

Cisco.Actualtests.100-101.v2013-11-28.by.Adam.137q



Number: 100-101
Passing Score: 800
Time Limit: 120 min
File Version: 12.5

Exam Code: 100-101

Exam Name: CCNA Interconnecting Cisco Networking Devices 1 (ICND1)



Sections

1. Operation of IP Data Networks
2. LAN Switching Technologies
3. IP addressing (IPv4 / IPv6)
4. IP Routing Technologies
5. IP Services
6. Network Device Security
7. Troubleshooting

Cisco ICND1-100-101**QUESTION 1**

Which two statements describe the operation of the CSMA/CD access method? (Choose two.)

- A. In a CSMA/CD collision domain, multiple stations can successfully transmit data simultaneously.
- B. In a CSMA/CD collision domain, stations must wait until the media is not in use before transmitting.
- C. The use of hubs to enlarge the size of collision domains is one way to improve the operation of the CSMA/CD access method.
- D. After a collision, the station that detected the collision has first priority to resend the lost data.
- E. After a collision, all stations run a random backoff algorithm. When the backoff delay period has expired, all stations have equal priority to transmit data.
- F. After a collision, all stations involved run an identical backoff algorithm and then synchronize with each other prior to transmitting data.

Correct Answer: BE

Section: LAN Switching Technologies

Explanation

Explanation/Reference:

Explanation:

Ethernet networking uses Carrier Sense Multiple Access with Collision Detect (CSMA/CD), a

protocol that helps devices share the bandwidth evenly without having two devices transmit at the same time on the network medium. CSMA/CD was created to overcome the problem of those collisions that occur when packets are transmitted simultaneously from different nodes. And trust me, good collision management is crucial, because when a node transmits in a CSMA/CD network, all the other nodes on the network receive and examine that transmission. Only bridges and routers can effectively prevent a transmission from propagating throughout the entire network! So, how does the CSMA/CD protocol work? Like this: when a host wants to transmit over the network, it first checks for the presence of a digital signal on the wire. If all is clear (no other host is transmitting), the host will then proceed with its transmission. But it doesn't stop there. The transmitting host constantly monitors the wire to make sure no other hosts begin transmitting. If the host detects another signal on the wire, it sends out an extended jam signal that causes all nodes on the segment to stop sending data (think, busy signal). The nodes respond to that jam signal by waiting a while before attempting to transmit again. Backoff algorithms determine when the colliding stations can retransmit. If collisions keep occurring after 15 tries, the nodes attempting to transmit will then time out.

QUESTION 2

Which address type does a switch use to make selective forwarding decisions?

- A. source IP address
- B. destination IP address
- C. source and destination IP address

- D. source MAC address
- E. destination MAC address

Correct Answer: E

Section: LAN Switching Technologies

Explanation

Explanation/Reference:

Explanation:

Switches analyze the destination MAC to make its forwarding decision since it is a layer 2 device. Routers use the destination IP address to make forwarding decisions.

QUESTION 3

On a Cisco switch, which protocol determines if an attached VoIP phone is from Cisco or from another vendor?

- A. RTP
- B. TCP
- C. CDP
- D. UDP

Correct Answer: C

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Cisco Discovery Protocol (CDP)

Reference:

<http://computernetworkingnotes.com/cisco-devices-administration-and-configuration/cisco-discovery-protocol.html>

Explanation:

The Cisco Unified IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.

Cisco Discovery Protocol (CDP) is a proprietary protocol designed by Cisco to help administrators collect information about both locally attached and remote devices. By using CDP, you can gather hardware and protocol information about neighbor devices, which is useful info for troubleshooting the network.

CDP messages are generated every 60 seconds as multicast messages on each of its active interfaces.

The information shared in a CDP packet about a Cisco device includes the following:

- Name of the device configured with the hostname command
- IOS software version
- Hardware capabilities, such as routing, switching, and/or bridging
- Hardware platform, such as 2600, 2950, or 1900
- The layer-3 address(es) of the device
- The interface the CDP update was generated on

QUESTION 4

A switch receives a frame on one of its ports. There is no entry in the MAC address table for the destination MAC address. What will the switch do with the frame?

- A. drop the frame
- B. forward it out of all ports except the one that received it
- C. forward it out of all ports
- D. store it until it learns the correct port

Correct Answer: B

Section: LAN Switching Technologies

Explanation

Explanation/Reference:

QUESTION 5

At which layer of the OSI model does the protocol that provides the information that is displayed by the show cdp neighbors command operate?

- A. application
- B. transport
- C. network
- D. physical
- E. data link

Correct Answer: E

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Cisco Discovery Protocol (CDP)

Reference:

<http://computernetworkingnotes.com/cisco-devices-administration-and-configuration/cisco-discovery-protocol.html>

Explanation:

CDP is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco- manufactured devices (routers, bridges, access servers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. With CDP, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices running lower-layer, transparent protocols.

CDP allows devices to share basic configuration information without even configuring any protocol specific information and is enabled by default on all interfaces.

CDP is a Datalink Protocol occurring at Layer 2 of the OSI model.

CDP is not routable and can only go over to directly connected devices.

CDP is enabled, by default, on all Cisco devices. CDP updates are generated as multicasts every 60 seconds with a hold-down period of 180 seconds for a missing neighbor. The `no cdp run` command globally disables CDP, while the `no cdp enable` command disables CDP on an interface. Use `show cdp neighbors` to list out your directly connected Cisco neighboring devices. Adding the `detail` parameter will display the layer-3 addressing configured on the neighbor.

QUESTION 6

Which two characteristics apply to Layer 2 switches? (Choose two.)

- A. increases the number of collision domains
- B. decreases the number of collision domains
- C. implements VLAN
- D. decreases the number of broadcast domains
- E. uses the IP address to make decisions for forwarding data packets

Correct Answer: AC

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Explanation:

Layer 2 switches offer a number of benefits to hubs, such as the use of VLANs and each switch port is in its own separate collision domain, thus eliminating collisions on the segment.

QUESTION 7

Which two commands will display the current IP address and basic Layer 1 and 2 status of an interface? (Choose two.)

- A. router#show version
- B. router#show ip interface
- C. router#show protocols
- D. router#show controllers
- E. router#show running-config

Correct Answer: CD

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

Show protocols command displays the status of configured Layer 2 and 3 protocols while show controllers displays statistics for interface hardware layer 1.

QUESTION 8

Which two characteristics describe the access layer of the hierarchical network design model? (Choose two.)

- A. layer 3 support
- B. port security
- C. redundant components
- D. VLANs
- E. PoE

Correct Answer: BD

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Original answer was "A" and "B"

The Hierarchical Network Model

Reference 1:

<http://www.ciscopath.com/content/61/>

Reference 2:

http://www.mcmcs.com/cisco/guides/hierarchical_model.shtml

Explanation:

Access layer

The main purpose of the access layer is to provide direct connection to devices on the network and controlling which devices are allowed to communicate over it. The access layer interfaces with end devices, such as PCs, printers, and IP phones, to provide access to the rest of the network. The access layer can include routers, switches, bridges, hubs, and wireless access points (AP).

Switch features in the Access layer:

- Port security
- VLANs
- Fast Ethernet/Gigabit Ethernet
- Power over Ethernet (PoE)
- Link aggregation
- Quality of Service (QoS)

QUESTION 9

What is the purpose of assigning an IP address to a switch?

- A. provides local hosts with a default gateway address
- B. allows remote management of the switch
- C. allows the switch to respond to ARP requests between two hosts
- D. ensures that hosts on the same LAN can communicate with each other

Correct Answer: B

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

Explanation:

Switch is a layer 2 device and doesn't use network layer for packet forwarding. The IP address may be used only for administrative purposes such as Telnet access or for network management purposes.

QUESTION 10

Which three statements are true about the operation of a full-duplex Ethernet network? (Choose three.)

- A. There are no collisions in full-duplex mode.
- B. A dedicated switch port is required for each full-duplex node.
- C. Ethernet hub ports are preconfigured for full-duplex mode.
- D. In a full-duplex environment, the host network card must check for the availability of the network media before transmitting.
- E. The host network card and the switch port must be capable of operating in full-duplex mode.

Correct Answer: ABE

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Explanation:

Half-duplex Ethernet is defined in the original 802.3 Ethernet and Cisco says you only use one wire pair with a digital signal running in both directions on the wire. It also uses the CSMA/CD protocol to help prevent collisions and to permit retransmitting if a collision does occur. If a hub is attached to a switch, it must operate in half-duplex mode because the end stations must be able to detect collisions. Half-duplex Ethernet--typically 10BaseT--is only about 30 to 40 percent efficient as Cisco sees it, because a large 10BaseT network will usually only give you 3- to 4Mbps--at most. Full-duplex Ethernet uses two pairs of wires, instead of one wire pair like half duplex. Also, full duplex uses a point-to-point connection between the transmitter of the transmitting device and the receiver of the receiving device, which means that with full-duplex data transfer, you get a faster data transfer compared to half duplex. And because the transmitted data is sent on a different set of wires than the received data, no collisions occur. The reason you don't need to worry about collisions is because now Full-duplex Ethernet is like a freeway with multiple lanes instead of the single-lane road provided by half duplex. Full-duplex Ethernet is supposed to offer 100 percent efficiency in both directions; this means you can get 20Mbps with a 10Mbps Ethernet running full duplex, or 200Mbps for FastEthernet.

QUESTION 11

What is the subnet address for the IP address 172.19.20.23/28?

- A. 172.19.20.0
- B. 172.19.20.15
- C. 172.19.20.16
- D. 172.19.20.20
- E. 172.19.20.32

Correct Answer: C

Section: IP addressing (IPv4 / IPv6)
Explanation

Explanation/Reference:

QUESTION 12

What is the subnet address of 172.16.159.159/22?

- A. 172.16.0.0
- B. 172.16.128.0
- C. 172.16.156.0
- D. 172.16.159.0
- E. 172.16.159.128
- F. 172.16.192.0

Correct Answer: C

Section: IP addressing (IPv4 / IPv6)
Explanation

Explanation/Reference:

Explanation:

Converting to binary format it comes to

11111111.11111111.11111100.00000000 or 255.255.252.0

Starting with 172.16.0.0 and having increment of 4 we get.

172.16.0-3

172.16.4-7 etc.

QUESTION 13

An administrator is working with the 192.168.4.0 network, which has been subnetted with a /26 mask. Which two addresses can be assigned to hosts within the same subnet? (Choose two.)

- A. 192.168.4.61
- B. 192.168.4.63
- C. 192.168.4.67
- D. 192.168.4.125
- E. 192.168.4.128

F. 192.168.4.132

Correct Answer: CD

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

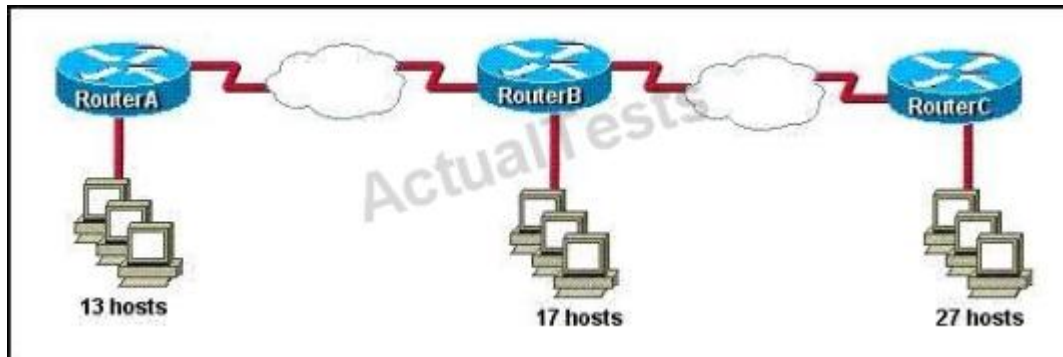
Explanation:

Only the values of host with 67 and 125 fall within the range of /26 CIDR subnet mask, all others lie beyond it.

QUESTION 14

Refer to the exhibit.

The internetwork is using subnets of the address 192.168.1.0 with a subnet mask of 255.255.255.224. The routing protocol in use is RIP version 1. Which address could be assigned to the FastEthernet interface on RouterA?



- A. 192.168.1.31
- B. 192.168.1.64
- C. 192.168.1.127
- D. 192.168.1.190
- E. 192.168.1.192

Correct Answer: D

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:**QUESTION 15**

What is the network address for the host with IP address 192.168.23.61/28?

- A. 192.168.23.0
- B. 192.168.23.32
- C. 192.168.23.48
- D. 192.168.23.56
- E. 192.168.23.60

Correct Answer: C

Section: IP addressing (IPv4 / IPv6)

Explanation**Explanation/Reference:**

Explanation:

Convert bit-length prefix to quad-dotted decimal representation, then from it find the number of bits used for subnetting you can find previously calculated number of subnets by separating subnets each having value of last bit used for subnet masking Find that your IP address is in which subnet, that subnet's first address is network address and last address is broadcast address. Based on above steps the answer is option C.

QUESTION 16

What is the best practice when assigning IP addresses in a small office of six hosts?

- A. Use a DHCP server that is located at the headquarters.
- B. Use a DHCP server that is located at the branch office.
- C. Assign the addresses by using the local CDP protocol.
- D. Assign the addresses statically on each node.

Correct Answer: D

Section: IP Services

Explanation**Explanation/Reference:**

Explanation:

Its best to use static addressing scheme where the number of systems is manageable rather than use dynamic protocol as it is easy to operate and manage.

QUESTION 17

Which two statements describe the IP address 10.16.3.65/23? (Choose two.)

- A. The subnet address is 10.16.3.0 255.255.254.0.
- B. The lowest host address in the subnet is 10.16.2.1 255.255.254.0.
- C. The last valid host address in the subnet is 10.16.2.254 255.255.254.0
- D. The broadcast address of the subnet is 10.16.3.255 255.255.254.0.
- E. The network is not subnetted.

Correct Answer: BD

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

Explanation:

The mask 255.255.254.0 (/23) used with a Class A address means that there are 15 subnet bits and 9 host bits. The block size in the third octet is 2 (256 - 254). So this makes the subnets in 0, 2, 4, 6, etc., all the way to 254. The host 10.16.3.65 is in the 2.0 subnet. The next subnet is 4.0, so the broadcast address for the 2.0 subnet is 3.255. The valid host addresses are 2.1 through 3.254

QUESTION 18

Given a Class C IP address subnetted with a /30 subnet mask, how many valid host IP addresses are available on each of the subnets?

- A. 1
- B. 2
- C. 4
- D. 8
- E. 252
- F. 254

Correct Answer: B

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

Explanation:

/30 CIDR corresponds to mask 55.255.255.252 whose binary is 11111100 which means 6 subnet bits and 2 host bits which means 62 subnets and 2 hosts per subnet.

QUESTION 19

Which one of the following IP addresses is the last valid host in the subnet using mask 255.255.255.224?

- A. 192.168.2.63
- B. 192.168.2.62
- C. 192.168.2.61
- D. 192.168.2.60
- E. 192.168.2.32

Correct Answer: B

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

Explanation:

With the 224 there are 8 networks with increments of 32 One of these is 32 33 62 63 where 63 is broadcast so 62 is last valid host out of given choices.

QUESTION 20

An administrator is in the process of changing the configuration of a router. What command will allow the administrator to check the changes that have been made prior to saving the new configuration?

- A. Router# show startup-config
- B. Router# show current-config
- C. Router# show running-config
- D. Router# show memory
- E. Router# show flash
- F. Router# show processes

Correct Answer: C

Section: IP Routing Technologies**Explanation****Explanation/Reference:**

Explanation:

This command followed by the appropriate parameter will show the running configuration hence the admin will be able to see what changes have been made, and then they can be saved.

QUESTION 21

Which statements accurately describe CDP? (Choose three.)

- A. CDP is an IEEE standard protocol.
- B. CDP is a Cisco proprietary protocol.
- C. CDP is a datalink layer protocol.
- D. CDP is a network layer protocol.
- E. CDP can discover directly connected neighboring Cisco devices.
- F. CDP can discover Cisco devices that are not directly connected.

Correct Answer: BCE

Section: Operation of IP Data Networks**Explanation****Explanation/Reference:**

Explanation:

CDP (Cisco Discovery Protocol) is a proprietary protocol designed by Cisco to help administrators collect information about both locally attached and remote devices. By using CDP, you can gather hardware and protocol information about neighbor devices containing useful info for troubleshooting and documenting the network.

QUESTION 22

On a live network, which commands will verify the operational status of router interfaces? (Choose two.)

- A. Router# show interfaces
- B. Router# show ip protocols
- C. Router# debug interface
- D. Router# show ip interface brief

E. Router# show start

Correct Answer: AD

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

Both these commands will show the current status of the interfaces, either in show or debug mode both will display the information.

QUESTION 23

Which router command will configure an interface with the IP address 10.10.80.1/19?

- A. router(config-if)# ip address 10.10.80.1/19
- B. router(config-if)# ip address 10.10.80.1 255.255.0.0
- C. router(config-if)# ip address 10.10.80.1 255.255.255.0
- D. router(config-if)# ip address 10.10.80.1 255.255.224.0
- E. router(config-if)# ip address 10.10.80.1 255.255.240.0
- F. router(config-if)# ip address 10.10.80.1 255.255.255.240

Correct Answer: D

Section: IP Routing Technologies

Explanation

Explanation/Reference:

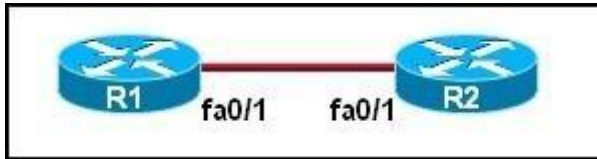
Explanation:

255.255.224 equal /19 in CIDR format hence the answer.

QUESTION 24

Refer to the exhibit.

The two routers have had their startup configurations cleared and have been restarted. At a minimum, what must the administrator do to enable CDP to exchange information between R1 and R2?



- A. Configure the router with the cdp enable command.
- B. Enter no shutdown commands on the R1 and R2 fa0/1 interfaces.
- C. Configure IP addressing and no shutdown commands on both the R1 and R2 fa0/1 interfaces.
- D. Configure IP addressing and no shutdown commands on either of the R1 or R2 fa0/1 interfaces.

Correct Answer: B

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

If the shut down commands are not entered, then CDP can exchange information between the two routers, else it would fail.

QUESTION 25

What two things does a router do when it forwards a packet? (Choose two.)

- A. switches the packet to the appropriate outgoing interfaces
- B. computes the destination host address
- C. determines the next hop on the path
- D. updates the destination IP address
- E. forwards ARP requests

Correct Answer: AC

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

Without following these two processes namely switching the packet to appropriate interface and telling the packet where to go by providing it with a destination IP address, the purpose of the same would not be solved.

QUESTION 26

Which two of these functions do routers perform on packets? (Choose two.)

- A. examine the Layer 2 headers of inbound packets and use that information to determine the next hops for the packets
- B. update the Layer 2 headers of outbound packets with the MAC addresses of the next hops
- C. examine the Layer 3 headers of inbound packets and use that information to determine the next hops for the packets
- D. examine the Layer 3 headers of inbound packets and use that information to determine the complete paths along which the packets will be routed to their ultimate destinations
- E. update the Layer 3 headers of outbound packets so that the packets are properly directed to valid next hops
- F. update the Layer 3 headers of outbound packets so that the packets are properly directed to their ultimate destinations

Correct Answer: BC

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

This is the basic function of the router to receive incoming packets and then forward them to their required destination. This is done by reading layer 3 headers of inbound packets and update the info to layer 2 for further hopping.

QUESTION 27

Which statements are true regarding ICMP packets? (Choose two.)

- A. They acknowledge receipt of TCP segments.
- B. They guarantee datagram delivery.
- C. TRACERT uses ICMP packets.
- D. They are encapsulated within IP datagrams.
- E. They are encapsulated within UDP datagrams.

Correct Answer: CD

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

QUESTION 28

The command `ip route 192.168.100.160 255.255.255.224 192.168.10.2` was issued on a router. No routing protocols or other static routes are configured on the router. Which statement is true about this command?

- A. The interface with IP address 192.168.10.2 is on this router.
- B. The command sets a gateway of last resort for the router.
- C. Packets that are destined for host 192.168.100.160 will be sent to 192.168.10.2.
- D. The command creates a static route for all IP traffic with the source address 192.168.100.160.

Correct Answer: C

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

160 it's actually network address of /27 so any address within the range of 160 network will be sent to 192.168.10.2

QUESTION 29

What does administrative distance refer to?

- A. the cost of a link between two neighboring routers
- B. the advertised cost to reach a network
- C. the cost to reach a network that is administratively set
- D. a measure of the trustworthiness of a routing information source

Correct Answer: D

Section: IP Routing Technologies

Explanation

Explanation/Reference:

What Is Administrative Distance?

Reference:

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094195.shtml

Explanation:

Administrative distance is the feature that routers use in order to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) with the help of an administrative distance value.

Explanation 2:

Administrative distance is the first criterion that a router uses to determine which routing protocol to use if two protocols provide route information for the same destination. Administrative distance is a measure of the trustworthiness of the source of the routing information. The smaller the administrative distance value, the more reliable the protocol.

QUESTION 30

Which IOS command is used to initiate a login into a VTY port on a remote router?

- A. router# login
- B. router# telnet
- C. router# trace
- D. router# ping
- E. router(config)# line vty 0 5
- F. router(config-line)# login

Correct Answer: B

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

VTY ports are telnet ports hence command B will initiate login or connection to the telnet port.

QUESTION 31

In the configuration of NAT, what does the keyword overload signify?

- A. When bandwidth is insufficient, some hosts will not be allowed to access network translation.
- B. The pool of IP addresses has been exhausted.
- C. Multiple internal hosts will use one IP address to access external network resources.
- D. If the number of available IP addresses is exceeded, excess traffic will use the specified address pool.

Correct Answer: C
Section: IP Services
Explanation

Explanation/Reference:
Configuring Basic NAT with overloading

Reference:
<http://evilrouters.net/2009/07/09/configuring-basic-nat-with-overloading/>

Explanation:

Overloading (having multiple clients all NAT'd to the same IP address) is probably the most common implementation (especially for those of us who run NAT on a Cisco box at home!).

QUESTION 32

What happens when computers on a private network attempt to connect to the Internet through a Cisco router running PAT?

- A. The router uses the same IP address but, a different TCP source port number for each connection.
- B. An IP address is assigned based on the priority of the computer requesting the connection.
- C. The router selects an address from a pool of one-to-one address mappings held in the lookup table.
- D. The router assigns a unique IP address from a pool of legally registered addresses for the duration of the connection.

Correct Answer: A
Section: IP Services
Explanation

Explanation/Reference:
Configuring Static PAT

Reference:
http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/nat_staticpat.html

Explanation:

Static PAT translations allow a specific UDP or TCP port on a global address to be translated to a specific port on a local address. That is, both the address and the port numbers are translated.

Static PAT is the same as static NAT, except that it enables you to specify the protocol (TCP or UDP) and port for the real and mapped addresses.

Static PAT enables you to identify the same mapped address across many different static statements, provided that the port is different for each statement. You cannot use the same mapped address for multiple static NAT statements.

Explanation 2:

Port Address Translation makes the PC connect to the Internet but using different TCP source port.

QUESTION 33

When configuring NAT, the Internet interface is considered to be what?

- A. local
- B. inside
- C. global
- D. outside

Correct Answer: D

Section: IP Services

Explanation

Explanation/Reference:

Explanation:

Network address translation or NAT requires the Internet to be considered as an outside interface else it won't serve the purpose it intends to.

QUESTION 34

The ip helper-address command does what?

- A. assigns an IP address to a host
- B. resolves an IP address from a DNS server
- C. relays a DHCP request across networks
- D. resolves an IP address overlapping issue

Correct Answer: C

Section: IP Services

Explanation

Explanation/Reference:

Reference:

<http://cisco.net.com/tcpip/dhcp/107-how-to-use-ip-helper-address-to-connect-remote-dhcp-server.html>

Explanation:

When the DHCP client sends the DHCP request packet, it doesn't have an IP address. So it uses the all-zeroes address, 0.0.0.0, as the IP source address. And it doesn't know how to reach the DHCP server, so it uses a general broadcast address, 255.255.255.255, for the destination. So the router must replace the source address with its own IP address, for the interface that received the request. And it replaces the destination address with the address specified in the ip helper- address command. The client device's MAC address is included in the payload of the original DHCP request packet, so the router doesn't need to do anything to ensure that the server receives this information.

QUESTION 35

Refer to the exhibit.

The network administrator made the entries that are shown and then saved the configuration. From a console connection, what password or password sequence is required for the administrator to access privileged mode on Router1?

```
Router# configure terminal
Router(config)# hostname Router1
Router1(config)# enable secret sanfran
Router1(config)# enable password cisco
Router1(config)# line vty 0 4
Router1(config-line)# password sanjose
Router1(config-line)#
```

- A. cisco
- B. sanfran
- C. sanjose
- D. either cisco or sanfran
- E. either cisco or sanjose
- F. sanjose and sanfran

Correct Answer: B

Section: Network Device Security

Explanation

Explanation/Reference:

Explanation:

The enable secret password takes precedence over the enable password, so sanfran will be used.

QUESTION 36

The following commands are entered on the router:

```
Burbank(config)# enable secret fortress  
Burbank(config)# line con 0  
Burbank(config-line)# login  
Burbank(config-line)# password n0way1n  
Burbank(config-line)# exit  
Burbank(config)# service password-encryption
```

What is the purpose of the last command entered?

- A. to require the user to enter an encrypted password during the login process
- B. to prevent the vty, console, and enable passwords from being displayed in plain text in the configuration files
- C. to encrypt the enable secret password
- D. to provide login encryption services between hosts attached to the router

Correct Answer: B

Section: Network Device Security

Explanation

Explanation/Reference:

QUESTION 37

What is the effect of using the service password-encryption command?

- A. Only the enable password will be encrypted.
- B. Only the enable secret password will be encrypted.
- C. Only passwords configured after the command has been entered will be encrypted.
- D. It will encrypt the secret password and remove the enable secret password from the configuration.
- E. It will encrypt all current and future passwords.

Correct Answer: E

Section: Network Device Security

Explanation

Explanation/Reference:

Explanation:

Encryption further adds a level of security to the system as anyone having access to the database of passwords cannot reverse the process of encryption to know the actual passwords which isn't the case if the passwords are stored simply.

QUESTION 38

An administrator has connected devices to a switch and for security reasons, wants the dynamically learned MAC addresses from the address table added to the running configuration.

What must be done to accomplish this?

- A. Enable port security and use the keyword sticky.
- B. Set the switchport mode to trunk and save the running configuration.
- C. Use the switchport protected command to have the MAC addresses added to the configuration.
- D. Use the no switchport port-security command to allow MAC addresses to be added to the configuration.

Correct Answer: A

Section: Network Device Security

Explanation

Explanation/Reference:

Port Security with Sticky MAC Addresses

Reference:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/port_sec.pdf

Explanation:

Port security with sticky MAC addresses provides many of the same benefits as port security with static MAC addresses, but sticky MAC addresses can be learned dynamically. Port security with sticky MAC addresses retains dynamically learned MAC addresses during a link-down condition.

If you enter a **write memory** or **copy running-config startup-config** command, then port security with sticky MAC addresses saves dynamically learned MAC addresses in the startup-config file and the port does not have to learn addresses from ingress traffic after bootup or a restart.

Explanation2:

One can configure MAC addresses to be sticky. These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, the interface does not need to dynamically relearn them when the switch restarts, hence enabling security as desired.

QUESTION 39

A company has placed a networked PC in a lobby so guests can have access to the corporate directory. A security concern is that someone will disconnect the directory PC and re-connect their laptop computer and have access to the corporate network. For the port servicing the lobby, which three configuration steps should be performed on the switch to prevent this? (Choose three.)

- A. Enable port security.
- B. Create the port as a trunk port.
- C. Create the port as an access port.
- D. Create the port as a protected port.
- E. Set the port security aging time to 0.
- F. Statically assign the MAC address to the address table.
- G. Configure the switch to discover new MAC addresses after a set time of inactivity.

Correct Answer: ACF

Section: Network Device Security

Explanation

Explanation/Reference:

Explanation:

If port security is enabled and the port is only designated as access port, and finally static MAC address is assigned, it ensures that even if a physical connection is done by taking out the directory PC and inserting personal laptop or device, the connection cannot be made to the corporate network, hence ensuring safety.

QUESTION 40

Why would a network administrator configure port security on a switch?

- A. to prevent unauthorized Telnet access to a switch port
- B. to prevent unauthorized hosts from accessing the LAN
- C. to limit the number of Layer 2 broadcasts on a particular switch port
- D. block unauthorized access to the switch management interfaces

Correct Answer: B

Section: Network Device Security

Explanation

Explanation/Reference:

Explanation:

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port. If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs. Also, if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port, a violation is flagged.

QUESTION 41

How can you ensure that only the MAC address of a server is allowed by switch port Fa0/1?

- A. Configure port Fa0/1 to accept connections only from the static IP address of the server.
- B. Configure the server MAC address as a static entry of port security.
- C. Use a proprietary connector type on Fa0/1 that is incompatible with other host connectors.
- D. Bind the IP address of the server to its MAC address on the switch to prevent other hosts from spoofing the server IP address.

Correct Answer: B

Section: Network Device Security

Explanation

Explanation/Reference:

Explanation:

When the MAC address is configured as static entry, no other address is allowed.

QUESTION 42

Which IP addresses are valid for hosts belonging to the 10.1.160.0/20 subnet? (Choose three.)

- A. 10.1.168.0
- B. 10.1.176.1
- C. 10.1.174.255
- D. 10.1.160.255
- E. 10.1.160.0
- F. 10.1.175.255

Correct Answer: ACD

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

Explanation:

All IP address in IP ranges between : 10.1.160.1 and 10.1.175.254 are valid as shown below Address: 10.1.160.0 00001010.00000001.1010 0000.00000000 Netmask:255.255.240.0 = 2011111111.11111111.1111 0000.00000000 Wildcard:0.0.15.2550000000.00000000.0000 1111.11111111 Which implies that
Network: 10.1.160.0/20 00001010.00000001.1010 0000.00000000
HostMin:10.1.160.100001010.00000001.1010 0000.00000001
HostMax:10.1.175.25400001010.00000001.1010 1111.11111110
Broadcast:10.1.175.25500001010.00000001.1010 1111.11111111

QUESTION 43

If a host experiences intermittent issues that relate to congestion within a network while remaining connected, what could cause congestion on this LAN?

- A. half-duplex operation
- B. broadcast storms
- C. network segmentation
- D. multicasting

Correct Answer: B

Section: Troubleshooting

Explanation

Explanation/Reference:

Explanation:

A broadcast storm can consume sufficient network resources so as to render the network unable to transport normal traffic.

QUESTION 44

Given an IP address of 192.168.1.42 255.255.255.248, what is the subnet address?

- A. 192.168.1.8/29
- B. 192.168.1.32/27
- C. 192.168.1.40/29
- D. 192.168.1.16/28
- E. 192.168.1.48/29

Correct Answer: C

Section: IP addressing (IPv4 / IPv6)**Explanation****Explanation/Reference:**

Explanation:

248 mask uses 5 bits (1111 1000)

42 IP in binary is (0010 1010)

The base subnet therefore is the lowest binary value that can be written without changing the output of an AND operation of the subnet mask and IP ...

1111 1000 AND

0010 1010 equals

0010 1000 - which is .40

/24 is standard class C mask.

adding the 5 bits from the .248 mask gives /29

QUESTION 45

Which OSI layer header contains the address of a destination host that is on another network?

- A. application
- B. session
- C. transport
- D. network
- E. data link
- F. physical

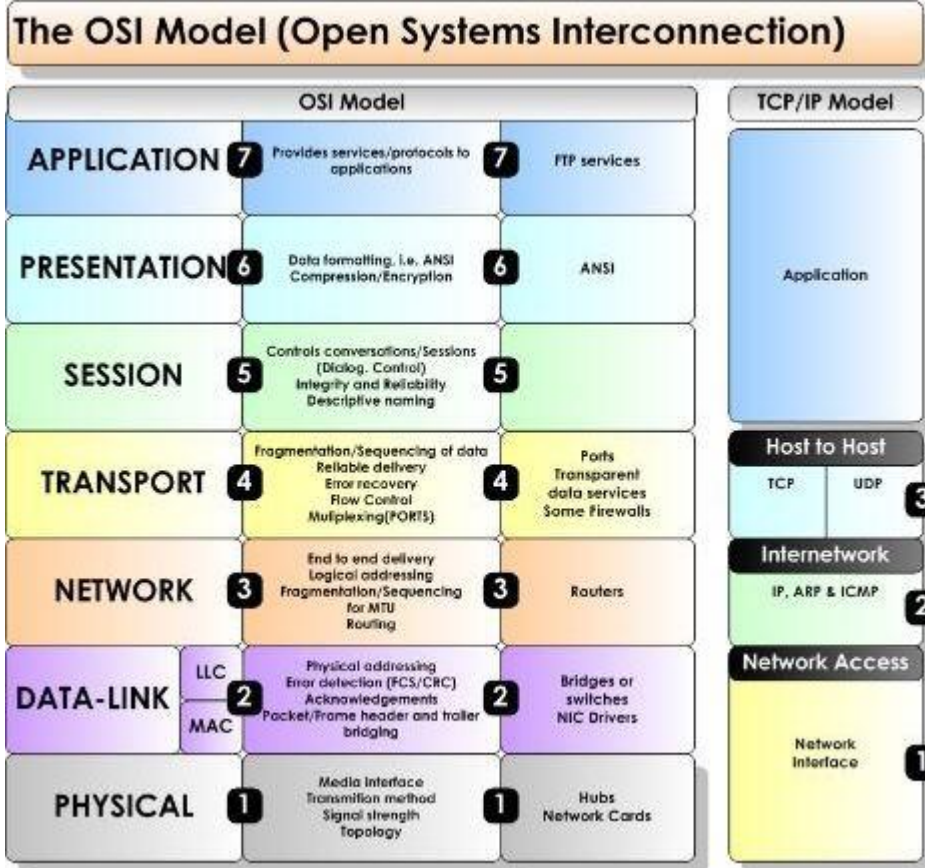
Correct Answer: D

Section: Operation of IP Data Networks

Explanation**Explanation/Reference:**

Explanation:

Only network address contains this information. To transmit the packets the sender uses network address and datalink address. But the layer 2 address represents just the address of the next hop device on the way to the sender. It is changed on each hop. Network address remains the same.



QUESTION 46

Which layer of the TCP/IP stack combines the OSI model physical and data link layers?

- A. Internet layer
- B. transport layer
- C. application layer
- D. network access layer

Correct Answer: D

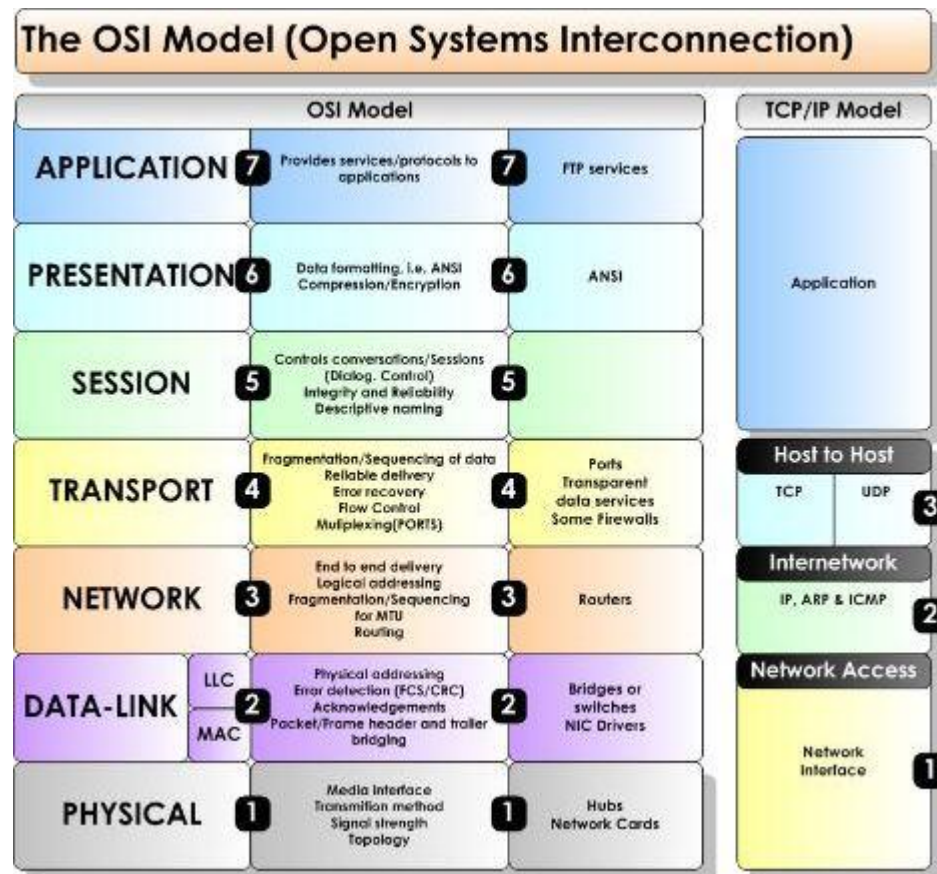
Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Explanation:

The Internet Protocol Suite, TCP/IP, is a suite of protocols used for communication over the internet. The TCP/IP model was created after the OSI 7 layer model for two major reasons. First, the foundation of the Internet was built using the TCP/IP suite and through the spread of the World Wide Web and Internet, TCP/IP has been preferred. Second, a project researched by the Department of Defense (DOD) consisted of creating the TCP/IP protocols. The DOD's goal was to bring international standards which could not be met by the OSI model. Since the DOD was the largest software consumer and they preferred the TCP/IP suite, most vendors used this model rather than the OSI. Below is a side by side comparison of the TCP/IP and OSI models.



QUESTION 47

Which protocol uses a connection-oriented service to deliver files between end systems?

- A. TFTP
- B. DNS
- C. FTP
- D. SNMP
- E. RIP

Correct Answer: C

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

QUESTION 48

Which network device functions only at Layer 1 of the OSI model?

A.



hub

B.



NIC

C.



router

D.



E.



Correct Answer: A

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Explanation:

Most hubs are amplifying the electrical signal; therefore, they are really repeaters with several ports. Hubs and repeaters are Layer 1 (physical layer) devices.

QUESTION 49

Which transport layer protocol provides best-effort delivery service with no acknowledgment receipt required?

- A. HTTP
- B. IP
- C. TCP
- D. Telnet
- E. UDP

Correct Answer: E

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Explanation:

UDP provides a connectionless datagram service that offers best-effort delivery, which means that UDP does not guarantee delivery or verify sequencing for any datagrams. A source host that needs reliable communication must use either TCP or a program that provides its own sequencing and acknowledgment services.

QUESTION 50

Which layer of the OSI model controls the reliability of communications between network devices using flow control, sequencing and acknowledgments?

- A. Physical
- B. Data-link
- C. Transport
- D. Network

Correct Answer: C

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Explanation:

Layer	Function	Examples
Application (Layer 7)	User interface	Telnet, HTTP
Presentation (Layer 6)	Handles encryption & changes to syntax	ASCII/EBCDIC, JPEG/MP3
Session (Layer 5)	Manages multiple applications and maintains synchronisation points	Operating systems, scheduling
Transport (Layer 4)	Provides reliable or best-effort delivery and (optional) error and flow control	TCP, UDP
Network (Layer 3)	Provides logical end-to-end addressing used by routers and hosts	IP
Data Link (Layer 2)	Creates frames from data bits, uses MAC addresses to access endpoints, and provides error detection but no correction	802.3, 802.2, HDLC, Frame Relay
Physical (Layer 1)	Specifies voltage, wire speed, and cable pin-outs	EIA/TIA, V.35

QUESTION 51

Drag and Drop Question

Drag the appropriate command on the left to the configuration task it accomplishes. (Not all options are used)

Select and Place:

login password cantCome1n	encrypt all clear text passwords
enable password uwi11NeverNo	protect access to the user mode prompt
service password-encryption	set privileged mode encrypted password
line console 0 password friendS0nly	set password to allow Telnet connections
enable secret noWay1n4u	set privileged mode clear text password
line vty 0 4 password 2hard2Guess	

Correct Answer:

login password cantCome1n	service password-encryption
enable password uwi11NeverNo	line console 0 password friendS0nly
service password-encryption	enable secret noWay1n4u
line console 0 password friendS0nly	line vty 0 4 password 2hard2Guess
enable secret noWay1n4u	enable password uwi11NeverNo
line vty 0 4 password 2hard2Guess	

Section: Network Device Security**Explanation****Explanation/Reference:****QUESTION 52**

Drag and Drop Question

Various protocols are listed to the left. On the right are applications for the use of those protocols. Drag the protocol on the left to an associated function for that protocol on the right. (Not all options are used)

Select and Place:

ICMP

DHCP

RARP

UDP

DNS

ARP

A PC sends packets to the default gateway IP address the first time since the PC turned on.

The network administrator is checking basic IP connectivity from a workstation to a server.

The TCP/IP protocol stack must find an IP address for packets destined for a URL.

A network device will automatically assign IP addresses to workstations.

Correct Answer:

ICMP	ARP
DHCP	ICMP
RARP	DNS
UDP	DHCP
DNS	
ARP	

Section: IP Services**Explanation****Explanation/Reference:****QUESTION 53**

Drag and Drop Question

Move a protocol or service on the left to a situation on the right where it would be used. (Not all options are used)

Select and Place:

OSPF

ARP

NAT

DNS

SQL

DHCP

A PC with address 10.1.5.10 must access devices on the Internet.

Only routers and servers require static IP addresses. Easy IP administration is required.

A PC only knows a server as **//Media Server**. IP needs to send data to that server.

A protocol is needed to replace current static routes with automatic route updates.

Correct Answer:

OSPF	NAT
ARP	DHCP
NAT	DNS
DNS	OSPF
SQL	
DHCP	

Section: IP Services**Explanation****Explanation/Reference:****QUESTION 54**

Drag and Drop Question

Drag the definition the left to the correct term on the right. (Not all options are used)

Select and Place:

a protocol that converts human-readable names into machine-readable addresses

used to assign IP addresses automatically and set parameters such as subnet mask and default gateway

a protocol for using HTTP or HTTPS to exchange XML-based messages over computer networks

a connectionless service that uses UDP to transfer files between systems

a protocol used to monitor and manage network devices

a reliable, connection-oriented service that uses TCP to transfer files between systems

SNMP

FTP

TFTP

DNS

DHCP

Correct Answer:

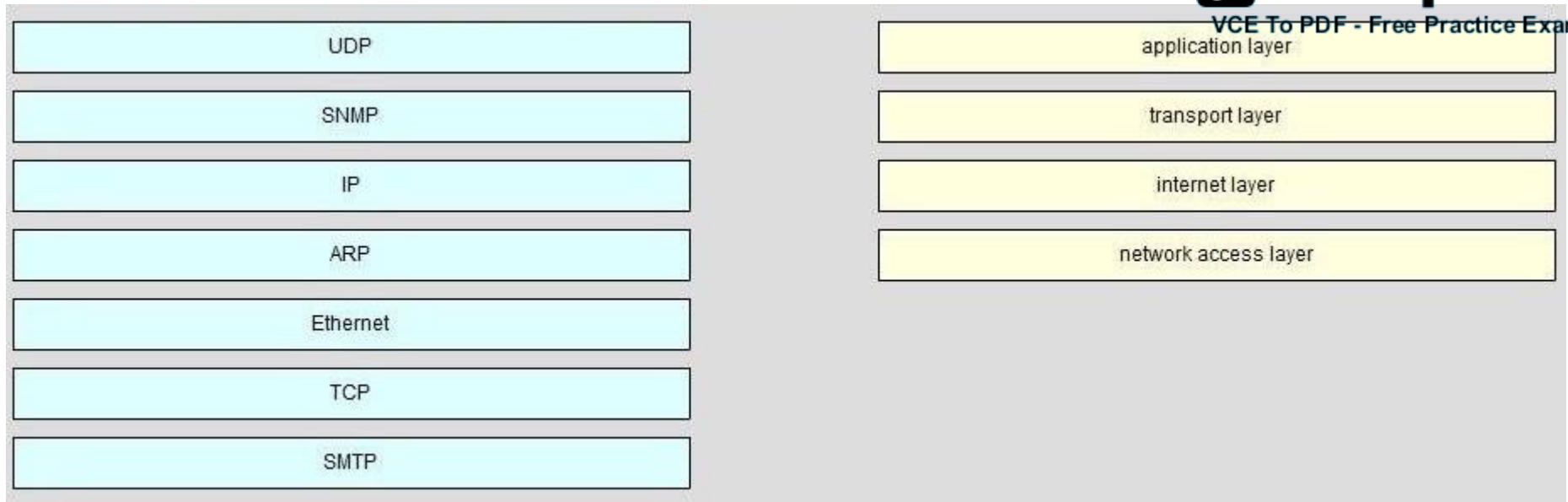
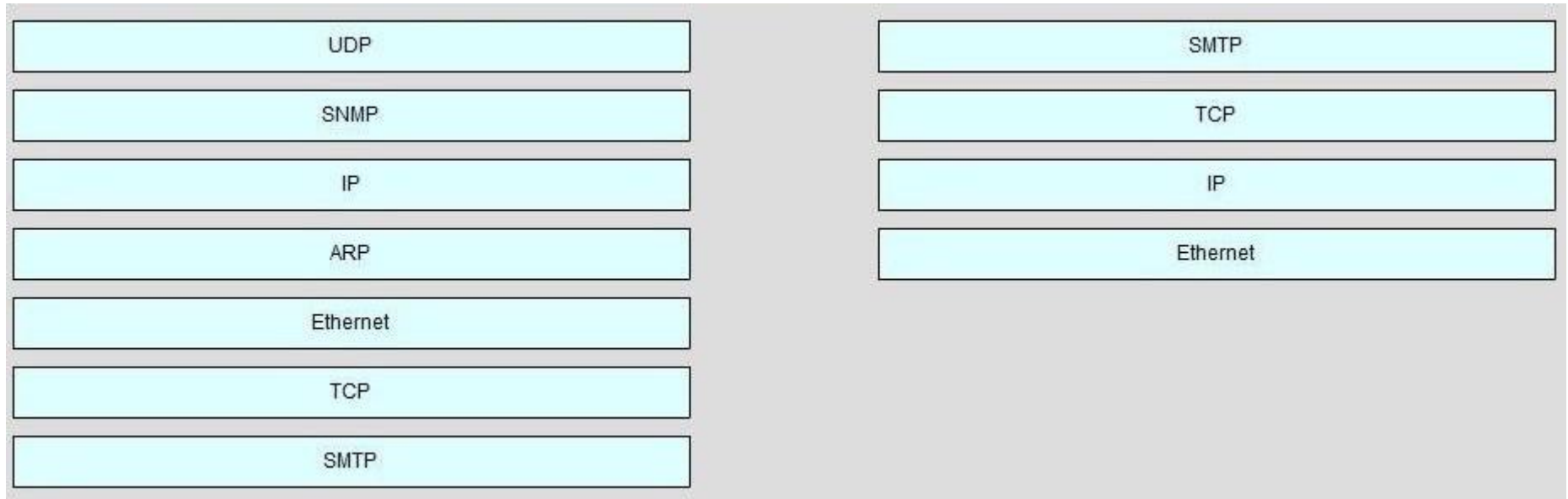
a protocol that converts human-readable names into machine-readable addresses	a protocol used to monitor and manage network devices
used to assign IP addresses automatically and set parameters such as subnet mask and default gateway	a reliable, connection-oriented service that uses TCP to transfer files between systems
a protocol for using HTTP or HTTPS to exchange XML-based messages over computer networks	a connectionless service that uses UDP to transfer files between systems
a connectionless service that uses UDP to transfer files between systems	a protocol that converts human-readable names into machine-readable addresses
a protocol used to monitor and manage network devices	used to assign IP addresses automatically and set parameters such as subnet mask and default gateway
a reliable, connection-oriented service that uses TCP to transfer files between systems	

Section: IP Services**Explanation****Explanation/Reference:****QUESTION 55**

Drag and Drop Question

On the left are various network protocols. On the right are the layers of the TCP/IP model. Assuming a reliable connection is required, move the protocols on the left to the TCP/IP layers on the right to show the proper encapsulation for an email message sent by a host on the LAN. (Not all options are used)

Select and Place:



**Correct Answer:**

Section: IP Services
Explanation

Explanation/Reference:

QUESTION 56
Hotspot Questions

Instructions



For both the Router and the Switch the simulated console mode needs to start and remain in enabled mode.

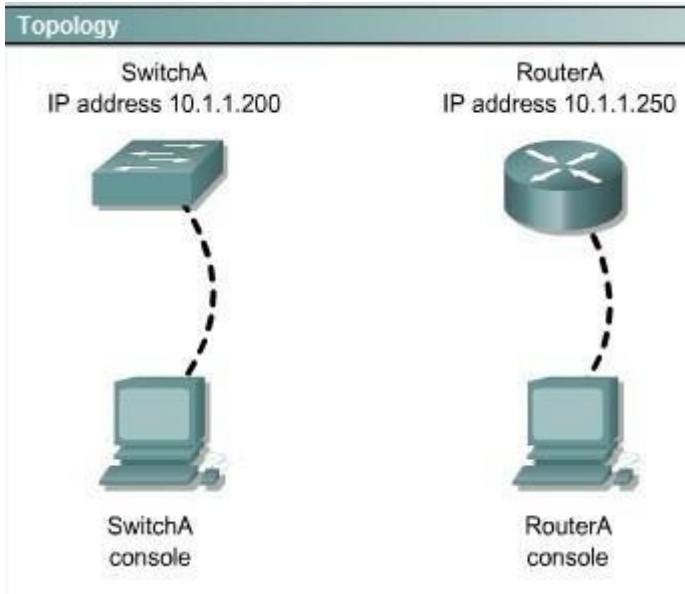
RouterA and SwitchA have been configured to operate in a private network which will connect to the Internet. You have been asked to review the configuration prior to cabling and implementation.

This task requires the use of various IOS commands to access and inspect the running configuration of RouterA and SwitchA. No configuration changes are necessary.

You will connect to RouterA and SwitchA via the console devices that are attached to each.

There are 4 multiple-choice questions with this task. Be sure to answer all of them before leaving this item. In order to score the maximum points you will need to have accessed both SwitchA and RouterA.

NOTE: The configuration command has been disabled for both the router and switch in this simulation.



Select two options which are security Issues which need to be modified before RouterA is used? (Choose two.)

- A. unencrypted weak password is configured to protect privilege mode
- B. inappropriate wording in banner message
- C. the virtual terminal lines have a weak password configured
- D. virtual terminal lines have a password, but it will not be used
- E. configuration supports un-secure web server access

Correct Answer: BD

Section: Troubleshooting

Explanation

Explanation/Reference:

Explanation:

(This answer can be done by simulation only, don't know user name password and banner message etc)

QUESTION 57

Hotspot Questions

Instructions



For both the Router and the Switch the simulated console mode needs to start and remain in enabled mode.

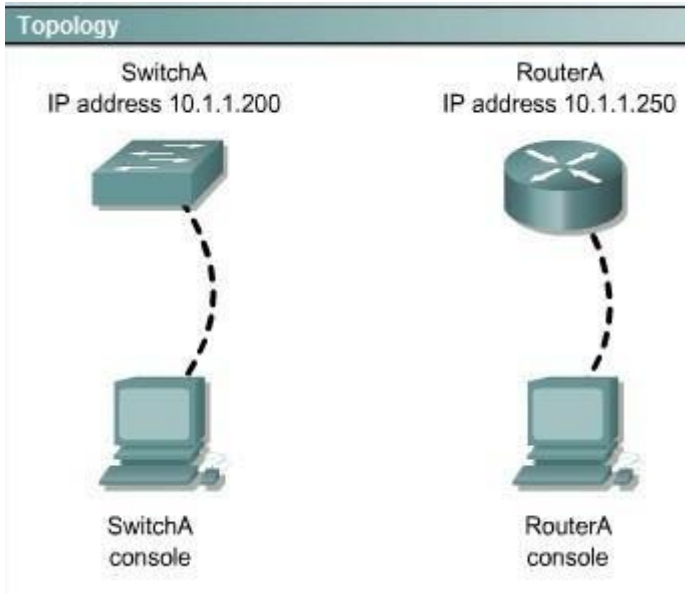
RouterA and SwitchA have been configured to operate in a private network which will connect to the Internet. You have been asked to review the configuration prior to cabling and implementation.

This task requires the use of various IOS commands to access and inspect the running configuration of RouterA and SwitchA. No configuration changes are necessary.

You will connect to RouterA and SwitchA via the console devices that are attached to each.

There are 4 multiple-choice questions with this task. Be sure to answer all of them before leaving this item. In order to score the maximum points you will need to have accessed both SwitchA and RouterA.

NOTE: The configuration command has been disabled for both the router and switch in this simulation.



Select three options which are security issues with the current configuration of SwitchA . (Choose three.)

- A. privilege mode is protected with an unencrypted password
- B. inappropriate wording in banner message
- C. virtual terminal lines are protected only by a password requirement
- D. both the username and password are weak
- E. telnet connections can be used to remotely manage the switch
- F. cisco user will be granted privilege level 15 by default

Correct Answer: ABD

Section: Troubleshooting

Explanation

Explanation/Reference:

Explanation:

(This answer can be done by simulation only, don't know user name password and banner message etc)

QUESTION 58

Hotspot Questions

Instructions



For both the Router and the Switch the simulated console mode needs to start and remain in enabled mode.

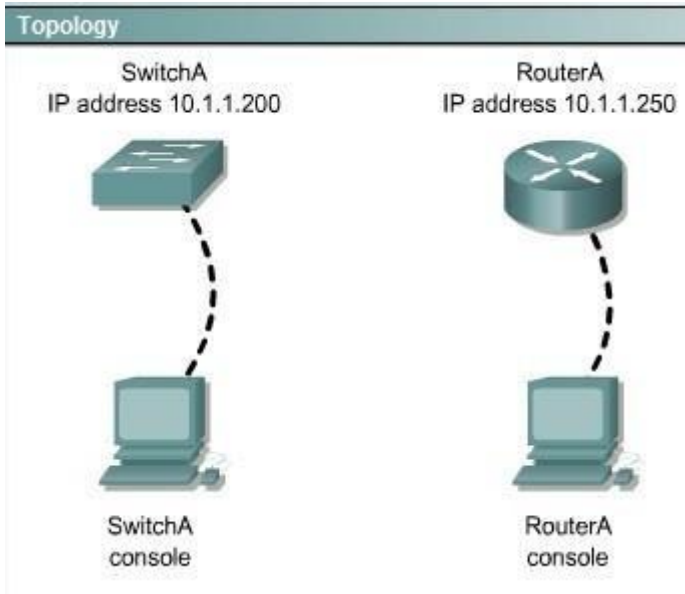
RouterA and SwitchA have been configured to operate in a private network which will connect to the Internet. You have been asked to review the configuration prior to cabling and implementation.

This task requires the use of various IOS commands to access and inspect the running configuration of RouterA and SwitchA. No configuration changes are necessary.

You will connect to RouterA and SwitchA via the console devices that are attached to each.

There are 4 multiple-choice questions with this task. Be sure to answer all of them before leaving this item. In order to score the maximum points you will need to have accessed both SwitchA and RouterA.

NOTE: The configuration command has been disabled for both the router and switch in this simulation.



Which two of the following are true regarding the configuration of RouterA? (Choose two.)

- A. at least 5 simultaneous remote connections are possible
- B. only telnet protocol connections to RouterA are supported
- C. remote connections to RouterA using telnet will succeed
- D. console line connections will never time out due to inactivity
- E. since DHCP is not used on FaO/1 there is not a need to use the NAT protocol

Correct Answer: AC

Section: Troubleshooting

Explanation

Explanation/Reference:

Explanation:

The IP address can accommodate 5 hosts at least, telnet can be accessed on the router

QUESTION 59

Hotspot Questions

Instructions



For both the Router and the Switch the simulated console mode needs to start and remain in enabled mode.

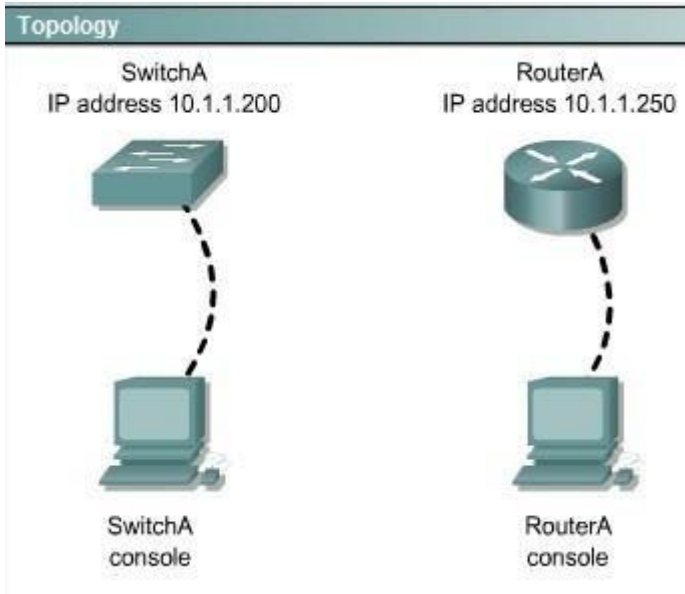
RouterA and SwitchA have been configured to operate in a private network which will connect to the Internet. You have been asked to review the configuration prior to cabling and implementation.

This task requires the use of various IOS commands to access and inspect the running configuration of RouterA and SwitchA. No configuration changes are necessary.

You will connect to RouterA and SwitchA via the console devices that are attached to each.

There are 4 multiple-choice questions with this task. Be sure to answer all of them before leaving this item. In order to score the maximum points you will need to have accessed both SwitchA and RouterA.

NOTE: The configuration command has been disabled for both the router and switch in this simulation.



Which of the following is true regarding the configuration of SwitchA?

- A. only 5 simultaneous remote connections are possible
- B. remote connections using ssh will require a username and password
- C. only connections from the local network will be possible
- D. console access to SwitchA requires a password

Correct Answer: B

Section: Troubleshooting

Explanation

Explanation/Reference:

Explanation:

Ssh login requires a user name and password always while other conditions may or may not be true.

QUESTION 60

An administrator must assign static IP addresses to the servers in a network. For network 192.168.20.24/29, the router is assigned the first usable host address while the sales server is given the last usable host address. Which of the following should be entered into the IP properties box for the sales server?

- A. IP address: 192.168.20.14
Subnet Mask: 255.255.255.248
Default Gateway: 192.168.20.9
- B. IP address: 192.168.20.254
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.20.1
- C. IP address: 192.168.20.30
Subnet Mask: 255.255.255.248
Default Gateway: 192.168.20.25
- D. IP address: 192.168.20.30
Subnet Mask: 255.255.255.240
Default Gateway: 192.168.20.17
- E. IP address: 192.168.20.30
Subnet Mask: 255.255.255.240
Default Gateway: 192.168.20.25

Correct Answer: C

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

QUESTION 61

What is the default administrative distance of the OSPF routing protocol?

- A. 90
- B. 100
- C. 110
- D. 120
- E. 130
- F. 170

Correct Answer: C

Section: IP Routing Technologies

Explanation

Explanation/Reference:
Default Distance Value Table

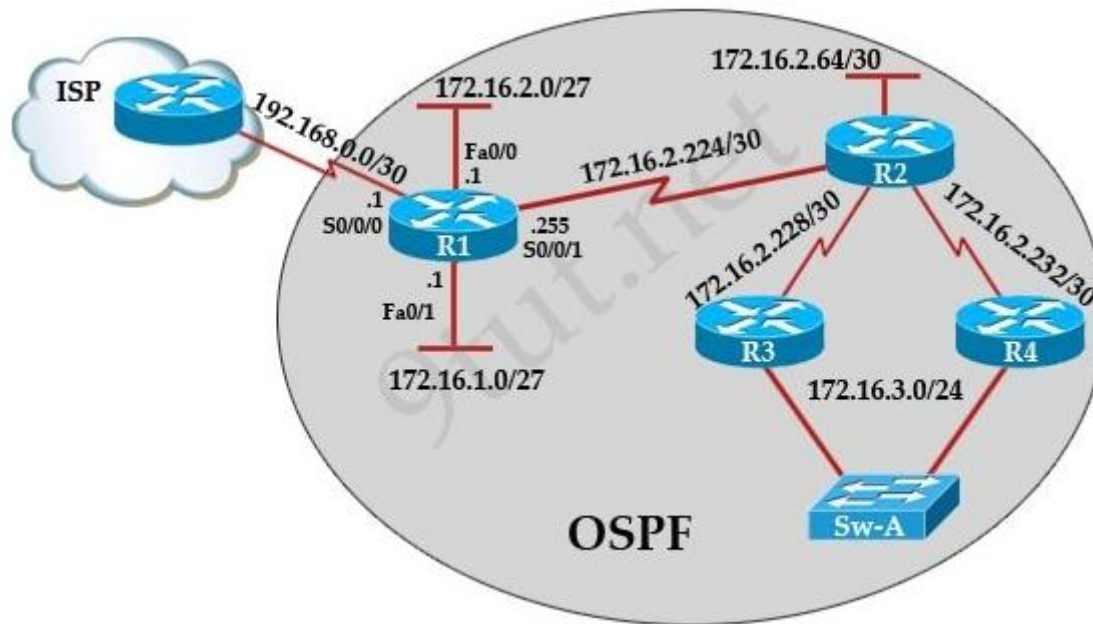
This table lists the administrative distance default values of the protocols that Cisco supports:

Route Source	Default Distance Values
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown*	255

* If the administrative distance is 255, the router does not believe the source of that route and does not install the route in the routing table.

QUESTION 62

After the network has converged, what type of messaging, if any, occurs between R3 and R4?



- A. No messages are exchanged
- B. Hellos are sent every 10 seconds.
- C. The full database from each router is sent every 30 seconds.
- D. The routing table from each router is sent every 60 seconds.

Correct Answer: B

Section: IP Routing Technologies

Explanation

Explanation/Reference:

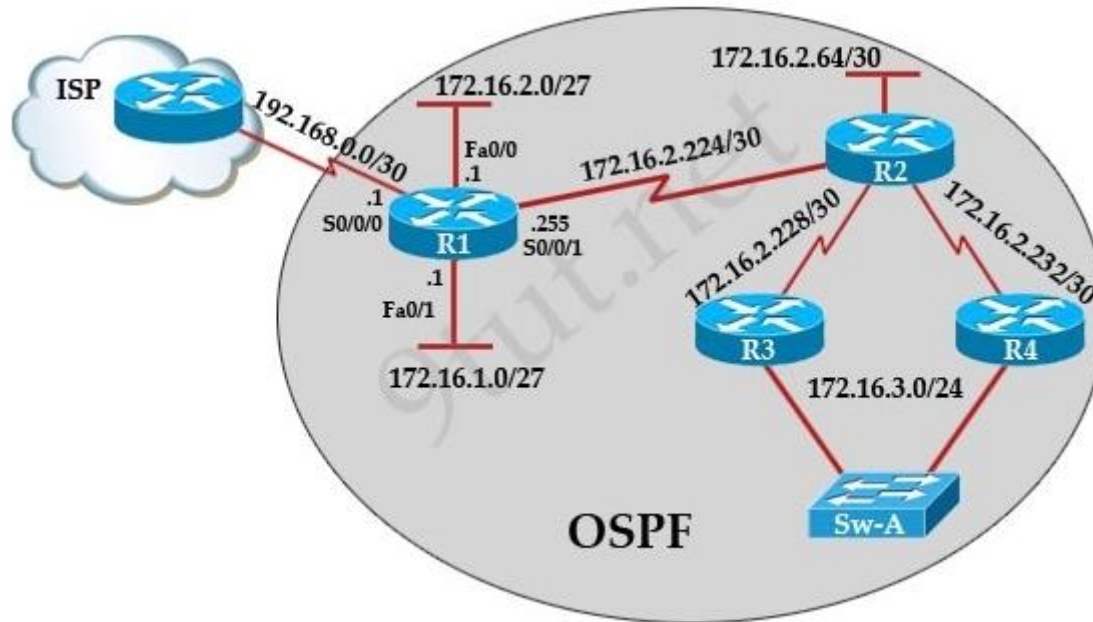
Explanation:

HELLO messages are used to maintain adjacent neighbors so even when the network is converged, hellos are still exchanged. On broadcast and point-to-point links, the default is 10 seconds, on NBMA the default is 30 seconds.

Although OSPF is a link-state protocol the full database from each router is sent every 30 minutes (not seconds) therefore, C and D are not correct.

QUESTION 63

R1 is configured with the default configuration of OSPF. From the following list of IP addresses configured on R1, which address will the OSPF process select as the router ID?



- A. 192.168.0.1
- B. 172.16.1.1
- C. 172.16.2.1
- D. 172.16.2.225

Correct Answer: A

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

The Router ID (RID) is an IP address used to identify the router and is chosen using the following sequence:

+ The highest IP address assigned to a loopback (logical) interface. + If a loopback interface is not defined, the highest IP address of all active router's

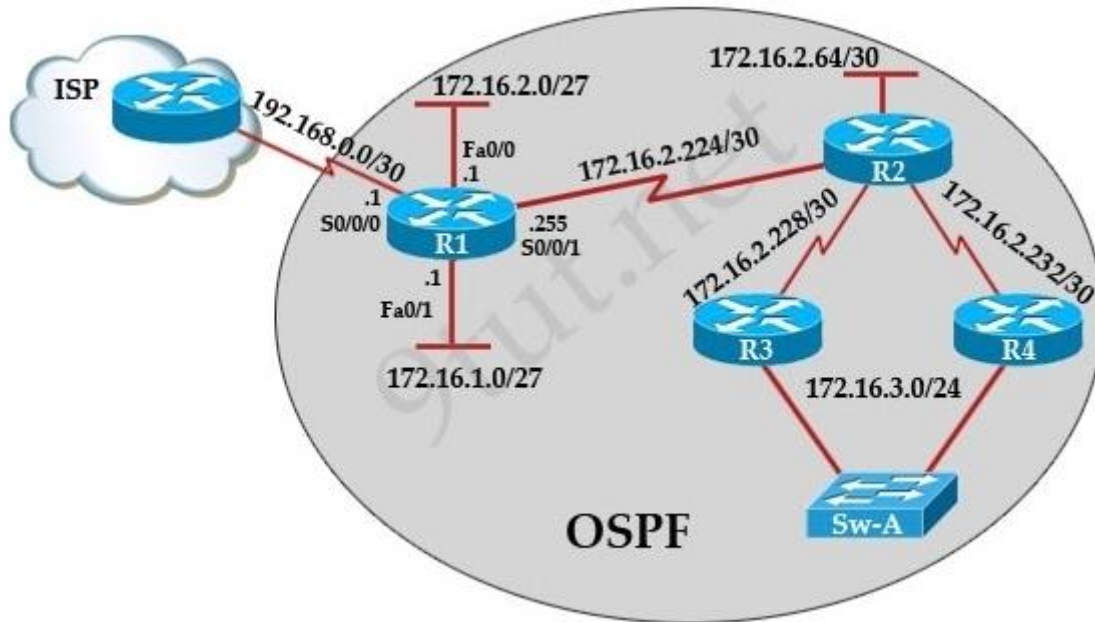
physical interfaces will be chosen.

+ The router ID can be manually assigned

In this case, because a loopback interface is not configured so the highest active IP address 192.168.0.1 is chosen as the router ID.

QUESTION 64

R1 is unable to establish an OSPF neighbor relationship with R3. What are possible reasons for this problem? (Choose two)



- A. All of the routers need to be configured for backbone Area 1.
- B. R1 and R2 are the DR and BDR, so OSPF will not establish neighbor adjacency with R3.
- C. A static route has been configured from R1 to R3 and prevents the neighbor adjacency from being established.
- D. The hello and dead interval timers are not set to the same values on R1 and R3.
- E. EIGRP is also configured on these routers with a lower administrative distance.
- F. R1 and R3 are configured in different areas.

Correct Answer: DF

Section: Troubleshooting

Explanation

Explanation/Reference:

Same as **Q105**

Explanation:

To become OSPF neighbors, routers must meet these requirements: Hello interval, Dead interval and AREA number -> D and F are correct.

QUESTION 65

What information does a router running a link-state protocol use to build and maintain its topological database? (Choose two)

- A. hello packets
- B. SAP messages sent by other routers
- C. LSAs from other routers
- D. beacons received on point-to-point links
- E. routing tables received from other link-state routers
- F. TTL packets from designated routers

Correct Answer: AC

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Link State Routing Protocols

Reference 1:

<http://www.ciscopress.com/articles/article.asp?p=24090&seqNum=4>

Explanation:

Link state protocols, sometimes called shortest path first or distributed database protocols, are built around a well-known algorithm from graph theory, E. W. Dijkstra's shortest path algorithm. Examples of link state routing protocols are:

- Open Shortest Path First (OSPF) for IP
-
- The ISO's Intermediate System to Intermediate System (IS-IS) for CLNS and IP
-
- DEC's DNA Phase V
-
- Novell's NetWare Link Services Protocol (NLSP)

Although link state protocols are rightly considered more complex than distance vector protocols, the basic functionality is not complex at all:

1. Each router establishes a relationship—an adjacency—with each of its neighbors.
2. Each router sends link state advertisements (LSAs), some
3. Each router stores a copy of all the LSAs it has seen in a database. If all works well, the databases in all routers should be identical.
4. The completed topological database, also called the link state database, describes a graph of the internetwork. Using the Dijkstra algorithm, each router calculates the shortest path to each network and enters this information into the route table.

OSPF Tutorial

Reference 2:

<http://www.9tut.com/ospf-routing-protocol-tutorial>

QUESTION 66

ROUTER# show ip route

192.168.12.0/24 is variably subnetted, 9 subnets, 3 masks

C 192.168.12.64 /28 is directly connected, Loopback1
C 192.168.12.32 /28 is directly connected, Ethernet0
C 192.168.12.48 /28 is directly connected, Loopback0
O 192.168.12.236 /30 [110/128] via 192.168.12.233, 00:35:36, Serial0
C 192.168.12.232 /30 is directly connected, Serial0
O 192.168.12.245 /30 [110/782] via 192.168.12.233, 00:35:36, Serial0
O 192.168.12.240 /30 [110/128] via 192.168.12.233, 00:35:36, Serial0
O 192.168.12.253 /30 [110/782] via 192.168.12.233, 00:35:37, Serial0
O 192.168.12.249 /30 [110/782] via 192.168.12.233, 00:35:37, Serial0
O 192.168.12.240/30 [110/128] via 192.168.12.233, 00:35:36, Serial 0

To what does the 128 refer to in the router output above?

- A. OSPF cost
- B. OSPF priority
- C. OSPF hop count
- D. OSPF ID number
- E. OSPF administrative distance

Correct Answer: A

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

The first parameter is the Administrative Distance of OSPF (110) while the second parameter is the cost of OSPF.

QUESTION 67

Which of the following describe the process identifier that is used to run OSPF on a router? (Choose two)

- A. It is locally significant.
- B. It is globally significant.
- C. It is needed to identify a unique instance of an OSPF database.
- D. It is an optional parameter required only if multiple OSPF processes are running on the router.
- E. All routers in the same OSPF area must have the same process ID if they are to exchange routing information.

Correct Answer: AC

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Reference:

<https://learningnetwork.cisco.com/thread/6248>

They are locally significant only, and have no bearing on the structure of any OSPF packet or LSA update. So you can have a separate process-id on every single router in your network if you so desire!

QUESTION 68

Open Shortest Path First (OSPF) is a routing protocol developed for Internet Protocol (IP) networks by the Interior Gateway Protocol (IGP) working group of the Internet Engineering Task Force (IETF). What is the default administrative distance of the OSPF routing protocol?

- A. 90
- B. 100
- C. 110
- D. 20

E. 130

F. 170

Correct Answer: C

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Default Distance Value Table

This table lists the administrative distance default values of the protocols that Cisco supports:

Route Source	Default Distance Values
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown*	255

* If the administrative distance is 255, the router does not believe the source of that route and does not install the route in the routing table.

QUESTION 69

Which address are OSPF hello packets addressed to on point-to-point networks?

- A. 224.0.0.5
- B. 172.16.0.1
- C. 192.168.0.5
- D. 223.0.0.1
- E. 254.255.255.255

Correct Answer: A

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Why Does the show ip ospf neighbor Command Reveal Neighbors in the Init State?

Reference:

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f11.shtml

Explanation:

OSPF hello packets have a destination address of 224.0.0.5 (the **all ospf routers multicast** address).

QUESTION 70

Which statements describe the routing protocol OSPF? (Choose three)

- A. It supports VLSM.
- B. It is used to route between autonomous systems.
- C. It confines network instability to one area of the network.
- D. It increases routing overhead on the network.
- E. It allows extensive control of routing updates.
- F. It is simpler to configure than RIP v2.

Correct Answer: ACE

Section: IP Routing Technologies

Explanation

Explanation/Reference:

OSPF Tutorial

Reference:

<http://www.9tut.com/ospf-routing-protocol-tutorial>

Explanation:

Routing overhead is the amount of information needed to describe the changes in a dynamic network topology. All routers in an OSPF area have identical copies of the topology database and the topology database of one area is hidden from the rest of the areas to **reduce routing overhead** because fewer routing updates are sent and smaller routing trees are computed and maintained (allow extensive control of routing updates and confine network instability to one area of the network).

QUESTION 71

How does a switch differ from a hub?

- A. A switch does not induce any latency into the frame transfer time.
- B. A switch tracks MAC addresses of directly-connected devices.
- C. A switch operates at a lower, more efficient layer of the OSI model.
- D. A switch decreases the number of broadcast domains.
- E. A switch decreases the number of collision domains.

Correct Answer: B

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Explanation:

Some of the features and functions of a switch include:

A switch is essentially a fast, multi-port bridge, which can contain dozens of ports. Rather than creating two collision domains, each port creates its own collision domain. In a network of twenty nodes, twenty collision domains exist if each node is plugged into its own switch port. If an uplink port is included, one switch creates twenty-one single-node collision domains. A switch dynamically builds and maintains a Content-Addressable Memory (CAM) table, holding all of the necessary MAC information for each port. For a detailed description of how switches operate, and their key differences to hubs.

QUESTION 72

What must occur before a workstation can exchange HTTP packets with a web server?

- A. A UDP connection must be established between the workstation and its default gateway.
- B. A UDP connection must be established between the workstation and the web server.
- C. A TCP connection must be established between the workstation and its default gateway.
- D. A TCP connection must be established between the workstation and the web server.
- E. An ICMP connection must be established between the workstation and its default gateway.
- F. An ICMP connection must be established between the workstation and the web server.

Correct Answer: D

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Common TCP/IP Ports

Reference:

<http://pentestlab.wordpress.com/2012/03/05/common-tcpip-ports/>

Explanation:

HTTP uses TCP port 80.

QUESTION 73

How does TCP differ from UDP? (Choose two.)

- A. TCP provides best effort delivery.
- B. TCP provides synchronized communication.
- C. TCP segments are essentially datagrams.
- D. TCP provides sequence numbering of packets.
- E. TCP uses broadcast delivery.

Correct Answer: BD

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Explanation:

TCP differs from UDP in the following ways: UDP provides best effort delivery. TCP provides synchronized communication. UDP segments are essentially datagrams. TCP provides sequence numbering of packets. UDP uses broadcast delivery.

Application	Telnet, FTP, etc
Transport	TCP, UDP
Network	IP, ICMP
Physical	drivers, interface card

QUESTION 74

A workstation has just resolved a browser URL to the IP address of a server. What protocol will the workstation now use to determine the destination MAC address to be placed into frames directed toward the server?

- A. HTTP
- B. DNS
- C. DHCP
- D. RARP
- E. ARP

Correct Answer: E

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Explanation:

The RARP protocol is used to translate hardware interface addresses to protocol addresses. The RARP message format is very similar to the ARP format. When the booting computer sends the broadcast ARP request, it places its own hardware address in both the sending and receiving fields in the encapsulated ARP data packet. The RARP server will fill in the correct sending and receiving IP addresses in its response to the message. This way the booting computer will know its IP address when it gets the message from the RARP server.

QUESTION 75

The network manager has requested a 300-workstation expansion of the network. The workstations are to be installed in a single broadcast domain, but each workstation must have its own collision domain. The expansion is to be as cost-effective as possible while still meeting the requirements. Which three items will adequately fulfill the request? (Choose three).

- A. one IP subnet with a mask of 255.255.254.0
- B. two IP subnets with a mask of 255.255.255.0
- C. seven 48-port hubs
- D. seven 48-port switches
- E. one router interface
- F. seven router interfaces

Correct Answer: ADE

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

Explanation:

of 255.255.254.0 can absorb 510 hosts being 23 bits mask and also 7*48 port switches can handle this much hosts and router interface is required to be minimum to avoid unnecessary wastage hence the answers.

QUESTION 76

What are two common TCP applications? (Choose two.)

- A. TFTP
- B. SMTP
- C. SNMP
- D. FTP
- E. DNS

Correct Answer: BD

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Common TCP/IP Ports

Reference:

<http://pentestlab.wordpress.com/2012/03/05/common-tcpip-ports/>

Explanation:

SMTP uses TCP port 25, while FTP uses TCP ports 20 and 21.

QUESTION 77

Which two options will help to solve the problem of a network that is suffering a broadcast storm? (Choose two.)

- A. a bridge
- B. a router
- C. a hub
- D. a Layer 3 switch
- E. an access point

Correct Answer: BD

Section: LAN Switching Technologies

Explanation

Explanation/Reference:

Explanation:

Routers and layer 3 switches will not propagate broadcast traffic beyond the local segment, so the use of these devices is the best method for eliminating broadcast storms.

QUESTION 78

What does a host on an Ethernet network do when it is creating a frame and it does not have the destination address?

- A. drops the frame
- B. sends out a Layer 3 broadcast message
- C. sends a message to the router requesting the address
- D. sends out an ARP request with the destination IP address

Correct Answer: D

Section: LAN Switching Technologies

Explanation

Explanation/Reference:

Explanation:

Understanding this concept is prime for understanding that when switch receives the data frame from the host not having the MAC address already in the MAC table, it will add the MAC address to the source port on the MAC address table and sends the data frame. If the switch already has the MAC address in it's table for the destination, it will forward the frame directly to the destination port. If it was not already in it's MAC table, then they frame

would have been flooded out all ports except for the port that it came from.

QUESTION 79

A switch has 48 ports and 4 VLANs. How many collision and broadcast domains exist on the switch (collision, broadcast)?

- A. 4, 48
- B. 48, 4
- C. 48, 1
- D. 1, 48
- E. 4, 1

Correct Answer: B

Section: LAN Switching Technologies

Explanation

Explanation/Reference:

Explanation:

A switch uses a separate collision domain for each port, and each VLAN is a separate broadcast domain.

QUESTION 80

Some routers have been configured with default routes. What are some of the advantages of using default routes? (Choose two)

- A. They establish routes that will never go down.
- B. They keep routing tables small.
- C. They require a great deal of CPU power.
- D. They allow connectivity to remote networks that are not in the routing table
- E. They direct traffic from the internet into corporate networks.

Correct Answer: BD

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Cisco administration 101: What you need to know about default routes

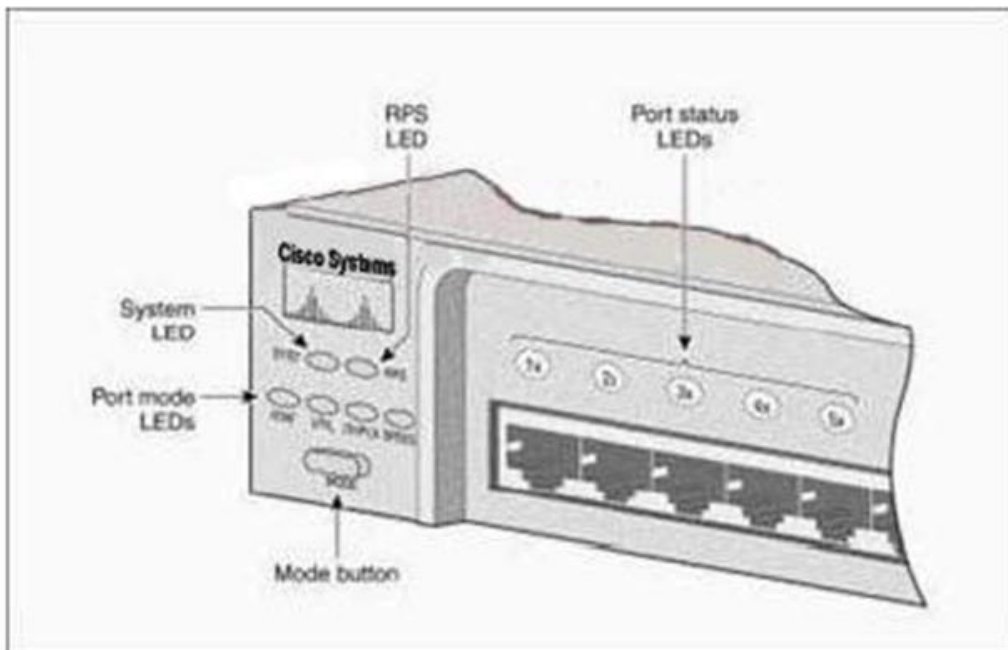
Reference:

<http://www.techrepublic.com/article/cisco-administration-101-what-you-need-to-know-about-default-routes/>

QUESTION 81

Refer to the exhibit.

After the power-on-self test (POST), the system LED of a Cisco 2950 switch turns amber. What is the status of the switch?



- A. The POST was successful.
- B. The switch has a problem with the internal power supply and needs an external power supply to be attached.
- C. POST failed and there is a problem that prevents the operating system from being loaded.
- D. The switch has experienced an internal problem but data can still be forwarded at a slower rate.
- E. The switch passed POST, but all the switch ports are busy.

Correct Answer: C

Section: Troubleshooting

Explanation

Explanation/Reference:**Troubleshoot and Understand POST Failure Messages**

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps607/products_tech_note09186a0080125913.shtml

Explanation:

Each time you power up the switch, eight Power-On Self Tests (POSTs) run automatically. POSTs check the most important system components before the switch begins to forward packets. When the switch begins the POST, the port status LEDs display amber for two seconds, and then display green. As each test runs, the port status LEDs go out. 1x is the first to go out. The port status LEDs for ports 2x through 8x go out sequentially as the system completes a test.

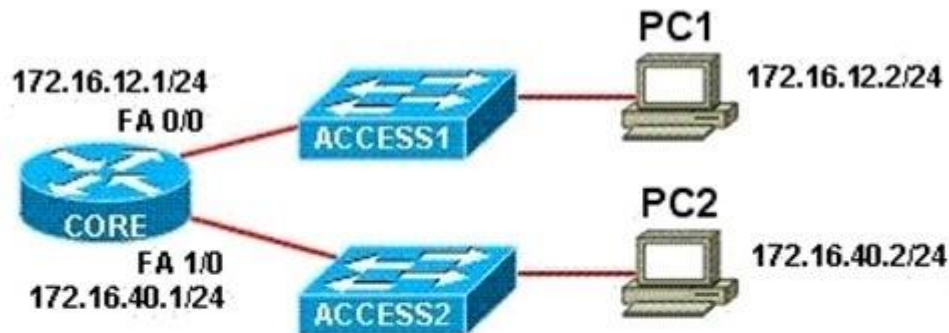
When the POST completes successfully, the port status LEDs go out. This indicates that the switch is operational. If a test fails, the port status LED associated with the test displays amber. The system LED also displays amber.

Note: From Cisco IOS Software Release 11.2(8.5)SA6 onwards, the port and system LEDs both remain amber after a POST failure. In the earlier Cisco IOS Software Releases, only the LEDs of failed linked ports remained amber.

QUESTION 82

Refer to the exhibit.

PC1 pings PC2. What three things will CORE router do with the data that is received from PC1? (Choose three.)



```

CORE# show arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 172.16.12.1      -          0001.4210.3BA9  ARPA   FastEthernet0/0
Internet 172.16.12.2      0          0010.111A.7AB0  ARPA   FastEthernet0/0
Internet 172.16.40.1      -          00D0.FF59.4A85  ARPA   FastEthernet1/0
Internet 172.16.40.2      0          00E0.80B7.EAB1  ARPA   FastEthernet1/0
CORE#
  
```

- A. The data frames will be forwarded out interface FastEthernet0/1 of CORE router.
- B. The data frames will be forwarded out interface FastEthernet1/0 of CORE router.
- C. CORE router will replace the destination IP address of the packets with the IP address of PC2.
- D. CORE router will replace the MAC address of PC2 in the destination MAC address of the frames.
- E. CORE router will put the IP address of the forwarding FastEthernet interface in the place of the source IP address in the packets.
- F. CORE router will put the MAC address of the forwarding FastEthernet interface in the place of the source MAC address.

Correct Answer: BDF

Section: IP Routing Technologies

Explanation

Explanation/Reference:

QUESTION 83

Which three statements are correct about RIP version 2? (Choose three)

- A. It uses broadcast for its routing updates.

- B. It supports authentication.
- C. It is a classless routing protocol.
- D. It has a lower default administrative distance than RIP version 1.
- E. It has the same maximum hop count as RIP version 1.
- F. It does not send the subnet mask any updates.

Correct Answer: BCE

Section: IP Routing Technologies

Explanation

Explanation/Reference:

QUESTION 84

To what type of port would a cable with a DB-60 connector attach?

- A. Serial port
- B. Console port
- C. Ethernet port
- D. Fibre optic port

Correct Answer: A

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

QUESTION 85

Which IP address is a private address?

- A. 12.0.0.1
- B. 168.172.19.39
- C. 172.20.14.36
- D. 172.33.194.30
- E. 192.169.42.34

Correct Answer: C

Section: IP addressing (IPv4 / IPv6)
Explanation

Explanation/Reference:

Answer: C

Explanation:

Private IP Address Ranges (RFC 1918)

Class	From	To	CIDR Mask	Decimal Mask
Class A (24 Bit)	10.0.0.0	10.255.255.255	/8	255.0.0.0
Class B (20 Bit)	172.16.0.0	172.31.255.255	/12	255.240.0.0
Class C (16 Bit)	192.168.0.0	192.168.255.255	/16	255.255.0.0

QUESTION 86

How many simultaneous Telnet sessions does a Cisco router support by default?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5
- F. 6

Correct Answer: E

Section: LAN Switching Technologies

Explanation

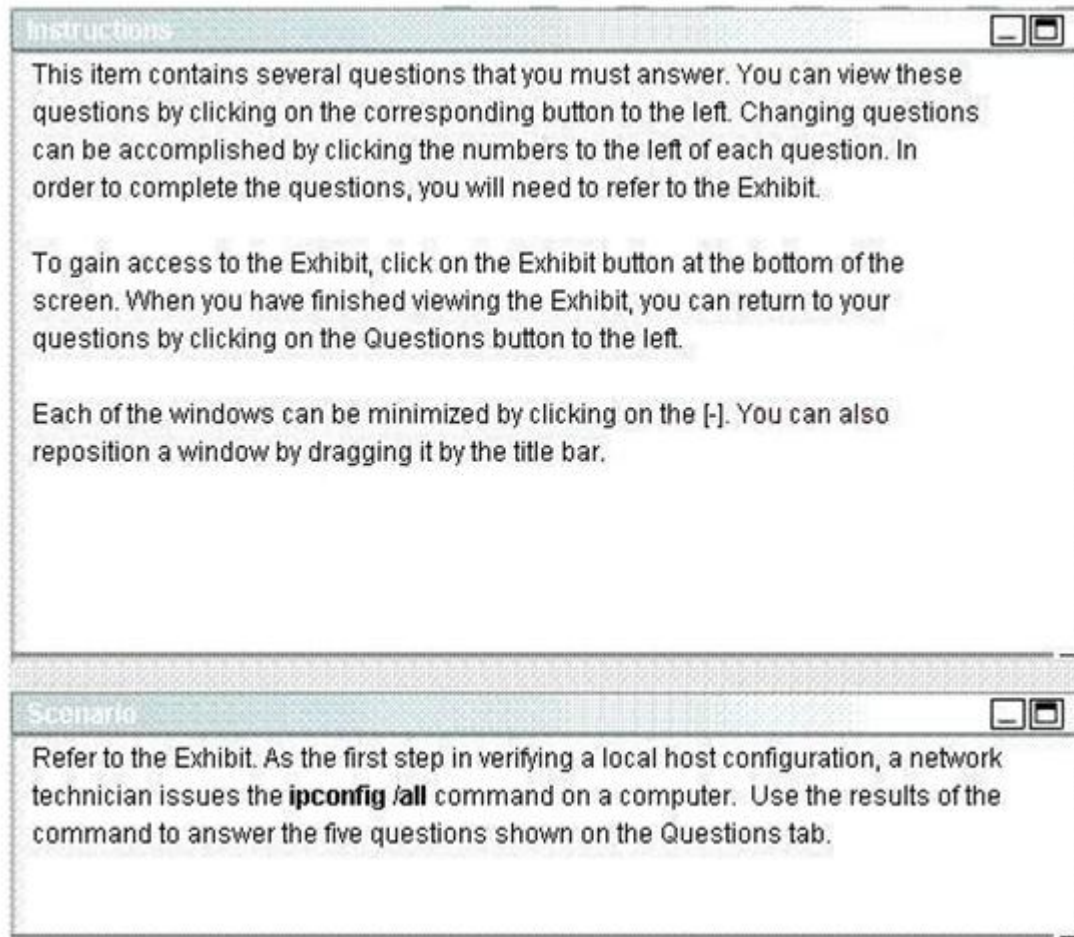
Explanation/Reference:

line vty 0 4

QUESTION 87

Refer to the exhibit.

What two things can the technician determine by successfully pinging from this computer to the IP address 172.16.236.1? (Choose two)




```
Exhibit
C:\WINNT\system32\cmd.exe

Connection-specific DNS Suffix . : cisco.com
Description . . . . . : Intel(R) PRO/1000 MT Mobile

Physical Address. . . . . : 00-0D-60-FD-F0-34
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 172.16.236.227
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.236.1
DHCP Server . . . . . : 172.16.3.2
DNS Servers . . . . . : 10.4.8.1
                       : 10.5.2.22
Primary WINS Server . . . . . : 10.69.2.87
Secondary WINS Server . . . . . : 10.69.235.228
Lease Obtained . . . . . : Monday, June 11, 2007 9:26:45 AM
Lease Expires . . . . . : Thursday, June 14, 2007 9:26:45 AM

Ethernet adapter Local Area Connection:

Media State . . . . . : Cable Disconnected
Description . . . . . : Cisco Systems Wireless LAN Adapter
Physical Address. . . . . : 00-0E-9B-48-86-2A
```

- A. The network card on the computer is functioning correctly.
- B. The default static route on the gateway router is correctly configured.
- C. The correct default gateway IP address is configured on the computer.
- D. The device with the IP address 172.16.236.1 is reachable over the network.
- E. The default gateway at 172.16.236.1 is able to forward packets to the internet.

Correct Answer: AD

Section: LAN Switching Technologies

Explanation

Explanation/Reference:

Explanation:

The source and destination addresses are on the same network therefore, a default gateway is not necessary for communication between these two

addresses.

QUESTION 88

Refer to the exhibit.

Why did the device return this message?

```
WG1R2#show ru
% Ambiguous command: "show ru"
WG1R2#_
```

- A. The command requires additional options or parameters
- B. There is no show command that starts with ru.
- C. The command is being executed from the wrong router mode.
- D. There is more than one show command that starts with the letters ru.

Correct Answer: D

Section: Troubleshooting

Explanation

Explanation/Reference:

Answer: D

Explanation:

Answer D is correct because when you type the incomplete command having more same more command same upto types characters it shows display the ambiguous command error.

QUESTION 89

What is the purpose of flow control?

- A. To ensure data is retransmitted if an acknowledgement is not received.

- B. To reassemble segments in the correct order at the destination device.
- C. To provide a means for the receiver to govern the amount of data sent by the sender.
- D. To regulate the size of each segment.

Correct Answer: C

Section: LAN Switching Technologies

Explanation

Explanation/Reference:

Flow Control

Reference:

<http://whatistechtarget.com/definition/flow-control>

Explanation:

Flow control is the management of data flow between computers or devices or between nodes in a network so that the data can be handled at an efficient pace. Too much data arriving before a device can handle it causes data overflow, meaning the data is either lost or must be retransmitted. For serial data transmission locally or in a network, the **Xon/Xoff** protocol can be used. For **modem** connections, either Xon/Xoff or CTS/RTS (Clear to Send/Ready to Send) commands can be used to control data flow.

In a network, flow control can also be applied by refusing additional device connections until the flow of traffic has subsided.

QUESTION 90

OSPF routing uses the concept of areas. What are the characteristics of OSPF areas? (Chose three)

- A. Each OSPF area requires a loopback interface to be configured
- B. Areas may be assigned any number from 0 to 65535
- C. Area 0 is called the backbone area
- D. Hierarchical OSPF networks do not require multiple areas
- E. Multiple OSPF areas must connect to area 0
- F. Single area OSPF networks must be configured in area 1

Correct Answer: BCE

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

I used to think the answers should be C D E and here is my explanation:

OSPF can use an active interface for its router ID, so a loopback interface is not a must -> A is incorrect.

OSPF Area is a 32-bit number so we can use up to $2^{32} - 1 = 4294967296 - 1$ (since Area 0 is the first area). Remember that only process ID is a 16-bit number and ranges from 1 to 65535 -> B is incorrect.

F is incorrect too because single area OSPF networks must be configured in Area 0, which is called the backbone area.

For answer D, it is a bit hard to guess what they want to say about "hierarchical" but we should understand "Hierarchical OSPF networks" as "OSPF networks". D is correct because we can only have one area (area 0 – the backbone area) for our networks.

But TT commented on 01-11-2010:

Especially to note on choice B, D, and E:

Choice B: we all know that The areas can be any number from 0 to 4.2 billion and 1 to 65,535 for the Process ID. As choice B specifies 'area' (be aware, it's not saying 'process id'), there is no reason to say that we cannot assign numbers from 0 to 65535 for area # (it is using 'may be', not 'have to be' or 'ought to be'). Hence, we do not worry about assigning '0'.

Choice E: as Area 0 is the backbone, we all understand that any areas in a OSPF network have to be connected to it. And actually this is implicitly saying that multiple areas form a hierarchical OSPF network, as Area 0 being a root and others being its leaves.

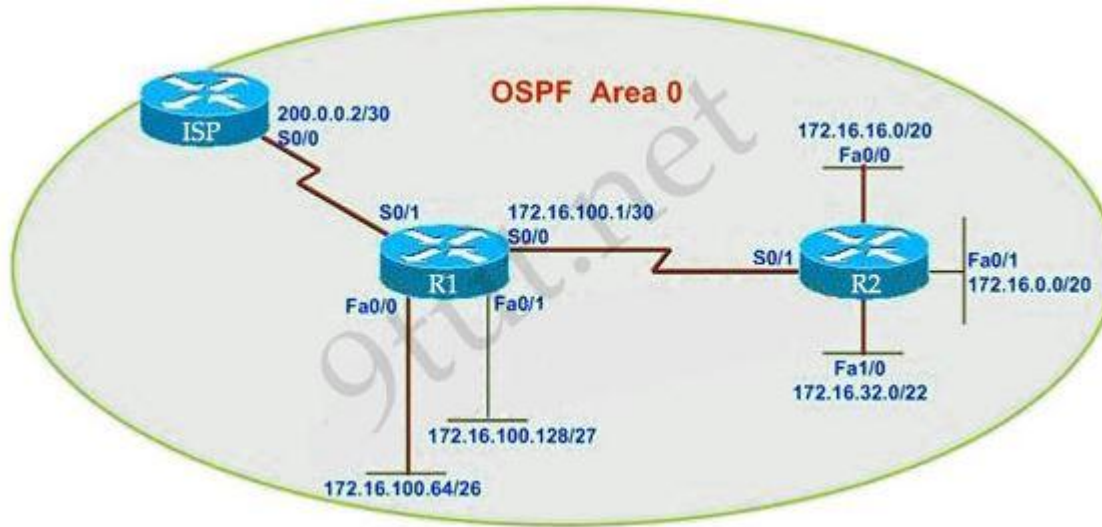
Choice D: when it specifies 'Hierarchical', at least 2 areas should be required to form such topology (of course that includes Area 0)

Although Choice B is not an absolutely accurate statement since it not only can be assigned up to 65535, it is still a correct answer. And again, it specifies 'area', not 'process id', so '0' can be included. Finally, it would be meaningless to call OSPF a hierarchical network if no more than one area is present.

I reviewed the question and think it is a more suitable solution with choice B than choice D, surely it is a tricky question!

QUESTION 91

Part of the OSPF network is shown below:



Configuration exhibit:

R1 routing commands:

```
ip route 0.0.0.0 0.0.0.0 serial0/0
router ospf 1
network 172.16.100.0 0.0.0.3 area 0
network 172.16.100.64 0.0.0.63 area 0
network 172.16.100.128 0.0.0.31 area 0
default-information originate
```

You work as a network technician, study the exhibits carefully. Assume that all router interfaces are operational and correctly configured. In addition, assume that OSPF has been correctly configured on router R2. How will the default route configured on R1 affect the operation of R2?

- A. Any packet destined for a network that is not directly connected to router R2 will be dropped immediately.
- B. Any packet destined for a network that is not directly connected to router R1 will be dropped.
- C. Any packet destined for a network that is not directly connected to router R2 will be dropped immediately because of the lack of a gateway on R1.
- D. The network directly connected to a router R2 will not be able to communicate with the 172.16.100.0, 172.16.100.28 and 172.16.100.64 subnetworks.
- E. Any packet destined for a network that is not referenced in the routing table of router R2 will be directed to R1. R1 will then send that packet back to R2 and a routing loop will occur.

Correct Answer: E
Section: IP Routing Technologies
Explanation

Explanation/Reference:
Explanation:

First, notice that the more-specific routes will always be favored over less-specific routes regardless of the administrative distance set for a protocol. In this case, because we use OSPF for three networks (172.16.100.0 0.0.0.3, 172.16.100.64 0.0.0.63, 172.16.100.128 0.0.0.31) so the packets destined for these networks will not be affected by the default route.

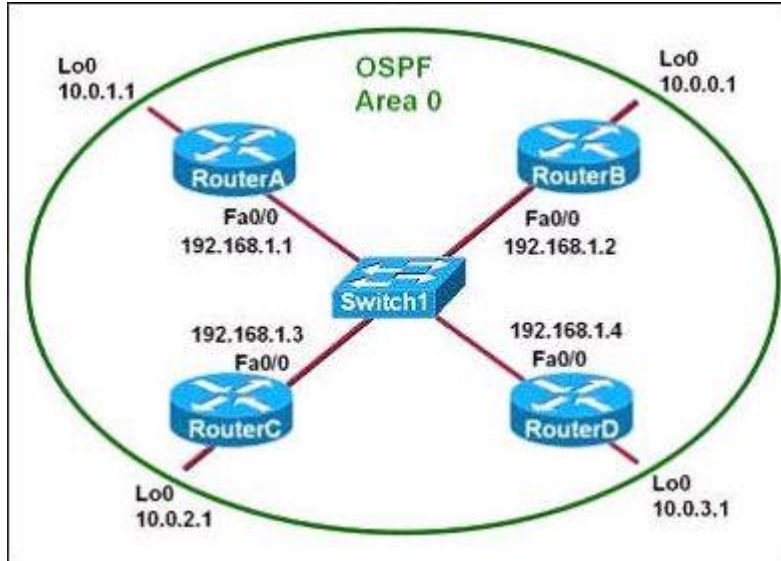
The default route configured on R1 "ip route 0.0.0.0 0.0.0.0 serial0/0" will send any packet whose destination network is not referenced in the routing table of router R1 to R2, it doesn't drop anything so answers A, B and C are not correct. D is not correct too because these routes are declared in R1 and the question says that "OSPF has been correctly configured on router R2", so network directly connected to router R2 can communicate with those three subnetworks.

As said above, the default route configured on R1 will send any packet destined for a network that is not referenced in its routing table to R2; R2 in turn sends it to R1 because it is the only way and a routing loop will occur.

QUESTION 92

Refer to the exhibit.

Which two statements are true about the loopback address that is configured on RouterB? (Choose two)



- A. It ensures that data will be forwarded by RouterB.
- B. It provides stability for the OSPF process on RouterB.
- C. It specifies that the router ID for RouterB should be 10.0.0.1.
- D. It decreases the metric for routes that are advertised from RouterB.
- E. It indicates that RouterB should be elected the DR for the LAN.

Correct Answer: C

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

A loopback interface never comes down even if the link is broken so it provides stability for the OSPF process (for example we use that loopback interface as the router-id) -> B is correct.

The router-ID is chosen in the order below:

- + The highest IP address assigned to a loopback (logical) interface.
 - + If a loopback interface is not defined, the highest IP address of all active router's physical interfaces will be chosen.
- > The loopback interface will be chosen as the router ID of RouterB -> C is correct.

QUESTION 93

Which characteristics are representative of a link-state routing protocol? (Choose three)

- A. provides common view of entire topology
- B. exchanges routing tables with neighbors
- C. calculates shortest path
- D. utilizes event-triggered updates
- E. utilizes frequent periodic updates

Correct Answer: ACD

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

Each of the routers running link-state routing protocol learns the paths to all the destinations in its "area" so we can say A is correct although it is a bit unclear.

Link-state routing protocols generate routing updates only (not the whole routing table) when a change occurs in the network topology so B is not correct.

Link-state routing protocol like OSPF uses Dijkstra algorithm to calculate the shortest path -> C is correct.

Unlike Distance vector routing protocol (which utilizes frequent periodic updates), link-state routing protocol utilizes event-triggered updates (only sends update when a change occurs) -> D is correct but E is not correct.

QUESTION 94

City# show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.12.48	YES	manual	up	up
FastEthernet0/1	192.168.12.65	YES	manual	up	up
Serial0/0	192.168.12.121	YES	manual	up	up
Serial0/1	unassigned	YES	unset	up	up
Serial0/1.102	192.168.12.125	YES	manual	up	up
Serial0/1.103	192.168.12.129	YES	manual	up	up
Serial0/1.104	192.168.12.133	YES	manual	up	up

City#

A network associate has configured OSPF with the command:

City(config-router)# network 192.168.12.64 0.0.0.63 area 0

After completing the configuration, the associate discovers that not all the interfaces are participating in OSPF.

Which three of the interfaces shown in the exhibit will participate in OSPF according to this configuration statement? (Choose three)

- A. FastEthernet0/0
- B. FastEthernet0/1
- C. Serial0/0
- D. Serial0/1.102
- E. Serial0/1.103
- F. Serial0/1.104

Correct Answer: BCD

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

Explanation:

The "network 192.168.12.64 0.0.0.63 equals to network 192.168.12.64/26. This network has:

- + Increment: 64 (/26= 1111 1111.1111 1111.1111 1111.1100 0000)
- + Network address: 192.168.12.64
- + Broadcast address: 192.168.12.127

Therefore all interface in the range of this network will join OSPF -> B C D are correct.

QUESTION 95

When running OSPF, what would cause router A not to form an adjacency with router B?



- A. The loopback addresses are on different subnets.
- B. The values of the dead timers on the routers are different.
- C. Route summarization is enabled on both routers.
- D. The process identifier on router A is different than the process identifier on router.

Correct Answer: B

Section: IP Routing Technologies

Explanation

Explanation/Reference:

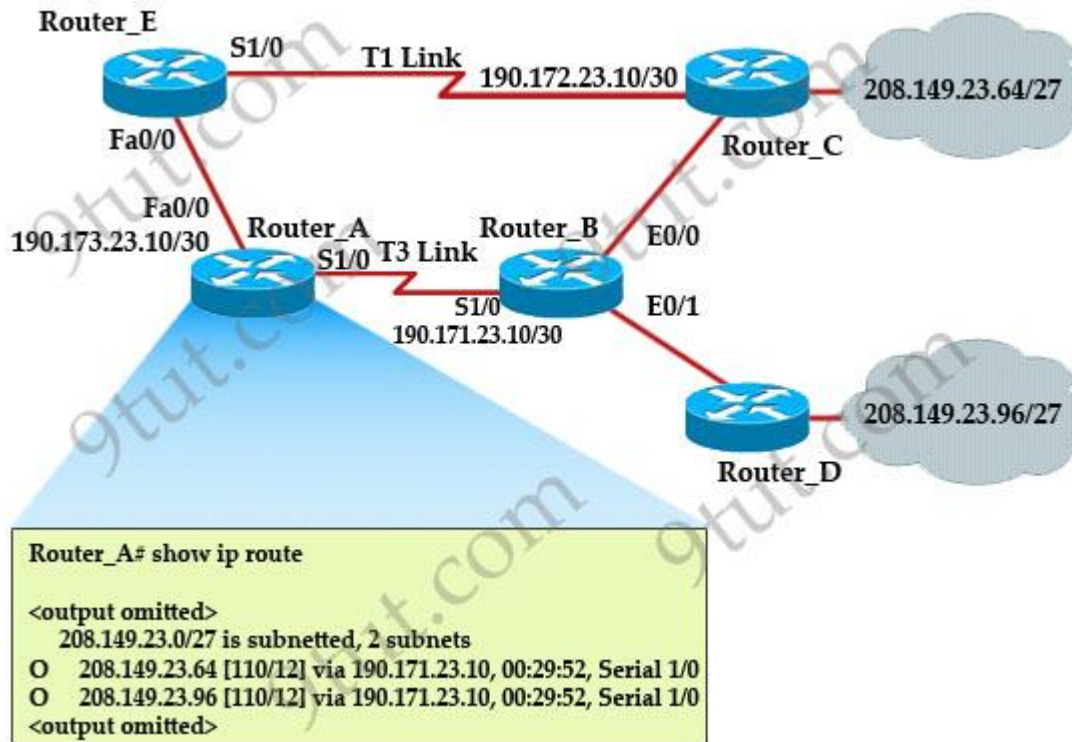
Explanation:

To form an adjacency (become neighbor), router A & B must have the same Hello interval, Dead interval and AREA number.

QUESTION 96

Refer to the exhibit.

The network is converged. After link-state advertisements are received from Router_A, what information will Router_E contain in its routing table for the subnets 208.149.23.64 and 208.149.23.96?



- A. 208.149.23.64[110/13] via 190.173.23.10, 00:00:00:07, FastEthernet0/0
208.149.23.96[110/13] via 190.173.23.10, 00:00:00:16, FastEthernet0/0
- B. 208.149.23.64[110/1] via 190.173.23.10, 00:00:00:07, Serial1/0
208.149.23.96[110/3] via 190.173.23.10, 00:00:00:16, FastEthernet0/0
- C. 208.149.23.64[110/13] via 190.173.23.10, 00:00:00:07, Serial1/0
208.149.23.96[110/13] via 190.173.23.10, 00:00:00:16, Serial1/0
208.149.23.96[110/13] via 190.173.23.10, 00:00:00:16, FastEthernet0/0
- D. 208.149.23.64[110/13] via 190.173.23.10, 00:00:00:07, Serial1/0

208.149.23.96[110/13] via 190.173.23.10, 00:00:00:16, Serial1/0

Correct Answer: A

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

Router_E learns two subnets, subnets 208.149.23.64 and 208.149.23.96 via Router_A through FastEthernet interface. The interface cost is calculated with the formula $108 / \text{Bandwidth}$. For FastEthernet it is $108 / 100 \text{ Mbps} = 108 / 100,000,000 = 1$. Therefore the cost is **12** (learned from Router_A) + **1** = **13** for both subnets -> B is not correct.

The cost through T1 link is much higher than through T3 link ($T1 \text{ cost} = 108 / 1.544 \text{ Mbps} = 64$; $T3 \text{ cost} = 108 / 45 \text{ Mbps} = 2$) so surely OSPF will choose the path through T3 link -> Router_E will choose the path from Router_A through FastEthernet0/0, not Serial1/0 -> C & D are not correct.

In fact, we can quickly eliminate answers B, C and D because they contain at least one subnet learned from Serial1/0 -> they are surely incorrect.

QUESTION 97

Which commands are required to properly configure a router to run OSPF and to add network 192.168.16.0/24 to OSPF area 0? (Choose two)

- A. Router(config)#router ospf 1
- B. Router(config)#router ospf 0
- C. Router(config)#router ospf area 0
- D. Router(config-router)#network 192.168.16.0 0.0.0.255 area 0
- E. Router(config-router)#network 192.168.16.0 0.0.0.255 0
- F. Router(config-router)#network 192.168.16.0 255.255.255.0 area 0

Correct Answer: AD

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Enabling OSPF

Reference:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/12-4t/iro-cfg.html#GUID-588D1301-F63C-4DAC-BF1C-C3735EB13673

Explanation:

In the router ospf process-id ranges from 1 to 65535 so, 0 is an invalid process-id number -> A is correct but, B is not correct.

To configure OSPF, we need a wildcard in the “network” statement, not a subnet mask. We also need to assign an area to this process -> D is correct.

QUESTION 98

Which parameter or parameters are used to calculate OSPF cost in Cisco routers?

- A. Bandwidth, Delay and MTU
- B. Bandwidth
- C. Bandwidth and MTU
- D. Bandwidth, MTU, Reliability, Delay and Load

Correct Answer: B

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

The well-known formula to calculate OSPF cost is

$\text{Cost} = 108 / \text{Bandwidth}$

so B is the correct answer.

QUESTION 99

Refer to the exhibit.

Why are two OSPF designated routers identified on Core-Router?

Neighbor_ID	Pri	State	Dead Time	Address	Interface
208.149.23.194	1	Full/DR	00:00:33	190.172.32.10	Ethernet1
208.149.23.60	1	Full/BDR	00:00:33	190.172.32.10	Ethernet0
208.149.23.130	1	Full/DR	00:00:39	190.172.32.10	Ethernet0

- A. Core-Router is connected to more than one multi-access network.

- B. The router at 208.149.23.130 is a secondary DR in case the primary fails.
- C. Two router IDs have the same OSPF priority and are therefore tied for DR election
- D. The DR election is still underway and there are two contenders for the role.

Correct Answer: A

Section: IP Routing Technologies

Explanation

Explanation/Reference:

Explanation:

OSPF elects one DR per multi-access network. In the exhibit there are two DR so there must have more than one multi-access network.

QUESTION 100

What is the default maximum number of equal-cost paths that can be placed into the routing of a Cisco OSPF router?

- A. 16
- B. 2
- C. Unlimited
- D. 4

Correct Answer: D

Section: LAN Switching Technologies

Explanation

Explanation/Reference:

Reference:

http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/routing/configuration/guide/rc37ospf.html

Explanation:

The default number of equal-cost paths that can be placed into the routing of a Cisco OSPF router is 4. We can change this default value by using "maximum-paths" command:

Router(config-router)#maximum-paths 2

Note: Cisco routers support up to 16 equal-cost paths. In detail, the default number of maximum paths is 32 for Cisco CRS-1 routers and 16 for Cisco XR 12000 Series Routers. The range is from 1 to 32 for Cisco CRS-1 routers and 1 to 16 for Cisco XR 12000 Series Routers.

QUESTION 101

What is the OSPF default frequency, in seconds, at which a Cisco router sends hello packets on a multiaccess network?

- A. 10
- B. 40
- C. 30
- D. 20

Correct Answer: A

Section: IP Routing Technologies

Explanation

Explanation/Reference:

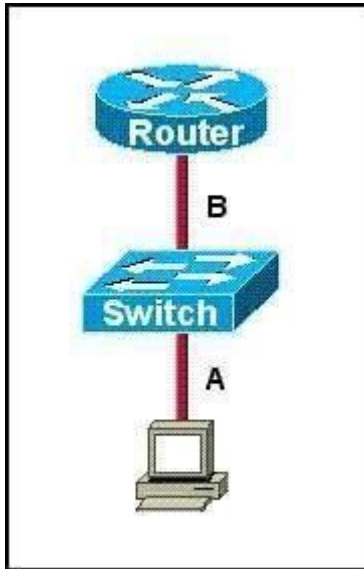
Explanation:

On broadcast multiaccess and point-to-point links, the default is 10 seconds. On NBMA, the default is 30 seconds.

QUESTION 102

Refer to the exhibit.

The two connected ports on the switch are not turning orange or green. What would be the most effective steps to troubleshoot this physical layer problem? (Choose three.)



- A. Ensure that the Ethernet encapsulations match on the interconnected router and switch ports.
- B. Ensure that cables A and B are straight-through cables.
- C. Ensure cable A is plugged into a trunk port.
- D. Ensure the switch has power.
- E. Reboot all of the devices.
- F. Reseat all cables.

Correct Answer: BDF

Section: Troubleshooting

Explanation

Explanation/Reference:

QUESTION 103

Which command can you use to manually assign a static IPV6 address to a router interface?

- A. ipv6 address PREFIX_1::1/64
- B. ipv6 autoconfig 2001:db8:2222:7272::72/64
- C. ipv6 autoconfig

D. ipv6 address 2001:db8:2222:7272::72/64

Correct Answer: D

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

QUESTION 104

The network administrator is using a Windows PC application that is called putty.exe for remote communication to a switch for network troubleshooting. Which two protocols could be used during this communication? (Choose two.)

- A. SNMP
- B. HTTP
- C. Telnet
- D. RMON
- E. SSH

Correct Answer: CE

Section: IP Services

Explanation

Explanation/Reference:

QUESTION 105

What should be part of a comprehensive network security plan?

- A. Allow users to develop their own approach to network security.
- B. Physically secure network equipment from potential access by unauthorized individuals.
- C. Encourage users to use personal information in their passwords to minimize the likelihood of passwords being forgotten.
- D. Delay deployment of software patches and updates until their effect on end-user equipment is well known and widely reported.
- E. Minimize network overhead by deactivating automatic antivirus client updates.

Correct Answer: B

Section: Network Device Security

Explanation

Explanation/Reference:**QUESTION 106**

Which two of these statements are true of IPv6 address representation? (Choose two.)

- A. There are four types of IPv6 addresses: unicast, multicast, anycast, and broadcast.
- B. A single interface may be assigned multiple IPv6 addresses of any type.
- C. Every IPv6 interface contains at least one loopback address.
- D. The first 64 bits represent the dynamically created interface ID.
- E. Leading zeros in an IPv6 16 bit hexadecimal field are mandatory.

Correct Answer: BC

Section: IP addressing (IPv4 / IPv6)

Explanation**Explanation/Reference:****IPv6 Addressing**

Reference:

http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8026003d.pdf

Explanation:

- A single interface may be assigned multiple addresses of any type (unicast, anycast, multicast).
- Every IPv6-enabled interface must contain at least one loopback and one link-local address.
- Optionally, every interface can have multiple unique local and global addresses.

IPv6 host addresses can be assigned in multiple ways:

- Static configuration
- Stateless autoconfiguration
- DHCPv6

When IPv6 is used over Ethernet networks, the Ethernet MAC address can be used to generate the 64-bit interface ID for the host. This is called the EUI-64 address.

Since MAC addresses use 48 bits, additional bits must be inserted to fill the 64 bits required.

QUESTION 107

A network administrator cannot connect to a remote router by using SSH. Part of the show interfaces command is shown.

```
router#show interfaces  
Serial0/1/0 is up, line protocol is down
```

At which OSI layer should the administrator begin troubleshooting?

- A. physical
- B. data link
- C. network
- D. transport

Correct Answer: B

Section: IP Services

Explanation

Explanation/Reference:

Serial 0 is up, line protocol is down

Reference:

<https://learningnetwork.cisco.com/thread/12389>

Explanation:

I think the indication here is "Serial 0 is up, line protocol is down". What causes this indication? Correct me if I am wrong. When you have this indication, a cable unplugged is not a correct answer. If you check the output of your "show interface serial 0" comand again, you should notice it as "Serial 0 is down, line protocol is down. Under the "show ip int brief" you should see status = down and protocol = down as opposed to up, down. Becuase you disconnected the cable, layer 1 will go down, which is indicated by the serial 0 down status. The line protocol status is for layer 2. So, a cable unplugged is not a correct answer to "Serial 0 is up, line protocol is down". Hope this helps.

Layer	Function	Examples
Application (Layer 7)	User interface	Telnet, HTTP
Presentation (Layer 6)	Handles encryption & changes to syntax	ASCII/EBCDIC, JPEG/MP3
Session (Layer 5)	Manages multiple applications and maintains synchronisation points	Operating systems, scheduling
Transport (Layer 4)	Provides reliable or best-effort delivery and (optional) error and flow control	TCP, UDP
Network (Layer 3)	Provides logical end-to-end addressing used by routers and hosts	IP
Data Link (Layer 2)	Creates frames from data bits, uses MAC addresses to access endpoints, and provides error detection but no correction	802.3, 802.2, HDLC, Frame Relay
Physical (Layer 1)	Specifies voltage, wire speed, and cable pin-outs	EIA/TIA, V.35

QUESTION 108

Which option is a valid IPv6 address?

- A. 2001:0000:130F::099a::12a
- B. 2002:7654:A1AD:61:81AF:CCC1
- C. FEC0:ABCD:WXYZ:0067::2A4
- D. 2004:1:25A4:886F::1

Correct Answer: D

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

IPv6 Addressing

Reference:

<http://www.ipv6.com/articles/general/IPv6-Addressing.htm>

Explanation:

IPv6 Address Notation

IPv6 addresses are denoted by eight groups of hexadecimal quartets separated by colons in between them.

Following is an example of a valid IPv6 address: 2001:cdba:0000:0000:0000:0000:3257:9652

Any four-digit group of zeroes within an IPv6 address may be reduced to a single zero or altogether omitted. Therefore, the following IPv6 addresses are similar and equally valid:

2001:cdba:0000:0000:0000:0000:3257:9652
2001:cdba:0:0:0:0:3257:9652
2001:cdba::3257:9652

The URL for the above address will be of the form:

`http://[2001:cdba:0000:0000:0000:0000:3257:9652]/`

QUESTION 109

What is the purpose of the switchport command?

```
Switch(config-if)# switchport port-security maximum 1  
Switch(config-if)# switchport port-security mac-address 0018.DE8B.4BF8
```

- A. It ensures that only the device with the MAC address 0018.DE8B.4BF8 will be able to connect to the port that is being configured.
- B. It informs the switch that traffic destined for MAC address 0018.DE8B.4BF8 should only be sent to the port that is being configured.
- C. It will act like an access list and the port will filter packets that have a source or destination MAC of 0018.DE8B.4BF8.
- D. The switch will shut down the port of any traffic with source MAC address of 0018.DE8B.4BF8.

Correct Answer: A

Section: Network Device Security

Explanation

Explanation/Reference:

QUESTION 110

How many bits are contained in each field of an IPv6 address?

- A. 24
- B. 4
- C. 8
- D. 16

Correct Answer: D

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:
IPv6 Addressing

Reference:

http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8026003d.pdf

Explanation:

One of the key advantages IPv6 brings is the exponentially larger address space. The following will outline the basic address architecture of IPv6.

128-bit-long addresses

Represented in hexadecimal format:

- Uses CIDR principles: prefix/prefix length
- x:x:x:x:x:x:x, where x is a 16-bit hex field
- The last 64 bits are used for the interface ID

QUESTION 111

Which three approaches can be used while migrating from an IPv4 addressing scheme to an IPv6 scheme (Choose three)

- A. static mapping of IPv4 address to IPv6 addresses
- B. configuring IPv4 tunnels between IPv6 islands
- C. use DHCPv6 to map IPv4 addresses to IPv6 addresses
- D. use proxying and translation (NAT-PT) to translate IPv6 packets into IPv4 packets
- E. configure IPv6 directly
- F. enable dual-stack routing

Correct Answer: BDF

Section: IP addressing (IPv4 / IPv6)
Explanation

Explanation/Reference:
The IPv6 Transition

Reference 1:
<http://www.opus1.com/ipv6/howdoitransitiontoipv6.html>

Explanation:

Connecting IPv6 islands with tunnels

An IPv6 island is a network made of IPv6 links directly connected by IPv6 routers. In the early days of IPv6 deployment, there are many IPv6 islands. IPv6 in IPv4 tunnels are used to connect those islands together. In each island, one (or more) dual stack routers are designated to encapsulate and decapsulate IPv6 packets within IPv4 packets. Different mechanisms have been developed to manage tunnels: automatic tunnels³, configured tunnels³, tunnel brokers³, 6over4³, 6to4³,...

Reference 2:
<http://www.petri.co.il/ipv6-transition.htm>

Network Address Translation - Protocol Translation (NAT-PT)

The NAT-PT method enables the ability to either statically or dynamically configure a translation of a IPv4 network address into an IPv6 network address and vice versa. For those familiar with more typically NAT implementations, the operation is very similar but includes a protocol translation function. NAT-PT also ties in an Application Layer Gateway (ALG) functionality that converts Domain Name System (DNS) mappings between protocols.

Dual Stack

The simplest approach when transitioning to IPv6 is to run IPv6 on all of the devices that are currently running IPv4. If this is something that is possible within the organizational network, it is very easy to implement. However, for many organizations, IPv6 is not supported on all of the IPv4 devices; in these situations other methods must be considered.

QUESTION 112

Which statement about IPv6 is true?

- A. Addresses are not hierarchical and are assigned at random.
- B. Only one IPv6 address can exist on a given interface.
- C. There are 2.7 billion addresses available.
- D. Broadcasts have been eliminated and replaced with multicasts.

Correct Answer: D

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference: IPv6 Address Types

Reference:

[http://technet.microsoft.com/en-us/library/cc757359\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc757359(v=ws.10).aspx)

Explanation:

IPv6 has three types of addresses, which can be categorized by type and scope:

Unicast addresses. A packet is delivered to one interface.

Multicast addresses. A packet is delivered to multiple interfaces.

Anycast addresses. A packet is delivered to the nearest of multiple interfaces (in terms of routing distance).

IPv6 does not use broadcast messages.

Unicast and anycast addresses in IPv6 have the following scopes (for multicast addresses, the scope is built into the address structure):

Link-local. The scope is the local link (nodes on the same subnet).

Site-local. The scope is the organization (private site addressing).

Global. The scope is global (IPv6 Internet addresses).

In addition, IPv6 has special addresses such as the loopback address. The scope of a special address depends on the type of special address. Much of the IPv6 address space is unassigned.

QUESTION 113

What are two recommended ways of protecting network device configuration files from outside network security threats? (Choose two.)

- A. Allow unrestricted access to the console or VTY ports.
- B. Use a firewall to restrict access from the outside to the network devices.
- C. Always use Telnet to access the device command line because its data is automatically encrypted.
- D. Use SSH or another encrypted and authenticated transport to access device configurations.
- E. Prevent the loss of passwords by disabling password encryption.

Correct Answer: BD

Section: Network Device Security

Explanation**Explanation/Reference:****QUESTION 114**

A receiving host has failed to receive all of the segments that it should acknowledge. What can the host do to improve the reliability of this communication session?

- A. decrease the window size
- B. use a different source port for the session
- C. decrease the sequence number
- D. obtain a new IP address from the DHCP server
- E. start a new session using UDP

Correct Answer: A

Section: Troubleshooting

Explanation**Explanation/Reference:****QUESTION 115**

Which command enables IPv6 forwarding on a cisco router?

- A. ipv6 host
- B. ipv6 unicast-routing
- C. ipv6 local
- D. ipv6 neighbor

Correct Answer: B

Section: IP addressing (IPv4 / IPv6)

Explanation**Explanation/Reference:**

Enabling IPv6 on Cisco IOS Software Technology

Reference:

<http://www.ciscopress.com/articles/article.asp?p=31948&seqNum=4>

Explanation:

The first step of enabling IPv6 on a Cisco router is the activation of IPv6 traffic forwarding to forward unicast IPv6 packets between network interfaces. By default, IPv6 traffic forwarding is disabled on Cisco routers.

The ipv6 unicast-routing command is used to enable the forwarding of IPv6 packets between interfaces on the router. The syntax for this command is as follows:

Router(config)#ipv6 unicast-routing

The ipv6 unicast-routing command is enabled on a global basis.

QUESTION 116

Identify the four valid IPv6 addresses. (Choose four.)

- A. ::
- B. ::192:168:0:1
- C. 2000::
- D. 2001:3452:4952:2837::
- E. 2002:c0a8:101::42
- F. 2003:dead:beef:4dad:23:46:bb:101

Correct Answer: ABEF

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

IPv6 Address Validation

Reference 1:

<http://www.intermapper.com/ipv6validator>

Reference 2:

http://www.ripe.net/lir-services/new-lir/ipv6_reference_card.pdf

Explanation:

Address	Value	Description
Global	2000::/3	These are assigned by the IANA and used on public networks. They are equivalent to IPv4 global (sometimes called public) addresses. ISPs summarize these to provide scalability in the Internet.
Reserved	(range)	Reserved addresses are used for specific types of anycast as well as for future use. Currently about 1/256th of the IPv6 address space is reserved.
Private	FE80::/10	Like IPv4, IPv6 supports private addressing, which is used by devices that don't need to access a public network. The first two digits are FE, and the third digit can range from 8 to F.
Loopback	::1	Like the 127.0.0.1 address in IPv4, 0:0:0:0:0:0:0:1, or ::1, is used for local testing functions; unlike IPv4, which dedicates a complete A class block of addresses for local testing, only one is used in IPv6.
Unspecified	::	0.0.0.0 in IPv4 means "unknown" address. In IPv6, this is represented by 0:0:0:0:0:0:0:0, or ::, and is typically used in the source address field of the packet when an interface doesn't have an address and is trying to acquire one dynamically.

QUESTION 117

Which two statements describe characteristics of IPv6 unicast addressing? (Choose two.)

- A. Global addresses start with 2000::/3.
- B. Link-local addresses start with FE00:/12.
- C. Link-local addresses start with FF00::/10.
- D. There is only one loopback address and it is ::1.
- E. If a global address is assigned to an interface, then that is the only allowable address for the interface.

Correct Answer: AD
Section: IP addressing (IPv4 / IPv6)
Explanation

Explanation/Reference:
IPv6 Address Validation

Explanation:

Address	Value	Description
Global	2000::/3	These are assigned by the IANA and used on public networks. They are equivalent to IPv4 global (sometimes called public) addresses. ISPs summarize these to provide scalability in the Internet.
Reserved	(range)	Reserved addresses are used for specific types of anycast as well as for future use. Currently about 1/256th of the IPv6 address space is reserved.
Private	FE80::/10	Like IPv4, IPv6 supports private addressing, which is used by devices that don't need to access a public network. The first two digits are FE, and the third digit can range from 8 to F.
Loopback	::1	Like the 127.0.0.1 address in IPv4, 0:0:0:0:0:0:0:1, or ::1, is used for local testing functions; unlike IPv4, which dedicates a complete A class block of addresses for local testing, only one is used in IPv6.
Unspecified	::	0.0.0.0 in IPv4 means "unknown" address. In IPv6, this is represented by 0:0:0:0:0:0:0:0, or ::, and is typically used in the source address field of the packet when an interface doesn't have an address and is trying to acquire one dynamically.

QUESTION 118

A network administrator is trying to add a new router into an established OSPF network. The networks attached to the new router do not appear in the routing tables of the other OSPF routers. Given the information in the partial configuration shown below, what configuration error is causing this problem?

```
Router(config)# router ospf 1
Router(config-router)# network 10.0.0.0 255.0.0.0 area 0
```

- A. The process id is configured improperly.
- B. The OSPF area is configured improperly.
- C. The network wildcard mask is configured improperly.
- D. The network number is configured improperly.
- E. The AS is configured improperly.
- F. The network subnet mask is configured improperly.

Correct Answer: C

Section: IP Routing Technologies

Explanation

Explanation/Reference:

QUESTION 119

Which statement is true?

- A. An IPv6 address is 64 bits long and is represented as hexadecimal characters.
- B. An IPv6 address is 32 bits long and is represented as decimal digits.
- C. An IPv6 address is 128 bits long and is represented as decimal digits.
- D. An IPv6 address is 128 bits long and is represented as hexadecimal characters.

Correct Answer: D

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

IPv6 Addressing

Reference:

http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8026003d.pdf

Explanation:

One of the key advantages IPv6 brings is the exponentially larger address space. The following will outline the basic address architecture of IPv6.

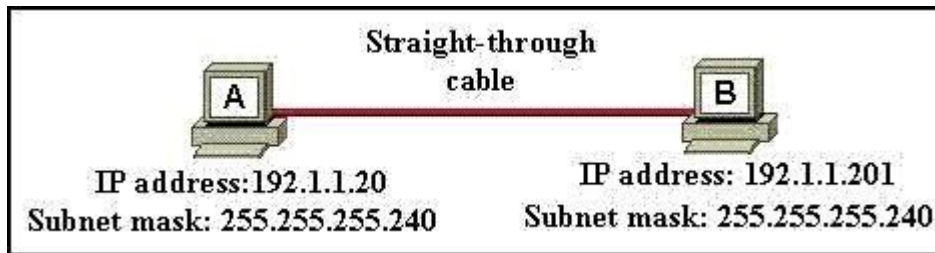
128-bit-long addresses

Represented in hexadecimal format:

- Uses CIDR principles: prefix/prefix length
- x:x:x:x:x:x:x, where x is a 16-bit hex field
- The last 64 bits are used for the interface ID

QUESTION 120

A network administrator is connecting PC hosts A and B directly through their Ethernet interfaces as shown in the graphic. Ping attempts between the hosts are unsuccessful. What can be done to provide connectivity between the hosts? (choose two.)



- A. A crossover cable should be used in place of the straight-through cable.
- B. A rollover cable should be used in place of the straight-through cable.
- C. The subnet masks should be set to 255.255.255.192
- D. A default gateway needs to be set on each host.
- E. The hosts must be reconfigured to use private IP addresses for direct connections of this type.
- F. The subnet masks should be set to 255.255.255.0

Correct Answer: AF

Section: Operation of IP Data Networks

Explanation

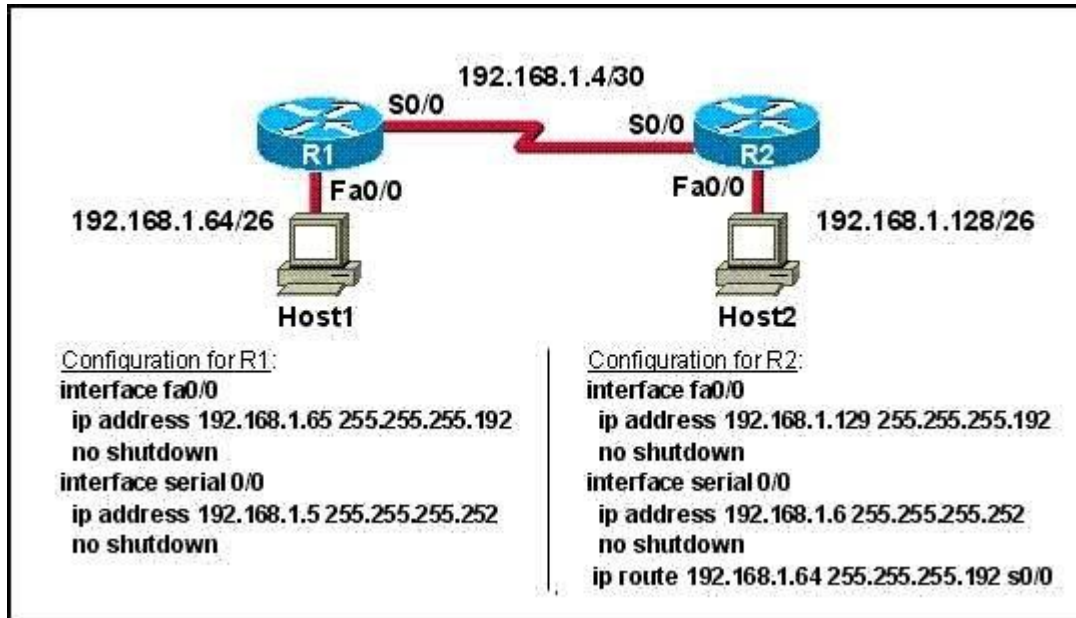
Explanation/Reference:

QUESTION 121

Refer to the exhibit.

A technician pastes the configurations in the exhibit into the two new routers shown. Otherwise, the routers are configured with their default configurations.

A ping from Host1 to Host 2 fails, but the technician is able to ping the S0/0 interface of R2 from Host 1. The configurations of the hosts have been verified as correct. What could be the cause of the problem?



- A. The serial cable on R1 needs to be replaced.
- B. The interfaces on R2 are not configured properly
- C. R1 has no route to the 192.168.1.128 network.
- D. The IP addressing scheme has overlapping subnetworks.
- E. The ip subnet-zero command must be configured on both routers.

Correct Answer: C

Section: Troubleshooting

Explanation

Explanation/Reference:

Explanation:

Without a static route pointing to host 2 network the router is unaware of the path to take to reach that network and reply traffic cannot be sent.

QUESTION 122

Refer to the exhibit.

Serial 0/0 does not respond to a ping request from a host on the FastEthernet 0/0 LAN. How can this problem be corrected?

BHM# show ip interface brief					
Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.16.1	YES	NVRAM	up	up
Serial0/0	192.168.15.2	YES	NVRAM	administratively down	down
FastEthernet0/1	192.168.17.1	YES	NVRAM	up	up
Serial0/1	unassigned	YES	NVRAM	administratively down	down

- A. Enable the Serial 0/0 interface.
- B. Correct the IP address for Serial 0/0.
- C. Correct the IP address for FastEthernet 0/0
- D. Change the encapsulation type on Serial 0/0
- E. Enable autoconfiguration on the Serial 0/0 interface

Correct Answer: A

Section: Troubleshooting

Explanation

Explanation/Reference:

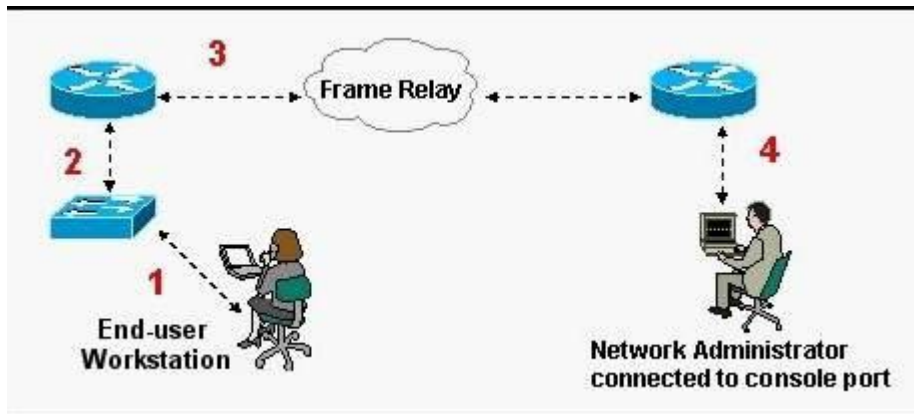
Explanation:

Serial 0/0 interface is administratively down therefore, you will have to run the "no shutdown" command to enable the interface for data.

QUESTION 123

Refer to the exhibit.

What kind of cable should be used to make each connection that is identified by the numbers shown?



- A. 1 - Ethernet Crossover cable
2 - Ethernet straight-through cable
3 - Fiber Optic cable
4 - Rollover cable
- B. 1 - Ethernet straight-through cable
2 - Ethernet straight-through cable
3 - Serial cable
4 - Rollover cable
- C. 1 - Ethernet rollover cable
2 - Ethernet crossover cable
3 - Serial cable
4 - Null-modem cable
- D. 1 - Ethernet straight-through cable
2 - Ethernet Crossover cable
3 - Serial cable
4 - Rollover cable
- E. 1 - Ethernet straight-through cable
2 - Ethernet Crossover cable
3 - Serial cable
4 - Ethernet Straight-through cable

Correct Answer: B

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:**QUESTION 124**

Which of the following are types of flow control? (choose three.)

- A. buffering
- B. cut-through
- C. windowing
- D. congestion avoidance
- E. load balancing

Correct Answer: ACD

Section: Operation of IP Data Networks

Explanation

Explanation/Reference:

Flow Control Types (Transmission Control over networks)

Reference:

<http://www.info-it.net/cisco/ccna/exam-tips/flow-control.php>

Explanation:

Congestion

During Transfer of data, a high speed computer is generating data traffic a lot faster than the network device can handle in transferring to destination, so single gateway or destination device can not handle much amount of traffic that is called "**Congestion**".

Buffering

The Technie is used to control the data transfer when we have congestion, when a network device receive a data it stores in memory section and then transfer to next destination this process called "**Buffering**".

Windowing

Whereas Windowing is used for flow control by the Transport layer.

Say the sender device is sending segments and the receiver device can accommodate only a fixed number of segments before it can accept more, the two devices negotiate the window size during the connection setup. This is done so that the sending device doesn't overflow the receiving device's buffer.

Also the receiving device can send a single acknowledgement for the segments it has received instead of sending an acknowledgement after every segment received.

Also, this window size is dynamic meaning, the devices can negotiate and change the window size in the middle of a session. So if initially the window size is three and the receiving device thinks that it can accept more number of segments in its buffer it can negotiate with the sending device and it increase it to say 5 for example.

Windowing is used only by TCP since UDP doesn't use or allow flow control.

QUESTION 125

If an ethernet port on a router was assigned an IP address of 172.16.112.1/20, what is the maximum number of hosts allowed on this subnet?

- A. 1024
- B. 2046
- C. 4094
- D. 4096
- E. 8190

Correct Answer: C

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

Explanation:

Each octet represents eight bits. The bits, in turn, represent (from left to right):

128, 64, 32, 16, 8, 4, 2, 1

Add them up and you get 255. Add one for the all zeros option, and the total is 256.

Now take away one of these for the network address (all zeros) and another for the broadcast address (all ones). Each octet represents 254 possible hosts. Or 254 possible networks. Unless you have subnet zero set on your network gear, in which case you could conceivably have 255.

The CIDR addressing format (**/20**) tells us that 20 bits are used for the network portion, so the maximum number of networks are 2^{20} minus one if you have subnet zero enabled, or minus 2 if not.

You asked about the number of hosts. That will be 32 minus the number of network bits, minus two. So calculate it as $(2^{(32-20)})-2$, or $(2^{12})-2 = 4094$

QUESTION 126

Refer to the exhibit.

Why was this message received?

```
WG1R2#telnet 10.3.1.2
Trying 10.3.1.2 ... Open

Password required, but none set

[Connection to 10.3.1.2 closed by foreign host]
WG1R2#_
```

- A. No VTY password has been set.
- B. No enable password has been set.
- C. No console password has been set.
- D. No enable secret password has been set.
- E. The login command has not been set on CON 0
- F. The login command has not been set on the VTY ports.

Correct Answer: A

Section: Troubleshooting

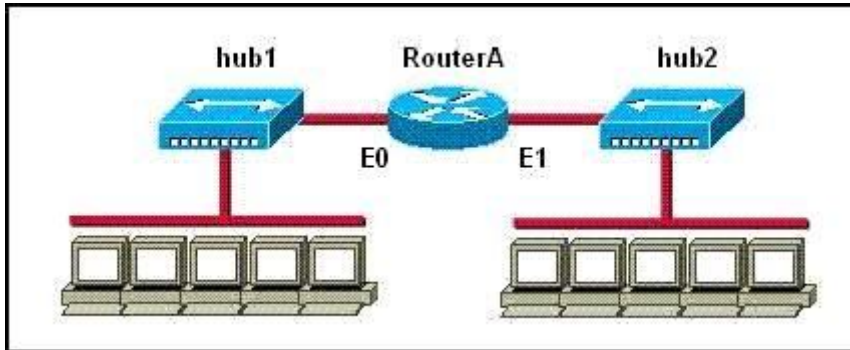
Explanation

Explanation/Reference:

QUESTION 127

Refer to the exhibit.

How many collision domains are shown?



- A. one
- B. two
- C. three
- D. four
- E. six
- F. twelve

Correct Answer: B

Section: LAN Switching Technologies

Explanation

Explanation/Reference:

Explanation:

Hubs create single collision and broadcast domains.

QUESTION 128

Refer to the exhibit.

After configuring two interfaces on the HQ router, the network administrator notices an error message. What must be done to fix this error?

```
HQ# configure terminal
HQ(config)# interface fastethernet 0/0
HQ(config-if)# ip address 192.168.1.17 255.255.255.0
HQ(config-if)# no shutdown
HQ(config-if)# interface serial 0/0
HQ(config-if)# ip address 192.168.1.65 255.255.255.240
HQ(config-if)# no shutdown
% 192.168.1.0 overlaps with FastEthernet0/0
```

- A. The serial interface must be configured first.
- B. The serial interface must use the address 192.168.1.2
- C. The subnet mask of the serial interface should be changed to 255.255.255.0
- D. The subnet mask of the FastEthernet interface should be changed to 255.255.255.240
- E. The address of the FastEthernet interface should be changed to 192.168.1.66

Correct Answer: D

Section: Troubleshooting

Explanation

Explanation/Reference:

QUESTION 129

What does the "Inside Global" address represent in the configuration of NAT?

- A. the summarized address for all of the internal subnetted addresses
- B. the MAC address of the router used by inside hosts to connect to the Internet
- C. a globally unique, private IP address assigned to a host on the inside network
- D. a registered address that represents an inside host to an outside network

Correct Answer: D

Section: IP Routing Technologies

Explanation

Explanation/Reference:

NAT: Local and Global Definitions

Reference:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094837.shtml

Explanation:

Cisco defines these terms as:

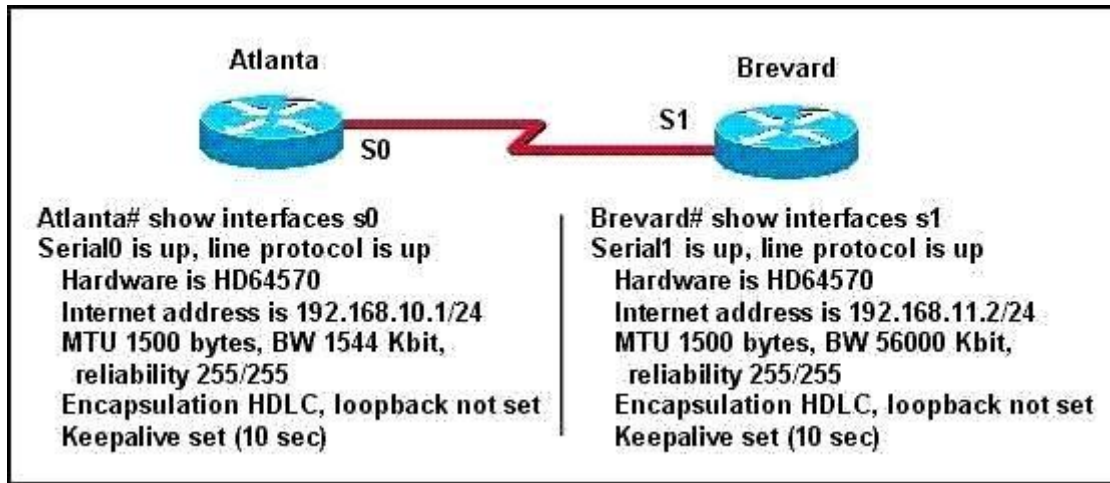
- **Inside local address**—The IP address assigned to a host on the inside network. This is the address configured as a parameter of the computer OS or received via dynamic address allocation protocols such as DHCP. The address is likely not a legitimate IP address assigned by the Network Information Center (NIC) or service provider.
- **Inside global address**—A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world.
- **Outside local address**—The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it is allocated from an address space routable on the inside.
- **Outside global address**—The IP address assigned to a host on the outside network by the host owner. The address is allocated from a globally routable address or network space.

These definitions still leave a lot to be interpreted. For this example, this document redefines these terms by first defining local address and global address. Keep in mind that the terms inside and outside are NAT definitions. Interfaces on a NAT router are defined as inside or outside with the NAT configuration commands, ip nat inside destination and ip nat outside source . Networks to which these interfaces connect can then be thought of as inside networks or outside networks, respectively.

- **Local address**—A local address is any address that appears on the inside portion of the network.
- **Global address**—A global address is any address that appears on the outside portion of the network.

QUESTION 130

Two routers named Atlanta and Brevard are connected by their serial interfaces as shown in the exhibit, but there is no data connectivity between them. The Atlanta router is known to have a correct configuration. Given the partial configurations shown in the exhibit, what is the problem on the Brevard router that is causing the lack of connectivity?



- A. A loopback is not set.
- B. The IP address is incorrect.
- C. The subnet mask is incorrect.
- D. The serial line encapsulations are incompatible.
- E. The maximum transmission unit (MTU) size is too large.
- F. The bandwidth setting is incompatible with the connected interface.

Correct Answer: B

Section: Troubleshooting

Explanation

Explanation/Reference:

Explanation:

The IP address of routers are in different networks.

QUESTION 131

Which of the following statements are TRUE regarding Cisco access lists? (Choose two.)

- A. In an inbound access list, packets are filtered as they enter an interface.
- B. In an inbound access list, packets are filtered before they exit an interface.

- C. Extended access lists are used to filter protocol-specific packets.
- D. You must specify a deny statement at the end of each access list to filter unwanted traffic.
- E. When a line is added to an existing access list, it is inserted at the beginning of the access list.

Correct Answer: AC

Section: IP Services

Explanation

Explanation/Reference:

Explanation:

In an inbound access list, packets are filtered as they enter an interface. Extended access lists are used to filter protocol specific packets. Access lists can be used in a variety of situations when the router needs to be given guidelines for decision-making. These situations include:

- Filtering traffic as it passes through the router
- To control access to the VTY lines (Telnet)
- To identify "interesting" traffic to invoke Demand Dial Routing (DDR) calls
- To filter and control routing updates from one router to another

There are two types of access lists, standard and extended. Standard access lists are applied as close to the destination as possible (outbound), and can only base their filtering criteria on the source IP address. The number used while creating an access list specifies the type of access list created. The range used for standard access lists is 1 to 99 and 1300 to 1999. Extended access lists are applied as close to the source as possible (inbound), and can base their filtering criteria on the source or destination IP address, or on the specific protocol being used. The range used for extended access lists is 100 to 199 and 2000 to 2699.

Other features of access lists include:

- Inbound access lists are processed before the packet is routed.
- Outbound access lists are processed after the packet has been routed to an exit interface.
- An "implicit deny" is at the bottom of every access list, which means that if a packet has not matched any preceding access list condition, it will be filtered (dropped).
- Access lists require at least one permit statement, or all packets will be filtered (dropped).
- One access list may be configured per direction for each Layer 3 protocol configured on an interface

The option stating that in an inbound access list, packets are filtered before they exit an interface is incorrect. Packets are filtered as they exit an interface when using an outbound access list.

The option stating that a deny statement must be specified at the end of each access list in order to filter unwanted traffic is incorrect. There is an implicit deny at the bottom of every access list.

When a line is added to an existing access list, it is not inserted at the beginning of the access list. It is inserted at the end. This should be taken into consideration. For example, given the following access list, executing the command `access-list 110 deny tcp 192.168.5.0 0.0.0.255 any eq www` would have NO effect on the packets being filtered because it would be inserted at the end of the list, AFTER the line that allows all traffic.


```
access-list 110 permit ip host 192.168.5.1 any
access-list 110 deny icmp 192.168.5.0 0.0.0.255 any echo
access-list 110 permit any any
```

QUESTION 132

Which statements are TRUE regarding Internet Protocol version 6 (IPv6) addresses? (Choose three.)

- A. An IPv6 address is divided into eight 16-bit groups.
- B. A double colon (::) can only be used once in a single IPv6 address.
- C. IPv6 addresses are 196 bits in length.
- D. Leading zeros cannot be omitted in an IPv6 address.
- E. Groups with a value of 0 can be represented with a single 0 in IPv6 address.

Correct Answer: ABE

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

Explanation:

IPv6 addresses are divided into eight 16-bit groups, a double colon (::) can only be used once in an IPv6 address, and groups with a value of 0 can be represented with a single 0 in an IPv6 address.

The following statements are also true regarding IPv6 address:

- **IPv6 addresses are 128 bits in length.**
- **Eight 16-bit groups are divided by a colon (:).**
- **Multiple groups of 16-bit 0s can be represented with double colon (::).**
- **Double colons (::) represent only 0s.**
- **Leading zeros can be omitted in an IPv6 address.**

The option stating that IPv6 addresses are 196 bits in length is incorrect. IPv6 addresses are 128 bits in length.

The option stating that leading zeros cannot be omitted in an IPv6 address is incorrect. Leading zeros can be omitted in an IPv6 address.

QUESTION 133

Which of the following IP addresses are valid Class B host addresses if a default Class B mask is in use? (Choose two.)

- A. 10.6.8.35
- B. 133.6.5.4
- C. 192.168.5.9
- D. 127.0.0.1
- E. 190.6.5.4

Correct Answer: BE

Section: IP addressing (IPv4 / IPv6)

Explanation

Explanation/Reference:

Explanation:

The IP addresses 133.6.5.4 and 190.6.5.4 are both valid Class B addresses when a default mask is in use. The Class B default mask is 255.255.0.0 and the range of valid addresses is 128.0.0.0-191.255.255.255.

The IP address 10.6.8.35 is a Class A address. The Class A default mask is 255.0.0.0 and the range of valid addresses is 1.0.0.0 - 127.255.255.255, with the exception of the range 127.0.0.1 - 127.255.255.255, which is reserved and cannot be assigned.

The IP address 192.168.5.9 is a Class C address. The Class C default mask is 255.255.255.0 and the range of valid addresses is 192.0.0.0 - 223.255.255.255.

The IP address 127.0.0.1 is a Class A address, but it comes from a reserved portion that cannot be assigned. The range 127.0.0.1 - 127.255.255.255 is used for diagnostics, and although any address in the range will work as a diagnostic address, 127.0.0.1 is known as the loopback address. If you can ping this address, or any address in the 127.0.0.1 - 127.255.255.255 range, then the NIC is working and TCP/IP is installed. The Class A default mask is 255.0.0.0 and the range of valid addresses is 1.0.0.0 - 127.255.255.255, with the exception of the range 127.0.0.1 - 127.255.255.255, which is reserved and cannot be assigned.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.

QUESTION 134

From which of the following attacks can Message Authentication Code (MAC) shield your network?

- A. DoS
- B. DDoS
- C. spoofing
- D. SYN floods

Correct Answer: C

Section: Network Device Security

Explanation

Explanation/Reference:

Explanation:

Message Authentication Code (MAC) can shield your network from spoofing attacks. Spoofing, also known as masquerading, is a popular trick in which an attacker intercepts a network packet, replaces the source address of the packets header with the address of the authorized host, and reinserts fake information which is sent to the receiver. This type of attack involves modifying packet contents. MAC can prevent this type of attack and ensure data integrity by ensuring that no data has changed. MAC also protects against frequency analysis, sequence manipulation, and ciphertext-only attacks.

MAC is a secure message digest that requires a secret key shared by the sender and receiver, making it impossible for sniffers to change both the data and the MAC as the receiver can detect the changes.

A denial-of-service (DoS) attack floods the target system with unwanted requests, causing the loss of service to users. One form of this attack generates

a flood of packets requesting a TCP connection with the target, tying up all resources and making the target unable to service other requests. MAC does not prevent DoS attacks. Stateful packet filtering is the most common defense against a DoS attack.

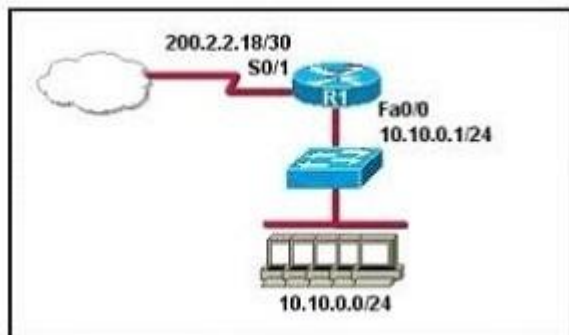
A Distributed Denial of Service attack (DDoS) occurs when multiple systems are used to flood the network and tax the resources of the target system. Various intrusion detection systems, utilizing stateful packet filtering, can protect against DDoS attacks.

In a SYN flood attack, the attacker floods the target with spoofed IP packets and causes it to either freeze or crash. A SYN flood attack is a type of denial of service attack that exploits the buffers of a device that accept incoming connections and therefore cannot be prevented by MAC. Common defenses against a SYN flood attack include filtering, reducing the SYN-RECEIVED timer, and implementing SYN cache or SYN cookies.

QUESTION 135

Refer to the exhibit.

A company wants to use NAT in the network shown. Which commands will apply the NAT configuration to the proper interfaces? (Choose two.)



- A. R1(config)# interface serial0/1
R1(config-if)# ip nat inside
- B. R1(config)# interface serial0/1
R1(config-if)# ip nat outside
- C. R1(config)# interface fastethernet0/0
R1(config-if)# ip nat inside
- D. R1(config)# interface fastethernet0/0
R1(config-if)# ip nat outside
- E. R1(config)# interface serial0/1
R1(config-if)# ip nat outside source pool 200.2.2.18 255.255.255.252
- F. R1(config)# interface fastethernet0/0
R1(config-if)# ip nat inside source 10.10.0.0 255.255.255.0

Correct Answer: BC
Section: IP Routing Technologies
Explanation

Explanation/Reference:

QUESTION 136

How many addresses will be available for dynamic NAT translation when a router is configured with the following commands?

```
Router(config)#ip nat pool TAME 209.165.201.23 209.165.201.30 netmask 255.255.255.224
Router(config)#ip nat inside source list 9 pool TAME
```

- A. 7
- B. 8
- C. 9
- D. 10
- E. 24
- F. 32

Correct Answer: B
Section: IP addressing (IPv4 / IPv6)
Explanation

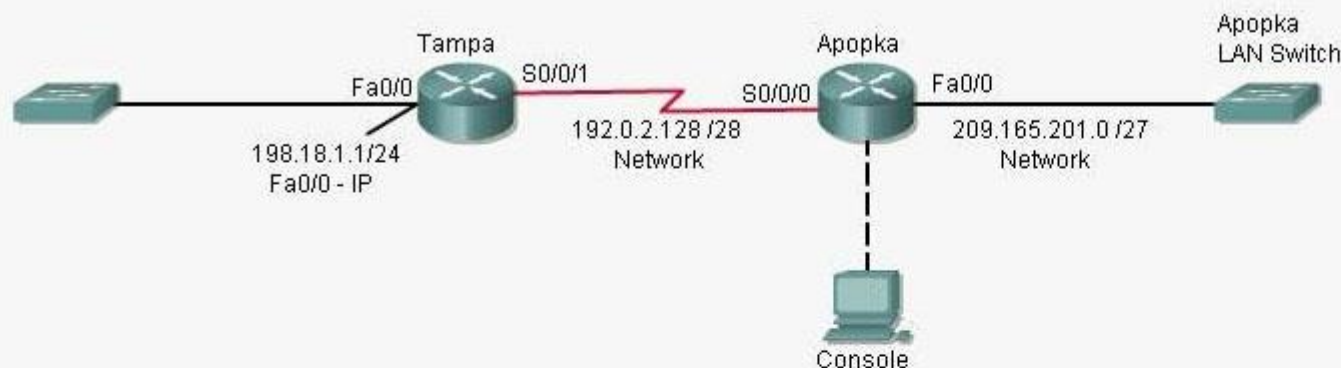
Explanation/Reference:
Explanation:

209.165.201.23 to 209.165.201.30 provides for 8 addresses.

QUESTION 137

Read the scenario and sort the the appropriate commands in order to configure the router.
On the real simulation during the exam you will be required to type the actual commands in order to configure the router.

Topology



Instructions

To configure the router (**Apopka**) click on the console host icon that is connected to a router by a serial console cable (shown in the diagram as a dashed black line).

You can click on the buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation. The **help** command does not display all commands of the help system.



Scenario

Central Florida Widgets recently installed a new router in their Apopka office. Complete the network installation by performing the initial router configurations and configuring RIPv2 routing using the router command line interface (CLI) on the Apopka router.

Configure the router per the following requirements:

Name of the router is **Apopka**

Enable-secret password is **ish555ana**

The password to access user EXEC mode using the console is **New2Rtr**

The password to allow telnet access to the router is **sir890us**

IPv4 addresses must be configured as follows:

Ethernet network **209.165.201.0 /27** - router has **second** assignable host address in subnet.

Serial network is **192.0.2.128 /28** - router has **last** assignable host address in the subnet.

Interfaces should be enabled.

Routing protocol is **RIPv2**.

Build List and Reorder:

Ordered List Title	Answer Choices Title
<div><div>▲</div><div>▼</div></div>	<div>Enable-secret password (cisco10): Apopka(config)#enable secret cisco10</div> <div>Apopka(config)#interface Fa0/0 Apopka(config-if)#ip address 209.165.201.2 255.255.255.224 Apopka(config-if)#no shutdown Apopka(config-if)#exit</div> <div>Apopka(config)#line console 0 Apopka(config-line)#password RouterPass Apopka(config-line)#login Apopka(config-line)#exit</div> <div>Apopka(config)#router rip Apopka(config-router)#version 2 Apopka(config-router)#network 209.165.201.0 Apopka(config-router)#network 192.0.2.128 Apopka(config-router)#end</div> <div>Apopka(config)#interface S0/0/0 (or use interface S0/0 if not successful) Apopka(config-if)#ip address 192.0.2.142 255.255.255.240 Apopka(config-if)#no shutdown Apopka(config-if)#exit</div> <div>Apopka(config)#line vty 0 4 Apopka(config-line)#password scan90 Apopka(config-line)#login Apopka(config-line)#exit</div> <div>Apopka#copy running-config startup-config</div> <div>Router>enable Router#config terminal Router(config)#hostname Apopka</div>

<< Move

Remove >>

Correct Answer:

```
Router>enable
Router#config terminal
Router(config)#hostname Apopka
Apopka(config)#enable secret cisco10
Apopka(config)#line console 0
Apopka(config-line)#password RouterPass
Apopka(config-line)#login
Apopka(config-line)#exit
Apopka(config)#line vty 0 4
Apopka(config-line)#password scan90
Apopka(config-line)#login
Apopka(config-line)#exit
Apopka(config)#interface Fa0/0
Apopka(config-if)#ip address 209.165.201.2
255.255.255.224
Apopka(config-if)#no shutdown
Apopka(config-if)#exit
Apopka(config)#interface S0/0/0 (or use
interface S0/0 if not successful)
Apopka(config-if)#ip address 192.0.2.142
255.255.255.240
Apopka(config-if)#no shutdown
Apopka(config-if)#exit
Apopka(config)#router rip
Apopka(config-router)#version 2
Apopka(config-router)#network 209.165.201.0
Apopka(config-router)#network 192.0.2.128
Apopka(config-router)#end
Apopka#copy running-config startup-config
```

Section: IP Routing Technologies
Explanation

Explanation/Reference: