



## NWC204-Truyền-Kỳ - Imao

Networking (Trường Đại học FPT)



Scan to open on Studocu

## Contents

I. MODULE 1-3 .....	1
II. MODULE 4-7 .....	28
III. MODULE 8-10 .....	51
IV. MODULE 11-13 .....	80
V. MODULE 14-15 .....	103
VI. MODULE 16-17 .....	121
VII. FINAL EXAM (INTRODUCTION TO NETWORKS) .....	145

## I. MODULE 1-3

1. During a routine inspection, a technician discovered that software that was installed on a computer was secretly collecting data about websites that were visited by users of the computer. Which type of threat is affecting this computer?

- DoS attack
- identity theft
- **spyware**
- zero-day attack

2. Which term refers to a network that provides secure access to the corporate offices by suppliers, customers and collaborators?

- Internet
- intranet
- **extranet**
- extendednet

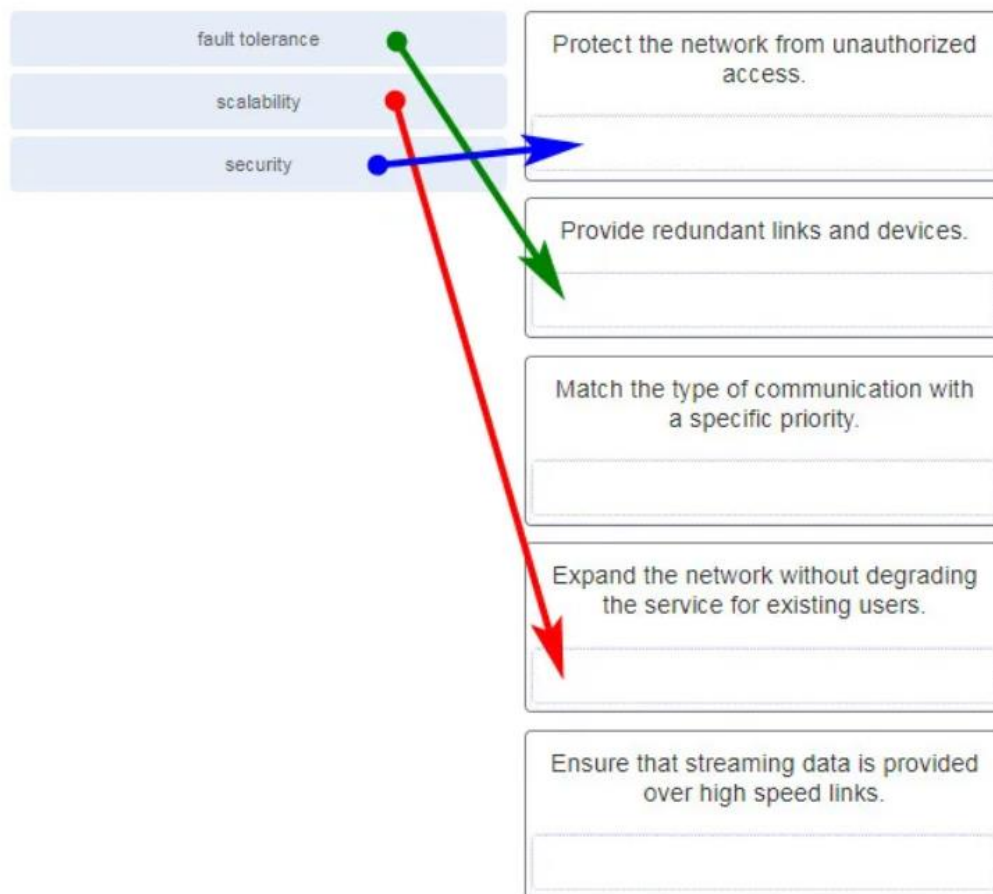
3. A large corporation has modified its network to allow users to access network resources from their personal laptops and smart phones. Which networking trend does this describe?

- cloud computing
- online collaboration
- **bring your own device**
- video conferencing

4. What is an ISP?

- It is a standards body that develops cabling and wiring standards for networking.
- It is a protocol that establishes how computers within a local network communicate.
- **It is an organization that enables individuals and businesses to connect to the Internet.**
- It is a networking device that combines the functionality of several different networking devices in one.

**5. Match the requirements of a reliable network with the supporting network architecture. (Not all options are used.)**



**6. 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

**Explanation:** 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.

### 7. 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.~~

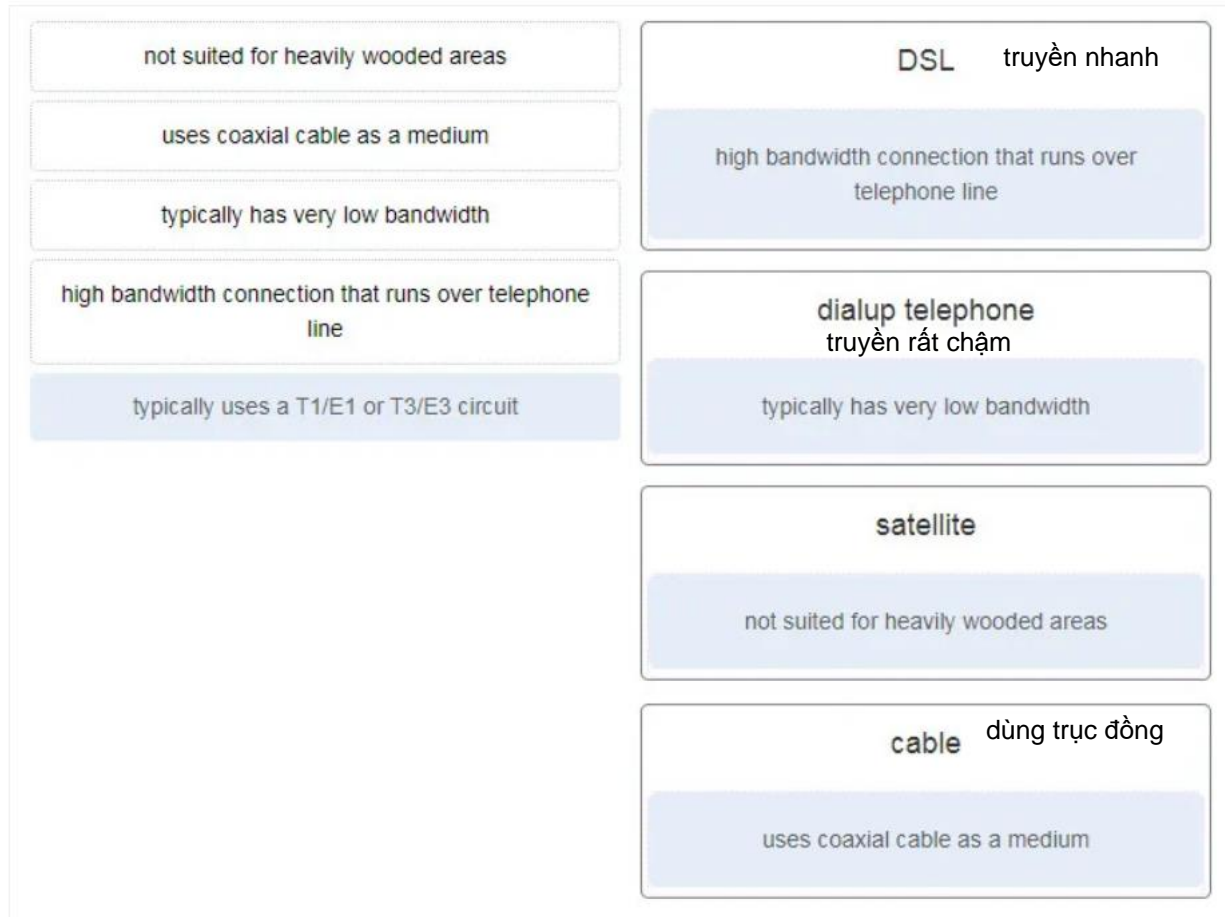
**Explanation:** Powerline networking adds the ability to connect a device to the network using an adapter wherever there is an electrical outlet. The network uses existing electrical wiring to send data. It is not a replacement for physical cabling, but it can add functionality in places where wireless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

### 8. A networking technician is working on the wireless network at a medical clinic. The technician accidentally sets up the wireless network so that patients can see the medical records data of other patients. Which of the four network characteristics has been violated in this situation?

- fault tolerance
- scalability
- **security**
- Quality of Service (QoS)
- reliability

**Explanation:** Network security includes protecting the confidentiality of data that is on the network. In this case, because confidential data has been made available to unauthorized users, the security characteristic of the network has failed.

### 9. Match each characteristic to its corresponding Internet connectivity type. (Not all options are used.)



## ITN (Version 7.00) – Basic Network Connectivity and Communications Exam 5

**Explanation:** 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.

### 10. What two criteria are used to help select a network medium from various network media? (Choose two.)    môi trường, khoảng cách truyền

- 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 intermediate devices installed in the network
- **the environment where the selected medium is to be installed**

**Explanation:** 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.

**11. What type of network traffic requires QoS?** quality of service

- email voice, video
- on-line purchasing
- **video conferencing**
- wiki

**12. 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

**Explanation:** 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.

**13. 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** vty 0 15, line console 0, privilege
- **console interface**
- Ethernet interface
- boot IOS mode
- **privileged EXEC mode**
- router configuration mode

**Explanation:** Access to the VTY and console interfaces can be restricted using passwords. Out-of-band management of the router can be restricted in both user EXEC and privileged EXEC modes.

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

virtual interface

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

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

**15. What function does pressing the Tab key have when entering a command in IOS?**

- It aborts the current command and returns to configuration mode.
- It exits configuration mode and returns to user EXEC mode.
- It moves the cursor to the beginning of the next line.
- **It completes the remainder of a partially typed word in a command.**

**Explanation:** Pressing the Tab key after a command has been partially typed will cause the IOS to complete the rest of the command.

**16. 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?** reload

- **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.

**Explanation:** 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.

**17. An administrator uses the Ctrl-Shift-6 key combination on a switch after issuing the ping command. What is the purpose of using these keystrokes?** stop ping

- to restart the ping process
- **to interrupt the ping process**
- to exit to a different configuration mode
- to allow the user to complete the command

**Explanation:** To interrupt an IOS process such as ping or traceroute, a user enters the Ctrl-Shift-6 key combination. Tab completes the remainder of parameters or arguments within a command. To exit from configuration mode to privileged mode use the Ctrl-Z

keystroke. CTRL-R will redisplay the line just typed, thus making it easier for the user to press Enter and reissue the ping command.

**18. Refer to the exhibit. A network administrator is configuring access control to switch SW1. If the administrator uses a console connection to connect to the switch, which password is needed to access user EXEC mode?**

```
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# enable password letmein
SW1(config)# enable secret secretin
SW1(config)# line console 0
SW1(config-line)# password lineconin
SW1(config-line)# login
SW1(config-line)# exit
SW1(config)# line vty 0 15
SW1(config-line)# password linevtyin
SW1(config-line)# login
SW1(config-line)# end
SW1#
```

CCNA-1-v7-Modules-1-3-Basic Network Connectivity and Communications Exam  
Answers 14 telnet : vty

- letmein
- secretin
- **lineconin**
- linevtyin

**Explanation:** Telnet accesses a network device through the virtual interface configured with the line VTY command. The password configured under this is required to access the user EXEC mode. The password configured under the line console 0 command is required to gain entry through the console port, and the enable and enable secret passwords are used to allow entry into the privileged EXEC mode.

**19. A technician configures a switch with these commands:**

```
SwitchA(config)# interface vlan 1
SwitchA(config-if)# ip address 192.168.1.1 255.255.255.0
SwitchA(config-if)# no shutdown
```

**What is the technician configuring?** switch virtual interface



- Telnet access
- **SVI**
- password encryption
- physical switchport access

**Explanation:** For a switch to have an IP address, a switch virtual interface must be configured. This allows the switch to be managed remotely over the network.

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

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

**Explanation:** 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.

**21. 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.** -> volatile
- RAM is a component in Cisco switches but not in Cisco routers.
- RAM is able to store multiple versions of IOS and configuration files.

**Explanation:** 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.

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

- ~~Branch2!~~
- **RM-3-Switch-2A4**      contain no space
- ~~Floor(15)~~      use letter, digit and dashes
- ~~HO Floor 17~~      start with letter
- **SwBranch799**

**Explanation:** Some guidelines for naming conventions are that names should:  
Start with a letter  
Contain no spaces

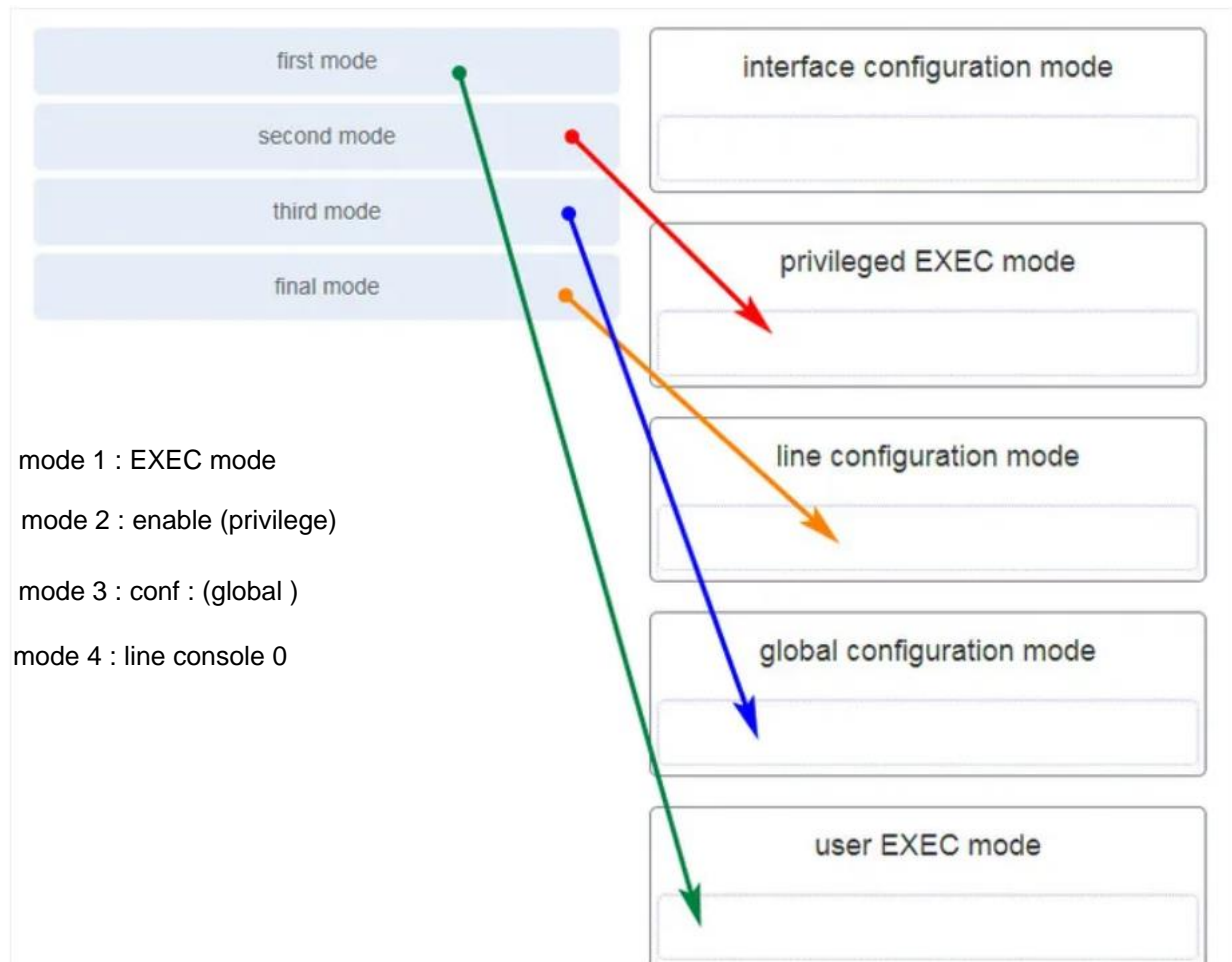
End with a letter or digit  
Use only letters, digits, and dashes  
Be less than 64 characters in length

### 23. How is SSH different from Telnet?

- SSH makes connections over the network, whereas Telnet is for out-of-band access.
- **SSH provides security to remote sessions by encrypting messages and using user authentication. Telnet is considered insecure and sends messages in plaintext.**
- SSH requires the use of the PuTTY terminal emulation program. Tera Term must be used to connect to devices through the use of Telnet.
- SSH must be configured over an active network connection, whereas Telnet is used to connect to a device from a console connection.

**Explanation:** SSH is the preferred protocol for connecting to a device operating system over the network because it is **much more secure than Telnet**. Both SSH and Telnet are used to connect to devices over the network, and so are both used in-band. PuTTY and Terra Term can be used to make both SSH and Telnet connections.

**24. 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.)**



## CCNA-1-v7-Modules-1-3-Basic Network Connectivity and Communications Exam Answers 24

**Explanation:** 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.

### 25. What are three characteristics of an SVI? (Choose three.)

no physical interface, remotely manage, vlan1

- It is designed as a security protocol to protect switch ports.
- **It is not associated with any physical interface on a switch.**
- It is a special interface that allows connectivity by different types of media.
- It is required to allow connectivity by any device at any location.
- **It provides a means to remotely manage a switch.**

- **It is associated with VLAN1 by default.**

**Explanation:** Switches have one or more switch virtual interfaces (SVIs). SVIs are created in software since there is no physical hardware associated with them. Virtual interfaces provide a means to remotely manage a switch over a network that is using IP. Each switch comes with one SVI appearing in the default configuration “out-of-the-box.” The default SVI interface is VLAN1.

**26. What command is used to verify the condition of the switch interfaces, including the status of the interfaces and a configured IP address?**

- ipconfig
- ping
- traceroute
- **show ip interface brief**

**Explanation:** The show ip interface brief command is used to display a brief synopsis of the condition of the device interfaces. The ipconfig command is used to verify TCP/IP properties on a host. The ping command is used to verify Layer 3 connectivity. The traceroute command is used to trace the network path from source to destination.

27. Match the description with the associated IOS mode. (Not all options are used.)

3 changes made affect the operation of the device as a whole

2 accessed by entering the **enable** command

2 identified by a prompt ending with the # character

1 limited number of basic monitoring commands

3 accessed by entering the **configure terminal** command

1 the first entrance into the CLI of an IOS device

used to enable the password for vty lines

user EXEC mode

limited number of basic monitoring commands

the first entrance into the CLI of an IOS device

privileged EXEC mode

accessed by entering the **enable** command

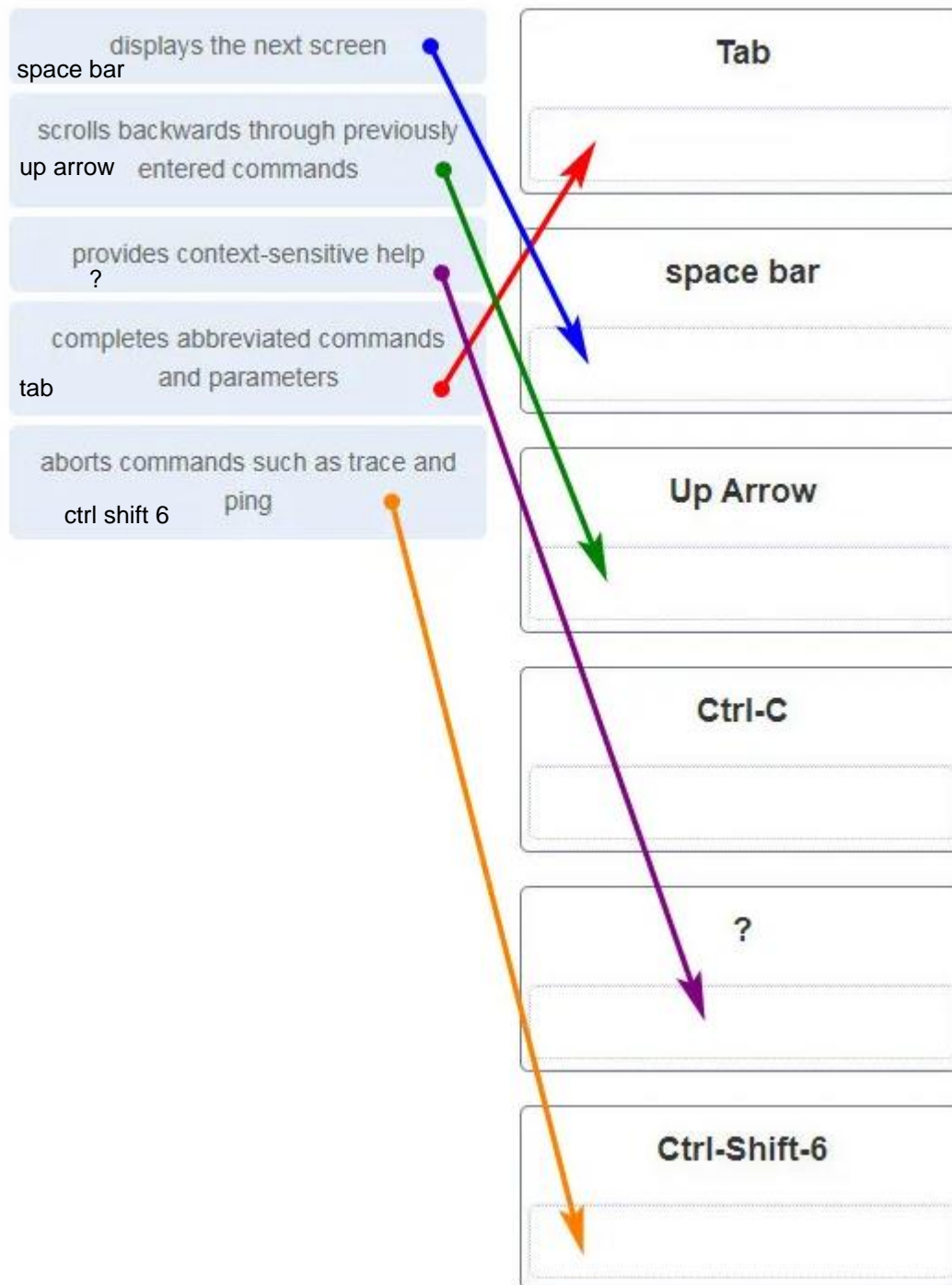
identified by a prompt ending with the # character

global configuration mode

changes made affect the operation of the device as a whole

accessed by entering the **configure terminal** command

28. Match the definitions to their respective CLI hot keys and shortcuts. (Not all options are used.)



**Explanation:** 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

**29. In the show running-config command, which part of the syntax is represented by running-config ?**

- the command
- **a keyword**
- a variable
- a prompt

keyword

**Explanation:** The first part of the syntax, show, is the command, and the second part of the syntax, running-config, is the keyword. The keyword specifies what should be displayed as the output of the show command.

**30. After making configuration changes on a Cisco switch, a network administrator issues a copy running-config startup-config command. What is the result of issuing this command?**

- The new configuration will be stored in flash memory.
- **The new configuration will be loaded if the switch is restarted.**
- The current IOS file will be replaced with the newly configured file.
- The configuration changes will be removed and the original configuration will be restored.

**Explanation:** With the copy running-config startup-config command, the content of the current operating configuration replaces the startup configuration file stored in NVRAM. The configuration file saved in NVRAM will be loaded when the device is restarted.

**31. What command will prevent all unencrypted passwords from displaying in plain text in a configuration file?**

- (config)# enable password secret
- (config)# enable secret Secret\_Password
- (config-line)# password secret
- **(config)# service password-encryption**
- (config)# enable secret Encrypted\_Password

ser. - -

**Explanation:** To prevent all configured passwords from appearing in plain text in configuration files, an administrator can execute the service password-encryption command. This command encrypts all configured passwords in the configuration file.

**32. A network administrator enters the service password-encryption command into the configuration mode of a router. What does this command accomplish?**

- This command encrypts passwords as they are transmitted across serial WAN links.
- **This command prevents someone from viewing the running configuration passwords.**
- This command enables a strong encryption algorithm for the enable secret password command.
- This command automatically encrypts passwords in configuration files that are currently stored in NVRAM.
- This command provides an exclusive encrypted password for external service personnel who are required to do router maintenance.

**Explanation:** The startup-config and running-config files display most passwords in plaintext. Use the service password-encryption global config command to **encrypt all plaintext passwords in these files.**

**33. 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

**Explanation:** 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.

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

- 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.

**Explanation:** When the data is traveling from the PC to the network, the transport layer sends segments to the internet layer. The internet layer sends packets to the network



access layer, which creates frames and then converts the frames to bits. The bits are released to the network media.

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

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

**Explanation:** 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.



**Explanation:** 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.

### 37. Which name is assigned to the transport layer PDU?

- bits
- data
- frame
- packet
- **segment**

**Explanation:** Application data is passed down the protocol stack on its way to be transmitted across the network media. During the process, various protocols add information to it at each level. At each stage of the process, a PDU (protocol data unit) has a different name to reflect its new functions. The PDUs are named according to the protocols of the TCP/IP suite:

Data – The general term for the PDU used at the application layer.

Segment – transport layer PDU

Packet – network layer PDU

Frame – data link layer PDU

Bits – A physical layer PDU used when physically transmitting data over the medium

**38. When IPv4 addressing is manually configured on a web server, which property of the IPv4 configuration identifies the network and host portion for an IPv4 address?**

- DNS server address
- **subnet mask** host portion
- default gateway
- DHCP server address not manual

**Explanation:** There are several components that need to be entered when configuring IPv4 for an end device:

IPv4 address – uniquely identifies an end device on the network

Subnet mask – determines the network address portion and host portion for an IPv4 address

Default gateway – the IP address of the router interface used for communicating with hosts in another network

DNS server address – the IP address of the Domain Name System (DNS) server

DHCP server address (if DHCP is used) is not configured manually on end devices. It will be provided by a DHCP server when an end device requests an IP address.

**39. What process involves placing one PDU inside of another PDU?**

- **encapsulation**
- encoding
- segmentation
- flow control

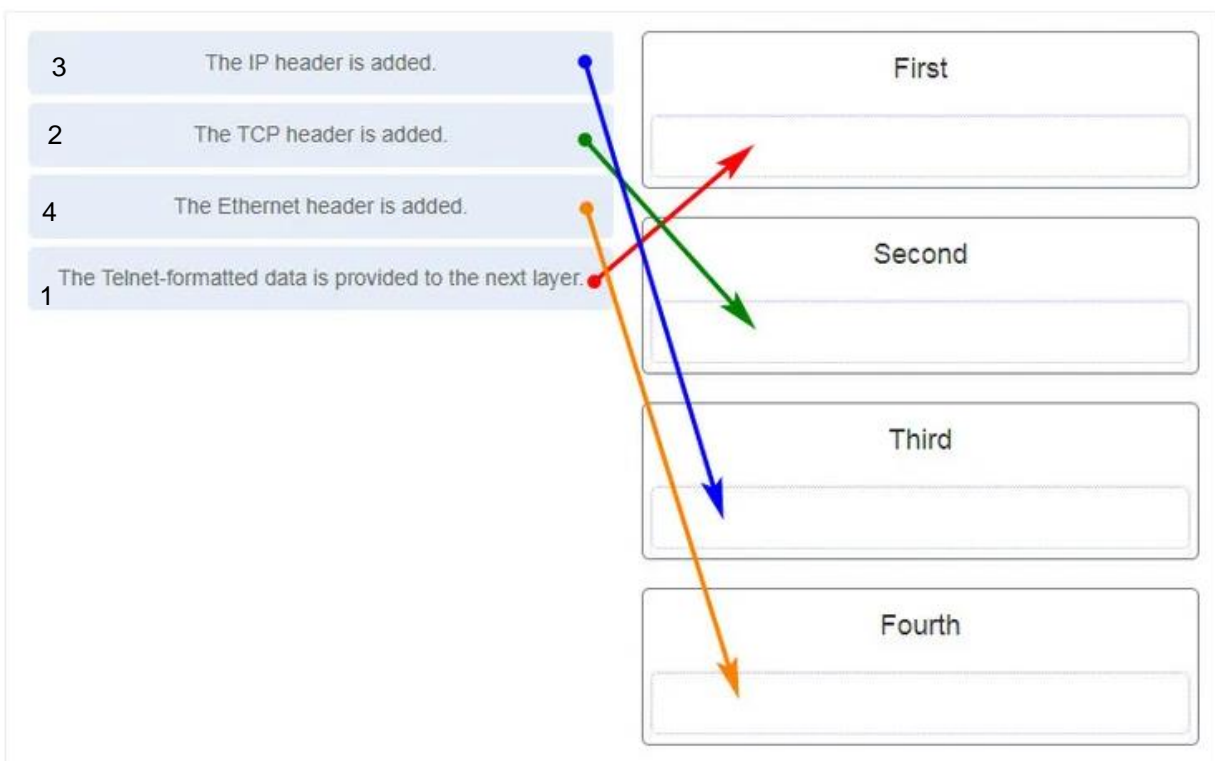
**Explanation:** When a message is placed inside of another message, this is known as encapsulation. On networks, encapsulation takes place when one protocol data unit is carried inside of the data field of the next lower protocol data unit.

40. What layer is responsible for routing messages through an internetwork in the TCP/IP model?

- **internet**
- transport
- network access
- session osi layer

**Explanation:** The TCP/IP model consists of four layers: application, transport, internet, and network access. Of these four layers, it is the internet layer that is responsible for routing messages. The session layer is not part of the TCP/IP model but is rather part of the OSI model.

41. For the TCP/IP protocol suite, what is the correct order of events when a Telnet message is being prepared to be sent over the network?



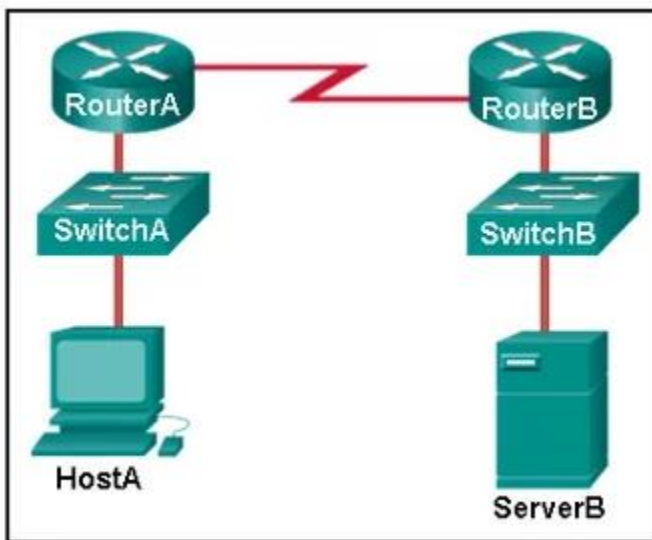
CCNA-1-v7-Modules-1-3-Basic Network Connectivity and Communications Exam  
Answers 41

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

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

**Explanation:** 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.

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



packet to destination device

frame contains MAC address of the router

- ~~ServerB will generate a packet with the destination IP address of RouterB.~~
- ServerB will generate a frame with the destination MAC address of SwitchB.
- ~~ServerB will generate a packet with the destination IP address of RouterA.~~
- **ServerB will generate a frame with the destination MAC address of RouterB.**
- **ServerB will generate a packet with the destination IP address of HostA.**
- ServerB will generate a frame with the destination MAC address of RouterA.

**Explanation:** In order to send data to HostA, ServerB 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.

**44. Which method allows a computer to react accordingly when it requests data from a server and the server takes too long to respond?**

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

**Explanation:** If a computer makes a request and does not hear a response within an acceptable amount of time, the computer assumes that no answer is coming and reacts accordingly.

**45. A web client is receiving a response for a web page from a web server. From the perspective of the client, what is the correct order of the protocol stack that is used to decode the received transmission?**

IP trước TCP

- **Ethernet, IP, TCP, HTTP**
- HTTP, TCP, IP, Ethernet
- Ethernet, TCP, IP, HTTP
- HTTP, Ethernet, IP, TCP

**Explanation:**

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.

**46. Which two OSI model layers have the same functionality as a single layer of the TCP/IP model? (Choose two.)**

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

**Explanation:** The OSI data link and physical layers together are equivalent to the TCP/IP network access layer. The OSI transport layer is functionally equivalent to the TCP/IP transport layer, and the OSI network layer is equivalent to the TCP/IP internet layer. The OSI application, presentation, and session layers are functionally equivalent to the application layer within the TCP/IP model.

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

- physical layer

- data link layer
- **network layer**
- transport layer

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

#### 48. What is a characteristic of multicast messages?

- **They are sent to a select group of hosts.**
- They are sent to all hosts on a network. broadcast
- They must be acknowledged.
- They are sent to a single destination. unicast

**Explanation:** Multicast is a one-to-many type of communication. Multicast messages are addressed to a specific multicast group.

#### 49. Which statement is correct about network protocols?

exchange message between host and destination

- 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.

**Explanation:** 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.

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

different OS can communicate

- 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.

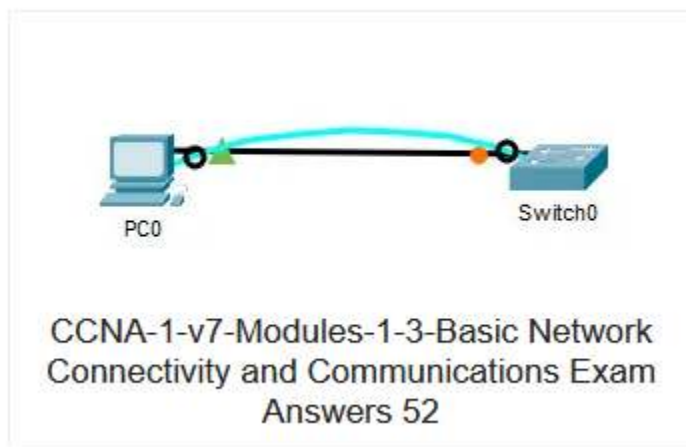
**Explanation:** An advantage of network devices implementing open standard protocols, such as from the TCP/IP suite, is that clients and servers running different operating systems can communicate with each other. Open standard protocols facilitate innovation and competition between vendors and across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

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

- **a router** path of message
- a firewall protect
- a web server
- a DSL modem provide Internet connection

**Explanation:** 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.

**52. Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.**



CCNA-1-v7-Modules-1-3-Basic Network Connectivity and Communications Exam Answers 52

**What is the IP address of the switch virtual interface (SVI) on Switch0?**

- **192.168.5.10**
- 192.168.10.5
- 192.168.10.1
- 192.168.5.0



**Explanation:** After the enable command is issued, the show running-configuration command or the show ip interfaces brief command will display the IP address of the switch virtual interface (SVI).

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

manage remotely

- 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

**Explanation:** 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.

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

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

must enable

CCNA-1-v7-Modules-1-3-Basic Network Connectivity and Communications Exam  
Answers 54

- The entire command, configure terminal, must be used.
- The administrator is already in global configuration mode.
- **The administrator must first enter privileged EXEC mode before issuing the command.**
- The administrator must connect via the console port to access global configuration mode.

**Explanation:** In order to enter global configuration mode, the command configure terminal, or a shortened version such as config t, must be entered from privileged EXEC mode. In this scenario the administrator is in user EXEC mode, as indicated by the > symbol after the hostname. The administrator would need to use the enable command to move into privileged EXEC mode before entering the configure terminal command.

**55. What term describes a network owned by one organization that provides safe and secure access to individuals who work for a different organization?**

outside -> extranet

- **extranet**
- cloud
- BYOD
- quality of service

**56. What term describes storing personal files on servers over the internet to provide access anywhere, anytime, and on any device?**

- **cloud**
- BYOD
- quality of service
- converged network

**57. What term describes a network where one computer can be both client and server?**

- **peer-to-peer**
- cloud
- BYOD
- quality of service

**58. What term describes a type of network used by people who work from home or from a small remote office?**

- **SOHO network** Small Office Home Office
- BYOD
- quality of service
- converged network

**59. What term describes a computing model where server software runs on dedicated computers?**

- **client/server**
- internet
- intranet
- extranet

**61. What term describes a technology that allows devices to connect to the LAN using an electrical outlet?**

- **powerline networking**
- internet
- intranet
- extranet

62. What term describes a policy that allows network devices to manage the flow of data to give priority to voice and video?

Qos

- **quality of service**
- internet
- intranet
- extranet

63. What term describes a private collection of LANs and WANs that belongs to an organization?

organization, private -> intranet

- **intranet**
- internet
- extranet
- peer-to-peer

64. What term describes the ability to use personal devices across a business or campus network?

bring ur own device

- **BYOD**
- internet
- intranet
- extranet

65. At which OSI layer is a **source IP address** added to a PDU during the encapsulation process?

- **network layer**
- data link layer
- transport layer
- application layer

66. At which OSI layer is a destination port number added to a PDU during the encapsulation process?

- **transport layer** TCP, UDP
- data link layer
- network layer
- application layer

67. At which OSI layer is **data** added to a PDU during the encapsulation process?

- **application layer** layer 1

- data link layer
- network layer
- transport layer

68. At which OSI layer is a **source IP address** added to a PDU during the encapsulation process?

- **network layer**
- data link layer
- application layer
- presentation layer

69. Which of the following is the name for all computers connected to a network that participate directly in network communication?

- Servers
- Intermediary device
- **Host media**

70. At which OSI layer is a **destination IP address** added to a PDU during the encapsulation process?

network layer : ip address

- **network layer**
- application layer
- transport layer
- presentation layer

71. At which OSI layer is a **source MAC address** added to a PDU during the encapsulation process?

data link: MAC address

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

72. At which OSI layer is a **source port number** added to a PDU during the encapsulation process?

- **transport layer**
- application layer
- network layer
- presentation layer
- data link layer

73. At which OSI layer is a **destination MAC** address added to a PDU during the encapsulation process?

- **data link layer**
- transport layer
- application layer
- network layer

74. When data is encoded as **pulses of light**, which media is being used to transmit the data?

- Wireless                      cáp quang
- **Fire optic cable**
- Copper cable

75. Which two devices are intermediary devices? (Choose two)

- Host
- **Router**
- **Switch**
- Servers

## II. MODULE 4-7

1. What is the purpose of the OSI physical layer?

- controlling access to media
- **transmitting bits across the local media**
- performing error detection on received frames
- exchanging frames between nodes over physical network media

2. 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.**

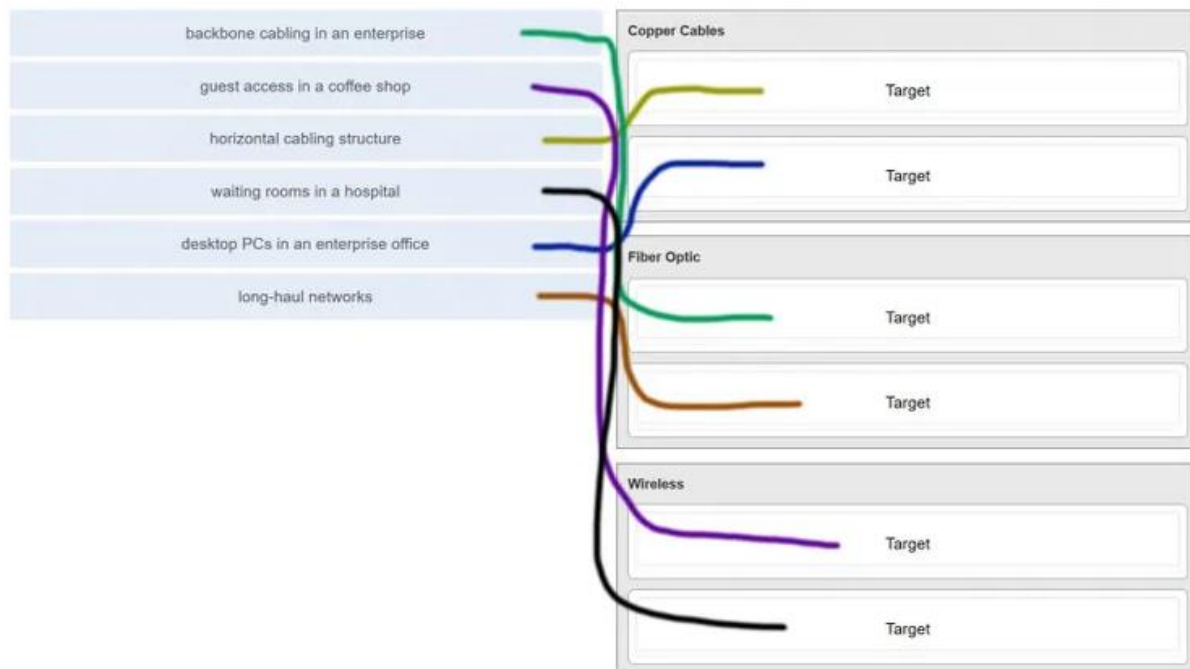
3. Which characteristic describes crosstalk?

- 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

#### 4. Which procedure is used to reduce the effect of crosstalk in copper cables?

- requiring proper grounding connections
- **twisting opposing circuit wire pairs together**
- wrapping the bundle of wires with metallic shielding
- designing a cable infrastructure to avoid crosstalk interference
- avoiding sharp bends during installation

#### 5. Match the situation with the appropriate use of network media.



#### 6. A network administrator is measuring the transfer of bits across the company backbone for a mission critical financial application. The administrator notices that the network throughput appears lower than the bandwidth expected. Which three factors could influence the differences in throughput? (Choose three.)

amount of traffic, type of traffic, latency

- **the amount of traffic that is currently crossing the network**
- the sophistication of the encapsulation method applied to the data
- **the type of traffic that is crossing the network**
- **the latency that is created by the number of network devices that the data is crossing**
- the bandwidth of the WAN connection to the Internet
- the reliability of the gigabit Ethernet infrastructure of the backbone

**Explanation:** Throughput usually does not match the specified bandwidth of physical links due to multiple factors. These factors include, the amount of traffic, type of traffic, and latency created by the network devices the data has to cross.

**7. What are two characteristics of fiber-optic cable? (Choose two.)**

- **It is not affected by EMI or RFI.**
- Each pair of cables is wrapped in metallic foil.
- It combines the technique of cancellation, shielding, and twisting to protect data.
- It typically contains 4 pairs of fiber-optic wires.
- **It is more expensive than UTP cabling is.**

**Explanation:** Fiber-optic cabling supports higher bandwidth than UTP for longer distances. Fiber is **immune to EMI and RFI**, but **costs more**, requires more skill to install, and requires more safety precautions.

**8. What is a primary role of the Physical layer in transmitting data on the network?**

create signal

- **create the signals that represent the bits in each frame on to the media**
- provide physical addressing to the devices
- determine the path packets take through the network
- control data access to the media

**Explanation:** The OSI physical layer provides the means to transport the bits that make up a frame across the network media. This layer accepts a complete frame from the data link layer and encodes it as a series of signals that are transmitted to the local media.

**9. With the use of unshielded twisted-pair copper wire in a network, what causes crosstalk within the cable pairs?**

magnetic field

- **the magnetic field around the adjacent pairs of wire**
- the use of braided wire to shield the adjacent wire pairs
- the reflection of the electrical wave back from the far end of the cable
- the collision caused by two nodes trying to use the media simultaneously

**Explanation:** Crosstalk is a type of noise, or interference that occurs when signal transmission on one wire interferes with another wire. When current flows through a wire a magnetic field is produced. The produced magnetic field will interface the signal carried in the adjacent wire.

10. Refer to the graphic. What type of cabling is shown?



- STP
- UTP
- coax
- **fiber**

**Explanation:** Network cabling include different types of cables:

- UTP cable consists of four pairs of color-coded wires that have been twisted together and then encased in a flexible plastic sheath.
- STP cable uses four pairs of wires, each wrapped in a foil shield, which are then wrapped in an overall metallic braid or foil.
- Coaxial cable uses a copper conductor and a layer of flexible plastic insulation surrounds the copper conductor.
- Fiber cable is a flexible, extremely thin, transparent strand of glass surrounded by plastic insulation.

11. In addition to the cable length, what two factors could **interfere with the communication** carried over UTP cables? (Choose two.)

- **crosstalk** crosstalk, magnetic
- bandwidth
- size of the network
- signal modulation technique
- **electromagnetic interference**

**Explanation:** Copper media is widely used in network communications. However, copper media is limited by distance and signal interference. Data is transmitted on copper cables as electrical pulses. The electrical pulses are susceptible to interference from two sources:

- **Electromagnetic interference (EMI) or radio frequency interference (RFI)** – EMI and RFI signals can distort and corrupt the data signals being carried by copper media.



- **Crosstalk** – Crosstalk is a disturbance caused by the electric or magnetic fields of a signal on one wire interfering with the signal in an adjacent wire.

12. Refer to the graphic. What type of cabling is shown?



- STP                      utp: dây có màu
- **UTP**
- coax
- fiber

13. Which two devices commonly affect wireless networks? (Choose two.)

- Blu-ray players
- home theaters                      ảnh hưởng bởi các thiết bị phát sóng
- **cordless phones**
- **microwaves**
- incandescent light bulbs
- external hard drives

**Explanation:** Radio Frequency Interference (RFI) is the interference that is caused by radio transmitters and other devices that are transmitting in the same frequency.

14. Which two statements describe the services provided by the **data link layer**? (Choose two.)

access frame, layer 3 pdu

- It defines the end-to-end delivery addressing scheme.
- It maintains the path between the source and destination devices during the data transmission.
- **It manages the access of frames to the network media.**
- It provides reliable delivery through link establishment and flow control.
- It ensures that application data will be transmitted according to the prioritization.
- **It packages various Layer 3 PDUs into a frame format that is compatible with the network interface.**

**Explanation:** The data link layer is divided into two sub layers, namely Logical Link Control (LLC) and Media Access Control (MAC). LLC forms a frame from the network

layer PDU into a format that conforms to the requirements of the network interface and media. A network layer PDU might be for IPv4 or IPv6. The MAC sub layer defines the media access processes performed by the hardware. It manages the frame access to the network media according to the physical signaling requirements (copper cable, fiber optic, wireless, etc.)

**15. 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

**Explanation:** 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.

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

- logical address
- physical address
- data
- **error detection**

**Explanation:** 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.

**17. Which statement describes a characteristic of the **frame header fields** of the data link layer?**

- They all include the flow control and logical connection fields.
- Ethernet frame header fields contain Layer 3 source and destination addresses.
- **They vary depending on protocols.**
- They include information on user applications.

**Explanation:** All data link layer protocols encapsulate the Layer 3 PDU within the data field of the frame. However, the structure of the frame and the fields that are contained in the header vary according to the protocol. Different data link layer protocols may use different fields, like priority/quality of service, logical connection control, physical link control, flow control, and congestion control.

**18. A network team is comparing physical WAN topologies for connecting remote sites to a headquarters building. Which topology provides high availability and connects some, but not all, remote sites?**

- mesh
- **partial mesh**
- hub and spoke
- point-to-point

**Explanation:** Partial mesh topologies provide high availability by interconnecting multiple remote sites, but do not require a connection between all remote sites. A mesh topology requires point-to-point links with every system being connected to every other system. A point-to-point topology is where each device is connected to one other device. A hub and spoke uses a central device in a star topology that connects to other point-to-point devices.

**19. Which two fields or features does Ethernet examine to determine if a received frame is passed to the data link layer or discarded by the NIC? (Choose two.)**

- auto-MDIX
- CEF
- **Frame Check Sequence**
- **minimum frame size**
- source MAC address

**Explanation:** An Ethernet frame is not processed and is discarded if it is smaller than the minimum (64 bytes) or if the calculated **frame check sequence (FCS)** value does not match the received FCS value. Auto-MDIX (automatic medium-dependent interface crossover) is Layer 1 technology that detects cable straight-through or crossover types. The source MAC address is not used to determine how the frame is received. CEF (Cisco Express Forwarding) is a technology used to expedite Layer 3 switching.

**20. Which media communication type does not require media arbitration in the data link layer?**

- deterministic
- half-duplex
- **full-duplex**
- controlled access

**Explanation:** Half-duplex communication occurs when both devices can both transmit and receive on the medium but cannot do so simultaneously. **Full-duplex communication occurs when both devices can transmit and receive on the medium at the same time and therefore does not require media arbitration.** Half-duplex communication is typically contention-based, whereas controlled (deterministic) access is applied in technologies where devices take turns to access the medium.

## 21. 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.

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

## 22. What is a characteristic of the LLC sublayer? layer 3

- It provides the logical addressing required that identifies the device.
- It provides delimitation of data according to the physical signaling requirements of the medium.
- It places information in the frame allowing multiple Layer 3 protocols to use the same network interface and media.
- It defines software processes that provide services to the physical layer.

**Explanation:** The Logical Link Control (LLC) defines the software processes that provide services to the network layer protocols. The information is placed by LLC in the frame and identifies which network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IPv4 and IPv6, to utilize the same network interface and media.

## 23. What are three ways that media access control is used in networking? (Choose three.)

csma, data frame, data link layer

- Ethernet utilizes CSMA/CD.
- Media access control provides placement of data frames onto the media.
- Contention-based access is also known as deterministic.
- 802.11 utilizes CSMA/CD.
- Data link layer protocols define the rules for access to different media.
- Networks with controlled access have reduced performance due to data collisions.

**Explanation:** Wired Ethernet networks use CSMA/CD for media access control. IEEE 802.11 wireless networks use CSMA/CA, a similar method. Media access control defines the way data frames get placed on the media. The controlled access method is deterministic, not a contention-based access to networks. Because each device has its own time to use the medium, controlled access networks such as legacy Token Ring do not have collisions.

**24. During the encapsulation process, what occurs at the data link layer for a PC connected to an Ethernet network?**

- An IP address is added.
- The logical address is added.
- **The physical address is added.** mac address
- The process port number is added.

**Explanation:** The Ethernet frame includes the source and destination physical address. The trailer includes a CRC value in the Frame Check Sequence field to allow the receiving device to determine if the frame has been changed (has errors) during the transmission.

**25. What three items are contained in an Ethernet header and trailer? (Choose three.)**

- source IP address source, destination MAC, error-checking
- **source MAC address**
- destination IP address
- **destination MAC address**
- **error-checking information**

**Explanation:** Layer 2 headers contain the following:

- **Frame start and stop indicator flags** at the beginning and end of a frame
- Addressing – for Ethernet networks this part of the header contains **source and destination MAC addresses**
- Type field to indicate what Layer 3 protocol is being used
- **Error detection** to determine if the frame arrived without error

**26. What type of communication rule would best describe CSMA/CD?**

- **access method**
- flow control access
- message encapsulation
- message encoding

**Explanation:** Carrier sense multiple access collision detection (CSMA/CD) is the access method used with Ethernet. The access method rule of communication dictates how a network device is able to place a signal on the carrier. CSMA/CD dictates those rules on an Ethernet network and CSMA/CA dictates those rules on an 802.11 wireless LAN.

**27. Which three basic parts are common to all frame types supported by the data link layer? (Choose three.)**

header, data, trailer

- **header**
- type field
- MTU size
- **data**
- **trailer**
- CRC value

**Explanation:** The data link protocol is responsible for NIC-to-NIC communications within the same network. Although there are many different data link layer protocols that describe data link layer frames, each frame type has three basic parts:

- Header
- Data
- Trailer

## 28. Which statement is true about the CSMA/CD access method that is used in Ethernet?

csma/cd : listen before transmit

- When a device hears a carrier signal and transmits, a collision cannot occur.
- A jamming signal causes only devices that caused the collision to execute a backoff algorithm.
- **All network devices must listen before transmitting.**
- Devices involved in a collision get priority to transmit after the backoff period.

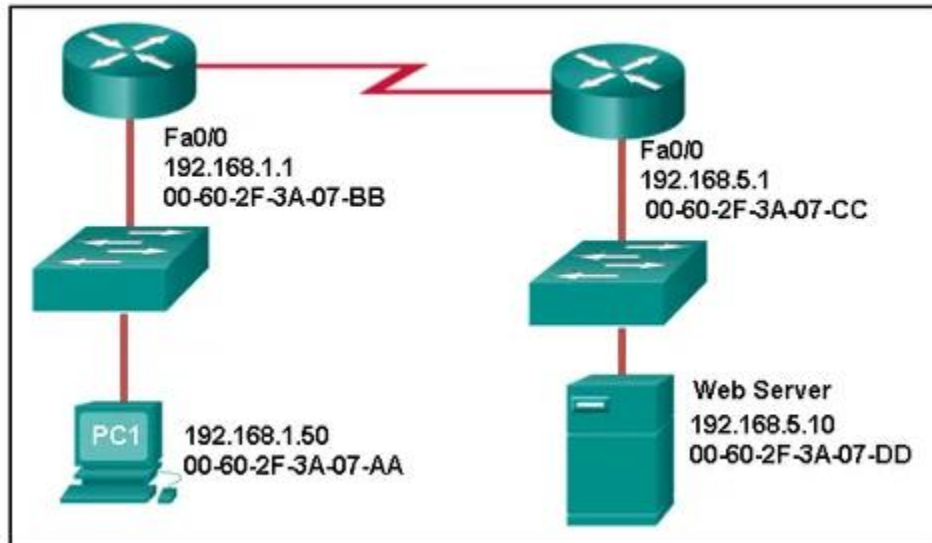
**Explanation:** Legacy bus-topology Ethernet LAN uses CSMA/CD as network media access control protocol. It works by detecting a collision in the medium and backing off (after transmitting a jam signal) as necessary. **When one host wants to transmit a frame, it listens on the medium to check if the medium is busy.** After it senses that no one else is transmitting, the host starts transmitting the frame, it also monitors the current level to detect a collision. If it detects a collision, it transmits a special jam signal so that all other hosts can know there was a collision. The other host will receive this jam signal and stop transmitting. After this, both hosts enter an exponential backoff phase and retry transmission.

## 29. What is the auto-MDIX feature on a switch?

- the automatic configuration of an interface for 10/100/1000 Mb/s operation
- **the automatic configuration of an interface for a straight-through or a crossover Ethernet cable connection**
- the automatic configuration of full-duplex operation over a single Ethernet copper or optical cable
- the ability to turn a switch interface on or off accordingly if an active connection is detected

**Explanation:** The auto-MDIX enables a switch to use a crossover or a straight-through Ethernet cable to connect to a device regardless of the device on the other end of the connection.

**30. Refer to the exhibit. What is the destination MAC address of the Ethernet frame as it leaves the web server if the final destination is PC1?**



- 00-60-2F-3A-07-AA
- 00-60-2F-3A-07-BB
- **00-60-2F-3A-07-CC**
- 00-60-2F-3A-07-DD

**Explanation:** The destination MAC address is used for local delivery of Ethernet frames. The MAC (Layer 2) address changes at each network segment along the path. As the frame leaves the web server, it will be delivered by using the MAC address of the default gateway.

**31. 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

**Explanation:** With shared memory buffering, the number of frames stored in the buffer is restricted only by the of the entire memory buffer and not limited to a single port buffer. This permits larger frames to be transmitted with fewer dropped frames. This is important to asymmetric switching, which applies to this scenario, where frames are

being exchanged between ports of different rates. With port-based memory buffering, frames are stored in queues that are linked to specific incoming and outgoing ports making it possible for a single frame to delay the transmission of all the frames in memory because of a busy destination port. Level 1 cache is memory used in a CPU. Fixed configuration refers to the port arrangement in switch hardware.

**32. What are two examples of the cut-through switching method? (Choose two.)**

- store-and-forward switching
  - **fast-forward switching**
  - CRC switching
  - **fragment-free switching**
  - QOS switching
- fast-forward, fragment-free

**Explanation:** Store-and forward switching accepts the entire frame and performs error checking using CRC before forwarding the frame. Store-and-forward is often required for QOS analysis. Fast-forward and fragment-free are both variations of the cut-through switching method where only part of the frame is received before the switch begins to forward it.

**33. Which frame forwarding method receives the entire frame and performs a CRC check to detect errors before forwarding the frame?**

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

**Explanation:** Fast-forward and fragment-free switching are variations of cut-through switching, which begins to forward the frame before the entire frame is received.

**34. 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**
- FCS: detect error

**Explanation:** The FCS field in a frame is used to detect any errors in the transmission and receipt of a frame. This is done by comparing the CRC value within the frame against a computed CRC value of the frame. If the two values do not match, then the frame is discarded.

**35. Which switching method has the lowest level of latency?**



fast-forward: lowest latency

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

store and forward : highest latency

**Explanation:** Fast-forward switching begins to forward a frame after reading the destination MAC address, resulting in the lowest latency. Fragment-free reads the first 64 bytes before forwarding. Store-and-forward has the highest latency because it reads the entire frame before beginning to forward it. Both fragment-free and fast-forward are types of cut-through switching.

**36. 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.)**

fastest, full duplex, auto-MDIX

- **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.

**Explanation:** Modern switches can negotiate to work in full-duplex mode if both switches are capable. They will negotiate to work using the fastest possible speed and the auto-MDIX feature is enabled by default, so a cable change is not needed.

**37. Which advantage does the store-and-forward switching method have compared with the cut-through switching method?**

- collision detecting
- **frame error checking**
- faster frame forwarding
- frame forwarding using IPv4 Layer 3 and 4 information

**Explanation:** A switch using the store-and-forward switching method performs an error check on an incoming frame by comparing the FCS value against its own FCS calculations after the entire frame is received. In comparison, a switch using the cut-through switching method makes quick forwarding decisions and starts the forwarding process without waiting for the entire frame to be received. Thus a switch using cut-through switching may send invalid frames to the network. The performance of store-

and-forward switching is slower compared to cut-through switching performance. Collision detection is monitored by the sending device. Store-and-forward switching does not use IPv4 Layer 3 and 4 information for its forwarding decisions.

**38. When the **store-and-forward method** of switching is in use, what part of the Ethernet frame is used to perform an **error check**?**

crc trailer

- **CRC in the trailer**
- source MAC address in the header
- destination MAC address in the header
- protocol type in the header

**Explanation:** The cyclic redundancy check (CRC) part of the trailer is used to determine if the frame has been modified during transit. If the integrity of the frame is verified, the frame is forwarded. If the integrity of the frame cannot be verified, then the frame is dropped.

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

store and forward : crc

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

**Explanation:** 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.

**40. What are two actions performed by a Cisco switch? (Choose two.)**

using source MAC, utilize MAC address

- building a routing table that is based on the first IP address in the frame header
- **using the source MAC addresses of frames to build and maintain a MAC address table**
- forwarding frames with unknown destination IP addresses to the default gateway
- **utilizing the MAC address table to forward frames via the destination MAC address**
- examining the destination MAC address to add new entries to the MAC address table

**Explanation:** Important actions that a switch performs are as follows:

- When a frame comes in, the switch examines the Layer 2 source address to build and maintain the Layer 2 MAC address table.
- It examines the Layer 2 destination address to determine how to forward the frame. When the destination address is in the MAC address table, then the frame is sent out a particular port. When the address is unknown, the frame is sent to all ports that have devices connected to that network.

**41. Which two statements describe features or functions of the **logical link control sublayer** in Ethernet standards? (Choose two.)** implemented in software, data link

- **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.

**Explanation:** 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).

**42. What is the auto-MDIX feature?** straight-through, or crossover

- **It enables a device to automatically configure an interface to use a straight-through or a crossover cable.**
- It enables a device to automatically configure the duplex settings of a segment.
- It enables a device to automatically configure the speed of its interface.
- It enables a switch to dynamically select the forwarding method.

**Explanation:** The auto-MDIX feature allows the device to configure its network port according to the cable type that is used (straight-through or crossover) and the type of device that is connected to that port. When a port of a switch is configured with auto-MDIX, this switch can be connected to another switch by the use of either a straight-through cable or a crossover cable.

**43. What is one advantage of using the **cut-through switching method** instead of the **store-and-forward** switching method?**

- has a positive impact on bandwidth by dropping most of the invalid frames
- makes a fast forwarding decision based on the source MAC address of the frame

- has a **lower latency appropriate for high-performance computing applications**
- provides the flexibility to support any mix of Ethernet speeds

**Explanation:** Cut-through switching provides lower latency switching for high-performance computing (HPC) applications. Cut-through switching allows more invalid frames to cross the network than store-and-forward switching. The cut-through switching method can make a forwarding decision as soon as it looks up the destination MAC address of the frame.

#### 44. Which is a multicast MAC address?

- FF-FF-FF-FF-FF-FF
- 5C-26-0A-4B-19-3E
- **01-00-5E-00-00-03**
- 00-26-0F-4B-00-3E

**Explanation:** Multicast MAC addresses begin with the special value of **01-00-5E**.

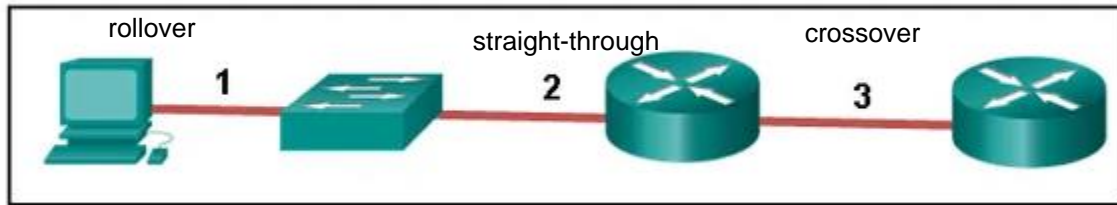
#### 45. Refer to the exhibit. What is wrong with the displayed termination?



- 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.

**Explanation:** 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.

46. 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

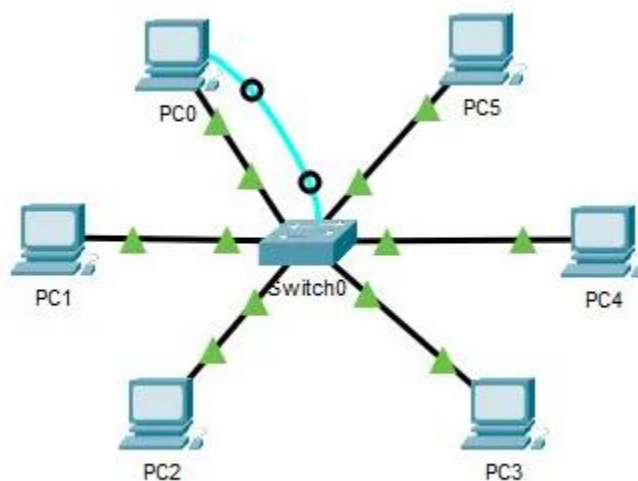
**1 - rollover, 2 - straight-through, 3 - crossover**

1 - crossover, 2 - rollover, 3 - straight-through

1 - crossover, 2 - straight-through, 3 - rollover

**Explanation:** 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.

47. Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.



Which port does Switch0 use to send frames to the host with the IPv4 address 10.1.1.5?

- Fa0/1
- Fa0/5
- Fa0/9
- **Fa0/11**

**Explanation:** Issuing the command **ipconfig /all** from the PC0 command prompt displays the IPv4 address and MAC address. When the IPv4 address 10.1.1.5 is pinged from PC0, the switch stores the source MAC address (from PC0) along with the port to which PC0 is connected. When the destination reply is received, the switch takes the destination MAC address and compares to MAC addresses stored in the MAC address table. Issuing the **show mac-address-table** on the PC0 Terminal application displays two dynamic MAC address entries. The MAC address and port entry that does not belong to PC0 must be the MAC address and port of the destination with the IPv4 address 10.1.1.5.

#### 48. What does the term “attenuation” mean in data communication?

- **loss of signal strength as distance increases**
- time for a signal to reach its destination
- leakage of signals from one cable pair to another
- strengthening of a signal by a networking device

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

#### 49. What makes **fiber preferable to copper cabling** for interconnecting buildings? (Choose three.)

greater distance, emi/rfi, greater bandwidth

- **greater distances per cable run**
- lower installation cost
- **limited susceptibility to EMI/RFI**
- durable connections
- **greater bandwidth potential**
- easily terminated

**Explanation:** Optical fiber cable transmits data over longer distances and at higher bandwidths than any other networking media. Unlike copper wires, fiber-optic cable can transmit signals with less attenuation and is completely immune to EMI and RFI.

#### 50. What OSI physical layer term describes the process by which one **wave** **modifies another wave?**

wave - > modulation

- **modulation**
- IEEE
- EIA/TIA
- air

51. What OSI physical layer term describes the capacity at which a medium can **carry data**?

carry data -> bandwidth

- **bandwidth**
- IEEE
- EIA/TIA
- air

53. What OSI physical layer term describes the measure of the **transfer of bits** across a medium over a given period of time?

- **throughput**
- bandwidth
- latency
- goodput

transfer bits -> throughput

54. What OSI physical layer term describes the amount of time, including delays, for data to travel from one point to another?

- **latency**
- bandwidth
- throughput
- goodput

55. What OSI physical layer term describes the amount of **time, including delays**, for data to travel from one point to another?

- **latency**
- fiber-optic cable
- air
- copper cable

56. What OSI physical layer term describes the measure of **usable data** transferred over a given period of time?

- **goodput**
- fiber-optic cable
- air
- copper cable

usable data -> goodput

57. What OSI physical layer term describes the physical medium which uses **electrical pulses**?

- **copper cable**
- fiber-optic cable
- air
- goodput

58. What OSI physical layer term describes the physical medium that uses the propagation of **light**?

- **fiber-optic cable** light -> fiber-optic
- goodput
- latency
- throughput

59. What OSI physical layer term describes the physical medium for **microwave transmissions**?

- **air** microwave -> air
- goodput
- latency
- throughput

60. Which two functions are performed at the **MAC sublayer of the OSI data link layer**? (Choose two.)

- Adds Layer 2 control information to network protocol data.
- Places information in the frame that identifies which network layer protocol is being used for the frame.
- **Controls the NIC responsible for sending and receiving data on the physical medium.**
- **Implements a trailer to detect transmission errors.**
- Enables IPv4 and IPv6 to utilize the same network interface and media.

**Case 2:**      nic  
                 implement a trailer  
                 synchronization  
                 physical technology  
                 mechanism

- **Provides synchronization between source and target nodes.**
- **Integrates various physical technologies.**
- Communicates between the networking software at the upper layers and the device hardware at the lower layers.
- Adds Layer 2 control information to network protocol data.
- Enables IPv4 and IPv6 to utilize the same network interface and media.



### Case 3:

- Enables IPv4 and IPv6 to utilize the same network interface and media.
- **Provides synchronization between source and target nodes.**
- **Implements a trailer to detect transmission errors.**
- Adds Layer 2 control information to network protocol data.
- Places information in the frame that identifies which network layer protocol is being used for the frame.

### Case 4:

- Enables IPv4 and IPv6 to utilize the same network interface and media.
- Adds Layer 2 control information to network protocol data.
- **Integrates various physical technologies.**
- Communicates between the networking software at the upper layers and the device hardware at the lower layers.
- **Provides synchronization between source and target nodes.**

### Case 5:

- Places information in the frame that identifies which network layer protocol is being used for the frame.
- **Integrates various physical technologies.**
- Adds Layer 2 control information to network protocol data.
- **Controls the NIC responsible for sending and receiving data on the physical medium.**
- Communicates between the networking software at the upper layers and the device hardware at the lower layers.

### Case 6:

- **Controls the NIC responsible for sending and receiving data on the physical medium**
- **Provides a mechanism to allow multiple devices to communicate over a shared medium.**

61. Which two functions are performed at the **LLC sublayer of the OSI data link layer**? (Choose two.)

enable ipv4, v6

add layer 2 control

place in4 in frame

- **Enables IPv4 and IPv6 to utilize the same network interface and media.**
- **Places information in the frame that identifies which network layer protocol is being used for the frame.**
- Integrates various physical technologies.

- Implements a process to delimit fields within a Layer 2 frame.
- Controls the NIC responsible for sending and receiving data on the physical medium.

**64. Which two functions are performed at the LLC sublayer of the OSI data link layer? (Choose two.)**

- **Adds Layer 2 control information to network protocol data.**
- **Places information in the frame that identifies which network layer protocol is being used for the frame.**
- Performs data encapsulation.
- Controls the NIC responsible for sending and receiving data on the physical medium.
- Integrates various physical technologies.

**66. Which two functions are performed at the LLC sublayer of the OSI data link layer? (Choose two.)**

- **Adds Layer 2 control information to network protocol data.**
- **Enables IPv4 and IPv6 to utilize the same network interface and media.**
- Provides data link layer addressing.
- Implements a trailer to detect transmission errors.
- Provides synchronization between source and target nodes.

**68. Which two functions are performed at the LLC sublayer of the OSI data link layer? (Choose two.)**

- **Enables IPv4 and IPv6 to utilize the same network interface and media.**
- **Adds Layer 2 control information to network protocol data.**
- Integrates various physical technologies.
- Implements a trailer to detect transmission errors.
- Provides synchronization between source and target nodes.

**71. What action will occur if a switch receives a frame with the destination MAC address FF:FF:FF:FF:FF:FF?**

- **The switch forwards it out all ports except the ingress port.**
- The switch shares the MAC address table entry with any connected switches.
- The switch does not forward the frame.
- The switch sends the frame to a connected router because the destination MAC address is not local.

**73. What action will occur if a switch receives a frame with the destination MAC address 01:00:5E:00:00:D9?**

- **The switch forwards it out all ports except the ingress port.**

- The switch does not forward the frame.
- The switch sends the frame to a connected router because the destination MAC address is not local.
- The switch shares the MAC address table entry with any connected switches.

**74. What action will occur if a host receives a frame with a destination MAC address of FF:FF:FF:FF:FF:FF?**

process frame

- **The host will process the frame.**
- The host forwards the frame to the router.
- The host sends the frame to the switch to update the MAC address table.
- The host forwards the frame to all other hosts.

**75. What action will occur if a switch receives a frame and does have the source MAC address in the MAC table?**

refresh timer

- **The switch refreshes the timer on that entry.**
- The switch adds it to its MAC address table associated with the port number.
- The switch forwards the frame to the associated port.
- The switch sends the frame to a connected router because the destination MAC address is not local.

**76. What action will occur if a host receives a frame with a destination MAC address of FF:FF:FF:FF:FF:FF?**

- **The host will process the frame.**
- The host returns the frame to the switch.
- The host replies to the switch with its own IP address.
- The host forwards the frame to all other hosts.

**78. What action will occur if a host receives a frame with a destination MAC address it does not recognize?**

discard

- **The host will discard the frame.**
- The host replies to the switch with its own IP address.
- The host forwards the frame to all other hosts.
- The host returns the frame to the switch.

**79. Which type of UTP cable is used to connect a PC to a switch port?**

- console
- rollover
- crossover
- **straight-through**

**Explanation:** A rollover cable is a Cisco proprietary cable used to connect to a router or switch console port. A straight-through (also called patch) cable is usually used to interconnect a host to a switch and a switch to a router. A crossover cable is used to interconnect similar devices together, for example, between two switches, two routers, and two hosts.

### III. MODULE 8-10

1. Which information is used by routers to **forward a data packet toward its destination?**

- source IP address
- **destination IP address**
- source data-link address
- destination data-link address

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

- 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.

3. A router receives a packet from the Gigabit 0/0 interface and determines that the packet needs to be forwarded out the Gigabit 0/1 interface. What will the router do next?      create layer 2

- route the packet out the Gigabit 0/1 interface
- **create a new Layer 2 Ethernet frame to be sent to the destination**
- look into the ARP cache to determine the destination IP address
- look into the routing table to determine if the destination network is in the routing table

4. Which IPv4 address can a host use to **ping the loopback interface?**

- 126.0.0.1
- 127.0.0.0
- 126.0.0.0
- **127.0.0.1**

**5. A computer can access devices on the same network but cannot access devices on other networks. What is the probable cause of this problem?**

- The cable is not connected properly to the NIC.
- The computer has an invalid IP address.
- The computer has an incorrect subnet mask.
- **The computer has an invalid default gateway address.**

**6. Which statement describes a feature of the IP protocol?**

- IP encapsulation is modified based on network media.
- IP relies on Layer 2 protocols for transmission error control.
- MAC addresses are used during the IP packet encapsulation.
- **IP relies on upper layer services to handle situations of missing or out-of-order packets.**

**Explanation:** IP protocol is a connection-less protocol, considered unreliable in terms of end-to-end delivery. It does not provide error control in the cases where receiving packets are out-of-order or in cases of missing packets. It relies on upper layer services, such as TCP, to resolve these issues.

**7. 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.

**Explanation:** The large number of public IPv6 addresses eliminates the need for NAT. Sites from the largest enterprises to single households can get public IPv6 network addresses. This avoids some of the NAT-induced application problems that are experienced by applications that require end-to-end connectivity.

**8. Which parameter does the router use to choose the path to the destination when there are multiple routes available?**

- **the lower metric value that is associated with the destination network**
- the lower gateway IP address to get to the destination network
- the higher metric value that is associated with the destination network
- the higher gateway IP address to get to the destination network

**9. What are two services provided by the OSI network layer? (Choose two.)**

- performing error detection
- **routing packets toward the destination**
- **encapsulating PDUs from the transport layer**
- placement of frames on the media
- collision detection

**Explanation:** The OSI network layer provides several services to allow communication between devices:

- addressing
- encapsulation
- routing
- de-encapsulation

Error detection, placing frames on the media, and collision detection are all functions of the data link layer.

**10. Within a production network, what is the purpose of configuring a switch with a default gateway address?**

- Hosts that are connected to the switch can use the switch default gateway address to forward packets to a remote destination.
- A switch must have a default gateway to be accessible by Telnet and SSH.
- **The default gateway address is used to forward packets originating from the switch to remote networks.**
- It provides a next-hop address for all traffic that flows through the switch.

**Explanation:** A default gateway address allows a switch to forward packets that originate on the switch to remote networks. A default gateway address on a switch does not provide Layer 3 routing for PCs that are connected on that switch. A switch can still be accessible from Telnet as long as the source of the Telnet connection is on the local network.

**11. What is a basic characteristic of the IP protocol?**

- **connectionless**
- media dependent
- user data segmentation
- reliable end-to-end delivery

**Explanation:** Internet Protocol (IP) is a network layer protocol that **does not require initial exchange of control information** to establish an end-to-end connection before packets are forwarded. Thus, IP is connectionless and does not provide reliable end-to-

end delivery by itself. IP is media independent. User data segmentation is a service provided at the transport layer.

**12. 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

**Explanation:** 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.

**13. 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**

**Explanation:** 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

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

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

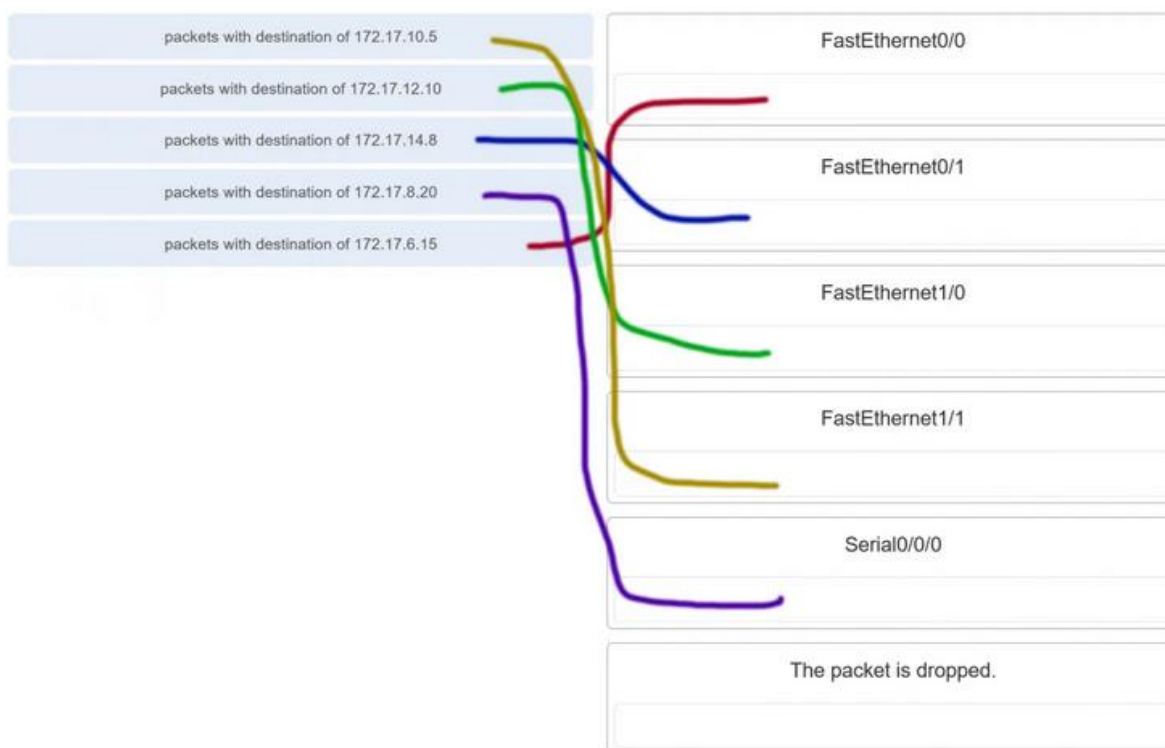
**Explanation:** It is the Protocol field in the IP header that identifies the upper-layer protocol the packet is carrying. The Version field identifies the IP version. The

Differential Services field is used for setting packet priority. The Identification field is used to reorder fragmented packets.

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

```
<output omitted>
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

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



**Explanation:** Packets with a destination of 172.17.6.15 are forwarded through Fa0/0. Packets with a destination of 172.17.10.5 are forwarded through Fa1/1. Packets with a destination of 172.17.12.10 are forwarded through Fa1/0. Packets with a destination of 172.17.14.8 are forwarded through Fa0/1. Because network 172.17.8.0 has no entry in the routing table, it will take the gateway of last resort, which means that packets with a



destination of 172.17.8.20 are forwarded through Serial0/0/0. Because a gateway of last resort exists, no packets will be dropped.

**16. What information does the loopback test provide?**

- The TCP/IP stack on the device is working correctly.
- The device has end-to-end connectivity.
- DHCP is working correctly.
- The Ethernet cable is working correctly.
- The device has the correct IP address on the network.

**17. 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

**Explanation:** 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.

**18. 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.

**Explanation:** Hosts must maintain their own local routing table to ensure that network layer packets are directed to the correct destination network. This local table typically contains a route to the loopback interface, a route to the network that the host is connected to, and a local default route, which represents the route that packets must take to reach all remote network addresses.

**19. When transporting data from real-time applications, such as streaming audio and video, which field in the IPv6 header can be used to inform the routers and switches to maintain the same path for the packets in the same conversation?**

- Next Header

- **Flow Label**
- Traffic Class
- Differentiated Services

**Explanation:** The **Flow Label** in IPv6 header is a 20-bit field that provides a special service for real-time applications. This field can be used to **inform routers and switches to maintain the same path for the packet flow** so that packets will not be reordered.

**20. 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**.**

**Explanation:** When a PC wants to send data on the network, it always knows the IP address of the destination. However, it also needs to discover the MAC address of the destination. ARP is the protocol that is used to discover the MAC address of a host that belongs to the same network.

**21. Under which two circumstances will a switch **flood a frame out of every port except the port that the frame was received on**? (Choose two.)**

- **The frame has the **broadcast address** as the destination address.**
- **The **destination address is unknown** to the switch.**
- The source address in the frame header is the broadcast address.
- The source address in the frame is a multicast address.
- The destination address in the frame is a known unicast address.

**Explanation:** A switch will flood a frame out of every port, except the one that the frame was received from, under two circumstances. **Either the frame has the broadcast address as the destination address, or the destination address is unknown to the switch.**

**22. 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.

**Explanation:** One of the negative issues with ARP requests is that they are sent as a broadcast. This means **all devices on the local link must receive and process the request.**

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

- 0.0.0.0
- 255.255.255.255
- **FFFF.FFFF.FFFF**
- AAAA.AAAA.AAAA
- the physical address of the destination host

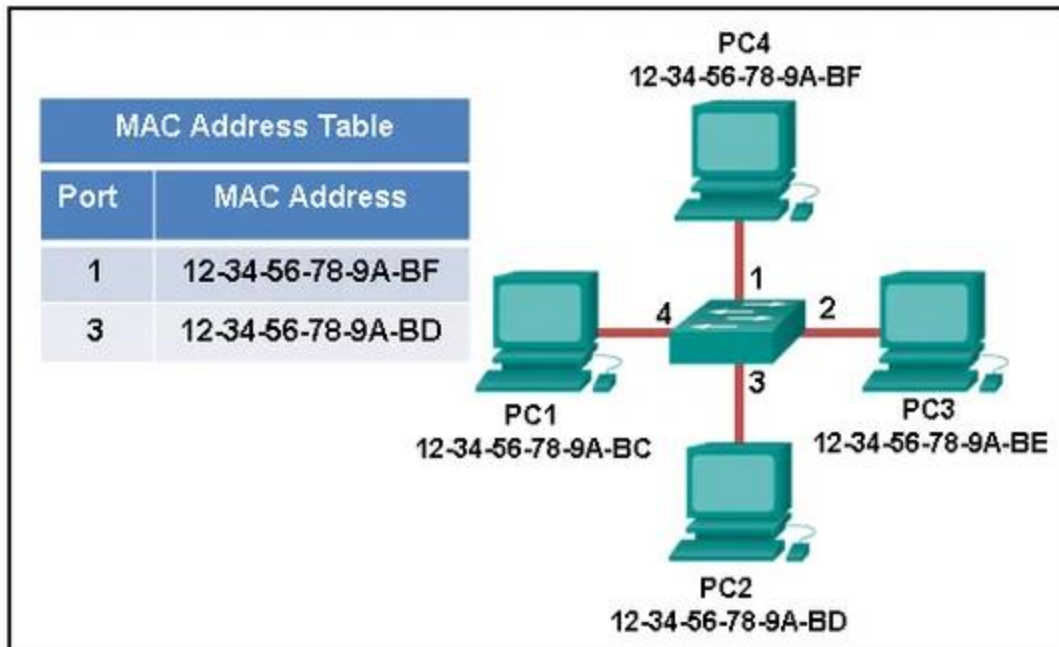
**Explanation:** The purpose of an ARP request is to find the MAC address of the destination host on an Ethernet LAN. The ARP process sends a Layer 2 broadcast to all devices on the Ethernet LAN. The frame contains the IP address of the destination and the broadcast MAC address, FFFF.FFFF.FFFF. The host with the IP address that matches the IP address in the ARP request will reply with a unicast frame that includes the MAC address of the host. Thus the original sending host will obtain the destination IP and MAC address pair to continue the encapsulation process for data transmission.

**24. 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.

**Explanation:** 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.

**25. 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.

**Explanation:** 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.

**26. Which two types of IPv6 messages are used in place of ARP for address resolution?**

- anycast
- broadcast
- echo reply
- echo request
- **neighbor solicitation**
- **neighbor advertisement**

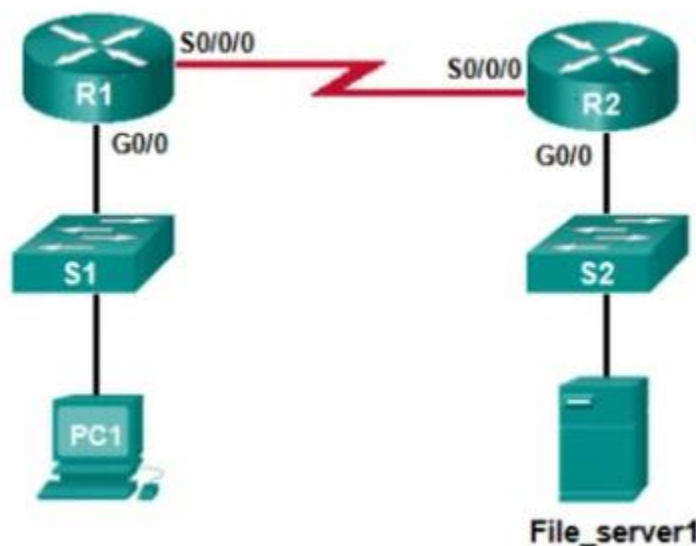
**Explanation:** IPv6 does not use ARP. Instead, ICMPv6 neighbor discovery is used by sending neighbor solicitation and neighbor advertisement messages.

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

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

**Explanation:** In an ARP spoofing attack, a malicious host intercepts ARP requests and replies to them so that network hosts will map an IP address to the MAC address of the malicious host.

**28. Refer to the exhibit. PC1 attempts to connect to File\_server1 and sends an ARP request to obtain a destination MAC address. Which MAC address will PC1 receive in the ARP reply?**



- the MAC address of S1
- **the MAC address of the G0/0 interface on R1**
- the MAC address of the G0/0 interface on R2
- the MAC address of S2
- the MAC address of File\_server1

**29. Where are IPv4 address to Layer 2 Ethernet address mappings maintained on a host computer?**

- neighbor table
- **ARP cache**
- routing table

- MAC address table

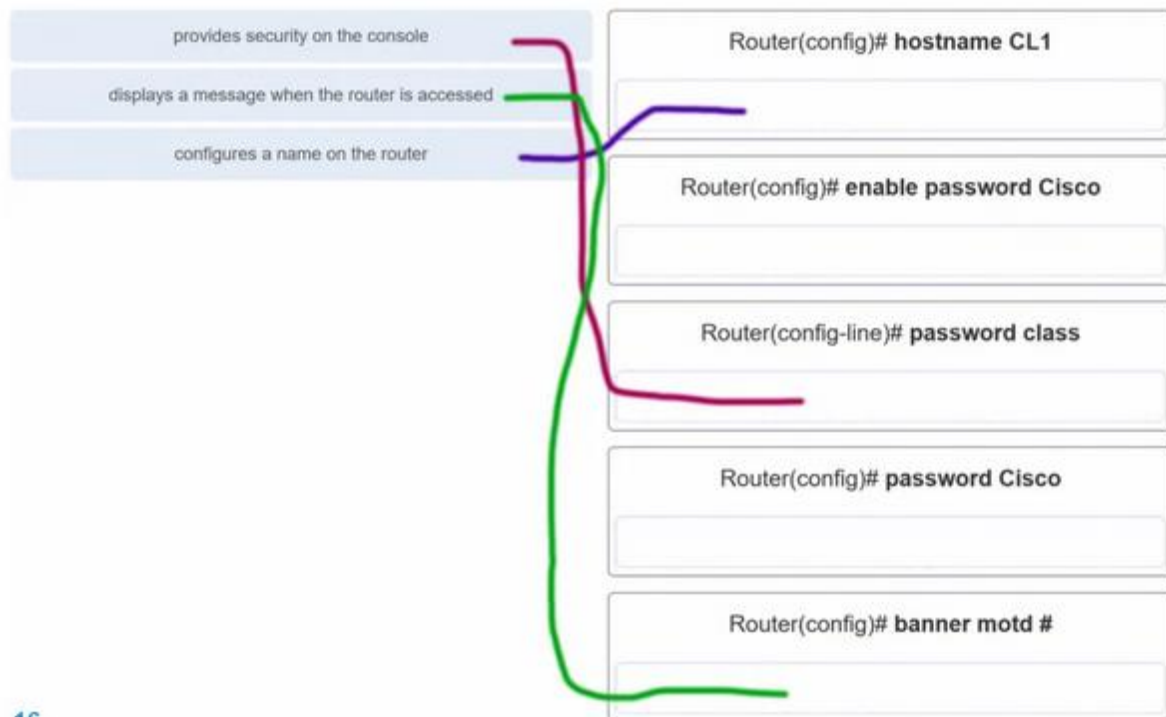
**Explanation:** The ARP cache is used to store IPv4 addresses and the Ethernet physical addresses or MAC addresses to which the IPv4 addresses are mapped. Incorrect mappings of IP addresses to MAC addresses can result in loss of end-to-end connectivity.

**30. What important information is examined in the Ethernet frame header by a Layer 2 device in order to forward the data onward?**

- source MAC address
- source IP address
- **destination MAC address**
- Ethernet type
- destination IP address

**Explanation:** The Layer 2 device, such as a switch, uses the destination MAC address to determine which path (interface or port) should be used to send the data onward to the destination device.

**31. Match the commands to the correct actions. (Not all options are used.)**

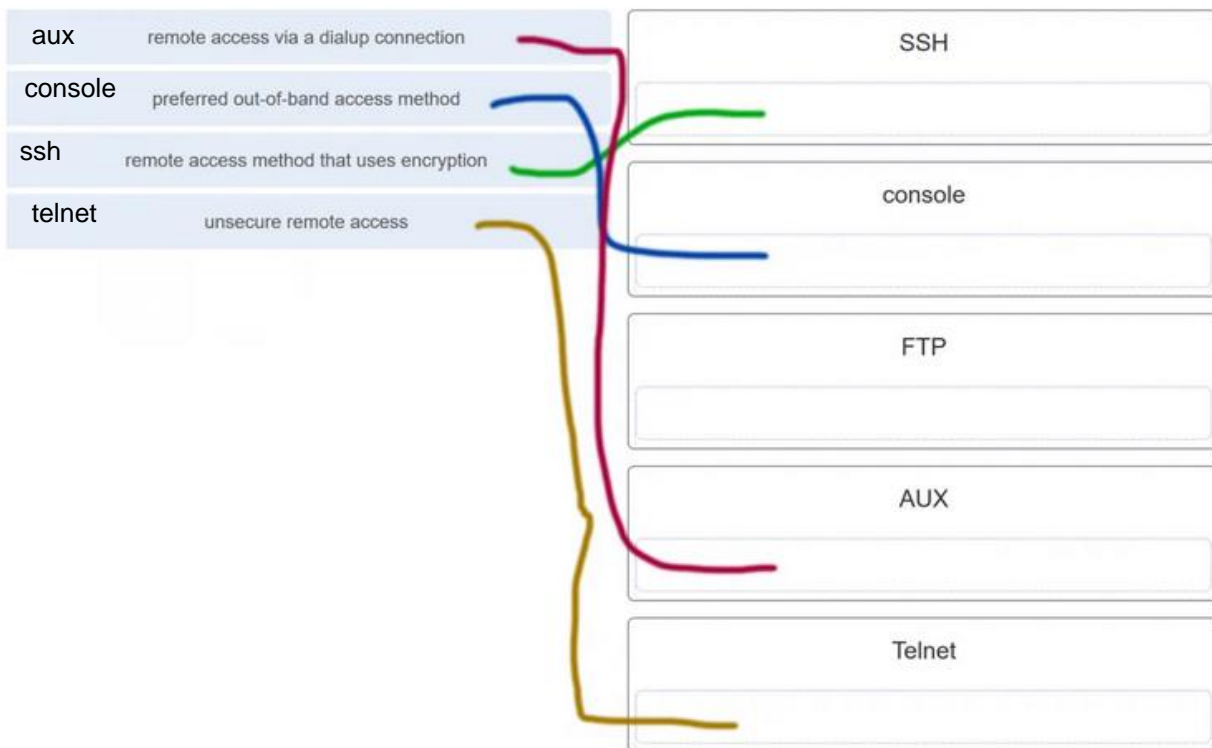


32. A new network administrator has been asked to enter a banner message on a Cisco device. What is the fastest way a network administrator could test whether the banner is properly configured?

- 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.**

**Explanation:** While at the privileged mode prompt such as Router#, type **exit**, press **Enter**, and the banner message appears. Power cycling a network device that has had the **banner motd** command issued will also display the banner message, but this is not a quick way to test the configuration.

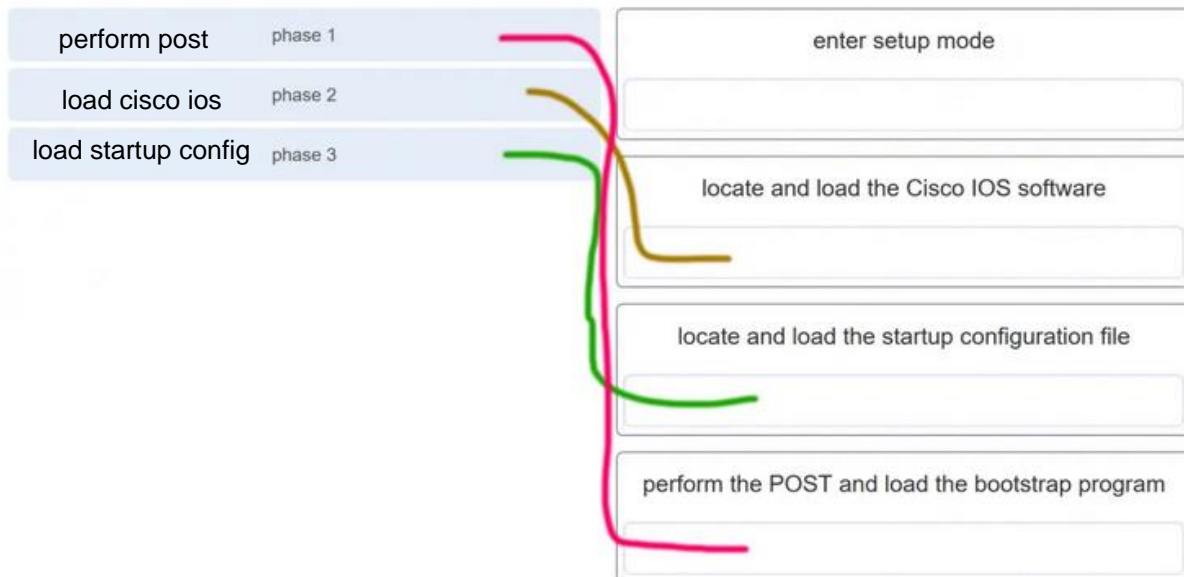
33. A network administrator requires access to manage routers and switches locally and remotely. Match the description to the access method. (Not all options are used.)



**Explanation:** Both the console and AUX ports can be used to directly connect to a Cisco network device for management purposes. However, it is more common to use the console port. The AUX port is more often used for remote access via a dial up connection. SSH and Telnet are both remote access methods that depend on an active

network connection. SSH uses a stronger password authentication than Telnet uses and also uses encryption on transmitted data.

**34. Match the phases to the functions during the boot up process of a Cisco router. (Not all options are used.)**



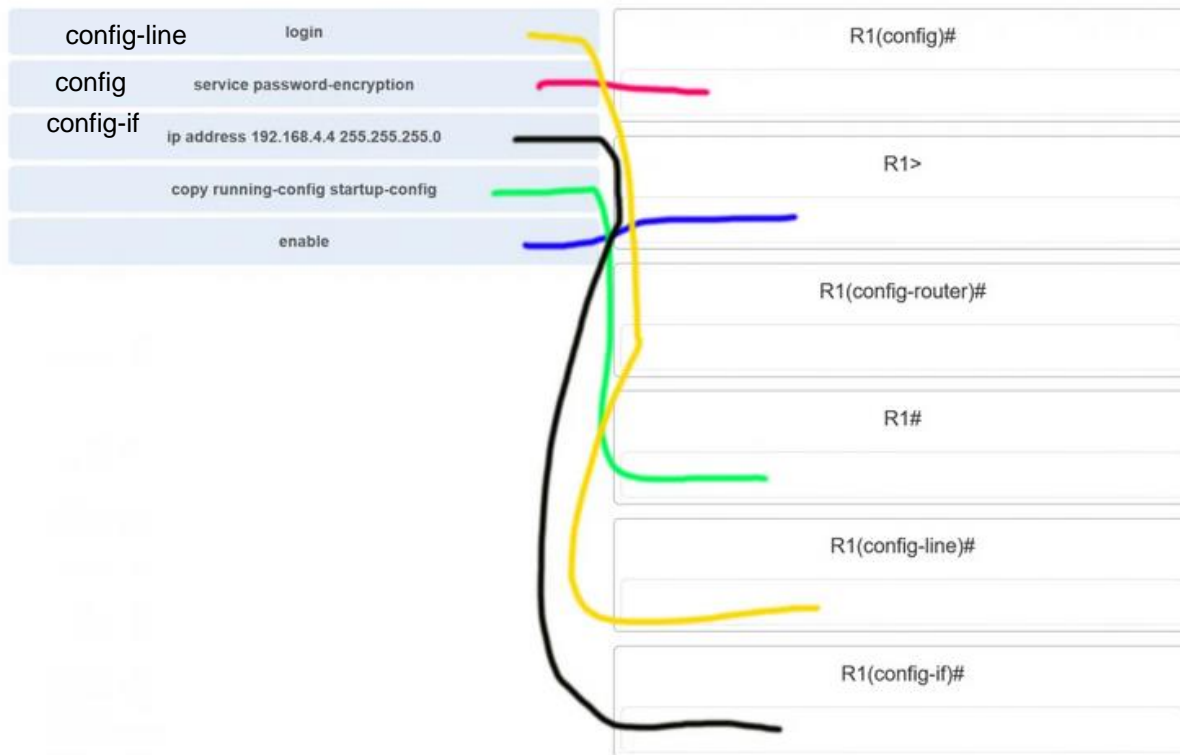
**Explanation:** There are three major phases to the bootup process of a Cisco router:

1. Perform the POST and load the bootstrap program.
2. Locate and load the Cisco IOS software.
3. Locate and load the startup configuration file

If a startup configuration file cannot be located, the router will enter setup mode by displaying the setup mode prompt.

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





**Explanation:** 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.

### 36. What are two functions of NVRAM? (Choose two.)

- to store the routing table
- **to retain contents when power is removed**
- **to store the startup configuration file**
- to contain the running configuration file
- to store the ARP table

**Explanation:** NVRAM is permanent memory storage, so the startup configuration file is preserved even if the router loses power.

### 37. 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.

**Explanation:** If a router cannot locate the startup-config file in NVRAM, it will enter setup mode to allow the configuration to be entered from the console device.

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

- The switch will have a management interface with the address 172.16.100.1.
- **The switch can be remotely managed from a host on another network.**
- The switch can communicate with other hosts on the 172.16.100.0 network.
- The switch is limited to sending and receiving frames to and from the gateway 172.16.100.1.

**Explanation:** A default gateway address is typically configured on all devices to allow them to communicate beyond just their local network. In a switch this is achieved using the command `ip default-gateway <ip address>`.

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

- The SSH client on the switch is enabled.
- **Communication between the switch and remote users is encrypted.**
- The switch requires a username/password combination for remote access.
- The switch requires remote connections via a proprietary client software.

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

**40. Refer to the exhibit. A user PC has successfully transmitted packets to `www.cisco.com`. Which IP address does the user PC target in order to forward its data off the local network?**

```

PC>tracert www.cisco.com

Tracing route to 172.24.2.1 over a maximum of 30 hops:

  1  1 ms    0 ms    0 ms    172.20.0.254
  2  0 ms    0 ms    0 ms    172.20.1.18
  3  1 ms    1 ms    1 ms    172.20.1.1
  4  2 ms    0 ms    1 ms    172.20.1.22
  5  2 ms    2 ms    2 ms    172.24.255.17
  6  2 ms    2 ms    3 ms    172.24.255.13
  7  2 ms    1 ms    2 ms    172.24.255.4
  8  3 ms    1 ms    1 ms    172.24.2.1

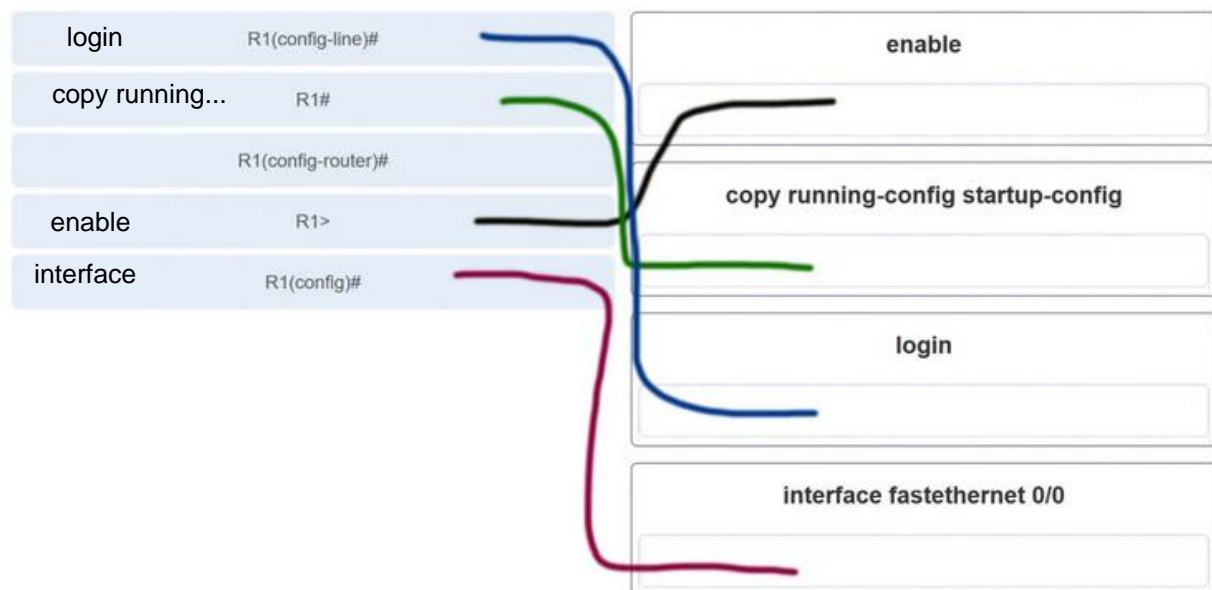
Trace complete.

```

- 172.24.255.17
- 172.24.1.22

- **172.20.0.254**
- 172.24.255.4
- 172.20.1.18

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



**Explanation:** The **enable** command is entered at the R1> prompt. The **login** command is entered at the R1(config-line)# prompt. The **copy running-config startup-config** command is entered at the R1# prompt. The **interface fastethernet 0/0** command is entered at the R1(config)# prompt.

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

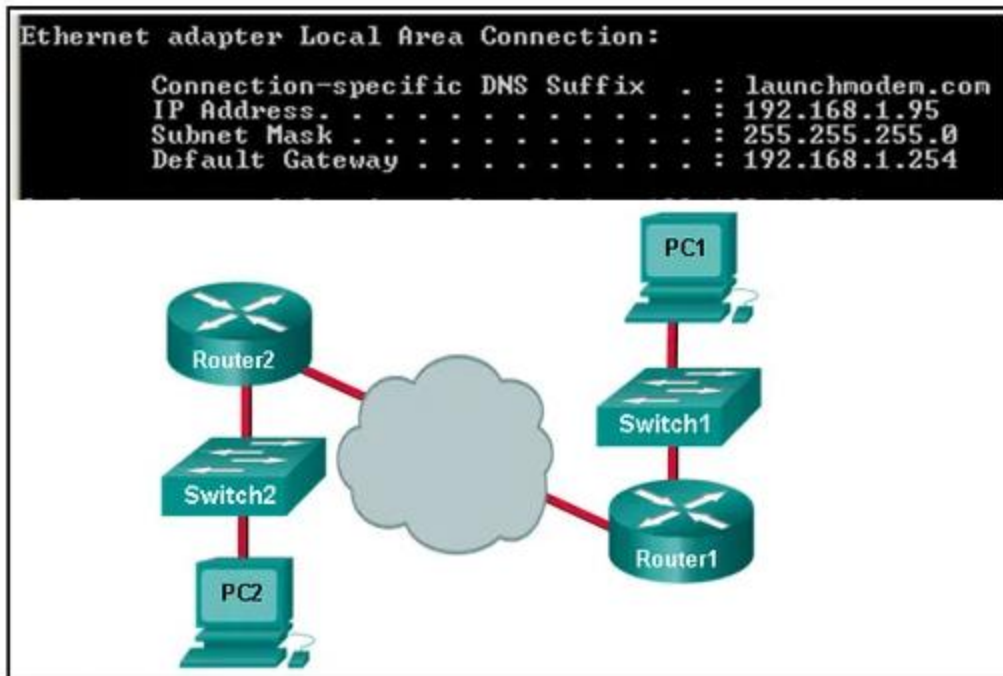
- interface fastethernet 0/0
  - line vty 0 4
  - **line console 0**
  - enable secret cisco
  - **login**
  - **password cisco**
- line console, login, password

**Explanation:** The three commands needed to password protect the console port are as follows:

- **line console 0**
- **password cisco**
- **login**

The **interface 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. The 0 and 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.

**43. Refer to the exhibit. Consider the IP address configuration shown from PC1. What is a description of the default gateway address?**



- It is the IP address of the Router1 interface that connects the company to the Internet.
- **It is the IP address of the Router1 interface that connects the PC1 LAN to Router1.**
- It is the IP address of Switch1 that connects PC1 to other devices on the same LAN.
- It is the IP address of the ISP network device located in the cloud.

**Explanation:** The default gateway is used to route packets destined for remote networks. The default gateway IP address is the address of the first Layer 3 device (the router interface) that connects to the same network.

**44. Which two functions are primary functions of a router? (Choose two.)**

- **packet forwarding**
- microsegmentation
- domain name resolution
- **path selection**
- flow control

**Explanation:** A router accepts a packet and accesses its **routing table** to determine the appropriate exit interface based on the destination address. The router then **forwards** the packet out of that interface.

**45. What is the effect of using the Router# copy running-config startup-config command on a router?**

- The contents of ROM will change.
- The contents of RAM will change.
- **The contents of NVRAM will change.**
- The contents of flash will change.

**Explanation:** The command **copy running-config startup-config** copies the running-configuration file from RAM into NVRAM and saves it as the startup-configuration file. Since NVRAM is non-volatile memory it will be able to retain the configuration details when the router is powered off.

**46. 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.

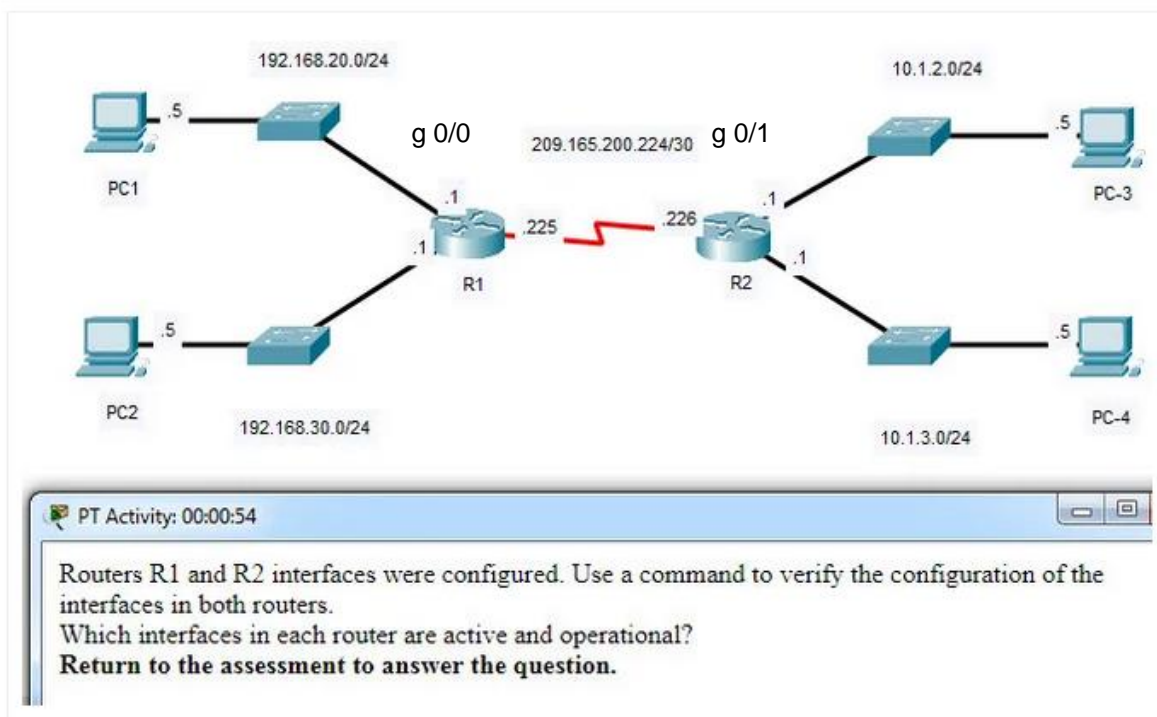
**Explanation:** When a host needs to send a message to another host located on the same network, it can forward the message directly. However, when a host needs to send a message to a remote network, it must use the router, also known as the default gateway. This is because the data link frame address 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.

**47. 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.

**Explanation:** 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.

**48. Open the PT activity. Perform the tasks in the activity instructions and then answer the question.**



**Which interfaces in each router are active and operational?**

R1: G0/0 and S0/0/0  
R2: G0/0 and S0/0/0

R1: G0/1 and S0/0/1  
R2: G0/0 and S0/0/1

**R1: G0/0 and S0/0/0**  
**R2: G0/1 and S0/0/0**

R1: G0/0 and S0/0/1  
R2: G0/1 and S0/0/1

**Explanation:** The command to use for this activity is **show ip interface brief** in each router. The active and operational interfaces are represented by the value “up” in the “Status” and “Protocol” columns. The interfaces in R1 with these characteristics are G0/0 and S0/0/0. In R2 they are G0/1 and S0/0/0.

**49. Which term describes a field in the IPv4 packet header used to identify the next level protocol?**

- **protocol**
- destination IPv4 address
- source IPv4 address
- TTL

**50. Which term describes a field in the IPv4 packet header that contains an 8-bit binary value used to determine the priority of each packet?**

- **differentiated services**
- destination IPv4 address
- source IPv4 address
- protocol

**51. Which term describes a field in the IPv4 packet header that contains a 32-bit binary value associated with an interface on the sending device?**

- **source IPv4 address**
  - destination IPv4 address
  - protocol
  - TTL
- sending device: source

**52. Which term describes a field in the IPv4 packet header used to detect corruption in the IPv4 header?**

- **header checksum**
- source IPv4 address
- protocol
- TTL

**Explanation:** The header checksum is used to determine if any errors have been introduced during transmission.

**53.**

```
RTR1(config)# interface gi0/1
RTR1(config-if)# description Connects to the Marketing LAN
```



```
RTR1(config-if)# ip address 10.27.15.17 255.255.255.0
RTR1(config-if)# no shutdown
RTR1(config-if)# interface gi0/0
RTR1(config-if)# description Connects to the Payroll LAN
RTR1(config-if)# ip address 10.27.14.148 255.255.255.0
RTR1(config-if)# no shutdown
RTR1(config-if)# interface s0/0/0
RTR1(config-if)# description Connects to the ISP
RTR1(config-if)# ip address 10.14.15.254 255.255.255.0
RTR1(config-if)# no shutdown
RTR1(config-if)# interface s0/0/1
RTR1(config-if)# description Connects to the Head Office WAN
RTR1(config-if)# ip address 203.0.113.39 255.255.255.0
RTR1(config-if)# no shutdown
RTR1(config-if)# end
```

**Refer to the exhibit. A network administrator is connecting a new host to the Payroll LAN. The host needs to communicate with remote networks. What IP address would be configured as the default gateway on the new host?**

- **10.27.14.148**
- 10.27.14.1
- 10.14.15.254
- 203.0.113.39
- 10.27.15.17

**54. Which term describes a field in the IPv4 packet header that contains a unicast, multicast, or broadcast address?**

- **destination IPv4 address**
- protocol
- TTL
- header checksum

**55. Which term describes a field in the IPv4 packet header used to limit the lifetime of a packet?**

time to live

- **TTL**
- source IPv4 address
- protocol
- header checksum

**56. Which term describes a field in the IPv4 packet header that contains a 4-bit binary value set to 0100?**

- **version**
- source IPv4 address
- protocol
- TTL

57. Which term describes a field in the IPv4 packet header used to identify the next level protocol?

- **protocol**
- version
- differentiated services
- header checksum

58. Which term describes a field in the IPv4 packet header that contains a 4-bit binary value set to 0100?

- **version**
- differentiated services
- header checksum
- TTL

59. What property of ARP causes cached IP-to-MAC mappings to remain in memory longer?

- **Entries in an ARP table are time-stamped and are purged after the timeout expires.**
- A static IP-to-MAC address entry can be entered manually into an ARP table.
- The type field 0x806 appears in the header of the Ethernet frame.
- The port-to-MAC address table on a switch has the same entries as the ARP table on the switch.

60. What property of ARP allows MAC addresses of frequently used servers to be fixed in the ARP table?

- **A static IP-to-MAC address entry can be entered manually into an ARP table.**
- Entries in an ARP table are time-stamped and are purged after the timeout expires.
- The type field 0x806 appears in the header of the Ethernet frame.
- The port-to-MAC address table on a switch has the same entries as the ARP table on the switch.

62. What property of ARP allows hosts on a LAN to send traffic to remote networks?

- **Local hosts learn the MAC address of the default gateway.**
- The destination MAC address FF-FF-FF-FF-FF-FF appears in the header of the Ethernet frame.
- The source MAC address appears in the header of the Ethernet frame.
- The port-to-MAC address table on a switch has the same entries as the ARP table on the switch.

63.

```
Floor(config)# interface gi0/1
Floor(config-if)# description Connects to the Registrar LAN
Floor(config-if)# ip address 192.168.235.234 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# interface gi0/0
Floor(config-if)# description Connects to the Manager LAN
Floor(config-if)# ip address 192.168.234.114 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# interface s0/0/0
Floor(config-if)# description Connects to the ISP
Floor(config-if)# ip address 10.234.235.254 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# interface s0/0/1
Floor(config-if)# description Connects to the Head Office WAN
Floor(config-if)# ip address 203.0.113.3 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# end
```

**Refer to the exhibit. A network administrator is connecting a new host to the Registrar LAN. The host needs to communicate with remote networks. What IP address would be configured as the default gateway on the new host?**

- **192.168.235.234**
- 192.168.235.1
- 10.234.235.254
- 203.0.113.3
- 192.168.234.114

64. What property of ARP **forces all Ethernet NICs** to process an ARP request?

- **The destination MAC address FF-FF-FF-FF-FF-FF appears in the header of the Ethernet frame.**
- The source MAC address appears in the header of the Ethernet frame.
- The type field 0x806 appears in the header of the Ethernet frame.
- ARP replies are broadcast on the network when a host receives an ARP request.

65. What property of ARP causes a reply only to the **source sending** an ARP request?

- **The source MAC address appears in the header of the Ethernet frame.**
- The destination MAC address FF-FF-FF-FF-FF-FF appears in the header of the Ethernet frame.
- The type field 0x806 appears in the header of the Ethernet frame.
- ARP replies are broadcast on the network when a host receives an ARP request.

66. What property of ARP causes the request to be **flooded out all ports** of a switch except for the port receiving the ARP request?

- **The destination MAC address FF-FF-FF-FF-FF-FF appears in the header of the Ethernet frame.**
- The type field 0x806 appears in the header of the Ethernet frame.
- Entries in an ARP table are time-stamped and are purged after the timeout expires.
- ARP replies are broadcast on the network when a host receives an ARP request.

**67. What property of ARP causes the NICs receiving an ARP request to pass the data portion of the Ethernet frame to the ARP process?**

- **The type field 0x806 appears in the header of the Ethernet frame.**
- The destination MAC address FF-FF-FF-FF-FF-FF appears in the header of the Ethernet frame.
- Entries in an ARP table are time-stamped and are purged after the timeout expires.
- ARP replies are broadcast on the network when a host receives an ARP request.

**68. What property of ARP causes the NICs receiving an ARP request to pass the data portion of the Ethernet frame to the ARP process?**

- **The type field 0x806 appears in the header of the Ethernet frame.**
- The destination MAC address FF-FF-FF-FF-FF-FF appears in the header of the Ethernet frame.
- Entries in an ARP table are time-stamped and are purged after the timeout expires.
- The port-to-MAC address table on a switch has the same entries as the ARP table on the switch.

**69.**

```

Main(config)# interface gi0/1
Main(config-if)# description Connects to the Service LAN
Main(config-if)# ip address 172.29.157.156 255.255.255.0
Main(config-if)# no shutdown
Main(config-if)# interface gi0/0
Main(config-if)# description Connects to the Engineering LAN
Main(config-if)# ip address 172.29.156.36 255.255.255.0
Main(config-if)# no shutdown
Main(config-if)# interface s0/0/0
Main(config-if)# description Connects to the ISP
Main(config-if)# ip address 10.156.157.254 255.255.255.0
Main(config-if)# no shutdown
Main(config-if)# interface s0/0/1
Main(config-if)# description Connects to the Head Office WAN
Main(config-if)# ip address 198.51.100.177 255.255.255.0
Main(config-if)# no shutdown

```

Main(config-if)# end

**Refer to the exhibit. A network administrator is connecting a new host to the Service LAN. The host needs to communicate with remote networks. What IP address would be configured as the default gateway on the new host?**

- **172.29.157.156**
- 172.29.157.1
- 10.156.157.254
- 198.51.100.177
- 172.29.156.36

**70.**

```
BldgA(config)# interface gi0/1
BldgA(config-if)# description Connects to the Medical LAN
BldgA(config-if)# ip address 192.168.191.189 255.255.255.0
BldgA(config-if)# no shutdown
BldgA(config-if)# interface gi0/0
BldgA(config-if)# description Connects to the Client LAN
BldgA(config-if)# ip address 192.168.190.70 255.255.255.0
BldgA(config-if)# no shutdown
BldgA(config-if)# interface s0/0/0
BldgA(config-if)# description Connects to the ISP
BldgA(config-if)# ip address 10.190.191.254 255.255.255.0
BldgA(config-if)# no shutdown
BldgA(config-if)# interface s0/0/1
BldgA(config-if)# description Connects to the Head Office WAN
BldgA(config-if)# ip address 198.51.100.213 255.255.255.0
BldgA(config-if)# no shutdown
BldgA(config-if)# end
```

**Refer to the exhibit. A network administrator is connecting a new host to the Medical LAN. The host needs to communicate with remote networks. What IP address would be configured as the default gateway on the new host?**

- **192.168.191.189**
- 192.168.191.1
- 10.190.191.254
- 198.51.100.213
- 192.168.190.70

**71.**

```
Floor(config)# interface gi0/1
Floor(config-if)# description Connects to the Registrar LAN
Floor(config-if)# ip address 192.168.225.223 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# interface gi0/0
Floor(config-if)# description Connects to the Manager LAN
Floor(config-if)# ip address 192.168.224.103 255.255.255.0
```

```

Floor(config-if)# no shutdown
Floor(config-if)# interface s0/0/0
Floor(config-if)# description Connects to the ISP
Floor(config-if)# ip address 10.224.225.254 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# interface s0/0/1
Floor(config-if)# description Connects to the Head Office WAN
Floor(config-if)# ip address 203.0.113.246 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# end

```

**Refer to the exhibit. A network administrator is connecting a new host to the Registrar LAN. The host needs to communicate with remote networks. What IP address would be configured as the default gateway on the new host?**

- **192.168.225.223**
- 192.168.225.1
- 10.224.225.254
- 203.0.113.246
- 192.168.224.103

**72.**

```

Floor(config)# interface gi0/1
Floor(config-if)# description Connects to the Registrar LAN
Floor(config-if)# ip address 10.118.63.65 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# interface gi0/0
Floor(config-if)# description Connects to the Manager LAN
Floor(config-if)# ip address 10.118.62.196 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# interface s0/0/0
Floor(config-if)# description Connects to the ISP
Floor(config-if)# ip address 10.62.63.254 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# interface s0/0/1
Floor(config-if)# description Connects to the Head Office WAN
Floor(config-if)# ip address 209.165.200.87 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# end

```

**Refer to the exhibit. A network administrator is connecting a new host to the Manager LAN. The host needs to communicate with remote networks. What IP address would be configured as the default gateway on the new host?**

- **10.118.62.196**
- 10.118.62.1
- 10.62.63.254
- 209.165.200.87
- 10.118.63.65

**73.**

```
HQ(config)# interface gi0/1
HQ(config-if)# description Connects to the Branch LAN
HQ(config-if)# ip address 172.19.99.99 255.255.255.0
HQ(config-if)# no shutdown
HQ(config-if)# interface gi0/0
HQ(config-if)# description Connects to the Store LAN
HQ(config-if)# ip address 172.19.98.230 255.255.255.0
HQ(config-if)# no shutdown
HQ(config-if)# interface s0/0/0
HQ(config-if)# description Connects to the ISP
HQ(config-if)# ip address 10.98.99.254 255.255.255.0
HQ(config-if)# no shutdown
HQ(config-if)# interface s0/0/1
HQ(config-if)# description Connects to the Head Office WAN
HQ(config-if)# ip address 209.165.200.120 255.255.255.0
HQ(config-if)# no shutdown
HQ(config-if)# end
```

**Refer to the exhibit. A network administrator is connecting a new host to the Store LAN. The host needs to communicate with remote networks. What IP address would be configured as the default gateway on the new host?**

- **172.19.98.230**
- 172.19.98.1
- 10.98.99.254
- 209.165.200.120
- 172.19.99.99

**74.**

```
HQ(config)# interface gi0/1
HQ(config-if)# description Connects to the Branch LAN
HQ(config-if)# ip address 172.20.133.132 255.255.255.0
HQ(config-if)# no shutdown
HQ(config-if)# interface gi0/0
HQ(config-if)# description Connects to the Store LAN
HQ(config-if)# ip address 172.20.132.13 255.255.255.0
HQ(config-if)# no shutdown
HQ(config-if)# interface s0/0/0
HQ(config-if)# description Connects to the ISP
HQ(config-if)# ip address 10.132.133.254 255.255.255.0
HQ(config-if)# no shutdown
HQ(config-if)# interface s0/0/1
HQ(config-if)# description Connects to the Head Office WAN
HQ(config-if)# ip address 198.51.100.156 255.255.255.0
HQ(config-if)# no shutdown
HQ(config-if)# end
```

**Refer to the exhibit. A network administrator is connecting a new host to the Store LAN. The host needs to communicate with remote networks. What IP address would be configured as the default gateway on the new host?**

- **172.20.132.13**
- 172.20.132.1
- 10.132.133.254
- 198.51.100.156
- 172.20.133.132

**75.**

```
Main(config)# interface gi0/1
Main(config-if)# description Connects to the Service LAN
Main(config-if)# ip address 192.168.167.166 255.255.255.0
Main(config-if)# no shutdown
Main(config-if)# interface gi0/0
Main(config-if)# description Connects to the Engineering LAN
Main(config-if)# ip address 192.168.166.46 255.255.255.0
Main(config-if)# no shutdown
Main(config-if)# interface s0/0/0
Main(config-if)# description Connects to the ISP
Main(config-if)# ip address 10.166.167.254 255.255.255.0
Main(config-if)# no shutdown
Main(config-if)# interface s0/0/1
Main(config-if)# description Connects to the Head Office WAN
Main(config-if)# ip address 198.51.100.189 255.255.255.0
Main(config-if)# no shutdown
Main(config-if)# end
```

**Refer to the exhibit. A network administrator is connecting a new host to the Service LAN. The host needs to communicate with remote networks. What IP address would be configured as the default gateway on the new host?**

- **192.168.167.166**
- 192.168.167.1
- 10.166.167.254
- 198.51.100.189
- 192.168.166.46

**76.**

```
BldgA(config)# interface gi0/1
BldgA(config-if)# description Connects to the Medical LAN
BldgA(config-if)# ip address 192.168.201.200 255.255.255.0
BldgA(config-if)# no shutdown
BldgA(config-if)# interface gi0/0
BldgA(config-if)# description Connects to the Client LAN
BldgA(config-if)# ip address 192.168.200.80 255.255.255.0
BldgA(config-if)# no shutdown
BldgA(config-if)# interface s0/0/0
```



```
BldgA(config-if)# description Connects to the ISP
BldgA(config-if)# ip address 10.200.201.254 255.255.255.0
BldgA(config-if)# no shutdown
BldgA(config-if)# interface s0/0/1
BldgA(config-if)# description Connects to the Head Office WAN
BldgA(config-if)# ip address 203.0.113.222 255.255.255.0
BldgA(config-if)# no shutdown
BldgA(config-if)# end
```

**Refer to the exhibit. A network administrator is connecting a new host to the Medical LAN. The host needs to communicate with remote networks. What IP address would be configured as the default gateway on the new host?**

- **192.168.201.200**
- 192.168.201.1
- 10.200.201.254
- 203.0.113.222
- 192.168.200.80

## IV. MODULE 11-13

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

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

**Explanation:** 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.

**2. How many valid host addresses are available on an IPv4 subnet that is configured with a /26 mask?**

- 254
- 190
- 192
- **62**
- 64

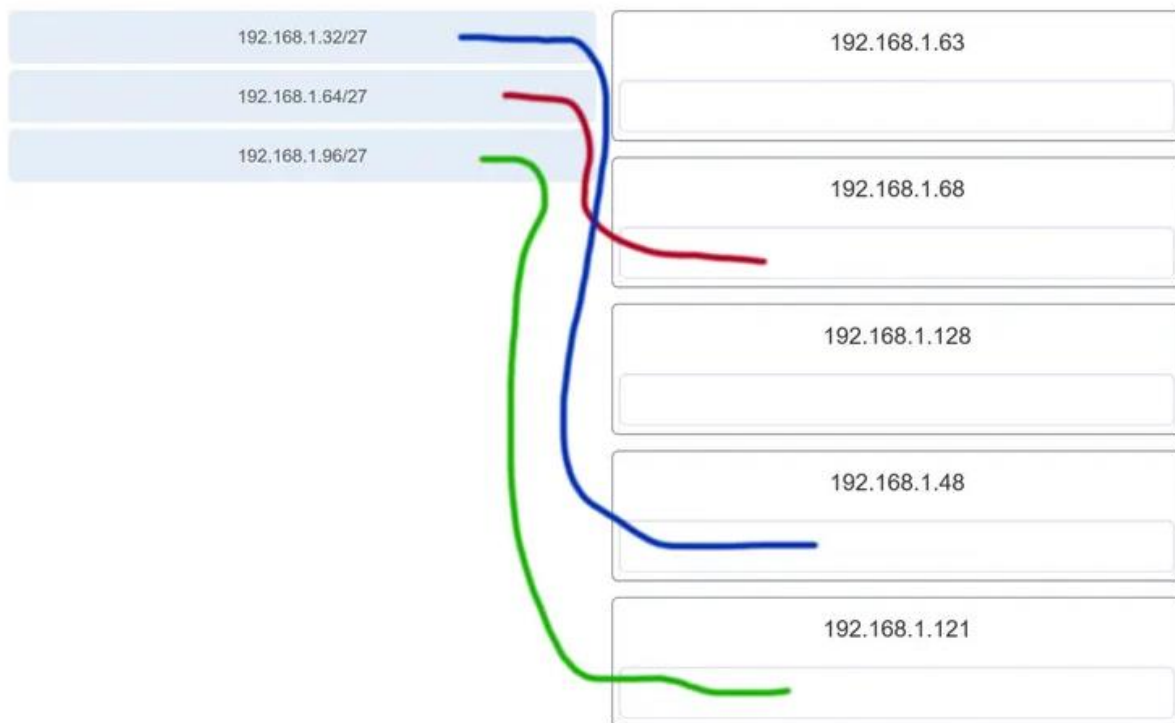
**3. Which subnet mask would be used if 5 host bits are available?**

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

4. 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

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



**Explanation:** 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

6. 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

**Explanation:** 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

**7. 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

$$2^3 = 8$$

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

**8. How many host addresses are available on the 192.168.10.128/26 network?**

- 30
- 32
- 60
- **62**
- 64

$$2^6 - 2$$

**Explanation:** A /26 prefix gives 6 host bits, which provides a total of 64 addresses, because  $2^6 = 64$ . Subtracting the network and broadcast addresses leaves 62 usable host addresses.

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

$$2^{10} - 2$$

10 bits are borrowed

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

**Explanation:** 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 ( $2^{10} - 2 = 1022$ ).

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



**11. What three blocks of addresses are defined by RFC 1918 for private network use? (Choose three.)**

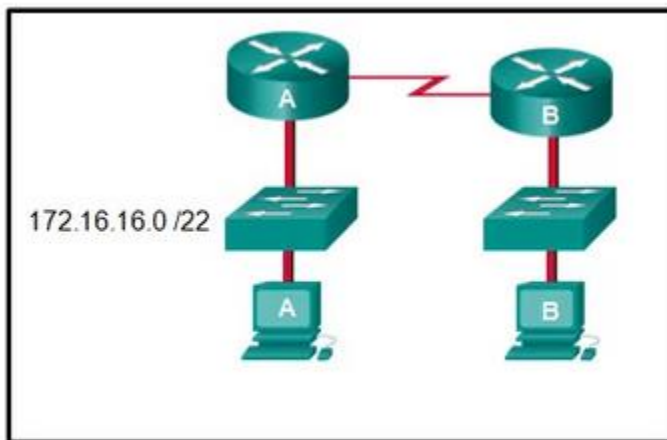
- **10.0.0.0/8**
- **172.16.0.0/12**
- **192.168.0.0/16**
- 100.64.0.0/14
- 169.254.0.0/16
- 239.0.0.0/8

*Handwritten in red:*  
 10/8  
 172/12  
 192/16

**Explanation:** RFC 1918, Address Allocation for Private Internets, defines three blocks of IPv4 address for private networks that should not be routable on the public Internet.

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

**12. Refer to the exhibit. An administrator must send a message to everyone on the router A network. What is the broadcast address for network 172.16.16.0/22?**



change 1024 to subnet mask 255.255.252.0

$$255 - 252 = 3$$

$$3 + 16 = 19$$

broadcast address = last address - > 255

172.16.19.255

- 172.16.16.255
- 172.16.20.255
- **172.16.19.255**
- 172.16.23.255
- 172.16.255.255

**Explanation:** The 172.16.16.0/22 network has 22 bits in the network portion and 10 bits in the host portion. Converting the network address to binary yields a subnet mask of 255.255.252.0. The range of addresses in this network will end with the last address available before 172.16.20.0. Valid host addresses for this network range from 172.16.16.1-172.16.19.254, making 172.16.19.255 the broadcast address.

**13. A site administrator has been told that a particular network at the site must accommodate 126 hosts. Which subnet mask would be used that contains the required number of host bits?**

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

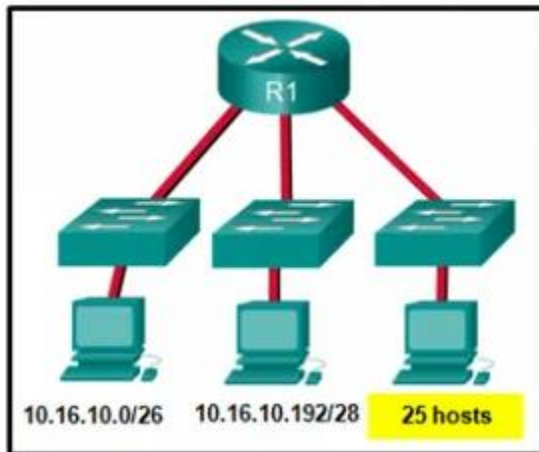
$$n = 7$$

$$256 - 2^n$$

**Explanation:** 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.

**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?**

25 host  $\rightarrow n = 5 \Rightarrow /27$



- 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

**Explanation:** 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 and 10.16.10.128/26. 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. What is the usable number of host IP addresses on a network that has a /26 mask?**

- 256
- 254

$$2^{n-2}$$

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

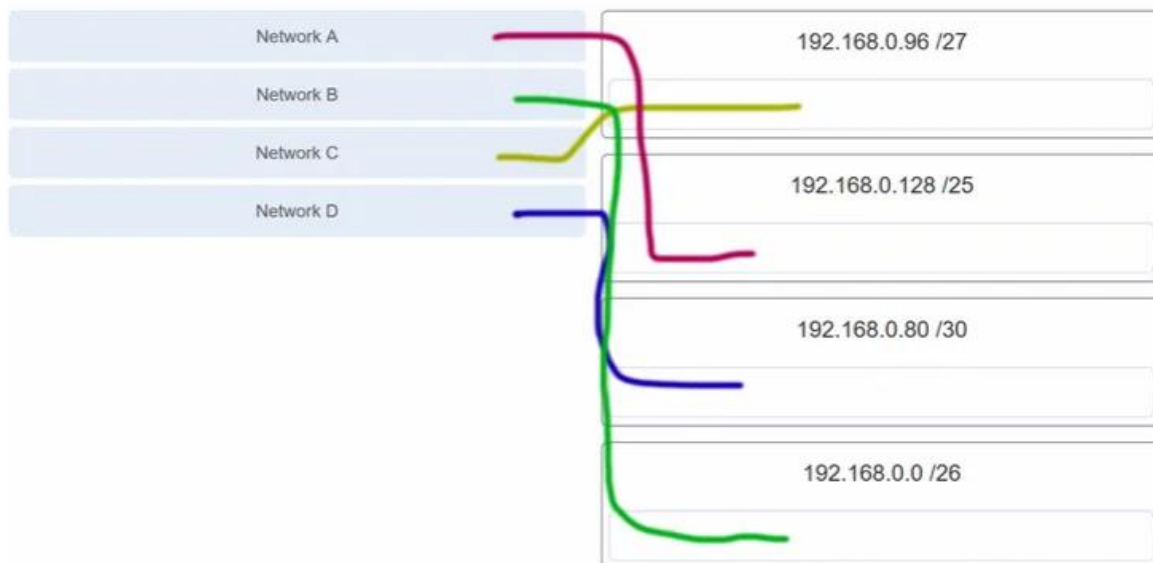
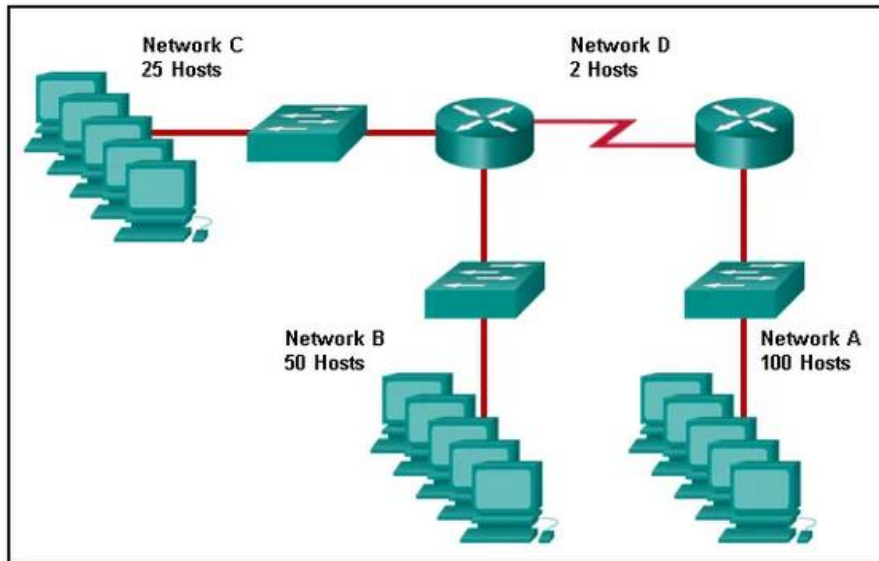
**Explanation:** A /26 mask is the same as 255.255.255.192. The mask leaves 6 host bits. With 6 host bits, 64 IP addresses are possible. One address represents the subnet number and one address represents the broadcast address, which means that 62 addresses can then be used to assign to network devices.

**16. Which address prefix range is reserved for IPv4 multicast?**

- 240.0.0.0 – 254.255.255.255
- **224.0.0.0 – 239.255.255.255** 224 -239
- 169.254.0.0 – 169.254.255.255
- 127.0.0.0 – 127.255.255.255

**Explanation:** Multicast IPv4 addresses use the reserved class D address range of 224.0.0.0 to 239.255.255.255.

**17. Refer to the exhibit. Match the network with the correct IP address and prefix that will satisfy the usable host addressing requirements for each network.**



**Explanation:** Network A needs to use 192.168.0.128 /25, which yields 128 host addresses.

Network B needs to use 192.168.0.0 /26, which yields 64 host addresses.

Network C needs to use 192.168.0.96 /27, which yields 32 host addresses.

Network D needs to use 192.168.0.80 /30, which yields 4 host addresses.

**18. A high school in New York (school A) is using videoconferencing technology to establish student interactions with another high school (school B) in Russia. The videoconferencing is conducted between two end devices through the Internet. The network administrator of school A configures the end device with the IP address 209.165.201.10. The administrator sends a request for the IP address for the end device in school B and the response is 192.168.25.10. Neither**



school is using a VPN. The administrator knows immediately that this IP will not work. Why?

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

19. Which three addresses are **valid public addresses**? (Choose three.)

- **198.133.219.17**
- 192.168.1.245
- 10.15.250.5
- **128.107.12.117**
- 172.31.1.25
- **64.104.78.227**

**Explanation:** The ranges of **private IPv4 addresses** are as follows:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

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

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

**Explanation:** 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.

21. 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

**Explanation:** 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.

## 22. Which address is a valid IPv6 link-local unicast address?

- FEC8:1::FFFF
- FD80::1:1234
- **FE80::1:4545:6578:ABC1**
- FE0A::100:7788:998F
- FC90:5678:4251:FFFF

**Explanation:** IPv6 LLAs are in the fe80::/10 range. The /10 indicates that the first 10 bits are 1111 1110 10xx xxxx. The first hextet has a range of 1111 1110 1000 0000 (fe80) to 1111 1110 1011 1111 (febf).

## 23. 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~~

**Explanation:** The rules for reducing the notation of IPv6 addresses are:

1. Omit any leading 0s (zeros) in any hextet.
2. Replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros with a double colon (::) .
3. The double colon (::) can only be used once within an address.

## 24. 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**
- $64 - 48 = 16$   
 $2^{16} = 65536$

**Explanation:** 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.

**25. Given IPv6 address prefix 2001:db8::/48, what will be the last subnet that is created if the subnet prefix is changed to /52?**

- 2001:db8:0:f00::/52
  - 2001:db8:0:8000::/52
  - 2001:db8:0:f::/52
  - **2001:db8:0:f000::/52**
- $52 - 48 = 4$   
 $2^4 = 16$

**Explanation:** Prefix 2001:db8::/48 has 48 network bits. If we subnet to a /52, we are moving the network boundary four bits to the right and creating 16 subnets. The first subnet is 2001:db8::/52 the last subnet is 2001:db8:0:f000::/52.

**26. 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 .**

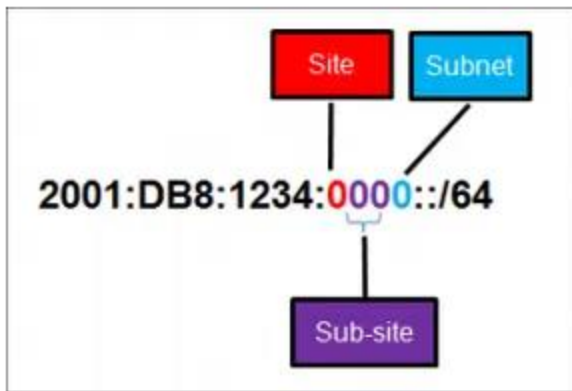
**Explanation:** All the addresses have the part 2001:0DB8:BC15:00A in common. Each number or letter in the address represents 4 bits, so the prefix-length is /60.

**27. What type of IPv6 address is FE80::1?**

- loopback
- **link-local**
- multicast
- global unicast

**Explanation:** Link-local IPv6 addresses start with FE80::/10, which is any address from FE80:: to FEBF::. Link-local addresses are used extensively in IPv6 and allow directly connected devices to communicate with each other on the link they share.

**28. 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?**



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

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

29. What is used in the **EUI-64 process** to create an IPv6 interface ID on an IPv6 enabled interface?

- **the MAC address of the IPv6 enabled interface**
- a randomly generated 64-bit hexadecimal address
- an IPv6 address that is provided by a DHCPv6 server
- an IPv4 address that is configured on the interface

**Explanation:** The EUI-64 process uses the MAC address of an interface to construct an interface ID (IID). Because the MAC address is only 48 bits in length, 16 additional bits (FF:FE) must be added to the MAC address to create the full 64-bit interface ID.

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

- 2001:DB8:BC15
- **2001:DB8:BC15:A** first 64 bits
- 2001:DB8:BC15:A:1
- 2001:DB8:BC15:A:12

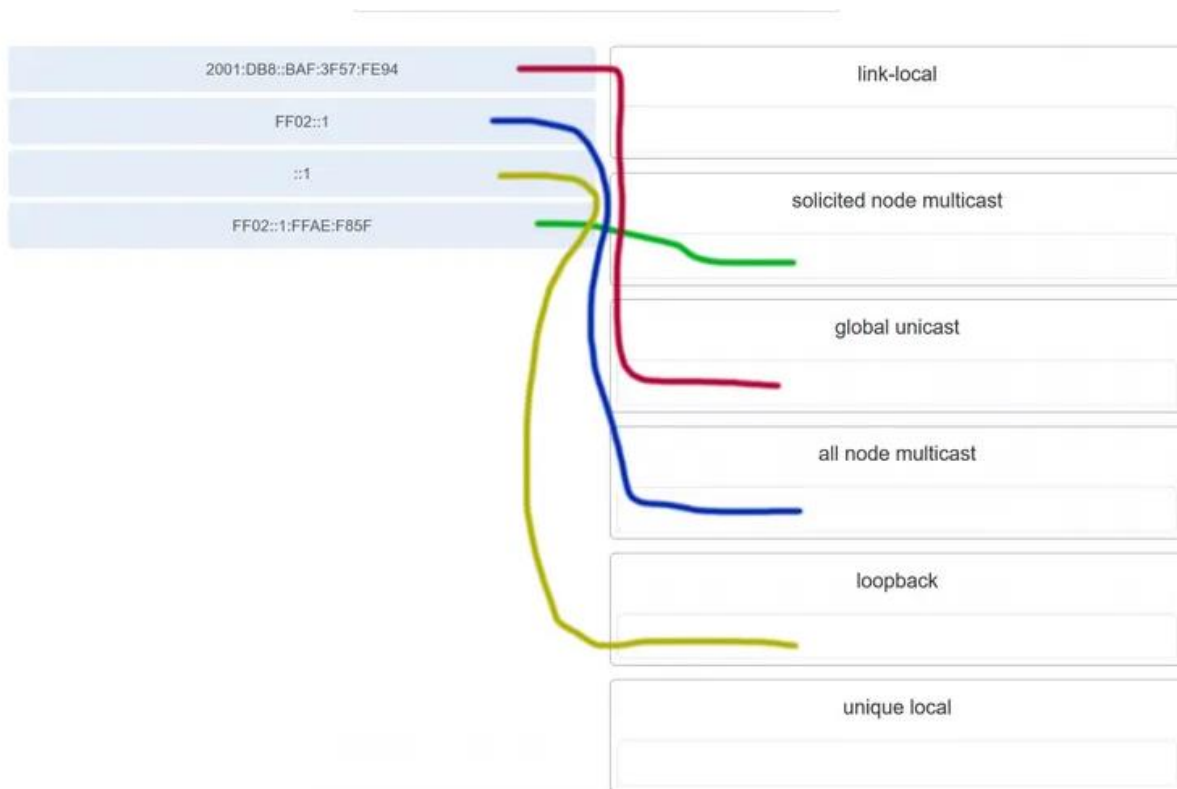
**Explanation:** The network portion, or prefix, of an IPv6 address is identified through the prefix length. A /64 prefix length indicates that the first 64 bits of the IPv6 address is the network portion. Hence the prefix is 2001:DB8:BC15:A.

**31. 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

**Explanation:** 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.

**32. Match the IPv6 address with the IPv6 address type. (Not all options are used.)**



**Explanation:** 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.

**33. Which IPv6 prefix is reserved for communication between devices on the same link?**

- FC00::/7
- 2001::/32
- **FE80::/10**
- FFFF::/7

**Explanation:** IPv6 link-local unicast addresses are in the FE80::/10 prefix range and are not routable. They are used only for communications between devices on the same link.

**34. Which type of IPv6 address refers to any unicast address that is assigned to multiple hosts?**

- unique local
- global unicast
- link-local
- **anycast**

**Explanation:** The IPv6 specifications include anycast addresses. An anycast address is any unicast IPv6 address that is assigned to multiple devices.

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

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

**Explanation:** 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.

**36. Which service provides dynamic global IPv6 addressing to end devices without using a server that keeps a record of available IPv6 addresses?**

- stateful DHCPv6
- **SLAAC**
- static IPv6 addressing
- stateless DHCPv6

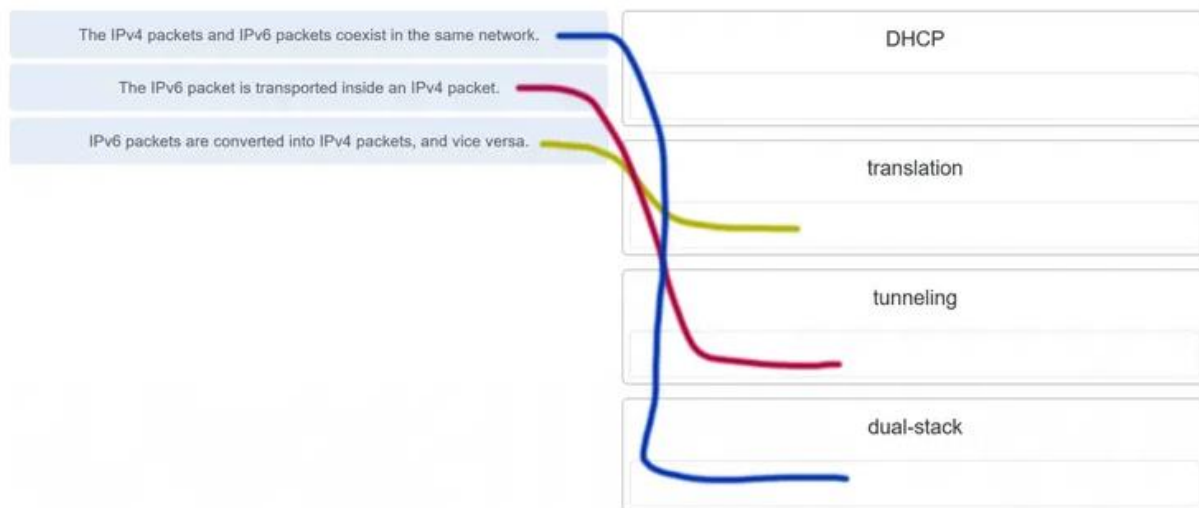
**Explanation:** Using stateless address autoconfiguration (SLAAC), a PC can solicit a router and receive the prefix length of the network. From this information the PC can then create its own IPv6 global unicast address.

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

- ARPv6
- DHCPv6
- **ICMPv6**
- UDP

**Explanation:** 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.

**38. Three methods allow IPv6 and IPv4 to co-exist. Match each method with its description. (Not all options are used.)**

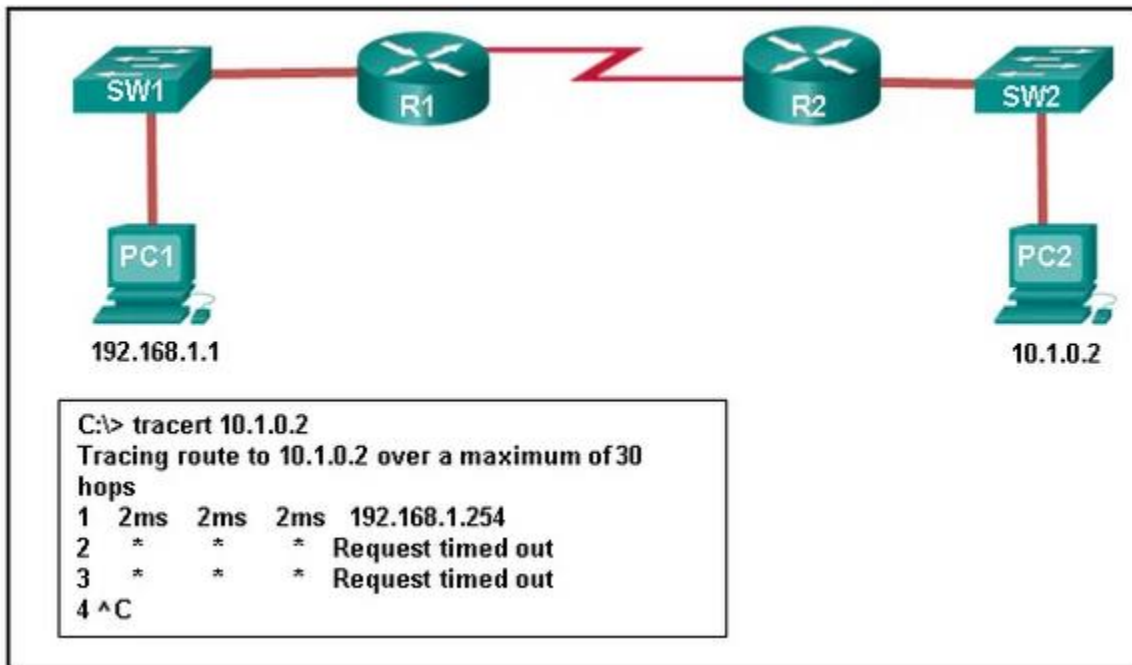


**39. A technician uses the ping 127.0.0.1 command. What is the technician testing?**

- **the TCP/IP stack on a network host**
- connectivity between two adjacent Cisco devices
- connectivity between a PC and the default gateway
- connectivity between two PCs on the same network

- physical connectivity of a particular PC and the network

40. 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

41. Which protocol is used by the traceroute command to send and receive echo-requests and echo-replies?

- SNMP
- **ICMP**
- Telnet
- TCP

**Explanation:** Traceroute uses the ICMP (Internet Control Message Protocol) to send and receive echo-request and echo-reply messages.

42. Which ICMPv6 message is sent when the IPv6 hop limit field of a packet is decremented to zero and the packet cannot be forwarded?



- network unreachable
- **time exceeded**
- protocol unreachable
- port unreachable

**Explanation:** ICMPv6 uses the hop limit field in the IPv6 packet header to determine if the packet has expired. If the hop limit field has reached zero, a router will send a time exceeded message back towards the source indicating that the router cannot forward the packet.

**43. A user executes a traceroute over IPv6. At what point would a router in the path to the destination device drop the packet?**

- when the value of the Hop Limit field reaches 255
- **when the value of the Hop Limit field reaches zero**
- when the router receives an ICMP time exceeded message
- when the target host responds with an ICMP echo reply message

**Explanation:** When a traceroute is performed, the value in the Hop Limit field of an IPv6 packet determines how many router hops the packet can travel. Once the Hop Limit field reaches a value of zero, it can no longer be forwarded and the receiving router will drop the packet.

**44. 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

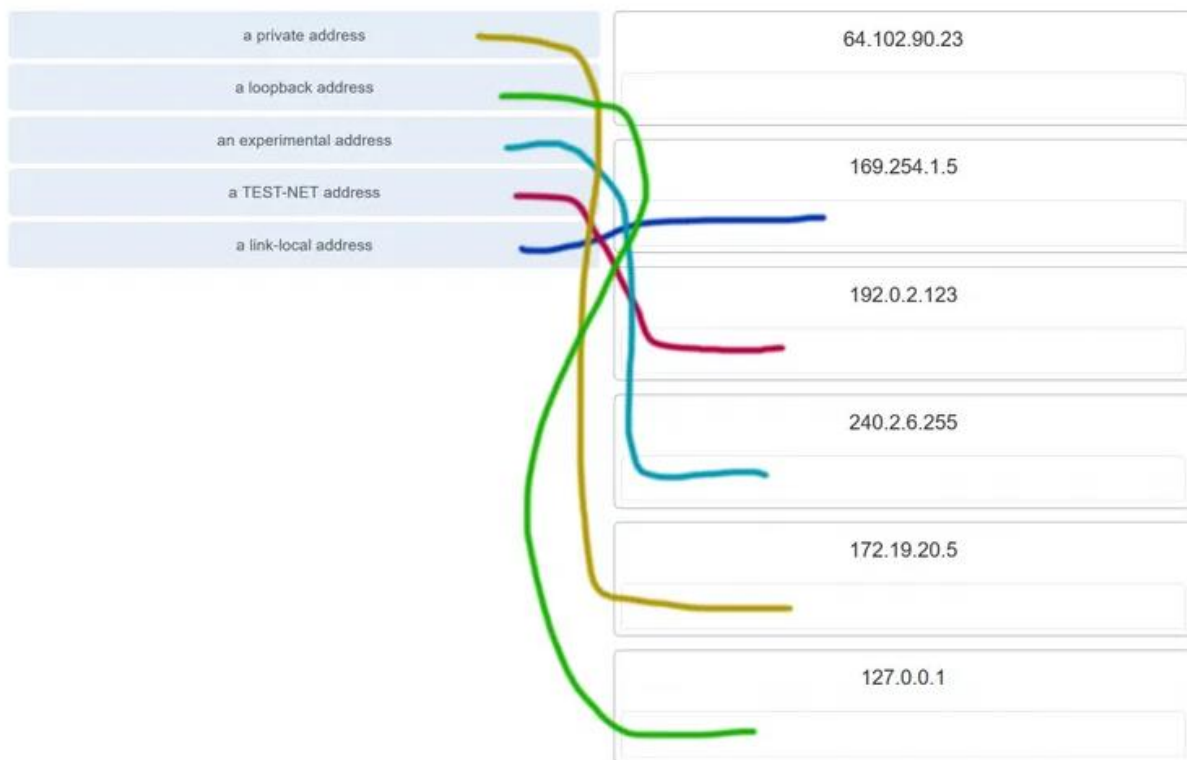
**Explanation:** The purpose of ICMP messages is to provide feedback about issues that are related to the processing of IP packets.

**45. What source IP address does a router use by default when the traceroute command is issued?**

- the highest configured IP address on the router
- a loopback IP address
- **the IP address of the outbound interface**
- the lowest configured IP address on the router

**Explanation:** When sending an echo request message, a router will use the IP address of the exit interface as the source IP address. This default behavior can be changed by using an extended ping and specifying a specific source IP address.

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



**Explanation:** 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.

47. A user issues a ping 192.135.250.103 command and receives a response that includes a code of 1. What does this code represent?

- **host unreachable**
- protocol unreachable
- port unreachable
- network unreachable

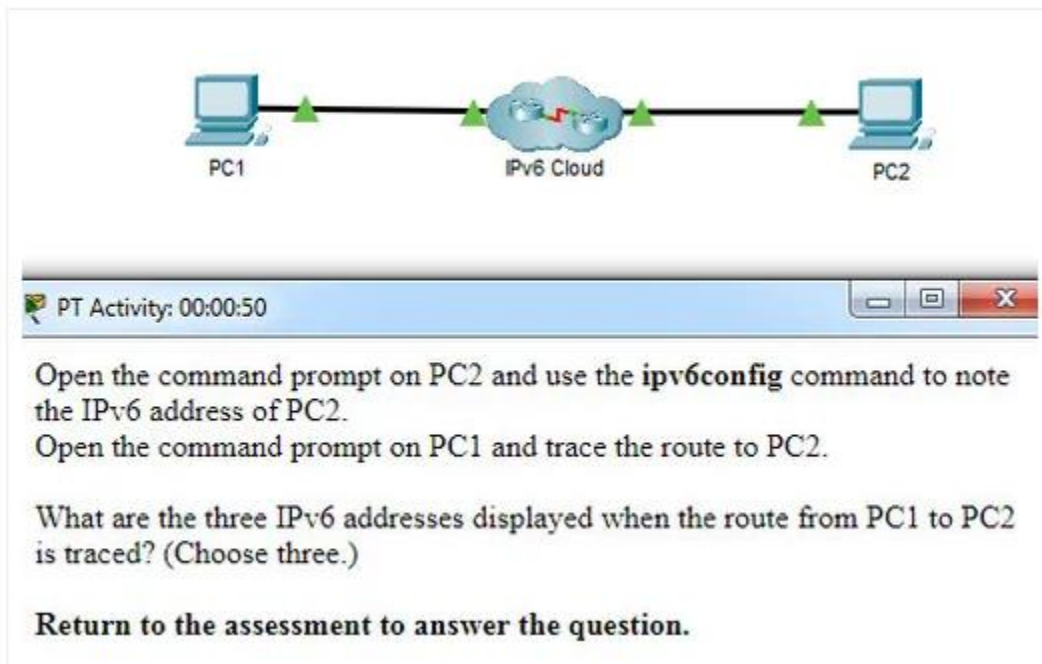
48. Which subnet would include the address 192.168.1.96 as a usable host address?

- **192.168.1.64/26**
- 192.168.1.32/27
- 192.168.1.32/28

- 192.168.1.64/29

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

**49. Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.**



PT Activity: 00:00:50

Open the command prompt on PC2 and use the **ipv6config** command to note the IPv6 address of PC2.

Open the command prompt on PC1 and trace the route to PC2.

What are the three IPv6 addresses displayed when the route from PC1 to PC2 is traced? (Choose three.)

**Return to the assessment to answer the question.**

**What are the three IPv6 addresses displayed when the route from PC1 to PC2 is traced? (Choose three.)**

- **2001:DB8:1:1::1**
- 2001:DB8:1:1::A
- 2001:DB8:1:2::2
- **2001:DB8:1:2::1**
- 2001:DB8:1:3::1
- **2001:DB8:1:3::2**
- 2001:DB8:1:4::1

**Explanation:** Using the **ipv6config** command on PC2 displays the IPv6 address of PC2, which is 2001:DB8:1:4::A. The IPV6 link-local address, FE80::260:70FF:FE34:6930, is not used in route tracing. Using the **tracert**

**2001:DB8:1:4::A** command on PC1 displays four addresses: 2001:DB8:1:1::1, 2001:DB8:1:2::1, 2001:DB8:1:3::2, and 2001:DB8:1:4::A.

**50. A host is transmitting a **broadcast**. Which host or hosts will receive it?**

- **all hosts in the same subnet**
- a specially defined group of hosts
- the closest neighbor on the same network
- all hosts on the Internet

**Explanation:** A **broadcast is delivered to every host that has an IP address within** the same network.

**51. A host is transmitting a unicast. Which host or hosts will receive it?**

- **one specific host**
- a specially defined group of hosts
- all hosts on the Internet
- the closest neighbor on the same network

**52. A user issues a ping 2001:db8:FACE:39::10 command and receives a response that includes a code of 3. What does this code represent?**

- **address unreachable**
- network unreachable
- host unreachable
- protocol unreachable

**53. A host is transmitting a **multicast**. Which host or hosts will receive it?**

- **a specially defined group of hosts**
- the closest neighbor on the same network
- one specific host
- directly connected network devices

**60. Which is the compressed format of the IPv6 address 2001:0db8:0000:0000:a0b0:0008:0001?**

- **2001:db8::a0b0:8:1**
- 2001:db8::ab8:1:0:1000
- 2001:db80:0:1::80:1
- 2001:db80:::1::80:1

**61. Which is the compressed format of the IPv6 address fe80:09ea:0000:2200:0000:0000:0fe0:0290?**

- **fe80:9ea:0:2200::fe0:290**
- fe80:9:20::b000:290
- fe80:9ea0::2020:0:bf:e0:9290
- fe80:9ea0::2020::bf:e0:9290

**62. Which is the compressed format of the IPv6 address 2002:0042:0010:c400:0000:0000:0000:0909?**

- **2002:42:10:c400::909**
- 200:420:110:c4b::910:0:90
- 2002:4200::25:1090:0:99
- 2002:42::25:1090:0:99

**63. Which is the compressed format of the IPv6 address 2001:0db8:0000:0000:0ab8:0001:0000:1000?**

- **2001:db8::ab8:1:0:1000**
- 2001:db8::a0b0:8:1
- 2001:db8:1::ab8:0:1
- 2001:db8:0:1::8:1

**64. Which is the compressed format of the IPv6 address 2002:0420:00c4:1008:0025:0190:0000:0990?**

- **2002:420:c4:1008:25:190::990**
- 2002:42:10:c400::909
- 2002:4200::25:1090:0:99
- 2002:42::25:1090:0:99

**65. Which is the compressed format of the IPv6 address 2001:0db8:0000:0000:0000:a0b0:0008:0001?**

- **2001:db8::a0b0:8:1**
- 2001:db8:1::ab8:0:1
- 2001:db8::ab8:1:0:1000
- 2001:db8:0:1::8:1

**66. Which is the compressed format of the IPv6 address fe80:0000:0000:0000:0220:0b3f:f0e0:0029?**

- **fe80::220:b3f:f0e0:29**
- fe80:9ea:0:2200::fe0:290
- fe80:9ea0::2020:0:bf:e0:9290

- fe80:9ea0::2020::bf:e0:9290

67. Which is the compressed format of the IPv6 address 2001:0db8:0000:0000:0000:a0b0:0008:0001?

- **2001:db8::a0b0:8:1**
- 2001:db8::ab8:1:0:1000
- 2001:db80:0:1::80:1
- 2001:db8:0:1::8:1

68. Which is the compressed format of the IPv6 address 2002:0042:0010:c400:0000:0000:0000:0909?

- **2002:42:10:c400::909**
- 2002:4200::25:1090:0:99
- 2002:420:c4:1008:25:190::990
- 2002:42::25:1090:0:99

69. Which is the compressed format of the IPv6 address fe80:09ea:0000:2200:0000:0000:0fe0:0290?

- **fe80:9ea:0:2200::fe0:290**
- fe80:9ea0::2020:0:bf:e0:9290
- fe80::220:b3f:f0e0:29
- fe80::0220:0b3f:f0e0:0029

70. A user issues a ping 2001:db8:FACE:39::10 command and receives a response that includes a **code of 2** . What does this code represent?

- **beyond scope of the source address**
- communication with the destination administratively prohibited
- address unreachable
- no route to destination

71. A user issues a ping 192.135.250.103 command and receives a response that includes a code of 1 . What does this code represent?

- **host unreachable**
- beyond scope of the source address
- address unreachable
- communication with the destination administratively prohibited

72. A user issues a ping fe80:65ab:dcc1::100 command and receives a response that includes a code of 3. What does this code represent?

- **address unreachable**
- communication with the destination administratively prohibited
- beyond scope of the source address
- no route to destination

73. A user issues a ping 10.10.14.67 command and receives a response that includes a **code of 0**. What does this code represent?

- **network unreachable**
- protocol unreachable
- port unreachable
- host unreachable

74. A user issues a ping fe80:65ab:dcc1::100 command and receives a response that includes a code of 4. What does this code represent?

- **port unreachable**
- host unreachable
- protocol unreachable
- network unreachable

75. A user issues a ping 198.133.219.8 command and receives a response that includes a code of 0 . What does this code represent?

- **network unreachable**
- protocol unreachable
- port unreachable
- host unreachable

76. A user issues a ping 2001:db8:3040:114::88 command and receives a response that includes a code of 4 . What does this code represent?

- **port unreachable**
- host unreachable
- protocol unreachable
- network unreachable

77. A user issues a ping 2001:db8:FACE:39::10 command and receives a response that includes a code of 2. What does this code represent?

- **beyond scope of the source address**
- host unreachable
- protocol unreachable

- network unreachable

## V. MODULE 14-15

1. Which action is performed by a client when **establishing communication with a server** via the use of **UDP at the transport layer**?

- The client sets the window size for the session.
- The client sends an ISN to the server to start the 3-way handshake.
- **The client randomly selects a source port number.**
- The client sends a synchronization segment to begin the session.

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

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

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

- 0 to 255
- **0 to 1023** range tcp -udp: 0 - 1023
- 256 – 1023
- 1024 – 49151

192.168.1.10:54321

4. What is a **socket**? source IP(or destination IP) : port number

- 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

5. 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**  $1000/100 = 10$
- 100 segments



- 1000 segments

**Explanation:** 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.

**6. Which factor determines TCP window size?** amount of data destination can process

- 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

**Explanation:** 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.

**7. 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.

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

**8. Which three fields are used in a UDP segment header? (Choose three.)**

- Window Size
- **Length**
- **Source Port**
- Acknowledgment Number
- **Checksum**
- Sequence Number

**Explanation:** A UDP header consists of only the **Source Port, Destination Port, Length, and Checksum fields**. Sequence Number, Acknowledgment Number, and Window Size are TCP header fields.

**9. What are two roles of the transport layer in data communication on a network? (Choose two.)**

- **identifying the proper application for each communication stream**
- **tracking the individual communication between applications on the source and destination hosts**
- providing frame delimiting to identify bits making up a frame
- performing a cyclic redundancy check on the frame for errors
- providing the interface between applications and the underlying network over which messages are transmitted

**Explanation:** The transport layer has several responsibilities. The primary responsibilities include the following:

- Tracking the individual communication streams between applications on the source and destination hosts
- Segmenting data at the source and reassembling the data at the destination
- Identifying the proper application for each communication stream through the use of port numbers

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

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

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

destination, source port

**11. What **important information** is **added to the TCP/IP transport layer header** to **ensure communication and connectivity with a remote network device**?**

- timing and synchronization
- **destination and source port numbers**
- destination and source physical addresses
- destination and source logical network addresses

**12. 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.

**Explanation:**

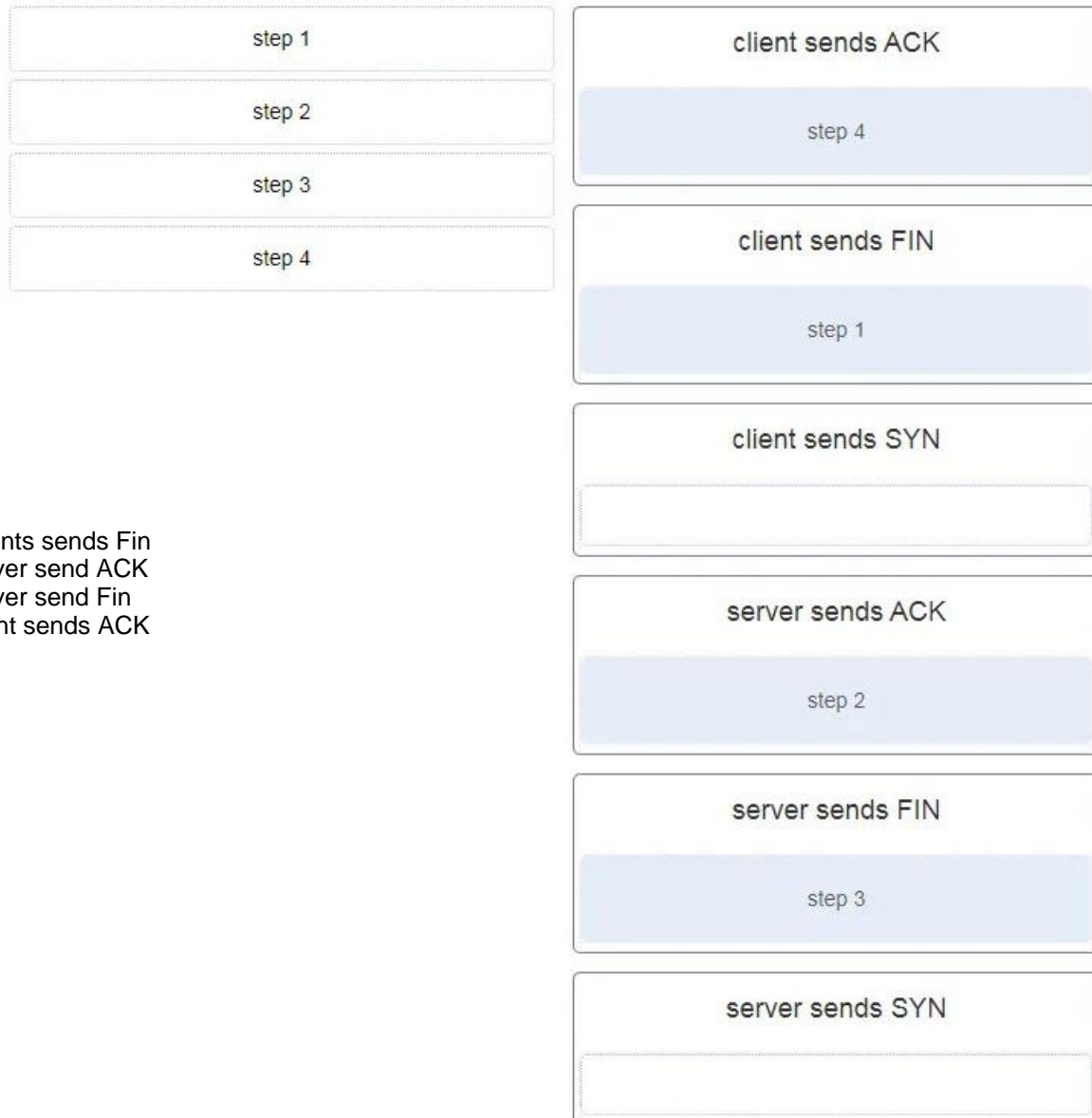
TCP:

- 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.

**13. A client application needs to terminate a TCP communication session with a server. Place the termination process steps in the order that they will occur. (Not all options are used.)**



**Explanation:** In order to terminate a TCP session, the client sends to the server a segment with the FIN flag set. The server acknowledges the client by sending a segment with the ACK flag set. The server sends a FIN to the client to terminate the server to client session. The client acknowledges the termination by sending a segment with the ACK flag set.

**14. 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

**Explanation:** 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.

**15. Which protocol or service uses UDP for a client-to-server communication and TCP for server-to-server communication?**

- HTTP
- FTP
- **DNS**
- SMTP

**Explanation:** Some applications may use both TCP and UDP. DNS uses UDP when clients send requests to a DNS server, and TCP when two DNS servers directly communicate.

**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.

**Explanation:** 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 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

**Explanation:** 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.

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

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

**Explanation:** 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.**

**19. Which three statements characterize **UDP**? (Choose three.)**

connectionless  
error detection -> UDP  
low overhead

- **UDP provides basic **connectionless** transport layer functions.**
- UDP provides connection-oriented, fast transport of data at Layer 3.
- **UDP relies on application layer protocols for **error detection**.**
- **UDP is a **low overhead** protocol that does not provide sequencing or flow control mechanisms.**
- UDP relies on IP for error detection and recovery.
- UDP provides sophisticated flow control mechanisms.

**Explanation:** UDP is a simple protocol that provides the basic transport layer functions. It has much **lower overhead** than TCP because it is **not connection-oriented** and does not offer the sophisticated retransmission, sequencing, and flow control mechanisms that provide reliability.

**20. Which two fields are included **in the TCP header but not in the UDP header**? (Choose two.)**

- **window**
- checksum
- source port
- destination port
- **sequence number**

**Explanation:** The **sequence number and window fields are included in the TCP header but not in the UDP header.**

**21. Which field in the TCP header indicates the status of the three-way handshake process?**

- window
- reserved
- checksum
- **control bits**

**Explanation:** The value in the control bits field of the TCP header indicates the progress and status of the connection.

**22. 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**

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

**23. Which two types of applications are best suited for UDP? (Choose two.)**

- applications that need data flow control
- applications that require reliable delivery
- **applications that handle reliability themselves**
- applications that need the reordering of segments
- **applications that can tolerate some data loss, but require little or no delay**

**Explanation:** Applications that can tolerate some data loss, require a simple request and reply, and handle reliability themselves are best suited for UDP. UDP has low overhead and no requirement of reliability. TCP provides services for reliability, controlling data flow, and the reordering of segments.

**24. How are port numbers used in the TCP/IP encapsulation process?**

- Source port numbers and destination port numbers are not necessary when UDP is the transport layer protocol being used for the communication.
- Source port and destination port numbers are randomly generated.
- **If multiple conversations occur that are using the same service, the source port number is used to track the separate conversations.**
- Destination port numbers are assigned automatically and cannot be changed.

**Explanation:** Both UDP and TCP use port numbers to provide a unique identifier for each conversation. Source **port numbers** are randomly generated and are used to **track different conversations**. Destination port numbers identify specific services by using either a default port number for the service or a port number that is assigned manually by a system administrator.

**25. In what two situations would **UDP be better than TCP** as the preferred transport protocol? (Choose two.)**

- when applications need to guarantee that a packet arrives intact, in sequence, and unduplicated
- **when a faster delivery mechanism is needed**
- when delivery overhead is not an issue
- **when applications do not need to guarantee delivery of the data**
- when destination port numbers are dynamic

**Explanation:** UDP is a very simple transport layer protocol that does not guarantee delivery. Devices on both ends of the conversation are not required to keep track of the conversation. UDP is used as the transport protocol for applications that need a speedy, best-effort delivery.

**26. What are three **responsibilities of the transport layer**? (Choose three.)**

- **meeting the reliability requirements of applications, if any**
- **multiplexing multiple communication streams from many users or applications on the same network**
- **identifying the applications and services on the client and server that should handle transmitted data**
- directing packets towards the destination network
- formatting data into a compatible form for receipt by the destination devices
- conducting error detection of the contents in frames

**Explanation:** The transport layer has several responsibilities. Some of the primary responsibilities include the following:

**Tracking the individual communication** streams between applications on the source and destination hosts

**Segmenting data at the source** and reassembling the data at the destination

**Identifying the proper application for each communication** stream through the use of port numbers

Multiplexing the communications of multiple users or applications over a single network

Managing the **reliability requirements of applications**

**27. 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.

**Explanation:** 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.

**28. Which two protocols may devices use in the application process that sends email? (Choose two.)**

- HTTP
- SMTP
- POP
- IMAP
- DNS
- POP3

**Explanation:** POP, POP3, and IMAP are protocols that are used to retrieve email from servers. SMTP is the default protocol that is used to send email. DNS may be used by the sender email server to find the address of the destination email server.

**29. 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.

**Explanation:** 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.

**30. What is the function of the HTTP GET message?**

- to request an HTML page from a web server
- to send error information from a web server to a web client
- to upload content to a web server from a web client
- to retrieve client email from an email server using TCP port 110

**Explanation:** There are three common HTTP message types:

- GET – used by clients to request data from the web server
- POST – used by clients to **upload data** to a web server
- PUT – used by clients to upload data to a web server

**31. Which OSI layer provides the interface between the applications used to communicate and the underlying network over which messages are transmitted?**

- **application**
- presentation
- session
- transport

**Explanation:** The application layer is the layer that is closest to the end user and provides the interface between the underlying network and **the applications used to communicate**.

**32. Which networking model is being used when an author uploads one chapter document to a file server of a book publisher?**

- peer-to-peer
- master-slave
- **client/server**
- point-to-point

**Explanation:** In the **client/server network model**, a network device assumes the role of server in order to **provide a particular service** such as file **transfer and storage**. In the client/server network model, a dedicated server does not have to be used, but if one is present, the network model being used is the client/server model. In contrast, a peer-to-peer network does not have a dedicated server.

**33. 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.

**Explanation:** 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.

**34. In what networking model would eDonkey, eMule, BitTorrent, Bitcoin, and LionShare be used?**

- **peer-to-peer**
- client-based

- master-slave
- point-to-point

**Explanation:** In a peer-to-peer networking model, data is exchanged between two network devices without the use of a dedicated server. Peer-to-peer applications such as Shareaz, eDonkey, and Bitcoin allow one network device to assume the role of server, while one or more other network devices assume the role of client using the peer-to-peer application.

**35. What is a common protocol that is used with peer-to-peer applications such as WireShare, Bearshare, and Shareaza?**

- Ethernet
- **Gnutella**
- POP
- SMTP

**Explanation:** The Gnutella protocol is used when one user shares an entire file with another user. A person would load a Gnutella-based application such as gtk-gnutella or WireShare and use that application to locate and access resources shared by others.

**36. What is a key characteristic of the peer-to-peer networking model?**

- wireless networking
- social networking without the Internet
- network printing using a print server
- **resource sharing without a dedicated server**

**Explanation:** The peer-to-peer (P2P) networking model allows data, printer, and resource sharing without a dedicated server.

**37. 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**

**Explanation:** 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.

**38. 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.**

**Explanation:** 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.

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

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

làm việc với data -> application layer

**Explanation:** 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.

**40. What is an advantage of SMB over FTP?**

- Only with SMB can data transfers occur in both directions.
- Only SMB establishes two simultaneous connections with the client, making the data transfer faster.
- SMB is more reliable than FTP because SMB uses TCP and FTP uses UDP.
- **SMB clients can establish a long-term connection to the server.**

**Explanation:** SMB and FTP are **client/server protocols** that are used for **file transfer**. SMB allows the connecting device to access resources as if they were on the local client device. SMB and FTP use the TCP protocol for connection establishment and they can transfer data in both directions. FTP requires two connections between the client and the server, one for commands and replies, the other for the actual file transfer.

**41. 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**

**Explanation:** 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 is commonly used to manage IP addressing.

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

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

**Explanation:** 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.

**43. What type of information is contained in a DNS MX record?**

- the FQDN of the alias used to identify a service
- the IP address for an FQDN entry
- **the domain name mapped to mail exchange servers**
- the IP address of an authoritative name server

**Explanation:** MX, or mail exchange messages, are used to map a domain name to several mail exchange servers that all belong to the same domain.

**44. Which three protocols operate at the application layer of the TCP/IP model? (Choose three.)**

- ARP
  - TCP
  - UDP
  - **FTP**
  - **POP3**
  - **DHCP**
- application: ftp, pop ,dhcp  
transport : tcp, udp  
network: arp

**Explanation:** FTP, DHCP, and POP3 are application layer protocols. TCP and UDP are transport layer protocols. ARP is a network layer protocol.

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

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

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

**46. Which applications or services allow hosts to act as client and server at the same time?**

- client/server applications
- email applications
- **P2P applications**
- authentication services

**Explanation:** P2P applications allow the **clients to behave as servers** if needed. When using authentication services, email exchange, and client/server applications, one host acts as server and the other acts as client at all times.

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

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

**Explanation:** Peer-to-peer networks have **decentralized resources** because every computer can serve as both a server and a client. One computer might assume the role of server for one transaction while acting as a client for another transaction. Peer-to-peer networks can **share resources among network devices without the use of a dedicated server.**

**48. 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.

**Explanation:** The source and destination port numbers are used to **identify the correct application and window within that application.**

**49. 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

**Explanation:** The three upper layers of the OSI model, the session, presentation, and application layers, provide application services similar to those provided by the TCP/IP model application layer. Lower layers of the OSI model are more concerned with data flow.

50. A PC that is communicating with a web server has a TCP window size of 6,000 bytes when sending data and a packet size of 1,500 bytes. Which byte of information will the web server acknowledge after it has received two packets of data from the PC?

- 3001
  - 6001
  - 4500
  - 6000
- $3000+1$

51. A PC that is communicating with a web server has a TCP window size of 6,000 bytes when sending data and a packet size of 1,500 bytes. Which byte of information will the web server acknowledge after it has received three packets of data from the PC?

- 4501
  - 6001
  - 6000
  - 4500
- $4500+1$

52. A PC that is communicating with a web server has a TCP window size of 6,000 bytes when sending data and a packet size of 1,500 bytes. Which byte of information will the web server acknowledge after it has received four packets of data from the PC?

- 6001
  - 3001
  - 1501
  - 1500
- $6000+1$

60. A client creates a packet to send to a server. The client is requesting TFTP service. What number will be used as the destination port number in the sending packet?

- 69
- 67



- 53
- 80

61. A client creates a packet to send to a server. The client is requesting **FTP** service. What number will be used as the **destination port number** in the sending packet?

- **21**
- 69
- 67
- 80

62. A client creates a packet to send to a server. The client is requesting **SSH** service. What number will be used as the destination port number in the sending packet?

- **22**
- 69
- 67
- 80

63. A client creates a packet to send to a server. The client is requesting **HTTP** service. What number will be used as the destination port number in the sending packet?

- **80**
- 67
- 53
- 69

64. A client creates a packet to send to a server. The client is requesting **POP3** service. What number will be used as the destination port number in the sending packet?

- **110**
- 67
- 53
- 69
- 443
- 161
- 80

65. A client creates a packet to send to a server. The client is requesting **telnet service**. What number will be used as the destination port number in the sending packet?

- **23**
- 443
- 161
- 110

67. A client creates a packet to send to a server. The client is requesting **SNMP service**. What number will be used as the destination port number in the sending packet?

- **161**
- 443
- 110
- 80

68. A client creates a packet to send to a server. The client is requesting **SMTP service**. What number will be used as the destination port number in the sending packet?

- **25**
- 443
- 161
- 110

69. A client creates a packet to send to a server. The client is requesting **HTTPS service**. What number will be used as the destination port number in the sending packet?

- **443**
- 161
- 110
- 80

## **VI. MODULE 16-17**

1. Which component is designed to **protect against unauthorized communications to** and from a computer?

- security center
- port scanner

- antimalware
- antivirus
- **firewall**

2. Which command will block **login attempts** on RouterA for a period of 30 seconds if there are 2 failed login attempts within 10 seconds?

attempts - failed- second

- RouterA(config)# login block-for 10 attempts 2 within 30
- **RouterA(config)# login block-for 30 attempts 2 within 10**
- RouterA(config)# login block-for 2 attempts 30 within 10
- RouterA(config)# login block-for 30 attempts 10 within 2

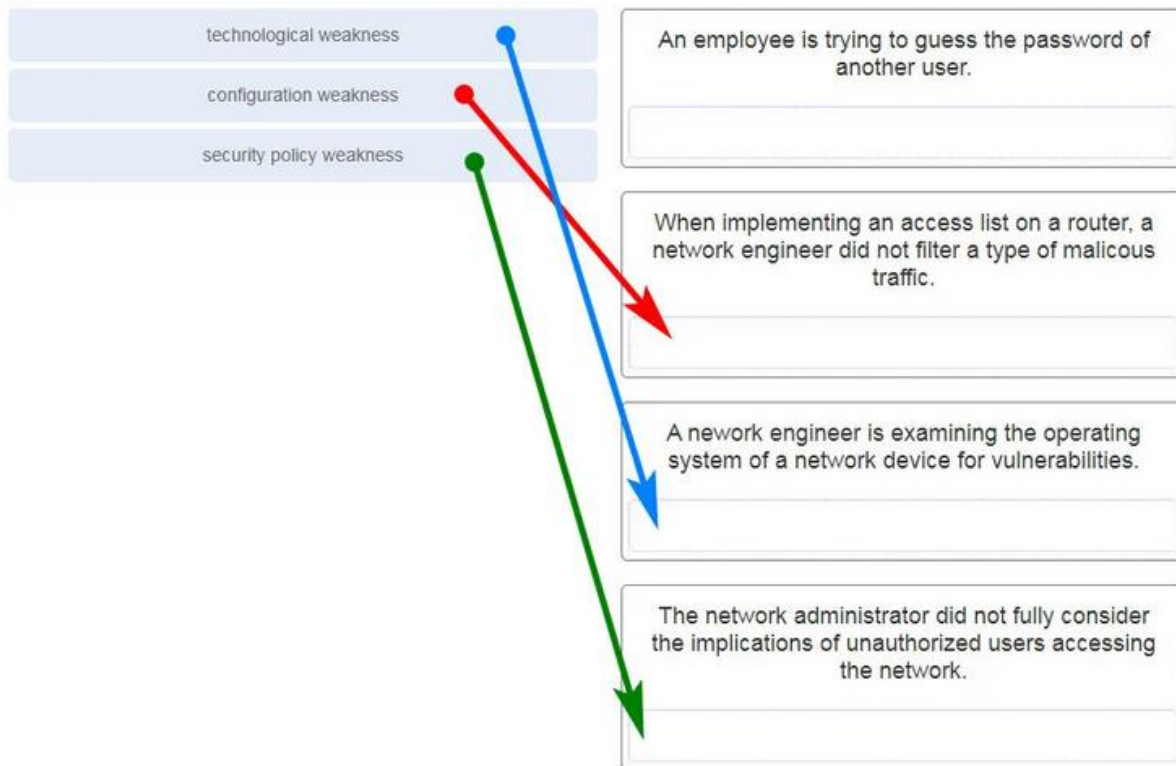
3. What is the purpose of the **network security accounting function**?

- 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

4. What type of attack may involve the use of tools such as **nslookup and fping**?

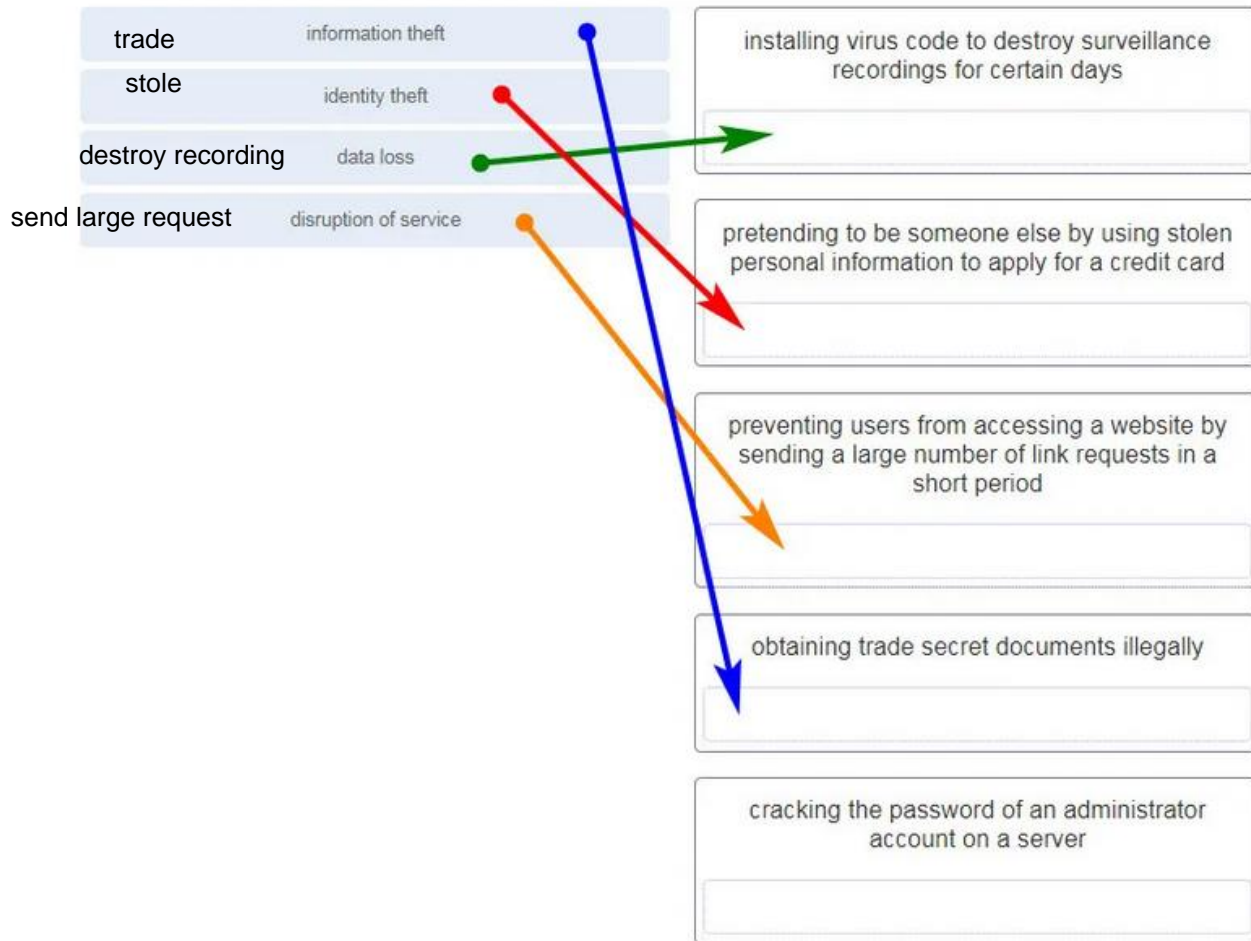
- access attack
- **reconnaissance attack**
- denial of service attack
- worm attack

5. Match each weakness with an example. (Not all options are used.)



**Explanation:** An employee who is trying to guess the password of another user exemplifies not a weakness but an attack.

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



**Explanation:**

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.

**7. Which example of **malicious code** would be classified as a **Trojan** horse?**

- **malware that was written to look like a video game**
- malware that requires manual user intervention to spread between systems

- malware that attaches itself to a legitimate program and spreads to other programs when launched
- malware that can automatically spread from one system to another by exploiting a vulnerability in the target

**Explanation:** A Trojan horse is malicious code that has been written specifically to look like a legitimate program. This is in contrast to a virus, which simply attaches itself to an actual legitimate program. Viruses require manual intervention from a user to spread from one system to another, while a worm is able to spread automatically between systems by exploiting vulnerabilities on those devices.

#### 8. What is the difference between a virus and a worm?

- Viruses self-replicate but worms do not.
- **Worms self-replicate but viruses do not.**
- Worms require a host file but viruses do not.
- Viruses hide in legitimate programs but worms do not.

**Explanation:** Worms are able to self-replicate and exploit vulnerabilities on computer networks without user participation.

#### 9. Which attack involves a compromise of data that occurs between two end points?

- denial-of-service
- **man-in-the-middle attack**
- extraction of security parameters
- username enumeration

**Explanation:** Threat actors frequently attempt to access devices over the internet through communication protocols. Some of the most popular remote exploits are as follows:

- **Man-In-the-middle attack (MITM)** – The threat actor gets between devices in the system and intercepts all of the data being transmitted. This information could simply be collected or modified for a specific purpose and delivered to its original destination.
- **Eavesdropping attack** – When devices are being installed, the threat actor can intercept data such as security keys that are used by constrained devices to establish communications once they are up and running.
- **SQL injection (SQLi)** – Threat actors use a flaw in the Structured Query Language (SQL) application that allows them to have access to modify the data or gain administrative privileges.
- **Routing attack** – A threat actor could either place a rogue routing device on the network or modify routing packets to manipulate routers to send all packets to the chosen destination of the threat actor. The threat actor could then drop specific

packets, known as selective forwarding, or drop all packets, known as a sinkhole attack.

**10. Which type of attack involves an adversary attempting to gather information about a network to identify vulnerabilities?**

- **reconnaissance**
- DoS
- dictionary
- man-in-the-middle

**Explanation:** Reconnaissance is a type of attack where the intruder is looking for wireless network vulnerabilities.

11. Match the description to the type of firewall filtering. (Not all options are used.)

stateful packet inspection	prevents or allows access based on the operating system of the source or destination device
URL filtering	
application filtering	
packet filtering	prevents or allows access based on the port numbers used in the request
	application filtering
	prevents or allows access based on whether the traffic is in response to requests from internal hosts
	stateful packet inspection
	prevents or allows access based on web addresses or keywords
	URL filtering
	prevents or allows access based on the IP or MAC addresses of the source and destination
	packet filtering

**Explanation: Stateful packet inspection:** Prevents or allows access based on whether the traffic is in response to requests from internal hosts.

**URL filtering:** Prevents or allows access based on web addresses or keywords.

**Application filtering:** Prevents or allows access based on the port numbers used in the request.

**Packet filtering:** Prevents or allows access based on the IP or MAC addresses of the source and destination.



## 12. 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

**Explanation:** 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.

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

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

**Explanation:** **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.

## 14. When applied to a router, which command would help mitigate brute-force password attacks against the router?

- exec-timeout 30
- service password-encryption
- banner motd \$Max failed logins = 5\$
- **login block-for 60 attempts 5 within 60**

**Explanation:** The **login block-for** command **sets a limit on the maximum number of failed login** attempts allowed within a defined period of time. If this limit is exceeded, no further logins are allowed for the specified period of time. This helps to **mitigate brute-force password** cracking since it will significantly increase the amount of time required to crack a password. The **exec-timeout** command specifies how long the session can be idle before the user is disconnected. The **service password-encryption** command encrypts the passwords in the running configuration. The **banner motd** command displays a message to users who are logging in to the device.

15. Identify the steps needed to configure a switch for SSH. The answer order does not matter. (Not all options are used.)

required steps for SSH configuration

- Create a local user.
- Generate RSA keys.
- Configure a domain name.
- Use the login local command.
- Use the transport input ssh command.

**Explanation:** The **login** and **password cisco** commands are used with Telnet switch configuration, not SSH configuration.

16. What feature of **SSH makes it more secure than Telnet** for a device management connection?

- confidentiality with IPsec
- stronger password requirement
- random one-time port connection
- **login information and data encryption**

**Explanation:** Secure Shell (SSH) is a protocol that **provides a secure management connection to a remote device.** SSH provides security by providing encryption for both authentication (username and password) and the transmitted data. Telnet is a protocol that uses unsecure plaintext transmission. SSH is assigned to TCP port 22 by default. Although this port can be changed in the SSH server configuration, the port is not dynamically changed. SSH does not use IPsec.

17. What is the advantage of using SSH over Telnet?

- SSH is easier to use.
- SSH operates faster than Telnet.
- **SSH provides secure communications to access hosts.**
- SSH supports authentication for a connection request.

**Explanation:** SSH provides a secure method for remote access to hosts by encrypting network traffic between the SSH client and remote hosts. Although both Telnet and SSH request authentication before a connection is established, Telnet does not support encryption of login credentials.

**18. What is the role of an IPS?** intrusion prevention system

- **detecting and blocking of attacks in real time**
- connecting global threat information to Cisco network security devices
- authenticating and validating traffic
- filtering of nefarious websites

**Explanation:** An **intrusion prevention system** (IPS) provides **real-time detection** and blocking of attacks.

**19. A user is redesigning a network for a small company and wants to ensure security at a reasonable price. The user deploys a new application-aware firewall with intrusion detection capabilities on the ISP connection. The user **installs a second firewall** to separate the company network from the public network. Additionally, the user installs an IPS on the internal network of the company. What approach is the user implementing?**

- attack based
- risk based                      bảo mật lớp
- structured
- **layered**

**Explanation:** Using different defenses at various points of the network creates a layered approach.

**20. What is an accurate description of **redundancy**?**

- configuring a router with a complete MAC address database to ensure that all frames can be forwarded to the correct destination
- configuring a switch with proper security to ensure that all traffic forwarded through an interface is filtered
- designing a network to use multiple virtual devices to ensure that all traffic uses the best path through the internetwork

- **designing a network to use multiple paths between switches to ensure there is no single point of failure**

**Explanation:** Redundancy attempts to remove any single point of failure in a network by using multiple physically cabled paths between switches in the network.

**21. A network administrator is upgrading a small business network to give high priority to real-time applications traffic. What two types of network services is the network administrator trying to accommodate? (Choose two.)**

- **voice**
- **video**
- instant messaging
- FTP
- SNMP

**Explanation:** Streaming media, such as video, and voice traffic, are both examples of real-time traffic. Real-time traffic needs higher priority through the network than other types of traffic because it is very sensitive to network delay and latency.

**22. What is the purpose of a small company using a protocol analyzer utility to capture network traffic on the network segments where the company is considering a network upgrade?**

- to identify the source and destination of local network traffic
- to capture the Internet connection bandwidth requirement
- **to document and analyze network traffic requirements on each network segment**
- to establish a baseline for security analysis after the network is upgraded

**Explanation:** An important prerequisite for considering network growth is to understand the type and amount of traffic that is crossing the network as well as the current traffic flow. By using a protocol analyzer in each network segment, the network administrator can document and analyze the network traffic pattern for each segment, which becomes the base in determining the needs and means of the network growth.

**23. Refer to the exhibit. An administrator is testing connectivity to a remote device with the IP address 10.1.1.1. What does the output of this command**

indicate?

U: do not have route to dest  
!: successful      . : connection time out

```
Switch# ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

- Connectivity to the remote device was successful.
- **A router along the path did not have a route to the destination.**
- A ping packet is being blocked by a security device along the path.
- The connection timed out while waiting for a reply from the remote device.

**Explanation:** In the output of the ping command, an exclamation mark (!) indicates a response was successfully received, a period (.) indicates that the connection timed out while waiting for a reply, and the letter "U" indicates that a router along the path did not have a route to the destination and sent an ICMP destination unreachable message back to the source.

**24. Which method is used to send a ping message specifying the source address for the ping?**

- Issue the ping command from within interface configuration mode.
- **Issue the ping command without specifying a destination IP address.**
- Issue the ping command without extended commands.
- Issue the ping command after shutting down un-needed interfaces.

**Explanation:** By issuing the ping command without a destination IP address in privileged EXEC mode, the Cisco IOS enters extended ping mode. This allows the user to implement extended commands which include source IP address.

**25. A network engineer is analyzing reports from a recently performed network baseline. Which situation would depict a possible latency issue?**

- a change in the bandwidth according to the show interfaces output
- a next-hop timeout from a traceroute
- **an increase in host-to-host ping response times**
- a change in the amount of RAM according to the show version output

**Explanation:** While analyzing historical reports an administrator can compare host-to-host timers from the ping command and depict possible latency issues.

**26. Which statement is true about Cisco IOS ping indicators?**

- ~~'!' indicates that the ping was unsuccessful~~ and that the device may have issues finding a DNS server.
- **'U' may indicate that a router along the path did not contain a route to the destination address and that the ping was unsuccessful.**
- '.' indicates that the ping was successful but the response time was longer than normal.
- A combination of '.' and '!' indicates that a router along the path did not have a route to the destination address and responded with an ICMP unreachable message.

**Explanation:** The most common indicators of a ping issued from the Cisco IOS are "!", ".", and "U". The "!" indicates that the ping completed successfully, verifying connectivity at Layer 3. The "." may indicate that a connectivity problem, routing problem, or device security issue exists along the path and that an ICMP destination unreachable message was not provided. The "U" indicates that a router along the path may not have had a route to the destination address, and that it responded with an ICMP unreachable message.

**27. A user reports a lack of network connectivity. The technician takes control of the user machine and attempts to ping other computers on the network and these pings fail. The technician pings the default gateway and that also fails. What can be determined for sure by the results of these tests?**

- The NIC in the PC is bad.
- The TCP/IP protocol is not enabled.
- The router that is attached to the same network as the workstation is down.
- **Nothing can be determined for sure at this point.**

**Explanation:** In networks today, a failed ping could mean that the other devices on the network are blocking pings. Further investigation such as checking network connectivity from other devices on the same network is warranted.

**28. 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?**

ipv6

- **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.

**29. Why would a network administrator use the tracert utility?**

- to determine the active TCP connections on a PC

- to check information about a DNS name in the DNS server
- **to identify where a packet was lost or delayed on a network**
- to display the IP address, default gateway, and DNS server address for a PC

**Explanation:** The **tracert** utility is used to identify the path a packet takes from source to destination. **Tracert** is commonly used when packets are dropped or not reaching a specific destination.

**30. 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?**

verify

- 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.

**Explanation:** The **show cdp neighbors** command can be used to prove that Layer 1 and Layer 2 connectivity exists between two Cisco devices. For example, if two devices have duplicate IP addresses, a ping between the devices will fail, but the output of **show cdp neighbors** will be successful. The **show cdp neighbors detail** could be used to verify the IP address of the directly connected device in case the same IP address is assigned to the two routers.

**31. A network engineer is troubleshooting connectivity issues among interconnected Cisco routers and switches. Which command should the engineer use to find the IP address information, host name, and IOS version of neighboring network devices?**

- show version
- show ip route
- show interfaces
- **show cdp neighbors detail**

**Explanation:** The **show cdp neighbors detail** command reveals much information about neighboring Cisco devices, including the IP address, the capabilities, host name, and IOS version. The **show interfaces** and **show version** commands display information about the local device.

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

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

**Explanation:** The `value of the configuration register` can be verified with the `show version` command.

**33. 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`**

**Explanation:** 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.

**34. Which command can an administrator issue on a Cisco router to `send debug messages to the vty lines`?**

- **`terminal monitor`**
- `logging console`
- `logging buffered`
- `logging synchronous`

**Explanation:** Debug messages, like other IOS log messages, are sent to the console line by default. Sending these messages to the terminal lines requires the **`terminal monitor`** command.

**35. By following a `structured troubleshooting approach`, a network administrator `identified a network issue` after a conversation with the user. What is the next step that the administrator should take?**

- Verify full system functionality.
  - Test the theory to determine cause.
  - **`Establish a theory of probable causes.`**
- identify  
establish theory  
test  
establish plan  
verify  
document findings



- Establish a plan of action to resolve the issue.

**Explanation:** A structured network troubleshooting approach should include these steps in sequence:

1. Identify the problem.
2. Establish a theory of probable causes.
3. Test the theory to determine cause.
4. Establish a plan of action to resolve the issue.
5. Verify full system functionality and implement preventive measures.
6. Document findings, actions, and outcomes.

**36. Users are complaining that they are unable to browse certain websites on the Internet. An administrator can successfully ping a web server via its IP address, but cannot browse to the domain name of the website. Which troubleshooting tool would be most useful in determining where the problem is?**

- netstat
- tracert
- nslookup
- ipconfig

**Explanation:** The nslookup command can be used to look up information about a particular DNS name in the DNS server. The information includes the IP address of the DNS server being used as well as the IP address associated with the specified DNS name. This command can help verify the DNS that is used and if the domain name to IP address resolution works.

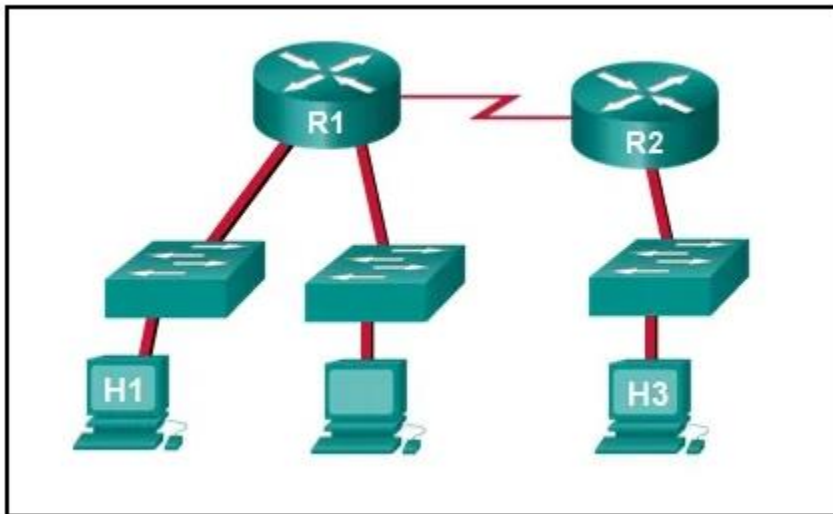
**37. An employee complains that a Windows PC cannot connect to the Internet. A network technician issues the ipconfig command on the PC and is shown an IP address of 169.254.10.3. Which two conclusions can be drawn? (Choose two.)**

- The PC cannot contact a DHCP server.
- The DNS server address is misconfigured.
- The default gateway address is not configured.
- The PC is configured to obtain an IP address automatically.
- The enterprise network is misconfigured for dynamic routing.

**Explanation:** When a Windows PC is configured to obtain an IP address automatically, the PC will try to obtain an IP address from a DHCP server. When the PC cannot contact a DHCP server, Windows will automatically assign an address belonging to the 169.254.0.0/16 range.

**38. Refer to the exhibit. Host H3 is having trouble communicating with host H1. The network administrator suspects a problem exists with the H3 workstation and wants to prove that there is no problem with the R2 configuration. What tool**

could the network administrator use on router R2 to prove that communication exists to host H1 from the interface on R2, which is the interface that H3 uses when communicating with remote networks?

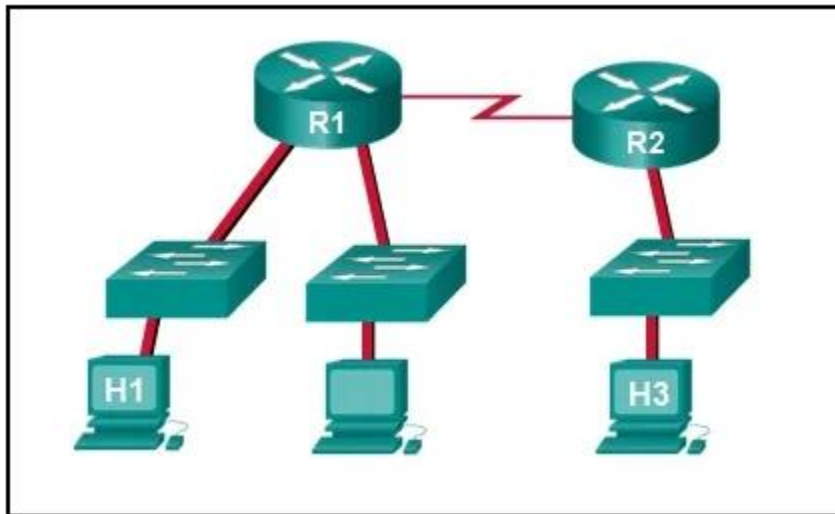


- traceroute
- show cdp neighbors
- Telnet
- **an extended ping**

**Explanation:** An **extended ping** allows an administrator to **select specific ping features**. For example in this situation, the network administrator could do an extended ping and specify a source address of the gigabit Ethernet port on the router. The destination address would be the IP address of host H1. **If the ping succeeds connectivity exists from the Ethernet router interface on R2 to device H1.**

**39. 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.**

**Explanation:** 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.

**40. Which network service automatically assigns IP addresses to devices on the network?**

- **DHCP**
- Telnet
- DNS
- traceroute

**Explanation:** Dynamic Host Configuration Protocol (DHCP) can be used to allow end devices to automatically configure IP information, such as their IP address, subnet mask, DNS server, and default gateway. The DNS service is used to provide domain name resolution, mapping hostnames to IP addresses. Telnet is a method for remotely accessing a CLI session of a switch or router. **Traceroute** is a command used to determine the path a packet takes as it traverses the network.

**41. Which command can an administrator execute to determine what interface a router will use to reach remote networks?**

- show arp
- show interfaces
- **show ip route**
- show protocols

**Explanation:** The **show ip route** command is used to display the IP routing table of the router. The IP routing table will show a list of known local and remote networks and the interfaces that the router will use to reach those networks.

**42. On which two interfaces or ports can security be improved by configuring executive timeouts? (Choose two.)**

- Fast Ethernet interfaces
- **console ports**
- serial interfaces
- **vty ports**
- loopback interfaces

**Explanation:** **Executive timeouts** allow the Cisco device to automatically disconnect users after they have been idle for the specified time. **Console, vty, and aux ports can be configured with executive timeouts.**

**43. When configuring SSH on a router to implement secure network management, a network engineer has issued the login local and transport input ssh line vty commands. What three additional configuration actions have to be performed to complete the SSH configuration? (Choose three.)**

- Set the user privilege levels.
- **Generate the asymmetric RSA keys.**
- **Configure the correct IP domain name.**
- Configure role-based CLI access.
- **Create a valid local username and password database.**
- Manually enable SSH after the RSA keys are generated.

rsa key  
correct ip domain  
username password

**Explanation:** SSH is automatically enabled after the **RSA keys** are generated. Setting user privilege levels and configuring role-based CLI access are good security practices but are not a requirement of implementing SSH.

**44. What is considered the most effective way to mitigate a worm attack?**

- Change system passwords every 30 days.
- Ensure that all systems have the most current virus definitions.
- Ensure that AAA is configured in the network.
- **Download security updates from the operating system vendor and patch all vulnerable systems.**

**Explanation:** Because worms take advantage of vulnerabilities in the system itself, the most effective way to mitigate worm attacks is to download security updates from the operating system vendor and patch all vulnerable systems.

**45. Which statement describes the ping and tracert commands?**

- **Tracert shows each hop, while ping shows a destination reply only.**
- Tracert uses IP addresses; ping does not.
- Both ping and tracert can show results in a graphical display.
- Ping shows whether the transmission is successful; tracert does not.

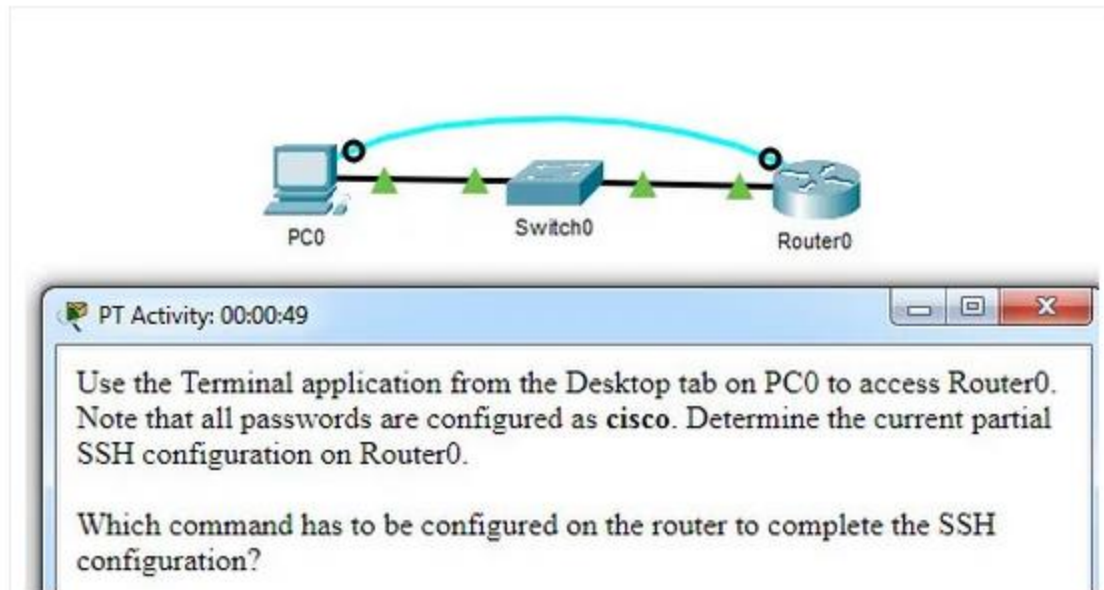
**Explanation:** The **ping** utility tests end-to-end connectivity between the two hosts. However, if the message does not reach the destination, there is no way to determine where the problem is located. On the other hand, the **tracert** utility (**tracert** in Windows) traces the route a message takes from its source to the destination. **Tracert** displays each hop along the way and the time it takes for the message to get to that network and back.

**46. A technician is to document the current configurations of all network devices in a college, including those in off-site buildings. Which protocol would be best to use to securely access the network devices?**

- FTP
- HTTP
- **SSH** securely access (encrypt data)
- Telnet

**Explanation:** Telnet sends passwords and other information in clear text, while SSH encrypts its data. FTP and HTTP do not provide remote device access for configuration purposes.

**47. Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.**



Which command has to be configured on the router to complete the SSH configuration?

- service password-encryption
- **transport input ssh**
- enable secret class
- ip domain-name cisco.com

**Explanation:** The missing command to complete the SSH configuration is **transport input ssh** in **line vty 0 4** mode. The commands **service password-encryption** and **enable secret class** do configure secure features on the router, but are not required to configure SSH. The command **ip domain-name cisco.com** is not required because the command **ip domain-name span.com** has been used.

48. An administrator decides to use “WhatAreYouWaiting4” as the password on a newly installed router. Which statement applies to the password choice?

- **It is strong because it uses a passphrase.**
- It is weak because it is often the default password on new devices.
- It is weak since it uses easily found personal information.
- It is weak since it is a word that is easily found in the dictionary.

49. An administrator decides to use “pR3s!d7n&0” as the password on a newly installed router. Which statement applies to the password choice?

- **It is strong because it uses a minimum of 10 numbers, letters and special characters.**
- It is weak because it is often the default password on new devices.
- It is weak since it uses easily found personal information.

- It is weak since it is a word that is easily found in the dictionary.

**50. An administrator decides to use “5\$7\*4#033!” as the password on a newly installed router. Which statement applies to the password choice?**

- **It is strong because it contains 10 numbers and special characters.**
- It is weak because it is often the default password on new devices.
- It is weak since it uses easily found personal information.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.

**51. An administrator decides to use “pR3s!d7n&0” as the password on a newly installed router. Which statement applies to the password choice?**

- **It is strong because it uses a minimum of 10 numbers, letters and special characters.**
- It is weak since it is a word that is easily found in the dictionary.
- It is strong because it uses a passphrase.
- It is strong because it contains 10 numbers and special characters.

**52. An administrator decides to use “12345678!” as the password on a newly installed router. Which statement applies to the password choice?**

- **It is weak because it uses a series of numbers or letters.**
- It is strong because it uses a passphrase.
- It is weak since it is a word that is easily found in the dictionary.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.

**53. An administrator decides to use “admin” as the password on a newly installed router. Which statement applies to the password choice?**

- **It is weak because it is often the default password on new devices.**
- It is strong because it uses a passphrase.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.
- It is strong because it contains 10 numbers and special characters.

**54. An administrator decides to use “Feb121978” as the password on a newly installed router. Which statement applies to the password choice?**

- **It is weak because it uses easily found personal information.**
- It is strong because it uses a passphrase.
- It is weak since it is a word that is easily found in the dictionary.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.

**55. An administrator decides to use “password” as the password on a newly installed router. Which statement applies to the password choice?**

- **It is weak because it is a commonly used password.**
- It is weak since it is a word that is easily found in the dictionary.
- It is strong because it uses a passphrase.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.

**56. An administrator decides to use “RobErT” as the password on a newly installed router. Which statement applies to the password choice?**

- **It is weak since it uses easily found personal information.**
- It is strong because it uses a passphrase.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.
- It is strong because it contains 10 numbers and special characters.

**57. An administrator decides to use “Elizabeth” as the password on a newly installed router. Which statement applies to the password choice?**

- **It is weak because it uses easily found personal information.**
- It is strong because it uses a passphrase.
- It is weak since it is a word that is easily found in the dictionary.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.

**Explanation:** Rules for strong passwords:

\* minimum of **8 characters, preferably 10.**

\* use complex combinations of **numbers, special characters, and upper and lower case letters.**

\* **avoid repetition,** common dictionary words, letter or number sequences.

\* **avoid** names of children, relatives, pets, birthdays, or any easily identifiable **personal information.**

\* can be created by misspelling words or replacing vowels with numbers or special characters.

**58. A network technician is troubleshooting an issue and needs to verify the IP addresses of all interfaces on a router. What is the best command to use to accomplish the task?**

- **show ip interface brief**      verify ip address : show ip
- nslookup
- ipconfig getifaddr en0
- show ip route



59. Students who are **connected to the same switch** are having **slower than normal response times**. The administrator suspects a duplex setting issue. What is the best command to use to accomplish the task?

- **show interfaces** display switch information
- ipconfig getifaddr en0
- copy running-config startup-config
- show ip nat translations

60. A user wants to **know the IP address of the PC**. What is the best command to use to accomplish the task?

- **ipconfig** check ip address
- copy running-config startup-config
- show interfaces
- show ip nat translations

61. A student wants to save a router configuration to NVRAM. What is the best command to use to accomplish the task?

- **copy running-config startup-config**
- show interfaces
- show ip nat translations
- show ip route

62. A support technician needs to **know the IP address of the wireless interface on a MAC**. What is the best command to use to accomplish the task?

- **ipconfig getifaddr en0**
- copy running-config startup-config
- show interfaces
- show ip nat translations

63. A network technician is **troubleshooting an issue and needs to verify all of the IPv6 interface addresses on a router**. What is the best command to use to accomplish the task?

- **show ipv6 interface**
- show interfaces
- show ip nat translations
- show ip route

64. A teacher is having difficulties connecting his PC to the classroom network. He needs to **verify that a default gateway is configured correctly**. What is the best command to use to accomplish the task?

- **ipconfig** dùng cho máy tính
- copy running-config startup-config
- show interfaces
- show ip nat translations

65. Only employees connected to IPv6 interfaces are **having difficulty connecting to remote networks**. The analyst wants to verify that IPv6 routing has been enabled. What is the best command to use to accomplish the task?

- **show running-config**
- show interfaces
- copy running-config startup-config
- show ip nat translations

66. An administrator is **troubleshooting connectivity issues** and needs to **determine the IP address of a website**. What is the best command to use to accomplish the task?

- **nslookup** lấy ip của website
- show ipv6 route
- show ipv6 interface
- copy startup-config running-config

67. 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.

**Explanation:** 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.**

## VII. FINAL EXAM (INTRODUCTION TO NETWORKS)

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

- **video**
- web
- file transfer

- **voice**
- peer to peer

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

- **ZigBee**
- LoRaWAN
- 5G
- Wi-Fi

**Explanation:** ZigBee is an IEEE 802.15.4 wireless standard designed for creating personal-area networks. Low energy, power, and data rate requirements make Zigbee a popular protocol for connecting home automation devices.

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

- application
- network access
- **internet**
- transport

**Explain:**

The OSI model network layer corresponds directly to the internet layer of the TCP/IP model and is used to describe protocols that address and route messages through an internetwork.

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

- **DNS**
- email
- file
- web

**Explain:**

A DNS server stores records that are used to resolve IP addresses to host names. Some DNS record types include the following:

A – an end device IPv4 address  
 NS – an authoritative name server  
 AAAA – an end device IPv6 address  
 MX – a mail exchange record

**5. 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.

**6. What service is provided by DNS?**

- **Resolves domain names, such as cisco.com, into IP addresses.**
- A basic set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the web.
- Allows for data transfers between a client and a file server.
- Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.

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

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

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

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

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

- client-based
- master-slave
- point-to-point
- **peer-to-peer (P2P)**

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

**10. What characteristic describes a virus?**

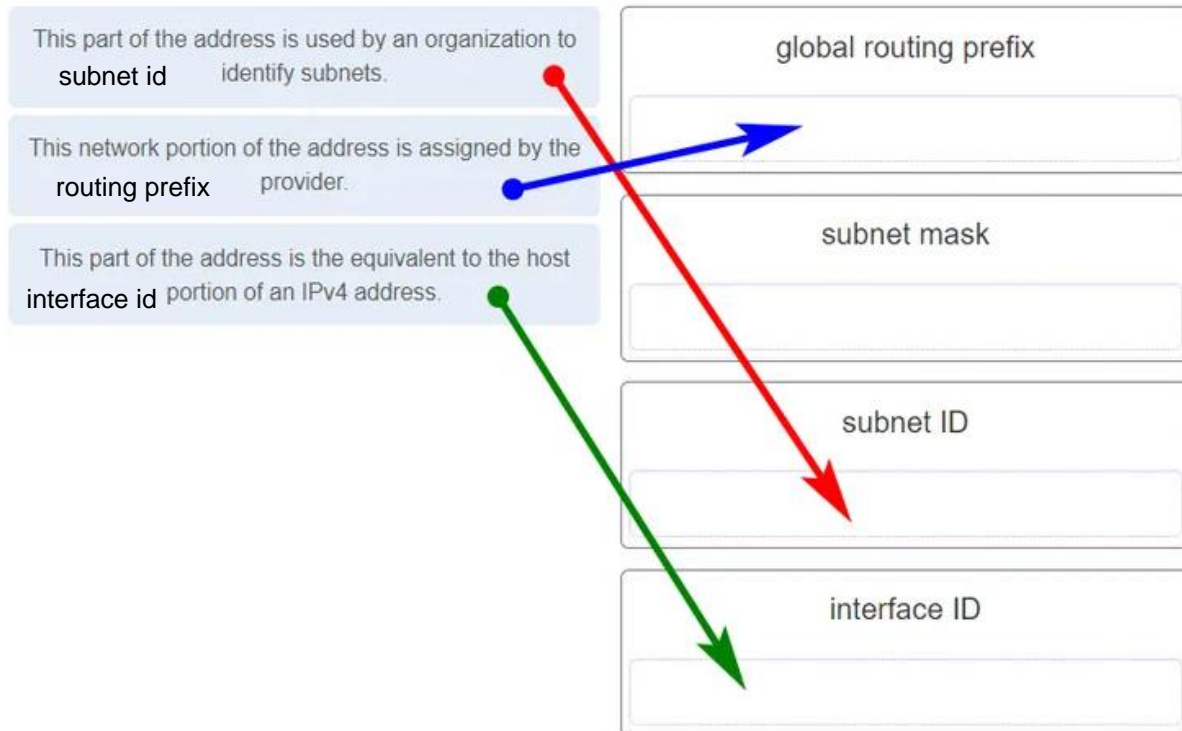
- a network device that filters access and traffic coming into a network
- the use of stolen credentials to access private data
- an attack that slows or crashes a device or network service
- **malicious software or code running on an end device**

**11. Three bank employees** are using the corporate network. The first employee uses a web browser to view a company web page in order to read some announcements. The second employee accesses the corporate database to perform some financial transactions. The third employee participates in an important live audio conference with other corporate managers in branch offices. If QoS is implemented on this network, what will be the priorities from highest to lowest of the different data types?

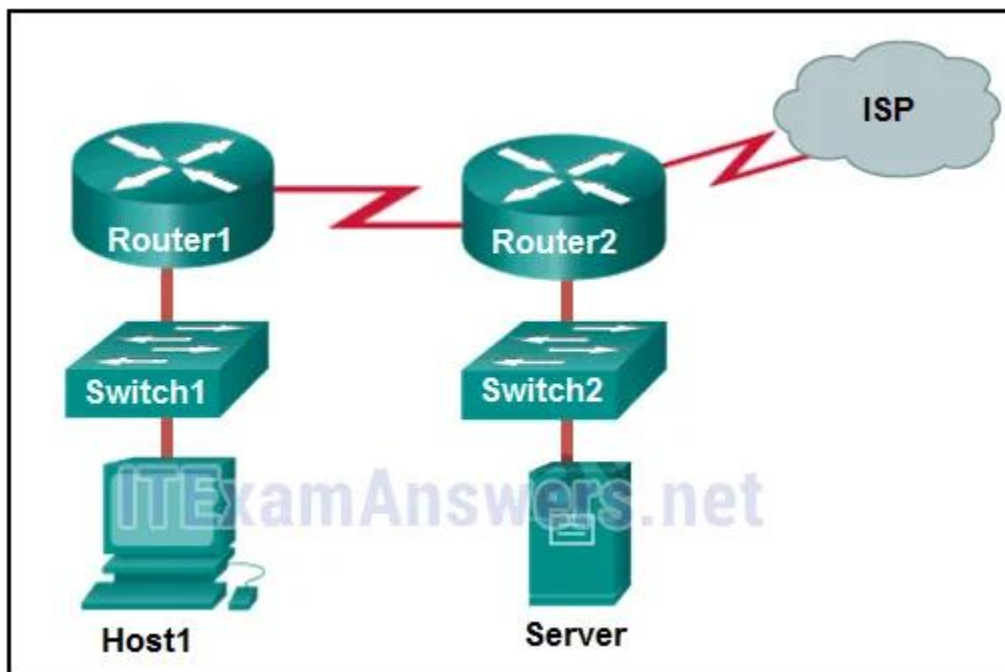
- financial transactions, web page, audio conference
- **audio conference, financial transactions, web page**
- financial transactions, audio conference, web page
- audio conference, web page, financial transactions

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

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



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

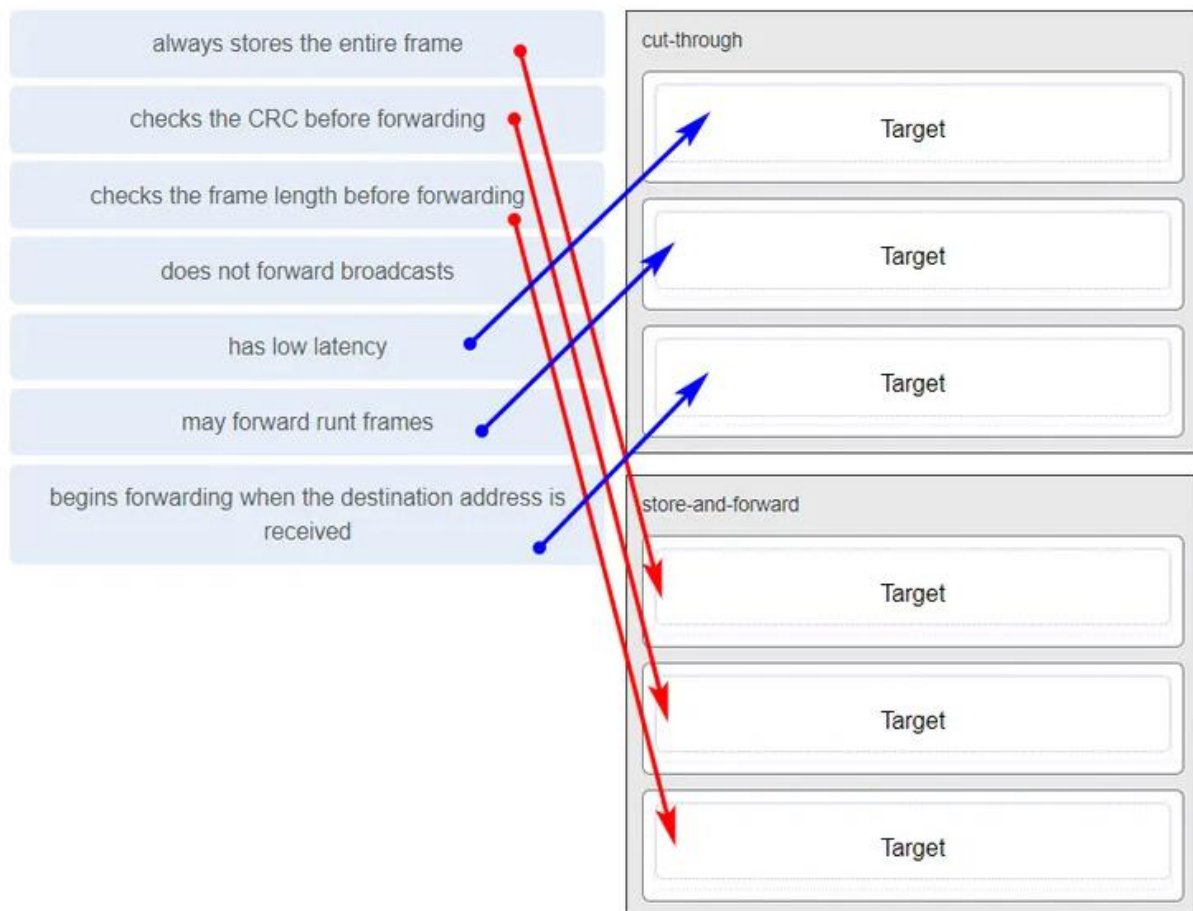


- only application and Internet layers
- only Internet and network access layers

- 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

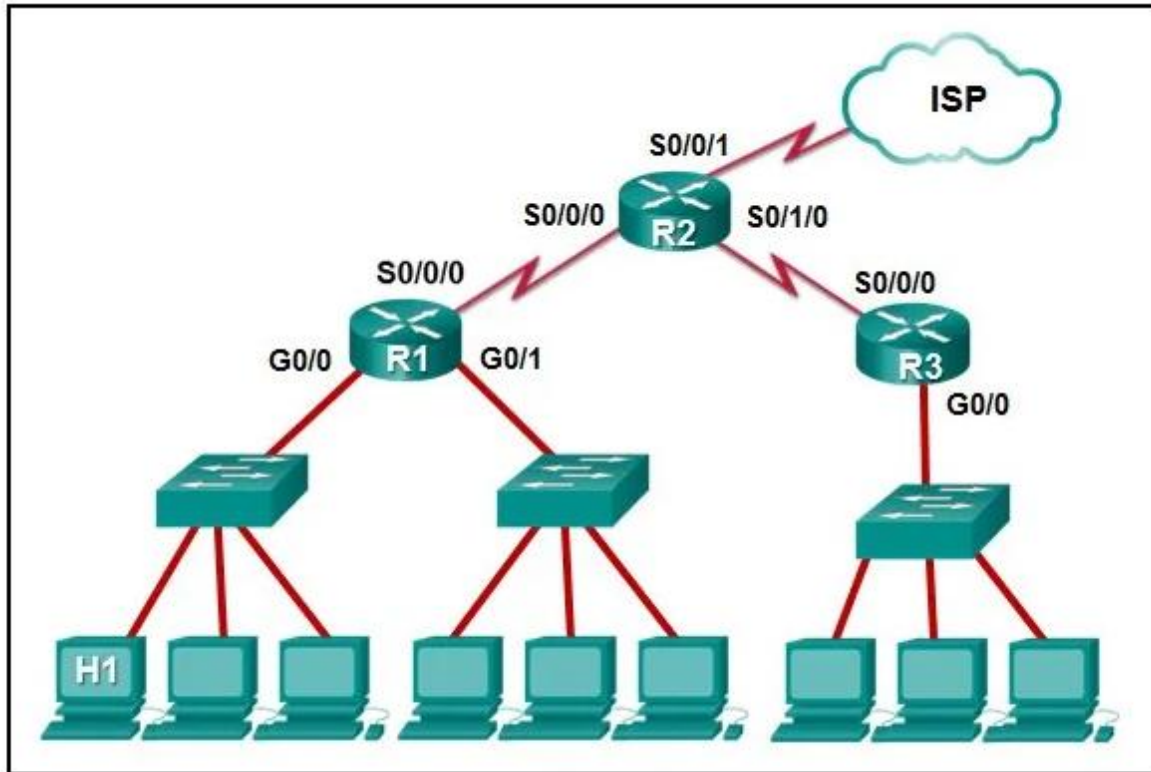
**Explanation:** The TCP/IP model contains the application, transport, internet, and network access layers. A file transfer uses the FTP application layer protocol. The data would move from the application layer through all of the layers of the model and across the network to the file server.

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



**Explanation:** 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.

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



- R1: S0/0/0
- R2: S0/0/1
- **R1: G0/0**
- R2: S0/0/0

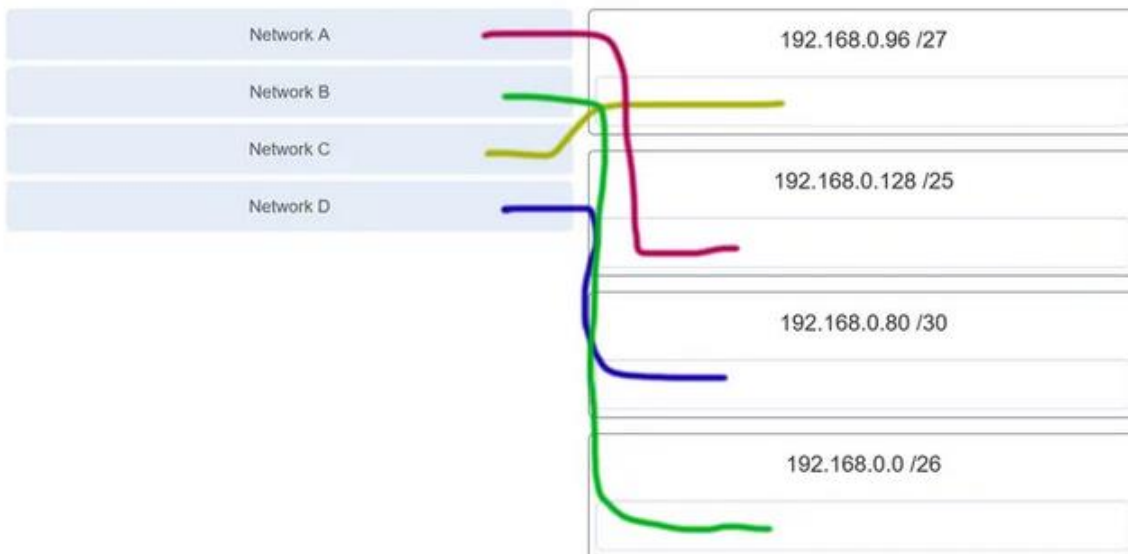
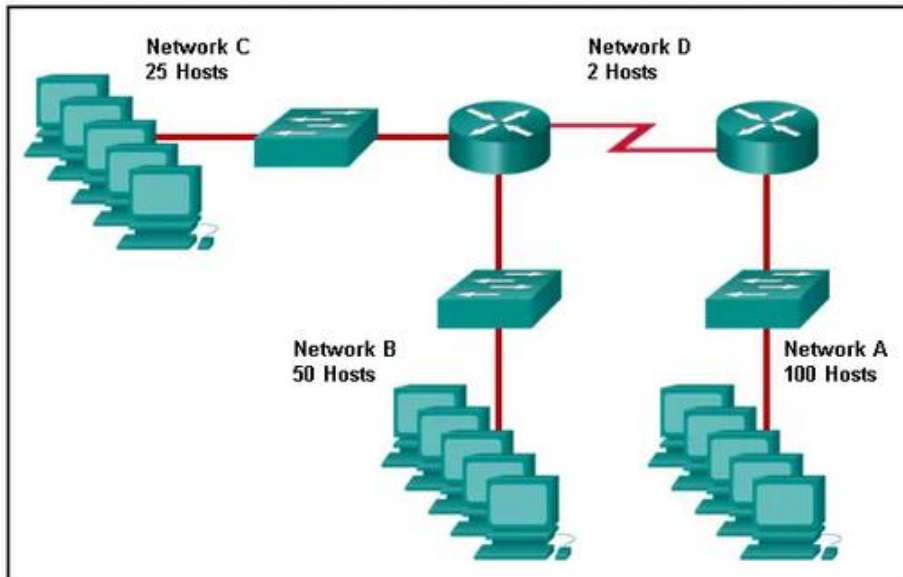
**Explanation:** The default gateway for host H1 is the router interface that is attached to the LAN that H1 is a member of. In this case, that is the G0/0 interface of R1. H1 should be configured with the IP address of that interface in its addressing settings. R1 will provide routing services to packets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

16. What service is provided by **Internet Messenger**?

- **An application that allows real-time chatting among remote users.**
- Allows remote access to network devices and servers.
- Resolves domain names, such as cisco.com, into IP addresses.
- Uses encryption to provide secure remote access to network devices and servers.



17. Refer to the exhibit. Match the network with the correct IP address and prefix that will satisfy the usable host addressing requirements for each network.



**Explanation:** Network A needs to use 192.168.0.128 /25, which yields 128 host addresses.


Network B needs to use 192.168.0.0 /26, which yields 64 host addresses.

Network C needs to use 192.168.0.96 /27, which yields 32 host addresses.

Network D needs to use 192.168.0.80/30, which yields 4 host addresses.

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

<output omitted>



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

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

- DHCP
- **ARP**
- DNS
- ICMP

**Explanation:** The table that is shown corresponds to the output of the arp -a command, a command that is used on a Windows PC to display the ARP table.

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

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

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

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

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

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

- **DNS**
- NetBIOS (NetBT)
- POP3
- IMAP

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

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

24. What characteristic describes a **Trojan horse**?

- **malicious software or code running on an end device**
- an attack that slows or crashes a device or network service
- the use of stolen credentials to access private data
- a network device that filters access and traffic coming into a network

25. What service is provided by **HTTPS**?

- Uses encryption to provide secure remote access to network devices and servers.
- Resolves domain names, such as cisco.com, into IP addresses.
- **Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.**
- Allows remote access to network devices and servers.

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

- The data flow is being tracked based on the destination MAC address of the technician PC.
- **The data flow is being tracked based on the source port number that is used by each application.**
- The data flow is being tracked based on the source IP address that is used by the PC of the technician.

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

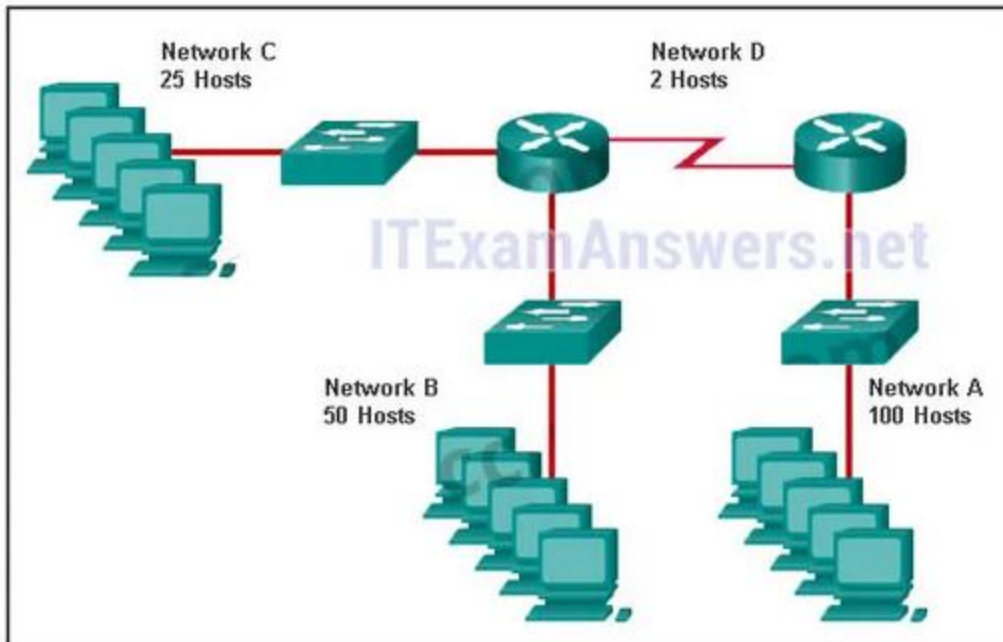
**Explanation:**

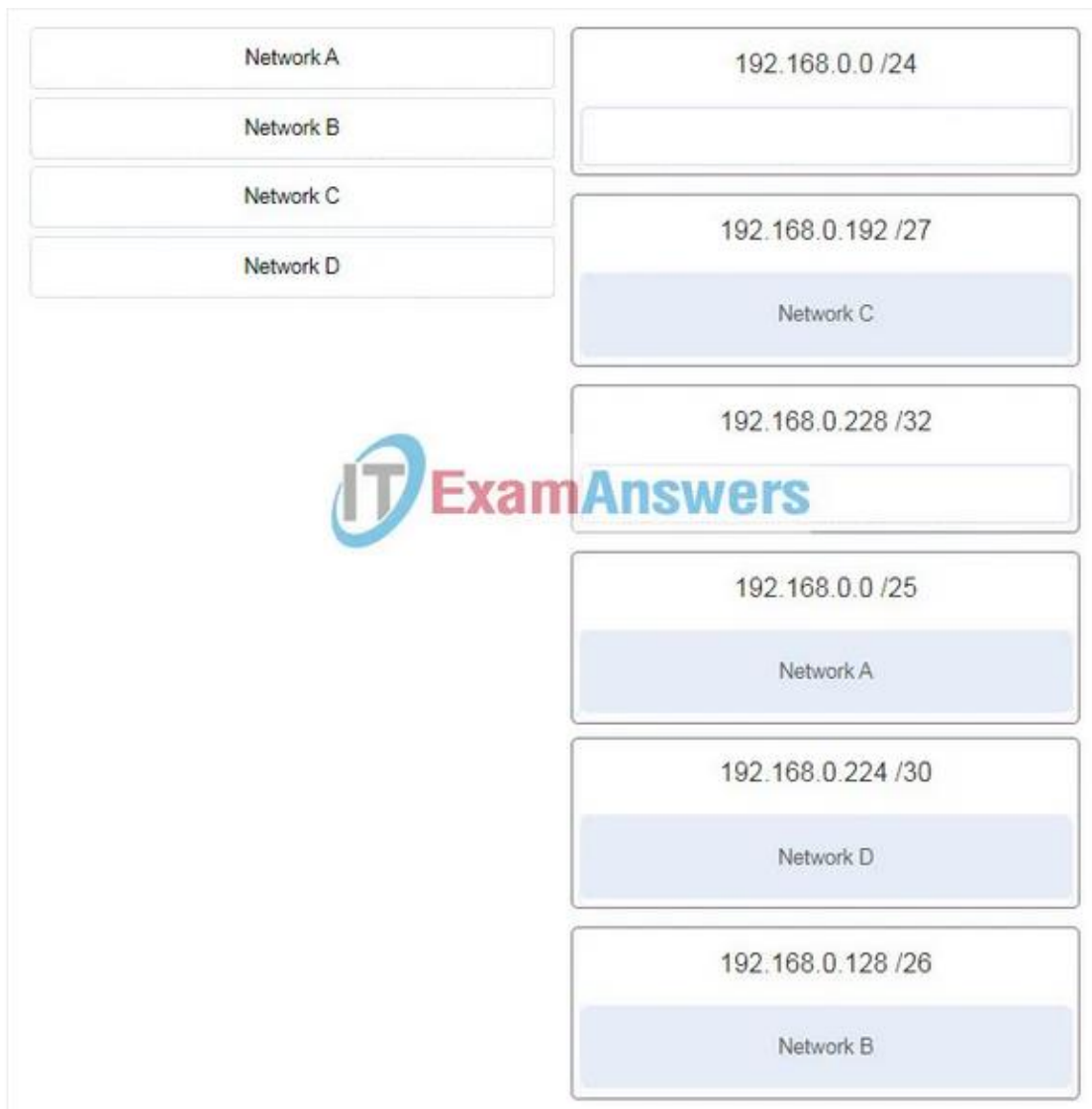
The source port number of an application is randomly generated and used to individually keep track of each session connecting out to the Internet. Each application will use a unique source port number to provide simultaneous communication from multiple applications through the Internet.

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

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

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





ITN (Version 7.00) – ITNv7 Final Exam

**Explanation:**

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.

**29. What characteristic describes a DoS attack?**

- the use of stolen credentials to access private data
- a network device that filters access and traffic coming into a network
- software that is installed on a user device and collects information about the user
- **an attack that slows or crashes a device or network service**

30. Match the application protocols to the correct transport protocols



31. What service is provided by SMTP?

- **Allows clients to send email to a mail server and the servers to send email to other servers.**
- Allows remote access to network devices and servers.
- Uses encryption to provide secure remote access to network devices and servers.
- An application that allows real-time chatting among remote users.

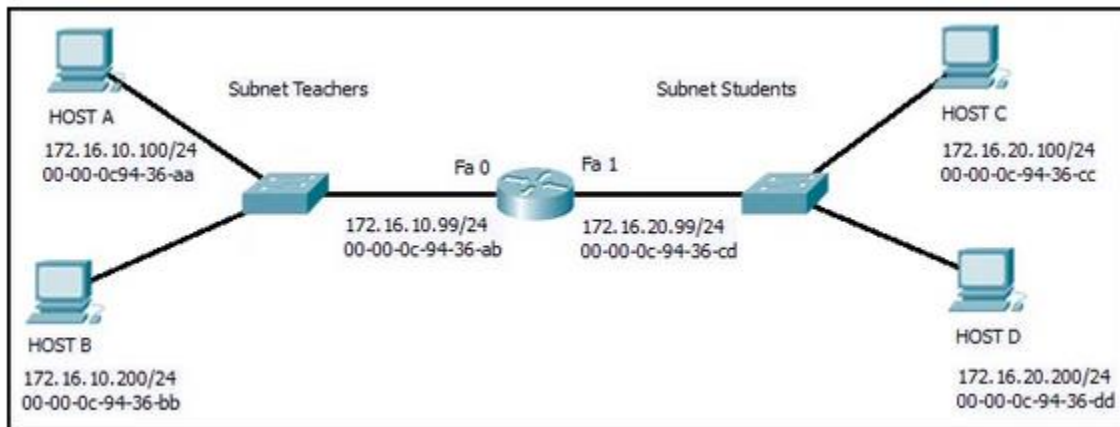
32. Which scenario describes a function provided by the transport layer?

- 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.

**Explain:**

The source and destination port numbers are used to identify the correct application and window within that application.

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



**Layer 2 destination address = 00-00-0c-94-36-ab**

**Layer 2 source address = 00-00-0c-94-36-bb**

**Layer 3 destination address = 172.16.20.200**

**Layer 3 source address = 172.16.10.200**

Layer 2 destination address = 00-00-0c-94-36-dd

Layer 2 source address = 00-00-0c-94-36-bb

Layer 3 destination address = 172.16.20.200

Layer 3 source address = 172.16.10.200

Layer 2 destination address = 00-00-0c-94-36-cd

Layer 2 source address = 00-00-0c-94-36-bb

Layer 3 destination address = 172.16.20.99

Layer 3 source address = 172.16.10.200

Layer 2 destination address = 00-00-0c-94-36-ab

Layer 2 source address = 00-00-0c-94-36-bb

Layer 3 destination address = 172.16.20.200

Layer 3 source address = 172.16.10.200

**34. What does the term “attenuation” mean in data communication?**

- strengthening of a signal by a networking device
- leakage of signals from one cable pair to another
- time for a signal to reach its destination
- **loss of signal strength as distance increases**



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

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

- The entire command, configure terminal, must be used.
- The administrator is already in global configuration mode.
- **The administrator must first enter privileged EXEC mode before issuing the command.**
- The administrator must connect via the console port to access global configuration mode.

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

- TCP
- IP
- UDP
- **POP**
- **DNS**
- Ethernet

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

- automation
- accounting
- authentication
- **authorization**

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

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

- **message size**
- **message encoding**
- connector specifications
- media selection

- **delivery options**
- end-device installation

**39. 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.

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

**What three network characteristics are described in this scenario? (Choose three.)**

- **security**
- **quality of service**
- scalability
- powerline networking
- integrity
- **fault tolerance**

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

- **improper termination**
- low-quality shielding in cable
- installing cables in conduit
- **low-quality cable or connectors**
- loss of light over long distances

**Explanation:** When terminated improperly, each cable is a potential source of physical layer performance degradation.

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

- **192.168.1.64/26**
- 192.168.1.32/27
- 192.168.1.32/28
- 192.168.1.64/29

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

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

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

- This host does not have a default gateway configured.
- **There are 4 hops between this device and the device at 192.168.100.1.**
- **There is connectivity between this device and the device at 192.168.100.1.**
- The connectivity between these two hosts allows for videoconferencing calls.
- The average transmission time between the two hosts is 2 milliseconds.

**Explain:**

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

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

- Capture traffic on the weekends when most employees are off work.
- **Capture traffic during peak utilization times to get a good representation of the different traffic types.**
- Only capture traffic in the areas of the network that receive most of the traffic such as the data center.
- **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.

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

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

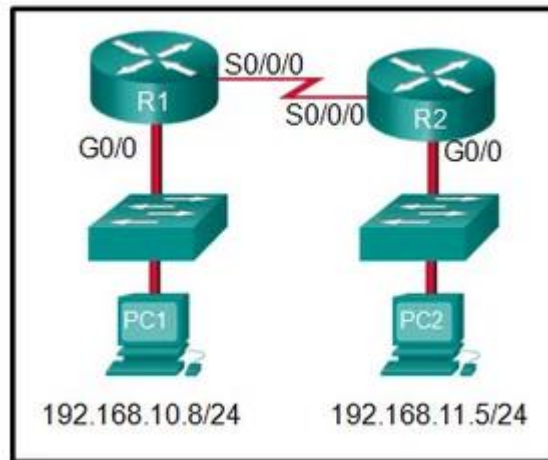
- All router interfaces will be automatically activated.
- **The IPv6 enabled router interfaces begin sending ICMPv6 Router Advertisement messages.**
- Each router interface will generate an IPv6 link-local address.
- It statically creates a global unicast address on this router.

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

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

**Explanation:** The TCP/IP model consists of four layers: application, transport, internet, and network access. The OSI model consists of seven layers: application, presentation, session, transport, network, data link, and physical. The top three layers of the OSI model: application, presentation, and session map to the application layer of the TCP/IP model.

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



header attached by PC1?

- nothing, because the router has a route to the destination network
- open the header and use it to determine whether the data is to be sent out S0/0/0
- open the header and replace the destination MAC address with a new one
- **remove the Ethernet header and configure a new Layer 2 header before sending it out S0/0/0**

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

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

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

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

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

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

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

- **255.255.255.128**
- 255.255.255.240
- 255.255.255.248
- 255.255.255.224

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

- **Neighbor Solicitation**
- Destination Unreachable
- Host Confirmation
- Time Exceeded
- **Router Advertisement**
- Route Redirection

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

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

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

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

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

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

- tracert
- ipconfig
- netstat
- **nslookup**

**Explain:**

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

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

- implements CSMA/CD over legacy shared half-duplex media
- **enables IPv4 and IPv6 to utilize the same physical medium**
- integrates Layer 2 flows between 10 Gigabit Ethernet over fiber and 1 Gigabit Ethernet over copper
- implements a process to delimit fields within an Ethernet 2 frame
- **places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame**

**Other case:**

- responsible for internal structure of Ethernet frame
- applies source and destination MAC addresses to Ethernet frame
- **handles communication between upper layer networking software and Ethernet NIC hardware**
- **adds Ethernet control information to network protocol data**
- implements trailer with frame check sequence for error detection

**Other case:**

- integrates Layer 2 flows between 10 Gigabit Ethernet over fiber and 1 Gigabit Ethernet over copper
- **places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame**
- implements CSMA/CD over legacy shared half-duplex media
- **adds Ethernet control information to network protocol data**
- applies source and destination MAC addresses to Ethernet frame

#### Other case:

- **enables IPv4 and IPv6 to utilize the same physical medium**
- **adds Ethernet control information to network protocol data**
- applies source and destination MAC addresses to Ethernet frame
- responsible for the internal structure of Ethernet frame
- implements trailer with frame check sequence for error detection

#### Other case:

- **enables IPv4 and IPv6 to utilize the same physical medium**
- applies source and destination MAC addresses to Ethernet frame
- integrates Layer 2 flows between 10 Gigabit Ethernet over fiber and 1 Gigabit Ethernet over copper
- **handles communication between upper layer networking software and Ethernet NIC hardware**
- responsible for internal structure of Ethernet frame

**Explanation:** The data link layer is actually divided into two sublayers:

+ Logical Link Control (LLC): This upper sublayer defines the software processes that provide services to the network layer protocols. It places information in the frame that identifies which network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IPv4 and IPv6, to utilize the same network interface and media.

+ Media Access Control (MAC): This lower sublayer defines the media access processes performed by the hardware. It provides data link layer addressing and delimiting of data according to the physical signaling requirements of the medium and the type of data link layer protocol in use.

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

- The switch can communicate with other hosts on the 172.16.100.0 network.
- **The switch can be remotely managed from a host on another network.**
- The switch is limited to sending and receiving frames to and from the gateway 172.16.100.1.
- The switch will have a management interface with the address 172.16.100.1.



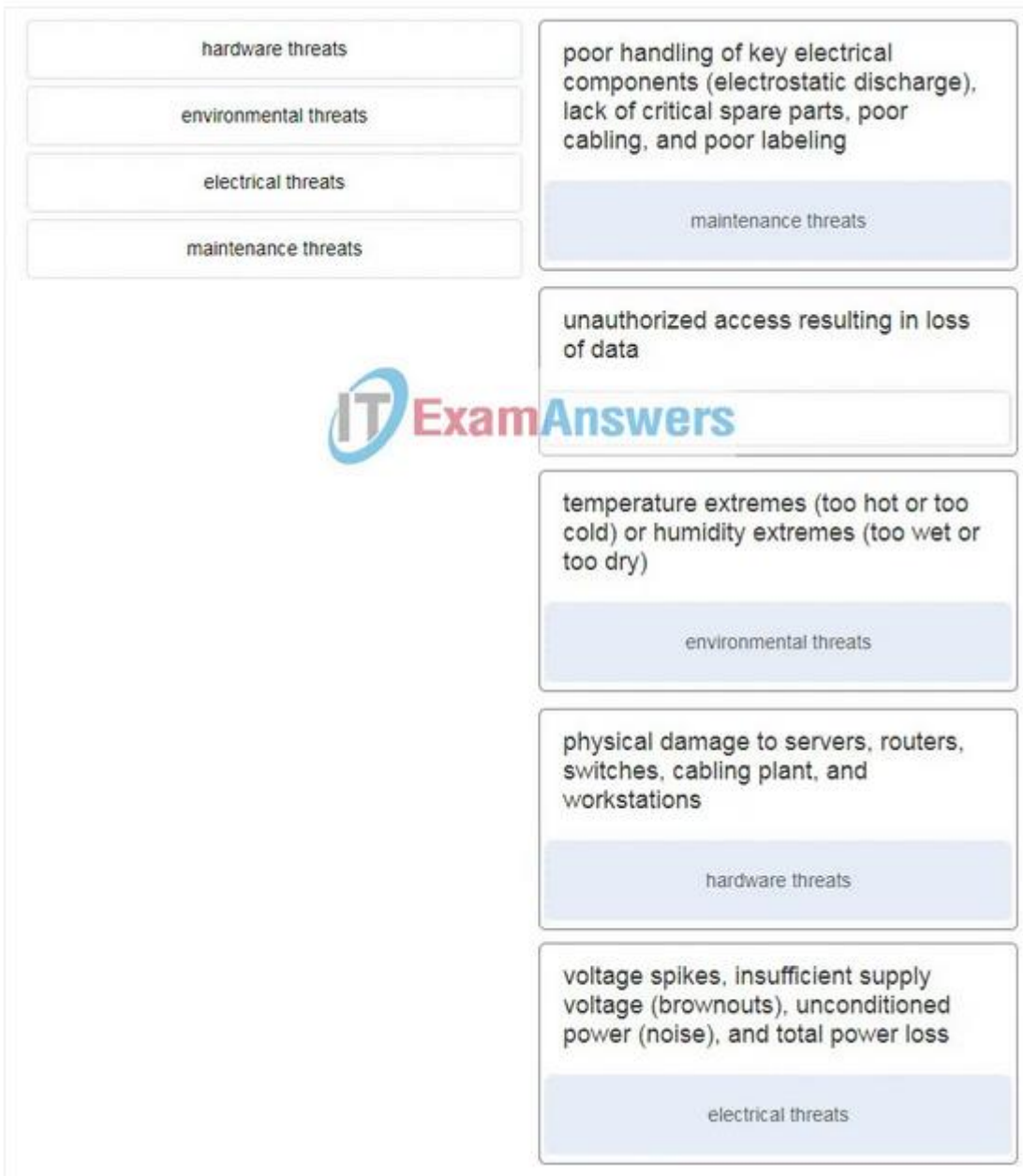
**Explanation:** A default gateway address is typically configured on all devices to allow them to communicate beyond just their local network. In a switch this is achieved using the command `ip default-gateway <ip address>`.

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

- The SSH client on the switch is enabled.
- The switch requires a username/password combination for remote access.
- **Communication between the switch and remote users is encrypted.**
- The switch requires remote connections via a proprietary client software.

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

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



59. A disgruntled employee is using some free wireless networking tools to determine information about the enterprise wireless networks. This person is planning on using this information to hack the wireless network. What type of attack is this?

- DoS
- access
- **reconnaissance**
- Trojan horse

**Explanation:** A reconnaissance attack is the unauthorized discovery and documentation of various computing networks, network systems, resources, applications, services, or vulnerabilities.

**60. What service is provided by HTTP?**

- Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.
- Allows for data transfers between a client and a file server.
- An application that allows real-time chatting among remote users.
- **A basic set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the web.**

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

- FTP
- **DHCP**
- Telnet
- SSH

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

- Switches become overloaded because they concentrate all the traffic from the attached subnets.
- **The ARP request is sent as a broadcast, and will flood the entire subnet.**
- The network may become overloaded because ARP reply messages have a very large payload due to the 48-bit MAC address and 32-bit IP address that they contain.
- A large number of ARP request and reply messages may slow down the switching process, leading the switch to make many changes in its MAC table.
- **All ARP request messages must be processed by all nodes on the local network.**

**Explanation:** ARP requests are sent as broadcasts:

(1) All nodes will receive them, and they will be processed by software, interrupting the CPU.

(2) The switch forwards (floods) Layer 2 broadcasts to all ports.

A switch does not change its MAC table based on ARP request or reply messages. The switch populates the MAC table using the source MAC address of all frames. The ARP payload is very small and does not overload the switch.

**63. A group of Windows PCs in a new subnet has been added to an Ethernet network. When testing the connectivity, a technician finds that these PCs can**

access local network resources but not the Internet resources. To troubleshoot the problem, the technician wants to initially confirm the IP address and DNS configurations on the PCs, and also verify connectivity to the local router. Which three Windows CLI commands and utilities will provide the necessary information? (Choose three.)

- netsh interface ipv6 show neighbor
- arp -a
- tracert
- **ping**
- **ipconfig**
- **nslookup**
- telnet

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

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

65. What characteristic describes antispyware?

- **applications that protect end devices from becoming infected with malicious software**
- a network device that filters access and traffic coming into a network
- software on a router that filters traffic based on IP addresses or applications
- a tunneling protocol that provides remote users with secure access into the network of an organization

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

- Telnet
- AUX
- **SSH**
- Console

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

- Implement a VPN.
- Implement network firewalls.

- Implement RAID.
- Implement strong passwords.
- **Update the operating system and other application software.**
- **Install and update antivirus software.**

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

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

- brute-force attack
- **Trojan horse**
- DoS
- buffer overflow

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

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

- User Datagram Protocol field
- transport layer error check field
- flow control field
- **frame check sequence field**
- error correction process field

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

- **255.255.255.248**
- 255.255.255.0
- 255.255.255.128
- 255.255.255.192

**71. What service is provided by POP3?**

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

- An application that allows real-time chatting among remote users.
- Allows remote access to network devices and servers.
- Uses encryption to provide secure remote access to network devices and servers.

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

- antispyware
- **virtual private networks**
- **intrusion prevention systems**
- strong passwords
- antivirus software

**73. What characteristic describes antivirus software?**

- **applications that protect end devices from becoming infected with malicious software**
- a network device that filters access and traffic coming into a network
- a tunneling protocol that provides remote users with secure access into the network of an organization
- software on a router that filters traffic based on IP addresses or applications

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

- It checks the value of the TTL field and if it is 0, it discards the packet and sends a Destination Unreachable message to the source host.
- It checks the value of the TTL field and if it is 100, it discards the packet and sends a Destination Unreachable message to the source host.
- **It decrements the value of the TTL field by 1 and if the result is 0, it discards the packet and sends a Time Exceeded message to the source host.**
- It increments the value of the TTL field by 1 and if the result is 100, it discards the packet and sends a Parameter Problem message to the source host.

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

- DNS
- DHCP
- SMTP
- **TFTP**

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

- Configure DNS on the router.
- Generate two-way pre-shared keys.
- **Configure the IP domain name on the router.**
- **Generate the SSH keys.**
- **Enable inbound vty SSH sessions.**
- Enable inbound vty Telnet sessions.

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

- handles communication between upper layer networking software and Ethernet NIC hardware
- implements trailer with frame check sequence for error detection
- places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame
- implements a process to delimit fields within an Ethernet 2 frame
- adds Ethernet control information to network protocol data

**Case 2:**

- places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame
- adds Ethernet control information to network protocol data
- responsible for internal structure of Ethernet frame
- enables IPv4 and IPv6 to utilize the same physical medium
- implements trailer with frame check sequence for error detection

**Case 3:**

- integrates Layer 2 flows between 10 Gigabit Ethernet over fiber and 1 Gigabit Ethernet over copper
- enables IPv4 and IPv6 to utilize the same physical medium
- handles communication between upper layer networking software and Ethernet NIC hardware
- adds Ethernet control information to network protocol data
- implements CSMA/CD over legacy shared half-duplex media

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

- all IPv6 enabled devices on the local link
- all IPv6 DHCP servers

- all IPv6 enabled devices across the network
- **all IPv6 configured routers on the local link**

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

- **subnet ID**
- subnet mask
- broadcast address
- **global routing prefix**
- **interface ID**

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

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

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

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

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

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

- token passing
- **CSMA/CA**
- priority ordering
- CSMA/CD



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

- provides the formatting of data
- provides end-to-end delivery of data between hosts
- provides delivery of data between two applications
- **provides for the exchange of frames over a common local media**

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

- to ensure that segments arrive in order at the destination
- to end communication when data transmission is complete
- to inform a source to retransmit data from a specific point forward
- **to request that a source decrease the rate at which it transmits data**

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

**85. What characteristic describes spyware?**

- a network device that filters access and traffic coming into a network
- **software that is installed on a user device and collects information about the user**
- an attack that slows or crashes a device or network service
- the use of stolen credentials to access private data

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

- **store-and-forward switching**
- borderless switching
- ingress port buffering
- cut-through switching

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

- FEC0::/10
- FDEE::/7
- **FE80::/10**
- FF00::/8

**Explain:**

Link-local addresses are in the range of FE80::/10 to FEBF::/10. The original IPv6

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

**88. What service is provided by FTP?**

- A basic set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the web.
- An application that allows real-time chatting among remote users.
- **Allows for data transfers between a client and a file server.**
- Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.

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

- **DNS server**
- source port number
- HTTP server
- source MAC address
- **default gateway**

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

- NAT adds authentication capability to IPv4.
- **NAT introduces problems for some applications that require end-to-end connectivity.**
- NAT will impact negatively on switch performance.
- **NAT provides a solution to slow down the IPv4 address depletion.**
- NAT improves packet handling.
- NAT causes routing tables to include more information.

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

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

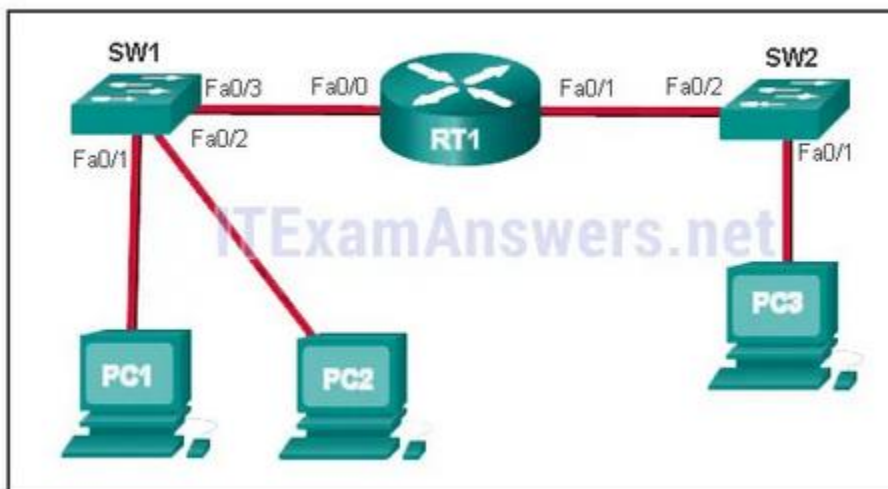
- 0C6F:65FF:FEC2:BDF8
- **1E6F:65FF:FEC2:BDF8**
- C16F:65FF:FEC2:BDF8
- 106F:65FF:FEC2:BDF8

**Explanation:** To derive the EUI-64 interface ID by using the MAC address 1C-6F-65-C2-BD-F8, three steps are taken.

- Change the seventh bit of the MAC address from a binary 0 to a binary 1 which changes the hex C, into a hex E.
- Insert hex digits FFFE into the middle of the address.
- Rewrite the address in IPv6 format.

The three steps, when complete, give the interface ID of **1E6F:65FF:FEC2:BDF8**.

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



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

**93. What service is provided by BOOTP?**

- Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.
- Allows for data transfers between a client and a file server.
- **Legacy application that enables a diskless workstation to discover its own IP address and find a BOOTP server on the network.**
- A basic set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the web.

**94. What characteristic describes adware?**

- a network device that filters access and traffic coming into a network
- **software that is installed on a user device and collects information about the user**
- the use of stolen credentials to access private data
- an attack that slows or crashes a device or network service

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

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

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

requires a specific user interface

no dedicated server is required

a background service is required

client and server roles are set on a per request basis

devices can only function in one role at a time

peer-to-peer network

no dedicated server is required

client and server roles are set on a per request basis

peer-to-peer application

requires a specific user interface

a background service is required

ITN (Version 7.00) – ITNv7 Final Exam

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 application

[#] 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.

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

- error detection
- frame delimiting
- **accessing the media**
- **data encapsulation**

- logical addressing

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

Switch# show ip interface brief					
Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	manual	up	up
FastEthernet0/2	unassigned	YES	manual	down	down
FastEthernet0/3	unassigned	YES	manual	down	down
FastEthernet0/5	unassigned	YES	manual	down	down
FastEthernet0/6	unassigned	YES	manual	down	down
(output omitted)					
FastEthernet0/23	unassigned	YES	manual	down	down
FastEthernet0/24	unassigned	YES	manual	down	down
Vlan1	192.168.11.3	YES	manual	up	up

- 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.

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

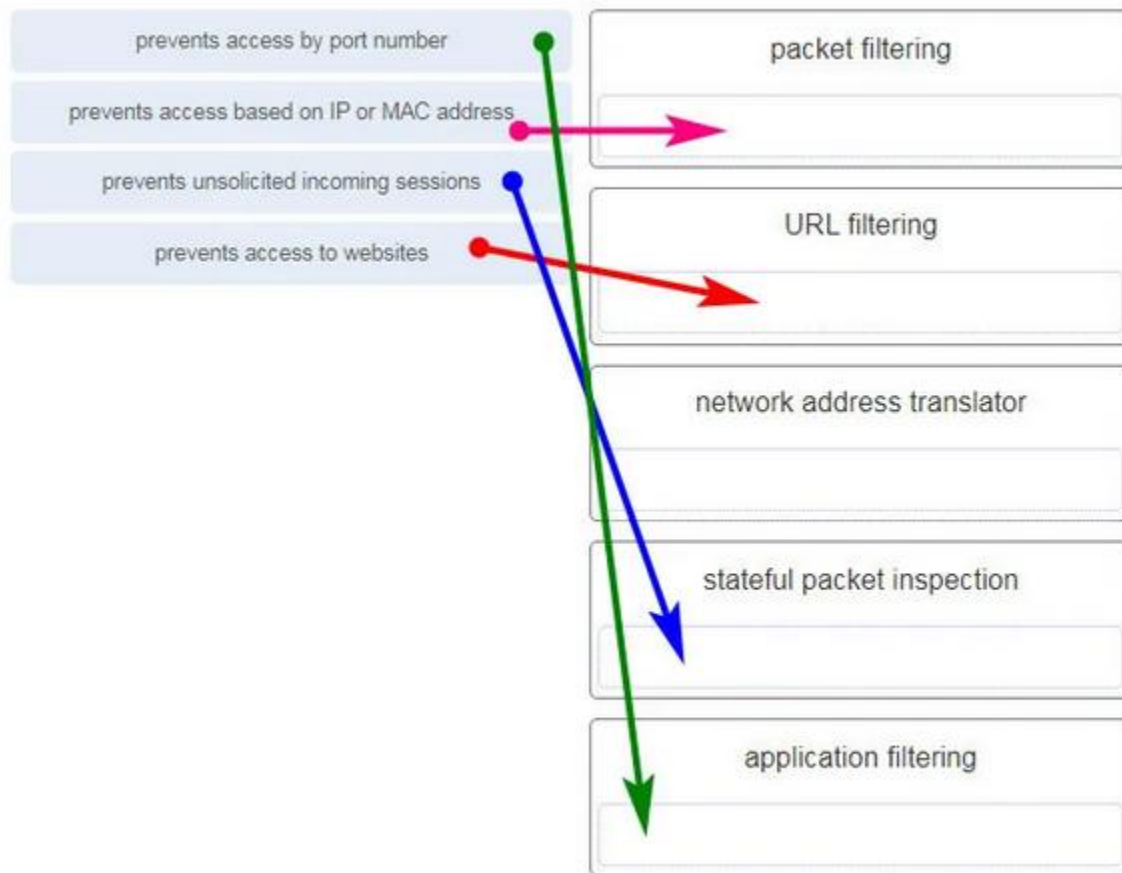


100. What is the subnet ID associated with the IPv6 address 2001:DA48:FC5:A4:3D1B::1/64?

- 2001:DA48::/64
- 2001:DA48:FC5::A4:/64
- **2001:DA48:FC5:A4::/64**
- 2001::/64



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



- packet filtering – prevents access based on IP or MAC address
- URL filtering – prevents access to websites
- network address translator – (none)
- stateful packet inspection – prevents unsolicited incoming sessions
- application filtering – prevents access by port number

**Explain:** Firewall products come packaged in various forms. These products use different techniques for determining what will be permitted or denied access to a network. They include the following:

- + Packet filtering – Prevents or allows access based on IP or MAC addresses
- + Application filtering – Prevents or allows access by specific application types based on port numbers
- + URL filtering – Prevents or allows access to websites based on specific URLs or keywords
- + Stateful packet inspection (SPI) – Incoming packets must be legitimate responses to requests from internal hosts. Unsolicited packets are blocked unless permitted



specifically. SPI can also include the capability to recognize and filter out specific types of attacks, such as denial of service (DoS)

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

- syslog records and messages
- **the network performance baseline**
- debug output and packet captures
- network configuration files

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

- It requires encrypted passwords to be used when connecting remotely to a router or switch with Telnet.
- **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 encrypts passwords as they are sent across the network.

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

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

- **The Source Address field name from IPv4 is kept in IPv6.**
- The Version field from IPv4 is not kept in IPv6.
- The Destination Address field is new in IPv6.
- The Header Checksum field name from IPv4 is kept in IPv6.
- **The Time-to-Live field from IPv4 has been replaced by the Hop Limit field in IPv6.**

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

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

**105. A network administrator wants to have the same network mask for all networks at a particular small site. The site has the following networks and number of devices:**

**IP phones – 22 addresses**

**PCs – 20 addresses needed**

**Printers – 2 addresses needed**

**Scanners – 2 addresses needed**

The network administrator has deemed that 192.168.10.0/24 is to be the network used at this site. Which single subnet mask would make the most efficient use of the available addresses to use for the four subnetworks?

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

**106. What characteristic describes identity theft?**

- **the use of stolen credentials to access private data**
- software on a router that filters traffic based on IP addresses or applications
- software that identifies fast-spreading threats
- a tunneling protocol that provides remote users with secure access into the network of an organization

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

- 255.255.255.240
- **255.255.255.0**
- 255.255.255.248
- 255.255.255.224

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

- cost per meter (foot)
- **cable lengths**
- connector color
- **pinouts**

- **connector types**
- tensile strength of plastic insulator

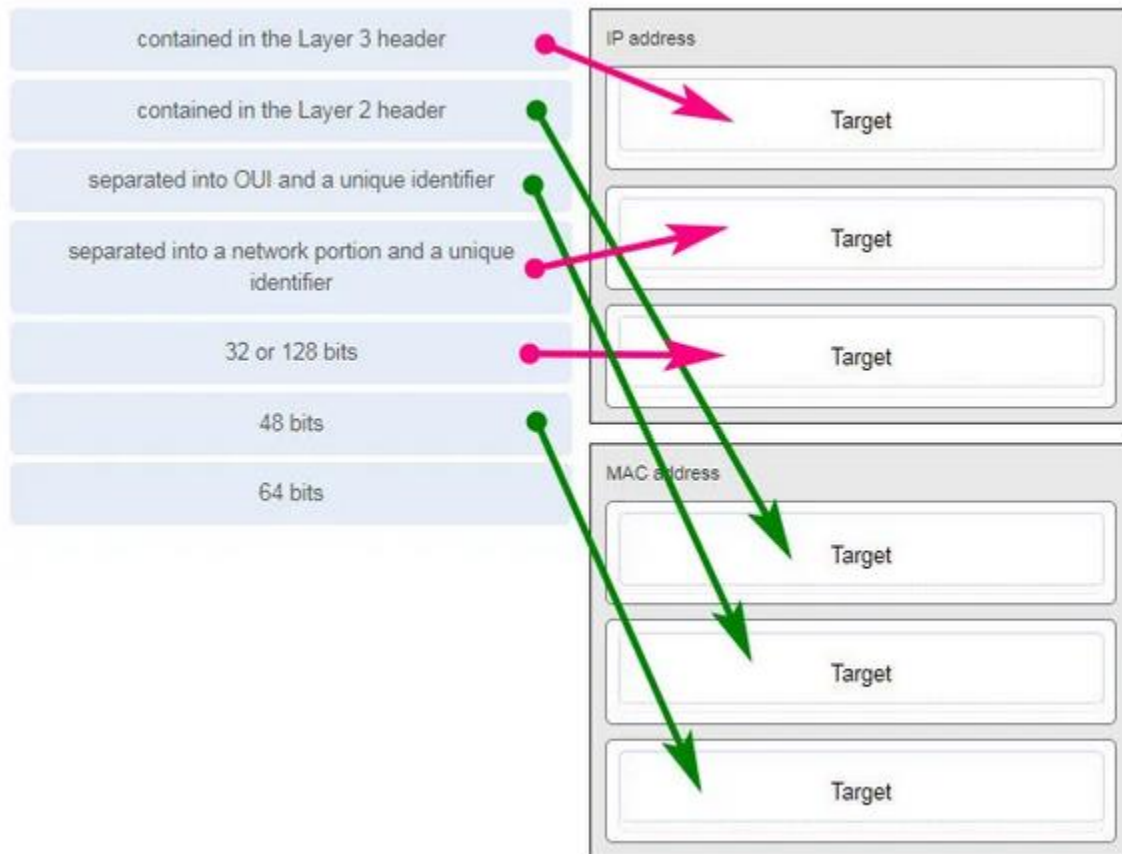
109. Refer to the exhibit. What is wrong with the displayed termination?



- 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.

**Explanation:** 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.

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



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

- **IMAP**
- FTP
- SSH
- Telnet

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

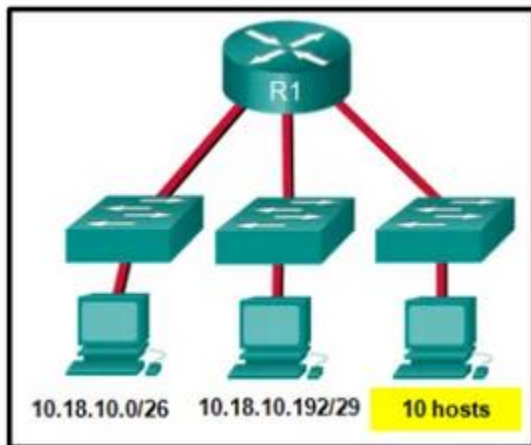
- default window size
- connectionless communication
- **port numbering**
- 3-way handshake
- ability to carry digitized voice
- **use of checksum**

**Explain:**

Both TCP and UDP use source and destination port numbers to distinguish different data streams and to forward the right data segments to the right applications. Error

checking the header and data is done by both protocols by using a checksum calculation to determine the integrity of the data that is received. TCP is connection-oriented and uses a 3-way handshake to establish an initial connection. TCP also uses window to regulate the amount of traffic sent before receiving an acknowledgment. UDP is connectionless and is the best protocol for carry digitized VoIP signals.

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



- 10.18.10.200/28
- **10.18.10.208/28**
- 10.18.10.240/27
- 10.18.10.200/27
- 10.18.10.224/27
- **10.18.10.224/28**

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

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

- **FTP**
- LDAP
- SLP
- SNMP

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

- attached Ethernet cable
- IP address
- **MAC address**
- RJ-45 port
- TCP/IP protocol stack

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

- 255.255.255.192
- 255.255.255.248
- 255.255.255.224
- **255.255.255.240**

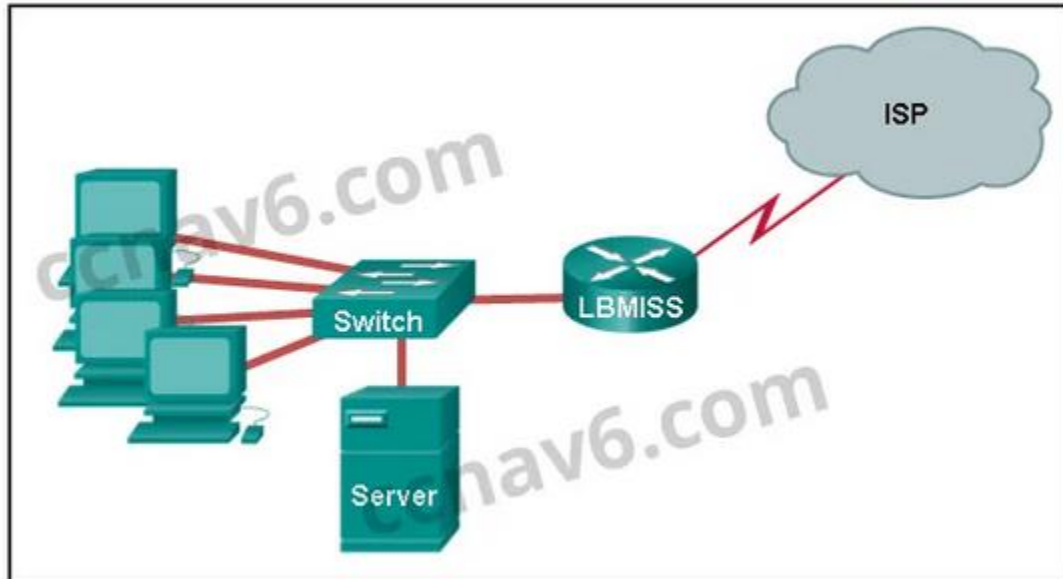
**117. What technique is used with UTP cable to help protect against signal interference from crosstalk?**

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

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

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

properties of the workgroup server to allow connectivity to the Internet?



- 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

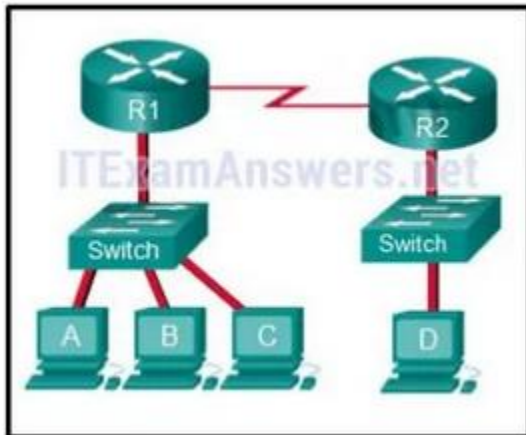
**Explain:**

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)

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

host A?



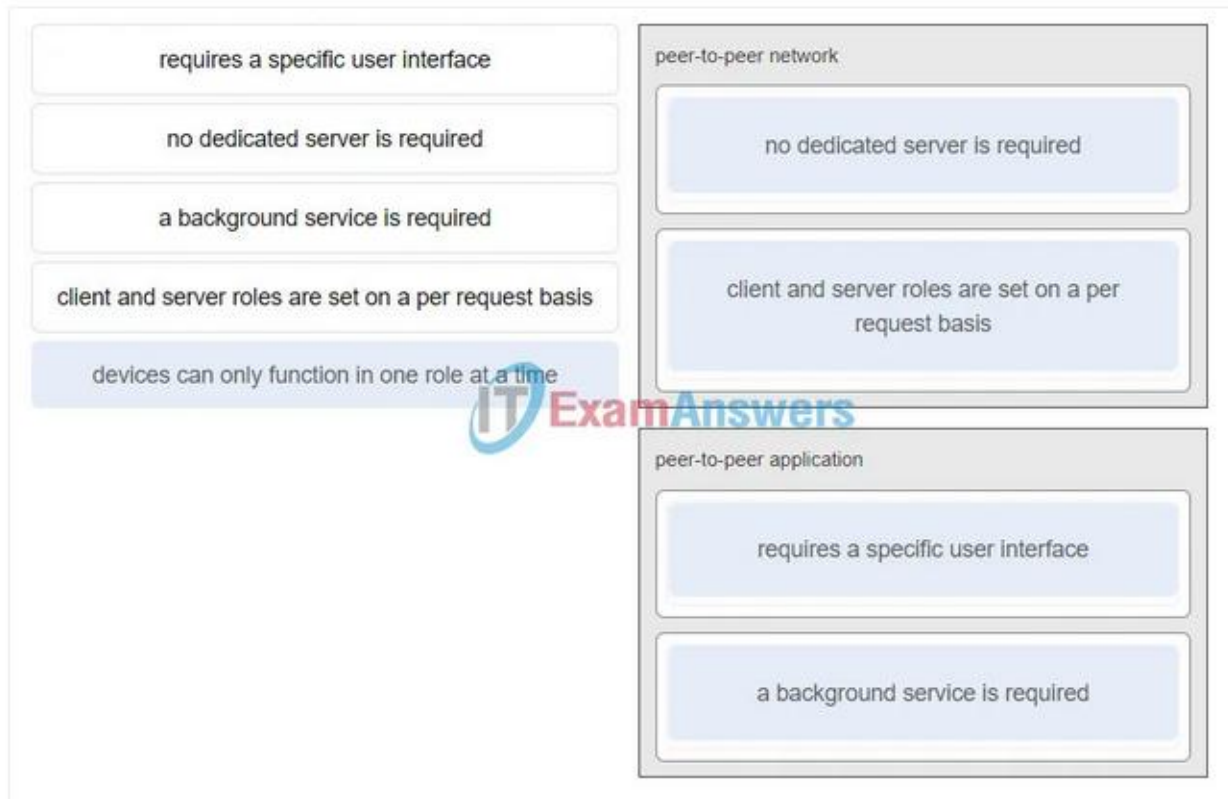
- only host D
- only router R1
- only hosts A, B, and C
- only hosts A, B, C, and D
- only hosts B and C
- **only hosts B, C, and router R1**

**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.

**120. 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 application

[#] requires a specific user interface

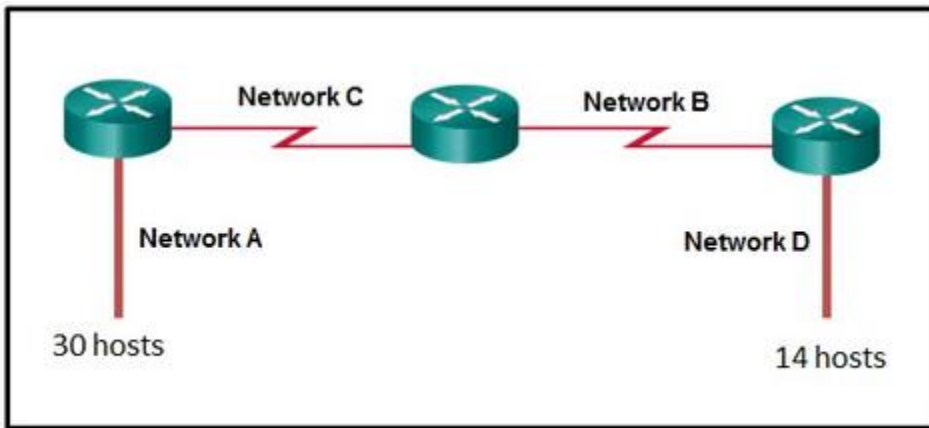
[#] a background service is required

### 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.

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

subnets?



- 88
- **200**
- 72
- 224
- 158

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



LC conector



SC conector



BNC



RJ 11

**True Answer:**



RJ 45 (true answer)

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

- **SSH**
- SMB/CIFS
- HTTPS
- SLP

**124. What characteristic describes an IPS?**

- a tunneling protocol that provides remote users with secure access into the network of an organization
- **a network device that filters access and traffic coming into a network**
- software that identifies fast-spreading threats
- software on a router that filters traffic based on IP addresses or applications

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

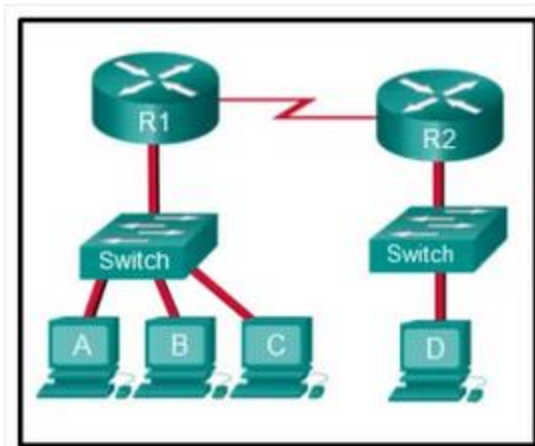
### 125. What service is provided by DHCP?

- An application that allows real-time chatting among remote users.
- Allows remote access to network devices and servers.
- **Dynamically assigns IP addresses to end and intermediary devices.**
- Uses encryption to provide secure remote access to network devices and servers.

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



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



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

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

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

- Bluetooth
- **Zigbee**
- WiMAX
- Wi-Fi

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

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

- **neighbor solicitations**
- echo requests
- **neighbor advertisements**
- echo replies

- router solicitations
- router advertisements

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

- It must send a DHCPv6 INFORMATION-REQUEST message to request the address of the DNS server.
- It must send a DHCPv6 REQUEST message to the DHCPv6 server to request permission to use this address.
- It must send an ICMPv6 Router Solicitation message to determine what default gateway it should use.
- **It must send an ICMPv6 Neighbor Solicitation message to ensure that the address is not already in use on the network.**

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

- The default gateway is not operational.
- The default gateway device is configured with the wrong IP address.
- **Security rules are applied to the default gateway device, preventing it from processing ping requests.**
- The TCP/IP stack on the default gateway is not working properly.

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

- **256**
- 512
- 1024
- 4096

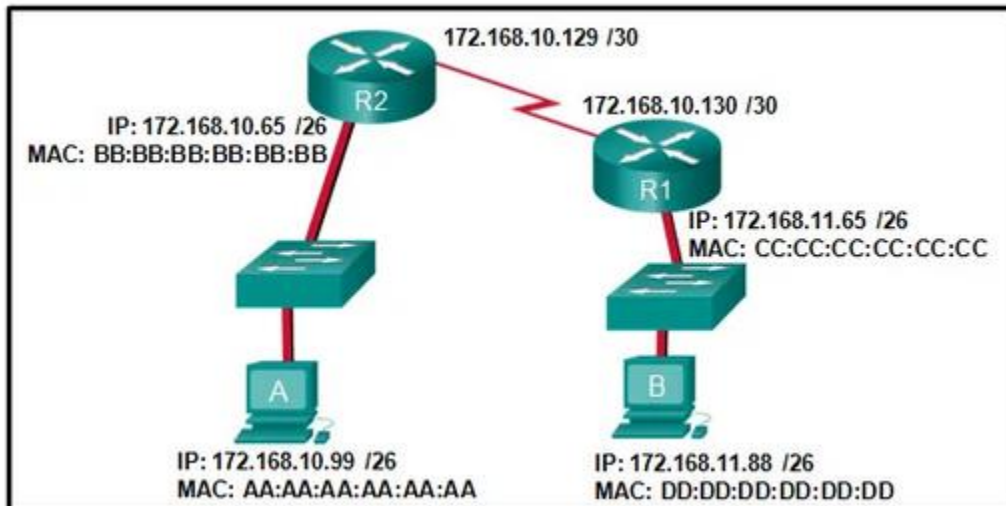
**133. What subnet mask is needed if an IPv4 network has 40 devices that need IP addresses and address space is not to be wasted?**

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

**Explanation:** In order to accommodate 40 devices, 6 host bits are needed. With 6 bits, 64 addresses are possible, but one address is for the subnet number and one address

is for a broadcast. This leaves 62 addresses that can be assigned to network devices. The mask associated with leaving 6 host bits for addressing is 255.255.255.192.

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



- DD:DD:DD:DD:DD:DD
- 172.168.10.99
- CC:CC:CC:CC:CC:CC
- 172.168.10.65
- **BB:BB:BB:BB:BB:BB**
- AA:AA:AA:AA:AA:AA

**Explain:**

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

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

- Technology is integrated into every-day appliances allowing them to interconnect with other devices, making them more 'smart' or automated.
- **Network capabilities are extended without requiring investment in new infrastructure, personnel, or software.**
- End users have the freedom to use personal tools to access information and communicate across a business network.



- Home networking uses existing electrical wiring to connect devices to the network wherever there is an electrical outlet, saving the cost of installing data cables.

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

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

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

**137. 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 the packet to a remote network.

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

- The device with the electronic token is the only one that can transmit after a collision.
- **A device listens and waits until the media is not busy before transmitting.**
- **After detecting a collision, hosts can attempt to resume transmission after a random time delay has expired.**

- **All of the devices on a segment see data that passes on the network medium.**
- A jam signal indicates that the collision has cleared and the media is not busy.
- Devices can be configured with a higher transmission priority.

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

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

- 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.

**140. 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

**Explain:**

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

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

- **directing data packets to destination hosts on other networks**
- placing data on the network medium

- carrying data between processes that are running on source and destination hosts
- providing dedicated end-to-end connections
- **providing end devices with a unique network identifier**

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

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

- Directly connected interfaces will have two route source codes in the routing table: C and S .
- If there are two or more possible routes to the same destination, the route associated with the higher metric value is included in the routing table.
- The netstat -r command can be used to display the routing table of a router.
- The routing table lists the MAC addresses of each active interface.
- **It stores information about routes derived from the active router interfaces.**
- **If a default static route is configured in the router, an entry will be included in the routing table with source code S .**

**143. What characteristic describes a VPN?**

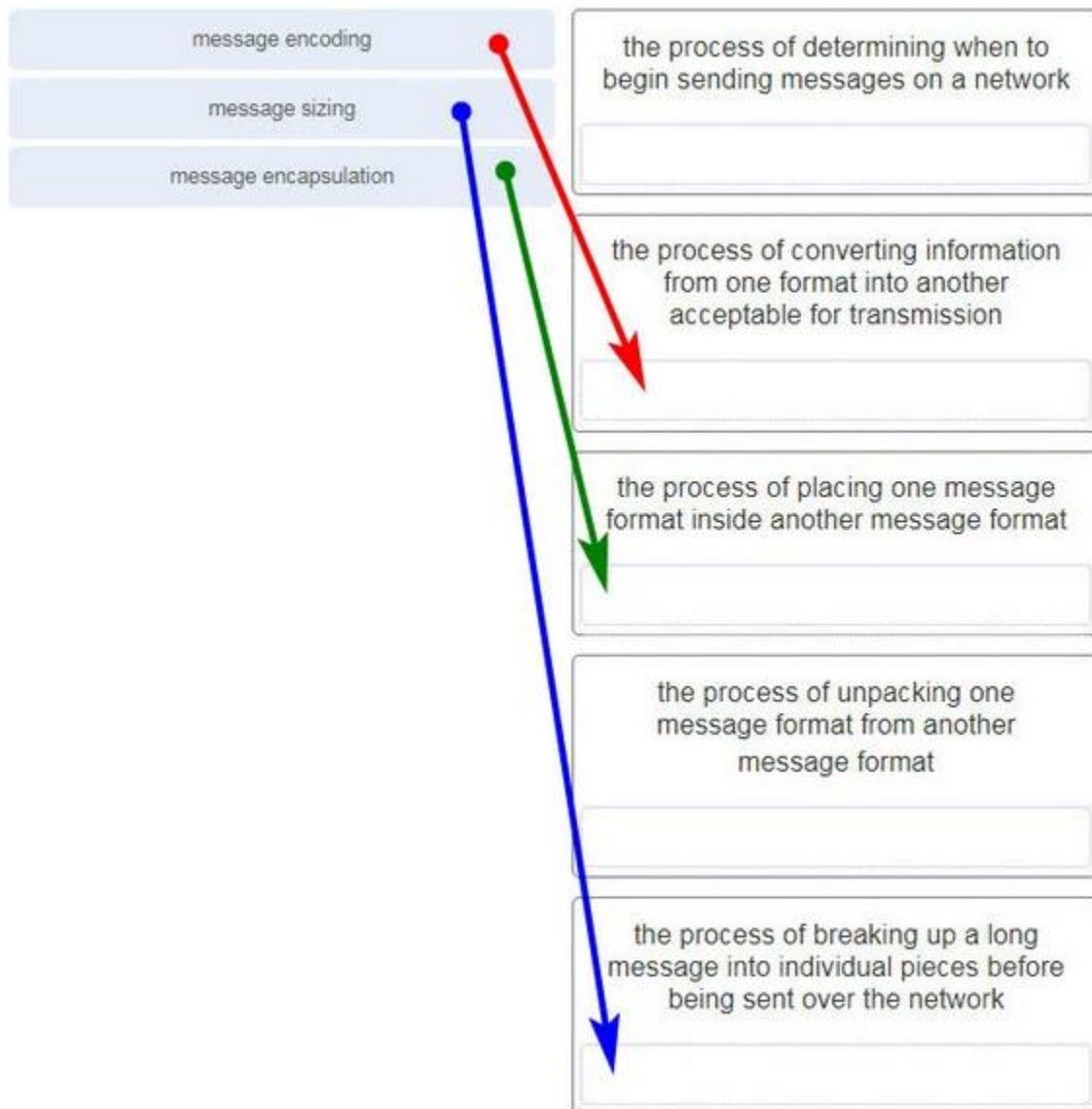
- software on a router that filters traffic based on IP addresses or applications
- software that identifies fast-spreading threats
- **a tunneling protocol that provides remote users with secure access into the network of an organization**
- a network device that filters access and traffic coming into a network

**144. 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

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

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



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

- the network domain of the destination host
- the IP address of the default gateway
- the MAC address of the destination host
- **the MAC address of the default gateway**

**Explanation:** A frame is encapsulated with source and destination MAC addresses. The source device will not know the MAC address of the remote host. An ARP request will be sent by the source and will be responded to by the router. The router will respond

with the MAC address of its interface, the one which is connected to the same network as the source.

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

- A company can monopolize the market.
- The protocol can only be run on equipment from a specific vendor.
- An open standard protocol is not controlled or regulated by standards organizations.
- **It encourages competition and promotes choices.**

**Explain:**

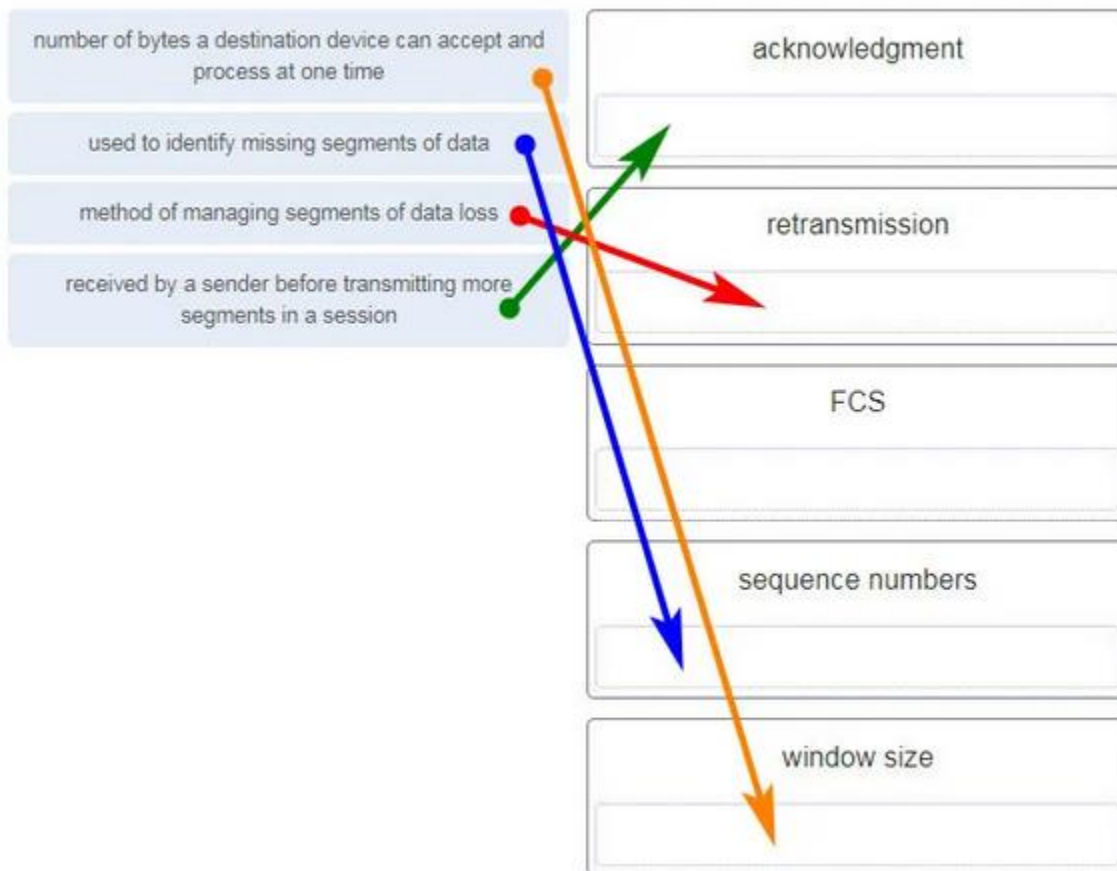
A monopoly by one company is not a good idea from a user point of view. If a protocol can only be run on one brand, it makes it difficult to have mixed equipment in a network. A proprietary protocol is not free to use. An open standard protocol will in general be implemented by a wide range of vendors.

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

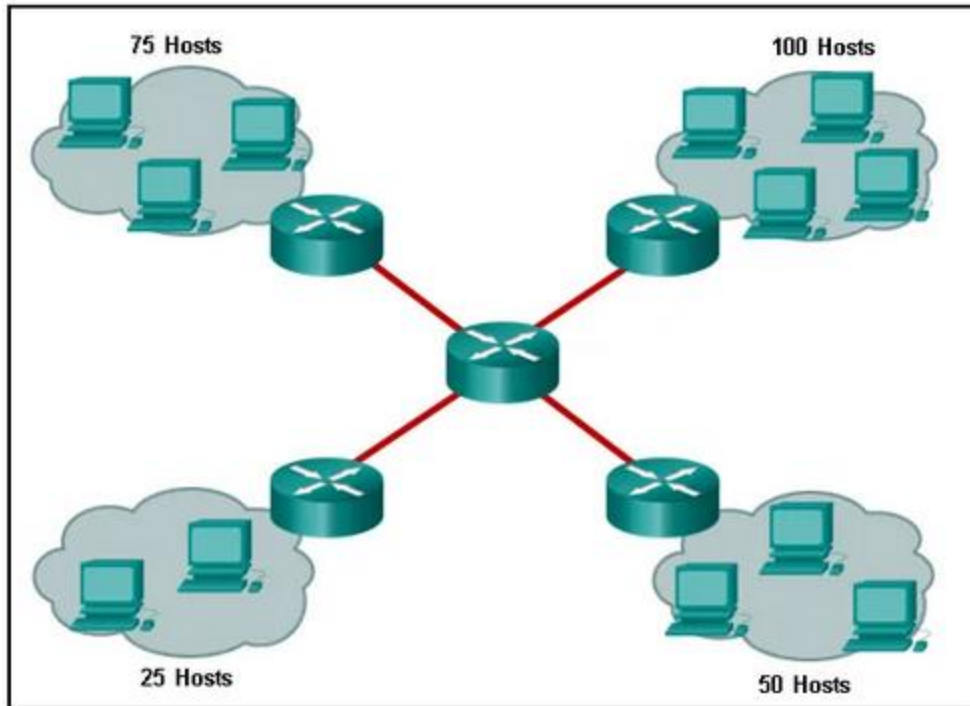
- **The source port field identifies the running application or service that will handle data returning to the PC.**
- The TCP process running on the PC randomly selects the destination port when establishing a session with the server.
- **UDP segments are encapsulated within IP packets for transport across the network.**
- **The UDP destination port number identifies the application or service on the server which will handle the data.**
- TCP is the preferred protocol when a function requires lower network overhead.
- The TCP source port number identifies the sending host on the network.

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

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



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



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

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

**151. A network administrator wants to have the same subnet mask for three subnetworks at a small site. The site has the following networks and numbers of devices:**

Subnetwork A: IP phones – 10 addresses  
 Subnetwork B: PCs – 8 addresses  
 Subnetwork C: Printers – 2 addresses

**What single subnet mask would be appropriate to use for the three subnetworks?**

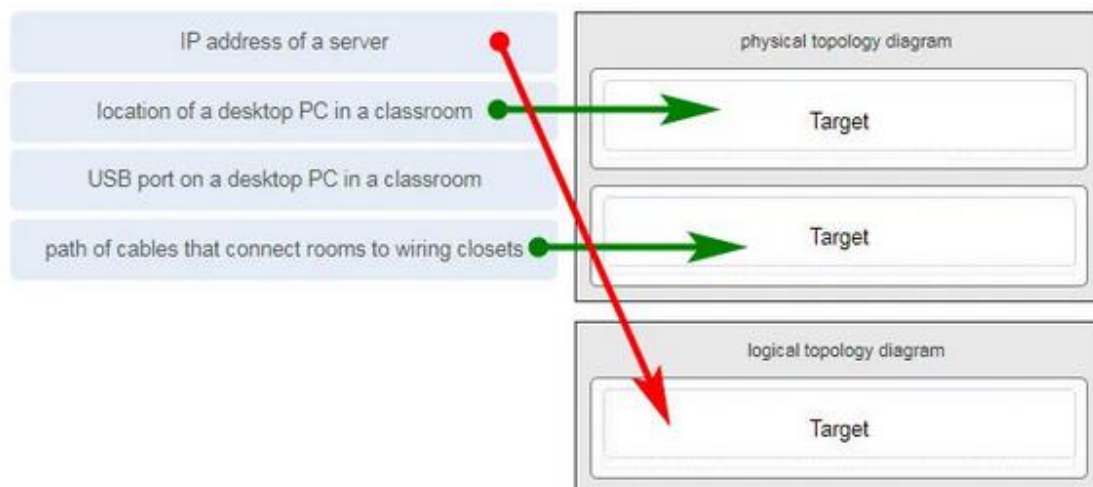
- 255.255.255.0
- **255.255.255.240**
- 255.255.255.248
- 255.255.255.252



**Explain:**

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

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



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

- **IP addresses**
- interface descriptions
- MAC addresses
- next-hop addresses
- **Layer 1 statuses**
- speed and duplex settings

**Explanation:** The command show ip interface brief shows the IP address of each interface, as well as the operational status of the interfaces at both Layer 1 and Layer 2. In order to see interface descriptions and speed and duplex settings, use the command show running-config interface. Next-hop addresses are displayed in the routing table with the command show ip route, and the MAC address of an interface can be seen with the command show interfaces.

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



- ping
- nslookup
- **tracert**
- ipconfig /displaydns

**Explanation:** The Command Prompt command tracert will map the path from the PC to the web server and measure transit delays of packets across the network.

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

- Header Length
- Differentiated Services
- **Time-to-Live**
- Fragment Offset

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

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

- **Fiber optic cabling requires different termination and splicing expertise from what copper cabling requires.**
- Fiber optic cabling requires specific grounding to be immune to EMI.
- Fiber optic cabling is susceptible to loss of signal due to RFI.
- Fiber optic cable is able to withstand rough handling.
- **Fiber optic provides higher data capacity but is more expensive than copper cabling.**

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

a link-local address	127.0.0.1
a public address	a loopback address
an experimental address	172.18.45.9
a loopback address	
IT ExamAnswers	
	240.2.6.255
	an experimental address
	198.133.219.2
	a public address
	169.254.1.5
	a link-local address

ITN (Version 7.00) – ITNv7 Final Exam

**158. A user is executing a traceroute 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.

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

- virus
- **worm**
- phishing
- spam

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