Part 5

QUESTION 401
On a newly installed router, the following access list is added to the HSSI interface for incoming traffic:
Access-list 101 permit tcp any 10.18.10.0 0.0.0.255 eq tcp
What is the effect of the "any" keyword in the above access list?

A. check any of the bits in the source address
B. permit any wildcard mask for the address
C. accept any source address
D. check any bit in the destination address
E. permit 255.255.255.255 0.0.0.0
F. accept any destination

Answer: C

Explanation:
The "any" in this list is the source address to filter. If it is set to any or "0.0.0.0 255.255.255.255", then any source address will be filtered. In the example above, the access list is stating that any TCP traffic from any source going to the 10.18.10.0/24 network will be allowed.

QUESTION 402
Which one of the following commands will display the placement and direction of an IP access control list on the interfaces of a router?

A. show interface list
B. show ip route
C. show ip interface
D. show ip interface brief
E. show interface

Answer: C

Explanation:
The command "show ip interface" will include a reference to the access lists enabled on the interface.

QUESTION 403
The relevant portion of the Barrymore router configuration is displayed below:
Barrymore#show running-config
<some output text omitted>
enable password cisco
!
username Central password 0 cisco

```
!
interface BRI0/0
ip address 192.168.0.1 255.255.255.0
encapsulation ppp
dialer idle-timeout 180
dialer map ip 192.168.0.2 name Remote 5552000
dialer-group 1
isdn switch-type basic-ni
no fair-queue
ppp authentication chap
!
ip route 192.168.20.0 255.255.255.0 192.168.0.2
!
router rip
network 192.168.0.0
!
access-list 129 deny tcp 192.168.0.0 0.0.0 255 host
192.168.20.5 eq www
access-list 128 permit ip any any
dialer-list 1 protocol ip list 128
```

In your effort to conserve precious bandwidth, you set up some ACL's to deny internet access to the remote server located at 192.168.20.5. A few minutes after reconfiguring (as shown in the exhibit above) you notice that some web traffic is still going through.
Based on the above output, what do you suspect as to why the traffic still traveling over the ISDN link?

A. Broadcasts are creating "interesting" traffic.
B. The access-list is not configured correctly.
C. The command ip access-group 129 out is missing from the bri0/0 interface.
D. The dialer-group has not been applied to outbound traffic.

Answer: C

Explanation:
In this case the access list is correctly created using access list number 129. The problem is that ACL 129 has not been applied anywhere. We wish to apply this access list to the BRI 0/0 interface, in the outbound direction.
Incorrect Answers:
A, D. In this example, the question does not relate to the ISDN call establishment. It is assumed that the link works correctly and that the interesting traffic is configured correctly. This is simply an access list issue, not an ISDN issue.
B. The access list is indeed configured correctly; it just needs to be applied to the interface.

QUESTION 404
You are a technician at Certkiller . Your assistant applied an IP access control list to Router CK1 . You want to check the placement and direction of the access control list.
Which command should you use?

A. show access-list
B. show ip access-list
C. show ip interface
D. show interface
E. show interface list

Answer: A

Explanation:
To display the contents of current access lists, use the show access-lists command in privileged EXEC mode.

QUESTION 405
Exhibit


```
Certkiller1 (config)# ip nat pool c-pool 66.179.148.33 66.179.148.34
    netmask 255.255.255.248
Certkiller1 (config)# access-list 1 permit 192.168.9.0 0.0.0.248
Certkiller1 (config)# ip nat inside source list 1 pool c-pool overload
Certkiller1 (config)# interface fastethernet 0/0
Certkiller1 (config-if)# ip nat inside
Certkiller1 (config)# interface serial 0/0
Certkiller1 (config-if)# ip nat outside
```

Refer to the exhibit and sequence of configuration commands shown in the graphic. The network at Certkiller 1 has just been configured for NAT as shown. Initial tests indicate that the network is functioning properly.
However, several users report that they cannot access the Internet. What is the problem?

A. The NAT pool does not have enough IP addresses.
B. The access list is not permitting all of the LAN host addresses to be translated.
C. The NAT inside and NAT outside interfaces are reversed.
D. The link between the Certkiller routers and the Certkiller 2 ISP

Answer: B

QUESTION 406
After attempting to telnet into a router, you are denied and you receive the error

message "password required, but none set." What configuration changes will allow telnet access into this router?

A. router(config)# line con 0
router(config-line)# password welcome
router(config-line)# login
B. router(config)# line aux 0 4
router(config-line)# password welcome
router(config-line)# login
C. router(config)# line vty 0 4
router(config-line)# password welcome
router(config-line)# login
D. router(config)# line tty 0 4
router(config-line)# password welcome
router(config-line)# enable login

Answer: C

Explanation:
Several concurrent Telnet connections to a router are allowed. The line vty 0 4 command signifies that this configuration applies to vtys (virtual teletypes/terminals) 0 through 4.
Reference:
CCNA Self-Study CCNA INTRO exam certification Guide (Cisco Press, ISBN 1-58720-094-5) page 178.
Incorrect Answers:

A. This will prompt users connecting via a console cable for a password, and then allow access.
B. This will configure access via the aux port.
D. Routers do not have TTY access.

QUESTION 407
While attempting to gain access into a router remotely, you issue the telnet command as shown below:

Based on the information above, which set of commands will correct this problem?

A. ACCESS1(config)# line console 0
ACCESS1(config-line)# password cisco
B. Remote27(config)# line console 0
Remote27(config-line)# login

Remote27(config-line)# password cisco
C. Remote27(config)# line vty 0 4
Remote27(config-line)# login
Remote27(config-line)# password cisco
D. ACCESS1(config)# line vty 0 4
ACCESS1(config-line)# login
ACCESS2(config-line)# password cisco
E. ACCESS1(config)# enable password cisco
F. Remote27(config)# enable password cisco

Answer: D

Explanation:
The vty lines on the remote router (the one you are trying to telnet into) needs to be configured to allow access.
Incorrect Answers:
A, B. The connection you need to establish isn't a console session but a virtual terminal session, so answer choices A and B are incorrect.
C. This is the corrct syntax, but it is being placed on the wrong router. The access needs to be applied to the remote router, not the local one.
E, F. Answer choices E and F are incorrect because they refer to the enable password, which is different then the virtual terminal line passwords.

QUESTION 408
While troubleshooting a serial line problem, you enable ppp authentication debugging as shown below:
#debug ppp authentication
ppp serial1: Send CHAP challenge id=34 to remote
ppp serial1: CHAP challenge from P1R2
ppp serial1: CHAP response received from P1R2
ppp serial1: CHAP response id=34 received from P1R2
ppp serial1: Send CHAP success id=34 to remote
ppp serial1: Remote passed CHAP authentication
ppp serial1: Passed CHAP authentication
ppp serial1: Passed CHAP authentication with remote
Based on the command output above, what type of 'handshake' was used for PPP authentication?

A. one-way
B. two-way
C. three-way
D. four-way
E. no handshakes required during authentication
F. None of the above

Answer: C

Explanation:
As shown in the above output, CHAP is the mechanism that is being utilized here. CHAP uses a three-way handshake. After the PPP link is established, the host sends a "challenge" message to the remote node. The remote node responds with a value calculated using a one-way hash function. The host checks the response against its own calculation of the expected hash value. If the hash value match, the authentication is acknowledged; otherwise, the connection is terminated.

QUESTION 409
The Certkiller Central and Remote offices are configured as shown below:

Central# show running-config	Remote# show running-config
<some output text omitted>	<some output text omitted>
interface Serial0/0	interface Serial0/0
ip address 10.0.8.1 255.255.248.0	ip address 10.0.15.2 255.255.248.0
encapsulation frame-relay	encapsulation frame-relay
frame-relay map ip 10.0.15.2 200	frame-relay map ip 10.0.8.1 100
!	!
router rip	router rip
network 10.0.0.0	network 10.0.0.0

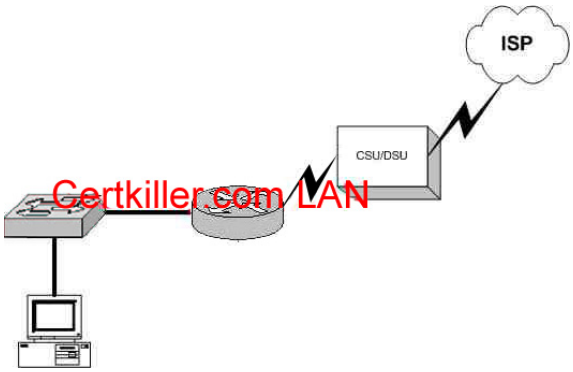
The remote router can be successfully pinged from the central office but the remote users can't access the server at the central office.
Based on the output above, what do you suspect is the cause of this problem?

A. The Frame Relay PVC is down.
B. The IP addressing on the Central/Remote serial link is incorrect.
C. RIP routing information is not being forwarded.
D. Frame Relay inverse-ARP is not properly configured.

Answer: C

Explanation: By looking to he output we can see that there are routes and routing protocol is RIP. The remote server can be pinged, we know now that there is a physical connection (for that answer A + B can be eliminated.
You don't need the ' Inverse-ARP for taking access - not in this connection! and for that the only possible answer will be the C

QUESTION 410
The Certkiller network is displayed below:



You are brand new to the company, and you are in the process of discovering the Certkiller network's topology. You have been given a Visio of the network diagram above. Based on this information, what conclusion can you make about the type of Certkiller Internet connection? (Select all that apply)

A. They are using DSL
B. They are using frame relay
C. ISDN is being used
D. A dedicated T1 circuit is being used
E. They are using a wireless ISP
F. They are using a POTS dial up connection

Answer: B, D
The correct answer should be "Frame Relay" & "Dedicated T1". Both WAN technologies use CSU/DSU. These are the only two choices that could be correct based on the fact that a CSU/DSU is being used.
Incorrect Answers:

A. DSL uses a modem instead of a CSU/DSU
C. ISDN uses a terminal adapter/NT
E, F. CSU/DSU's are not used in wireless and dial up connections.

QUESTION 411
You are trying to bring up a new Certkiller location onto your existing frame relay network. The new location is using an Adtran router and you are having difficulties getting the site to connect via frame to your Cisco HQ router. What is the most likely cause of the problem?

A. Mismatched LMI types.
B. Incompatible encapsulation types.
C. Mismatching IP addresses.
D. Incorrect DLCI.
E. None of the above

Answer: A

Explanation:

Three LMI protocol options are available in Cisco IOS software: Cisco, ITU, and ANSI. Each LMI option is slightly different and therefore is incompatible with the other two. As long as both the DTE and DCE on each end of an access link use the same LMI standard, LMI works fine. The default LMI type in a Cisco router is Cisco. Since this is proprietary, this LMI type is incompatible with the LMI type used by other vendors.
Reference: CCNA Self-Study CCNA ICND exam certification Guide (Cisco Press, ISBN 1-58720-083-X) Page 381.

QUESTION 412
The Certkiller 1 and Certkiller 2 routers are connected together as shown below:

Users on the Certkiller 1 LAN are able to successfully access the resources on the Certkiller 2 network. However, users on Certkiller 1 are unable to telnet to the Certkiller 2 router. What do you suspect are the likely causes of this problem? (Select two answer choices)

A. PPP authentication configuration problem.
B. A misconfigured IP address or subnet mask
C. An access control list
D. A defective serial cable.
E. No clock rate on interface s0 on Certkiller 2
F. A missing vty password.

Answer: C, F

Explanation:
An ACL or a router configured without a VTY password will prevent users from being able to telnet into a router.
Incorrect Answers:
A, B, D, E. We know that the network is connected together and communicating back and forth because of the two way CHAP authentication happening. In addition, the LAN users are able to get to each other with no problems. Therefore A is incorrect, B is incorrect, D is incorrect, and E is incorrect.

QUESTION 413
You are an administrator of a network that uses PPP for CHAP authentication over ever WAN link. What command would you enter to display the CHAP authentication as it occurs in real time?

A. show ppp authentication
B. debug PAP authentication
C. debug PPP authentication

D. show interface serial0
E. show CHAP authentication

Answer: C

Explanation:
Whenever you're asked to display a process in real time, you must use a debug command as show commands do not display anything in real time. Debug PPP authentication will display the authentication process of a PPP line, including the CHAP process.
Incorrect Answers:
A, D, E. This will not display the output in real time.
B. We wish to see information relating to CHAP, not PAP.
Reference: CCNA Self-Study CCNA ICND exam certification Guide (Cisco Press, ISBN 1-58720-083-X) Page 314.

QUESTION 414
You are troubleshooting a WAN connection for Certkiller , and on the router you execute the, "debug ppp authentication" command, and view the following output:
#debug ppp authentication
PPP Serial1: Send CHAP challenge id=34 t remote
PPP Serial1: CHAP challenge from P1R2
PPP Serial1: CHAP response received form P1R2
PPP Serial1: CHAP response id=34 received from P1R2
PPP Serial1: Send CHAP success id=34 to remote
PPP Serial1: Remote passed CHAP authentication
PPP Serial1: Passed CHAP authentication
PPP Serial1: Passed CHAP authentication with remote
What kind of handshake was used for the PPP authentication?

A. one-way
B. two-way
C. three-way
D. No handshakes required during authentication
E. None of the above

Answer: C

Explanation:
CHAP uses a one-way hash algorithm, with input to the algorithm being a password and a shared random number. The CHAP challenge states the random number; both routers are preconfigured with the password. The challenged router runs the hash algorithm using the just-learned random number and the secret password and sends the results back to the router that sent the challenge. The router that sent the challenge runs the same algorithm using the random number (sent across the link) and the password (not sent across the link). If the results match, the passwords must match.

QUESTION 415
Study the output script and the network topology exhibit below:
Certkiller 1# show running-config
<some output text omitted>
interface serial0/0
bandwidth 64
ip address 172.16.100.2 255.255.0.0
encapsulation frame-relay
frame-relay map ip 172.16.100.1 200 broadcast

The Router Certkiller 1 in Hong Kong is connected to the router Certkiller 2 in Tokyo via a new Frame Relay link. However, Certkiller 1 is unable to communicate with Certkiller 2. Based on the above output, what do you suspect as the underlying cause of this problem?

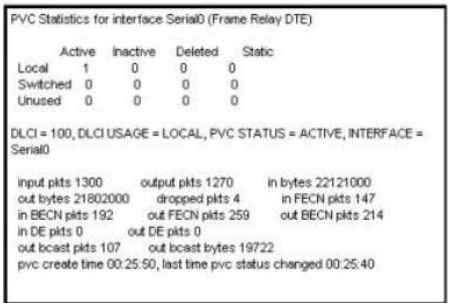
A. Bandwidth configuration incorrect
B. IP address not correct
C. Improper map statement
D. Improper LMI configuration

Answer: C

Explanation: From looking at the diagram you can see that Hong Kong's DLCI is 100, while Tokyo's DLCI is 200.
The Frame Relay map command is an interface configuration mode command that statically defines a mapping between a network layer address and a DLCI.
Incorrect Answers:

A. The bandwidth statement is not used by the routers at a physical or data link layer, so this statement will not have any impact on the function of the frame relay circuit.
B. We do not know what the IP address of the Tokyo side is, so this can not be assumed.
D. The default LMI type is Cisco, and since both routers in this network appear to be Cisco's, we can assume that this is acceptable.

QUESTION 416
While troubleshooting an issue with your frame relay network, you issue the "show frame pvc" command as shown in the exhibit below:


PVC Statistics for interface Serial0 (Frame Relay DTE)

	Active	Inactive	Deleted	Static
Local	1	0	0	0
Switched	0	0	0	0
Unused	0	0	0	0

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

input pkts 1300 output pkts 1270 in bytes 22121000
out bytes 21802000 dropped pkts 4 in FECN pkts 147
in BECN pkts 192 out FECN pkts 259 out BECN pkts 214
in DE pkts 0 out DE pkts 0
out bcast pkts 107 out bcast bytes 19722
pvc create time 00:25:50, last time pvc status changed 00:25:40

You're a network administrator at a Certkiller branch office, that's connected to the central headquarters by means of Frame Relay. You've been getting complaints that the connection has suddenly become slow, so you make the assumption that there's too much traffic going through the link.
Taking into consideration the above output from the 'show frame relay pvc' command; which command output value is indicating that there's congestion between the local router and the corporate site?

A. in DE packets 0
B. last time PVC status changed 00:25:40
C. in BECN packets 192
D. DLCI = 100
E. in FECN packets 147

Answer: C

Explanation:
BECN stands for Backward Explicit Congestion Notification. The BECN tells the transmitting device that the Frame Relay network is congested and that it should "back off" to allow better throughput. BECN and FECN go hand to hand together, but since the question specifically asks for what's indicating congestion between the local router and corporate site, BECN is correct.

QUESTION 417
In order to troubleshoot an issue with the Certkiller frame relay network, you log into a remote router via a telnet session and issue the command "debug frame-relay lmi". After a long wait, you fail to see any output. What could be the cause of this problem?

A. The IP addresses are configured incorrectly.
B. Frame Relay LMI messages not displayed in real time.
C. The administrator must issue the enable frame-relay lmi debug command.
D. The administrator must issue the terminal monitor command.
E. Debug messages can only be received once through the console port.
F. The administrator must issue the show frame-relay lmi vty 0 4 command-

Answer: D

Explanation:
In order to see any debugging output from a remote telnet session, the "terminal monitor" command will need to be issued. By default, the network server sends the output from the debug commands to the console terminal. Sending output to a terminal (virtual console) produces less overhead than sending it to the console. Use the privileged EXEC command terminal monitor to send output to a terminal.
Reference:http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/dbook/daple.htm

---

QUESTION 418
The configuration of the remote Certkiller 3 router is displayed below:

```
hostname Certkiller 3
!
enable password gatekeeper
!
isdn switch-type basic-5ess
!
!
username Central password Certkiller
interface BRI0
ip address 192.168.0.1 255.255.255.0
encapsulation ppp
dialer idle-timeout 180
dialer map ip 192.168.0.2 name Remote 6662000
dialer-group 1
no fair-queue
ppp authentication chap
!
router rip
network 192.168.0.2
!
no ip classless
ip route 192.168.10.0 255.255.0.0 192.168.0.2
ip route 192.168.20.0 255.255.0.0 192.168.0.2
!
dialer-list 1 protocol ip permit
```

The Certkiller 3 router is unable to call the remote site. What is the underlying cause of this problem?

A. The authentication password is missing from the dialer map command.
B. The switch-type must be configured.
C. Routing updates are being blocked by the applied dialer-list.
D. The dialer list only permits one protocol.
E. The name in the dialer-map must match the name in the username command.
F. None of the above

Answer: E

Explanation:
The username in the above exhibit is "Central", while the dialer-map name is "Remote". Since the names don't match the call can't be completed.

QUESTION 419
You are attempting to troubleshoot a frame relay problem you are having within the Certkiller network, but you are unsure where to start. You begin by entering the command:
'Router# show frame-relay
Which three options will you be prompted for? (Select three answers choices)

A. dlci
B. clients
C. pvc
D. neighbors
E. lmi
F. map

Answer: C, E, F

Explanation:
The valid options for, 'show frame-relay' are: show frame-relay map, show frame-relay lmi, & show frame-relay pvc. In the Cisco IOS, if you don't type in a command specific enough, it will prompt you to select an option.
Incorrect Answers:
A, B, D. Show frame-relay dlci, show frame-relay clients, and show frame-relay neighbors are all invalid commands.

QUESTION 420
The relevant portion of two different Certkiller routers are displayed below:

```
<some output text omitted>

interface serial0/0
 ip address 10.0.1.1 255.255.255.0
 encapsulation frame-relay
!
router igrp 1
network 10.0.0.0
```

```
<some output text omitted>

interface fastethernet0/0
 ip address 10.10.1.2 255.255.255.0
!
interface serial10/0
 ip address 10.0.1.2 255.255.255.0
 encapsulation frame-relay
!
router igrp 2
network 10.0.0.0
```


Users on these two routers are experiencing connectivity problems and are unable to reach each other. After reviewing the command output, what is the most likely cause of the problem?

A. Incorrect IP addressing.
B. Frame relay is incorrectly configured.
C. IGRP is incorrectly configured.

D. Link state routing protocol is needed.
E. None of the above.

Answer: C

Explanation:
With IGRP, the process number, or autonomous system number, must match. In this case the router on the left is configured with IGRP 1, while the router on the left is configured with IGRP 2. This is resulting in the routers not exchanging IGRP routing information with each other.
Incorrect Answers:

A. The IP addressing used here will work. Although IGRP does not support VLSM, all networks are configured using a /24 subnet mask.
B. Since both routers are obviously Cisco (IGRP is Cisco proprietary) the frame relay configuration is not the problem. Had one of the routers been non-Cisco, then the keyword "ietf" should be placed at the end of the frame-relay encapsulation command.
D. Link state routing is not required in this network.

QUESTION 421
You have just installed a new web server on the Certkiller network. You are required to ensure that the web server is accessible from the Internet. The network uses private addressing, so an IP-to-registered address mapping is required.
To do this, you enter the following command:
Certkiller (config)# ip nat inside source static 192.168.2.1 198.18.1.254
You unsuccessfully try to ping the Internet from a PC host on the LAN. During the troubleshooting process, you enter the "show ip nat translations" command but the output is blank.
What is the most likely cause of the problem?

A. The keyword overload is missing from the command.
B. The NAT pool must be defined first.
C. An access list must be defined to create static NAT translations.
D. The interfaces must be configured for NAT.
E. None of the above

Answer: D

Explanation:
In order to successfully configure a static NAT translation, the interfaces must be configured for NAT, in addition to the global NAT command that was entered. The router interface that lies on the inside part of the network must be defined using the "ip nat inside" command. Similarly, the WAN interface that is being used for the Internet connection must be defined using the "ip nat outside" command.
Incorrect Answers:

A. In order to make an internal server reachable from the Internet, a static one to one NAT entry must be configured for the server. The keyword "overload" is used to configure many to one NAT, or PAT.
B, C. This need not be done in order to create a static NAT entry. These steps are typically done in setting up NAT so that inside LAN users can access the Internet via NAT.

QUESTION 422
Certkiller .com is configuring the serial interface of a Cisco router to connect to the router of a new ISP. A full T1 is being used for the Internet connection. After issuing the show interface serial 0/0 command, it is observed that the interface is UP and the line protocol is DOWN.
Which of the following commands could fix this problem?

A. Border# copy running-config startup-config
B. Border(config)# no shutdown
C. Border(config-if)# encapsulation ppp
D. Border(config-if)# no cdp enable
E. Border(config-if)# ip routing

Answer: C

Explanation:
By default, a serial interface on a Cisco router is set for HDLC encapsulation. Many ISP's use PPP encapsulation for the layer 2 protocol since the connection is a point to point type and PPP is an industry standard, while HDLC is Cisco proprietary. Changing the default encapsulation type to PPP could fix this problem.
Incorrect Answers:

A. This will save the current configuration into NVRAM, but will have no affect with the current state of the serial interface.
B. If the interface was manually shut down the status would be "administratively down, line protocol down."
D. CDP is enabled by default on all interfaces, but whether or not CDP is running would not have any impact on the functionality of the serial interface.
E. IP routing is enabled by default. Additionally, IP routing does not need to be running on the router in order for the serial interface to work.

QUESTION 423
Network topology Exhibit

You work as a network engineer at Certkiller .com. The topology of the Certkiller .com network is displayed in the exhibit. Router Certkiller A is unable to

reach router Certkiller B. Both routes are running IOS version 12.0. After reviewing the command output and the network topology exhibit, what is the most likely cause of the problem?

A. Incorrect bandwidth configuration
B. Incorrect LMI configuration
C. Incorrect map statement
D. Incorrect IP address

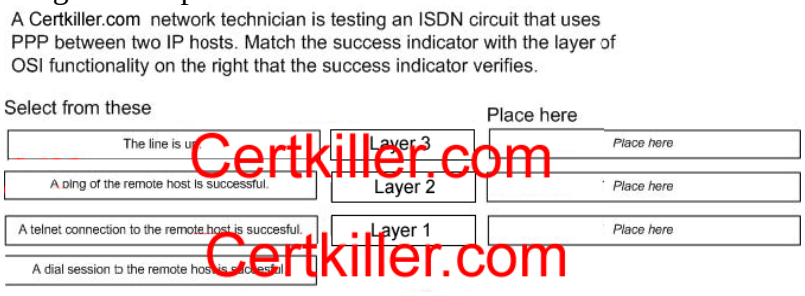
Answer: C
Study the exhibit. The routers have been configured with wrong DLCI.

QUESTION 424
Which command can be used to determine the type of cable attached to the Serail 0/0 interface on a router?

A. show interfaces serial 0/0
B. show running-config
C. show version
D. show controllers serial 0/0
E. show ip interface
F. show line serial 0/0

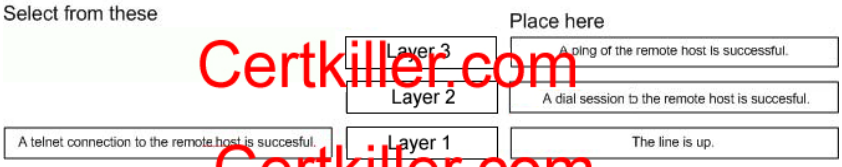
Answer: D
The show controllers command shows that the physical layer is working and what type of cable is connected. In the output below, Prasit is connected at the DCE end and Spicey at the DTE end.
prasit#
show controllers serial 0
HD unit 1, idb = 0xF22E4, driver structure at 0xF7778
buffer size 1524 HD unit 0 1, V.35 DCE cable, clockrate 64000
!--- Output suppressed.

QUESTION 425
Drag and Drop



Answer:

A Certkiller.com network technician is testing an ISDN circuit that uses PPP between two IP hosts. Match the success indicator with the layer of OSI functionality on the right that the success indicator verifies.



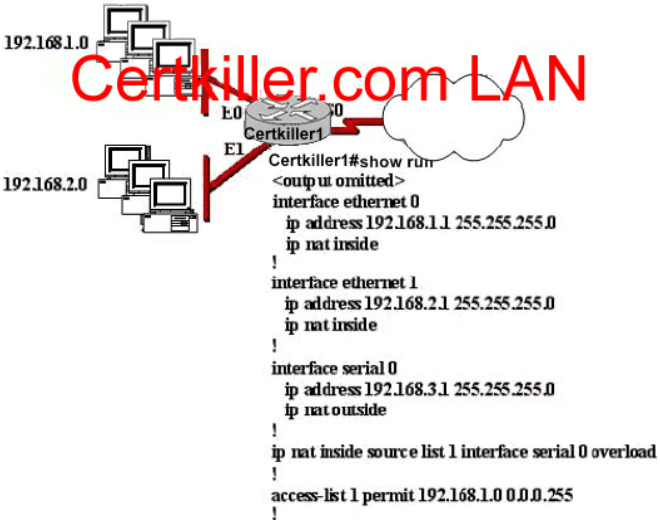
QUESTION 426

Based only on the topology and the output from the router shown in the graphic, what is the most likely reason Host A cannot ping Host B?

A. A bad or disconnected cable.
B. An improperly configured SPID.
C. A missing route on CK1 and CK2 .
D. Improperly configured ISDN switch type.
E. An improperly configured IP address.

Answer: B
Answer A is incorrect
B is the right answer even given this status "TEI = 73, Ces = 2, SAPI = 0, State = TEI_ASSIGNED
TEI = 104, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED"
The above status indicate that the circuit is partially up
The real problem was a misconfigured SPID1 indicated by the word " spid1 NOT valid" even SPID2 was correct. So there was a configuration issue here.

QUESTION 427
Exhibit



The network administrator has configured NAT as shown in the exhibit. Some clients can access the Internet while others cannot.
What should the network administrator do to resolve this problem?

A. Configure an IP NAT pool.
B. Properly configure the ACL.
C. Apply the ACL to the S0 interface.
D. Configure another interface with the ip nat outside command.
E. Configure the ip nat inside and ip nat outside commands

Answer: B
E is incorrect. The IP NAT INSIDE & IP NAT OUTSIDE are present on each of the 3 interfaces.
"Some clients can access the Internet while others cannot." his is a huge hint that either ; ACL is blocking some people or you are not using overload when you should or that you are using 2 inside subnets like in this example & 1 of those does not have the IP NAT INSIDE statement against it.
Answer B would be the best

QUESTION 428
In the "host to host" layer of the DOD model, which of the following is a valid connection oriented protocol?

A. ARP
B. RARP
C. TCP
D. UDP
E. IP
F. ICMP
G. BootP

Answer: C

Explanation:
Transport Protocol is a connection oriented protocol that resides at the Host to Host layer of the DOD stack and handles connection oriented communication. In the Department of Defense layer, the host to host layer translates to layer 4 of the OSI model.

QUESTION 429
Which of the following protocols operate at the 'Application layer' of the OSI model? (Select all valid answers)

A. TCP
B. Telnet
C. FTP
D. ARP
E. IP
F. None of the above

Answer: B, C

Explanation:
The application layer is the top layer of the OSI model and is used to describe the end user applications that can be used over a network.

Layer Name	**Examples**
Application (layer 7)	Telnet, HTTP, FTP, WWW browsers, NFS, SMTP gateways, SNMP

Reference: CCNA Self-Study CCNA INTRO exam certification Guide (Cisco Press, ISBN 1-58720-094-5) Page 34.
Incorrect Answers:

A. TCP resides at layer 4.
D. ARP is a function of the data link layer, which is layer 2.
E. IP is used at layer 3 (network layer).

QUESTION 430
Which OSI layer is associated with the following: The acknowledgement of transmissions, sequencing, and flow control across a network?

A. Layer 2
B. Layer 3
C. Layer 4
D. Layer 5
E. Layer 6
F. Layer 7

Answer: C
Explanation

The Transport layer (Layer 4) defines several functions, including the choice of protocols. The most important Layer 4 functions are error recovery and flow control. The transport layer may provide for retransmission, i.e., error recovery, and may use flow control to prevent unnecessary congestion by attempting to send data at a rate that the network can accommodate, or it might not, depending on the choice of protocols. Multiplexing of incoming data for different flows to applications on the same host is also performed. Reordering of the incoming data stream when packets arrive out of order is included. Examples include: TCP, UDP, and SPX.

QUESTION 431
Which of the protocols below, operates at Layer 2 of the OSI model, and is used to maintain a loop-free network?

A. RIP
B. STP
C. IGRP
D. CDP
E. VTP

Answer: B

Explanation:
STP (spanning tree protocol) operates on layer 2 to prevent loops in switches and bridges.
Incorrect Answers:
A, C. RIP and IGRP are routing protocols, which are used at layer 3 to maintain a loop free routed environment.
D. CDP does indeed operate at layer 2, but it doest not provide for a loop free topology. CDP is used by Cisco devices to discover information about their neighbors.
E. VTP is the VLAN Trunking Protocol, used to pass VLAN information through switches. It relies on the STP mechanism to provide a loop free network.

QUESTION 432
In the communications industry, what are the features and benefits of using the layered OSI model? (Select the two best answers)

A. It encourages industry standardization by defining what functions occur at each layer of the model.
B. It necessitates changes in functionality in one layer to other layers.
C. It enables equipment efficiency from different vendors to use the same electronic components.
D. It divides the network communication process into smaller and simpler components, thus aiding component development, design, and troubleshooting.
E. It supports the evolution of multiple competing standards, and thus enhances business equipment manufacturing opportunities.

Answer: A, D

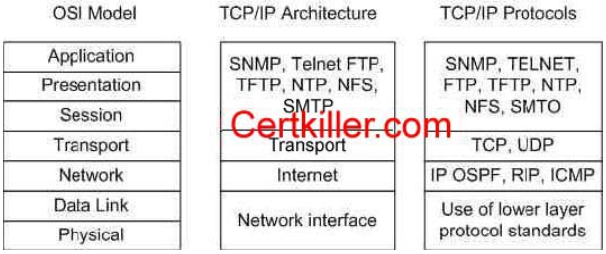
Explanation:
The OSI (Open System Interconnection) reference model was created as a reference point for communications devices. A layered approach is used to segment the entire telecommunications process into a series of smaller steps.
A is correct because it encourages a level of standardization by encouraging that functions be compared to known layers. D is also correct because it allows engineers to focus on the development, refining, and perfection of simpler components.

QUESTION 433
The TCP/IP network model differs from the more popular OSI model. Which of the layers below belong to the TCP/IP model? (Select all that apply)

A. application layer
B. session layer
C. transport layer
D. internet layer
E. network layer
F. data link layer
G. physical layer

Answer: A, C, D

Explanation:



TCP/IP's architecture does not use the presentation and session layers. The application layer protocols use the transport layer services directly. The OSI transport layer provides connection-oriented service; in TCP/IP, this service is provided by TCP. TCP/IP also provides connectionless service in the transport layer with UDP.
The Internet layer of TCP/IP corresponds to the network layer of the OSI model. Although OSI network-layer protocols provide connection-oriented (Connection-Model Network Service (CMNS), X.25) or Connectionless Network Service (CLNS), IP provides only connectionless network service. The routing protocols are network layer protocols with an IP protocol number.
Reference: CCNA ICND Exam Certification Guide by Wendell Odem, Page 268.

QUESTION 434
At which layer of the OSI model is the optimal path to a network destination determined at?

A. Data Link

B. Session
C. Physical
D. Presentation
E. Network
F. Transport

Answer: E

Explanation:
The Network layer (Internet layer in the DOD model) provides logical addressing and routing through an internetwork. The network layer is layer 3 of the OSI model.

QUESTION 435
In the OSI model, at which layers do WANs operate at? (Select two answer choices)

A. Application layer
B. Presentation layer
C. Session layer
D. Transport layer
E. Network layer
F. Data link layer
G. Physical layer

Answer: F, G

Explanation:
WAN (Wide Area Network) operates at OSI Layer 1(Physical) and Layer 2 (Data link) layers. The WAN provides for the exchanging of data packets between Routers and the LAN's that the routers support

---

QUESTION 436
Which one of the following is the most commonly used layer 2 network device?

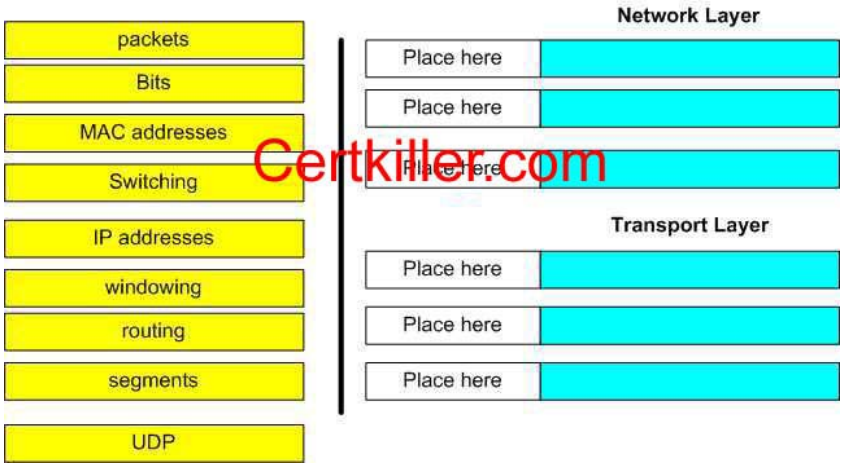
A. Hub
B. Bridge
C. Switch
D. Router
E. Repeaters
F. None of the above

Answer: C

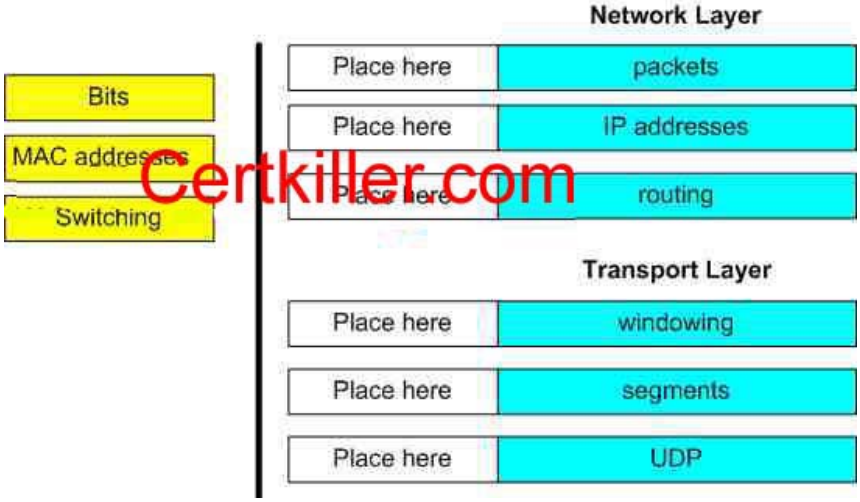
Explanation:
A switch segments the network and uses an ASIC for fast switching. Switches have become the more common of the layer two devices, as they offer more features and benefits than bridges.

Incorrect Answers:
A, E. Hubs and repeaters operate at layer one.
B. Bridges have become somewhat obsolete, as switches have become more and more prevalent.
D. Routers operate at layers 3 and 4.

QUESTION 437
Classify the terms on the left into their proper OSI layer categorizes on the right. Do this by dragging and dropping the correct terms on the left with the correct answers on the right hand side. Note that not all left side options will be used.



Correct Answer:



QUESTION 438
Which three of the following OSI model layers also belong to the TCP/IP model? (Select three answer choices)

A. The application layer
B. The session layer
C. The data link layer

D. The transport layer
E. The network interface layer
F. The physical layer

Answer: A, D, E

Explanation:
The Application, Transport, and the Network Interface Layers are all part of the TCP/IP layer model. (The application and transport layer are also layers of the OSI model as well.) However, the session layer, the data link layer, and the physical layer are all exclusively part of the OSI model.

QUESTION 439
Which three of the protocols below belong to the application layer? (Select three answer choices)

A. ARP
B. HTTPS
C. SMTP
D. CDP
E. TFTP
F. ICMP

Answer: B, C, E

Explanation:
The application layer is the highest OSI layer, and protocols at this layer are end-user oriented. HTTPS so people can get information on the internet, SMTP so people can manage networks, and TFTP so people can download files.
Incorrect Answers:
A, D, F. ARP, CDP, ICMP are protocols that equipment like routers and switches use to communicate with themselves, and belong to lower levels on the model.

QUESTION 440
Which of the following layers of the TCP/IP model most closely corresponds to the network layer of the OSI model?

A. Application
B. Internet
C. Transport
D. Network
E. Data Link

Answer: B

Explanation:

The DOD model consists of the Application/Process, Host to Host, Internet and Network Access layers. The only answer with a DoD model layer (also called the TCP/IP model), is the Internet layer.

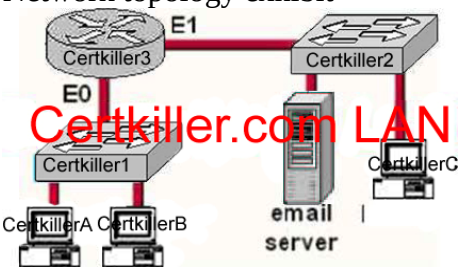
QUESTION 441
You have set up an Internet based FTP server, where people can upload and download files. In terms of the OSI model, what is the highest layer used during the FTP sessions.

A. Application
B. Presentation
C. Session
D. Transport
E. Internet
F. Data Link
G. Physical

Answer: A

Explanation:
The application layer is the highest layer (layer 7) of the OSI model, and is reserved for end user applications. Since FTP is itself an application, layer 7 is the highest layer used.
Incorrect Answers:
B, C, D, E, F, G. In any given FTP session, all of these layers will be used at some point but they are incorrect because the question asked for the highest layer used by FTP.

QUESTION 442
Network topology exhibit



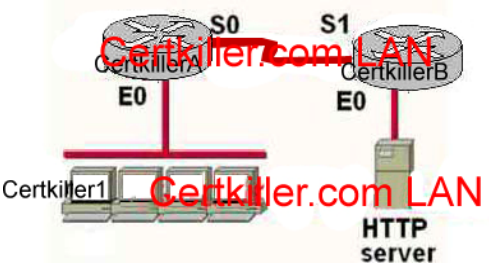
Host Certkiller A needs to communications with the e-mail server shown in the exhibt.
What address will be placed on the destination address field of the frame when it leaves host Certkiller A?

A. The MAC address of Certkiller A
B. The MAC address of switch Certkiller 1
C. The MAC address of the E0 interface of the Certkiller 3 router.
D. The MAC address of the E1 interface of the Certkiller 3 router.
E. The MAC address of switch Certkiller 2
F. The MAC address of the email server

Answer: C

Explanation:
If the destination host is in the remote segment than the router will change the MAC address of the source to its own. The inverse ARP protocol is by default on. Remember that IP address is not changed after forwarding. The MAC address is changed after crossing each broadcast domain.

QUESTION 443
Network topology Exhibit



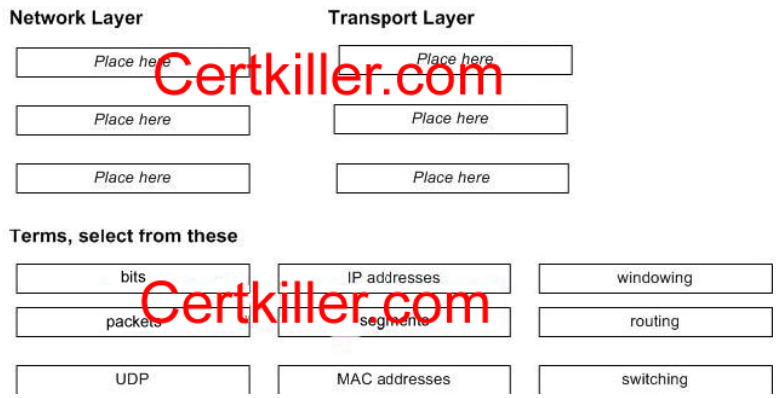
You work as a network engineer at Certkiller .com. The topology of the Certkiller .com network is displayed in the exhibit. Host Certkiller 1 has established a connection with the HTTP server attached to interface E0 of the Certkiller B router. Which of the following statements describe the information contained in protocol data units sent from host Certkiller 1 to this server? Select three

A. The destination port number in a segment header will have a value of 80.
B. The destination port number in a segment header will have a unique value greater than or equal to 1023.
C. The destination address of a frame will be the MAC address of the HTTP server interface.
D. The destination address of a frame will be the MAC address of the E0 interface of the Certkiller A router.
E. The destination IP address of a packet will be the IP address of the the E0 interface of the Certkiller A router.
F. The destination address of a packet will be the IP address of the HTTP-Server

Answer: A, D, F

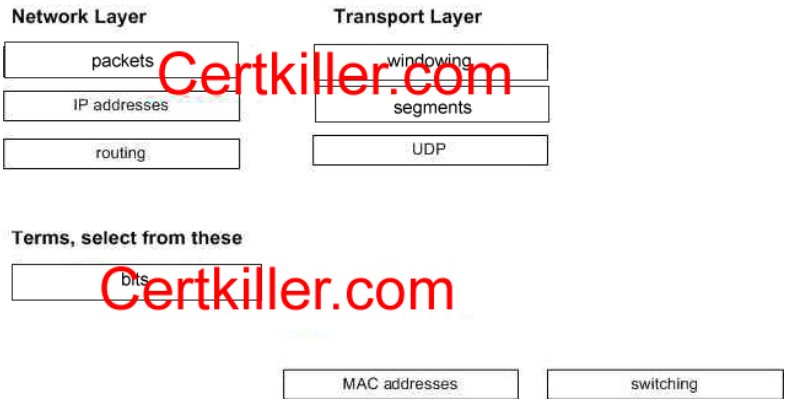
QUESTION 444

Your boss at Certkiller.com asks you to match the terms with the appropriate OSI layer. Not all options are used



Answer:

Your boss at Certkiller.com asks you to match the terms with the appropriate OSI layer. Not all options are used



QUESTION 445

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

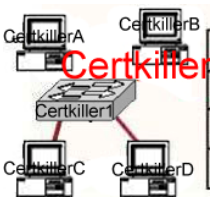
A. application
B. presentation
C. session
D. transport
E. network
F. data link
G. physical

Answer: E

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 446
Exhibit



Switch 1 switch table

Host	MAC Address	Port
A	00-0A-8A-47-E6-12	0/5
D	01-00-CD-22-03-14	0/9
B	01-1B-25-AB-32-E8	0/2

Host Certkiller B sends a frame to host Certkiller C.
What will the switch to with the frame?

A. Drop the frame
B. Send the frame out all ports except port 0/2
C. Return the frame to host Certkiller B
D. Send an ARP request for host Certkiller C
E. Send an ICMP Host Unreachable message to Host Certkiller B
F. Record the destination MAC address in the switching table and send the frame directly to Host Certkiller C

Answer: B

An Ethernet switch appears to use the same logic as a transparent bridge. However, the internal logic of the switch is optimized for performing the basic function of choosing when to forward and when to filter a frame. Just as with a transparent bridge, the basic logic of a LAN switch is as follows:

Step 1 A frame is received.

Step 2 If the destination is a broadcast or multicast, forward on all ports.

Step 3 If the destination is a unicast and the address is not in the address table, forward on all ports.

Step 4 If the destination is a unicast and the address is in the address table, forward the frame out the associated port, unless the MAC address is associated with the incoming port.

\

QUESTION 447
By default, which of the following factors determines the spanning-tree path cost?

A. It is the individual link cost based on latency
B. It is the sum of the costs based on bandwidth
C. It is the total hop count
D. It is dynamically determined based on load

Answer: B

Explanation:
"The STP cost is an accumulated total path cost based on the available bandwidth of each of the links."

Reference: Sybex CCNA Study Guide 4th Edition (Page 323)
Note:
A path cost value is given to each port. The cost is typically based on a guideline established as part of 802.1d. According to the original specification, cost is 1,000 Mbps (1 gigabit per second) divided by the bandwidth of the segment connected to the port. Therefore, a 10 Mbps connection would have a cost of (1,000/10) 100.
To compensate for the speed of networks increasing beyond the gigabit range, the standard cost has been slightly modified. The new cost values are:

Bandwidth	STP Cost Value
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2

You should also note that the path cost can be an arbitrary value assigned by the network administrator, instead of one of the standard cost values.
Incorrect Answers:
A, D. The STP process does not take into account the latency or load of a link. STP does not recalculate the link costs dynamically.
C. Hop counts are used by RIP routers to calculate the cost of a route to a destination. The STP process resides at layer 2 of the OSI model, where hop counts are not considered.

QUESTION 448
What is the purpose of the spanning-tree algorithm in a switched LAN?

A. To provide a monitoring mechanism for networks in switched environments.
B. To manage VLANs across multiple switches.
C. To prevent switching loops in networks with redundant switched paths.
D. To segment a network into multiple collision domains.
E. To prevent routing loops in networks.

Answer: C
STP is used in LANs with redundant paths or routes to prevent loops in a layer 2 switched or bridged LAN.
Incorrect Answers:
A, B. The primary purpose of STP is to prevent loops, not for monitoring or management of switches or VLANs.
D. VLANs are used to segment a LAN into multiple collision domains, but the STP process alone does not do this.
E. Routers are used to prevent routing loops at layer 3 of the OSI model. STP operates at layer 2.

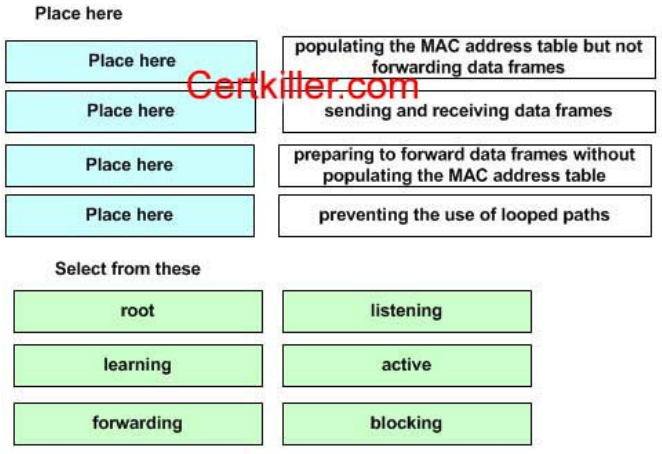
QUESTION 449
Which two of the following values does STP take into consideration when it elects the root bridge? (Select two answer choices)

A. The BPDU version number
B. The access layer bridge setting
C. The Bridge ID
D. The spanning-tree update number
E. The bridge priority
F. The VLAN number

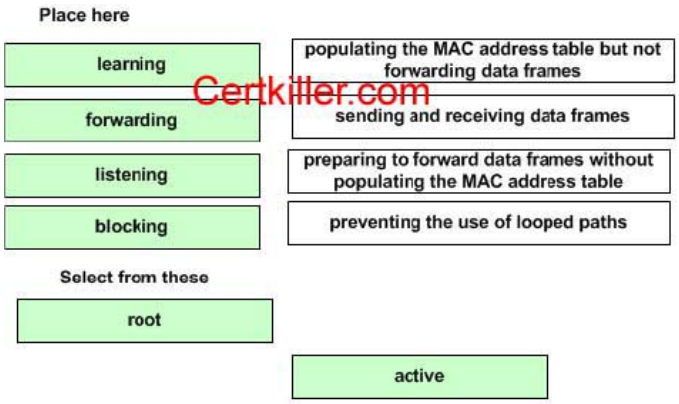
Answer: C, E

Explanation:
The bridges elect a root bridge based on the bridge IDs in the BPDUs. The root bridge is the bridge with the lowest numeric value for the bridge ID. Because the two part bridge ID starts with the priority value, essentially the bridge with the lowest priority becomes the root. For instance, if one bridge has priority 100, and another bridge has priority 200, the bridge with priority 100 wins, regardless of what MAC address was used to create the bridge ID or each bridge/switch.
Reference: CCNA Self-Study CCNA ICND Exam Certification Guide (Cisco Press, ISBN 1-58720-083-X) Page 39

QUESTION 450
Match the Spanning-Tree Protocol states from the bottom to the slot on the upper left that matches their corresponding function on the right.
(Not all the options are used.)



Answer:



Explanation:
The various STP states are shown below:
• Listening - Listens to incoming Hello messages to ensure that there are no loops, but does not forward traffic or learn MAC addresses on the interface.
• Learning -learns MAC addresses and builds a filter table but does not forward frames.
• Forwarding - Sends and receives all data on the bridged port.
• Blocking - are used to prevent network loops.
Reference: CCNA Study guide Second Edition (Sybex, Todd Lammle) page 82.

QUESTION 451
The spanning tree information from 4 switches on the Certkiller network is displayed below. Despite their names, all four switches are on the same LAN.
Tampa#show spanning-tree
Spanning tree 1 is executing the IEEE compatible Spanning Tree protocol
Bridge Identifier has priority 32768, address 0002.fd29.c505
Configured hello time 2, max age 20. forward delay 15

Miami#show spanning-tree
Spanning tree 1 is executing the IEEE compatible Spanning Tree protocol
Bridge Identifier has priority 16384, address 0002.fd29.c504
Configured hello time 2, max age 20, forward delay 15

London#show spanning-tree
Spanning tree 1 is executing the IEEE compatible Spanning Tree protocol
Bridge Identifier has priority 8192, address 0002.fd29.c503
Configured hello time 2, maxage 20, forward delay 15

Cairo#show spanning-tree
Spanning tree 1 is executing the IEEE compatible Spanning Tree
protocol
Bridge Identifier has priority 4096, address 0002.fd29.c502
Configured hello time 2, maxage 20, forward delay 15
Based on the outputs of the above exhibit, which one of the switches is the spanning tree root bridge?

A. Miami
B. London
C. Tampa
D. Cairo

Answer: D

Explanation: Cairo is the correct answer because it has the lowest Bridge priority. The default priority value is 32768 (same as Tampa), and the bridge with the lowest priority will become the root bridge.
A root bridge is chosen based on the results of the BPDU process between the switches. Initially, every switch considers itself the root bridge. When a switch first powers up on the network, it sends out a BPDU with its own BID as the root BID. When the other switches receive the BPDU, they compare the BID to the one they already have stored as the root BID. If the new root BID has a lower value, they replace the saved one. But if the saved root BID is lower, a BPDU is sent to the new switch with this BID as the root BID. When the new switch receives the BPDU, it realizes that it is not the root bridge and replaces the root BID in its table with the one it just received. The result is that the switch that has the lowest BID is elected by the other switches as the root bridge.

QUESTION 452
Which of the following are spanning tree port states? (Select three answer choices)

A. learning
B. spanning
C. listening
D. forwarding
E. initializing
F. filtering
G. permitting

Answer: A, C, D

Explanation:
There are 4 STP states that a bridge port can be in: Blocking, Listening, Learning, and

Forwarding:

Spanning-Tree Intermediate States

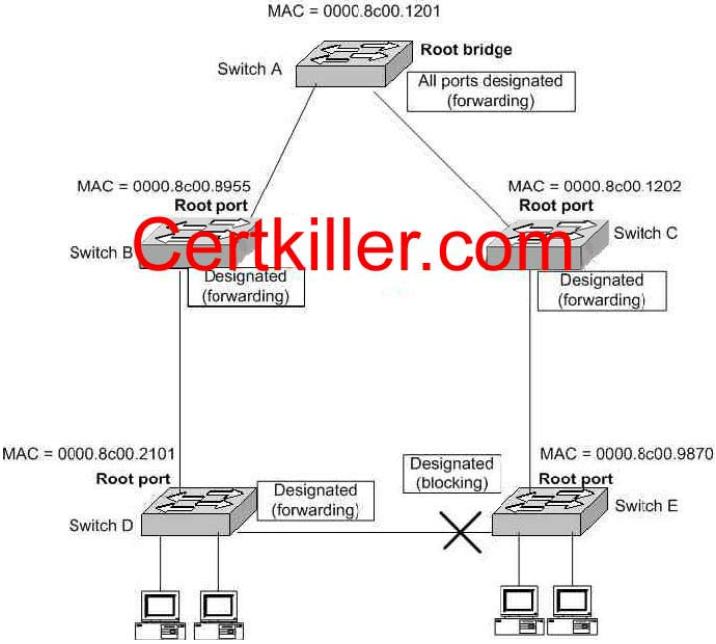
State	Forwards Data Frames?	Learns MACs Based on Received Frames?	Transitory or Stable State?
Blocking	No	No	Stable
Listening	No	No	Transitory
Learning	No	Yes	Transitory
Forwarding	Yes	Yes	Stable

QUESTION 453
What are the switch and bridge port characteristics of a layer two spanning-tree network that is fully converged?

A. All switch and bridge ports are in the forwarding state.
B. All switch and bridge ports are in the stand-by state.
C. All switch and bridge ports are assigned as either root or designated ports.
D. All switch and bridge ports are in either the forwarding or blocking state.
E. All switch and bridge are either blocking or looping.

Answer: D

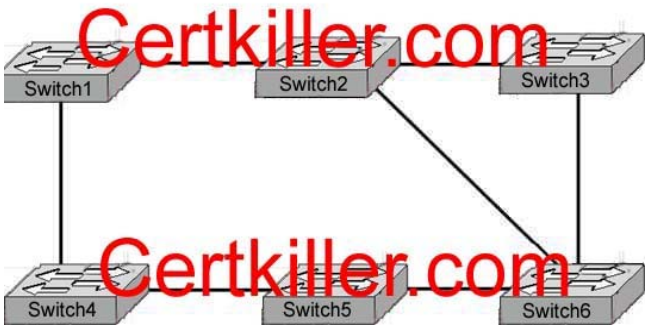
Explanation:
When a switch first comes up, it will be in the listening and learning states. This is needed so that the switch learns the MAC addresses of the devices on the LAN, and to learn where any loops in the network may exist. After this initial period of listening and learning, the ports will be forwarding to the hosts, or blocking certain ports that create a loop in the network. An example of this is shown below:



In the above figure, after the network has converged, spanning tree protocol puts each

port either in designated (Forwarding) or Non-designated (Blocking) state. So, Choice D is correct.
If you get a converged spanning-tree network, you have only two port states.
Forwarding an Blocking. Forwarding: all traffic will be forwarded
Blocking: all traffic to devices who will create a loop in a spanning-tree network - will be blocked. It is possible to get redundantes paths in big switched an routed networks.

QUESTION 454
The Certkiller LAN consists of 6 switches connected together as shown in the diagram below:



What is the name of the potential problem of this switch setup, and what protocol can prevents its occurrence. (Select only one answer choice)

A. routing loops, hold down timers
B. switching loops, split horizon
C. routing loops, split horizon
D. switching loops, VTP
E. routing loops, STP
F. switching loops, STP

Answer: F

Explanation: The spanning-Tree Protocol (STP) prevents loops from being formed when switches or bridges are interconnected via multiple paths. Spanning-Tree Protocol implements the 802.1D IEEE algorithm by exchanging BPDU messages with other switches to detect loops, and then removes the loop by shutting down selected bridge interfaces. This algorithm guarantees that there is one and only one active path between two network devices.

QUESTION 455
In a switched LAN network, what is the Spanning-Tree algorithm used for?

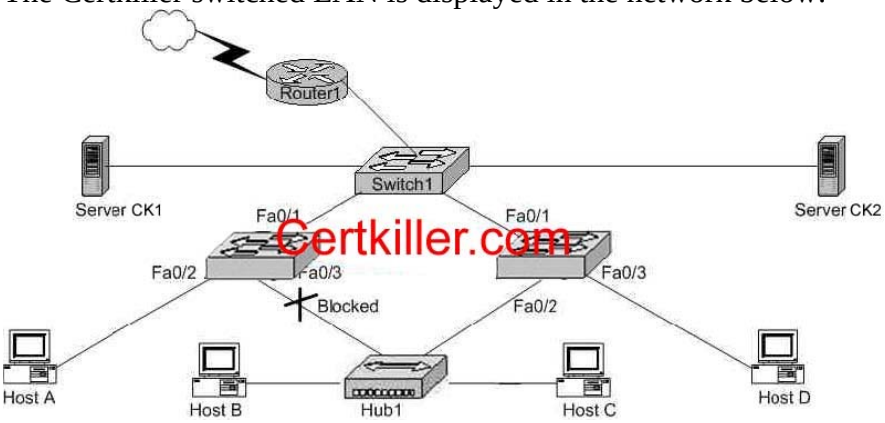
A. It is used to provide a mechanism for routing updates in switched environments.
B. It is used to prevent routing loops in networks with redundant routes.
C. It is used to prevent switching loops in networks with redundant switched routes.
D. It is used to manage, the addition, deletion, and naming of VLANs across multiple

switches.
E. It is used to segment a network into multiple collision domains.
F. None of the above.
G. All of the above are functions of STP.

Answer: C

Explanation:
To avoid loops, all bridging devices, including switches, use STP. STP causes each interface on a bridging device to settle into a blocking state or a forwarding state. Blocking means that the interface cannot forward or receive data frames. Forwarding means that the interface can send and receive data frames. By having a correct subset of the interfaces blocked, a single currently active logical path will exist between each pair of LANs. STP resides at the data link layer, so it is used to prevent loops within a switched network. It is not used to prevent routing loops; that is the function of the mechanisms within a routing protocol.
Not B: Of course: to a SWITCH there are SWITCHING Loops. To a switch ROUTING - Loops are impossible..
Reference:
CCNA Self-Study CCNA INTRO exam certification Guide (Cisco Press, ISBN 1-58720-094-5) page 248.

QUESTION 456
The Certkiller switched LAN is displayed in the network below:



In the network shown in the diagram, which ports on Switch2 are receiving BPDUs?

A. Fa 0/1 only
B. Fa 0/2 only
C. Fa 0/3 only
D. Fa 0/1 and Fa 0/2 only
E. Fa 0/1 and Fa 0/3 only
F. All three ports

Answer: E

Explanation:
Spanning-Tree Protocol (STP) prevents loops from being formed when switches or bridges are interconnected via multiple paths. Spanning-Tree Protocol implements the 802.1D IEEE algorithm by exchanging BPDU messages with other switches to detect loops, and then removes the loop by shutting down selected bridge interfaces. This algorithm guarantees that there is one and only one active path between two network devices.

QUESTION 457
In which Spanning-Tree states does a switch port learn MAC addresses? Select two.

A. blocking
B. listening
C. forwarding
D. learning
E. relaying

Answer: B, D

Explanation:
STP uses a couple of port states besides forwarding and blocking.
1. Listening - Listens to incoming Hello messages to ensure that there are no loops, but does not forward traffic. This is an interim state between blocking and forwarding.
2. Learning - Still listens to BPDUs, plus learns MAC addresses from incoming frames. It does not forward traffic. This is an interim state between blocking and forwarding.
3. Disabled - Administratively down.
Reference: Cisco CCNA intro 640-821

QUESTION 458
Which of the statements below are true regarding the availability of bandwidth on a network? (Select all that apply.)

A. Bandwidth availability is decreasing.
B. Bandwidth availability is infinite.
C. Bandwidth is used when analyzing network performance.
D. Bandwidth availability is finite.
E. Bandwidth availability is fixed.

Answer: C, D

Explanation: C is correct because performance analyzing software is notorious for consuming bandwidth. Most network management devices use SNMP, which consumes bandwidth. D is correct because although new technologies are providing for more bandwidth and a network can be engineered to give more priority to different devices,

there is a finite amount of bandwidth available at any given time.
Incorrect Answers:

A. This is incorrect because new technologies are actually increasing the amount of potential bandwidth.
B. For any given network, the amount of bandwidth available to end users is usually fixed, and based on the speed of the connection to access connection. For example, any given PC with a 10/100 NIC will be limited to 100Mbps of throughput at any given time.
E. This is incorrect because it's always possible to upgrade a scalable technology or allocate resources differently.

QUESTION 459
Which one of the following actions would actually increase congestion on an Ethernet network?

A. Increasing the number of collision domains.
B. Micro-segmenting the network.
C. Adding hubs for connectivity to the network.
D. Putting additional switches in the network.
E. Implementing VLANs in the network.

Answer: C

Explanation:
All of the answer choices above except for C are all good ways of reducing network congestion. Hubs on the other hand increase congestion, because they allow the addition of more users, therefore more potential traffic, more collisions (if it's a half-duplex) and their use will result in increased overall congestion.
Incorrect Answers:
A, B, D, E. These answers all describe the use of VLANs, which are used to decrease the size of any given collision domain and to decrease the amount of link level multicast and broadcast traffic.

QUESTION 460
You have an Ethernet network. Which of the conditions below can lead to increased congestion on your network? (Select two answer choices)

A. The use of Full-Duplex Mode.
B. The Creation on New Collision Domains.
C. The Creation on New Broadcast Domains.
D. The Addition of Hubs to the Network.
E. The use of switches in the Network.
F. The Amount of ARP or IPX SAP Traffic.

Answer: D, F

Explanation:
Hubs on their own don't create congestion, but the hosts that connect to them do. Generally, the addition of hubs means additional hosts connected to the hubs, all within the same collision domain. Finally, as networks become larger, more broadcast traffic such as ARP requests and IPX SAP packets get generated, which can lead to increased network congestion.
Incorrect Answers:

A. This is incorrect because the use of full duplex will increase the amount of bandwidth while eliminating collisions at the same time.
B, C. These methods describe the use of segmentation and VLAN use, which will decrease traffic on the individual segments.
E. This is incorrect because switches are the preferred method of reducing collision domains.

QUESTION 461
Which of the following can lead to the contribution of LAN traffic congestion? (Select all that apply)

A. Too many hosts in a broadcast domain
B. Full duplex operation
C. Broadcast storms
D. Multicasting
E. Segmentation
F. Low bandwidth

Answer: A, C, D, F

Explanation:
Choice A is correct because the more hosts on a broadcast domain, the more traffic that is created. Choice C contributes to congestion because broadcast storms can become very problematic, and lead to complete network saturation. Multicasts are similar to broadcasts in their use on a LAN. Finally, if there is not enough bandwidth, traffic sessions can time out. This leads to new transmissions and the re-sending of data, which can lead to more congestion.
Incorrect Answers:
B, E. These are incorrect because full duplex operation and segmented networks actually result in less congestion.

QUESTION 462
You have been contracted by Certkiller to replace the network cabling of their LAN's. The System Administrator gives you specific instructions that he needs to use cabling in the LAN that is NOT susceptible to EMI.
What kind of cable would you use to satisfy the administrator's needs?

A. Thicknet coaxial cable.

B. Thinnet coaxial cable.
C. Category 5 UTP cable.
D. Category 5 STP cable.
E. Fiber optic cable.
F. All of the above

Answer: E

Explanation:
EMI stands for Electro-Magnetic Interference, which can cause the corruption of packets as they traverse the network. If this is a major concern then fiber is the best choice. Fiber optic cable is more secure, supports longer distances and higher speeds, and is not susceptible to EMI. The major drawback of fiber is that it is the most expensive choice.

QUESTION 463
What is the IEEE standard associated with Gigabit Ethernet? (Select two answer choices)

A. 802.11
B. 802.5
C. 802.3ab
D. 802.3ae
E. 802.3z
F. 802.3u

Answer: C, E

Explanation:
The IEEE 802.3z standard describes 1000BASE-SX.
The 1000BaseT standard was released in June 1999, defined by IEEE 802.3ab.
Incorrect Answers:

A. This describes the standard used for wireless networks.
B. This is the standard for token ring networks.
D. On June 17, 2002 the IEEE 802.3ae specification for 10 Gigabit Ethernet was approved as an IEEE standard by the IEEE Standards Association (IEEE-SA) Standards Board.
F. IEEE 802.3u describes the standard for 100BASE-TX.

QUESTION 464
On a half-duplex Ethernet LAN, two hosts attempt to send data simultaneously, resulting in a collision. Following this collision, what will the hosts do? (Select all valid answers)

A. The destination host sends a request to the source for retransmission.
B. The jam signal indicates that the collision has been cleared.

C. The hosts will attempt to resume transmission after a time delay has expired.
D. An electrical pulse indicates that the collision has cleared.
E. The router on the segment will signal that the collision has cleared.
F. The hosts will do nothing, as the higher layers are responsible for data error correction and re-transmission.

Answer: C

Explanation:
When a host on an Ethernet LAN has information to send, the following steps are taken:
1. A device with a frame to send listens until Ethernet is not busy.
2. When the Ethernet is not busy, the sender begins sending the frame.
3. The sender listens to make sure that no collision occurred.
4. Once the senders hear the collision, they each send a jamming signal, to ensure that all stations recognize the collision.
5. After the jamming is complete, each sender randomizes a timer and waits that long.
6. When each timer expires, the process starts over with step 1.

QUESTION 465
Which of the following statements correctly describe the differences between halfduplex and full-duplex Ethernet? (Select two answer choices.)

A. Full-duplex Ethernet uses CSMA/CD to prevent collisions.
B. Half-duplex Ethernet uses a loopback circuit to detect collisions.
C. A full-duplex Ethernet card allows 20Mbps for data transmission.
D. Full-duplex Ethernet makes use of two pairs of wires for data.
E. An Ethernet hub can operate both half and full duplex simultaneously.

Answer: B, D

Explanation:
Half-duplex Ethernet send and receives on the same line, so a loopback needs to be set to detect collisions. Alternatively, full-duple Ethernet doesn't have to because it uses two pairs of wire, one to send and the other to receive. Collisions are not possible on full duplex Ethernet networks.
Incorrect Answers:

A. Full duplex uses both pairs of wires, so transmissions are sent on the first pair, and data that is received come in on the other pair. This prevents collisions.
C. Full duplex allows for data to be sent and received at the same time. It will not double the amount of bandwidth at any given time. The speed of the Ethernet link will remain at 10/100.
E. Hubs are shared devices and can only support one mode, unlike switches.

QUESTION 466
Why is full-duplex Ethernet superior to its single-duplex counterpart? (Select two answer choices.)

A. It uses inexpensive hubs
B. It operates without collisions
C. It operates on switches
D. It provides faster data transfer
E. It utilizes fewer wiring pairs

Answer: B, D

Explanation:
Full duplex Ethernet allows concurrent sending and receiving, which allows the full bandwidth to be used for both sending and receiving. The result is a collision free network with increased throughput.
Incorrect Answers:
A, C. These are incorrect because full duplex doesn't require hubs or switches. Full duplex operation can be used on switch and router ports, as well as PC hosts.
E. This is incorrect because full duplex actually uses more wiring pairs. In full duplex, both wire pairs are used. Half duplex uses only a single pair.

QUESTION 467
What are the differences between full-duplex Ethernet and half-duplex Ethernet? (Select all that apply)

A. Half-duplex Ethernet operates in a shared collision domain.
B. Full-duplex Ethernet has a lower effective throughput.
C. Half-duplex Ethernet operates in a private collision domain.
D. Full-duplex Ethernet allows two-way communication.
E. Half-duplex Ethernet operates in a private broadcast domain.

Answer: A, D

Explanation:
The original Ethernet specifications used a shared bus, over which only one frame could be sent at any point in time. So, a single device could not be sending a frame and receiving a frame at the same time because it would mean that a collision was occurring. Half duplex stations use CSMA/CD to prevent collisions on the network, because the collision domain is shared. Full duplex Ethernet eliminated the need to collision detection, by allowing for two way communication.
Incorrect Answers:
B. Full duplex effectively doubles the throughput of half-duplex operation, because data can be both sent and received at the full 10/100 speed.
C, E. In half duplex operation, the network is shared between all devices in the collision domain.

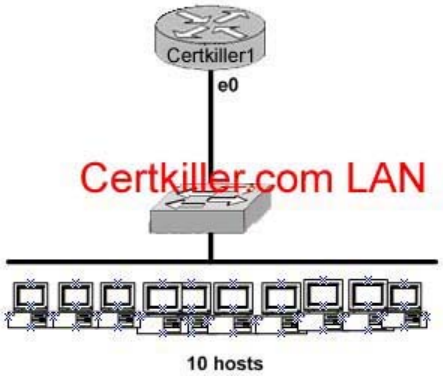
QUESTION 468
When you compare the differences between half-duplex and full-duplex Ethernet, which of the following characteristics are exclusive to half-duplex? (Select two answer choices)

A. Half-duplex Ethernet operates in a shared collision domain.
B. Half-duplex Ethernet operates in an exclusive broadcast domain.
C. Half-duplex Ethernet has efficient throughput.
D. Half-duplex Ethernet has lower effective throughput.
E. Half-duplex Ethernet operates in an exclusive collision domain.

Answer: A, D

Explanation:
A single device could not be sending a frame and receiving a frame at the same time because it would mean that a collision was occurring. So, devices simply chose not to send a frame while receiving a frame. That logic is called half-duplex logic.
Ethernet switches allow multiple frames to be sent over different ports at the same time. Additionally, if only one device is connected to a switch port, there is never a possibility that a collision could occur. So, LAN switches with only one device cabled to each port of the switch allow the use of full-duplex operation. Full duplex means that an Ethernet card can send and receive concurrently.
Reference: CCNA Self-Study CCNA INTRO exam certification Guide (Cisco Press, ISBN 1-58720-094-5) Page 62-63.

QUESTION 469
The Certkiller LAN consists of 10 PC users as shown in the diagram below:



Each of the hosts is connected to their own 10Mbps half-duplex switch port to the e0 interface of a router. How much bandwidth is available to each individual host?

A. 1 Mbps
B. 10 Mbps
C. 20 Mbps
D. 100 Mbps
E. 120 Mbps

Answer: B

Explanation:
Although ten hosts are sharing a 10Mbps half duplex connection, there are still 10Mbps available to them under the best hypothetical circumstances. Unlike hubs, each switch port will be allocated the entire bandwidth. Hubs are shared devices, so in this example if there was a hub in place then the 10 hosts would all be sharing one 10Mbps connection.

QUESTION 470
Which of the following data network would you implement if you wanted a wireless network that had a relatively high data rate, but was limited to very short distances?

A. Broadband personal comm. Service (PCS)
B. Broadband circuit
C. Infrared
D. Spread spectrum
E. Cable

Answer: C

Explanation:
A good example of the range of an infrared is a television remote control or a garage door opener. Infrared networks are capable of high data rates, but they are limited in the distance between the infrared points, and also by the fact that a line of sight between the nodes is usually required.
Incorrect answers:
A, D. Although these are both wireless methods, the data rate capabilities are somewhat limited, especially when compared to infrared links.
B, E. Although these are both capable of relatively high data rates, they do not use wireless technology.

QUESTION 471
Which IEEE standard is used to define Wi-Fi?

A. IEEE 802.3
B. IEEE 802.5
C. IEEE 802.11h
D. IEEE 802.11c
E. IEEE 802.11

Answer: E

Explanation:
IEEE 802.11 was the original standard for wireless networks. However, the standard had

a few ambiguities allowed for potential problems with compatibility between devices. To ensure compatibility, a group of companies formed the Wireless Ethernet Compatibility Alliance (WECA), which has come to be known as the Wi-Fi Alliance, to ensure that their products would work together. The term Wi-Fi is now used to refer to any IEEE 802.11 wireless network products that have passed the Wi-Fi Alliance certification tests.
Incorrect Answers:

A. This is the standard used for Ethernet networks.
B. This is the standard used in Token Ring networks.
C, D. These standards are not currently used. The most prevalent types of wireless 802.11 networks are 802.11a, 802.11b, and 802.11g.

QUESTION 472
What is the maximum data rate specified by the IEEE 802.11B standard for wireless LANS?

A. 10 Mbps
B. 11 Mbps
C. 54 Mbps
D. 100 Mbps
E. none of the above

Answer: B

Explanation:
The maximum speed for 802.11b is 11 Mbps.
Incorrect Answers:

A. This is the maximum speed for legacy Ethernet networks.
C. This is the maximum speed supported by the other prevalent wireless standards, 802.11a and 802.11g.
D. This is the maximum speed of fast Ethernet connections.

QUESTION 473
Assuming you build networks to exact specifications, what is the recommended maximum length a 10BaseT cable can be before it has to be segmented or repeated?

A. 100 meters
B. 100 feet
C. 100 yards
D. 200 meters

Answer: A

Explanation:
The distance standards are in meters and 10BaseT has a distance restriction of 100

meters. If you go further then that, you compromise data integrity. 10BastT is the predominant cable type used in Ethernet networks.

QUESTION 474
Which of the following are actual varieties of network crosstalk? (Select all the valid answer choices)

A. near-end crosstalk(NEXT)
B. middle open-end crosstalk(MOEXT)
C. power sum near-end crosstalk(PSNEXT)
D. jitterry crosstalk(JEXT)
E. far end crosstalk(FEXT)

Answer: A, C, E

Explanation:
Near End Crosstalk (NEXT) is crosstalk measured at the transmitting end of the cable. Far End Crosstalk (FEXT) is measured at the far end from where the signal was injected into the cable. Power Sum NEXT (PSNEXT) is basically a mathematical calculation that simulates all four wire pairs being energized at the same time. PSNEXT calculations are used to ensure that a cable will not exceed crosstalk noise performance requirements when all pairs are operating simultaneously. PSNEXT is typically used in Gigabit Ethernet, rather than 10BaseT or 100BaseT.
Reference: Sybex CCNA 4.0 - P. 30

QUESTION 475
Which of the following processes, is used to find the hardware address of a LAN device?

A. Inverse-ARP
B. Reverse-ARP
C. Proxy ARP
D. ARP

Answer: D

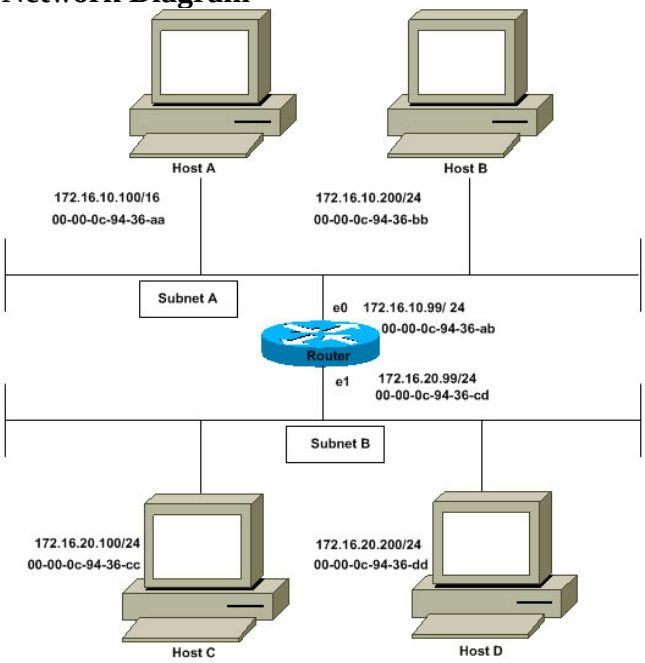
Explanation:
When a device needs to resolve a logical IP address to the physical Ethernet address (MAC), it uses the Address Resolution Protocol (ARP.)
Incorrect Answers:
A, B. Inverse ARP (sometimes also referred to reverse ARP), is used to resolve a known hardware MAC address to the IP address.

QUESTION 476
Which one of the protocols below allows a router to respond to an ARP request destined to a remote host?

A. Gateway DP
B. Reverse ARP
C. proxy ARP
D. Inverse ARP
E. indirect ARP

Answer: C

Explanation:
Below is an example taken from Cisco describing how proxy ARP operates:
Network Diagram



The Host A (172.16.10.100) on Subnet A needs to send packets to Host D (172.16.20.200) on Subnet B. As shown in the diagram above, Host A has a /16 subnet mask. What this means is that Host A believes that it is directly connected to all of network 172.16.0.0. When Host A needs to communicate with any devices it believes are directly connected, it will send an ARP request to the destination. Therefore, when Host A needs to send a packet to Host D, Host A believes that Host D is directly connected, so it sends an ARP request to Host D.
To reach Host D (172.16.20.200), Host A needs the MAC address of Host D. Therefore, Host A broadcasts an ARP request on Subnet A, as below:

Sender's MAC Address	Sender's IP Address	Target MAC Address	Target IP Address
00-00-0c-94-36-aa	172.16.10.100	00-00-00-00-00-00	172.16.20.200

In above ARP request, Host A (172.16.10.100) is requesting that Host D (172.16.20.200) send its MAC address. The above ARP request packet is then encapsulated in an Ethernet

frame with Host A's MAC address as the source address and a broadcast (FFFF.FFFF.FFFF) as the destination address. Since the ARP request is a broadcast, it reaches all the nodes in the Subnet A, including the router's e0 interface, but does not reach Host D. The broadcast will not reach Host D because routers, by default, do not forward broadcasts.
Since the router knows that the target address (172.16.20.200) is on another subnet and can reach Host D, it will reply with its own MAC address to Host A.

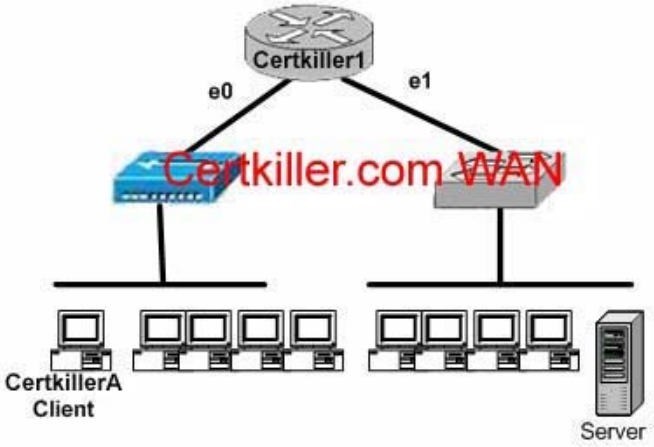
Sender's MAC Address	Sender's IP Address	Target MAC Address	Target IP Address
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-aa	172.16.10.100

Above is the Proxy ARP reply that the router sends to Host A. The proxy ARP reply
packet is encapsulated in an Ethernet frame with router's MAC address as the source address and Host A's MAC address as the destination address. The ARP replies are always unicast to the original requester.
On receiving this ARP reply, Host A updates its ARP table as below:

IP Address	MAC Address
172.16.20.200	00-00-0c-94-36-ab

From now on Host A will forward all the packets that it wants to reach 172.16.20.200 (Host D) to the MAC address 00-00-0c-94-36-ab (router). Since the router knows how to reach Host D, the router forwards the packet to Host D. The ARP cache on the hosts in Subnet A is populated with the MAC address of the router for all the hosts on Subnet B. Hence, all packets destined to Subnet B are sent to the router. The router forwards those packets to the hosts in Subnet B.
Reference: http://www.cisco.com/warp/public/105/5.html

QUESTION 477
The Certkiller A host and Server are separated by the Certkiller 1 router as shown in the diagram below:



The host Certkiller A is downloading a file from the server. What is the source MAC

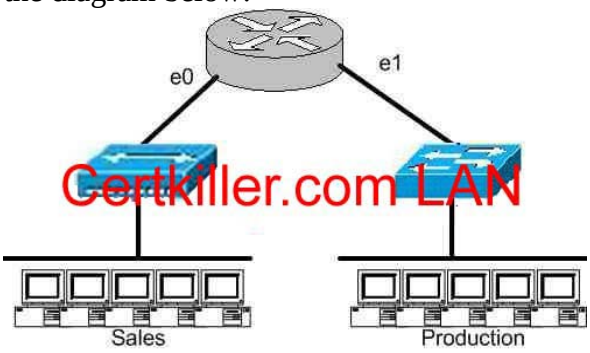
address on the frames that Certkiller A receives from the server on the network above? (Select only one answer choice)

A. The MAC address of router interface e0.
B. The MAC address of router interface e1.
C. The MAC address of Certkiller A.
D. The MAC address of the server network interface.

Answer: D

Explanation:
Even though the frames are passing through a router, the source and destination MAC address will not change during the data transmission.

QUESTION 478
The Sales and Production networks are separated by a Certkiller router as shown in the diagram below:



Which of the following statements most accurately describes the characteristics of the above networks broadcast and collision domains? (Select the two best answer choices)

A. There are two broadcast domains in the network.
B. There are four broadcast domains in the network.
C. There are six broadcast domains in the network.
D. There are four collision domains in the network.
E. There are five collision domains in the network.
F. There are seven collision domains in the network.

Answer: A, F

Explanation:
We have two broadcast domains total in this network, one with the Sales network and another consisting of the Production network. We have 5 computers and one port for E1 so we have 6 collision domains because a switch is being used in the Production department and one collision domain for the Sales department because a hub is being used there.

QUESTION 479
Which of the addresses below is an example of a valid unicast address?

A. 172.31.128.255./18
B. 255.255.255.255
C. 192.168.24.59/30
D. FFFF.FFFF.FFFF
E. 224.0.0.5

Answer: A
Explanation
If we take this address and convert it to binary we have:
10101100.00100000.10|000000.11111111 = valid IP
Incorrect Answers:
B. This is the all hosts broadcast address
C. This is a broadcast address for this given subnet.
D. This is reserved for the all hosts broadcast MAC address.
E. This is a reserved, class D address. Class D addresses are reserved for multicast use. This particular address is used by OSPF routers.

QUESTION 480
Two stations on a LAN transmit at the same time, resulting in a collision. What happens when a collision occurs on the network? (Choose all that apply)

A. Each device on the Ethernet segment stops transmitting for a short time.
B. A jam signal informs all devices that a collision occurred.
C. When data transmission resumes, the devices that were involved in the collision have priority to transmit.
D. The devices that are involved in the collision stops transmitting for a short time.
E. The collision invokes a random back-off algorithm.

Answer: B, D, E

Explanation:
When a host on an Ethernet LAN has information to send, the following steps are taken:
1. A device with a frame to send listens until Ethernet is not busy.
2. When the Ethernet is not busy, the sender begins sending the frame.
3. The sender listens to make sure that no collision occurred.
4. Once the senders hear the collision, they each send a jamming signal, to ensure that all stations recognize the collision.
5. After the jamming is complete, each sender randomizes a timer and waits that long.
6. When each timer expires, the process starts over with step 1.
Incorrect Answers:

A. Only the stations involved in the collision stop transmitting for a short time, not all

stations on the LAN.
C. No priority is given to any stations once a collision has occurred.

QUESTION 481
A trunk is configured between two Catalyst switches in the Certkiller network as shown in the diagram below:

Based on the information above, how many broadcast domains exist in the diagram?

A. One
B. Two
C. Three
D. Four
E. Five
F. Six

Answer: C

Explanation:
VLANs are used to logically segment a LAN network into multiple sub-networks. Each sub-network then resides in its own separate broadcast domain. In this case, there are 3 separate VLANs on this network, creating 3 different broadcast domains. The Trunk itself is used to carry information for all 3 of these VLANs, and the trunk itself is not considered to reside in a broadcast domain.

QUESTION 482
Network topology exhibit

Which statements describe the interconnections displayed in the exhibit? Select two

A. Traffic from host Certkiller A to host Certkiller D will be collision free.
B. Traffic from host Certkiller C to host Certkiller G will be collision free.
C. Traffic from host Certkiller E to host Certkiller G will be collision free.
D. Host Certkiller B can be connected at full duplex.

E. Host Certkiller F can be connected at full duplex.

Answer: A, D

QUESTION 483
Which of the following are true of Ethernet technology?

A. Hosts use a logical ring topology.
B. Hosts use a logical bus topology
C. Hosts must wait for an electronic signal to transfer data.
D. Hosts are directly connected to a wiring concentrator called a MSAU.

Answer: B

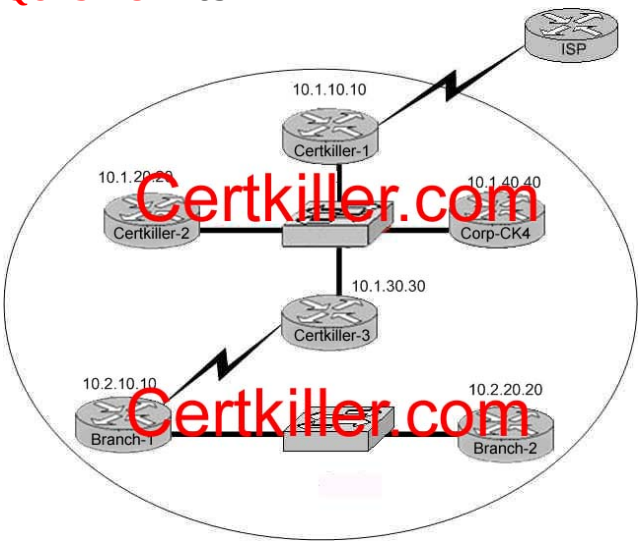
QUESTION 484
With regard to Ethernet media access methods, which of the following are true?
(Choose all that apply.)

A. A device waits for an electronic signal before transmitting.
B. A device listens and waits until the media is not busy before transmitting.
C. All devices on an Ethernet segment see data that passes on the network medium.
D. Only the sender and the receiver devices see data that passes on the network medium.
E. Ethernet networks allow you to configured devises with higher transmission priority.

Answer: B, C

Explanation:
Ethernet uses CSMA/CD access method.
CSMA/CD logic helps prevent collisions and also defines how to act when a collision does occur. The CSMA/CD algorithm words like this:
1. A device with a frame to send listens until the Ehternet is not busy.
2. When the Ethernet is not busy, the sender begins sending the frame.
3. The sender listens to make sure that no collision occurred.
4. Once the senders hear the collision, they each send a jamming signal, to ensure that all stations recognize the collision.
5. After the jamming is complete, each sender randomizes a timer and waits that long.
6 When each timer expires, the process starts over with Step 1.
So, all devices on the Ethernet need to use CSMA/CD to avoid collisions and to recover when inadvertent collisions occur.
Reference: Cisco CCNA intro 640-821 p.55

QUESTION 485



The internetwork infrastructure of Certkiller consists of a single OSPF area as shown in the graphic. There is concern that a lack of router resources is impeding internetwork performance. As part of examining the router resources, the OSPF DRs need to be known. All the router OSPF priorities are ad the default and the router IDs are shown with each router.
Which routers are likely to have been elected as DR? (Choose two)

A. Certkiller -1
B. Certkiller -2
C. Certkiller -3
D. Certkiller -4
E. Branch-1
F. Branch-2

Answer: D, F

QUESTION 486
Part of the job as a network administrator is being able to make a distinction between routed protocols and routing protocols.
Which of the following statements is true regarding them? (Choose all that apply)

A. A routing protocol is assigned to an interface and determines the method of packet delivery.
B. A routed protocol is assigned to an interface and determines the method of packet delivery.
C. A routing protocol determines the path of a packet through a network.
D. A routed protocol determines the path of a packet through a network.
E. A routing protocol operates at the transport layer of the OSI model.
F. A routed protocol updates the routing table of a router.

Answer: B, C

Explanation:
A routing protocol learns routes and puts those routes in a routing table. Examples of routing protocols are EIGRP, OSPF, and BGP.
A routed protocol is the type of packet forwarded, or routed, through a network. Examples of routed protocols include IP, IPX, and Appletalk.
Incorrect Answers:

A. Routing protocols are assigned to routers. This answer correctly describes a routed protocol.
D. This describes the function of a routing protocol.
E. Routing protocols operate at layer 3, which is the network layer, of the OSI model.
F. This is a function of a routing protocol.

QUESTION 487
Which one of the routing protocol below does NOT use a distance vector algorithm to calculate a route to a given destination? (Select all that apply)

A. RIP
B. IPX RIP
C. IGRP
D. OSPF
E. IS-IS

Answer: D

Explanation:
Only OSPF and IS-IS are true link-state routing protocols. The other choices are distance-vector routing protocols.

QUESTION 488
Non-contiguous networks can pose a problem for network reachability in certain circumstances. Which of the following routing protocols have means of minimizing the risk? (Select three choices)

A. RIP v1
B. RIP v2
C. EIGRP
D. IGRP
E. OSPF
F. VLSM

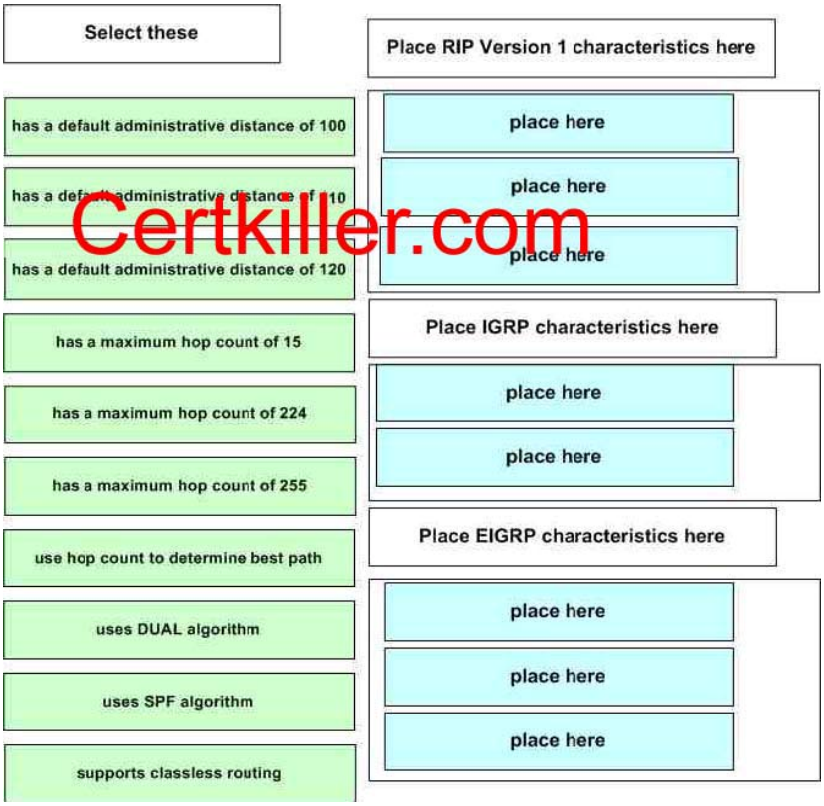
Answer: B, C, E

Explanation:
OSPF, RIP version 2, and EIGRP all provide support for discontiguous networks. This is

provided by the fact that subnet mask information is advertised along with the routes, and these protocols all support Variable Length Subnet Maks (VLSM).
Incorrect Answers:

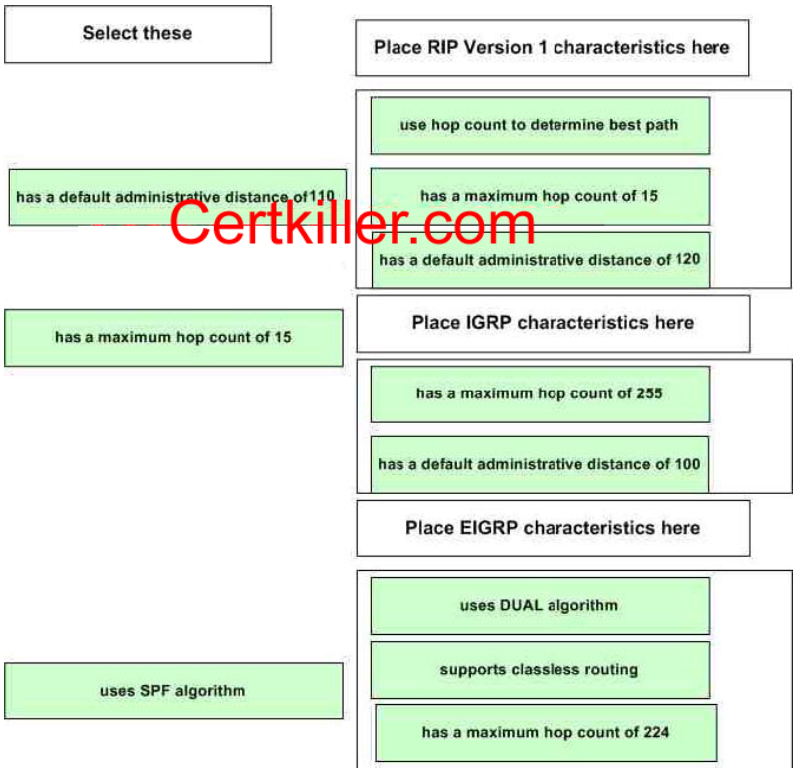
A. Whenever RIP version 1 advertises a network across a different major net boundary, RIP summarizes the advertised network at the major net boundary. RIP version 2 is an updated version of RIP, and one of the main features that it was able to provide over RIPv1 is support for VLSM information.
D. IGRP does not support VLSM. Like RIP version 2, EIGRP is the updated version of IGRP, which provides support for VLSM.
F. VLSM is the feature that is required to support non-contiguous networks, but VLSM is not itself a routing protocol.

QUESTION 489
Study the exhibit below regarding various routing protocols and their characteristics:



Move the correct statements on the left to its associated routing protocol on the right side. (Note: Not all choices will be used)

Answer:



Explanation:
Enhanced IGRP (EIGRP)
It is a classless, enhanced distance-vector, Cisco proprietary protocol. Like IGRP, EIGRP uses the concept of an autonomous system to describe the set of contiguous routers that run the same routing protocol and share routing information. But unlike IGRP, EIGRP includes the subnet mask in its route updates. The advertisement of subnet information allows us to use VLSM and summarization when designing our networks. EIGRP is sometimes referred to as a hybrid routing protocol because it has characteristics of both distance-vector and link-state protocols.
EIGRP has a maximum hop count of 224.
EIGRP supports two types of routes:
Internal EIGRP route: These are routes originated within a specific autonomous system by EIGRP routers that are members of the same autonomous system. The administrative distance of an internal EIGRP route is 90.
External EIGRP route: These routes appear within EIGRP routing tables due to either manual or automatic redistribution, and they represent networks that originated outside of the EIGRP autonomous system. The administrative distance of an external EIGRP route is 170.
Reference: Todd Lammle, CCNA Study Guide 4th Edition, Sybex Inc. 2004, Page 266 & 270.
EIGRP Metric
EIGRP metric is different than that of IGRP by a factor of 256 because of the metric field size: IGRP uses only 24 bits in its update packet for the metric field, whereas EIGRP uses 32 bits in its update packet for the metric field. The difference of 8 bits requires the IGRP

metric to be multiplied by 256 to obtain the EIGRP metric.
Reference: Troubleshooting IP Routing Protocols, Cisco Press, ISBN 1-58705-019-6,

---

QUESTION 490
Which of the following technologies can be used in distance vector routing protocols to prevent routing loops? (Select two)

A. Spanning Tree Protocol
B. Shortest path first tree
C. Link-state advertisements (LSA)
D. Hold-down timers
E. Split horizon
F. VRP

Answer: D, E

Explanation:
In order to prevent information from looping throughout a network, distance vector protocols, such as RIP version 2, use the following mechanisms:
• Split horizon - the routing protocol advertises routes out an interface only if they were not learned from updates entering that interface.
• Hold-down timer - After finding out that a router to a subnet has failed, a router waits a certain period of time before believing any other routing information about that subnet.
In addition to these, a finite number of hops are also used. This ensures that packets do not loop through a network indefinitely.
Reference: CCNA Self-Study CCNA ICND exam certification Guide (Cisco Press, ISBN 1-58720-083-X) Page 154.

QUESTION 491
Which of the following routing protocols are less likely prone to problems in non contiguous networks? (Select all valid responses)

A. IGRP
B. ICMP
C. OSPF
D. RIP v1
E. RIP v2
F. EIGRP

Answer: C, E, F

Explanation:
OSPF, RIP v2, and EIGRP all support VLSM information, which will eliminate the problems that can arise from non contiguous networks.
Incorrect Answers:

A, D. IGRP and RIP version 1 are distance vector routing protocols that do not support VLSM information, so they are prone to problems that can arise from discontiguous network schemes.
B. ICMP (Internet Control Message Protocol) is not a routing protocol. It is used primarily for the management and monitoring of networks.

QUESTION 492
Which of the following statements describe the characteristic of link state routing protocols? (Choose all that apply.)

A. The exchange of an advertisement is triggered by a change in the network.
B. All routers exchange routing tables with each other in a multipoint network.
C. Packets are routed based upon the shortest path to the destination.
D. Paths are chosen depending on the cost efficiency factor.
E. Every router in an OSPF area is capable of representing the entire network topology.
F. Only the designated router in an OSPF area can represent the entire network topology.

Answer: A, C, E

Explanation:
The predominant link state routing protocols are OSPF and IS-IS. The following describes the features and functionality of OSPF:
Open Shortest Path First
• Each router discovers its neighbors on each interface. The list of neighbors is kept in a neighbor table.
• Each router uses a reliable protocol to exchange topology information with its neighbors.
• Each router places the learned topology information into its topology database.
• Each router runs the SPF algorithm against its own topology database.
• Each router runs the SPF algorithm against its own topology database to calculate the best routes to each subnet in the database.
• Each router places the best roué to each subnet into the IP routing table.
The following list points out some of the key features of OSPF:
• Converges very quickly - from the point of recognizing a failure, it often can converge in less than 10 seconds.
• Supports VLSM.
• Uses short Hello messages on a short regular interval, with the absence of hello messages indicating that a neighbor is no longer reachable.
• Sends partial updates when link status changes and floods full updates every 30 minutes. The flooding, however, does not happened all at once, so the overhead s minimal.
• Uses cost for the metric.
Reference: CCNA Self-Study CCNA INTRO exam certification Guide (Cisco Press, ISBN 1-58720-094-5) Page 417

QUESTION 493
In EIGRP, what kind of route information is stored in RAM and maintained by way of hello packets and update packets? (Select two answer choices)

A. Neighbor Table
B. SRF Table
C. RTP Table
D. Topology Table
E. Query Table
F. Dual Table

Answer: A, D

Explanation:
In EIGRP the only two tables of significance are the neighbor table and the topology table.
Reference: Sybex CCNA StudyGuide edition 4, Page 271.

QUESTION 494
What is the maximum number of hops OSPF allows before it deems a network unreachable?

A. 15
B. 16
C. 99
D. 255
E. Unlimited

Answer: E
OSPF is a link state protocol. Link state protocols do not use hops to mark networks as unreachable. Instead OSPF implements a steady state operation to its adjacent neighbors by sending and receiving small Hello packets periodically. When an OSPF router does not receive a Hello packet for a specified time period, it assumes that the neighbor is down. The router then runs the SPF algorithm to calculate new routes.
Reference:
Certkiller 640-801 Study Guide, Section 5.2 "Steady State Operation".
Incorrect Answers:

A. This is the maximum number of hops that a RIP network could use before the route is deemed unreachable.
B. When a RIP routes receives a routing update for a route that shows a hop count of 16, the route is considered to be unreachable. RIP routers use this to prevent packets from looping through the network indefinitely, but OSPF routers do not.

QUESTION 495
On the topic of the OSPF hello protocol; which of the statements below are true? (Select two answer choices)

A. The OSPF Hello protocol provides dynamic neighbor discovery.
B. The OSPF Hello protocol detects unreachable neighbors in 90 second intervals.
C. The OSPF Hello protocol maintains neighbor relationships.
D. The OSPF Hello protocol negotiates correctness parameters between neighboring interfaces.
E. The OSPF Hello protocol uses timers to elect the router with the fastest links at the designated router.
F. The OSPF Hello protocol broadcast hello packets throughout the internetwork to discover all routers that are running OSPF.

Answer: A, C

Explanation:
The Hello Packet
OSPF contains a protocol (the Hello protocol) that is used to establish and maintain relationships between neighboring nodes. These relationships are called adjacencies. Adjacencies are the basis for the exchange of routing data in OSPF.
It is through the use of this protocol, and packet type, that an OSPF node discovers the other OSPF nodes in its area. Its name is intentionally significant; the Hello protocol establishes communications between potential neighboring routers. The Hello protocol uses a special subpacket structure that is appended to the standard 24-octet OSPF header. Together, these structures form a hello packet.
All routers in an OSPF network must adhere to certain conventions that must be uniform throughout the network. These conventions include the following:
• The network mask
• The interval at which hello packets will be broadcast (the hello interval)
• The amount of time that must elapse before a non responding router will be declared dead (that is, the router dead interval) by the other routers in the network
• All routers in an OSPF network must agree to use the same value for each of these parameters; otherwise, the network might not operate properly. These parameters are exchanged using hello packets. Together, they comprise the basis for neighborly communications. They ensure that neighbor relationships (known as adjacencies) are not formed between routers in different subnets and that all members of the network agree on how frequently to stay in contact with each other.
The hello packet also includes a listing of other routers (using their unique router IDs) that the source router has recently been in contact with. This field, the Neighbor field, facilitates the neighbor discovery process. The hello packet also contains several other fields such as Designated Router and Backup Designated Router. These fields are useful in maintaining adjacencies and support the operation of the OSPF network in both periods of stability and convergence.

QUESTION 496
A routing table contains static, RIP, and IGRP routes destined to the same network and network mask; with each set to its default administrative distance. Which route will it take?

A. The RIP route
B. The static route
C. The IGRP route
D. All three with a round robin load balancing technique.

Answer: B

Explanation:
To decide which route to use, IOS uses a concept called Administrative Distance. Administrative distance is a number that denotes how believable an entire routing protocol is on a single router. The lower the number, the better, or more believable the routing protocol.

Route Type	**Administrative Distance**
• Static	1
• IGRP	100
• RIP	120

Reference:
CCNA Self-Study CCNA ICND exam certification Guide (Cisco Press, ISBN 1-58720-083-X) Page 177

QUESTION 497
You are an administrator and you've just configured OSPF on a router with both physical and logical interfaces. Which of the following factors determine the router ID?

A. The lowest network number of any interface.
B. The highest network number of any interface.
C. The highest IP address of any logical interface.
D. The middle IP address of any logical interface.
E. The lowest IP address of any physical interface.
F. The highest IP address of any physical interface.
G. The lowest IP address of any logical interface.

Answer: F

Explanation:
The OSPF topology database includes information about routers and the subnets, or links, to which they are attached. To identify the routers in the neighbor table's topology database, OSPF uses a router ID (RID) for each router. A router's OSPF RID is that router's highest IP address on a physical interface when OSPF starts running.
Note: The OSPF router ID is a 32-bit IP address selected at the beginning of the OSPF

process. The highest IP address configured on the router is the router ID. If a loopback address is configured, then it is the router ID. In case of multiple loopback addresses, the highest loopback address is the router ID. Once the router ID is elected it doesn't change unless the IP address is removed or OSPF restarts.
Reference: CCNA Self-Study CCNA ICND exam certification Guide (Cisco Press, ISBN 1-58720-083-X) Page 208

QUESTION 498
Under which network type circumstance would an OSPF router establish router adjacencies while not performing the DR/BDR election process?

A. Point-to-point
B. Broadcast
C. Non-broadcast multi-access
D. Backbone area 0
E. None of the above

Answer: A

Explanation:
If there's a point to point connection, there's no need for a designated router or a backup designated router election since only two routers can exist on a point to point network segment.
Incorrect Answers:
B, C. All OSPF routers in a broadcast and non-broadcast multi-access network go through the DR and BDR election process.
D. The backbone area is not a network type, but a collection of OSPF networks links. Area 0 is reserved as the backbone area, and routers within area 0 may or may not go through the DR/BDR election process, depending on the network type.

QUESTION 499
On the assumption that every OSPF router in a particular area is configured with the same priority value; which secondary value would be used as a router ID when there is no loopback interface set?

A. The IP address of the first Fast Ethernet interface.
B. The IP address of the console management interface.
C. The highest IP address among its active interfaces.
D. The lowest IP address among its active interfaces.
E. The priority value until a loopback interface is configured.

Answer: C

Explanation:
Ordinarily the loopback interface would be selected as the router ID, but since there is no loopback interface set, the router ID will be the IP address of the first active interface. If

by chance that particular interface has more than one IP address, then the highest address will be selected as the Router ID in theory. In practice, the first interface to come up in an OSPF router will become the router ID, since the election process is non-preemptive.

QUESTION 500
What are the different characteristics of distance vector and link state routing protocols?

A. Distance vector protocols send the entire routing table to directly connected neighbors.
B. Distance vector protocols are responsible for sending updates to all networks listed in the routing table.
C. Link state protocols are responsible for sending the entire routing table to the whole network.
D. Link state protocols send updates regarding their own links status to all other routers on the network.
E. None of the above

Answer: A, D

Explanation:
Distance Vector Protocols:
Distance Vector Protocols advertise routing information by sending messages, called routing updates, out the interfaces on a router. These updates contain a series of entries, with each entry representing a subnet and a metric.
Link-State Protocols:
Sends partial updates when link status changes and floods full updates every 30 minutes. The flooding, however, does not happen all at once, so the overhead is minimal.
Reference: CCNA Self-Study CCNA INTRO exam certification Guide (Cisco Press, ISBN 1-58720-094-5) Page 413 + 419