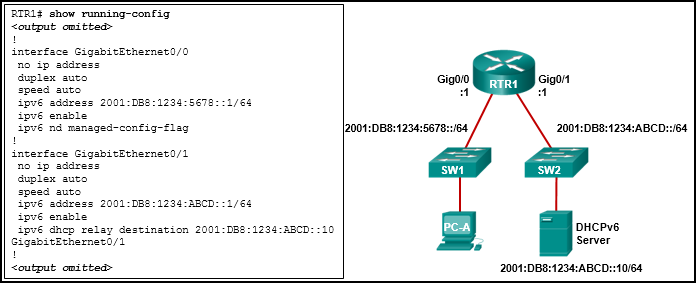
**Step 4**

**DHCPv6 REPLY**

Refer to curriculum topic: 10.2.1  
A stateless DHCPv6 client would send a DHCPv6 INFORMATION-REQUEST message as step 3 in the process.

Question 8

2 / 2 pts



Refer to the exhibit. PC-A is unable to receive an IPv6 address from the stateful DHCPv6 server. What is the problem?

**The ipv6 dhcp relay command should be applied to interface Gig0/0.**

The **ipv6 nd managed-config-flag** should be applied to interface Gig0/1.

The **ipv6 nd managed-config-flag** command should be **ipv6 nd other-config-flag**.

The **ipv6 dhcp relay** command should use the link-local address of the DHCP server.

Refer to curriculum topic: 10.2.4  
The **ipv6 dhcp relay** command must be applied to the interface where the clients are located. The **ipv6 dhcp relay** command can use either the link-local or global unicast address of the DHCPv6 server, or even a multicast address. The **ipv6 nd managed-config-flag** indicates to the clients that they should use stateful DHCPv6 and is also applied to the interface where the clients are located.

Question 9

2 / 2 pts

Which command will allow a network administrator to check the IP address that is assigned to a particular MAC address?

**Router# show ip dhcp binding**

Router# **show ip dhcp pool**

Router# **show ip dhcp server statistics**

Router# **show running-config I section\_dhcp**

Refer to curriculum topic: 10.1.2  
The **show ip dhcp binding** command will show the leases, including IP addresses, MAC addresses, lease expiration, type of lease, client ID, and user name.

Question 10

2 / 2 pts

What is the most likely scenario in which the WAN interface of a router would be configured as a DHCP client to be assigned a dynamic IP address from an ISP?

There is a web server for public access on the LAN that is attached to the router.

The router is also the gateway for a LAN.

**It is a SOHO or home broadband router.**

The router is configured as a DHCP server.

Refer to curriculum topic: 10.1.3  
SOHO and home broadband routers are typically set to acquire an IPv4 address automatically from the ISP. The IP address that is assigned is typically a dynamic address to reduce the cost, but a static IP address is possible with more cost. However, if the router is assigned a dynamic IP address, DNS issues will result in the web server behind the router not being easily accessible to the public. Routers are typically also gateways for LANs, but this has no bearing on whether the router is configured as a DHCP client on its WAN link or not. Likewise, a router can be configured to be a DHCP client in order to obtain an IP address from the ISP, but at the same time, it can be configured as a DHCP server to serve the IP addressing for the devices on its LAN.

Question 11

2 / 2 pts

Match the DHCP message types to the order of the DHCPv4 process. (Not all options are used.)

**Step 1**

**DHCPDISCOVER**

**Step 2**

**DHCPOFFER**

**Step 3**

**DHCPREQUEST**

**Step 4**

**DHCPACK**

Refer to curriculum topic: 10.1.1  
The broadcast DHCPDISCOVER message finds DHCPv4 servers on the network. When the DHCPv4 server receives a DHCPDISCOVER message, it reserves an available IPv4 address to lease to the client and sends the unicast DHCPOFFER message to the requesting client. When the client receives the DHCPOFFER from the server, it sends back a DHCPREQUEST. On receiving the DHCPREQUEST message the server replies with a unicast DHCPACK message. DHCPREPLY and DHCPINFORMATION-REQUEST are DHCPv6 messages.

Question 12

2 / 2 pts

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

DHCPACK

DHCPDISCOVER

DHCPOFFER

**DHCPREQUEST**

Refer to curriculum topic: 10.1.1  
When the client receives the DHCPOFFER from the server, it sends back a DHCPREQUEST broadcast message. On receiving the DHCPREQUEST message, the server replies with a unicast DHCPACK message.

Question 13

2 / 2 pts

Fill in the blank. Do not abbreviate.  
An administrator is troubleshooting a DHCPv4 issue on a router. By issuing the **debug ip** **dhcp** command, the administrator can watch, in real time, the IP address assignments that are performed by the router.

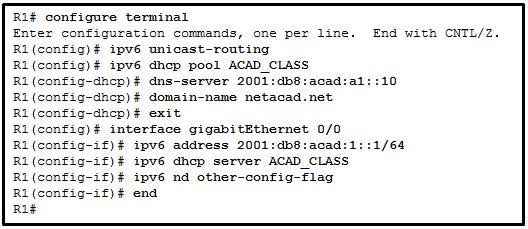
**Answer 1:**

**server event**

Refer to curriculum topic: 10.1.4  
The **debug ip dhcp server events** command reports IP address assignments and database updates as they happen.

Question 14

2 / 2 pts



Refer to the exhibit. A network administrator is configuring a router for DHCPv6 operation. Which conclusion can be drawn based on the commands?

The DHCPv6 server name is ACAD\_CLASS.

**The router is configured for stateless DHCPv6 operation.**

Clients would configure the interface IDs above 0010.

The router is configured for stateful DHCPv6 operation, but the DHCP pool configuration is incomplete.

Refer to curriculum topic: 10.2.2  
The DHCPv6 is for the stateless DHCPv6 operation that is indicated by changing the O flag to 1 and leaving the M flag as default, which is 0. Therefore, it is not configured for stateful DHCPv6 operation. Although the DNS server has the interface ID 0010, clients in stateless DHCPv6 operation will configure their interface IDs either by EUI-64 or a random number. The ACAD\_CLASS is the name of the DHCP pool, not the DHCP server name.

# Chapter 11 Quiz

Question 1

2 / 2 pts



Refer to the exhibit. Router R1 is configured for PAT. What is a possible reason that the addresses in the network are not translated?

**Access-list 1 is misconfigured.**

NAT-POOL2 has not been bound to the ACL.

Interface Fa0/1 should be identified as the outside NAT interface.

Interface S0/0/0 should be identified as the inside NAT interface.

Refer to curriculum topic: 11.2.3  
The wildcard mask in the access control entry does not allow traffic from both the 192.168.11.0/24 and the 192.168.12.0/24 networks. The correct configuration command is R1(config)# **access-list 1 permit 192.168.0.0 0.0.255.255**.

Question 2

2 / 2 pts

A company designs its network so that the PCs in the internal network are assigned IP addresses from DHCP servers, and the packets that are sent to the Internet are translated through a NAT-enabled router. What type of NAT enables the router to populate the translation table from a pool of unique public addresses, as the PCs send packets through the router to the Internet?

static NAT

**dynamic NAT**

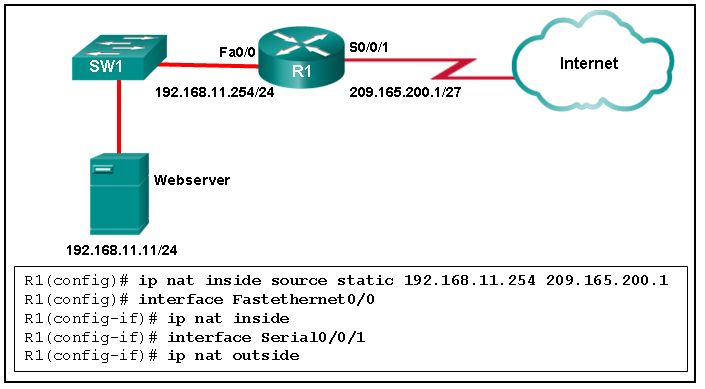
PAT

ARP

Refer to curriculum topic: 11.1.2  
ARP is the address resolution protocol and is used to obtain the MAC address of the destination device. Static NAT is a one-to-one mapping between the local and global addresses of a device. PAT, otherwise known as NAT overload, maps multiple private IP addresses to a singular public address or group of addresses. Dynamic NAT uses a pool of public IP addresses and assigns them to requesting devices on a first-come, first-served basis. In the case of dynamic NAT, each device would have a unique public IP address from the pool of public IP addresses as the source IP address in the packets that they send.

Question 3

2 / 2 pts



Refer to the exhibit. Router R1 is configured with static NAT. Addressing on the router and the web server are correctly configured, but there is no connectivity between the web server and users on the Internet. What is a possible reason for this lack of connectivity?

Interface Fa0/0 should be configured with the command **ip nat outside**.

The NAT configuration on interface S0/0/1 is incorrect.

The inside global address is incorrect.

**The router NAT configuration has an incorrect inside local address.**

Refer to curriculum topic: 11.2.1  
The correct syntax would be R1(config)# **ip nat inside source static 192.168.11.11 209.165.200.1**. (The inside local address is 192.168.11 and the inside global address is 209.165.200.1.)

Question 4

2 / 2 pts

What are two benefits of NAT? (Choose two.)

**It saves public IP addresses.**

**It adds a degree of privacy and security to a network.**

It increases routing performance.

It makes troubleshooting routing issues easier.

It makes tunneling with IPsec less complicated.

Refer to curriculum topic: 11.1.3

Question 5

2 / 2 pts

Which method is used by a PAT-enabled router to send incoming packets to the correct inside hosts?​

**It uses the destination TCP or UDP port number on the incoming packet.**

It uses the source TCP or UDP port number on the incoming packet.

It uses the source IP address on the incoming packet.

It uses a combination of the source TCP or UDP port number and the destination IP address on the incoming packet.

Refer to curriculum topic: 11.1.2  
A PAT-enabled router maintains a table that consists of a mapping of inside local IP addresses and TCP/UDP port numbers to outside local addresses and TCP/UDP port numbers. When traffic returns to the router from the public network, the router would compare the destination port to the PAT mapping table to determine to which inside host the traffic should be sent.

Question 6

2 / 2 pts

When configuring NAT on a Cisco router, what is the inside local IP address?

the IP address of an inside host as it appears to the outside network

the IP address of an outside host as it appears to the inside network

**the IP address of an inside host as it appears to the inside network**

the configured IP address assigned to a host in the outside network

Refer to curriculum topic: 11.1.1

Question 7

2 / 2 pts

A network administrator configures the border router with the command R1(config)# **ip nat inside source list 4 pool corp**. Which ACL is required to be configured in order for this command to function?

an access list named corp that defines the starting and ending public IP addresses

an access list named corp that defines the private addresses that are affected by NAT

an access list that is numbered 4 that defines the starting and ending public IP addresses

**an access list that is numbered 4 that defines the private addresses that are affected by NAT**

Refer to curriculum topic: 11.2.2  
In order for the **ip nat inside source list 4 pool corp** command to work, the following procedure needs to be used:

* Create an access list that defines the private IP addresses affected by NAT.
* Establish a NAT pool of starting and ending public IP addresses using the **ip nat pool** command.
* Use the **ip nat inside source list** command to associate the access list with the NAT pool.
* Apply NAT to internal and external interfaces by using the **ip nat inside** and **ip nat outside** commands.

Question 8

2 / 2 pts

What is correct in relation to NAT for IPv6?

It is used to convert private IPv6 addresses to public IPv6 addresses.​

**It is a temporary mechanism to assist in the migration from IPv4 to IPv6.**

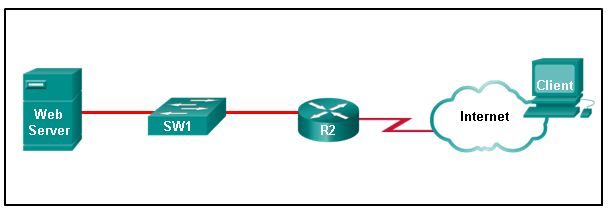
NAT64 has been deprecated by IETF in favor of NAT-PT.

Dual stack is an example of implementation of NAT for IPv6.

Refer to curriculum topic: 11.2.5  
NAT for IPv6 is a temporary measure to aid in the move from IPv4 to IPv6. NAT64 is replacing NAT-PT. Dual stack is a  method for running IPv4 and IPv6 on the same network.

Question 9

2 / 2 pts



Refer to the exhibit. Router R2 is configured with static NAT. Place in order the steps that occur when the client accesses the web server through the router. (Not all options are used.)

**Step 1**

**The client uses the inside global address of the web server as the destination address to send a packet to the web server.**

**Step 2**

**R2 receives the packet on its outside interface, then checks and locates the destination address in its NAT table.**

**Step 3**

**R2 replaces the inside global address with the inside local address of the web server and forwards the packet to the web server.**

**Step 4**

**The web server uses the outside global address of the client as the destination address when responding.**

**Step 5**

**R2 receives the packet from the web server. R2 checks the NAT table, then translates the source address of the web server into an inside global address and forwards the packet.**

Refer to curriculum topic: 11.2.1  
Static NAT translations are usually used when clients on the outside network (Internet) need to reach servers on the inside (internal) network. The process begins with the client trying to communicate with the web server by the use of the inside global address of the web server as the destination address. The router receives this on its outside interface, consults its NAT table, locates the destination address, and forwards the packet to the web server on the internal network via its inside local address. The web server response goes to the router, which replaces the web server inside local address with the global address (NAT table) and forwards the packet to the client on its external interface.

Question 10

2 / 2 pts

What is the purpose of entering the command **ip nat inside source static tcp 192.168.10.2 80 209.165.200.223 8080** at the global configuration prompt?

It identifies the inside NAT interface on the router.

It prevents the router from establishing a connection with any device that does not have the specified address and port number.

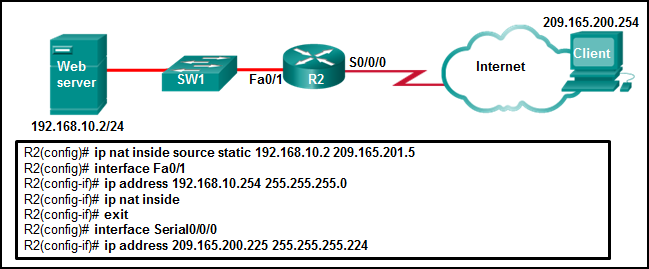
**It binds the inside local address and local port to the specified inside global address and global port.**

It enables a one to one translation between different internal port numbers.

Refer to curriculum topic: 11.2.4  
The displayed command establishes static translation between an inside local address and local port and an inside global address and global port. In order to identify the inside NAT interface, the command Router(config-if)**# ip nat inside** would have to be entered on the respective interface.

Question 11

2 / 2 pts



Refer to the exhibit. A technician is configuring R2 for static NAT to allow the client to access the web server. What is a possible reason that the client PC cannot access the web server?

**Interface S0/0/0 should be identified as the outside NAT interface.**

Interface Fa0/1 should be identified as the outside NAT interface.

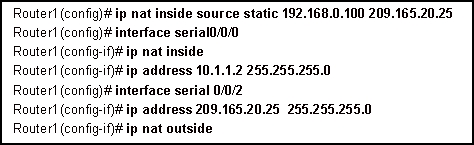
The IP NAT statement is incorrect.

The configuration is missing a valid access control list.

Refer to curriculum topic: 11.2.1  
Interface S0/0/0 should be identified as the outside NAT interface. The command to do this would be R2(config-if)# **ip nat outside**.

Question 12

2 / 2 pts



Refer to the exhibit. Which address or addresses represent the inside global address?

10.1.1.2

192.168.0.100

**209.165.20.25**

any address in the 10.1.1.0 network

Refer to curriculum topic: 11.2.1

Question 13

2 / 2 pts

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

7

**8**

9

10

24

31

Refer to curriculum topic: 11.2.2

Question 14

2 / 2 pts

What is true regarding the differences between NAT and PAT?

PAT uses the word "overload" at the end of the access-list statement to share a single registered address.

Static NAT allows an unregistered address to map to multiple registered addresses.

Dynamic NAT allows hosts to receive the same global address each time external access is required.

**PAT uses unique source port numbers to distinguish between translations.**

Refer to curriculum topic: 11.1.2

Question 15

2 / 2 pts

A network administrator wants to examine the active NAT translations on a border router. Which command would perform the task?

**Router# show ip nat translations**

Router# show ip nat statistics

Router# clear ip nat translations

Router# debug ip nat translations

Refer to curriculum topic: 11.3.1  
The **clear** **ip nat translations** command clears all dynamic address translation entries from the NAT translation table. The **debug ip nat** command is used to verify the operation of NAT. The **show ip nat statistics** command displays information about the total number of active translations, NAT configuration parameters, the number of addresses in the pool, and the number that have been allocated. The **show ip nat translations** command displays the active NAT translations.