Exam : 350-001

Title : Cisco Certified Internetworking Expert

Ver : 05-09-07

QUESTION 1
Layer 6 of the 7-Layer OSI model is responsible for which of the following?

A. Common Data Compression and Encryption Schemes
B. Establishing, managing, and terminating communication sessions
C. Synchronizing communication
D. Determining resource availability
E. None of the above

Answer: A

Explanation:
Layer 6 is the Presentation Layer. This layer provides independence from differences in data representation (e.g., encryption and compression) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.
Incorrect Answers:
B: This describes layer 5 of the OSI model, which is the Session Layer.
C, D: These are not responsibilities of the Presentation Layer.

QUESTION 2
Which of the following is a component of the Data Link Layer of the OSI model?

A. NIC
B. Repeater
C. Multiplexer
D. Hub
E. Router

Answer: A

Explanation:
The data link layer is layer 2 in the OSI model, and deals with things like MAC addresses, and link level technologies such as Ethernet and Token Ring. Network interface cards (NICs) typically implement a specific data link layer technology, so they are often called "Ethernet cards", "Token Ring cards", and so on. They also include a 48 bit MAC address, also called a burned in address since these addresses are burned into the cards.
Incorrect Answers:
B, C, D: Repeaters, Hubs, and Multiplexers deal with the physical connections of devices into a network, and they are considered to reside on the physical layer of the OSI model (layer 1).

E: Routers operate at layer 3 and 4 of the OSI model, since they deal with things like layer 3 IP addresses, and TCP/UDP ports.

QUESTION 3
Which statement is true regarding the use of TFTP?

A. TFTP lies at the Transport layer and runs over IP.
B. TFTP lies at the Application layer and runs over FTP.
C. TFTP lies at the Transport layer and runs over ICMP.
D. TFTP lies at the Application layer and runs over TCP.
E. TFTP lies at the Application layer and runs over UDP.

Answer: E

Explanation:
Trivial File Transfer Protocol (TFTP) is a simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password). It is an application that uses UDP port 69.

QUESTION 4
In a data communication session between two hosts, the session layer in the OSI model generally communicates with what other layer of the OSI model?

A. The Physical layer of the peer
B. The data link layer of the peer
C. The peer's presentation layer
D. The peer's application layer
E. The peer's session layer

Answer: E

Explanation:

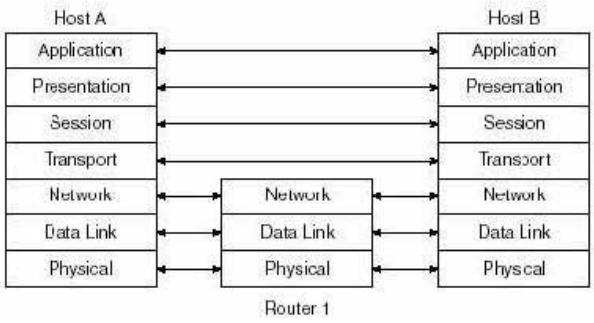
Interactions Between the Same Layers on Different Computers

Layer *N* must interact with Layer *N* on another computer to successfully implement its functions. For example, the transport layer (Layer 4) can send data, but if another computer does not acknowledge that the data was received, the sender will not know when to perform error recovery. Likewise, the sending computer encodes a destination network layer address (Layer 3) in the network layer header. If the intervening routers do not cooperate by performing their network layer tasks, the packet will not be delivered to the true destination.

To interact with the same layer on another computer, each layer defines a header and, in some cases, a trailer. Headers and trailers are additional data bits, created by the sending computer's software or hardware, that are placed before or after the data given to Layer *N* by Layer *N*+1. The information needed for this layer to communicate with the same layer process on the other computer is encoded in the header and trailer. The receiving computer's Layer *N* software or hardware interprets the headers and trailers created by the sending computer's Layer *N*, learning how Layer *N*'s processing is being handled, in this case.

Figure 3-3 provides a conceptual perspective on the same-layer interactions. The application layer on Host A communicates with the application layer on Host B. Likewise, the transport, session, and presentation layers on Host A and Host B also communicate. The bottom three layers of the OSI model have to do with delivery of the data; Router 1 is involved in that process. Host A's network, physical, and data link layers communicate with Router 1; likewise, Router 1 communicates with Host B's physical, data link, and network layers. Figure 3-3 provides a visual representation of the same-layer interaction concepts.

Figure 3-3 *Same-Layer Interactions on Different Computers*



QUESTION 5
Which layers do the OSI model and the TCP/IP models share in common? (Choose all that apply)

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

Answer: A, D

Explanation:
The TCP/IP reference model has the following layers:
Application, Transport, Internet, and Host to Network.
Incorrect Answers:
B, C, E, F. The TCP/IP reference model does not have a presentation layer, a session layer, a physical layer, or a data-link layer.

QUESTION 6
Under the OSPF process of your router's configuration, you type in "redistribute

igrp 25 metric 35 subnets" in order to redistribute your OSPF and IGRP routing information. What affect did the "subnets" keyword have in your configuration change?

A. It resulted in OSPF recognizing non-classful networks.
B. It had no effect since IGRP will summarize class boundaries by default.
C. It forced IGRP into supporting VLSM information.
D. It caused OSPF to accept networks with non-classful masks.

Answer: D

Explanation:
Whenever there is a major net that is subnetted, you need to use the keyword subnet to redistribute protocols into OSPF. Without this keyword, OSPF only redistributes major network boundaries. It is possible to run more than one OSPF process on the same router, but running more than one process of the same protocol is rarely needed, and it consumes the router's memory and CPU.
Incorrect Answers:

A. OSPF already always recognizes non-classful networks and their VLSM information.
B. Although IGRP does indeed summarize by class boundaries, OSPF does not by default. The "subnets" keyword enables OSPF to use VLSM information from the IGRP routes.
C. IGRP does not support VLSM routing information.

QUESTION 7
Which routing protocols do not need to have their router ID reachable by other routers within any given network in order to maintain proper network connectivity? (Choose all that apply)

A. EIGRP
B. OSPF
C. BGP
D. LDP
E. TDP
F. None of the above

Answer: A, B, C

Explanation:
The router ID of each router does not necessarily need to be reached by other routers in the network for EIGRP and OSPF. BGP uses TCP as the reliable exchange of information between routers, and BGP routers do not need to even be directly connected.
Incorrect Answers:
D, E. LDP and TDP are not routing protocols.

QUESTION 8
Which of the following does On Demand Routing use to transport ODR information from router to router?

A. RIP
B. BGP
C. CDP
D. UDP
E. LSP

Answer: C

Explanation:
ODR uses information from the Cisco Discovery Protocol (CDP).
Incorrect Answers:
A, B, D, E. ODR has nothing to do with RIP, BGP, UDP, or LSP.

QUESTION 9
A router running multiple protocols learns how to reach a destination through numerous different methods. Which of the following information will the router use first to determine the best way to reach the given destination?

A. The length of the network mask of a route.
B. The administrative distance of a route.
C. The metric of a route.
D. None of the above.

Answer: A

Explanation:
Most specific network match is always used first.
Incorrect Answers:
B, C: The administrative distance and metric is consulted only for routes with the same network mask length.

QUESTION 10
Which of the following routing protocols has a default administrative distance less that the default IS-IS AD?

A. External EIGRP routes
B. iBGP routes
C. Internal EIGRP routes
D. RIP version 1 routes
E. eBGP

Answer: C, E

Explanation:
The default IS-IS administrative distance is 115. Internal EIGRP routes are 90, and external BGP is 20.
Incorrect Answers:

A. External EIGRP routes have an AD of 170.
B. Interior BGP routes have an AD of 200.
D. RIP routes have an AD of 120.

QUESTION 11
Which of the following are key differences between RIP version 1 and RIP version 2? (Choose all that apply)

A. RIP version 1 supports authentication while RIP version 2 does not.
B. RIP version 2 uses multicasts while RIP version 1 does not.
C. RIP version 1 uses hop counts as the metric while RIP version 2 uses bandwidth information.
D. RIP version 1 does not support VLSM while RIP version 2 does.
E. RIP version 1 is distance vector while RIP version 2 is not.

Answer: B, D

Explanation:
Both Classless Routing and Multicast updates (224.0.0.9) were impossible with RIP v1 and are available with RIP version 2.
Incorrect Answers:

A. RIPv2 supports neighbor authentication. RIPv1 does not support this.
C. Both RIP version use hop counts as the metric.
E. Both RIP versions are distance vector routing protocols.

QUESTION 12
You are deciding which routing protocol to implement on your network. When weighing the different options, which of the following are valid considerations?

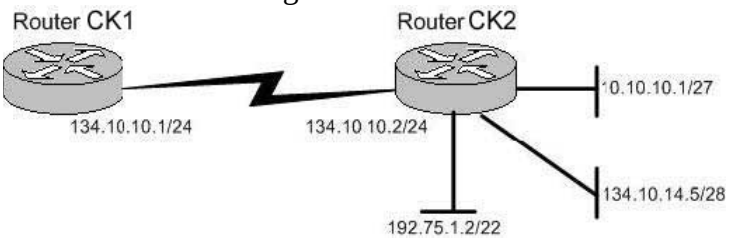
A. Distance vector protocols have a finite limit of hop counts whereas link state protocols place no limit on the number of hops.
B. Distance vector protocols converge faster than link state protocols.
C. RIP is a distance vector protocol. RIP v2 and OSPF are link state protocols.
D. Distance vector protocols only send updates to neighboring routers. Link state protocols depend on flooding to update all routers in the within the same routing domain.

Answer: A

Explanation:

Only A is true.
Incorrect Answers:
B. Link state protocols have the benefit of better convergence than distance vector protocols.
C. RIPv2 is a distance vector protocol, just like RIP version 1.
D. Link state protocols do not flood updates to every router within the same domain, just within their area.

QUESTION 13
The Certkiller network contains two routers named Router CK1 and Router CK2 as shown in the following exhibit:



Both Router CK1 and Router CK2 are running RIPv1. Both routers are configured to advertise all of their attached networks via RIP. Which of the networks connected to Router CK2 will be advertised to Router CK1 ?

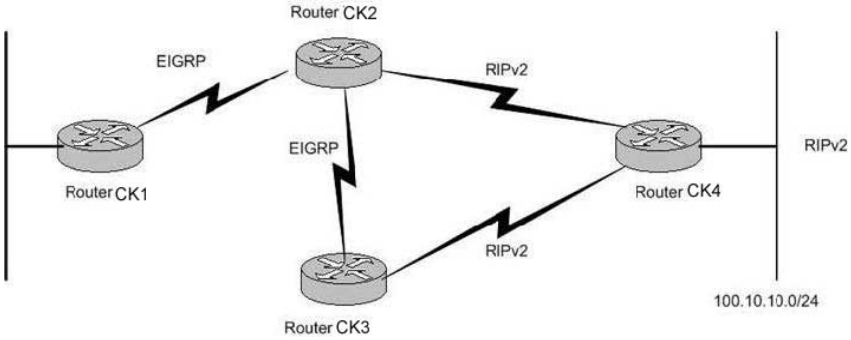
A. 10.10.10.0/27 and 134.10.15.0/28
B. 10.0.0.0/8 and 192.75.0.0/24
C. 134.10.15.0/28 and 192.75.0.0/22
D. Only 10.0.0.0/8
E. Only 134.10.15.0/28
F. Only 10.10.10.0/27
G. None of the above

Answer: D

Explanation:
Only one subnet 10.0.0.0/8 will be advertised.
In this scenario we are being tested on the following concepts:
RIP V1 performs auto summarization at network boundaries by default. It treats the subnets to be advertised differently depending upon several attributes of the respective subnets.
Here is the process RIP v1 uses to advertise, assuming that there are no filters (such as distribute-lists, or route-maps) to block the packet:
Is the route to be advertised part of the major network of the interface?
If it is, then advertise. If it is not, then summarize the network to its classful boundary and send it out.
This is the fate of the 10.10.10.0/27 subnet, which will be summarized as 10.0.0.0/8 and sent out.
Incorrect Answers:
A, C, E. If the route is part of the major network, check to see of the subnet mask

matches that of the outgoing interface. If the subnet mask does match then advertise the route out the interface. If the subnet mask of the route does not match the interface's subnet mask, then do not advertise the route out the interface unless the route is a host route (/32). This is the fate of the 134.10.15.0/28 subnet, which will not be sent out (advertised) at all.
B, C. Super net advertisement (advertising any network prefix less than its classful major network) is not allowed in RIP route summarization. This is the fate of the 192.75.1.2/22 subnet, which will be not be sent out (advertised) at all.
F. The 10.10.10.0/27 network will be summarized and sent as10.0.0.0/8.
Please note:
If the route is a host route then advertise it out.

QUESTION 14
You are the network administrator at Certkiller . The Routing protocols which run between the different routers in the Certkiller network are shown in the following exhibit:



On Router CK3 RIPv2 is being redistributed into EIGRP. No other redistribution is done to the network.
With regard to this scenario, who owns the route for subnet 100.10.1.0/24 in the routing table of Router CK1 ?

A. Nobody, because the route is neither in the routing table of Router CK1 , nor EIGRP topology table.
B. External EIGRP.
C. The route is only in the EIGRP topology table only and not in the routing table of Router CK1 .
D. Internal EIGRP.
E. The route is only but is in the EIGRP topology table as an active route and not in the routing table of Router CK1 .

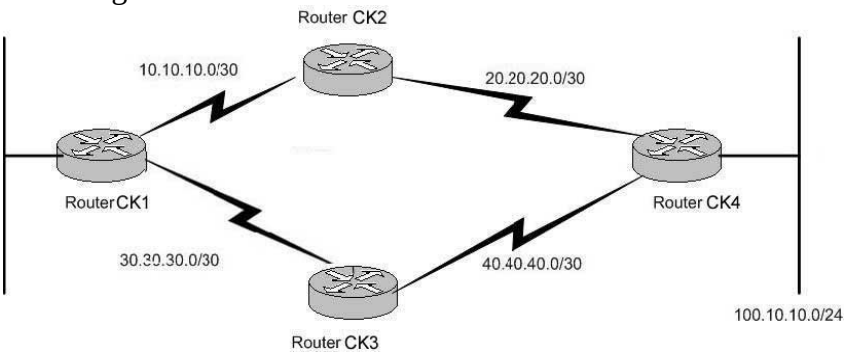
Answer: B

Explanation:
External EIGRP will own the route, because the route is from outside the AS. Routes that are redistributed into EIGRP are automatically considered external EIGRP routes.
Incorrect Answers:

A. Since RIPv2 allows for VLSM information to be carried in the route, there are no

concerns about the route not being advertised due to summarization. Since RIPv2 is being redistributed into EIGRP, CK1 will learn about the route via CK2 and CK3 .
C, E. This route will be in both the EIGRP table, as well as the IP routing table.
D. Redistributed routes always show up as External routes.
Note: From the perspective of router CK1 , all routes are EIGRP learned, since that is the only protocol running on this router. Although the AD of RIP is lower than external EIGRP routes, RIP is not being configured on CK1 so it will not learn this route via RIP.

QUESTION 15
The router topology for the multi-protocol Certkiller network is shown in the following exhibit:



The current configuration for Router CK1 , Router CK2 , Router CK3 , and Router CK4 are as follows:
Router CK1 :
interface loopback0
ip address 1.1.1.1 255.255.255.255
router eigrp 10
network 1.0.0.0
network 10.0.0.0
interface loopback1
ip address 4.4.4.4 255.255.255.255
Router CK2
router eigrp 10
network 10.0.0.0
network 20.0.0.0
no auto-summary
Router CK3
router ospf 10
network 30.30.30.0 0.0.0.255 area 0
network 40.40.40.0 0.0.0.255 area 0
Router CK4
router eigrp 10
redistribute connected metric 1400 230 1 255 1500
network 20.0.0.0
no auto-summary
router ospf 10
redistribute connected metric 100 subnets

network 40.40.40.0 0.0.0.255 area 0
router bgp 10
network 100.10.1.0 mask 255.255.255.0
neighbor 1.1.1.1 remote-as 10
neighbor update-source loopback
no auto-summary
Your newly appointed Certkiller trainee wants to know who owns the subnet 100.10.1.0/24 in the routing table of Router CK1 .
What would your reply be?

A. Router CK1 does not have this subnet in its routing table.
B. EIGRP
C. OSPF
D. BGP
E. RIP
F. It is there as a static route.

Answer: B

Explanation:
Routers CK1 , CK2 , and CK4 are all EIGRP neighbors with all relevant subnets advertised, so this route will show up as an EIGRP route.
Incorrect Answers:
C, D, E. Router CK1 is only running the EIGRP protocol, so the other routing protocols are completely ruled out.

QUESTION 16
Which of the following are Distance Vector routing protocols? (Choose all that apply)

A. OSPF
B. BGP
C. RIP version 1
D. ISIS
E. EIGRP
F. RIP version 2

Answer: C, E, F

Explanation:
Both RIP version 1 and RIP version 2 are distance vector protocols.
EIGRP is an enhanced distance vector protocol, relying on the Diffused Update Algorithm (DUAL) to calculate the shortest path to a destination within a network
Incorrect Answers:
A, D. OSPF and ISIS are link state routing protocols.

B. BGP is a path vector protocol, which is similar to a distance vector protocol, but with a key difference. A distance vector protocol chooses routes based on hop count, where BGP chooses routes that traverse the least number of Autonomous Systems, among other things.

QUESTION 17
As the administrator of the Certkiller network, you are planning to implement a dynamic routing protocol to replace the static routes. When comparing link state and distance vector routing protocols, what set of characteristics best describe Link-State routing protocols?

A. Fast convergence and lower CPU utilization
B. High CPU utilization and prone to routing loops
C. Slower convergence time and average CPU utilization
D. Fast convergence and greater CPU utilization
E. None of the above

Answer: D

Explanation:
Link State protocols, such as IS-IS and OSPF, converge more quickly than their distance vector counterparts, through the use of flooding and triggered updates. In link state protocols, changes are flooded immediately and computed in parallel.
Triggered updates improve convergence time by requiring routers to send an update message immediately upon learning of a route change. These updates are triggered by some event, such as a new link becoming available or an existing link failing.
The main drawbacks to Link State protocols are the amount of CPU overhead involved in calculating route changes and memory resources that are required to store neighbor tables, route tables, and a complete topology map.

QUESTION 18
A customer has a router with an interface connected to an OSPF network, and an interface connected to an EIGRP network. Both OSPF and EIGRP have been configured on the router. However, routers in the OSPF network do not have route entries in the route table for all of the routers form the EIGRP network. The default-metric under OSPF is currently set to 16. Based on this information, what is the most likely cause of this problem?

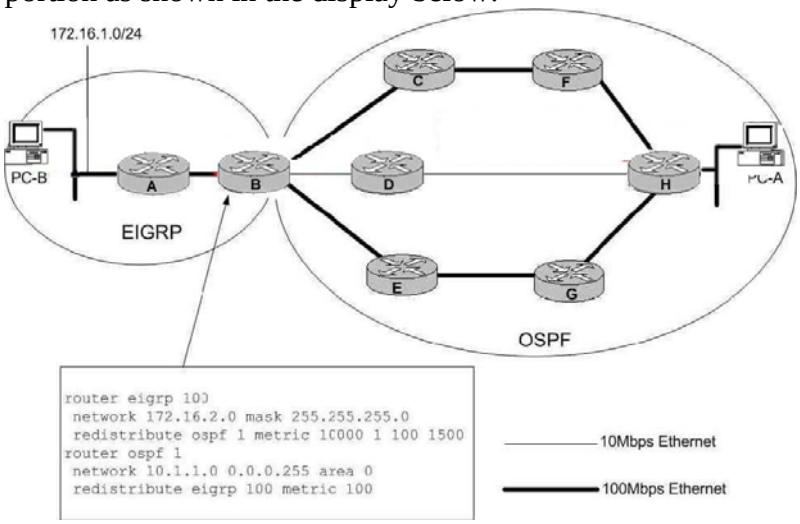
A. The 'subnets' keyword was not used under the OSPF process when redistributing EIGRP into OSPF.
B. EIGRP is configured as a Stub area, and therefore routes will not be redistributed unless a route-map is used to individually select the routes for redistribution.
C. The 'subnets' keyword was not used the EIGRP process when redistributing between OSPF into EIGRP.
D. The default metric for OSPF is set to 16, and therefore all EIGRP routes that are redistributed are assigned this metric, and are automatically considered unreachable by

EIGRP.
E. A metric was not assigned as part of the redistribution command for EIGRP routes redistributing into OSPF, and the default behavior is to assign a metric of 255, which is considered unreachable by OSPF.

Answer: A

Explanation:
When routes are redistributed into OSPF, only routes that are not subnetted are redistributed if the subnets keyword is not specified. It is generally a good idea to include the "subnets" keyword at all times when redistributing routes from other protocols into OSPF.
Incorrect Answers:
B. There is nothing in this question to lead us to believe that stub networks are being used at all. Even if they were, route maps would not be needed to redistribute the EIGRP and OSPF routes.
C. The "subnets" keyword needs to be placed under the OSPF process, not the EIGRP process.
D. EIGRP routes with a metric of 16 are acceptable, and not considered unreachable. If the routing protocol used was RIP instead of EIGRP then this would be true.
E. When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.

QUESTION 19
The Certkiller WAN consists of an OSPF network portion and an EIGRP routed portion as shown in the display below:



Given the network and OSPF configuration shown in the exhibit, what statement is true regarding traffic flowing from PC-A to PC-B?

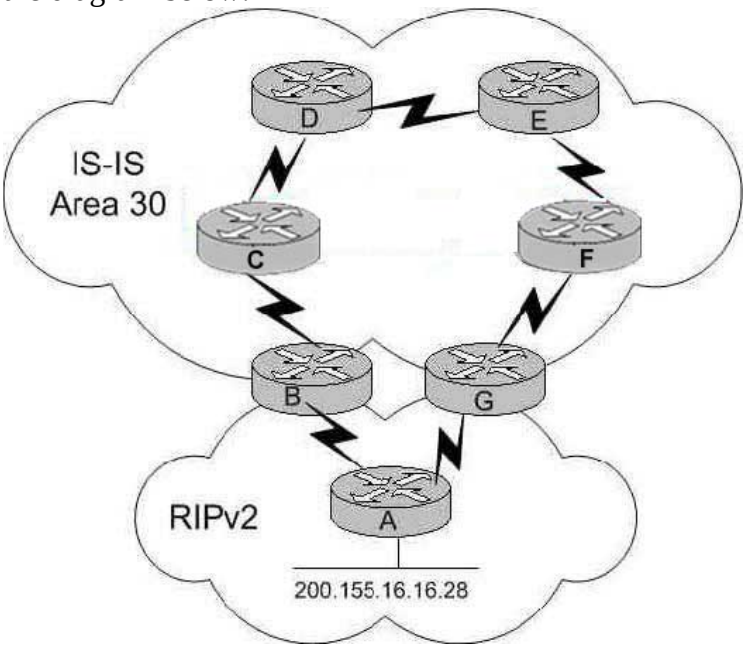
A. Traffic will only flow on the shortest, low-speed path, PC-A-H-D-B-A-PC-B.
B. Traffic will flow on both of the high speed paths (PC-A-H-F-C-B-A-PC-B and

PC-A-H-G-E-B-A-PC-B) but not the slow-speed path.
C. Traffic will flow on all three of the paths.
D. Traffic will flow uni-directionally on one of the high-speed paths form PC-A to PC-B, and uni-directionally on the other high-speed path from PC-B to PC-A.
E. Traffic will flow bi-directionally on only one of the high-speed paths, and the path selected will be based on the OSPF process IDs.

Answer: B

Explanation:
The default metric for OSPF is 100,000,000 divided by the bandwidth. For each 100 Mbps fast Ethernet link, the OSPF cost will be 1. For the slower, 10 Mbps Ethernet link, the OSPF cost will be 10, so the traffic will be routed around the slower link to the high speed links even though more hops are involved, because each high speed link across the entire OSPF cloud will have a total cost of 3 (1+1+1). This is true even though the redistributed routes are external type-2 routes. By default, OSPF will load balance traffic across up to four equal cost paths. Therefore, choice B is correct in that traffic will utilize both high speed links.

QUESTION 20
The Certkiller network is redistributing IS-IS and RIP version 2 routes as shown in the diagram below:



Routers B and G both advertise RIP learned routes into IS-IS. Network is added to Router A via an Ethernet port and Router B is the First router to learn about this new network. After the network has converged, what path will Router G take to reach network 200.155.16.16?

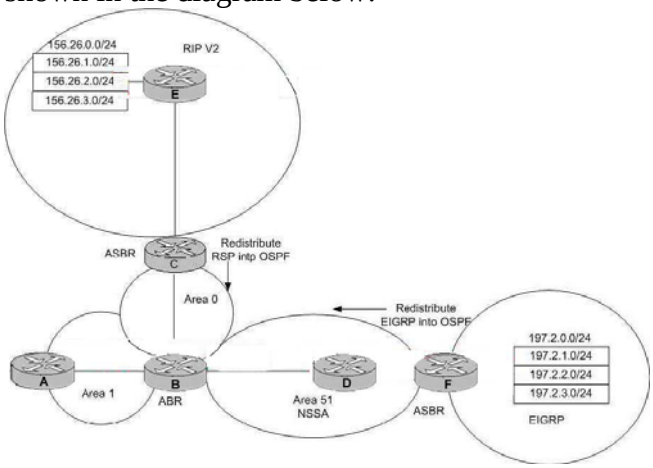
A. Router G takes the direct path through router A.
B. Router G takes the path through routers, F, E, D, C, B, A.

C. Router G will oscillate between the path through router A and the path through router F.
D. Router G and router B will both think the other router is the best path to network 200.155.16.16, causing a routing loop.
E. The answer can not be determined unless the default-metric used in the redistribution is known.

Answer: B

Explanation:
When a router receives identical route and subnet mask information for a given network from two different routing protocols, the route with the lowest administrative distance is chosen. IS-IS has a lower administrative Distance than RIP, so this route is installed in the routing table and used, even though it is obviously not the optimal route in this specific example.

QUESTION 21
The Certkiller network uses multiple IP routing protocols with redistribution, as shown in the diagram below:



Area 51 is configured as a NSSA Totally Stub, using the "area 51 stub no-summary" command. Which routers are in the routing table of Router D?

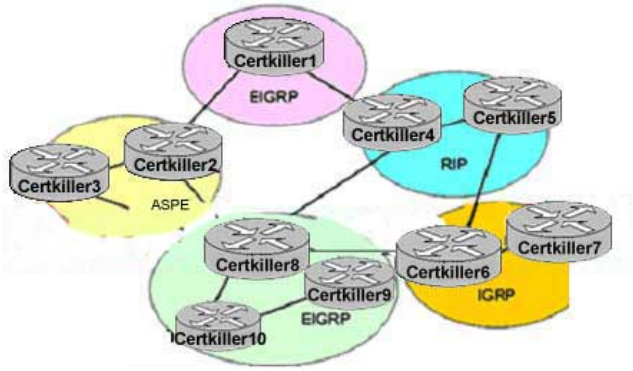
A. Redistributed EIGRP and RIP routes, one OSPF default route, OSPF inter and intra-area routes
B. Redistributed EIGRP routes and OSPF intra-area routes
C. Redistributed EIGRP routes and OSPF inter and intra-area routes
D. Redistributed EIGRP routes, an OSPF default route and OSPF intra-area routes
E. Redistributed EIGRP and RIP routes and an OSPF default route

Answer: D

Explanation:
In the network diagram above, Area 51 is defined as a totally NSSA stub area. EIGRP routes cannot be propagated into the OSPF domain because redistribution is not allowed

in the stub area. However, if we define area 51 as NSSA, we can inject EIGRP routes into the OSPF NSSA domain by creating type 7 LSAs. Redistributed RIP routes will not be allowed in area 51 because NSSA is an extension to the stub area. The stub area characteristics still exist, including no type 5 LSAs allowed.
There are two ways to have a default route in an NSS
A. When you configure an area as
NSSA, by default the NSSA ABR does not generate a default summary route. In the case of a stub area or an NSSA totally stub area, the NSSA ABR does generate a default summary route. In addition, all OSPF intra-area routes are allowed in a totally NSSA area.
Incorrect Answers:
A, E. The RIP will become external OSPF routes after the redistribution takes place. Since External OSPF routes from a different area are not injected into NSSA areas, no RIP routes will be seen on router D.
B. By making the not-so-stubby area a totally not-so-stubby area, a default route is injected, so D is the preferred choice over B.
C. Inter-area routes are not seen on routers within a totally NSSA.

QUESTION 22
The Certkiller network is displayed below:



Based on the information above, what path would router Certkiller 8 use to reach a network on router Certkiller 1? (Assume that mutual route redistribution takes place at all protocol boundaries)

A. Router Certkiller 8 takes the path through Certkiller 6.
B. Router Certkiller 8 takes the path through Certkiller 4.
C. Router Certkiller 8 takes the path through Certkiller 3.
D. Router Certkiller 8 takes the path through Certkiller 2.
E. None of the above.

Answer: A

Explanation:
Assuming that redistribution of routes is taking place on all routers, Certkiller 8 would receive multiple routes to the same network destination. Because of this, Certkiller 8 would choose to install the route with the lowest Administrative Distance into the routing

table. The default AD of the routes shown above is:
EIGRP: 90
IGRP: 100
OSPF: 110
RIP: 120
Therefore, router Certkiller 8 will go through the IGRP route via router Certkiller 6.

QUESTION 23
You need to make a new cable that is to be used for connecting a switch directly to another switch using Ethernet ports. What pinouts should be used for this cable?

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

Answer: A

Explanation:
Straight through cables are used when connecting PC hosts and router Ethernet ports to switches. Crossover cables are needed for switch to switch, and router to router connections. More information on crossover cables and their pinouts follows:

First Side of cable			**goesto**		**Second Side of cable**
Color	**Name**	**Pin**	**Pin**	**Name**	**Color**
White/ Orange	TX+	1	3	RX+	**White/** Orange
Orange	TX-	2	6	RX-	**Orange**
White/Green	RX+	3	1	TX+	
Green	RX-	6	2	TX-	**Green**

Blue	Extra Pins	4	4	Optional Pins (can be connected straight to same color pins). **But not used in transmission**	**Blue**
				.	
White/Blue	5		5	**White/Blue**	
White/Brown	7		7	**White/**Brown	
Brown	8		8	**Brown**	

Reference: http://www.infonewsindia.com/pinout/pinoutnetwork.html

---

QUESTION 24
The ITU-T Q.920 and ITU-T Q.921 drafts formally specify which protocol?

A. HDLC
B. PPP
C. LAPD
D. HSRP
E. LLC

Answer: C

Explanation:
The LAPD protocol is formally specified in ITU-T Q.920 and ITU-T Q.921.
Incorrect Answers:
A, D. HDLC and HSRP are both Cisco proprietary and are not formally specified in any ITU-T drafts.

QUESTION 25
What is the maximum transmit value for LLC flow control, as defined formally in the IEEE 802.2 LLC standard?

A. 15
B. 127
C. 256
D. 1023
E. 4096

Answer: B

Explanation:
According to the IEEE 802.2 Logical Link Control specification, the maximum transmit value for LLC flow control is 127. The LLC flow control techniques for bridged LANs is described as follows:
Overview:
This annex describes a technique, called dynamic window flow control, to control the offering of frames to the network by an LLC entity when congestion is detected or suspected. It is most effective in a bridged LAN. The technique is one of recovery from congestion and does not prevent congestion in a bridged LAN.It is not a substitute for proper network sizing. The method employs the transmit window already permitted by the standard to regulate the flow between two LLCs using the connection-mode service. Congestion in one direction of a logical link connection is treated independently of congestion in the other direction. The technique does not involve communication with the bridges, but rather relies on a simple algorithm implemented by the LLCs. MAC protocols are unaffected.All actions described in this annex apply to the station transmitting in the direction of the congestion. The receiver does not participate, except through normal LLC procedures, and does not require knowledge of the transmitter's participation. The service interface between the data link layer and the network layer is also unchanged.
Definitions
k: The transmit window size in use at any given time.
kmax: The maximum transmit window size, which is the maximum value that the transmit window k may have. The value of kmax shall not exceed 127.

QUESTION 26
Which is the proper signal for pin 6 of a PHY without an internal crossover MDI Signal according to the IEEE 802.3 CSMA/CD specification?

A. Receive +
B. Transmit +
C. Receive -
D. Transmit -
E. Contact 6 is not used.

Answer: C

Explanation:
The four pins that are used are 1, 2, 3, and 6 as shown below:

1 Rx+
2 Rx-
3 Tx+
6 Tx-
The table below shows the pin and corresponding signal for the RJ-45 connector pinouts.

RJ-45 Connector Pinout	
Pin	**Signal**
1	TX+
2	TX-
3	RX+
6	RX-

QUESTION 27
What is the standard transport protocol and port used for SYSLOG messages?

A. UDP 514
B. TCP 520
C. UDP 530
D. TCP 540
E. UDP 535

Answer: A

Explanation:
For a complete list of TCP/UDP well known port numbers, see the following link:
http://www.iana.org/assignments/port-numbers
UDP 514This port has been left open for use by the SYSLOG service.
TCP and UDP Ports:
In addition to the standard network ports, Cisco Works uses these TCP and UDP ports:

Port Number	Type	Description
42340	TCP	CiscoWorks2000 Daemon Manager, the tool that manages server processes

42342	UDP	Osagent
42343	TCP	JRun
42344	TCP	ANI HTTP server
7500	UDP	Electronic Switching System (ESS) Service port
7500	TCP	ESS Listening port
7580	TCP	ESS HTTP port
7588	TCP	ESS Routing port
1741	TCP	Port used for the CiscoWorks2000 HTTP
		server
161	UDP/TCP	Standard port for SNMP Polling
162	UDP/TCP	Standard port for SNMP Traps
514	**UDP**	**Standard port for SYSLOG**
69	TCP/UDP	Standard port for TFTP
23	TCP/UDP	Standard port for Telnet

References:
http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_tech_note09186a0080207605.shtml#udp
http://www.cisco.com/en/US/products/sw/cscowork/ps4737/products_tech_note09186a00800e2d78.shtml

---

QUESTION 28
A new Syslog server is being installed in the Certkiller network to accept network

management information. What characteristic applies to these Syslog messages? (Select three)

A. Its transmission is reliable.
B. Its transmission is secure.
C. Its transmission is acknowledged.
D. Its transmission is not reliable.
E. Its transmission is not acknowledged.
F. Its transmission is not secure.

Answer: D, E, F

Explanation:
Syslog is a method to collect messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Cisco devices can send their log messages to a Unix-style SYSLOG service. A SYSLOG service simply accepts messages, and stores them in files or prints them according to a simple configuration file. This form of logging is the best available for Cisco devices because it can provide protected long-term storage for logs. This is useful both in routine troubleshooting and in incident handling. Syslog uses UDP port 514. Since it is UDP based, the transmission is a best effort, and insecure.
Incorrect Answers:
A, C. Syslog uses UDP as the transport layer protocol, not TCP. Since UDP relies on an unreliable method of communication, syslog is not reliable.
B. Syslog has no way of providing a secure transmission by itself. Only by tunneling the syslog data through a secure channel such as IPSec can it be sent securely.

QUESTION 29
A user is having problems reaching hosts on a remote network. No routing protocol is running on the router and it's using only a default to reach all remote networks. An extended ping is used on the local router and a remote file server with IP address 10.5.40.1 is pinged. The results of the ping command produce 5 "U" characters. What does the result of this command indicate about the network?

A. An upstream router in the path to the destination does not have a route to the destination network.
B. The local router does not have a valid route to the destination network.
C. The ICMP packet successfully reached the destination, but the reply form the destination failed.
D. The ping was successful, but congestion was experienced in the path to the destination.
E. The packet lifetime was exceeded on the way to the destination host.

Answer: A

Explanation:

Even though the router is using a default route to get to all networks, at some point the packet is reaching a router that does not know how to reach the destination. The underlying reason for the failure is unknown, but when a ping is used and the response is a series of U replies, then the destination is unreachable by a router. Since the nearest router is using a default route, then the problem must be with an upstream router.
The table below lists the possible output characters from the ping facility:

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates the network server timed out while waiting for a reply.
U	A destination unreachable error PDU was received.
Q	Source quench (destination too busy).
M	Could not fragment.
?	Unknown packet type.
&	Packet lifetime exceeded.

Incorrect Answers:
B. The local router is using a default route, so all networks are considered to be known and reachable by the local router.
C. If the Ping packet could reach all the way to the remote host, a "U" response would not be generated.
D. This type of scenario would most likely result in a source quench response, which would be a Q.
E. This would mean a "&" response, as shown in the table above.

QUESTION 30
What protocols are considered to be UDP small servers? (Choose all that apply)

A. Echo
B. Daytime
C. Chargen
D. Discard
E. DHCP
F. Finger

Answer: A, C, D

Explanation:
TCP and UDP small servers are servers (daemons, in Unix parlance) that run in the router which are useful for diagnostics.
The UDP small servers are:
1. Echo: Echoes the payload of the datagram you send.
2. Discard: Silently pitches the datagram you send.
3. Chargen: Pitches the datagram you send and responds with a 72 character string of ASCII characters terminated with a CR+LF.
These 3 servers are enabled when the "service UDP-small-servers" command.
Reference:
http://www.cisco.com/warp/public/66/23.html
Incorrect Answers:
B. Daytime: Returns system date and time, if correct. It is correct if you are running Network Time Protocol (NTP) or have set the date and time manually from the exec level. The command to use is telnet x.x.x.x daytime. Daytime is a TCP small server.
E. Although DHCP uses UDP, it is not considered a UDP small server by Cisco.
F. The router also offers finger service and async line bootp service, which can be independently turned off with the configuration global commands no service finger and no ip bootp server, respectively. This is in addition to the TCP and UDP small servers.

QUESTION 31
Which protocols are considered to be TCP small servers? (Choose all that apply).

A. Echo
B. Time
C. Daytime
D. Chargen
E. Discard
F. Finger
G. DHCP

Answer: A, C, D, E

Explanation:
TCP and UDP small servers are servers (daemons, in Unix parlance) that run in the router which are useful for diagnostics.
TCP Small Servers are enabled with the service tcp-small-servers command
The TCP small servers are:
* Echo: Echoes back whatever you type by using the telnet x.x.x.x echo command.
* Chargen: Generates a stream of ASCII data. The command to use is telnet x.x.x.x chargen.
* Discard: Throws away whatever you type. The command to use is telnet x.x.x.x discard.

* Daytime: Returns system date and time, if correct. It is correct if you are running Network Time Protocol (NTP) or have set the date and time manually from the exec level. The command to use is telnet x.x.x.x daytime.
Replace x.x.x.x with the address of your router. Most routers inside Cisco run the small servers.
Incorrect Answers:
F. DHCP is not considered a UDP small server by Cisco.
G. The router also offers finger service and async line bootp service, which can be independently turned off with the configuration global commands no service finger and no ip bootp server, respectively. This is in addition to the TCP and UDP small servers.

QUESTION 32
Which of the following statements are NOT true regarding the TCP sliding window protocol? (Choose all that apply)

A. It allows the transmission of multiple frames before waiting for an acknowledgement.
B. The size of the sliding window can only increase or stay the same.
C. The initial window offer is advertised by the sender.
D. The receiver must wait for the window to fill before sending an ACK.
E. The sender need not transmit a full window's worth of data.
F. The receiver is required to send periodic acknowledgements.

Answer: B, C

Explanation:
The sliding window algorithm allows for the window size to decrease slowing down the transmission of data. TCP uses a window of sequence numbers to implement flow control. The receiver indicates the amount of data to be sent. The receiver sends a window with every ACK that indicates a range of acceptable sequence numbers beyond the last received segment. The window allows the receiver to tell the sender how many bytes to transmit. Therefore, the statements in B and C are not true (the question asked for the false statements, not the true ones).
Incorrect Answers:
A, F. In TCP, a sender transmits only a limited amount of data before the receiver must send an acknowledgement. Windows usually include multiple packets, but if the sender doesn't get acknowledgements within a set time, all the packets must be retransmitted.
D, E. Both of these are true statements regarding the TCP sliding window mechanism.
Additional Info:
In Win 2000 and XP, the default TCP window size is 16K bytes - meaning no more than 11 frames can be outstanding without an acknowledgement. For 11 frames at 12 microseconds each, any delay of 132 microseconds or more would cause retransmissions.

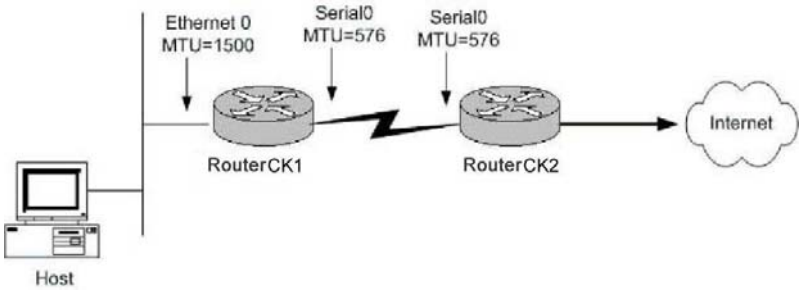
QUESTION 33
A new data T1 line is being installed. What choices do you have for provisioning the framing types? (Choose all that apply)

A. B8ZS
B. SF
C. AMI
D. LLC
E. ESF
F. All of the above

Answer: B, E

Explanation:
SuperFraming and Extended SuperFraming are the two T1 framing types.
Incorrect Answers:
A, C. B8ZS and AMI are coding options and are not used for framing. Two typical combinations that T1's are provisioned are B8ZS/ESF and AMI/SF.
D. LLC (Logical Link Control) is not related to T1.

QUESTION 34
The Certkiller network is shown in the following exhibit:



The host sends a 1500 byte TCP packet to the Internet with the DF (Don't Fragment) bit set.
Will router CK1 be able to forward this packet to router CK2 ?

A. Yes, it will ignore the DF bit and fragment the packet because routers do not recognize the DF bit.
B. Yes, it will forward the packet without fragmenting it because the DF bit is set.
C. No, it will drop the packet and wait for the host to dynamically decrease its MTU size.
D. Yes, it will fragment the packet, and send back ICMP type 3 code 4 (fragmentation needed but DF bit set) messages back to the host.
E. No, it will drop the packet, and send back ICMP type 3 code 4 (fragmentation needed but DF bit set) message back to the host.

Answer: E

Explanation:
Since the DF bit in the IP packet is set, the router will not be allowed to fragment the packet. Also the MTU size on the routers serial interface is restricted to 576, hence the packet will not be allowed to pass through and it will be dropped.
Incorrect Answers:

A. Routers do indeed recognize the DF bit and will adhere to it.
B. With the DF bit set, the packet will not be fragmented, and since 1500 bytes is too large to go through the 576 byte interface, it will be dropped.
C. In this case, router will always send an ICMP error code back to the source stating what the problem is before dropping it.
D. With the DF bit set the router is not allowed to fragment the packet.

QUESTION 35
With regard to TCP headers, what control bit tells the receiver to reset the TCP connection?

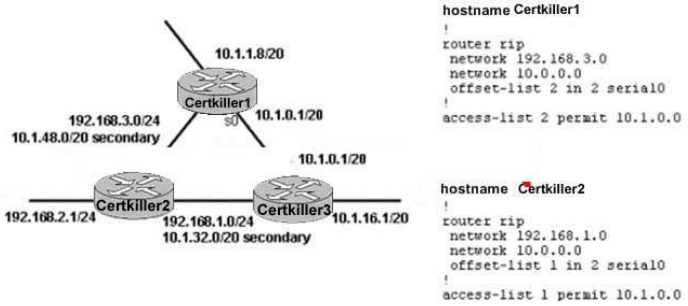
A. ACK
B. SYN
C. SND
D. PSH
E. RST
F. CLR

Answer: E

Explanation:
The RST flag resets the TCP connection.
Incorrect Answers:

A. ACK is used to acknowledge data that has been sent.
B. SYN is used to synchronize the sequence numbers.
C. SND is not a TCP control bit.
D. PSH is used to tell the receiver to pass the information to the application.
F. CLR is not a valid TCP control bit.

QUESTION 36
The Certkiller RIP network is displayed below:




```
hostname Certkiller1
!
router rip
 network 192.168.3.0
 network 10.0.0.0
 offset-list 2 in 2 serial0
!
access-list 2 permit 10.1.0.0
```

```
hostname Certkiller2
!
router rip
 network 192.168.1.0
 network 10.0.0.0
 offset-list 1 in 2 serial0
!
access-list 1 permit 10.1.0.0
```

What statement is correct regarding the configuration in the figure?

A. The RIP metric between Certkiller 1 and Certkiller 3 remains "1".
B. The RIP metric between Certkiller 1 and Certkiller 3 is "2" because the offset-list command is changing the metric to "2".
C. The RIP metric between Certkiller 1 and Certkiller 3 is "3" because the offset-list

command is changing the metric to "3" by adding 2 to the existing metric.
D. The RIP metric cannot be changed and Load sharing will be done between the two paths that exist from Certkiller 1 and Certkiller 3 (and vice-versa) because the offset-list command is specifying that there be a 2:1 load sharing ratio for the two paths.

Answer: C

Explanation:
The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric. In this case, an offset of 2 is added to the routing update, making the total RIP metric 3.

QUESTION 37
Router CK1 is running BGP as well as OSPF. You wish to redistribute all OSPF routes into BGP. What command do you need to change to ensure that ALL available OSPF networks are in the BGP routing table?

A. redistribute ospf 1 match external
B. redistribute ospf 1 match external 1
C. redistribute ospf 1 match external all internal all
D. redistribute ospf 1 match internal all external 1 external 2
E. redistribute ospf 1 match internal external 1 external 2
F. None of the above

Answer: E

Explanation:
In this case, all OSPF routes are redistributed into BGP by using both the internal and external keywords, as shown in this Router configuration:
router bgp 100
redistribute ospf 1 match internal external 1 external 2
Reference:
http://www.cisco.com/en/US/tech/ CK3 65/technologies_tech_note09186a00800943c5.shtml

---

QUESTION 38
You wish to copy a file from a server into router CK1 . Which of the following IOS "copy" commands is NOT valid?

A. copy tftp: flash:
B. copy tftp flash
C. copy tftp\\flash\\
D. copy tftp: //flash:\\

Answer: C

Explanation:
The following are valid copy commands:
/erase Erase destination file system.
bootflash: Copy from bootflash: file system
flash: Copy from flash: file system
ftp: Copy from ftp: file system
null: Copy from null: file system
nvram: Copy from nvram: file system
rcp: Copy from rcp: file system
system: Copy from system: file system
tftp: Copy from tftp: file system
The most common use of the copy command is the copy tftp flash command. The full syntax is copy tftp: flash: "flash file name."

QUESTION 39
On router CK1 the IOS command "ospf auto-cost reference-bandwidth 500" command was configured. Based on this, what will be the OSPF metric for a Fast Ethernet interface on router CK1 ?

A. 1
B. 5
C. 50
D. 500
E. 5000
F. 50000
G. None of the above

Answer: B

Explanation:
In Cisco IOS Release 10.3 and later releases, by default OSPF will calculate the OSPF metric for an interface according to the bandwidth of the interface. For example, a 64K link will get a metric of 1562, and a T1 link will have a metric of 64.
The OSPF metric is calculated as the ref-bw value divided by the bandwidth, with ref-bw equal to 108 by default, and bandwidth determined by the bandwidth (interface) command. The calculation gives FDDI a metric of 1.
If you have multiple links with high bandwidth (such as FDDI or ATM), you might want to use a larger number to differentiate the cost on those links.
Note: The value set by the "ip ospf cost" command overrides the cost resulting from the auto-cost command.
Example:
The following example changes the cost of the Fast Ethernet link to 5, while the gigabit Ethernet link remains at a cost of 1. Thus, the link costs are differentiated.
router ospf 1
auto-cost reference-bandwidth 500

In this example, the OSPF cost is found by taking the reference bandwidth and dividing it by the bandwidth of the link, which is 100 Mbps for Fast Ethernet (500/100) = 5.

QUESTION 40
On your Terminal Server you are seeing spurious signals on line 6 of an asynchronous port due to contention issues. What command will fix this issue?

A. flowcontrol hardware
B. transport input none
C. no exec
D. exec-timeout 0 0

Answer: C

Explanation:
The "no exec" command is an optional command for reverse telnet configurations. Adding this line lessons the likelihood of contention over the asynchronous port. An executive process exists on all lines and buffer data to each other. At times, it can make it difficult to use a reverse telnet session. The command "no exec" will fix this.
Incorrect Answers:

A. Console ports do not use flow control. If the terminal server is connecting to Cisco console ports then the "Flowcontrol hardware" would have no bearing.
B. This will fundamentally cut off all telnet and reverse telnet traffic from the line.
D. This will disable the timeout value, but will not fix problems relating to spurious signals and contention issues.

QUESTION 41
From the IOS command line interface, you accidentally press the Esc B keys while typing in a configuration line. What is the result of this action?

A. The cursor will move to the beginning of the entire command
B. The cursor will move back one character.
C. The cursor will move back one word
D. The cursor will remain in the same location.
E. Noting, this is not a valid shortcut.

Answer: C

Explanation:
The following table describes the different shortcut options and functions that are available from the Cisco Command Line Interface:

Keystroke	Function

Ctrl-A	Jumps to the first character of the command line.
Ctrl-B or the left arrow key	Moves the cursor back one character.
Ctrl-C	Escapes and terminates prompts and tasks.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Jumps to the end of the current command line.
Ctrl-F or the right arrow key1	Moves the cursor forward one character.
Ctrl-K	Deletes from the cursor to the end of the command line.
Ctrl-L; Ctrl-R	Repeats current command line on a new line.
Ctrl-N or the down arrow key1	Enters next command line in the history buffer.
Ctrl-P or the up arrow key1	Enters previous command line in the history buffer.
Ctrl-U; Ctrl-X	Deletes from the cursor to the beginning of the command line.
Ctrl-W	Deletes last word typed.
Esc B	Moves the cursor back one word.
Esc D	Deletes from the cursor to the end of the word.
Esc F	Moves the cursor forward one word.

Delete key or Backspace key	Erases mistake when entering a command; re-enter command after using this key.

Incorrect Answers:

A. This will be the result of the Ctrl-A command.
B. This will be the result of the Ctrl-B command, not Esc B.

QUESTION 42
Which command will display both the local and all remote SNMP engine Identification information?

A. Show SNMP ID
B. Show engine
C. Show SNMP engineID
D. Show SNMP engine ID
E. Show SNMP stats
F. Show SNMP mib
G. Show SNMP users

Answer: C

Explanation:
The following is a sample output from a Cisco router:
Certkiller #show snmp ?
mib show mib objects context
engineID show local and remote SNMP engine IDs
group show SNMPv3 groups
pending snmp manager pending requests
sessions snmp manager sessions
stats show snmp statistics
user show SNMPv3 users
| Output modifiers
<cr>
Certkiller #
Reference: CCO login required.
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a

---

QUESTION 43
What would occur as a result of the clear ip route * command being issued? (Choose two)

A. A router would recalculate its entire table and re-establish its neighbor relationships.
B. A router would recalculate its entire routing table but its neighbor relationship would not be affected.
C. Only link state routing protocols would be recalculated and only those neighbor relationships re-established.
D. Only the routing table would be recalculated.
E. Only its neighbor relationship would be re-established.

Answer: B, D

Explanation:
The use of the * means that all routing table entries will be deleted within the routing table, forcing the router to calculate a new routing table. The underlying neighbor adjacencies are not affected by this command. To force the router to re-establish neighbor relationships, the "clear ip xxx neighbor" command, where xxx is the routing protocol in use. For example, to clear all of the OSPF neighbor relationships, use the "clear ip ospf neighbor" command.

QUESTION 44
Which IOS example will configure a remote user in a group called remotegroup to receive traps at the v3 security model and the authNoPriv security level?

A. snmp engineid remote 16.20.11.14 000000100a1ac151003
snmp enable traps config
snmp manager
B. snmp-server group remotegroup v3 noauth
snmp-server user remote remotegroup remote 16.20.11.14 v3
snmp-server host 16.20.11.14 inform version 3 noauth remoteuser config
C. snmp-server group remotegroup v3 noauth
snmp-server user remoteAuthUser remoteAuthGroup remote 16.20.11.14 v3 auth md5 password1
D. snmp-server group remotegroup v3 priv
snmp-server user remote PrivUser remotePrivGroup remote 16.20.11.14 v3 auth md5 password1 priv des56 password2

Answer: B

Explanation:
snmp-server user:
To configure a new user to a Simple Network Management Protocol group, use the snmp-server user global configuration command. To remove a user from an SNMP group, use the no form of the command.
snmp-server user username [groupname remote ip-address [udp-port port] {v1| v2c | v3}[encrypted][auth {md5 | sha}auth-password [priv des56 priv password]] [access access-list]
no snmp-server user

Syntax Description

username	The name of the user on the host that connects to the agent.
groupname	(Optional) The name of the group to which the user is associated.
remote	(Optional) Specifies the remote copy of SNMP on the router.
ip-address	(Optional) The IP address of the device that contains the remote copy of SNMP.
udp-port	(Optional) Specifies a UDP port of the host to use.
port	(Optional) A UDP port number that the host uses. The default is 162.
v1	(Optional) The least secure of the possible security models.
v2c	(Optional) The second least secure of the possible security models. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
v3	(Optional) The most secure of the possible security models.
encrypted	(Optional) Specifies whether the password appears in encrypted format (a series of digits, masking the true characters of the string).
auth	(Optional) Initiates an authentication level setting session.

md5	(Optional) The HMAC-MD5-96 authentication level.
sha	(Optional) The HMAC-SHA-96 authentication level.
auth-password	(Optional) A string (not to exceed 64 characters) that enables the agent to receive packets from the host.
priv	(Optional) The option that initiates a privacy authentication level setting session.
des56	(Optional) The CBC-DES privacy authentication algorithm.
priv password	(Optional) A string (not to exceed 64

Incorrect Answers:

A. The SNMP engineid is an invalid command.
C, D. In these examples, the MD5 authentication level is used. In this question we want the user to use no authentication.

QUESTION 45
You want to refresh the routing table of CK1 . What command will clear all routes from a routing table on this Cisco router?

A. clear ip route all
B. clear ip route
C. clear all route ip
D. clear ip route neighbor
E. None of the above

Answer: E

Explanation:
To delete all of the routing entries, the "*" keyword must be added to the "clear ip route" statement. The correct syntax would be "clear ip route *".
To delete routes from the IP routing table, use the clear ip route EXEC command.

clear ip route {network [mask] | *}
Syntax Description

network	Network or subnet address to remove.
mask	(Optional) Subnet address to remove.
*	Removes all routing table entries.

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a008023

QUESTION 46
The Certkiller network has a number of routers with very high speed interfaces, and you want to ensure that this is reflected in the OSPF process. What IOS command would be used to reset the cost calculation process so that high-speed interfaces can be correctly calculated?

A. (config-if)#ip ospf cost xxx
B. (config-if)# ip ospf interface-speed xxx
C. (config-if)# ip ospf auto-cost reference-bandwidth xxx
D. (config-router)# ospf auto-cost reference-bandwidth xxx
E. (config)# ip ospf auto-cost reference-bandwidth xxx

Answer: D

Explanation:
You can change the reference bandwidth in Cisco IOS Software Release 11.2 and later using the ospf auto-cost reference-bandwidth command under router ospf. By default, reference bandwidth is 100 Mbps.
To control how OSPF calculates default metrics for the interface, use the ospf auto-cost command in router configuration mode.
Syntax Description

reference-bandwidthref-bw	Rate in megabits per second
	(bandwidth). The range is 1 to
	4294967; the default is 100.

Defaults
100 megabits per second

Command Modes
Router configuration
Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines
In Cisco IOS Release 10.3 and later, by default OSPF will calculate the OSPF metric for an interface according to the bandwidth of the interface. For example, a 64K link will get a metric of 1562, and a T1 link will have a metric of 64.
The OSPF metric is calculated as ref-bw divided by bandwidth, with ref-bw equal to 108 by default, and bandwidth determined by the bandwidth command. The calculation gives FDDI a metric of 1.
If you have multiple links with high bandwidth (such as FDDI or ATM), you might want to use a larger number to differentiate the cost on those links.
The value set by the ip ospf cost command overrides the cost resulting from the auto-cost command.
Examples
The following example changes the cost of the FDDI link to 10, while the gigabit Ethernet link remains at a cost of 1. Thus, the link costs are differentiated.
router ospf 1
ospf auto-cost reference-bandwidth 1000

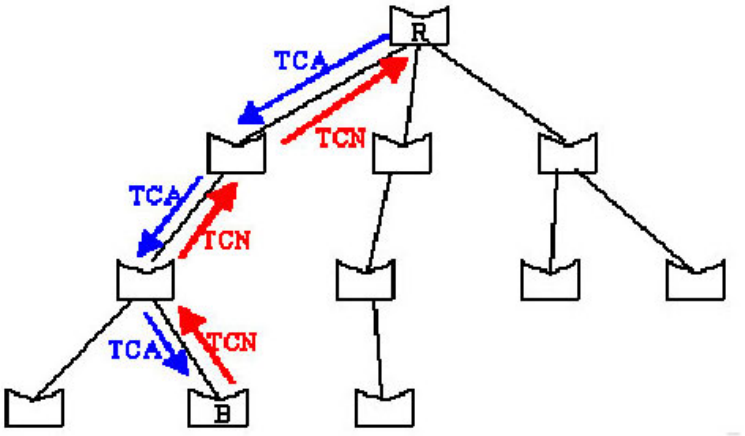
QUESTION 47
In a bridged LAN, the number if BPDU's with the TCA bit set is incrementing rapidly. What could be the cause of this? (Choose all that apply).

A. BPDU's with the TCA bit set is part of the normal operation of a bridged LAN.
B. Improper cabling is being used in the network.
C. There is no spanning tree portfast configured on the ports connecting 2 workstations.
D. The root switch is experiencing problems due to high CPU utilization and is not sending any BPDUs.
E. None of the above.

Answer: B, C

Explanation:
In normal STP operation, a bridge keeps receiving configuration BPDUs from the root bridge on its root port, but it never sends out a BPDU toward the root bridge. So, in order to achieve that, a special BPDU called the topology change notification (TCN) BPDU has been introduced. Thus, when a bridge needs to signal a topology change, it starts sending TCNs on its root port. The designated bridge receives the TCN, acknowledges it,

and generates another one for its own root port. And so on until the TCN hits the root bridge.



Bridge B notifies a topology change by sending a TCN on its root port. The TCN is acknowledged and forwarded up to the root bridge R.

The TCN is a very simple BPDU that contains absolutely no information that a bridge sends out every hello_time seconds (this is locally configured hello_time, not the hello_time specified in configuration BPDUs). The designated bridge acknowledges the TCN by immediately sending back a normal configuration BPDU with the topology change acknowledgement (TCA) bit set. The bridge notifying the topology change will not stop sending its TCN until the designated bridge has acknowledged it, so the designated bridge answers the TCN even though it does not receive configuration BPDU from its root.
The portfast feature is a Cisco proprietary change in the STP implementation. The command is applied to specific ports and has two effects:
1. Ports coming up are put directly in the forwarding STP mode, instead of going through the learning and listening process. Note that STP is still running on ports with portfast.
2. The switch never generates a TCN when a port configured for portfast is going up or down.
Reference:
http://www.cisco.com/en/US/tech/ CK3 89/ CK6 21/technologies_tech_note09186a0080094797.shtml#portfastcomma

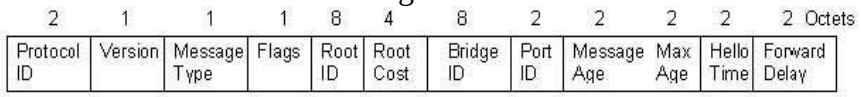
---

QUESTION 48
The Certkiller LAN is a bridged network running the 802.1D spanning tree protocol. Which of the following are paramenters that a bridge will receive from the root bridge.

A. Maxage
B. Root Cost
C. Forward delay
D. A,B, and C
E. None of the above

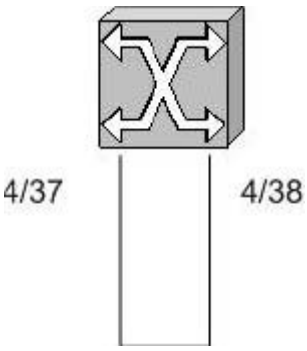
Answer: D

Explanation:
A, B and C are all located in the BPDU which each switch gets from the root bridge.
The BPDUs are in the following format:



1. Protocol ID - indicates that the packet is a BPDU.
2. Version - the version of the BPDU being used.
3. Message Type - the stage of the negotiation.
4. Flags - two bits are used to indicate a change in topology and to indicate acknowledgement of the TCN BPDU.
5. Root ID - the root bridge priority (2 bytes) followed by the MAC address (6 bytes).
6. Root Path Cost - the total cost to from this particular bridge to the designated root bridge.
7. Bridge ID - the bridge priority (2 bytes) followed by the MAC address (6 bytes), lowest value wins! The default bridge priority is 0x8000 (3276810).
8. Port ID - the ID of the port from which are transmitted the BPDUs, a root port, this is made up of the configured port priority and the bridge MAC address.
9. Message Age - timers for aging messages (only has effect on the network if the root bridge is configured with this parameter).
10. Maximum Age
- the maximum message age before information from a BPDU is dropped because it is too old and no more BPDUs have been received. (only has effect on the network if the root bridge is configured with this parameter). The default value for this is 20 seconds.
11. Hello Time - the time between BPDU configuration messages sent by the root bridge (only has effect on the network if the root bridge is configured with this parameter). The default value for this is 2 seconds.
12. Forward Delay - this temporarily stops a bridge from forwarding data to give a chance for information of a topology change to filter through to all parts of the network. This means that ports that need to be turned off in the new topology have a chance to be switched off before the new ports are turned on (only has effect on the network if the root bridge is configured with this parameter).
Reference:
http://www.rhyshaden.com/ethernet.htm

QUESTION 49
A small office LAN contains only one switch, which was put in place without any of the default configurations changed. You have noticed that somebody in the office has looped a cable by connecting one end to port 4/37 and the other to port 4/38 as shown below:
All links are 10/100
Configuration is default



Which of the following statements is true?

A. Port 4/38 will be blocked.
B. Both ports will be forwarding.
C. Port 4/37 will be blocking.
D. Both ports will be blocked.
E. Port 4/38 will continuously move between the listening and learning states.
F. Port 4/37 will be stuck in the learning state.

Answer: A

Explanation:
Port priority is based on lowest priority, and lowest port number. Because of this, then 4/37 would become the root port and 4/38 would be blocking. The default mode of a Catalyst switch is to enable the STP process for all VLANs.
Incorrect Answers:
B. Even though this switch will effectively become the root switch, and all ports in a root switch should be in the "forwarding state" a loop will occur in this case, and so one of the ports must be blocking. Since the priority of 4/38 is lower by default, it will be blocking.

QUESTION 50
Which of the following statements regarding Transparent Bridge tables are FALSE? (Choose all that apply.)

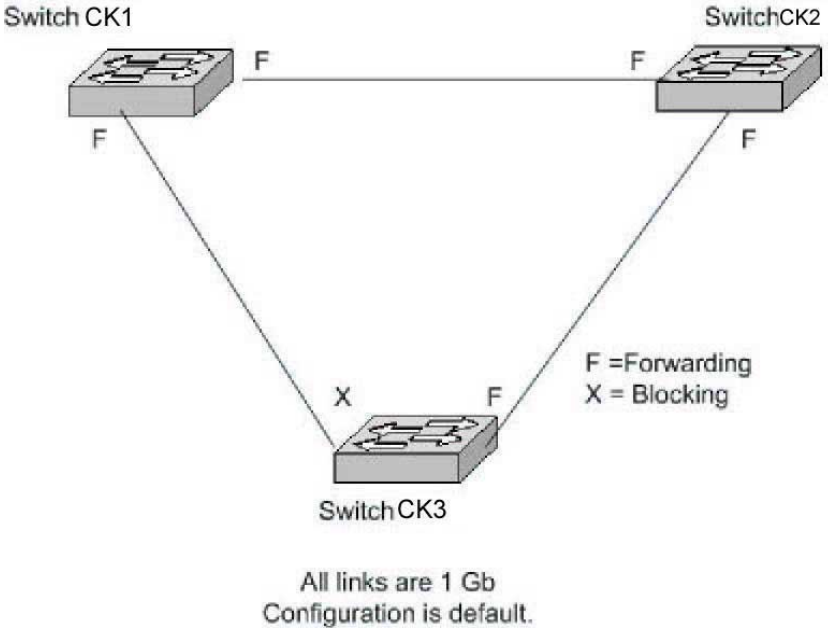
A. Decreasing the bridge table aging time would reduce flooding.
B. Increasing the bridge table aging time would reduce flooding.
C. Bridge table entries are learned by way of examining the source MAC address of each frame.
D. Bridge table entries are learned by examining destination MAC addresses of each frame.
E. The bridge aging time should always be more than the aggregate time for detection and recalculation of the spanning tree.

Answer: A, D

Explanation:
Basic fundamental behind TB is to learn the network topology by means of storing the

source MAC address of a packet, and the corresponding interface from which the packet came in on the network. This information is stored in the bridge table. To keep the bridge table small and manageable entries are deleted after a specified period of time, known as bridge table aging time. Once an entry is removed from the bridge table, and a packet arrives for which the information is no longer there in the bridge table, the packet will be flooded out of all interfaces except the interface on which it was received.
An increase in the bridge table aging time will reduce flooding.
Incorrect Answers:
B. Increasing the aging table time will indeed reduce the flooding, since the source MAC addresses are cached for a longer period of time.
C. This statement is also true. Bridge tables are built by looking at the source MAC address to learn which stations are attached to the bridge ports.
E. The aging time should indeed be longer than the convergence time for the spanning tree algorithm in order to prevent information from timing out and being re-learned, which will just begin the STP process again.

QUESTION 51
The Certkiller network is shown in the following exhibit:



You issue the "set spantree root 1" command on Switch CK1 . What will happen as a result of this change? (Choose all that apply).

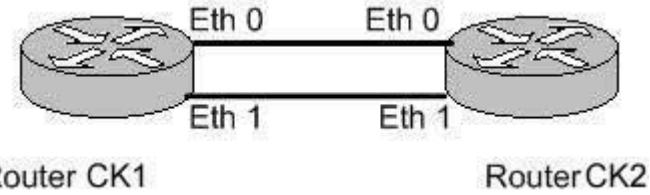
A. No other switch in the network will be able to become root as long as Switch CK1 remains up and running in this topology.
B. Switch CK1 will change its Spanning Tree priority to become the root for Vlan 1, only.
C. The port that used to be blocking on Switch CK3 will be changed to forwarding.
D. The link between Switch CK1 and Switch CK2 will remain forwarding throughout the reconvergence of the Spanning Tree domain.

Answer: B, C

Explanation:
The syntax specified in this question only makes CK1 root
for Vlan 1 only.
The set spantree root {vlan_id} command sets the priority of
the switch to 8192 for the VLAN or VLANs specified in
{vlan_id} .
Note:The default priority for switches is 32768. This command setting means that the Certkiller switch will be selected as the root switch because it has the lowest priority.
Certkiller -Switch> (enable) set spantree root 1
VLAN 1 bridge priority set to 8192.
VLAN 1 bridge max aging time set to 20.
VLAN 1 bridge hello time set to 2.
VLAN 1 bridge forward delay set to 15.
Switch is now the root switch for active VLAN 1.
Certkiller -Switch> (enable)
Because Switch 1 will become the root, the link between CK 3 and CK 1 will be forwarding, which means the link between CK2 and CK3 will change from forwarding to blocking.
Incorrect Answers:

A. It is important to remember that the "set spantree root" command merely changes the spanning tree switch priority from 32768 to 8192 so that it is much more likely to become the root for the particular VLAN. If another switch already has a priority lower than 8192, then this command will make the switch the root by lowering it to one below the existing value. For example, if another switch is already configured with a priority of 8192, then issueing the "set spantree root" command will configure the new switch with a priority of 8191. However, another switch could still become the root if it were configured with a lower priority after this command was issues on another switch.
D: After the "set span root 1" command is set, CK1 will send a PDU to CK2 and a new STP election will occur. During this time, the port will transition into the blocking, listening, and learning states and during this time the forwarding of traffic will be temporarily halted.
Reference: Cisco LAN Switching, Clark and Hamilton, Cisco Press, Page 197.

QUESTION 52
The Certkiller network consists of only 2 routers as below:



You perform the following router configurations:
Router CK1 :
no ip routing

!
interface Ethernet 0
no ip address
bridge-group 1
!
interface Ethernet 1
no ip address
bridge-group 1
!
bridge 1 protocol ieee
Router CK2 :
no ip routing
!
interface Ethernet 0
no ip address
bridge-group 2
!
interface Ethernet 1
no ip address
bridge-group 2
!
bridge 2 protocol ieee
bridge 2 priority 63500
Based on this configuration, which router will become the root, and which ports will be forwarding?

A. Router CK2 will become the root.
One port on Router CK1 will be forwarding, and the other will be blocking.
One port on Router CK2 will be forwarding, and the other will be blocking.
B. Both Router CK1 and Router CK2 will become the root in an independent spanning tree.
All ports on Router CK1 and Router CK2 will be forwarding.
C. Router CK1 will become the root.
Both ports on Router CK1 will be forwarding.
Both ports on Router CK2 will be forwarding.
D. Router CK2 will become the root.
Both ports on Router CK1 will be forwarding.
One port on Router CK2 will be forwarding, and the other will be blocking.
E. Router CK1 will become the root.
Both ports on Router CK1 will be forwarding.
One port on Router CK2 will be forwarding, and the other will be blocking.

Answer: E

Explanation:
Bridge 1's priority is at default 32768, Bridge 2 is at 63500, Bridge 1 (with a lower

Bridge ID) will be Root Bridge. All ports on the root bridge are always in forwarding state, hence both the ports on Bridge 1 will be in forwarding state. As per STP any other Bridge can only have one connection to the Root Bridge in the forwarding state, hence only one port on Bridge 2 will be forwarding.
Incorrect Answers:
A, D. CK2 has a bridge priority configured as 63500, while CK1 is left with the default. Since the default value is 32768 and lower is preferred, CK1 will become the root.
C. Only the single root port will be forwarding.

QUESTION 53
What spanning-tree protocol timer determines how often the root bridge send configuration BDPUs?

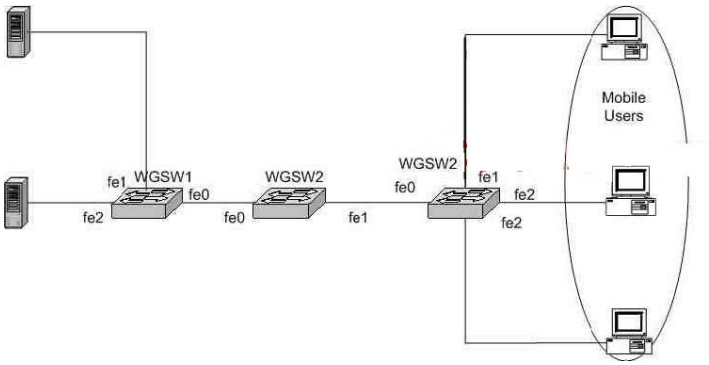
A. STP Timer
B. Hold Timer
C. Hello Timer
D. Max Age Timer
E. Forward Delay Timer

Answer: C

Explanation:
The STP Hello Time is the time between each Bridge Protocol Data Unit (BPDU) that is sent on a port. This is equal to two seconds by default, but can be tuned to be between one and ten seconds.
Incorrect Answers:

A. The Max Age, Forward Delay, and Hello Timers are all considered to be STP timers.
B. Hold timers are used in routing protocols to avoid inconsistent information and loops, but they are not an STP timer.
D. The Max Age Timer controls the maximum length of time a bridge port saves its configuration BPDU information. This is 20 seconds by default and can be tuned to be between six and 40 seconds.
E. The Forward Delay Timer is the time spent in the listening and learning state. This is by default equal to 15 seconds, but can be tuned to be between four and 30 seconds.

QUESTION 54
The Certkiller network topology is displayed below:



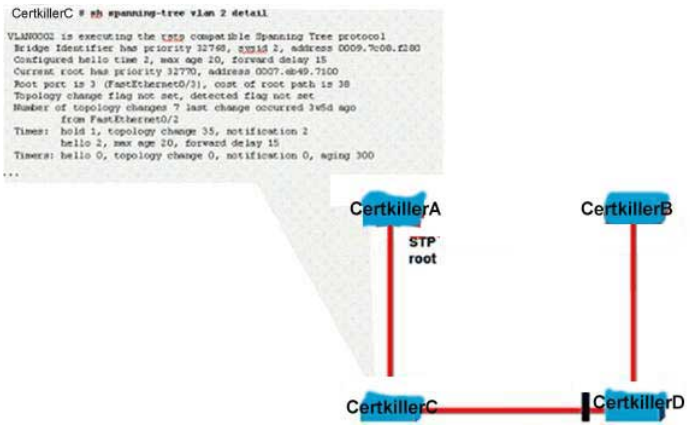
WGSW3 has been set up to provide access to mobile users in a conference room. Portfast has been enabled on all access ports. The following command is entered on WGSW3:
Switch(config)#spanning-tree portfast bpduguard
What happens if a switch or bridge is connected to one of the access ports?

A. Any access port that receives a BDPU packet will be disabled.
B. The access port will reject any BDPU packets that they receive.
C. Portfast will be disabled on any access port that receives a BDPU packet.
D. The bridge can join the BDPU topology, but it is blocked form becoming the root bridge.
E. Only BDPU packets that are NOT superior to the current root bridge will be accepted on the access port.

Answer: A

Explanation:
The STP portfast BPDU guard enhancement is designed to allow network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports with STP portfast enabled are not allowed to influence the STP topology. This is achieved by disabling the port with portfast configured upon reception of BPDU. The port is transitioned into errdisable state, and a message is printed on the console. The following is an example of the message printed out as a result of BPDU guard operation:
2000 May 12 15:13:32 %SPANTREE-2-RX_PORTFAST:Received BPDU on PortFast enable port. Disabling 2/1
2000 May 12 15:13:32 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1

QUESTION 55
The following was executed on switch Certkiller C:



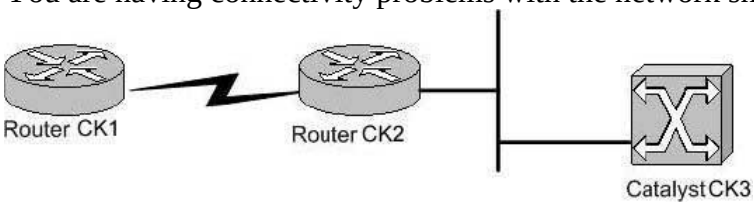
If all switches in the Certkiller network run the same type of spanning tree, what is the total number of spanning tree topology changes that occurred in this network?

A. 7
B. 35
C. Can not be determined. Only the root bridge tracks the complete amount of topology changes
D. 0
E. 2

Answer: A

Explanation:
The role of the TC mechanism is to correct L2 forwarding tables after the forwarding topology has changed. This is necessary to avoid a connectivity outage because, after a TC, some MAC addresses previously accessible through particular ports might become accessible through different ports. TC shortens the forwarding table aging time on all switches in the VLAN where the TC occurs; thus, if the address is not relearned, it will age-out and flooding will occur to ensure packets reach the destination MAC address. TC is triggered by the change of a port's STP state to or from the STP forwarding state. Note:With Rapid STP or Multiple STP (IEEE 802.1w and IEEE 802.1s), TC is triggered by a change of the port's state to forwarding, as well as the role change from designated to root. With Rapid STP, the L2 forwarding table is immediately flushed, as opposed to 802.1d, which shortens the aging time. The immediate flushing of the forwarding table restores connectivity faster, but will cause more flooding.
In the output shown above, the total number of topology changes for VLAN 2 is shown to be 7, with the last change occurring 3 weeks and 5 days ago.

QUESTION 56
You are having connectivity problems with the network shown below:



Router CK2 is able to ping the Catalyst switch CK3 , but router CK1 cannot.
What is the probable cause of this problem?

A. There is no VTP domain on the Catalyst switch.
B. The incorrect VLAN is attached to the command interface of the Catalyst.
C. There is no default route configured on the switch.
D. An incorrect IP address on the switch.
E. ICMP packets are being filtered on the switch CK3

Answer: C

Explanation:
Without a default route on Cat CK3 , CK3 will not know how to get packets back to CK1 . Catalyst CK3 would be able to ping router CK2 without a default route, however, because they share the same IP subnet.
Incorrect Answers:
A, B. VTP and VLAN information that is configured incorrectly could explain problems associated with local LAN users attached to the CK3 , but this would not explain why CK1 would not be able to reach CK3 .
D. If CK3 had an incorrect IP address, then CK2 would not be able to ping CK3 .
E. If all ICMP packets were filtered, then CK2 would also not be able to ping CK3 . This answer could be the problem only if ICMP were being filtered from router CK1 .

QUESTION 57
What is the Cisco recommended best practice PaGP setting for ports Etherchannel trunks?

A. on - on
B. auto - auto
C. desirable - on
D. desirable - auto
E. desirable - desirable

Answer: E

Explanation:
Using PAgP to Configure EtherChannel (Recommended)
PAgP facilitates the automatic creation of EtherChannel links by exchanging packets between channel-capable ports. The protocol learns the capabilities of port groups dynamically and informs the neighboring ports.
After PAgP identifies correctly paired channel-capable links, it groups the ports into a channel. The channel is then added to the spanning tree as a single bridge port. A given outbound broadcast or multicast packet is transmitted out one port in the channel only, not out every port in the channel. In addition, outbound broadcast and multicast packets transmitted on one port in a channel are blocked from returning on any other port of the channel.

There are four user-configurable channel modes: on, off, auto, and desirable. PAgP packets are exchanged only between ports in auto and desirable mode. Ports configured in on or off mode do not exchange PAgP packets. For switches to which you want to form an EtherChannel, it is best to have both switches set to desirable mode. This gives the most robust behavior if one side or the other encounters error situations or is reset. The default mode of the channel is auto.
Both the auto and desirable modes allow ports to negotiate with connected ports to determine if they can form a channel. The determination is based on criteria such as port speed, trunking state, and native VLAN.
Ports can form an EtherChannel when they are in different channel modes as long as the modes are compatible. This list provides examples:
* A port in desirable mode can successfully form an EtherChannel with another port that is in desirable or auto mode.
* A port in auto mode can form an EtherChannel with another port in desirable mode.
* A port in auto mode cannot form an EtherChannel with another port that is also in auto mode, since neither port initiates negotiation.
* A port in on mode can form a channel only with a port in on mode because ports in on mode do not exchange PAgP packets.
* A port in off mode cannot form a channel with any port.
Reference:
http://www.cisco.com/en/US/tech/ CK3 89/ CK2 13/technologies_tech_note09186a00800949c2.shtml#pagptoconfig
Additional Information:
The Best practices for Cisco Catalyst switch configurations can be found in this document:
http://www.cisco.com/en/US/products/hw/switches/ps700/products_white_paper09186a00801b49a4.shtml#cg6
From this Best Practices document:
Cisco Configuration Recommendation for L2 ChannelsCisco recommends enabling PAgP and using a setting of desirable-desirable on all EtherChannel links. Refer to the output below for more information:
Switch(config)#interface type slot/portSwitch(config-if)#no ip address!--- Ensures that there is no IP!--- address assigned to the LAN port.Switch(config-if)#channel-group <number> mode desirable!--- Specify the channel number and the PAgP mode.Verify the configuration, as shown below.
Switch#show run interface port-channel numberSwitch#show running-Config interface type slot/portSwitch#show interfaces type slot/port etherchannelSwitch#show etherchannel <number> port-channel

---

QUESTION 58
You wish to implement Ethernet Channels in your switched LAN. Which of the following are valid statements that should be kept in mind before this implementation? (Choose all that apply)

A. Ports within a Fast Ether Channel need to have identical duplex and speed settings.
B. Port Aggregation Protocol (PAGP) facilitates the automatic creation of Fast Ether channels links.

C. Ports within a Fast Ether Channel may be assigned to multiple VLANs.
D. Fast Ethernet Channels can not be configured as a trunk.
E. Only Fast Ethernet ports can be channeled.

Answer: A, B

Explanation:
You can not mix and match different types of Ethernet ports, such as 10M, 100M, GIGE, etc into the same channel. All ports in the channel need to have the same speed settings. Similarly, all ports need to be configured to have identical duplex settings.
The Port aggregation protocol (PAgP) aids in the automatic creation of Fast EtherChannel links. PAgP packets are sent between Fast EtherChannel-capable ports in order to negotiate the forming of a channel.
Incorrect Answers:
C. Ports in the channel can only be assigned to one VLAN.
D. Ethernet channels can indeed be set up as trunks.
E. Ethernet channels can be set up for fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet.

QUESTION 59
A new Catalyst switch is added to the Certkiller switched LAN. Users attached to the new switch are having connectivity problems. Upon troubleshooting, you realize that the new switch is not dynamically learning any VLAN information via VTP from the other switches. What could be causing this problem?

A. The other switches are different Catalyst models.
B. There are no users on one of the existing switches.
C. The other upstream switches are VTP clients.
D. The VTP domain name is not properly configured.
E. The native VLAN on the trunk is VLAN 1.

Answer: D

Explanation:
In order for VTP information to be propagated throughout the network, every LAN switch participating in the VTP domain must have the exact same VTP domain name configured.
Incorrect Answers:

A. All Catalyst switch models support VTP.
B. The number of users or types of devices attached to any switch has absolutely no bearing on the functionality of VTP.
C. VTP clients can pass updates to each other to propagate VLAN info throughout the network. All VTP client switches do not necessarily need to be directly connected to a VTP server.
E. VLAN 1 is the default VLAN for all Catalyst switches. Although it is not necessarily

recommended that all switches use this default VLAN, VTP information would be able to pass throughout the network if they did.

QUESTION 60
The Certkiller network is implementing a new Layer 3 Switching architecture. When an IP packet is Layer 3-switched from a source in one VLAN to a destination in another VLAN, what field in a packet will be rewritten?

A. Layer 3 destination address
B. Layer 3 source address
C. Layer 2 TTL
D. Layer 3 TTL
E. Layer 3 Transport Protocol

Answer: D

Explanation:
When a packet is Layer 3 switched, the source and destination MAC address, as well as the IP TTL and IP checksum is rewritten.

	Layer		**Layer**				**Data**	**FCS**
	2		**3 IP**					
	Etherne	**t**	**Header**					
	Header							
		Source		Source	TTL			
	Destinat	ionMAC	Destinat	ionIP		Checksu	m	
	MAC		IP					
	Router	Host-A	Host-B	Host-A	n	value1		
Receive	**d**MAC	MAC						
Frame	Address	Address						
	Next	Router	Host-B	Host-A	n-1	value2		

Rewritt	**en**Hop	MAC						
Frame	MAC	Address						
	Address							

The Table above displays the details of the received frame that are indicated and then the details required for the rewritten frame that is transmitted after routing are shown. Notice that the following fields must be modified for the rewritten frame that is forwarded to the next hop routing device:
1. Destination MAC address: The MAC address of the next hop must be written to the rewritten frame.
2. Source MAC address: The source MAC address must be written to the MAC address of the router.
3. IP TTL: This must be decremented by one, as per the normal rules of IP routing.
4. IP Header Checksum: This must be recalculated, as the TTL field changes.
The process of how the data plane operations shown in Table 6-1 are implemented is where the difference between a traditional router and Layer 3 switch lie. A traditional router uses the same general purpose CPU used to perform control plane operations to also implement data plane operations, meaning data plane operations are handled in software. A Layer 3 switch on the other hand uses an ASIC to perform data plane operations because it is very easy to program the very simple operations required for the data plane into an ASIC. In this respect, the data plane is implemented in hardware because a series of hardware operations are programmed into the ASIC that perform the data plane operations required for routing a packet.
Reference: Justin Menga, CCNP Practical Studies: Layer 3 switching.

QUESTION 61
By default, which of the following VLANs are eligible for pruning in a Catalyst 6509 switch? (Choose all that apply)

A. VLAN 1
B. VLAN 2
C. VLAN 999
D. VLAN 1000
E. VLAN 1001
F. VLAN 4094

Answer: B, C, D

Explanation:
By default, VLANs 2-1000 are pruning eligible in a Catalyst switch. For the default VLAN settings in Catalyst switches see the following document:

http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products_configuration_guide_chapter09186a

---

QUESTION 62
You have ISL trunks configured between two Catalyst switches, and you wish to load share traffic between them. Which method of load sharing can you utilize?

A. Load sharing of traffic over parallel ISL trunks on a per flow basis.
B. Load sharing of traffic over parallel ISL trunks on a per VLAN basis.
C. Load sharing of traffic over parallel ISL trunks on a per packet basis.
D. Automatic round robin load sharing of VLAN traffic.

Answer: B

Explanation:
It is possible to load share over parallel ISL trunks on a per-VLAN basis, using either path costs or port priorities, or a combination of these two methods. However, this will only load share traffic from different VLANs, and not evenly distribute traffic from the same VLAN as the STP process will only allow a single VLAN to use one of the ISL trunks.
Incorrect Answers:
A, C. It is not possible to load share on a per flow or per packet basis as any given VLAN will only traverse over one of the ISL trunks. The other trunk will be in a blocking state for that particular VLAN.
D. Automatic load sharing is not possible over parallel ISL trunks.

QUESTION 63
You are trying to bring up an ISL trunk link between two switches. The trunk mode on the local end is set to auto. However, the ISL trunk never comes up.
What is the probable cause of this problem? (Choose all that apply.)

A. The trunk mode on the remote end is set to on.
B. The trunk mode on the remote end is set to off.
C. The trunk mode on the remote end is set to auto.
D. The trunk mode on the remote end is set to desirable.
E. The trunk mode on the remote end is set to nonegotiate.

Answer: B, C, E

Explanation:
The trunk mode can be: auto, Desirable, On, nonegotiate, and Off. When set to "off" ISL is not allowed on this port regardless of the mode configured on the other end. When set to "auto" the port listens for Dynamic Trunking Protocol (DTP) frames from the remote device. Auto does not propagate any intent to become a trunk; it is solely dependent on the remote device to make the trunking decision. Thus, if both ends are set to Auto, no trunking will occur. When set to nonegotiate, DTP is not spoken to the neighboring

switch. nonegotiate automatically enables ISL trunking on its port, regardless of the state of its neighboring switch. However, according to Cisco when one end is set to auto, and the other end is set to nonegotiate, then the result is a non-trunking port (see the table at the middle of the Cisco link, used as a reference).
Incorrect Answers:

A. When set to "on", DTP is spoken to the neighboring switch. On automatically enables ISL trunking on its port, regardless of the state of its neighboring switch. It remains an ISL trunk unless it receives an ISL packet that explicitly disables the ISL trunk. The Cisco TAC recommends that desirable trunking mode be configured on the ports.
D. In desirable mode, DTP is spoken to the neighboring switch. Desirable communicates to the neighboring switch that it is capable of being an ISL trunk, and would like the neighboring switch to also be an ISL trunk.
Reference:
http://www.cisco.com/warp/public/793/lan_switching/2.html

QUESTION 64
The Certkiller corporate LAN consists of numerous Catalyst switches and a large number of VLANs. You are seeing an excessive amount of broadcasts across your trunk links. In an effort to reduce unnecessary traffic, VLAN Trunk Protocol (VTP) pruning is enabled. Which of the following statements is true regarding this change?

A. Traffic on VLAN 1 can be pruned.
B. Pruning eligibility is determined by the amount of ports assigned to a VLAN.
C. VTP pruning is a way to detect the removal of a VLAN within a VTP domain.
D. VTP version 2 is backward compatible with VTP version 1.
E. VTP pruning only affects traffic from VLANs that are pruning eligible.

Answer: E

Explanation:
VTP pruning enhances network bandwidth use by reducing unnecessary flooded traffic, such as broadcast, multicast, unknown, and flooded unicast packets. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices. By default, VTP pruning is disabled. VTP pruning does not prune traffic from VLANs that are pruning-ineligible.
Incorrect Answers:

A. VLAN 1 is always pruning-ineligible, meaning traffic from VLAN 1 cannot be pruned.
B. Pruning eligibility is based only on the VLANs that need the given broadcast information across the trunks. It has nothing to do with the number of ports assigned to that VLAN.
C. VTP Pruning simply reduces the broadcast and multicast traffic. It does not change, add, or delete the VLANs in a VTP domain.
D. VTP version1 and VTP version2 are not interoperable on network devices in the same

VTP domain. Every network device in the VTP domain must use the same VTP version. Do not enable VTP version2 unless every network device in the VTP domain supports version2.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_4_2/config/vlans.htm#xtocid79802

QUESTION 65
After performing some testing on a Catalyst switch in a lab, it is connected to the production network to another Catalyst switch via the supervisor Gigabit Ethernet port. Soon after this, users complain that they have lost all connectivity to the network. What could have caused this to happen?

A. You did not issue the set spantree uplinkfast enable 1/1 command before connecting to the corporate switch.
B. You did not make the trunk mode set to on or desirable for the trunk to the supervisor of the other switch.
C. You did not make the VTP mode transparent in the new switch.
D. The dynamic CAM entries were not cleared after the new switch was connected to the network.
E. The new switch had the wrong VTP domain name.

Answer: C

Explanation:
The most likely cause of this happening is that the new switch was configured to participate in the VTP domain, but that it was set to server mode. The default mode is VTP server, which can override the VLAN information and get propagated to other switches in the network. In transparent mode, the switch will not participate in VTP, and it cannot override existing VTP settings.
Understanding the VTP Domain:
A VTP domain (also called a VLAN management domain) is made up of one or more interconnected network devices that share the same VTP domain name. A network device can be configured to be in one and only one VTP domain. You make global VLAN configuration changes for the domain using either the command-line interface (CLI) or Simple Network Management Protocol (SNMP).
By default, the Catalyst6500 series switch is in VTP server mode and is in the no-management domain state until the switch receives an advertisement for a domain over a trunk link or you configure a management domain.
If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The switch ignores advertisements with a different management domain name or an earlier configuration revision number.
If you configure the switch as VTP transparent, you can create and modify VLANs but the changes affect only the individual switch.
When you make a change to the VLAN configuration on a VTP server, the change is propagated to all network devices in the VTP domain. VTP advertisements are

transmitted out all trunk connections.
VTP maps VLANs dynamically across multiple LAN types with unique names and internal index associations. Mapping eliminates excessive device administration required from network administrators.
Understanding VTP Modes:
You can configure a Catalyst6500 series switch to operate in any one of these VTP modes:
Server-In VTP server mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version and VTP pruning) for the entire VTP domain. VTP servers advertise their VLAN configuration to other network devices in the same VTP domain and synchronize their VLAN configuration with other network devices based on advertisements received over trunk links. VTP server is the default mode.
Client-VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
Transparent-VTP transparent network devices do not participate in VTP. A VTP transparent network device does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent network devices do forward VTP advertisements that they receive out their trunking LAN ports.
Incorrect Answers:

A. The set spantree uplinkfast enable command increases the path cost of all ports on the switch, making it unlikely that the switch will become the root switch. This obviously would not cause the problem described in this question.
B. This would affect the trunk coming up between the switches, but would not cause this kind of connectivity issue in this question. In this case, even if the trunk did not come up, end users would not even notice.
D. The CAM entries would have no impact, especially since no end stations were plugged into it in the lab.
E. The wrong VTP domain name would mean that this switch would not be participating in this particular VTP domain. In this specific case, this would have actually fixed the problem.

QUESTION 66
You are trying to set up an Ethernet channel between switch A and switch B. After issuing the command "set port channel 3/1-2 on" on switch B, connectivity to switch B is lost. The following messages appear on switch B as a result of this.
Switch-B> (enable)
%SPANTREE-2-CHNMISCFG: STP loop - channel 3/1-2 is disabled in vlan 1.
%PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1-2
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/1-2
You then disable the Ethernet Channel on Switch-B, but you still have no connectivity to Switch-A.
Which command will restore connectivity to switch A?

A. clear port error 3/1-2
B. set port enable 3/1-2
C. set trunk channel 3/1-2 desirable isl
D. set port channel 3/1-2 enable

Answer: B

Explanation:
The message clearly indicates that the ports 2/1-4 have been disabled. This is a consequence of spantree as shown by the "channel 3/1-2 is disabled in vlan 1" message. This will make the ports affected go into an err-disable state. To fix this, the ports need to be manually re-enabled with the "set port enable" command.

QUESTION 67
A switch is configured for an ISL trunk, with the trunk mode set to on. A new switch is added to the network, but the trunk will not come up.
What is the probable cause of this problem?

A. The native VLANs are not the same.
B. The trunks need to be set to "on" or "auto".
C. The trunks need to be set to "desirable" or "nonegotiate".
D. The VTP domain names carried in the Dynamic Inter-Switch Link (DISL) messages are not the same.
E. The Unidirectional Link Detection timers are shorter than the Spanning Tree Protocol (STP) timers.

Answer: D
VTP domain names on an ISL trunk must be the same. DTP packets will not pass between switches that are in different VTP domains.
Incorrect Answers:

A. The VLANs can be different for each switch and the trunk will still come up if set up correctly.
B, C. Since one end of the trunk is set to on, the other end can be set to either on, auto, desirable, or nonegotiate for the trunk to come up.
E. These timers will have no bearing on the trunk formation.
Reference:
http://www.cisco.com/warp/public/793/lan_switching/2.html

QUESTION 68
You are designing a new switched LAN and VLAN information will need to be shared between switches. What VLAN trunking protocol contains the following features?
-26 byte header and a 4 byte frame check sum
- Supports up 1024 VLANs
- Supports a single instance of spanning tree per-VLAN

A. ISL
B. 802.1d
C. 802.1q
D. 802.1v
E. 802.10

Answer: A

Explanation:
ISL is a Cisco proprietary protocol for interconnecting multiple switches and maintaining VLAN information as traffic goes between switches. ISL uses Per VLAN Spanning Tree (PVST) which runs one instance of Spanning Tree Protocol (STP) per VLAN. PVST allows for optimizing the root switch placement for each VLAN and supports load balancing of VLANs over multiple trunk links.
With ISL, an Ethernet frame is encapsulated with a header that transports VLAN IDs between switches and routers. A 26-byte header that contains a 10-bit VLAN ID is prepended to the Ethernet frame. This 10 byte-VLAN ID provide for up to 1024 VLANs. The FCS field consists of four bytes in an ISL packet. This sequence contains a 32-bit CRC value, which is created by the sending MAC and is recalculated by the receiving MAC to check for damaged frames. The FCS is generated over the DA, SA, Length/Type, and Data fields. When an ISL header is attached, a new FCS is calculated over the entire ISL packet and added to the end of the frame

---

QUESTION 69
A switch can belong to how many VTP domains?

A. 1
B. 2
C. 1 to 1005
D. 1 to 4096
E. It depends upon memory
F. It depends on the number of available IDB blocks

Answer: A
Explanation
A Catalyst switch can only be configured to belong in only one VTP domain, using the "set VTP domain" command. If you attempt to use additional "set vtp domain" commands, you will simply overwrite the previous command and the switch will belong to the newly configured domain.

QUESTION 70
The Certkiller network administrator has set all Certkiller switches to transparent VTP mode. What is a key advantage to configuring all switches in an enterprise network to VTP transparent mode?

A. It ensures consistency between VLAN numbering for all switches in the switched network.
B. It prevents network administrator's form accidentally deleting VLAN information from all switches.
C. It allows for more rapid deployment of VLANs throughout the enterprise.
D. It reduces the size of the spanning tree network and improves STP convergence time as a result.
E. It reduces the total number of VLANs required in the enterprise network.

Answer: B

Explanation:
A major advantage to configuring all switches within a domain to transparent mode is that VLAN configuration settings on other switches will not get overridden. A mistake that many administrators make is installing a new switch into t domain when it is configured as a VTP server. The default mode is VTP server, which can override the VLAN information and get propagated to other switches in the network. This can mean the deletion of all of the other VLANs within the switched network. In transparent mode, the switch will not participate in VTP, and it cannot override existing VTP settings.
Understanding the VTP Domain:
A VTP domain (also called a VLAN management domain) is made up of one or more interconnected network devices that share the same VTP domain name. A network device can be configured to be in one and only one VTP domain. You make global VLAN configuration changes for the domain using either the command-line interface (CLI) or Simple Network Management Protocol (SNMP).
By default, the Catalyst6500 series switch is in VTP server mode and is in the no-management domain state until the switch receives an advertisement for a domain over a trunk link or you configure a management domain.
If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The switch ignores advertisements with a different management domain name or an earlier configuration revision number.
If you configure the switch as VTP transparent, you can create and modify VLANs but the changes affect only the individual switch.
When you make a change to the VLAN configuration on a VTP server, the change is propagated to all network devices in the VTP domain. VTP advertisements are transmitted out all trunk connections.
VTP maps VLANs dynamically across multiple LAN types with unique names and internal index associations. Mapping eliminates excessive device administration required from network administrators.
Understanding VTP Modes:
You can configure a Catalyst6500 series switch to operate in any one of these VTP modes:
Server-In VTP server mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version and VTP pruning) for the entire VTP domain. VTP servers advertise their VLAN configuration to other network devices in the

same VTP domain and synchronize their VLAN configuration with other network devices based on advertisements received over trunk links. VTP server is the default mode.
Client-VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
Transparent-VTP transparent network devices do not participate in VTP. A VTP transparent network device does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent network devices do forward VTP advertisements that they receive out their trunking LAN ports.

QUESTION 71
A new Certkiller switch has been configured as a VTP client, and added to the existing VTP domain. Shortly after the ISL link is brought up to the rest of the network, the whole network goes down. What could have caused this to happen? (Choose the most likely option).

A. The configuration revision of the switch inserted was higher than the configuration revision of the VTP domain.
B. This is not an issue that could be related to the inserted switch since it was configured as a VTP client.
C. The inserted switch was incorrectly configured for VTP v2 and caused an unstable condition.
D. VLAN 1 was incorrectly deleted on the switch before insertion causing an unstable condition.

Answer: A

Explanation:
Even though the Catalyst switch is configured as a VTP client, and not a server, it can erase the information of an existing network. Cisco explains the problem as follows:
How a Recently Inserted Switch Can Cause Network Problems
This problem occurs when you have a large switched domain, which is all in the same VTP domain, and you want to add one switch in the network.
This switch was previously used in the lab, and a good VTP domain name was entered. It was configured as a VTP client, and connected to the rest of the network. Then, the ISL link was brought up to the rest of the network. In just a few seconds, the whole network is down. What could have happened?
The configuration revision of the switch you inserted was higher than the configuration revision of the VTP domain. Therefore, your recently-introduced switch, with almost no configured VLANs, has erased all VLANs through the VTP domain.
This happens whether the switch is a VTP client or a VTP server. A VTP client can erase VLAN information on a VTP server. You can tell that this has happened when many of the ports in your network go into inactive state, but continue to be assigned to a nonexistent VLAN.
Solution:

Quickly reconfigure all of the VLANs on one of the VTP servers.
What to Remember:
Always make sure that the configuration revision of all switches inserted into the VTP domain is lower than the configuration revision of the switches already in the VTP domain.
Reference: http://www.cisco.com/warp/customer/473/21.html#vtp_ts_cav

---

QUESTION 72
The Certkiller network is bonding some of the Ethernet connections via PaGP in order to increase the backbone bandwidth. In PagP, what mode combination will allow a channel to be formed?

A. Auto-auto
B. Desirable-on
C. On-auto
D. Auto-desirable

Answer: D

Explanation:
The Port Aggregation Protocol (PAgP) modes are off, auto, desirable, and on. Only the combinations auto-desirable, desirable-desirable, and on-on will allow a channel to be formed.
The PAgP modes are explained below.
1. off: PAgP will not run. The channel is forced to remain down.
2.auto: PAgP is running passively. The formation of a channel is desired; however, it is not initiated.
3. desirable: PAgP is running actively. The formation of a channel is desired and initiated.
4. On: PAgP will not run. The channel is forced to come up.
Only the combinations of auto-desirable, desirable-desirable, and on-on will allow a channel to be formed. If a device on one side of the channel does not support PAgP, such as a router, the device on the other side must have PAgP set to on.

QUESTION 73
Certkiller is using extended VLANs (VLAN IDs 1006-4094) on their switches. What should he VTP mode be set to before configuring extended-range VLANs?

A. Client
B. Server
C. Transparent
D. Client or Server
E. Client or Transparent
F. Server or Transparent

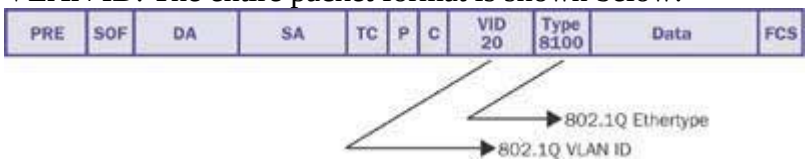
Answer: C

Explanation:
VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements.
However, in VTP version 2, transparent switches do forward VTP advertisements that they receive from other switches from their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode. The switch must be in VTP transparent mode when you create extended-range VLANs.

QUESTION 74
Both ISL and 802.1Q is being used in the Certkiller network. When comparing the differences in ISL and 802.1Q, which of the following are true? (Select three)

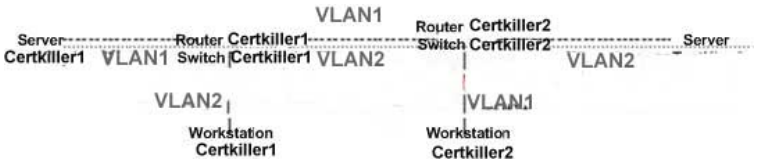
A. 802.1q allows the encapsulation of multiple trunks within a single trunk.
B. 802.1q supports fewer VLANs than ISL.
C. ISL is more efficient than 802.1q due to its smaller header size.
D. ISL supports the processing of untagged frames.
E. 802.1q uses a tag protocol ID of 0x8100

Answer: A, D, E
Both 802.1Q and ISL allows for the use of multiple trunks within any single trunk.
ISL supports the use of untagged frames on the trunk. All untagged frames are associated with the native VLAN, which is VLAN 1 by default.
The IEEE 802.1Q specification defines the Ethertype field to be 8100 in the presence of a VLAN ID. The entire packet format is shown below:



Incorrect Answers:
B. 802.1Q supports up to 4096 VLANS, while ISL supports a maximum of 1024.
C. ISL encapsulation adds 30 bytes to the entire frame, while the 802.1Q tag is only 4 bytes in length.

QUESTION 75
The Certkiller network is illustrated below:



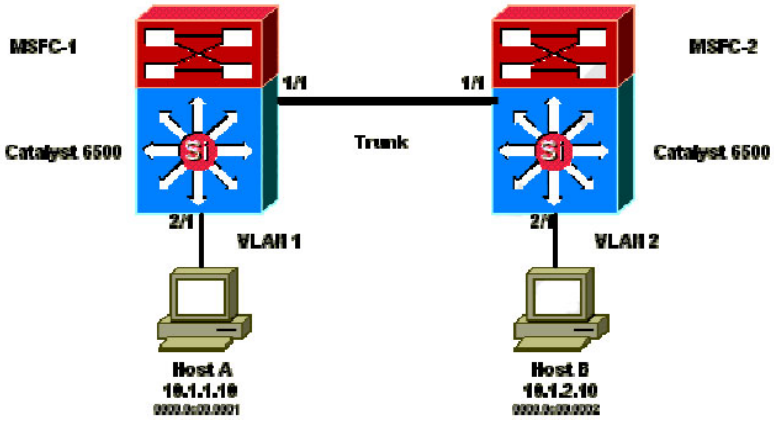
In the shown diagram, Server Certkiller 1's default gateway points to Router Certkiller 1's VLAN1 interface and Server Certkiller 2's default gateway points to Router Certkiller 2's VLAN2 interface. Between Switch Certkiller 1 and Certkiller 2, both VLANs 1 and 2 are being forwarded over a trunk. When there is data transfer between the servers workstations, WS Certkiller 1 and WS Certkiller 2 see a lot of

input traffic.
How can we limit this problem?

A. Increase aging time on routers
B. Disable MAC address aging time on the switches
C. Disable ARP timeout on routers
D. Reduce MAC address aging time on the switches
E. Bring ARP aging time on Routers and MAC address aging time on switches close to each other

Answer: E

Explanation:
The problem described in this question is related to asymmetric routing, due to each workstation having different default gateways. The default ARP cache aging time on a router is 4 hours. The default aging time of the switch content-addressable memory (CAM) entry is 5 minutes. The ARP aging time of the host workstations is not significant for this discussion. However, the example sets the ARP aging time to 4 hours.
This diagram illustrates this issue. This topology example includes Catalyst 6500s with Multilayer Switch Feature Cards (MSFCs) in each switch. The switches are interconnected via a trunk which carries traffic for VLAN 1 and VLAN 2.

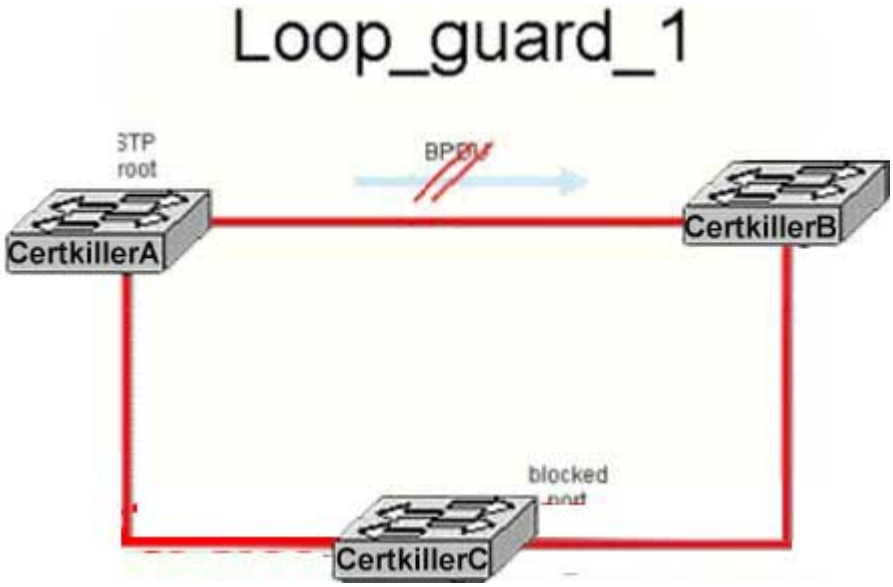


Consequences of Asymmetric Routing:
Consider the case of the continuous ping of host B by host
A. Remember that host A
sends the echo packet to MSFC1, and host B sends the echo reply to MSFC2, which is in an asymmetric routing state. The only time that Switch 1 learns the source MAC of host B is when host B replies to an ARP request from MSFC1. This is because host B uses MSFC2 as its default gateway and does not send packets to MSFC1 and, consequently, Switch 1. Since the ARP timeout is 4 hours by default, Switch 1 ages the MAC address of host B after 5 minutes by default. Switch 2 ages host A after 5 minutes. As a result, Switch 1 must treat any packet with a destination MAC of host B as an unknown unicast. The switch floods the packet that comes from host A and is destined for host B out all ports. In addition, because there is no MAC address entry host B in Switch 1, there is no MLS entry as well.
The echo reply packets that come from host B experience the same issue after the MAC

address entry for host A ages on Switch 2. Host B forwards the echo reply to MSFC2, which in turn routes the packet and sends it out on VLAN 1. The switch does not have an entry host A in the MAC address table and must flood the packet out all ports in VLAN 1. Asymmetric routing issues do not break connectivity. However, asymmetric routing can cause excessive unicast flooding and MLS entries that are missing. There are three configuration changes that can remedy this situation:
1. Adjust the MAC aging time on the respective switches to 14,400 seconds (4 hours) or longer.
2. Change the ARP timeout on the routers to 5 minutes (300 seconds).
3. Change the MAC aging time and ARP timeout to the same timeout value.
Reference:
http://www.cisco.com/en/US/tech/ CK6 48/ CK3 62/technologies_tech_note09186a0080094afd.shtml

---

QUESTION 76
The Certkiller switched LAN is shown below:

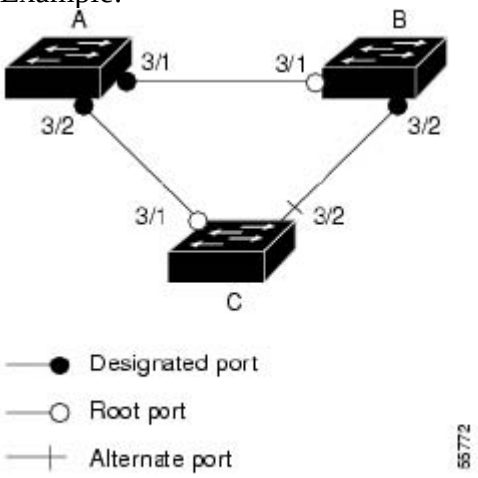


Due to hardware failure on the link between switches Certkiller A and Certkiller B, Spanning Tree BPDUs from switch Certkiller A are no longer received by switch Certkiller B, but the link remains up (see the drawing) Provided LoopGuard feature is configured on all ports, which port will be put into 'Loop-inconsistent' state?

A. Port on switch Certkiller C connecting to switch Certkiller B
B. Port on switch Certkiller B connecting to switch Certkiller C
C. LoopGuard would not detect any issue in this scenario
D. Port on switch Certkiller A connecting to switch Certkiller B and port on switch Certkiller B connecting to switch Certkiller A

Answer: C
Understanding How Loop Guard Works:
Loop guard helps prevent bridging loops that could occur because of a uni-directional link failure on a point-to-point link. When enabled globally, the loop guard applies to all point-to-point ports on the system. Loop guard detects root ports and blocked ports and

ensures that they keep receiving BPDUs from their designated port on the segment. If a loop guard enabled root or blocked port stop a receiving BPDUs from its designated port, it transitions to the loop-inconsistent blocking state, assuming there is a physical link error on this port. The port recovers from this loop-inconsistent state as soon as it receives a BPDU.
You can enable loop guard on a per-port basis. When you enable loop guard, it is automatically applied to all of the active instances or VLANs to which that port belongs. When you disable loop guard, it is disabled for the specified ports. Disabling loop guard moves all loop-inconsistent ports to the listening state.
Example:



The figure above illustrates the following configuration:
Switches A and B are distribution switches.
Switch C is an access switch.
Loop guard is enabled on ports 3/1 and 3/2 on Switches A, B, and C.
Enabling loop guard on a root switch has no effect but provides protection when a root switch becomes a nonroot switch.
These caveats apply to loop guard:
Spanning tree always chooses the first operational port in the channel to send the BPDUs. If that link becomes unidirectional, loop guard blocks the channel, even if other links in the channel are functioning properly.
If a set of ports that are already blocked by loop guard are grouped together to form a channel, spanning tree loses all the state information for those ports and the new channel port may obtain the forwarding state with a designated role.
Note
You can enable UniDirectional Link Detection (UDLD) to help isolate the link failure. A loop may occur until UDLD detects the failure, but loop guard will not be able to detect it.
Loop guard has no effect on a disabled spanning tree instance or a VLAN.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080160

QUESTION 77
Your Catalyst switch is configured to support Multi Layer Switching (MLS). The switch contains an access list designed to prevent certain users from using ports 20 and 21 to reach the Internet. Because of this, which flow mask will be needed to create each MLS shortcut?

A. Destination flow mask
B. Full flow mask
C. Source flow mask
D. Partial flow mask
E. Destination-source mask
F. Session flow mask

Answer: B

Explanation:
The three types of IP MLS modes are destination-ip, destination-source-ip, and full-flow-ip. Full flow-ip is in effect when an extended access list is applied..
To Block FTP traffic we require an extended access-list, which acts on layer 3 as well as layer 4 information in a packet. Because of this, the full flow mask is needed, which uses layer 3 and layer 4 information to create the shortcuts.
Incorrect Answers:

A. Destination-ip mode is the default mode. It is used when no access list is applied to the router's MLS-enabled interface.
C, D, F. These types of flow masks do not exist.
E. Source-destination-ip mode is in use when a standard access list is applied.
Reference:
http://www.cisco.com/warp/public/473/13.html#flowchart

QUESTION 78
While looking through the log files of your Catalyst switch, you notice that the following two messages are displayed somewhat infrequently:
%MLS-4-MOVEOVERFLOW:Too many moves, stop MLS for 5 sec(20000000)
%MLS-4-RESUMESC:Resume MLS after detecting too many moves
What is the most likely cause of this problem?

A. A transitory Spanning Tree loop
B. A permanent Spanning Tree loop
C. A faulty cable
D. Faulty switch port
E. A Pinnacle sync failure

Answer: A

Explanation:

If you see these messages infrequently, it is most likely a transitory L2 (spanning-tree) loop, resulting in packet flooding in one or more VLANs. However, if you are seeing an excessive number of these messages (for example, if your syslog server log file or your switch console are being flooded with these messages), the problem might be due to the following reasons:
* a permanent L2 (spanning-tree) loop
* one or more faulty switch ports
* a bad cable (for example, a unidirectional fiber link)
* other bad hardware (not necessarily on the switch generating the messages)
* misconfigured device (for example, a traffic generator sending traffic to two switch ports using the same MAC address)
Incorrect Answers:
B, C, D. These are all possible causes, but not the most probably cause. The fact that only a few of these error messages are appearing tells us that A is the best choice.
E. This choice is the least likely to be the cause of the errors messages. A pinnacle Sync failure is a hardware error and Cisco does not cite this as a reason for the MLS errors at all.
Reference:
Common CatOS Error Messages on Cisco Catalyst Switches
http://www.cisco.com/warp/public/473/34.shtml

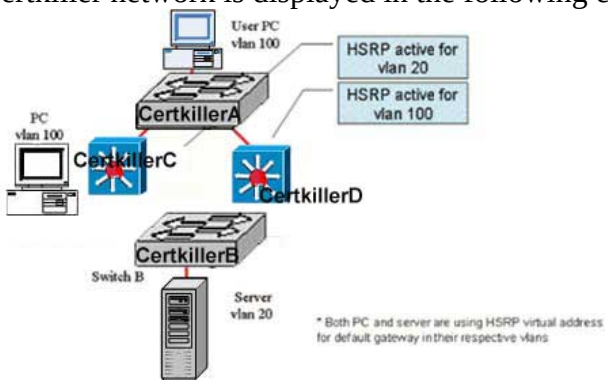
QUESTION 79
You have just recently implemented the Multilayer switching feature on your Catalyst Switch. How will this change affect your network?

A. The MLS Switching Engine will forward the first packet in every flow.
B. The MLS Route Processor will forward the first packet in every flow.
C. The MLS Switching Engine will forward all traffic.
D. The MLS Route Processor will forward all traffic.

Answer: B

Explanation:
Multi-Layer Switching (MLS) has become a highly desired method of accelerating routing performance through the use of dedicated Application Specific Integrated Circuits (ASICs). Traditional routing is done through a central CPU and software. MLS offloads a significant portion of routing (packet rewrite) to hardware, and thus has also been termed switching. MLS and Layer 3 switching are equivalent terms. It works by utilizing the MLS Route Processor, which forwards only the first packet in every source-destination flow. The remaining packets in the flow are then switched by the Switching Engine.
Incorrect Answers:
A, C. The Switching Engine is utilized after the first packet is processed by the Route processor. The packets in each flow are then routed once, and then switched.
D. MLS works by only running the first packet in any flow through the relatively resource intensive routing process.

QUESTION 80
The Certkiller network is displayed in the following exhibit:

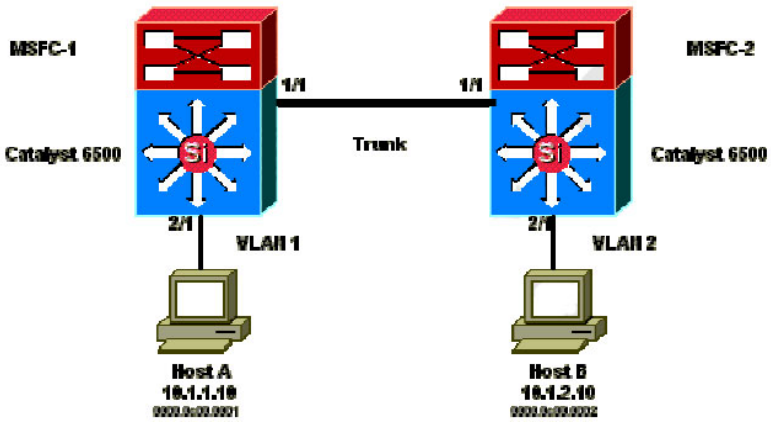


You connect a PC to Switch Certkiller C and captured some packets in VLAN 100. You have noticed that unicast packets from the Server in VLAN 20 to User PC in VLAN 100 are constantly being flooded affecting the performance of other devices in VLAN 100. What is the most appropriate way to fix this issue?

A. Configure the MAC address of Server in vlan 100 as static on Switch Certkiller C
B. Configure MAC address of PC in vlan 100 as static on switch Certkiller D
C. Configure static ARP entry for PC address in vlan 100 on switch Certkiller C
D. Configure MAC address table aging and ARP aging timers to match on switches Certkiller C and Certkiller D
E. Disable HSRP on switch Certkiller C

Answer: D

Explanation:
The default ARP cache aging time on a router is 4 hours. The default aging time of the switch content-addressable memory (CAM) entry is 5 minutes. The ARP aging time of the host workstations is not significant for this discussion. However, the example sets the ARP aging time to 4 hours.
This diagram illustrates this issue. This topology example includes Catalyst 6500s with Multilayer Switch Feature Cards (MSFCs) in each switch. Although this example uses MSFCs, you can use any router instead of the MSFC. Example routers that you can use include the Route Switch Module (RSM), Gigabit Switch Router (GSR), and Cisco 7500. The hosts are directly connected to ports on the switch. The switches are interconnected via a trunk which carries traffic for VLAN 1 and VLAN 2.



Consequences of Asymmetric Routing
Consider the case of the continuous ping of host B by host A. Remember that host A sends the echo packet to MSFC1, and host B sends the echo reply to MSFC2, which is in an asymmetric routing state. The only time that Switch 1 learns the source MAC of host B is when host B replies to an ARP request from MSFC1. This is because host B uses MSFC2 as its default gateway and does not send packets to MSFC1 and, consequently, Switch 1. Since the ARP timeout is 4 hours by default, Switch 1 ages the MAC address of host B after 5 minutes by default. Switch 2 ages host A after 5 minutes. As a result, Switch 1 must treat any packet with a destination MAC of host B as an unknown unicast. The switch floods the packet that comes from host A and is destined for host B out all ports. In addition, because there is no MAC address entry host B in Switch 1, there is no MLS entry as well.
The echo reply packets that come from host B experience the same issue after the MAC address entry for host A ages on Switch 2. Host B forwards the echo reply to MSFC2, which in turn routes the packet and sends it out on VLAN 1. The switch does not have an entry host A in the MAC address table and must flood the packet out all ports in VLAN 1. Asymmetric routing issues do not break connectivity. However, asymmetric routing can cause excessive unicast flooding and MLS entries that are missing. There are three configuration changes that can remedy this situation:
1. Adjust the MAC aging time on the respective switches to 14,400 seconds (4 hours) or longer.
2. Change the ARP timeout on the routers to 5 minutes (300 seconds).
3. Change the MAC aging time and ARP timeout to the same timeout value.
Reference:
http://www.cisco.com/en/US/tech/ CK6 48/ CK3 62/technologies_tech_note09186a0080094afd.shtml

---

QUESTION 81
A workstation has been connected to the Certkiller LAN using a Category 5e cable. The workstation can connect to the rest of the network through the switch (i.e has full connectivity), but is suffering from much slower than expected performance. Looking at the interface statistics on the switch, many "runts" are being detected. Using software to read the counters on the workstation NIC, many FCS and alignment errors are occurring. What is the most likely cause of these errors?

A. Bad Network Interface Card on the workstation
B. Bad cable between the workstation and the switch
C. The port has incorrectly been configured as an 802.1q trunk port
D. Mismatched speed settings between the workstation and the switch
E. Mismatched duplex setting between the workstation and the switch
F. None of the above.

Answer: E

Explanation:
In half-duplex environments, it is possible for both the switch and the connected device to sense the wire and transmit at exactly the same time and result in a collision. Collisions can cause runts, FCS, and alignment errors, caused when the frame is not completely copied to the wire, which results in fragmented frames.
When operating at full-duplex, FCS, cyclic redundancy checks (CRC), alignment errors, and runt counters should be minimal. If the link is operating at full-duplex, the collision counter is not active. If the FCS, CRC, alignment, or runt counters are incrementing, check for a duplex mismatch. Duplex mismatch is a situation in which the switch is operating at full-duplex and the connected device is operating at half-duplex, or the other way around. The result of a duplex mismatch is extremely slow performance, intermittent connectivity, and loss of connection.
The following describes the errors and their meanings:
Alignment Errors: Alignment errors are a count of the number of frames received that do not end with an even number of octets and have a bad CRC.
FCS Errors: FCS error count is the number of frames that were transmitted or received with a bad checksum (CRC value) in the Ethernet frame. These frames are dropped and not propagated onto other ports.
Runts: These are frames smaller than 64 bytes with a bad FCS value.

QUESTION 82
Ethernet LAN's are used throughout the Certkiller network. How much data can be carried in a single standard Ethernet frame?

A. Up to 4096 bytes
B. No limit
C. Up to 1500 bytes
D. Up to 1518 bytes
E. Up to 4400 bytes

Answer: C

Explanation:
A standard Ethernet frame MTU is 1500 bytes. The MTU size or packet size refers only to Ethernet payload. Ethernet frame size refers to the whole Ethernet frame, including the header and the trailer. This question asked for the amount of data that can be carried, which is the payload.

Note: Preamble is not calculated in frame size so DA (6 bytes) SA (6 bytes) Type (2 bytes) data + pad (1500 bytes) FCS (4bytes) = a total of 1518
Incorrect Answers:
D. A standard Ethernet frame MTU is 1500 bytes. This does not include the Ethernet header and Cyclic Redundancy Check (CRC) trailer, which is 18 bytes in length, to make the total Ethernet frame size of 1518. So the total size of an Ethernet packet can be as large as 1518 bytes, but the maximum payload is only 1500 bytes.

QUESTION 83
Which of the following will cause a switch port to go into the err-disable state? (Choose all that apply)

A. Duplex mismatch.
B. Unidirectional Link Detection.
C. AN incorrect VTP domain name is configured on the switch.
D. Ethernet channeling is configured on the port.
E. VLANs on the trunk were not matching on both sides.

Answer: A, B

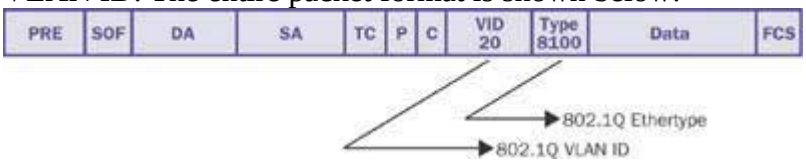
Explanation:
If the interface status is err-disable in the output of the "show interface status" command, refer to the common reasons below. When a port is error-disabled, the LED associated with the port on the front panel will be solid orange.
The reasons for the interface going into "err-disable" state are varied. Some of the possibilities include the following:
1. duplex mismatch (A is correct)
2. port-channel misconfiguration
3. Bridge Protocol Data Unit (BPDU) Guard violation
4. UniDirectional Link Detection (UDLD) condition (B is correct)
5. late-collision detection
6. link-flap detection
7. security violation
8. Port Aggregation Protocol (PAgP) flap
9. Layer 2 Tunneling Protocol (L2TP) Guard
10. DHCP snooping rate-limiting
11. EtherChannel guard detects a misconfigured EtherChannel
Incorrect Answers:
C. The VTP configuration relates to the switch as a whole and has no impact on individual ports.
D. Although the port could be in the err-disable state if the Ethernet channeling feature is not set correctly on both ends, simply configuring channeling will not cause the port to go into this state by itself.
E. VLAN mismatches have no bearing on port status.

QUESTION 84
802.1Q trunking uses which Ethertype to identify itself?

A. 8100
B. 8021
C. 802A
D. 2020
E. None of the above

Answer: A

Explanation:
The IEEE 802.1Q specification defines the Ethertype field to be 8100 in the presence of a VLAN ID. The entire packet format is shown below:



QUESTION 85
In an 802.3 LAN, PAUSE frames are used for inhibiting data transmissions for a period of time. Which MAC address does this PAUSE mechanism use in order to accomplish this?

A. 00-00-00-00-00-00
B. 00-00-0C-00-00-0F
C. 01-04-0C-07-AC-3C
D. 01-80-C2-00-00-01
E. FF-FF-FF-FF-FF-FF

Answer: D

Explanation:
The globally assigned 48-bit multicast address 01-80-C2-00-00-01 has been reserved for use in MAC Control PAUSE frames for inhibiting transmission of data frames from a DTE in a full duplex mode IEEE 802.3 LAN. IEEE 802.1D-conformant bridges will not forward frames sent to this multicast destination address, regardless of the state of the bridge's ports, or whether or not the bridge implements the MAC Control sub-layer.
Reference:http://www.techfest.com/networking/lan/ethernet3.htm

---

QUESTION 86
A single end station failure can be prevented from disrupting the Spanning Tree algorithm in a LAN according to the 802.1D specification. 802.1D recommends preventing this by:

A. Clearing the Topology Change flag.

B. Re-setting the Topology Change flag to one (1).
C. Configuring the Bridge Forward Delay to less than 1/2 of the Bridge Maxage.
D. Disabling the 801.1D Change Detection Parameter.
E. Disabling the Topology Change Notifications.

Answer: D

Explanation:
The intent of the 802.1D standard is that the detectable failure of a MAC should cause the Bridge Port supported by that MAC to enter the Disabled state. A transition to the Disabled Port state causes the Bridge to initiate a topology change notification, unless, for the Port concerned, topology change detection has been explicitly disabled. Disabling this change detection will result in the prevention of the MAC failure to disrupt the Spanning Tree.

QUESTION 87
What trunking protocol uses an internal tagging mechanism that inserts a 4 byte tag field in the original Ethernet frame?

A. ISL
B. 802.1P
C. DTP
D. 802.1Q
E. DVP

Answer: D

Explanation:
802.1Q is the IEEE standard for tagging frames on a trunk and supports up to 4096 VLANs. IEEE 802.1q uses an internal tagging mechanism which inserts a 4 byte tag field in the original Ethernet frame itself between the Source Address and Type/Length fields. Since the frame is altered, the trunking device re-computes the frame check sequence (FCS) on the modified frame.
Incorrect Answers:

A. In ISL, a 26-byte header that contains a 10-bit VLAN ID is inserted at the beginning of the Ethernet frame.
B, C, E. These are not trunk encapsulation options.

QUESTION 88
Which of the following are true regarding Unidirectional Link Detection? (Choose all that apply.)

A. UDLD uses auto-negotiation to take care of physical signaling and fault detection.
B. Both devices on the link need to support Unidirectional Link Detection.
C. It works by exchanging protocol packets between the neighboring devices.

D. It performs tasks that autonegotiation cannot perform.
E. UDLD is a layer one protocol.

Answer: A, B, C, and D

Explanation:
In order to detect the unidirectional links before the forwarding loop is created, Cisco designed and implemented the UDLD protocol.
UDLD is a Layer 2 (L2) protocol that works with the Layer 1 (L1) mechanisms to determine the physical status of a link. At L1, auto-negotiation takes care of physical signaling and fault detection. UDLD performs tasks that auto-negotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected ports.
When you enable both auto-negotiation and UDLD, L1 and L2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.
UDLD works by exchanging protocol packets between the neighboring devices. In order for UDLD to work, both devices on the link must support UDLD and have it enabled on respective ports.
Each switch port configured for UDLD will send UDLD protocol packets containing the port's own device/port ID, and the neighbor's device/port IDs seen by UDLD on that port. Neighboring ports should see their own device/port ID (echo) in the packets received from the other side.
If the port does not see its own device/port ID in the incoming UDLD packets for a specific duration of time, the link is considered unidirectional.
Incorrect Answers:
E. UDLD is a Layer 2 (L2) protocol that works with the Layer 1 (L1) mechanisms to determine the physical status of a link.
Reference: http://www.cisco.com/warp/public/473/77.html

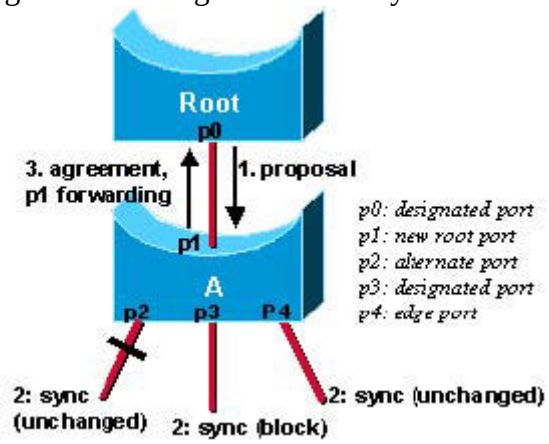
QUESTION 89
On a Certkiller bridge running the rapid spanning tree protocol, which port will send a BPDU with the proposal flag?

A. Designated port in forwarding state
B. Designated port in non-forwarding state or the Root port in forwarding state
C. Root port in blocking state
D. Alternate port
E. None of the above

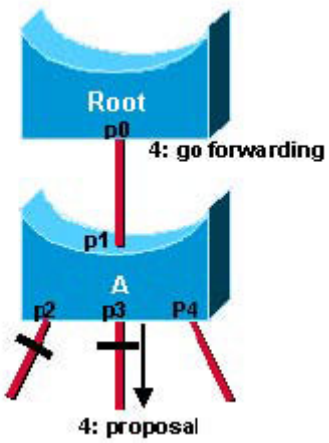
Answer: B

Explanation:
Proposal/Agreement Sequence:
When a port has been selected by the STA to become a designated port, 802.1d still waits twice <forward delay> seconds (2x15 by default) before transitioning it to the forwarding state. In RSTP, this condition corresponds to a port with a designated role but a blocking

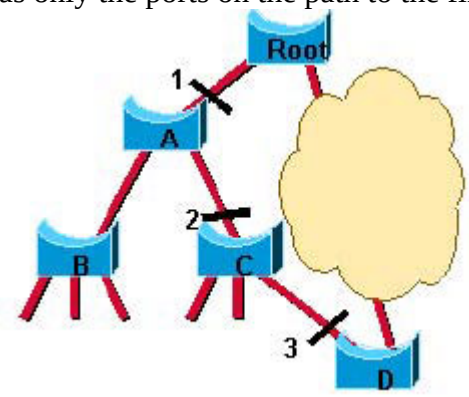
state. The diagrams below illustrate how fast transition is achieved step-by-step. Suppose a new link is created between the root and Switch
A. Both ports on this link are put in a
designated blocking state until they receive a BPDU from their counterpart.



When a designated port is in a discarding or learning state (and only in this case), it sets the proposal bit on the BPDUs it sends out. This is what happens for port p0 of the root bridge, as shown in Step 1 of the diagram above. Because Switch A receives superior information, it immediately knows that p1 is going to be its new root port. Switch A then starts a sync to ensure that all of its ports are in-sync with this new information. A port is in-sync if it meets either of the following criteria:
1. The port is in blocking state (which means discarding, in a stable topology).
2. The port is an edge port.
In order to illustrate the effect of the sync mechanism on different kind of ports, suppose there exists an alternate port p2, a designated forwarding port p3, and an edge port p4 on Switch
A. Notice that p2 and p4 already meet one of the criteria listed above. In order to be in sync (Step 2 of the diagram above), Switch A just needs to block port p3, assigning it the discarding state. Now that all of its ports are in sync, Switch A can now unblock its newly selected root port p1 and reply to the root by sending an agreement message (Step 3). This message is a copy of the proposal BPDU, with the agreement bit set instead of the proposal bit. This ensures that port p0 knows exactly to which proposal the agreement it receives corresponds to.



Once p0 receives that agreement, it can immediately transition to forwarding. This is Step 4 of the figure above. Notice that port p3 was left in a designated discarding state after the sync. In Step 4, that port is in the exact same situation as was port p0 during Step 1. It then starts proposing to its neighbor, attempting to quickly transition to forwarding.
1. The proposal agreement mechanism is very fast, as it does not rely on any timers. This wave of handshakes propagates quickly towards the edge of the network, and quickly restores connectivity after a change in the topology.
2. If a designated discarding port does not receive an agreement after having sent a proposal, it slowly transitions to the forwarding state, falling back to the traditional 802.1d listening-learning sequence. This could happen for instance if the remote bridge doesn't understand RSTP BPDUs, or if the remote bridge's port is blocking.
3. Cisco introduced an enhancement to the sync mechanism that allows a bridge to put only its former root port in the discarding state when syncing. Detailing the way this mechanism works is beyond the scope of this document. However, one can safely assume that it will be invoked in most common reconvergence cases. The scenario described in the Convergence with 802.1w section of this document now becomes extremely efficient, as only the ports on the path to the final blocked port are temporarily confused.



Reference: http://www.cisco.com/warp/public/473/146.html#agree

---

QUESTION 90
A new Certkiller switch is running the rapid spanning tree protocol (RSTP). Upon a topology change, what happens to dynamic entries in the L2 forwarding table?

A. All entries are removed (purged)
B. Aging timer it set to 15 seconds, so idle entries age out
C. Only entries behind port where TC was received are removed
D. All entries are removed except for entries behind edge ports
E. All entries are removed except for those behind edge ports and the port where the TC notification was received
F. None of the above

Answer: E

Explanation:
Topology Change Detection

In RSTP, only non-edge ports moving to the forwarding state cause a topology change. This means that a loss of connectivity is not considered as a topology change any more, contrarily to 802.1d (that is, a port that moves to blocking no longer generates a TC).
When a RSTP bridge detects a topology change, the following happens:
1. It starts the TC While timer with a value equal to twice the hello time for all its non-edge designated ports and its root port if necessary.
2. It flushes the MAC addresses associated with all these ports.
Topology Change Propagation
When a bridge receives a BPDU with the TC bit set from a neighbor, the following happens:
1. It clears the MAC addresses learnt on all its ports except the one that received the topology change.
2. It starts the TC While timer and sends BPDUs with TC set on all its designated ports and root port (RSTP no longer uses the specific TCN BPDU, unless a legacy bridge needs to be notified).
Reference: http://www.cisco.com/warp/public/473/146.html#agree

---

QUESTION 91
All of the Certkiller LAN switches are running the Rapid Spanning Tree Protocol (RSTP). On a bridge running RSPT, BPDU information on the port will be aged:

A. After MaxAge time
B. 15 seconds
C. RSTP does not age out BPDU information on ports
D. After BPDU Age will reach MaxAge or after 3 hello times -which ever occurs first
E. After 6 seconds

Answer: D

Explanation:
On a given port, if hellos are not received for three consecutive times, protocol information can be immediately aged out (or if max_age expires). Because of the previously mentioned protocol modification, BPDUs are now used as a keep-alive mechanism between bridges. A bridge considers that it has lost connectivity to its direct neighboring root or designated bridge if it misses three BPDUs in a row. This fast aging of the information allows quick failure detection. If a bridge fails to receive BPDUs from a neighbor, it is certain that the connection to that neighbor has been lost, as opposed to 802.1d where the problem could have been anywhere on the path to the root.
Reference:
http://www.cisco.com/en/US/partner/tech/ CK3 89/ CK6 21/technologies_white_paper09186a0080094cfa.shtml

---

QUESTION 92
In RSTP (Rapid Spanning Tree Protocol) what is the port that provides an alternative path to the leaves of the Spanning Tree and what state is it in when it is not in the active topology?

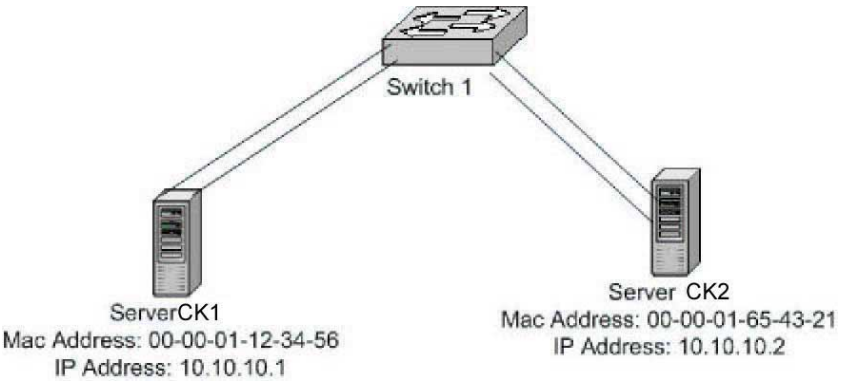
A. Root port and listening
B. Designated port and learning
C. Backup port and discarding
D. Alternate port and forwarding
E. Alternate port and learning

Answer: C

Explanation:
The RSTP provides rapid convergence of the spanning tree by assigning port roles and by determining the active topology. The RSTP builds upon the IEEE 802.1D STP to select the switch with the highest switch priority (lowest numerical priority value) as the root switch. Then the RSTP assigns one of these port roles to individual ports:
1. Root port-provides the best path (lowest cost) when the switch forwards packets to the root switch.
2. Designated port-connects to the designated switch, which incurs the lowest path cost when forwarding packets from that LAN to the root switch. The port through which the designated switch is attached to the LAN is called the designated port.
3. Alternate port-offers an alternate path toward the root switch to that provided by the current root port.
4. Backup port-acts as a backup for the path provided by a designated port toward the leaves of the spanning tree. A backup port can exist only when two ports are connected together in a loopback by a point-to-point link or when a switch has two or more connections to a shared LAN segment.
5. Disabled port-has no role within the operation of the spanning tree.
A port with the root or a designated port role is included in the active topology. A port with the alternate or backup port role is excluded from the active topology.
In a stable topology with consistent port roles throughout the network, the RSTP ensures that every root port and designated port immediately transition to the forwarding state while all alternate and backup ports are always in the discarding state (equivalent to blocking in 802.1D).
Reference:
http://www.cisco.com/en/US/partner/products/hw/switches/ps628/products_configuration_guide_chapter09186a

---

QUESTION 93
The Certkiller network has 2 servers that are to be load balanced. They are connected to a Cisco switch via etherchannels, using 2 ports for each server as shown below:



With regard to this network, which of he following statements are true?

A. Both channels should be given the same channel-id.
B. Load balancing of traffic between two servers will not work.
C. Spanning Tree needs to be disabled on the VLAN for the channel to come up.
D. Channeling to a server is not supported.
E. Channeling to the servers will work only for Fast Ethernet.
F. Up to 4 links can be aggregated per channel

Answer: B

Explanation:
Traffic to each individual server will be load balanced over the Ethernet links in each channel, but traffic can not be load balanced between the servers. In order to do this, a load balancing device will need to be installed.
Incorrect Answers:

A. In this instance there are 2 separate channels, so they will need to have different channel ID's. A single channel consists of Ethernet connections that terminate on the same device on each end.
C. Spanning tree is supported over etherchannel, and should not be disabled.
D. Channeling works between switches, routers, and servers.
E. Channeling works over Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet links.
F. Up to 8 links can be aggregated per channel.

QUESTION 94
The Certkiller switched LAN network is upgrading many of the switch links to Gigabit Ethernet. Which of the following IEEE standards are used for Gigabit Ethernet? (Choose all that apply)

A. 802.3z
B. 802.3ab
C. 802.3ad
D. 802.3af
E. All of the above

Answer: A, B

Explanation:
The Gigabit Ethernet standard is described in the IEEE 802.3z standard, which was defined in 1998. The 802.3ab document specifically describes the 1000BASE-T standard, which was done in 1999. Both describe Gigabit speed implementations, with 802.3z using fiber and 802.3ab using copper.
Incorrect Answers:
C. This standard describes Ethernet Link Aggregation.
D. The 802.3af standard describes a method for providing DTE power via MDI. This is useful for power over Ethernet implementations such as VOIP phones, providing for 15.4 Watts of power per port.

QUESTION 95
Which of the following statements regarding the use of SPAN on a Catalyst 6500 are true?

A. With SPAN an entire VLAN can be configured to be the source.
B.
If the source port is configured as a trunk port, the traffic on the destination port will also be tagged, irrespective of the configuration on the destination port.
C. In any active SPAN session, the destination port will not participate in Spanning Tree.
D. It is possible to configure SPAN to have a Gigabit port as the destination port.
E. In one SPAN session it is possible to monitor multiple ports that do not belong to the same VLAN.

Answer: A, C, D, E

Explanation:
A destination port (also called a monitor port) is a switch port where SPAN sends packets for analysis. If the trunking mode of a SPAN destination port is "on" or "nonegotiate" during SPAN session configuration, the SPAN packets forwarded by the destination port have the encapsulation as specified by the trunk type; however, the destination port stops trunking, and the show trunk command reflects the trunking status for the port prior to SPAN session configuration.
For a detailed discussion on SPAN and RSPAN refer the link below.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_6_3/confg_gd/span.htm

---

QUESTION 96
In order to maximize the speed and duplex setting resulting from auto-negotiation, the Certkiller network administrator has configured all Ethernet ports of a workgroup switch to 100 Mbps, full-duplex. When a workstation NIC configured for auto-negotiation is connected to the switch, the resulting negotiated parameters are 100 Mbps, half-duplex.
What statement best accounts for this result?

A. The workstation NIC must not be properly set for auto-negotiation as the highest port speed and duplex should result from this setup.
B. The port speed is auto-negotiated by the burst of Fast link pulses sent upon port initialization, but duplex negotiation does not use FLPs.
C. The switch should be configured for portfast since the spanning tree protocol leaves the port in the blocking state as it initializes, causing the auto-negotiation process to fail.
D. Without auto-negotiation on the switch, FLPs will not be sent to the workstation, and as a result, the workstation will configure itself to half-duplex.
E. There is problem with the NIC, most likely resulting from order drivers since auto-negotiation will allow the workstation NIC to learn what speed and duplex setting have been configured on the switch.

Answer: D

Explanation:
Speed determination issues may result in no connectivity. However, issues with autonegotiation of duplex generally do not result in link establishment issues. Instead, autonegotiation issues mainly result in performance-related issues. The most common problems when investigating NIC issues deal with speed and duplex configuration. The table below summarizes all possible settings of speed and duplex for FastEthernet NICs and switch ports.
The following table displays all of the various options:

Configuration NIC (Speed/Duplex)		Configuration Switch (Speed/Duplex)	Resulting NIC Speed/Duplex	Resulting Catalyst Speed/Duplex	Comments
AUTO		AUTO	1000 Mbps, Full-duplex	1000 Mbps, Full-duplex	Assuming maximum capability of Catalyst switch, and NIC is 1000 Mbps, full-duplex.
1000 Mbps, Full-duplex		AUTO	1000 Mbps, Full-duplex	1000 Mbps, Full-duplex	Link is established, but the switch does not see

					any autonegotiation information from NIC. Since Catalyst switches support only full-duplex operation with 1000 Mbps, they default to full-duplex, and this happens only when operating at 1000 Mbps.
1000 Mbps, Full-duplex		1000 Mbps, Full-duplex	1000 Mbps, Full-duplex	1000 Mbps, Full-duplex	Correct Manual Configuration
100 Mbps, Full-duplex		1000 Mbps, Full-duplex	No Link	No Link	Neither side establishes link, due to speed mismatch
100 Mbps, Full-duplex		Leading the way inAUTO	IT testing and certifi100 Mbps, Full-duplex c	100 Mbps, Half-duplexation tools, www.test	**Duplex Mismatch 1**king.com
AUTO		100 Mbps, Full-duplex	100 Mbps, Half-duplex	100 Mbps, Full-duplex	**Duplex Mismatch 1**
100 Mb		100 Mb	100 Mb	100 Mb	**C t**

1 A duplex mismatch may result in performance issues, intermittent connectivity, and loss of communication. When troubleshooting NIC issues, verify that the NIC and switch are using a valid configuration.
2 Some third-party NIC cards may fall back to half-duplex operation mode, even though both the switchport and NIC configuration have been manually configured for 100 Mbps,

full-duplex. This behavior is due to the fact that NIC autonegotiation link detection is still operating when the NIC has been manually configured. This causes duplex inconsistency between the switchport and the NIC. Symptoms include poor port performance and frame check sequence (FCS) errors that increment on the switchport. To troubleshoot this issue, try manually configuring the switchport to 100 Mbps, half-duplex. If this action resolves the connectivity problems,you may be running into this NIC issue. Try updating to the latest drivers for your NIC, or contact your NIC card vendor for additional support
Note: Per the IEEE 802.3u specification, it is not possible to manually configure one link partner for 100 Mbps full-duplex and still auto-negotiate to full-duplex with the other link partner. Attempting to configure one link partner for 100 Mbps full-duplex and the other link partner for auto-negotiation will result in a duplex mismatch. This is a result of one link partner auto-negotiating and not seeing any auto-negotiation parameters from the other link partner and defaulting to half-duplex.

QUESTION 97
During routine maintenance, your issue the show interface Fast Ethernet 0 command on Router CK1 . The output from the command is shown in the following exhibit:
FastEthernet0 is up, line protocol is up
Hardware is DEC21140, address is 00e0.1ea8.e299 (bia
00e0.1ea8.e299)
Description: Ethernet 100Mbps
Internet address is 10.11.11.1/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load
3/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
Half-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters 6 weeks, 3 days
Queuing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1953000 bits/sec, 652 packets/sec
5 minute output rate 1407000 bits/sec, 600 packets/sec
47250970 packets input, 3285704002 bytes, 0 no buffer
Received 257038 broadcast, 1056 runts, 0 giants, 0 throttles
1918 input errors, 462 CRC, 0 frame, 0 overrun, 0 ignored, 0
abort
0 watchdog, 0 multicast
311 input packets with dribble condition detected
46457848 packets output, 3093573182 bytes, 0 underruns
0 output errors 759 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Based on the information above, should you be concerned with the operation of this

interface?

A. Yes. There is a physical problem with the connection since there are recorded Runts and CRCs.
B. No. The interface is normal for a 100mb full duplex environment.
C. Yes. There are an excessive amount of collisions that could result from a cable that is too long.
D. No. Collisions, runts and CRC's are normal for a 100mb half-duplex connection.
E. None of the above.

Answer: D

Explanation:
Many performance issues with NICs may be related to data link errors. Excessive errors usually indicate a problem. When operating at half-duplex setting, some data link errors such as FCS, alignment, runts, and collisions are normal. Generally, a one percent ratio of errors to total traffic is acceptable for half-duplex connections. If the ratio of errors to input packets is greater than two or three percent, performance degradation may be noticed.
Incorrect Answers:
A, C. The error counts are normal considering the number of packets that have passed through since the last clearing of counters.
B. The output above clearly says that this interface is operating in half duplex mode. However, if it were actually running in full duplex mode, then there would be reason for alarm as collisions are not possible on a full duplex link.

QUESTION 98
You are connecting a new 10/100 NIC to a Catalyst 5000 switch port. You want to achieve the most optimal settings possible. Which settings should you use?

A. NIC: 100 Mbps & Full-duplex
Catalyst: Auto
B. NIC: Auto
Catalyst: 100 Mbps & Full-duplex
C. NIC: 100 Mbps & Half-duplex
Catalyst: Auto
D. NIC: 100 Mbps & Half-duplex
Catalyst: 10 Mbps & Half-duplex

Answer: C

Explanation:
The speed and duplex cannot be Hard-Coded as full duplex on only one link. This will result a duplex mismatch. The default setting, when set to auto, is always (half-duplex) for port switch or NIC card. Note that setting the connections to auto on both devices is acceptable.

Incorrect Answers:

A. The Catalyst will default to half duplex, causing a mismatch.
B. The NIC will default to half duplex, causing a mismatch.
D. In this case both the Catalyst and the NIC have their information hard coded, but the throughput speeds do not match.
Reference:
http://www.cisco.com/warp/public/473/46.html

QUESTION 99
You are connecting a new PC with a 10/100 NIC to a Catalyst switch. The switch port is configured for auto negotiation for the speed and duplex settings. Which of the following settings on the PC will cause a duplex mismatch?

A. 100mb, half duplex
B. auto-negotiation speed, half duplex
C. Auto-negotiation
D. 100mb, full duplex
E. 10mb, half duplex

Answer: D

Explanation:
Auto set on the switch side with 100mbps full-duplex will result in a duplex-mismatch because auto negotiation always defaults to half-duplex. Per the IEEE 802.3u specification, it is not possible to manually configure one link partner for 100 Mbps full-duplex and still auto-negotiate to full-duplex with the other link partner. Attempting to configure one link partner for 100 Mbps full-duplex and the other link partner for auto-negotiation will result in a duplex mismatch. This is a result of one link partner auto-negotiating and not seeing any auto-negotiation parameters from the other link partner and defaulting to half-duplex.
Incorrect Answers:
A, B, C, E. With auto-negotiation set on the switch, any combination will be acceptable with the exception of full duplex. In the past, there were some issues with having each end set to "auto" but these issues have been resolved and is now a supported configuration from Cisco.
Reference:
http://www.cisco.com/warp/public/473/46.html

QUESTION 100
The Certkiller network includes a Full Duplex Gigabit link between a Router and a Switch. Periodically, you notice the collision counter incrementing slowly. What could be the cause of this problem?

A. The Router is receiving too much traffic and is asserting the Collision signal to be slow down the rate that the switch is sending traffic.

B. Both the Router and the Switch are transmitting at the same time.
C. The switch and the router might be running an ISL trunk.
D. A bug or faulty equipment.
E. A few collisions are normal.

Answer: D

Explanation:
In full duplex mode collisions are impossible so it could only be a bug or problem with hardware. Full-duplex mode allows stations to transmit and receive data simultaneously. This makes for more efficient use of the available bandwidth by allowing open access to the medium. Conversely, this mode of operation can function only with Ethernet switching hubs or via Ethernet cross-over cables between interfaces capable of full-duplex Ethernet. Full-duplex mode expects links to be point-to-point links. There are also no collisions in full-duplex mode, so CSMA/CD is not needed.
Incorrect Answers:

A. There is no such slow down mechanism as described here for a LAN.
B. This would indeed be the cause of a collision in a half duplex LAN, but full duplex allows stations to listen and send at the same time.
C. Trunking alone does affect the number of collisions on a segment.
E. While a few collisions are indeed normal operation for a half duplex LAN, this does not apply for a full duplex segment.

QUESTION 101
You are a technician at Certkiller . You are connecting a new PC to a Catalyst 5000 switch port. After a short time, you notice some performance and intermittent connectivity issues with the PC. As a result of troubleshooting the issue, it is determined that the cause is a duplex mismatch between the PC and switch. Which combination below would cause this?

A. NIC: 100 Mbps & Half-duplex
Catalyst: Auto
B. NIC: 100 Mbps & Full-duplex
Catalyst: Auto
C. NIC: Auto
Catalyst: 100 Mbps & Half-duplex
D. NIC: Auto
Catalyst: Auto

Answer: B

Explanation:
The speed and duplex cannot be Hard-Coded on only one link. This will result a duplex mismatch. When set to auto, the duplex always defaults to half-duplex for both the switch port and for a NIC.

Reference:
http://www.cisco.com/warp/public/473/46.html

QUESTION 102
Which of the following is used in Ethernet networks? (Choose all that apply)

A. Non Canonical format MAC addresses.
B. CSMA/CD for media access.
C. Canonical format MAC addresses.
D. 802.5 encapsulated frames.
E. 802.3 encapsulated frames

Answer: B, C, E

Explanation:
B. Carrier Sense Multi Access with Collision Detection (CSMA/CD) is the media access method on Ethernet network.
C. Ethernet uses the Canonical MAC address format, which means the Least Significant Bit is transmitted first and the Most Significant Bit is transmitted last. The canonical transmission is also known as LSBfirst.
E. Ethernet is 802.3.
Incorrect Answers:

A. Ethernet and Token Ring topologies read MAC addresses differently. For example, a MAC address of 4040.4040.4040 on Ethernet is read as 0202.0202.0202 on Token Ring. Token Rings use Non-canonical MAC address formats, also known as MSB first.
D. Token Ring uses 802.5
Reference:
http://www.cisco.com/en/US/tech/ CK3 31/ CK6 60/technologies_tech_note09186a008012811e.shtml

---

QUESTION 103
You are seeing a few errors on the LAN port of your Cisco router and suspect that the problem is with the link between the router and the switch. This link is configured for 100MB full duplex operation. In order to verify the problem, you connect a hub between the router and the switch so that you can connect your PC on this link and capture the packets. With your PC, you see a very large number of CRC errors, alignment errors, and late collisions. You are seeing the number of these errors increment quickly. What could be the cause of this?

A. Either the Router or the Switch is faulty.
B. These errors will not cause a performance problem.
C. The cabling is causing these errors and should be replaced.
D. Adding the Hub in between might have caused these errors.

Answer: D

Explanation:
The errors cited can all be attributed to increased cable distance, and the fact that the hub most likely does not support Full Duplex.
Incorrect Answers:

A. There were only a few errors on the port before the insertion of the hub into the network. If the router or switch were faulty, we would be seeing these errors at all times.
B. Although some errors, especially collisions, are normal in an Ethernet network, anything more than 2-3% of the packets having errors is excessive and indicates a network problem.
C. Similar to
A. The fact that the excessive errors were seen only after the hub was placed in between the connection indicates that the errors were actually caused by the troubleshooting.

QUESTION 104
If a Certkiller LAN switch Gigabit Ethernet or 10-Gigabit Ethernet port's receive buffer becomes full, what protocol can be used to request the remote port to delay sending frames for a specified time?

A. 802.lU
B. 802.3Z
C. 802.1D
D. 802.3
E. 802.3AF
F. None of the above

Answer: B

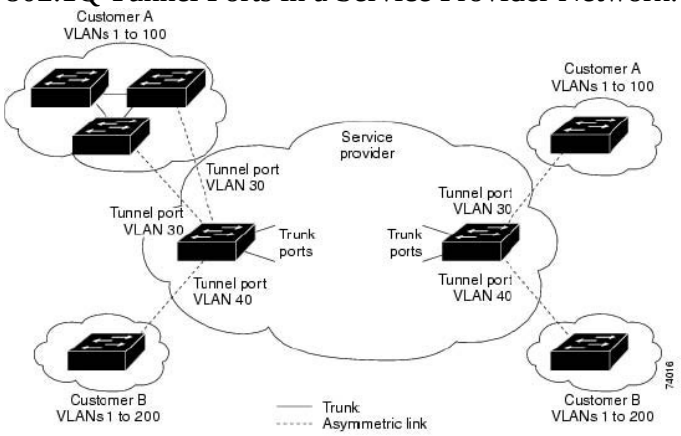
Explanation:
802.3Z defines the standard for Gigabit Ethernet. Included in this is a flow control mechanism.
IEEE 802.3Z Flow Control:
Gigabit Ethernet ports on 802.3Z compliant switch ports use flow control to inhibit the transmission of packets to the port for a period of time; other Ethernet ports use flow control to respond to flow control requests.
If a Gigabit Ethernet port receive buffer becomes full, the port transmits a "pause" packet that tells remote ports to delay sending more packets for a specified period of time. All Ethernet ports (1000Mbps, 100Mbps, and 10Mbps) can receive and act upon "pause" packets from other devices.
Incorrect Answers:
A: This draft defined some technical and editorial changes to the 802.1 standard.
C: This defines the Spanning Tree Protocol
D: This defines the CSMA/CD Ethernet standard.
E: This defines power over Ethernet standards commonly used for VOIP applications.

QUESTION 105
Certkiller Telecom is a service provider that wants to offer service for transporting dot1q trunk traffic between remote customer sites. This service provider has Catalyst switches in its network with ISL trunks in the core. What feature can Certkiller Telecom use with current setup to provide the service to the customer over a single VLAN?

A. VLAN translation
B. Layer 2 Protocol Tunneling
C. VLAN mapping
D. Dot1q Tunneling
E. None of the above

Answer: D

Explanation:
The VLAN ranges required by different customers in the same Service Provider network might overlap, and customer traffic through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the 802.1Q specification.
802.1Q tunneling enables Service Providers to use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated.
A port configured to support 802.1Q tunneling is called a tunnel port. When you configure tunneling, you assign a tunnel port to a VLANID that is dedicated to tunneling. Each customer requires a separate Service Provider VLAN ID, but that Service Provider VLANID supports VLANs of all the customers.
802.1Q Tunnel Ports in a Service Provider Network:



When configuring 802.1Q tunneling on an edge switch, you must use 802.1Q trunk ports for sending packets into the Service Provider network. However, packets going through the core of the Service Provider network can be carried through 802.1Q trunks, ISL trunks, or nontrunking links.
Reference:

http://www.cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_chapter09186a00801f

---

QUESTION 106
Troubleshooting STP convergence errors reveals that a switched network has multiple bridging loops, which is periodically causing problems. What Cisco IOS switching feature, if used improperly, would most likely cause these errors?

A. Port Fast
B. Uplink Fast
C. Backbone Fast
D. Dot1q Trunking
E. Fast EtherChannel

Answer: A

Explanation:
Spanning tree PortFast causes a spanning tree port to enter the forwarding state immediately, bypassing the listening and learning states. You can use PortFast on switch ports connected to a single workstation or server to allow those devices to connect to the network immediately, rather than waiting for spanning tree to converge. PortFast should be used only when connecting a single end station to a switch port. Otherwise, you might create a network loop.
Incorrect Answers:
B. UplinkFast provides fast convergence after a spanning tree topology change and achieves load balancing between redundant links using uplink groups. An uplink group is a set of ports (per VLAN), only one of which is forwarding at any given time. Specifically, an uplink group consists of the root port (which is forwarding) and a set of blocked ports, except for self-looping ports. The uplink group provides an alternate path in case the currently forwarding link fails.
C. BackboneFast is initiated when a root port or blocked port on a switch receives inferior BPDUs from its designated bridge. An inferior BPDU identifies one switch as both the root bridge and the designated bridge. When a switch receives an inferior BPDU, it indicates that a link to which the switch is not directly connected (an indirect link) has failed (that is, the designated bridge has lost its connection to the root bridge). Under normal spanning tree rules, the switch ignores inferior BPDUs for the configured maximum aging time.
The switch tries to determine if it has an alternate path to the root bridge. If the inferior BPDU arrives on a blocked port, the root port and other blocked ports on the switch become alternate paths to the root bridge. (Self-looped ports are not considered alternate paths to the root bridge.) If the inferior BPDU arrives on the root port, all blocked ports become alternate paths to the root bridge. If the inferior BPDU arrives on the root port and there are no blocked ports, the switch assumes that it has lost connectivity to the root bridge, causes the maximum aging time on the root to expire, and becomes the root switch according to normal spanning tree rules.
If the switch has alternate paths to the root bridge, it uses these alternate paths to transmit

a new kind of PDU called the Root Link Query PDU. The switch sends the Root Link Query PDU out all alternate paths to the root bridge. If the switch determines that it still has an alternate path to the root, it causes the maximum aging time on the ports on which it received the inferior BPDU to expire. If all the alternate paths to the root bridge indicate that the switch has lost connectivity to the root bridge, the switch causes the maximum aging times on the ports on which it received an inferior BPDU to expire. If one or more alternate paths can still connect to the root bridge, the switch makes all ports on which it received an inferior BPDU its designated ports and moves them out of the blocking state (if they were in blocking state), through the listening and learning states, and into the forwarding state.
D. The 802.1Q trunking method is the industry standard for trunk links, and can be used as an alternative to ISL. The use of either trunking method alone will not cause any bridging loops.
E. Fast Etherchannel simply provides a way to bond multiple Ethernet links into one larger channel. It will not introduce any STP loops into the network.

QUESTION 107
The speed and duplex settings are being configured for each port in a Catalyst switch. When trying to set the duplex mode on Port 1/1, what does the following message mean: "Port 1/1 is in auto-sensing mode"?

A. Port 1/1 has auto-negotiated the duplex correctly.
B. An error has occurred - the duplex setting of auto is not valid.
C. CDP has detected that both sides are set for auto-negotiating.
D. An error has occurred - the duplex is now mismatched.

Answer: B

Explanation:
When a port is in auto-sensing mode, both its speed and duplex are determined by auto-sensing. An error message is generated if you attempt to set the transmission type of auto-sensing ports. On a 10/100 module, if a port speed is set to auto, its transmission type (duplex) will also set to auto automatically, i.e., the duplex of an auto-speed port is not settable. The only two configurable choices for duplex settings are full and half.

QUESTION 108
The Certkiller network is experiencing network connectivity problems soon after an end-user disconnected her PC and connects a switch with an unknown configuration into an access layer switch port, which has spanning-tree portfast configured. What should be configured on the access layer switch to prevent the network connectivity problems? (Select two)

A. Certkiller 2950(config-if)# spanning-tree portfast bpdufilter enable
B. Certkiller 2950(config-if)# spanning-tree portfast bpduguard enable
C. Certkiller 2950(config-if)# no spanning-tree portfast
D. Certkiller 2950(config-if)# spanning-tree link-type point-to-point

E. Certkiller 2950(config-if)# spanning-tree link-type shared
F. Certkiller 2950(config)# no spanning-tree backbonefast
G. Certkiller 2950(config)# no spanning-tree uplinkfast

Answer: B, C

Explanation:
The following explains the portfast Bridge Protocol Data Unit (BPDU) guard feature. This feature is one of the Spanning-Tree Protocol (STP) enhancements created by Cisco to enhance switch network reliability, manageability, and security.
STP configures a meshed topology into a loop-free, tree-like topology. When the link on a bridge port goes up, there is STP calculation done on that port. The result of the calculation will be the transition of the port into forwarding or blocking state, depending on the position of the port in the network, and the STP parameters. This calculation and transition period usually takes about 30-50 seconds. At this time, no user data is passing via the port. Some user applications may timeout during this period.
To allow immediate transition of the port into forwarding state, the STP portfast feature is enabled. Portfast transitions the port into STP forwarding mode immediately upon linkup. The port still participates in STP in the event that if the port is to be a part of the loop, it will eventually transition into STP blocking mode.
As long as the port is participating in STP, there is a possibility that some device attached to that port and also running STP with lower bridge priority than that of the current root bridge, will assume the root bridge function and affect active STP topology, thus rendering the network suboptimal. Permanent STP recalculation caused by the temporary introduction and subsequent removal of STP devices with low (zero) bridge priority represent a simple form of Denial of Service (DoS) attack on the network.
The STP portfast BPDU guard enhancement is designed to allow network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports with STP portfast enabled are not allowed to influence the STP topology. This is achieved by disabling the port with portfast configured upon reception of BPDU. The port is transitioned into errdisable state, and a message is printed on the console. This is done via the use of the "spanning-tree portfast bpduguard enable" command.
Reference:
http://www.cisco.com/en/US/tech/ CK3 89/ CK6 21/technologies_tech_note09186a008009482f.shtml

---

QUESTION 109
A Certkiller LAN switch has been configured as shown below:

```
Switch(config)# wrr-queue bandwidth 10 20 70 1
Switch(config)# no wrr-queue cos-map
Switch(config)# wrr-queue cos-map 1 0 1
Switch(config)# wrr-queue cos-map 2 2 4
Switch(config)# wrr-queue cos-map 3 3 6 7
Switch(config)# wrr-queue cos-map 4 5
```

What does the IOS configuration displayed in the exhibit accomplish on a Catalyst

2900 switch?

A. It enables frames with a CoS 0 or CoS 1 marking to be serviced by WRR (Weight Round Robin) queing with a weighting value of 1.
B. It enables frames with a CoS 5 marking to be serviced by the expedite queue.
C. It guarantees 10% of the link bandwidth to Queue 1 and 20% to queue 2 and 70% to queue 3. Queue 4 is not used.
D. It sets up the 3 CoS-to-DSCP mappings and DSCP-to-CoS mappings.
E. It sets up the WRR queueing where frames with a CoS of 3 or 6 or 7 will have the highest priority.

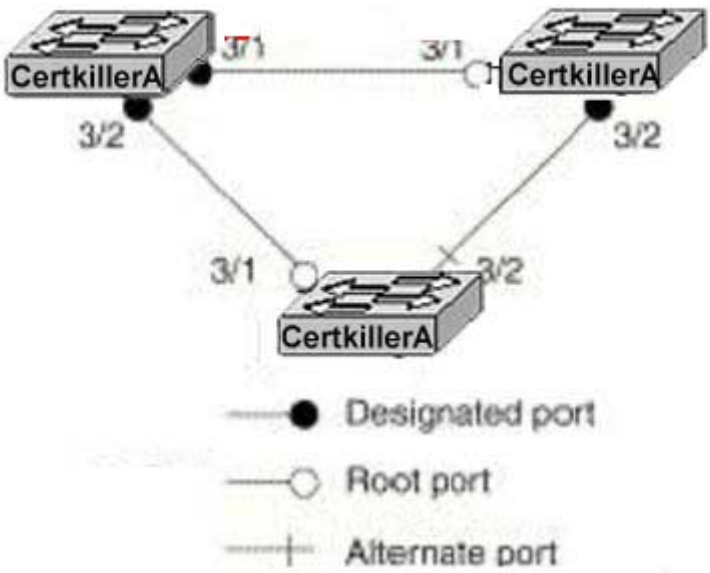
Answer: E

Explanation:
WRR allows bandwidth sharing at the egress port. This command defines the bandwidths for egress WRR through scheduling weights. Four queues participate in the WRR unless you enable the egress expedite queue. The expedite queue is a strict-priority queue that is used until it is empty before using one of the WRR queues.
There is no order of dependencies for the wrr-queue bandwidth command. If you enable the egress priority, the weight ratio is calculated with the first three parameters; otherwise, all four parameters are used.
The WRR weights are used to partition the bandwidth between the queues in the event all queues are nonempty. For example, entering weights of 1:3 means that one queue gets 25 percent of the bandwidth and the other queue gets 75 percent as long as both queues have data.
Entering weights of 1:3 do not necessarily lead to the same results as entering weights at 10:30. Weights at 10:30 mean that more data is serviced from each queue and the latency of packets being serviced from the other queue goes up. You should set the weights so that at least one packet (maximum size) can be serviced from the lower priority queue at a time. For the higher priority queue, set the weights so that multiple packets are serviced at any one time.
To map CoS values to drop thresholds for a queue, use the wrr-queue cos-map command. Use the no form of this command to return to the default settings.
wrr-queue cos-map queue-id threshold-id cos-1 ... cos-n
no wrr-queue cos-map
Syntax Description

queue-id	Queue number; the valid value is 1.
threshold-id	Threshold ID; valid values are from 1
	to 4.
cos-1 ... cos-n	CoS value; valid values are from 0 to
	7.

Defaults
The defaults are as follows:
Receive queue 1/drop threshold 1 and transmit queue 1/drop threshold 1: CoS 0 and 1.
Receive queue 1/drop threshold 2 and transmit queue 1/drop threshold 2: CoS 2 and 3.
Receive queue 2/drop threshold 3 and transmit queue 2/drop threshold 1: CoS 4 and 6.
Receive queue 2/drop threshold 4 and transmit queue 2/drop threshold 2: CoS 7

QUESTION 110
The Certkiller switched LAN is shown below:



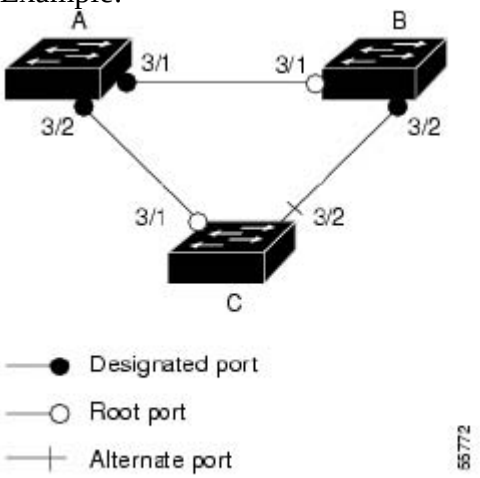
In the shown diagram, Switch Certkiller A is the Root of Spanning Tree If there is a Unidirectional link failure between switches Certkiller A and Certkiller C, and Switch Certkiller C stops receiving BPDUs from Switch Certkiller A, it will transition its blocked port to the forwarding state and we can have a Spanning Tree loop. What features can we use to prevent this from happening? (Choose Two)

A. Portfast
B. Portfast BPDU guard
C. UDLD
D. Portfast BPDU filter
E. Loopguard

Answer: C, E

Explanation:
Loop guard helps prevent bridging loops that could occur because of a uni-directional link failure on a point-to-point link. When enabled globally, the loop guard applies to all point-to-point ports on the system. Loop guard detects root ports and blocked ports and ensures that they keep receiving BPDUs from their designated port on the segment. If a

loop guard enabled root or blocked port stop a receiving BPDUs from its designated port, it transitions to the loop-inconsistent blocking state, assuming there is a physical link error on this port. The port recovers from this loop-inconsistent state as soon as it receives a BPDU.
You can enable loop guard on a per-port basis. When you enable loop guard, it is automatically applied to all of the active instances or VLANs to which that port belongs. When you disable loop guard, it is disabled for the specified ports. Disabling loop guard moves all loop-inconsistent ports to the listening state.
If you enable loop guard on a channel and the first link becomes unidirectional, loop guard blocks the entire channel until the affected port is removed from the channel.
Example:



In this example:
Switches A and B are distribution switches.
Switch C is an access switch.
Loop guard is enabled on ports 3/1 and 3/2 on Switches A, B, and C.
Enabling loop guard on a root switch has no effect but provides protection when a root switch becomes a nonroot switch.
Note:
You can enable UniDirectional Link Detection (UDLD) to help isolate the link failure. A loop may occur until UDLD detects the failure, but loop guard will not be able to detect it.
Loop guard has no effect on a disabled spanning tree instance or a VLAN.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080160

QUESTION 111
You are implementing NAT (Network Address Translation) on the Certkiller network. Which of the following are features and functions of NAT? (Choose all that apply)

A. Dynamic network address translation using a pool of IP addresses.

B. Destination based address translation using either route maps or extended access-lists.
C. NAT overloading for many to one address translations.
D. Inside and outside source static network translation that allows overlapping network address spaces on the inside and the outside.
E. NAT can be used with HSRP to provide for ISP redundancy.
F. All of the above.

Answer: A, B, C, and D

Explanation:
A, B, C, D all describe various methods of implementing NAT.
Incorrect Answers:
E. With HSRP, the standby router would not have the NAT entries of the primary router, so when the fail-over occurs, connections will time out and fail.
Reference:
http://www.cisco.com/en/US/partner/tech/ CK6 48/ CK3 61/technologies_white_paper09186a0080091cb9.shtml
http://www.cisco.com/en/US/partner/tech/ CK6 48/ CK3 61/technologies_q_and_a_item09186a00800e523b.shtml

---

QUESTION 112
Which attributes should a station receive form a DHCP server?

A. IP address, network mask, MAC address and DNS server
B. IP address, DNS, default gateway and MAC address
C. IP address, network mask, default gateway and host name
D. IP address, network mask, default gateway and MAC address
E. None of the above

Answer: E

Explanation:
DHCP servers can supply the following information to hosts on the LAN:
IP address
Subnet mask
Primary DNS server
Secondary DNS servers
Default gateway.
Incorrect Answers:
A, B, D. MAC addresses are burned in addresses that are obtained from the NIC hardware of a PC, not a DHCP server.
C. DHCP servers do not supply host names (such as those used in NetBIOS) or MAC addresses.

QUESTION 113
Which Cisco specific method should be configured on routers to support the need

for a single default gateway for LAN hosts when there are two gateway routers providing connectivity to the network?

A. DHCP
B. RIP
C. OSPF
D. HSRP
E. VRRP

Answer: D

Explanation:
Hot Standby Routing Protocol enables a virtual gateway on LAN networks, and enables the ability to provide a single default gateway for hosts to use, even though multiple routers are in use. This can provide for a level of load balancing, along with automatic failover capability for redundancy.
Additional Information on HSRP follows:

Hot Standby Routing Protocol (HSRP)

Hot Standby Routing Protocol (HSRP) is a Cisco proprietary protocol that brings routing functionality to end devices that would otherwise be incapable of taking advantage of redundant network connections. HSRP enables a pair of Cisco routers to work together to present the appearance of a single virtual default-gateway to end devices on a LAN segment. When you configure HSRP, the administrator assigns the virtual IP address whereas the Cisco IOS chooses a MAC address that falls within Cisco's MAC address block.

HSRP uses a priority scheme that enables routers within the same *standby group* to determine which is the *Active router* and which is the *Standby router*. The router with the highest priority is designated as the Active router; this would be the router that will forward all traffic. The mode of the router (Active/Standby) is communicated among routers within the same HSRP group through the HSRP Hello Protocol. A router that is a member of an HSRP group assumes it is in the Active mode until it hears an HSRP Hello that contains a priority that is higher than that configured on its interface. By default, the HSRP Hellos are sent out every 3 seconds and the hold timer is 10 seconds. If an HSRP router in Standby mode misses three consecutive HSRP Hellos, the router will assume that the Active router is finished and will transition into Active mode.

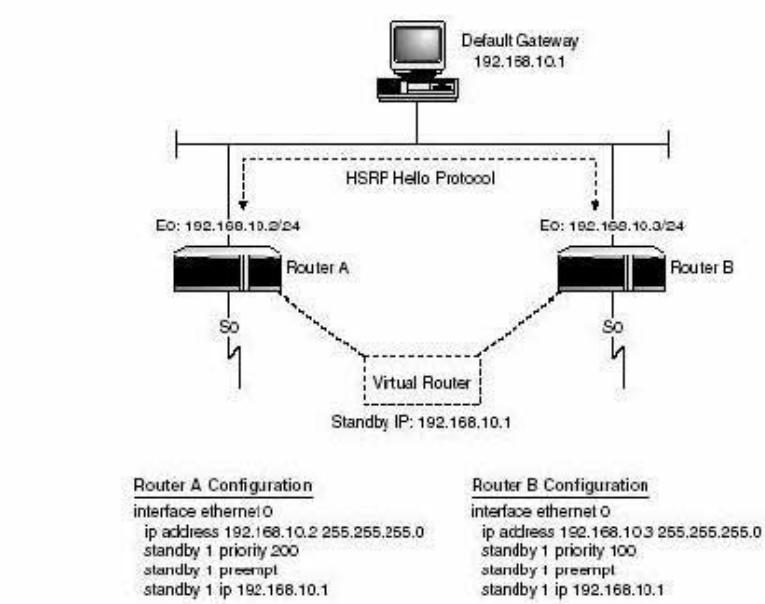


Figure 8.9
Simple HSRP example.

Incorrect Answers:

A. DHCP is the Dynamic Host Configuration Protocol, used to provide IP addressing, default gateway, and DNS information to LAN hosts.
B, C. These are routing protocols, and do not provide a means for allowing 2 or more routers to act as a single default gateway.
E. VRRP is the Virtual Router Redundancy Protocol, which is very similar to HSRP. The major difference between the two is that HSRP is Cisco proprietary, while VRRP is an industry standard. This question asked for a Cisco specific solution.

QUESTION 114
You are attempting to properly subnet the IP space of one of the Certkiller location. For the network "200.10.10.0" there is a need for 3 loopback interfaces, 2 point to point links, one Ethernet with 50 stations and one Ethernet with 96 stations. What option below would be the most efficient (for saving IP addresses)?

A. 200.10.10.1/32, 200.10.10.2/32, 200.10.10.3/32
200.10.10.4/30, 200.10.10.8/30
200.10.10.64/26, 200.10.10.128/25
B. 200.10.10.0/32, 200.10.10.1/32, 200.10.10.2/32
200.10.10.4/32, 200.10.10.8/31
200.10.10.64/26, 200.10.10.128/25
C. 200.10.10.1/32, 200.10.10.2/32, 200.10.10.3/32
200.10.10.4/31, 200.10.10.8/32
200.10.10.64/27, 200.10.10.128/27
D. D. 200.10.10.1/31, 200.10.10.2/31, 200.10.10.3/31
200.10.10.4/30, 200.10.10.8/30
200.10.10.64/27, 200.10.10.128/26

E. There is not enough address available on that network for these subnets.

Answer: A

Explanation:
Choice A will provide the necessary subnetting to achieve all of the necessary network/host combinations that are needed at this location. Since each loopback interface is used only as an internal network to the router, no actual hosts are needed so the host subnet mask of a /32 will be sufficient for all three loopback interfaces. Point to point networks commonly use the /30 subnet mask, since in any point to point link, only two hosts are needed (one for the serial interface of the router at each end). Finally, the subnet mask of /26 will provide for 62 useable addresses and the final subnet mask of /25 will provide for 126 useable IP hosts on the second Ethernet network.
Incorrect Answers:
B. This answer includes /32 network masks for the Pt-Pt links, which can not be used for the two point to point links, since they do not provide any useable IP addresses.
C. This answer includes /32 network masks for the Pt-Pt links, which can not be used for the two point to point links, since they do not provide any useable IP addresses. In addition, the subnet mask of /27 provides for only 30 useable IP addresses for the two Ethernet segments.
D. The /27 subnet mask will provide for only 30 useable IP addresses for one of the Ethernet networks, which is insufficient.
Note: Until IOS version 12.2, a /31 address could not be used for point to point links because it does not provide useable IP addresses. However, /31 addressing for point to point links has been an option in Cisco IOS since version 12.2 and is an IEEE standard defined in RFC 3021 http://www.faqs.org/rfcs/rfc3021.html

---

QUESTION 115
What option is the best way to apply CIDRI if a service provider wants to summarize the following addresses: 200.1.0.0/16, 200.2.0.0/16, 200.3.0.0/16, 200.5.0.0/16, 200.6.0.0/16, 200.7.0.0/16?

A. 200.0.0.0/14, 200.4.0.0/15, 200.6.0.0/16, 200.7.0.0/16
B. 200.0.0.0/16
C. 200.4.0.0/14, 200.2.0.0/15, 200.2.0.0/16, 200.1.0.0/16
D. 200.4.0.0/14, 200.2.0.0/15, 200.1.0.0/16
E. 200.0.0.0/18

Answer: D

Explanation:
The Network 200.4.0.0/14 will encompass the 200.5.0.0, 200.6.0.0 and 200.7.0.0 networks. The second summarization, 200.2.0.0/15 will take care of both the 200.2.0.0 and 200.3.0.0 networks. Finally, the last network is needed in order to include the only remaining network, which is 200.1.0.0/16. This will summarize all 6 networks using only 3 statements.

Incorrect Answers:

A. Although this answer will also fulfill the needs of summarizing all 6 networks, it is not the most efficient way as 4 network entries are needed here, instead of only 3 in answer choice D.
B. This will mean that only the 200.0.0.0/16 network is advertised, which is not even one of the networks that need to be summarized.
C. This is also not the most efficient choice, as the third statement (200.2.0.0/16) is redundant, since this network is already included in the 200.2.0.0/15 summarized route.
E. This network mask would not include all of the needed networks.

QUESTION 116
Which Network Address Translation type describes the internal network that uses private network addresses?

A. Inside local
B. Inside global
C. Outside local
D. Outside global
E. None of the above

Answer: A

Explanation:
Cisco uses the term inside local for the private IP addresses and inside global for the public IP addresses. The enterprise network that uses private addresses, and therefore that needs NAT, is the "inside" part of the network. The Internet side of the NAT function is the "outside" part of the network. A host that needs NAT has the IP address it uses inside the network, and it needs an IP address to represent it in the outside network.
Incorrect Answers:
B. The inside global address is a legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world.
C. The outside local address is the IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it is allocated from an address space routable on the inside.
D. The outside global address the IP address assigned to a host on the outside network by the host's owner. The address is allocated from a globally routable address or network space.

QUESTION 117
A network administrator of Certkiller .com is using a private IP address space for the company network with many to one NAT to allow the users to have access to the Internet. Shortly after this, a web server is added to the network. What must be done to allow outside users access to the web server via the Internet?

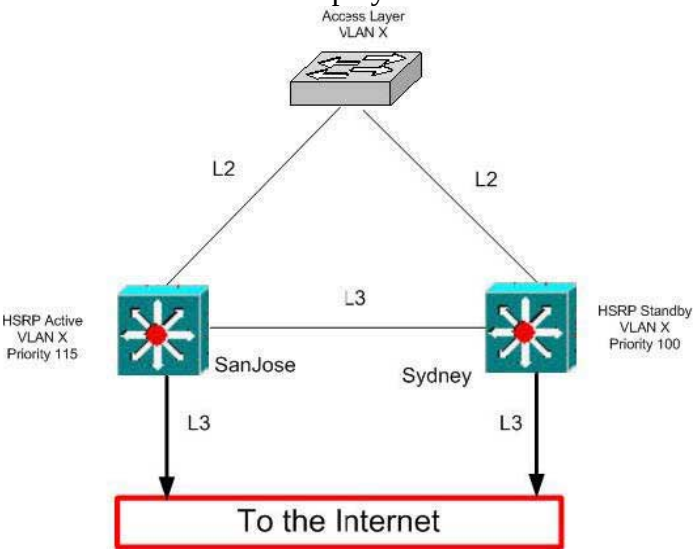
A. Use a dynamic mapping with the reversekeyword.

B. Place the server's internal IP address in the external NAT records.
C. There must be a static one to one NAT entry for the web server's address.
D. Nothing more needs to be done as dynamic NAT is automatic.
E. Place the server's IP address into the NAT pool.

Answer: C

Explanation:
Without a static NAT mapping, the server will be NATed out of the NAT pool. Sine many to one NAT (PAT) uses dynamic port mapping, no outside stations will be able to reach the server consistently.

QUESTION 118
The Certkiller LAN is displayed below:



Users in VLAN X behind the Access Layer switch complain that they cannot access the Internet when both layer 3 links in the San Jose switch fail. When only one of the L3 links in San Jose fail, users are still able to get to the Internet. Which command should be used to ensure connectivity to the Internet, even if both L3 San Jose links fail?

A. Standby track
B. Standby timer
C. Standby authentication
D. Standby use-bia
E. Standby priority

Answer: A

Explanation:
Interface tracking allows you to specify another interface on the router for the HSRP process to monitor in order to alter the HSRP priority for a given group.
If the specified interface's line protocol goes down, the HSRP priority of this router is reduced, allowing another HSRP router with higher priority to become active.

Incorrect Answers:
B. Standby timer is used to set the hello time between HSRP routers.
C. Standby authentication is used as a security measure between HSRP routers, using a password authentication process.
D. By default, HSRP uses the preassigned HSRP virtual MAC address on Ethernet and FDDI, or the functional address on Token Ring. To configure HSRP to use the interface's burnt-in address as its virtual MAC address, instead of the default, use the standby use-bia command.
E. The priority is used to determine which router will be the active one.
Reference:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs009.htm

---

QUESTION 119
A diskless workstation boots up and uses BOOTP to obtain the information it needs from a BOOTP server. How will the diskless client obtain the information it needs from the server?

A. The BootP client will use a telnet application to connect to the server, after which the client will use the DHCP server to get hold of the memory image.
B. The BootP client will obtain the memory image after which the client will use a second protocol to gather the necessary information.
C. The BootP client will use a second protocol to gather the necessary information, and then the BootP server will send memory image.
D. The BootP server will gather and provide the client with the information necessary to obtain an image and then the client will use a second protocol to obtain the memory image.
E. None of above.

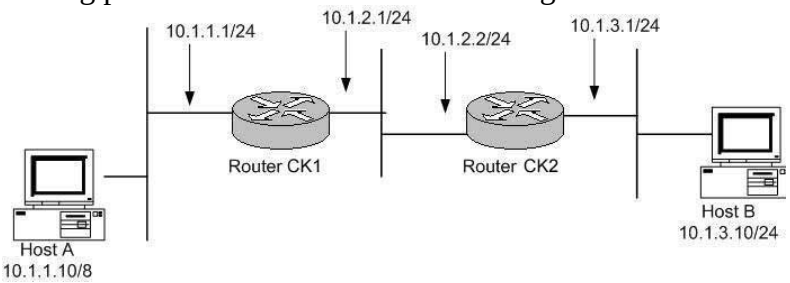
Answer: D

Explanation:
This RFC describes an IP/UDP bootstrap protocol (BOOTP), which allows a diskless client machine to discover its own IP address, the address of a server host, and the name of a file to be loaded into memory and executed. The bootstrap operation can be thought of as consisting of TWO PHASES. This RFC describes the first phase, which could be labeled `address determination and boot file selection'. After this address and filename information is obtained, control passes to the second phase of the bootstrap where a file transfer occurs. The file transfer will typically use the TFTP protocol, since it is intended that both phases reside in PROM on the client. However BOOTP could also work with other protocols such as SFTP or FTP. This RFC suggests a proposed protocol for the ARPA-Internet community, and requests discussion and suggestions for improvements.
BOOTP procedure summary.
Diskless workstation broadcasts a bootp request on port 67. Server responds to this request on port 68. Server provides the client with two pieces information.
1.IP address of client and Hostname of the Server.
2.File name required by client to boot.

The Client then uses TFTP to obtain this file from the Server and boot.
Incorrect Answers:

A. Telnet is not used.
B. The memory image is the last step, not the first.
C. The client must first receive some basic information before using a second protocol, such as TFTP.

QUESTION 120
You want to ensure that Host A has connectivity with Host B. Host A and Host B are connected via Router CK1 and Router CK2 . A has an 8 bit network mask while Host B has a 24 bit network mask. The Certkiller network is shown in the following exhibit. No routing protocols or static routes are configured on either CK1 or CK2 .



Which of the following is required to enable Host A to send packets to Host B?

A. Host A must have a default gateway address of 10.1.1.1.
B. Host B must have a default gateway address of 10.1.3.1.
C. Proxy ARP must be enabled on Router CK1 .
D. Proxy ARP must be enabled on Router CK2 .
E. Host A will not be able to reach host B until routing is enabled in this network.

Answer: B, C

Explanation:
The default gateway for any host must reside on the same subnet as that host so Host B must have its default gateway set to CK2 . In order for packets to reach host B, then host A must have its default gateway set to CK2 also. This will only work if proxy ARP is enabled on CK1 . This is because Host A will assume that Host B is on the same network statement, because its subnet mask is /8. It will therefore ARP to reach Host B. Because of this, CK1 must have proxy ARP enabled to pass the request on to Host B.
For the return traffic, Host B must use a default gateway, because for it to reach Host A a default gateway must be used since it is on a different network segment.
Incorrect Answers:

A. If host A sets its default gateway to CK1 , then it will not be able to send traffic to host B, since no routing exists. All hosts must have a default gateway that resides on the same LAN subnet.
D. Proxy ARP needs to be enabled on CK1 , not CK2 , to pass the traffic to host B.

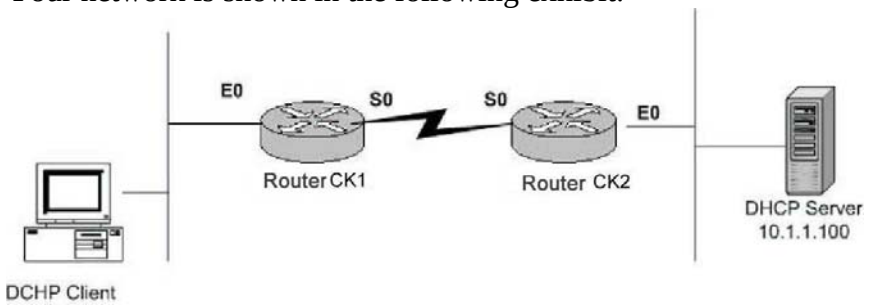
QUESTION 121
Which of the following DNS resource records are valid? (Choose all that apply)

A. NS
B. PTR
C. MX
D. FQDN
E. A
F. None of the above

Answer: A, B, C, E

Explanation:
NS (Name Service), PTR (Pointer), MX (Mail Exchange), and A records are all DNS resource record types.
Incorrect Answers: D
FQDN is Fully Qualified Domain name, for example, www.cisco.com. It has nothing do with DNS Resource Records.

QUESTION 122
Your network is shown in the following exhibit:



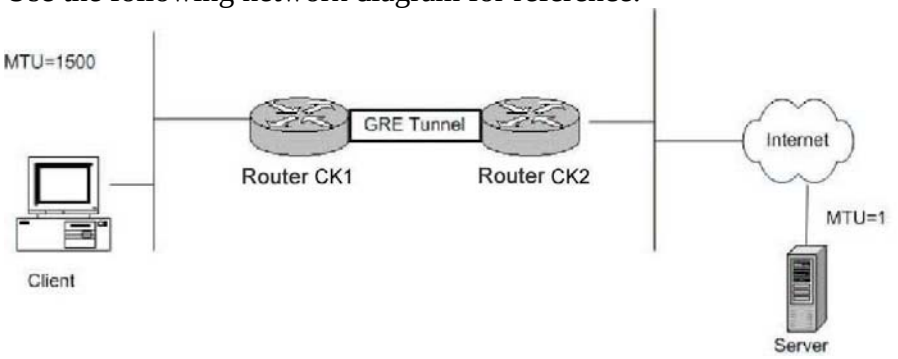
You want all PC's at CK1 to be able to obtain their IP address dynamically from the DHCP server that resides at CK2 . Currently, the hosts are not able to obtain an IP address, and they are receiving error messages saying that the DHCP server is busy or is unavailable. What must be done to enable these PC's to obtain dynamic IP addresses.

A. Enable the command "ip helper-address 10.1.1.100" under the S0 interface on Router CK1 .
B. Enable the command "ip helper-address 10.1.1.100" under the E0 interface on Router CK1 .
C. Enable the command "ip helper-address 255.255.255.255" under the E0 interface on Router CK1 .
D. Enable the command "ip helper-address 255.255.255.255" under the S0 interface on Router CK2 .
E. Enable the command "ip helper-address 10.1.1.100" in global configuration mode on router CK1 .
F. Enable the command "ip helper-address 10.1.1.100" in global configuration mode on router CK2 .

Answer: B

Explanation:
By default, routers drop all broadcast packets sent through them. Because DHCP clients use BOOTP packets, which are broadcasted to all hosts (255.255.255.255), they will be dropped by router CK1 . The "ip helper-address" command enables the router to forward these BOOTP broadcast packets to a specific host, as specified by the address following the "ip helper-address" command. Note that this command must be placed on the router's interface that is receiving the broadcast packets from the hosts, which is E0 of the CK1 router.

QUESTION 123
Use the following network diagram for reference:



There is a GRE tunnel between two routers, CK1 and CK2 . Small files can be sent and received through this tunnel, but large files can not. In addition to this, many web pages are not able to be seen.
On CK1 , you issue the "debug ip icmp" command and try to ping the server with IP address 10.1.1.1 and see the following:
ICMP: dst (10.10.10.10) frag. needed and DF set unreachable sent to
10.1.1.1
How can this problem be solved? (Choose all that apply.)

A. Ensure that no filters exist between the tunnel endpoints blocking ICMP.
B. Increase the IP MTU on the tunnel interfaces to 1500.
C. Enable "ip unreachables" on all interfaces on Router CK2 .
D. Decrease the physical interface MTU on the serial interfaces of CK1 and CK2 to less than 1476 bytes.
E. If the physical link between Router CK1 and Router CK2 is able to support a MTU size greater than 1524 bytes, then increase the interface MTU between the tunnel end points to match 1524.

Answer: A, E
Reference:
Refer to "Why Can't I Browse the Internet when Using a GRE Tunnel?"
http://www.cisco.com/warp/public/105/56.html

QUESTION 124
Select the mode that NTP servers can associate with each other:

A. Client and Server
B. Peer
C. Broadcast/Multicast
D. B and C
E. All the above

Answer: B

Explanation:
NTP synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows events to be correlated when system logs are created and other time-specific events occur. An NTP association can be a peer association (meaning that this system is willing to either synchronize to the other system or to allow the other system to synchronize to it), or it can be a server association (meaning that only this system will synchronize to the other system, and not the other way around). An NTP server can only be configured as a peer to another NTP server.

QUESTION 125
A customer wants to install a new frame-relay router in their network. One goal is to ensure that the new router has the correct configuration to maintain a consistent time and date, like the other routers in the network. The customer wants to configure the new router to periodically poll a UNIX server that has a very reliable and stable clock for the correct time. This will synchronize the new router's clock with the UNIX server. What command should be configured on the new router to synchronize its clock with a centralized clock service?

A. ntp master
B. ntp server
C. ip ntp clock
D. ntp peer
E. sntp master
F. All of the above

Answer: B

Explanation:
To allow the system clock to be synchronized by a time server, use the ntp server global configuration command.
Incorrect Answers:

A. This command will configure the router to act as the NTP master server, providing time information to other devices.
C. This is an invalid command.

D. Use this command if you want to allow the router to synchronize with an NTP peer, or vice versa.
E. SNTP is a simpler version of NTP used by lower end Cisco devices. If SNTP were to be used, the correct syntax would be "sntp server" and not "sntp master."

QUESTION 126
What should be configured on redundant routers to support the need for a default gateway on LAN network hosts when there are two gateway routers providing connectivity to the rest of the network?

A. DHCP
B. RIP
C. OSPF
D. HSRP
E. BOOTP

Answer: D

Explanation:
The Hot Standby Router Protocol (HSRP) provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from default gateway failures in the network. It is implemented on networks where there are two or more gateway routers that provide connectivity to the rest of the network with the standby router acting as an automatic failover should the primary router fail.
Incorrect Answers:
A, E: DHCP and BOOTP are used to provide IP addressing, DNS, and default gateway information to end user hosts.
B, C: RIP and OSPF are routing protocols, and will not provide for automatic default gateway redundancy for PC hosts.

QUESTION 127
With regard to the File Transfer Protocol (FTP), which of the following statements are true?

A. FTP always uses one TCP session for both control and data.
B. With passive mode FTP, both the control and data TCP sessions are initiated from the client.
C. With active mode FTP, the server used the "PORT" command to tell the client on which port it wished to send the data.
D. FTP always uses TCP port 20 for the data session and TCP port 21 for the control session.
E. FTP always uses TCP port 20 for the control session and TCP port 21 for the data session.

Answer: B

Explanation:
For a detailed discussion on FTP refer the link below.
Incorrect Answers:

A. FTP always uses two separate TCP sessions, one for control and one for data.
C. In FTP active mode the client (not the server) uses the PORT command to tell the server on which port it expects the server to send the data.
D, E. These statements are too general as FTP behaves differently based on whether the mode of operation is active or passive.
Reference:
http://www.cisco.com/warp/public/759/ipj_2-3/ipj_2-3_oneb.html

---

QUESTION 128
You use a telnet application to access your Internet router. What statement is true about the telnet application?

A. Telnet does not use a reliable transport protocol.
B. Telnet is a secure protocol because it encrypts every message sent.
C. Telnet sends user names, passwords and every other message in clear text.
D. Telnet encrypts user names, passwords but sends every other message in clear text.
E. Telnet uses UDP as transport protocol.

Answer: C

Explanation:
Telnet is inherently insecure since it sends all data in plain text. This is an important consideration when using telnet across the Internet. For this reason, more secure remote access applications such as SSH have been developed.
Incorrect Answers:
A, E: Telnet uses TCP port 23, which is a reliable protocol.
B, D: No portion of a telnet packet is encrypted or authenticated.

QUESTION 129
What is the method used by SMTP servers on Internet to validate the e-mail address of the message sender?

A. It checks the user address with the MTA sending the message.
B. It validates the domain of the sender address with a DNS server.
C. It does not check the sender address.
D. It checks if the IP address of the MTA sending the message is not spoofed.
E. It checks if the domain of the MTA sending the message matches with the domain of the sender of the message.

Answer: C

Explanation:

When e-mail is handed off today from one organization to another, as a rule no authentication of the sender of the e-mail or the computers delivering it on the sender's behalf takes place.
Due to the spread of SPAM and emails coming from spoofed locations, measures can be taken to minimize their effect. The MTA Authentication Records in DNS Internet Draft describes mechanisms by which a domain owner can publish its set of outgoing Mail Transfer Agents (MTAs), and mechanisms by which SMTP servers can determine what email address is allegedly responsible for most proximately introducing a message into the Internet mail system, and whether that introduction is authorized by the owner of the domain contained in that email address.
However, as a standard rule today, no SMTP server is required to take any security measures to validate the message sender.

QUESTION 130
Upon which protocol or protocols does TFTP rely on?

A. IP and TCP
B. NFS
C. FTP
D. UDP
E. ICMP and UDP
F. TCP

Answer: D

Explanation:
The Trivial File Transfer Protocol (TFTP) is a simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password). TFTP uses UDP port 69.

QUESTION 131
Identify the TCP port numbers with their associated programs: 443, 389, 137, 110, and 23 in the proper sequence:

A. BGP, POP3, SNMP, TFTP, Telnet
B. LDAP, SNMP, TFTP, POP3, Telnet
C. HTTPS, SNMP, POP3, DNS, Telnet
D. Finger, DHCP Server, NetBios Name Server, POP3, Telnet
E. HTTPS, LDAP, NetBios Name Server, POP3, Telnet
F. None of the above

Answer: E

Explanation:
The following shows the TCP port numbers used with the associated applications:
HTTPS (secure WWW): 443

LDAP: 389 on the directory server
NetBios Name Server: 137
POP3: 110
Telnet: 23
Incorrect Answers:

A. BGP uses TCP port 179.
B, C. SNMP uses TCP port 161.
D. Finger uses TCP port 79 while DHCP uses 67 (BOOTP)
A complete list of TCP port numbers and their assignments can be found here:
http://www.iana.org/assignments/port-numbers

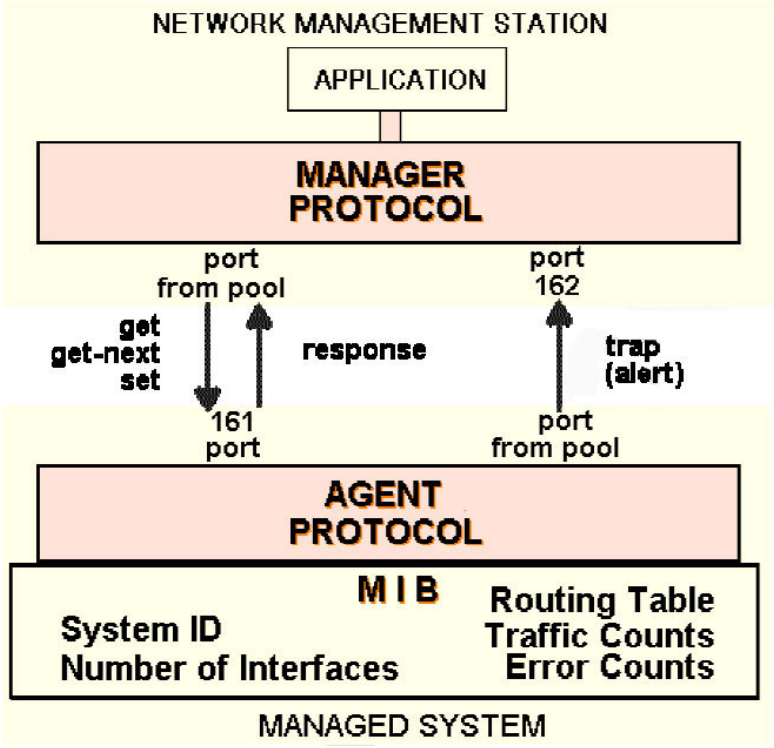
QUESTION 132
On what lower level transport protocol does SNMP rely and why?

A. TCP, because SNMP requires the reliability of TCP, which ensures packets are transmitted reliably, in event that a packet is lost in the network.
B. UDP, because SNMP is an application that does not require the reliability provided by TCP.
C. IP, because SNMP requires the reliability of IP packets, which can detect lost packets and retransmit them if required.
D. UDP, because SNMP is an application that requires the reliability of UDP and UDP's ability to detect lost packets and retransmit them.
E. TCP, because SNMP is an application that does not require detection and retransmission of lost packets.

Answer: B

Explanation:
SNMP uses the User Datagram Protocol (
UDP) as the transport protocol for passing data between managers and agents. UDP, defined in RFC 768, was chosen over the Transmission Control Protocol (TCP) because it is connectionless; that is, no end-to-end connection is made between the agent and the NMS when datagrams (packets) are sent back and forth. This aspect of UDP makes it unreliable, since there is no acknowledgment of lost datagrams at the protocol level. It's up to the SNMP application to determine if datagrams are lost and retransmit them if it so desires. This is typically accomplished with a simple timeout. The NMS sends a UDP request to an agent and waits for a response. The length of time the NMS waits depends on how it's configured. If the timeout is reached and the NMS has not heard back from the agent, it assumes the packet was lost and retransmits the request. The number of times the NMS retransmits packets is also configurable.
At least as far as regular information requests are concerned, the unreliable nature of UDP isn't a real problem. At worst, the management station issues a request and never receives a response. For traps, the situation is somewhat different. If an agent sends a trap and the trap never arrives, the NMS has no way of knowing that it was ever sent. The agent doesn't even know that it needs to resend the trap, because the NMS is not required

to send a response back to the agent acknowledging receipt of the trap.
The upside to the unreliable nature of UDP is that it requires low overhead, so the impact on your network's performance is reduced. SNMP has been implemented over TCP, but this is more for special-case situations in which someone is developing an agent for a proprietary piece of equipment. In a heavily congested and managed network, SNMP over TCP is a bad idea. It's also worth realizing that TCP isn't magic, and that SNMP is designed for working with networks that are in trouble -- if your network never failed, you wouldn't need to monitor it. When a network is failing, a protocol that tries to get the data through but gives up if it can't is almost certainly a better design choice than a protocol that will flood the network with retransmissions in its attempt to achieve reliability.
SNMP uses the UDP port 161 for sending and receiving requests, and port 162 for receiving traps from managed devices. Every device that implements SNMP must use these port numbers as the defaults, but some vendors allow you to change the default ports in the agent's configuration. If these defaults are changed, the NMS must be made aware of the changes so it can query the device on the correct ports.



SNMP use of UDP port numbers.

QUESTION 133
In your network, you want the ability to send some traffic around less congested links. To do this, you want to bypass the normal routed hop-by-hop paths. What technology should you implement?
What should you use?

A. Traffic engineering
B. Traffic tunneling

C. Traffic policing
D. Traffic shaping
E. Traffic routing

Answer: A

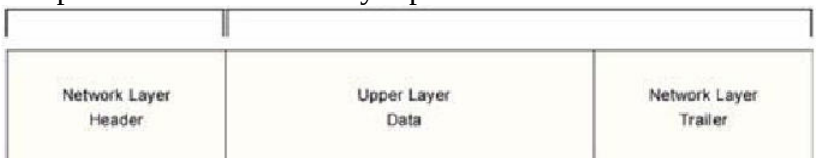
Explanation:
Traffic engineering allows you to bypass the routing protocol information to send traffic over alternative paths.
Incorrect Answers:
B. Using tunnels will not force the traffic over the tunnels to bypass the normal hop by hop routed topology.
C, D. Traffic policing and traffic shaping are methods of QoS.
E. Traffic routing is not a well defined Cisco term.

QUESTION 134
Which of the following are found in a basic Network Layer Packet? (Choose all that apply)

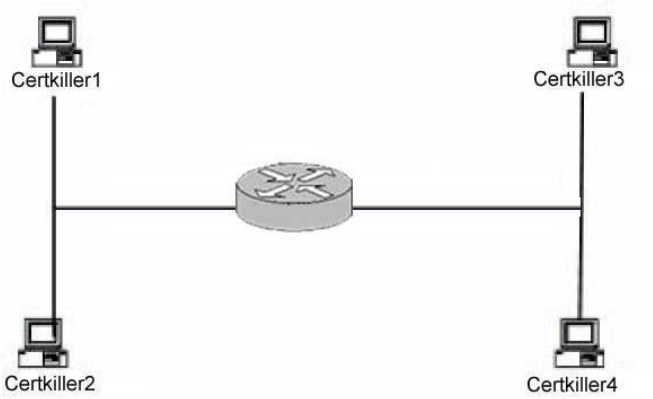
A. Network Layer Trailer
B. Upper Layer Data
C. Network Layer Data
D. Network Layer Header
E. Data Link Layer Header
F. Checksum

Answer: A, B, and D

Explanation:
A packet is an information unit whose source and destination are network-layer entities. A packet is composed of the network-layer header (and possibly a trailer) and upper-layer data. The header and trailer contain control information intended for the network-layer entity in the destination system. Data from upper-layer entities is encapsulated in the network-layer header and trailer. The figure illustrates the basic components of a network-layer packet.



QUESTION 135
The Certkiller network is shown in the following exhibit:



Host Certkiller 3 sends a message to host Certkiller 4. Which type of delivery is this?

A. Direct delivery
B. Partial delivery
C. Installment delivery
D. Indirect delivery
E. Instant delivery
F. Guarantee delivery

Answer: A.

Explanation:
Direct delivery implies that both the devices are on the same network segment (IP subnet) and no router is required for communication between the two.
Incorrect Answers:
D. In indirect delivery the two devices are on different network segments (IP subnets) and a router will be required for the two to communicate.

QUESTION 136
Real Time Protocol uses which of the following as the transport mechanism?

A. RTCP
B. UDP
C. TCP
D. BRI/ISDN
E. None of the above.

Answer: B

Explanation:
RTP uses UDP for transport.
Incorrect Answers:

A. There is no such thing as RTCP.
C. Since RTP is used for real time traffic, it would not make sense to use TCP for

transport, as it provides more overhead that UDP. In addition, the reliable mechanism of TCP is useless for real time traffic such as voice and video traffic, since packets that are resent are too late too late.

QUESTION 137
What should be used to compress Voice over IP packets on a low-speed Frame Relay circuit?

A. TCP header compression
B. FRF.9 payload compression
C. Cisco proprietary payload compression
D. RTP header compression
E. Predictor payload compression

Answer: D

Explanation:
Since VOIP uses the real time protocol (RTP), compressing this type of traffic will be best. RTP is the Internet-standard protocol for the transport of real-time data. It is intended to provide end-to-end network transport functions for applications that support audio, video, or simulation data over multicast or unicast network services.
RTP provides support for real-time conferencing of groups of any size within the Internet. This support includes source identification and support for gateways such as audio and video bridges as well as multicast-to-unicast translators. RTP offers QoS feedback from receivers to the multicast group, as well as support for the synchronization of different media streams.
RTP includes a data portion and a header portion. The data portion of RTP is a thin protocol that provides support for the real-time properties of applications, such as continuous media, including timing reconstruction, loss detection, and content identification.
The header portion of RTP is considerably large. The minimal 12 bytes of the RTP header, combined with 20 bytes of IP header (IPH) and 8 bytes of UDP header, create a 40-byte IP/UDP/RTP header. For compressed-payload audio applications, the RTP packet typically has a 20-byte to 160-byte payload. Given the size of the IP/UDP/RTP header combinations, it is inefficient to transmit the IP/UDP/RTP header without compressing it.
To avoid the unnecessary consumption of available bandwidth, the RTP header compression feature-referred to as CRTP-is used on a link-by-link basis.
RTP can be used over frame relay, HDLC, and PPP links and is meant to be used over slow links (less that 2 Mbps).

QUESTION 138
What best describes the IPv6 Solicited-node Multicast address?

A. For each unicast and anycast addresses configured on an interface of the node or a router, a corresponding solicited-node multicast addresses is automatically enabled.

B. The solicited-node multicast address is scoped at the local link.
C.
Since ARP is not used the in IPv6, the solicited-node multicast addresses is used by nodes and router to learn the link layer address of the neighbor nodes and routers on the same local link.
D. Duplicate Address Detection (DAD) is used to verify if the IPv6 address is already in used on it's local link, before it configure it's own IPv6 address with stateless auto-configuration, Solicited-node multicast addresses probe the local link to make sure.
E. All of the above
F. None of the above

Answer: E

Explanation:
In IP version 6, the solicited-node multicast address facilitates efficient querying of network nodes during address resolution. IPv6 uses the Neighbor Solicitation message to perform address resolution. In IPv4, the ARP Request frame is sent to the MAC-level broadcast, disturbing all nodes on the network segment regardless of whether a node is running IPv4. For IPv6, instead of using ARP requests and disturbing all IPv6 nodes on the local link by using the local-link scope all-nodes address, the solicited-node multicast address is used as the Neighbor Solicitation message destination.
The solicited-node multicast address consists of the prefix FF02::1:FF00:0/104 and the last 24-bits of the IPv6 address that is being resolved.
The following steps show an example of how the solicited-node address is handled for the node with the link-local IPv6 address of FE80::2AA:FF:FE28:9C5A, and the corresponding solicited-node address is FF02::1:FF28:9C5A:
1. To resolve the FE80::2AA:FF:FE28:9C5A address to its link layer address, a node sends a Neighbor Solicitation message to the solicited-node address of FF02::1:FF28:9C5A.
2. The node using the address of FE80::2AA:FF:FE28:9C5A is listening for multicast traffic at the solicited-node address FF02::1:FF28:9C5
A. For interfaces that correspond
to a physical network adapter, it has registered the corresponding multicast address with the network adapter.
As shown in this example, by using the solicited-node multicast address, address resolution that commonly occurs on a link can occur without disturbing all network nodes. In fact, very few nodes are disturbed during address resolution. Because of the relationship between the network interface MAC address, the IPv6 interface ID, and the solicited-node address, in practice, the solicited-node address acts as a pseudo-unicast address for efficient address resolution.
Reference:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wcetcpip/html/cmconmulticastipv6addresses.asp

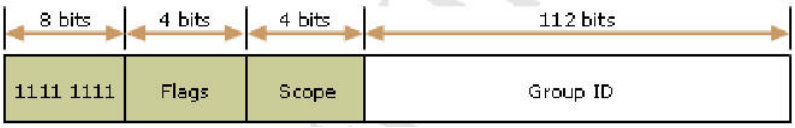
---

QUESTION 139
What is a main difference between the IPv6 and IPv4 multicast?

A. IPv6 has significantly more address space (128 bits), so overlapping addresses are less likely.
B. Multicast Listener Discovery (MLD) replaces IGMP in IPv6 multicasts.
C. MSDP and dense mode multicast is not part of IPv6 multicast.
D. The first 8 bits of Ipv6 Multicast address are always FF (1111 1111).
E. All of the above

Answer: E

Explanation:
A multicast address identifies multiple interfaces, and is used for one-to-many communication. With the appropriate multicast routing topology, packets addressed to a multicast address are delivered to all interfaces that are identified by the address.
IPv6 multicast addresses have the Format Prefix of 1111 1111. An IPv6 address is simple to classify as multicast because it always begins with FF. Multicast addresses cannot be used as source addresses.
Multicast addresses include additional structure to identify their flags, scope, and multicast group, as shown in the following illustration.



MLD is used to exchange membership status information between IPv6 routers that support multicasting and members of multicast groups on a network segment. Membership in a multicast group is reported by individual member hosts, and membership status is periodically polled by multicast routers. MLD is defined in RFC 2710, "Multicast Listener Discovery (MLD) for IPv6." IGMP is not used in IPv6.

QUESTION 140
What best describes the functionality of the Multicast Listener Discovery (MLD)?

A. IPv6 routers use MLD to discover multicast listeners on directly attached links.
B. For each Unicast and Anycast addresses configured on an interface of the node or a router, a corresponding entry is automatically enabled.
C. The MLD addresses is scoped to the local link.
D. Since the ARP is not used in the IPv6, the MLD is used by nodes and routers to learn the link layer address of the neighbor nodes and routers on the same local link.
E. MLD is used to verify if the IPv6 address is already in use on it's local link, before it configure it's own IPv6 address with stateless auto-configuration.

Answer: A

Explanation:
The purpose of Multicast Listener Discovery (MLD) is to enable each IPv6 router to discover the presence of multicast listeners (that is, nodes wishing to receive multicast packets) on its directly attached links, and to discover specifically which multicast

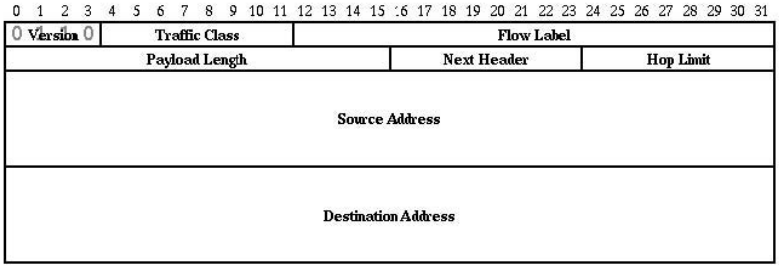
addresses are of interest to those neighboring nodes. This information is then provided to whichever multicast routing protocol is being used by the router, in order to ensure that multicast packets are delivered to all links where there are interested receivers.
MLD is an asymmetric protocol, specifying different behaviors for multicast listeners and for routers. For those multicast addresses to which a router itself is listening, the router performs both parts of the protocol, including responding to its own messages.
If a router has more than one interface to the same link, it need perform the router part of MLD over only one of those interfaces. Listeners, on the other hand, must perform the listener part of MLD on all interfaces from which an application or upper-layer protocol has requested reception of multicast packets.

QUESTION 141
The Certkiller network is migrating from IPv4 to IPv6. What IPv6 header field has a similar function as the "Type of Service" field in an IPv4 header?

A. Flow Label
B. Version
C. Next Header
D. Traffic Class
E. None of above

Answer: D

Explanation:
The IPV6 header is shown below:
Packet Fields



Version
The version field exists for the same purpose as in IPv4, namely to differentiate between different versions of the protocol. Obviously it carries the value of "6" for all IPv6 packets.
Traffic Class
This is similar to the Type of Service (ToS) bits in IPv4, except that it tries to describe the type of traffic rather than the type of service.
Flow Label
This is used to label a "flow" of packets. On problem with a packet switching network is that there's no good way to tell if a bunch of separate packets are related to each other.
Payload Length
This is the length of the packet not including the IPv6 header. It replaces the Total

Length field in IPv4. Unlike IPv4, IPv6 headers are of a fixed length, and there's no point in adding a constant to the length field.
Next Header
This is like the Protocol field from IPv4 - it identifies the higher level protocol. However, unlike IPv4, this is not always a transport layer protocol like TCP or UDP. It takes on special values which are used to implement the IPv6 extension and option mechanisms.
Hop Limit
This is like the TTL (Time To Live) field from IPv4 - it's used to minimize the resources that a packet consumes in the event of a routing loop. Its name has been changed to reflect the actual usage of the field. Namely, it is decremented every hop, rather than every second as was originally intended.
Source/Destination Address
These have the same purpose in IPv4, but have been expanded to 128 bits.
Reference: http://www.mit.edu/~elliot/internet/1998/ipv6-notes.html

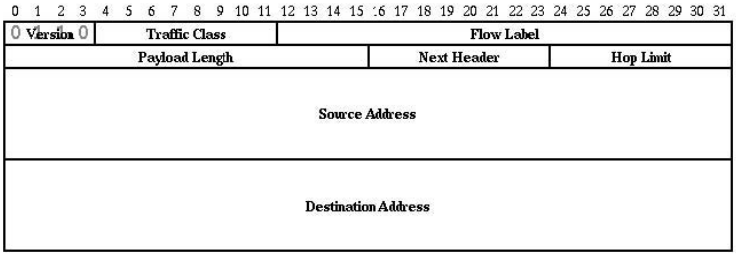
---

QUESTION 142
When comparing the header fields in IP version 4 and IP version 6, what lPv6 header field has a similar function as the IPv4 header field "Type of Service"?

A. Flow Label
B. Version
C. Next Header
D. None of above
E. All of the above

Answer: D

Explanation:
This question is fundamentally the same as number 4 above, except the correct answer "Traffic Class" has been omitted, making choice D correct.
In an IPv6 header, the "Traffic Class" field similar in function to the "ToS" field in IPv4.
The IPV6 header is shown below:
Packet Fields



Version
The version field exists for the same purpose as in IPv4, namely to differentiate between different versions of the protocol. Obviously it carries the value of "6" for all IPv6 packets.
Traffic Class
This is similar to the Type of Service (ToS) bits in IPv4, except that it tries to

describe the type of traffic rather than the type of service.
Flow Label
This is used to label a "flow" of packets. On problem with a packet switching network is that there's no good way to tell if a bunch of separate packets are related to each other.
Payload Length
This is the length of the packet not including the IPv6 header. It replaces the Total Length field in IPv4. Unlike IPv4, IPv6 headers are of a fixed length, and there's no point in adding a constant to the length field.
Next Header
This is like the Protocol field from IPv4 - it identifies the higher level protocol. However, unlike IPv4, this is not always a transport layer protocol like TCP or UDP. It takes on special values which are used to implement the IPv6 extension and option mechanisms.
Hop Limit
This is like the TTL (Time To Live) field from IPv4 - it's used to minimize the resources that a packet consumes in the event of a routing loop. Its name has been changed to reflect the actual usage of the field. Namely, it is decremented every hop, rather than every second as was originally intended.
Reference: http://www.mit.edu/~elliot/internet/1998/ipv6-notes.html

---

QUESTION 143
Which of the following are legal representations of the IPv6 prefix 12AB00000000CD3? (Choose Two)

A. 12AB:0000:0000:CD30:0000:0000:0000:0000/60
B. 12AB:0:0:CD3/60
C. 12AB:: CD3/60
D. 12AB:0:0:CD30::/60
E. 12AB::CD3::/60

Answer: A, D

Explanation:
IPv6 Address Compaction:
In IPv6, the leading zeroes in a 16-bit segment can be compacted.
Example:
fe80:0210:1100:0006:0030:a4ff:000c:0097 becomes fe80:210:1100:6:30:a4ff:c:97
All zeroes in one or more contiguous 16-bit segments can also be represented with a double colon(::).
Example:
ff02:0000:0000:0000:0000:0000:0000:0001Becomes ff02::1.
However, double colons can only be used once in any one address.
Example:
2001:0000:0000:0013:0000:0000:0b0c:3701
Can be:
2001::13:0:0:b0c:3701 or 2001:0:0:13::b0c:3701, but not 2001::13::b0c:3701
For IPv6 Prefix Representation, CIDR-like notations are used to specify the address

prefix length. Examples of this include:
3ffe:0:0:2300:ce21:233:fea0:bc94/60 and 201:468:1102:1::1/64
Finally, an IPv6 Prefix Compaction example is:
2002:0000:0000:18d0:0000:0000:0000:0000/60
Can be represented as:
2002::18d0:0:0:0:0/60
2002:0:0:18d0::/60
In the example shown in this question, 12AB00000000CD3 can be represented either as:
12AB:0000:0000:CD30:0000:0000:0000:0000/60 or 12AB:0:0:CD30::/60

QUESTION 144
IPv6 is being implemented in the Certkiller network. Which of the following is a valid IPv6 Address Type? (Choose Three)

A. Broadcast
B. Multicast
C. Anycast
D. Unicast

Answer: B, C, D

Explanation:
With IPv6 the IETF sought to carve the new address space into functional categories, each of which would enable more-efficient routing through a more-sophisticated hierarchy. These functional categories are known as anycast, unicast, and multicast. Noticeably absent was the broadcast address type. IPv6 doesn't use broadcast addresses, but it satisfies that function through the multicast address type.
IPv6 defines three address types:
Unicast:
Identifies an interface of an individual node.
Multicast:
Identifies a group of interfaces, usually on different nodes. Packets that are sent to the multicast address go to all members of the multicast group.
Anycast:
Identifies a group of interfaces, usually on different nodes. Packets that are sent to the anycast address go to the anycast group member node that is physically closest to the sender.

QUESTION 145
Router CK1 needs to be configured with RIP to support IPv6. Which of the following are the minimum required tasks to configure IPv6 RIP on a Cisco router? (Choose Two)

A. Customizing IPv6 RIP
B. Configuring Tags for RIP routes
C. Enable IPv6 RIP on the interface
D. Configuring IPv6 Multicast routing
E. Enable IPv6 on the router

Answer: C, E

Explanation:
Before configuring the router to run IPv6 RIP, two things must be done. First, globally enable IPv6 using the "ipv6 unicast-routing" global configuration command. Secondly, enable IPv6 on any interfaces on which IPv6 RIP is to be enabled. These are the required

minimum configuration prerequisites.
Incorrect Answers:
A, B, D: These choices describe optional IPv6 RIP configurations. A list of optional components for configuring RIP for IPv6 is shown below:
Customizing IPv6 RIP (optional)
Redistributing Router into an IPv6 RIP Routing Process (optional)
Configuring Tags for RIP Routes (optional)
Filtering IPv6 RIP Routing Updates (optional)
Verifying IPv6 RIP Configuration and Operation (optional)
Reference:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00801d6601.html

---

QUESTION 146
Which types of SNMPv1 messages are sent from the NMS (Network Management Station) using SNMP version 1 to the Agent?

A. Trap, Get and Set
B. Get, Set and Getnext
C. Get, Set, Getnext and GetBulk
D. Get, Set and GetBulk
E. Trap only

Answer: B

Explanation:
SNMP itself is a simple request/response protocol, and the SNMPv1 operations used by the NMS are defined as below.
Get: Allows the NMS to retrieve an object variable from the agent.
GetNext: Allows the NMS to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a NMS wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set: Allows the NMS to set values for object variables within an agent.
Incorrect Answers:
A, E. SNMP traps are used by the agent to inform the NMS of some events.
C, D. GetBulk is used in SNMPv2, not version 1. SNMPv2 defines two new operations: GetBulk and Inform. The GetBulk operation is used to efficiently retrieve large blocks of data. The Inform operation allows one NMS to send trap information to another NMS and to then receive a response. In SNMPv2, if the agent responding to GetBulk operations cannot provide values for all the variables in a list, it provides partial results.

QUESTION 147
What is the difference between the community formats of SNMPv1 SNPMv2c?

A. With SNPMv1, communities are sent as clear text and on SNPMv2c they are encrypted.
B. On SNPMv1 communities are encrypted and on SNPMv2c they are sent as clear text.

C. There is no difference because both versions send encrypted communities.
D. There is no difference because both versions send communities as clear text.
E. SNMPv2c does not use communities.

Answer: D

Explanation:
The original Internet standard Network Management Framework, described in RFCs 1155, 1157, and 1213, is called the SNMP version 1 (SNMPv1) framework. Relevant portions of the proposed framework for version 2C of the Simple Network Management Protocol (SNMPv2C) are described in RFCs 1901 through 1908.
SNMPv1 and SNMPv2c use a community string match for user authentication. Community strings provided a weak form of access control in earlier versions of SNMP. SNMPv3 provides much improved access control using strong authentication and should be preferred over SNMPv1 and SNMPv2c wherever it is supported. Both versions send communities as clear text messages.

QUESTION 148
Network management tools use Management Information Base (MIB) information to monitor and manage networks. Which of the following is NOT part of the MIB-2 specification, as defined in RFC 1213? (Choose all that apply)

A. The System Group
B. The TCP Group
C. The Transmission Group
D. The Enterprises Group
E. The RMON Group
F. The ICMP Group

Answer: D, E

Explanation:
RFC 1213 defines the "Management Information Base for Network Management of TCP/IP-based internets: MIB-II" specification. It defines all of the following groups: System, Interfaces, Address Translation, IP, ICMP, TCP, UDP, EGP, Transmission, and SNMP. The RMON group is not part of RFC 1213, nor is the Enterprises Group

---

QUESTION 149
Which statements are true about the purpose and functionality between SNMP and MIBs? (Select three)

A. A Management Information Base (MIB) is a collection of information that is organized hierarchically.
B. A Management Information Base (MIB) is a collection of network device information that is organized in a bulk transfer mode to the management station.
C. MIBs are accessed using a network-management protocol such as SNMP.

D. MIBs are accessed using a network-management protocol such as TCP.
E. MIBs are comprised of managed objects and are identified by the object identifiers.
F. MIBs are comprised of managed objects and are identified by the lmhosts table.

Answer: A, C, E

Explanation:
The Cisco MIB variables are accessible via the Simple Network Management Protocol (SNMP), which is an application-layer protocol designed to facilitate the exchange of management information between network devices. The SNMP system consists of three parts: SNMP manager, SNMP agent, and MIB.
The MIB structure is logically represented by a tree hierarchy. The root of the tree is unnamed and splits into three main branches: Consultative Committee for International Telegraph and Telephone (CCITT), International Organization for Standardization (ISO), and joint ISO/CCITT.
Finally, each group of MIB variables is accompanied by an illustration that indicates the specific object identifier for each variable.

QUESTION 150
Which options are true regarding the privacy capability using cryptography and the authentication method for SNMPv1, SNMPv2c and SNMPv3? (Choose all that apply)

A. SNMPv1 has no privacy and uses community for authentication.
B. SNMPv2c has privacy and uses community for authentication.
C. SNMPv2c has privacy and uses usernames for authentication.
D. SNMPv3 has privacy and use community for authentication.
E. SNMPv3 has privacy and uses usernames for authentication.

Answer: A, E

Explanation:
SNMPv1 and SNMPv2 use the notion of communities to establish trust between managers and agents. An agent is configured with three community names: read-only, read-write, and trap. The community names are essentially passwords; there's no real difference between a community string and the password you use to access your account on the computer. The three community strings control different kinds of activities. As its name implies, the read-only community string lets you read data values, but doesn't let you modify the data. For example, it allows you to read the number of packets that have been transferred through the ports on your router, but doesn't let you reset the counters. The read-write community is allowed to read and modify data values; with the read-write community string, you can read the counters, reset their values, and even reset the interfaces or do other things that change the router's configuration. Finally, the trap community string allows you to receive traps (asynchronous notifications) from the agent.
SNMPv3 not only encrypts all transmissions but also enables the responder (usually an

SNMP agent) to authenticate the user generating the request, guarantee the integrity of the message using a digital signature, and apply complex and granular access-control rules to each request. It also lets the administrator specify these levels of protection in varied combinations (unsecured, authenticated and authenticated with encryption). In addition, any number of access-control rules can be applied at the SNMP agent or manager. While this level of security was completely impractical in hardware 10 years ago, today's infrastructure devices have enough RAM and CPU cycles to support not only this advanced SNMP security but also full-fledged Web management services--all in firmware.

QUESTION 151
Which security features are defined in SNMPv3? (Select all that apply)

A. Authentication
B. Domain checking
C. Accounting
D. Privacy

Answer: A, D

Explanation:
SNMP Version 3 (SNMPv3) adds security and remote configuration capabilities to the previous versions. The SNMPv3 architecture introduces the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control.
The principal security enhancements defined in SNMP version 3 is authentication, privacy, and access control.
Incorrect Answers:
B, C. SNMP version 3 provides no defines no mechanisms for checking the domain or accounting.

QUESTION 152
What SNMP message type reports events to the NMS reliably?

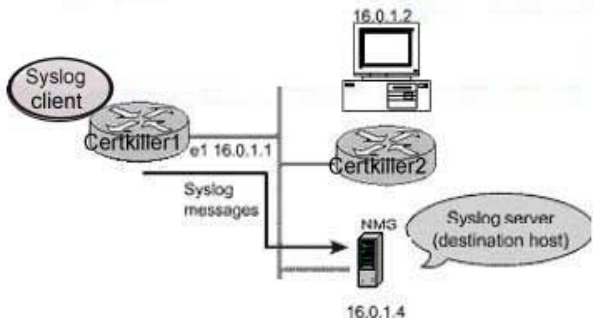
A. Get
B. Response
C. Inform
D. Trap
E. Get Bulk

Answer: C

Explanation:
SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform

request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.
However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform message may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

QUESTION 153
The Certkiller LAN is displayed below:



What should the Cisco IOS commands look like in the Certkiller 1 router to perform the exhibit?

A. logging source-interface fastethernet 0/0
logging 16.0.1.4
logging facility sys9
logging on
B. logging 16.0.1.4
logging trap debugging
logging facility sys9
logging source-interface serial0
logging on
C. logging 16.0.1.4
logging trap debugging
logging facility sys9
logging source-interface ethernet1
logging on
D. logging 16.0.1.1
logging trap 7
logging source-interface serial 1
logging origin-id ip

Answer: C

Explanation:
In the example displayed above, the syslog server resides at 16.0.1.4 so we will want to send all SNMP traps to this IP address. In addition, the source interface information that

should be sent to this server is the ethernet 1 interface, since this is the address used for all messages sent to the server.
Incorrect Answers:

A. In this example the wrong interface source is uses. In addition, the logging level information that should be sent to the server is not specified.
B. Here the wrong interface is configured as the logging source
D. This choice specified the wrong source interface, as well as the wrong IP address of the syslog server.

QUESTION 154
SNMP version 3 has been implemented throughout the Certkiller network. On SNMPv3 which message types are classified as Unconfirmed Class PDU? Select all that apply.

A. Get
B. Trap
C. Inform
D. Report
E. Response

Answer: B, D, E

Explanation:
SNMP PDU Classes
SNMPv1 originally defined six PDUs. The number of PDUs was expanded and some changes made to their name and use in SNMPv2 and SNMPv3. The current SNMP Framework categorizes the PDUs into different classes. These classes describe both the function of each message type and the kind of communication they use to perform their task (polling versus interrupting).
Table 210 shows the main SNMPv2/SNMPv3 PDU classes, describes them, and shows which PDUs are in each class in SNMPv2/SNMPv3. These classes were not used in SNMPv1 but for clarity I also show which messages from SNMPv1 fall into the classes conceptually:

Table 210: SNMP PDU (Message) Classes

SNMPv3 PDU Class	Description	SNMPv1 PDUs	SNMPv2/SNMPv3 PDUs
Read	Messages that read management information from a managed device using a polling mechanism.	GetRequest-PDU, GetNextRequest-PDU	GetRequest-PDU, GetNextRequest- GetBulkRequest-PDU

Write	Messages that change management information on a managed device to affect the device's operation.	SetRequest-PDU	SetRequest-PDU
Response	Messages sent in response to a previous request.	GetResponse-PDU	Response-PDU
Notification	Messages used by a device to send an interrupt-like notification to an SNMP manager.	Trap-PDU	Trapv2-PDU, InformRequest-PDU

The GetBulkRequest-PDU and InformRequest-PDU messages are new in SNMPv2/v3. The GetResponse-PDU message was renamed just Response-PDU (since it is in fact a response and not a message that "gets" anything), and the new Trapv2-PDU replaces Trap-PDU.
There are three other "special" classes defined by the current SNMP Framework. The Internal class contains a special message called Report-PDU defined for internal SNMP communication. The SNMP standards also provide two classes called Confirmed and Unconfirmed, used to categorize the messages in my table above based on whether or not they are acknowledged. The Report-PDU, Trapv2-PDU, and Response-PDU messages are considered Unconfirmed and the rest are Confirmed.
Reference:
http://www.tcpipguide.com/free/t_SNMPProtocolGeneralOperationCommunicationMethodsan-2.htm

---

QUESTION 155
In SNMP, which of the following choices is not part of the MIB-2, as defined in RFC 1213?

A. System
B. Enterprises
C. Transmission
D. TCP
E. RMON

Answer: B, E

Explanation:
From RFC 1213, the following list the various groups in MIB-II
system OBJECT IDENTIFIER ::= { mib-2 1 }

interfaces OBJECT IDENTIFIER ::= { mib-2 2 }
at OBJECT IDENTIFIER ::= { mib-2 3 }
ip OBJECT IDENTIFIER ::= { mib-2 4 }
icmp OBJECT IDENTIFIER ::= { mib-2 5 }
tcp OBJECT IDENTIFIER ::= { mib-2 6 }
udp OBJECT IDENTIFIER ::= { mib-2 7 }
egp OBJECT IDENTIFIER ::= { mib-2 8 }
-- historical (some say hysterical)
-- cmot OBJECT IDENTIFIER ::= { mib-2 9 }
transmission OBJECT IDENTIFIER ::= { mib-2 10 }
snmp OBJECT IDENTIFIER ::= { mib-2 11 }
Reference: http://www.faqs.org/rfcs/rfc1213.html

QUESTION 156
SNMP is being used to provide network information to the Certkiller Network Operations Center. In SNMP, what is an example of a managed device (sometimes called network elements)?

A. Routers and Switches
B. Hubs and Bridges
C. Printers, Firewalls and Servers
D. All of the above

Answer: D

Explanation:
SNMP Basic Components:
An SNMP-managed network consists of three key components: managed devices, agents, and network-management systems (NMSs).
A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be routers and access servers, switches and bridges, hubs, computer hosts, or printers.
An agent is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.
An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network.
Reference: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm

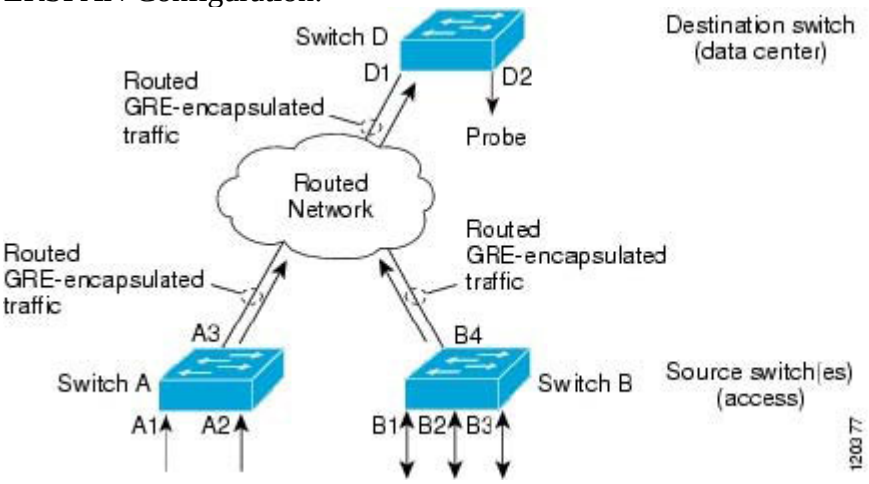
---

QUESTION 157
What feature among the following choices can be used to transport monitoring session traffic from a Certkiller Catalyst switch across a routed IP network to a sniffer on a remote site?

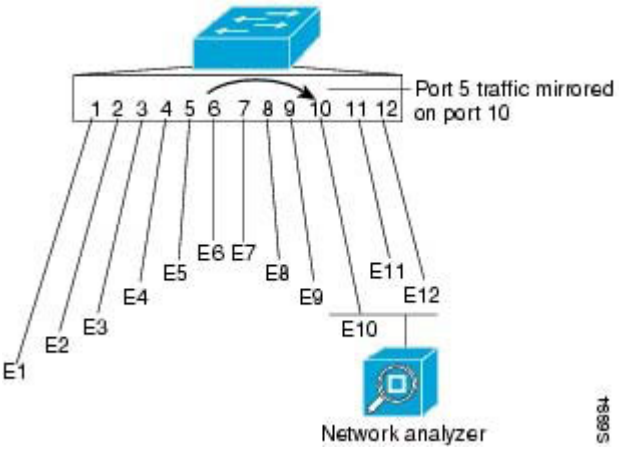
A. Protocol filtering
B. SPAN
C. RSPAN
D. ERSPAN
E. None of the above

Answer: D

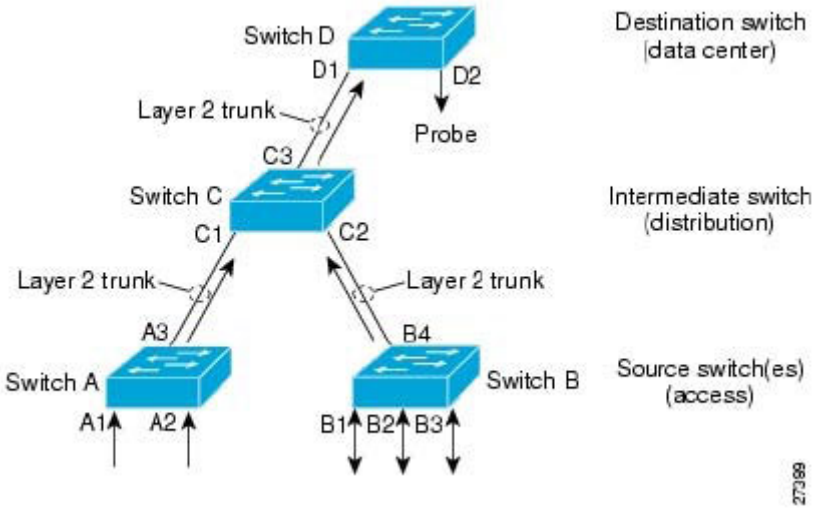
Explanation:
ERSPAN Overview:
ERSPAN supports source ports, source VLANs, and destination ports on different switches, which provides remote monitoring of multiple switches across your network ERSPAN consists of an ERSPAN source session, routable ERSPAN GRE-encapsulated traffic, and an ERSPAN destination session. You separately configure ERSPAN source sessions and destination sessions on different switches.
To configure an ERSPAN source session on one switch, you associate a set of source ports or VLANs with a destination IP address, ERSPAN ID number, and optionally with a VRF name. To configure an ERSPAN destination session on another switch, you associate the destination ports with the source IP address, ERSPAN ID number, and optionally with a VRF name. .
The ERSPAN source session copies traffic from the source ports or source VLANs and forwards the traffic using routable GRE-encapsulated packets to the ERSPAN destination session. The ERSPAN destination session switches the traffic to the destination ports.
ERSPAN Configuration:



Incorrect Answers:
A: Filtering can not be used to send traffic to a remote protocol analyzer.
B: Local Span is used to send traffic to a local sniffer as described below:
A local SPAN session is an association of source ports and source VLANs with one or more destination ports. You configure a local SPAN session on a single switch. Local SPAN does not have separate source and destination sessions.
Figure52-1 Example SPAN Configuration



C: RSPAN supports source ports, source VLANs, and destination ports on different switches, which provides remote monitoring of multiple switches across your network RSPAN consists of an RSPAN source session, an RSPAN VLAN, and an RSPAN destination session. You separately configure RSPAN source sessions and destination sessions on different switches.
The traffic for each RSPAN session is carried as Layer2 nonroutable traffic over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. All participating switches must be trunk-connected at Layer2.
Figure52-2 RSPAN Configuration



Reference:
http://www.okena.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008016

QUESTION 158
Router CK1 is configured for OSPF. Under the OSPF process, you type in the "area 1 range" command. Which LSA types will be acted upon (summarized) as a result? (Choose all that apply)

A. Type 1
B. Type 2

C. Type 3
D. Type 4
E. Type 5

Answer: A, B

Explanation:
Area range command is used for summarizing routes on the boundary of two OSPF areas. The information to be summarized is contained in two types of LSAs: Type 1 and Type2. Type 1 LSAs are Router LSAs and are generated by each router in an OSPF network. Type 2 LSAs are network LSAs, which are generated by the DR. Both Type1 and Type 2 LSAs are flooded within the originating area only. Only when the information needs to be conveyed to another area in a summarized form area-range command is used, which acts on the information provided by these two LSAs.
Reference:
CCIE Professional Development Routing TCP/IP Volume I by Jeff Doyle page 471.
Incorrect Answers:
C. Type 3 LSA are the result of type 1 and type 2 summaries that are created by the area range command.
D. Type 4 LSAs are ASBR summary LSAs
E. Type 5 LSAs are AS External LSAs

QUESTION 159
A change in the topology of the Certkiller OSPF network causes the flooding operation. Which OSPF packet types are used in this LSA Flooding?

A. Hello
B. Link State Update
C. Link State Request
D. Database description
E. Link State Acknowledgement

Answer: B, E

Explanation:
A change in the OSPF network topology is represented as a change in one or more of the OSPF Link State Advertisements (LSAs). Flooding is the process by which changed or new LSAs are sent throughout the network, and are used to ensure that the database of every OSPF router is updated and an identical database is maintained. This flooding makes use of two OSPF packet types: Link State Update packets (type 4), and Link State Acknowledgement packets (type 5).
Reference: Jeff Doyle, "Routing TCP/IP volume 1" page 451.

QUESTION 160
Router CK1 is configured for OSPF and is connected to two areas: area 0 and area 1. You then configure area 1 as a stub area. Which LSAs will now operate inside of area 1?

A. Type 7
B. Type 1 and 2
C. Type 1, 2, and 5
D. Type 3 and 4
E. Type 1, 2 and 3

Answer: E

Explanation:
Only type 1, 2, and 3 LSAs will be allowed inside of a stub area.
Incorrect Answers:

A. Type 7 LSAs are used for NSSA, not stubby areas.
B. Network Summary LSAs (Type 3) are also allowed.
Reference:
CCIE Professional Development Routing TCP/IP Volume I by Jeff Doyle page 479.

QUESTION 161
Study the Exhibits below carefully:
The following exhibit is an illustration of the output from an ASBR:
ASBBR#show ip ospf database external
OSPF Router with ID (15.33.4.2) (Process ID 10)
Type-5 AS External Link States
LS age: 15
Options: (No TOS-capability, DC)
LS Type: AS External Link
Link State ID: 10.10.1.0 (External Network Number)
Advertising Router: 15.33.4.2
LS Seq Number: 80000002
Checksum: 0x513
Length: 36
Network Mask: /24
Metric Type: 1 (Comparable directly to link state metric)
TOS: 0
Metric: 10
Forward Address: 0.0.0.0
External Route Tag: 0
And this exhibit is an illustration from a router in the network:
Router CK1 #show ip ospf border-routers
OSPF Process 10 internal Routing Table
Codes: i-intra-area route, I-Inter-area route
15.33.4.2(2) via 30.0.0.1, Serial0/0, ASBR, Area0, SPF 4
Based on this information what is the total metric for the route to subnet 10.10.1.0/24 on Router CK1 ?

A. 1
B. 8
C. 12
D. 20
E. 22

Answer: C

Explanation:
The metric of the external link shows 10. Then we need to add 2 from the inter-area metric, for a total of 12.

QUESTION 162
In your OSPF network serial 0 on your router, CK1 , is in area 1. Later, you configure serial 0 as passive. What is the effect of this configuration change?

A. OSPF will accept the routing updates from neighbors.
B. OSPF will form all the available adjacencies out of that interface.
C. OSPF will not insert any of the learned routes in the local routing table.
D. OSPF will not form any adjacency out of that interface.
E. None of the above.

Answer: D

Explanation:
With passive-interface, an adjacency will never occur out of that interface, as no hello packets are exchanged out of a passive interface.
Incorrect Answers:

A. Normally, defining an interface as passive will accomplish this. No routes will be sent out, but routes can still be received. OSPF differs because link state protocols need information for the entire network topology. Defining an interface as passive with OSPF means that the adjacency will not be established, therefore, no routes will be able to be received on that interface.

QUESTION 163
You are the network administrator at Certkiller . The Certkiller network contains four Routers named CK1 , CK2 , CK3 , and CK4 . All four routers are connected to a hub via Ethernet interfaces. All four routers have a basic OSPF configuration of a network statement for the Ethernet network. During routine maintenance, you issue the show ip ospf neighbor command on Router CK2 . The output from the show ip ospf neighbor command shows 2WAY/DROTHER for its neighbor, Router CK3 . What conclusions can you draw from this output? (Choose all that apply)

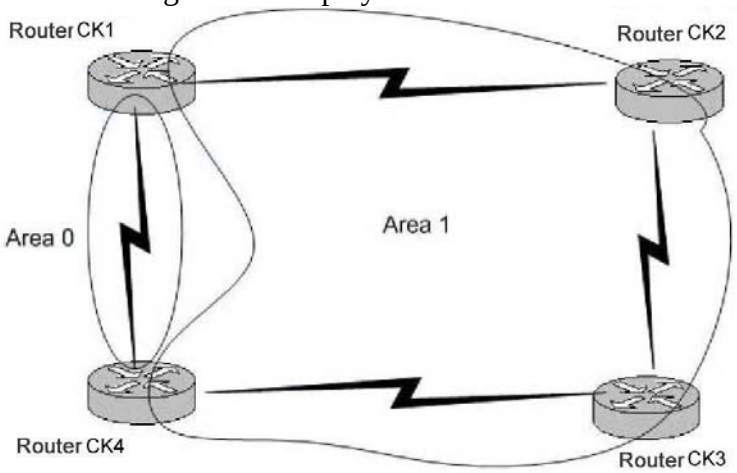
A. Router CK2 is the DR or BDR.
B. Router CK3 is not a DR or BDR.

C. Router CK2 - Router CK3 adjacency is not yet FULL.
D. Router CK2 is not the DR.
E. Router CK4 is the DR.

Answer: B, D

Explanation:
OSPF routers can have one of three neighbor relationships: Designated Router (DR), Backup Designated Router (BDR), or neither. For neither, the router neighbor relationship will show as 2WAY/DROTHER.
Incorrect Answers:
A, C. 2WAY/DROTHER means that the two routers are neither the DR nor the BDR.
E. Either Router CK1 or Router CK4 is the DR. Based on the information that is provided we cannot be sure which one it is.

QUESTION 164
The following exhibit displays the Certkiller OSPF network:



Router CK2 needs to send a string of packets to router CK4 . How will router CK2 decide the path to take to reach CK4 ?

A. CK2 will select a path after considering the costs inside Area 1 only.
B. CK2 will alternate between Router CK1 and Router CK3 if the costs are equal.
C. CK 2 will always go through Router CK1 with no regard for costs.
D. CK2 will select a path after considering the costs inside both Area 0 and Area 1.
E. None of the above.

Answer: A

Explanation:
OSPF prefers Intra Area Path over Inter Area Paths.
Incorrect Answers:
B. The Answer B is incorrect because OSPF does not conduct ECMP load balancing on multiple paths with equal cost if the respective paths span through more than one area. B is incorrect for several reasons. If a packet has to alternate between two paths that means

Per Packet load balancing is in effect. Which is normally in place for links less than 56k. For higher link speeds fast switching (default switching mode) is enabled. In this mode all packets to one destination in a target subnet are sent over one path, since route lookup is not performed for every packet, it is rather performed per flow. So B is totally ruled out.
C. Even though router CK1 is the most direct way to reach area 0, OSPF will always prefer to stay in the same area over traversing multiple areas.
D. OSPF prefers Intra area paths, so only the costs associated with reaching CK4 via area 1 will be considered first.
Reference:
http://www.riverstonenet.com/support/ospf/interface-costs.htm

---

QUESTION 165
Router CK1 is configured for OSPF. Interface serial 0 is configured to be in area 0 and interface serial 1 is configured to be in area 1. Under the OSPF process "area 1 nssa default-information-originate" is configured. Which of the following are true? (Choose all that apply)

A. CK1 will inject a type 3 default route into area 1.
B. CK1 will inject a type 7 default route into area 1.
C. CK1 will inject a type 7 default route into area 0.
D. CK1 needs a default route in its routing table to inject a default into area 1.
E. CK1 does not need a default route in its routing table to inject a default into area 1.

Answer: B, D

Explanation:
Type 7 routes are injected into OSPF NSSA areas, and the default information originate command will make CK1 inject type 7 default routes into area 1. As a rule, an OSPF router will need a default route itself before injecting a default route into an area, unless the keyword "always" is used in the configuration. For example, "default-information originate always."
Incorrect Answers:

A. In a NSSA area, the NSSA area generates the default route with the "default-information originate" command, but unlike other default routes that use type 3 information, NSSA default routes use type 7.
C. CK1 will inject a type 7 NSSA route into area 1, not area 0. Area 0 can not be an NSSA.
E. Using the command shown in the question above will not create the route, because a previous default route did not already exist within the routing table. A default route would have been injected only if the keyword "always" was inserted.
Reference:
www.cisco.com/en/US/tech/ CK3 65/technologies_tech_note09186a0080094a74.shtml

---

QUESTION 166
Which of the following OSPF routers can generate a type 4 ASBR-summary LSA? (Choose all that apply)

A. ABRs
B. DR
C. BDR
D. ASBRs

Answer: A

Explanation:
Type 4 LSAs are only put out by ABRs and only in two cases: 1. There is an ASBR that the ABR needs to tell the backbone area about. 2. There is a legacy router that is incapable of demand circuits. These last two are indication LSAs and are put out only by an ABR putting itself in the ASBR position, but it is still not an ASBR. An ASBR would not be responsible for reporting either of these situations.

QUESTION 167
Routers CK1 and CK2 are in the same LAN and both are running OSPF. Which multicast IP address will CK1 and CK2 use for sending routing updates to each other? (Choose all that apply)

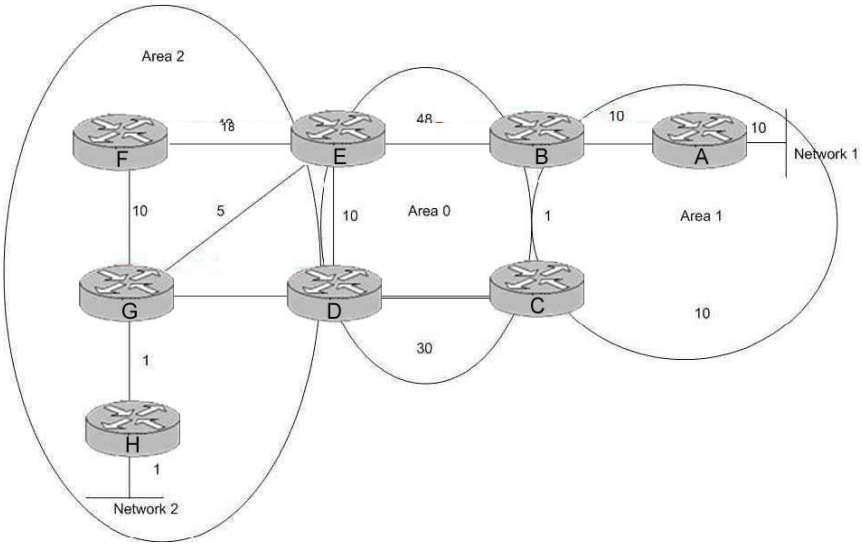
A. 224.0.0.10
B. 224.0.0.1
C. 224.0.0.13
D. 224.0.0.5
E. 224.0.0.9
F. 224.0.0.6

Answer: D, F

Explanation:
224.0.0.5 is the all-OSPF routers multicast and 224.0.0.6 is the Designated Routers multicast address.
Incorrect Answers:

A. 224.0.0.10 is used for IGRP.
B. 224.0.0.1 is reserved for all systems on the subnet.
D. 224.0.0.13 is used by PIM.
E. 224.0.0.9 is reserved for RIP version 2 announcements.

QUESTION 168
The Certkiller WAN utilizes OSPF as shown below. The OSPF metric for each link is displayed in the diagram as follows:



What is the OSPF shortest path from Network 2 to Network 1 with the OSPF link costs shown in the exhibit?

A. H G D B A
B. H G E C B A
C. H G F D B A
D. H G E D B A

Answer: B

Explanation:
Cost of links from Network 2 to Network 1 is:

A. H G D B A = 1+1 +5 +48 +10 = 65
B. H G E C B A = 1+1+1+30+1+10= 44
C. H G F D B A = 1+1+10+48+48+10= 118
D. H GE D B A = 1+1+1+10+48+10= 71
Therefore, the shortest path is the lowest cost path which is option B. It is important to remember that OSPF uses the total cost of the metrics from a source to a given destination, and the number of hop counts is irrelevant.

QUESTION 169
The Certkiller router CK2 is experiencing OSPF problems with a neighbor across a frame relay network. During troubleshooting, OSPF event debugging was issued as shown below:
CK2 #debug ip ospf events
OSPF events debugging is on
CK2 #
00:16:22: OSPF: Rcd hello from 192.168.0.6 area 4 from
Ethernet 0/0 16.16.26.6
00:16:22: OSPF: End of hello processing
00:16:22: OSPF: Send hello to 244.0.0.5 area 4 on

Ethernet0/0 from 116.16.26.2
CK2 #
00:16:28: OSPF: Rcd hello from 192.168.0.3 area 3 from
Serial1/0 116.16.32.1
00:16:28: OSPF: Mismatched hello parameters from
116.16.32.1
00:16:28: OSPF: Dead R 40 C 120, Hello R 10 C 30 Mask R
255.255.255.252 C 255.255.255.252
CK2 :
00:16:32: OSPF: Rcd hello from 192.168.0.6 area 4 from
Ethernet0/0 116.16.26.6
00:16:32: OSPF: End of hello processing
00:16:32: OSPF: Send hello to 224.0.0.5 area 4 on
Ethernet0/0 from 116.16.26.2
Based on the information above, what is the most likely reason for the OSPF problems across the frame relay link?

A. This router is in area 4 while its neighbor is configured to be in area 3.
B. There is mismatch between the OSPF frame-relay parameters configured on this router and those configured on its neighbor.
C. The OSPF network mode configured on this router is not the same as the mode configured on its neighbor.
D. This router has a frame-relay interface DLCI statement that is using the broadcast mode. While its neighbor is using a point-to-point mode.
E. None of the above.

Answer: C

Explanation:
The default timers for a broadcast network (LAN) are: Hello 10 seconds, Dead 40 seconds
The default timers for an NBMA network (Frame Relay) are: Hello 30 seconds, Dead 120 seconds.
The problem above shows that these timers do not match at each end. The "Dead R 40 C 120, Hello R 10 C 30" means that the configured Dead time is 120 seconds locally on this router, but the received update shows it is configured to be 40 seconds. Similarly, the received hello packet shows that it has a hello time of 10 seconds, where router CK2 is configured for 30 seconds. Although the remote router may have had their timers changed manually within the OSPF process, the most likely cause of the problem is that router CK2 is configured with a network type of NBMA and the other router is configured with a network type of broadcast.
Incorrect Answers:

A. It is common for a router with multiple interfaces to be in different OSPF areas. Each network link must be in the same area, but each router can have multiple interfaces, that each belongs to a different area.

B. The Frame relay parameters do not appear to be misconfigured, just the OSPF timer values.
D. The timers on the local router, CK2 , is 30 seconds for the Hello and 120 seconds for the dead, so this router is configured with a NBMA or pt-pt type, while the remote router is using a broadcast network type.

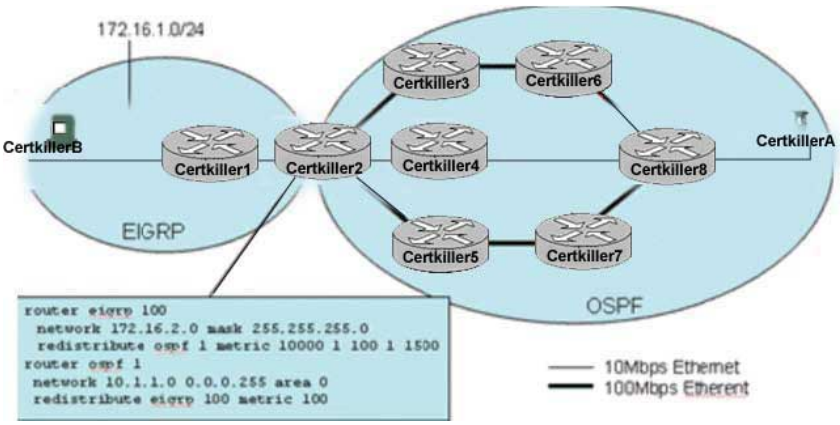
QUESTION 170
Which of the following statements are true regarding the SPF calculation? (Select three)

A. The Dijkstra algorithm is run two times.
B. The previous routing table is saved.
C. The present routing table is invalidated.
D. A router calculates the shortest-path cost using their neighbor(s) as the root for the SPF tree.
E. Cisco routers use a default OSPF cost of 10^7/BW.

Answer: A, B, C

Explanation:
The Dijkstra algorithm code itself is run two times. The first time deals with routers and the second time always deals with networks.
When the Shortest Path First (SPF) algorithm is computed by an OSPF router, the previous routing table is save before the calculation and used in case any problems arise with the new one. It then invalidates the present routing table and performs the calculation using ITSELF as root in the SPF tree.
Incorrect Answers:
D. The router itself is the root, not the neighbor. A router periodically advertises its status or link state to its adjacencies. Link state advertisements flood throughout an area ensuring that all routers have exactly the same topological database. This database is a collection of the link state advertisements received from each router belonging to an area. From the information in this database, each router can calculate a shortest path tree with itself designated as the root of the tree.
E. The default OSPF cost of any link is 10^8/Bandwidth, or 100,000,000/BW.

QUESTION 171
The Certkiller network is displayed below:



Given the network and OSPF configuration shown above, what statement is true regarding traffic flowing from PC- Certkiller A to PC- Certkiller B?

A. Traffic will only flow on the shortest, low-speed path, PC- Certkiller A - Certkiller 8 - Certkiller 4 - Certkiller 2- Certkiller 1 - PC- Certkiller B.
B. Traffic will flow on both the high speed paths (PC- Certkiller A - Certkiller 8 - Certkiller 6- Certkiller 3 - Certkiller 2 - Certkiller 1 - PC- Certkiller B and PC- Certkiller A - Certkiller 8 - Certkiller 7 - Certkiller 5 - Certkiller 2 - Certkiller 1 - PC- Certkiller B) but not the slow-speed path.
C. Traffic will flow on all three of the paths.
D. Traffic will flow uni-directionally on one of the high-speed paths from PC Certkiller A to PC- Certkiller B, and uni-directionally on one of the high speed paths from PC- Certkiller B o PC- Certkiller A.
E. Traffic will flow bi-directionally on only one of the high-speed paths, and the path selected will be based on the OSPF process IDs.

Answer: B

Explanation:
OSPF uses the bandwidth of the links for the metric, and by default the 100 Mbps links will have an OSPF metric of 1 while the low speed links will have a metric of 10 so only the high speed Ethernet links will be used.
By default, OSPF load balances on up to four equal cost paths. Since both high speed paths will have a metric of 3 (1+1+1) from router Certkiller 8 to Certkiller 2 they traffic will load balance over the two paths.

QUESTION 172
What statement is correct regarding OSPF adjacencies and link-state database synchronization?

A. Full adjacency occurs when OSPF routers reach the LOADING state.
B. Adjacency relationship begins in the EXSTART state.
C. All OSPF neighbors establish adjacencies in the FULL state with all other routers on the broadcast network.
D. The INIT state indicates that a router has received a Hello packet from a neighbor and

has seen their own ROUTERID in the Hello packet.

Answer: B

Explanation:
The various states in which a neighbor can be are discussed below.
1. Down - the initial state of a neighbor conversation.
2. Attempt - indicates that an attempt should be made to contact the neighbor.
3. Init - hello packet has been received from the neighbor.
4. 2-Way - communication between two routers is bi-directional.
5. ExStart - first step to creating an adjacency between the two neighboring routers.
6. Exchange - the router is sending data description packets to the neighbor.
7. Loading - Link state request packets are sent to the neighbor.
8. Full - the neighboring routers are fully adjacent.
Incorrect Answers:

A. Full adjacency only occurs after the OSPF router has reached a FULL state.
C. In a broadcast network, all routers only become adjacent with the Designated Router (DR).
D. This state specifies that the router has received a hello packet from its neighbor, but the receiving router's ID was not included in the hello packet. When a router receives a hello packet from a neighbor, it should list the sender's router ID in its hello packet as an acknowledgment that it received a valid hello packet.

QUESTION 173
OSPF is running on the Certkiller network. In OSPF, what LSA type would only cause a partial SPF calculation?

A. Type 1
B. Type 2
C. Type 4
D. Type 7
E. Type 9

Answer: D

Explanation:
OSPF Type 7 LSA's are reserved for Not So Stubby Areas (NSSA). This area accepts Type 7 LSAs which are external route advertisements like Type 5s but they are only flooded within the NSS
A. This is usually used when connecting to a branch office running an IGP. Normally this would have to be a standard area since a stub area would not import the external routes. If it was a standard area linking the ISP to the branch office then the ISP would receive all the Type 5 LSAs from the branch which it does not want. Because Type 7 LSAs are only flooded to the NSSA the ISP is saved from the

external routes whereas the NSSA can still receive them. Therefore, when this LSA is generated, only a partial SPF calculation needs to be performed.

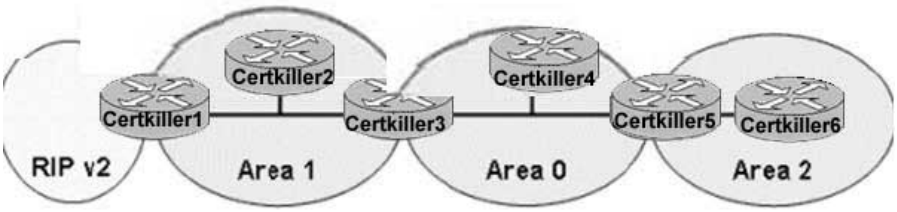
QUESTION 174
OSPF is being used as the routing protocol in the Certkiller network. Which two statements regarding the SPF calculation on these OSPF routers are true? (Select two)

A. The existing routing table is saved so that changes in routing table entries can be identified.
B. The present routing table is invalidated and is built again from scratch.
C. The Cisco router calculates the shortest-path cost using their neighbor(s) as the root for the SPF tree.
D. Cisco routers use a default OSPF cost of 10^7/BW.

Answer: A, B

Explanation:
When an OSPF router performs a new SPF calculation, the existing routing table is saved and used as a baseline for changes made to the network topology. When any SPF calculation is made, the OSPF neighbor or neighbors is used as the root of the SPF routing tree.
Incorrect Answers:
C. The root of the SPF tree is always the router itself, not the neighboring router.
D. The default cost for all OSPF links is 10^8/BW, or 100,000,000/ configured bandwidth.

QUESTION 175
The Certkiller OSPF/RIPv2 network is displayed below:



Area 1 is an OSPF Not So Stubby Area (NSSA). What type of LSA will Certkiller 3 send out area 0 to indicate the presence of an ASBR in Area 1?

A. A type 5 because P-bit has been set in the type 4 LSA that was sent from Certkiller 1 to Certkiller 3.
B. A type 4 because the E-bit was set in the type 7 LSA that was sent from Certkiller 1 to Certkiller 3.
C. A type 1 because the B-bit was set in the LSA that was propagated from Certkiller 1 to Certkiller 3.
D. A type 3 because the E-bit was set in the type 1 LSA that was sent from Certkiller 1 to Certkiller 3.

Answer: B

Explanation:
In this case a type 5 LSA would be sent by the ASBR, which is Certkiller 1.
Type 5 Link State advertisements are generated by the ASBR and describe links external to the Autonomous System (AS). This LSAS is flooded to all areas except stub areas.
Here Certkiller 1 is considered to be an ASBR since it is directly connected with the RIP version 2 network.
The E-bit reflects the associated area's External Routing Capability. AS external link advertisements are not flooded into/through OSPF stub areas. The E-bit ensures that all members of a stub area agree on that area's configuration.
LSA type 3 and 4 are summary link advertisements generated by ABRs describing inter-area routes. Type 3 describes routes to networks and is used for summarization. Type 4 describes routes to the ASBR. Since Certkiller 3 needs to advertise the presence of an ASBR, it will send out a type 4 LSA to area 0.
Reference:http://www.cisco.com/warp/public/104/ospfdb6.html

QUESTION 176
What statement is accurate regarding OSPF areas?

A. Redistribution is allowed into all types of OSPF areas.
B. When routes are redistributed into an OSPF stub area, they enter as type-5 LSAs.
C. Redistribution is allowed into an OSPF stub area, but not into an OSPF not-so-stubby area.
D. When routes are redistributed into an OSPF not-so-stubby area, they enter as type-5 LSAs.
E. When routes are redistributed into an OSPF not-so-stubby area, they enter as type-7 LSAs.

Answer: E

Explanation:
When routes are redistributed into OSPF, these routes are considered to be external routes. External LSAs are type 5 LSAs. Not so stubby areas allow external routes to be advertised into OSPF network while retaining the charactersistics of a stub area. To do this, the ASBR (the one doing the redistributing) in the NSSA will originate a type 7 LSA to advertise the external destinations.
Reference: Jeff Doyle, Routing TCP/IP volume 1, page 483.
Incorrect Answers:

A. Type 5 LSAs are only allowed into Backbone (area 0) and non backbone, non-stub areas.
B. Type 5 LSAs (external LSAs) are not allowed into stub or totally stub areas.
C. The opposite is true. External LSAs are allowed into NSSA, but not stub areas.

D. Type 5 LSAs are not inserted into NSSA for external routes. Type 7 LSAs are created for this purpose.

QUESTION 177
Within the Certkiller OSPF network, which statement is true regarding the LSA's contained in the link state database? (Choose all that apply).

A. The LSRefreshTime is 30 minutes.
B. LSA's can only be reflooded by the router that originated the LSA.
C. When an LSA reaches its MaxAge the router will send out a purge message to the other routers within its area.
D. All LSAs contained in the LSDB expire at the same time unless they are refreshed.
E. The MaxAge of an LSA is 3600 seconds.

Answer: A, E

Explanation:
Each OSPF LSA has an age, which indicates whether the LSA is still valid. Once the LSA reaches the maximum age (one hour), it is discarded. During the aging process, the originating router sends a refresh packet every 30 minutes to refresh the LS
A. Refresh
packets are sent to keep the LSA from expiring, whether there has been a change in the network topology or not. Checksumming is performed on all LSAs every 10 minutes. The router keeps track of LSAs it generates and LSAs it receives from other routers. The router refreshes LSAs it generated; it ages the LSAs it received from other routers.
Incorrect Answers:
B. Each LSA gets refreshed when it is 30minutes old, independent of the other LSAs used by other OSPF routers.
C. Purge messages are not sent to neighboring routers since each router uses its own timers.
D. Global synchronization can be problematic in OSPF networks. This problem is solved by each LSA having its own timer. Each LSA gets refreshed when it is 30minutes old, independent of other LSAs, so the CPU is used only when necessary.

QUESTION 178
Which of the following is are considered to be attributes of BGP routes? (Choose all that apply)

A. Origin
B. Weight
C. Local Preference
D. Community
E. Cluster List

Answer: A, C, D, E

Explanation:
Origin, Local Preference, Community, and Cluster List are all BGP attributes.
ORIGIN Well-known mandatory, Type code 1 RFC 1771
LOCAL_PREF Well-Known discretionary, Type code 5 RFC 1771
COMMUNITY Optional transitive, Type 8 RFC 1997
CLUSTER_LIST Optional nontransitive, Type code 10 RFC 1966
Incorrect Answers:
B. Cisco routers do indeed use weight during the BGP route decision making process. In fact, it is the first parameter that is looked at. However, weight is a Cisco-only parameter, and is therefore not considered a BGP attribute.

QUESTION 179
You are the network administrator at Certkiller . You want to advertise the network 190.72.27.0/27 to an EBGP peer.
What command should you use?

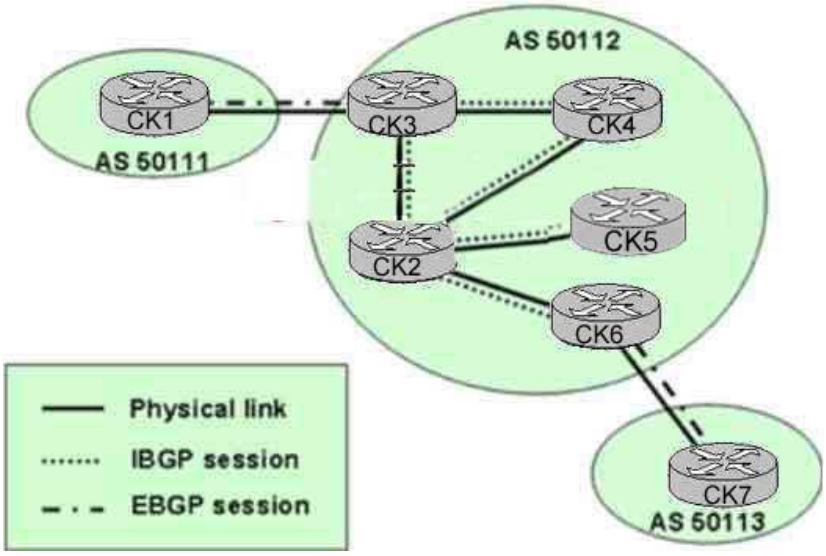
A. network 190.72.27.0
B. network 190.72.27.0 mask 255.255.255.224
C. network 190.72.27.0 mask 255.255.225.240
D. network 190.72.27.0 mask 0.0.0.31.

Answer: B

Explanation:
The correct syntax is: network ip-address mask subnet-mask where ip-address is the network address and subnet-mask is the subnet mask. In this case the network address is 190.72.27.0. The subnet mask is a 27 bit subnet mask (11111111.11111111.11111111.11100000) that equates to 255.255.255.224.
Incorrect Answers:

A. If no mask is specified, the default class mask is used. In the 190.72.27.0 case it would be a /16.
C. Here the wrong mask is used.
D. This is the inverse mask, which is normally used by OSPF when specifying the network mask, but not by BGP.

QUESTION 180
The Certkiller BGP network consists of AS 50112 as shown in the diagram below:



Based on the physical connectivity and the IBGP peering shown, what router within the Transit AS 501112 should be setup as the route reflector and which routers should be setup as the clients based on the recommended route reflector design rules?

A. CK4 should be the route reflector with CK2 and CK5 as its clients.
B. CK2 should be the route reflector with CK5 and CK6 as its clients.
C. CK3 should be the route reflector with CK2 and CK4 as its clients.
D. CK2 should be the route reflector with CK4 and CK5 as its clients.
E. CK4 should be the route reflector with CK2 and CK3 as its clients.
F. All of the above are valid options.

Answer: B

Explanation:
Within any BGP autonomous system, every IBGP speaker must have a fully meshed peering arrangement with every other iBGP speaker. This is due to the fact that a BGP speaker will not advertise a route learned via another iBGP speaker to a third iBGP speaker. The use of route reflectors is one way to maintain connectivity throughout the AS without having a fully meshed peering arrangement. By relaxing this restriction a bit and by providing additional control, we can allow a router to advertise (reflect) iBGP learned routes to other iBGP speakers.
When using route reflectors, the clients need only peer to the route reflector. In the example above, if router CK2 is configured as the route reflector, with routers CK5 and CK6 set up as clients, then 5 and 6 need only peer with CK2 . In doing this, all other routers are fully meshed. No other answer choices will allow us to maintain a fully meshed iBGP configuration.

QUESTION 181
Routers CK1 and CK2 are configured for BGP. Both routers reside in AS 65234. Routes from Router CK2 show up in the BGP table on Router CK1 , but not in the IP routing table.

What could be the cause of this problem?

A. Synchronization is off.
B. The BGP peers are down.
C. BGP multi-hop is disabled on Router CK1 .
D. Router CK1 is not receiving the same routes via an internal protocol.

Answer: D

Explanation:
BGP Synchronization says: "If your autonomous system is passing traffic from another AS to a third AS, BGP should not advertise a route before all routers in your AS have learned about the route via IGP." Therefore, we can assume that synchronization is on and that the BGP routes have not yet been learned by an IGP.
Incorrect Answers:

A. If synchronization is off the routes would show up in the IP routing table on CK1 .
B. If the BGP peers were down, then the routers would not be sending and receiving BGP route information to each other.
C. BGP multi-hop is only useful for EBGP peers, not IBGP peers.

QUESTION 182
You have a router running BGP for the Internet connections as well as IGRP for use internally. You configure the network backdoor command on this router under the BGP process. What will this do?

A. It will change the distance of an iBGP route to 20.
B. It will change the distance of an eBGP route to 200.
C. It will change the distance of an IGRP route to 20.
D. It will not change the distance of the route.

Answer: B

Explanation:
Backdoor only makes the IGP learned route the preferred route. To specify a backdoor route to a BGP border router that will provide better information about the network, use the network backdoor router configuration command. To remove an address from the list, use the no form of this command.
By definition, eBGP updates have a distance of 20 that is lower than the IGP distances. Default distance is 120 for RIP, 100 for IGRP, 90 for EIGRP, and 110 for OSPF.
By default, BGP has the following distances, but that could be changed by the distance command:
distance bgp external-distance internal-distance local-distance
external-distance:20
internal-distance:200
local-distance:200

If we want RTA to learn about 160.10.0.0 via RTB (IGP), then we have two options:
* Change eBGP's external distance or IGP's distance, which is not recommended.
* Use BGP backdoor.
BGP backdoor makes the IGP route the preferred route
RTA learns 160.10.0.0 from RTB via EIGRP with distance 90, and also learns it from RTC via eBGP with distance 20. Normally eBGP is preferred, but because of the backdoor command EIGRP is preferred
References:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_command_summary_chapter09186a00800d
http://www.cisco.com/en/US/tech/ CK3 65/ CK8 0/technologies_tech_note09186a00800c95bb.shtml#bgpbackdoor

---

QUESTION 183
You have two routers running BGP to two different ISP's. You wish to influence the way that traffic comes into your network from the Internet, but your company policy prohibits the use of BGP communities. What is the best way to influence this traffic?

A. Adjust the cost of your routers.
B. Use MED values.
C. Increase the weight value on one of your routers.
D. Decrease the local preference value on one of your routers.
E. Use AS-path prepending.
F. Use Metrics.

Answer: E

Explanation:
When influencing incoming traffic from the Internet, the two most widely used methods are AS Path Prepending and Multi-Exit Discriminators (MED). AS Path prepending works by adding AS paths to certain network ranges, making them appear to the Internet to be further away than they really are. MEDs are used to advertise metrics to the neighbor AS to influence the incoming path that traffic should take to reach certain destinations. In this case, AS Path Prepending is preferred over the use of MEDs because AS path prepending information is distributed to all networks within the Internet. MEDs are only used between neighboring Autnomous Systems. Another advantage to path prepending is that the AS path information is ranked higher in the BGP decision process than the MED information. IN fact, MED information is one of the last things considered in the BGP path decision algorithm.
Note: Although one method of using AS Path prepending requires the use of communities, it is not required to use communities for simply sending prepending information.
Incorrect Answers:
A, C, D, F. These are all methods for influencing traffic going out to the Internet, not

coming in.
E. This would be an acceptable way to influence traffic, but would not be the best way.

QUESTION 184
Your router is multi-homed to three different ISP's for Internet access. You then configure "bgp deterministic-med" under the BGP routing process configuration of your router. What effect does this change have on your network?

A. It configures BGP to compare MEDs between different ASs.
B. It makes the default metric count the worst possible metric.
C. It makes the default metric count the best possible metric.
D. It configures BGP to reorder the entries by neighbor AS.
E. It configures BGP to reorder the entries by MED.

Answer: D

Explanation:
There is sometimes confusion between the two Border Gateway Protocol (BGP) configuration commands bgp deterministic-med and bgp always-compare-med. Enabling the bgp deterministic-med command ensures the comparison of the MED variable when choosing routes advertised by different peers in the same autonomous system. Enabling the bgp always-compare-med command ensures the comparison of the MED for paths from neighbors in different autonomous systems. The bgp always-compare-med command is useful when multiple service providers or enterprises agree on a uniform policy for setting MED. Thus, for network X, if Internet Service Provider A (ISP A) sets the MED to 10, and ISP B sets the MED to 20, both ISPs agree that ISP A has the better performing path to X.
When BGP receives multiple routes to a particular destination, it lists them in the reverse order that they were received, from the newest to the oldest. BGP then compares the routes in pairs, starting with the newest entry and moving toward the oldest entry (starting at top of the list and moving down). For example, entry1 and entry2 are compared. The better of these two is then compared to entry3, and so on. The bgp always-compare-med command reorders the entries by neighbor AS.
Incorrect Answers:

A. The router would compare MEDs between different AS numbers if the "bgp always-comapre-med" was configured, not the bgp deterministic-med command.
B, C. This command does not affect the default BGP metric.
E. This command reorders the entries based on AS number, not MED.
Reference:
http://www.cisco.com/en/US/tech/ CK3 65/technologies_tech_note09186a0080094925.shtml

---

QUESTION 185
Which of the following attributes are "well known" BGP attributes? (Choose all that apply)

A. Atomic-aggregate
B. MED
C. Next-hop
D. AS-path
E. Origin
F. Weight
G. Aggregator

Answer: A, C, D, E

Explanation:
The following BGP attributes are all well known:
Well Known, Mandatory attributes: AS_PATH, NEXT-HOP and ORIGIN
Well Known, Discretionary attributes: LOCAL_PREF and ATOMIC_AGGREGATE
Incorrect Answers:
B, E, F. The optional, transitive attributes are AGGREGATOR and COMMUNITY. The optional non-transitive attributes include MULTI_EXIT_DISC (MED, the ORIGINATOR_ID. and CLUSTER_LIST.
Reference:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/bgp.htm

---

QUESTION 186
In BGP routing, what does the rule of synchronization mean?

A. It means that a BGP router can only advertise an iBGP-learned route provided that the route is in the only in the BGP table.
B. It means that a BGP router can only advertise an eBGP-learned route provided that the route is an IGP route in the routing table.
C. It means that a BGP router can only advertise an iBGP-learned route provided that the route is in the routing table of all its iBGP neighbors.
D. It means that a BGP router can only advertise an eBGP-learned route provided that the route is metric 0 in the BGP table.
E. It means that a BGP router can only advertise an iBGP-learned route provided that the route is an IGP route in the routing table.

Answer: E

Explanation:
The BGP rule of synchronization states that a BGP router should not advertise to external neighbors destinations learned from IBGP neighbors unless those destinations are also known via an IGP.
Incorrect Answers:
B, D. Synchronization is used to ensure that you don't develop black holes by advertising local routes to the rest of the world, when the local routers don't even know how to get to the route in question. That's why synchronization with the IGP is not a concern when you either create a full iBGP mesh, or implement route reflectors, confederations, or both.

Therefore, synchronization is implemented only for IBGP routes, not EBGP.
C. The route needs only be in the routing table of its own router, not every neighboring router.
Reference:
"Internet Routing Architectures" Sam Halabi page 143, Cisco Press.

QUESTION 187
What is the correct sequence order that BGP routers use when determining the best route to any given destination?

A. MED, Local preference, AS-path, Weight, Origin Code
B. Origin Code, MED, Weight, AS Path, Local Preference
C. Weight, Local Preference, AS-path, Origin Code, MED
D. Weight, Local Preference, MED, AS-Path, Origin Code
E. MED, Weight, Local Preference, Origin Code, AS Path

Answer: C

Explanation:
How the Best Path Algorithm Works
BGP assigns the first valid path as the current best path. It then compares the best path with the next path in list, until it reaches the end of the list of valid paths. Following is a list of rules used to determine the best path:
1. Prefer the path with the largest WEIGHT. Note: WEIGHT is a Cisco-specific parameter, local to the router on which it's configured.
2. Prefer the path with the largest LOCAL_PREF.
3. Prefer the path that was locally originated via a network or aggregate BGP subcommand, or through redistribution from an IGP. Local paths sourced by network/redistribute commands are preferred over local aggregates sourced by the aggregate-address command.
4. Prefer the path with the shortest AS_PATH. Note the following:
5. 1. This step is skipped if bgp bestpath as-path ignore is configured.
2. An AS_SET counts as 1, no matter how many ASs are in the set.
3. The AS_CONFED_SEQUENCE is not included in the AS_PATH length.
4. Prefer the path with the lowest origin type: IGP is lower than EGP, and EGP is lower than INCOMPLETE.
5. Prefer the path with the lowest multi-exit discriminator (MED).

QUESTION 188
You are setting up BGP on router CK1 and you wish to simplify the configuration file through the use of BGP peer groups. Which of the following best describes the proper use of BGP peer groups?

A. They should be used for peers with common community values
B. They should be used for peers with common inbound announcement policies
C. They should be used for peers with common outbound announcement policies

D. They should be sued to combine MED inbound policies
E. They should be used to peers with common transitive AS policies

Answer: C

Explanation:
The major benefit of specifying a BGP peer group is that it reduces the amount of system resources (CPU and memory) used in an update generation, and it also simplifies the BGP configuration. It reduces the load on system resources by allowing the routing table to be checked only once, and updates to be replicated to all peer group members instead of being done individually for each peer in the peer group. Depending on the number of peer group members, the number of prefixes in the table, and the number of prefixes advertised, this can significantly reduce the load. Cisco recommends that you group together peers with identical outbound announcement policies.

QUESTION 189
Router CK1 is being configured for as both an IBGP peer to the other routers within the Certkiller network, and as an EBGP peer to the ISP. Select the BGP attributes that are required to be sent to these BGP neighbors from CK1 :

A. AS_PATH
B. MED
C. NEXT_HOP
D. LOCAL_PREF
E. ORIGIN
F. ROUTER_ID

Answer: A, C, E

Explanation:
AS-PATH, NEXT-HOP, and ORIGIN are all well known, mandatory BGP attributes, which is defined below:
Well known mandatory attributes: These attributes must be recognized by all BGP speakers, and must be included in all update messages. Almost all of the attributes impacting the path decision process, described in the next section, are well known mandatory attributes.
Origin Code
The ORIGIN is a well known mandatory attribute that indicates the origin of the prefix, or rather, the way in which the prefix was injected into BGP. There are three origin codes, listed in order or preference:
1. IGP, meaning the prefix was originated from information learned from an interior gateway protocol
2. EGP, meaning the prefix originated from the EGP protocol, which BGP replaced
3. INCOMPLETE, meaning the prefix originated from some unknown source
AS Path
The AS_PATH is a well-known mandatory attribute and is the list of all autonomous systems the prefixes contained in this update have passed through. The local

autonomous system number is added by a BGP speaker when advertising a prefix to an eBGP peer.
Next Hop
The BGP NEXT_HOP is a well-known mandatory attribute. The Next Hop attribute is set when a BGP speaker advertises a prefix to a BGP speaker outside its local autonomous system (it may also be set when advertising routes within an AS, this will be discussed in later sections). The Next Hop attribute may also serve as a way to direct traffic to another speaker, rather than the speaker advertising the route itself.
Incorrect Answers:
B. The MUTLI_EXIT_DISC (MED) is an optional non-transitive attribute that provides a mechanism for the network administrator to convey to adjacent autonomous systems to optimal entry point in the local AS.
D. The LOCAL_PREF attribute is a well-known attribute that represents the network operator's degree of preference for a route within the entire AS. It is not a mandatory attribute and it is not applied to all BGP updates.
F. The router ID is not a well known, mandatory BGP attribute.

QUESTION 190
Assume the following routes are in the BGP routing table of router CK1 .
172.16.0.0/24
172.16.1.0/24
172.16.2.0/24
172.16.3.0/24
Also assume the following commands have been configured:
router bgp 1
neighbor 10.1.1.1 remote-as 2
aggregate-address 172.16.0.0 255.255.252.0 suppress-map specific
access-list 1 permit 172.16.2.0 0.0.0.3.255
route-map specific permit 10
match ip-address 1
Which BGP routes will CK1 advertise?

A. 172.16.0.0/22
B. 172.16.0.0/22, 172.16.2.0/24, 172.16.3.0/24
C. 172.16.0.0/22, 172.16.0.0/24, 172.16.1.0/24
D. 172.16.2.0/24 and 172.16.3.0/24
E. 172.16.0.0/22 and 172.16.1.0/24

Answer: A

Explanation:
BGP allows the aggregation of specific routes into one route using the aggregate-address address mask command. Aggregation applies to routes that exist in the BGP routing table. This is in contrast to the network command, which applies to the routes that exists in IP routing table. Aggregation can be performed if at least one or more of the specific routes of the aggregate address exist in the BGP routing table. In this specific example,

the router will summarize the routes into 172.16.0.0/22, as long as at least one of the more specific 172.16 assumed routes actually exist in the routing table. Normally, aggregate addresses are advertised in addition to the more specific subnets. However, in this case the suppress map will filter the more specific routes, advertising only the 172.16.0.0/22 route.

QUESTION 191
A BGP router in the Certkiller network called P1R3 is configured as shown below:
!
hostname P1R3
!
! Output omitted
!
router bgp 50001
synchronization
bgp log-neighbor-changes
neighbor 10.200.200.11 remote-as 50001
neighbor 10.200.200.11 update-source loopback0
neighbor 10.200.200.12 remote-as 20001
neighbor 10.200.200.12 update-source Loopback0
neighbor 10.200.200.14 remote-as 50001
neighbor 10.200.200.14 update-source Loopback0
no auto-summary
PIR3#show ip bgp summary
BGP router identifier 10.200.200.13, local As number 50001
BGP table version is 1, main routing table version 1
6 network entries using 606 bytes of memory
7 path entires using 336 bytes of memory
4 BGP path attribute entries using 240 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1254 total bytes of memory
BGP activity 6/0 prefixes, 7/2 paths, scan interval 60 secs
Neighbor V AS MsgRcvd MsqSent TblVer InO OutO Up/Down State/Pfxrcd
10.200.200.11 4 50001 9 4 1 0 0 00:00: 14 6
10.200.200.12 4 50001 9 4 1 0 0 00:00: 14 6
10.200.200.14 4 50001 4 4 1 0 0 00:00: 14 0
PIR#show ip bgp
BGP table version is 1, local router: ID is 10.200.200.13
Status Codes: s suppressed, d damped, h history, * valid, > best, I - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
* i10.0.0.0 10.200.200.12 0 100 0 i
* i 10.200.200.11 0 100 0 i
* i192.168.11.0 10.200.200.12 0 100 0 50998 50222 50223 i

* i 10.200.200.11 0 100 0 50998 50222 50223 i
* i192.168.12.0 10.200.200.12 0 100 0 50998 50222 50223 i
* i 10.200.200.11 0 100 0 50998 50222 50223 i
* i192.168.13.0 10.200.200.12 0 100 0 50998 50222 50223 i
* i 10.200.200.11 0 100 0 50998 50222 50223 i
* i192.168.14.0 10.200.200.11 0 100 0 50998 50222 50223 i
* i 10.200.200.11 0 100 0 50998 50222 50223 i
<output omitted>
PIR#show ip route
Codes: C - connected, s - static, I IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, 0 - OSPF< IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - is-is, su - IS-IS summary, L1 - IS-IS leval-1, L2 - IS-IS level - 2
Ia - IS-IS inter area, * - candidate default, U - per-user static route
O - ODR, P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
o 10.200.200.11/32 [110/11] via 10.1.1.1, 00:06:38, Ethernet0/0
o 10.200.200.14/32 [110/65] via 10.1.3.4, 00:06:38, Seriall/0
o 10.200.200.12/32 [110/75] via 10.1.1.1, 00:06:38, Ethernet0/0
c 10.200.200.13/32 is directly connected, Loopback0
c 10.1.3.0/24 is directly connected, Seriall/0
o 10.1.2.0/72 [110/74] via 10.1.3.4, 00:06:38, Seriall/0
c 10.1.1.0/24 is directly connected, Ethernet0/0
c 10.1.0.0/24 [110/74] via 10.1.1.1, 00:06:38, Ethernet 0/0
Router PIR3 is running an IBGP full-mesh with its IBGP neighbors (10.200.200.11, 10.200.200.12, and 10.200.200.14). Based on the BGP configuration and the show command outputs above, why are BGP routes not being selected in the BGP table and placed into the IP routing table?

A. Because the 10.200.200.11 and 10.200.200.12 neighbors are setting the Weight to 0
B. Because the 10.200.200.11 and 10.200.200.12 neighbors are setting the MED to 0
C. Because the 10.200.200.11 and 10.200.200.12 neighbors are not using next-hop-self
D. Because synchronization is enabled on PIR 3
E. Because there are no routes to reach the next-hops

Answer: D

Explanation:
A BGP router with synchronization enabled will not advertise iBGP-learned routes to other eBGP peers if it is not able to validate those routes in its IGP. Assuming that IGP has a route to iBGP-learned routes, the router will announce the iBGP routes to eBGP peers. Otherwise the router treats the route as not being synchronized with IGP and does not advertise it. Disabling synchronization using the no synchronization command under

router BGP prevents BGP from validating iBGP routes in IGP. By default, synchronization is enabled on all BGP routers.

QUESTION 192
With regards to BGP and the administrative distance in a routed environment, which statement is correct?

A. The administrative distance of all BGP routes is 20, which explains why BGP routes are preferred over any IGP (such as OSPF).
B. BGP is a path vector protocol, and thus does not employ the concept of administrative distance.
C. BGP dynamically adjusts its administrative distance to match that of the IGP within the AS to eliminate routing confusion.
D. BGP actually employs two different administrative distance values: IBGP is 20, while EBGP is 200.
E. BGP actually employs two different administrative distance values: IBGP is 200, while EBGP is 20.

Answer: E

Explanation:
BGP employs the use of two separate administrative distances, based on the type of BGP route. (Internal or External)
The table below lists the administrative distance default values of the protocols that Cisco supports:

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

Incorrect Answers:

A. Only external BGP routes have an AD of 20. Internal BGP routes are given a high AD to prevent these routes from overriding the routes from the IGP routing protocols, such as OSPF, EIGRP, RIP, etc.
B. BGP is indeed considered a path vector routing protocol, but it does also use the concept of AD, as shown in the table above.
C. The AD of BGP routes is static, with the default values shown in the table. These values can be configured to use different values, but they will still be considered static and will not change dynamically.
D. BGP does indeed use two different values, but the values used are the reverse. EBGP is 20 while IBGP is 200.

QUESTION 193
You are configuring the Certkiller Internet router as a BGP peer to your ISP's router. After doing this, which BGP attributes will be carried in every BGP update (both IBGP and EBGP)?

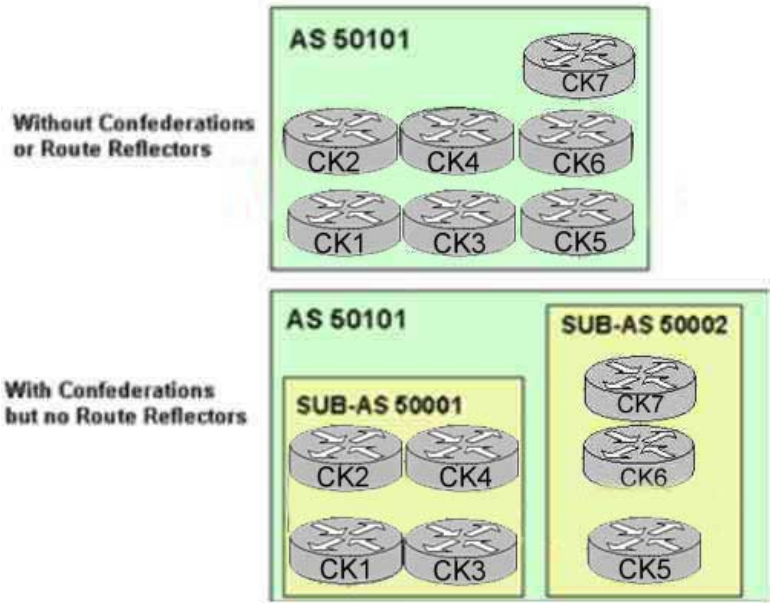
A. Origin, AS-Path, Next Hop
B. Origin, local preference, AS-Path
C. Router-ID, Origin, AS-Path
D. Router-ID, Local-Preference, Next-Hop
E. AS-Path, Local Preference, Next-Hop

Answer: A

Explanation:
Origin, AS-PATH, and Next-Hop are all well known, mandatory BGP attributes, which is defined below:
Well known mandatory attributes: These attributes must be recognized by all BGP speakers, and must be included in all update messages. Almost all of the attributes impacting the path decision process, described in the next section, are well known mandatory attributes.
Origin Code
The ORIGIN is a well known mandatory attribute that indicates the origin of the prefix, or rather, the way in which the prefix was injected into BGP. There are three origin codes, listed in order or preference:
1. IGP, meaning the prefix was originated from information learned from an interior gateway protocol
2. EGP, meaning the prefix originated from the EGP protocol, which BGP replaced
3. INCOMPLETE, meaning the prefix originated from some unknown source
AS Path
The AS_PATH is a well-known mandatory attribute and is the list of all autonomous systems the prefixes contained in this update have passed through. The local autonomous system number is added by a BGP speaker when advertising a prefix to an eBGP peer.

Next Hop
The BGP NEXT_HOP is a well-known mandatory attribute. The Next Hop attribute is set when a BGP speaker advertises a prefix to a BGP speaker outside its local autonomous system (it may also be set when advertising routes within an AS, this will be discussed in later sections). The Next Hop attribute may also serve as a way to direct traffic to another speaker, rather than the speaker advertising the route itself.
Incorrect Answers:
B, D, E. The LOCAL_PREF attribute is a well-known attribute that represents the network operator's degree of preference for a route within the entire AS. It is not a mandatory attribute that is applied to all BGP updates.
C, D. The router ID is not a well known, mandatory BGP attribute.

QUESTION 194
The Certkiller BGP network has been assigned AS number 50101 as shown below:



The Certkiller AS 50101 network is split into two AS numbers (Sub-AS 50001 and Sub-AS 50002) using Confederations without any route reflectors. Sub-AS 50001 contains 4 routers and sub-AS 50002 contains the other 3 routers. Based on this information, how many IBGP sessions are required?

A. 9 IBGP sessions using Confederations with two sub-ASs where one of the sub-AS contains 4 routers and the other sub-As contains the other 3 routes.
B. 11 IBGP sessions using Confederations with two sub-ASs where one of the sub-AS contains 4 routers and the other sub-As contains the other 3 routes.
C. 18 IBGP sessions using Confederations with two sub-ASs where one of the sub-AS contains 4 routers and the other sub-As contains the other 3 routes.
D. 21 IBGP sessions using Confederations with two sub-ASs where one of the sub-AS contains 4 routers and the other sub-As contains the other 3 routes.
E. 25 IBGP sessions using Confederations with two sub-ASs where one of the sub-AS contains 4 routers and the other sub-As contains the other 3 routes.

Answer: A

Explanation:
The advantage of confederations is that they sharply reduce the number of IBGP peering sessions. IBGP is used normally within each member AS, but a special version of EBGP known as confederations. EBGP is run between the autonomous systems.
Confederations are another way of scaling IBGP. Defined in RFC 3065, this feature introduces a divide-and-conquer approach to remove the full mesh requirement.
Using confederations an AS is split into multiple sub-ASs, but the network still appears as one AS to the outside world. Each sub-AS number is stripped from AS path at the confederation border. A full IBGP mesh is only required within each sub-AS, which is usually a manageable number of routers. In very large networks, you can even configure route reflection within a sub-AS. Typically private ASs are assigned for each sub-AS number.
With IBGP, all routers are to be configured as a fully meshed topology. The number of connections needed for any fully meshed configuration can be found by the formula:
N (N-1)
2
There are 4 Sub-AS peers in 5001 so that makes 4*3 / 2 = 6 peer sessions.
Similarly, there are 3 peers in Sub-As 5002, so we have 3*2 / 2 = 3 peer sessions
Therefore, the total number of peering sessions is 9(6+3).
Reference: Jeff Doyle, "Routing TCP/IP" Vol. II page 287

QUESTION 195
Router CK1 is used as the Certkiller Internet router and is configured for BGP. The Ip BGP information of this router is displayed below:
CK1 # show ip bgp
BGP table version is 12, local router ID is 172.16.1.2
Status code: s supported, d damped, h history, * valid, > best,
i - internal Origin codes: i IGP, e - EGP ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*> 192.168.0.0/16 172.16.1.1 0 0 50103 {50101, 50102} i
Given above information, why does the 192.168.0.0/16 prefix contain an AS-PATH of 50 103 { 50101, 50102}

A. Because AS 50101 and AS 50102 are Transit AS's
B. Because AS 50103 is using BGP confederations with two sub-ASs (sub-AS 50101 and sub-AS 50102)
C. Because it is an aggregate route and the more specific routes have passed through AS 50101 and AS 50102
D. Because AS 50103 is using AS-Path pre-pending to influence the return traffic
E. Because AS 50103 is performing route summarization using the network 192.168.0.0. mask 255.255.0.0 command

Answer: C

Explanation:
In this example, the 192.168.0.0/16 route includes the SET {50101, 50102}. This indicates that aggregate route of 192.168.0.0 actually summarizes routes that have passed through AS 50101 and AS 50102. The AS-SET information is preserved because it becomes important in avoiding loops as it maintains an indication of where the route has been.
Incorrect Answers:

A. Transit AS numbers are displayed normally in the IP BGP table.
B. Confederations are seen as only one single AS to the rest of the Internet, so they will not appear as an AS-SET to EBGP peers.
D. AS Path prepending is displayed normally, and if this were the case then you would see multiple entries in a row for the same AS number.
E. Summarized routes only appear in an AS SET when the more specific routes have passed through multiple different AS numbers.
Reference: Bassam Halabi, "Internet Routing Architectures" Cisco Press, page 359.

QUESTION 196
The IP BGP information for a specific network on router CK1 is displayed below:
CK1 #show ip bgp 10.254.0.0
BGP routing table entry for 10.254.0.0/24, version 8
Paths: (2 available, best #1, table
Default-IP-Routing-Table, not advertised
Advertised to non peer-group peers:
10.1.0.2 10.200.200.13 10.200.200.14
50998
172.31.1.3 from 172.31.1.3 (172.31.1.3)
Origin IGP, metric 0, localpref 100, valid, external, best
Community: 50998:1 no-export
50998
172.31.1.3 from 10.1.0.2 (10.200.200.12)
Origin IGP, metric 0, localpref 100, valid, internal
Router CK1 , which is in Transit AS 50001, is not propagating the 10.254.0.0/24 prefix to its neighboring ASs. Based the "show IP BGP 10.254.0.0" output shown, determine a possible cause of this problem.

A. Because the 10.254.0.0/24 prefix is tagged with the no-export community
B. Because the best path chosen by BGP is the IBGP learned path
C. Because the best path chosen by BGP is the EBGP learned path
D. Because the 10.254.0.0/24 prefix has a MED of 0
E. Because of the EBGP split horizon rule

Answer: A

Explanation:
From the output shown above, the 10.254.0.0 route is indeed tagged with the BGP

community of no-export. The Well Known BGP community of NO EXPORT means that the route can be advertised to other IBGP peers, but it is not to be passed to EBGP peers. If the BGP community of NO ADVERTISE was used instead, then this route would not be forwarded to both IBGP as well as EBGP peers.
Incorrect Answers:
B, C. Regardless of the path that the BGP route was learned, the default behavior is to forward the route to EBGP peers.
D. The metric 0 shown in the example above is the normal behavior for IBGP learned routes.
E. BGP does not use the split horizon rule. This rule applies to distance vector interior routing protocols. BGP is considered to be a path vector external routing protocol.

QUESTION 197
The Certkiller network is using BGP for Internet routing, and part of the router configuration is shown below:

```
router bgp 50101
neighbor 10.1.1.1 remote-as 50102
neighbor 10.2.2.2 remote-as 50103
neighbor 10.2.2.2 route-map test2 out
neighbor 10.1.1.1 route-map test out
!
ip as-path access-list 1 permit _50104$
ip as-path access-list 2 permit .*
!
route-map test permit 10
match as-path 1
set metric 140
!
route-map test permit 20
match as-path 2
!
route-map test2 permit 10
set metric 100
```

Based on the configuration above, which statement is correct?

A. All prefixes originating in AS 50104 will be advertised to the 10.1.1.1 neighbor with a MED of 150.
B. All prefixes not originating in AS 50104 will be advertised to the 10.1.1.1 neighbor with a MED of 0.
C. All prefixes not originating in AS 50104 will be advertised to the 10.1.1.1 neighbor.
D. All prefixes will be advertised to the neighbor with a MED of 100.
E. All prefixes originating in AS 50104 will be advertised to the 10.2.2.2 and the 10.1.1.1 neighbor with a MED of 100.

Answer: B

Explanation:
For the 10.1.1.1 BGP peer, route-map "test" is being applied. This route map has two statement entries. The first states that all traffic originating from AS 50104 (as shown by the "
ip as-path access-list 1 permit _50104$" command statement) should have the MED set to 140. The regular expression ".*" matches everything else, so all other traffic is to be routed normally. Since the default MED value is 0, all other traffic not originating in AS will be advertised to the 10.1.1.1 peer with a MED of 0.
Incorrect Answers:

A. The MED value advertised to the 10.1.1.1 peer that originated from AS 50104 will have the MED value set to 140, not 150.
C. All prefixes, even the one originating from AS 50104 will be advertised to the 10.1.1.1 neighbor. The only difference with traffic originating from AS 50104 is that the MED values will be changed.
D, E. The default MED value is 0, not 100. The default local preference value is 100.

QUESTION 198
Assume that a BGP router has learned prefix 63.0.0.0/8 from two different BGP neighbors. Which statement regarding the BGP route selection process and how this route will be installed is correct?

A. The update from the neighbor that has the highest weight and the highest local preference becomes the preferred path.
B. The update from the neighbor that has the shortest AS path becomes the preferred path.
C. The update from the neighbor that has the highest local preference and the highest MED becomes the preferred path.
D. The update from the neighbor that has the lowest local preference becomes the preferred path.
E. The update from the neighbor that has the highest MED becomes the preferred path.

Answer: A

Explanation:
BGP selects only one path as the best path. When the path is selected, BGP puts the selected path in its routing table and propagates the path to its neighbors. BGP uses the following criteria, in the order presented, to select a path for a destination:
1. If the path specifies a next hop that is inaccessible, drop the update.
2. Prefer the path with the largest weight.
3. If the weights are the same, prefer the path with the largest local preference.
4. If the local preferences are the same, prefer the path that was originated by BGP running on this router.
5. If no route was originated, prefer the route that has the shortest AS_path.
6. If all paths have the same AS_path length, prefer the path with the lowest origin type (where IGP is lower than EGP, and EGP is lower than Incomplete).

7. If the origin codes are the same, prefer the path with the lowest MED attribute.
8. If the paths have the same MED, prefer the external path over the internal path.
9. If the paths are still the same, prefer the path through the closest IGP neighbor.
10. Prefer the path with the lowest IP address, as specified by the BGP router ID.
Incorrect Answers:
B: Although this statement is correct, the weight and local preference values have a higher precedence than the AS path length.
C, E: The lowest MED is preferred, not the highest.
D: A higher local preference is preferred over a lower one.

QUESTION 199
The Certkiller network is using BGP for external routing. If a BGP router has more than one route to the same IP prefix, in what order are BGP attributes examined in making a best path route selection?

A. LOCAL_PREF, MED, AS_PATH, WEIGHT, ORIGIN
B. WEIGHT, LOCAL_PREF, ORIGIN, AS_PATH; MED
C. WEIGHT, LOCAL_PREF, AS_PATH, ORIGIN, MED
D. WEIGHT; LOCAL_PREF, AS_PATH, MED, ORIGIN
E. MED, LOCAL_PREF, WEIGHT, ORIGIN, AS_PATH

Answer: C

Explanation:
BGP assigns the first valid path as the current best path. It then compares the best path with the next path in list, until it reaches the end of the list of valid paths. The following is a list of rules used to determine the best path.
1. Prefer the path with the highest WEIGHT.
Note: WEIGHT is a Cisco-specific parameter, local to the router on which it's configured.
2. Prefer the path with the highest LOCAL_PREF. Note the following:
3. Prefer the path that was locally originated via a network or aggregate BGP subcommand, or through redistribution from an IGP.
4. Prefer the path with the shortest AS_PATH.
5. Prefer the path with the lowest ORIGIN type: IGP is lower than EGP, and EGP is lower than INCOMPLETE.
6. Prefer the path with the lowest multi-exit discriminator (MED). Note the following:
7. Prefer external (eBGP) over internal (iBGP) paths. If bestpath is selected, go to Step 9 (multipath).
8. Prefer the path with the lowest IGP metric to the BGP next hop. Continue, even if bestpath is already selected.
9. Check if multiple paths need to be installed in the routing table for BGP Multipath. Continue, if bestpath is not selected yet.
10. 1. When both paths are external, prefer the path that was received first (the oldest one).
2. Prefer the route coming from the BGP router with the lowest router ID. The router ID

is the highest IP address on the router, with preference given to loopback addresses. It can also be set manually using the bgp router-id command.
3. If the originator or router ID is the same for multiple paths, prefer the path with the minimum cluster list length. This will only be present in BGP route-reflector environments. It allows clients to peer with RRs or clients in other clusters. In this scenario, the client must be aware of the RR-specific BGP attribute.
4. Prefer the path coming from the lowest neighbor address. This is the IP address used in the BGP neighbor configuration, and corresponds to the remote peer used in the TCP connection with the local router
Reference:
www.cisco.com/en/US/tech/ CK3 65/technologies_tech_note09186a0080094431.shtml

---

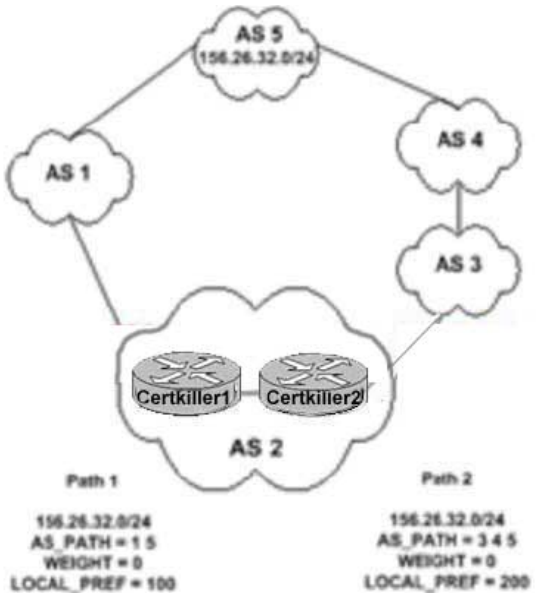
QUESTION 200
The router CK1 is being configured for BGP, and the configuration will contain both IBGP and EBGP peers. Which statements regarding IBGP and EBGP neighbors are correct? (Select three)

A. BGP updates from an IBGP peer are propagated to other IBGP and EBGP peers.
B. BGP updates from an EBGP peer are propagated to other IBGP and EBGP pees.
C. IBGP peers must be directly connected. If not, the IBGP-multihop option must be configured.
D. EBGP peers must be directly connected; otherwise, the EBGP-multihop option must be configured.
E. IBGP neighbors peering can be established using the loopback interface.
F. EBGP neighbor peering must use the physical interface address to establish peering

Answer: B, D, E

Explanation:
When a BGP router receives a BGP routing update from an EBGP neighbor, the update is propagated to all IBGP neighbors. It is important to note that the same is not true for routing updates received via an IBGP neighbor, as these updates are not passed on to all IBGP peers. This is why IBGP speakers must be configured in a full mesh.
For EBGP peers, the best method is to use the directly connected interfaces as the peering IP addresses. If not, then EBGP multihop must be used. Multihop is used only in EBGP, not in IBGP.
It is recommended to use the loopback interface when configuring IBGP peers, since this interface is always up. For IBGP, the peering IP address needs to only be reachable via the IGP, so they do not need to be directly connected.

QUESTION 201
The Certkiller network is running BGP as displayed in the diagram below:



What path will routers Certkiller 1 and Certkiller 2 take to reach the 156.36.32.0/24 network in AS 5?

A. Both will use the path through AS 1 due to Certkiller 1 having the shortest AS_PATH attributre.
B. Certkiller 1 will use the path through AS 1 and Certkiller 2 will use the path through AS 3.
C. Both will use the path through AS 1 due to Certkiller 1 having a lower LOCAL_PREF value.
D. Both Certkiller 1 and Certkiller 2 will use the path through AS 3 due to Certkiller 2 having a higher LOCA_PREF value.

Answer: D

Explanation:
BGP uses the following criteria, in the order presented, to select a path for a destination:
1. If the path specifies a next hop that is inaccessible, drop the update.
2. Prefer the path with the largest weight.
3. If the weights are the same, prefer the path with the largest local preference.
4. If the local preferences are the same, prefer the path that was originated by BGP running on this router.
5. If no route was originated, prefer the route that has the shortest AS_path.
6. If all paths have the same AS_path length, prefer the path with the lowest origin type (where IGP is lower than EGP, and EGP is lower than Incomplete).
7. If the origin codes are the same, prefer the path with the lowest MED attribute.
8. If the paths have the same MED, prefer the external path over the internal path.
9. If the paths are still the same, prefer the path through the closest IGP neighbor.
10. Prefer the path with the lowest IP address, as specified by the BGP router ID.
Based on the information above, the value of the Local Preference is considered before

the length of the AS Path. When comparing the Local Preference value, the higher one is preferred.

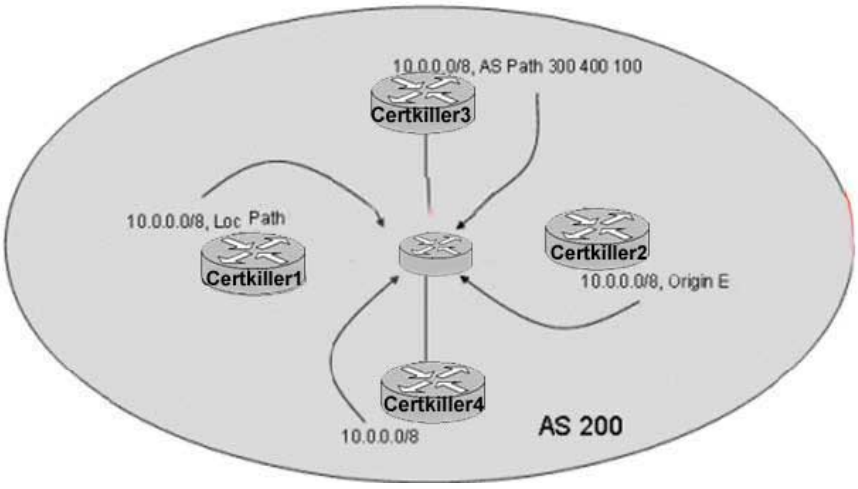
QUESTION 202
Router CK 1 and CK2 are IBGP peers. Which BGP attributes are carried in all IBGP routing updates? (Select 3)

A. MED
B. Local Preference
C. Weight
D. Community
E. AS-path
F. Cost
G. Origin

Answer: B, E, G

Explanation:
There are three well-known mandatory attributes. These must be included in updates propagated to all peers (both INGP and EBGP) and includes AS-PATH, NEXT-HOP and ORIGIN.
In addition to these three, all IBGP speakers must also carry the Local Preference information. The Local Preference is relevant when there is more than one path to a network outside of the current AS for instance if your network is connected to more than one ISP. Each of the routers that link to outside the AS can set a preference value for routes advertised into the AS, and this value indicates the router's preference for these routes. Only IBGP routers share the local preference values it does not leave the AS. The higher the value the more preferable the route is so if there are multiple paths to this network the route with the highest Local Preference is chosen and all traffic destined for the network is sent this way.

QUESTION 203
The Certkiller network resides in AS 200 as shown in the diagram below:



A BGP router receives updates for prefix 10.0.0.0/8 sourced from AS 100 from four different BGP neighbors. Certkiller 1 has the Local Preference of the prefix set to 50, while the other three neighbors do nothing with Loc Pref. Neighbor Certkiller 2 advertises the prefix with an AS path length of 3, while all other neighbors have an AS Path length of 2. The advertisement from neighbor Certkiller 3 has the origin code set to E, while the other have it set to I. And Neighbor Certkiller 4 does nothing to any of the attributes. What statement is true?

A. Neighbor Certkiller 1 is the preferred path to prefix 10.0.0.0/8, since a higher local preference is better, and local preference is compared before the others.
B. Neighbor Certkiller 2 is the preferred path to prefix 10.0.0.0/8, since a longer AS Path is better, and AS path is compared before the others.
C. Neighbor Certkiller 3 is the preferred path to prefix 10.0.0.0/8, since an origin code of E is better than I, and origin code is compared before the others.
D. Neighbor Certkiller 4 is the preferred path to prefix 10.0.0.0/8 only after neighbor Certkiller 2 dies.
E. Neighbor Certkiller 3 is the preferred path to prefix 10.0.0.0/8 only after neighbor Certkiller 4 dies.

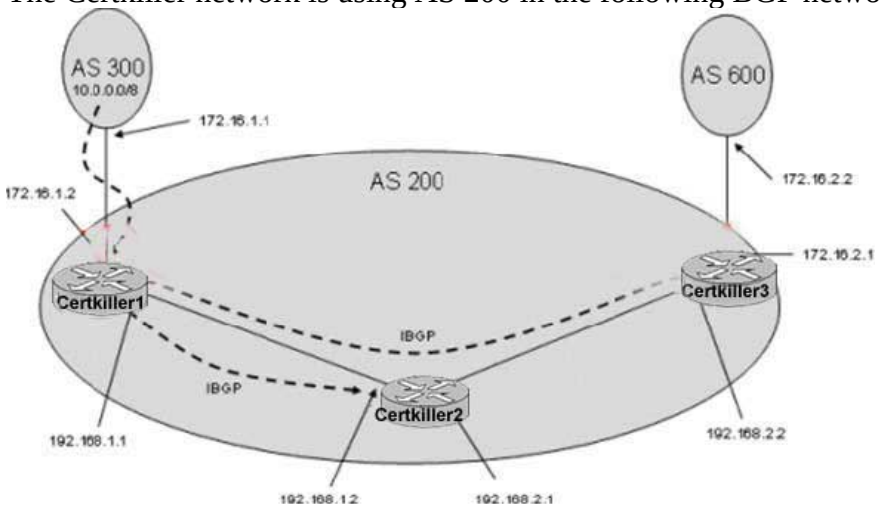
Answer: E

Explanation:
Based on the information provided, the route for 10.0.0.0/8 will be preferred from the following routers, in order:
1. Certkiller 4
2. Certkiller 3
3. Certkiller 2
4. Certkiller 1
BGP uses the following criteria, in the order presented, to select a path for a destination:
1. If the path specifies a next hop that is inaccessible, drop the update.
2. Prefer the path with the largest weight.
3. If the weights are the same, prefer the path with the largest local preference.
4. If the local preferences are the same, prefer the path that was originated by BGP running on this router.
5. If no route was originated, prefer the route that has the shortest AS_path.
6. If all paths have the same AS_path length, prefer the path with the lowest origin type (where IGP is lower than EGP; and EGP is lower than Incomplete).
7. If the origin codes are the same, prefer the path with the lowest MED attribute.
Incorrect Answers:

A. The default local preference value is 100, so router Certkiller 1 will be the last router used because its local preference was set to 50.
B. A shorter AS path is preferred over a longer one.
C. An origin code of I (Internal) is preferred over an origin code of E (External).
D. Using the information given here, router Certkiller 4 will be preferred over all the

others, and router Certkiller 2 will be used only if routers Certkiller 4 and Certkiller 3 both fail.

QUESTION 204
The Certkiller network is using AS 200 in the following BGP network:



Router Certkiller1 Configuration:

```
Certkiller1 (config)# router bgp 200
Certkiller1 (config-bgp)# neighbor 192.168.1.2 remote-as 200
Certkiller1 (config-bgp)# neighbor 192.168.1.2 next-hop-self
Certkiller1 (config-bgp)# neighbor 192.168.2.2 remote-as 200
```

Router Certkiller 1 receives an EBGP update containing 10.0.0.0/8 sourced from AS 300. Router Certkiller 1 then advertises 10.0.0.0/8 to routers Certkiller 2 and Certkiller 3 via IBGP. What does router Certkiller 3 use as a BGP next hop to reach network 10.0.0.0/8?

A. 172.16.1.1
B. 172.16.1.2
C. 192.168.1.1
D. 192.168.1.2
E. 192.168.2.1

Answer: A

Explanation:
The EBGP next-hop attribute is the IP address that is used to reach the advertising router. For EBGP peers, the next-hop address is the IP address of the connection between the peers. For IBGP, the EBGP next-hop address is carried into the local AS, as illustrated below:
Figure39-5 BGP AS-path Attribute

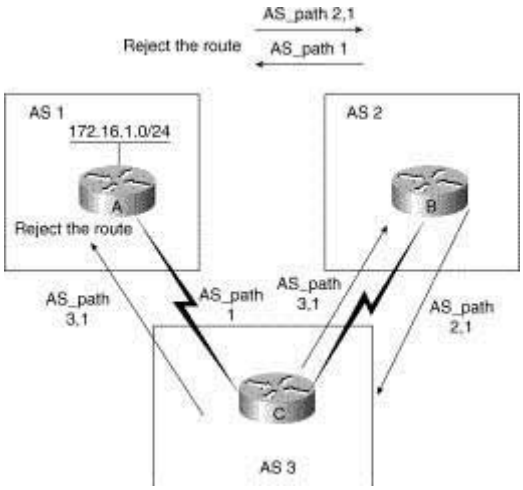
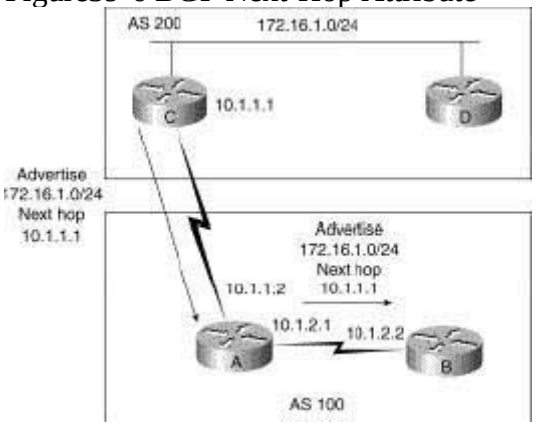


Figure39-6 BGP Next-Hop Attribute



Router C advertises network 172.16.1.0 with a next hop of 10.1.1.1. When Router A propagates this route within its own AS, the EBGP next-hop information is preserved. If Router B does not have routing information regarding the next hop, the route will be discarded. Therefore, it is important to have an IGP running in the AS to propagate next-hop routing information.

Incorrect Answers:

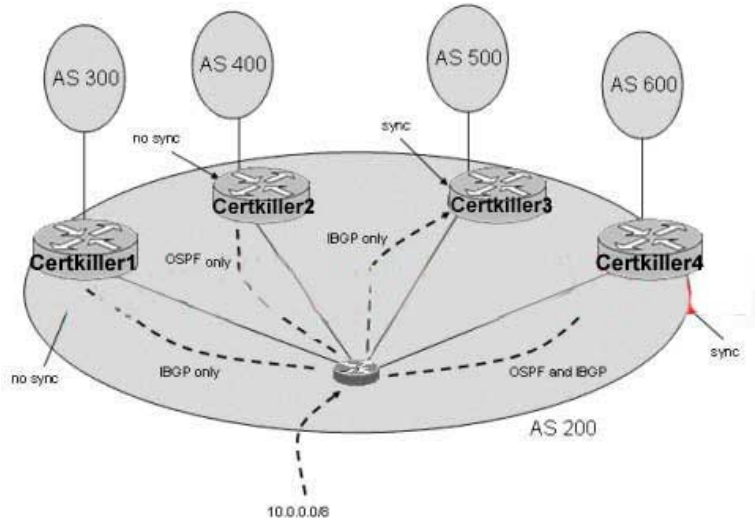
C: This would be the correct answer from router Certkiller 2's perspective, as the BGP next-hop-self configuration command was used for this peer. However, the next-hop-self command was not used for the Certkiller 3 peer, making the regular next hop rules apply. In order for Certkiller 1 to advertise itself as the next hop to all IBGP peers, it would need the "next-hop-self" command configured for all peers.

Reference: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/bgp.htm

---

QUESTION 205

The Certkiller BGP network is using AS 200 as shown in the diagram below:



A router receives an EBGP update with prefix 10.0.0.0/8. This update is then forwarded to all BGP neighbors within its AS.
Which neighbors advertise 10.0.0.0/8 with EBGP updates of their own?

A. Only router Certkiller 1 advertises 10.0.0.0/8 into AS 300.
B. Both router Certkiller 1 and router Certkiller 2 advertise 10.0.0.0/8 into their respective neighbor ASs.
C. Both router Certkiller 1 and router Certkiller 4 advertise 10.0.0.0/8 into their respective neighbor ASs.
D. Both router Certkiller 2 and router Certkiller 4 advertise 10.0.0.0/8 into their respective neighbor ASs.
E. Routers Certkiller 1, Certkiller 2, and Certkiller 4 advertise 10.0.0.0/8 into their respective neighbor ASs.

Answer: C

Explanation:
A BGP router with synchronization enabled will not advertise iBGP-learned routes to other eBGP peers if it is not able to validate those routes in its IGP. Assuming that IGP has a route to iBGP-learned routes, the router will announce the iBGP routes to eBGP peers. Otherwise the router treats the route as not being synchronized with IGP and does not advertise it. Disabling synchronization using the no synchronization command under router BGP prevents BGP from validating iBGP routes in IGP. By default, synchronization is on for all BGP routers.
In this example, Certkiller 1 will advertise this route to its EBGP peer due to the fact that synchronization is disabled. Although synchronization is enabled on router Certkiller 4, it will advertise the route because it is running both OSPF and BGP, so this route will match the corresponding route within the OSPF table and be advertised.
Incorrect Answers:

A. Both Certkiller 1 and Certkiller 4 will advertise this route.
B, C, D. Certkiller 2 will not advertise this route. Since it is not an IBGP peer, it will not

receive the routing update in the first place so it will not be able to forward this route on to the other AS.

QUESTION 206
The Certkiller 1 BGP routing routes are displayed below:

```
CertKiller1 #show ip route bgp
B    192.168.12.0/24 [200/0] via 2.2.2.2, 00:53:00
B    192.168.13.0/24 [200/0] via 2.2.2.2, 00:53:00
B    192.168.14.0/24 [200/0] via 2.2.2.2, 00:53:00
B    192.168.15.0/24 [200/0] via 2.2.2.2, 00:53:00
B    192.168.16.0/24 [200/0] via 2.2.2.2, 00:53:00
B    192.168.20.0/24 [200/0] via 2.2.2.2, 00:52:57
B    192.168.21.0/24 [200/0] via 2.2.2.2, 00:52:57
B    192.168.22.0/24 [200/0] via 2.2.2.2, 00:52:57
B    192.168.23.0/24 [200/0] via 2.2.2.2, 00:52:57
B    192.168.24.0/24 [200/0] via 2.2.2.2, 00:52:57

CertKiller1 #show run
!
! Partial show run output
!
router ppp 65101
 aggregate-address 192.168.12.0 255.255.252.0 summary-only
 aggregate-address 192.168.20.0 255.255.252.0 as-set
 neighbor 2.2.2.2 remote-as 65101
 neighbor 2.2.2.2 update-source loopback0
 neighbor 2.2.2.2 next-hop-self
 neighbor 10.1.1.1 remote-as 65104
```

Based on the show ip route bgp output and the partial show run output shown, which BGP prefixes will be advertised by Certkiller 1 to the 10.1.1.1 neighbor?

A. 192.168.12.0/22, 192.168.16.0/24, 192.168.20.0/22, 192.168.20.0/24, 192.168.21.0/24, 192.168.22.0/22, 192.168.23.0/24, 192.168.24.0/24
B. 192.168.12.0/22, 192.168.20.0/22, 192.168.20.0/24, 192.168.21.0/24, 192.168.22.0/22, 192.168.23.0/24, 192.168.24.0/24
C. 192.168.12.0/22, 192.168.20.0/22, 192.168.20.0/24, 192.168.21.0/24, 192.168.22.0/22, 192.168.23.0/24
D. 192.168.12.0/22, 192.168.20.0/22, 192.168.20.0/24
E. 192.168.12.0/22, 192.168.20.0/22
F. All routes will be advertised, since there are no route filters in place.

Answer: A

Explanation:
When the aggregate-address command is used within BGP routing, the aggregated address is advertised, along with the more specific routes. The exception to this rule is through the use of the summary-only command. The "summary-only" keyword suppresses the more specific routes and announces only the summarized route.
Using the as-set argument creates an aggregate address with a mathematical set of autonomous systems (AS). This as-set summarizes the AS_PATH attributes of the all of the individual routes. This can be useful to avoid routing loops while aggregating routes.
Again, unless the "summary-only" keyword is used with the as-set command the summary route is advertised along with the more specific routes.

In the example above, the 192.168.12.0, 192.168.13.0, 192.168.14.0, and 192.168.15.0 networks will be summarized into the only 192.168.12/22 route, which will be advertised. Along with this one route, the others will also be advertised, as well as one additional 192.168.20.0/22 route. In total, 8 different routes will be advertised.

QUESTION 207
Many of the Certkiller BGP routers are configured using peer groups. Which of the following correctly display the common properties of BGP peer groups?

A. Community values
B. Inbound policies
C. Outbound policies
D. MED inbound policies
E. Transitive AS policies
F. None of the above

Answer: C

Explanation:
BGP neighbors who share the same outbound policies can be grouped together in what is called a BGP peer group. Instead of configuring each neighbor with the same policy individually, Peer group allows to group the policies which can be applied to individual peer thus making efficient update calculation along with simplified configuration.
Reference:
www.cisco.com/en/US/tech/ CK3 65/technologies_tech_note09186a0080093fb7.shtml

---

QUESTION 208
While verifying the BGP configuration of router Certkiller 1, you issue the following command:

```
Certkiller1#show route-map setweight
route-map test, permit, sequence 10
  Match clauses:
    ip address prefix-lists: filter
    as-path (as-path filter): 1 2

  Set clauses:
    weight 200
  Policy routing matches: 0 packets, 0 bytes
```

Based upon the show route-map setweight output shown above, which matching routes will be set to a weight of 200?

A. Routes that match the prefix-list named filter
AND
also match either the as-path filter 1 OR 2

B. Routes that match the prefix-list named filter
OR
also match either the as-path filter 1 AND 2
C. Routes that match the prefix-list named filter
AND
also match either the as-path filter 1 AND 2
D. Routes that match the prefix-list named filter
OR
also match either the as-path filter 1 OR 2

Answer: A

Explanation:
When the match clauses are shown on different lines, then all of the match conditions must be met. In this example, both the IP prefix list named "filter" and the AS path filter must match in order to set the weight to 200 as shown. However, in this configuration, there are two AS path filters configured, numbered 1 and 2. In this case, only one of the two filters needs to be matched. If all three of the criteria had needed to be met, then there would be three distinct lines listed under the match clauses.

QUESTION 209
An EIGRP multicast flow timer is defined as which of the following?

A. The timeout timer after which EIGRP retransmits to the neighbor in non CR mode, through unicasts.
B. The time interval that EIGRP hello packets are sent.
C. The timer after which EIGRP will not forward multicast data traffic.
D. The timer interval between consecutive transmitted EIGRP hello intervals.
E. The timeout timer after which EIGRP retransmits to the neighbor in CR mode, through unicasts.
F. None of the above.

Answer: E

Explanation:
After pair of routers become neighbors, they will send routing updates (and other packets) to one another using a reliable multicast scheme. For example, if router one has a series of packets which must be transmitted to routers two, three, and four such as a routing table update, it will send the first packet to the EIGRP multicast address, 224.0.0.10, and wait for an acknowledgment from each of its neighbors on its Ethernet interface (in this case, routers two, three and four). Let's assume that routers two and four do answer, but router three does not.
Router one will wait until the multicast flow timer expires on the Ethernet interface, then send out a special packet, a sequence TLV, telling router three not to listen to any further multicast packets from router one, then it will continue transmitting the remainder of the update packets as multicast to all other routers on the network. The sequence TLV

indicates an out-of-sequence multicast packet. Those routers not listed in the packet enter Conditional Receive (CR) mode, and continue listening to multicast. While there are some routers in this mode, the Conditional Receive bit will be set in multicast packets. In this case, router one will send out a sequence TLV with router three listed, so routers two and four will continue listening to further multicast updates.

QUESTION 210
Which components are factored in by default when an EIGRP metric is calculated? (Choose all that apply)

A. MTU
B. Delay
C. Load
D. Bandwidth
E. Reliability

Answer: B, D

Explanation:
By default, EIGRP uses only bandwidth and Delay when calculating the metric. EIGRP uses these scaled values to determine the total metric to the network:
1. metric = [K1 * bandwidth + (K2 * bandwidth) / (256 - load) + K3 * delay] * [K5 / (reliability + K4)]
The default values for K are:
1. K1 = 1
2. K2 = 0
3. K3 = 1
4. K4 = 0
5. K5 = 0
For default behavior, you can simplify the formula as: Metric = Bandwidth + Delay
Incorrect Answers:

A. The MTU is tracked but never used in calculating the metric for IGRP or EIGRP at any time.
C, E. Although Load and Reliability are K values that can indeed be factored into the metric, by default their K value is 0 so they are not used.
Reference:
http://www.cisco.com/warp/public/103/eigrp-toc.html#eigrpmetrics

---

QUESTION 211
The topology of a network changes causing an EIGRP router to go into the active state. The DUAL process shows a new route that meets the EIGRP Feasibility Condition. In regards to this specific route, which of the following is true?

A. The Feasible Distance of the new route must be equal to one.
B. The Feasible Distance of the new route must be higher than one.

C. The Reported Distance of the new route must be equal to Feasible Distance.
D. The Reported Distance of the new route must be higher than Feasible Distance.
E. The Reported Distance of the new route must be lower than Feasible Distance.

Answer: E

Explanation:
The following are some terms relating to EIGRP:
1. Feasible Distance: The lowest calculated metric to each destination
2. Feasibility Condition: A condition that is met if a neighbor's advertised distance to a destination is lower that the router's Feasible Distance to that same destination.
3. Successor: The neighbor that has been selected as the next hop for a given destination based on the Feasibility Condition.
Reference:
Jeff Doyle, Routing TCP/IP, Volume I, Chapter 8: Enhanced Interior Gateway Routing Protocol (EIGRP), p.336-337, Cisco Press, (ISBN 1-57870-041-8)
Incorrect Answers:
A: The metric of the new route needs only to be less than the current metric to the destination (feasible distance), and does not necessarily need to equal one.
B: It is feasible that the new metric to the destination could equal one, and also be lower than the current metric.
C, D: The reported distance must be lower than the feasible distance.
Additional info:
The Feasible Condition is met when the receiving router has a Feasible Distance (FD) to a particular network and it receives an update from a neighbor with a lower advertised or Reported Distance (RD) to that network. The neighbor then becomes a Feasible Successor (FS) for that route because it is one hop closer to the destination network. There may be a number of Feasible Successors in a meshed network environment.
The RD for a neighbor to reach a particular network must always be less than the FD for the local router to reach that same network. In this way EIGRP avoids routing loops. This is why routes that have RD larger than the FD are not entered into the Topology table.
Reference:
Ravi Malhotra, IP Routing, Chapter 4: Enhanced Interior Gateway Routing Protocol (EIGRP), O'Reilly Press, January 2002 (ISBN 0-596-00275-0)

QUESTION 212
Which of the following EIGRP packets require an acknowledgement? (Choose all that apply)

A. Hello
B. Query
C. Reply
D. Update
E. Ack
F. None of the above

Answer: B, C, D

Explanation:
Updates are used to convey reachability of destinations. When a new neighbor is discovered, update packets are sent so the neighbor can build up its topology table. In this case, update packets are unicast. In other cases, such as a link cost change, updates are multicast. Updates are always transmitted reliably.
Queries and replies are sent when destinations go into Active state. Queries are always multicast unless they are sent in response to a received query. In this case, it is unicast back to the successor that originated the query. Replies are always sent in response to queries to indicate to the originator that it does not need to go into Active state because it has feasible successors. Replies are unicast to the originator of the query. Both queries and replies are transmitted reliably.
EIGRP reliable packets are: Update, Query and Reply.
EIGRP unreliable packets are: Hello and Ack.
Incorrect Answers:
A, E. Hellos are multicast for neighbor discovery/recovery. They do not require acknowledgment. A hello with no data is also used as an acknowledgment (ack). Acks are always sent using a unicast address and contain a non-zero acknowledgment number.
Reference: Cisco BSCN version 1.0 study guide, pages 6-18.

QUESTION 213
Which of the following types of EIGRP packets contain the Init flag?

A. Hello/Ack
B. Query
C. Reply
D. Update
E. None of the above

Answer: D

Explanation:
In EIGRP header there is an 8-bit flag value. The rightmost bit is init.
Which when set to 0x00000001 indicates that the enclosed route entries are the first in a new neighbor relationship.
Also the route entries are carried in update packet not hello packet.
Additional Info:
The following debug output displays the Init Sequence increasing only with the update packet.
Router# debug eigrp packetEIGRP: Sending HELLO on Ethernet0/1 AS 109, Flags 0x0, Seq 0, Ack 0EIGRP: Sending HELLO on Ethernet0/1 AS 109, Flags 0x0, Seq 0, Ack 0EIGRP: Sending HELLO on Ethernet0/1 AS 109, Flags 0x0, Seq 0, Ack 0EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24, AS 109,
Flags 0x1, Seq 1, Ack 0EIGRP: Sending HELLO/ACK on
Ethernet0/1 to 192.195.78.24, AS 109, Flags 0x0, Seq 0, Ack

1EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
AS 109, Flags 0x0, Seq 0, Ack 1EIGRP: Received UPDATE on
Ethernet0/1 from 192.195.78.24, AS 109, Flags 0x0, Seq 2,
Ack 0Incorrect Answers:

A. Hellos are multicast for neighbor discovery/recovery. They do not require acknowledgment. A hello with no data is also used as an acknowledgment (ack). Acks are always sent using a unicast address and contain a non-zero acknowledgment number.
B, C. Queries and replies are sent when destinations go into Active state. Replies are always sent in response to queries to indicate to the originator that it does not need to go into Active state because it has feasible successors. Replies are unicast to the originator of the query. Both queries and replies are transmitted reliably.
Reference: "Routing TCP/IP" Jeff Doyle Pg364

QUESTION 214
In your EIGRP network you notice that the neighbor relationship between two of your routers was recently restarted. Which of the following could have occurred to have caused this? (Choose all that apply)

A. The clear ip route command was issued.
B. The ARP cache was cleared.
C. The IP cache was cleared.
D. An update packet with Init flag set from a known, already established neighbor relationship was received by one of the routers.
E. The IP EIGRP neighbor relationship was cleared manually.

Answer: D, E

Explanation:
D as well as E will result in EIGRP relationship to be restarted.
The reason for D: If a router receives an update packet with the init flag set it clearly implies that this packet is the first after a new neighbor relationship has been established.
The reason for E: If we clear the IP EIGRP neighbor relationship it will automatically result in EIGRP neighbor relationship to be restarted.
Incorrect Answers:

A. This will clear the IP routing table, but will not have any affect on the EIGRP neighbor relationship.
B. This will only clear the MAC address learned ARP cache.
C. This also will not have any affect on the EIGRP neighbor relationship.

QUESTION 215
The Certkiller EIGRP network has a router named Router CK2 . Router CK2 is connected to an EIGRP neighbor, CK1 . CK1 is defined as a stub. With regard to this network, which of the following are true?

A. Router CK1 will not advertise any network routes to CK2 .
B. Router CK2 will send only summary routes to CK1 .
C. Router CK2 will not query CK1 about any internal route.
D. Router CK2 will not query CK1 about any external route.
E. Router CK2 will not query CK1 about any route.
F. None of the above.

Answer: E

Explanation:
E is the best choice, as an EIGRP router will not query a stub neighbor about any route.
Incorrect Answers:

A. CK1 will still be required to advertise its network routes to the neighbor, even though it is configured as a stub.
B. CK2 still sends all routes to CK1 .
C, D. Although both of these are true, since CK2 will not query CK1 about any route, E is a better choice.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s15/eigrpstb.htm

---

QUESTION 216
The Certkiller network uses EIGRP as the routing protocol and has an ISDN connection that is used as a backup to their frame relay network. The ISDN link successfully comes up when the frame relay network fails, but no routing traffic will pass over the ISDN link. What could be the cause of this problem?

A. The dialer-list is blocking EIGRP.
B. The EIGRP configuration is incorrect.
C. The encapsulation is different on the opposite ends of the link.
D. There is a network type mismatch.
E. The broadcast keyword is missing from the dialer-map.

Answer: E

Explanation:
For routing protocol traffic to pass over the ISDN link, the broadcast keyword must be present in the dialer map.
Incorrect Answers:

A. Although the dialer list may indeed be blocking EIGRP updates, so that these updates do not initiate ISDN calls, one the ISDN link is up, all traffic will be able to traverse this link, and not just the traffic that is defined as interesting.
C, D. If this were the case, there would be a problem with the ISDN link connecting in the first place.

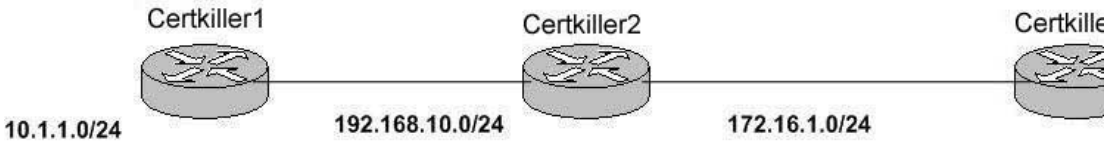
QUESTION 217
How is the metric for a summarized route derived when the interface summary command for EIGRP is used?

A. It is derived from the route that has the biggest metric.
B. It is derived from the route that has the smallest metric.
C. It is derived from the interface that has the summary command configured on it.
D. It is derived from the route that has the shortest matching mask.
E. It is derived from the default-metric.

Answer: B

Explanation:
According to Cisco's EIGRP design guide, "The metric is the best metric from among the summarized routes."
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfeigrp.htm#1001078
"...EIGRP will advertise the summary address out the interface with a metric equal to the minimum of all more specific routes."

QUESTION 218
Routers Certkiller 1, Certkiller 2, and Certkiller 3 are all configured for EIGRP as shown below:



Certkiller 1 has the following configuration:
router eigrp 1
network 192.168.10.0
redistribute connected
Which routes would show up in the routing table of Certkiller 3 as EIGRP routes? (Choose all that apply)

A. 10.1.0.0/16
B. 10.0.0.0/24
C. 10.0.0.0/8
D. 10.1.1.0/24
E. 192.168.10.0/24

Answer: C, E

Explanation:
EIGRP will perform auto-summarization of External Routes. Since the 10.1.1.0 network was redistributed into EIGRP via a connected network, this will automatically make this route external to EIGRP. The 192.168.10.0 network will also show up in the routing table

as an EIGRP route through the normal EIGRP process.
Additional Info:
Auto-Summarization
EIGRP performs an auto-summarization
each time it crosses a border between two different major networks.
For example, in Figure 13, Router Two advertises only the 10.0.0.0/8 network to Router One, because the interface Router Two uses to reach Router One is in a different major network.

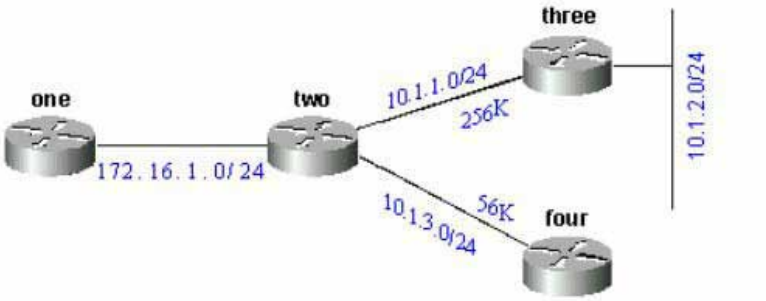
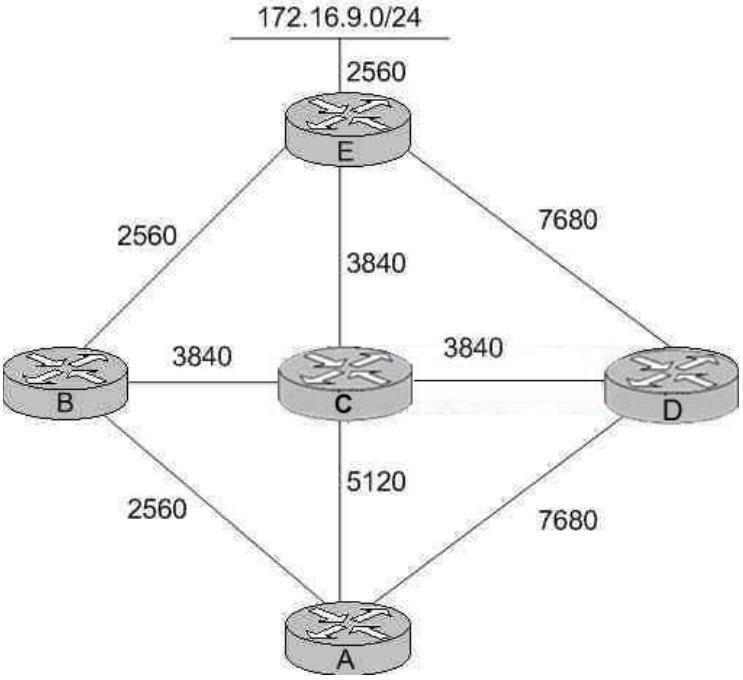


Figure 13

On Router One, this looks like the following:
one#show ip eigrp topology 10.0.0.0
IP-EIGRP topology entry for 10.0.0.0/8
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 11023872
Routing Descriptor Blocks:
172.16.1.1 (Serial0), from 172.16.1.2, Send flag is 0x0
Composite metric is (11023872/10511872), Route is Internal
Vector metric:
Minimum bandwidth is 256 Kbit
Total delay is 40000 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500
Hop count is 1
This route is not marked as a summary route in any way; it looks like an internal route. The metric is the best metric from among the summarized routes. Note that the minimum bandwidth on this route is 256k; although there are links in the 10.0.0.0 network that have a bandwidth of 56k.
On the router doing the summarization, a route is built to null0 for the summarized address:
two#show ip route 10.0.0.0
Routing entry for 10.0.0.0/8, 4 known subnets
Attached (2 connections)
Variably subnetted with 2 masks
Redistributing via eigrp 2000
C 10.1.3.0/24 is directly connected, Serial2
D 10.1.2.0/24 [90/10537472] via 10.1.1.2, 00:23:24, Serial1
D 10.0.0.0/8 is a summary, 00:23:20, Null0

C 10.1.1.0/24 is directly connected, Serial1
The route to 10.0.0.0/8 is marked as a summary through Null0. The topology table entry for this summary route looks like the following:
two#show ip eigrp topology 10.0.0.0
IP-EIGRP topology entry for 10.0.0.0/8
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 10511872
Routing Descriptor Blocks:
0.0.0.0 (Null0), from 0.0.0.0, Send flag is 0x0
(note: the 0.0.0.0 here means this route is originated by this router)
Composite metric is (10511872/0), Route is Internal
Vector metric:
Minimum bandwidth is 256 Kbit
Total delay is 20000 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500
Hop count is 0
Incorrect Answers:
A, B, D. Any more specific routes in the 10.0.0.0 network will be summarized into one 10.0.0.0/8 network. Again, since the 10.0.0.0 network was learned by EIGRP only via redistribution, it is external as far as EIGRP is concerned.

QUESTION 219
The Certkiller EIGRP network topology is displayed below, along with the EIGRP metric values for each link:



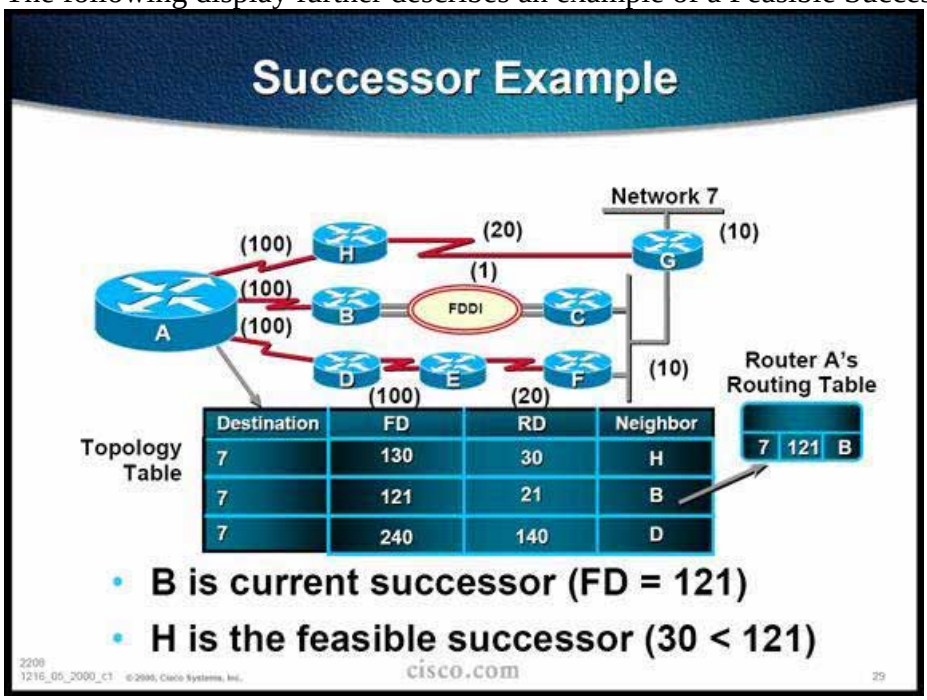
From the perspective of router A shown above, which of the following routers would be considered the successor and the feasible successors to the 172.16.9.0/24 network? (Select two choices below)

A. B is the successor
B. C is the successor
C. D is the successor
D. B is a feasible successor
E. C is a feasible successor
F. D is a feasible successor.
G. E is a feasible successor

Answer: A, E

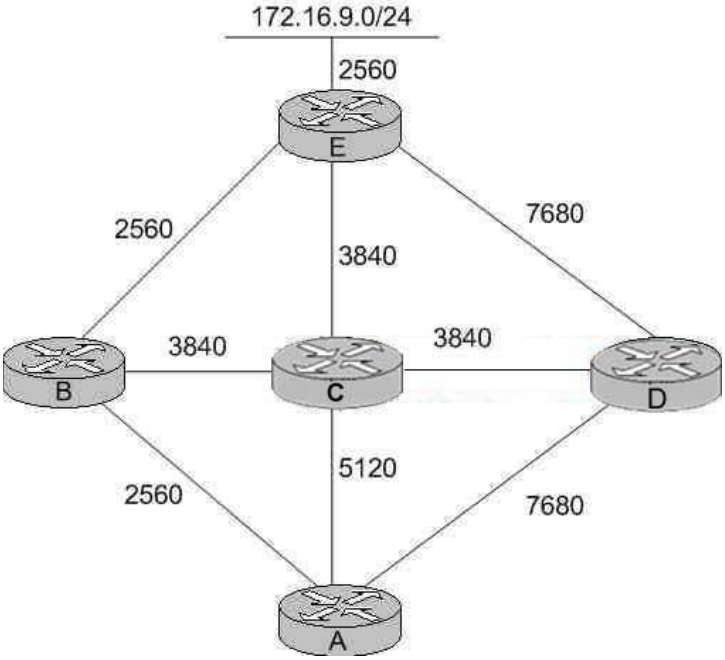
Explanation:
The following are some terms relating to EIGRP:
1. Feasible Distance: The lowest calculated metric to each destination
2. Feasibility Condition: A condition that is met if a neighbor's advertised distance to a destination is lower that the router's Feasible Distance to that same destination.
3. Successor: The neighbor that has been selected as the next hop for a given destination based on the Feasibility Condition.
4. Feasible Successor: A neighbor whose Reported Distance (RD) is less than the Feasible Distance (FD).
The Feasible Condition is met when the receiving router has a Feasible Distance (FD) to a particular network and it receives an update from a neighbor with a lower advertised or Reported Distance (RD) to that network. The neighbor then becomes a Feasible Successor (FS) for that route because it is one hop closer to the destination network. There may be a number of Feasible Successors in a meshed network environment.
The RD for a neighbor to reach a particular network must always be less than the FD for the local router to reach that same network. In this way EIGRP avoids routing loops. This is why routes that have RD larger than the FD are not entered into the Topology table.
In this example, Router B would be the successor, with a feasible distance of 7680 (2560+2560+2560). Therefore, only routers with an AD of less than 7680 will become successors. In this case, router C will have an Advertised Distance of 6400 so it is a FS. Router D has a RD of 10240, and since it must be less than the current FD, it will not become a FS.
Reference:
Jeff Doyle, Routing TCP/IP, Volume I, Chapter 8: Enhanced Interior Gateway Routing Protocol (EIGRP), p.336-337, Cisco Press, (ISBN 1-57870-041-8)

The following display further describes an example of a Feasible Successor:



QUESTION 220

The Certkiller EIGRP network is displayed in the following diagram:



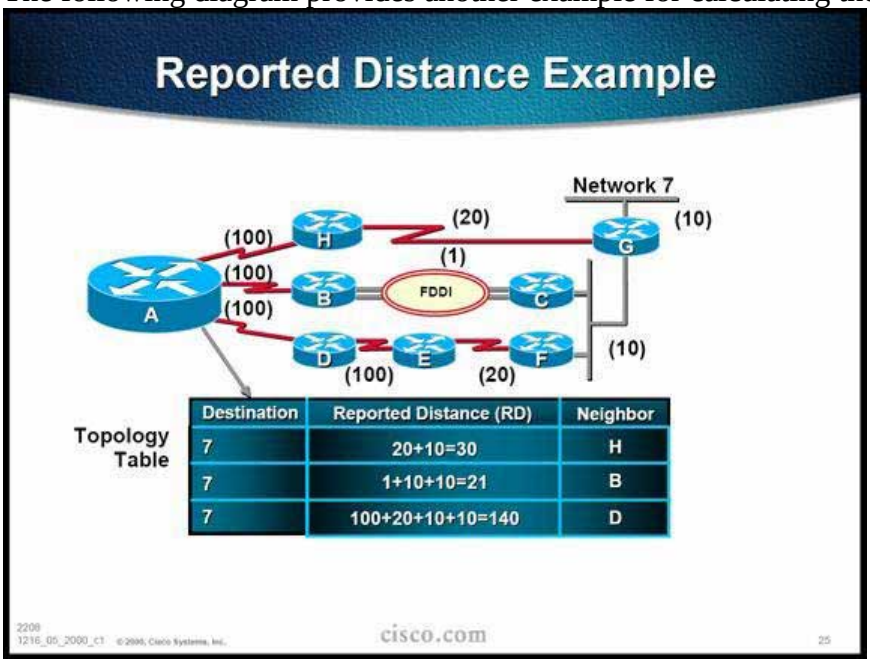
The associated EIGRP metric is listed as shown above for each of the links. Based on this information, what is the reported distance (advertised distance) to network 172.16.9.0/24 from router C to router A?

A. 5120
B. 6400

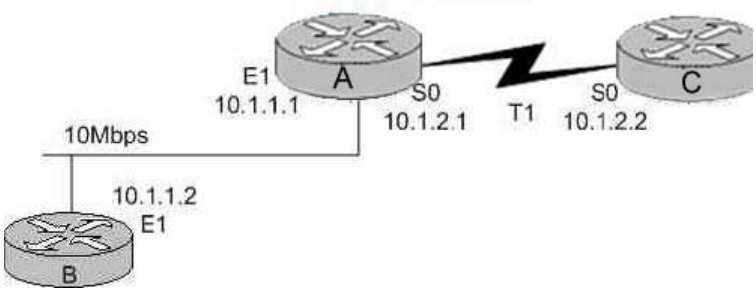
C. 17,920
D. 10,240
E. 11,520
F. 2560
G. None of the above

Answer: B

Explanation:
The following are some terms relating to EIGRP:
1. Feasible Distance: The lowest calculated metric to each destination
2. Feasibility Condition: A condition that is met if a neighbor's advertised distance to a destination is lower that the router's Feasible Distance to that same destination.
3. Successor: The neighbor that has been selected as the next hop for a given destination based on the Feasibility Condition.
4. Feasible Successor: A neighbor whose Reported Distance (RD) is less than the Feasible Distance (FD).
In the example above, the Feasible Distance to network 172.16.9.0/24 from C to A would be the distance that this network is from router C. In this case, the distance is 2560+3840=6400, so Choice B is correct.
The following diagram provides another example for calculating the RD:



QUESTION 221
The Certkiller EIGRP network is displayed in the exhibit below:



The "Show IP EIGRP neighbor" command is issued on the router
A. Router A is
configured with the default EIGRP settings. After issuing this command, which of the following answer choices correctly describe the expected output?

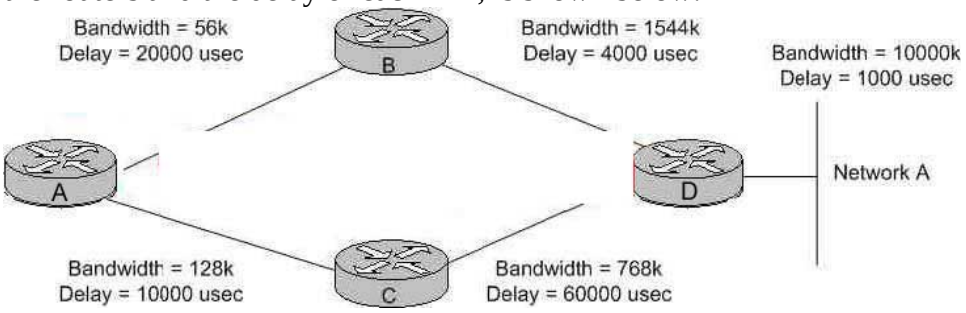
A. routerA#show ip eigrp neighbor
IP-EIGRP neighbors for process 1
H Address Interface Hold Uptime SRTT RTO Q Seq
(Sec) (ms) Cnt Num
1 10.1.1.2 Et1 13 12:00:53 12 300 0 620
0 10.1.2.2 S0 174 12:00:56 17 200 0 645
B. routerA#show ip eigrp neighbor
IP-EIGRP neighbors for process 1
H Address Interface Hold Uptime SRTT RTO Q Seq
(Sec) (ms) Cnt Num
1 10.1.1.2 Et1 20 12:00:53 12 300 0 620
0 10.1.2.2 S0 190 12:00:56 17 200 0 645
C. routerA#show ip eigrp neighbor
IP-EIGRP neighbors for process 1
H Address Interface Hold Uptime SRTT RTO Q Seq
(Sec) (ms) Cnt Num
1 10.1.1.2 Et1 174 12:00:53 12 300 0 620
0 10.1.2.2 S0 13 12:00:56 17 200 0 645
D. routerA#show ip eigrp neighbor
IP-EIGRP neighbors for process 1
H Address Interface Hold Uptime SRTT RTO Q Seq
(Sec) (ms) Cnt Num
1 10.1.1.2 Et1 185 12:00:53 12 300 0 620
0 10.1.2.2 S0 19 12:00:56 17 200 0 645

Answer: A

Explanation:
The value in the Hold column of the command output should never exceed the hold time, and should never be less than the hold time minus the hello interval (unless, of course, you are losing hello packets). If the Hold column usually ranges between 10 and 15 seconds, the hello interval is 5 seconds and the hold time is 15 seconds. If the Hold column usually has a wider range - between 120 and 180 seconds - the hello interval is 60 seconds and the hold time is 180 seconds.

The EIGRP default timer settings are:
Hello Interval: 5 seconds for all high speed links
60 seconds for low speed links (T1 or less)
The default hold timer is less 3 times the hello interval. Since this question tells us that the default values are used, the Router A would have a value of not more than 15 seconds for the Ethernet peer and 180 seconds for the serial peer, so choice A is correct.
Incorrect Answers:
B, D. The timers for both the Ethernet and serial peers are above the maximum theoretical values for a working EIGRP network, assuming that the default timers are being used.
C. The timer values in this choice is wrong. High speed links such as ethernet use a shorter hello interval than low speed T1 links.

QUESTION 222
The Certkiller EIGRP network, along with the configured bandwidth statements of the routers and the delay of each link, is shown below:



Assuming that all EIGRP routers are all using default configurations, what path would router A choose to route packets to network A?

A. Router A takes the path through router B.
B. Router A takes the path through router C.
C. Router A would load balance to both router B and router C.
D. Neither path would be chosen as there is a loop in the network.
E. The metrics shown are too large, and the route to network A would be considered unreachable.

Answer: B

Explanation:
When all 5 of the K values are set to the default values, the EIGRP metric calculation for each link is found by the default formula of (Bandwidth + Delay) x 256. The metric calculation is the same as IGRP, but the result is multiplied by 256 for finer granularity. In this case, the bandwidth component is found in the same was as the OSPF metric, which is 10,000,000/bandwidth. It is important to note that only the minimum outgoing bandwidth is used, so along any path from A to Z, the slowest link among all the hops is used as the chosen metric for the bandwidth portion. This is true for both IGRP and EIGRP (See Routing TCP/IP by Jeff Doyle, page 243-244). The delay metric is found by adding the total delay of the path (in microseconds) and dividing by 10.

For this question, the shortest path can be found by comparing the two different choices that we really have (through router B or router C). For the path through router B the bandwidth metric is:
(10 million/56) + (24000/10) x 256 = (178571 + 2400) x 256 = 46328683.
For the path going through router C:
(10 million/128) + (70000/10) x 256 = (78125 + 7000) x 256 = 21792000.
Note that only the lowest bandwidth metric was used along the entire path, where as the delay was added at each hop. Also note that the calculation for the path from router D to network A was omitted, since this value would be simply added to the metrics above would not change the answer.
Incorrect Answers:

A. The path through this router has a higher metric and so would not be used.
C. By default, EIGRP would load balance over equal cost paths. Although these paths are not equally valued, load balancing could occur despite this if the "variance" EIGRP feature was used. However, the variance command is not enabled by default.
D. Although a loop does exist, EIGRP routers maintain loop avoidance techniques, including keeping track of hop counts used. For IGRP and EIGRP, there is a maximum hop count of 100 hops.
E. Both of the metric listed above are well within the maximum limits set by EIGRP.

QUESTION 223
The Certkiller network is using EIGRP as the routing protocol, and the EIGRP topology information for router R4 is displayed below:

```
R4#sh ip eigrp top
IP-EIGRP Topology Table for AS(10)/ID(140.140.3.1)

Codes: P - Passive  A- Active, U  Update, Q - Qurry, R - Reply,
       r - reply Status, s - sia status

P 140.140.0.0/16, 1 successors, FD is 128256
        via Summary (128256/0), Null0
P 170.170.0.0/16, 1 successors, FD is 2809856
        via 116.16.34.3 (2809856/2297856), Serial1/0
P 190.190.0.0/16, 1 successors, FD is 2297856
        via 116.16.34.9 (2297856/128256), Serial1/0
P 130.130.0.0/16, 1 successors, FD is 2297856
        via 116.16.34.3 (2297856/128256), Serial1/0
P 140.140.1.0/24, 1 successors, FD is 128256
        via Connected, Loopback1
P 116.16.37.0/30, 1 successors, FD is 2681856
        via 116.16.34.3 (2681856/2169856), Serial1/0
P 116.16.34.0/23  1 successors, FD is 2169856
        via Connected, Serial1/0
P 116.0.0.0/8, 1 successors, FD is 2169856
        via Summary (2169856/0), Null0
```

Based on the information above, which of the following statements is true?

A. The routers 116.16.34.3 and 116.16.34.9 are EIGRP neighbors to CK4 .
B. The 116.16.37.0 network is reachable via the 116.16.34.9 interface.
C. A static route has been configured to summarize the 140.0.0.0 network and route it to the NULL 0 interface.
D. Interface serial 1/0 is most likely a frame relay interface with four DLCIs: one to the 170.170.0.0 network, one to the 130.130.0.0 network and one to the 116.16.37.0 network.
E. All of the above

Answer: A

Explanation:
The IP address following the "via" entry is the peer that told the software about this destination. When issuing this command, the first n of these entries, where N is the number of successors, are the current successors. The remaining entries on the list are feasible successors. In the example above, the router CK4 is learning routes from both of these two peers, so they are EIGRP neighbors to CK4 .
Incorrect Answers:
B. This network is reachable via the 116.16.34.3 neighbor, not 116.16.34.2.
C. The routing entry for the 140.0.0.0/8 network is known via the summary, not a static route. EIGRP uses auto-summarization by default, which has produced this route.
D. All three of these networks are known via the same IP peer. Although it is possible that 4 separate PVC's are built to the same IP address peer, there is no reason to assume that this is the case in this example. It actually looks like there may be 3 total DLCIs on this serial interface, not 4.

QUESTION 224
The CertK WAN is displayed in the diagram below, along with the partial configuration files of routers CK1 and CK2 :


```
hostname CK1
!
interface Ethernet0/0
 ip address 172.16.1.10 255.255.255.0
!
interface Serial6/0
 ip address 192.168.1.5 255.255.255.252
!
router eigrp 10
 network 172.16.0.0
 network 192.168.1.0
```

```
hostname CK2
!
interface Ethernet0/0
 ip address 172.17.1.10 255.255.255.0
!
interface Serial6/0
 ip address 192.168.1.16 255.255.255.252
!
router eigrp 11
 network 172.17.0.0
 network 192.168.1.0
```

Based on the above information, what would be the most likely reason that the routing tables do not contain routes for each of the remote networks?

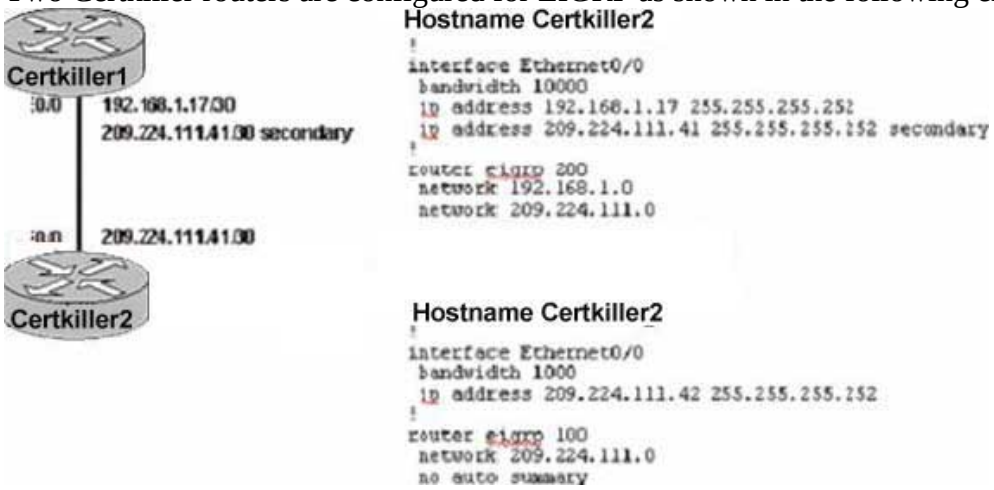
A. The routers interfaces are not functioning properly.
B. IP routing is not enabled on the routers.
C. The routers are not members of the same autonomous system.

D. The routers only pass locally significant routing information.
E. The routers are using different routing protocols.
F. Auto-summarization is not disabled on the routers.

Answer: C

Explanation:
The number following the "router eigrp" command is known as the process ID, and is used to denote the Autonomous System of the network that the router is in. The process ID can be any number between 1 and 65535 (0 is not allowed) and it can be randomly chosen, as long as it is the same for all EIGRP processes in routers that are to share the routing information. In the example above, router CK1 is configured to use EIGRP process 10, while router CK2 is using EIGRP process 11
Reference: Jeff Doyle, "Routing TCP/IP volume 1" page 377.

QUESTION 225
Two Certkiller routers are configured for EIGRP as shown in the following exhibit:



Router Certkiller 1 and router Certkiller 2 are unable to form an EIGRP neighbor relationship. What are two reasons for this problem? (Select two).

A. The bandwidth settings on the interfaces do not match.
B. The routers belong to different autonomous systems.
C. EIGRP can not form a neighbor relationship using secondary addresses.
D. The network statement under router EIGRP does not match the subnetted network configured on the Ethernet interface.
E. Auto summarization has not been correctly configured on router Certkiller 1.

Answer: B, C

Explanation:
EIGRP, unlike OSPF, checks for the Autonomous System number on neighboring routers before becoming neighbors. EIGRP will only form a neighbor relationship with other routers in the same AS.
Since EIGRP always sources data packets from the primary address, Cisco recommends

that you configure all routers on a particular subnet with primary addresses that belong to the same subnet. Routers do not form EIGRP neighbors over secondary networks. Therefore, if all routers' primary IP addresses do not agree, problems can arise with neighbor adjacencies.
Incorrect Answers:

A. Manually setting the bandwidth will affect the overall metric of the individual EIGRP routes, but will not affect the state of the neighbor relationship.
D. Although they do not match, EIGRP will still work as long as the EIGRP interface is included within the subnet mask used for the EIGRP process.
E. In EIGRP, automatic summarization is on by default. Whether this is enabled or disabled will have no effect on the neighbor relationship.

QUESTION 226
Certkiller .com is designing a large network with core, distribution, and access layers. EIGRP is the routing protocol that will be used throughout the network. Each distribution router has WAN connectivity to at least 20 access routers. Every router in the network has an explicit route to every possible subnet. All hosts in the network should be able to reach any other host, anywhere within the network. What should be done to optimize the routing configuration?

A. Ensure IP address space is allocated so that routes can be summarized at the core routers.
B. Filter routes in the distribution layer so that every access router doesn't have an explicit route to every subnet.
C. Filter routes in the access layer so that every access router doesn't have an explicit route to every subnet.
D. Ensure IP address space is allocated so that routes can be summarized at each distribution router.

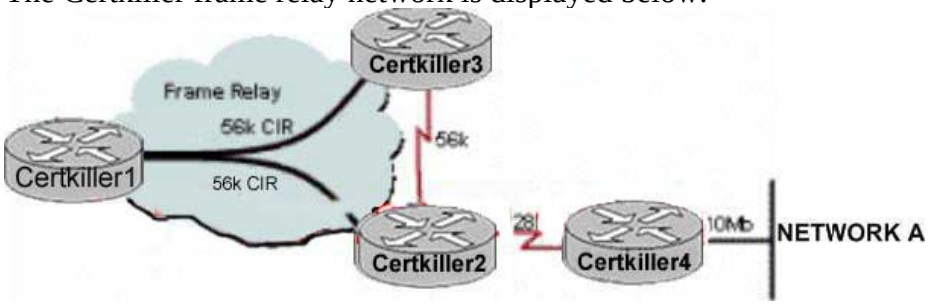
Answer: D

Explanation:
The best way to reduce the number of routes within the routing table is via route summarization. In order to optimize the network using this approach, summarization should take place on the distribution layer of a three tiered network design. When doing this, it is important to ensure that proper planning takes place to ensure that enough IP address space is allocated at each distribution router, in order to summarize all of the remote locations into one single network route.
Incorrect Answers:

A. Core routers should focus solely on routing data packets as quickly as possible. The use of any ancillary technologies such as access lists, packet classification, and route filtering. These technologies are best suited to be placed on the distribution layer network devices.

B, C: Either of these choices could result in some hosts becoming unreachable from other hosts within the Certkiller network.

QUESTION 227
The Certkiller frame relay network is displayed below:



Assume that no subinterfaces are used on router Certkiller 1 and EIGRP is the routing protocol in use. What is the effect on routing updates if router Certkiller 1 learns about network A from router Certkiller 2, assuming default configurations are being used?

A. Router Certkiller 1 will advertise the route to network A to router Certkiller 3.
B. Router Certkiller 1 will advertise the route to network A to router Certkiller 2 and Certkiller 3.
C. Router Certkiller 1 will load balance between router Certkiller 2 and router Certkiller 3.
D. Router Certkiller 1 will not advertise the route to network A to router Certkiller 3.

Answer: D

Explanation:
Split horizon controls the sending of IP Enhanced IGRP update and query packets. When split horizon is enabled on an interface, these packets are not sent for destinations for which this interface is the next hop. This reduces the possibility of routing loops.
By default, split horizon is enabled on all interfaces.
Split horizon blocks route information from being advertised by a router out of any interface from which that information originated. This behavior usually optimizes communications among multiple routing devices, particularly when links are broken. However, with nonbroadcast networks (such as Frame Relay and SMDS), situations can arise for which this behavior is less than ideal. In the example above, when router Certkiller 1 sees the route advertisement from Certkiller 2, it will not advertise this route out the same interface, which is also the connection to Certkiller 3. If we were to use sub-interfaces or disable split horizons on Certkiller 1, then it would indeed advertise the route.
Incorrect Answers:
A, B: The Split Horizon rule, which is enabled by default, prevents this.
C: Certkiller 1 will only load balance over equal cost routes by default. In this case, Certkiller 2 will always be used to reach network A since the route via Certkiller 3 will be seen with a higher metric.
Note: We could configure Certkiller 1 to load balance in this situation, using the "variance" router process configuration command.

QUESTION 228
A router is being configured to override the normal routed behavior of certain traffic types. To do this, Policy Based Routing is used. Which of the following statements is FALSE with regards to the application of policy based routing (PBR)?

A. PBR can not be used to set the IP precedence.
B. PBR can not set the DSCP in one statement.
C. PBR can be used to set the next hop IP address.
D. PBR can be used to match on the length of a packet.
E. All of the above are true

Answer: A

Explanation:
PBR gives you a flexible means of routing packets by allowing you to configure a defined policy for traffic flows, lessening reliance on routes derived from routing protocols. To this end, PBR gives you more control over routing by extending and complementing the existing mechanisms provided by routing protocols. PBR allows you to set the IP precedence. It also allows you to specify a path for certain traffic, such as priority traffic over a high-cost link.
You can set up PBR as a way to route packets based on configured policies. For example, you can implement routing policies to allow or deny paths based on the identity of a particular end system, an application protocol, or the size of packets.
PBR allows you to perform the following tasks:
1. Classify traffic based on extended access list criteria. Access lists, then, establish the match criteria.
2. Set IP Precedence bits, giving the network the ability to enable differentiated classes of service.
3. Route packets to specific traffic-engineered paths; you might need to route them to allow a specific QoS through the network.
Policies can be based on IP address, port numbers, protocols, or size of packets. For a simple policy, you can use any one of these descriptors; for a complicated policy, you can use all of them.

QUESTION 229
The router CK1 is being configured to filter BGP routes. In a BGP peering relationship with a customer where routing information is exchanged, which prefix list filter(s) will ensure that only class-B address space networks are accepted by the router?

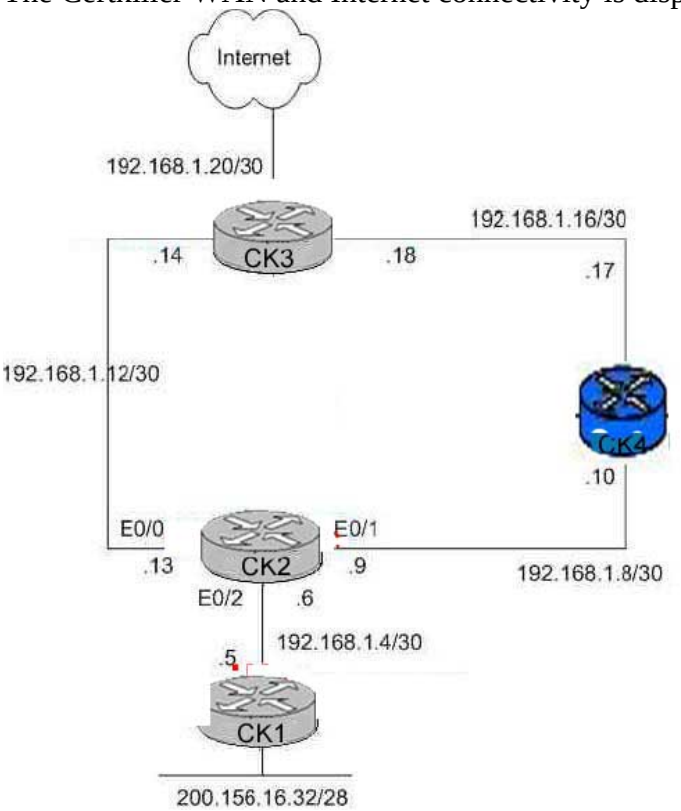
A. ip prefix-list list-A permit 191.0.0.0/3 le 16
B. ip prefix-list list-B permit 0.0.0.0/0 ge 16 le 24
C. ip prefix-list list-C permit 128.0.0.0/2 ge 17
D. ip prefix-list list-D permit 0.0.0.0/0 ge 16
ip prefix-list list-D permit 0.0.0.0/0 le 23
E. ip prefix-list list-E permit 128.0.0.0/1 ge 16
ip prefix-list list-E permit 191.0.0.0/3 le 23

Answer: E

Explanation:
In a prefix list configuration, the "ge" keyword means greater than or equal to, while the "le" keyword means less than or equal to. Choice E correctly describes the two statements that are needed. The first line specifies that any route larger that 128.0.0.0/1 with a prefix range greater than or equal to 16 will match the filter. The second line specifies that any route less than 191.0.0.0/3 with a network mask of less than or equal to 23 will also be match. Therefore, only addresses that fall in the class B range will pass through the filter.
Incorrect Answers:

A. This will allow all class A and B networks to pass through.
B. This will permit address space from 16 to 24 bits in length from all network class ranges from passing through the filter.
C. This will allow all 128.0.0.2 prefixes with network masks greater than or equal to 17 bits in length. It is not restrictive enough to allow only class B networks.
D. This will allow all routes (from every network class) with network masks of between 16 and 23 bits in length.

QUESTION 230
The Certkiller WAN and Internet connectivity is displayed below:



Router CK2 is configured as follows:
hostname CK2
!

```
interface Ethernet0/0
ip address 192.168.1.13 255.255.255.252
!
interface Ethernet0/1
ip address 192.168.1.9 255.255.255.252
!
interface Ethernet0/2
ip address 192.168.1.6 255.255.255.252
ip policy route-map net-200
!
router eigrp 1
network 192.168.1.0
!
access-list 101 permit ip 200.155.16.32 0.0.0.15 any
!
route-map net-200 permit 10
match ip address 101
set interface Ethernet0/1
!
route-map net-10 permit 20
!
end
```

It is desired that all traffic from network 200.155.16.32/28 be sent to the internal through the firewall-enabled router CK4 . Router CK2 has been configured for policy-based routing as shown on the exhibit above. The policy-based configuration is not working. Debug and show commands indicate that Router CK2 has an "Incomplete" ARP entry for network 192.168.1.20. What is the best method to resolve this issue?

A. Configure a static route to the 192.168.1.20 network in router CK2
B. Configure ip proxy-arp on the router's Ethernet 0/1 and 0/2 interface
C. Configure a static ARP entry for the 192.168.1.20 network on router CK2
D. Reconfigure the "set interface" command to "set ip next-hop" with the IP address of the firewall
E. Open the TCP ports on the firewall that are currently blocking ARP requests form router CK2

Answer: D

Explanation:
When configuring policy based routing on a multi-access network such as an Ethernet LAN, issues can arise when the interface is used as the next hop, rather than specifying the IP address. In this specific example, if we issue the "show arp" command we will see something similar to the following:
Cisco_Wan_Router# show arp
Protocol Address Age (min) Hardware Addr Type Interface

Internet 192.168.1.9 - 00b0.64cb.eab1 ARPA Ethernet0/1
Internet 192.168.1.10 3 0010.7b81.0b19 ARPA Ethernet0/1
Internet 192.168.1.20 0 Incomplete ARPA
Router CK2 attempts to do what it was instructed and tries to put the packets directly onto the Ethernet 0/1 interface. This requires that the router send an Address Resolution Protocol (ARP) request for the destination address of 192.1.1.1, which the router realizes is not on this interface, and hence the ARP entry for this address is "Incomplete," as seen by the show arp command. An encapsulation failure then occurs as the router is unable to put the packet on the wire with no ARP entry.
By specifying the IP address of the firewall as the next-hop, we can prevent this problem and make the route-map work as intended.
Configuration change should be:
!
route-map net-200 permit 10
match ip address 101
set ip next-hop 192.168.1.10
!
Reference:
http://www.cisco.com/en/US/partner/tech/ CK3
65/technologies_tech_note09186a008009481d.shtml#configforfire

---

QUESTION 231
Part of the configuration for router CK1 is displayed in the diagram below:

```
Hostname Certkiller1
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip local policy route-map
!
ip local policy route-map reroute
ip classless
!
ip access-list extended reroute-acl
 permit tcp any 172.16.1.0 0.0.0.255 eq telnet
!
route-map mark-em-up permit 10
 match ip address reroute-acl
 set ip precedence flash
 set ip next-hop 192.168.1.20
!
route-map reroute permit 10
 match ip address reroute-acl
 set ip next-hop 192.168.1.25
```

Policy-Based routing has been configured on CK1 to sort traffic according to an administrative policy.
Which is the result from applying this configuration to Certkiller 1? (Select all that apply)

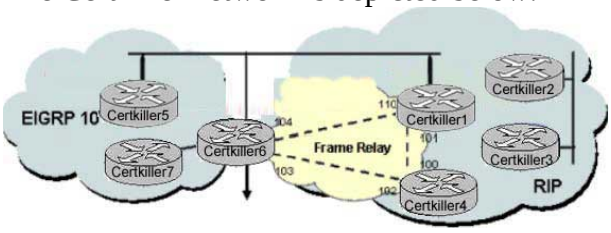
A. All Telnet traffic destined to hosts on the 172.16.1.0/24 network will be forwarded to 192.168.1.20.

B. All telnet traffic will be marked with IP Precedence Flash.
C. Telnet traffic to destinations on the 172.16.1.0/24 network initiated from console connections on the router will be policy-routed to 192.168.1.25.
D. Any telnet traffic transiting this router and exiting interface Ethernet 0/0 will be policy-routed to 192.168.1.20.
E. If an administrator Telnets to Certkiller 1 and then subsequently telnets to 172.168.1.55, the session will be directed to 192.168.1.25

Answer: A, E

Explanation:
Choice A correctly describes the function of the normal policy based routing part of the configuration. In addtition to this, a local policy route map has been configured. By default, packets that are originated from the router are not policy routed, unless a local policy route map is configured as shown in this example. Because this has been applied to router Certkiller 1, telnet traffic originated from the router as described in choice E will be policy routed to the next hop IP address of 192.168.1.25.
Incorrect Answers:
B. Only telnet traffic destined to the 172.16.1.0/24 subnet will be marked with the flash IP precedence value.
C. Only packets that originate from the router are policy routed according to the local policy. This does not apply to connections that orignate from the console interface.
D. Again, only telnet traffic that matches the reroute-acl access list will be policy routed, not all telnet traffic.

QUESTION 232
The Certkiller network is depicted below:



Router Certkiller 6 is configured as shown below:

```
router rip
  version 2
  redistribute eigrp 10
  passive-interface default
  no passive-interface serial0/0.103
  network 10.0.0.0
  Default-metric
  no auto-summary
router eigrp 10
  redistribute rip
  passive-interface default
  no passive-interface fastethernet0/0
  no passive-interface fastethernet0/1
  network 10.0.0.0
  default-metric 10000 0 255 1 1500
  no auto-summary
!
access-list 1 deny 10.5.x.3
access-list 1 deny 10.5.x.3 0.0.0.3
access-list 1 deny 10.7.7.0 0.0.0.15
access-list 1 deny 10.50.50.0 0.0.0.7
access-list 1 permit any
```

You are required to configure redistrubition of IGP protocols to ensure full IP visability between all routers. As a safety precaution you must ensure that Certkiller 6 can not learn EIGRP routes it previously advertised into the RIP domain back from Certkiller 4.
What should you do in this scenario?

A. Apply a distribute-list command to the FastEthernet and serial interfaces
B. Apply a distribute-list command to the router rip area with the serial 0/0.103 interface only
C. Apply a distribute-list command to the router EIGRP area with the serial interfaces
D. Apply a route-map to the FastEthernet interfaces
E. Apply a route-map and distribute-list command to complete the configuration

Answer: B

Explanation:
In order to prevent the EIGRP subnet routes from being advertised back to router Certkiller 6, we need to apply a distribute list command to the RIP routing process. The distribute list command should specify the routes that were configured in access-list 1. This will prevent the EIGRP subnets from being advertised back in via RIP. Since interface serial 0/0.103 is used as the connection to router Certkiller 4, the distribute list should be applied to this interface only. The other serial link to router Certkiller 1 does not need to be included, since this interface is specified as passive, by the "passive-interface default" configuration line.
Incorrect Answers:
A: Applying a distribute list to the fast Ethernet interfaces would result in lost connectivity between the EIGRP routers.
C: The distribute list needs to be applied to the RIP routing process, not the EIGRP

process since you want to filter the incoming networks from the RIP network on the frame relay network.
D, E: It is not necessary to use route-maps for simply filtering network subnets.

QUESTION 233
Routers CK1 and CK2 are in the same LAN, and both are running RIP version 2. During a troubleshooting session you place a sniffer on the LAN network. Using the sniffer you see routers CK1 and CK2 sending routing updates to each other every 30 seconds. Which IP address should you expect to see these updates destined to? (Choose all that apply)

A. 224.0.0.10
B. 255.255.255.255
C. 224.0.0.13
D. 224.0.0.5
E. 224.0.0.9
F. 224.0.0.6

Answer: E

Explanation:
RIPV2 sends periodic route updates sent every 30 seconds to multicast address 224.0.0.9.
Incorrect Answers:

A. 224.0.0.10 is used by EIGRP
D, F. These are the multicast addresses used by OSPF
Reference:
CCIE Routing and Switching Exam Certification Guide Page 338

QUESTION 234
What is the destination IP address of routing update packets used by RIPv2?
What would your reply be?

A. 224.0.0.1
B. 224.0.0.10
C. 224.0.0.5
D. 224.0.0.9
E. 255.255.255.255

Answer: D

Explanation:
224.0.0.9 is the RIP v2s multicast address.
Incorrect Answers:

A. This is the multicast address destined for all hosts on the subnet.
B. This is the multicast address used by EIGRP.

C. This address is used by OSPF.
E. This is the all hosts broadcast address.

QUESTION 235
The router CK1 is using RIPv2 as the routing protocol, and the partial configuration file is displayed below:
interface Ethernet 1
ip address 10.1.1.1 255.255.255.0
ip summary-address rip 10.2.0.0 255.255.0.0
ip split-horizon
!
router rip
network 10.0.0.0
What is a result of the configuration shown for router CK1 ?

A. The 10.2.0.0 network overrides the auto summary address of 10.1.1.1.
B. The 10.2.0.0 network is advertised out interface E1, and the auto summary address is not advertised.
C. The auto summary address of 10.1.1.1.1 will be advertised out interface E1 and the interface summary-address is not advertised.
D. Neither the auto summary address nor the interface summary-address is advertised because split horizon is enabled.
E. Both the auto summary address and the interface summary-address are advertised out of interface E1.

Answer: D

Explanation:
If split horizon is enabled, neither auto-summary nor interface summary addresses (those configured with the ip summary-address rip command) are advertised. The split horizon mechanism blocks information about routes from being advertised by a router out of any interface from which that information originated. It is enabled on all interfaces by default.
Reference:
http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1830/products_feature_guide09186a0080087ad1.ht

---

QUESTION 236
A customer has a frame-relay network with 2 sites - a headquarters site and a remote site - with a single PVC connecting the 2 sites. The network is running RIP version II. The company is now expanding and adding another remote site in the frame relay network and has ordered a second PVC between the new remote site and the headquarters site. All frame-relay interface IP addresses are in a single subnet. The customer configured frame-relay DLCI mappings and can successfully ping from the new remote to the headquarters site as well as the other remote site. However, the new router does not have a route in its route table to the other remote

site's LAN, and cannot ping the LAN interface or any hosts on that LAN. What is most likely causing the problem?

A. Neighbor statements are not configured on the two remote sites, pointing to all other sites.
B. The headquarters site router has split-horizon enabled on the frame-relay interface.
C. The frame-relay IP to DLCI mappings are incorrectly configured.
D. RIP cannot propagate routing updates over a partial mesh frame-relay configuration, so another routing protocol should be selected.
E. Triggered updates should be configured on the headquarters router, to directly forward routing updates between the two remote sites.

Answer: B

Explanation:
RIP version 2 is a distance vector routing protocols, and by default all distance vector routing protocols utilize the split horizon rule to avoid routing loops. The split horizon rule blocks routing updates to be sent over the same interface that the route was learned from. In this case, the routes from the remote frame relay sites will not be sent to the other remote locations. In a hub and spoke topology such as this, the only way to ensure full connectivity between all locations using RIPv2 is to use sub-interfaces, or to disable the use of split horizons on the physical serial interface.

QUESTION 237
A RIP Version 2 router is sending RIP updates to its neighbor that include several contiguous IP subnet routes in the 10.1.1.0/24 space. What command should be configured to aggregate the routes into a single route in the update to the RIP neighbor?

A. summary-address rip 10.1.1.0 255.255.255.0, configured under the RIP process or the interface
B. summary-address 10.1.1.0 255.255.255.0, configured under the RIP process
C. ip summary-address rip 10.1.1.0 255.255.255.0, configured under the interface
D. rip summary-address 10.1.1.0 255.255.255.0, configured under the interface
E. ip rip summary-address 10.1.1.0 255.255.255.0, configured under the interface
F. None of the above

Answer: C

Explanation:
The "ip summary-address rip" command causes the router to summarize a given set of routes learned via RIP version 2 or redistributed into RIP version 2. Host routes are especially applicable for summarization. To configure IP summary addressing, use the following commands in global configuration mode:

	Command	Purpose

Step1	`Router(config)#`interface ethernet1	Enters interface configuration mode.
Step2	`Router(config-if)#`ip summary-address rip`ip_address``ip_network_mask`	Specifies the IP address and network mask that identify the routes to be summarized.

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d

---

QUESTION 238
What is the default seed metric for routes redistributed into RIPv2?

A. 1
B. 15
C. 16
D. 120
E. Infinity

Answer: A

Explanation:
When routes are redistributed into RIP, the default metric applied to the route is 1. Because RIP (both version 1 and version 2) uses hop count as the metric, the routes will be viewed as being 1 hop away.
Note: When connected routes are redistributed into RIP, the default seed metric is 0.
Incorrect Answers:
B, C. Since RIP considers a route with a hop count of 16 as unreachable (infinity) using these values as the default metric will make all routes unreachable when advertised to RIP peer routers.
D. This is the default AD of RIP.
E. This would make all routes unreachable. Note that choices C and E are effectively the same answer.

QUESTION 239
Router CK1 is running RIP Version II and has 2 interfaces. CK1 has received RIP routing updates from its neighbors on both interfaces. The first interface receives a routing update for network 10.1.1.0/24 with a metric of 3 while the second interface also receives a routing update for network 10.1.1.0/24 with a metric of 5. Which interface(s) will router CK1 select to forward packets to network 10.1.1.0/24?

A. The router will choose the first interface because it has the lowest metric.
B. The router will load share across both interfaces in a weighted fashion, sending the

first 3 packets out of the first interface, and the next 5 packets out of the second interface.
C. The router will choose the second interface because it has the highest metric.
D. The router will equally load share packets across both interfaces in a round robin fashion, because both are valid RIP Version II routes.
E. The router will ignore the RIP metrics and compare the administrative distance of each route, and choose the interface with the lowest administrative distance.

Answer: A

Explanation:
Although load sharing occurs when there are equal cost paths to a destination, it does not occur when the paths are not equal. Sometimes the router must select a route from among many learned via the same routing process with the same administrative distance. In this case, the router chooses the path with the lowest cost (or metric) to the destination. RIP version 2 uses hop count as the metric, like version 1. In this case, only the path with a metric of 3 will be chosen over the path with a metric of 5 hops.

QUESTION 240
The relevant configuration and ip route information on router CE11A is displayed below:

```
! CE11A Partial Running-Config
!
interface Serial2/0.101 point-to-point
 ip address 150.1.11.17 255.255.255.240
 ip summary-address rip 192.168.1.80 255.255.255.252
 frame-relay interface-dlci 101


 network 150.1.0.0
 network 192.168.1.0
 no auto-summary
!
! Output Omitted



CE11A#show ip route connected

     192.168.1.0/32 is subnetted, 5 subnets
C       192.168.1.81 is directly connected, Loopback2
C       192.168.1.80 is directly connected, Loopback1
C       192.168.1.83 is directly connected, Loopback3
C       192.168.1.82 is directly connected, Loopback6
C       192.168.1.84 is directly connected, Loopback4
     150.1.0.0/28 is subnetted, 2 subnets
C       150.1.11.16 is directly connected, Serial2/0.101
```

Based upon the partial configuration and the show ip route connected output shown in the exhibit, which RIPv2 updates will be sent out of the Serial2/0.101 sub interface from router CE11A? (Select all that apply)

A. 192.168.1.0/24
B. 192.168.1.80/30
C. 192.168.1.84/30

D. 192.168.1.80/32
E. 192.168.1.81/32
F. 192.168.1.82/32
G. 192.168.1.83/32
H. 192.168.1.84/32

Answer: B, H

Explanation:
By default, RIP version 2 summurizes networks automatically. In the configuration example above, automatic summarization has been disabled. However, the "IP summary address" configuration statement takes precedence over automatic network summary, so the individual host loopback addresses will be summarized into one 192.168.1.80/30 network route. This will summarize the 192.168.1.80, 192.168.1.81, 192.168.1.82, and 192.168.1.83 networks into one route, leaving only the 192.168.1.84 network. This single host route will then also be advertised, since the automatic summarization feature was disabled.

QUESTION 241
Part of the configuration file for router Certkiller 1 is displayed below:

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip summary-address rip 10.2.0.0 255.255.0.0
 Half Dulex
!
router rip
 network 10.0.0.0
```

You have configured RIPv2 summarization on Certkiller 1 interface Ethernet 0/0 but the routes are still not being summarized. Looking at the Certkiller 1 partial configuration above, what could be causing the problem?

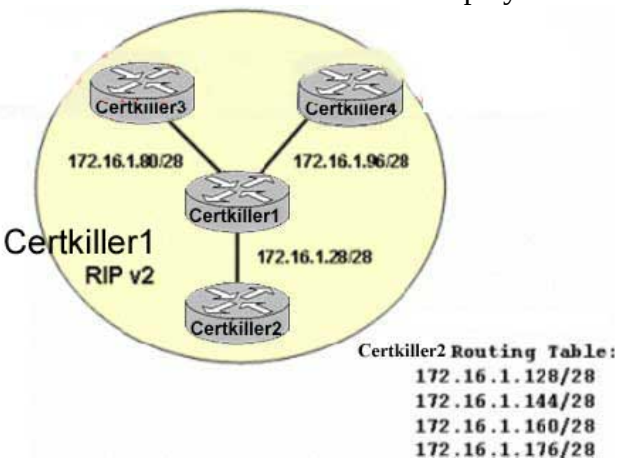
A. You need also to enable the auto summerazation under the RIP process.
B. You need also to disable the auto summerazation under the RIP process.
C. RIP does not support summarization on interface basis.
D. Split horizon is enabled on an interface basis.
E. The mask configured on the "ip summary-address" command must be /24 bits.

Answer: D

Explanation:
Cisco routers can summarize routes in two ways:
1.
Automatically, by summarizing subprefixes to the classful network boundary when crossing classful network boundaries (autosummary)
2. As specifically configured, advertising a summarized local IP address pool on the specified interface.
Autosummary will override the configured summary-address feature on a given interface

except when both of the following conditions are true:
1. The configured interface summary-address and the IP address of the configured interface share the same major network (the classful, nonsubnetted portion of the IP address).
2. Split horizon is not enabled on the interface.
Note: If split horizon is enabled, neither an autosummary address nor the interface summary-address is advertised.
In the following example configuration, the major network is 10.0.0.0. The 10 in the address defines a Class A address space, allowing space for 0.x.x.x unique hosts where x defines unique bit positions in the addresses for these hosts. The summary of the major net defines the prefix as implied by the class (A, B, or C) of the address, without any network mask. The summary address 10.2.0.0 overrides the autosummary address of 10.0.0.0, 10.2.0.0 is advertised out interface E1, and 10.0.0.0 is not advertised:
int Ethernet 0/0
ip address 10.1.1.1 255.255.255.0
ip summary-address rip 10.2.0.0 255.255.0.0
no ip split-horizon
router rip
network 10.0.0.0
The above configuration is what should have been configured on router Certkiller 1, by disabling split horizons.
Incorrect Answers:
A, B: By default, automatic summarization is already enabled. In this example, we need to disabled it. Automatic summarization is not the problem, however, since the manually configured summary address will override the automatically summarized address.
C: To configure IP summary addressing, use the "ip summary-address rip ip_address ip_network_mask" under the interface configuration:
E: The following subnet restrictions apply:
Supernet advertisement (advertising any network prefix less than its classful major network) is not allowed in RIP route summarization, other than advertising a supernet learned in the routing tables. Supernets learned on any interface that is subject to configuration are still learned. For example, the following summarization is invalid:
interface E1
..
ip summary-address rip 10.0.0.0 252.0.0.0 (invalid supernet summarization)
Each route summarization on an interface must have a unique major net, even if the subnet mask is unique. For example, the following is not permitted:
int E1
...
ip summary-address rip 10.1.0.0 255.255.0.0
ip summary-address rip 10.2.0.0 255.255.0.0 (or different mask)
However, the subnet mask used does not need to be a /24.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d

QUESTION 242
The Certkiller RIP version 2 network is displayed below:



Assuming that route summarization has been configured, which routes are displayed in Certkiller 1's routing table? (Select all that apply)

A. 172.l6.1.48/28
B. 172.l6.1.128/24
C. 172.l6.1.128/25
D. 172.l6.1.128/26
E. 172.l6.1.128/27

Answer: D

Explanation:
Summarizing routes in RIP Version 2 improves scalability and efficiency in large networks. Summarizing IP addresses means that there is no entry for child routes (routes that are created for any combination of the individual IP addresses contained within a summary address) in the RIP routing table, reducing the size of the table and allowing the router to handle more routes.
Summary IP address functions more efficiently than multiple individually advertised IP routes, because:
1. The summarized routes in the RIP database are processed first.
2. Any associated child routes that are included in a summarized route are skipped as RIP looks through the routing database, reducing the processing time required.
Cisco routers can summarize routes in two ways:
1. Automatically, by summarizing subprefixes to the classful network boundary when crossing classful network boundaries (autosummary)
2. specified interface, (on a network access server) so that the address pool can be provided to dialup clients
In our example, router Certkiller 2 could summarize the 4 network routes in the table into onr route, which is 172.16.1.128/26. Since the other 172.16.1.X subnets are coming from different sources, they can not be summarized.

QUESTION 243
To display the routing table of router CK1 , the "show ip route" command was issued. Router CK1 is running OSPF. Which one of the following statements is correct regarding the OSPF information in a routing table?

A. A routing designated with only an "O" represents either a type-1 or type-2 LSA.
B. A route that has been redistributed into OSPF can only be represented with either an "E1" or "E2" designation.
C. Routes that are within an area (intra-area) are marked with an "IA" in the routing table.
D. Type-7 LSAs display routes redistributed into OSPF from another process, and thus are shown with either an "E1" or "E2" marking.
E. All LSA types have unique designations in the IP routing table.

Answer: B

Explanation:
The following OSPF codes are used in the IP routing tables of OSPF routers:
O - OSPF
IA - OSPF inter area
N1 - OSPF NSSA external type 1
N2 - OSPF NSSA external type 2
E1 - OSPF external type 1
E2 - OSPF external type 2
When redistributing routes into OSPF, the routes are considered to be learned from an external means, so they will always display as external type 1 or external type 2 routes. These routes will appear as E1 or E2 in the routing table.
Incorrect Answers:

A. A route designated with an "O" only represents a generic OSPF learned route.
C. Routes displayed as "IA" are inter-area, not intra-area.
D. Type 7 routes are displayed as normal OSPF routes.
E. The designations in the routing table are not based on LSA types. They are based only on the type of OSPF route.

QUESTION 244
While troubleshooting an issue with a serial interface on the Certkiller 4 router, you issue the "show interface" command as shown below:

```
Certkiller4#sho int ser 0/1
Serial0/1 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 142.16.13.3/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  LMI eng sent  154467, LMI stat recvd 154468, LMI upd recvd 0, DTE LMI up
  LMI eng recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 0/0, interface broadcasts 0
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters 2w3d
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (actBW 1544 Kbit, DLY 20000 usec,
     Reserved Conversations 0/0, txload 1/255, rxload 1/255
     Available Bandwidth 1158 kAME-RELAY, loopback not set
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     259810 packets input, 33080103 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 4 throttles
     1 input errors, 0 CRC, 1 frame, 0 overrun, 0 ignored, 0 abort
     260370 packets output, 32082918 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     3 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Based on the information above, how many times has the interface been reset by the telco service provider?

A. 0
B. 1
C. 3
D. 4
E. 1023
F. None of the above

Answer: C

Explanation:
Carrier transitions appear in the output of the show interfaces serial exec command whenever there is an interruption in the carrier signal (such as an interface reset at the remote end of a link).
Incorrect Answers:
B. The output shows 1 interface reset, but Interface resets that appear in the output of the "show interfaces serial" exec command are the result of missed keepalive packets, and are not indicative of resets sent by the service provider.
Reference: "Troubleshooting Serial Lines"
http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1915.htm#xtocid7

QUESTION 245
The show ip bgp regexp [regexp] command is most useful when performing which

type of BGP troubleshooting?

A. To verify and troubleshoot BGP Prefix-list filtering configurations.
B. To verify and troubleshoot BGP AS-Path filtering configurations.
C. To verify and troubleshoot BGP route-maps configurations.
D. To verify and troubleshoot BGP synchronization problems.
E. To verify and troubleshoot BGP AS-path prepending configurations.

Answer: B

Explanation:
A regular expression is a pattern to match against an input string. You specify the pattern that a string must match when you compose a regular expression. Matching a string to the specified pattern is called "pattern matching." Pattern matching either succeeds or fails. You can use regular expressions in the ip as-path access-list command with Border Gateway Protocol (BGP) to filter AS path information. To display routes matching the autonomous system path regular expression, use the "show ip bgp regexp" command in EXEC mode.

QUESTION 246
You want traffic on your frame relay link to conform to specific policies. Because of this, you configure traffic shaping as follows:
Router configuration:
ip cef
class-map match-all gold
match ip dscp 10 12 14
class-map match-all bronze
match ip dscp 26 28 30
class-map match-all silver
match ip dscp 18 20 22
policy-map SHAPE
class gold
shape peak 512000
bandwidth percent 50
class bronze
shape average 384000
bandwidth percent 20
class silver
bandwidth percent 30
shape peak 448000
interface Serial4/0
encapsulation frame-relay
ip address 14.34.34.51 255.255.255.0
service-policy output SHAPE
end
You verify your configuration using the "show policy-map" command as shown below:

Router CertK #sh policy-map inter s4/0
Serial4/0
Service-policy output: SHAPE (1865)
Class-map: gold (match-all) (1866/2)
0 packets, 0 bytes
1 minute offered rate 0 bps, drop rate 0 bps
Match: ip dscp 10 12 15 (1868)
Traffic Shaping
Target Byte Sustain Excess Interval Increment Adapt
Rate Limit bits/int bits/int (ms) (bytes) (active)
1024000 3200 12800 12800 25 3299 -
Queue Packets Bytes Packets Bytes
Depth Delayed Delayed Active
0 0 0 0 no
Weighted Fair Queueing
Output Queue: Conversation 265
Bandwidth 50% Max Threshold 64 (packets)
(pkts matched/bytes matched) 0/0
(pkts discards/bytes discards/tail drops) 0/0/0
Based on this information, what is the CIR value for all the traffic marked with DSCP values 10?

A. 128000
B. 256000
C. 512000
D. 1024000
E. Cannot be determined

Answer: D

Explanation:
In shape peak you should use the formula:
Peak Rate = AvgRate * (1+Be/Bc)
That will be 1024000 for the config 512000
Not C: 512000 is alright if it was shape average.

QUESTION 247
What are the primary reasons to implement traffic shaping on a network? (Choose all that apply).

A. To regulate and thus control the average queue size by indicating when transmission of packets should be halted temporarily.
B. To control access to available bandwidth on the network.
C. To define Layer 3 aggregate or granular bandwidth rate limits.
D. To control the maximum rate of traffic on an interface.
E. To ensure that traffic conforms to the policies established for it.

F. To prevent denial of service attacks.
G. To drop high levels of unwanted traffic.

Answer: B, E

Explanation:
According to Cisco, the primary reasons to use traffic shaping are to control access to available bandwidth, to ensure that traffic conforms to specific policies, and to regulate the flow of traffic in order to avoid congestion.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4224/sw_confg/traffic.htm

---

QUESTION 248
You have set up priority queuing on the serial interface of your router as follows:
priority-list 1 protocol ip high list 101
priority-list 1 protocol ip medium list 102
priority-list 1 protocol ip normal list 103
priority-list 1 protocol ip low list 104
priority-list 1 default low
access-list 101 permit ip any any precedence critical
access-list 102 permit ip any any precedence flash
access-list 103 permit ip any any precedence priority
access-list 104 permit ip any any precedence network
A packet reaches the router with an IP Precedence value of 4. What priority will this packet be assigned by the router?

A. Low
B. Normal
C. Medium
D. High
E. Critical
F. Flash

Answer: A

Explanation:
The IP precedence values are shown below:
0 : routine
1 : priority
2 : immediate
3 : flash
4 : flash Override
5 : critical
6 : internet
7 : network
In this example, IP precedence 4 (flash override) was not explicitly defined in the priority

list, so it will be handled by the default queue. In this case, the default queue is given a priority of low.

QUESTION 249
A Certkiller router's interface is configured for traffic shaping as follows:
interface Serial1.1 point-to-point
ip address 10.16.1.1 255.255.255.252
frame-relay class Certkiller
frame-relay interface-dlci 220
!!
map-class frame-relay Certkiller
frame-relay cir 128000
frame-relay bc 8000
frame-relay be 8000
no frame-relay adaptive-shaping
In what are the bc and be parameters measured in the above configuration?

A. Bits per millisecond.
B. Bits per interval.
C. Bytes per interval.
D. Bytes per second.
E. Bits per second.
F. Bytes per millisecond.

Answer: B

Explanation:
The Sustain (bc) and excess (be) are configured bit per interval.
The following is sample output of the show traffic-shape command:
Target Rate = CIR = 100000 bits/s
Mincir = CIR/2 = 100000/2 = 50000 bits/s
Sustain = Bc = 8000 bits/int
Excess = Be = 8000 bits/int
Interval = Bc/CIR = 8000/100000 = 80 ms
Increment = Bc/8 = 8000/8 = 1000 bytes
Byte Limit = Increment + Be/8 = 1000 + 8000/8 = 2000 bytes
Reference:
http://www.cisco.com/warp/public/125/framerelay_ts_cmd.html

QUESTION 250
Consider the following scenario: An interface has been configured for custom queuing across a DS3 interface. Bandwidth has been allocated for three application flows: A, B and C. The average packet for each application is as follows:
Application A= 2000
Application B= 1000
Application C= 500

You wish to configure the router to allow for 20% of the bandwidth to be allocated to flow A, 50% for flow B, and the remaining 30% for flow C. If only one packet is serviced for flow A per pass, how many packets need to be allowed on flow C to maintain the 20:50:30 ratio?

A. 3
B. 4
C. 5
D. 6
E. 500
F. More information needed

Answer: D

Explanation:
If flow A uses 20% of the bandwidth and flow C uses 30%, then C uses 1.5 times the bandwidth as
A. The average byte size of A is 2000 bytes. 2000 times 1.5 is 3500 bytes.
That would give the bandwidth of 3000 bytes for flow C. Since the average packet size of C is 500 bytes, 3000/500 = 6.

QUESTION 251
Your VOIP network needs to give priority to the VOIP traffic across the serial interface of a router. You wish to support this by implementing a solution that enables the router to service the Voice traffic in a strict priority queue. All other non-voice traffic should be serviced using the weighted fair queuing mechanism. Which command should you enable on this serial interface?

A. fair-queue
B. ip cef
C. priority-group
D. ip rtp priority
E. priority-queuing

Answer: D

Explanation:
The "ip rtp priority" command creates a strict priority queue for voice packets while providing WFQ for non-voice traffic. To reserve a strict priority queue for a set of Real-Time Transport Protocol (RTP) packet flows belonging to a range of User Datagram Protocol (UDP) destination ports, use the ip rtp priority command in interface configuration mode. This command is most useful for voice applications, or other applications that are delay-sensitive.
This command extends and improves on the functionality offered by the ip rtp reserve command by allowing you to specify a range of UDP/RTP ports whose voice traffic is guaranteed strict priority service over any other queues or classes using the same output

interface. Strict priority means that if packets exist in the priority queue, they are dequeued and sent first-that is, before packets in other queues are dequeued.
Incorrect Answers:

A. This command can be used for the default class (commonly known as the class-default class) only. You can use it in conjunction with either the queue-limit command or the random-detect command. The class-default class is the default class to which traffic is directed if that traffic does not satisfy the match criteria of other classes whose policy is defined in the policy map.
B. This will enable Cisco Express Forwarding, which will not fulfill the requirements of this question.
C. C, E. This will enable priority queuing, which could indeed be used to give RTP packets priority over other protocols, but used alone will not provide the mechanism for having the other traffic types serviced in a WFQ manner as described in this question.
Reference:
http://www.ciscocom/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a7

QUESTION 252
A serial interface with flow-based WFQ is carrying 25 flows in the following fashion:
* Twelve flows are marked as IP Precedence 0.
* Ten flows are marked as IP Precedence 1.
* Three flows are marked as IP Precedence 5.
Based on the above information, how much interface bandwidth is allocated to one of flows that are marked as IP Precedence 5?

A. 1%
B. 4%
C. 12%
D. 15%
E. 33%
F. Cannot tell from the information given

Answer: C

Explanation:
The total parts are found by adding one to each Precedence value, multiplying by the number of flows in that Precedence, and then totaling the parts (weights). Interface bandwidth is allocated to one of flows that are marked as IP Precedence is calculated as shown below.
(5+1) 6 6
---------- = ---------- = ------ = 12%
[12*(0+1)]+ [10*(1+1)]+ [3*(5+1)] 12+20+18 50
Incorrect Answers:
B. If we took one flow and divided it by the number of total flows, the answer would be 4% (1/25). However, the correct answer is found using the formula above.

QUESTION 253
Using the 3 layer hierarchical approach to a network, What QoS functions are performed at the access layer? (Choose 2)

A. Packet classification
B. Congestion management
C. Classification preservation.
D. Congestion avoidance
E. Admission control

Answer: A, E

Explanation:
As per Cisco's Hierarchical network model, There are 3 network layers: The Core layer, The distribution layer, and the Access layer. The Core or backbone of the network should not be involved in Processor intensive tasks. Tasks such as packet classification and access control are limited to the access layer and in some cases to the distribution layer. It is the edge routers that classify the QoS traffic, as well as control the QoS admissions into the network.
Incorrect Answers:
B, D. These are functions of the distribution layer. It could be argued that certain aspects of congestion avoidance and management are handled by edge routers, options A and D are better choices.
C. Differentiated Services markings are marked at the access layer edge routers, but preserved throughout the network at the distribution and core layers.

QUESTION 254
You need to give your new VOIP traffic priority over other traffic types in your network. To do this, you plan to implement custom queuing. What statement is FALSE about custom queuing?

A. Custom queuing defines up to 16 queues.
B. Custom queuing has one preemptive priority queue. This can be extended to multiple priority queues by configuring the 'lowest-custom' queue in the 'queue-list'.
C. In custom queuing there is a weight assigned to each queue which specifies how each queue is treated.
D. With custom queuing you cannot specify a minimum bandwidth guarantee per queue.
E. In custom queuing you can classify based on the incoming interface.

Answer: B

Explanation:
With custom queuing there is no pre-emptive queue. Bandwidth is statically serviced based on the configuration, and the queue that is being serviced at any given time will finish before servicing the next queue.

Custom Queuing (CQ)
With CQ, bandwidth is allocated proportionally for each different class of traffic. CQ allows you to specify the number of bytes or packets to be drawn from the queue, which is especially useful on slow interfaces
Why Use CQ?
You can use the Cisco IOS QoS CQ feature to provide specific traffic guaranteed bandwidth at a potential congestion point, assuring the traffic a fixed portion of available bandwidth and leaving the remaining bandwidth to other traffic. For example, you could reserve half of the bandwidth for SNA data, allowing the remaining half to be used by other protocols.
If a particular type of traffic is not using the bandwidth reserved for it, then unused bandwidth can be dynamically allocated to other traffic types.
Restrictions
CQ is statically configured and does not adapt to changing network conditions. With CQ enabled, the system takes longer to switch packets than FIFO because the packets are classified by the processor card.

QUESTION 255
Which of the following is a required configuration parameter for setting up NBAR?

A. match protocol IP
B. match nbar type 1
C. match ftp session passive
D. match protocol http
E. match url www.cisco.com

Answer: D

Explanation:
Configuring a Traffic Class
To configure a traffic class and the match criteria that will be used to identify traffic as belonging to that class, use the class-map global configuration command. To define the match criteria, use the following commands beginning in global configuration mode.
In the following procedure, all traffic matching a specified protocol will be classified as belonging to the traffic class. The traffic class will classify traffic while the traffic policy configuration will determine how to treat the traffic.
For instance, if you wanted all FTP traffic to be marked with the QoS group value of 1, you would use the match protocol ftp command in class-map configuration mode, and use the set qos-group 1 command in policy-map class configuration mode (assuming the traffic policy uses the specified class). Therefore, the classification purpose (classifying FTP traffic) would be handled in the traffic class, while the QoS feature (marking the QoS group value to 1) would be handled in the traffic policy.
Configuring a Traffic Class with NBAR Example
In the following example, the class-map class1 command uses the NBAR classification of SQL*Net as its matching criterion:

Router(config)# class-map class1
Router(config-cmap)# match protocol sqlnet

QUESTION 256
The Certkiller network is using Class of Service to prioritize the traffic throughout the network. Setting the CoS IP Precedence bits can be done in what situation?

A. For ATM CLP traffic only
B. To set the frame-relay DE bit
C. When we receive HDLC frame with DEADBEEF pattern
D. On a router on ISL or DOT1Q trunks in the output direction only
E. None of the above
F. All of the above

Answer: E

Explanation:
CoS refers to the ability of a network to provide differentiated service to selected network traffic over packet networks and cell networks. By default, the Cisco IOS software leaves the IP Precedence value untouched, preserving the precedence value set in the header, allowing all internal network devices to provide service based on the IP Precedence setting. This policy follows the standard approach stipulating that network traffic should be sorted into various types of service at the basic perimeter of the network and that those types of service should be implemented in the core of the network. Routers in the core of the network can then use the precedence bits, for example, to determine the order of transmission, the likelihood of packet drop, and so on.
You can use any of the following features to set the IP precedence in packets:
1. Policy-Based Routing
2. QoS Policy Propagation via Border Gateway Protocol
3. Committed Access Rate
Incorrect Answers:
A, B. The COS bit can be set for any FR/ATM traffic, using policy based routing. Frame relay and ATM networks can be configured to adjust traffic settings based on the Cell Loss Priority (CLP) and frame DE values, but the CoS bit is not limited to this type of traffic only.
C. The CoS bits can not be used based on layer 2 information in PPP and HDLC links, since specific identifiers are needed.
D. The CoS IP Precedence bits can be set based on both incoming and outgoing traffic.

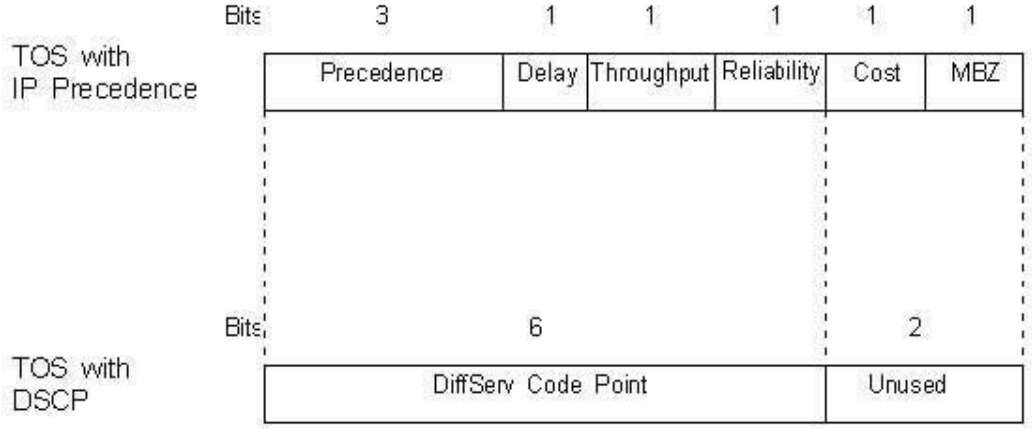
QUESTION 257
The Certkiller network plans to implement some method of quality of service using DSCP information. In comparing the different options which of the following statements is TRUE?

A. The IP precedence and DSCP have no overlapping fields.
B. The DSCP contains class selectors for backward compatibility with the IP precedence.

C. The DSCPD is exactly the same as IP precedence; the name change is merely as marketing naming convention.
D. The last 2 bit of the DSCP overlaps with the IP precedence.
E. DSCP is only for TEC; IP precedence is for UDP
F. None of the above.

Answer: A

Explanation:
DiffServ introduces the concept of the DiffServ Code Point (DSCP) that uses the first 6 bits of the TOS field thereby giving 26 = 64 different values. RFC 2474 describes the Differentiated Services (DS) field and the DiffServ Code Point (DSCP). A comparison of these two is displayed below:



As you can see from the comparison of the two packet formats, there are no overlapping fields.

QUESTION 258
The Certkiller network is using QoS to prioritize the critical traffic over busy links. What command would be used to configure Modular QoS CLI (MQC) to allow for a maximum bandwidth of 64 kb/s during times of network congestion; and when there is no congestion, to allow the use of more bandwidth?

A. bandwidth 64
B. priority 64
C. police 64000 confirm-action transmit exceed-action drop
D. shape average 64000
E. all of the above

Answer: A

Explanation:
MQC is a framework that provides a clear separation between a classification policy and the specification of other parameters that act on the results of that applied classification policy.

Broadly, MQC is configured and implemented as follows:
1. Define a traffic class with the class-map command.
2. Create a service policy by associating the traffic class with one or more QoS features (using the policy-map command).
3. Attach the service policy to the interface with the service-policy command.
To specify the bandwidth to be applied, configure the bandwidth as follows:

Router(config-pmap-c)# bandwidth {bandwidth-kbps | percent percent}	Specifies a minimum bandwidth guarantee to a traffic class. A minimum bandwidth guarantee can be specified in kilobits per second or by a percentage of the overall available bandwidth.

Incorrect Answers:
B. This is used to specify the priority of the traffic, but not the actual bandwidth to be used.
C. This command configures policing on the interface, so any traffic exceeding the 64 kbps will be dropped, even when there is no congestion.
D. This is used to specify the average traffic shaping, as specified by the CIR.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5014/products_feature_guide_chapter09186a008008813a.h

---

QUESTION 259
Priority queuing is being configured on router CK1 to give mission critical traffic priority over the WAN link. What statement is true with regard to priority queuing?

A. There are 4 priority queues: high, medium, normal, low.
B. The high and medium queues have precedence over the default queue.
C. The classification is configurable with the 'priority-list' command
D. The default queue is the normal queue, by default.
E. All of the above.
F. None of the above.

Answer: E

Explanation:
There are four priority queues: high, medium, normal, and low- listed in order from highest to lowest priority.
The default queue is the normal queue. Traffic that is not explicitly defined in the priority list will be assigned this priority by default.
Priority queuing is configured using the "priority-list" command.
Example:

In the following example, queuing priority for all telnet and SMTP traffic is assigned the high priority.
priority-list 1 protocol ip high tcp 23
priority-list 1 protocol ip high tcp 25

QUESTION 260
The IP precedence of a packet can be determine from:

A. All 8 bits of the ToS byte
B. Bits 3, 4 and 6 of the ToS byte.
C. The three most significant bits of the ToS byte.
D. The three least significant bits of the ToS byte.

Answer: C

Explanation:
This DSCP field definition allows for up to 64 distinct values (levels of service), 0 through 63, of classification on IP frames. The last two bits represent the Early Congestion Notification (ECN) bits. IP Precedence is only the 3 most significant bits of the ToS field. As a result, IP Precedence maps to DSCP by using IP Precedence as the 3 high-order bits and padding the lower-order bits with 0.

QUESTION 261
Part of the configuration file of router CK1 is shown in the diagram below:

```
!
ip cef
!
class-map match-all bulk
 match protocol ftp
 match protocol tftp
!
policy-map mark
 class bulk
service-policy

int fastethernet0/0
 ip address 10.1.1.1 255.255.255.0
 service-policy input mark
!
```

Based upon the MQC configuration shown in the exhibit, what statement is correct?

A. ip cef must be disabled (using no ip cef) in order for the NBAR classification (match protocol) commands to function.
B. All non-FTP and non-TFTP incoming traffic to the fa0/0 interface will be classified into the class-default traffic class and marked as DSCP 0.
C. All incoming traffic to the fa0/0 interface will be classified into the class-default traffic class and no DSCP marking will be performed.
D. Either FTP or TFTP incoming traffic to the fa0/0 interface willb e marked as af11.

E. None of the above.

Answer: C

Explanation:
Based on the configuration above, the service policy named mark will be applied to all traffic incoming on the fast ethernet 0/0 interface. In the policy map, all matching traffic will be assigned the Differentiated Services Code Point of assured forwarding 11. In this case, only traffic that is both FTP and TFTP will match the class-match due to the "match-all" keyword. Since a packet can not be both TFTP and FTP, no traffic will match and the default action will be taken.
Incorrect Answers:
D: This would be true if the "match-any" keyword was used in the "bulk" policy, but in this example the traffic must be both FTP and TFTP, which is not possible.

QUESTION 262
The relevant part of a Certkiller router's configuration is displayed below:

```
ip cef
!
class-map match-all VoIP-Remark
 match ip dscp ef
 match ip dscp cs3
 match ip dscp af31
!
class-map match-any VoIP-RTP
 match protocol rtp audio
 match access-group name VoIP-RTP
!
policy-map Policy-NoTrust
 class VoIP-RTP
  set ip dscp ef
 class VoIP-Remark
  set ip dscp default
!
interface Ethernet0
 description Outside Interface
 ip address 192.168.1.1 255.255.255.0
 service-policy input Policy-NoTrust
!
interface FastEthernet0
 description Inside Interface
 ip address 192.168.2.1 255.255.255.0
!
!
ip access-list extended
 permit udp any any range 16384 32767
```

Classed-Based marking has been configured as shown above to sort traffic into classes for appropriate treatment by upstream routers. Unfortunately, traffic received by an upstream router on the 192.168.1.0/24 network is not appropriately marked; VoIP packets are not marked *EF* and packets previously set by end-users as CS3 and EF are not remarked to DSCP 00000. Which of the following issues could be the cause of the problem? (Select two).

A. Using NBAR to classify RTP traffic requires that IP CEF be disabled.

B. The VoIP-RTP access list includes both even and odd-numbered ports starting from 16384; while RTP only uses even-numbered ports.
C. The router has been improperly configured to only mark traffic flowing in the wrong direction.
D. The set ip dscp default command does not mark the packet with dscp 0000, but instead resets the command use back to Cisco IOS default settings.
E. The Class-map VoIP-Remark has been improperly configured to simultaneously match more than one traffic type.

Answer: C, E

Explanation:
The first problem is that the service policy named Policy-NoTrust is being applied to the input direction of the ethernet interface, when it should be applied in the outbound direction for the upstream routers to see the correct DSCP markings of the packets.
The second problem is the fact that the keyword "match-all" is being applied to the VOIP-Remark class map. This keyword instructs the IOS that all of the criteria in the entire map must match in order to be applied. In the configuration above, only a packet that matches all three of the criteria (DSCP EF, DSCP CS3, and DSCP AF21) will be marked, instead of packets that match any one of those. In this example, the correct syntax should have been "class-map match-any VoIP-Remark"

QUESTION 263
Router CK1 is configured for QoS as shown below:

```
!
ip cef
!
class-map match-all cos3and4
 match cos 3 4
!
class-map match-all trans
 match protocol http
 match protocol telnet
!
class-map match-all scavenger
 match protocol napster
 match cos 1

policy-map ccietest
 class cos3and4
  set dscp af33
 class trans
  set dscp af21
 class scavenger
  set dscp cs1
!
interface fastethernet0/0
 ip address 10.1.1.1 255.255.255.0
 service-policy input ccietest
```

Based on the configuration displayed in the exhibit, what statement is correct about ingress traffic to the fa0/0 interface on CK1 ?

A. All ingress frames marked as COS 0 will be marked as DSCP 0.
B. All ingress frames marked as COS 1 will be marked as DSCP cs1.
C. All ingress HTTP traffic will be marked as DSCP af21.
D. All ingress Napster traffic will be marked as DSCP cs1.
E. All ingress frames marked as COS 3 or COS 4 will be marked as DSCP af33.
F. None of the above.

Answer: E

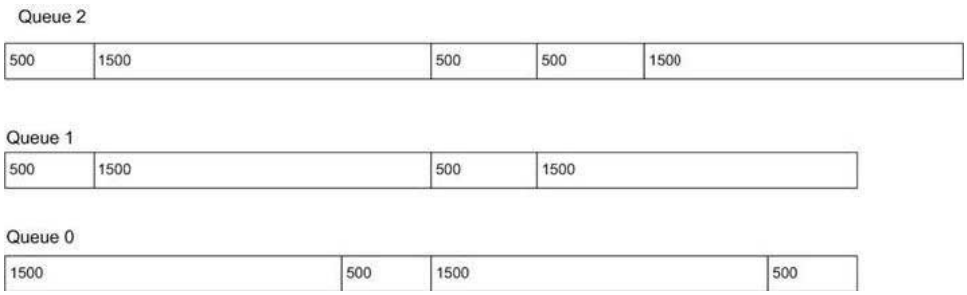
Explanation:
Since the "match cos 3 4" statement lies within a single configuration line, only one or the other need to match. When the keyword "match-all" is used, all distinct lines must match for the rule to take effect. Since the values shown in choice E are displayed in a single line, all traffic with COS values of 3 or 4 will match, and will subsequently be forwarded after being marked as AF33.
Additional info:
To access the QoS class map configuration mode to configure QoS class maps, use the class-map command. Use the no form of this command to delete a class map.
class-map name [match-all | match-any]
no class-map name [match-all | match-any]
Syntax Description

name	Class map name.
match-all	(Optional) Matches all match criteria in the class map.
match-any	(Optional) Matches one or more match criteria.

When you do not specify the match-all or match-any keyword, the default is match-all.
Incorrect Answers:

A. CoS values of 0 are not automatically marked with a DSCP value of 0
B, D. Here, only frames marked as COS and using the Napster protocol will be marked with a DSCP value of 1.
C. Only traffic that is both HTTP and Telnet will be marked as such. This is obviously not possible since HTTP uses port 80 while telnet uses port 23.

QUESTION 264
The following are 3 separate queues for a router configured to prioritize traffic:



Queue 2 is a low-latency queue running in alternate-priority mode. The interface MTU is 1500. The queue weights are as follows:
Weight of 1 for Queue 2
Weight of 2 for Queue 1
Weight of 1 for Queue 0
Assume that all the default counters are currently zero (0) and Queue 2 will be serviced first, how many packets will be left in Queue 2 after both of the other queues have been serviced once?

A. 0
B. 1
C. 3
D. 500
E. 1500

Answer: B

Explanation:
Since the example states that Q2 is serviced alternately with Q1 and Q0, the order goes Q2, Q1, Q2, Q0, Q2, etc. The quantum values calculated as MTU + (weight-1)*512 per queue are: Q2 = 1500, Q1= 2012 (MTU + (weight-1)*512) & Q0 = 1500. Therefore immediately after Q0 is serviced there is still a single packet in Q2.
Further clarification (step by step):
MTU is 1500.
Weight of1 for Queue 0 => 1500 bytes will be de-queued in first round
Weight of2 for Queue 1 =>1500 +(2-1)*512 =2012 bytes will be de-queued per round
Weight of1 for Queue 2=> 1500 bytes will be de-queued in first round
Sequence of de queuing operation...
Q2 first (500 byte) and second (1500 byte) packet offloaded. Deficit 1500-2000= --500
Q1 first (500 byte) second (1500 byte) third (500 byte packet offloadedDeficit2012-2500=-488
Q2 1500 -500 = 1000 bytes can be off loaded third (500 byte) and fourth (500 byte) packet are removed. last packet 1500 byte still remains.
Q0 First (1500 byte) packet is off loaded.
Q 2 Is being served after both the other queues have had their initial pass.
How many packets remain in Q 2 after first runis what the question is asking.
The answer is 1.

QUESTION 265
Which of the following is FALSE regarding differences between Generic Traffic Shaping

(GTS) and Frame Relay Traffic Shaping (FRTS)?

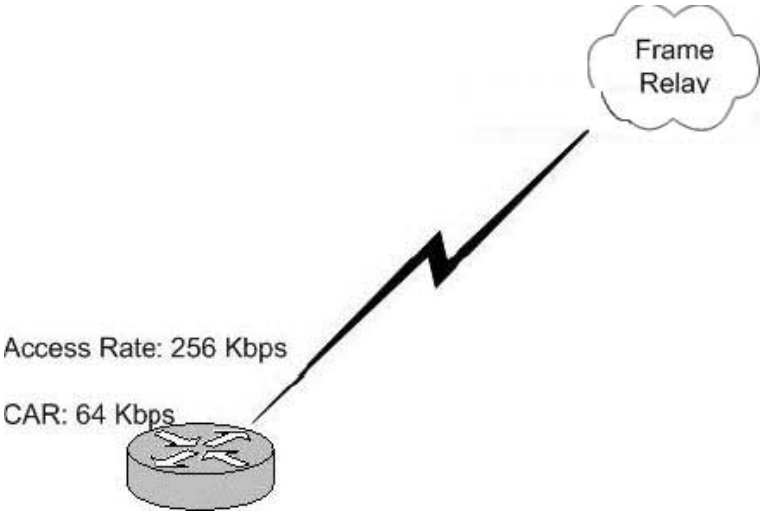
A. GTS supports the traffic group command while FRTS does not.
B. For GTS, the shaping queue is weighted fair queue (WFQ). FRTS does not support WFQ. With FRTS, the queue can be a CQ, PQ or FIFO.
C. FRTS supports shaping on a per-DLCI basis, while GTS is configurable per interface or subinterface.
D. GTS works with a variety of Layer 2 technologies, including Frame Relay, ATM, Switched Multimegabit Data Service, and Ethernet. FRTS is supported only on Frame Relay interfaces.

Answer: B

Explanation:
B. For FRTS, the queue can indeed be a weighted fair queue (configured by the frame-relay fair-queue command), a strict priority queue with WFQ (configured by the frame-relay ip rtp priority command in addition to the frame-relay fair-queue command), custom queuing (CQ), priority queuing (PQ), or first-in, first-out (FIFO).
Differences Between Traffic-Shaping Mechanisms
Generic traffic shaping (GTS), class-based shaping, distributed traffic shaping (DTS), and Frame Relay traffic shaping (FRTS) are similar in implementation, share the same code and data structures, but differ in regard to their CLIs and queue types used. Following are some examples in which these mechanisms differ:
1.
For GTS, the shaping queue is a weighted fair queue. For FRTS, the queue can be a weighted fair queue (configured by the frame-relay fair-queue command), a strict priority queue with WFQ (configured by the frame-relay ip rtp priority command in addition to the frame-relay fair-queue command), custom queuing (CQ), priority queuing (PQ), or first-in, first-out (FIFO).
2. For class-based shaping, GTS can be configured on a class, rather than only on an access control list (ACL). To do so, you must first define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces. Traffic shaping can be applied to each defined class.
3. FRTS supports shaping on a per-DLCI basis; GTS is configurable per interface or subinterface.
Incorrect Answers:
A, C, D. These statements are all true. For more on FRTS and GTS see the following URL (towards the bottom):
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800b

---

QUESTION 266
The Certkiller router shown in the following exhibit has a frame relay link with a port speed of 256K and a PVC CIR speed of 64K. The Certkiller router is receiving a notification form the Frame Relay provider that there is congestion in the network.



You want the router to react dynamically to this notification from the Frame relay provider.
What command should you issue to do this?

A. traffic-shape adaptive 64000
B. fair-queue 64000
C. shape peak 256000 64000
D. frame-relay class Certkiller

Answer: A
When the provider is sending messages to the frame relay customer that there is congestion notifications, they send Backward Explicit Congestion Notification messages (BECNs). As you can see from the definition below, the traffic shape adaptive command enables the router to react to this:
traffic-shape adaptive [bit-rate] configures minimum bit rate to which traffic is shaped when backward explicit congestion notifications (BECNs) are received on an interface.
With adaptive GTS, the router uses backward explicit congestion notifications (BECNs) to estimate the available bandwidth and adjust the transmission rate accordingly. The actual maximum transmission rate will be between the rate specified in the traffic-shape adaptive command and the rate specified in the traffic-shape rate command.
As you can see this fulfills the requirement of the question about the Frame Relay network sending information about congestion.
Incorrect Answers:
B, C. These commands will not enable the router to dynamically react to the BECN messages.
D. The Frame-relay class is command is setting up a map class. When a map class is applied to the main interface all the VC gets the traffic shaping from the main interface. This command needs too much assuming while the traffic-rate command does not.

QUESTION 267
In the Certkiller Frame Relay network, Class Based Shaping is being used to increase network performance. Which of the following is a true statement regarding Class

Based Shaping?

A. CB shaping allows to rate-limit traffic in both incoming and outgoing directions.
B. CB shaping provides a rate-limiting functionality with an associated amount of buffers, to store temporary out of profile traffic.
C. CB shaping can only be configured in a child policy in a hierarchical policy map.
D. CB shaping is a versatile feature which allows to both queue and remark traffic in input.
E. None of the above
F. All of the above

Answer: B

Explanation:
Traffic shaping allows you to control the traffic going out an interface in order to match its transmission to the speed of the remote, target interface and to ensure that the traffic conforms to policies contracted for it. Traffic adhering to a particular profile can be shaped to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches. This is done with the use of buffers, which are used to temporarily store traffic that is queued. An optional Class Based Shaping command allows for the maximum number of buffers to be adjusted.
Incorrect Answers:
A, D. Class Based Shaping is used for rate limiting outgoing traffic only. It does not provide for any mechanism to shape of mark incoming traffic.
C. Class Based Shaping uses class-map statements. A set of hierarchical policy maps are not required for configuring CBS.

QUESTION 268
The Certkiller network is using FRTS to optimize the data flows within the network. In frame-relay traffic shaping (FRTS), what is the Committed burst (Bc) parameter?

A. The Bc is optional, and can be 0. It tells IOS how much extra bandwidth can be used on top of the CIR.
B. The Bc is a parameter which needs to be negotiated with the provider of the frame-relay circuit. It defines the percentage of the frame-relay circuit IOS will use to send bursty traffic.
C. Bc is a mandatory parameter when configuring FRTS. It defines a traffic rate up to which IOS will send traffic.
D. Bc defines the amount of token added to the token bucket at each interval. The token bucket algorithm is used in FRTS. If not configured, it defaults to 56000 bits.
E. Bc is total size of the token bucket. This includes the excess burst and conform burst.
F. None of the above are true.

Answer: A

Explanation:
Bc (Committed Burst) is defined as the Maximum number of bits the frame relay network commits to transfer over a Committed Rate Measurement Interval (Tc). Tc = Bc / CIR. It is an optional parameter that defaults to 7000 bits, but it can indeed be set to 0, which means that no traffic will be able to burst above the CIR.
Incorrect Answers:
B. The Bc is a value specified in bits per interval, not in a percentage.
C. Bc is optional, not mandatory. The only mandatory configuration guidelines for FRTS is to specify the interface with frame-relay encapsulation, and to enable FRTS with the "frame-relay traffic-shaping" interface command.
D. The default committed burst size is 7000 bits, when no value is specified. The default Bc value for priority queuing on frame relay links is 56000, but it is 7000 for regular FRTS.
E. Bc is the committed burst rate, not the total burst.

QUESTION 269
In weighted fair queuing (WFQ), one can configure a 'congestive-discard-threshold' (CDT). What is the CDT value used for?

A. This threshold specifies from which point on IOS should start using WFQ.
B. The CDT specifies the number of messages allowed in each queue.
C. The CDT specifies the maximum amount of messages to be used by WFQ for high bandwidth traffic, dropping packets from the most aggressive flow.
D. The CDT defines a value from when IOS starts to account all messages in the WFQ system in conjunction with Netflow.
E. CDT refers to the maximum amount of dynamic flows IOS will allow for WFQ.
F. None of the above

Answer: C

Explanation:
WFQ provides traffic priority management that automatically sorts among individual traffic streams without requiring that you first define access lists. WFQ can also manage duplex data streams such as those between pairs of applications, and simplex data streams such as voice or video. There are two categories of WFQ sessions: high bandwidth and low bandwidth. Low-bandwidth traffic has effective priority over high-bandwidth traffic, and high-bandwidth traffic shares the transmission service proportionally according to assigned weights.
Example: The following example requests a fair queue with a congestive discard threshold of 64 messages, 512---dynamic queues, and 18 RSVP queues:
interface Serial 3/0
ip unnumbered Ethernet 0/0
fair-queue 64 512 18
When WFQ is enabled for an interface, new messages for high-bandwidth traffic streams are discarded after the configured or default congestive messages threshold has been met. However, low-bandwidthconversations, which include control message conversations,

continue to enqueue data. As a result, the fair queue may occasionally contain more messages than its configured threshold number specifies.

QUESTION 270
What is true about Class based Weighted Fair Queuing (CBWFQ)?

A. CBWFQ provides delay, jitter and bandwidth guarantees to traffic.
B. CBWFQ can be configured on any interface in either input or output.
C. CBWFQ has to be configured with the Modular QoS CLI. The resulting service-policy has to be applied on output.
D. CBWFQ can only be configured in a hierarchical policy-map. The parent policy-map does policing and the child policy-map does CBWFQ.
E. All of the above
F. None of the above

Answer: C

Explanation:
To configure CBWFQ, there are 3 required steps: Defining class maps, configuring class policy in the policy map, and attaching the service policy and enabling CBWFQ. This is done using the new IOS syntax called Modular QoS. You must use the Modular QoS CLI to configure class based marking.
Incorrect Answers:

A. There is no way to specify traffic guarantees for jitter and delay, as the underlying network that is used for transport will have the greatest impact on these values.
B. The CBWFQ service policy can only be applied to outbound interfaces.
D. Although CBWFQ is typically configured using this method, it not not required for all implementations.
Reference: Distributed QoS, Odom/Cavanaugh, Cisco Press, page 176.

QUESTION 271
CAR has been configured on router CK1 . What best defined Committed Access Rate (CAR)?

A. CAR allows metering of traffic for traffic shaping.
B. CAR is a feature that allows the rate limiting of traffic in either the incoming or outgoing direction.
C. CAR is part of a set of features to be used in conjunction with queuing to form a hierarchical policy. CAR must always be applied in a parent policy-map, whereas CBWFQ should be applied in a child policy-map.
D. CAR is a queuing feature.
E. CAR matches only on UDP port range {16384 - 32767}.

Answer: B

Explanation:
The Committed Access Rate (CAR) and Distributed CAR (DCAR) services limit the input or output transmission rate on an interface or subinterface based on a flexible set of criteria.
The rate-limiting feature of CAR provides the network operator with the means to define Layer 3 aggregate or granular access, or egress bandwidth rate limits, and to specify traffic handling policies when the traffic either conforms to or exceeds the specified rate limits. Aggregate access or egress matches all packets on an interface or subinterface. Granular access or egress matches a particular type of traffic based on precedence. You can designate CAR rate-limiting policies based on physical port, packet classification, IP address, MAC address, application flow, and other criteria specifiable by access lists or extended access lists. CAR rate limits may be implemented either on input or output interfaces or subinterfaces including Frame Relay and ATM subinterfaces.
An example of use of CAR's rate-limiting capability is application-based rates limiting HTTP World Wide Web traffic to 50 percent of link bandwidth, which ensures capacity for non-Web traffic including mission-critical applications.

QUESTION 272
QoS mechanisms have been put in place within the Certkiller network using IP precedence. This IP precedence can be defined as:

A. The ToS byte is the IP precedence
B. The middle 4 bits of the ToS byte
C. The 3 left most bits of the ToS byte
D. The 3 right most bits of the ToS byte
E. The right most bit of the ToS byte

Answer: C

Explanation:
Within the Type of Service (TOS) byte, the three most significant bits are the IP precedence bits. The TOS byte is displayed below:
ToS Byte
P2 P1 P0 T2 T1 T0 CU1 CU0
1. IP precedence-three bits (P2 to P0)
2. Delay, Throughput and Reliability-three bits (T2 to T0)
3. CU (Currently Unused)-two bits(CU1-CU0)
Reference: http://www.cisco.com/warp/public/105/dscpvalues.html

---

QUESTION 273
You wish to enable the Resource Reservation protocol on one of the interfaces of a router. Which of the following commands will accomplish this?

A. ip rsvp sender
B. ip rsvp enable
C. ip rsvp bandwidth

D. rsvp enable
E. ip rsvp reservation
F. RSVP is enabled in global configuration mode, not in interface configuration mode.

Answer: C

Explanation:
ip rsvp bandwidth is the command that enables RSVP
Incorrect Answers:
F. RSVP is configured on a per interface basis, not in global configuration mode.

QUESTION 274
Which of the following statements is valid regarding Custom Queuing?

A. Custom queuing always services the highest priority traffic first before servicing the lower priority traffic.
B. Custom queuing looks at groups of packets from the similar source-destination pairs.
C. Custom queuing processes the queue based on the number of packets sent.
D. Custom queuing will not proceed to a next queue unless the current queue is empty.
E. Custom queuing can prevent one type of traffic from saturating the entire link.

Answer: E

Explanation:
CQ allows fairness not provided with priority queuing (PQ). With CQ, you can control the available bandwidth on an interface when it is unable to accommodate the aggregate traffic enqueued. Associated with each output queue is a configurable byte count, which specifies how many bytes of data should be delivered from the current queue by the system before the system moves on to the next queue. When a particular queue is being processed, packets are sent until the number of bytes sent exceeds the queue byte count defined by the queue-list queue byte-count command, or until the queue is empty.
With custom queuing, all queues will be serviced. With priority queuing, a bandwidth hog can dominate the link.
Incorrect Answers:
A, D Custom queue uses a round robin mechanism, ensuring that one type of traffic (even ones with the highest priority) does not completely starve out the lower priority queues. Once the byte count for that queue is fulfilled, the next queue is serviced.
B, C. Custom queues are serviced based on the number of bytes sent for each queue, not on the number of packets sent. This prevents traffic with bigger packets (such as FTP) from dominating a link with smaller packets (such as a RTP session).

QUESTION 275
Due to intermittent congestion issues on a link, Committed Access Rate (CAR) has been configured on an interface. During a period of congestion, a packet arrives that causes the compounded debt to be greater than the value set for the extended burst. Which of the following will occur due to this? (Choose all that apply).

A. CAR's exceed action takes effect, dropping the packet.
B. A token is removed from the bucket.
C. The packet will be queued and eventually serviced.
D. The compounded debt value is effectively set to zero (0).
E. The packet is buffered by the CAR process.

Answer: A, D

Explanation:
Here is how the extended burst capability works. If a packet arrives and needs to borrow n number of tokens because the token bucket contains fewer tokens than its packet size requires, then CAR compares the following two values:
1. Extended burst parameter value
2. Compounded debt. Compounded debt is computed as the sum over all ai.
3. 1. i indicates the ith packet that attempts to borrow tokens since the last time a packet was dropped.
2.
a indicates the actual debt value of the flow after packet i is sent. Actual debt is simply a count of how many tokens the flow has currently borrowed.
If the compounded debt is greater than the extended burst value, CAR's exceed action takes effect. After a packet is dropped, the compounded debt is effectively set to 0. CAR will compute a new compounded debt value equal to the actual debt for the next packet that needs to borrow tokens.
If the actual debt is greater than the extended limit, all packets will be dropped until the actual debt is reduced through accumulation of tokens in the token bucket.
Incorrect Answers:
B. Dropped packets do not count against any rate or burst limit. That is, when a packet is dropped, no tokens are removed from the token bucket.
C, E. After the exceed action takes place, the packet is dropped immediately and is not buffered.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart4/qcpolts.htm

---

QUESTION 276
In an effort to minimize the risks associated from DOS and ICMP flooding attacks, the following is configured on the serial interface of a router:
interface serial 0
rate-limit input access-group 199 128000 4000 4000 conform-action
transmit exceed-action drop
access-list 199 permit icmp any any
What QoS feature is this an example of?

A. CBWFQ
B. LLQ
C. RSVP

D. CAR
E. WFQ
F. FRTS

Answer: D

Explanation:
Committed Access Rate (CAR) is used to rate limit traffic. In this example, all ICMP traffic that exceeds the defined level will be dropped. This will prevent an ICMP flood attack from saturating the link.
CAR definition:
Rate limiting is one mechanism to use to allow a network to run in a degraded manner, but remain up when it is receiving a stream of Denial of Service (DoS) attack packets as well actual network traffic. Rate limiting can be achieved in a number of methods using Cisco IOS(r) software. Namely, through Committed Access Rate (CAR), Traffic Shaping, and both Shaping and Policing through Modular Quality of Service Command Line Interface (QoS CLI).
Incorrect Answers:

A. Class-based weighted fair queuing (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces Packets satisfying the match criteria for a class constitute the traffic for that class. A queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide09186a0080087a84.html
B, C. RSVP and LLQ (low latency queuing) are often implemented in voice and video data networks, but are not typically used for preventing DOS attacks.
F. FRTS is frame relay traffic shaping. It is not clear from this example that the link is even using frame relay as the transport link.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_tech_note09186a00800fb50a.shtml

---

QUESTION 277
Which of the following are functions of Random Early Discard (RED)? (Choose all that apply)

A. To avoid global synchronization for TCP traffic.
B. To provide unbiased support for bursty traffic.
C. To minimize packet delay jitter.
D. To ensure that high priority traffic gets sent first.
E. To prevent the starvation of the lower priority queues.

Answer: A, B, C

Explanation:
When it comes to Quality of Service, there are 2 separate approaches. The first is congestion management, which is setting up queues to ensure that the higher priority traffic gets serviced in times of congestion. The other is congestion avoidance, which works by dropping packets before congestion on the link occurs. Random Early Detection (RED) is a congestion avoidance mechanism that takes advantage of TCP's congestion control mechanism.
RED takes a proactive approach to congestion. Instead of waiting until the queue is completely filled up, RED starts dropping packets with a non-zero drop probability after the average queue size exceeds a certain minimum threshold. A drop probability ensures that RED randomly drops packets from only a few flows, avoiding global synchronization. A packet drop is meant to signal the TCP source to slow down. Responsive TCP flows slow down after packet loss by going into slow start mode.
Incorrect Answers:
D. This would be a function of priority queuing, not RED. Weighted RED (WRED) is used to assign priorities to traffic and works to not drop the higher priority traffic types, but RED does not.
E. This is a function of custom queuing, which is a congestion management mechanism, not a congestion avoidance mechanism such as RED.
Reference:
'IP Quality of Service' page 130, Cisco Press.

QUESTION 278
You issue the following configuration change on router CK1 :
ip rsvp sender 225.1.1.1 192.1.2.1 UDP 3030 192.1.2.1 serial0 20
What is the effect of this change?

A. The router will simulate receiving RSVP PATH messages destined to multicast address 225.1.1.1 from source 192.1.2.1.
The previous hop of the PATH message is 192.1.2.1, and the message was received on interface serial 0.
B. The router will simulate generating RSVP RESV messages destined to multicast address 225.1.1.1 from source 192.1.2.1.
The next hop of the PATH message is 192.1.2.1, and the message was received on interface serial 0.
C. The router will act as if it was sending RSVP PATH messages destined to multicast address 225.1.1.1 from source 192.1.2.1.
The next hop of the PATH message is 192.1.2.1, and the message was received on interface serial 0.
D. The router will act as if it was receiving RSVP RESV messages destined to multicast address 225.1.1.1 from source 192.1.2.1.
The previous hop of the PATH message is 192.1.2.1, and the message was received on interface serial 0.

Answer: A

Explanation:
This command causes the router to act as if it were receiving PATH messages destined to multicast address 225.1.1.1 from a source 12.1.2.1. The previous hop of the PATH message is 12.1.2.1, and the message was received on interface Serial 0.
To enable a router to simulate receiving and forwarding Resource Reservation Protocol (RSVP) PATH messages, use the ip rsvp sender global configuration command. To disable this feature, use the no form of this command.
ip rsvp sender session-ip-address sender-ip-address {tcp | udp | ip-protocol} session-dport sender-sport previous-hop-ip-address previous-hop-interface bandwidth burst-size
Incorrect Answers:
B. This answer describes the "ip rsvp reservation-host" command.
C. This answer describes the "ip rsvp sender-host" command
D. The "ip rsvp sender" command simulates a host that is receiving PATH messages, not RESV messages.

QUESTION 279
Rate Limiting is configured on the Ethernet interface of a router as follows:
interface Ethernet 0
rate-limit input access-group rate limit 1 1000000 10000 10000
conform-action
access-list rate-limit 1 mask 07
What effect will this configuration have?

A. The command access rate policing limits all TCP traffic to 10Mbps.
B. Traffic matching access-list 7 is rate limited.
C. Voice traffic with DiffServ code point 43 is guaranteed.
D. Traffic with IP Precedence values of 0, 1, and 2 will be policed.

Answer: D

Explanation:
Use the mask keyword to assign multiple IP precedence's to the same rate-limit list. To determine the mask value, perform the following steps:
Step 1 Decide which precedence's you want to assign to this rate-limit access list.
Step 2 Convert the precedence's into an 8-bit numbers with each bit corresponding to one precedence. For example, an IP precedence of 0 corresponds to 00000001, 1 corresponds to 00000010, 6 corresponds to 01000000, and 7 corresponds to 10000000.
Step 3 Add the 8-bit numbers for the selected precedence's together. For example, the mask for precedence's 1 and 6 is 01000010.
Step 4 Convert the binary mark into the corresponding hexadecimal number. For example, 01000010 becomes 0x42. This value is used in the access-list rate-limit command. Any packets that have an IP precedence of 1 or 6 will match this access list. A mask of FF matches any precedence, and 00 does not match any precedence.
In this example, a mask of 07 translates to 00000111, so IP precedence 0, 1, and 2 will be policed.

QUESTION 280
When configuring Low Latency Queuing (LLQ), a bandwidth parameter is needed. What does this parameter specify?

A. It provides a built in policer to limit the priority traffic in the LLQ during congestion.
B. This parameter is optional, since the LLQ will always have precedence over other queues.
C. This parameter should be as low as possible. It represents bandwidth which will always be reserved. It reduces the amount of bandwidth on the interface, even if it is not used by any LLQ traffic.
D. It represents the reference CIR to calculate the burst size of the token bucket of the built-in policer.
E. None of the above.

Answer: A

Explanation:
The bandwidth argument is used to specify the maximum amount of bandwidth allocated for packets belonging to a class configured with the priority command. The bandwidth parameter both guarantees bandwidth to the priority class and restrains the flow of packets from the priority class.
When the device is not congested, the priority class traffic is allowed to exceed its allocated bandwidth. When the device is congested, the priority class traffic above the allocated bandwidth is discarded.
Reference :http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a0080080232.html#47

QUESTION 281
What statement is FALSE with regards to Weighted RED (WRED)?

A. WRED is a congestion avoidance mechanism, based on the adaptive nature of TCP traffic for congestion.
B. WRED is a queuing feature.
C. WRED allows for differentiated dropping behavior based on either IP precedence or DSCP.
D. WRED is configurable in a CBWFQ policy-map.
E. All of the above are false statements.

Answer: B
Explanation
The WRED algorithm provides congestion avoidance on network interfaces by providing buffer management, andby allowing Transmission Control Protocol (TCP) traffic to throttle back before buffers are exhausted. This helps avoid tail drops and global synchronization issues, maximizing network usage and TCP-based application performance. WRED works by selectively dropping packets before congestion occurs, so

it is considered to be a congestion avoidance feature, not a queuing feature.
Incorrect Answers:

A. WRED is only useful when the bulk of the traffic is TCP/IP traffic. With TCP, dropped packets indicate congestion, so the packet source will reduce its transmission rate. With other protocols, packet sources may not respond or may resend dropped packets at the same rate. Thus, dropping packets does not decrease congestion.
C. WRED works with the IP precedence or DSCP values to determine which packets get dropped first. You can configure WRED to ignore IP Precedence when making drop decisions so that nonweighted RED behavior is achieved.
D. WRED can indeed be configured in a policy map that is applied to class based weighted fair queuing as specified in the following:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00801b2406.html

---

QUESTION 282
Routers CK1 , CK2 , and CK3 are configured in a hub and spoke frame relay environment, with router CK1 as the hub. You have configured Router CK1 , Router CK2 , and Router CK3 to run IGRP over the frame relay connections. No sub-interfaces are used. You have configured a single IP subnet on all the Frame Relay interfaces. Router CK1 can reach both router CK2 and CK3 , but CK2 and CK3 can not reach each other.
What is the probable cause of this problem?

A. Router CK1 is missing frame maps.
B. Router CK2 and Router CK3 are not performing frame map updates.
C. LMI mismatches between routers CK2 and CK3 .
D. Split-horizon is enabled on Router CK1 .
E. Split-horizon is disabled on Router CK1 .

Answer: D

Explanation:
The rule of split horizons is the problem with distance vector protocols such as IGRP. The split horizon rule prohibits a router from advertising a route through an interface that the router itself uses to reach that destination. Without sub-interfaces, split-horizon goes into effect, and all routes learned from the Serial interface will not be advertised out of that interface.
Incorrect Answers:
A, B. If the problem was related to missing frame maps or missing updates, then any given location would have issues reaching any location. In this case, router CK2 and CK3 are both able to reach CK1 with no problems.

QUESTION 283
You are troubleshooting a frame relay problem with the serial0 interface on one of your Certkiller routers. When the interface is brought up, it stays up for a short time before it goes back down. You issue the show interface command, and from this you can see that your interface shows LMI status messages sent, but none received. What could be the

problem?

A. There are too many input errors on the line.
B. The Frame-Relay lmi-type is set incorrectly.
C. Too many sub-interfaces are exceeding IDB limits.
D. The DCD not set correctly for a Frame-Relay circuit.
E. Keepalives are not set correctly on both ends.

Answer: B

Explanation:
In a frame relay configuration, the router's interface always assumes that the connection is up first. Only after missing three consecutive LMI status messages will the interface go down. This explains why the interface shows an "up" status for a short time before going back down. In this case the counters for LMI sent is increasing while the counters for LMI rcvd is still 0. This clearly indicates a case of misconfigured LMI type.
For a detailed discussion on how to troubleshoot serial lines, refer the link below.
http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1915.htm#xtocid195571
Incorrect Answers:
C. IDB units are Individual Data Blocks, which are units that consume memory resources for each sub-interface that is created. In order to surpass the IDB limits of most routers, thousands of sub-interfaces will need to be created. In addition, after this threshold is met, no more sub-interfaces can be created. Since this question is referring to an already configured router, this is not the problem.
D, E. Although both of these issues could cause problems with the serial lines staying up, they do not explain the fact that LMI status inquiries are received back. Even with keepalives or DCD information set incorrectly, the LMI messages should still be sent and received.

QUESTION 284
The Certkiller WAN consists of a frame relay network using ANSI LMI. What is the maximum theoretical number of DLCI's that can be advertised on a Frame-Relay interface with an MTU of 1500 bytes when using ANSI LMI?

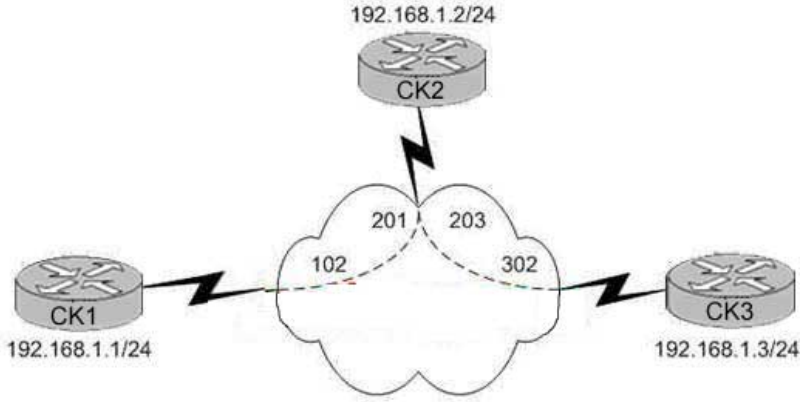
A. 1024
B. 1023
C. 992
D. 297
E. 186
F. 796

Answer: D

Explanation:
The formula for finding the maximum number of DLCI's for ANSI is (1500-13)/5=max DLCIs = 297.4. See below for the specifics for how this formula is generated:

Analysis
In a PVC information packet, the Report Type (RT) portion is one byte long and the KeepAlive (KA) portion is two bytes long. For the ANSI and Q933a LMIs, the PVC information is 3 bytes long, whereas for the Cisco LMI it is 6 bytes long due to the additional "bw" (for BandWidth) value. The "bw" value represents the Committed Information Rate (CIR); the actual bw value will only be seen if the frame relay switch is configured to forward this information.
The static overhead in each case is 13 bytes [Entire LMI packet minus IEs (10 bytes) + RT (1 byte) + KA (2 bytes)]. We can subtract this number from the Maximum Transmission Unit (MTU) to get the total available bytes for DLCI information. We then divide that number by the length of the PVC IE (5 bytes for ANSI and Q933a, 8 bytes for Cisco) to get the maximum theoretical number of DLCIs for the interface:
For ANSI or Q933a, the formula is: (MTU - 13) / 5= max DLCIs.
For Cisco, the formula is (MTU - 13) / 8= max DLCIs.

QUESTION 285
The Certkiller frame relay network is displayed in the diagram below, along with the partial configuration of router CK1 :




```
!Hostname CK1
interface Serial0/0
  ip address 192.168.1.1 255.255.255.0
  encapsulation frame-relay
```

What command must be added to interface serial 0/0 of CK1 to allow it to ping CK3 ?

A. frame-relay inverse-arp ip
B. frame-relay interface-dlci 302
C. encapsulation frame-relay ietf
D. frame-relay map ip 192.168.1.3 102 broadcast
E. None of the above

Answer: D

Explanation:
The frame relay map command is used to map layer 3 addresses to layer 2 DLCI information. In this case, the router CK1 is configured to statically map IP address 192.168.1.3 to DLCI 102.

Incorrect Answers:

A. Inverse ARP creates dynamic address mappings, as contrasted with the frame-relay map command, which defines static mappings between a specific protocol address and a specific DLCI. In this case, there is not a PVC that directly connects CK1 and CK3 , so Inverse ARP alone will not be sufficient.
B. This command should be used on point to point subinterfaces, not on the physical serial interface because it will map all IP addresses to the 302 DLCI, which is incorrect.
C. This command should be used to connect a Cisco router to a non-Cisco frame relay router.

QUESTION 286
The CK1 frame relay router is configured for frame relay traffic shaping as shown in the diagram below:

hostname CK1
!
interface Serial0/0
bandwidth 384
encapsulation frame-relay
!
interface Serial0/0.101
bandwidth 128
ip address 192.168.1.1 255.255.0
frame-relay interface-dlci 101
class ccie
!
map-class frame-relay ccie
frame-relay cir 128000
frame-relay bc 16000
frame-relay be 0
frame-relay adaptive-shaping becn
Router CK1 is receiving BECNs. What is the lowest rate CK1 will shape its output traffic to?

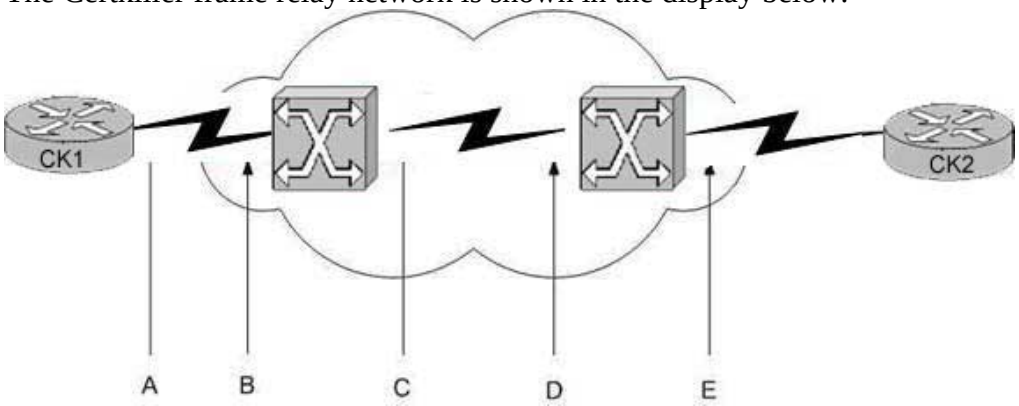
A. 0 kbps
B. 16 kbps
C. 64 kbps
D. 128 kbps
E. 384 kbps

Answer: C

Explanation:

The minimum CIR is value is specified by the "frame-relay mincir" command. This command is optional, and if it is omitted from the configuration, the default value is found by dividing the CIR value that is specified by two. In this specific example, it is 128000/2 for a minimum value of 64 kbps, so choice C is correct.
Some additional information on Frame Relay Adaptive Traffic Shaping can be found below:
The Adaptive Frame Relay Traffic Shaping for Interface Congestion feature enhances Frame Relay traffic shaping functionality by adjusting permanent virtual circuit (PVC) sending rates based on interface congestion. When this new feature is enabled, the traffic-shaping mechanism monitors interface congestion. When the congestion level exceeds a configured value called queue depth, the sending rate of all PVCs is reduced to the minimum committed information rate (minCIR). As soon as interface congestion drops below the queue depth, the traffic-shaping mechanism changes the sending rate of the PVCs back to the committed information rate (CIR). This process guarantees the minCIR for PVCs when there is interface congestion.
NoteThe sum of the minCIR values for all PVCs on the interface must be less than the usable interface bandwidth.
This new feature works in conjunction with backward explicit congestion notification (BECN) and Foresight functionality. If interface congestion exceeds the queue depth when adaptive shaping for interface congestion is enabled along with BECN or ForeSight, then the PVC sending rate is reduced to the minCIR. When interface congestion drops below the queue depth, then the sending rate is adjusted in response to BECN or ForeSight.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087b91.html

QUESTION 287
The Certkiller frame relay network is shown in the display below:

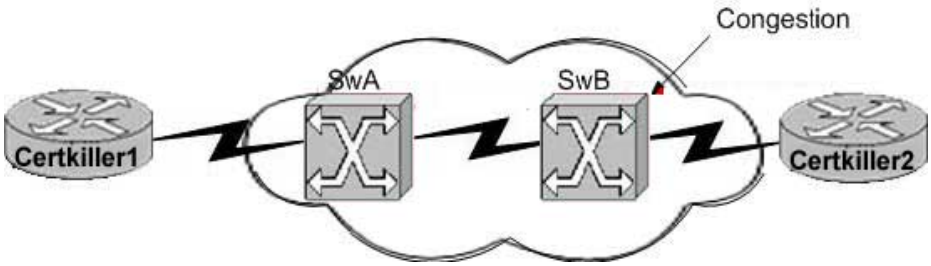


At which interfaces can the DE bit be set for frame relay packets flowing from CK1 to CK2 ? (Select all that apply)

A. A
B. B
C. C
D. D
E. E

Answer: A, B, C, D
Explanation
The frame relay provider's backbone is shared by many users and possibly multiple services. To keep you (and everybody else) from sending more data than the network can hold, frames sent above your contracted rate may be marked as Discard Eligible (DE). DE bits are set by the carrier network, not your equipment. They are also an indication of congestion within the frame relay network, so the DE bits are set on the interior of the carrier network, not at the provider edge to customer edge portion. If your equipment receives DE-marked frames, this indicates that data sent at this rate in the future may get dropped. This may be an early indicator of traffic rates that you didn't plan for in the design of your frame relay WAN.
Frame relay equipment notices congestion when it sees frames marked with the Forward Error Correction Notification (FECN) and Backward Error Correction (BECN) bits. These merely indicate an overload within the carrier network, and are only of value in monitoring the carrier's health.
The Cisco router can be configured to mark packets as DE using the "frame-relay de-list" command, making choice A also correct.
Incorrect Answers:
E: The DE bits are set between the carrier's frame relay switches, not between the frame relay switches and the customer provided routers. The DE frames are also used only within the network provider, so they would not be marked on interface E since the frame is going directly to the customer router.

QUESTION 288
The Certkiller frame relay network is depicted below:



Traffic from Certkiller 1 to Certkiller 2 is experiencing congestion. What device sets the BECN bit?

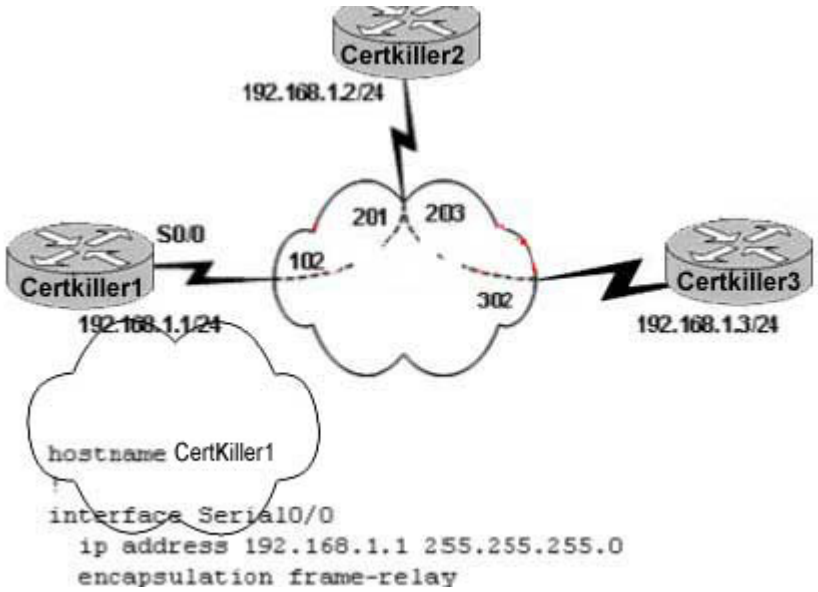
A. Certkiller 1 sets the BECN bit on outgoing packets.
B. Certkiller 2 sets the BECN bit on outgoing packets.
C. SwB sets the BECN bit on packets from Certkiller 1 to Certkiller 2.
D. SwB sets the BECN bit on packets from Certkiller 2 to Certkiller 1.

Answer: D

Explanation:
If device A is sending data to device B across a Frame Relay infrastructure and one of the intermediate Frame Relay switches encounters congestion, congestion being full buffers, over subscribed port, overloaded resources, etc, it will set the BECN bit on packets being returned to the sending device and the FECN bit on the packets being sent to the receiving device. This has the effect of telling the sending router to Back off and apply flow control like traffic Shaping and informs the receiving device that the flow is congested and that it should inform upper layer protocols, if possible, that it should close down windowing etc to inform the sending application to slow down.
A FECN tells the receiving device that the path is congested so that the upper layer protocols should expect some delay. The BECN tells the transmitting device that the Frame Relay network is congested and that it should "back off" to allow better throughput.
FECN (Forward Error Congestion Notification)
BECN (Backward Error Congestion Notification)
Reference: http://www.sins.com.au/network/frame-relay-fecn-becn.html

---

QUESTION 289
The Certkiller frame relay network is displayed in the following diagram:

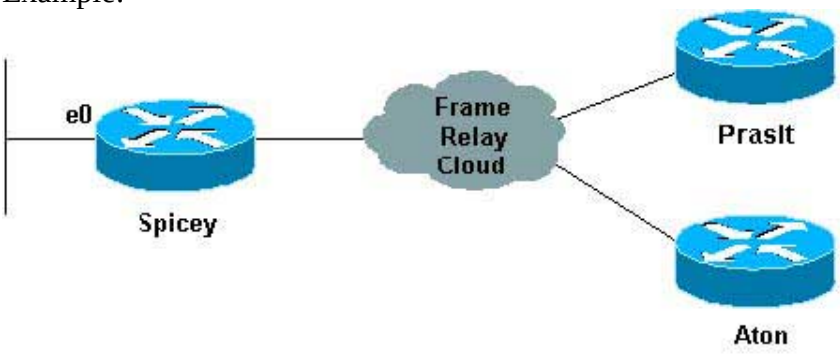


What command must be added to interface serial 0/0 of Certkiller 1 to allow it to ping the Certkiller 3 remote site?

A. frame-relay inverse-arp ip
B. framy-relay interface-dlci 302
C. encapsulation frame-relay ietf
D. frame-relay map ip 192.168.1.3 102 broadcast
E. frame-relay map ip 192.168.1.3 302 broadcast

Answer: D

Explanation:
Connecting from Spoke to Spoke:
You cannot ping from one spoke to another spoke in a hub and spoke configuration using multipoint interfaces because there is no mapping for the other spokes' IP addresses. Only the hub's address is learned via the Inverse Address Resolution Protocol (IARP). If you configure a static map using the frame-relay map command for the IP address of a remote spoke to use the local data link connection identifier (DLCI), you can ping the addresses of other spokes. The local DLCI should be specified when using the "frame-relay map" command, which is 102 in this example.
Example:



Configuration:Prasit
prasit#show running-configinterface Ethernet0ip address 123.123.123.1
255.255.255.0!interface Serialip address 3.1.3.2 255.255.255.0encapsulation
frame-relayframe-relay map ip 3.1.3.3 150frame-relay interface-dlci 150 Reference:
http://www.cisco.com/en/US/tech/ CK7 13/ CK2 37/technologies_tech_note09186a008014f8a7.shtml

---

QUESTION 290
Split Horizon is often used with Poison Reverse to prevent routing loops. Of the following choices, which statement is FALSE regarding the rule of Split Horizon?

A. It can cause problems on cetain Frame-Relay Hub-and Spoke configurations.
B. It is enabled by default on multipoint Frame-Relay subinterfaces.
C. It can be disabled for IP/RIP and IPX/RIP.
D. It aids in preventing routing loops.
E. None of the above.

Answer: C

Explanation:
For both point to point and point to multipoint sub-interfaces, split horizon is disabled by default. For physical serial frame relay multipoint interfaces, it is enabled by default.
Frame Relay subinterfaces provide a mechanism for supporting partially meshed Frame Relay networks. Most protocols assume transitivity on a logical network; that is, if station A can talk to station B, and station B can talk to station C, then station A should be able to talk to station C directly. This is true on LANs, but is not true on Frame Relay networks unless A is directly connected to C.
Additionally, certain protocols such as AppleTalk and transparent bridging could not be supported on partially meshed networks because they require "split horizon," in which a packet received on an interface cannot be transmitted out the same interface even if the packet is received and transmitted on different virtual circuits.
By configuring Frame Relay subinterfaces, a single physical interface is treated as multiple virtual interfaces. This allows us to overcome split horizon rules. Packets received on one virtual interface can now be forwarded out another virtual interface, even if they are configured on the same physical interface.
Subinterfaces address these limitations by providing a way to subdivide a partially meshed Frame Relay network into a number of smaller, fully meshed (or point-to-point) subnetworks. Each subnetwork is assigned its own network number and appears to the protocols as if it is reachable through a separate interface. (Note that point-to-point subinterfaces can be unnumbered for use with IP, reducing the addressing burden that might otherwise result.)
IP RIP can indeed have split horizon disabled. This can be accomplished via the use of sub-interfaces, or with the "no ip split-horizon" interface command. This will disable split horizons for IP traffic, including RIP. However, IPX RIP traffic can not be disabled so this statement is false.
Incorrect Answers:
A: This statement is true. For networks using distance vector routing protocols, spoke site

to spoke site connectivity can be affected due to the split horizon rule.
B: Cisco serial interfaces are multipoint interfaces by default unless specified as a point-to-point subinterface. Though less common than point-to-point subinterfaces, it is possible to divide the interface into separate virtual multipoint subinterfaces. Multipoint interfaces/subinterfaces are still subject to the split-horizon limitations as discussed above. All nodes attached to a multipoint subinterface belong to the same network number. Typically, multipoint subinterfaces are used in conjunction with point-to-point interfaces in cases where an existing multipoint frame relay cloud is migrating to a subinterfaced point-to-point network design. A multipoint subinterface is used to keep remote sites on a single network number while slowly migrating remote sites to their own point-to-point subinterface network.
D: Routing loop prevention is the reason why split horizon was created.
References:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_guide_chapter09186a008008

http://www.alliancedatacom.com/manufacturers/cisco-systems/framerelay_design/subinterfaces.asp

---

QUESTION 291
On router CK1 , you want to view the status of a frame relay connection. Which "show" commands will display the status of a Frame-Relay PVC? (Select all that apply)

A. show frame relay pvc
B. show frame-relay pvc
C. show frame-relay interface
D. show frame-relay lmi
E. show frame-relay map
F. show frame relay interface

Answer: B, E

Explanation:
The following is the example output from the show frame-relay pvc command, which explicitly displays the PVC status:
CK1 #show frame-relay pvc
PVC Statistics for interface Serial0 (Frame Relay DCE)
Active Inactive Deleted Static
Local 1 0 0 0
Switched 0 0 0 0
Unused 0 0 0 0
DLCI = 101, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0
input pkts 207 output pkts 239 in bytes 15223
out bytes 14062 dropped pkts 0 in FECN pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 17 out bcast bytes 3264

PVC create time 00:11:32, last time PVC status changed 00:11:32
Similarly, for show frame-relay map:
CK1 #show frame-relay map
Serial3/1/0.100(D1) (up): point-to-point(D2) dlci, dlci
401(D3)(0x191,0x6410),
broadcast(D4)
status defined, active(D5)
Serial3/1/0.120 (up): point-to-point dlci, dlci 402(0x192,0x6420),
broadcast
status defined, active
Incorrect Answers:
A: This is an invalid command, as the Cisco IOS syntax uses frame-relay, not frame relay.
C: The "show frame-relay interface resource" command is a FR to ATM internetworking command that will show PVC stats for Cisco ATM switches. It is not really a valid router IOS command, and it does not show the status of the individual PVC's
D: The following is sample output from the show frame-relay lmi command when the interface is a data terminal equipment (DTE) device:
CK1 # show frame-relay lmi
LMI Statistics for interface Serial1 (Frame Relay DTE) LMI TYPE = ANSI
Invalid Unnumbered info 0 Invalid Prot Disc 0
Invalid dummy Call Ref 0 Invalid Msg Type 0
Invalid Status Message 0 Invalid Lock Shift 0
Invalid Information ID 0 Invalid Report IE Len 0
Invalid Report Request 0 Invalid Keep IE Len 0
Num Status Enq. Sent 9 Num Status msgs Rcvd 0
Num Update Status Rcvd 0 Num Status Timeouts 9
None of the fields above explicitly show the status of the the PVC.
F: This is an invalid command

QUESTION 292
You are seeing a large number of clocking problems on the serial interface of one of your routers. Which of the following would NOT cause this? (Choose all that apply.)

A. Several cables connected together in a row.
B. Impedance mismatching.
C. Improper DSU configuration.
D. Mismatching encapsulations on each end.
E. Improper CSU configuration.

Answer: B, D

Explanation:
Impedance problems would cause errors on the line but not clocking problems. Although the encapsulation for any serial interface should match on each end for proper connectivity, this would also not cause clocking problems.

Incorrect Answers:
A, C, E are all possible causes for clocking problems.

QUESTION 293
A serial interface on a Cisco router is being connected to an external CSU/DSU. The CSU/DSU has an RS-232 interface with a DB-25 connection. Which cables would be used to connect the router to the external CSU/DSU?

A. DB-60 female to DB-25 male (DTE)
B. DB-60 male to DB-25 female (DTE)
C. DB-60 male to DB-25 female (DCE)
D. DB-60 female to DB-25 female (DTE)
E. None of the above

Answer: A

Explanation:
Devices that communicate over a serial interface are divided into two classes: DTE and DCE. The most important difference between these types of devices is that the DCE device supplies the clock signal that paces the communications on the bus. The following chart is a guideline for choosing the correct cable.
DTE DCE Selectable DTE or DCE*
Device Terminals, Data Service Unit/Channel Service Unit (DSU/CSU), Multiplexers Modems Hubs, Routers
Gender Male Female Either
* Selectable devices usually have a jumper, switch, or software command used to select DTE or DCE.
Incorrect Answers:
B, D. The DB-25 connection should be female, not male.
C. As shown by the chart above, the cable should be DTE, since it is connecting to a CSU/DSU.

QUESTION 294
Which of the following statement is true regarding clocking for a Cisco T1 interface?

A. The clock source command selects a source for the interface to clock received data. By default, it is clock source loop-timed (specifies that the T1/E1 interface takes the clock from the Tx (line) and uses it for Rx).
B. Routers are DTEs and NEVER supply clocking to T1/E1 line.
C. The clock source command specifies the location of the NTP server for timing.
D. The clock source selects a source for the interface to clock outgoing data. The default is clock source line -Specifies that the T1/E1 link uses the recovered clock from the line.
E. The clock source identifies the stratum level associated with the router T1/E1. The default is Stratum 1.

Answer: D

Explanation:
Clocking can either be internal, looped, or line. The default is line, meaning that the router is receiving clocking from the carrier network line.
Incorrect Answers:
C, E. These answers relate to NTP services, which are used for providing time stamping information to the router and does not relate to clocking. Stratum levels provide a hierarchy to the NTP source, with the highest level as 1.

QUESTION 295
You are troubleshooting connection problems from router CK1 . In doing so, you issue the "show interface serial 0" command and see: "serial 0 is up, line protocol down (disabled)." What can you conclude from this?

A. The Serial0 interface is operating properly.
B. The Serial0 interface needs to be enabled with the no shut down command.
C. The Serial0 interface is not working properly due to telco service problems.
D. The Serial0 interface is using the wrong protocol.
E. A loop exists in the circuit.

Answer: C

Explanation:
The line: Serial 0 is up, line protocol is down (disabled) indicates a telephone company service problem or a CSU/DSU hardware problem.
Incorrect Answers:
A. A properly working serial interface would show "serial 0 is up, line protocol is up"
B. If the interface was manually shut down, it would read: "serial 0 is administratively down, line protocol is down"
D. The protocols that ride over the serial interface do not affect the interface state. If the wrong encapsulation was configured, then the interface would most likely be down.
E. If a loop exists in the interface, then it would show up as looped, such as "serial 0 is up, line protocol is up (looped)."
Reference:
http://www.cisco.com/en/US/products/hw/voiceapp/ps967/products_administration_guide_chapter09186a00801

QUESTION 296
Router CK1 has Long Haul GBIC interface. You wish to connect it to router CK2 across your Metropolitan Area Network (MAN) using Single Mode Fiber. What is the maximum distance that router CK2 can be placed away from CK1 ?

A. 2 km
B. 10 km
C. 100 meters.
D. None of the above.

Answer: B

Explanation:
Single Mode fiber allows 10 km of distance.
Incorrect Answers:
A. 2 km is the distance limitation for multimode fiber, not single mode.
C. 100 meters is the maximum distance limitation for CAT5 Ethernet, not for single mode fiber.

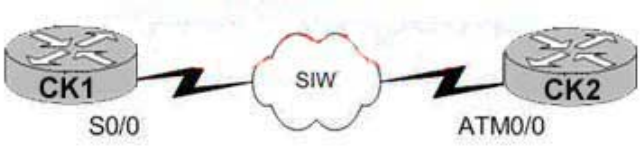
QUESTION 297
Which of the following are standards for physical WAN interfaces? (Choose all that apply)

A. 802.11
B. HSSI
C. V.35
D. RFC 1711
E. 802.5
F. 802.3
G. EIA/TIA 232
H. ISO 8648

Answer: B, C, G

Explanation:
EIA/TIA 232, EIA/TIA 449 EIA 530, and V.35 are for Interfaces that connect Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange. HSSI is a high speed serial interface supporting higher speed circuits.
Incorrect Answers:
A. 802.11 defines standards for wireless networks.
D. RFC 1711 defines classifications in email routing. It has absolutely nothing to do with WAN interfaces.
E. IEEE 802.5 is Token-Ring.
F. IEEE 802.3 is Ethernet.
H. ISO 8648 is an architectural model of the OSI Network Layer.

QUESTION 298
The Certkiller network is implementing VOIP on the frame relay/ATM internetworking network as displayed below:




```
hostname CK1
!
interface Serial0/0
  bandwidth 128
  encapsulation frame-relay IETF
!
interface Serial0/0.101
  bandwidth 128
  ip address 192.168.1.1 255.255.255.0
  frame-relay interface-dlci 101 IETF
```

```
hostname CK2
!
interface ATM0/0
 mtu 1500
 no ip address
 atm framing chitplcp
 no atm ilmi-keepalive
!
Interface ATM0/0.101
  bandwidth 128
  ip address 192.168.1.2 255.255.255.0
  pvc 1/101
    vbr-nrt 128 128
    broadcast
    encapsulation aal5nlpid
```

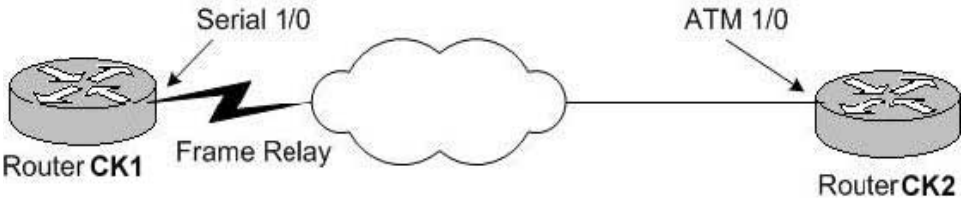
Voice quality on the network is being affected by FTP traffic. What is required to enable fragmentation of the large FTP packets?

A. Configure FRF.12 fragmentation on the Frame Relay interface.
B. Fragmentation is already provided by default from the ATM network.
C. Fragmentation is not supported with frame relay to ATM service internetworking.
D. Configure MLPPP on the Frame Relay and ATM interfaces.
E. Configure PPP link fragmentation and interleaving on the CK1 and CK2 routers.

Answer: A

Explanation:
The purpose of end-to-end FRF.12 fragmentation is to support real-time and non-real-time data packets on lower-speed links without causing excessive delay to the real-time data. FRF.12 fragmentation is defined by the FRF.12 Implementation Agreement. This standard was developed to allow long data frames to be fragmented into smaller pieces (fragments) and interleaved with real-time frames. In this way, real-time and non-real-time data frames can be carried together on lower-speed links without causing excessive delay to the real-time traffic.
End-to-end FRF.12 fragmentation is recommended for use on permanent virtual circuits (PVCs) that share links with other PVCs that are transporting voice and on PVCs transporting Voice over IP (VoIP). Although VoIP packets should not be fragmented, they can be interleaved with fragmented packets.
Incorrect Answers:
B. Fragmentation adjustments are not normally performed on ATM networks, since all data transmissions are sent using fixed length, 53 byte ATM cells.
C. Fragmentation support is available, via the FRF.12 standard.
D, E. MLPPP and LFI are features of PPP encapsulated serial circuits. Frame relay and ATM networks can not be configured using PPP encapsulation.

QUESTION 299
Two routers, CK1 and CK2 , are configured for OSPF. Router CK2 is the HQ router with an ATM DS3, while router CK1 is a remote router connected via Frame Relay. These two locations are connected via Frame Relay to ATM internetworking as shown below:



Router CK1 shows the EXSTART state for neighbor Router CK2 .
Router CK2 shoes the EXCHANGE state for neighbor Router CK1 .
What would be the most probable reason for this?

A. Multicast address 224.0.0.5 is being filtered at router CK1 .
B. Multicast address 224.0.0.6 is being filtered at router CK2 .
C. There is an MTU mismatch.
D. This is the normal OSPF operation.
E. There is an OSPF network type mismatch.

Answer: C

Explanation:
This problem is caused by MTUs being mismatched.
Incorrect Answers:
A, B. OSPF uses multicast addresses 224.0.0.5 and 224.0.0.6 for routing updates, but these addresses are only used on multi-access network such as a LAN segment. Even if these two routers were connected this way, the neighbor relationship would not reach past the first stage if these packets were filtered.
D. The correct OSPF operation would be a 2 way exchange.
E. With an OSPF network type mismatch, the routers would not even be able to reach the exchange/exstart stage.
Reference:
http://www.cisco.com/warp/public/104/12.html

QUESTION 300
When troubleshooting a T1 problem on your network, you discover that a number of RED alarms are being generated. What does this red alarm on a T1 indicate?

A. The CSU cannot synchronize with the framing pattern on the T1 line.
B. The far end equipment has a problem with the signal it is receiving from the upstream equipment.
C. There is an alarm on the line upstream form the equipment connected to the port generating the alarm.
D. There is an alarm from the equipment connected to the port generating the alarm.
E. The CSU is in a loopback.

Answer: A

Explanation:
A RED alarm is known as a Transmit Sending Remote Alarm.
A Red alarm is declared when the channel service unit (CSU) cannot synchronize with the framing pattern on the T1 line.
Reference:
http://www.cisco.com/en/US/tech/ CK7 13/ CK6 28/technologies_tech_note09186a00801069ff.shtml#topic5

QUESTION 301
With regard to PPPoA, which of the following statements are true? (Choose all that apply.)

A. PPPoA contains information about NCP LCP and supports all AAL.
B. PPPoA uses adaptation layer 5 (AAL5) as the framed protocol and is used primarily in xDSL.
C. PPPoA is not a standard based protocol.
D. In PPPoA architecture, IP address allocation for the subscriber CPE uses IPCP negotiation.
E. PPPoA supports all ppp features except password PAP CHAP.

Answer: B, D

Explanation:
Point-to-Point Protocol (PPP) (RFC 1331) provides a standard method of encapsulating higher layer protocols across point-to-point connections. It extends the High-Level Data Link Control (HDLC) packet structure with a 16-bit protocol identifier that contains information about the content of the packet.
The packet contains three types of information:
* Link Control Protocol (LCP) negotiates link parameters, packet size, or type of authentication
* Network Control Protocol (NCP) contains information about higher layer protocols including IP and IPX, and their control protocols (IPCP for IP)
* Data frames containing data
PPP over ATM adaptation layer 5 (AAL5) (RFC 2364) uses AAL5 as the framed protocol, which supports both PVC and SVC. PPPoA was primarily implemented as part of ADSL. It relies on RFC1483, operating in either Logical Link Control-Subnetwork Access Protocol (LLC-SNAP) or VC-Mux mode. A customer premise equipment (CPE) device encapsulates the PPP session based on this RFC for transport across the ADSL loop and the digital subscriber line access multiplexer (DSLAM).
Incorrect Answers:

A. PPPoA does not support every AAL and uses only AAL5.
C. PPPoA is standards based.
E. CHAP (Challenge authentication protocol) is supported in PPPoA.

Reference:
http://www.cisco.com/warp/public/794/pppoa_arch.html

QUESTION 302
Under one of the serial interfaces of your router you see the following configured:
Interface serial 0/0
Encapsulation PPP
IP address 10.1.1.1 255.255.255.252
Invert txclock
What is a reason for the "invert txclock" command being configured?

A. It synchronizes TXD and RXD clocks.
B. It corrects systems that use long cables that experience high error rates when operating at the higher transmission speeds.
C. It is used for adjusting the transmit clock properties of the PPP negotiation process.
D. It inverts the phase of the local clock used for timing incoming data the serial line.
E. It is used to allow the interface to provide clocking, rather than receiving clocking from the line.

Answer: B

Explanation:
Systems that use long cables or cables that are not transmitting the TxC signal (transmit echoed clock line, also known as TXCE or SCTE clock) can experience high error rates when operating at the higher transmission speeds. For example, if a PA-8T synchronous serial port adapter is reporting a high number of error packets, a phase shift might be the problem. Inverting the clock might correct this shift.
Incorrect Answers:
B. The invert txclock command is not related to PPP.
E. This describes the purpose of the clocking source configuration for a serial line. The correct configuration command for determining the clocking source is "clock source".

QUESTION 303
A router has a T1 private line connection, with the encapsulation type set to HDLC.
Which of the following are transfer modes that could be supported over this HDLC circuit? (Choose all that apply)

A. LAPB
B. ARB
C. ABM
D. ARM
E. NRM
F. LAPD

Answer: A, C, D, and E

Explanation:
The following are all transfer types supported by HDLC:
ARM - Asynchronous Response Mode. It is an HDLC communication mode involving one primary and at least one secondary, where either the primary or one of the secondaries can initiate transmissions.
ABM - Asynchronous Balanced Mode. It is an HDLC and derivative protocol, communication mode supporting peer-oriented point-to-point communications between two stations, where either station can initiate transmission.
NRM - Normal Response Mode
LAPB - Link Access Procedure Balanced
Incorrect Answers:
B, F. ARB and LAPD are not acronyms that apply to HDLC.

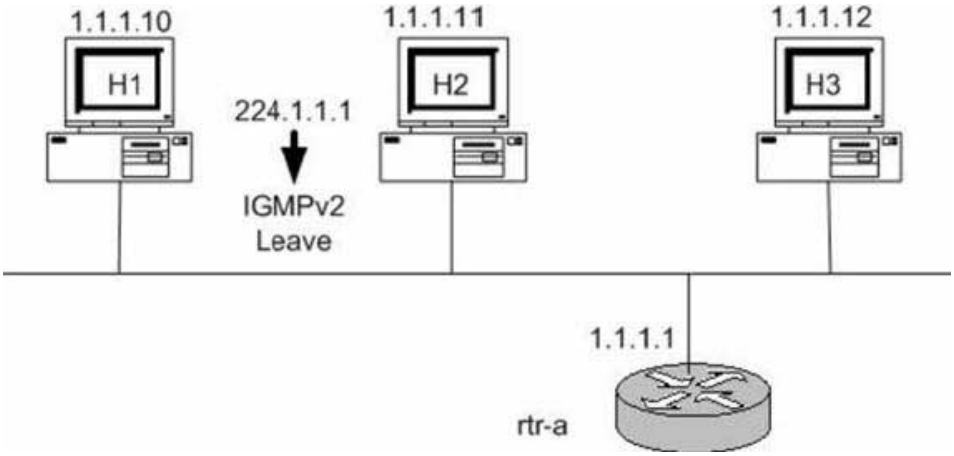
QUESTION 304
A Certkiller branch office uses Telnet and FTP to access an application at the main office over a point to point T1 HDLC link. You wish to increase the performance over this link through the use of a compression algorithm. What compression type will provide the best performance improvement?

A. Compressed Real-time Transport Protocol
B. TCP header compression
C. Stacker compression
D. Predictor compression

Answer: C

Explanation:
You can configure point-to-point software compression for all LAPB, PPP, and HDLC encapsulations using either the predictor or stacker compression methods. Compression reduces the size of frames via lossless data compression. HDLC encapsulations support the Stacker compression algorithm. PPP and LAPB encapsulations support both predictor and Stacker compression algorithms.
When compression is performed in software installed in the router's main processor, it might significantly affect system performance.
Compression requires that both ends of the serial link be configured to use compression.

QUESTION 305
Part of the Certkiller IP multicast network is shown below:



H1, H2, H3, and rtr-a are all IGMP version 2 devices. Host 2 and Host 3 belong to the 224.1.1.1 group. After a while, H2 sends out an IGMPv2 Leave message to leave the 224.1.1.1 group. How will rtr-a react to this leave message?

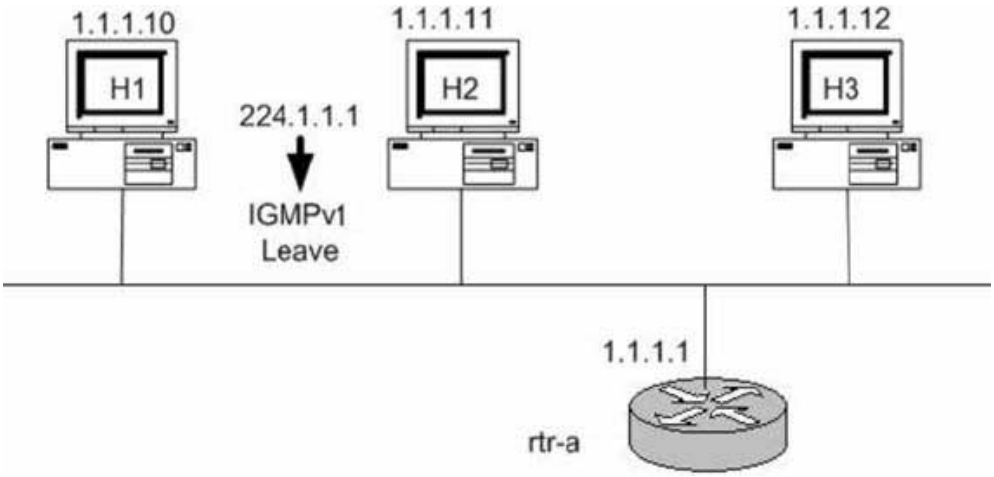
A. It will send an IGMPv2 Query to the all multicast hosts address 224.255.255.255.
B. It will send an IGMPv2 Group Specific Query to 224.1.1.1
C. It will send an IGMPv2 Leave Acknowledgement to Hosts H1 and H3.
D. It will send an IGMPv2 General Query to 224.1.1.1
E. It will send an IGMPv2 Group Specific Query to 224.0.0.1.

Answer: B

Explanation:
In IGMP version 2, a Leave message is responded by a group specific query from the router to check if there are any additional hosts participating in the multicast session. The group specific query is always destined for the multicast address that is being used.
Incorrect Answers:

A. The address 224.255.255.255 would never be used in this situation. In fact, the notion of a multicast "broadcast" does not exist.
C. Lave messages are not acknowledged.
D. General Query messages are not used.
E. The group specific query is always destined for the multicast address that is being used, which is 224.1.1.1 in this case.

QUESTION 306
The Certkiller network has a mix of IGMP version 1 and version 2 devices in its IP multicast network as shown below:



H1 and H2 are both IGMPv2 speakers and are also members of group 224.1.1.15. H3 is an IGMPv1 speaker and sends an IGMPv1 Membership Report to join group 224.1.1.15. What will happen?

A. The router rtr-a will do nothing, since there are already members of group 224.1.1.15 on the subnet.
B. The router rtr-a will ignore all IGMPv2 Leave messages while the IGMPv1 host is a member of group 224.1.1.15.
C. The router rtr-a will stop sending IGMPv2 Group-Specific queries in response to IGMPv1 Leaves received on this subnet for groups 224.1.1.15, while the IGMPv1 hosts is a member of group 224.1.1.15.
D. The router rtr-a will ignore the IGMPv1 Membership Report because router rtr-a is an IGMPv2 speaker and IGMPv1 are not compatible.

Answer: B

Explanation:
With IGMP version 1 and version 2 on the same network, routers will revert to v1, so the router will ignore the leave requests from all v2 members as long as the v1 member is still active for that multicast session.
Incorrect Answers:

A. Although there are already members on the same segment, the routers must be aware of the fact that there are a mix of v1 and v2 devices, so that the v2 leave messages can be ignored.
C. When the v1 device leaves the multicast session, the router must still send the group query out to see if the v2 devices are also still actively participating in the multicast session.
D. IGMP version 2 was designed to be backward compatible with version 1.
Reference:
"CCIE Professional Development Routing TCP/IP Volume II" by Jeff Doyle and Jennifer De Haven Carroll, Page 414.

QUESTION 307
IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP messages to their local multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.
Hosts need to actively communicate to the local multicast router that they intend to leave a group. If there are no replies, the router rimes out the group and stops forwarding the traffic. In order for this to work, what needs to be implemented?

A. IGMPv1
B. IGMPv2
C. IGMPv3
D. IGMPv4
E. CGMP

Answer: B

Explanation:
The Internet Group Management Protocol (IGMP) is used by IP hosts to report their host group memberships to any immediately neighboring multicast routers. IGMP messages are encapsulated in IP datagrams, with an IP protocol number of 2. IGMP has versions IGMP v1, v2 and v3.
In IGMPv2, leave messages were added to the protocol. This allowed group membership termination to be quickly reported to the routing protocol, which is important for high-bandwidth multicast groups and/or subnets with highly volatile group membership.
Incorrect Answers:

A. IGMPv1: Hosts can join multicast groups. There were no leave messages. Routers were using a time-out based mechanism to discover the groups that are of no interest to the members.
C. IGMPv3: Major revision of the protocol. It allows hosts to specify the list of hosts from which they want to receive traffic from. Traffic from other hosts is blocked inside the network. It also allows hosts to block inside the network packetsthat come from sources that sent unwanted traffic.
D. IGMPv4 is not yet in use.
E. CGMP is the Cisco Group Management Protocol (CGMP) which is a multicast protocol used by Cisco LAN switches, and not routers.

QUESTION 308
In the Certkiller network, hosts need to actively communicate to the local multicast router that they intend to leave a group. The router then sends out a group-specific query and determines if any remaining hosts are interested in receiving the traffic. If there are no replies, the router times out the group and stops forwarding the traffic. In order for this to work, what needs to be implemented?

A. IGMPv1
B. IGMPv2
C. IGMP snooping
D. DVMRO
E. CGMP
F. RGMP

Answer: B

Explanation:
IGMP version 2 is the Industry-standard protocol for managing multicast group membership, including support for IGMP-leave messages and group-specific queries. Leave Group message is a new type different from IGMP version 1. Membership Report is issued by host that want to join a specific multicast group (GDA). When IGMP router receive the Membership Report, it will add the GDA to the multicast routing table and start forwarding the IGMP traffic to this group. Membership Queries are issued by router at regular intervals to check whether there is still a host interested in the GDA in that segment. Host Membership Reports are sent either when the host wants to receive GDA traffic or response for a membership query from IGMP router.
If a host does not want to receive the IGMP traffic any more, it sends a Leave Group message. When the multicast router receives this Leave Group message, it removes the GDA from the multicast routing table. In addition, IGMP multicast routers periodically send Host Membership Query messages (hereinafter called Queries) to discover which host groups have members on their attached local networks.If no Reports are received for a particular group after some number of Queries, the routers assume that that group has no local members and that they need not forward remotely-originated multicasts for that group onto the local network. In addition, IGMP version 2 has leave mechanisms.
Incorrect Answers:

A. In IGMP version 1, hosts can join multicast groups. There were no leave messages. Routers were using a time-out based mechanism to discover the groups that are of no interest to the members.
D, F. These are incorrect terms for this IP multicasting functionality.
E. CGMP is used between Cisco switches and routers to provide for IP multicast information to be passed between the two.

QUESTION 309
The default behaviour for a Layer 2 switch is to forward all multicast traffic to every port that belongs to the destination LAN on the switch. This behavior reduces the efficiency of the switch, whose purpose is to limit traffic to the ports that need to receive the data. In an effort to increase the efficiency of the Certkiller network, you wish to utilize different protocols on the LAN.
Choose the correct protocols to handle IP multicast efficiently in the Certkiller layer 2 switched IP network. (Select the best choice).

A. Use Router-Port Group Mangement Protocol (RGMP) on subnets that include end

users or receiver clients. Use Cisco Group Management Protocol (CGMP), IGMP Snooping on routed segments that contain only routers, such as in a collapsed backbone.
B. Use Router-Port Group Mangement Protocol (RGMP) on subnets that include end users or receiver clients and routes segments that contain only routers, such as in a collapsed backbone.
C. Use Cisco Group Management Protocol (CGMP), IGMP Snooping on subnets that include end users or receiver clients. Use Router-Port Group Management Protocol (RGMP) on routed segments that contain only routers, such as in a collapsed backbone.
D. Use Cisco Group Management Protocol (CGMP) on subnets that include end users or receiver clients and routed segments that contain only routers, such as in a collapsed backbone.
E. Use IGMP Snooping on subnets that include end users or receiver clients and routed segments that contain only routers, such as in a collapsed backbone.

Answer: C

Explanation:
The purpose of Cisco Group Management Protocol (CGMP) and Internet Group Management Protocol (IGMP) snooping is to restrain multicast traffic in a switched network. By default, a LAN switch floods multicast traffic within the broadcast domain. This can consume a lot of bandwidth if many multicast servers are sending streams to the segment.
IGMP snooping is a feature that allows the switch to "listen in" on the IGMP conversations between hosts and routers. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the GDA list for that group. And, when the switch hears an IGMP Leave, it removes the host's port from the CAM table entry.
RGMP constrains multicast traffic that exits the Cisco Router through ports to which only disinterested multicast routers are connected. RGMP reduces network congestion by forwarding multicast traffic to only those routers that are configured to receive it.
Note: To use RGMP, you must enable IGMP snooping on the Cisco router. IGMP snooping constrains multicast traffic that exits through LAN ports to which hosts are connected. IGMP snooping does not constrain traffic that exits through LAN ports to which one or more multicast routers are connected.

QUESTION 310
How are Layer 3 multicast IP addresses mapped to Token Ring MAC addresses? (Choose all that apply).

A. All IP Multicast addresses are mapped to broadcast MAC address FFFF.FFFF.FFFF.
B. All IP Multicast addresses are mapped to network MAC address 0000.0000.0000.
C. All IP Multicast addresses are mapped to Functional Address C000.0004.0000.
D. In the same method as is used in Ethernet networks.
E. Token ring MAC addresses are not mapped to IP multicast addresses.

Answer: A, C

Explanation:
By default, IP multicast datagrams on Token Ring LAN segments used the MAC-level broadcast address 0xFFFF.FFFF.FFFF. That places an unnecessary burden on all devices that do not participate in IP multicast. The IP multicast over Token Ring LANs feature defines a way to map IP multicast addresses to a single Token Ring MAC address.
This feature defines the Token Ring functional address (0xc000.0004.0000) that should be used over Token Ring. A functional address is a severely restricted form of multicast addressing implemented on Token Ring interfaces. Only 31 functional addresses are available. A bit in the destination MAC address designates it as a functional address.
The implementation used by Cisco Systems complies withRFC 1469, IP Multicast over Token-Ring Local Area Networks.
Reference:
See RFC 1469, IP Multicast over Token-Ring Local Area Networks
Also see
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/np1_c/1cmulti.htm#21101

QUESTION 311
The IANA owns a block of Ethernet MAC address that start with 01:00:5E in haxadecimal formal. Half of this block is allocated for multicast addresses. The range from 0100.5e00.0000 through 0100.5e7f.ffff is the available range of Ethernet MAC address for IP multicast.
This allocation allow for 23 bits in the Ethernet address to correspond to the IP multicast group address. The mapping places the lower 23 bits of the IP multicast group address into these available 23 bits in the Ethernet address.
Because the upper five bits of the IP multicast address are dropped in this mapping, the resulting address in not unique. In fact, 32 different multicast group IDs map to the same Ethernet address.
225.1.1.1 and 237.1.1.1 have been assigned to map to the same multicast MAC address on a Layer 2 switch. What will occur?

A. If one user is subscribed to Group A (as designated by 225.1.1.1) and the other user is subscribed to Group B (as designated by 237.1.1.1), they would both receive only the streams meant for them. Group A would go to 225.1.1.1 and group B would go to 237.1.1.1
B. If one user is subscribed to Group A (as designated by 237.1.1.1) and the other user is subscribed to Group B (as designated by 225.1.1.1), they would both receive only the first stream that reached the network.
C. If one user is subscribed to Group A (as designated by 225.1.1.1) and the other user is subscribed to Group B (as designated by 237.1.1.1), they would both receive both streams, A and B streams.
D. If one user is subscribed to Group A (as designated by 225.1.1.1) and the other user is subscribed to Group B (as designated by 237.1.1.1), both of them would not receive A and B streams.
E. None of the above

Answer: C

Explanation:
Although mathematically there are 32 possibilities for overlap of addresses it is very unlikely to happen in real life. If it does, the impact is that another set of stations receives the multicast traffic. This is still far preferable to ALL stations receiving the traffic. This is always the case where two IP multicast addresses share the same MAC address.

QUESTION 312
Which IP address maps to the Ethernet multicast MAC address of 01-00-5e-10-20-02? (Choose all that apply)

A. 224.128.10.2
B. 225.128.10.2
C. 224.10.20.2
D. 225.10.20.2
E. 239.144.32.2
F. 224.16.32.2
G. All of the above
H. None of the above

Answer: E, F

Explanation:
Ethernet interfaces map the lower 23 bits of the IP multicast address to the lower 23 bits of the MAC 0100.5e00.0000. As an example, the IP multicast address 224.0.0.2 is mapped to the MAC layer as 0100.5e00.0002.
1. HEX 01 = 00-5e (all Multicast Addresses);
2. HEX 10 = 00010000 - could be both 16 and 144 (decimal) due to the fact that we ignore the first bit of the second octet when converting to binary;
3. HEX 20 = 00100000 = 32;
4. HEX 02 = 00000010 = 2.

QUESTION 313
What is the class D IP address range 239.0.0.0-239.255.255.255 used for?

A. Administratively Scoped multicast traffic meant for internal use.
B. Link-local multicast traffic made up of network control messages meant to stay in the local subnet.
C. Global Internet multicast traffic meant to travel throughout the Internet.
D. Any valid multicast data stream for use with multicast applications.
E. Routing protocol use.

Answer: A

Explanation:

The 239 address range is reserved for IP multicast traffic that is to be used for internal use only. It is similar to RFC 1918 private IP address space, except instead of specifying unicast address ranges it specifies multicast.
Incorrect Answers:
B, E. Link level multicast messages, such as those used by routing protocols, use the 224.0.0.0 address range. For example, IGRP uses 224.0.0.10 and OSPF uses 224.0.0.5 and 224.0.0.6.
C, D. This address range should never be seen in the Internet. It is reserved for private use only.
Reference:
Jeff Doyle Volume II chapter on IP Multicast.

QUESTION 314
You wish to implement a multicast video application over your private, internal network. To do this, you need to use a private multicast range of IP addresses across your network. Which IP range should you use?

A. 224.0.0.0 - 224.255.255.255
B. 226.0.0.0 - 226.255.255.255
C. 241.0.0.0 - 241.255.255.255
D. 239.0.0.0 - 239.255.255.255
E. 240.0.0.0 - 254.255.255.255.

Answer: D

Explanation:
The reserved, administratively scoped IPv4 multicast address space is defined to be the range 239.0.0.0 to 239.255.255.255. Administratively scoped multicast addresses are for use only on a private network and are not to be used on the Internet.
Reference:
RFC 2365 - http://www.faqs.org/rfcs/rfc2365.html

QUESTION 315
The Certkiller network is using IP multicast within to conserve bandwidth during the training video seminars. In this IP multicast network, which of the following correctly describes scoping?

A. Scoping is the restriction of multicast data transport to certain limited regions of the network. There are two types: TTL scoping and administrative scoping.
B. Scoping is used by SSM to locate the sources and receivers in certain limited regions of the network. There are two types: TTL scoping and administrative scoping.
C. Scoping is a process used in MSDP to locate the sources and receivers in different AS.
D. PIM dense mode uses scoping to locate the sources and receivers in order to built shared trees.

Answer: A

Explanation:
Traditionally, IP multicast uses a Time to Live (TTL) parameter in an IP multicast application and multicast routers to control the multicast distribution. When you define the TTL value in an IP multicast application, contents don't transmit beyond the TTL value. For example, if you set Site Server's Active Channel Multicaster TTL value to 10, you ensure that Site Server's Web contents don't multicast beyond 10 router hops. Each multicast packet carries a TTL value in its IP header. Just as in unicast, every time a multicast router forwards a multicast packet, the router decreases the packet's TTL by 1. As an alternative to TTL scoping, the Internet Engineering Task Force (IETF) proposed Administratively Scoped IP Multicast as an Internet standard in its Request for Comments (RFC) 2365 in July 1998. Administrative scoping lets you scope a multicast to a certain network boundary (e.g., within your organization) by using an administratively scoped address. IETF has designated IP multicast addresses between 239.0.0.0 and 239.255.255.255 as administratively scoped addresses for local use in intranets. You can configure routers that support administratively scoped addressing on the border of your network to confine your private multicast region. You can also define multiple isolated multicast regions in your network so that sensitive multicast data will travel only within a designated area.

QUESTION 316
The Certkiller network is implementing IP multicast and they want to ensure that the IP addresses they used are contained within the Certkiller autonomous system. What is the range of limited scope/administrative scope addresses that should be used?

A. Addresses in the 232.0.0.0/8 range
B. Addresses in the 239.0.0.0/8 range
C. Addresses in the 224.0.0.0/8 range
D. Addresses in the 229.0.0.0/8 range
E. Addresses in the 234.0.0.0/8 range
F. None of the above

Answer: B
Explanation
The range of addresses from 239.0.0.0 through 239.255.255.255 contains limited scope addresses or administratively scoped addresses. These are defined by RFC 2365 to be constrained to a local group or organization. Routers are typically configured with filters to prevent multicast traffic in this address range from flowing outside an autonomous system (AS) or any user-defined domain. Within an autonomous system or domain, the limited scope address range can be further subdivided so those local multicast boundaries can be defined. This also allows for address reuse among these smaller domains. These addresses are the IP multicast version of the private, RFC 1918, addresses used for unicast.
Reference:http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ipmulti.htm

---

QUESTION 317
In an IP multicast network, the more sources an application has, the less frequently traffic is sent from each end. Each time a source starts to send packets, protocol operations take place and a forwarding state is established. For applications with a large number of sources, this state can time-out before the source would to only create a large number of sources, this state can time-out before sources would not only create a large amount of forwarding state (requiring memory), but they could also require high CPU usage o the routing processor due to the accounting of frequently changing state. In addition, the signaling within the router between the routing processor and forwarding hardware can become another potential bottleneck of continuously large amount of traffic signaling must go to the routing processor and equally large amounts of forwarding state changes must go to the forwarding engine(s).
The Certkiller network is implementing IP multicast, and they wish to avoid the problems described above. Based on this information, what IP multicast technology would you recommend?
Caution: This protocol should avoid maintaining source-specific forwarding state, thereby reducing the amount of memory needed by the number of sources per multicast group, requiring much less traffic signaling in the protocol, preventing the "bursty source" problem, saving on CPU requirements for protocol operations and avoiding potential internal performance limits.

A. PIM Dense Mode (PIM DM)
B. PIM Sparse Mode (PIM SM)
C. Distance Vector Multicast Routing Protocol (DVMRP)
D. Multicast Open Shortest Path First (MOSPF)
E. Bi-Directional PIM

Answer: E

Explanation:
Bidirectional-PIM is a variant of the Protocol Independent Multicast (PIM) suite of routing protocols for IP multicast. In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco IOS implementation of PIM supports three modes for a multicast group:
1. Bidirectional mode
2. Dense mode
3. Sparse mode
A router can simultaneously support all three modes or any combination of them for different multicast groups. In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address need not be a router, but can be any unassigned IP address on a network that is reachable throughout the PIM domain. Using this technique is the preferred configuration for establishing a redundant RP configuration for bidir-PIM.

In PIM dense mode (PIM-DM), PIM-SM, and most other multicast routing protocols such as Distance Vector Multicast Routing Protocol (DVMRP) and Multicast Open Shortest Path First (MOSPF), protocol operations and maintenance of packet forwarding state depend on signaling the presence or expiration of traffic (where "signaling" refers to both the packet forwarding engine to routing protocol process within the routers and the packet exchange part of the routing protocol). Triggering PIM assert messages, PIM register messages, and source tree forwarding state are all examples of traffic signaling. There are several advantages to traffic signaling, but they can lead to problems for applications with a large number of sources. For example, the more sources an application has, the less frequently traffic is sent from each sender. Each time a source starts to send packets, protocol operations take place and forwarding state is established. For applications with a large number of sources, this state can time out before the source sends again, resulting in "bursty sources." Therefore, applications with a large number of sources would not only create a large amount of forwarding state (requiring memory), but they also could require high CPU usage on the Route Processor due to the accounting of frequently changing state. In addition, the signaling within the router between the Route Processor and forwarding hardware can become a bottleneck if continuously large amounts of traffic signaling must go to the Route Processor and equally large amounts of forwarding state changes must go to the forwarding engines.
Bidir-PIM solves all these problems. Not only does bidir-PIM avoid maintaining source-specific forwarding state, therefore reducing the amount of memory needed by the number of sources per multicast group, but it also does not require any traffic signaling in the protocol. Thus, bidir-PIM prevents the "bursty source" problem, saving on CPU requirements for protocol operations and avoiding potential router internal performance limits.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1612/products_feature_guide09186a0080080a41.html

---

QUESTION 318
You are a technician at Certkiller . Your newly appointed Certkiller trainee wants to know which IP protocol is used to send PIMv2 control messages.
What would your reply be?

A. UDP
B. TCP
C. BGP
D. Protocol number 107
E. Protocol number 103

Answer: E

Explanation:
All PIM control messages have protocol number 103.
Reference:
http://www.ietf.org/proceedings/99mar/I-D/draft-ietf-pim-v2-dm-01.txt

---

QUESTION 319
IP multicast addresses in the range of 224.0.0.0 through 224.0.0.255 are reserved for what purpose?

A. It is reserved for Administratively Scoped multicast traffic intended to remain inside a private network.
B. It is reserved for Administratively Scoped multicast traffic that is not supposed to be transmitted onto the Internet.
C. It is reserved for link-local multicast traffic consisting of network control messages that is not supposed to leave the local subnet.
D. Any valid multicast data stream used by multicast applications.
E. Global Internet multicast traffic intended to travel throughout the Internet.

Answer: C

Explanation:
As found in RFC1112. These addresses are used by many routing protocols such as OSPF and RIPv2, in order to sent updates to all neighbors on the same segment.
Incorrect Answers:
Administratively Scoped IP multicast addresses are contained in the 239.0.0.0-239.255.255.255 range. (Not A, Not B)
The 224.0.0.0/8 network range is not intended to be used outside of the local subnet link. (Not D, Not E)

QUESTION 320
Which of the following PIMv2 Sparse mode control messages are also used in PIM Dense mode? (Choose all that apply.)

A. Graft
B. Join
C. Prune
D. Register
E. Assert
F. Hello
G. Register

Answer: B, C, E, F
PIM-DM uses the following PIMV2 messages.
- Hello
- Join/Prune
- Graft
- Graft-Ack
- Assert
PIM-SM uses the following PIMV2 messages
- Hello
- Bootstrap

- Candidate-RP-Advertisement
- Join/Prune
- Assert
- Register
- Register-Stop

Reference:
'CCIE Professional Development Routing TCP/IP Volume 2' in the section 'Understanding IP Multicast Routing' pages 475 and 488.

QUESTION 321
What best describes the Source Specific Multicast (SSM) functionality?

A. SSM is an extension of the DVMRP protocol that allows for an efficient data delivery mechanism in one-to-many communications.
B. SSM requires MSDP to discover the active sources in other PIM domains.
C. In SSM routing of multicast traffic is entirely accomplished with source trees. The RP is used to direct receivers to the appropriate source tree.
D. Using SSM, the receiver application can signal its intention to join a particular source by using the INCLUDE mode in IGMPv3.
E. None of the above

Answer: D

Explanation:
The Internet Standard Multicast (ISM) service is described in RFC 1112, Host Extensions for IP Multicasting. This service consists of the delivery of IP datagrams from any source to a group of receivers called the multicast host group. The datagram traffic for the multicast host group consists of datagrams with an arbitrary IP unicast source address S and the multicast group address G as the IP destination address. Systems will receive this traffic by becoming members of the host group. Membership to a host group simply requires signalling the host group through IGMP Version 1, 2, or 3.
In SSM, delivery of datagrams is based on (S, G) channels. Traffic for one (S, G) channel consists of datagrams with an IP unicast source address S and the multicast group address G as the IP destination address. Systems will receive this traffic by becoming members of the (S, G) channel. In both SSM and ISM, no signalling is required to become a source. However, in SSM, receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources. In other words, receivers can receive traffic only from (S, G) channels to which they are subscribed, whereas in ISM, receivers need not know the IP addresses of sources from which they receive their traffic. The proposed standard approach for channel subscription signalling utilizes IGMP INCLUDE mode membership reports, which are supported only in IGMPv3.
Incorrect Answers:

A. SSM is associated with PIM in IPv6 multicast networks. It is not associated with DVMP.
B. SSM builds off of PIM-SM, but also requires an update to IGMP. IGMP version 3

includes a larger header, where the source address can be specified, in addition to the group address. This means that a router no longer needs to communicate with an RP in order to locate the source, and also means that MSDP is no longer needed since its only purpose is to pass information among RPs.
C. PIM-SSM is made possible by IGMPv3. Because hosts can now indicate interest in specific sources using IGMPv3, PIM can create state directly along the path to those sources using SSM. SSM does not require a rendezvous point (RP) to operate.

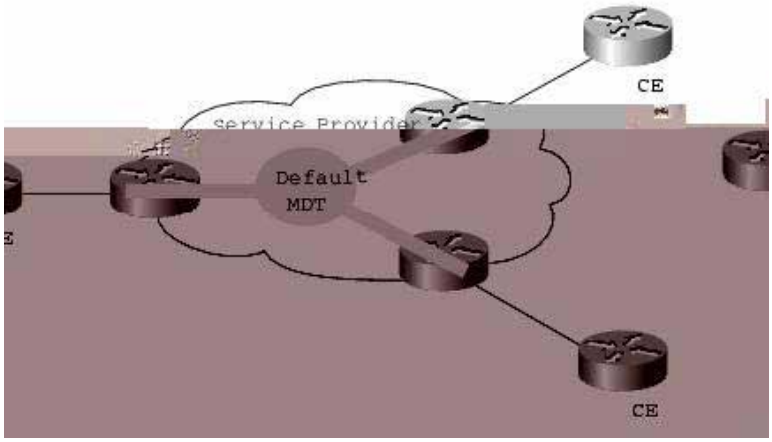
QUESTION 322
The Certkiller network is setting up a VPN for the IP multicast traffic. What best describes the MDT role in MVPN operations?

A. PE routers that have CE routers who are intended recipients of the data only join data MDT. PE routers signal use of data-MDT via a UDP packet on port 3232, which is sent via the default MDT: This packet contains an all-PIM routers message, indicating the group is joined if required.
B. CE routers do not have a PIM adjacency across the provider network with remote CE routers, but rather have an adjacency with their local routes an the PE router. When the PE router receives an MDT packet. It performs an RPF check. During the transmission of the packet through the Provider network, the normal RPF rules apply. However, at the remote's PE, the router needs to ensure that the originating PE router was the correct one for that CE. It does this by checking the BGP next hop address of the customer's packet's source address. This next hop address should be the source address of the MDT packet. The PE also checks that there is a PIM neighbor relationship with the remote PE.
C. A unique Group address is required to be used as MDT for each particular customer. A unique source address for the Multicast packet in the provider network is also required. This source address is recommended to be the address of the loopback interface, which is used as the source for the IBGP, as this address is used for the RPF check at remote PE.
D. PE routers are the only routers that need to be MVPN aware and able to signal to remote PE's information regarding the MVPN. It is therefore fundamental that all PE routers have a BGP relationship with each other. Either directly or via a Route Reflector. The source address of the Default-MDT will be the same address used to source the IBGP sessions with the remote PE routers that belong to the same VPN and MVRF.
E. All of the above.

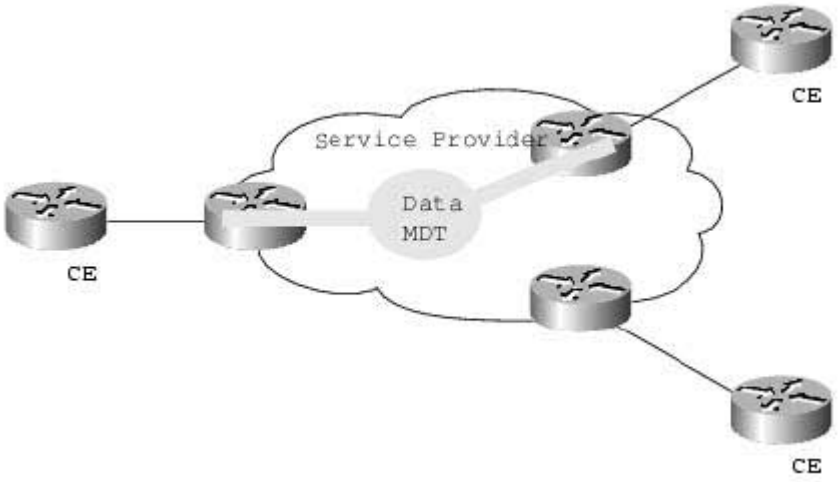
Answer: E

Explanation:
Cisco MVPN Details:
While there are significant deployment obstacles to each of the preceding MVPN solutions, Multicast Domains is the most attractive alternative because:
1. The provider must configure a native IP multicast network within their core network; this includes both the P and PE routers.
2. IP Multicast is a mature technology that has been deployed since Cisco IOS Software 10.0. This minimizes risk for the provider network, because a new feature will not have to be introduced into its core to support MVPNs.

Multicast Domain Solution
This method originally had less than optimal performance, because it requires that all PE routers connected to a customer receive all of that customer's Multicast data regardless of the presence of an interested receiver in that location. When enhancements resolved this characteristic with a new methodology, it became a truly attractive solution.
Figure 3
Default MDT Concept

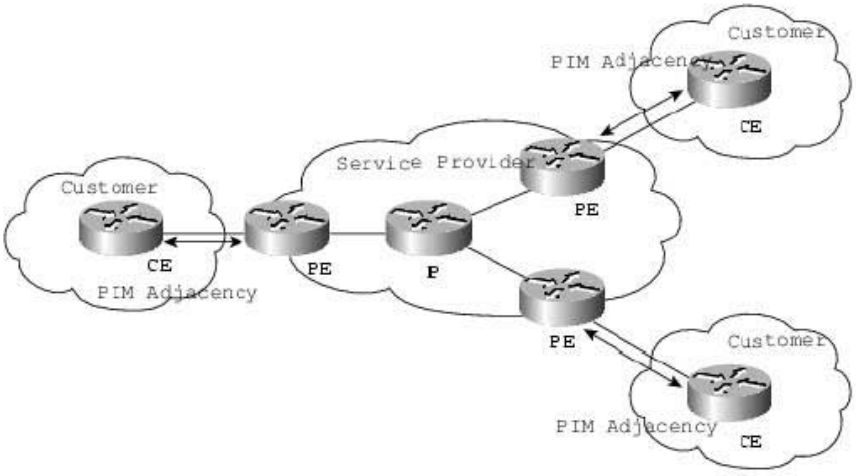


The aforementioned enhancement is the addition of ephemeral trees that are created `on the fly'. These trees distribute multicast group data that exceeds a certain configured threshold of Bandwidth (BW) to only those PE who have joined this new tree. These are tress are called MDT-data trees. The word data is appended as these groups are designed to be used for groups that will require a higher amount of bandwidth to deliver their data.
Figure 4
Data MDT Concept

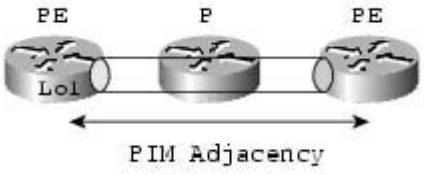


This diagram indicates that the Data MDT is only joined by those PE routers that have CE routers who are intended recipients of the data.
PE routers signal use of Data-MDT via a UDP packet on port number 3232, which is sent via the default MDT. This packet contains an all-PIM routers message, indicating the group to be joined if required.
Interaction of Customer and Providers Multicast Network

It is important to remember that the customer's IP Multicast network has no relationship to the provider's multicast network. From the perspective of the provider, the customer's IP Multicast packets are merely data to the provider's distinctive IP Multicast network.
It is important to understand that PIM, and in particular PIM-SM, are the only supported multicast protocols for MVPN. Bi-Dir PIM may be supported in the future, when it is deemed stable enough for the core of a provider network.
Figure 5
Customer PIM Adjacencies



CE routers do not have a PIM adjacency across the provider network with remote CE routers, but rather have an adjacency with their local routers and the PE router.
When the PE router receives an MDT packet, it performs an RPF check. During the transmission of the packet through the Provider network, the normal RPF rules apply. However, at the remote's PE, the router needs to ensure that the originating PE router was the correct one for that CE. It does this by checking the BGP next hop address of the customer's packet's source address. This next hop address should be the source address of the MDT packet. The PE also checks that there is a PIM neighbourship with the remote PE.
Currently, only a single MVRF is supported per customer. This limitation precludes the customer also receiving Internet or any other outside domain's Multicast traffic
A unique Group address is required to be used as MDT for each particular customer. A unique source address for the Multicast packet in the provider network is also required. This source address is recommended to be the address of the loopback interface, which is used as the source for the IBGP, as this address is used for the RPF check at remotePE.
If the provider uses MDT-data groups, then these will also need to be configured. These MDT-data groups must be unique for each customer.
The PE routers must have a PIM adjacency to each other. No other routing protocols may use these MTIs.
Figure 6
Provider's PIM Adjacencies



BGP Requirements
PE routers are the only routers that need to be MVPN aware and able to signal to remote PE's information regarding the MVPN. It is therefore fundamental that all PE routers have a BGP relationship with each other. Either directly or via a Route Reflector.
The source address of the Default-MDT will be the same address used to source the iBGP sessions with the remote PE routers that belong to the same VPN and MVRF.
When PIM-SSM is used for transport inside the provider core, it is via this BGP relationship that the PEs indicate that they are MVPN capable and provide for source discovery. This capability is indicated via the updated BGP message.
Reference:
http://www.cisco.com/en/US/tech/ CK8 28/technologies_white_paper09186a00800a3db6.shtml

---

QUESTION 323
An enterprise customer runs their core network as an ISP network where they have different Autonomous Systems (AS). The BGP core runs OSPF for Intra-connection only. Data center A is in AS 1, data center B is in AS 2, and data center C is in AS 3. The remote locations will be running an IGP and redistribute their routes into BGP core. They would like to enable multicast throughout their network to support multicast applications.
Based upon the scenario, what would be the LEAST EFFECTIVE way to implement IP multicast?

A. This network runs essentially as an ISP's network with a BGP core and different AS. To implement multicast in this network they can enable MBGP over the BGP backbone.
B. This is customer's internal network and not a transit provider in the inter-domain SP routing. As log as there is no incongruence (between multicast and unicast topologies), there is no need to run MBGP. They simply run PIM-SM and MSDP for redundancy.
C. Running MBGP, besides BGP, should present negligible overhead and if done together with the introduction of IP multicast will help to avoid problems later on when the network has grown and some incongruence needs to be supported. At that point, the customer may need to upgrade to MBGP throughout the network to have the transitive nature of incongruence supported correctly, and this may then become an obstacle in deployment. Therefore, MBGP should be implemented.
D. It should be determined what IP multicast applications the customer is intending to run. Source Specific Multicast (SSM) should be recommended to the customer, since it would allow them to overcome MSDP and thus reduce the complexity of IP multicast in their deployment.
E. PIM uses the unicast routing information to perform the multicast forwarding function. They can simply implement Inter AS PIM to exchange the multicast routing information. This would be the easiest way to implement multicast in the current network where they leverage all the current unicast routing protocol information to populate the multicast

routing table, including Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest path First (OSPF), Border Gateway Protocol (BGP), and static routes. This approach would also cause less processing on the routers as PIM does not send and receive routing updates between routers.

Answer: B

Explanation:
The Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple PIM sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous point(s) in different domains. Each PIM-SM domain uses its own rendezvous points and does not need to depend on them in other domains. A rendezvous point runs MSDP over TCP to discover multicast sources in other domains. MSDP is also used to announce sources sending to a group. These announcements must originate at the domain's Rendezvous Point. MSDP depends heavily on MP-BGP for interdomain operation. Because of this, choice B is the least effective choice since it recommends running MSDP without MGBP.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/mbgp.htm

---

QUESTION 324
Certkiller .com runs a large IP multicast network with thousands of sources and thousands of groups and uses (S, G) entries for forwarding. The applications that are using IP multicast do not require a minimum latency and there is a sever impact on resources on routers and high memory consumption from the size of the multicast routing table.
What would be the right solution in this particular scenario which will decrease the resource issues on the routers, reduce the amount of memory needed by the large multicast routing tables and minimize the amount of state in each router?

A. Continue using (S, G) entries but add a rendezvous point (RP) in the topology
B. Use (*,G) entries with sources trees and a rendezvous point (RP) in the topology
C. Use shared trees with a rendezvous point (RP) in the topology
D. Use combination of source trees and shared trees without rendezvous point (RP) in the topology
E. Use PIM Sparse mode with (S,G) and (*,G) entries

Answer: C

Explanation:
Shortest path trees have the advantage of creating the optimal path between the source and the receivers. This guarantees the minimum amount of network latency for forwarding multicast traffic. This optimization does come with a price, though: The routers must maintain path information for each source. In a network that has thousands of sources and thousands of groups, this can quickly become a resource issue on the routers. Memory consumption from the size of the multicast routing table is a factor that

network designers must take into consideration.
Unlike source trees that have their root at the source, shared trees use a single common root placed at some chosen point in the network. This shared root is called the rendezvous point (RP).Shared trees have the advantage of requiring the minimum amount of state in each router. This lowers the overall memory requirements for a network that allows only shared trees. The disadvantage of shared trees is that, under certain circumstances, the paths between the source and receivers might not be the optimal paths-which might introduce some latency in packet delivery. Network designers must carefully consider the placement of the RP when implementing an environment with only shared trees.
Incorrect Answers:
A, E: Because of the potentially large number of difference multicast sources in this particular network, the use of individual (S, G) entries should be avoided.
B, D: The simplest form of a multicast distribution tree is a source tree whose root is the source of the multicast tree and whose branches form a spanning tree through the network to the receivers. Because this tree uses the shortest path through the network, it is also referred to as a shortest path tree (SPT). The shortest-path tree requires more memory than the shared tree, but reduces delay. Because we want to reduce the amount of memory needed, these choices are incorrect.
Reference:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ipmulti.htm#xtocid18

QUESTION 325
In the Certkiller IP multicast network with many sources which are also receivers, what protocol is used to allow the use of the same shared tree for traffic from sources towards RP and from RP towards receivers?

A. PIM Dense Mode (PIM DM)
B. PIM Sparse Mode (PIM SM)
C. Bidirectional PIM
C. Distance Vector Multicast Routing Protocol (DVMRP)
D. Multicast Open Shortest Path First (MOSPF)

Answer: C

Explanation:
Bidirectional-PIM is a variant of the Protocol Independent Multicast (PIM) suite of routing protocols for IP multicast. In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco IOS implementation of PIM supports three modes for a multicast group:
1. Bidirectional mode
2. Dense mode
3. Sparse mode
A router can simultaneously support all three modes or any combination of them for different multicast groups. In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In

bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address need not be a router, but can be any unassigned IP address on a network that is reachable throughout the PIM domain.

Figure1: Unidirectional Shared Tree and Source Tree

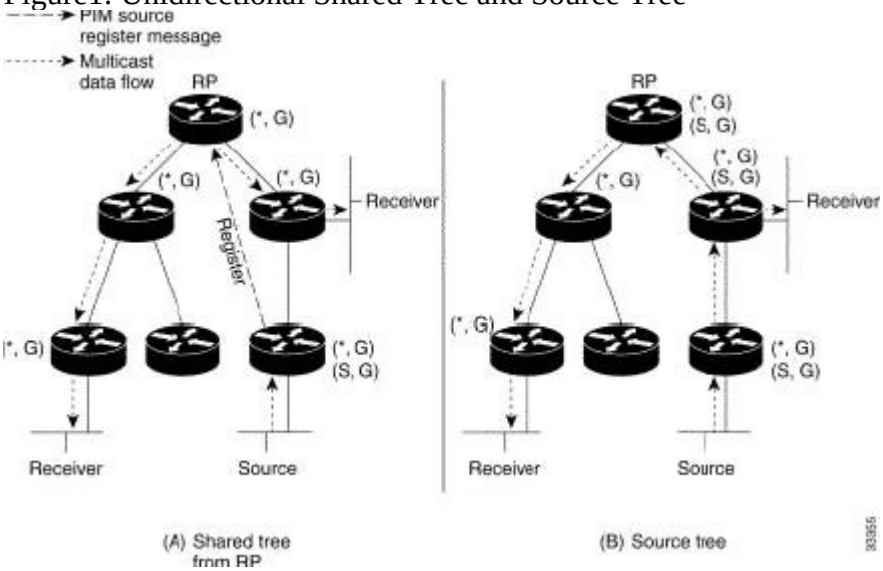
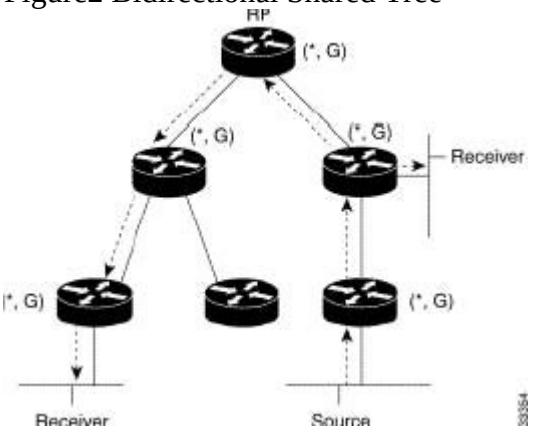


Figure2 Bidirectional Shared Tree



Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1612/products_feature_guide09186a0080080a41.html

---

QUESTION 326
Which of the following is used to calculate the upstream neighbor interface for a multicast route entry in a PIMv2 Sparse Mode network?

A. The address of the Mapping Agent.
B. The address of a directly connected member of the multicast group.
C. The address of the currently active Rendezvous Point for the multicast group.
D. The address of the PIM neighbor that sent the PIM Join message.
E. The address of the PIM neighbor that sent the PIM Hello message.

Answer: C

Explanation:
The address of the upstream neighbor in any PIMv2 Sparse Mode network is always calculated via the neighbor closest to the Rendezvous Point (RP).
Incorrect Answers:

A. The upstream neighbor for a multicast group is calculated from the RP, not the mapping agent.
B. The directly connected multicast neighbor would only be used if it were the nearest upstream neighbor toward the RP, which will not always be the case.
D, E. The neighbor that sends the PIM messages is not necessarily going to be the same neighbor that is upstream toward the RP, so these choices are also incorrect.
Reference:
CCIE Professional Development Routing TCP/IP Volume II by Jeff Doyle and Jennifer De Haven Carroll, Page 492.

QUESTION 327
What single choice listed below best describes PIM functionality?

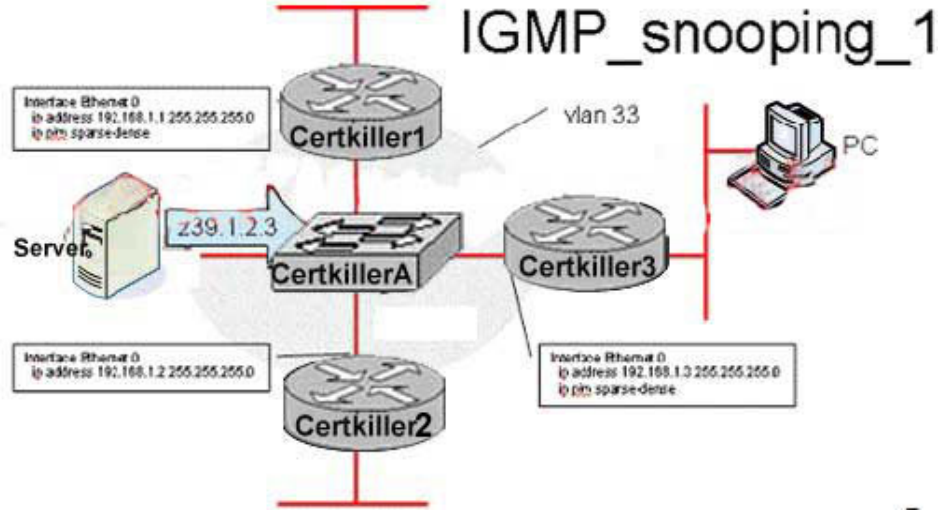
A. PIM uses the multicast routing information to perform the multicast forwarding function. PIM is a multicast routing protocol, and uses the multicast routing table to perform the RFP check. Like other routing protocols, PIM sends and receives routing updates between routers.
B. PIM uses unicast routing protocol information that populates the unicast routing table, including EIGRP, OSPF, BGP, and static routes.
C. PIM uses the multicast and unicast routing information to perform the multicast forwarding function. PIM uses the multicast routing table to perform the RPF check. Like other routing protocols, PIM does not send and receive routing updates between routers.
D. PIM uses multicast routing protocols to populate the multicast routing table, including Distance Vector Multicast Routing Protocol (DVMPR); Multicast OSPF (MOSPF), Multicast BGP
E. PIM uses the unicast routing information to perform the multicast forwarding function. Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the RPF check function instead of building up a completely independent multicast routing table. Unlike other routing protocols, PIM does not send and receive routing updates between routers.

Answer: E

Explanation:
Protocol-independent multicast (PIM) gets its name from the fact that it is IP routing protocol-independent. PIM can leverage whichever unicast routing protocols are used to populate the unicast routing table, including EIGRP, OSPF, BGP, or static routes. PIM uses this unicast routing information to perform the multicast forwarding function, so it is IP protocol-independent. Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the reverse path forwarding (RPF) check

function instead of building up a completely independent multicast routing table. PIM does not send and receive multicast routing updates between routers like other routing protocols do.

QUESTION 328
The Certkiller IP multicast network is shown below:



Which routers will multicast stream (239.1.2.3)?
Note: Switch Certkiller A is a catalyst running IGMP snooping. (Choose two)

A. Certkiller 1
B. Certkiller 2
C. Certkiller 3
D. IGMP snooping does not know receiver in vlan 33, so switch D will drop the multicast stream.
E. Router Certkiller 2 only after PC joins group 239.1.2.3

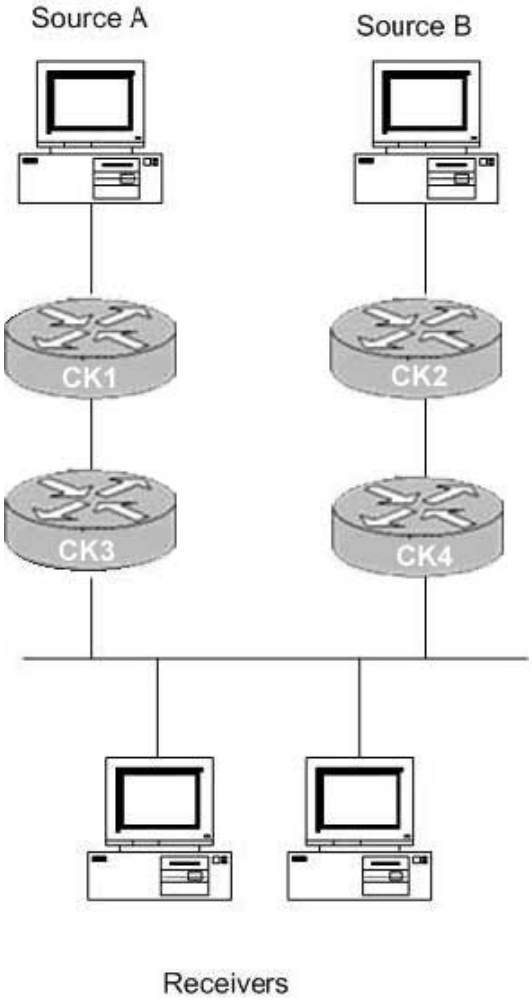
Answer: A, C

Explanation:
Based on the configuration examples shown in the diagram the Ethernet interfaces on router Certkiller 1 and Certkiller 3 are configured for sparse-dense mode. A description of this mode is below:
Sparse-Dense Mode:
An alternative to choosing just dense mode or just sparse mode is to run PIM in a single region in sparse mode for some groups and dense mode for other groups.
In sparse-dense mode, if the group is in dense mode, the interface will be treated as dense mode. If the group is in sparse mode, the interface will be treated in sparse mode. The group is "sparse" if the router knows about an RP for that group.
When an interface is treated in dense mode, it is populated in the outgoing interface list of the multicast routing table when either of the following conditions is true:
Members or DVMRP neighbors are on the interface.
Any of the PIM neighbors on the interface have not pruned for the group.

When an interface is treated in sparse mode, it is populated in the outgoing interface list of the multicast routing table when either of the following conditions is true:
Members or DVMRP neighbors are on the interface.
A PIM neighbor on the interface has received an explicit join message.
Since there is no information regarding the use of a RP we can safely assume that the interfaces would operate in Dense mode, therefore both Certkiller 1 and Certkiller 3 would stream these multicast messages.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800c

---

QUESTION 329
The Certkiller network is shown in the following exhibit:



Router CK1 is configured as follows:
ip multicast-routing
interface loopback0
ip address 192.168.1.1 255.255.255.0
ip pim send-RP-announce loopback0 scope 16 group-list 1
ip pim send-RP-discovery loopback0 scope 16

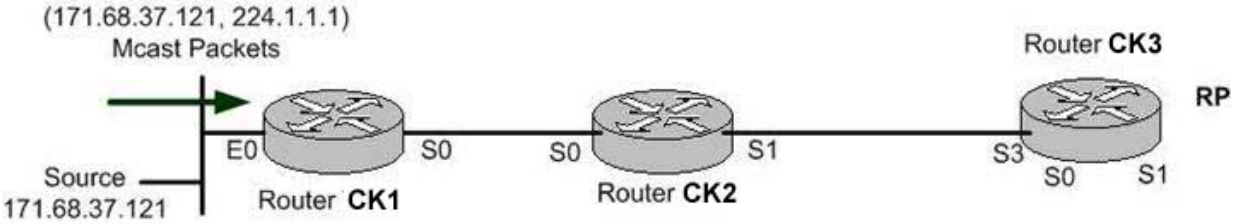
access-list 1 permit 239.0.0.0 0.255.255.255
Router CK2 is configured as follows:
ip multicast-routing
interface loopback 0
ip address 192.168.11.1 255.255.255.0
ip pim send-RP-announce loopback0 scope 16 group-list 1
ip pim send-RP-discovery loopback0 scope 16
access-list 1 permit 239.0.0.0 0.255.255.255
Which of the routers will take on the function of Mapping Agent and source Auto-RP Discovery messages to the 224.0.1.40 group?

A. Router CK1
B. Router CK2
C. Both Router CK1 and Router CK2
D. Neither, since the access lists configured do not match 224.0.1.40 multicast traffic.

Answer: C

Explanation:
If several RPs announce themselves for a multicast group range, the mapping agent chooses only one, which is the RP with the highest IP address. However, this is for selecting the RP. There is no election process for selecting the mapping agent that will source auto-RP discovery message. Both A and B will source this message.
Incorrect Answers:
A, B. If only one router were elected as a mapping agent, this would adversely affect the other source, since it would not have a mapping agent.
B. This would be the correct choice if the question were related to the RP election, and not the mapping agent election. When multiple routers contend to be the Rendezvous Point, the router with the highest IP address wins the tie-breaker and will be elected as the RP. However, there can be multiple mapping agents in the network, as would be the case in this situation.
D. All PIM-enabled routers automatically join the Cisco RP discovery group (224.0.1.40) that allows them to receive all group-to-RP mapping information. This information is distributed by an entity called RP mapping agent. Therefore, the access list is irrelevant in this case.

QUESTION 330
The Certkiller network is shown in the following exhibit:



While troubleshooting a problem with the IP multicast network, you see the following on router CK1 :

(*, 224.1.1.1), 00:00:03/00:00:00, RP 171.68.28.140, flags: SP
Incoming interface: Serial0, RPF nbr 171.68.28.191,
Outgoing interfaces list: Null
(171.68.37.121/32, 224.1.1.1), 00:00:03/00:02:56, flags FPT
Incoming interface: Ethernet0, RPF nbr 0.0.0.0, Registering
Outgoing interface list: Null
Which of the following could be the cause of the "Registering" condition on CK1 ?
(Choose all that apply)

A. Router CK1 has incorrectly calculated the RPF interface for the source (171.68.37.121) as Serial1.
B. Router CK3 (RP) failed to send a "Register-Stop" message to Router CK2 .
C. Router CK2 is IGMP version 1 while Router CK1 is an IGMP version 2 speaker.
D. PIM is not enabled on Router CK2 .
E. Registering is the normal operational status of an operational multicast session.

Answer: B, D

Explanation:
The Rendezvous Point will need to send a "Register Stop" in order to clear the registration process, and all routers in between the RP and the multicast source must be multicast enabled.
Incorrect Answers:

A. The output shows that this is not the problem, as router CK1 is correctly calculating the incoming interface as Ethernet 0.
C. IGMP is used by hosts, and IGMP version 2 is backwards compatible with version 1.
Reference:
Developing IP Multicast Networks, (from page 259, PIM register process).

QUESTION 331
What interface command must be configured for auto-rp to function properly?

A. ip pim dense-mode
B. ip pim sparse-dense-mode
C. ip pim sparse-mode
D. ip multicast helper

Answer: B

Explanation:
RPs are used by senders to a multicast group to announce their existence and by receivers of multicast packets to learn about new senders.
Auto-RP is a feature that automates the distribution of group-to-RP mappings in a PIM network. Auto-RP has the following benefits:
Configuring the use of multiple RPs within a network to serve different group ranges is

easy.
Auto-RP allows load splitting among different RPs and arrangement of RPs according to the location of group participants.
Auto-RP avoids inconsistent, manual RP configurations that can cause connectivity problems.
Example configuration using Auto-RP:
ip multicast-routing
interface ethernet 0/0
ip pim sparse-dense-mode
ip pim send-rp-announce ethernet 0 scope 16 group-list 1
ip pim rp-address 10.8.0.20 1
Incorrect Answers:

A. Rendezvous points are used in sparse mode multicasts, not dense mode.
C. If router interfaces are configured in sparse mode only a static RP address must also configured.
D. This is an invalid command.

QUESTION 332
The Certkiller network is utilizing IP multicast technology. Along with this, router CK1 is configured as an anycast Rendezvous Point (RP). What best describes the functionality of Anycast RP?

A. Anycast RP is a useful application of MSDP, MBGP and SSM that configures a multicast sparse mode network to provide for fault tolerance and load sharing within a single multicast domain.
B. Only a maximum of two RPs are configured with the same IP address (for example, 10.0.0.10) on loopback interfaces. The loopback address should not be configured as a host address (with a 32-bit mask). All the downstream routers are configured so that they know that 10.0.0.10 is the IP address of their local RP.
C. IP routing automatically selects the topologically closest RP for each source and receiver. Because some sources use only one RP and some receivers a different RP, MBGP enables RPs to exchange information about active sources. All the RPs are configured to be MSDP peers of each other.
D. Each RP will know about the active sources in its own area. If RP fails, IP routing converges and backup RP would become the active RP os this areas using HSRP.
E. Anycast RP is an implementation strategy that allows load sharing and redundancy in PIM sparse mode (PIM-SM) networks by configuring two or more RPs that have the same IP asddress anda CK using Multicast Source Discovery Protocol to share active source information.

Answer: E

Explanation:
IP multicast is deployed as an integral component in mission-critical networked applications throughout the world. These applications must be robust, hardened, and

scalable to deliver the reliability that users demand.
Using Anycast RP is an implementation strategy that provides load sharing and redundancy in Protocol Independent Multicast sparse mode (PIM-SM) networks. Anycast RP allows two or more rendezvous points (RPs) to share the load for source registration and the ability to act as hot backup routers for each other. Multicast Source Discovery Protocol (MSDP) is the key protocol that makes Anycast RP possible.
The main purpose of an Anycast RP implementation is that the downstream multicast routers will "see" just one address for an RP.
Reference:
http://www.cisco.com/en/US/tech/ CK8 28/technologies_white_paper09186a00800d6b60.shtml#57583

QUESTION 333
The Certkiller network is using multicasting for corporate video training sessions. All routers in the Certkiller network are enabled for IP multicast. How are these video streaming multicast packets forwarded by these routers? (Choose all that apply)

A. When a multicast packet arrives at a router, the router performs a Reverse Path forwarding (RPF) check on the packet. If the RPF check succeeds, the packet is forwarded, otherwise, it is dropped.
B. When traffic is flowing down the source tree the router looks up the source address in the unicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the source, if the packet has arrived on the interface leading back to source, the RPF check succeeds and the packets is forward. Otherwise, it is dropped.
C. When traffic is flowing down the source tree the router looks up the source address in the multicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the source. If the packet has arrived on the interface leading back to the source, the RPF check successfully the packets is forwarded. Otherwise, it is dropped.
D. When traffic is flowing down the source tree the router looks up the source address in the multicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the source and forward path to the receiver. If the reverse path and forward path is found successfully the packet is forwarded. Otherwise, it is dropped.
E. When a multicast packet arrives at a router, the router does not have to perform an RPF check on the packet. The router looks up the source address in the unicast routing table to determine if the destination path is present. If this succeeds the packet is forwarded. Otherwise, it is dropped.

Answer: A, B

Explanation:
Multicast Forwarding
In unicast routing, traffic is routed through the network along a single path from the source to the destination host. A unicast router does not consider the source address; it considers only the destination address and how to forward the traffic toward that destination. The router scans through its routing table for the destination address and then forwards a single copy of the unicast packet out the correct interface in the direction of

the destination.
In multicast forwarding, the source is sending traffic to an arbitrary group of hosts that are represented by a multicast group address. The multicast router must determine which direction is the upstream direction (toward the source) and which one is the downstream direction (or directions). If there are multiple downstream paths, the router replicates the packet and forwards it down the appropriate downstream paths (best unicast route metric)-which is not necessarily all paths. Forwarding multicast traffic away from the source, rather than to the receiver, is called Reverse Path Forwarding (RPF). RPF is described in the following section.
Reverse Path Forwarding (RPF)
PIM uses the unicast routing information to create a distribution tree along the reverse path from the receivers towards the source. The multicast routers then forward packets along the distribution tree from the source to the receivers. RPF is a key concept in multicast forwarding. It enables routers to correctly forward multicast traffic down the distribution tree. RPF makes use of the existing unicast routing table to determine the upstream and downstream neighbors. A router will forward a multicast packet only if it is received on the upstream interface. This RPF check helps to guarantee that the distribution tree will be loop-free.
RPF Check
When a multicast packet arrives at a router, the router performs an RPF check on the packet. If the RPF check succeeds, the packet is forwarded. Otherwise, it is dropped.
For traffic flowing down a source tree, the RPF check procedure works as follows:
1. The router looks up the source address in the unicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the source.
2. If the packet has arrived on the interface leading back to the source, the RPF check succeeds and the packet is forwarded.
3. If the RPF check in Step 2 fails, the packet is dropped.
Incorrect Answers:
C, D. The RPF lookup is done on the unicast routing table, not the multicast routing table.
E. RPF checks must be done in order to maintain a loop free multicast topology.

QUESTION 334
While troubleshooting an IP multicast issue, you issue the "show ip mroute" command:
Router#show ip mroute 236.2.3.23
IP Multicast Routing table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P -
Pruned
R - RP-bit set, F - Register flag, T - SPT-bit set, J - JOIN SPT
X - Proxy Join Timer Running
Timers: uptime/Expires
Interface state: Interface, next-hop or VCD, State/Mode
(*, 236.2.3.23), 00:09:49/00:04:23 RP 10.1.24.1, flags: SC
Incoming interface: Serial1.708, RPF nbr 10.1.20.2
Outgoing interface list:
Ethernet0, Forward/Sparse, 00:09:50/00:04:12

You are trying to trace this multicast address back to the source of this multicast shared tree. Based on the information above, what is the IP address of the upstream neighbor?

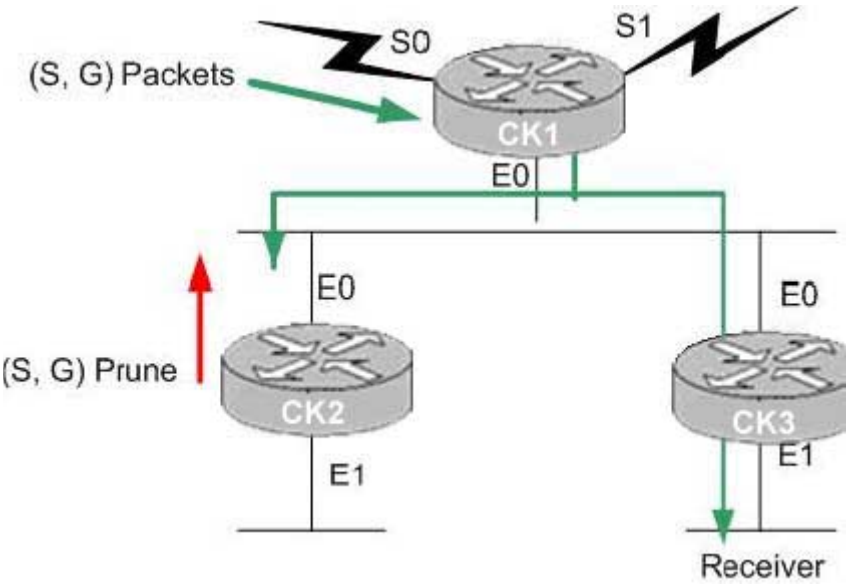
A. 10.1.24.1
B. 10.1.24.2
C. 10.1.20.2
D. 10.1.20.3
E. 236.2.3.23

Answer: C

Explanation:
The upstream neighbor is the IP address associated with the Reverse Path Forwarding Neighbor (RPF nbr), which is 10.1.20.2 in this case.
Incorrect Answers:

A. 10.1.24.1 is the IP address of the Rendezvous Point in this example, not the upstream neighbor.
E. 236.2.3.23 is the IP address of the IP multicast session.

QUESTION 335
Part of the Certkiller IP multicast network is shown below:



Router CK2 sends a (S, G) Prune message to the LAN segment. Will this cause router CK1 to stop the multicast flow to router CK3 ?

A. No. After seeing the Prune message from router CK2 , Router CK3 will send a Join message to router CK1 to override the Prune.
B. No. After seeing the Prune message from router CK2 , Router CK3 will send a Join message to router CK2 to override the Prune.
C. No. After seeing the Prune message from router CK2 , Router CK3 will send a Graft message to router CK2 to override the Prune from router CK2 .

D. Yes. Router CK3 will need to send a new Join message to re-join the multicast session.
E. It depends on whether the routers are IGMP version 1 or IGMP version 2.

Answer: A

Explanation:
After a prune, the router waits for joins, if none arrive, then the router drops the Group. In this case, router CK1 will hear the Join message from CK3 to prevent the flow of multicast traffic from being cut off to CK3 .
Incorrect Answers:
B. Router CK2 will send a Join message to the upstream neighbor, which is CK1 in this case, not CK2 .
C. No graft messages will be sent in this case.
E. IGMP versions are irrelevant.

QUESTION 336
What is the primary purpose for the RPF check in IP multicast networks?

A. To establish reverse flow path of multicast traffic from the receiver to the source.
B. To prevent multicast traffic looping through the network.
C. To determine interfaces inclusion in the outgoing interface list.
D. To prevent the movement of unauthorized multicast traffic.

Answer: B

Explanation:
Reverse Path Forwarding (RPF) provides loop avoidance. It is an algorithm used to forward multicast packets. The RPF rules are: If a router receives a datagram on an interface that it uses to send unicast packets to the source of that packet, then the packet has arrived on the RPF interface. If the packet arrives on the RPF interface, a router forwards the packet out the interfaces that are present in the outgoing interface list of a multicast routing table entry. If the packet does not arrive on the RPF interface, the packet is silently discarded.

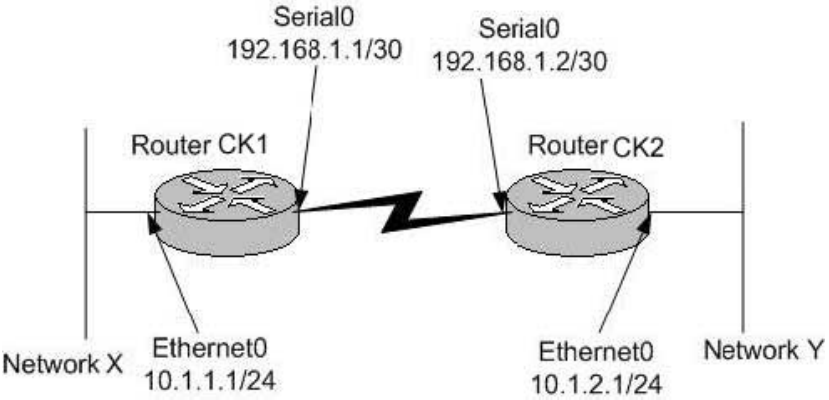
QUESTION 337
Which Multicast Protocols use Reverse Path Forwarding (RPF) information when sending multicast traffic streams to the receivers within the Certkiller network? (Select two)

A. DVMRP
B. PIM Sparse Mode
C. PIM Dense Mode
D. Multicast OSPF
E. PIM Sparse-Dense Mode

Answer: A, C

Explanation:
DVMRP uses a technique known as Reverse Path Forwarding. When a router receives a packet, it floods the packet out of allpaths except the one that leads back to the packet's source. Doing so allows a data stream to reach all LANs (possibly multiple times). If a router is attached to a set of LANs that donot want to receive a particular multicast group, the router can send a "prune" message back up the distribution tree tostopsubsequent packets from traveling where there are no members.
Dense-mode PIM uses Reverse Path Forwarding and looks a lot like DVMRP. The most significant difference between DVMRP and dense-mode PIM is that PIM works with whatever unicast protocol is being used; PIM does not require any particular unicast protocol.
Incorrect Answers:
B. Sparse-mode PIM is optimized for environments where there are many multipoint data streams. Each data stream goes to a relatively small number of the LANs in the internetwork. For these types of groups, Reverse Path Forwarding techniques waste bandwidth. Sparse-mode PIM works by defining a Rendezvous Point. When a sender wants to send data, it first sends to the Rendezvous Point.
D. Multicast OSPF (MOSPF) was defined as an extension to the OSPF unicast routing protocol. OSPF works by having each router in a network understand all of the available links in the network. Each OSPF router calculates routes from itself to all possible destinations.
MOSPF works by including multicast information in OSPF link state advertisements. An MOSPF router learns which multicast groups areactive on which LANs.
MOSPF builds a distribution tree for each source/group pair and computes a tree for active sources sending to the group. The tree state is cached, and trees must be recomputed when alink state change occurs or when the cache times out.

QUESTION 338
The Certkiller network consists of network X and Y that are connected via Router CK1 and Router CK2 . The Certkiller network is shown in the following exhibit:



You wish to set up an IPSec VPN between routers CK1 and CK2 . Now, which of the following crypto access-lists must be configured on Router CK1 in order to send LAN to LAN traffic across the encrypted VPN tunnel?

A. access-list 101 permit ip host 192.168.1.1 host 192.168.1.2
B. access-list 101 permit ip 10.1.1.0.0.0.0.255 host 192.168.1.2
C. access-list 101 permit ip 10.1.1.0.0.0.0.255 10.1.2.0.0.0.0.255
D. access-list 101 permit ip 10.1.1.0.0.0.0.255 10.1.2.0.0.0.0.255
access-list 101 permit ip 10.1.2.0.0.0.0.255 10.1.1.0.0.0.0.255
E. access-list 10 permit ip 10.1.1.0.0.0.0.255 10.1.2.0.0.0.0.255

Answer: C

Explanation:
The format of the command for configuring IPSec is shown below:
access-list 101 permit "Source Network Addresses on X" "Destination Network Subnets on Y"
Incorrect Answers:

A. You define the traffic that is to be sent over the encrypted tunnel, which is all traffic from subnet X to subnet Y, not the serial interfaces.
B. This would only be useful for traffic going from subnet X to the serial interface of CK2 , not for LAN to LAN traffic.
D. You only need to specify the traffic from X to Y on router CK1 , as this is the traffic that will be encrypted. The second line of this access list would need to be applied to router CK2 only.
E. Access list 100 or higher must be used, as this is an extended access list.

QUESTION 339
You try to perform a traceroute to an Internet destination from your PC, but the Traceroute hangs when it reaches the router. Currently, there is an inbound access-list applied to the serial interface on the Internet router with a single line: "access-list 101 permit tcp any any".
What access-list entry may you need to be added to the access-list in order to get traceroute to work?

A. access-list 101 permit tcp any any
B. access-list 101 permit icmp any any time-exceeded
access-list 101 permit icmp any any port-unreachable
C. access-list 101 permit icmp any any time-exceeded
access-list 101 permit icmp any any echo-reply
D. access-list 101 permit icmp any any echo
access-list 101 permit icmp any any net-unreachable
E. access-list 101 permit udp any any
access-list 101 permit icmp any any protocol-unreachable

Answer: B

Explanation:
Port-unreachable and time-exceeded are the ICMP messages that Cisco traceroute uses,

so these ports must be permitted to allow the traceroute to go through.
Incorrect Answers:
A, C, D, E. None of these options give us both the time-exceeded and port-unreachable ICMP ports that need to be opened in the access list to allow traceroute through.

QUESTION 340
You are writing an access list on a router to prevent users on the Ethernet LAN connected to Ethernet interface 0 from accessing a TFTP server (10.1.1.5) located on the LAN connected to Ethernet interface 1. Which of the following would be the correct configuration change if applying the ACL inbound on the Ethernet 0 interface?

A. access-list 1 deny tcp 0.0.0.0 255.255.255.255 10.1.1.5. 0.0.0.0 eq 69
B. access-list 100 deny tcp 0.0.0.0 255.255.255.255 10.1.1.5. 0.0.0.0 eq 69
C. access-list 100 deny tcp 0.0.0.0 255.255.255.255 10.1.1.5. 0.0.0.0 eq 68
D. access-list 100 deny tcp 10.1.1.5 0.0.0.0 0.0.0.0 255.255.255.255 eq 69
E. access-list 100 deny tcp 0.0.0.0 255.255.255.255 10.1.1.5. 0.0.0.0 eq port 68
F. None of the above

Answer: F

Explanation:
TFTP uses UDP port 69, so choice F would be the correct access list entry. An extended access list is needed when filtering based on source and destination address, as well as layer 4 port information. However, all of the choices listed are filtering based on TCP ports, and since TFTP uses UDP none are correct.
Incorrect Answers:

A. This is an invalid command, since using source and destination information along with port numbers requires an extended access list.
B. This would be the correct choice if UDP was specified as the transport layer protocol instead of TCP.
C, E. In addition to incorrectly specifying TCP instead of UDP, the port number of 68 is also incorrect.
D. The order of the IP address arrangement is incorrect. This access list will block all TCP port 69 traffic sourced from the TFTP server, not destined to it. This choice is also incorrectly using TCP instead of UDP.

QUESTION 341
You wish to allow only telnet traffic to a server with an IP address 10.1.1.100. You add the following access list on the router:
access-list 101 permit tcp any host 10.1.1.100 eq telnet
access-list 101 deny ip any any
You then apply this access list to the inbound direction of the serial interface. Which types of packets will be permitted through the router after this change? (Choose all that apply)

A. A non-fragment packet en route to the server on port 21.
B. A non-initial fragment packet en route to the server on port 23.
C. A non-initial fragment packet passing through to another host that's not 10.1.1.100.
D. A non-initial fragment packet going to the server on port 21.
E. An initial-fragment or non-fragment packet en route to the server on port 23.

Answer: B, D, E

Explanation:
B, E: Telnet (port 23) is permitted by ACL.
D: A non initial fragment destined to the server will indeed be permitted. The reason for this is that the first line of ACL has some L3 and some L4 information which needs to be matched for a packet to be permitted.
Since a non initial frame matches the L3 information it will pass the layer 3 check. Moreover, since it isa non initial frame it will contain no L4 information in it. Hence the packet will be permitted.
Incorrect Answers:
A, C. For non-initial fragments, only telnet packets going to the 10.1.1.100 address will be allowed.

QUESTION 342
The following access list is configured on router CK1 :
access-list 100 deny udp 0.0.0.0 255.255.255.255 10.1.1.5 0.0.0.0 eq 69
What does the access-list accomplish?
Note: Assume that all other traffic is permitted with a permit all statement at the end of the access list.

A. It blocks all incoming traffic arriving on E0 from accessing any FTP server.
B. It blocks all incoming traffic, except traffic addresses to 10.1.1.5, from accessing any FTP servers.
C. It blocks all incoming traffic arriving on E0 from accessing the FTP server with an address of 10.1.1.5.
D. It blocks all incoming UDP traffic.
E. This access list is trying to block traffic from accessing a TFTP server. However, this is only half of what is needed to accomplish that. You would also need the following:
access-list deny tcp 0.0.0.0 255.255.255.255 10.1.1.5 0.0.0.0 eq 69

Answer: E

Explanation:
The access list shown above is designed to block UDP port 69 traffic from all sources to the destination device with the IP address of 10.1.1.5. Port 69 is used for TFTP. Both TCP and UDP ports are used with the TFTP application, so in order to block all TFTP traffic another access list block TCP port 69 should also be applied.
Incorrect Answers:
A, B: TFTP traffic is being blocked, not FTP. In addition, this traffic is being blocked

only for traffic destined to a single server, not all traffic.
C. TFTP uses port 69, not FTP. FTP uses ports 20 and 21. Since TFTP uses both TCP and UDP, both ports will need to be filtered.
D. Only UDP port 69 traffic destined to a single server is being filtered, not all UDP traffic.
Reference:http://www.ibiblio.org/security/articles/ports.html

---

QUESTION 343
Private VLANs are set up in a Cisco switch for 3 ports as shown below:
tamer (enable) show pvlan
Primary Secondary Secondary-Type Port
------- --------- -------------- -------
500 501 community 5/37
500 502 isolated 5/38-39
tamer (enable) show pvlan mapping
Port Primary Secondary
---- -------- ---------
15/1 500 501-502
interface vlan 500
ip address 10.10.10.2 255.255.255.0
ip proxy-arp
A PC called CKHost is plugged in to port 5/38, using ip address 10.10.10.137/24. Based on the information above, CKHost has which of the following?

A. Layer 3 connectivity with Port 5/37 and port 5/39.
B. Layer 2 connectivity with Port 5/39 but not with port 5/37.
C. Layer 3 connectivity with Port 5/39 but not with port 5/37.
D. Layer 2 connectivity with Port 5/37 and port 5/39.
E. None of the above.

Answer: A
Private VLAN ports can be one of the following:
1. Promiscuous- A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.
2. Isolated- An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. PVLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic from isolated port is forwarded only to promiscuous ports.
3. Community- Community ports communicate among themselves and with their promiscuous ports. These interfaces are separated at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN.
In this case CKHost is in an isolated VLAN, so it will have complete layer 2 separation from all other ports. However, there is nothing preventing routing from taking place, and with inter-vlan routing CKHost will have layer 3 connectivity to the other ports.

QUESTION 344
The Certkiller network administrator wants to authenticate LAN users attached to ports on the existing Catalyst 6509 switch. In order to do this, the following is configured:
aaa new-model
username myname password abc123
aaa authentication ppp access-dotx local
aaa authentication login access1 local
aaa authentication dotlx default radius
dotlx system-auth-control
tacacs-server host 192.168.1.15 key qvert123
radius-server host 192.168.2.27 key poiuy098
!
interface fastethernet 5/1
dotlx port control auto
What is the effect of the configuration on users attempting to access FastEthernet 5/1?

A. They will be authenticated via ppp using the local database.
B. The will be authenticated via ppp using the server at IP address 192.168.1.15.
C. They will be authenticated via ppp using the server at IP address 192.168.2.27
D. They will be authenticated via 802.1x using the local database.
E. They will be authenticated via 802.1x using the server at IP address 192.168.1.150.
F. They will be authenticated via 802.1x using the server at IP address 192.168.2.27.

Answer: F

Explanation:
When you enable 802.1X port-based authentication, note the following syntax information:
To create a default list that is used when a named list is not specified in the authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.
Enter at least one of these keywords:
group radius-Use the list of all RADIUS servers for authentication.
none-Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.
This example shows how to enable AAA and 802.1X on Fast Ethernet port 5/1:
Router# configure terminal
CK1 (config)# aaa new-model
CK1 (config)# aaa authentication dot1x default group radius
CK1 (config)# dot1x system-auth-control
CK1 (config)# interface fastethernet 5/1
CK1 (config-if)# dot1x port-control auto
CK1 (config-if)# end

In this example, the default 802.1x authentication method is configured to be RADIUS, and the RADIUS server is located at IP address 192.168.2.27.

QUESTION 345
For security reasons, you wish to maintain a degree of logical separation between your servers and the rest of the LAN. The servers should be able to see broadcasts and multicasts only from each other and the default gateway. They should not see this type of traffic from other LAN devices. What kind of ports should be configured for these servers on the Catalyst switch?

A. Span Ports.
B. Private Ports.
C. Community Ports.
D. Isolated Ports.
E. Promiscuous Ports.
F. Access Ports.

Answer: C

Explanation:
Private VLANs provide Layer-2 isolation between ports within the same private VLAN on the Catalyst 6000 family switches. Ports belonging to a private VLAN are associated with a common set of supporting VLANs that are used to create the private VLAN structure.
There are three types of private VLAN ports: promiscuous, isolated, and community. Community ports communicate among themselves and with their promiscuous ports. These ports are isolated at Layer 2 from all other ports in other communities or isolated ports within their private VLAN. They communicate directly only with each other and their default gateway.
Incorrect Answers:

A. SPAN ports are used for network analyzers to capture data packets. They do not provide any level of security between users.
B. This question is an example of a type of private VLAN. However, there is no notion of a private port.
D. A promiscuous port communicates with all other private VLAN ports and is the port used to communicate with devices such as routers, LocalDirector, backup servers, and administrative workstations.
E. An isolated port has complete Layer 2 separation from all other ports within the same private VLAN with the exception of the promiscuous port.
F. Access ports do not exist.

QUESTION 346
Based on the VLAN Access Control List (VACL) configuration below, how many total mask entries are required in the Ternary Content Addressable table?
set security acl ip Control_Access permit host 100.1.1.100

set security acl ip Control_Access deny 100.14.11.0 255.255.255.0
set security acl ip Control_Access permit host 172.16.84.99
set security acl ip Control_Access deny 177.163.4.0 255.255.255.128
set security acl ip Control_Access permit host 72.16.82.3
set security acl ip Control_Access deny host 175.17.1.4
set security acl ip Control_Access permit host 191.169.99.150
set security acl ip Control_Access deny host 191.169.230.1

A. 2
B. 3
C. 4
D. 6
E. 8

Answer: B

Explanation:
There will be 3: One to cover the 6 separate host (255.255.255.255) masks, one for the 255.255.255.128 mask, and the third for the 255.255.255.0 mask.
Ternary CAM (TCAM) is a hardware piece of memory designed for rapid table lookups by the ACL engine on the PFC and PFC2. The ACL engine performs ACL lookups based on packets passing through the switch's hardware. The result of the ACL engine lookup into the TCAM determines how the switch handles a packet. For example, the packet might be permitted or denied. The TCAM has a limited number of entries that are populated with mask values and pattern values.
Incorrect Answers:
A, C. In the example above there are 3 different subnet masks, not 2 or 4.
D. Although there are 6 different entries with host masks (255.255.255.255), we need to account for the other two mask entries.
E. Although there are a total of 8 VLAN access control entries in this example, there are only a total of 6 of them share a single mask entry and will be counted as only one in the TCAM.
References:
For a detailed discussion on TCAM refer the link below.
http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a00800c9470.shtml

---

QUESTION 347
With regard to the use of VLAN Access Control Lists (VACL) on a Catalyst 6500 series switch, which of the following are true statements? (Choose all that apply.)

A. VACLs can be used to forward, drop, and redirect traffic based on Layer 2 and Layer 3 information.
B. VACLs cannot be used when using QoS on the switch.
C. VACLs can be used together with router interface access lists.
D. VACLs can be used for traffic that is being Layer 3 switched.
E. VACLs cause extra latency for traffic passing through the switch.

Answer: A, C, D

Explanation:
VACLs are similar to Router/IOS ACLs in terms of their definition, but they are used by Catalyst 6000 family switches to access control all packets it switches, including packets bridged within a VLAN. It can be used to act on layer 2 and 3 information, and can be used in conjunction with RACL's.
Incorrect Answers:
B. VACLs can be used when using QoS on the switch. VACLs cause extra latency for traffic passing through the switch. For a detailed discussion on VACLs please go through the link below.
E. VACLs can be configured on a Catalyst 6500 at L2 without the need for an additional router. They are enforced at wire speed so there is no performance penalty in configuring VACLs on a Catalyst 6500. Since the lookup of VACLs is performed in hardware, regardless of the size of the access list, the forwarding rate remains unchanged.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_6_3/confg_gd/acc_list.htm#1052397

QUESTION 348
A new Catalyst 6500 running Cat OS was recently installed in the Certkiller network. In order to increase the security of your LAN, you configure this Catalyst switch using port security. What statement is true about port security?

A. Port security can be configured on a trunk port.
B. Prot security can be configured on a SPAN destination port.
C. If a security violation occurs, the Link LED for that port turns orange, and a link-down trap is sent to the Simple Network Management Protocol (SNMP) manager.
D. Port security can be configured on a SPAN source port.
E. Static CAM entries can be configured on a port configured with port security.
F. Ports that were disabled due to security violations will be automatically re-enabled when the host with the valid MAC address is re-connected.

Answer: C

Explanation:
Port Security Configuration Guidelines
When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or autoconfigured (learned) on the port. If a MAC address of a device attached to the port differs from the list of secure addresses, the port either shuts down permanently (default mode), shuts down for the time you have specified, or drops incoming packets from the insecure host. The port's behavior depends on how you configure it to respond to a security violation.
If a security violation occurs, the Link LED for that port turns orange, and a link-down trap is sent to the Simple Network Management Protocol (SNMP) manager. An SNMP trap is not sent if you configure the port for restrictive violation mode. A trap is sent only

if you configure the port to shut down during a security violation.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps700/products_configuration_guide_chapter09186a008007f
Incorrect Answers:
A, B, D, E. These incorrect answers can be summarized in the following statements:
1. You cannot configure port security on the trunk port of a 6500 with Cat OS.
2. You cannot enable port security on a SPAN destination port of the 6500 with Cat OS.
3. You cannot configure dynamic, static, or permanent CAM entries on a secure port.
4. When you enable port security on a port, any static or dynamic CAM entries associated with the port are cleared; any currently configured permanent CAM entries are treated as secure.
F. When a port becomes disabled due to a security violation, the switch port can only be enabled again after manual intervention.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007f

---

QUESTION 349
After properly configuring multiple VLANs, a The Certkiller network has decided to increase the security of its VLAN environment. Which of the following can be done on a switched network to enhance security measures? (Choose all that apply).

A. If a port is connected to a "Foreign" device, make sure to disable CDP, DTP, PagP, UDLD, and any other unnecessary protocol, and to enable Uplinkfst/BPDU guard on it.
B. Enable the rootguard feature to prevent a directly or indirectly connected STP-capable device to affect the location of the root bridge.
C. Configure the VTP domains appropriately or turn off VTP altogether if you want to limit or prevent possible undesirable protocol interactions with regard to network-wide VLAN configuration.
D. Disable all unused ports and place them in an unused VLAN to avoid unauthorized access.
E. Set the native VLAN ID to match the port VLAN ID (PVID) of any 802.1Q trunks to prevent spoofing from one VLAN to another.

Answer: B, C, D

Explanation:
The root guard feature is designed to provide a way to enforce the root bridge placement in the network, and to prevent unauthorized devices from becoming the root.
Turning off VTP if it is not used is generally a good idea, as a new switch with a higher ID value that is inserted into the VTP domain can be used to modify and delete all of the VLANs in an existing network.
It is also a best practice to disable and isolate all unused ports, as this will prevent unauthorized users from entering the LAN, and plugging into the network via an unused port.

Incorrect Answers:

A. UDLD is a useful feature that provides no security risks. It is recommended to have this feature enabled. BPDU guard and root guard are similar, but their impact is different. BPDU guard disables the port upon BPDU reception if portfast is enabled on the port. This effectively denies devices behind such ports to participate in STP.
E. If a user's native VLAN I D is the same as the port VLAN ID (PVID) of the 802.1Q trunk, then the user can send frames from his VLAN and have them "hop" to other VLANs. This weakness is part of the 802.1Q specification and does not apply to Cisco ISL trunking ports.
The workaround for this threat is to ensure that every 802.1Q trunking port has a PVID, or native VLAN ID, that is unique throughout the campus network.

QUESTION 350
Passwords for Enterprise guests should normally be:

A. Easy to remember
B. Time limited to the guest visit
C. Be the same as the username
D. Be at least 10 characters
E. Contain uppercase letters

Answer: B

Explanation:
When guest access is required for visitors to the enterprise, the most important security measures that should be taken is to ensure that the guest user access is restricted to only the network resources that are needed, and for the passwords to only be active for the duration of the visit. This will prevent future unauthorized access into the network using these passwords.
Incorrect Answers:

A. Generally, passwords should be somewhat easy to remember for the users, while remaining secure. It is more important to use passwords that are not easily guessed than to provide for an easy to remember one.
C. This should never be done, since it is so easily guessed.
D. Although having enough characters to provide for a secure password is essential, secure passwords can be created with the use of fewer than 10 characters. For regular users, enforcing a rule of long passwords may be preferred, it is generally not necessary for guest access.
E. Although passwords should indeed contain a mix of lower and upper case letters, as well as numerical and special characters, this is not necessarily a requirement for guest users.

QUESTION 351
When segmenting guest traffic across the enterprise wireless network you should

take which of the following approaches?

A. Always give guest traffic higher priority
B. Always give guest traffic lower priority
C. Separate guest traffic as close to the edge as possible
D. Use a firewall
E. Use Access Lists
F. None of the above

Answer: C

Explanation:
You should consider the following implementation criteria before deploying wireless VLANs:
Use policy groups (a set of filters) to map wired polices to the wireless side.
Use IEEE 802.1x to control user access to VLANs by using either RADIUS-based VLAN assignment or RADIUS-based SSID access control.
Use separate VLANs to implement different classes of service.
Adhere to any other criteria specific to your organization's network infrastructure.
Based on these criteria, you could choose to deploy wireless VLANs using the following strategies:
Segmentation by user groups-you can segment your WLAN user community and enforce a different security policy for each user group. For example, you could create three wired and wireless VLANs in an enterprise environment for full- and part-time employees, as well as providing guest access.
Segmentation by device types-You can segment your WLAN to enable different devices with different security levels to access the network. For example, you have hand-held devices that support only 40- or 128-bit static WEP coexisting with other devices using IEEE 802.1x with dynamic WEP in the same ESS. Each of these devices would be isolated into separate VLANs.
For segmenting guest users from the rest of the network, the guest VLAN traffic should be segmented at the network edge, before the traffic reaches the core of the network. This is generally done at the VLAN level, before guest traffic reaches a router access list or firewall.

QUESTION 352
What are the differences between TACACS+ and RADIUS? (Choose all that apply)

A. TACACS+ uses UDP while RADIUS uses TCP for transport.
B. RADIUS and TACACS+ encrypts the entire body of the packet.
C. RADIUS is an IETF standard, while TACACS+ is not.
D. TACACS+ sends a separate request for authorization, while RADIUS uses the same request for authentication and authorization.
E. RADIUS offers multi-protocol support while TACACS+ does not.

Answer: C, D

Explanation:
* RADIUS uses UDP while TACACS+ uses TCP.
* RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted while TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header.
* RADIUS combines authentication and authorization while TACACS+ uses the AAA architecture, which separates authentication, authorization, and accounting.
* TACACS+ offers multiprotocol support while RADIUS does not support AppleTalk Remote Access (ARA) protocol, NetBIOS Frame Protocol Control protocol, Novell Asynchronous Services Interface (NASI) and X.25 PAD connection.
* RADIUS does not allow users to control which commands can be executed on a router and which cannot. Therefore, RADIUS is not as useful for router management or as flexible for terminal services. TACACS+ on the other hand does allow users to control the authorization of router commands on a per-user or per-group basis.
Reference:
TACACS+ and RADIUS Comparison, http://www.cisco.com/warp/public/480/10.html

---

QUESTION 353
You want to prevent all telnet access to your Cisco router. In doing so, you type in the following:
line vty 0 4
no login
password cisco
Will this prevent all telnet access to the router as desired?

A. Yes. The "no login" command disables all telnet access, even though the password is cisco.
B. Yes. The VTY password is needed but not set, so all access will be denied.
C. No. The VTY password is cisco.
D. No. No password is needed for VTY access.
E. No. The password is login.

Answer: D

Explanation:
"No Login" will not prompt users for any initial login, allowing them to access the router without a password.

QUESTION 354
A new TACACS+ server is configured to provide authentication to a NAS for remote access users. A user tries to connect to the network and fails. The NAS reports a FAIL message. What could be the problem? (Choose all that apply).

A. The TACACS+ service is not running on the server.
B. The password for this user is incorrect.

C. The username does not exist in the TACACS+ user database.
D. The NAS server lost its route to the TACACS+ server.
E. The TACACS+ server is down.

Answer: B, C

Explanation:
A FAIL condition is a result of incorrect username/password information. It means that an authentication request was successfully received, but that it had failed.
A FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt1/scdaaa.htm
Incorrect Answers:
A, D, E. These would have resulted in an ERROR condition instead of a FAIL condition. With an error, the NAS would query the next authentication method.

QUESTION 355
While setting up remote access for your network, you type in the "aaa new-model" configuration line in your Cisco router. Which authentication methods have you disabled as a result of this change? (Choose all that apply.)

A. RADIUS
B. RADIUS+
C. Extended TACACS (XTACACS)
D. TACACS
E. TACACS+
F. Kerberos

Answer: C, D

Explanation:
When you enable AAA, you can no longer access the commands to configure the older deprecated protocols, TACACS or Extended TACACS. If you decided to use TACACS or Extended TACACS in your security solution, do not enable AAA.

QUESTION 356
With regard to IPSec, which of the following are true?

A. IPSec supports Multicast.
B. IPSec does not support Multicast.
C. IPSec supports Multicast in IOS 12.x or later.

D. IPSec supports Multicast in IOS 10.x or earlier.
E. IPSec supports Multicast only in combination with GRE tunnels.

Answer: B

Explanation:
IPSec does not support multicast, as secure IPSec tunnels are always between unicast hosts.
Incorrect Answers:
C, D, E. Cisco does not support IPSec protection for multicast traffic on any IOS release.

QUESTION 357
You are setting up a secure connection to another company's device. You are not certain that they are using Cisco so you want your router to manually exchange the RSA public keys between each other. How should you configure your router?

A. Use IPSec with RSA signatures
B. Use IPSec with RSA encrypted nonces
C. Use IPSec with manual keying
D. Use Cisco Encryption Technology
E. Use IPSec using preshared keys
F. Use IPSec using RSA authentication

Answer: C

Explanation:
Manual keying is usually only necessary when configuring a Cisco device to encrypt traffic to another vendor's device, which does not support IKE. If IKE is configurable on both devices, it is preferable to using manual keying.
Incorrect Answers:
A, B, F. In this question we want the keys to be exchanged manually, so this not the best choice.
E. Preshared keys are static keys that do not change, but they can not be keyed manually.
Reference:
Cisco - "Configuring IPSec Manual Keying between Routers"

QUESTION 358
Which of the following are security services provided by IPSec?

A. Data integrity
B. Data origin authentication
C. Data confidentiality
D. Protection for multicast/broadcast traffic
E. Anti-replay

Answer: A, B, C, E

Explanation:
Data integrity, data origin authentication, data confidentiality, and protection from replay are all security features and functions of IPSec
Incorrect Answers:
D. IPSec provides no security against multicast and broadcast traffic. In fact, IPSec does not support multicast traffic.

QUESTION 359
You wish to change the IKE policies of your IPSec configuration in your site to site router VPN. Which of the following are valid ISAKMP policy parameters that can be changed in the configurations?

A. Security Association's lifetime
B. Encryption algorithm
C. Hash algorithm
D. Authentication method
E. Diffie-Hellman group identifier
F. All of the above
G. None of the above

Answer: F
There are five parameters to define in each IKE policy:

Parameter	Accepted Values	Keyword	Default Value
encryption algorithm	56-bit DES-CBC	**des**	56-bit DES-CBC
hash algorithm	SHA-1 (HMAC variant) MD5 (HMAC variant)	**sha** **md5**	SHA-1
authentication method	RSA signatures RSA encrypted nonces pre-shared keys	**rsa-sig** **rsa-encr** **pre-share**	RSA signatures
Diffie-Hellman group identifier	768-bit Diffie-Hellman or 1024-bit Diffie-Hellman	**1** **2**	768-bit Diffie-Hellman
security association's lifetime			

QUESTION 360
Unauthorized access to Cisco devices can be prevented through different privilege level settings. How many of these privilege levels exist?

A. 5
B. 16
C. 4
D. 0
E. 15

Answer: B

Explanation:
There are 16 privilege-levels (0 to 15, inclusive).
Incorrect Answers:

A. This is the default number of vty sessions that can be placed on a router for remote telnet access (vty levels 0-4, inclusive).
E. The highest level is level 15, but we must also count the lowest level (level 0) for a total of 16.

QUESTION 361
Router CK1 has been configured for authentication as shown in the following display:

```
enable secret 483924
!
aaa new-model
username myname password abc123
aaa authentication login default enable
aaa authentication login access1 local
aaa authentication login access2 radius tacacs+
aaa authentication login access3 tacacs+ local
tacacs-server host 192.168.1.15 key qwert123
radius-server host 192.168.2.27 key poiuy098
!
Line console 0
login authentication access3
!
line vty 0 4
password dfgh456
login
```

What method is being used to secure the console port of this router?

A. Authentication is being done using the local database.
B. Authentication is being done using the login password dfgh456.
C. Authentication is being done using the enable password as a default

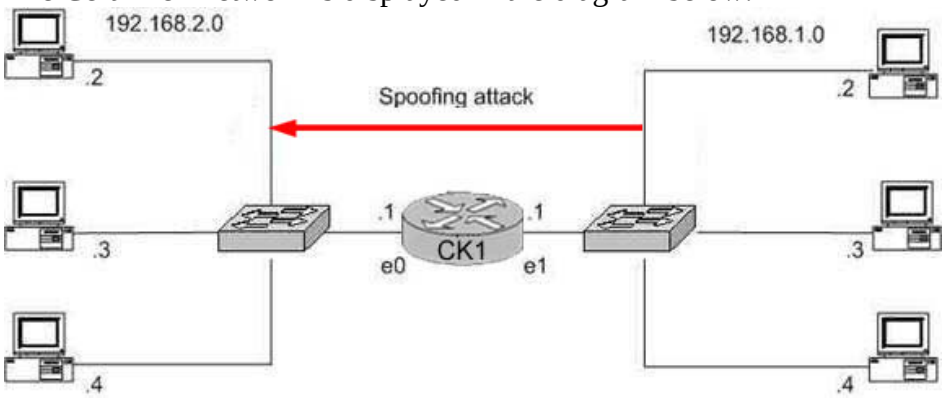
D. Authentication is being done using the server at IP address 192.168.1.15. If a connection to that server fails, the local database will be used.
E. Authentication is being done using the server at IP address 192.168.2.27

Answer: D

Explanation:
The router is using the keyword access3 for authentication for the console port. Access3 points to two different methods for authentication; the first is TACACS+ which is located at 192.168.1.15. If the authentication connection to the server fails, then the local database will be used as a backup.
Incorrect Answers:

A. Based on the configuration file above, TACAS+ is the primary authentication method and the local database is to only be used as a backup method.
B. This is the password that is to be used for Telnet access, not the console password.
C. The enable password is not used, since the login authentication information is taken from the "access3" keyword.
E. This is the IP address of the RADIUS server, not the TACACS+ server.

QUESTION 362
The Certkiller Network is displayed in the diagram below:



You want to block all IP spoofing attacks that originate on the 192.168.1.0 network using a spoofed address outside the 192.168.1.0 range form being sent into the 192.168.2.0 network. However, all other traffic must be permitted. No access lists currently exist on the router. Which of the following configurations would accomplish this task when applied to E1 on CK1 as an input filter?

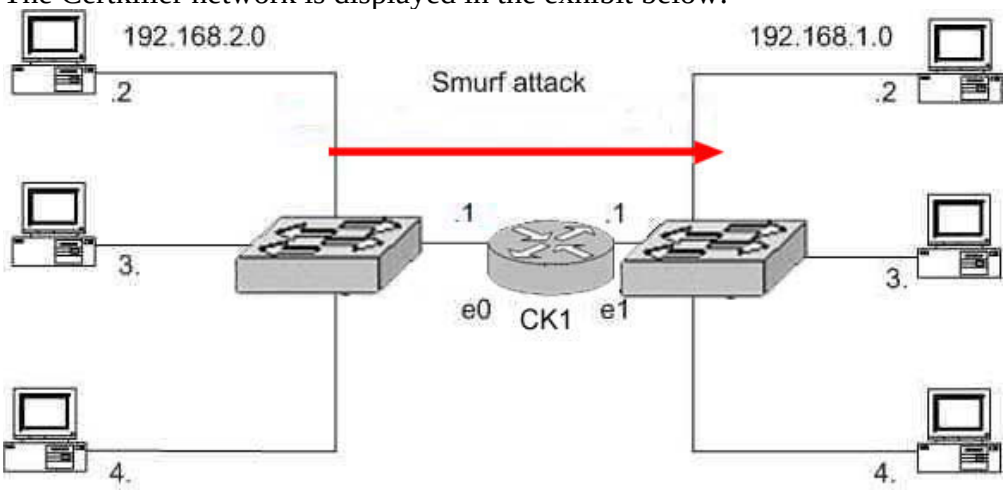
A. access-list 1 permit 192.168.1.0 0.0.0.255
B. access-list 100 permit ip any 192.168.2.0 0.0.0.255
C. access-list 1 deny 192.168.2.0 0.0.0.255
access-list 1 permit any
D. access-list 1 deny 192.168.2.0 0.0.0.255
access-list 1 deny 192.168.1.0 0.0.0.255
access-list 1 permit any
E. access-list 100 deny ip 192.168.2.0 0.0.0.255 any

access-list 100 permit ip any any

Answer: A

Explanation:
The access list in choice A will prevent all incoming traffic sourced from the 192.168.2.0/24 network from interface Ethernet 1 of router CK1 due to the implicit deny all. In the diagram above, hosts on the 192.168.2.0 network should only be a used as a destination for traffic coming from this interface. Only traffic sourced from 192.168.1.0/24 should be seen in the input direction of this interface on CK1 . If any traffic does not match the access list on choice A it could only be the result of a spoofed IP address and should be dropped.
Incorrect Answers:
B. This will allow all traffic (from any source) to reach the 192.168.2.0 network. This will not prevent spoofed IP addresses from the network on E1 to go through.
C. This would prevent spoofed packets that were spoofed only from the 192.168.2.0/24 network. This will not prevent all spoofed addresses outside of the 192.168.1.0 network, as required.
D. This will prevent the two networks from communicating at all.
E. This choice could also be used to prevent the spoofed traffic as required, but it will only prevent spoofed traffic that is IP based. Therefore, the access list in choice C is a better fit for this situation.

QUESTION 363
The Certkiller network is displayed in the exhibit below:



You want to block all Smurf attacks that originate on the 192.168.2.0 network from being sent into the 192.168.1.0 network. However, all other traffic must be permitted. No access lists currently exist on the router. Which of the following configuration excerpt would accomplish this task when applied to E0 on CK1 as an input filter?

A. access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 deny any
B. access-list 1 deny 192.168.1.0 0.0.0.255

access-list 1 permit any
C. access-list 100 permit ip any 192.168.1.0 0.0.0.255
acess-list 100 deny ip any any
D. access-list 100 deny icmp any 192.168.1.255 0.0.0.0 echo
access-list 100 permit icmp any 192.168.1.0 0.0.0.255 echo
eccess-list 100 permit ip any any
E. access-list 100 deny icmp any 192.168.1.255 0.0.0.0 echo-reply
access-list 100 permit icmp any any echo-reply
access-list 100 permit ip any any

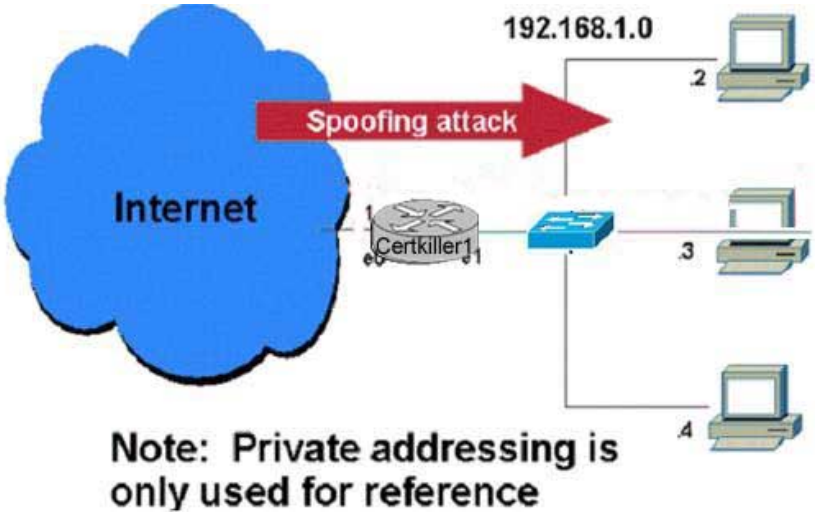
Answer: D

Explanation:
Anatomy of a SMURF Attack
A SMURF attack (named after the program used to perform the attack) is a method by which an attacker can send a moderate amount of traffic and cause a virtual explosion of traffic at the intended target. The method used is as follows:
1. The attacker sends ICMP Echo Request packets where the source IP address has been forged to be that of the target of the attack.
2. The attacker sends these ICMP datagrams to addresses of remote LANs broadcast addresses, using so-called directed broadcast addresses. These datagrams are thus broadcast out on the LANs by the connected router.
3. All the hosts which are "alive" on the LAN each pick up a copy of the ICMP Echo Request datagram (as they should), and sends an ICMP Echo Reply datagram back to what they think is the source. If many hosts are "alive" on the LAN, the amplification factor can be considerably (100+ is not uncommon).
4. The attacker can use largish packets (typically up to ethernet maximum) to increase the "effectiveness" of the attack, and the faster network connection the attacker has, the more damage he can inflict on the target and the target's network.
Not only can the attacker cause problems for the target host, the influx of traffic can in fact be so great as to have a seriously negative effect on the upstream network(s) from the target. In fact, those institutions being abused as amplifier networks can also be similarly affected, in that their network connection can be swamped by the Echo Reply packets destined for the target.
In this example, answer choice D is correct as it prevents all ICMP messages destined to the broadcast IP address.
Note: The Cisco IOS command "no ip directed-broadcasts" is also an effective way to prevent smurf and fraggle attacks on the network.
Incorrect Answers:

A. This will permit all traffic sourced from the 192.168.2.0/24 network, including the smurf attack packets.
B. This choice will deny all traffic sourced from the 192.168.1.0 incoming on the e0 interface. Although this is probably a good choice, as it will effectively prevent all spoofed IP traffic (as the 192.168.1.0/24 network should never be a source IP address in the incoming direction of this interface) we wish to only prevent the smurfed traffic, so E

is a better choice.
C. This choice will only permit traffic that is destined to the 192.168.1.0 network. If additional networks exist behind the 192.168.1.0 network, such as traffic to the Internet, it will not be allowed through the CK1 router.
E. It would be preferable to stop the attack before the replies are sent, rather than simply filtering the replies.

QUESTION 364
The Certkiller network is connected to the Internet as shown in the diagram below:



Certkiller 1 is currently configured and passing traffic. You want to block all IP spoofing attacks that originate in the Internet from being sent into the 192.168.1.0 network. However, normal traffic must be permitted. No access lists currently exist on the router. What configuration excerpt would accomplish this task when applied to Certkiller 1?

A. access-list 100 permit ip any 192.168.1.0 0.0.0.255
access-list 100 deny any any
interface Ethernet 0
access-group 100 in
B. ip cef
interface Ethernet 0
ip verify unicast reverse-path
C. ip cef
interface Ethernet 1
ip verify unicast reverse-path
D. access-list 100 permit icmp 192.168.1.0 0.0.0.255 any echo
access list 100 deny ip any any
interface Ethernet 1
access-group 100 out
E. access-list 100 permit icmp 192.168.1.0 0.0.0.255 any echo
access list 100 deny ip any any
interface Ethernet 0
access-group 100 in

Answer: B

Explanation:
Use the ip verify unicast reverse-path interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.
When Unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source address appears in the routing table and matches the interface on which the packet was received. This "look backwards" ability is available only when Cisco Express Forwarding (CEF) is enabled on the router because the lookup relies on the presence of the Forwarding Information Base (FIB). CEF generates the FIB as part of its operation.
Unicast RPF is an input function and is applied only on the input interface of a router at the upstream end of a connection.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800c

---

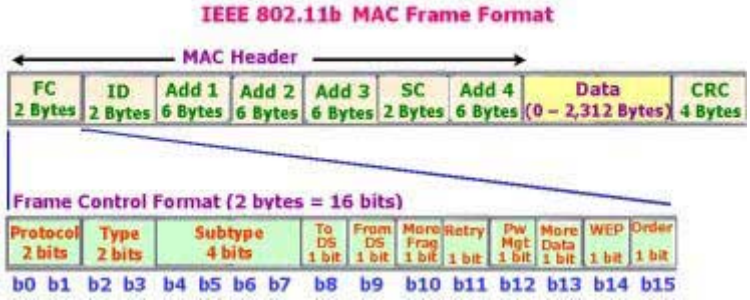
QUESTION 365
While troubleshooting some intermittent 802.11b wireless LAN problems, you use a protocol analyzer. While looking at the wireless LAN packets, which of the following should you find as part of the Frame Control Field? (Choose all that apply)

A. Duration
B. Power Management
C. Order
D. Wired Equivalent Privacy
E. Retry
F. More Fragment

Answer: B, C, D, E, F

Explanation:
The IEEE 802.11b MAC Frame Format Contains the following:
1. Frame Control (FC): protocol version and frame type (management, data and control).
2. Duration/ID (ID)
3. 1. Station ID is used for Power-Save poll message frame type.
2. The duration value is used for the Network Allocation Vector (NAV) calculation.
3. Address fields (1-4) contain up to 4 addresses (source, destination, sender and receiver addresses) depending on the frame control field (the ToDS and FromDS bits).
4. Sequence Control consists of fragment number and sequence number. It is used to represent the order of different fragments belonging to the same frame and to recognize packet duplications.

5. Data is information that is transmitted or received.
6. CRC contains a 32-bit Cyclic Redundancy Check (CRC).



The Frame Control Format contains all of the following:
1. Protocol Version indicates the version of IEEE 802.11 standard.
2. Type & Subtype: Type - Management, Control and Data , Subtype - RTS, CTS, ACK etc
3. To DS is set to 1 when the frame is sent to Distribution System (DS)
4. From DS is set to 1 when the frame is received from the Distribution System (DS)
5. More Fragment is set to 1 when there are more fragments belonging to the same frame following the current fragment
6. Retry indicates that this fragment is a retransmission of a previously transmitted fragment. (For receiver to recognize duplicate transmissions of frames)
7. Power Management indicates the power management mode that the station will be in after the transmission of the frame.
8. More Data indicates that there are more frames buffered to this station.
9. WEP indicates that the frame body is encrypted according to the WEP (wired equivalent privacy) algorithm.
10. Order indicates that the frame is being sent using the Strictly-Ordered service class.
Incorrect Answers:
A. Duration is not a part of the FCF.

QUESTION 366
When comparing wireless Point to Point (p2p) and Point to Multipoint (p2mp) networks, which of the following statements are true?

A. There are more bridges in a p2p network.
B. There are more root bridges in a p2mp network.
C. There is one root bridge and one or more non-root bridges in a p2mp network
D. There is higher throughput in p2mp network.
E. P2p networks are more secure

Answer: C
Wireless bridges can be deployed to establish a direct link between two sites. The network traffic between the two sites is bridged or forwarded to the other bridge as if it were within one network. This is called a point-to-point link.
A point-to-multipoint wireless link is an expansion of the point-to-point link in which one centralized bridge can establish multiple point-to-point links. Using point-to-multipoint connections, multiple remote sites, such as buildings, can be linked

together into a single logical network. In a point-to-multipoint architecture, these remote sites are linked to a single root bridge at a centralized site.
Incorrect Answers:

A. In a point to point wireless connection there are only 2 bridges.
B. There is only 1 root bridge in a multipoint network, while both bridges in a p2p network are considered to be root bridges.
D. Because in a multipoint wireless network, such as a hot spot, the bandwidth is shared between the nodes there is less throughput.
E. There are no security advantages to either method.

QUESTION 367
A wireless system based on the 802.1X standard is being implemented on the Certkiller network. What are the three main components of an 802.1X architecture?

A. Authenticator, Certificate Server, Authentication Server
B. Client, Authenticator, Certificate Server
C. Authenticator, Authentication Server, Supplicant
D. Client, Authentication Server, Supplicant
E. Certificate Server, Supplicant, Authenticator

Answer: C

Explanation:
802.1X authentication for wireless LANs has three main components: The Supplicant (usually the client software); the Authenticator (usually the access point); and the Authentication Server (usually a Remote Authentication Dial-In User Service server, although RADIUS is not specifically required by 802.1X).
The client tries to connect to the access point. The access point detects the client and enables the client's port. It forces the port into an unauthorized state, so only 802.1X traffic is forwarded. Traffic such as Dynamic Host Configuration Protocol, HTTP, FTP, Simple Mail Transfer Protocol and Post Office Protocol 3 is blocked. The client then sends an EAP-start message.
The access point will then reply with an EAP-request identity message to obtain the client's identity. The client's EAP-response packet containing the client's identity is forwarded to the authentication server.
The authentication server is configured to authenticate clients with a specific authentication algorithm. The result is an accept or reject packet from the authentication server to the access point.
Upon receiving the accept packet, the access point will transition the client's port to an authorized state, and traffic will be forwarded.

QUESTION 368
CCX version 1 and version 2 require support for:

A. WEP, Wi-Fi compliance, Cisco pre-standard CKIP

B. WPA Compliance, and WPA 2 Compliance
C. Cisco LEAP, support multiple SSIDs/VLANs, pre-standard eDCF
D. AES Encryption
E. All of the above

Answer: A

Explanation:
Makers of 802.11 wireless LAN clients now can make their products support special security features offered inCiscowireless networks under Cisco Compatible Extensions (CCX), a licensing and testing program used to certify compatibility within Cisco wireless networks.
Cisco has already developed a CCX specification that includes the company's implementations of strong user authentication and encryption, Rossi said. CCX Version 1 includes compliance with the Cisco Wireless Security Suite, compatibility with Cisco's mechanism for assigning WLAN clients to virtual LANs, and full Wi-Fi and 802.11 standards compliance, according to the company.
CCX Version 2 will add support for the IEEE 802.1x authentication typePEAP(Protected Extensible Authentication Protocol) and compliance with WPA (Wi-Fi Protected Access) when using various 802.1x authentication types. It also will have some new Cisco WLAN capabilities that improve roaming and WLAN management. WPA is a specification developed by the Wi-Fi Alliance industry group.
Incorrect Answers:
B, C. These are all functions of CCX version 2 only and were not supported in version 1.
D. AES is the advanced encryption standard, used to increase the security of standard DES and 3DES encryption schemes. AES will be supported with CCX version 3.

QUESTION 369
The Certkiller network is replacing the 802.11 a/b devices with 802.11g devices. What statement is FALSE about the 802.11g standard?

A. It operates in the same frequency spectrum as 802.11b.
B. It has the same number of non overlapping channels as 802.11a.
C. It requires antennas specific to the 2.4 GHz band.
D. All statements above are true about the 802.11g standard.
E. None of the above statements are correct.

Answer: B

Explanation:
802.11g is an extension to 802.11b, the basis of the majority of wireless LANs in existence today. 802.11g will broaden 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM (orthogonal frequency division multiplexing) technology. Because of backward compatibility, an 802.11b radio card will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. You should be able to upgrade the newer 802.11b access points to be 802.11g compliant via

relatively easy firmware upgrades.
Similar to 802.11b, 802.11g operates in the 2.4GHz band, and the transmitted signal uses approximately 30MHz, which is one third of the band. This limits the number of non-overlapping 802.11g channels to three, which is the same as 802.11b.
A big difference with 802.11a is that it operates in the 5GHz frequency band with twelve separate non-overlapping channels. As a result, you can have up to twelve access points set to different channels in the same area without them interfering with each other. This makes access point channel assignment much easier and significantly increases the throughput the wireless LAN can deliver within a given area. In addition, RF interference is much less likely because of the less-crowded 5 GHz band.
Reference: http://www.wi-fiplanet.com/tutorials/article.php/1009431

QUESTION 370
The IEEE standard controlling client network access in WPA authentication is:

A. EAP-TLS
B. EAP
C. 802.1X
D. 802.1Q
E. All of the above

Answer: C

Explanation:
The IEEE 802.1x standard defines 802.1x port-based authentication as a client-server based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server validates each client connected to a switch port before making available any services offered by the switch or the LAN.
Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.
In a Cisco wireless network, the 802.1X standard and the Extensible Authentication Protocol are synonomous, but the industry standard is the 802.1X method, making choice C the best answer.

QUESTION 371
In a Wireless network environment, why do point-to-multipoint links usually have less maximum range than a point to point link?

A. The total sum of the energy is distributed across numerous radios in a point to multi-point architecture versus most of the RF energy being distributed between only two points in a point to point architecture.
B. Point-to-point antennas usually employ higher gain antennas at both link ends than point-to-point links.
C. Point-to-multipoint archetectures require lower power settings than point to point

links.
D. On a statistical basis, a point-to-point link is more likely to be a greater distance than point to multi-point
E. All of the above.

Answer: E

Explanation:
Range is one of the most difficult of criteria to ensure; it is easier to predict outdoors than indoors due to the relatively larger amount of multipath observed in indoor environments. In simple terms, range is determined by transmit power, receive sensitivity, antenna gain, and transmission medium.
In point-to-multipoint systems, the FCC has limited the maximum EIRP (effective isotropic radiated power) to 36 dBm. EIRP = TX power + antenna gain. For every dB that the transmitter power is reduced, the antenna may be increased by 1 dB. (29 dBm TX, +7 dB antenna = 36 dBm EIRP, 28 dBm TX, +8 dB antenna = 36 dBm EIRP).
The Cisco Aironet 2.4 GHz Bridge transmitter power is 20 dBm, which is 10 dBm lower than maximum. This then allows the use of antennas up to 10 dB over the initial 6dBi limit, or 16dBi.
In point-to-point systems for 2.4 GHz systems using directional antennas, the rules have changed. Because a high gain antenna has a narrow beamwidth, the likelihood is high that it will cause interference to other area users. Under the rule change, for every dB the transmitter is reduced below 30 dBm the antenna may be increased from the initial 6dBi, by 3 dB. (29 dB transmitter means 9dBi antenna, 28 dB transmitter means 12dBi antenna). Because we are operating at 20 dBm, which is 10 dB below the 30 dBm level, we can increase the out antenna by 30 dB. Note thatCisco has never tested, and therefore is not certified, with any antenna larger than 21dBi.
The main issue that comes to question here is, what differentiates a point-to-point from a multipoint system.
In Figure 8, point A communicates to a single point, B, and point B communicates to a single point A; therefore, it is simple to see that both locations see this as a point-to-point installation.
In Figure 9, point A communicates to more than one (or multiple) points; therefore, point A is operating in a multipoint configuration, and the largest antenna permitted is 16dBi. Point B or point C can each communicate to only one point, (point A); therefore, point B and point C actually operate in a single-point or point-to-point operation, and a larger antenna may be used.
Figure 8. Point-to-Point Wireless Bridge Solution

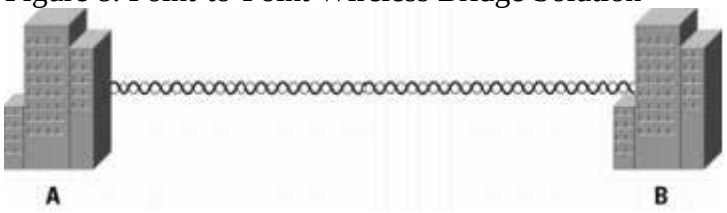
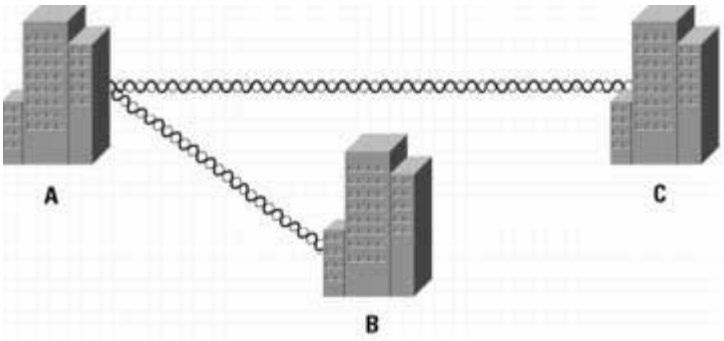


Figure 9. Point-to-Multipoint Wireless Bridge Solution



Amplifiers-The FCC Rules, Section 15.204-Part C, states "External radio frequency power amplifiers shall not be marketed as separate products..." Part D states "Only the antenna with which an intentional radiator (transmitter) is originally authorized may be used with the intentional radiator." This means that unless the amplifier manufacturer submits the amplifier for testing with the radio and antenna, it cannot besold in the U.S. If it has been certified, then it must be marketed and sold as a complete system, including transmitter, antenna, and coax. Italsomust be installed exactly this way.
Reference:
http://www.cisco.com/en/US/products/hw/wireless/ps469/products_data_sheet09186a008008883b.html

---

QUESTION 372
What IEEE 802-x standard supports eight adjacent channels in the UUNI-1 and UUNI-2 bands designated for indoor use?

A. 802.11g
B. 802.11a
C. 802.11b
D. 802.11i
E. None of the above

Answer: B

Explanation:
Commonly referred to as "Wi-Fi," 802.11 refers to the standards issued by IEEE for WLANs. 802.11 transmits data over the air in an unlicensed frequency, such as the 2.4 GHz band.
Common extensions of the 802.11 standard include:
1. 802.11a - uses the 5 GHz band and an orthogonal (8 channel) frequency division multiplexing as the signal modulation technique rather than FHSS or DSSS.
2. 802.11b - uses the 2.4 GHz band and DSSS for signal modulation.
3. 802.11g - Allows for faster data rates than 802.11b in the 2.4 GHz band. 802.11g is compatible with both 802.11a and 802.11b and uses similar modulation techniques for both standards.
802.11a uses the 8 channels present in the lowest 2 U-NII bands, providing for a 200Mhz spectrum. 802.11a defines 8 channels in that spectrum, at 25Mhz centers.
Incorrect Answers:
A, C: The 802.11b/g standard defines a total of 14 frequency channels. The FCC allows

channels 1 through 11 within the U.S.; whereas, most of Europe can use channels 1 through 13. In Japan, you have only one choice: channel 14. 802.11g is fundamentally the same as 802.11b, except it is designed for higher throughput.
D: 802.11i deals with the security limitations of wireless networking. It is a very recent specification designed for enhancing wirless security.

QUESTION 373
What device can function as a Wireless Domain Server capable of RF aggregation?

A. BR1300
B. AP1200
C. WLSM
D. AP1100
E. All of the above

Answer: E

Explanation:
Cisco SWAN Wireless Domain Services (WDS) is a collection of Cisco IOS Software features that expand WLAN client mobility, simplify WLAN deployment and management, and enhance WLAN security. These services-supported today on access points, Cisco and Cisco Compatible client devices, and the Cisco Catalyst 6500 Series WLSM, and other Cisco LAN switches and routers in 2005-include radio management aggregation, fast secure roaming, client tracking, and WAN link remote site survivability. Cisco SWAN WDS radio management aggregation supports RF managed services such as rogue access point detection for WLAN threat defense, interference detection, assisted site surveys, and self-healing WLANs.
Reference:
http://www.cisco.com/en/US/products/ps6108/products_data_sheet0900aecd801b914f.html

---

QUESTION 374
You are in the planning stages for the new Certkiller wireless network, and are determining the types of antennas that should be utilized. Which of the following are four basic antenna types that can be used?

A. Dipole, non-pole, ground effect, bipole
B. Omnidirectional, patch, yagi, parabola
C. High gain, omni, point to point, point to multi-point
D. Wall mount, mast mount, pole mount, window mount
E. Directional, omni-directional, dipole, distributed

Answer: B

Explanation:
The basic antenna types and their descriptions are provided below:
Omnidirectional Antennas:

An omnidirectional antenna provides a 360-degree radiation pattern. This type of antenna is used when coverage in all directions is required and when communicating with wireless client devices. Antennas in this category are available in different gain ratings (typically 2.2 to 12 dBi).
Directional Antennas:
A directional antenna provides a stronger radiation pattern in a specific direction by focusing the radiation energy to provide a greater coverage distance. Directional antennas include the Yagi antenna, the patch antenna, and the parabolic dish antenna.

QUESTION 375
You have been assigned the task of setting up access points within a building for wireless users. The best position for an Access Point in a corporate wireless network is: (Select the best answer).

A. The center of the building
B. In a position determined by a site survey
C. At the edges of the building
D. At the edge of the coverage area shown by the site survey in the ceiling or the floor
E. Away from any metal or glass

Answer: B

Explanation:
Because of differences in component configuration, placement, and physical environment, every network application is a unique installation. Before installing the system, you should perform a site survey to determine the optimum utilization of networking components and to maximize range, coverage, and network performance. Consider the following operating and environmental conditions when performing a site survey:
1. Data rates - Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. A decrease in receiver threshold sensitivity occurs as the radio data increases.
2. Antenna type and placement - Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height.
3. Physical environment - Clear or open areas provide better radio range than closed or filled areas. Also, the less cluttered the work environment, the greater the range.
4. Obstructions - A physical obstruction such as metal shelving or a steel pillar can hinder performance of the client adapter. Avoid locating the workstation in a location where there is a metal barrier between the sending and receiving antennas.
5. Building materials - Radio penetration is greatly influenced by the building material used in construction. For example, drywall construction allows greater range than concrete blocks. Metal or steel construction is a barrier to radio signals.

QUESTION 376
A new Cisco Wirless network is being installed in a Certkiller location, and you need

to determine the best antenna to be used. What is the fundamental difference between an omni-directional and directional antenna?

A. Cisco omni-directional antennas always have the letter "0" in their part number.
B. Omni-directionla antennas always look like straight rods.
C. Directional antennas always look like a dish.
D. Omni-directional antennas distribute RF energy in a relatively even manner in most directions while directional antennas uswe most of the available RF energy in a specific direction with a specific RF coverage shape.
E. There is no real technical difference, omni-directional and directional antennas are both dipoles.

Answer: D

Explanation:
Omnidirectional Antennas
An omnidirectional antenna provides a 360-degree radiation pattern. This type of antenna is used when coverage in all directions is required and when communicating with wireless client devices. Antennas in this category are available in different gain ratings (typically 2.2 to 12 dBi).
Directional Antennas
A directional antenna provides a stronger radiation pattern in a specific direction by focusing the radiation energy to provide a greater coverage distance. Directional antennas include the Yagi antenna, the patch antenna, and the parabolic dish antenna.
Parabolic dishes have very high gain (typically 21 dBi) along with a very narrow radiation angle (typically 12.5 degrees) and must be accurately aimed at the other antenna. Yagi antennas have high gain (typically 13.5 dBi) and a wider radiation angle (typically 25 to 30 degrees). Yagi antennas must also be properly aimed at the other antenna. Patch antennas have high gain (typically 6 dBi) and a relatively broad radiation angle. The patch antenna is more tolerant of orientation, but must still be positioned to face the direction of the other antenna.
Reference:
http://www.cisco.com/en/US/products/hw/wireless/ps458/products_installation_guide_chapter09186a008007f74

QUESTION 377
You need to purchase a number of Wi-Fi handsets for the Certkiller network and need to compare and contrast the different options. Identify the primary Wi-Fi voice handset vendors other than Cisco:

A. Symbol
B. Nortel
C. Avaya
D. Spectralink

Answer: D

Explanation:
Wireless handset pioneer SpectraLink is the most sought-after partner in the VoWi-Fi industry. PBX vendors want to offer a range of handset options, and SpectraLink's product line includes everything from small, stripped-down models to ruggedized devices with push-to-talk capabilities. Now that Symbol Technologies is focused on voice-enabling mobile terminals, the choices have pretty much come down to reselling SpectraLink's handsets or building your own, or using Cisco.
SpectraLink recently enhanced its 802.11 offerings with a docking station that includes an integrated speakerphone and charging cradle. The vendor boasts another asset in its SpectraLink Voice Priority protocol, which is supported by established vendors and WLAN start-ups alike.
Reference: http://www.networkworld.com/research/2004/0503vowifi.html

---

QUESTION 378
The Certkiller WLSE has detected numerous rogue AP's within the network. How does the WLSE determine that an AP is a rogue AP?

A. The AP's SSID does not exist in the WLSE database of know BSSIDs.
B. The AP's BSSID does not exist in the WLSE database of know BSSIDs.
C. The AP does not respond to SNMP Queries.
D. The AP can not be discovered through CDP.
E. A CCX client reports the AP as rogue.

Answer: B

Explanation:
The WLSE determines whether an AP is a rogue by performing the following steps:
1.
While Radio Monitoring is enabled, the APs report the BSSIDs of their neighboring APs.
2.
WLSE compares the BSSIDs of the APs with those in the managed list. Any AP not in the managed list is considered to be rogue and a fault is reported.
After a rogue AP has been detected by WLSE:
1.
The WLSE receives frame reports from the reporting and scanning APs. These reports contain the MAC addresses of any clients associated with the rogue AP.
2.
WLSE tries to locate the MAC addresses of both the client and the rogue in the switches via a CAM table search (using the approach described in the following note) to determine which port is forwarding packets to the client via the rogue.
Reference:
http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_chapter09186a008052dbf0.htm

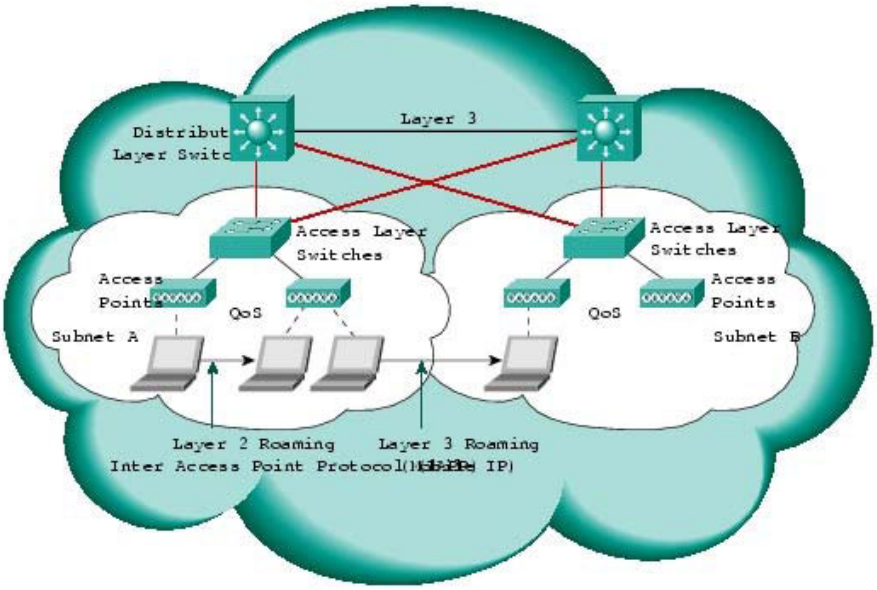
---

QUESTION 379
When comparing the differences between fast secure roaming options within a wireless network, what is the major difference between L2 and L3 fast secure roaming?

A. L3 roaming is faster than L2 roam.
B. L3 roaming requires extra hardware other than the access points and WDS.
C. L2 roaming is more secure than a L3 roam.
D. L3 roaming is required for IP telephony.
E. L2 roaming is standardized, where as L3 roaming is not.

Answer: B

Explanation:
Networks are normally partitioned into discrete L2 domains corresponding to Internet Protocol (IP) subnets. Thispartitioning and the difference between L2 and Layer 3 (L3) roaming are illustrated in the figure below.
Layer 2 and Layer 3 Roaming:



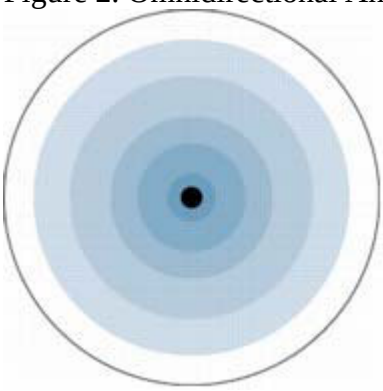
L2 roaming occurs when a WLAN client moves between wireless access points that are part of the same IP subnet.
A L3 roam occurs when the client roams to an access point in a different subnet. Mobile IP capability is required to provide seamless roaming across L3 subnet boundaries. Every L3 roam is preceded by a L2 link-layer roam.
With layer 2 fast secure roaming, only an access point and the WDS is required. As can be seen in the diagram above, layer 3 FSR requires additional layer 3 devices.
Reference:
http://www.cisco.com/en/US/partner/products/hw/wireless/ps458/prod_technical_reference09186a00801c5223.h

QUESTION 380
The Certkiller wireless network administrator must determine the correct antenna to use. In most cases, where should a directional antenna be installed versus an omni-directional antenna?

A. Lecture theaters, especially where the ceilings are higher than 10 meters
B. Convention halls where the ceilings are higher than 10 meters
C. Hallways where coverage into adjacent areas is not desired
D. Point to point outdoor links
E. All of the above
F. None of the above

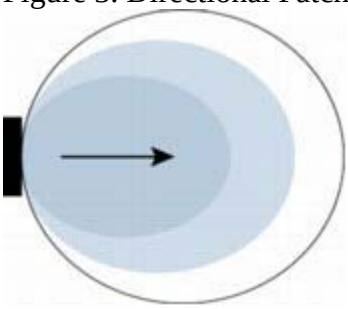
Answer: D

Explanation:
Cisco offers several different styles of antennas for use with both access points and bridges in the 2.4 GHz product line, as well as the 5 GHz BR1400 bridge. Every antenna offered for sale has been FCC-approved. Each type of antenna will offer different coverage capabilities. As the gainof an antenna increases, there is some tradeoff to its coverage area. Usually gain antennas offer longer coverage distances, but only in a certain direction. The radiation patterns below will help to show the coverage areas of the styles of antennas that Cisco offers: omnidirectional, yagis, and patch antennas.
Omnidirectional Antennas:
An omnidirectional antenna (Figure 2) is designed to provide a 360-degree radiation pattern. This type of antenna is used when coverage in all directions from the antenna is required. The standard 2.14dBi "Rubber Duck" is one style of omnidirectional antenna.
Figure 2. Omnidirectional Antenna:



Directional Antennas:
Directional antennas come in many different styles and shapes. An antenna does not offer any added power to the signal; it simply redirects the energy it receives from the transmitter. By redirecting this energy, it has the effect of providing more energy in one direction, and less energy in all other directions. As the gain of a directional antenna increases, the angle of radiation usually decreases, providing a greater coverage distance, but with a reduced coverage angle. Directional antennas include yagi antennas (Figure 4), patch antennas (Figure 3), and parabolic dishes. Parabolic dishes have a very narrow RF energy path and the installer must be accurate in aiming these at each other.

Figure 3. Directional Patch Antenna:



Recommendations for some common installation environments are outlined below:
Warehousing/Manufacturing-In most cases, these installations require a large coverage area. Experience has shown that an omnidirectional antenna mounted at 20 to 25 feet typically provides the best overall coverage. Of course, this also depends upon the height of the racking, material on the rack, and ability to locate the antenna at this height. Mounting the antenna higher will sometimes actually reduce coverage, as the angle of radiation from the antenna is more outward than down. The antenna should be placed in the center of the desired coverage cell and in an open area for best performance. In cases where the radio unit will be located against a wall, a directional antenna such as a patch or yagi can be used for better penetration of the area. The coverage angle of the antenna will affect the coverage area.
Small Office/Small Retail-The standard dipole may provide adequate coverage in these areas depending on the location of the radio device. However, in a back corner office a patch antenna may provide better coverage. It can be mounted to the wall above most obstructions for best performance. Coverage of this type antenna depends on the surrounding environment.
Enterprise/Large Retail-In most cases, these installations require a large coverage in Experience has shown that omnidirectional antennas mounted just below the ceiling girders or just below the drop ceiling typically provide the best coverage (this will vary with stocking, type of material, and building construction). The antenna should be placed in the center of the desired coverage cell and in an open area for best performance. In cases where the radio unit will be located in a corner, or at one end of the building, a directional antenna such as a patch or yagican be used for better penetration of the area. Also, for areas that are long and narrow-such as long rows of racking-a directional antennaat one end may provide better coverage. The radiation angle of the antennas will also affect the coverage area.
Point-to-Point-When connecting two points together (such as a wireless bridge), the distance, obstructions, and antenna location must be considered. If the antennas can be mounted indoors and the distance is very short (several hundred feet), the standard dipole or mast mount 5.2dBiomnidirectional may be used. An alternative is to use two patch antennas. For very long distances (1/2 mi. or more), directional high-gainantennas must be used. These antennas should be installed as high as possible, and above obstructions such as trees, buildings, and so on; andif directional antennas are used, they must be aligned so that their main radiated power lobes are directed at each other. With a line-of-site configuration, distances of up to 25 miles at 2.4 GHz and 12 miles at 5 GHz can be reached using parabolic dish antennas, if a clear line-of-site ismaintained. With the use of directional antennas, fewer interference possibilities exist and there is less

possibility of causing interference to anyone else.
Point-to-Multipoint Bridge-In this case (in which a single point is communicating to several remote points), the use of an omnidirectional antenna at the main communication point must be considered. The remote sites can use a directional antenna that is directed at the main point antenna.
Reference:
http://www.cisco.com/en/US/customer/products/hw/wireless/ps469/products_data_sheet09186a008008883b.htm

---

QUESTION 381
The Certkiller network is performing site surveys at all of their location in order to plan for the installation of wireless networking devices. In terms of wireless networking, what are leading indicators of links with excessive occlusion (blockage with physical elements)?

A. Coverage area less than 10 square meters at signals greater than-65 dBm
B. Drips in RF signal in excess of 20 dBm over distances of less than two meters
C. Inability to physically see the infrastructure device
D. Distance in excess of 20 meters from an infrastructure device in a carpeted environment
E. All of the above.

Answer: C

Explanation:
Occlusion is defined as an obstruction or a closure of a passageway or vessel. If the wireless access point can not be physically seen, then there is an excessive amount of physical elements (boxes, walls, warehouse shelving, etc) that is blocking the view. This can lead to poor wireless signals.

QUESTION 382
What are the main advantages of the Cisco SWAN architecture?

A. Security
B. Layer 3 mobility
C. Visibility and management of the wireless network
D. Centralized Management
E. None of the above

Answer: D

Explanation:
The Cisco Structured Wireless-Aware Network (SWAN) provides the framework to integrate and extend wired and wireless networks to deliver the lowest possible total cost of ownership for companies deploying wireless LANs (WLANs). Cisco SWAN extends "wireless awareness" into important elements of the network infrastructure, providing the

same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations have come to expect from their wired LANs.
From small businesses to large-scale enterprise multinational companies; within WLAN campus deployments or branch offices; at universities; in retail, manufacturing, or healthcare industries; or at hot spot locations, Cisco SWAN reduces overall operational expenses by simplifying network deployment, operations and management. With Cisco SWAN, several, hundreds, or thousands of central or remotely located Cisco Aironet Series access points can be managed from a single management console. Cisco SWAN's flexibility allows network managers to design networks to meet their specific needs, whether implementing a highly integrated network design or a simple overlay network.
Reference:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html

---

QUESTION 383
As the administrator of the Certkiller network, you are considering the benefits and disadvantages of installing a wireless LAN at your Headquarters office. In weighing in these considerations, what is NOT a reason for deploying wireless in a corporate environment?

A. There is a need to eliminate rouge Access Points in the organization and increase LAN security.
B. The organization needs to provide greater mobility to users.
C. Wireless is cheaper to deploy than a wired network.
D. The employer wishes to obtain greater productivity from the employees.
E. All of the above are wireless networking features

Answer: A

Explanation:
Although there are many benefits for deploying a wireless network from a cost and productivity perspective, it can introduce some security issues. Access points can be difficult to secure, and sometimes corporate employees will install their own access points within the office in order to increase the range. In addition, weak security measures are often used in wireless networks. The original IEEE 802.11 security standard had modest security goals in Wired Equivalent Privacy (WEP), including native authentication, where users are required to prove they are authorized for access and encryption to provide data protection. The protocols in WEP are now easily defeated.
Incorrect Answers:
B. A major goal of the use of wireless networks is to provide for a more mobile workforce.
C. Wireless networks can be cheaper to deploy in a new office environment, as the added costs associated with CAT5 cable drops are eliminated. In addition, fewer switches are needed, since each access point can handle many users, but only requires one switch port.
D. This is true as users can now carry their laptops with them to other areas of a building, such as conference rooms, enabling them to continue working even during meetings and conferences.

QUESTION 384
The WLSE is being configured for managing the Certkiller WLAN. When the WLSE generates an alarm, what actions can the device take?

A. Send an e-mail to an administrator
B. Disable the switch port that the rouge Access Point is connected to
C. Send a message to a syslog server
D. Generate an SNMP trap
E. All of the above

Answer: E

Explanation:
When a fault is detected, the WLSE can send automated notifications in the form of SNMP traps, syslog messages, and email alerts. You can specify multiple recipients for each notification type, and choose to deliver the message using either a plain text or XML format.

QUESTION 385
The Certkiller network plans to implement the use of Public Wireless hot spots and security issues are a concern. Which of the following are primary requirements in PWLAN security? (Choose all that apply)

A. Encryption of user data
B. IPSec encryption
C. Accounting of time, and throughput
D. 802.1x
E. Broadcast SSIDs

Answer: A, D

Explanation:
Two of the chief security concerns for public wireless (PWLAN) use is user authentication, which is addressed with the 802.1x/EAP suite of protocols, and the encryption of individual user data.
The Cisco PWLAN solution has implemented numerous features in the Cisco IOS Software for Cisco's access zone routers (AZR) that help mitigate the risk of session hijacking associated with malicious IP spoofing activity.
Operators can take advantage of key features available in Cisco access points to prevent local peer attacks as well as preventing man-in-the-middle spoofing of infrastructure addresses.
Cisco access points support all 802.1x/EAP methods available today, in addition to supporting WPA for air link encryption.

QUESTION 386
A wireless LAN needs to be implemented in a new Certkiller location. How is a baseline RF environment established?

A. With a carefully detailed RF site survey and supporting documentation.
B. With a carefully detailed RF site survey only.
C. By using WLSE's Assisted Site Survey feature.
D. Usually with a spectrum analyzer

Answer: A

Explanation:
To establish the feasibility of any wireless LAN (WLAN) or radio frequency (RF) project, a site survey, complete with supporting documentation, should be performed. A WLAN site survey takes into account the radius around one or more Access Points and the structural components of the facility to determine coverage. This survey involves verifying a clear line of site between points, consulting topographical maps, and global positioning systems to pinpoint locations and to evaluate needs relating to mounting equipment and towers. A number of documents are generated from this survey including a Bill of Materials, requirements for tower and antenna placement, drawings and site-related documents including construction materials, and a plan to implement.

QUESTION 387
When implementing corporate guest access an important consideration of the RF coverage is:

A. That the area RF coverage should offer high data rates only.
B. That the RF coverage offers low latency roaming.
C. That the area of RF coverage avoids leakage outside the building as much as possible.
D. That the RF coverage is as secure as possible.
E. That the area RF coverage is as large as possible.

Answer: C

Explanation:
When setting up a wireless network for corporate guest access, an important consideration is to ensure that the radio frequency coverage is maintained within the building. The leaking of the RF coverage to the outside leaves the potential for unauthorized access from unknown, outside users. When RF access leaks to the outside, hackers are able to pick up the signals and obtain unatuhorized wireless Internet access.

QUESTION 388
A site survey needs to be completed at one of the remote Certkiller locations. How does a site survey confirm a deployment plan?

A. By auditing the signal strengths in selected physical areas.

B. By auditing the channel selections in selected physical areas.
C. By auditing the various direction antenna performances in specific physical areas.
D. By ensuring an optimal number of RF instrastructure devices are deployed
E. All of the above

Answer: E

Explanation:
A site survey should be completed at every wireless location in order to optimize the wireless network infrastructure.
Keep the following guidelines in mind when preparing to perform a site survey:
1. Perform the site survey when the RF link is functioning with all other systems and noise sources operational.
2. Execute the site survey entirely from the mobile station.
3. When using the active mode, conduct the site survey with all variables set to operational values.
Additional Information
Also consider the following operating and environmental conditions when performing a site survey:
1. Data rates-Sensitivity and range are inversely proportional to data bit rates. Therefore, the maximum radio range is achieved at the lowest workable data rate, and a decrease in receiver threshold sensitivity occurs as the radio data increases.
2. Antenna type and placement-Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height.
3. Physical environment-Clear or open areas provide better radio range than closed or filled areas. Also, the less cluttered the work environment, the greater the range.
4. Obstructions-A physical obstruction such as metal shelving or a steel pillar can hinder the performance of wireless devices. Avoid placing these devices in a location where a metal barrier is between the sending and receiving antennas.
5. Building materials-Radio penetration is greatly influenced by the building material used in construction. For example, drywall construction allows greater range than concrete blocks, and metal or steel construction is a barrier to radio signals.
Reference:
http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guide_chap

---

QUESTION 389
You are trying to determine if a Cisco SWAN environment would fit your network needs. SWAN deployments are most often deployed in what types of networks?

A. Large enterprises
B. Branch offices
C. Hot spots
D. Campus Environments
E. All of the above

Answer: E

Explanation:
The following was taken from Cisco marketing literature (note the words in bold below):
Cisco SWAN
Cisco SWAN provides the framework to integrate and extend wired and wireless networks to deliver the lowest possible total cost of ownership for companies deploying WLANs. All Cisco Aironet access points are part of the Cisco SWAN framework. Cisco SWAN extends "wireless awareness" into important elements of the network infrastructure, providing the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations have come to expect from their wired LANs.
From small businesses to large-scale enterprises and multinational companies; within WLAN campus deployments or branch offices; at universities; in retail, manufacturing, or healthcare industries; or at hot spot locations, Cisco SWAN reduces overall operational expenses by simplifying network deployment, operations, and management. With Cisco SWAN, several, hundreds, or thousands of central or remotely located Cisco Aironet access points can be managed from a single management console. Cisco SWAN's flexibility allows network managers to design networks to meet their specific needs, whether implementing a highly integrated network design or a simple overlay network.
Reference:
http://www.cisco.com/en/US/products/ps6108/products_data_sheet0900aecd801b914f.html

---

QUESTION 390
Certkiller is using the WLSE to manage their Cisco wireless network. What network connectivity tools are available on the WLSE administration page?

A. Ping and traceroute only
B. SNMP reachable, Ping and Traceroute only
C. Ping, Traceroute, and SNMP reachable only
D. Ping, traceroute, nslookup, tcp port scan, SNMP reachable only
E. Ping, Traceroute, L2 Traceroute, nslookup, and SNMP reachable only

Answer: D

Explanation:
The following chart display the various connectivity tools available on the WLSE administration interface:

Connectivity Tools		
Button	Description	Results
Ping	Tests device reachability.	If successful, statistics are displayed on the packets transmitted and received.
Traceroute	Detects routing errors between the WLSE and a device.	If successful, the routes to the device are displayed.
NSLookup	Looks up hostname or IP address information via the name server.	If successful, displays the name server name and IP address and the device name and IP address.
TCP Port Scan	Finds the active ports on a device.	Displays the active ports.
SNMP Reachable	Tries to reach a device by using SNMP. To reach a device by using SNMP, the device's credentials must be in the WLSE database. To check credentials, select Administration > Devices > Discover > Device Credentials > SNMP Communities.	If the device is reachable, its sysObjID is displayed. If no sysObjID is returned: • The query may be timing out because the device is busy or is remotely located. • The SNMP agent in the device may not be functioning.

Reference:
http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_chapter09186a00801d08a8.htm

---

QUESTION 391
What is NOT an optimal method for detecting co-channel reference?

A. A properly planned and documented site survey, with continued monitoring of the radiating environment.
B. Well enforced policies on the deployment of rogue APs.
C. Deploying WLSE
D. Deploying SWAN

Answer: B

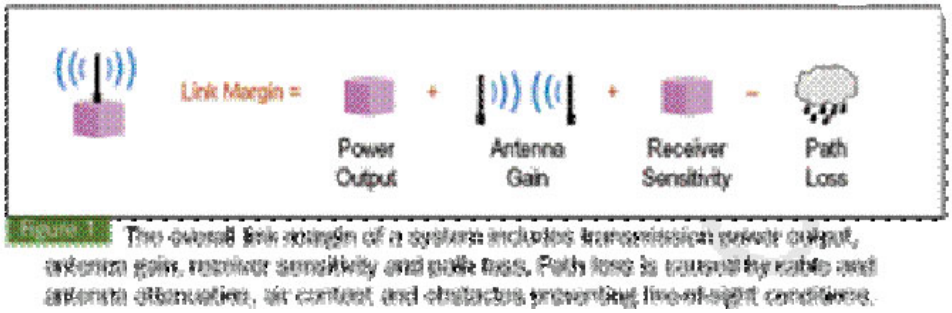
Explanation:
The use of rogue Access Points (APs) should be completely avoided within an enterprise wireless LAN. Simply establishing a policy against the deployment of rogue APs alone will not be effective. The Wireless site should be continuously maintained and monitored to ensure that the introduction of outside access points does not occur, via the Cisco SWAN model through the use of the WLSE.

QUESTION 392
The Certkiller WLAN is experiencing problems associated with poor link margins. What are the leading indicators of insufficient link margin?

A. Difference of less than 10 dBm from signal to node
B. Links works fine initially but flaps or goes down shortly after being turned up
C. Competing sources of 802.11 arrive in the radiating area
D. Link initially deployed at full power settings on infrastructure and client devices but link still goes down shortly after being turned up.
E. All of the above

Answer: E

Explanation:
Transmission range in a system is determined by link margin calculations. Figure 1 shows the overall link margin of a system that includes transmission power output, antenna gain, receiver sensitivity and path loss. Such path loss is due to cable and antenna attenuation, air content and obstacles preventing line-of-sight conditions. Achieving long range with wireless transceiver modules requires an effective combination of output power, antenna gain and receiver sensitivity. Each of these specifications can have dramatic effects on the link margin of a wireless link path.



All of the answer choices are symptoms that can be caused by problems associated with poor link margin.

QUESTION 393
A Certkiller user has an 802.11g/a capable client card. They are able to associate to a Cisco BR1300 without any trouble; however, they are not able to associate to a Cisco BR1400, although all the wireless settings appear to be correctly configured. What is the most likely explanation?

A. The BR1300 is hard-coded not to accept client associations, while the 1400 is capable of this feature.
B. 802.11a bridging uses the UNII-3 frequency band which is in a different frequency band than what 802.11a clients use.
C. The BR1400 can only accept one associated connection, which is already taken up by the radio on the other end of the bridge link.
D. The BR1400 uses a unique MAC layer protocol implementation that prevents any clients from associating.
E. The user is trying associate to the root bridge of the 802.11a bridging link. Only non-root bridges can accept a client association.
F. None of the above

Answer: D

Explanation:
The BR1400 is designed for building to building connectivity and only supports the Root BR and Non-Root BR roles, and does not support client associations. Only other BR1400s can associate to a root BR1400. However, multiple non-root BR devices can connect to the root BR1400. If the bridge is associated and is the root bridge, its default IP address is 10.0.0.1. If it is a non-root bridge, it is given an IP address by the root bridge. The IP address is found from the MAC address by browsing the root bridge Association window or using Cisco's supplied IPSU utility. This bridge is designed for building-to-building wireless connectivity.
Reference:
http://www.cisco.com/en/US/about/ac123/ac114/ac173/Q3-04/netpro_express.html

---

QUESTION 394
The Certkiller wireless network appears to be having some problems related to co-channel interference. Which are good indicators that interference problems are from a co-channel or adjacent channel source?

A. WLSE indicates levels of 2.4 GHz RF in excess of -45 dBm from non-AP sources within 5 meters of 802.11 clients.
B. Non native radios with signals within 10 dB of the closest 802.11 infrastructure device.
C. Rogue APs operating on the same channel near approved infrastructure devices.
D. Non-native radios with higher gain antennas then the closest approved 802.11 infrastructure device.

Answer: C

Explanation:
A limited number of available channels results in limited network capacity. When access points set to the same channel are within range of each other, they become mutual interferers, degrading the performance of each device. This relatively small number of

channels and resulting cochannel interference limits wireless LAN capacity when operating in the narrow 2.4-GHz band. When the access points, both approved and rogue, operate on the same channel, interference can occur when the are positioned close to each other.

QUESTION 395
A new WLSE is being installed at the Certkiller NOC. Which are the primary functions of the Wireless LAN Solutions Engine 1130? (Select three)

A. Fault monitoring
B. Authentication Server 802.1X clients
C. Configuration Management
D. Wireless client management
E. Radio Management

Answer: A, C, E

Explanation:
The WLSE has the following major features:
Configuration-Allows you to apply configuration changes to access points.
Fault and policy monitoring-Monitors device fault and performance conditions, LEAP server responses, and policy misconfigurations.
Reporting-Allows you to track device, client and security information. You can email, print, and export reports.
Firmware-Allows you to upgrade the firmware on access points and bridges.
Radio management-Helps you manage your WLAN radio environment.
WLSE administration-Manage WLSE software, including software upgrades, monitoring the WLSE, backing up data, and using two WLSEs as a redundant, highly available WLAN management solution.
Deployment Wizard-Configures and discovers access points used in a Cisco Structured Wireless-Aware Network (SWAN) framework.
The WLSE operates by gathering fault, performance, and configuration information about Cisco devices that it discovers in your network. The devices must be properly configured for discovery. After devices are discovered, you decide which devices to manage with the WLSE.
Reference:
http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_guide_chapter09186a0080362

QUESTION 396
You are experiencing some 802.1x issues on one of the Certkiller locations. When troubleshooting 802.1X authentications, what command is most useful?

A. debug dot11 aaa authenticator all
B. debug aaa authenticator all
C. debug dot11 aaa radius all

D. debug dot11 802.1x all
E. debug 802.1x all

Answer: A

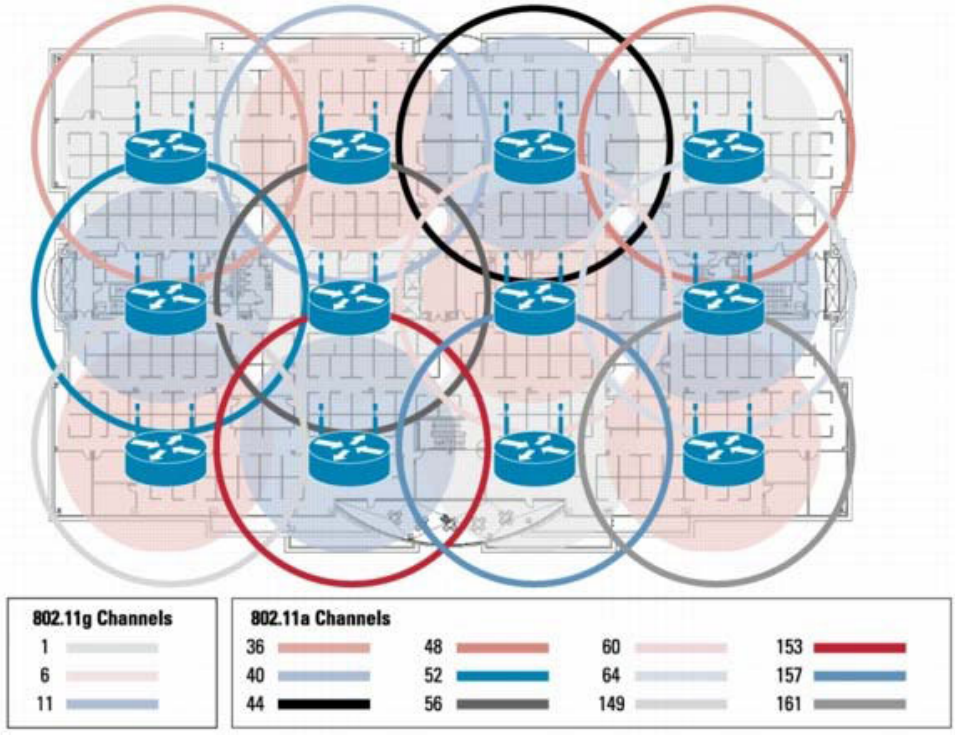
Explanation:
Use the debug dot11 aaa privileged EXEC command to activate debugging of dot11 authentication, authorization, and accounting (AAA) operations.
debug dot11 aaa authenticator all-Shows the various negotiations that a client goes through as it associates and authenticates through the 802.1x or EAP process. This debug was introduced in Cisco IOS Software Release 12.2(15)JA. This command obsoletes debug dot11 aaa dot1x all in that and later releases.

QUESTION 397
A Certkiller location is having issues with their wireless network implementation.
What are common signs of deficient radio channel planning? (Select all that apply)

A. No site survey
B. Evidence of rogue APs
C. No documentation of channel plan
D. All radios APs set to same channel

Answer: A, C, D

Explanation:
A well planned dual-band deployment may look like the deployment shown in Figure 1 below:
Figure 1: A Sample Dual-Band Deployment



In this example, a site survey is conducted to optimize the 2.4 GHz (802.11b/g) network, depending on the required coverage and throughput requirements. The number of 802.11b-only and 802.11g-only clients should be factored in, as these clients will be using the 2.4-GHz network. For some networks, this number can be expected to decline over time, since client devices like laptops and handhelds will be replenished with dual-band capable devices (which will use an available 5-GHz channel a priori, as discussed previously). Because only three nonoverlapping channels are available in the 2.4-GHz band, interference from adjacent cells must be considered. This interference is generally compensated for by reducing the transmit power of the radios.
As is the case with any well planned wireless implementation, the channel plan should be well documented.
Incorrect
Answer:
B: The evidence of rogue access points can occur at any time and although it may be a sign of poor wireless planning in general, it is not a sign of poor radio channel planning specifically.
Reference:
http://www.cisco.com/en/US/partner/products/hw/wireless/ps4570/products_white_paper0900aecd8027a5f7.shtm

---

QUESTION 398
A site survey is being conducted at a Certkiller location. How are nulls identified during a site survey? (Choose two)

A. By measuring physical areas with an RF site survey tool, and determining that a specified area does not generate a minimum of 10 dBm (decibels per milliwat) or greater

signal than noise, and signal sufficient for planned link speeds with the current planned RF infrastructure element deployment scheme.
B. By using WLSE's Assisted Site Survey
C. By using minimum power settings on all 802.11 radios
D. By using highly directional antennas as part of the site survey
E. None of the above; null areas generally does not exist

Answer: A, B

Explanation:
When performing a radio frequency (RF) site survey, such as the Cisco WLSE Assisted Site Survey Tool, it's important to define the range boundary of an access point based on signal-to-noise (SNR) ratio, which is the signal level (in dBm) minus the noise level (in dBm).
The SNR of an access point signal, measured at the user device, decreases as range to the user increases because the applicable free space loss between the user and the access point reduces signal level. An increase in RF interference from microwave ovens and cordless phones, which increases the noise level, also decreases SNR.
SNR directly impacts the performance of a wireless LAN connection. A higher SNR value means that the signal strength is stronger in relation to the noise levels, which allows higher data rates and fewer retransmissions -- all of which offers better throughput. Of course the opposite is also true. A lower SNR requires wireless LAN devices to operate at lower data rates, which decreases throughput.
Real-World Values:
> 40dB SNR = Excellent signal (5 bars); always associated; lightening fast.
25dB to 40dB SNR = Very good signal (3 - 4 bars); always associated; very fast.
15dB to 25dB SNR = Low signal (2 bars); always associated; usually fast.
10dB - 15dB SNR = very low signal (1 bar); mostly associated; mostly slow.
5dB to 10dB SNR = no signal; not associated (null area)
Therefore, an area that does not generate a minimum of 10db will result in a null area.

QUESTION 399
A Wireless network is being installed in one of the Certkiller locations. How is RF gain best utilized in most wireless deployments? (Choose Two)

A. By ensuring that the maximum amount of RF energy is deployed where it will be most likely used
B. By deploying radios at full RF power
C. By using directional antennas where appropriate
D. By testing to ensure Automatic Gain Circuitry is operating to specification

Answer: A, C

Explanation:
The gain of an antenna represents how well it increases effective signal power, with decibels (dB) as the unit of measure.

A directional antenna (often called a yagi) transmits and receives RF energy more in one direction than others. This radiation pattern is similar to the light that a flashlight or spotlight produces. Most antenna manufacturers provide illustrations indicating the radiation pattern. The higher gain antennas will have a narrower beam width, which limits coverage on the sides of the antennas. Directional antennas have gains much higher than omni-directional antennas, such as 12 dBi and higher.
High gain antennas work best for covering large, narrow areas, or supporting point-to-point links between buildings. In some cases, a directional antenna will reduce the number of access points needed within a facility. For example, a long loading dock of a distribution center many require three access points having omnis, but the use of a high gain directional antenna would likely only require a single access point.

QUESTION 400
Certkiller is utilizing VOIP on a wireless LAN. How many simultaneous WLAN VOIP calls can be supported by an AP with Quality of Service enabled, assuming that the G.711 codec is used?

A. 64
B. 12
C. 8
D. 7
E. None without proxy ARP enabled

Answer: D

Explanation:
The following network capacity guidelines apply to sizing the Wireless IP Telephony network:
No more than 7 concurrent G.711 calls per AP.
No more than 8 concurrent G.729 calls per AP.
Reference:
http://www.cisco.com/en/US/products/hw/phones/ps379/products_implementation_design_guide_chapter09186a

---

QUESTION 401
What is eDCA?

A. The difference in the delay used by 802.11 management frames, and data frames
B. The time taken between the when a channel becomes free and a radio tries to send a frame
C. The standard 802.11 contention mechanism
D. A mechanism for adjusting the random backoff of WLAN traffic based in traffic classification
E. An authentication type for handheld devices

Answer: D

Explanation:
EDCA (Enhanced Distributed Channel Access) was specified in the 802.11e draft. EDCA, also known as prioritized DCF, improves on DCF by giving higher-priority traffic an advantage during contention. Instead of waiting the normal period before transmitting after the back-off period expires, higher-priority traffic can attempt to transmit only after a PIFS (point coordination function interframe space) period and associated back-off time. Using the EDCA scheme, nodes that offer high-priority traffic, an example being VoIP phones, have a higher probability of gaining channel access than the nodes offering lower-priority traffic, such as PC downloads.

QUESTION 402
The Certkiller network is utilizing Voice over Wireless LANs to provide for a mobile workforce. How would you design frequency overlap for voice over WLAN versus 802.11 for data only?

A. You would ensure that all areas where an 802.11 voice call could be initiated is covered by at least two RF infrastructure devices.
B. You would configure all the RF instrastructure devices to select optimal channels as required.
C. You would ensure each cell is at least 20% overlapped by second RF infrastructure device.
D. You would ensure all infrastructure RF devices were set to maximum power.
E. None of the above.

Answer: C

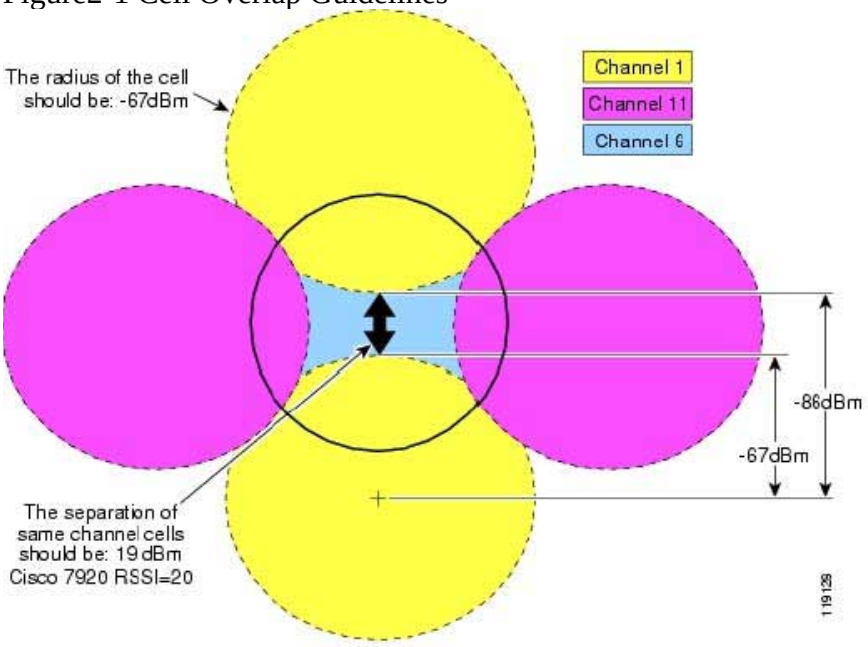
Explanation:
The critical components in the wireless network are the access points (APs) that provide the "hot spots" or wireless links to the network. Cisco requires that CiscoIOS is running on the APs that support voice calls since Cisco IOS provides features for managing voice traffic.
The AP has a transmission range or coverage area that depends on its type of antenna and transmission power. The access point coverage range generally varies from 500 to 1000 feet. To provide effective coverage, access points need a range overlap of approximately 20 percent to allow uninterrupted connections as phone users roam from one access point to another.
Reference:
http://www.cisco.com/en/US/products/hw/phones/ps379/products_administration_guide_chapter09186a0080246

QUESTION 403
The Certkiller network plans on using VOIP phones over the Wireless data network. When deploying a low latency wireless network, what are the key guidelines that should be maintained?

A. The access points requirements.
B. Use fixed channels, static WEP keys, all AP on the same channel.
C. Dynamic channels, diversity antenna, overlapping channels with more than 20% RSSI
D. Use fixed channels, diversity antenna, same transmit power on phone as the AP, overlapping channels have less than 20% RSSI.
E. Use fixed channels, CCKM, all AP on the channel, diversity antennas.

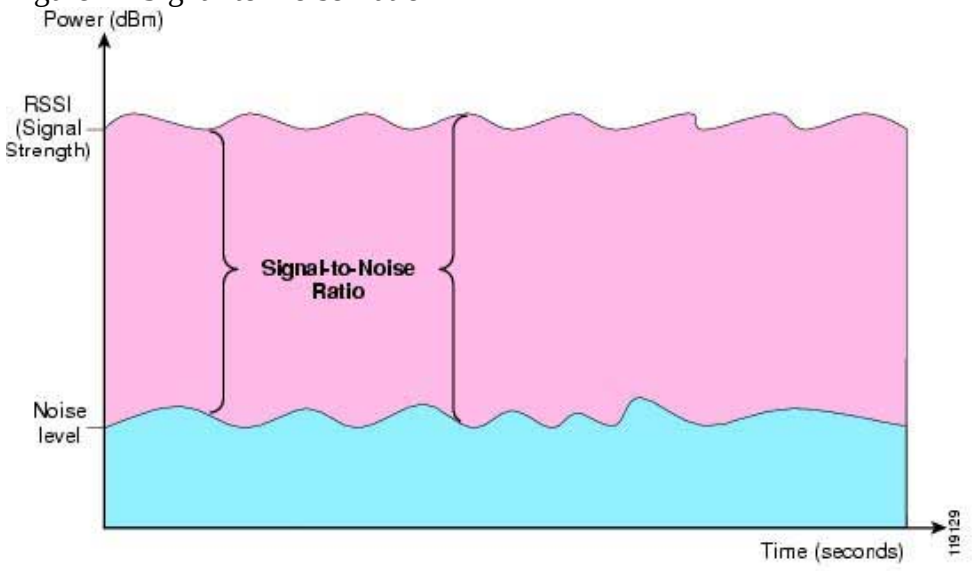
Answer: D

Explanation:
Recommended Environment for A Low Latency, VOIP network:
Deploy a minimum of two APs on non-overlapping channels, with a Received Signal Strength Indicator (RSSI) that is greater than 35 at all times in the phone's site survey utility.
Deploy no more than one AP per overlapping channel set, with a received signal strength indicator (RSSI) that is greater than 35.
Although APs might appear to have an RSSI that is less than 35 (on overlapping APs), this situation can still cause interference and should be minimized as much as possible. (This interference or noise will degrade voice quality.)
Noise is additive. Having three extra APs on the same channel, all with low RSSI, can be as harmful as a single extra AP with a higher RSSI.
Figure2-1 shows a typical deployment, with a 15% to 20% overlap of a given AP's cell from each of the adjoining cells. This configuration provides almost complete redundancy throughout the cell, thus complying with the above requirements.
Figure2-1 Cell Overlap Guidelines



Two of the APs (including the one with which the wireless phone is associated) must have an RSSI that is greater than 35 (which is equivalent to a receiver threshold of -67 decibels per milliwatt) and a channel utilization QoS Basis Service Set (QBSS) load that

is less than 45. This requirement provides for smoother roaming and a backup AP if one of the APs suddenly becomes unavailable or busy.
The QBSS load represents the percentage of time that the channel is in use by the AP. The overall channel load might be much higher than the QBSS load because several APs could be sharing the same RF channel and background or environmental noise could add to the load too. The Cisco7920 Wireless IP Phone uses the QBSS load in its roaming algorithm. The measured QBSS load will vary, depending on the time of day when you perform the site survey. For example, at night (when the network is largely idle), the QBSS load will usually be very low. Therefore, you should perform the site survey during peak hours. You can reduce the QBSS load by adding APs as needed.
Maintain at least 11Mbps of available link speed at all times for data clients as well as voice clients.
Maintain an AP coverage overlap of at least 15% to 20%.
Note:
In certain situations, data rates below 11 Mbps must be enabled for legacy devices. This lower speed will affect voice quality and the RF environment, and it is not the recommended setting. If you have to enable both 11Mbps and 2Mbps, these low speeds will reduce the number of simultaneous calls that each AP can handle and will also increase the overlap because they will extend the range of the APs.
Maintain a packet error rate (PER) no higher than 1% (or a success rate of 99%).
Maintain a minimum signal-to-noise ratio (SNR) of 25dB (see Figure2-2).
Figure2-2 Signal-to-Noise Ratio



Try to use the same transmit power on the AP and on the phones. If the transmit power of the APs varies, set the transmit power of the phones to the highest transmit power of the APs.
All AP antennas must use diversity.
APs in an optimal setting can handle seven G.711 or eight G.729 concurrent phone calls. If more concurrent phone calls are needed in a single location (a high usage area, for example), plan to have load-balancing APs available during the site survey. Overlapped basic service sets (BSSs, or APs sharing the same RF channel) reduce the number of concurrent phone calls per AP.

Reference:
http://www.cisco.com/en/US/products/hw/phones/ps379/products_implementation_design_guide_chapter09186a

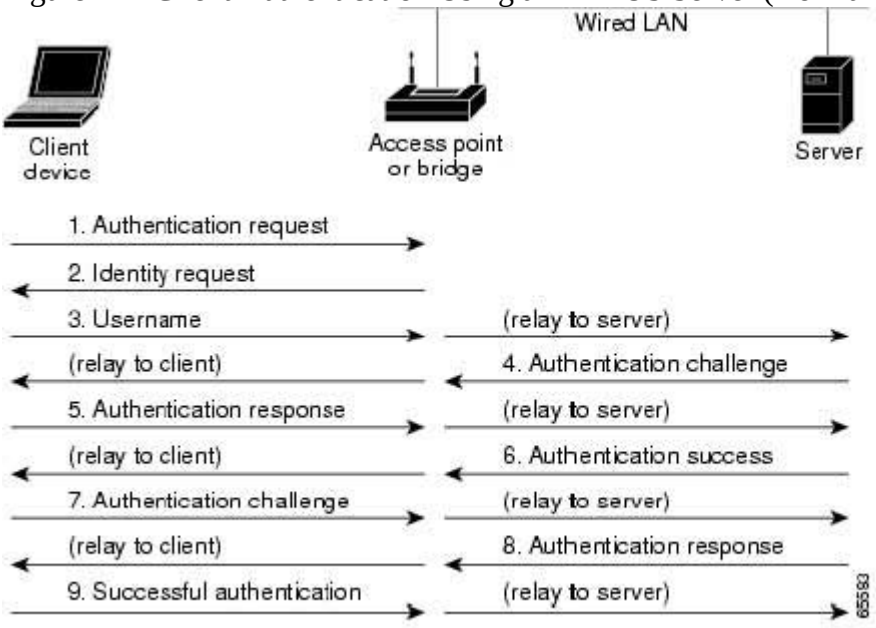
---

QUESTION 404
Within the Certkiller WLAN, fast secure roaming needs to be implemented to support wireless VOIP. What components are necessary when implementing fast secure L3 roaming?

A. AP, clients, WLSE
B. AP, CCX clients
C. AP, CCX clients WLSE
D. AP and clients
E. AP, CCX clients, WLSM

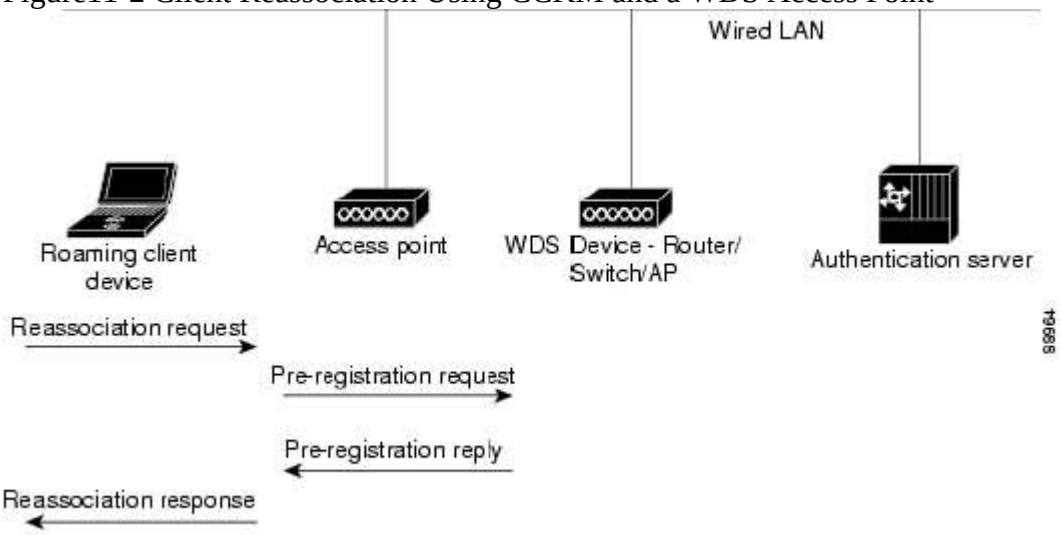
Answer: B

Explanation:
Access points in many wireless LANs serve mobile client devices that roam from access point to access point throughout the installation. Some applications running on client devices require fast reassociation when they roam to a different access point. Voice applications, for example, require seamless roaming to prevent delays and gaps in conversation.
During normal operation, LEAP-enabled client devices mutually authenticate with a new access point by performing a complete LEAP authentication, including communication with the main RADIUS server, as in Figure11-1.
Figure11-1 Client Authentication Using a RADIUS Server (Normal operation)



When you configure your wireless LAN for fast, secure roaming, however,

LEAP-enabled client devices roam from one access point to another without involving the main server. Using Cisco Centralized Key Management (CCKM), an access point configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client so quickly that there is no perceptible delay in voice or other time-sensitive applications. Figure11-2 shows client authentication using CCKM.
Figure11-2 Client Reassociation Using CCKM and a WDS Access Point



The WDS access point maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the client sends a reassociation request to the new access point, and the new access point relays the request to the WDS access point. The WDS access point forwards the client's credentials to the new access point, and the new access point sends the reassociation response to the client. Only two packets pass between the client and the new access point, greatly shortening the reassociation time. The client also uses the reassociation response to generate the unicast key.
Since the AP acts as the WDS, only a CCKM client and AP is required to configure the fast secure L3 roaming feature.
Reference:
http://www.cisco.com/en/US/products/ps5861/products_configuration_guide_chapter09186a008021e5d9.html#w

---

QUESTION 405
The Certkiller network has recently installed a Cisco Works Wireless LAN Solutions Engine (WLSE) to aid in the maintenance and management of the wireless LAN devices. When upgrading the firmware on access points, the WLSE can perform which of the following functions? (Choose the best option)

A. Upgrade firmware, validate the target AP type and convert configurations from VxWorks to IOS all at a scheduled time/date
B. Upgrade firmware of the access point only
C. Upgrade firmware, and convert configurations from VxWorks to IOS at a scheduled time/date

D. Update firmware, and convert configuration from VxWorks to IOS immediately

Answer: A

Explanation:
The WLSE is a hardware and software solution for managing Cisco wireless devices. The configuration feature allows you to apply a set of configuration changes to access points and connected switch ports. Using the firmware feature, you can upgrade the firmware on access points and bridges. You can also use the WLSE to schedule tasks to be performed at a later date, and to convert non-IOS (VxWorks) configuration file versions to IOS versions. Upon completion of any scheduled tasks, the WLSE attempts to verify that the task had indeed completed successfully.

QUESTION 406
The Certkiller network is utilizing the Cisco Wireless LAN Solution Engine (WLSE) to manage the structured WLAN. The WLSE Location Manager performs which of the following functions:

A. Discovers the location of APs, and the links them with imported site survey data
B. Is a separate module in the Catalyst 6500 providing location based services for Mobile Applications
C. Builds a database of APs location, that is used in device grouping, and radio management
D. Contains the location of AP management devices, allowing them to correlate GPS data
E. None of the above.

Answer: C

Explanation:
The CiscoWorks WLSE is a centralized, systems-level solution for managing the entire Cisco Aironet wireless LAN (WLAN) infrastructure. The advanced radio frequency (RF) and device management features of the CiscoWorks WLSE simplify the everyday operation of WLANs, ensure smooth deployment, enhance security, and maximize network availability, while reducing deployment and operating expense. The CiscoWorks WLSE enables administrators to detect, locate, and mitigate rogue access points and RF interference. The assisted site survey feature automates the previously manual, expensive, and time consuming process of determining optimal access point settings including transmit power and channel selection. The CiscoWorks WLSE automatically configures access points and bridges, assures the consistent application of security policies, and proactively monitors faults and performance. The CiscoWorks WLSE is a core component of the Cisco Structured Wireless-Aware Network.
The Location Manager is a GUI that displays wireless access points and bridges on a building floor plan. The location of rogue access points and RF interference is represented visually on the floor plan, as is the coverage area of each access point.

QUESTION 407
What is the primary purpose of a template in the WLSE?

A. A template is used to model the RF distribution pattern from Access Points in Location Manager.
B. Templates are used to set up a model for setting alarm levels in the WLSE.
C. A template is used as create a configuration model for Access Points in the network.
D. Templates push out configuration files to the Access Points.
E. Templates are used to generate firmware upgrades to the WLAN components.

Answer: C

Explanation:
The WLSE is a GUI based Cisco works based tool used to maintain and manage Cisco Wireless networks. It centrally identifies and configures Access Points (AP) in customer-defined groups and reports on throughput and client associations, enabling optimized wireless network performance and overall operational efficiency. WLSE's centralized management capabilities are further enhanced with an integrated template-based configuration tool for added configuration ease and improved productivity. You can think of a configuration template as a configuration update file for an access point. This file might contain the update for only one parameter or a complete access point configuration.

QUESTION 408
The Cisco Compatible Extensions Program (CCX) provides which of the following with regards to wireless networking?

A. A way for Cisco to avoid joining the standards bodies for wireless LAN
B. Cheaper wireless network.
C. A more secure wireless network.
D. Faster wireless network with faster L3 roaming times.
E. A way for Cisco to accelerate the deployment of wireless features.

Answer: E

Explanation:
The Cisco Compatible Extensions Program for WLAN devices provides tested compatibility with licensed Cisco infrastructure innovations. Compatibility is assured through extensive, independent testing of third-party. The Cisco Compatible Extensions Program enables the widespread availability of wireless client devices that take advantage of the Cisco wireless network, accelerating the availability of innovative features while maintaining interoperability.

QUESTION 409
As part of the new Certkiller wireless network implementation, the use of the WLSE Radio Manger is planned. What are the main functions of the Radio Manager in the

WLSE?

A. Rogue access point detection, interference detection and client walk about
B. Client walkabout, AP scanning, RM assisted configuration, self healing and auto re-site survey
C. Client walkabout, interference detection, rogue access point detection, location based services.
D. RM assisted configuration, rouge access point detection, interference detection, location based services.
E. None of the above.

Answer: C

Explanation:
Radio Management
The Radio Manager tab displays information to help you manage your WLAN radio environment. All the device information shown under this tab is polled from the managed devices in your network.
The Radio Manager tab includes these options:
* Radio Monitoring
* AP Radio Scan
* Client Walkabout
* Location Manager
* RM Assisted Configuration
* Manage RM Measurements
The Radio Manager features simplify the deployment, expansion, and day-to-day management of the WLAN by:
* Automatically configuring network-wide radio parameters during initial deployment and network expansion.
* Continuously monitoring the radio environment, detecting interference and rogue APs, and alerting the WLAN administrator to radio network changes.
* Providing information to help visualize the network radio topology, including the path loss between APs and RF coverage
The Radio Manager provides these features:
* Rogue AP detection
* Interference detection
* Automatic radio parameter generation
The Radio Manager can generate optimal values for the radio parameters of a given group of APs. Each set of radio parameters can modify the following:
* AP frequency
* AP transmit power
* AP beacon interval
You can also choose to run these features manually. The following table summarizes which procedures produce the data required by the different Radio Manager features:

Feature	Run these procedures	Results are used in:
Rogue AP detection	Radio Monitoring	Location Manager
	AP Radio Scan	Faults
Interference detection	Radio Monitoring	Faults
Automatic radio parameter generation	AP Radio Scan	RM Assisted Configuration
	Client Walkabout (recommended)	Location Manager
		Radio Manager Reports

The results produced by these features constitute the radio knowledge base. This knowledge base is saved in the WLSE database and accessed by other Radio Manager features.

QUESTION 410
The new Cisco WDS features are being implemented in the Certkiller wireless network. What is true of the Wireless Domain Service (WDS)?

A. It runs only on an AP, connects to WLSE, responsible for all authentications from other APs on the subnet.
B. It runs only on an AP, implements CCKM, implements QoS for the wireless traffic.
C. It often runs on the AP, implements CCKM, securely connects to other APs on the subnet, connects to the WLSE and delegates Radio Management jobs from the WLSE to all other APs.
D. It connects the WLSE to the other APs on the subnet and delegates RM jobs from the WLSE.
E. Often runs on the AP, securely connects to other APs on the subnet, connects to the WLSE and delegates Radio Management jobs from the WLSE to all other APs.

Answer: E

Explanation:
WDS is a new feature for access points in Cisco IOS Software. WDS is a core functionality that enables other features such as Fast Secure Roaming, Wireless LAN Solution Engine (WLSE) interaction, and Radio Management. Relationships between the access points that participate in WDS must be established before any of these other WDS-based features can work. One of the primary purposes for WDS is to eliminate the need to have the authentication server validate user credentials every time and thereby reduce the time required for client authentications.
Client authentication is defined by one or more client server groups on the WDS access points.
When a client attempts to associate to an infrastructure access point, the infrastructure access point passes the user's credentials to the WDS access point for evaluation. If it is the first time that the WDS access point has seen a given user's credentials, it uses the authentication server to validate the credentials. The WDS access point then caches the

user's credentials, so it does not have to return to the authentication server when that user attempts authentication again (for example, reauthentication for rekeying, for roaming, or for when the user starts up the client device).
Incorrect Answers:
A: The WDS also runs on the WLSE in addition to the AP.

QUESTION 411
A new Cisco Works Wireless LAN Sloutions Engine (WLSE) is being implemented into the Certkiller network. This WLSE does NOT perform what network management function?

A. Aggregating SNMP and syslogs from its managed APs.
B. SNMP queries of the APs
C. The aggregation of Radio Management data
D. CDP Discovery
E. The WLSE performs none of the above functions.

Answer: A

Explanation:
CiscoWorks WLSE may be transparently integrated with other network management systems, operations support systems, and CiscoWorks applications through syslog messages, Simple Network Management Protocol (SNMP) traps, and an Extensible Markup Language (XML) interface. Although the WLSE can be used with Syslog and SNMP servers, it can not be used as a Syslog or SNMP server. Syslog and SNMP messages can not be effectively sent to the WLSE from the access points.
Incorrect Answers:
B. One of the tools available via the WLSE is the SNMP Query Tool. This tool allows you to find the value of a specified SNMP variable. Normally, this tool is used under the direction of Cisco TAC when they are assisting you with troubleshooting a problem.
C. Following are some of the WLSE radio management features that are supported: Radio Monitoring, AP Radio Scan, Client Walkabout, RMAssisted Configuration, Self Healing, Auto Re-Site Survey, Location Manager.
D. By default, the WLSE runs a CDP discovery every 24 hours.
Reference:
http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_data_sheet0900aecd801d706e.html

---

QUESTION 412
An SSG is being utilized within the Certkiller Public Wireless LAN. What best describes the function of an SSG in a Public Wireless LAN (PWLAN)?

A. The SSG provides connectivity, client address management, security services, and routing across a WAN from each wireless access point to the service provider data center.
B. The SSG providees subscriber authentication and maintains the state of all users in the hotspot.

C. The SSG is an http proxy that provides captive portal capabilities to the service provider hot spot network.
D. 'The SSG is a central device that allows wireless clients to cross layer three subnets with sub-second roam times.
E. The SSG provides central management for the PWLAN hotspot network

Answer: B

Explanation:
Access control of the PWLAN is based on the extremely flexible Cisco IOS Service Selection Gateway (SSG) technology that is now available across a broad range of platforms, including the Cisco 2651XM Router , Cisco 2691 Router, Cisco 3725 Router, Cisco 3745 Router, Cisco 7200 Series, and Cisco 7301 Router. Together with the Cisco CNS Subscriber Edge Services Manager (SESM), the Cisco SSG provides subscriber authentication, service selection, service connection, and accounting capabilities to subscribers of Internet and intranet services.
The Cisco CNS SESM works with the Cisco SSG to provide complete control over the subscriber experience, supporting customization and personalization based on device, client, location, service, and other criteria to offer higher value to end users and maximize service and advertising revenue.
The Cisco SSG access control platform can proxy EAP authentication messages from hot-spot access points and automatically create user sessions upon successful EAP authentication, thereby eliminating the need for "double authentication," first at Layer 2 with 802.1x/EAP and then at Layer 3 through the Web portal. This feature allows an operator to take advantage of the Cisco SSG for centralized accounting record generation for both 802.1x/EAP and Web-authenticated users.
Reference:
http://www.cisco.com/en/US/netsol/ns341/ns396/ns177/ns436/netbr09186a00801f9f3d.html

---

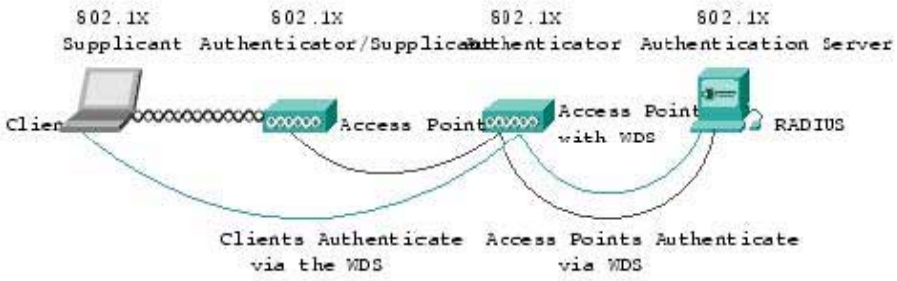
QUESTION 413
In the Wireless Certkiller network, Layer 2 Fast Secure Roaming technology has been implemented. Layer 2 Fast Secure Roaming is enabled by what type of device?

A. An ACS or other AAA server
B. A device running as a WDS
C. The Ethernet switch
D. The WLSE
E. A firewall

Answer: B

Explanation:
In Layer 2 Fast Secure Roaming, the Wireless Domain Services (WDS) act as a central authentication entity that supports a fast client rekey, rather than requiring a full RADIUS reauthentication each time the client roams. All access points and clients in a L2 domain 802.1X authenticate to a RADIUS server via the WDS that performs the role

of 802.1X authenticator. Because all clients and access points authenticate via the WDS, the WDS is able to establish shared keys between itself and every other entity in the L2 domain. These shared keys enable CCKM fast secure roaming. The following diageam illustrates access points and clients authenticating to WDS.



The WDS function is written in Cisco IOS Software and initially runs on Cisco IOS Software on Cisco Aironet access points only. In the future, WDS be available in Cisco router and switch infrastructure products.
At least one WDS is required per L2 domain. The CCKM architecture supports WDS redundancy via a MAC-layer multicast primary WDS election process. If redundant WDS are configured, the WDS with the highest priority is elected to be the primary WDS. If equal or no priorities are configured, a primary is dynamically determined. Redundancy provides a cold backup. If the primary WDS fails, all authenticated clients continue to operate, until a roaming event occurs, at which point the client completes a full initial authentication to the RADIUS server, via the backup WDS. All access points in a L2 domain dynamically learn the address of the active WDS via an L2 multicast. The address of the WDS is not configured in any access point.
Reference:
http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00801c5223.html#wp

---

QUESTION 414
The WLSE and the WLSM perform which roles in the wireless network?

A. WLSE is responsible for management and the WLSM is responsible for Mobility.
B. WLSE is responsible for security and the WLSM is responsible for Management.
C. WLSM is responsible for management and the WLSE is responsible for Mobility.
D. WLSM is responsible for security and the WLSE is responsible for Management.
E. WLSE is responsible for security and the WLSM is responsible for Mobility.

Answer: A

Explanation:
The Cisco Wireless LAN Services Module (WLSM) integrates wired and wireless network services in very large enterprises. It also enables fast secure inter-subnet roaming, which is particularly important for latency-sensitive applications such as wireless voice. Its fundamental purpose is to provide for mobile wireless networking.

The Cisco Works Wireless LAN Solution Engine (WLSE) manages and secures the radio-frequency (RF) airspace - to deliver the scalable management, security, and RF control enterprises required to deploy very large, stable wireless networks.
Reference:
http://www.cisco.com/en/US/about/ac123/ac114/ac173/Q3-04/ent_routed.html

---

QUESTION 415
How does a router behave in relation to an EIGRP stub neighbor?

A. It will send only default-routes toward stub EIGRP neighbors.
B. It well send only summary routes toward stub EIGRP neighbors.
C. It will not query the stub EIGRP neighbor about any internal route.
D. It will not query the stub EIGRP neighbor about any external route.
E. It will not query the stub EIGRP neighbor about any route.

Answer: E

QUESTION 416
An interface has been configured for custom queuing. Bandwidth has been allocated for three flows A, B and C with average packet sizes of 1000 bytes, 500 bytes and 250 bytes respectively. If flow A has been configured to allow one packet per servicing of its queue, how many packets need to be allowed for flow C in order to achieve a ratio of 20:50:30 for flows A, B and C respectively?

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

Answer: F

QUESTION 417
What effect do these configuration commands have?
line vty 0 4
no login
password cisco

A. The VTY password is cisco.
B. The login password is login
C. The VTY password is required but not set.
D. No password is required for VTY access.

Answer: D

QUESTION 418
Multicast addresses in the range of 239.0.0.0 through 239.255.255.255 are reserved for:

A. Administratively Scoped multicast traffic that is intended to remain inside of a private network and is never intended to be transmitted into the Internet.
B. Global Internet multicast traffic intended to travel throughout the Internet.
C. Link-local multicast traffic consisting of network control messages that never leave the local subnet.
D. Any valid multicast data stream.

Answer: A

QUESTION 419
What is the tiebreaker used by ISIS to elect the Designated IS on a LAN in a case where all the neighbors
have the same priority?

A. The lowest MAC address.
B. The highest router-ID.
C. The lowest router-ID.
D. The highest SNPA.
E. The lowest system-ID.

Answer: D

QUESTION 420
When using a sniffer directly connected to an access switch, the sniffer sees an excessive amount of BPDUs with the TCA bit set.
Which are the most likely explanations?

A. There are no problem in the network.
B. Ports connecting 2 workstations do not have spanning tree portfast configured.
C. Bad cabling is being used in the network.
D. The CPU utilization on the root switch is getting up to 99% and thus is not sending any BPDUs.

Answer: B, C

QUESTION 421
A network administrator is using a private IP address space for the network with NAT to allow the users to reach the Internet. However, there is a web server on the internal network that must have incoming access from the Internet. What will be required to accomplish this?

A. Put the web server's internal IP address in the external DNS records.

B. Use a dynamic mapping with the reverse keyword.
C. There must be a static NAT mapping for the web server's address.
D. Dynamic NAT will take care of this automatically.

Answer: C

Explanation:
Without a static NAT mapping, the server will be NATed out of the NAT pool. no outside stations will be able to reach him consistently.

QUESTION 422
Exhibit:
Routing protocols which run between the different routers are indicated in the image. On Router CK3 RIPv2 is being redistributed into EIGRP. No other redistribution is done to the network. Knowing this, who owns the route for subnet 100.10.1.0/24 in the routing table of Router CK1 ?

A. Internal EIGRP.
B. External EIGRP.
C. Nobody, the route is not in the routing table of Router CK1 , nor in the EIGRP topology table.
D. The route is not in the routing table of Router CK1 but is in the EIGRP topology table.
E. The route is not in the routing table of Router CK1 but is in the EIGRP topology table as an active route.

Answer: B

QUESTION 423
What is not a transfer mode supported by HDLC?

A. ARM
B. ARB
C. ABM
D. NRM
E. LAPB

Answer: B

QUESTION 424
Exhibit:
Router#show ip mroute 236.82.134.23
IP Multicast Routing table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
R - RP-bit set, F - Register flag, T - SPT-bit set, J - JOIN SPT
X - Proxy Join Timer Running
Timers: uptime/Expires

Interface state: Interface, next-hop or VCD, State/Mode
(*, 236.82.134.23), 00:09:49/00:04:23 RP 172.16.224.1, flags: SC
Incoming interface: Serial1.708, RPF nbr 172.16.2.242
Outgoing interface list:
Ethernet0, Forward/Sparse, 00:09:50/00:04:12
Given the output of the show ip mroute command shown, what is the IP address of the Upstream Neighbor on the Shared Tree?

A. 172.6.224.1
B. 192.168.1.1
C. 172.16.2.242
D. 172.16.3.254
E. It is not possible to determine the Upstream Neighbor from this information.

Answer: C

QUESTION 425
According to the IEEE 802.2 Logical Link Control specification, the maximum transmit value for LLC flow control is:

A. 15
B. 127
C. 255
D. 1023
E. 4095

Answer: D

QUESTION 426
The interface command Router (config-if)# invert txclock is used for what purpose?

A. It switches TXD and RXD to correct mis-wired cables.
B. It corrects systems that use long cables that experience high error rates when operating at the higher transmission speeds.
C. It configures the serial interface to monitor the DSR signal as the line up/down indicator.
D. It is used to correct situations where it is possible to send back-to-back data packets over serial interfaces faster than some hosts can receive them.

Answer: B

QUESTION 427
Current configuration:
!
version 12.0
service timestamps debug uptime

service timestamps log update
no service password-encryption
!
hostname Simon
!
enable secret 5 1XV53$hqb0Ra7gwpky0cmL4u3EW0
enable password cisco
Given the configuration shown above, what should you type to gain enable access on router Simon?

A. cisco
B. Simon
C. 4u3EW0
D. 1XV53$hqb0Ra7gwpky0cmL4u3EW0
E. Cannot tell

Answer: E

Explanation:
The enable secret password takes precedence over the enable password. in this example, the enable secret is encrypted. you would need to type the unencrypted password to gain access.

QUESTION 428
What statement is true concerning Multilayer Switching?

A. The first packet in every flow will be forwarded by the MLS Switching Engine.
B. The first packet in every flow will be forwarded by the MLS Route Processor.
C. Every 10th packet in every flow will be redirected to the MLS Route Processor.
D. Every 100th packet in every flow will be forwarded by the MLS Route Processor.
E. All traffic will be forwarded by the MLS Switching Engine.

Answer: B

QUESTION 429
Configuration:
interface ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip summary address rip 10.0.0.0 255.255.0.0
half-duplx
!!
Router rip
network 10.0.0.0
You have configured RIPV2 sumarization on R1 if eth0/0 but the routes still are not being summarized. Looking at the partial configuration what could be the problem:

A. you need to enable auto sumarization under rip process
B. you need to disable auto sumarization under rip process
C. RIP does not support sumarization on interface basis
D. split horizon is enabled on int e0/0
E. None of above

Answer: E