Exam : 642-845

Title : ONT - Optimizing Converged Cisco Networks

Ver : 07.31.07

QUESTION 1

You need to implement QoS for the Certkiller VOIP network. Which three statements are true about the data traffic characteristics of voice traffic? (Select three)

A. Voice packets require TCP for rapid retransmission of dropped packets.
B. Latency is not a concern as long as jitter is kept below 30 ms.
C. Voice packets require a fairly constant bandwidth reserved for voice control traffic as well as for the voice payload.
D. Voice packets do not require a specific type of queuing.
E. Latency must be kept below 150 ms.
F. Voice packets are rather small

Answer: C, E, F

Explanation:
QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies including Frame Relay, ATM, Ethernet and 802.3 networks, SONET, and IP-routed networks.
QoS features provide improved and more predictable network service by offering the following services:
1. Dedicated bandwidth
2. Improved loss characteristics
3. Congestion management and avoidance
4. Traffic shaping
5. Prioritization of traffic
Voice quality is directly affected by all three QoS quality factors such as loss, delay, and delay variation.
Loss causes voice clipping and skips. Industry standard codec algorithms can correct for up to 30 ms of lost voice. Cisco Voice over IP (VoIP) technology uses 20 ms samples of voice payload per VoIP packet. Only a single Real Time Transport (RTP) packet could be lost at any given time. If two successive voice packets are lost, the 30 ms correctable window is exceeded and voice quality begins to degrade.
Delay can cause voice quality degradation if it is above 200 ms. If the end-to-end voice delay becomes too long, the conversation sounds as if two parties are talking over a satellite link or a CB radio. The ITU standard for VoIP, G.114, states that a 150 ms one-way delay budget is acceptable for high voice quality. With respect to delay variation, there are adaptive jitter buffers within IP Telephony devices. These buffers can usually compensate for 20 to 50 ms of jitter.

QUESTION 2

Certkiller uses G.711 for the VOIP calls. When analog signals are digitized using the G.711 codec, voice samples are encapsulated into protocol data units (PDUs) involving which three headers? (Select three)

A. UDP
B. RTP
C. IP
D. TCP
E. Compressed RTP
F. H.323

Answer: A, B, C

Explanation:
When a VoIP device, such as a gateway, sends voice over an IP network, the digitized voice has to be encapsulated into an IP packet. Voice transmission requires features not provided by the IP protocol header; therefore, additional transport protocols have to be used. Transport protocols that include features required for voice transmission are TCP, UDP, and RTP. VoIP utilizes a combination of UDP and RTP.

QUESTION 3
VOIP has been rolled out to every Certkiller location. What are three features and functions of voice (VOIP) traffic on a network? (Select three)

A. Voice traffic is bursty
B. Voice traffic is retransmittable
C. Voice traffic is time-sensitive
D. Voice traffic is bandwidth intensive
E. Voice traffic is constant
F. Voice traffic uses small packet sizes

Answer: C, E, F

Explanation:
The benefits of packet telephony networks include
i. More efficient use of bandwidth and equipment: Traditional telephony networks use a 64-kbps channel for every voice call. Packet telephony shares bandwidth among multiple logical connections.
ii. Lower transmission costs: A substantial amount of equipment is needed to combine 64-kbps channels into high-speed links for transport across the network. Packet telephony statistically multiplexes voice traffic alongside data traffic. This consolidation provides substantial savings on capital equipment and operations costs.
iii. Consolidated network expenses: Instead of operating separate networks for voice and data, voice networks are converted to use the packet-switched architecture to create a single integrated communications network with a common switching and transmission system. The benefit is significant cost savings on network equipment and operations.
iv. Improved employee productivity through features provided by IP telephony: IP phones are not only phones, they are complete business communication devices. They offer directory lookups and access to databases through Extensible Markup Language (XML) applications. These applications allow simple integration of telephony into any

business application. For instance, employees can use the phone to look up information about a customer who called in, search for inventory information, and enter orders. The employee can be notified of a issue (for example, a change of the shipment date), and with a single click can call the customer about the change. In addition, software-based phones or wireless phones offer mobility to the phone user.

QUESTION 4
Certkiller is rolling out an H.323 VOIP network using Cisco devices. Which IOS feature provides dial plan scalability and bandwidth management for H.323 VoIP implementations?

A. Digital Signal Processors
B. Call Routing
C. Gatekeeper
D. Call Admission Control
E. None of the above

Answer: C

Explanation:
Enterprise voice implementations use components such as gateways, gatekeepers, Cisco Unified CallManager, and IP phones. Cisco Unified CallManager offers PBX-like features to IP phones. Gateways interconnect traditional telephony systems, such as analog or digital phones, PBXs, or the public switched telephone network (PSTN) to the IP telephony solution. Gatekeepers can be used for scalability of dial plans and for bandwidth management when using the H.323 protocol.

QUESTION 5
A Cisco router is being used as a VOIP gateway to convert voice signals in the Certkiller network. What steps are taken when a router converts a voice signal from analog to digital form? (Select two)

A. Quantization
B. Serialization
C. Packetization
D. Sampling

Answer: A, D

Explanation:
Step 1 Sampling: The analog signal is sampled periodically. The output of the sampling is a pulse amplitude modulation (PAM) signal.
Step 2 Quantization: The PAM signal is matched to a segmented scale. This scale measures the amplitude (height) of the PAM signal.
Step 3 Encoding: The matched scale value is represented in binary format.
Step 4 Compression: Optionally, voice samples can be compressed to reduce bandwidth

requirements. Analog-to-digital conversion is done by digital signal processors (DSPs), which are located on the voice interface cards. The conversion is needed for calls received on analog lines, which are then sent out to a packet network or to a digital voice interface.

QUESTION 6

You need to implement the proper IOS tools to ensure that VOIP works over the Certkiller network. Which queuing and compression mechanisms are needed to effectively use the available bandwidth for voice traffic? (Select two)

A. Priority Queuing (PQ) or Custom Queuing (CQ)
B. Real-Time Transport Protocol (RTP) header compression
C. Low Latency Queuing (LLQ)
D. Class-Based Weighted Fair Queuing (CBWFQ)
E. TCP header compression
F. UDP header compression

Answer: D, E

Explanation:
1. Class-based weighted fair queuing (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. By using CBWFQ, network managers can define traffic classes based on several match criteria, including protocols, access control lists (ACLs), and input interfaces. A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class. More than one IP flow, or "conversation", can belong to a class.
Once a class has been defined according to its match criteria, the characteristics can be assigned to the class. To characterize a class, assign the bandwidth and maximum packet limit. The bandwidth assigned to a class is the guaranteed bandwidth given to the class during congestion.
CBWFQ assigns a weight to each configured class instead of each flow. This weight is proportional to the bandwidth configured for each class. Weight is equal to the interface bandwidth divided by the class bandwidth. Therefore, a class with a higher bandwidth value will have a lower weight.
By default, the total amount of bandwidth allocated for all classes must not exceed 75 percent of the available bandwidth on the interface. The other 25 percent is used for control and routing traffic.
The queue limit must also be specified for the class. The specification is the maximum number of packets allowed to accumulate in the queue for the class. Packets belonging to a class are subject to the bandwidth and queue limits that are configured for the class.
2. TCP/IP header compression subscribes to the Van Jacobson Algorithm defined in RFC 1144. TCP/IP header compression lowers the overhead generated by the disproportionately large TCP/IP headers as they are transmitted across the WAN. TCP/IP header compression is protocol-specific and only compresses the TCP/IP header. The Layer 2 header is still intact and a packet with a compressed TCP/IP header can still travel across a WAN link.

TCP/IP header compression is beneficial on small packets with few bytes of data such as Telnet. Cisco's header compression supports Frame Relay and dial-on-demand WAN link protocols. Because of processing overhead, header compression is generally used at lower speeds, such as 64 kbps links.

QUESTION 7
You want to ensure the highest call quality possible for all VOIP calls in the Certkiller network. Which codec standard would provide the highest voice-quality, mean opinion score (MOS)?

A. G.711, PCM
B. G.729, CS-ACELP
C. G.729A, CS-ACELP
D. G.728, LDCELP
E. None of the above

Answer: A

Explanation:
When a call is placed between two phones, the call setup stage occurs first. As a result of this process, the call is logically set up, but no dedicated circuits (lines) are associated with the call. The gateway then converts the received analog signals into digital format using a codec, such as G.711 or G.729 if voice compression is being used.
When analog signals are digitized using the G.711 codec, 20 ms of voice consists of 160 samples, 8 bits each. The result is 160 bytes of voice information. These G.711 samples (160 bytes) are encapsulated into an RTP header (12 bytes), a UDP header (8 bytes), and an IP header (20 bytes). Therefore, the whole IP packet carrying UDP, RTP, and the voice payload has a size of 200 bytes. When G.711 is being used, the ratio of header to payload is smaller because of the larger voice payload. Forty bytes of headers are added to 160 bytes of payload, so one-fourth of the G.711 codec bandwidth (64 kbps) has to be added. Without Layer 2 overhead, a G.711 call requires 80 kbps.

QUESTION 8
When a router converts analog signals to digital signals as part of the VoIP process, it performs four separate steps. From the options shown below, which set of steps contains the steps in their correct sequence?

A. encoding
quantization
optional compression
sampling
B. optional compression
encoding
sampling
quantization
C. sampling

quantization
encoding
optional compression
D. optional compression
sampling
encoding
quantization
E. sampling
quantization
optional compression
encoding
F. encoding
optional compression
quantization
sampling
G. None of the above

Answer: C

Explanation:
Step 1 Sampling: The analog signal is sampled periodically. The output of the sampling is a pulse amplitude modulation (PAM) signal.
Step 2 Quantization: The PAM signal is matched to a segmented scale. This scale measures the amplitude (height) of the PAM signal.
Step 3 Encoding: The matched scale value is represented in binary format.
Step 4 Compression:
Optionally, voice samples can be compressed to reduce bandwidth requirements.
Analog-to-digital conversion is done by digital signal processors (DSPs), which are located on the voice interface cards. The conversion is needed for calls received on analog lines, which are then sent out to a packet network or to a digital voice interface.

QUESTION 9
Certkiller has determined that during its busiest hours, the average number of internal VoIP calls across the WAN link is four (4). Since this is an average, the WAN link has been sized for six (6) calls with no call admission control. What will happen when a seventh call is attempted across the WAN link?

A. The seventh call is routed via the PSTN.
B. The call is completed, but all calls have quality issues.
C. The call is completed but the seventh call has quality issues.
D. The call is denied and the original six (6) calls remain.
E. The call is completed and the first call is dropped.
F. None of the above.

Answer: B

Explanation:
IP telephony solutions offer Call Admission Control (CAC), a feature that artificially limits the number of concurrent voice calls to prevent oversubscription of WAN resources.
Without CAC, if too many calls are active and too much voice traffic is sent, delays and packet drops occur. Even giving Real-Time Transport Protocol (RTP) packets absolute priority over all other traffic does not help when the physical bandwidth is not sufficient to carry all voice packets. Quality of service (QoS) mechanisms do not associate individual RTP packets with individual calls; therefore, all RTP packets are treated equally. All RTP packets will experience delays, and any RTP packets may be dropped. The effect of this behavior is that all voice calls experience voice quality degradation when oversubscription occurs. It is a common misconception that only calls that are beyond the bandwidth limit will suffer from quality degradation. CAC is the only method that prevents general voice quality degradation caused by too many concurrent active calls.

QUESTION 10
While planning the new Certkiller VOIP network, you need to determine the size of the WAN links to use. To do this, you need to calculate the bandwidth required by each call. Which three pieces of information are used to calculate the total bandwidth of a VoIP call? (Select three)

A. The serialization of the interface
B. The quantization
C. The TCP overhead
D. The packetization size
E. The UDP overhead
F. The packet rate

Answer: D, E, F

Explanation:
Packet rate: Packet rate specifies the number of packets sent in a certain time interval. The packet rate is usually specified in packets per second (pps). Packet rate is the multiplicative inverse of the packetization period. The packetization period is the amount of voice (time) that will be encapsulated per packet, and is usually specified in milliseconds.
Packetization size: Packetization size specifies the number of bytes that are needed to represent the voice information that will be encapsulated per packet. Packetization size depends on the packetization period and the bandwidth of the codec used.
IP overhead: IP overhead specifies the number of bytes added to the voice information during IP encapsulation. When voice is encapsulated into Real-Time Transport Protocol (RTP), User Datagram Protocol (UDP), and IP, the IP overhead is the sum of all these headers.
Data link overhead: Data-link overhead specifies the number of bytes added during data-link encapsulation. The data-link overhead depends on the used data-link protocol,

which can be different per link.
Tunneling overhead: Tunneling overhead specifies the number of bytes added by any security or tunneling protocol, such as 802.1Q tunneling, IPsec, Generic Route Encapsulation (GRE), or Multiprotocol Label Switching (MPLS). This overhead must be considered on all links between the tunnel source and the tunnel destination.

QUESTION 11
Certkiller uses the distributed call processing model in their VOIP network. Which statement is true about the distributed call control in a VoIP network?

A. The VoIP endpoints have the intelligence to set up and control calls.
B. Call setup and control resides in call agents that are distributed throughout the network.
C. Call setup and control functionality is centralized in one call agent or cluster.
D. Each VoIP device has separate call control, voice packetization, and transport mechanisms.
E. None of the above.

Answer: A

Explanation:
Distributed call control is possible where the voice-capable device is configured to support call control directly. This is the case when protocols such as H.323 or SIP are enabled on the end devices. With distributed call control, the devices perform the call setup, call maintenance, and call teardown on their own. With distributed call control, each gateway makes its own, autonomous decisions and does not depend on the availability of another (centralized) device to provide call routing services to the gateway. Because each gateway has its own intelligence, there is no single point of failure. However, each gateway needs to have a local call routing table, which has to be configured manually. Therefore, administration of the distributed call control model is less scalable.

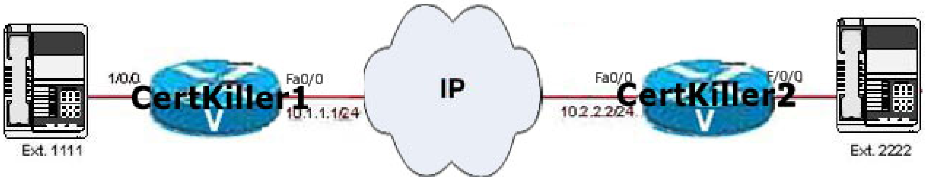
QUESTION 12
A Certkiller branch office has 15 IP phones connected to the main office using the distributed call processing model. Normally, the phones work with great quality. However, during very busy times when all of the agents are on the phone at the same time, the voice quality drops. Words, phrases, or both are dropped from conversations. What is the most likely cause of the problem?

A. Employees are watching videos over the Internet.
B. Header compression is not being used.
C. Call Admission Control has not been implemented.
D. More bandwidth is required for the office LAN.
E. IP phone traffic is not being classified correctly.
F. Large files are being downloaded over the WAN network.
G. None of the above.

Answer: C

Explanation:
IP telephony solutions offer Call Admission Control (CAC), a feature that artificially limits the number of concurrent voice calls to prevent oversubscription of WAN resources.
Without CAC, if too many calls are active and too much voice traffic is sent, delays and packet drops occur. Even giving Real-Time Transport Protocol (RTP) packets absolute priority over all other traffic does not help when the physical bandwidth is not sufficient to carry all voice packets. Quality of service (QoS) mechanisms do not associate individual RTP packets with individual calls; therefore, all RTP packets are treated equally. All RTP packets will experience delays, and any RTP packets may be dropped. The effect of this behavior is that all voice calls experience voice quality degradation when oversubscription occurs. It is a common misconception that only calls that are beyond the bandwidth limit will suffer from quality degradation. CAC is the only method that prevents general voice quality degradation caused by too many concurrent active calls.

QUESTION 13
Standard phones connect to Cisco router gateways as shown below:



Study the exhibit above carefully. Routers Certkiller 1 and Certkiller 2 are to be configured as VoIP gateways. On the basis of the information in the exhibit, which interface FastEthernet 0/0 configuration would be valid?

A. Certkiller 1(config-if)# dial-peer voice 1 voip
Certkiller 1(config-dial-peer)# destination-pattern 1111
Certkiller 1(config-dial-peer)# port 1/0/0
B. Certkiller 1(config-if)# dial-peer voice 1 pots
Certkiller 1(config-dial-peer)# destination-pattern 1111
Certkiller 1(config-dial-peer)# port 1/0/0
C. Certkiller 2(config-if)# dial-peer voice 1 voip
Certkiller 2(config-dial-peer)# destination-pattern 1111
Certkiller 2(config-dial-peer)# port 1/0/0
D. Certkiller 2(config-if)# dial-peer voice 1 pots
Certkiller 2(config-dial-peer)# destination-pattern 1111
Certkiller 2(config-dial-peer)# port 1/0/0
E. None of the above

Answer: B

Explanation:
Voice-Specific Commands

Command	Description
dial-peer voicetag type	Use the dial-peer voice command to enter the dial peer subconfiguration mode. The tag value is a number that has to be unique for all dial peers within the same gateway. The type value indicates the type of dial peer (for example, POTS or VoIP).
destination-pattern telephone_number	The destination-pattern command, entered in dial peer subconfiguration mode, defines the telephone number that applies to the dial peer. A call placed to this number will be routed according to the configuration type and port (in the case of a POTS type dial peer) or session target (in the case of a VoIP type dial peer) of the dial peer.
portport-number	The port command, entered in POTS dial peer subconfiguration mode, defines the port number that applies to the dial peer. Calls that are routed using this dial peer are sent to the specified port. The port command can be configured only on a POTS dial peer.
session target ipv4:ip-address	The session target command, entered in VoIP dial peer subconfiguration mode, defines the IP address of the target VoIP device that applies to the dial peer. Calls that are routed using this dial peer are sent to the specified IP address. The session target command can be configured only on a VoIP dial peer.

QUESTION 14

Call Admission Control is being utilized in the Certkiller VOIP network. Which two statements are true about CAC? (Select two)

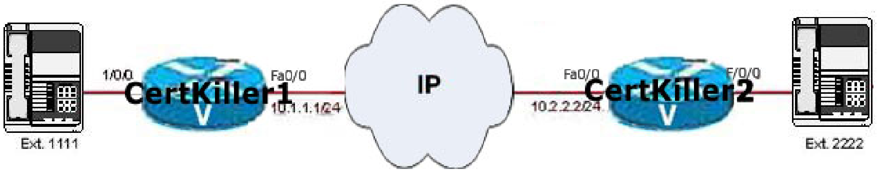
A. CAC is implemented in the call maintenance phase to allocate bandwidth resources.
B. CAC is implemented in the call setup phase to determine the destination of the call.
C. CAC is implemented in the call setup phase to allocate bandwidth resources.
D. CAC uses the Cisco RSVP (Resource Reservation Protocol) Agent to integrate call-processing capabilities with the underlying network infrastructure.
E. CAC is utilized during the call teardown phase to ensure that all resources have been released.

Answer: C, D

Explanation:
IP telephony solutions offer Call Admission Control (CAC), a feature that artificially limits the number of concurrent voice calls to prevent oversubscription of WAN resources.
Without CAC, if too many calls are active and too much voice traffic is sent, delays and packet drops occur. Even giving Real-Time Transport Protocol (RTP) packets absolute priority over all other traffic does not help when the physical bandwidth is not sufficient to carry all voice packets. Quality of service (QoS) mechanisms do not associate individual RTP packets with individual calls; therefore, all RTP packets are treated equally. All RTP packets will experience delays, and any RTP packets may be dropped. The effect of this behavior is that all voice calls experience voice quality degradation when oversubscription occurs. It is a common misconception that only calls that are beyond the bandwidth limit will suffer from quality degradation. CAC is the only method that prevents general voice quality degradation caused by too many concurrent active calls.

QUESTION 15

Part of the Certkiller VOIP network is shown below:



Study the exhibit carefully. Routers Certkiller 1 and Certkiller 2 are to be configured as VoIP gateways. Based on the information shown, which interface FastEthernet 0/0 configuration would be valid?

A. Certkiller 1(config-if)# dial-peer voice 2 voip
Certkiller 1(config-dial-peer)# destination-pattern 1111
Certkiller 1(config-dial-peer)# session target ipv4:10.1.1.1
B. Certkiller 2(config-if)# dial-peer voice 2 pots
Certkiller 2(config-dial-peer)# destination-pattern 1111
Certkiller 2(config-dial-peer)# session target ipv4:10.1.1.1

C. Certkiller 2(config-if)# dial-peer voice 2 voip
Certkiller 2(config-dial-peer)# destination-pattern 1111
Certkiller 2(config-dial-peer)# session target ipv4:10.1.1.1
D. Certkiller 1(config-if)# dial-peer voice 2 pots
Certkiller 1(config-dial-peer)# destination-pattern 1111
Certkiller 1(config-dial-peer)# session target ipv4:10.1.1.1
E. None of the above

Answer: C

Explanation:
Voice-Specific Commands

Command	Description
dial-peer voicetag type	Use the dial-peer voice command to enter the dial peer subconfiguration mode. The tag value is a number that has to be unique for all dial peers within the same gateway. The type value indicates the type of dial peer (for example, POTS or VoIP).
destination-pattern telephone_number	The destination-pattern command, entered in dial peer subconfiguration mode, defines the telephone number that applies to the dial peer. A call placed to this number will be routed according to the configuration type and port (in the case of a POTS type dial peer) or session target (in the case of a VoIP type dial peer) of the dial peer.
portport-number	The port command, entered in POTS dial peer subconfiguration mode, defines the port number that applies to the dial peer. Calls that are routed using this dial peer are sent to the specified port. The port command can be configured only on a POTS dial peer.

session target ipv4:ip-address	The session target command, entered in VoIP dial peer subconfiguration mode, defines the IP address of the target VoIP device that applies to the dial peer. Calls that are routed using this dial peer are sent to the specified IP address. The session target command can be configured only on a VoIP dial peer.

QUESTION 16

You want to ensure the highest level of audio quality in the Certkiller VOIP network. Which two statements are true about the digital audio in a VoIP network? (Select two)

A. Standard encoding techniques create an uncompressed digital data rate of 8000 bps.
B. Two methods of compression are u-law and a-law
C. Standard encoding techniques create an uncompressed digital data rate of 64,000 bps.
D. Two methods of quantization are linear and logarithmic.
E. Standard encoding techniques create an uncompressed digital data rate of 4000 bps.
F. Voice quality is not a concern if compression is not used.

Answer: C, D

Explanation:
Each sample is encoded in the following way:
One polarity bit: Indicates positive versus negative signals
Three segment bits: Identify the logarithmically sized segment number (0-7)
Four step bits: Identify the linear step within a segment.
Because 8000 samples per second are taken for telephony, the bandwidth that is needed per call is 64 kbps. This is the reason why traditional, circuit-based telephony networks use time-division-multiplexed lines, combining multiple channels of 64 kbps each (digital signal level 0 [DS-0]) in a single physical

QUESTION 17

Call Admission Control is being used on the Certkiller VOIP WAN. Which two statements are true about the function of CAC? (Select two)

A. CAC solves voice congestion problems by using QoS to give priority to UDP traffic.
B. CAC prevents oversubscription of WAN resources that is caused by too much voice traffic.
C. CAC artificially limits the number of concurrent voice calls.
D. CAC provides guaranteed voice quality on a link.
E. CAC is used to control the amount of bandwidth that is taken by a call on a link.

F. CAC allows an unlimited number of voice calls while severely restricting, if necessary, other forms of traffic.

Answer: B, C

Explanation:
IP telephony solutions offer Call Admission Control (CAC), a feature that artificially limits the number of concurrent voice calls to prevent oversubscription of WAN resources.
Without CAC, if too many calls are active and too much voice traffic is sent, delays and packet drops occur. Even giving Real-Time Transport Protocol (RTP) packets absolute priority over all other traffic does not help when the physical bandwidth is not sufficient to carry all voice packets. Quality of service (QoS) mechanisms do not associate individual RTP packets with individual calls; therefore, all RTP packets are treated equally. All RTP packets will experience delays, and any RTP packets may be dropped. The effect of this behavior is that all voice calls experience voice quality degradation when oversubscription occurs. It is a common misconception that only calls that are beyond the bandwidth limit will suffer from quality degradation. CAC is the only method that prevents general voice quality degradation caused by too many concurrent active calls.

QUESTION 18
You need to calculate the bandwidth required to support VOIP on one of the remote Certkiller locations. What is the minimum bandwidth required to support a single uncompressed telephony call at the standard sampling rate and sample size?

A. 16 kbps
B. 80 kbps
C. 64 kbps
D. 96 kbps
E. 48 kbps
F. 32 kbps
G. None of the above

Answer: C

Explanation:
Each sample is encoded in the following way:
One polarity bit: Indicates positive versus negative signals
Three segment bits: Identify the logarithmically sized segment number (0-7)
Four step bits: Identify the linear step within a segment.
Because 8000 samples per second are taken for telephony, the bandwidth that is needed per call is 64 kbps. This is the reason why traditional, circuit-based telephony networks use time-division-multiplexed lines, combining multiple channels of 64 kbps each (digital signal level 0 [DS-0]) in a single physical

QUESTION 19
Certkiller uses FXO interfaces on their VOIP gateways. What best describes an FXO interface?

A. Analog trunks that provide the Survivable Remote Site Telephony (SRST) feature
B. Analog trunks that provide VoIP gateway functionality
C. Analog trunks that connect a gateway to plain old telephone service (POTS) device such as analog phones, fax machines, and legacy voice-mail systems
D. Analog trunks that connect a gateway to a central office (CO) or private branch exchange (PBX)
E. None of the above.

Answer: D

Explanation:
Gateways use different types of interfaces to connect to analog devices, such as phones, fax machines, or PBX or public switched telephone network (PSTN) switches. Analog interfaces used at the gateways include these three types:
FXS: The FXS interface connects to analog end systems, such as analog phones or analog faxes, which on their side use the FXO interface. The router FXS interface behaves like a PSTN or a PBX, serving phones, answering machines, or fax machines with line power, ring voltage, and dial tones. If a PBX uses an FXO interface, it can also connect to a router FXS interface. In this case, the PBX acts like a phone.
FXO: The FXO interface connects to analog systems, such as a PSTN or a PBX, which on their side use the FXS interface. The router FXO interface behaves like a phone, getting line power, ring voltage, and dial tones from the other side. As mentioned, a PBX can also use an FXO interface toward the router (which will then use an FXS interface), if the PBX takes the role of the phone.
E&M: The E&M interface provides signaling for analog trunks. Analog trunks interconnect two PBX-style devices, such as any combination of a gateway (acting as a PBX), a PBX, and a PSTN switch. E&M is often defined to as "ear and mouth," but it derives from the term "earth and magneto." "Earth" represents the electrical ground, and "magneto" represents the electromagnet used to generate tones.

QUESTION 20
Analog interfaces are being utilized in a number of the Certkiller VOIP gateways.
Which two voice gateway analog-interface statements are true? (Select two)

A. An analog fax machine can connect to a Foreign Exchange Office (FXO) interface.
B. A router can use a Foreign Exchange Office (FXO) interface to connect to a PSTN.
C. A router can use a Foreign Exchange Station (FXS) interface to connect to a PBX.
D. An analog telephone can connect to a Foreign Exchange Station (FXS) interface.

Answer: B, D

Explanation:

Gateways use different types of interfaces to connect to analog devices, such as phones, fax machines, or PBX or public switched telephone network (PSTN) switches. Analog interfaces used at the gateways include these three types:
FXS: The FXS interface connects to analog end systems, such as analog phones or analog faxes, which on their side use the FXO interface. The router FXS interface behaves like a PSTN or a PBX, serving phones, answering machines, or fax machines with line power, ring voltage, and dial tones. If a PBX uses an FXO interface, it can also connect to a router FXS interface. In this case, the PBX acts like a phone.
FXO: The FXO interface connects to analog systems, such as a PSTN or a PBX, which on their side use the FXS interface. The router FXO interface behaves like a phone, getting line power, ring voltage, and dial tones from the other side. As mentioned, a PBX can also use an FXO interface toward the router (which will then use an FXS interface), if the PBX takes the role of the phone.

QUESTION 21
Two Certkiller locations are using a multi-site centralized call processing model. The voice gateway on the remote branch has lost IP connectivity to its Cisco CallManager server. Which feature enables the remote gateway to take the role of the call agent during the WAN failure?

A. Cisco CallManager Attendant Console
B. Automated alternate routing (AAR)
C. Real-Time Protocol (RTP)
D. Survivable Remote Site Telephony (SRST)
E. None of the above

Answer: D

Explanation:
In IP telephony environments, gateways support fallback scenarios for IP phones that have lost IP connectivity to their call agent (that is, Cisco Unified CallManager). This feature, called Cisco Survivable Remote Site Telephony (SRST), enables the gateway to take the role of the call agent during WAN failure. Local calls can then proceed even if IP connectivity to Cisco Unified CallManager is broken. In addition, Cisco SRST can route calls out to the PSTN and, thus, use the PSTN as the backup route for calls toward any site that is not reachable via IP.

QUESTION 22
A Cisco router is being used as a VOIP gateway to convert voice signals in the Certkiller network. When a router converts analog signals to digital signals, what three steps are always included in the process? (Select three)

A. Compression
B. Involution
C. Quantization
D. Encoding

E. Sampling
F. Companding

Answer: C, D, E

Explanation:
Step 1 Sampling: The analog signal is sampled periodically. The output of the sampling is a pulse amplitude modulation (PAM) signal.
Step 2 Quantization: The PAM signal is matched to a segmented scale. This scale measures the amplitude (height) of the PAM signal.
Step 3 Encoding: The matched scale value is represented in binary format.
Step 4 Compression: Optionally, voice samples can be compressed to reduce bandwidth requirements. Analog-to-digital conversion is done by digital signal processors (DSPs), which are located on the voice interface cards. The conversion is needed for calls received on analog lines, which are then sent out to a packet network or to a digital voice interface.

QUESTION 23
The Certkiller network has offices around the country. With the use of Cisco Unified CallManager, Certkiller has deployed a VoIP network in a multisite centralized configuration. Which IOS gateway feature should be deployed to enable VoIP devices to register with a local gateway and continue to function when the connection to the Cisco Unified CallManager is broken?

A. Automatic Alternate Routing (AAR)
B. Gatekeeper multizone
C. Call Admission Control (CAC)
D. Survivable Remote Site Telephony (SRST)
E. None of the above

Answer: D

Explanation:
In IP telephony environments, gateways support fallback scenarios for IP phones that have lost IP connectivity to their call agent (that is, Cisco Unified CallManager). This feature, called Cisco Survivable Remote Site Telephony (SRST), enables the gateway to take the role of the call agent during WAN failure. Local calls can then proceed even if IP connectivity to Cisco Unified CallManager is broken. In addition, Cisco SRST can route calls out to the PSTN and, thus, use the PSTN as the backup route for calls toward any site that is not reachable via IP.

QUESTION 24
A Cisco router is being used as a VOIP gateway to convert analog and digital voice signals in the Certkiller network. Which two statements are true about analog to digital conversion of voice signals for use in digital telephony networks? (Select two)

A. The output of the sampling process is a pulse code modulation (PCM) signal.
B. The three required steps in the analog to digital conversion are sampling, quantization, and encoding.
C. The three required steps in the analog to digital conversion are sampling, encoding, and compression.
D. The output of the sampling process is a pulse amplitude modulation (PAM) signal.
E. The three required steps in the analog to digital conversion are sampling, quantization, and compression.

Answer: B, D

Explanation:
Analog to digital conversion steps include these are:
Step 1 Sampling: The analog signal is sampled periodically. The output of the sampling is a pulse amplitude modulation (PAM) signal.
Step 2 Quantization: The PAM signal is matched to a segmented scale. This scale measures the amplitude (height) of the PAM signal.
Step 3 Encoding: The matched scale value is represented in binary format.
Step 4 Compression: Optionally, voice samples can be compressed to reduce bandwidth requirements.
Analog-to-digital conversion is done by digital signal processors (DSPs), which are located on the voice interface cards. The conversion is needed for calls received on analog lines, which are then sent out to a packet network or to a digital voice interface.

QUESTION 25
Many of the Cisco VOIP gateways used in the Certkiller network contain FXS interfaces. Which statement is true about Foreign Exchange Station (FXS) ports on a router?

A. The FXS interface connects directly to an IP phone and supplies ring, voltage, and dial tone.
B. The FXS interface allows an analog connection to be directed at the public switched telephone network (PSTN's) central office.
C. The FXS interface connects directly to a standard telephone, fax machine, or similar device and supplies ring, voltage, and dial tone.
D. The FXS interface connects directly to ISDN voice channels.
E. None of the above.

Answer: C

Explanation:
FXS: The FXS interface connects to analog end systems, such as analog phones or analog faxes, which on their side use the FXO interface. The router FXS interface behaves like a PSTN or a PBX, serving phones, answering machines, or fax machines with line power, ring voltage, and dial tones. If a PBX uses an FXO interface, it can also connect to a router FXS interface. In this case, the PBX acts like a phone.

QUESTION 26
VOIP gateways terminate a large of number of analog circuits in the Certkiller network. What three types of interfaces do voice gateways use to connect to analog interfaces? (Select three)

A. E1 CCS
B. E&M
C. Serial
D. FXS
E. FXO
F. T1 CAS

Answer: B, D, E

Explanation:
Gateways use different types of interfaces to connect to analog devices, such as phones, fax machines, or PBX or public switched telephone network (PSTN) switches. Analog interfaces used at the gateways include these three types:
FXS: The FXS interface connects to analog end systems, such as analog phones or analog faxes, which on their side use the FXO interface. The router FXS interface behaves like a PSTN or a PBX, serving phones, answering machines, or fax machines with line power, ring voltage, and dial tones. If a PBX uses an FXO interface, it can also connect to a router FXS interface. In this case, the PBX acts like a phone.
FXO: The FXO interface connects to analog systems, such as a PSTN or a PBX, which on their side use the FXS interface. The router FXO interface behaves like a phone, getting line power, ring voltage, and dial tones from the other side. As mentioned, a PBX can also use an FXO interface toward the router (which will then use an FXS interface), if the PBX takes the role of the phone.
E&M: The E&M interface provides signaling for analog trunks. Analog trunks interconnect two PBX-style devices, such as any combination of a gateway (acting as a PBX), a PBX, and a PSTN switch. E&M is often defined to as "ear and mouth," but it derives from the term "earth and magneto." "Earth" represents the electrical ground, and "magneto" represents the electromagnet used to generate tones.

QUESTION 27
Certkiller has several offices around the country. They have deployed a VOIP network with Cisco Unified CallManager in a multisite centralized configuration but there is a requirement to place a call agent at some of the remote sites. Which IOS gateway feature should be deployed at the remote site to enable local call control?

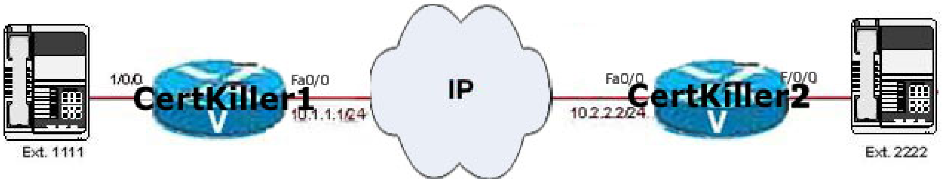
A. Survivable Remote Site Telephony (SRST)
B. Gatekeeper multizone
C. Cisco Unified CallManager Express (CME)
D. Call Admission Control (CAC)

E. Automatic Alternate Routing (AAR)
F. None of the above

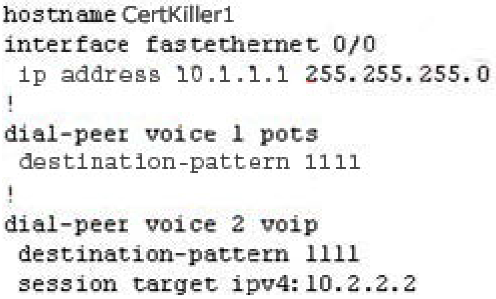
Answer: C

Explanation:
Cisco Unified CallManager is the IP-based PBX in an IP telephony solution. It acts as a call agent for IP phones and MGCP gateways and can also interact with H.323 or SIP devices using their protocols. For redundancy and load sharing, multiple Cisco Unified CallManager servers operate in a cluster. From an administration perspective, the whole cluster is a single logical instance.
Cisco IOS routers can permanently act as a call agent for IP phones. The feature that provides this functionality is Cisco Unified CallManager Express. With Cisco Unified CallManager Express, Cisco Unified CallManager functionality is provided by the router. If the router is also a voice gateway, it combines IP telephony and VoIP gateway functionality in a single box.
Cisco IOS gateways also support other features, such as call preservation (Real-Time Transport Protocol [RTP] stream) in case of a lost signaling channel, dual tone multifrequency (DTMF) relay capabilities, supplementary services support (for user functions, such as hold, transfer, and conferencing), and fax and modem support.

QUESTION 28
Two Certkiller phones connect to Cisco Gateway routers as shown below:

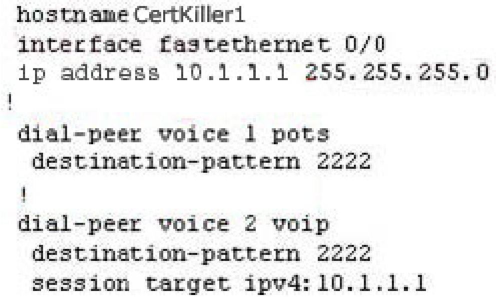


Certkiller 1 configuration exhibit:



```
hostname CertKiller1
interface fastethernet 0/0
 ip address 10.1.1.1 255.255.255.0
!
dial-peer voice 1 pots
 destination-pattern 1111
!
dial-peer voice 2 voip
 destination-pattern 1111
 session target ipv4:10.2.2.2
```

Certkiller 2 configuration exhibit:



```
 hostname CertKiller1
 interface fastethernet 0/0
 ip address 10.1.1.1 255.255.255.0
!
 dial-peer voice 1 pots
  destination-pattern 2222
  !
 dial-peer voice 2 voip
  destination-pattern 2222
  session target ipv4:10.1.1.1
```

Study the exhibits shown above. Both routers have been configured as VoIP gateways. They must also support traditional telephony devices to connect to analog telephones. Which two configuration changes would correctly support the voice requirements? (Select two)

A. On each router, under the dial-peer voice 1 pots configuration, add the port 1/0/0 command.
B. Under the dial-peer voice 2 voip configuration, change the destination pattern of 1111 to 2222 on the Certkiller 1 router, and 2222 to 1111 on the Certkiller 2 router.
C. Under the dial-peer voice 2 voip configuration, change the destination target address of 10.2.2.2 to 10.1.1.1 on the Certkiller 1 router, and the destination target address of 10.1.1.1 to 10.2.2.2 on the Certkiller 2 router.
D. On each router, configure dial-peer voice 1 as a voip connection and configure dial-peer voice 2 as a pots connection.
E. On each router, under the dial-peer voice 1 pots configuration, add the port fa0/0 command.
F. Under the dial-peer voice 1 pots configuration, change the destination pattern of 1111 to 2222 on the Certkiller 1 router, and 2222 to 1111 on the Certkiller 2 router.

Answer: A, B

Explanation:

Command	Description
dial-peer voicetag type	Use the dial-peer voice command to enter the dial peer subconfiguration mode. The tag value is a number that has to be unique for all dial peers within the same gateway. The type value indicates the type of dial peer (for example, POTS or VoIP).
destination-pattern telephone_number	The destination-pattern command, entered in dial peer subconfiguration mode, defines the telephone number that applies to the dial peer. A call placed to this number will be routed according to the configuration type and port (in the case of a POTS type dial peer) or session target (in the case of a VoIP type dial peer) of the dial peer.

portport-number	The port command, entered in POTS dial peer subconfiguration mode, defines the port number that applies to the dial peer. Calls that are routed using this dial peer are sent to the specified port. The port command can be configured only on a POTS dial peer.
session target ipv4:ip-address	The session target command, entered in VoIP dial peer subconfiguration mode, defines the IP address of the target VoIP device that applies to the dial peer. Calls that are routed using this dial peer are sent to the specified IP address. The session target command can be configured only on a VoIP dial peer.

QUESTION 29
You need to determine the correct ports to use on a new Cisco router which will be used as a VOIP gateway. Which two statements are true about voice ports on a router? (Select two)

A. Calls made to the PSTN can be made via FXS or T1/E1 trunk ports.
B. Analog and IP phones can be connected to the VoIP network via FXO or T1/E1 trunk ports.
C. Calls to the PSTN can be made via the use of FXO or T1/E1 trunk ports.
D. Calls between analog phones that are attached to the FXS ports in a VoIP network can be completely processed by voice-enabled routers.

Answer: C, D

Explanation:
FXS: The FXS interface connects to analog end systems, such as analog phones or analog faxes, which on their side use the FXO interface. The router FXS interface behaves like a PSTN or a PBX, serving phones, answering machines, or fax machines with line power, ring voltage, and dial tones. If a PBX uses an FXO interface, it can also connect to a router FXS interface. In this case, the PBX acts like a phone.
FXO: The FXO interface connects to analog systems, such as a PSTN or a PBX, which on their side use the FXS interface. The router FXO interface behaves like a phone, getting line power, ring voltage, and dial tones from the other side. As mentioned, a PBX can also use an FXO interface toward the router (which will then use an FXS interface), if the PBX takes the role of the phone.

QUESTION 30
A Cisco router acts as a voice gateway in the Certkiller network, converting digital to analog signals. Which statement is true about the digital to analog conversion process?

A. The two steps of digital to analog conversion are quantization and decoding.
B. The two steps of digital to analog conversion are decoding and filtering.
C. The two steps of digital to analog conversion are decompression and reconstruction of the analog signal.
D. The two steps of digital to analog conversion are decompression and filtering of the analog signal.
E. None of the above

Answer: B

Explanation:
Digital-to-analog conversion steps include these:
Step 1 Decompression: If the voice signal was compressed by the sender, it is first decompressed.
Step 2 Decoding: The received, binary formatted voice samples are decoded to the amplitude value of the samples. This information is used to rebuild a PAM signal of the original amplitude.
Step 3 Reconstruction of the analog signal: The PAM signal is passed through a properly designed filter that reconstructs the original analog wave form from its digitally coded counterpart. The whole process is simply the reverse of the analog-to-digital conversion. Like analog-to-digital conversion, digital-to-analog conversion is performed by DSPs, which are located on the voice interface cards. The conversion is needed for calls being received from a packet network or digital interfaces, which are then transmitted out an analog voice interface.

QUESTION 31
You want to use a Cisco router to handle all IP calls locally in a Certkiller office. Which functionality in the Cisco IOS software will enable a router to permanently act as a call agent for IP phones?

A. Media Gateway Control Protocol (MGCP)
B. Cisco CallManager Gateway (CMG)
C. Cisco CallManager Voice Gateway (CMVG)
D. Cisco CallManager Express (CME)
E. Cisco CallManager
F. None of the above

Answer: D

Explanation:

Cisco Unified CallManager is the IP-based PBX in an IP telephony solution. It acts as a call agent for IP phones and MGCP gateways and can also interact with H.323 or SIP devices using their protocols. For redundancy and load sharing, multiple Cisco Unified CallManager servers operate in a cluster. From an administration perspective, the whole cluster is a single logical instance.
Cisco IOS routers can permanently act as a call agent for IP phones. The feature that provides this functionality is Cisco Unified CallManager Express. With Cisco Unified CallManager Express, Cisco Unified CallManager functionality is provided by the router. If the router is also a voice gateway, it combines IP telephony and VoIP gateway functionality in a single box.
Cisco IOS gateways also support other features, such as call preservation (Real-Time Transport Protocol [RTP] stream) in case of a lost signaling channel, dual tone multifrequency (DTMF) relay capabilities, supplementary services support (for user functions, such as hold, transfer, and conferencing), and fax and modem support.

QUESTION 32
Router CK1 is being used as a VOIP gateway at a remote Certkiller office. Which statement is true about the functions provided by a Cisco voice gateway router?

A. ISDN Q signaling is not supported on a voice gateway router.
B. On a voice gateway router, analog signals are converted to digital signals before the encapsulation occurs.
C. Analog devices cannot be directly connected to a Cisco voice gateway device.
D. Voice gateways always require a call agent to process calls.
E. None of the above.

Answer: B

Explanation:
Step 1 Sampling: The analog signal is sampled periodically. The output of the sampling is a pulse amplitude modulation (PAM) signal.
Step 2 Quantization: The PAM signal is matched to a segmented scale. This scale measures the amplitude (height) of the PAM signal.
Step 3 Encoding: The matched scale value is represented in binary format.
Step 4 Compression: Optionally, voice samples can be compressed to reduce bandwidth requirements.
Analog-to-digital conversion is done by digital signal processors (DSPs), which are located on the voice interface cards. The conversion is needed for calls received on analog lines, which are then sent out to a packet network or to a digital voice interface.

QUESTION 33
You need to optimize the Certkiller VOIP network. To have the best possible voice quality and to effectively utilize the available bandwidth, which queuing and compression mechanisms need to be used? (Select two)

A. Class-based weighted fair queuing (CBWFQ)

B. TCP header compression
C. UDP header compression
D. Real-Time Transport Protocol (RTP) header compression
E. Priority Queuing (PQ) or Custom Queuing (CQ)
F. Low Latency Queuing (LLQ)

Answer: D, F

Explanation:
1. RTP is the Internet-standard protocol for the transport of real-time data, including audio and video. It can be used for media on demand as well as interactive services such as Internet telephony. RTP consists of a data part and a control part, called RTCP. The data part of RTP is a thin protocol that provides support for applications with real-time properties such as continuous media, for example, audio and video, including timing reconstruction, loss detection, and content identification. Compressed Real-Time Transport Protocol, or cRTP, is used on a link-by-link basis to compress the IP/UDP/RTP header. In a packet voice environment when framing speech samples every 20 milliseconds, this scenario generates a payload of 20 bytes. The total packet size comprises an IP header of 20 bytes, a UDP header of 8 bytes, and an RTP header of 12 bytes, combined with a payload of 20 bytes. It is evident that the size of the header is twice the size of the payload. When generating packets every 20 milliseconds on a slow link, the header consumes a large portion of the bandwidth. To avoid the unnecessary consumption of available bandwidth, CRTP is used on a link-by-link basis.
2.
The LLQ feature brings strict Priority Queuing (PQ) to CBWFQ. Strict PQ allows delay-sensitive data such as voice to be sent before packets in other queues are sent. Without LLQ, CBWFQ provides WFQ based on defined classes with no strict priority queue available for real-time traffic. For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth assigned to the class. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced fairly based on weight and no class of packets may be granted strict priority. This scheme poses problems for voice traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission manifesting as jitter in the heard conversation. LLQ provides strict priority queuing for CBWFQ, reducing jitter in voice conversations. LLQ enables the use of a single, strict priority queue within CBWFQ at the class level. Any class can be made a priority queue by adding the priority keyword. Within a policy map, one or more classes can be given priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is sent to the same, single, strict priority queue.

QUESTION 34
Voice and Video are being used on the Certkiller IP network. Which statement is true about the comparison of voice traffic with video traffic?

A. Video traffic requires the retransmission capabilities of TCP whereas voice uses UDP.

B. Video conferencing traffic tends to be much more bursty in nature and is more prone to have an impact on other traffic flows.
C. Video traffic is less sensitive to dropped packets than for voice traffic.
D. Voice traffic tends to be much more bursty in nature and is more prone to have an impact on other traffic flows.
E. Latency requirements are less stringent for video traffic than for voice traffic.
F. Voice traffic requires the retransmission capabilities of TCP whereas video uses UDP.
G. None of the above.

Answer: B

Explanation:
Packets that carry voice traffic are typically very small, they cannot tolerate delay and delay variation as they traverse the network. Voices will break up, and words will become incomprehensible. On the other hand, packets that carry file-transfer data are typically large and can survive delays and drops. It is possible to retransmit part of a dropped data file, but it is not feasible to retransmit a part of a voice conversation. The constant, small-packet voice flow competes with bursty data flows. Unless some mechanism mediates the overall flow, voice quality will be severely compromised at times of network congestion. The critical voice traffic must get priority. Voice and video traffic is very time-sensitive. It cannot be delayed or dropped, or the quality of voice and video will suffer.

QUESTION 35
You need to improve the quality of calls in the Certkiller VOIP network. What is a method for preventing general voice-quality degradation caused by too many concurrent active calls?

A. Compressed Real-Time Protocol (cRTP)
B. Committed Access Rate (CAR)
C. Call Admission Control (CAC)
D. Low Latency Queuing (LLQ)
E. None of the above

Answer: C

Explanation:
Networks must provide secure, predictable, measurable, and, sometimes, guaranteed services. Network administrators and architects can better achieve this performance from the network by managing delay, delay variation (jitter), bandwidth provisioning, and packet loss parameters with quality of service (QoS) techniques.
The LLQ feature brings strict Priority Queuing (PQ) to CBWFQ. Strict PQ allows delay-sensitive data such as voice to be sent before packets in other queues are sent. Without LLQ, CBWFQ provides WFQ based on defined classes with no strict priority queue available for real-time traffic. For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth assigned to the class. Therefore, the

bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced fairly based on weight and no class of packets may be granted strict priority. This scheme poses problems for voice traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission manifesting as jitter in the heard conversation. LLQ provides strict priority queuing for CBWFQ, reducing jitter in voice conversations. LLQ enables the use of a single, strict priority queue within CBWFQ at the class level. Any class can be made a priority queue by adding the priority keyword. Within a policy map, one or more classes can be given priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is sent to the same, single, strict priority queue.

QUESTION 36

QoS needs to be configured to support VOIP in the Certkiller network. Which two statements are true about the application of QoS in a converged network? (Select two)

A. Some packet loss can be corrected by codec algorithms.
B. End-to-end network delay times that exceed 250 ms for real-time traffic are considered unacceptable.
C. RSVP handles voice packet retransmission.
D. Fragmentation is a result of packet loss.
E. End-to-end network delay times that exceed 50 ms for real-time traffic are considered unacceptable.
F. End-to-end network delay is not a factor as long as the delay is consistent.

Answer: A, B

Explanation:
When addressing the QoS needs of video conferencing traffic the basic requirements are similar to those for voice. Loss should be no more than 1 percent, one-way latency should be no more than 150-200 ms and the average jitter should be no more than 30 ms. Due to its bursty nature, the minimum bandwidth guarantee is the size of the video conferencing session plus 20 percent. This means that a 384 Kbps video conferencing session requires 460 Kbps guaranteed priority bandwidth.

QUESTION 37

You want to implement QoS on the Certkiller network to increase the quality of VOIP calls. What are the voice traffic characteristics that QoS tools can affect?

A. Voice termination, transcoding, and conferencing
B. Bandwidth, delay, jitter, and packet loss
C. Sampling, quantization, encoding, and optional compression
D. Call setup and call teardown
E. None of the above

Answer: B

Explanation:
1. Loss: Loss refers to the percentage of packets that fail to reach their destination. Loss can result from errors in the network, corrupted frames and congested networks. For many TCP/IP based traffic flows, such as those associated with file and print services, small numbers of lost packets are of little concern as TCP/IP's retransmission mechanism will ensure their eventual arrival. However, for UDP traffic associated with real-time applications such as streaming media and voice, retransmission is not feasible and losses are less tolerable.
2. Delay and Latency: Delay or latency refers to the time it takes for a packet to travel from the source to the destination. Delay is comprised of fixed and variable delays. Fixed delays comprise such events as serialization and encoding/decoding. For example, a bit takes a fixed 100ns to exit a 10Mb Ethernet interface. Variable delays are often the result of congestion and include the time packets spend in network buffers waiting for access to the media.
3. Jitter: Delay variation or jitter is the difference in the delay times of consecutive packets. A jitter buffer is often used to smooth out arrival times, but there are instantaneous and total limits on buffering ability. Any type of buffering used to reduce jitter directly increases total network delay. In general, traffic requiring low latency also requires a minimum variation in latency.
4. Bandwidth: The bandwidth parameter uses the interface bandwidth to determine a best path to a destination network. When bandwidth is the metric, the router prefers the path with the highest bandwidth to a destination. For example, a Fast Ethernet (100 Mbps) is preferred over a DS-3 (45 Mbps).

QUESTION 38
You want to implement QoS on the Certkiller network to correct some quality issues. Which problem would be a cause for implementing QoS?

A. CRC errors
B. Tail drops
C. FCS errors
D. Line code violations
E. None of the above

Answer: B

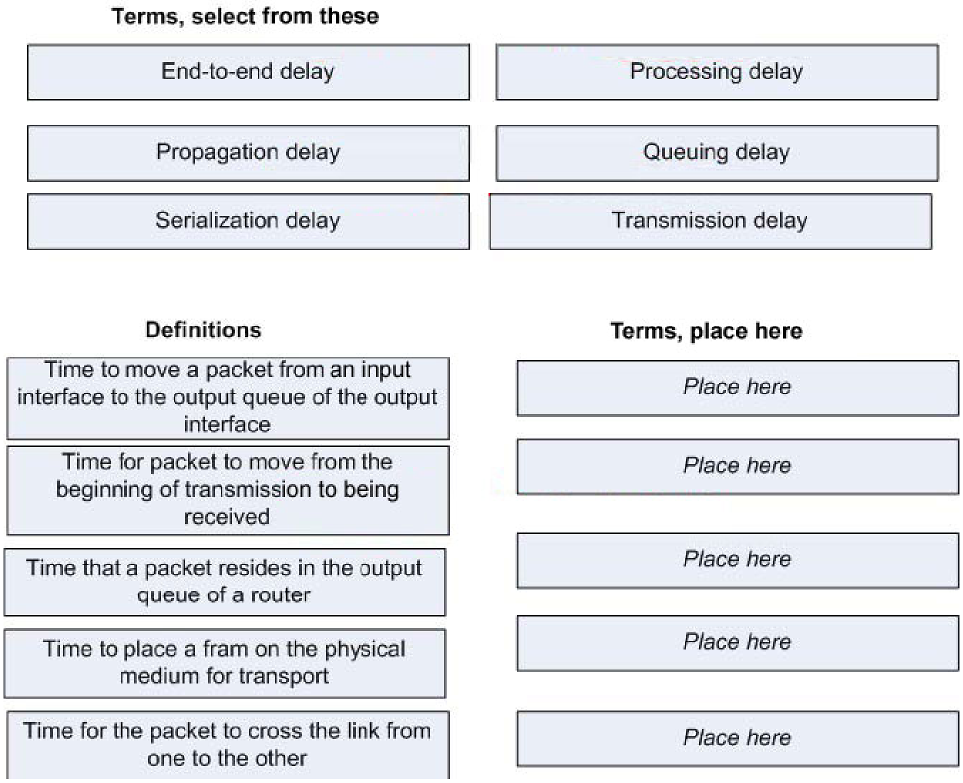
Explanation:
For network traffic causing longer-term congestion, a router using CBWFQ or any of several other queuing methods will need to drop some packets. A traditional strategy is tail drop. With tail drop, a router simply discards any packet that arrives at the tail end of a queue that has completely used up its packet-holding resources. Tail drop is the default queuing response to congestion. Tail drop treats all traffic equally and does not differentiate between classes of service.
When using tail drop, the router drops all traffic that exceeds the queue limit. Many TCP

sessions then simultaneously go into a slow start. This reduces the TCP window size. Consequently, traffic temporarily slows as much as possible. As congestion is reduced, window sizes begin to increase in response to the available bandwidth.

QUESTION 39

DRAG DROP

Drag each term next to the appropriate definition. Upon completion, there will be one term left unused.

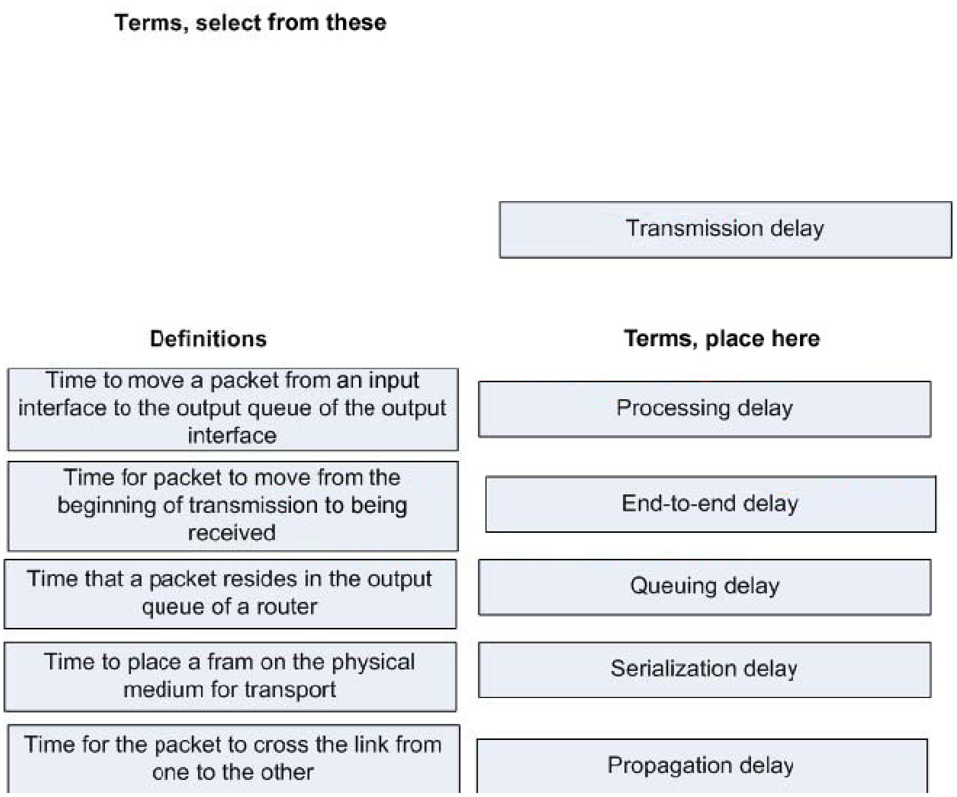


Terms, select from these

End-to-end delay	Processing delay
Propagation delay	Queuing delay
Serialization delay	Transmission delay

Definitions	Terms, place here
Time to move a packet from an input interface to the output queue of the output interface	Place here
Time for packet to move from the beginning of transmission to being received	Place here
Time that a packet resides in the output queue of a router	Place here
Time to place a fram on the physical medium for transport	Place here
Time for the packet to cross the link from one to the other	Place here

Answer:



Terms, select from these

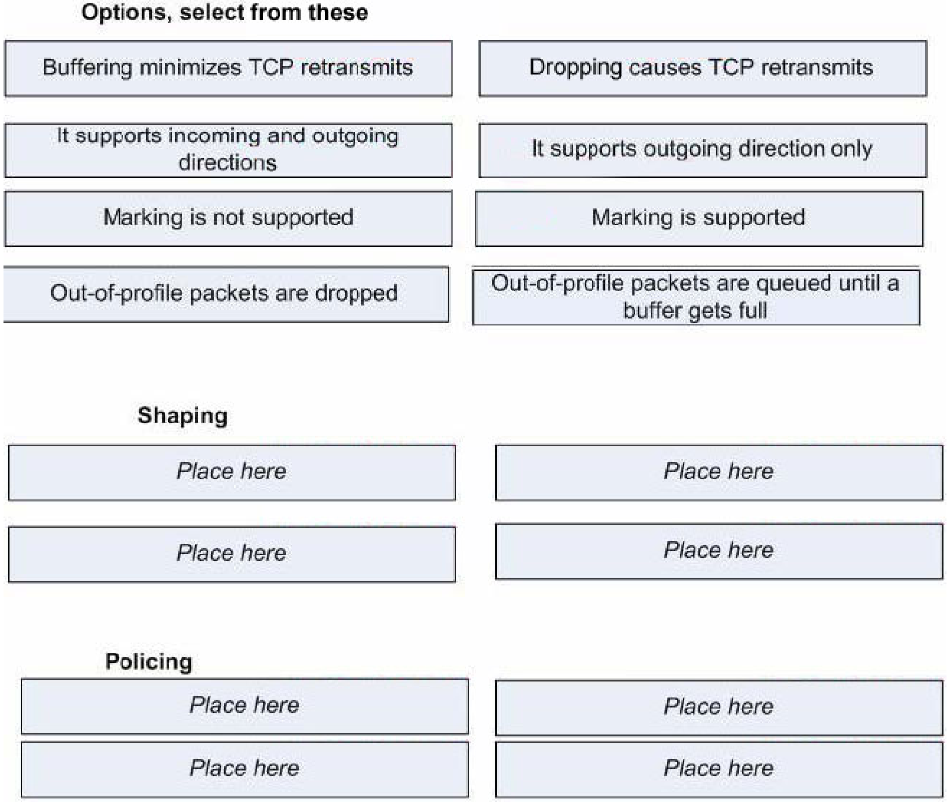
Transmission delay

Definitions	Terms, place here
Time to move a packet from an input interface to the output queue of the output interface	Processing delay
Time for packet to move from the beginning of transmission to being received	End-to-end delay
Time that a packet resides in the output queue of a router	Queuing delay
Time to place a fram on the physical medium for transport	Serialization delay
Time for the packet to cross the link from one to the other	Propagation delay

Explanation:
1. Processing delay:
The time that it takes for a router (or Layer 3 switch) to take the packet from an input interface and put it into the output queue of the output interface. The processing delay depends on various factors:
1. CPU speed
2. CPU utilization
3. IP switching mode
4. Router architecture
5. Configured features on both the input and output interfaces
2. Queuing delay: The time that a packet resides in the output queue of a router. Queuing delay depends on the number of packets already in the queue and their sizes. Queuing delay also depends on the bandwidth of the interface and the queuing mechanism.
3. Serialization delay: The time that it takes to place a frame on the physical medium for transport. This delay is typically inversely proportional to the link bandwidth.
4. Propagation delay: The time that it takes for the packet to cross the link from one end to the other. This time usually depends on the type of media. (For example, satellite links produce the longest propagation delay because of the high altitudes of communications satellites.)
5. End-to-end delay: Equals the sum of all propagation, processing, serialization, and queuing delays in the path.

QUESTION 40
DRAG DROP

Drag each statement on the left to the category that the statement best describes on the right.



Options, select from these

Buffering minimizes TCP retransmits

Dropping causes TCP retransmits

It supports incoming and outgoing directions

It supports outgoing direction only

Marking is not supported

Marking is supported

Out-of-profile packets are dropped

Out-of-profile packets are queued until a buffer gets full

Shaping

Place here

Place here

Place here

Place here

Policing

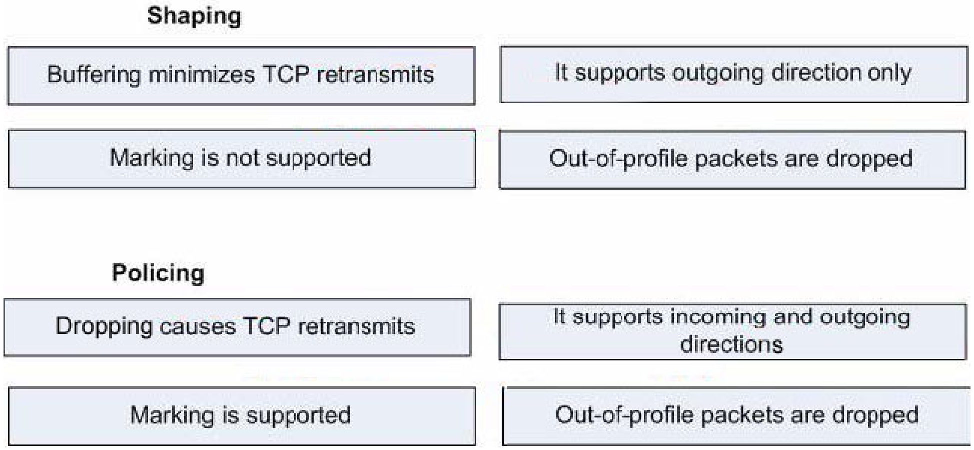
Place here

Place here

Place here

Place here

Answer:



Shaping

Buffering minimizes TCP retransmits

It supports outgoing direction only

Marking is not supported

Out-of-profile packets are dropped

Policing

Dropping causes TCP retransmits

It supports incoming and outgoing directions

Marking is supported

Out-of-profile packets are dropped

Explanation:

Policing can be applied to either the inbound or outbound direction, while shaping can be applied only in the outbound direction. Policing drops nonconforming traffic instead of queuing the traffic like shaping. Policing also supports marking of traffic. Traffic policing is more efficient in terms of memory utilization than traffic shaping because no additional queuing of packets is needed.

Both traffic policing and shaping ensure that traffic does not exceed a bandwidth limit, but each mechanism has different impacts on the traffic:

1. Policing drops packets more often, generally causing more retransmissions of

connection-oriented protocols, such as TCP.
2. Shaping adds variable delay to traffic, possibly causing jitter. Shaping queues excess traffic by holding packets in a shaping queue. Traffic shaping is used to shape the outbound traffic flow when the outbound traffic rate is higher than a configured rate. Traffic shaping smoothes traffic by storing traffic above the configured rate in a shaping queue. Therefore, shaping increases buffer utilization on a router and causes unpredictable packet delays. Traffic shaping can also interact with a Frame Relay network, adapting to indications of Layer 2 congestion in the WAN. For example, if the backward explicit congestion notification (BECN) bit is received, the router can lower the rate limit to help reduce congestion in the Frame Relay network.

QUESTION 41
The output queue of router CK1 has become congested. Which term defines packet drops that occur when more packets arrive on an interface that already has a congested output queue?

A. Ignore
B. Input queue drop
C. Discard packets
D. Underrun
E. Overrun
F. Tail drop
G. None of the above

Answer: F

Explanation:
For network traffic causing longer-term congestion, a router using CBWFQ or any of several other queuing methods will need to drop some packets. A traditional strategy is tail drop. With tail drop, a router simply discards any packet that arrives at the tail end of a queue that has completely used up its packet-holding resources. Tail drop is the default queuing response to congestion. Tail drop treats all traffic equally and does not differentiate between classes of service.
When using tail drop, the router drops all traffic that exceeds the queue limit. Many TCP sessions then simultaneously go into a slow start. This reduces the TCP window size. Consequently, traffic temporarily slows as much as possible. As congestion is reduced, window sizes begin to increase in response to the available bandwidth.

QUESTION 42
Certkiller needs to add QoS to their network to support their national VOIP deployment. Which statement about the application of QoS in a voice-enabled network is true?

A. QoS mechanisms are typically used to increase available bandwidth.
B. Fragmentation is used to create smaller voice packets to allow them to be transported more easily.

C. QoS mechanisms should be able to provide acceptable voice quality in congested networks.
D. RSVP is only applicable in a network that does not experience congestion.
E. None of the above

Answer: C

Explanation:
Loss causes voice clipping and skips. Industry standard codec algorithms can correct for up to 30 ms of lost voice. Cisco Voice over IP (VoIP) technology uses 20 ms samples of voice payload per VoIP packet. Only a single Real Time Transport (RTP) packet could be lost at any given time. If two successive voice packets are lost, the 30 ms correctable window is exceeded and voice quality begins to degrade.
Delay can cause voice quality degradation if it is above 200 ms. If the end-to-end voice delay becomes too long, the conversation sounds as if two parties are talking over a satellite link or a CB radio. The ITU standard for VoIP, G.114, states that a 150 ms one-way delay budget is acceptable for high voice quality.

QUESTION 43
Too much delay is causing VOIP quality issues within the Certkiller network. What are two major sources of delay that can be managed by QoS in voice-enabled networks? (Select two)

A. Header overhead
B. Voice packet serialization delay
C. Propagation delay
D. Packets dropped because of CRC errors
E. Congested egress queues

Answer: A, E

Explanation:
1. Header Overhead:
The combined overhead of IP, UDP, and RTP headers is enormously high, especially because voice is sent in relatively small packets and at high packet rates. When G.729 is used, the headers are twice the size of the voice payload. The pure voice bandwidth of the G.729 codec (8 kbps) has to be tripled for the whole IP packet. This total, however, is still not the final bandwidth requirement, because Layer 2 overhead must also be included. Without the Layer 2 overhead, a G.729 call requires 24 kbps. When G.711 is being used, the ratio of header to payload is smaller because of the larger voice payload. Forty bytes of headers are added to 160 bytes of payload, so one-fourth of the G.711 codec bandwidth (64 kbps) has to be added. Without Layer 2 overhead, a G.711 call requires 80 kbps.

QUESTION 44
You want to improve the application delays in the Certkiller network as much as

possible. What are four types of delay that contribute to end-to-end packet delay?

A. Queuing delay
B. Broadcast delay
C. Processing delay
D. Serialization delay
E. Propagation delay
F. Origination delay

Answer: A, C, D, E

Explanation:
1. Processing delay: The time that it takes for a router (or Layer 3 switch) to take the packet from an input interface and put it into the output queue of the output interface. The processing delay depends on various factors:
* CPU speed
* CPU utilization
* IP switching mode
* Router architecture
* Configured features on both the input and output interfaces
2. Queuing delay: The time that a packet resides in the output queue of a router. Queuing delay depends on the number of packets already in the queue and their sizes. Queuing delay also depends on the bandwidth of the interface and the queuing mechanism.
3. Serialization delay: The time that it takes to place a frame on the physical medium for transport. This delay is typically inversely proportional to the link bandwidth.
4.
Propagation delay: The time that it takes for the packet to cross the link from one end to the other. This time usually depends on the type of media. (For example, satellite links produce the longest propagation delay because of the high altitudes of communications satellites.)
5. End-to-end delay: Equals the sum of all propagation, processing, serialization, and queuing delays in the path.

QUESTION 45
You want to use QoS to fix a number of problems with the Certkiller converged network. For which two network problems would QoS be a good solution? (Select two)

A. Serialization delay
B. Routing table convergence issues
C. End-to-end delay
D. Lack of bandwidth
E. Inconsistent port costs
F. Poor file transfer rates

Answer: C, D

Explanation:
End-to-end delay: Equals the sum of all propagation, processing, serialization, and queuing delays in the path. The bandwidth parameter uses the interface bandwidth to determine a best path to a destination network. When bandwidth is the metric, the router prefers the path with the highest bandwidth to a destination. For example, a Fast Ethernet (100 Mbps) is preferred over a DS-3 (45 Mbps).

QUESTION 46
You are considering the benefits of implementing QoS within your enterprise network. What is the goal of QoS in a network?

A. To reduce hardware errors
B. To eliminate propagation delay
C. To eliminate jitter and packet loss
D. To prevent packets from being dropped
E. To increase available bandwidth
F. To provide predictable network service
G. All of the above
H. None of the above

Answer: F

Explanation:
In any bandwidth-limited network, QoS is used to reduce jitter, delay, and packet loss for time-sensitive and mission-critical applications. QoS is the ability of the network to provide better or "special" services to selected users and applications, to the detriment of other users and applications.
Cisco IOS QoS features enable network administrators to control and predictably service a variety of networked applications and traffic types, allowing network managers to take advantage of a new generation of media-rich and mission-critical applications. The goal of QoS is to provide better and more predictable network service by providing dedicated bandwidth, controlled jitter and latency, and improved loss characteristics. QoS achieves these goals by providing tools for managing network congestion, shaping network traffic, using expensive wide-area links more efficiently, and setting traffic policies across the network. QoS offers intelligent network services that, when correctly applied, help to provide consistent and predictable performance.

QUESTION 47
A stream of voice packets transmitted over a Certkiller WAN network encounters differing queuing delays. One router in the path used by the voice packets delays some of the packets for 4 ms while transmitting a large video file, but delays other packets only 2 ms. Another router delays some packets 5 ms, but transmits others in 2 ms. How would you best describe this type of problem?

A. Serialization delays

B. Jitter
C. Processing delays
D. Interference from bulk data traffic
E. End-to-end delay
F. None of the above

Answer: B

Explanation:
Delay variation or jitter is the difference in the delay times of consecutive packets. A jitter buffer is often used to smooth out arrival times, but there are instantaneous and total limits on buffering ability. Any type of buffering used to reduce jitter directly increases total network delay. In general, traffic requiring low latency also requires a minimum variation in latency.
As a design rule, voice networks cannot cope with more than 30 ms of jitter. Jitter in excess of 30 ms will result in degraded audio performance. Excessive jitter in a streaming video environment will result in jerky motion, loss of video quality or loss of video.

QUESTION 48
You want to ensure that some of the traffic on the network gets non-standard service. Which two traffic classes in a converged network require a QoS model other than the standard FIFO? (Select two)

A. Voice signaling
B. Peer to peer applications
C. Mission critical applications
D. World Wide Web traffic using load balanced web servers
E. Voice
F. Multicast routing protocols

Answer: C, E

Explanation:
Because of its stringent QoS requirements, voice traffic is almost always in a class by itself. Cisco has developed specific QoS mechanisms, such as LLQ, that ensure that voice always receives priority treatment over all other traffic.
After the applications with the most critical requirements have been defined, the remaining traffic classes are defined using business requirements.
A typical enterprise might define five traffic classes:
* Voice: Absolute priority for VoIP traffic.
* Mission-critical: Small set of locally defined critical business applications.
* Transactional: Database access, transaction services, interactive traffic, and preferred data services.
* Best effort: E-mail.
* Scavenger: The unspecified traffic is considered as less than best effort. Scavenger

applications, such as BitTorrent and other point-to-point applications, will be served by that class.

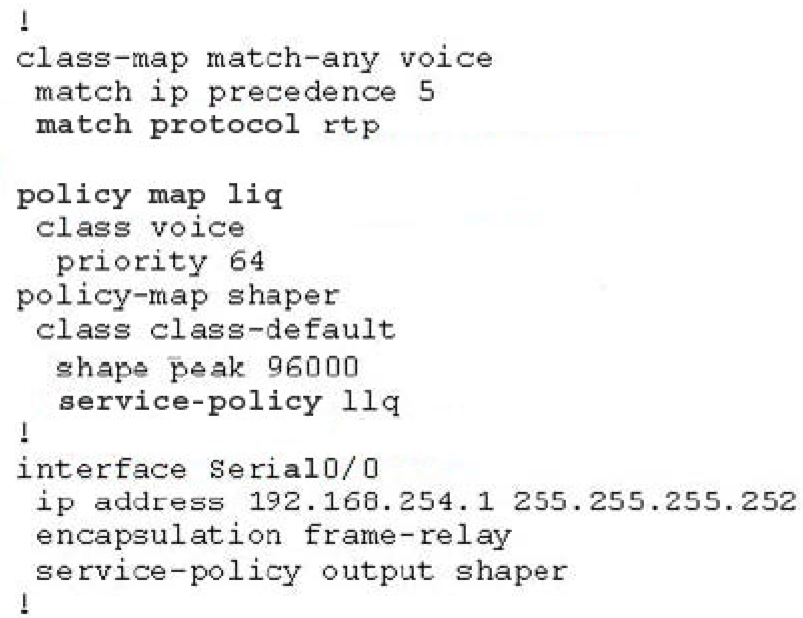
QUESTION 49
You want to decrease the overall delay of voice packets in the Certkiller converged network. Which three statements about end-to-end delay are true? (Select three)

A. End-to-end delay is the sum of propagation delays, processing delays, serialization delays, and queuing delays.
B. Coast-to-coast end-to-end delay over an optical link is about 20 ms.
C. Propagation delay is the time it takes to transmit a packet and is measured in bits-per-second (bps).
D. Propagation and serialization delays are related to the media.
E. Processing delay depends on various factors, which include CPU speed, CPU utilization, IP switching mode, and router architecture.
F. Serialization delay is the time it takes for a router to take the packet from an input interface and put it into the output queue of the output interface.

Answer: A, D, E

Explanation:
1. Processing delay: The time that it takes for a router (or Layer 3 switch) to take the packet from an input interface and put it into the output queue of the output interface. The processing delay depends on various factors:
* CPU speed
* CPU utilization
* IP switching mode
* Router architecture
* Configured features on both the input and output interfaces
2. Queuing delay: The time that a packet resides in the output queue of a router. Queuing delay depends on the number of packets already in the queue and their sizes. Queuing delay also depends on the bandwidth of the interface and the queuing mechanism.
3. Serialization delay: The time that it takes to place a frame on the physical medium for transport. This delay is typically inversely proportional to the link bandwidth.
4. Propagation delay: The time that it takes for the packet to cross the link from one end to the other. This time usually depends on the type of media. (For example, satellite links produce the longest propagation delay because of the high altitudes of communications satellites.)
5. End-to-end delay: Equals the sum of all propagation, processing, serialization, and queuing delays in the path.

QUESTION 50
Exhibit:



```
!
class-map match-any voice
 match ip precedence 5
 match protocol rtp

policy map liq
 class voice
  priority 64
policy-map shaper
 class class-default
  shape peak 96000
  service-policy llq
!
interface Serial0/0
 ip address 192.168.254.1 255.255.255.252
 encapsulation frame-relay
 service-policy output shaper
!
```

Study the exhibit carefully. A router has a 256 kbps Frame Relay circuit connected to interface serial 0/0. As a large FTP packet is being placed into the hardware transmit queue of interface serial 0/0, a voice packet is placed into the priority queue of that interface. How, and in what order, will the packets be transmitted?

A. The voice packet will be transmitted first, followed by the fragmented FTP packet.
B. The FTP packet will be fragmented and the voice packet will be interleaved.
C. The voice packet will be transmitted first, followed by the FTP packet in its entirety.
D. The FTP packet will be transmitted first in its entirety, followed by the voice packet.
E. None of the above.

Answer: D

QUESTION 51
With QOS there are generally two options; the Differentiated Services model and the Integrated Services model. What are two characteristics of the DiffServ model? (Select two)

A. Traffic that is divided into classes
B. Not scalable to large implementations
C. Service guarantee
D. QoS mechanisms that are used without prior signaling
E. Applications that signal their particular QoS and bandwidth requirements

Answer: A, D

Explanation:
The DiffServ model is similar to a concept known as "soft QoS." With soft QoS, QoS mechanisms are used without prior signaling. In addition, QoS characteristics (for example, bandwidth and delay), are managed on a hop-by-hop basis by policies that are

established independently at each intermediate device in the network. This action is also known as per-hop behavior (PHB). The soft QoS approach is not considered an end-to-end QoS strategy because end-to-end guarantees cannot be enforced. However, soft QoS is a more scalable approach to implementing QoS than hard QoS (the IntServ model), because many (hundreds or potentially thousands) of applications can be mapped into a small set of classes upon which similar sets of QoS behaviors are implemented. Although QoS mechanisms in this approach are enforced and applied on a hop-by-hop basis, uniformly applying global meaning to each traffic class provides both flexibility and scalability.

With DiffServ, network traffic is divided into classes based on business requirements. Each of the classes can then be assigned a different level of service. As the packets traverse a network, each of the network devices identifies the packet class and services the packet according to that class. It is possible to choose many levels of service with DiffServ. For example, voice traffic from IP phones is usually given preferential treatment over all other application traffic, e-mail is generally given best-effort service, and nonbusiness traffic can either be given very poor service or blocked entirely.

QUESTION 52

You need to determine the best method for implementing QoS on the Certkiller network. Which two statements are true about the various methods of implementing QoS? (Select two)

A. Cisco AutoQoS provides capabilities to automate VoIP deployments.
B. The auto qos global configuration command is used to configure Cisco AutoQoS.
C. Cisco AutoQoS can be used repeatedly to apply a single QoS policy to multiple interfaces.
D. The Modular QoS CLI (MQC) is the best way to fine tune QoS configurations.
E. The SDM QoS wizard is the fastest way to implement QoS.
F. Cisco AutoQoS includes an optional web-based GUI for automating the configuration of QoS services.

Answer: A, D

Explanation:

Cisco introduced the Modular QoS CLI (MQC) to simplify QoS configuration by making configurations modular. With MQC, QoS can be configured in a building-block approach using a single module repeatedly to apply policy to multiple interfaces.

Cisco AutoQoS represents innovative technology that simplifies the challenges of network administration by reducing QoS complexity, deployment time, and cost to enterprise networks. Cisco AutoQoS incorporates value-added intelligence in Cisco IOS software and Cisco Catalyst software to provision and assist in the management of large-scale QoS deployments. The first phase of Cisco AutoQoS VoIP offers straightforward capabilities to automate VoIP deployments for customers that want to deploy IP telephony but lack the expertise and staffing to plan and deploy IP QoS and IP services. The second phase, Cisco AutoQoS Enterprise, which is supported only on router interfaces, uses Network-Based Application Recognition (NBAR) to discover the traffic. After this discovery phase, the AutoQoS process can then configure the interface to support up to 10 traffic classes.

QUESTION 53
With QOS there are generally two options; the Differentiated Services model and the Integrated Services model. Which two statements are true about RSVP and the IntServ QoS model? (Select two)

A. The flow-based approach of RSVP is ideal for large, scalable implementations such as the public Internet.
B. RSVP specifically provides a level of service for rate-sensitive and delay-sensitive traffic.
C. RSVP is an IP protocol that uses IP protocol ID 46, and TCP/UDP ports 3455.
D. A drawback of implementing RSVP is the requirement to migrate to a supporting routing protocol.
E. RSVP is a routing protocol.
F. RSVP uses DSCP to signal QoS requirements to routers.

Answer: B, C

Explanation:
RSVP is a network control protocol that enables applications to obtain differing QoS for their data flows. Such a capability recognizes that different applications have different network performance requirements. Some applications, including the more traditional interactive and batch applications, require reliable delivery of data but do not impose any stringent requirements for the timeliness of delivery. Newer application types, including videoconferencing, IP telephony, and other forms of multimedia communications, require almost the exact opposite: Data delivery must be timely but not necessarily reliable. Thus, RSVP was intended to provide IP networks with the ability to support the divergent performance requirements of differing application types.
RSVP is an IP protocol that uses IP protocol ID 46 and TCP and UDP port 3455. It is important to note that RSVP is not a routing protocol. RSVP works in conjunction with routing protocols and installs the equivalent of dynamic access control lists (ACLs) along the routes that routing protocols calculate. Thus, implementing RSVP in an existing network does not require migration to a new routing protocol.

QUESTION 54
You need to configure QoS on a new Certkiller router. What are two steps needed to define a QoS policy for a traffic class? (Select two)

A. Assign priorities to the class.
B. Determine interfaces to which to apply policy.
C. Determine a minimum bandwidth guarantee.
D. Configure access control lists.

Answer: A, C

Explanation:
Complete these steps to implement QoS using the MQC:
Step 1 Configure traffic classification by using the class-map command.
Step 2 Configure traffic policy by associating the traffic class with one or more QoS features using the policy-map command.
Step 3 Attach the traffic policy to inbound or outbound traffic on interfaces, subinterfaces, or virtual circuits by using the service-policy command.

QUESTION 55
With QOS there are generally two options; the Differentiated Services model and the Integrated Services model. Which two statements about the DiffServ QoS model are true? (Select two)

A. Network traffic is identified by class, and the level of service is chosen for each class.
B. The DiffServ model relies on a fairly simple mechanism to provide QoS over a wide range of equipment.
C. The DiffServ model is more scalable than the IntServ model.
D. The flow-based approach of the DiffServ model is ideal for large scalable implementations such as the public Internet.
E. DiffServ requires RSVP to set up a path through the network to accommodate the requested QoS.
F. RSVP enables the DiffServ model to provide end-to-end QoS.

Answer: A, C

Explanation:
The DiffServ model is similar to a concept known as "soft QoS." With soft QoS, QoS mechanisms are used without prior signaling. In addition, QoS characteristics (for example, bandwidth and delay), are managed on a hop-by-hop basis by policies that are established independently at each intermediate device in the network. This action is also known as per-hop behavior (PHB). The soft QoS approach is not considered an end-to-end QoS strategy because end-to-end guarantees cannot be enforced. However, soft QoS is a more scalable approach to implementing QoS than hard QoS (the IntServ model), because many (hundreds or potentially thousands) of applications can be mapped into a small set of classes upon which similar sets of QoS behaviors are implemented. Although QoS mechanisms in this approach are enforced and applied on a hop-by-hop basis, uniformly applying global meaning to each traffic class provides both flexibility and scalability.
With DiffServ, network traffic is divided into classes based on business requirements. Each of the classes can then be assigned a different level of service. As the packets traverse a network, each of the network devices identifies the packet class and services the packet according to that class. It is possible to choose many levels of service with DiffServ. For example, voice traffic from IP phones is usually given preferential treatment over all other application traffic, e-mail is generally given best-effort service, and nonbusiness traffic can either be given very poor service or blocked entirely.

QUESTION 56

Certkiller has chosen to use the DiffServ model over the IntServ model. Which two statements about the DiffServ model are true? (Select two)

A. The primary goal of DiffServ is scalability.
B. The DiffServ field occupies the same eight bits of the MAC header that were previously used for the ToS field.
C. DiffServ uses the DiffServ field in the MAC header to mark frames into behavior aggregates (BAs).
D. A class can be identified as a single application, multiple applications with similar service needs, or be based on the source or destination IP addresses.
E. A drawback of the DiffServ model is that it does not provide backward compatibility with devices that can only use the ToS field.
F. The first six high-order bits of the DiffServ field are used to identify the Resource Reservation Protocol (RSVP) value.

Answer: A, D

Explanation:
The DiffServ model is similar to a concept known as "soft QoS." With soft QoS, QoS mechanisms are used without prior signaling. In addition, QoS characteristics (for example, bandwidth and delay), are managed on a hop-by-hop basis by policies that are established independently at each intermediate device in the network. This action is also known as per-hop behavior (PHB). The soft QoS approach is not considered an end-to-end QoS strategy because end-to-end guarantees cannot be enforced. However, soft QoS is a more scalable approach to implementing QoS than hard QoS (the IntServ model), because many (hundreds or potentially thousands) of applications can be mapped into a small set of classes upon which similar sets of QoS behaviors are implemented. Although QoS mechanisms in this approach are enforced and applied on a hop-by-hop basis, uniformly applying global meaning to each traffic class provides both flexibility and scalability.
With DiffServ, network traffic is divided into classes based on business requirements. Each of the classes can then be assigned a different level of service. As the packets traverse a network, each of the network devices identifies the packet class and services the packet according to that class. It is possible to choose many levels of service with DiffServ. For example, voice traffic from IP phones is usually given preferential treatment over all other application traffic, e-mail is generally given best-effort service, and nonbusiness traffic can either be given very poor service or blocked entirely.

QUESTION 57

With QOS there are generally two options; the Differentiated Services model and the Integrated Services model. Which two statements are true about the implementation of QoS? (Select two)

A. Implementing IntServ involves the utilization of RSVP.

B. Traffic should be classified and marked by the core network devices.
C. Implementing IntServ allows QoS to be performed by configuring only the ingress and egress devices.
D. Traffic should be classified and marked as close to the edge of the network as possible.
E. Implementing DiffServ involves the configuration of RSVP.

Answer: A, D

Explanation:
Cisco IOS QoS features enable network administrators to control and predictably service a variety of networked applications and traffic types, allowing network managers to take advantage of a new generation of media-rich and mission-critical applications. The goal of QoS is to provide better and more predictable network service by providing dedicated bandwidth, controlled jitter and latency, and improved loss characteristics. QoS achieves these goals by providing tools for managing network congestion, shaping network traffic, using expensive wide-area links more efficiently, and setting traffic policies across the network. QoS offers intelligent network services that, when correctly applied, help to provide consistent and predictable performance
Integrated Services (IntServ): IntServ can provide very high QoS to IP packets. Essentially, applications signal to the network that they will require special QoS for a period of time and that bandwidth should be reserved. With IntServ, packet delivery is guaranteed. However, the use of IntServ can severely limit the scalability of a network. IntServ uses Resource Reservation Protocol (RSVP) to explicitly signal the QoS needs of traffic of an application along the devices in the end-to-end path through the network. If network devices along the path can reserve the necessary bandwidth, the originating application can begin transmitting. If the requested reservation fails along the path, the originating application will not send any data.

QUESTION 58
The best QoS method needs to be determined for use in the Certkiller network. In which QoS model do applications signal the network that they require certain QoS parameters?

A. Best Effort
B. Hierarchical
C. DiffServ
D. IntServ
E. WFQ
F. CBWFQ
G. None of the above

Answer: D

Explanation:
Integrated Services (IntServ): IntServ can provide very high QoS to IP packets.

Essentially, applications signal to the network that they will require special QoS for a period of time and that bandwidth should be reserved. With IntServ, packet delivery is guaranteed. However, the use of IntServ can severely limit the scalability of a network.

QUESTION 59
You need to define a new QoS policy for use in the Certkiller network. What are two steps that are needed to define a QoS policy? (Select two)

A. Configure CBWFQ for best-effort traffic.
B. Establish timers.
C. Determine a specific transfer rate.
D. Set a minimum bandwidth guarantee.
E. Set a maximum bandwidth limit.
F. Increase bandwidth.

Answer: D, E

Explanation:
When you specify the priority command for a class, you can use the bandwidth argument to specify the maximum bandwidth in kilobits per second. You use this parameter to specify the maximum amount of bandwidth allocated for packets belonging to the 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.

QUESTION 60
Certkiller is contemplating the use of the IntServ model for their QoS needs. What is a drawback to using the IntServ model?

A. Admission control not supported
B. Not scalable to large implementations
C. UDP not supported
D. Use of dynamic port numbers
E. RSVP that signals QoS requests per individual flow
F. None of the above

Answer: B

Explanation:
IntServ also has these drawbacks:
1. There is continuous signaling because of the stateful RSVP architecture.
2. The flow-based approach is not scalable to large implementations, such as the public Internet, because RSVP has to track each individual flow. This circumstance would make end-to-end signaling very difficult. A possible solution is to combine IntServ with elements from the DiffServ model to provide the needed scalability.

QUESTION 61
You want to implement QoS on the Certkiller devices to support a converged network. What are the three steps to implement a QoS policy in a network? (Select three)

A. Divide traffic into classes.
B. Identify traffic requirements.
C. Label each class.
D. Define QoS policies for each class.
E. Choose DiffServ or IntServ as the QoS model.
F. Configure ACLs to define queues.

Answer: A, B, D

Explanation:
There are three basic steps involved in implementing QoS on a Network:
1. Identify traffic and its requirements. Study the network to determine the type of traffic running on the network and then determine the QoS requirements for the different types of traffic.
2. Group the traffic into classes with similar QoS requirements.
3. Define the QoS policies that will meet the QoS requirements for each traffic class.

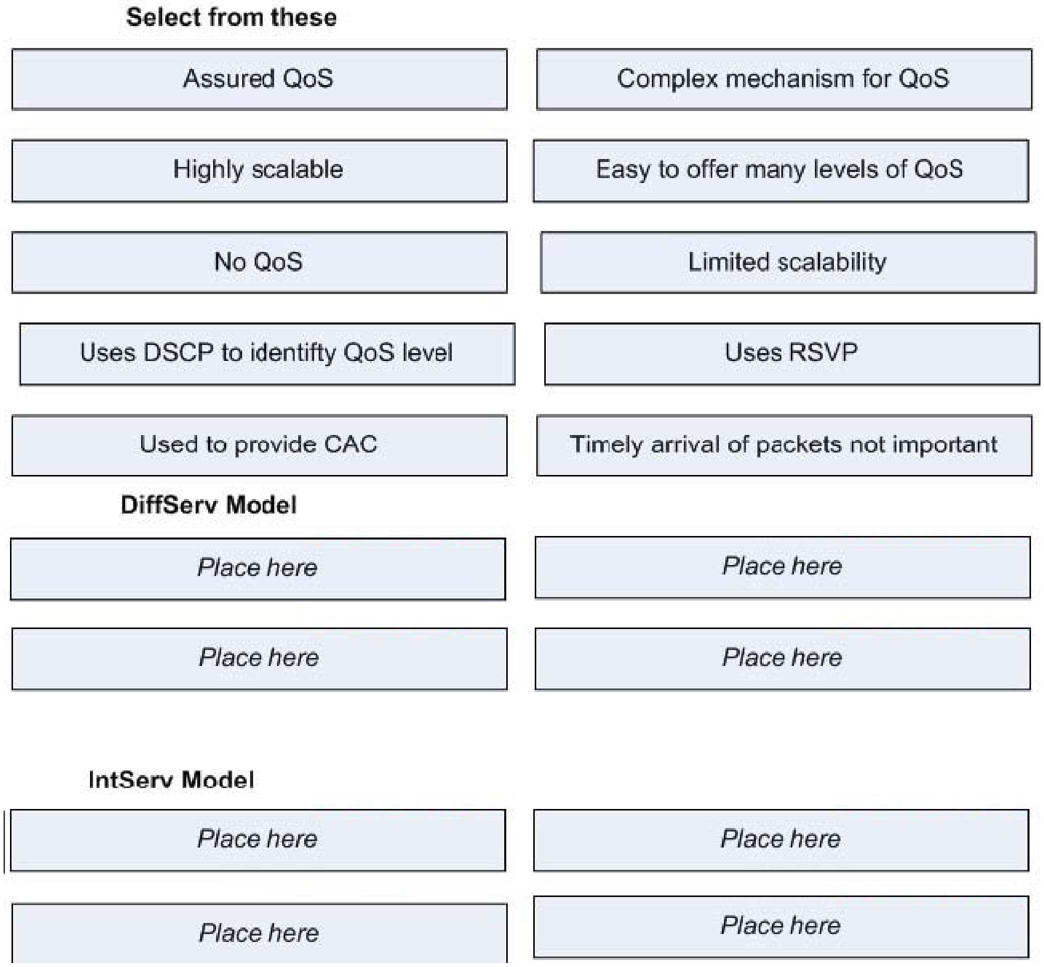
QUESTION 62
You have been tasked with setting up QoS policies on the Certkiller network. For defining the QoS policies for each traffic class, which parameters should be identified? (Select three)

A. Priority
B. Average bandwidth guarantee
C. Maximum bandwidth guarantee
D. IP precedence
E. Minimum bandwidth guarantee
F. Optimum bandwidth guarantee

Answer: A, C, E

Explanation:
When implementing QoS policies on network for each traffic class, you need to identify the parameters of: priority, Maximum bandwidth, Minimum Bandwidth Guarantee.
Example:
When you specify the priority command for a class, you can use the bandwidth argument to specify the maximum bandwidth in kilobits per second. You use this parameter to specify the maximum amount of bandwidth allocated for packets belonging to the 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.
priority{bandwidth | percent percentage} [burst]

QUESTION 63
DRAG DROP
Drag each descriptor on the left to the QoS model on the right to which the descriptor applies.
Note: Not all descriptors will be applied.



Select from these

Assured QoS	Complex mechanism for QoS
Highly scalable	Easy to offer many levels of QoS
No QoS	Limited scalability
Uses DSCP to identifty QoS level	Uses RSVP
Used to provide CAC	Timely arrival of packets not important

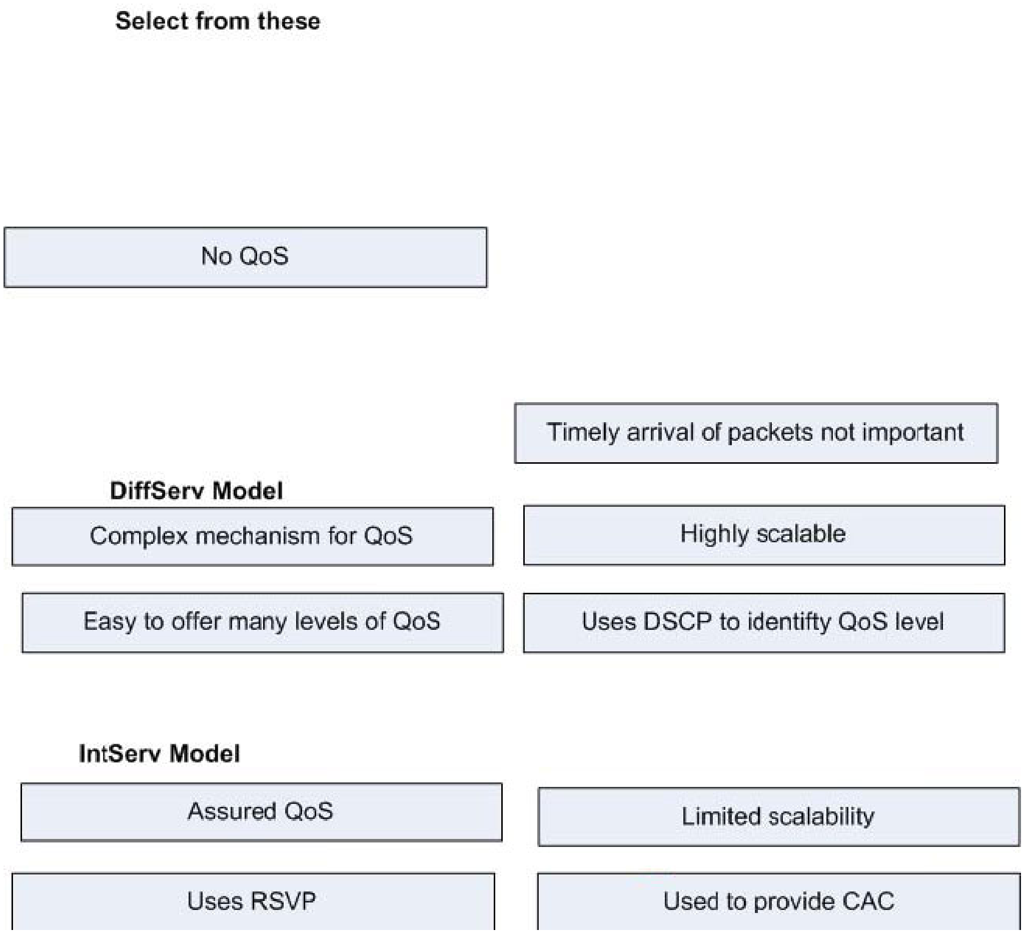
DiffServ Model

Place here	*Place here*
Place here	*Place here*

IntServ Model

Place here	*Place here*
Place here	*Place here*

Answer:



Select from these

No QoS

Timely arrival of packets not important

DiffServ Model

Complex mechanism for QoS

Highly scalable

Easy to offer many levels of QoS

Uses DSCP to identifty QoS level

IntServ Model

Assured QoS

Limited scalability

Uses RSVP

Used to provide CAC

Explanation:

Integrated Services (IntServ): IntServ can provide very high QoS to IP packets. Essentially, applications signal to the network that they will require special QoS for a period of time and that bandwidth should be reserved. With IntServ, packet delivery is guaranteed. However, the use of IntServ can severely limit the scalability of a network. IntServ uses Resource Reservation Protocol (RSVP) to explicitly signal the QoS needs of traffic of an application along the devices in the end-to-end path through the network. If network devices along the path can reserve the necessary bandwidth, the originating application can begin transmitting. If the requested reservation fails along the path, the originating application will not send any data.

DiffServ: The DiffServ model is similar to a concept known as "soft QoS." With soft QoS, QoS mechanisms are used without prior signaling. In addition, QoS characteristics (for example, bandwidth and delay), are managed on a hop-by-hop basis by policies that are established independently at each intermediate device in the network. This action is also known as per-hop behavior (PHB). The soft QoS approach is not considered an end-to-end QoS strategy because end-to-end guarantees cannot be enforced. However, soft QoS is a more scalable approach to implementing QoS than hard QoS (the IntServ model), because many (hundreds or potentially thousands) of applications can be mapped into a small set of classes upon which similar sets of QoS behaviors are implemented. Although QoS mechanisms in this approach are enforced and applied on a hop-by-hop basis, uniformly applying global meaning to each traffic class provides both flexibility

and scalability.
With DiffServ, network traffic is divided into classes based on business requirements. Each of the classes can then be assigned a different level of service. As the packets traverse a network, each of the network devices identifies the packet class and services the packet according to that class. It is possible to choose many levels of service with DiffServ. For example, voice traffic from IP phones is usually given preferential treatment over all other application traffic, e-mail is generally given best-effort service, and nonbusiness traffic can either be given very poor service or blocked entirely.

QUESTION 64
Which two statements about the best effort model for QoS are true? (Select two)

A. The default policy identifies a delay sensitive class, best effort class, and a default class.
B. The model provides guaranteed service.
C. Delay sensitive packets are given preferential treatment.
D. The model is still predominant on the Internet.
E. The model is highly scalable.
F. The default policy identifies a delay sensitive class and a default class.

Answer: D, E

Explanation:
Best-effort is a single service model in which an application sends data whenever it must, in any quantity, without requesting permission or first informing the network. For best-effort service, the network delivers data if it can, without any assurance of reliability, delay bounds, or throughput. The Cisco IOS QoS feature that implements best-effort service is FIFO queuing. FIFO is the default method of queuing for LAN and high speed WAN interfaces on switches and routers. Best-effort service is suitable for a wide range of networked applications such as general file transfers, e-mail and Web browsing.

QUESTION 65
Certkiller has decided to use IntServ in parts of their network as opposed to DiffServ. Which two Integrated Services (IntServ) functions are required on a router? (Select two)

A. DSCP classification
B. Monitoring
C. Scheduling
D. Admission control
E. Marking

Answer: C, D

Explanation:

The Integrated Services or IntServ architecture is a multiple service model that can accommodate multiple QoS requirements. In this model the application requests a specific kind of service from the network before it sends data. The request is made by explicit signaling. The application informs the network of its traffic profile and requests a particular kind of service that can encompass its bandwidth and delay requirements. The application is expected to send data only after it gets a confirmation from the network. It is also expected to send data that lies within its described traffic profile.
The network performs admission control, based on information from the application and available network resources. It also commits to meeting the QoS requirements of the application as long as the traffic remains within the profile specifications. The network fulfils its commitment by maintaining a per-flow state and then performing packet classification, policing, and intelligent queuing based on that state.
The Cisco IOS IntServ model allows applications to make use of the IETF Resource Reservation Protocol (RSVP), which can be used by applications to signal their QoS requirements to the router.

QUESTION 66
When comparing the two QOS models (DiffServ versus IntServ), which three statements are true about these QoS models? (Select three)

A. The DiffServ model can be used to deliver QoS based upon IP precedence, or source and destination addresses.
B. The best effort model is suitable for applications such as file transfer and e-mail
C. The DiffServ model requires applications to signal the network with QoS requirements.
D. The DiffServ model requires RSVP.
E. The IntServ model attempts to deliver a level of service based on the QoS specified by each packet
F. The IntServ model requires applications to signal the network with QoS requirements.

Answer: A, B, F

Explanation:
1. DiffServ Model:
The Differentiated Services or DiffServ architecture is an emerging standard from the IETF. This architecture specifies that each packet is classified upon entry into the network. The classification is carried in the IP packet header, using either the IP precedence or the preferred Differential Services Code Point (DSCP). These are represented using the first three or six bits of the Type of Service (ToS) field. Classification can also be carried in the Layer 2 frame in the form of the Class of Service (CoS) field embodied in ISL and 802.1Q frames.
Once packets are classified at the edge by access layer switches or by border routers, the network uses the classification to determine how the traffic should be queued, shaped, and policed.
2. IntServ Model:
The Integrated Services or IntServ architecture is a multiple service model that can

accommodate multiple QoS requirements. In this model the application requests a specific kind of service from the network before it sends data. The request is made by explicit signaling. The application informs the network of its traffic profile and requests a particular kind of service that can encompass its bandwidth and delay requirements. The application is expected to send data only after it gets a confirmation from the network. It is also expected to send data that lies within its described traffic profile.
The network performs admission control, based on information from the application and available network resources. It also commits to meeting the QoS requirements of the application as long as the traffic remains within the profile specifications. The network fulfils its commitment by maintaining a per-flow state and then performing packet classification, policing, and intelligent queuing based on that state.
The Cisco IOS IntServ model allows applications to make use of the IETF Resource Reservation Protocol (RSVP), which can be used by applications to signal their QoS requirements to the router.

QUESTION 67
You need to determine the best QoS strategy for use within the Certkiller network.
What are three considerations when choosing the QoS model to deploy in a network? (Select three)

A. The applications utilizing the network
B. The routing protocols being utilized in the network
C. Network addressing scheme
D. Cost of implementation
E. The amount of the control needed of the resources
F. The traffic destinations

Answer: A, D, E

QUESTION 68
RSVP is already being used in the Certkiller WAN, and you want to implement a QoS method that will take advantage of this. Which QoS model makes use of the Resource Reservation Protocol (RSVP)?

A. Best Effort
B. DSCP
C. NBAR
D. DiffServ
E. IntServ
F. None of the above.

Answer: E

Explanation:
Integrated Services (IntServ): IntServ can provide very high QoS to IP packets. Essentially, applications signal to the network that they will require special QoS for a

period of time and that bandwidth should be reserved. With IntServ, packet delivery is guaranteed. However, the use of IntServ can severely limit the scalability of a network. IntServ uses Resource Reservation Protocol (RSVP) to explicitly signal the QoS needs of traffic of an application along the devices in the end-to-end path through the network. If network devices along the path can reserve the necessary bandwidth, the originating application can begin transmitting. If the requested reservation fails along the path, the originating application will not send any data.

QUESTION 69

The Certkiller network needs to mark packets on the LAN. Which two statements about packet marking at the data link layer are true? (Select two)

A. In an 802.1q frame, the 3-bit 802.1p priority field is used to identify the class of service (CoS) priority.
B. Frames maintain their class of service (CoS) markings when transiting a non-802.1p link.
C. Through the use of DE markings, Frame Relay QoS supports up to 10 classes of service.
D. The 802.1p CoS markings are preserved through the LAN, but are not maintained end to end.
E. IEEE 802.1p supports up to 10 class of service (CoS) markings.

Answer: A, D

Explanation:
The 802.1Q standard is an IEEE specification for implementing VLANs in Layer 2 switched networks. The 802.1Q specification defines two 2-byte fields (tag protocol identifier [TPID] and tag control information [TCI]) that are inserted within an Ethernet frame following the source address field. The TPID field is currently fixed and assigned the value 0x8100. The TCI field is composed of three fields:
User priority bits (PRI) (3 bits): The specifications of this 3-bit field are defined by the IEEE 802.1p standard. These bits can be used to mark packets as belonging to a specific CoS. The CoS marking uses the three 802.1p user priority bits and allows a Layer 2 Ethernet frame to be marked with eight levels of priority (values 0-7). Three bits allow for eight levels of classification, allowing a direct correspondence with IP version 4 (IPv4) (IP precedence) type of service (ToS) values. The table lists the standard definitions the IEEE 802.1p specification defines for each CoS.

QUESTION 70

802.1p allows QoS parameters to be used at the MAC layer on a LAN. The IEEE 802.1p user priority field consists of how many bits?

A. 4
B. 1
C. 8
D. 3

E. 6
F. 2
G. None of the above

Answer: D

Explanation:
User priority bits (PRI) (3 bits): The specifications of this 3-bit field are defined by the IEEE 802.1p standard. These bits can be used to mark packets as belonging to a specific CoS. The CoS marking uses the three 802.1p user priority bits and allows a Layer 2 Ethernet frame to be marked with eight levels of priority (values 0-7). Three bits allow for eight levels of classification, allowing a direct correspondence with IP version 4 (IPv4) (IP precedence) type of service (ToS) values. The table lists the standard definitions the IEEE 802.1p specification defines for each CoS.

QUESTION 71
You need to classify different packets within the Certkiller network so that they can be marked. What are three traffic descriptors typically used to categorize traffic into different classes? (Select three)

A. DSCP
B. DLCI
C. Media type
D. IP precedence
E. Incoming interface
F. Outgoing interface

Answer: A, D, E

Explanation:
Classification is the process of identifying traffic and categorizing that traffic into classes. Classification uses a traffic descriptor to categorize a packet within a specific group to define that packet. Typically used traffic descriptors include these:
1. Incoming interface
2. IP precedence
3. differentiated services code point (DSCP)
4. Source or destination address
5. Application
After the packet has been classified or identified, the packet is then accessible for quality of service (QoS) handling on the network. Using classification, network administrators can partition network traffic into multiple classes of service (CoSs). When traffic descriptors are used to classify traffic, the source implicitly agrees to adhere to the contracted terms and the network promises QoS. Various QoS mechanisms, such as traffic policing, traffic shaping, and queuing techniques, use the traffic descriptor of the packet (that is, the classification of the packet) to ensure adherence to that agreement. Classification should take place at the network edge, typically in the wiring closet, within

IP phones, or at network endpoints. It is recommended that classification occur as close to the source of the traffic as possible.

QUESTION 72

Traffic on the Certkiller LAN needs to be classified and marked at the data link layer. Which three statements about classification marking of traffic at Layer 2 are true? (Select three)

A. A Frame Relay header includes a 1-bit discard eligible (DE) bit to provide the class of service (CoS).
B. The CoS field only exists inside Ethernet frames when 802.1Q or Inter-Switch Link (ISL) trunking is used.
C. An ATM header includes a 1-bit DE field to provide the CoS.
D. An MPLS EXP field is inserted in the Layer 3 IP precedence field to identify the CoS.
E. In the IEEE 802.1p standard, three bits are used to identify the user priority bits for the CoS.
F. In the IEEE 802.1q standard, six bits are used to identify the user priority bits for the CoS.

Answer: A, B, E

Explanation:
Marking is related to classification. Marking allows network devices to classify a packet or frame at the edge based on a specific traffic descriptor. Typically used traffic descriptors include these:
Data Link layer
* CoS (Inter-Switch Link [ISL], 802.1p)
* Multiprotocol Label Switching (MPLS) experimental (EXP) bits
* Frame Relay
Network layer
* DSCP
* IP precedence
Marking can be used to set information in the Layer 2 frame or Layer 3 packet headers. Marking a packet or frame with its classification allows subsequent network devices to easily distinguish the marked packet or frame as belonging to a specific class. After the packets or frames are identified as belonging to a specific class, QoS mechanisms can be uniformly applied to ensure compliance with administrative QoS policies.
Classification is the process of identifying traffic and categorizing that traffic into classes. Classification uses a traffic descriptor to categorize a packet within a specific group to define that packet. Typically used traffic descriptors include these:
1. Incoming interface
2. IP precedence
3. differentiated services code point (DSCP)
4. Source or destination address
5. Application
After the packet has been classified or identified, the packet is then accessible for quality

of service (QoS) handling on the network. Using classification, network administrators can partition network traffic into multiple classes of service (CoSs). When traffic descriptors are used to classify traffic, the source implicitly agrees to adhere to the contracted terms and the network promises QoS. Various QoS mechanisms, such as traffic policing, traffic shaping, and queuing techniques, use the traffic descriptor of the packet (that is, the classification of the packet) to ensure adherence to that agreement. Classification should take place at the network edge, typically in the wiring closet, within IP phones, or at network endpoints. It is recommended that classification occur as close to the source of the traffic as possible.

QUESTION 73
You want to implement QoS on your enterprise network using best practices.
Where is the least likely place for classification to be performed?

A. Access layer
B. Core layer
C. End system
D. Distribution layer
E. None of the above

Answer: B

Explanation:
The model provides a modular framework that allows flexibility in network design and facilitates ease of implementation and troubleshooting. The hierarchical model divides networks or their modular blocks into the access, distribution, and core layers, with these features:
The access layer is used to grant user access to network devices. In a network campus, the access layer generally incorporates switched LAN devices with ports that provide connectivity to workstations and servers. In the WAN environment, the access layer at remote sites or at a teleworker location may provide access to the corporate network across WAN technology.
The distribution layer aggregates the wiring closets, and uses switches to segment workgroups and isolate network problems in a campus environment. Similarly, the distribution layer aggregates WAN connection at the edge of the campus and provides policy-based connectivity.
The core layer (also referred to as the backbone) is a high-speed backbone and is designed to switch packets as fast as possible. Because the core is critical for connectivity, it must provide a high level of availability and adapt to changes very quickly. This is the layer where is the least likely classification placed.

QUESTION 74
Some of the Incoming packets seen on a Certkiller router are marked with the DSCP value 101110. Which PHB is identified in this DSCP value?

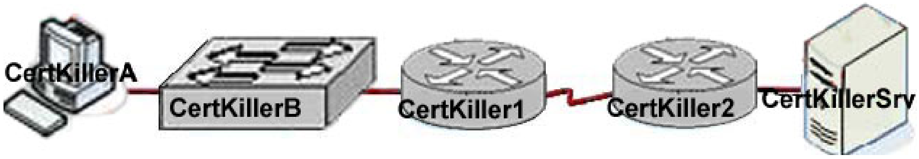
A. Class selector PHB

B. Expedited Forwarding (EF) PHB
C. Default PHB
D. Assured Forwarding (AF) PHB
E. None of the above

Answer: B

Explanation:
The EF PHB is identified based on the following:
1. The EF PHB ensures a minimum departure rate: The EF PHB provides the lowest possible delay to delay-sensitive applications.
2. The EF PHB guarantees bandwidth: The EF PHB prevents starvation of the application if there are multiple applications using EF PHB.
3. The EF PHB polices bandwidth when congestion occurs: The EF PHB prevents starvation of other applications or classes that are not using this PHB. Packets requiring EF should be marked with DSCP binary value 101110 (46 or 0x2E).
Non-DiffServ-compliant devices regard EF DSCP value 101110 as IP precedence 5 (101). This precedence is the highest user-definable IP precedence and is typically used for delay-sensitive traffic (such as VoIP). Bits 5 to 7 of the EF DSCP value are 101, which matches IP precedence 5 and allows backward compatibility.

QUESTION 75
Which two QoS fields should be used by R1 and R2 to classify the traffic sent from PC1 to Server1? (Select two)



A. Priority bits
B. DE bit
C. IP DSCP
D. CoS
E. IP precedence

Answer: C, E

Explanation:
The introduction of DSCP replaces IP precedence, a 3-bit field in the ToS byte of the IP header originally used to classify and prioritize types of traffic. However, DiffServ maintains interoperability with non-DiffServ-compliant devices (those that still use IP precedence). Because of this backward compatibility, DiffServ can be deployed gradually in large networks.
The meaning of the 8 bits in the DiffServ field of the IP packet has changed over time to meet the expanding requirements of IP networks.
Originally, the field was referred to as the ToS field, and the first three bits of the field (bits 7 to 5) defined a packet IP precedence value. A packet could be assigned one of six

priorities based on the value of the IP precedence value (eight total values minus two reserved ones). IP precedence 5 (101) was the highest priority that could be assigned (RFC 791). RFC 2474 replaced the ToS field with the DiffServ field, in which a range of eight values (class selector) is used for backward compatibility with IP precedence. There is no compatibility with other bits used by the ToS field. The class selector PHB was defined to provide backward compatibility for DSCP with ToS-based IP precedence. RFC 1812 simply prioritizes packets according to the precedence value. The PHB is defined as the probability of timely forwarding. Packets with higher IP precedence should be (on average) forwarded in less time than packets with lower IP precedence.

QUESTION 76

NBAR is being used to recognize the traffic traversing the Certkiller network. What are the steps for configuring stateful NBAR for dynamic protocols?

A. Configure a traffic class. Configure a traffic policy. Attach the traffic policy to an interface
B. Use the command ip nbar protocol-discovery to allow identification of stateful protocols. Use the command ip nbar port-map to attach the protocols to an interface.
C. Use the command match protocol to allow identification of stateful protocols. Use the command ip nbar port-map to attach the protocols to an interface.
D. Configure video streaming. Configure audio streaming. Attach the codec to an interface.
E. Use the command match protocol rtp to allow identification of real-time audio and video traffic. Use the command ip nbar port-map to extend the NBAR functionality for well-known protocols to new port numbers.
F. None of the above.

Answer: A

Explanation:
Network-Based Application Recognition (NBAR), a feature in Cisco IOS software, provides intelligent network classification for the infrastructure. NBAR is a classification engine that can recognize a wide variety of applications, including web-based applications and client and server applications that dynamically assign TCP or User Datagram Protocol (UDP) port numbers. After the application is recognized, the network can invoke specific services for that particular application. NBAR currently works with quality of service (QoS) features to ensure that the network bandwidth is best used to fulfill company objectives. These features include the ability to guarantee bandwidth to critical applications, limit bandwidth to other applications, drop selected packets to avoid congestion, and mark packets appropriately so that the network and the service provider network can provide QoS from end to end.
Complete the following steps to implement the QoS
Step 1 Configure traffic classification by using the class-map command.
Step 2 Configure traffic policy by associating the traffic class with one or more QoS features using the policy-map command.

Step 3 Attach the traffic policy to inbound or outbound traffic on interfaces, subinterfaces, or virtual circuits by using the service-policy command.

QUESTION 77

You need to implement NBAR into the Certkiller network. Which three configuration tasks are required to successfully deploy NBAR to recognize TCP and UDP stateful protocols? (Select three)

A. Use the "ip rsvp bandwidth" command to set a strict upper limit on the bandwidth NBAR uses, and to guarantee admission of any flows.
B. Use the "service-policy" command to attach a traffic flow to an interface on the router.
C. Use the "class-map" command to define one or more traffic classes by specifying the criteria by which traffic is classified.
D. Use the "policy-map" command to define one or more QoS policies (such as shaping, policing, and so on) to apply to traffic defined by a class map.
E. Use the "random-detect dscp" command to modify the default minimum and maximum thresholds for the DSCP value.
F. Over leased lines, use the "multilink ppp" command to reduce latency and jitter, and to create Distributed Link Fragmentation and interleaving.

Answer: B, C, D

Explanation:
Complete the following steps to implement the QoS
Step 1 Configure traffic classification by using the class-map command.
Step 2 Configure traffic policy by associating the traffic class with one or more QoS features using the policy-map command.
Step 3 Attach the traffic policy to inbound or outbound traffic on interfaces, subinterfaces, or virtual circuits by using the service-policy command.

QUESTION 78

The Certkiller network is using NBAR to classify applications that use well known static TCP and UDP ports. The company has recently added several applications that are not currently recognized by their NBAR implementation. A PDLM file has been downloaded to the routers to be used by NBAR for protocol matching. What action should be taken so that NBAR can use the data in the PDLM file?

A. Reboot the router so that NBAR will read the file into memory.
B. Configure the routers with the global "ip nbar port-map" command and reboot.
C. Configure the routers with the global "ip nbar pdlm" command.
D. Do nothing. NBAR automatically uses the data in the PDLM file once download is complete.
E. Stop and restart CEF so that NBAR will read the file into memory.
F. None of the above

Answer: C

Explanation:
NBAR is the first mechanism that supports dynamic upgrades without having to change the Cisco IOS version or restart a router. PDLMs contain the rules that are used by NBAR to recognize an application by matching text patterns in data packets, and they can be used to bring new or changed functionality to NBAR.
An external PDLM can be loaded at run time to extend the NBAR list of recognized protocols. PDLMs can be used to enhance an existing protocol-recognition capability. PDLMs allow NBAR to recognize new protocols without requiring a new Cisco IOS image or a router reload.
Router(Config)# ip nbar pdlm pdlm_name : Used to enhance the list of protocols recognized by NBAR through a PDLM.

QUESTION 79
You need to classify the specific traffic traversing the Certkiller network. Which classification tool can be used to classify traffic based on the HTTP URL?

A. Class-based policing
B. Committed access rate (CAR)
C. Network-based application recognition (NBAR)
D. Dial peers
E. Policy-based routing (PBR)
F. None of the above

Answer: C

Explanation:
Network-Based Application Recognition (NBAR), a feature in Cisco IOS software, provides intelligent network classification for the infrastructure. NBAR is a classification engine that can recognize a wide variety of applications, including web-based applications and client and server applications that dynamically assign TCP or User Datagram Protocol (UDP) port numbers. After the application is recognized, the network can invoke specific services for that particular application. NBAR currently works with quality of service (QoS) features to ensure that the network bandwidth is best used to fulfill company objectives. These features include the ability to guarantee bandwidth to critical applications, limit bandwidth to other applications, drop selected packets to avoid congestion, and mark packets appropriately so that the network and the service provider network can provide QoS from end to end.

QUESTION 80
NBAR has been configured on router CK1 . What is supported by the network-based application recognition (NBAR) feature?

A. Matching beyond the first 400 bytes in a packet payload
B. Multicast and switching modes other than Cisco Express Forwarding (CEF)
C. Subport classification

D. More than 24 concurrent URLs, hosts, or MIME-type matches
E. Fragmented packets
F. None of the above

Answer: C

Explanation:
NBAR is a classification and protocol discovery feature. NBAR can determine the mix of traffic on the network, which is important in isolating congestion problems.
NBAR can classify application traffic by subport classification, or looking beyond the TCP or UDP port numbers of a packet. NBAR looks into the TCP or UDP payload itself and classifies packets based on the content within the payload, such as transaction identifier, message type, or other, similar data.
Classification of HTTP, by URL, or by Multipurpose Internet Mail Extensions (MIME) type is an example of subport classification. NBAR classifies HTTP traffic by text within the URL, using regular expression matching. NBAR uses the UNIX filename specification as the basis for the URL specification format. The NBAR engine then converts the specification format into a regular expression.
The NBAR Protocol Discovery feature provides an easy way to discover application protocols that are transiting an interface. The feature discovers any protocol traffic supported by NBAR. NBAR Protocol Discovery can be applied to interfaces and can be used to monitor both input and output traffic. It maintains the following per-protocol statistics for enabled interfaces: Total number of input and output packets and bytes Input and output bit rates
An external Packet Description Language Module (PDLM) can be loaded at run time to extend the NBAR list of recognized protocols. PDLMs can also be used to enhance an existing protocol-recognition capability. PDLMs allow NBAR to recognize new protocols without requiring a new Cisco IOS image or a router reload.

QUESTION 81
Network Based Application Discovery is being used within the Certkiller network.
What is the purpose of the NBAR discovery protocol?

A. To build a database of all application data that passes through the router and queue the data accordingly
B. To build a Packet Description Language Module (PDLM) file to be used in protocol matching
C. To look into the TCP or UDP payload and classify packets based on the content
D. To discover applications and build class maps for data classification
E. None of the above

Answer: C

Explanation:
The NBAR Protocol Discovery feature provides an easy way to discover application protocols that are transiting an interface. The feature discovers any protocol traffic

supported by NBAR. NBAR Protocol Discovery can be applied to interfaces and can be used to monitor both input and output traffic. It maintains the following per-protocol statistics for enabled interfaces: Total number of input and output packets and bytes Input and output bit rates
An external Packet Description Language Module (PDLM) can be loaded at run time to extend the NBAR list of recognized protocols. PDLMs can also be used to enhance an existing protocol-recognition capability. PDLMs allow NBAR to recognize new protocols without requiring a new Cisco IOS image or a router reload.

QUESTION 82
NBAR is being used in the Certkiller network for application identification. Which three statements about the NBAR protocol are true? (Select three)

A. NBAR classifies HTTP traffic by text within the URL.
B. NBAR is used by IntServ as a classification and protocol discovery feature.
C. NBAR performs identification of Layer 4 through Layer 7 applications and protocols.
D. NBAR can be used to classify output traffic on a WAN link where tunneling or encryption is used.
E. Packet Description Language Modules (PDLMs) allow NBAR to recognize new protocols without requiring a new Cisco IOS image or a router reload.
F. NBAR is supported on logical interfaces such as Fast EtherChannel.

Answer: A, C, E

Explanation:
NBAR is a classification and protocol discovery feature. NBAR can determine the mix of traffic on the network, which is important in isolating congestion problems.
NBAR can classify application traffic by subport classification, or looking beyond the TCP or UDP port numbers of a packet. NBAR looks into the TCP or UDP payload itself and classifies packets based on the content within the payload, such as transaction identifier, message type, or other, similar data.
Classification of HTTP, by URL, or by Multipurpose Internet Mail Extensions (MIME) type is an example of subport classification. NBAR classifies HTTP traffic by text within the URL, using regular expression matching. NBAR uses the UNIX filename specification as the basis for the URL specification format. The NBAR engine then converts the specification format into a regular expression.
The NBAR Protocol Discovery feature provides an easy way to discover application protocols that are transiting an interface. The feature discovers any protocol traffic supported by NBAR. NBAR Protocol Discovery can be applied to interfaces and can be used to monitor both input and output traffic. It maintains the following per-protocol statistics for enabled interfaces: Total number of input and output packets and bytes Input and output bit rates

---

QUESTION 83
A new PDLM file has been downloaded from Cisco and needs to be used on a Certkiller router. Which command would add a new Packet Description Language

Module (PDLM) called citrix.pdlm to the list of protocols that would be recognized by network-based application recognition (NBAR)?

A. RTA(config)# ip nbar pdlm flash://citrix.pdlm
B. RTA(config)# ip nbar pdlm
C. RTA(config-if)# ip nbar pdlm flash://citrix.pdlm
D. RTA# ip nbar pdlm
E. RTA(config-if)# ip nbar pdlm
F. RTA# ip nbar pdlm flash://citrix.pdlm
G. None of the above

Answer: A

Explanation:
NBAR is the first mechanism that supports dynamic upgrades without having to change the Cisco IOS version or restart a router. PDLMs contain the rules that are used by NBAR to recognize an application by matching text patterns in data packets, and they can be used to bring new or changed functionality to NBAR.
An external PDLM can be loaded at run time to extend the NBAR list of recognized protocols. PDLMs can be used to enhance an existing protocol-recognition capability. PDLMs allow NBAR to recognize new protocols without requiring a new Cisco IOS image or a router reload.
Router(Config)# ip nbar pdlm pdlm_name : Used to enhance the list of protocols recognized by NBAR through a PDLM.

QUESTION 84
RED has been configured on many of the Certkiller routers. What are three random early detection (RED) dropping modes? (Select three)

A. Center drop
B. Head drop
C. Random drop
D. No drop
E. Tail drop

Answer: C, D, E

Explanation:
Random early detection (RED) is a dropping mechanism that randomly drops packets before a queue is full. The dropping strategy is based primarily on the average queue length-that is, when the average size of the queue increases, RED is more likely to drop an incoming packet than when the average queue length is shorter.
Because RED drops packets randomly, it has no per-flow intelligence. The rationale is that an aggressive flow will represent most of the arriving traffic, and it is likely that RED will drop a packet of an aggressive session. RED therefore punishes more aggressive sessions with a higher statistical probability and is able to somewhat

selectively slow the most significant cause of congestion. Directing one TCP session at a time to slow down allows for full utilization of the bandwidth rather than utilization that manifests itself as crests and troughs of traffic.
As a result of implementing RED, TCP global synchronization is much less likely to occur, and TCP can utilize link bandwidth more efficiently. In RED implementations, the average queue size also decreases significantly, because the possibility of the queue filling up is reduced. This is because of very aggressive dropping in the event of traffic bursts, when the queue is already quite full.
RED distributes losses over time and normally maintains a low queue depth while absorbing traffic spikes. RED can also utilize IP precedence or differentiated services code point (DSCP) bits in packets to establish different drop profiles for different classes of traffic.
RED is useful only when the bulk of the traffic is TCP traffic. With TCP, dropped packets indicate congestion, so the packet source reduces its transmission rate. With other protocols, packet sources might not respond or might re-send dropped packets at the same rate, and so dropping packets might not decrease congestion.
RED has three modes:
* No drop: When the average queue size is between 0 and the minimum threshold
* Random drop:When the average queue size is between the minimum and the maximum threshold
* Full drop (tail drop):When the average queue size is above the maximum threshold
* Random drop should prevent congestion (prevent tail drops).

QUESTION 85
You need to implement QoS on the Certkiller network. Which two queuing methods will allow a percentage of the available bandwidth to be allocated to each queue?
(Select two)

A. Weighted Fair Queuing (WFQ)
B. Priority Queuing (PQ)
C. Class-based WFQ (CBWFQ)
D. Custom Queuing (CQ)
E. Low Latency Queuing (LLQ)
F. First-In, First-Out Queuing (FIFO)

Answer: C, E

Explanation:
1. CBWFQ:
Class-based weighted fair queuing (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. By using CBWFQ, network managers can define traffic classes based on several match criteria, including protocols, access control lists (ACLs), and input interfaces. A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class. More than one IP flow, or "conversation", can belong to a class.
Once a class has been defined according to its match criteria, the characteristics can be

assigned to the class. To characterize a class, assign the bandwidth and maximum packet limit. The bandwidth assigned to a class is the guaranteed bandwidth given to the class during congestion.

CBWFQ assigns a weight to each configured class instead of each flow. This weight is proportional to the bandwidth configured for each class. Weight is equal to the interface bandwidth divided by the class bandwidth. Therefore, a class with a higher bandwidth value will have a lower weight.

By default, the total amount of bandwidth allocated for all classes must not exceed 75 percent of the available bandwidth on the interface. The other 25 percent is used for control and routing traffic.

The queue limit must also be specified for the class. The specification is the maximum number of packets allowed to accumulate in the queue for the class. Packets belonging to a class are subject to the bandwidth and queue limits that are configured for the class.

2. LLQ

The Low Latency Queuing (LLQ) feature provides strict priority queuing for class-based weighted fair queuing (CBWFQ), reducing jitter in voice conversations. Configured by the priority command, strict priority queuing gives delay-sensitive data, such as voice, preferential treatment over other traffic. With this feature, delay-sensitive data is sent first, before packets in other queues are treated. LLQ is also referred to as priority queuing/class-based weighted fair queuing (PQ/CBWFQ) because it is a combination of the two techniques.

For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth assigned to the class during configuration. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced equally, based on weight. No class of packets may be granted strict priority. This scheme poses problems for voice and video traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission, which manifest as jitter in the conversation.

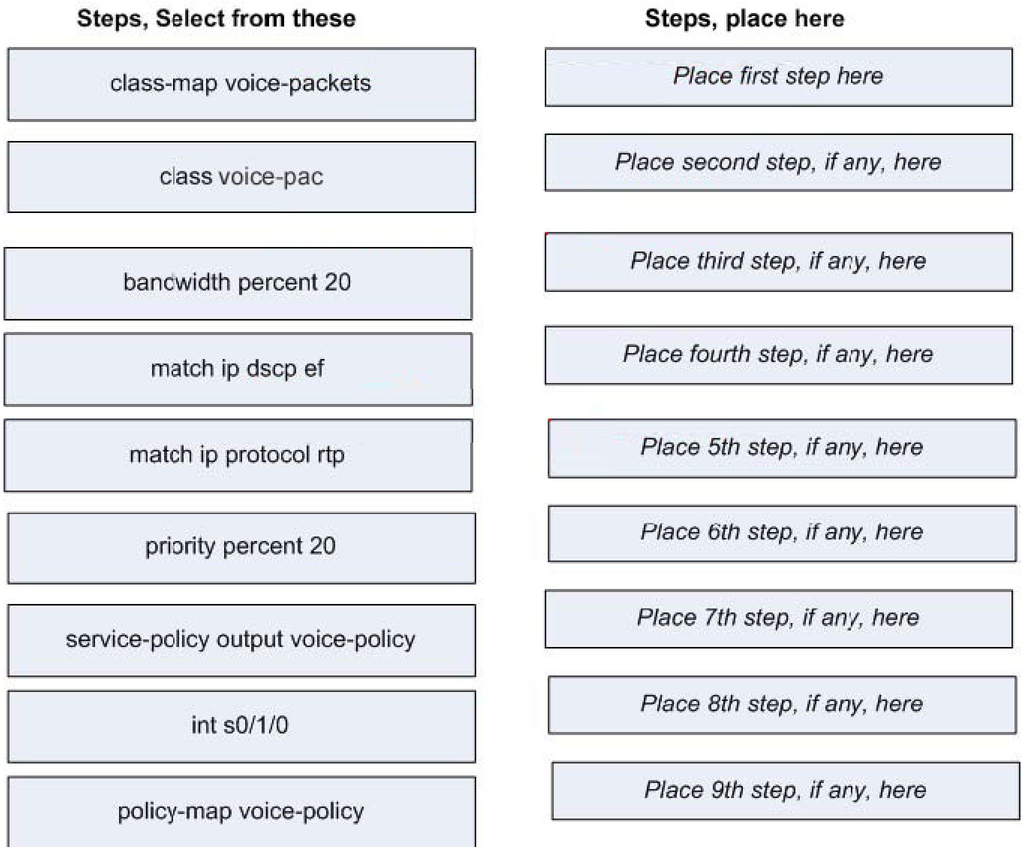
To enqueue a class of traffic to the strict priority queue, configure the priority command for the class after specifying the class within a policy map. Classes to which the priority command is applied are considered priority classes. Within a policy map, give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is enqueued to the same, single, strict priority queue and they will contend with each other for bandwidth

---

QUESTION 86

DRAG DROP

Using the fewest commands possible, drag the commands on the left to the blanks on the right to configure and apply a QoS policy that guarantees that voice packets receive 20 percent of the bandwidth on the S0/1/0 interface.



Steps, Select from these

class-map voice-packets

class voice-pac

bandwidth percent 20

match ip dscp ef

match ip protocol rtp

priority percent 20

service-policy output voice-policy

int s0/1/0

policy-map voice-policy

Steps, place here

Place first step here

Place second step, if any, here

Place third step, if any, here

Place fourth step, if any, here

Place 5th step, if any, here

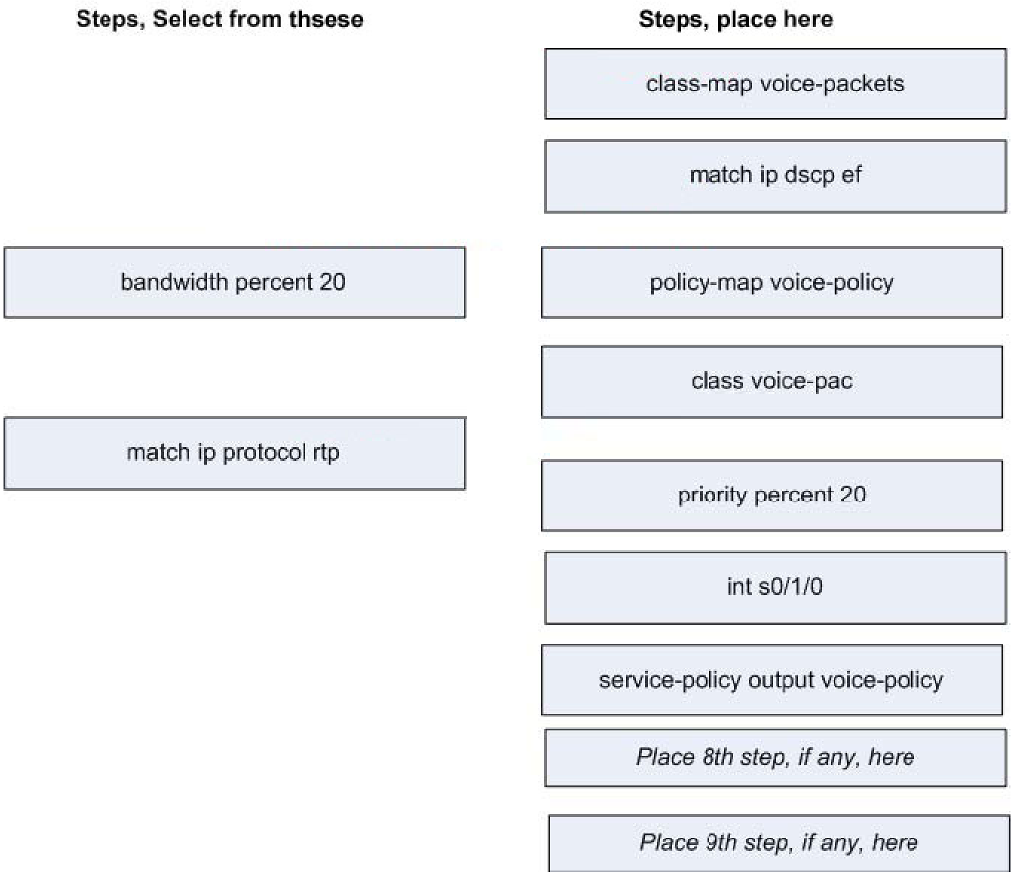
Place 6th step, if any, here

Place 7th step, if any, here

Place 8th step, if any, here

Place 9th step, if any, here

Answer:



Steps, Select from thsese

bandwidth percent 20

match ip protocol rtp

Steps, place here

class-map voice-packets

match ip dscp ef

policy-map voice-policy

class voice-pac

priority percent 20

int s0/1/0

service-policy output voice-policy

Place 8th step, if any, here

Place 9th step, if any, here

Explanation:
Complete the following steps to implement the QoS
Step 1 Configure traffic classification by using the class-map command.
A class map is created using the class-map global configuration command. Class maps are identified by case-sensitive names. Each class map contains one or more conditions that determine whether the packet belongs to the class. There are two ways of processing conditions when there is more than one condition in a
class map:
Match all: All conditions have to be met to bind a packet to the class.
Match any: At least one condition has to be met to bind the packet to the class.
The default match strategy of class maps is match all.
Step 2 Configure traffic policy by associating the traffic class with one or more QoS features using the policy-map command.
The name of a traffic policy is specified in the policy-map command (for example, issuing the policy-map class1 command would create a traffic policy named class1).
After you issue the policy-map command, you enter policy-map configuration mode.
You can then enter the name of a traffic class. Here is where you enter QoS features to apply to the traffic that matches this class.
Step 3 Attach the traffic policy to inbound or outbound traffic on interfaces, subinterfaces, or virtual circuits by using the service-policy command.
Using the service-policy command, you can assign a single policy map to multiple interfaces or assign multiple policy maps to a single interface (a maximum of one in each

direction, inbound and outbound). A service policy can be applied for inbound or outbound packets.

QUESTION 87

You need to determine the best queuing method for use on a new Certkiller router. Which two statements about queuing mechanisms are true? (Select two)

A. FIFO queuing is only appropriate for slower serial interfaces.
B. Only one queuing mechanism type can be applied to an interface.
C. Weighted fair queuing does not require the configuration of access lists to classify traffic.
D. Flow-based weighted fair queuing provides for queues to be serviced in a round-robin fashion.
E. Weighted fair queuing is the default queuing mechanism used for all but slower than E1 rate interfaces.

Answer: B, C

Explanation:
The weighted fair queuing algorithm arranges traffic into conversations, or flows. The sorting of traffic into flows is based on packet header addressing. Common conversation discriminators are as follows:
1. Source/destination network address
2. Source/destination Media Access Control (MAC) address
3. Source/destination port or socket numbers
4. Frame Relay data-link connection identifier (DLCI) value
5. Quality of service/type of service (QoS/ToS) value
The flow-based weighted fair queuing algorithm places packets of the various conversations in the fair queue before transmission. The order of removal from the fair queue is determined by the virtual delivery time of the last bit of each arriving packet. WFQ assigns a weight to each flow, which determines the transmit order for queued packets. In this scheme, lower weights are served first. Small, low-volume packets are given priority over large, high-volume conversation packets.
Weighted fair queuing is configured on a particular interface using the command fair-queue congestive-discard-threshhold. The congestive discard policy applies only to high-volume conversations that have more than one message in the queue. The discard policy tries to control conversations that would monopolize the link. If an individual conversation queue contains more messages than the congestive discard threshold, no new messages will be queued until the number of messages drops below one-fourth of the threshold value.

QUESTION 88

Congestion management is a QoS mechanism for dealing with periodic bursts of congestion. What are the three elements of configuring congestion management? (Select three)

A. FIFO configuration
B. Determining packet drop thresholds
C. Determining the random early detection method
D. Queue scheduling
E. Queue creation
F. Traffic classification

Answer: D, E, F

Explanation:
Congestion-management features control the congestion when it occurs. One way that network elements handle an overflow of arriving traffic is to use a queuing algorithm to sort the traffic and then determine some method of prioritizing it onto an output link. Each queuing algorithm was designed to solve a specific network traffic problem and has a particular effect on network performance. Many algorithms have been designed to serve different needs. A well-designed queuing algorithm provides some bandwidth and delay guarantees to priority traffic.

QUESTION 89
Queuing mechanisms have been put in place to support converged Certkiller network. Which two statements about queuing mechanisms are true? (Select two)

A. When no other queuing strategies are configured, all interfaces except serial interfaces at E1 speed (2.048 Mbps) and below use FIFO by default.
B. Serial interfaces at E1 speed (2.048 Mbps) and below use weighted fair queuing (WFQ) by default.
C. Weighted fair queuing (WFQ) is the simplest of queuing method.
D. An advantage of the round-robin queuing algorithm is its ability to prioritize traffic.
E. Priority queuing (PQ) uses a dynamic configuration and quickly adapts to changing network conditions.
F. Custom queuing (CQ) uses a dynamic configuration and quickly adapts to changing network conditions.

Answer: A, B

Explanation:
WFQ is one of the premier Cisco queuing techniques. It is a flow-based queuing algorithm that does two things simultaneously: It schedules interactive traffic to the front of the queue to reduce response time, and it fairly shares the remaining bandwidth among the various flows to prevent high-volume flows from monopolizing the outgoing interface.
The idea of WFQ is to have a dedicated queue for each flow without starvation, delay, or jitter within the queue. Furthermore, WFQ allows fair and accurate bandwidth allocation among all flows with minimum scheduling delay. WFQ makes use of the IP precedence bits as a weight when allocating bandwidth.
WFQ was introduced as a solution to the problems of the following queuing mechanisms:

1. FIFO queuing causes starvation, delay, and jitter.
2. Priority queuing (PQ) causes starvation of lower-priority classes and suffers from the FIFO problems within each of the four queues that it uses for prioritization.

The WFQ method is used as the default queuing mode on serial interfaces configured to run at or below E1 speeds (2.048 Mbps).

QUESTION 90

You need to ensure that all critical application traffic traverses the Certkiller network in a timely fashion. Which three methods would help prevent critical network-traffic packet loss on high speed interfaces? (Select three)

A. Policy routing
B. CBWFQ
C. WRED
D. LFI
E. Increase link capacity
F. WFQ

Answer: B, C, F

Explanation:

1. Class-based weighted fair queuing (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. By using CBWFQ, network managers can define traffic classes based on several match criteria, including protocols, access control lists (ACLs), and input interfaces. A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class. More than one IP flow, or "conversation", can belong to a class.

Once a class has been defined according to its match criteria, the characteristics can be assigned to the class. To characterize a class, assign the bandwidth and maximum packet limit. The bandwidth assigned to a class is the guaranteed bandwidth given to the class during congestion.

2. Weighted random early detection (WRED) combines RED with IP precedence or DSCP and performs packet dropping based on IP precedence or DSCP markings. As with RED, WRED monitors the average queue length in the router and determines when to begin discarding packets based on the length of the interface queue. When the average queue length exceeds the user-specified minimum threshold, WRED begins to randomly drop packets with a certain probability. If the average length of the queue continues to increase so that it becomes larger than the user-specified maximum threshold, WRED reverts to a tail-drop packet-discard strategy, in which all incoming packets are dropped. The idea behind using WRED is to maintain the queue length at a level somewhere below the maximum threshold and to implement different drop policies for different classes of traffic.

WRED can selectively discard lower-priority traffic when the interface becomes congested and can provide differentiated performance characteristics for different classes of service. WRED can also be configured to produce nonweighted RED behavior.

3. WFQ

When FIFO queuing is in effect, traffic is transmitted in the order received without regard for bandwidth consumption or the associated delays. File transfers and other high-volume network applications often generate series of packets of associated data known as packet trains. Packet trains are groups of packets that tend to move together through the network. These packet trains can consume all available bandwidth, and other traffic flows back up behind them.

Weighted fair queuing overcomes an important limitation of FIFO queuing. Weighted fair queuing is an automated method that provides fair bandwidth allocation to all network traffic. Weighted fair queuing provides traffic priority management that dynamically sorts traffic into conversations, or flows. Weighted fair queuing then breaks up a stream of packets within each conversation to ensure that bandwidth is shared fairly between individual conversations. There are four types of weighted fair queuing: flow-based, distributed, class-based, and distributed class-based.

Weighted fair queuing (WFQ) is a flow-based algorithm that schedules delay-sensitive traffic to the front of a queue to reduce response time, and also shares the remaining bandwidth fairly among high-bandwidth flows. By breaking up packet trains, WFQ assures that low-volume traffic is transferred in a timely fashion. Weighted fair queuing gives low-volume traffic, such as Telnet sessions, priority over high-volume traffic, such as File Transfer Protocol (FTP) sessions. Weighted fair queuing gives concurrent file transfers balanced use of link capacity. Weighted fair queuing automatically adapts to changing network traffic conditions

---

QUESTION 91

LLQ is being used throughout the Certkiller converged network. What is a feature of low latency queuing?

A. LLQ consists of a class-based weighted fair queuing with a priority queue for real-time traffic such as voice
B. LLQ consists of multiple priority queues with FIFO queuing for voice
C. LLQ consists of multiple FIFO priority queues with round-robin queuing for data
D. LLQ consists of a priority queue with multiple weighted fair queues for data
E. LLQ consists of multiple priority queues with weighted round-robin queues for data
F. None of the above

Answer: A

Explanation:

The Low Latency Queuing (LLQ) feature provides strict priority queuing for class-based weighted fair queuing (CBWFQ), reducing jitter in voice conversations. Configured by the priority command, strict priority queuing gives delay-sensitive data, such as voice, preferential treatment over other traffic. With this feature, delay-sensitive data is sent first, before packets in other queues are treated. LLQ is also referred to as priority queuing/class-based weighted fair queuing (PQ/CBWFQ) because it is a combination of the two techniques.

For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth assigned to the class during configuration. Therefore, the bandwidth assigned

to the packets of a class determines the order in which packets are sent. All packets are serviced equally, based on weight. No class of packets may be granted strict priority. This scheme poses problems for voice and video traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission, which manifest as jitter in the conversation.
To enqueue a class of traffic to the strict priority queue, configure the priority command for the class after specifying the class within a policy map. Classes to which the priority command is applied are considered priority classes. Within a policy map, give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is enqueued to the same, single, strict priority queue and they will contend with each other for bandwidth.

QUESTION 92
You want to implement a congestion avoidance mechanism within the Certkiller network. Which QoS tool is used to reduce the level of congestion in the queues by selectively dropping packets?

A. Weighted Random Early Detection (WRED)
B. Low Latency Queuing (LLQ)
C. Class-based Weighted Fair Queuing (CBWFQ)
D. Modified Deficit Round Robin (MDRR)
E. None of the above

Answer: A

Explanation:
Weighted random early detection (WRED) combines RED with IP precedence or DSCP and performs packet dropping based on IP precedence or DSCP markings. As with RED, WRED monitors the average queue length in the router and determines when to begin discarding packets based on the length of the interface queue. When the average queue length exceeds the user-specified minimum threshold, WRED begins to randomly drop packets with a certain probability. If the average length of the queue continues to increase so that it becomes larger than the user-specified maximum threshold, WRED reverts to a tail-drop packet-discard strategy, in which all incoming packets are dropped. The idea behind using WRED is to maintain the queue length at a level somewhere below the maximum threshold and to implement different drop policies for different classes of traffic.
WRED can selectively discard lower-priority traffic when the interface becomes congested and can provide differentiated performance characteristics for different classes of service. WRED can also be configured to produce nonweighted RED behavior.

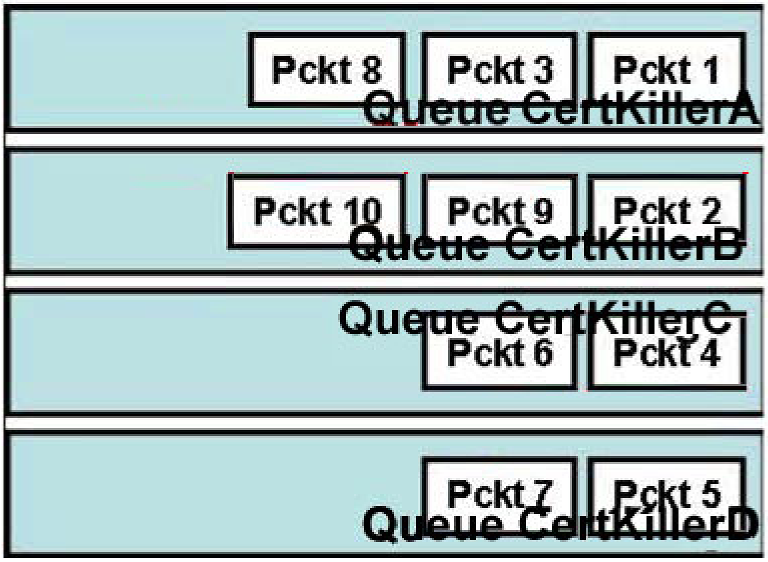
QUESTION 93
Interface congestion on a Certkiller link is causing drops in voice (UDP) and TCP packets. The drops result in jerky speech quality and slower FTP traffic flows.
Which two technologies would proactively address the TCP transfer rate and the voice problems in this network? (Select two)

A. CBWFQ
B. WRED
C. Traffic shaping
D. LLQ

Answer: B, D

Explanation:
1. Weighted random early detection (WRED) combines RED with IP precedence or DSCP and performs packet dropping based on IP precedence or DSCP markings. As with RED, WRED monitors the average queue length in the router and determines when to begin discarding packets based on the length of the interface queue. When the average queue length exceeds the user-specified minimum threshold, WRED begins to randomly drop packets with a certain probability. If the average length of the queue continues to increase so that it becomes larger than the user-specified maximum threshold, WRED reverts to a tail-drop packet-discard strategy, in which all incoming packets are dropped. The idea behind using WRED is to maintain the queue length at a level somewhere below the maximum threshold and to implement different drop policies for different classes of traffic.
WRED can selectively discard lower-priority traffic when the interface becomes congested and can provide differentiated performance characteristics for different classes of service. WRED can also be configured to produce nonweighted RED behavior.
2. The Low Latency Queuing (LLQ) feature provides strict priority queuing for class-based weighted fair queuing (CBWFQ), reducing jitter in voice conversations. Configured by the priority command, strict priority queuing gives delay-sensitive data, such as voice, preferential treatment over other traffic. With this feature, delay-sensitive data is sent first, before packets in other queues are treated. LLQ is also referred to as priority queuing/class-based weighted fair queuing (PQ/CBWFQ) because it is a combination of the two techniques.
For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth assigned to the class during configuration. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced equally, based on weight. No class of packets may be granted strict priority. This scheme poses problems for voice and video traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission, which manifest as jitter in the conversation.
To enqueue a class of traffic to the strict priority queue, configure the priority command for the class after specifying the class within a policy map. Classes to which the priority command is applied are considered priority classes. Within a policy map, give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is enqueued to the same, single, strict priority queue and they will contend with each other for bandwidth.

QUESTION 94
Four distinct packet queues in a Certkiller router are displayed below:

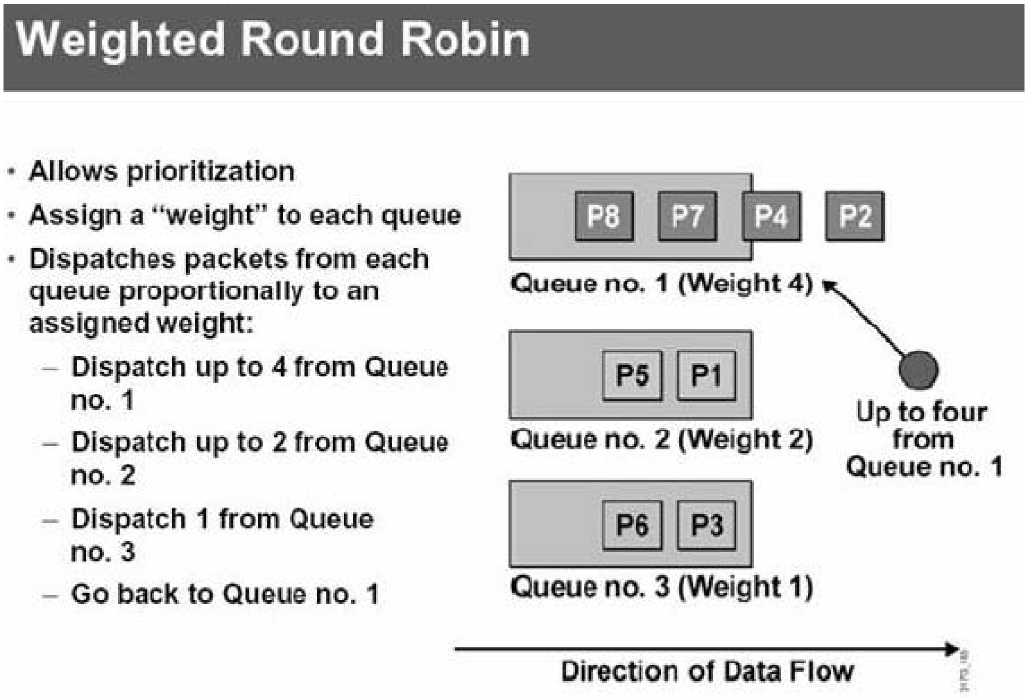


Study the exhibit carefully. Packet-based WRR (not byte-count WRR) is being used to control the output on an interface with four queues (A, B, C, D) configured. Each queue has an assigned weight of A=4, B=2, C=1, and D=1. If the queuing algorithm begins with Queue A and with packets placed into the four queues as shown in the exhibit, in which order will packets be selected from the queues for transmission?

A. 1, 3, 8, 2, 9, 4, 5, 10, 6, 7
B. 1, 2, 4, 5, 3, 9, 6, 7, 8 10
C. 1, 3, 8, 2, 4, 5, 9, 6, 7, 10
D. 1, 3, 8, 2, 9, 10, 4, 6, 5, 7
E. 1, 3, 2, 9, 4, 6, 5, 7, 8, 10
F. None of the above

Answer: A

Explanation:
In WRR, packets are accessed round-robin style, but queues can be given priorities called "weights." For example, in a single round, four packets from a high-priority class might be dispatched, followed by two from a middle-priority class, and then one from a low-priority class.



Weighted Round Robin

- Allows prioritization
- Assign a "weight" to each queue
- Dispatches packets from each queue proportionally to an assigned weight:
  - Dispatch up to 4 from Queue no. 1
  - Dispatch up to 2 from Queue no. 2
  - Dispatch 1 from Queue no. 3
  - Go back to Queue no. 1

Some implementations of the WRR algorithm provide prioritization by dispatching a configurable number of bytes each round rather than a number of packets. The Cisco custom queuing (CQ) mechanism is an example of this implementation.

QUESTION 95

Weighted random early detection (WRED) has been configured on a Certkiller router. Out of every 512 packets, how many packets will be dropped if the mark probability denominator has been configured with a value of 512?

A. 4
B. 2
C. 1
D. 8
E. 512
F. None of the above

Answer: C

Explanation:

The idea behind using WRED is to maintain the queue length at a level somewhere below the maximum threshold and to implement different drop policies for different classes of traffic. WRED can selectively discard lower-priority traffic when the interface becomes congested and can provide differentiated performance characteristics for different classes of service. WRED can also be configured to produce nonweighted RED behavior. For interfaces configured to use Resource Reservation Protocol (RSVP), WRED chooses packets from other flows to drop rather than the RSVP flows. Also, IP precedence or DSCP helps determine which packets are dropped, because traffic at a lower priority has

a higher drop rate than traffic at a higher priority (and, therefore, lower-priority traffic is more likely to be throttled back). In addition, WRED statistically drops more packets from large users than from small users. The traffic sources that generate the most traffic are more likely to be slowed down than traffic sources that generate little traffic.
WRED reduces the chances of tail drop by selectively dropping packets when the output interface begins to show signs of congestion. By dropping some packets early rather than waiting until the queue is full, WRED avoids dropping large numbers of packets at once and minimizes the chances of global synchronization. As a result, WRED helps maximize the utilization of transmission lines.

QUESTION 96
A portion of the configuration for router CK1 is displayed below:

```
Class-map match-any GOLD
match ip precedence ef
class-map match-any SILVER
Match ip dscp af31
Policy-map Branch
Class GOLD
Priority percent 20
Class SILVER
bandwidth percent 15
random-detect dscp-based
interface Serial0/1
description PPP link to BRANCH
bandwidth 1536
ip address 10.200.40.1 255.255.255.252
encapsulation ppp
```

This configuration has been used to prioritize voice traffic on the Certkiller network. After issuing several show commands, the administrator realizes the configuration is not working. What could be the problem?

A. Voice traffic should be mapped to a different DSCP value.
B. WRED is not configured for the voice traffic.
C. The policy map needs to be mapped to an interface.
D. The given LLQ configuration is not designed for voice traffic.
E. Custom queuing should be used on converged voice and data networks.
F. None of the above

Answer: C

Explanation:
Similar to access lists, policy maps must be mapped to an interface. Although the policy map portion of the configuration for prioritizing traffic is complete, the router needs to be informed which interface this policy needs to be applied to. To do this, Use the service-policy interface configuration command to attach a traffic policy to an interface and to specify the direction in which the policy should be applied (either on packets

coming into the interface or packets leaving the interface). In this example, this would be done with the "service-policy input Branch" or "service-policy output Branch" command.

QUESTION 97
You want to limit the amount of throughput on one of the Certkiller WAN links.
Which QoS mechanism will control the maximum rate of traffic that is sent or received on an interface?

A. Class-based shaping
B. LFI
C. Traffic shaping
D. Traffic policing
E. None of the above

Answer: D

Explanation:
Traffic policing drops excess traffic to control traffic flow within specified rate limits. Traffic policing does not introduce any delay to traffic that conforms to traffic policies. Traffic policing can cause more TCP retransmissions, because traffic in excess of specified limits is dropped. Traffic-policing mechanisms such as class-based policing or committed access rate (CAR) also have marking capabilities in addition to rate-limiting capabilities. Instead of dropping the excess traffic, traffic policing can mark and then send the excess traffic. This feature allows the excess traffic to be re-marked with a lower priority before the excess traffic is sent.

QUESTION 98
Traffic shaping has been enabled on a Certkiller frame relay router. Of the choices below, which Cisco IOS traffic-shaping mechanism statement is true?

A. Class-based policing is configured using the Modular QoS command-line (MQC) interface.
B. Both Frame Relay traffic shaping (FRTS) and virtual IP (VIP)-based Distributed Traffic Shaping (DTS) have the ability to mark traffic.
C. Distributed Traffic Shaping (DTS) is configured with the police command under the policy map configuration.
D. Only the Frame Relay traffic-shaping (FRTS) mechanism can interact with a Frame Relay network, adapting to indications of Layer 2 congestion in the WAN links.
E. None of the above.

Answer: A

Explanation:
Traffic shaping is an attempt to control traffic in ATM, Frame Relay, or Metro Ethernet networks to optimize or guarantee performance, low latency, or bandwidth. Traffic shaping deals with concepts of classification, queue disciplines, enforcing policies,

congestion management, quality of service (QoS), and fairness.
Traffic shaping provides a mechanism to control the volume of traffic being sent into a network (bandwidth throttling) by not allowing the traffic to burst above the subscribed (committed) rate. For this reason, traffic-shaping schemes need to be implemented at the network edges like ATM, Frame Relay, or Metro Ethernet to control the traffic entering the network. It also may be necessary to identify traffic with a granularity that allows the traffic-shaping control mechanism to separate traffic into individual flows and shape them differently.
Class-based policing is also available on some Cisco Catalyst switches. Class-based policing supports a single or dual token bucket. Class-based policing also supports single-rate or dual-rate metering and multiaction policing. Multiaction policing allows more than one action to be applied; for example, marking the Frame Relay DE bit and also the DSCP value before sending the exceeding traffic. Class-based policing is configured using the Cisco Modular QoS CLI (MQC), using the police command under the policy map configuration.

QUESTION 99
You need to consider the advantages and disadvantages of using traffic shaping versus traffic policing within your network. Which statement about traffic policing and which statement about traffic shaping are true? (Select two)

A. Traffic policing drops excess traffic in order to control traffic flow within specified rate limits.
B. Traffic shaping buffers excess traffic so that the traffic stays within the desired rate.
C. Traffic policing can cause UDP retransmissions when traffic in excess of specified limits is dropped.
D. A need for traffic shaping occurs when a service provider must rate-limit the customer traffic to T1 speed on an OC-3 connection.
E. Traffic policing and traffic conditioning are mechanisms that are used in an edge network to guarantee QoS.

Answer: A, B

Explanation:
Policing can be applied to either the inbound or outbound direction, while shaping can be applied only in the outbound direction. Policing drops nonconforming traffic instead of queuing the traffic like shaping. Policing also supports marking of traffic. Traffic policing is more efficient in terms of memory utilization than traffic shaping because no additional queuing of packets is needed.
Both traffic policing and shaping ensure that traffic does not exceed a bandwidth limit, but each mechanism has different impacts on the traffic:
Policing drops packets more often, generally causing more retransmissions of connection-oriented protocols, such as TCP.
Shaping adds variable delay to traffic, possibly causing jitter. Shaping queues excess traffic by holding packets in a shaping queue. Traffic shaping is used to shape the outbound traffic flow when the outbound traffic rate is higher than a configured rate.

Traffic shaping smoothes traffic by storing traffic above the configured rate in a shaping queue. Therefore, shaping increases buffer utilization on a router and causes unpredictable packet delays. Traffic shaping can also interact with a Frame Relay network, adapting to indications of Layer 2 congestion in the WAN. For example, if the backward explicit congestion notification (BECN) bit is received, the router can lower the rate limit to help reduce congestion in the Frame Relay network.

QUESTION 100
Traffic policing has been implemented on router CK1 using CAR. In a network where traffic policing is implemented, what happens when a packet enters the router and exceeds the set parameters?

A. Traffic is dropped or sent with an increased priority.
B. Traffic is sent with a bit set for discard-eligible.
C. Traffic is dropped or sent with the priority unchanged.
D. Traffic is dropped or sent with a different priority.
E. None of the above.

Answer: D

Explanation:
Traffic policing drops excess traffic to control traffic flow within specified rate limits. Traffic policing does not introduce any delay to traffic that conforms to traffic policies. Traffic policing can cause more TCP retransmissions, because traffic in excess of specified limits is dropped. Traffic-policing mechanisms such as class-based policing or committed access rate (CAR) also have marking capabilities in addition to rate-limiting capabilities. Instead of dropping the excess traffic, traffic policing can mark and then send the excess traffic. This feature allows the excess traffic to be re-marked with a lower priority before the excess traffic is sent out.

QUESTION 101
You need to consider the pros and cons of using traffic shaping and traffic policing within your network. Which statement about traffic policing and which statement about traffic shaping are true? (Select two)

A. Traffic shaping can be applied only in the outbound direction.
B. Traffic shaping can be applied only in the inbound direction.
C. Traffic shaping can be applied in both the inbound and outbound direction.
D. Traffic policing can be applied in both the inbound and outbound direction.
E. Traffic policing can be applied only in the inbound direction.
F. Traffic policing can be applied only in the outbound direction.

Answer: A, D

Explanation:
Policing can be applied to either the inbound or outbound direction, while shaping can be

applied only in the outbound direction. Policing drops nonconforming traffic instead of queuing the traffic like shaping. Policing also supports marking of traffic. Traffic policing is more efficient in terms of memory utilization than traffic shaping because no additional queuing of packets is needed.
Both traffic policing and shaping ensure that traffic does not exceed a bandwidth limit, but each mechanism has different impacts on the traffic:
Policing drops packets more often, generally causing more retransmissions of connection-oriented protocols, such as TCP.
Shaping adds variable delay to traffic, possibly causing jitter. Shaping queues excess traffic by holding packets in a shaping queue. Traffic shaping is used to shape the outbound traffic flow when the outbound traffic rate is higher than a configured rate. Traffic shaping smoothes traffic by storing traffic above the configured rate in a shaping queue. Therefore, shaping increases buffer utilization on a router and causes unpredictable packet delays. Traffic shaping can also interact with a Frame Relay network, adapting to indications of Layer 2 congestion in the WAN. For example, if the backward explicit congestion notification (BECN) bit is received, the router can lower the rate limit to help reduce congestion in the Frame Relay network.

QUESTION 102
You need to consider the advantages and disadvantages of using traffic shaping and policing within your network. Which two statements are true about traffic shaping and traffic policing? (Select two)

A. Traffic shaping queues excess traffic whereas traffic policing discards excess traffic.
B. Both traffic shaping and traffic policing cause retransmissions of connection-oriented protocols such as TCP.
C. Both traffic shaping and traffic policing support the marking and re-marking of traffic.
D. The effects of traffic shaping and traffic policing when configured on a router are applied to outgoing traffic.
E. Traffic shaping allows the traffic to exceed the bit rate whereas traffic policing prevents the traffic from exceeding the bit rate.

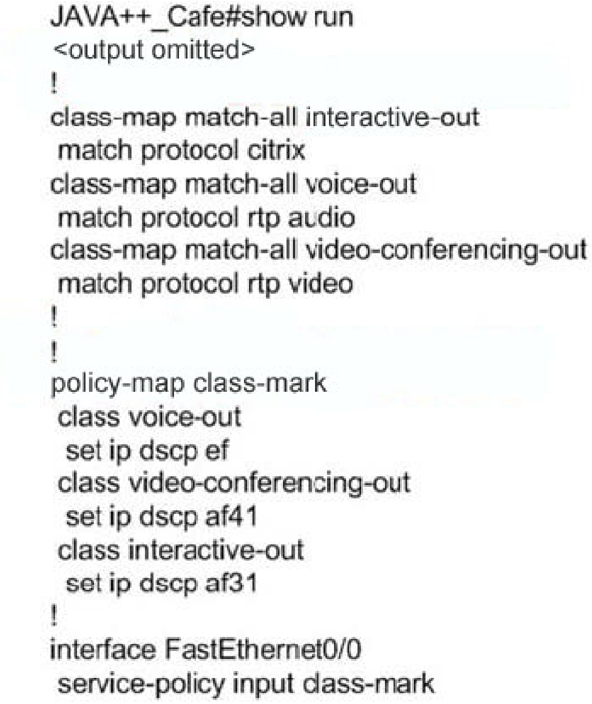
Answer: A, D

Explanation:
Policing can be applied to either the inbound or outbound direction, while shaping can be applied only in the outbound direction. Policing drops nonconforming traffic instead of queuing the traffic like shaping. Policing also supports marking of traffic. Traffic policing is more efficient in terms of memory utilization than traffic shaping because no additional queuing of packets is needed.
Both traffic policing and shaping ensure that traffic does not exceed a bandwidth limit, but each mechanism has different impacts on the traffic:
Policing drops packets more often, generally causing more retransmissions of connection-oriented protocols, such as TCP.
Shaping adds variable delay to traffic, possibly causing jitter. Shaping queues excess traffic by holding packets in a shaping queue. Traffic shaping is used to shape the

outbound traffic flow when the outbound traffic rate is higher than a configured rate. Traffic shaping smoothes traffic by storing traffic above the configured rate in a shaping queue. Therefore, shaping increases buffer utilization on a router and causes unpredictable packet delays. Traffic shaping can also interact with a Frame Relay network, adapting to indications of Layer 2 congestion in the WAN. For example, if the backward explicit congestion notification (BECN) bit is received, the router can lower the rate limit to help reduce congestion in the Frame Relay network.

QUESTION 103

Exhibit:



```
JAVA++_Cafe#show run
<output omitted>
!
class-map match-all interactive-out
 match protocol citrix
class-map match-all voice-out
 match protocol rtp audio
class-map match-all video-conferencing-out
 match protocol rtp video
!
!
policy-map class-mark
 class voice-out
  set ip dscp ef
 class video-conferencing-out
  set ip dscp af41
 class interactive-out
  set ip dscp af31
!
interface FastEthernet0/0
 service-policy input class-mark
```

Study the exhibit carefully. What does the configuration accomplish?

A. Creates a stateless mechanism to identify a group of peer-to-peer file-sharing applications
B. Creates a stateful mechanism to identify a group of peer-to-peer file-sharing applications
C. Enables a PDLM that contains the rules that are used by NBAR to recognize Layer 4 through Layer 7 applications and protocols
D. Configures a traffic class and policy for inbound voice and video traffic
E. Uses the NBAR protocol discovery feature via an SNMP MIB to analyze application traffic patterns in real time
F. None of the above

Answer: D

Explanation:
There are three steps of implementing QOS:

Step 1 Configure traffic classification by using the class-map command.
Step 2 Configure traffic policy by associating the traffic class with one or more QoS features using the policy-map command.
Step 3 Attach the traffic policy to inbound or outbound traffic on interfaces, subinterfaces, or virtual circuits by using the service-policy command.

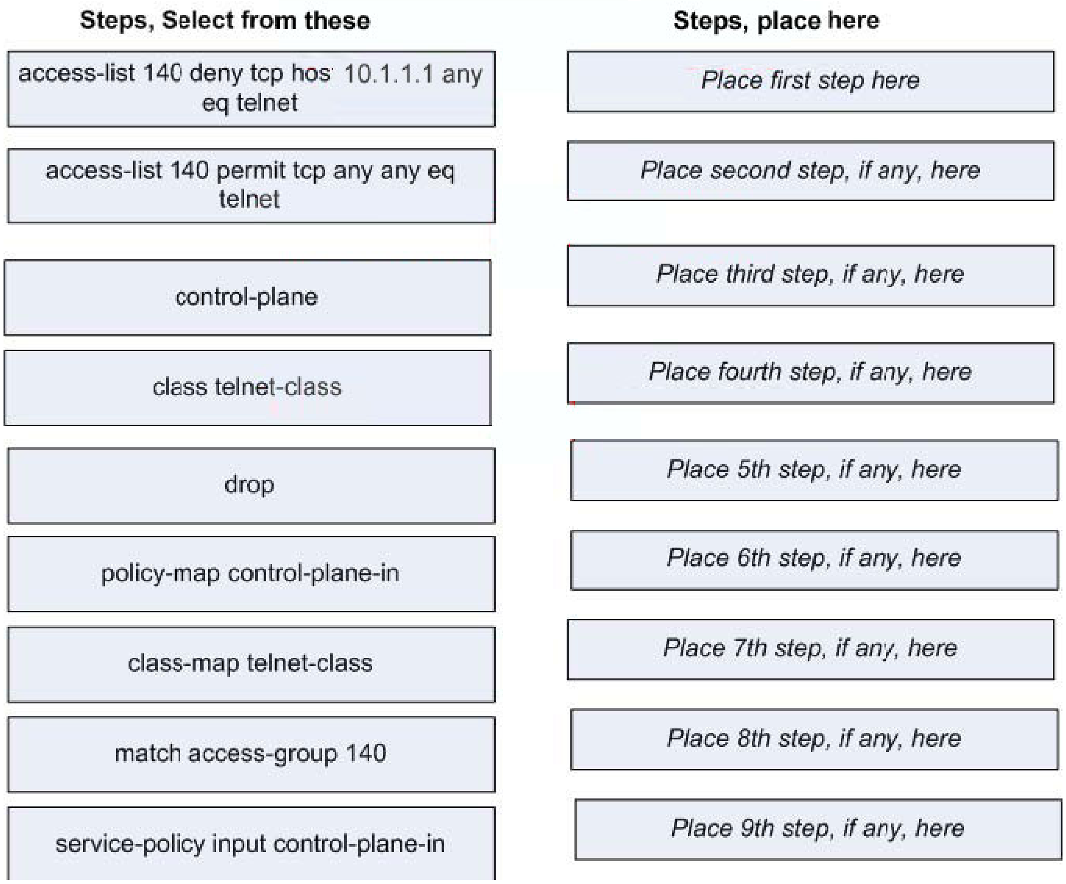
QUESTION 104
Control plane policing is being used on the Certkiller Internet router. What are three facts of control plane policing? (Select three)

A. It provides the control plane with a separate token bucket
B. It is a set of rules that can be established and associated with the ingress and egress ports of the control plane
C. It treats the control plane as a separate entity with its own ingress (input) and egress (output) ports
D. It enhances security of the control plane by tunneling packets to and from the control plane
E. It protects the control plane on a router from DoS attacks
F. It improves performance of the control plane by marking control plane packets with DSCP EF

Answer: B, C, E

Explanation:
The CoPP (Control Panel Policing) feature allows users to configure a QoS filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and DoS attacks. In this way, the control plane can help maintain packet forwarding and protocol states despite an attack or a heavy traffic load on the router or switch.
By protecting the Route Processor, CoPP helps ensure router and network stability during an attack. For this reason, a best-practice recommendation is to deploy CoPP as a key protection mechanism.

QUESTION 105
DRAG DROP
To configure Control Plan Policing (CoPP) to deny Telnet access only from the IP address 10.1.1.1, drag the commands on the left to the boxes on the right and place the commands in the proper order.



Steps, Select from these

access-list 140 deny tcp hos 10.1.1.1 any eq telnet

access-list 140 permit tcp any any eq telnet

control-plane

class telnet-class

drop

policy-map control-plane-in

class-map telnet-class

match access-group 140

service-policy input control-plane-in

Steps, place here

Place first step here

Place second step, if any, here

Place third step, if any, here

Place fourth step, if any, here

Place 5th step, if any, here

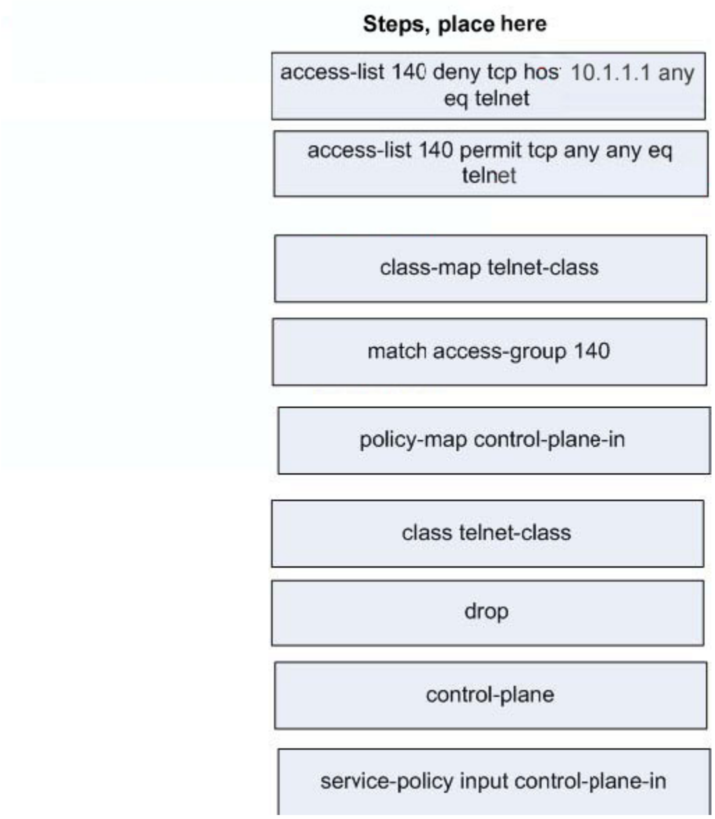
Place 6th step, if any, here

Place 7th step, if any, here

Place 8th step, if any, here

Place 9th step, if any, here

Answer:



Steps, place here

access-list 140 deny tcp host 10.1.1.1 any eq telnet

access-list 140 permit tcp any any eq telnet

class-map telnet-class

match access-group 140

policy-map control-plane-in

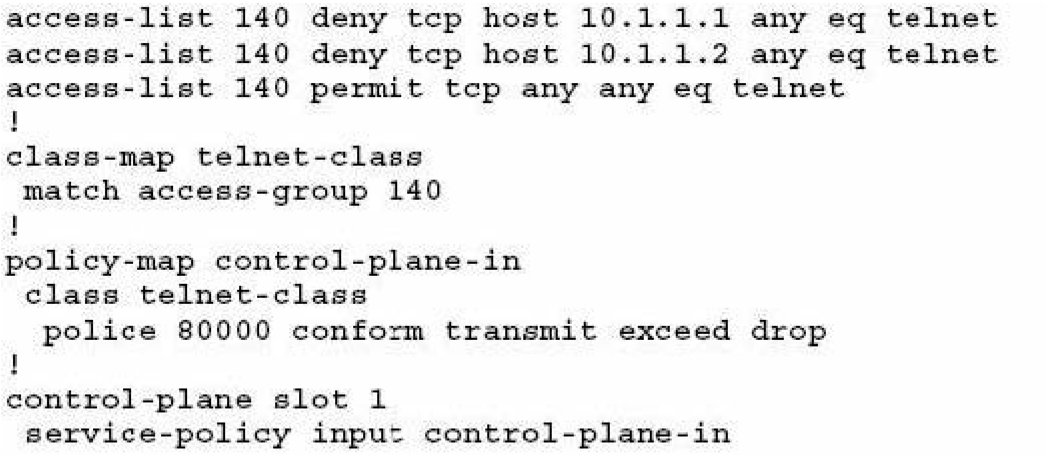
class telnet-class

drop

control-plane

service-policy input control-plane-in

Explanation:
The CoPP (Control Panel Policing) feature allows users to configure a QoS filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and DoS attacks. In this way, the control plane can help maintain packet forwarding and protocol states despite an attack or a heavy traffic load on the router or switch.
By protecting the Route Processor, CoPP helps ensure router and network stability during an attack. For this reason, a best-practice recommendation is to deploy CoPP as a key protection mechanism.
There are four steps required to configure CoPP:
Step1 Define a packet classification criteria.
Step 2 Define a service policy.
Step 3 Enter control-plane configuration mode.
Step 4 Apply QoS policy.
Example:



```
access-list 140 deny tcp host 10.1.1.1 any eq telnet
access-list 140 deny tcp host 10.1.1.2 any eq telnet
access-list 140 permit tcp any any eq telnet
!
class-map telnet-class
 match access-group 140
!
policy-map control-plane-in
 class telnet-class
  police 80000 conform transmit exceed drop
!
control-plane slot 1
 service-policy input control-plane-in
```

The example shows how to configure rate limiting (on input) for distributed control plane traffic. QoS policy is applied to the data plane to perform distributed control plane services on packets destined for the control plane from the interfaces on the line card in slot 1. Trusted hosts are configured with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets that enter through slot 1 to be policed at the specified rate. The MQC is used to match the traffic, limit the traffic, and apply the policy to the control plane (on input) in slot 1 at the end.

QUESTION 106

CoPP is being used as an additional layer of security within the Certkiller network. Which two Cisco router functional planes are protected by Control Plane Policing (CoPP)? (Select two)

A. Control plane
B. Service plane
C. Data plane
D. Hyper plane
E. Management plane
F. User Plane

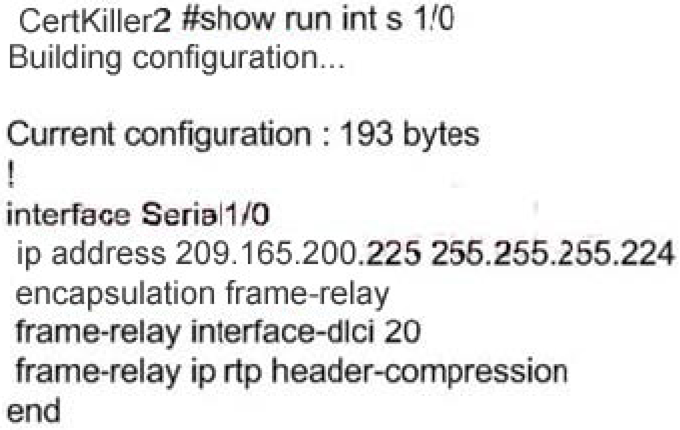
Answer: D, E

Explanation:
CoPP protects the control/management plane, not the data plane.
Because the Route Processor is critical to network operations, any service disruption to the Route Processor or the control and management planes can result in business-impacting network outages. A DoS attack targeting the Route Processor, which can be perpetrated either inadvertently or maliciously, typically involves high rates of punted traffic that result in excessive CPU utilization on the Route Processor itself. This type of attack, which can be devastating to network stability and availability, may display the following symptoms:

1. High Route Processor CPU utilization (near 100 percent).
2. Loss of line protocol keepalives and routing protocol updates, leading to route flaps

and major network transitions.
3. Slow or completely unresponsive interactive sessions via the command-line interface (CLI) due to high CPU utilization
4. Route Processor resource exhaustion, such as memory and buffers that are unavailable for legitimate IP data packets
5. Packet queue backup, which leads to indiscriminate drops (or drops due to lack of buffer resources) of other incoming packets
CoPP addresses the need to protect the control and management planes, ensuring routing stability, availability, and packet delivery. It uses the dedicated control-plane configuration command via the Cisco Modular QoS CLI (MQC) to provide filtering and rate-limiting capabilities for control plane packets.

QUESTION 107
A Certkiller router is configured as shown below:



```
 CertKiller2 #show run int s 1/0
Building configuration...

Current configuration : 193 bytes
!
interface Serial1/0
 ip address 209.165.200.225 255.255.255.224
 encapsulation frame-relay
 frame-relay interface-dlci 20
 frame-relay ip rtp header-compression
end
```

Study the exhibit shown above carefully. What is this configuration an example of?

A. Enabling distributed compressed Real-Time Transport Protocol
B. Enabling Real-Time Transport Protocol (RTP) header compression
C. Enabling latency and jitter reduction for Real-Time Transport Protocol traffic
D. Enabling modular QoS over Frame Relay
E. Enabling TCP header compression
F. None of the above

Answer: B

Explanation:
To reduce the huge bandwidth overhead caused by the IP, UDP, and RTP headers, RTP header compression (cRTP) can be used. The name is a bit misleading because cRTP not only compresses the RTP header, but it also compresses the IP and UDP headers.
cRTP is configured on a link-by-link basis. There is no problem in using cRTP on just some links within your IP network. In any case-even if cRTP is configured on all links in the path-a router that receives cRTP packets on one interface and routes them out another interface that is also configured for cRTP has to decompress the packet at the first interface and then compress it again at the second interface.
cRTP compresses the IP, UDP, and RTP headers from 40 bytes to 2 bytes if the UDP

checksum is not conserved (which is the default on Cisco devices) and to 4 bytes if the UDP checksum is also transmitted. cRTP is especially beneficial when the RTP payload size is small; for example, with compressed audio payloads between 20 and 50 bytes.

QUESTION 108
Compressed RTP has been enabled on the Certkiller network to make the WAN links more efficient. Which header or set of headers does cRTP compress?

A. Layer 2 and Layer 3
B. Layer 2
C. Layer 3 and Layer 4
D. Layer 4
E. Layer 3
F. None of the above

Answer: C

Explanation:
To reduce the huge bandwidth overhead caused by the IP, UDP, and RTP headers, RTP header compression (cRTP) can be used. The name is a bit misleading because cRTP not only compresses the RTP header, but it also compresses the IP and UDP headers.
cRTP is configured on a link-by-link basis. There is no problem in using cRTP on just some links within your IP network. In any case-even if cRTP is configured on all links in the path-a router that receives cRTP packets on one interface and routes them out another interface that is also configured for cRTP has to decompress the packet at the first interface and then compress it again at the second interface.
cRTP compresses the IP, UDP, and RTP headers from 40 bytes to 2 bytes if the UDP checksum is not conserved (which is the default on Cisco devices) and to 4 bytes if the UDP checksum is also transmitted. cRTP is especially beneficial when the RTP payload size is small; for example, with compressed audio payloads between 20 and 50 bytes.
cRTP works on the premise that most of the fields in the IP, UDP, and RTP headers do not change or that the change is predictable. Static fields include source and destination IP address, source and destination UDP port numbers, and many other fields in all three headers.

QUESTION 109
RTP header compression has been enabled on a Certkiller VOIP router. Which kinds of traffic are compressed when RTP header compression is enabled for the voice traffic?

A. IP, UDP, RTP, and data-link headers
B. IP and TCP headers
C. Data-link, IP, and TCP headers
D. IP, UDP, and RTP headers
E. Data-link header and trailer only
F. None of the above

Answer: D

Explanation:
To reduce the huge bandwidth overhead caused by the IP, UDP, and RTP headers, RTP header compression (cRTP) can be used. The name is a bit misleading because cRTP not only compresses the RTP header, but it also compresses the IP and UDP headers.
cRTP is configured on a link-by-link basis. There is no problem in using cRTP on just some links within your IP network. In any case-even if cRTP is configured on all links in the path-a router that receives cRTP packets on one interface and routes them out another interface that is also configured for cRTP has to decompress the packet at the first interface and then compress it again at the second interface.
cRTP compresses the IP, UDP, and RTP headers from 40 bytes to 2 bytes if the UDP checksum is not conserved (which is the default on Cisco devices) and to 4 bytes if the UDP checksum is also transmitted. cRTP is especially beneficial when the RTP payload size is small; for example, with compressed audio payloads between 20 and 50 bytes.
cRTP works on the premise that most of the fields in the IP, UDP, and RTP headers do not change or that the change is predictable. Static fields include source and destination IP address, source and destination UDP port numbers, and many other fields in all three headers.

QUESTION 110
On router CK1 , the "ip rtp header-compression" command was enabled. Which statement is true about this interface command when used on both sides of a Frame Relay point-to-point link?

A. The configuration will provide header compression for voice traffic.
B. The configuration will provide header compression for G.729 voice traffic only.
C. The configuration will provide header compression for both voice and TCP traffic.
D. The configuration can be applied only when the voice and TCP packets are relatively small.
E. None of the above.

Answer: A

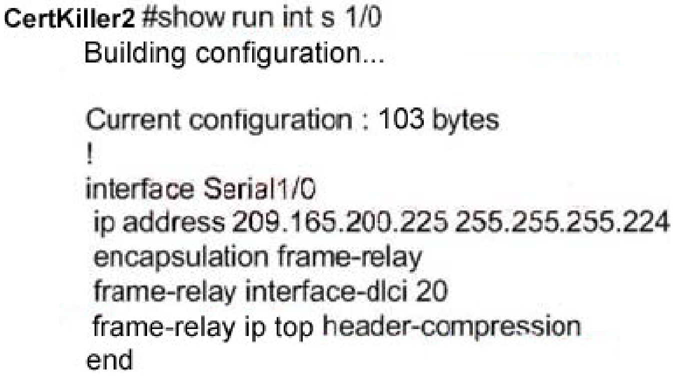
Explanation:
To reduce the huge bandwidth overhead caused by the IP, UDP, and RTP headers, RTP header compression (cRTP) can be used. The name is a bit misleading because cRTP not only compresses the RTP header, but it also compresses the IP and UDP headers.
cRTP is configured on a link-by-link basis. There is no problem in using cRTP on just some links within your IP network. In any case-even if cRTP is configured on all links in the path-a router that receives cRTP packets on one interface and routes them out another interface that is also configured for cRTP has to decompress the packet at the first interface and then compress it again at the second interface.
cRTP compresses the IP, UDP, and RTP headers from 40 bytes to 2 bytes if the UDP checksum is not conserved (which is the default on Cisco devices) and to 4 bytes if the

UDP checksum is also transmitted. cRTP is especially beneficial when the RTP payload size is small; for example, with compressed audio payloads between 20 and 50 bytes. cRTP works on the premise that most of the fields in the IP, UDP, and RTP headers do not change or that the change is predictable. Static fields include source and destination IP address, source and destination UDP port numbers, and many other fields in all three headers.

Use the ip rtp header-compression command to enable Routing Table Protocol (RTP) header compression for serial encapsulations, HDLC, or PPP. If the passive keyword is included, the software compresses outgoing RTP packets only if incoming RTP packets on the same interface are compressed. If the command is used without the passive keyword, the software compresses all RTP traffic.

QUESTION 111

The following output was shown on a Certkiller router:



```
CertKiller2 #show run int s 1/0
        Building configuration...

        Current configuration : 103 bytes
        !
        interface Serial1/0
         ip address 209.165.200.225 255.255.255.224
         encapsulation frame-relay
         frame-relay interface-dlci 20
         frame-relay ip top header-compression
        end
```

Based on the configuration file shown above, what is this an example of?

A. Enabling latency and jitter reduction for Transmission Control traffic
B. Enabling enhanced TCP header compression
C. Enabling distributed compressed Transmission Control Protocol
D. Enabling Real-Time Transport Protocol (RTP) header compression
E. Enabling TCP header compression
F. Enabling modular QoS over Frame Relay
G. None of the above

Answer: E

Explanation:

Compression increases the amount of data that can be sent through a transmission resource. Payload compression is primarily performed on Layer 2 frames and therefore compresses the entire Layer 3 packet. The Layer 2 payload compression methods include these:

* Stacker
* Predictor
* Microsoft Point-to-Point Compression (MPPC)

These algorithms differ vastly in their compression efficiency and in their use of router

resources.
Compression methods are based on eliminating redundancy. The protocol header is an item of repeated data. The protocol header information in each packet in the same flow does not change much over the lifetime of that flow. Using header-compression mechanisms, most header information can be sent only at the beginning of the session, stored in a dictionary, and then referenced in later packets by a short dictionary index.
The header-compression methods include:
* TCP
* Real-Time Transport Protocol (RTP)
* Class-based TCP
* Class-based RTP
TCP/IP header compression subscribes to the Van Jacobson Algorithm defined in RFC 1144. TCP/IP header compression lowers the overhead generated by the disproportionately large TCP/IP headers as they are transmitted across the WAN. TCP/IP header compression is protocol-specific and only compresses the TCP/IP header. The Layer 2 header is still intact and a packet with a compressed TCP/IP header can still travel across a WAN link.
TCP/IP header compression is beneficial on small packets with few bytes of data such as Telnet. Cisco's header compression supports Frame Relay and dial-on-demand WAN link protocols. Because of processing overhead, header compression is generally used at lower speeds, such as 64 kbps links.
Use the ip tcp header-compression command to enable TCP/IP header compression. The passive keyword compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If passive is not specified, the router will compress all traffic.

QUESTION 112
Voice activity detection (VAD) suppresses the transmission of silence patterns which can mean more bandwidth will become available over a given link. On average, and assuming that a link carries at least 24 calls, what percentage of total bandwidth could VAD save?

A. 15
B. 45
C. 55
D. 5
E. 35
F. 25
G. None of the above

Answer: E

Explanation:
In a circuit-switched telephony network, because of the nature of the network, the bandwidth of a call is permanently available and dedicated to that call. There is no way to take advantage of speech pauses, one-way audio transmission, or similar instances when

a link is not being utilized. In a packet network, however, VAD can take advantage of the fact that one-third of the average voice call consists of silence. VAD detects silence, for instance, caused by speech pauses or by one-way audio transmission while a caller is listening to music on hold (MoH) when being transferred. VAD suppresses the transmission of silence and, therefore, saves bandwidth. The amount of bandwidth that can be saved by VAD depends on several factors:
1. Type of audio: During a human conversation, the two parties do not generally talk at the same time. When MoH is played, the call usually turns into a one-way call. Because of the constantly playing music, no bandwidth can be saved in this direction of the call. However, the caller listening to the music does not send any audio and no packets have to be transmitted while the call is on hold.
2. Level of background noise: VAD needs to detect silence to be able to perform silence suppression. If the background noise is too high, VAD cannot detect silence and continues the transmission.
3. Others: Differences in the language and character of speakers have an impact to the amount of silence in a call. Some calls, such as conferences or broadcasts where only one or a few participants are speaking and most of the participants are listening, allow higher bandwidth savings than other calls.
On average, the use of VAD can save about 35 percent of bandwidth. Because of the factors mentioned, there is considerable deviation per individual call. Therefore, the average of 35 percent assumes a certain statistical distribution of call types, which is usually achieved only if a link carries at least 24 calls. If you are calculating bandwidth for fewer calls, you should not take VAD into account.

QUESTION 113
LFI has been configured on the serial interface of router CK1 . What is link fragmentation and interleaving (LFI)?

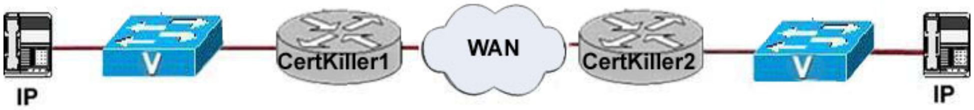
A. LFI is a Layer 2 technique in which smaller fragments are combined into large, equal-sized frames, and transmitted over the link in an interleaved fashion.
B. LFI is a Layer 2 technique in which large frames are broken into small, equal-sized fragments, and transmitted over the link in an interleaved fashion.
C. LFI is a Layer 2 technique in which header information is sent only at the beginning of the session, stored in a dictionary, and then referenced in later packets by a short dictionary index.
D. LFI is a Layer 3 technique in which header information is sent only at the beginning of the session, stored in a dictionary, and then referenced in later packets by a short dictionary index.
E. LFI is a QoS mechanism that allots bandwidth and enables the differentiation of traffic according to a policy.
F. None of the above.

Answer: B

Explanation:
LFI is a Layer 2 technique in which large frames are broken into small, equal-sized

fragments and transmitted over the link in an interleaved fashion. Using LFI, smaller frames are prioritized, and a mixture of fragments is sent over the link. LFI reduces the queuing delay of small frames because the small frames are sent almost immediately. LFI, therefore, reduces delay and jitter by expediting the transfer of smaller frames through the hardware transmit (Tx) queue. The LFI methods available include Multilink PPP (MLP), FRF.12, and FRF.11 Annex C.

QUESTION 114
Part of the Certkiller VOIP network is shown below:



In the network shown above, Low latency queuing (LLQ) has been configured to provide the highest throughput from VoIP packets. However, the VoIP traffic is still experiencing jitter and delay. Which QoS tool should be configured on the WAN link to allow voice packets to be transmitted as soon as they are queued?

A. Link fragmentation and interleaving
B. Priority queuing
C. RTP header compression
D. Custom queuing
E. Payload compression
F. Flow-based WRED
G. None of the above

Answer: A

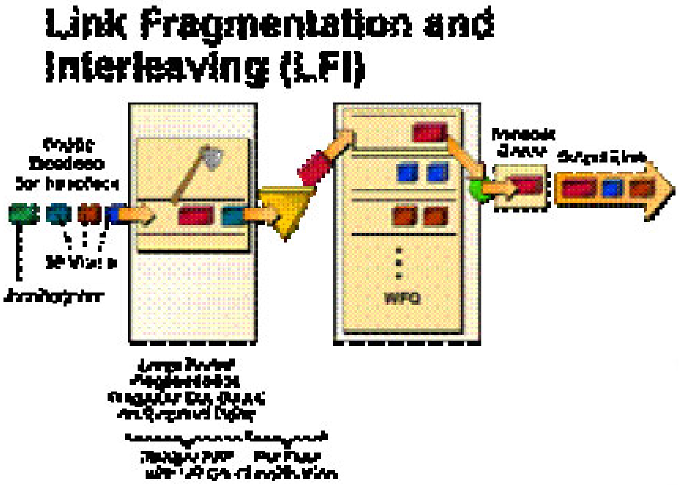
Explanation:
The use of a hybrid queuing method such as low latency queuing (LLQ) can provide low latency and low jitter for VoIP packets while servicing other data packets in a fair manner. But even if VoIP packets are always sent to the front of the software queue, there is still the issue of serialization delay. A large packet may be on its way out of the hardware queue, which uses FIFO. When a VoIP packet is sent to the front of the software queue, the serialization of the large packet in the hardware transmit queue can cause the VoIP packet to wait for a long time before it can be transmitted out. The solution is to fragment the large packets so that they never cause a VoIP packet to wait for more than a predefined amount of time. The VoIP packets must also be allowed to transmit in between the fragments of the larger packets (interleaving), or there will be no point in doing the fragmenting.
When you are configuring the proper fragment size to use on a link, a typical goal is to have a maximum serialization delay of around 10 to 15 ms. Depending on the LFI (Link fragmentation and interleaving) mechanisms being configured, the fragment size is either configured in bytes or in milliseconds.

QUESTION 115
You have a 512 kbps Frame Relay network, and you are experiencing some network latency with some real-time data because of the time it's taking to serialize packets. What could you do to reduce the delay on this network? (Choose two)

A. Link fragmentation and interleaving
B. Frame Relay traffic shaping
C. Low latency queuing
D. IP RTP header compression
E. Traffic classification and policing

Answer: A, C

Explanation:
Interactive traffic (Telnet, voice on IP, and the like) is susceptible to increased latency and jitter when the network processes large packets, (LAN-to-LAN FTP transfers traversing a WAN link, for example), especially as they are queued on slower links. The Cisco IOS Link Fragmentation and Interleaving (LFI) feature reduces delay and jitter on slower-speed links by breaking up large datagrams and interleaving low delay traffic packets with the resulting smaller packets;



LFI was designed especially for lower-speed links where serialization delay is significant.
The Low Latency Queueing feature brings strict priority queueing to Class-Based Weighted Fair Queueing. This feature is extremely useful for low speed links carrying time sensitive traffic such as voice and video.

QUESTION 116
You need to ensure that QoS parameters are maintained across the Certkiller VPN. Which QoS pre-classification option will require the use of the "qos pre-classify" command for the VPN traffic?

A. VPN traffic needs to be classified based on IP flow or Layer 3 information, such as source and destination IP address.

B. VPN traffic needs to be classified based on the Layer 2 header information.
C. VPN traffic needs to be classified based on the IP precedence or DSCP.
D. VPN traffic with Authentication Header (AH) needs to preserve the ToS byte.
E. None of the above.

Answer: A

Explanation:
The qos pre-classify command mechanism allows Cisco routers to make a copy of the inner IP header and to run a QoS classification before encryption, based on fields in the inner IP header. If the classification policy matches on the ToS byte, it is not necessary to use the qos pre-classify command, because the ToS value is copied to the outer header by default. In addition, a simple QoS policy that sorts traffic into classes based on IP precedence can be created. However, differentiating traffic within a class and separating it into multiple flow-based queues requires the qos pre-classify command.
You can apply a service policy to either the tunnel interface or to the underlying physical interface. The decision about where to apply the policy depends on the QoS objectives and on which header you need to use for classification, as follows:
* Apply the policy to the tunnel interface without qos pre-classify when you want to classify packets based on the pretunnel header.
* Apply the policy to the physical interface without qos pre-classify when you want to classify packets based on the post-tunnel header. In addition, apply the policy to the physical interface when you want to shape or police all traffic belonging to a tunnel and the physical interface supports several tunnels.
* Apply the policy to a physical interface and enable qos pre-classify when you want to classify packets based on the pretunnel header.

QUESTION 117
QoS pre-classification is being used on the Certkiller VPN. Which three characteristics of the traffic flow are taken into consideration when the QoS-for-VPNs feature (QoS pre-classify) provides packet classification and applies appropriate QoS service on tunnel interfaces? (Select three)

A. IP precedence bits
B. Destination IP address
C. DE bits
D. DSCP bits
E. Source IP address
F. Original port numbers

Answer: B, E, F

Explanation:
The qos pre-classify command mechanism allows Cisco routers to make a copy of the inner IP header and to run a QoS classification before encryption, based on fields in the inner IP header. If the classification policy matches on the ToS byte, it is not necessary to

use the qos pre-classify command, because the ToS value is copied to the outer header by default. In addition, a simple QoS policy that sorts traffic into classes based on IP precedence can be created. However, differentiating traffic within a class and separating it into multiple flow-based queues requires the qos pre-classify command.
Alternatively, traffic may need to be classified based on values other than IP precedence or DSCP. For example, packets may need to be classified based on IP flow or Layer 3 information, such as source and destination IP address. To do so, use the QoS for VPNs feature enabled with the qos pre-classify command.

QUESTION 118
Router CK1 has been configured with the pre-classification feature for QoS. QoS preclassification is a term used to describe what Cisco IOS feature?

A. AutoSecure
B. QoS for VPNs
C. Modular QoS Command-Line Interface
D. AutoQoS
E. None of the above.

Answer: B

Explanation:
Quality of service (QoS) preclassify is designed for tunnel interfaces. When the feature is enabled, the QoS features on the output interface classify packets before encryption, allowing traffic flows to be managed in congested environments. The result is more effective packet tunneling.
The QoS preclassify feature provides a solution for making Cisco IOS QoS services operate in conjunction with tunneling and encryption on an interface. Cisco IOS software can classify packets and apply the appropriate QoS service before data is encrypted and tunneled. This allows service providers and enterprises to treat voice, video, and mission-critical traffic with a higher priority across service provider networks while using VPNs for secure transport

QUESTION 119
QoS pre-classification needs to be implemented over a Certkiller VPN connection. Which two VPN protocols support QoS preclassification? (Select two)

A. S/MIME
B. SSL
C. PPTP
D. GRE
E. IPsec

Answer: D, E

Explanation:

When packets are encapsulated by a tunneling or encryption protocol, the original packet header is no longer available for examination. From the QoS perspective, providing differentiated levels of service is extremely difficult without the ability to examine the original packet header. The QoS markers normally found in the header of the IP packet must also be visible in the tunnel packet header, regardless of the type of tunnel.
The two primary tunneling protocol relevant to VPN these are:
1. GRE
2. IPSec
1. GRE
GRE tunneling allows routers between GRE-based tunnel endpoints to see the packet marking, improving the routing of premium service packets. Cisco IOS QoS technologies such as policy routing, weighted fair queuing (WFQ), and weighted random early detection (WRED) can operate on intermediate routers between GRE tunnel endpoints.
GRE tunnels are commonly used to provide dynamic routing resilience over IPsec. Normal IPsec configurations cannot transfer routing protocols, such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), or non-IP traffic, such as Internetwork Packet Exchange (IPX) and AppleTalk.
2. IPSec
The IPSec feature is supported across Cisco IOS-based 1600, 2x00, 36x0, 4x00, 4x00, 5x00, and 7x00 platforms, using IOS release greater than 12.0(x), Cisco PIX Firewalls, and VPN Client and Concentrators.
RFC 2401 describes the general framework for this architecture. Like all security mechanisms, RFC 2401 helps to enforce a security policy. The policy defines the need for security on various connections. These connections will be IP sessions. The framework provides data integrity, data authentication, data confidentiality, security association, and key management.

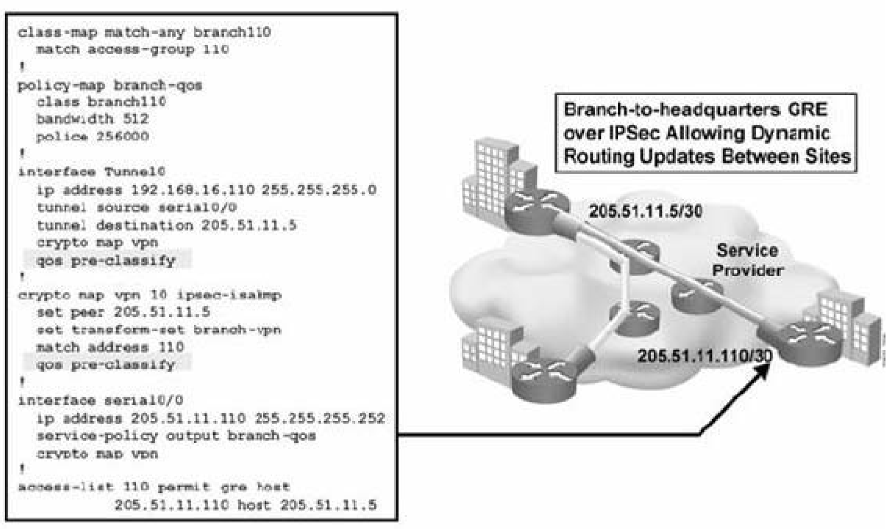
QUESTION 120
A GRE tunnel is configured between two Certkiller locations. Where should the service policy be applied to classify packets based on the pre-tunnel header?

A. In global configuration mode, apply the service policy and use the qos pre-classify command.
B. Apply the service policy on the physical interface but do not use the qos pre-classify command.
C. Apply the service policy on the tunnel interface but do not use the qos pre-classify command.
D. Apply the service policy on the tunnel interface and use the qos pre-classify command.
E. In global configuration mode, apply the service policy but do not use the qos pre-classify command.
F. None of the above.

Answer: C

Explanation:

GRE tunneling allows routers between GRE-based tunnel endpoints to see the packet marking, improving the routing of premium service packets. Cisco IOS QoS technologies such as policy routing, weighted fair queuing (WFQ), and weighted random early detection (WRED) can operate on intermediate routers between GRE tunnel endpoints. GRE tunnels are commonly used to provide dynamic routing resilience over IPsec. Normal IPsec configurations cannot transfer routing protocols, such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), or non-IP traffic, such as Internetwork Packet Exchange (IPX) and AppleTalk.
Here is the example:



```
class-map match-any branch110
  match access-group 110
!
policy-map branch-qos
  class branch110
  bandwidth 512
  police 256000
!
interface Tunnel0
  ip address 192.168.16.110 255.255.255.0
  tunnel source serial0/0
  tunnel destination 205.51.11.5
  crypto map vpn
  qos pre-classify
!
crypto map vpn 10 ipsec-isakmp
  set peer 205.51.11.5
  set transform-set branch-vpn
  match address 110
  qos pre-classify
!
interface serial0/0
  ip address 205.51.11.110 255.255.255.252
  service-policy output branch-qos
  crypto map vpn
!
access-list 110 permit gre host
          205.51.11.110 host 205.51.11.5
```

Branch-to-headquarters GRE over IPSec Allowing Dynamic Routing Updates Between Sites
205.51.11.5/30
Service Provider
205.51.11.110/30

QUESTION 121

QoS for a Certkiller VPN has been configured using the "qos pre-classify" command. Which two statements are true about the configuration options for this command? (Select two)

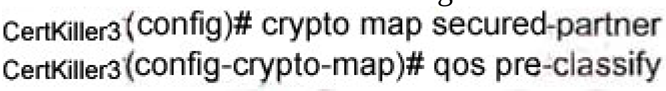
A. In an IPsec tunnel, the command is applied in the crypto map.
B. In a Generic Routing Encapsulation (GRE) tunnel, the command is applied on the tunnel interface.
C. In a GRE tunnel, the command is applied on the physical interface.
D. In a VPN over a Frame Relay tunnel, the command is applied on the virtual-template subinterface.
E. In an IPsec tunnel, the command is applied on the physical interface.

Answer: A, B

Explanation:
The qos pre-classify command mechanism allows Cisco routers to make a copy of the inner IP header and to run a QoS classification before encryption, based on fields in the inner IP header. If the classification policy matches on the ToS byte, it is not necessary to use the qos pre-classify command, because the ToS value is copied to the outer header by default. In addition, a simple QoS policy that sorts traffic into classes based on IP precedence can be created. However, differentiating traffic within a class and separating

it into multiple flow-based queues requires the qos pre-classify command.
Alternatively, traffic may need to be classified based on values other than IP precedence or DSCP. For example, packets may need to be classified based on IP flow or Layer 3 information, such as source and destination IP address. To do so, use the QoS for VPNs feature enabled with the qos pre-classify command.

QUESTION 122
Router Certkiller 3 has been configured as shown below:



```
CertKiller3(config)# crypto map secured-partner
CertKiller3(config-crypto-map)# qos pre-classify
```

Study the exhibit carefully shown above. What is this configuration an example of?

A. AutoQoS for the enterprise
B. Modular QoS CLI
C. QoS preclassification over an IPsec tunnel
D. QoS preclassification over a GRE tunnel
E. Voice and QoS features for IPsec
F. QoS preclassification over a L2TP tunnel
G. None of the above

Answer: C

Explanation:
The
qos pre-classify command mechanism allows Cisco routers to make a copy of the inner IP header and to run a QoS classification before encryption, based on fields in the inner IP header. If the classification policy matches on the ToS byte, it is not necessary to use the qos pre-classify command, because the ToS value is copied to the outer header by default. In addition, a simple QoS policy that sorts traffic into classes based on IP precedence can be created. However, differentiating traffic within a class and separating it into multiple flow-based queues requires the qos pre-classify command.
You can apply a service policy to either the tunnel interface or to the underlying physical interface. The decision about where to apply the policy depends on the QoS objectives and on which header you need to use for classification, as follows:
* Apply the policy to the tunnel interface without qos pre-classify when you want to classify packets based on the pretunnel header.
* Apply the policy to the physical interface without qos pre-classify when you want to classify packets based on the post-tunnel header. In addition, apply the policy to the physical interface when you want to shape or police all traffic belonging to a tunnel and the physical interface supports several tunnels.
* Apply the policy to a physical interface and enable qos pre-classify when you want to classify packets based on the pretunnel header.

QUESTION 123
You want to ensure that QoS parameters are preserved over a tunnel. What is applied to tunnel interfaces to allow QoS policies to be applied to packets going

through the tunnel?

A. QoS preclassification
B. Access list
C. Class map
D. Crypto map
E. Service policy
F. None of the above

Answer: A

Explanation:
Quality of service (QoS) preclassify is designed for tunnel interfaces. When the feature is enabled, the QoS features on the output interface classify packets before encryption, allowing traffic flows to be managed in congested environments. The result is more effective packet tunneling.
The QoS preclassify feature provides a solution for making Cisco IOS QoS services operate in conjunction with tunneling and encryption on an interface. Cisco IOS software can classify packets and apply the appropriate QoS service before data is encrypted and tunneled. This allows service providers and enterprises to treat voice, video, and mission-critical traffic with a higher priority across service provider networks while using VPNs for secure transport

---

QUESTION 124
You want to ensure that QoS parameters are preserved over the Certkiller VPN.
What is true regarding Quality of Service (QoS) for VPNs?

A. QoS preclassification is only supported on generic routing encapsulation (GRE) and IPsec VPNs.
B. QoS preclassification is supported on IPsec AH VPNs, but not on IPsec ESP VPNs.
C. The QoS-for-VPNs feature (QoS preclassification) is designed for VPN transport interfaces.
D. QoS preclassification is not required in Layer 2 Tunneling Protocol (L2TP), Layer 2 Forwarding (L2F), and Point-to-Point Tunneling Protocol (PPTP) VPNs.
E. With IPsec tunnel mode, the type of service (ToS) byte value is copied automatically from the original IP header to the tunnel header.
F. None of the above.

Answer: E

Explanation:
The qos pre-classify command mechanism allows Cisco routers to make a copy of the inner IP header and to run a QoS classification before encryption, based on fields in the inner IP header. If the classification policy matches on the ToS byte, it is not necessary to use the qos pre-classify command, because the ToS value is copied to the outer header by default. In addition, a simple QoS policy that sorts traffic into classes based on IP

precedence can be created. However, differentiating traffic within a class and separating it into multiple flow-based queues requires the qos pre-classify command.
You can apply a service policy to either the tunnel interface or to the underlying physical interface. The decision about where to apply the policy depends on the QoS objectives and on which header you need to use for classification, as follows:
* Apply the policy to the tunnel interface without qos pre-classify when you want to classify packets based on the pretunnel header.
* Apply the policy to the physical interface without
qos pre-classify when you want to classify packets based on the post-tunnel header. In addition, apply the policy to the physical interface when you want to shape or police all traffic belonging to a tunnel and the physical interface supports several tunnels.
* Apply the policy to a physical interface and enable qos pre-classify when you want to classify packets based on the pretunnel header.

QUESTION 125
Router CK1 was configured with the "qos pre-classify" command. Which statement about this command is true?

A. The qos pre-classify command is not necessary when the classification policy matches on the ToS byte.
B. The qos pre-classify command cannot be applied to an IPsec GRE tunnel.
C. The qos pre-classify command is entered in privileged EXEC mode.
D. The qos pre-classify command is entered in global configuration mode.
E. None of the above

Answer: A

Explanation:
The qos pre-classify command mechanism allows Cisco routers to make a copy of the inner IP header and to run a QoS classification before encryption, based on fields in the inner IP header. If the classification policy matches on the ToS byte, it is not necessary to use the qos pre-classify command, because the ToS value is copied to the outer header by default. In addition, a simple QoS policy that sorts traffic into classes based on IP precedence can be created. However, differentiating traffic within a class and separating it into multiple flow-based queues requires the qos pre-classify command.
You can apply a service policy to either the tunnel interface or to the underlying physical interface. The decision about where to apply the policy depends on the QoS objectives and on which header you need to use for classification, as follows:
* Apply the policy to the tunnel interface without qos pre-classify when you want to classify packets based on the pretunnel header.
* Apply the policy to the physical interface without qos pre-classify when you want to classify packets based on the post-tunnel header. In addition, apply the policy to the physical interface when you want to shape or police all traffic belonging to a tunnel and the physical interface supports several tunnels.
* Apply the policy to a physical interface and enable qos pre-classify when you want to classify packets based on the pretunnel header.

QUESTION 126

Exhibit #1:

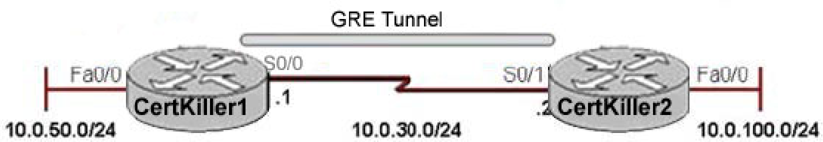
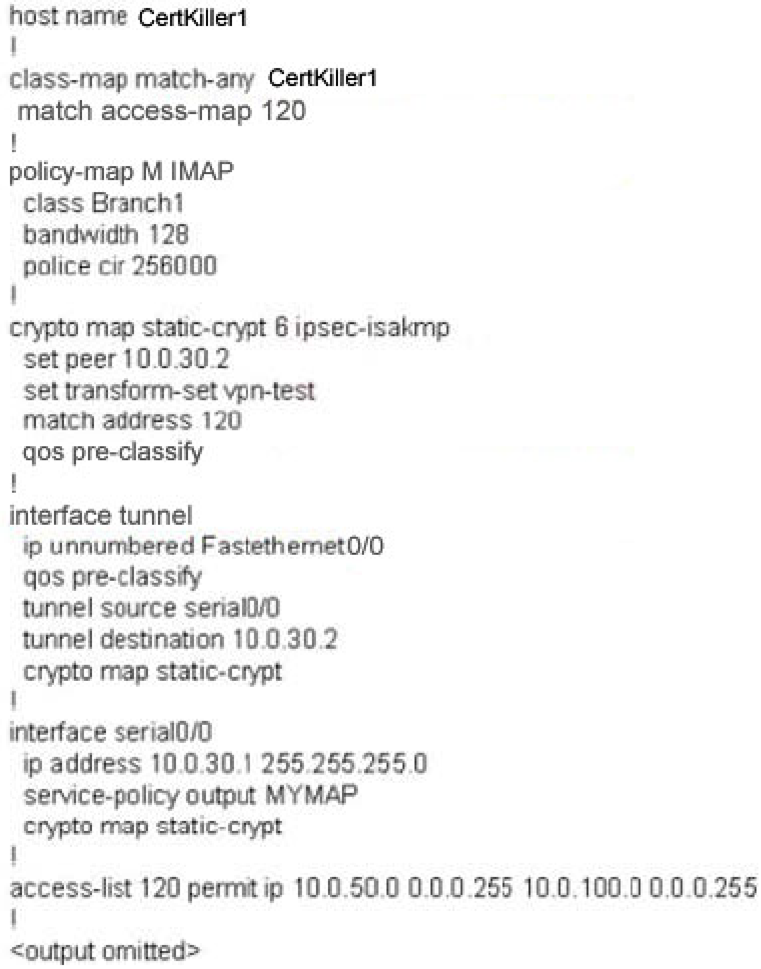


Exhibit #2.



```
host name CertKiller1
!
class-map match-any CertKiller1
 match access-map 120
!
policy-map M IMAP
  class Branch1
  bandwidth 128
  police cir 256000
!
crypto map static-crypt 6 ipsec-isakmp
  set peer 10.0.30.2
  set transform-set vpn-test
  match address 120
  qos pre-classify
!
interface tunnel
  ip unnumbered Fastethernet0/0
  qos pre-classify
  tunnel source serial0/0
  tunnel destination 10.0.30.2
  crypto map static-crypt
!
interface serial0/0
  ip address 10.0.30.1 255.255.255.0
  service-policy output MYMAP
  crypto map static-crypt
!
access-list 120 permit ip 10.0.50.0 0.0.0.255 10.0.100.0 0.0.0.255
!
<output omitted>
```

Study the exhibit shown below carefully. Quality of Service (QoS) is configured for traffic that is encrypted and carried over a GRE tunnel between the Certkiller 1 and Certkiller 2 routers in the Certkiller network. On the basis of the configuration provided, which statement is true about the QoS pre-classification feature applied on the outbound interface on router Certkiller 1?

A. The outbound traffic of the Tunnel1 interface on Branch1 router is policed at a rate of 256 kbps.
B. QoS features on the physical interface carrying the crypto map are able to classify packets on the original header information.
C. QoS features on the physical interface carrying the crypto map are able to classify packets on post encryption criteria.

D. The bandwidth of the Tunnel1 interface on Branch1 router is set to 128 kbps.
E. None of the above

Answer: B

Explanation:
The qos pre-classify command mechanism allows Cisco routers to make a copy of the inner IP header and to run a QoS classification before encryption, based on fields in the inner IP header. If the classification policy matches on the ToS byte, it is not necessary to use the qos pre-classify command, because the ToS value is copied to the outer header by default. In addition, a simple QoS policy that sorts traffic into classes based on IP precedence can be created. However, differentiating traffic within a class and separating it into multiple flow-based queues requires the qos pre-classify command.
You can apply a service policy to either the tunnel interface or to the underlying physical interface. The decision about where to apply the policy depends on the QoS objectives and on which header you need to use for classification, as follows:
* Apply the policy to the tunnel interface without qos pre-classify when you want to classify packets based on the pretunnel header.
* Apply the policy to the physical interface without qos pre-classify when you want to classify packets based on the post-tunnel header. In addition, apply the policy to the physical interface when you want to shape or police all traffic belonging to a tunnel and the physical interface supports several tunnels.
* Apply the policy to a physical interface and enable qos pre-classify when you want to classify packets based on the pretunnel header.

QUESTION 127
Auto QOS has been configured on a number of new Certkiller devices. Which two statements are true about AutoQoS? (Select two)

A. AutoQoS has evolved over two phases: AutoQoS VoIP and AutoQoS for Enterprise.
B. AutoQoS has evolved over two phases: AutoQoS for SP and AutoQoS for Enterprise.
C. AutoQoS for Enterprise is supported on Cisco router and switch platforms.
D. Prior to AutoQoS being configured, CEF must be enabled on the interface.
E. AutoQoS is deployed on switches in two phases: Auto-Discovery and Generating MQC-based policies.

Answer: A, D

Explanation:
Cisco AutoQoS represents innovative technology that simplifies the challenges of network administration by reducing QoS complexity, deployment time, and cost to enterprise networks. Cisco AutoQoS incorporates value-added intelligence in Cisco IOS software and Cisco Catalyst software to provision and assist in the management of large-scale QoS deployments. The first phase of Cisco AutoQoS VoIP offers straightforward capabilities to automate VoIP deployments for customers that want to deploy IP telephony but lack the expertise and staffing to plan and deploy IP QoS and IP

services. The second phase, Cisco AutoQoS Enterprise, which is supported only on router interfaces, uses Network-Based Application Recognition (NBAR) to discover the traffic. After this discovery phase, the AutoQoS process can then configure the interface to support up to 10 traffic classes.

QUESTION 128
The auto QOS feature is being configured on a new Certkiller router. Which two Cisco AutoQoS interface statements are true? (Select two)

A. AutoQoS is supported only on Frame Relay main interfaces and not on any subinterface configuration.
B. AutoQoS is supported on serial PPP and HDLC interfaces.
C. AutoQoS is supported on Frame Relay multipoint subinterfaces.
D. AutoQoS is supported on low-speed ATM PVCs in point-to-point subinterfaces.

Answer: B, D

Explanation:
Using Cisco AutoQoS, network administrators can implement the QoS features that are required for VoIP traffic without an in-depth knowledge of these underlying technologies:
1. PPP
2. Frame Relay
3. ATM
4. Link efficiency mechanisms, such as link fragmentation and interleaving (LFI)

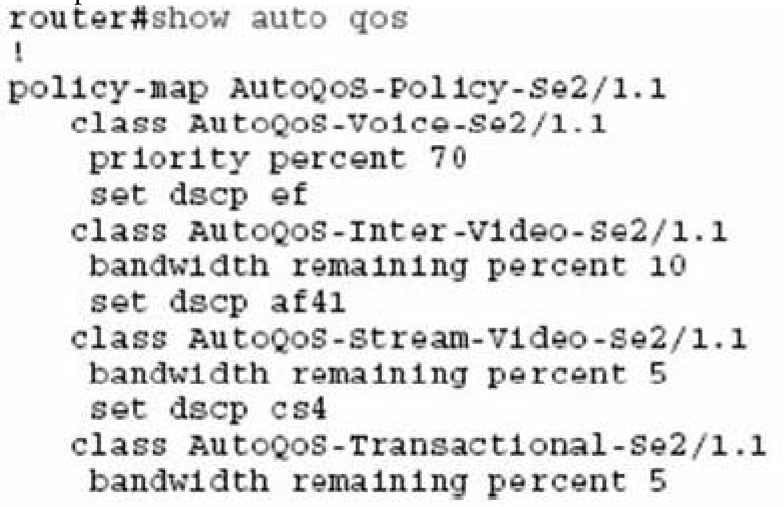
QUESTION 129
Cisco AutoQoS has been correctly configured on a Certkiller router. What information that is created by the AutoQoS feature will be displayed by the output from the "show auto qos" command?

A. Policy maps and class maps
B. Interface configurations and policy maps
C. Routing parameters, policy maps, and class maps
D. Interface configurations and class maps
E. Interface configurations, policy maps, and class maps
F. Interface configurations, routing parameters, policy maps, and class maps
G. None of the above

Answer: E

Explanation:
Displays the Cisco AutoQoStemplates (policy maps, class maps, and ACLs) created for a specific interface or all interfaces.

Example:



```
router#show auto qos
!
policy-map AutoQoS-Policy-Se2/1.1
   class AutoQoS-Voice-Se2/1.1
    priority percent 70
    set dscp ef
   class AutoQoS-Inter-Video-Se2/1.1
    bandwidth remaining percent 10
    set dscp af41
   class AutoQoS-Stream-Video-Se2/1.1
    bandwidth remaining percent 5
    set dscp cs4
   class AutoQoS-Transactional-Se2/1.1
    bandwidth remaining percent 5
```

QUESTION 130

The AutoQos feature was implemented on router CK1 . Which three DiffServ QoS mechanisms are enabled by AutoQoS? (Select three)

A. Congestion avoidance using WRED
B. Congestion management with CQ
C. Traffic shaping with class-based shaping
D. Traffic classification using NBAR
E. Traffic policing using CAR
F. Traffic classification using WRED

Answer: A, C, D

Explanation: When AutoQos Feature implemented on router
i. Congestion Avoidance using WRED
ii. Traffic Shaping with class based shaping
iii. Traffic classification with NBAR enabled
1. Weighted random early detection (WRED) combines RED with IP precedence or DSCP and performs packet dropping based on IP precedence or DSCP markings. As with RED, WRED monitors the average queue length in the router and determines when to begin discarding packets based on the length of the interface queue. When the average queue length exceeds the user-specified minimum threshold, WRED begins to randomly drop packets with a certain probability. If the average length of the queue continues to increase so that it becomes larger than the user-specified maximum threshold, WRED reverts to a tail-drop packet-discard strategy, in which all incoming packets are dropped.
2. Class-based traffic shaping uses the MQC to allow traffic to be shaped per traffic class as defined by the class map. Class-based traffic shaping can be used in combination with class-based weighted fair queuing (CBWFQ), in which the shaped rate is used to define an upper rate limit while the bandwidth statement within the CBWFQ configuration is used to define a minimum rate limit.

QUESTION 131

Auto-Discovery and AutoQoS template generation and installation have been enabled on an interface of a new Certkiller router. How will AutoQoS respond to changes made to bandwidth after the feature is configured?

A. Auto-Discovery phase is constantly on and will build a new profile which will have to be updated manually on the router.
B. Auto-Discovery phase will need to be manually enabled but the QOS template will update automatically.
C. The router will pick up the new traffic patterns at next boot-up.
D. Auto-Discovery phase and the QoS template deployment phase must be repeated manually.
E. Auto-Discovery phase is constantly on and will automatically update the QoS template.
F. None of the above.

Answer: D

Explanation:
The Auto-Discovery phase uses NBAR to detect network applications and protocols as they leave an interface, collect data from the offered traffic, and perform statistical analysis. The information collected will be used to build the AutoQoS templates
The
auto qos command generates Cisco AutoQoS for the Enterprise templates on the basis of the data collected during the autodiscovery phase and then installs the templates on the interface. These templates are then used to create class maps and policy maps for use on your network. After they are created, the class maps and policy maps are also installed on the interface.

QUESTION 132

Auto QoS has been implemented on a new Certkiller LAN switch. What are three of the functions that AutoQoS performs when it is configured on a switch? (Select three)

A. Synchronizes FIFO, PQ, CQ, and MDRR with WFQ, CBWFQ, and LLQ.
B. Enables strict priority queuing for voice traffic, and weighted round robin queuing for data traffic.
C. Adjusts link speeds to adapt to QoS needs.
D. Enables low latency queuing to ensure that voice traffic receives priority treatment.
E. Enforces a trust boundary on switch access ports and uplinks/downlinks.
F. Modifies queue sizes as well as queue weights where required.

Answer: B, E, F

Explanation:
The first phase of Cisco AutoQoS offers straightforward capabilities to automate VoIP

deployments for customers who want to deploy IP telephony but who lack the expertise or staffing to plan and deploy IP QoS and IP services. Cisco AutoQoS VoIP is the first release of Cisco AutoQoS and automates QoS settings for VoIP deployments only. This feature automatically generates interface configurations, policy maps, class maps, and access control lists (ACLs). Cisco AutoQoS VoIP automatically employs Cisco Network-Based Application Recognition (NBAR) to classify voice traffic and mark it with the appropriate differentiated services code point (DSCP) value. Cisco AutoQoS VoIP can be instructed to rely on, or trust, the DSCP markings previously applied to the packets.
The second phase of Cisco AutoQoS expands its capabilities beyond VoIP and it addresses the QoS requirements of enterprise converged networks. Cisco AutoQoS for the Enterprise adds an important step-users can observe the applications that have been discovered during the observation phase (autodiscovery), and review the QoS policy that Cisco AutoQoS for the Enterprise suggests without deploying that policy. Cisco AutoQoS for the Enterprise blends the design and implementation of QoS, based on the most common enterprise scenarios, into two major steps:
* It automatically discovers which applications are used in the enterprise network and generates optimal policy. This step employs the NBAR discovery mechanism.
* It implements the generated policy.

QUESTION 133
AutoQos is being implemented on many of the Cisco routers within the Certkiller network. Which two statements about Cisco AutoQoS are true? (Select two)

A. Cisco NBAR is a prerequisite for CEF.
B. A QoS service policy must already be enabled on the interface before Cisco AutoQoS can be enabled.
C. AutoQoS uses Cisco network-based application recognition (NBAR) to identify various applications and traffic types.
D. Cisco Express Forwarding (CEF) must be enabled at the interface or ATM PVC.
E. On a serial interface, before AutoQoS is enabled, the clock rate command must be used to specify a bandwidth other than the default 1.54 Mbps.
F. Any interface at or below 1.54 Mbps is classified as a low-speed interface.

Answer: C, D

Explanation:
The first phase of Cisco AutoQoS offers straightforward capabilities to automate VoIP deployments for customers who want to deploy IP telephony but who lack the expertise or staffing to plan and deploy IP QoS and IP services. Cisco AutoQoS VoIP is the first release of Cisco AutoQoS and automates QoS settings for VoIP deployments only. This feature automatically generates interface configurations, policy maps, class maps, and access control lists (ACLs). Cisco AutoQoS VoIP automatically employs Cisco Network-Based Application Recognition (NBAR) to classify voice traffic and mark it with the appropriate differentiated services code point (DSCP) value. Cisco AutoQoS VoIP can be instructed to rely on, or trust, the DSCP markings previously applied to the

packets.
NBAR Protocol Discovery is a commonly used NBAR feature that collects application and protocol statistics (that is, packet counts, byte counts, and bit rates) per interface. It enables you to generate real-time statistics on the applications in the network. It also gives you an idea of the traffic distribution at key points in the enterprise network. NBAR is an important element in many Cisco initiatives, including Cisco Service-Oriented Network Architecture (SONA).
Protocol Discovery has the application-specific intelligence to discover traffic types and is tightly integrated into Cisco QoS Solution.
Cisco Express Forwarding (CEF) must be enabled. Cisco AutoQoS uses NBAR to identify various applications and traffic types, and CEF is a prerequisite for NBAR..

QUESTION 134
The Certkiller network administrator is using the QOS SDM wizard on a new Cisco router. Which statement is correct about the Cisco QoS SDM wizard?

A. The SDM wizard is not able to monitor QoS policing traffic.
B. SDM QoS wizard provides real-time validation of application usage of WAN bandwidth.
C. The SDM QoS Wizard is pre-installed on enterprise routers.
D. The best-effort class will need to have its percentage entered in the QoS Policy Generation screen.
E. None of the above

Answer: B

Explanation:
Cisco Router and Security Device Manager (SDM) allows you to easily configure routing, security, and QoS services on Cisco routers while helping to enable proactive management through performance monitoring. Whether you are deploying a new router or installing Cisco SDM on an existing router, you can now remotely configure and monitor these routers without using the Cisco IOS software CLI. The Cisco SDM GUI aids nonexpert users of Cisco IOS software in day-to-day operations, provides easy-to-use smart wizards, automates router security management, and assists you through comprehensive online help and tutorials.
Cisco SDM smart wizards guide you step by step through router and security configuration workflow by systematically configuring the LAN and WAN interfaces, firewall, Network Address Translation (NAT) intrusion prevention system (IPS), and IPsec virtual private network (VPNs) routing, and QoS. Cisco SDM smart wizards can intelligently detect incorrect configurations and propose fixes. Online help embedded within Cisco SDM contains appropriate background information, in addition to step-by-step procedures to help you enter correct data in Cisco SDM. In the QoS configuration section of Cisco SDM, there are several options to define traffic classes and configure QoS policies in the network.
The Cisco SDM QoS wizard offers easy and effective optimization of LAN, WAN, and VPN bandwidth and application performance for different business needs (for example, voice and video, enterprise applications, and web). Three predefined categories are:

1. Real-time
2. Business-critical
3. Best-effort

In addition, the Cisco SDM QoS wizard supports NBAR, which provides real-time validation of application usage of WAN bandwidth against predefined service policies as well as QoS policing and traffic monitoring.

QUESTION 135

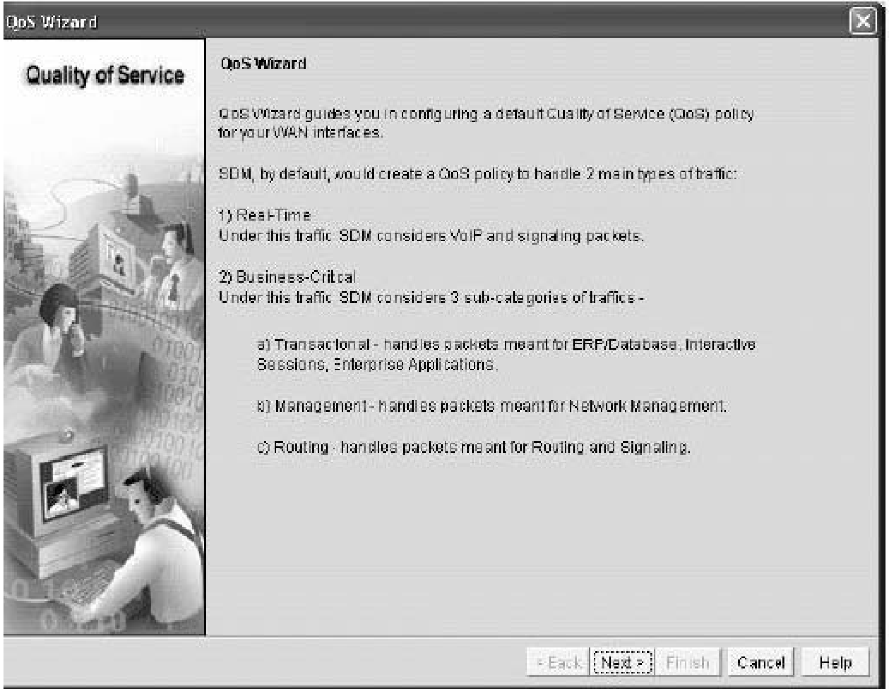
The Certkiller network administrator is using the SDM tool to set up QOS policies on a new router. Which two statements about the QoS policy generation phase of the Cisco SDM QoS wizard are true? (Select two)

A. The SDM QoS wizard will create three business-critical traffic classes to handle transactional, network management, and routing packets.
B. The SDM QoS wizard will create two business-critical traffic classes to handle transactional and network management packets.
C. The SDM QoS wizard will create three real-time traffic classes to handle VoIP, voice signaling, and video packets.
D. The SDM QoS wizard will create two real-time traffic classes to handle VoIP and voice signaling packets.
E. The SDM QoS wizard will create four real-time traffic classes to handle VoIP, voice signaling, video, and video streaming packets.
F. The SDM QoS wizard will create four business-critical traffic classes to handle transactional, network management, routing, and best-effort packets.

Answer: A, D

Explanation:
The Cisco SDM QoS wizard offers easy and effective optimization of LAN, WAN, and VPN bandwidth and application performance for different business needs (for example, voice and video, enterprise applications, and web). Three predefined categories are:
1. Real-time
2. Business-critical
3. Best-effort

The SDM QoS wizard will create three business-critical traffic classes to handle transactional, network management, and routing packets



QoS Wizard

QoS Wizard guides you in configuring a default Quality of Service (QoS) policy for your WAN interfaces.

SDM, by default, would create a QoS policy to handle 2 main types of traffic:

1) Real-Time
Under this traffic SDM considers VoIP and signaling packets.

2) Business-Critical
Under this traffic SDM considers 3 sub-categories of traffics -

a) Transactional - handles packets meant for ERP/Database, Interactive Sessions, Enterprise Applications.

b) Management - handles packets meant for Network Management.

c) Routing - handles packets meant for Routing and Signaling.

QUESTION 136
You need to set up QoS to support VOIP on a new Certkiller using the SDM. Which two QoS statements are true about the use of the SDM QoS wizard? (Select two)

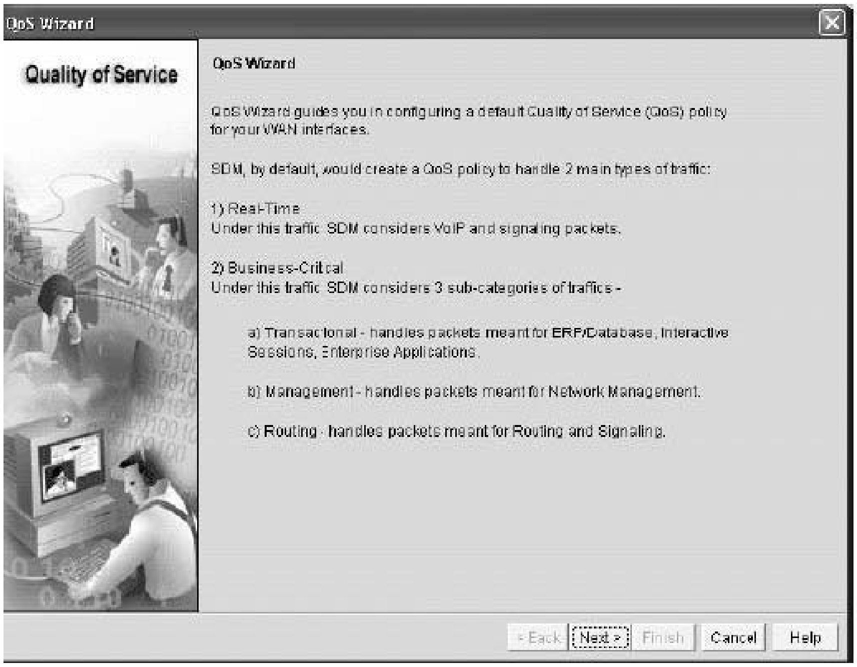
A. Business-critical traffic includes VoIP and voice signaling packets.
B. SDM creates a custom-queuing (CQ) or a priority-queuing (PQ) policy.
C. SDM creates a low latency queuing (LLQ) service policy with its associated classes.
D. SDM can be used to configure a basic QoS policy for incoming traffic on WAN interfaces and IPsec tunnels.
E. SDM can provide QoS for real-time traffic and business-critical traffic.
F. When allocating bandwidth, values can be entered in either bandwidth percentage or kilobytes per second (kBps).

Answer: C, E

Explanation:
The LLQ feature brings strict Priority Queuing (PQ) to CBWFQ. Strict PQ allows delay-sensitive data such as voice to be sent before packets in other queues are sent. Without LLQ, CBWFQ provides WFQ based on defined classes with no strict priority queue available for real-time traffic. For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth assigned to the class. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced fairly based on weight and no class of packets may be granted strict priority. This scheme poses problems for voice traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission manifesting as jitter in the heard conversation.

LLQ provides strict priority queuing for CBWFQ, reducing jitter in voice conversations.
The Cisco SDM QoS wizard offers easy and effective optimization of LAN, WAN, and VPN bandwidth and application performance for different business needs (for example, voice and video, enterprise applications, and web). Three predefined categories are:

1. Real-time
2. Business-critical
3. Best-effort



QoS Wizard

QoS Wizard guides you in configuring a default Quality of Service (QoS) policy for your WAN interfaces.

SDM, by default, would create a QoS policy to handle 2 main types of traffic:

1) Real-Time
Under this traffic SDM considers VoIP and signaling packets.

2) Business-Critical
Under this traffic SDM considers 3 sub-categories of traffics -

a) Transactional - handles packets meant for ERP/Database, Interactive Sessions, Enterprise Applications.

b) Management - handles packets meant for Network Management.

c) Routing - handles packets meant for Routing and Signaling.

QUESTION 137
You need to configure QoS on a new Certkiller router using SDM. What are two of the three predefined classes for the Cisco SDM wizard? (Select two)

A. Middle class
B. Voice
C. High priority
D. Business-critical
E. Best effort
F. Scavenger

Answer: D, E

Explanation:
The Cisco SDM QoS wizard offers easy and effective optimization of LAN, WAN, and VPN bandwidth and application performance for different business needs (for example, voice and video, enterprise applications, and web). Three predefined categories are:

1. Real-time
2. Business-critical
3. Best-effort

QUESTION 138

You need to configure QoS on a new Certkiller router using the Device Manager.
Which two statements about the QoS functionality of the Cisco SDM are true?
(Select two)

A. The SDM QoS wizard supports network-based application recognition (NBAR) to provide deep and stateful packet inspection.
B. To create and manage the QoS settings, the user must select the QoS wizard task under the Monitor option.
C. The SDM QoS wizard will apply custom queuing and priority queuing policies to the identified interfaces.
D. The SDM QoS wizard can be used to optimize LAN, WAN, and VPN interfaces.
E. The first step when using the SDM QoS wizard is to select the inbound interface on which the QoS policy must be applied.
F. The SDM QoS wizard will apply low latency-queuing, custom-queuing and priority-queuing policies to the identified interfaces.

Answer: A, D

Explanation:
Cisco Router and Security Device Manager (SDM) allows you to easily configure routing, security, and QoS services on Cisco routers while helping to enable proactive management through performance monitoring. Whether you are deploying a new router or installing Cisco SDM on an existing router, you can now remotely configure and monitor these routers without using the Cisco IOS software CLI. The Cisco SDM GUI aids nonexpert users of Cisco IOS software in day-to-day operations, provides easy-to-use smart wizards, automates router security management, and assists you through comprehensive online help and tutorials.
Cisco SDM smart wizards guide you step by step through router and security configuration workflow by systematically configuring the LAN and WAN interfaces, firewall, Network Address Translation (NAT) intrusion prevention system (IPS), and IPsec virtual private network (VPNs) routing, and QoS. Cisco SDM smart wizards can intelligently detect incorrect configurations and propose fixes. Online help embedded within Cisco SDM contains appropriate background information, in addition to step-by-step procedures to help you enter correct data in Cisco SDM. In the QoS configuration section of Cisco SDM, there are several options to define traffic classes and configure QoS policies in the network.
Cisco SDM QoS wizard supports NBAR, which provides real-time validation of application usage of WAN bandwidth against predefined service policies as well as QoS policing and traffic monitoring.

QUESTION 139

LLQ has been configured on a Certkiller device using SDM. SDM creates a low latency queuing (LLQ) service policy with its associated classes. What are the two types of low latency queuing available using the SDM QoS wizard?

A. FIFO queuing; to provide a means to hold packets while they are waiting to exit an interface
B. Custom queuing (CQ); which provides a queuing tool that services all queues, even during times of congestion
C. Weighted fair queuing (WFQ); which classifies packets based on flows
D. Priority queuing; to ensure a fixed amount of bandwidth
E. Bandwidth queuing; to ensure a minimum amount of bandwidth

Answer: D, E

Explanation:
The LLQ feature brings strict Priority Queuing (PQ) to CBWFQ. Strict PQ allows delay-sensitive data such as voice to be sent before packets in other queues are sent. Without LLQ, CBWFQ provides WFQ based on defined classes with no strict priority queue available for real-time traffic. For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth assigned to the class. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced fairly based on weight and no class of packets may be granted strict priority. This scheme poses problems for voice traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission manifesting as jitter in the heard conversation.
LLQ provides strict priority queuing for CBWFQ, reducing jitter in voice conversations.
LLQ enables the use of a single, strict priority queue within CBWFQ at the class level.
Any class can be made a priority queue by adding the priority keyword. Within a policy map, one or more classes can be given priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is sent to the same, single, strict priority queue.
Although it is possible to queue various types of real-time traffic to the strict priority queue, it is strongly recommend that only voice traffic be sent to it because voice traffic is well-behaved, whereas other types of real-time traffic are not. Moreover, voice traffic requires that delay be non-variable in order to avoid jitter. Real-time traffic such as video could introduce variation in delay, thereby thwarting the steadiness of delay required for successful voice traffic transmission.
When the priority command is specified for a class, it takes a bandwidth argument that gives maximum bandwidth in kbps. This parameter specifies the maximum amount of bandwidth allocated for packets belonging to the class configured. The bandwidth parameter both guarantees bandwidth to the priority class and restrains the flow of packets from the priority class. In the event of congestion, policing is used to drop packets when the bandwidth is exceeded.
Voice traffic queued to the priority queue is UDP-based and therefore not adaptive to the early packet drop characteristic of WRED. Because WRED is ineffective, the WRED random-detect command cannot be used with the priority command. In addition, because policing is used to drop packets and a queue limit is not imposed, the queue-limit command cannot be used with the priority command.

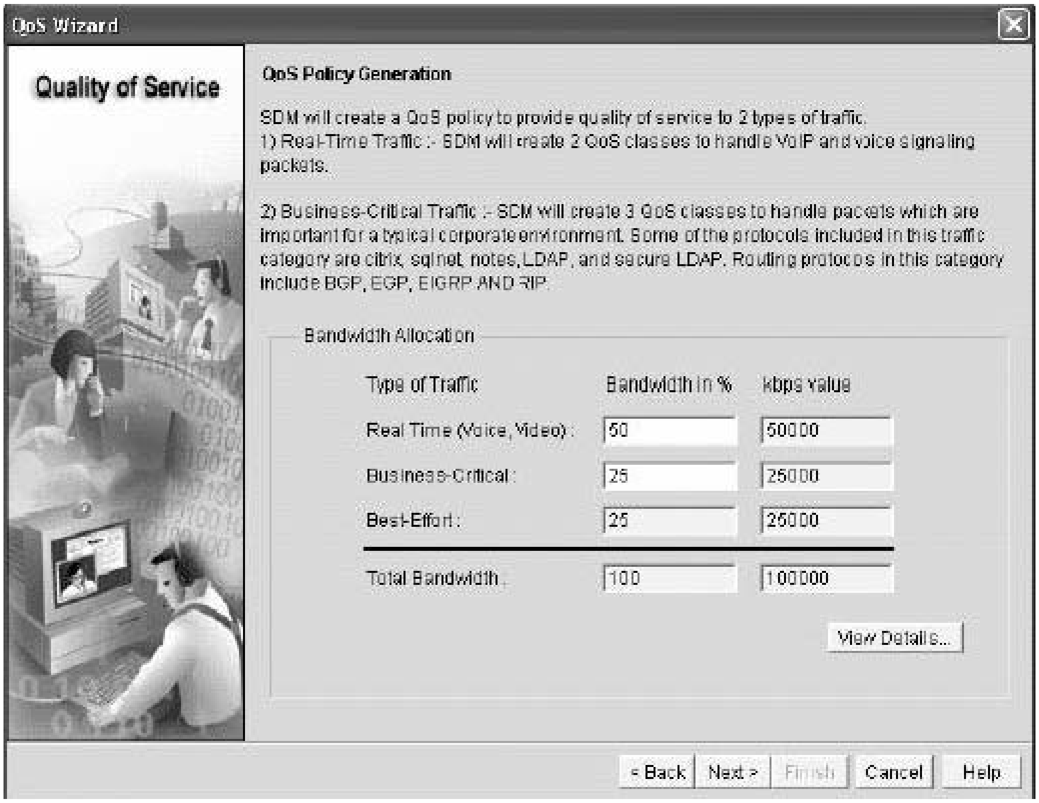
QUESTION 140

The Cisco Router and Security Device Manager (SDM) QoS wizard has a QoS policy generation phase, which you need to utilize on a new Certkiller router. Which two bandwidth allocation statements are true about this phase? (Select two)

A. The user must specify in kbps the amount of bandwidth to allocate for best-effort traffic.
B. The user must specify, as a percentage of the overall available bandwidth, the amount of bandwidth to allocate for best-effort traffic.
C. The user must specify, as a percentage of the overall available bandwidth, the amount of bandwidth to allocate for real-time traffic.
D. The user must specify, as a percentage of the overall available bandwidth, the amount of bandwidth to allocate for business-critical traffic.
E. The user must specify in kbps the amount of bandwidth to allocate for real-time traffic.
F. The user must specify in kbps the amount of bandwidth to allocate for business-critical traffic.

Answer: C, D

Explanation:
You are prompted to enter the percentages for each class. After you enter the numbers, Cisco SDM will automatically calculate the best-effort class and the bandwidth requirements for each class.



QoS Policy Generation

SDM will create a QoS policy to provide quality of service to 2 types of traffic.
1) Real-Time Traffic :- SDM will create 2 QoS classes to handle VoIP and voice signaling packets.

2) Business-Critical Traffic :- SDM will create 3 QoS classes to handle packets which are important for a typical corporate environment. Some of the protocols included in this traffic category are citrix, sqlnet, notes,LDAP, and secure LDAP. Routing protocos in this category include BGP, EGP, EIGRP AND RIP.

Bandwidth Allocation

Type of Traffic	Bandwidth in %	kbps value
Real Time (Voice, Video) :	50	50000
Business-Critical :	25	25000
Best-Effort :	25	25000
Total Bandwidth :	100	100000

QUESTION 141
The Certkiller network administrator uses the SDM to manage the Cisco routers within the network. Which two statements are correct about the SDM QOS wizard? (Select two)

A. The SDM wizard can detect incorrect configurations.
B. The SDM wizard can propose fixes.
C. The SDM wizard must be run on the local router.
D. The SDM QoS configuration is not displayed on the screen, but automatically uploaded to the RAM.

Answer: A, B

Explanation:
Cisco Router and Security Device Manager (SDM) allows you to easily configure routing, security, and QoS services on Cisco routers while helping to enable proactive management through performance monitoring. Whether you are deploying a new router or installing Cisco SDM on an existing router, you can now remotely configure and monitor these routers without using the Cisco IOS software CLI. The Cisco SDM GUI aids nonexpert users of Cisco IOS software in day-to-day operations, provides easy-to-use smart wizards, automates router security management, and assists you through comprehensive online help and tutorials.

QUESTION 142
A new Certkiller router has been configured using the "auto qos" configuration command. What action does this command perform?

A. It uses NBAR to detect network applications and protocols as they leave an interface.
B. It allows marked traffic to enter and leave the interface unchanged.
C. It creates and installs the QoS class maps and policy maps.
D. It initializes the discovery of traffic patterns on the network.
E. None of the above

Answer: C

Explanation:
The auto qos command generates Cisco AutoQoS for the Enterprise templates on the basis of the data collected during the autodiscovery phase and then installs the templates on the interface. These templates are then used to create class maps and policy maps for use on your network. After they are created, the class maps and policy maps are also installed on the interface.

QUESTION 143
Auto QOS has been configured on a number routers in the Certkiller Frame Relay network. Which statement is true about the configuration of AutoQoS on a Frame Relay interface?

A. AutoQoS can be configured from a different subinterface if the DLCI is already assigned to one subinterface.
B. AutoQoS can be configured on a Frame Relay DLCI only if a map class is attached to the DLCI.
C. Multilink PPP (MLP) over Frame Relay must be manually configured on low speed DLCIs.
D. For low-speed Frame Relay DLCIs with Frame Relay-to-ATM Interworking, the AutoQoS cannot be configured if a virtual template is already configured for the DLCI.
E. None of the above

Answer: D

Explanation:
Frame Relay DLCI Restrictions
1. Cisco AutoQoS has the following restrictions in Frame Relay environment:
2. Cisco AutoQoS cannot be configured on a Frame Relay DLCI if a map class is attached to the DLCI.
3. If a Frame Relay DLCI is already assigned to one subinterface, Cisco AutoQoS VoIP cannot be configured from a different subinterface.
4. For low-speed Frame Relay DLCIs configured for use on Frame Relay-to-ATM interworking, MLP over Frame Relay is configured automatically. The subinterface must have an IP address.
5. When MLP over Frame Relay is configured, this IP address is removed and put on the MLP bundle. Cisco AutoQoS must also be configured on the ATM side of the network.
6. For low-speed Frame Relay DLCIs with Frame Relay-to-ATM interworking, Cisco AutoQoS cannot be configured if a virtual template is already configured for the DLCI.

QUESTION 144
Auto QOS has been configured on a number of new Certkiller devices. What accurately describes the usage of a Cisco AutoQoS command?

A. On Catalyst switches, the "show auto discovery qos" command is used to display the data collected during the Auto-Discovery phase.
B. On Cisco routers, the "show mls qos maps" command is used to verify the CoS-to-DSCP maps for egress packet queuing.
C. On Cisco routers, the "show auto qos" command is used to display the AutoQoS interface templates, policy maps, class maps, and ACLs.
D. On Catalyst switches, the "show auto qos" command is used to display packet statistics of all classes that are configured for all service policies.
E. None of the above

Answer: C

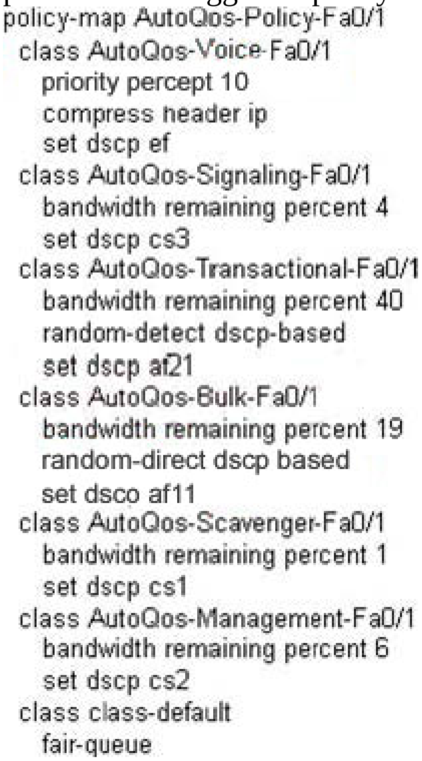
Explanation:
Syntax: show auto qos[interface interfacetype]

Displays the Cisco AutoQoS templates (policy maps, class maps, and ACLs) created for a specific interface or all interfaces

---

QUESTION 145

AutoQoS Discovery has run on the Certkiller network for several days and has produced the suggested policy shown in the exhibit below:



```
policy-map AutoQos-Policy-Fa0/1
  class AutoQos-Voice-Fa0/1
    priority percept 10
    compress header ip
    set dscp ef
  class AutoQos-Signaling-Fa0/1
    bandwidth remaining percent 4
    set dscp cs3
  class AutoQos-Transactional-Fa0/1
    bandwidth remaining percent 40
    random-detect dscp-based
    set dscp af21
  class AutoQos-Bulk-Fa0/1
    bandwidth remaining percent 19
    random-direct dscp based
    set dsco af11
  class AutoQos-Scavenger-Fa0/1
    bandwidth remaining percent 1
    set dscp cs1
  class AutoQos-Management-Fa0/1
    bandwidth remaining percent 6
    set dscp cs2
  class class-default
    fair-queue
```

Certkiller wishes to 1) allow more bandwidth for browser-type traffic, and 2) to allow greater bandwidth for file transfers because they expect an upcoming surge in movie uploads and downloads. Which two statements would you replace to best accomplish those goals without sacrificing voice quality? (Select two)

A. In class AutoQoS-Bulk-Fa0/1, replace bandwidth remaining percent 19 with bandwidth remaining percent 25.
B. In class class-default, replace fair-queue with bandwidth remaining percent 50.
C. In class AutoQoS-Signaling- Fa0/1, replace bandwidth remaining percent 4 with bandwidth remaining percent 1.
D. In class AutoQoS-Scavenger-Fa0/1, replace bandwidth remaining percent 1 with bandwidth remaining percent 10.
E. In class AutoQoS-Transactional-Fa0/1, replace bandwidth remaining percent 40 with bandwidth remaining percent 20.
F. In class AutoQoS-Transactional-Fa0/1, replace bandwidth remaining percent 40 with bandwidth remaining percent 30.

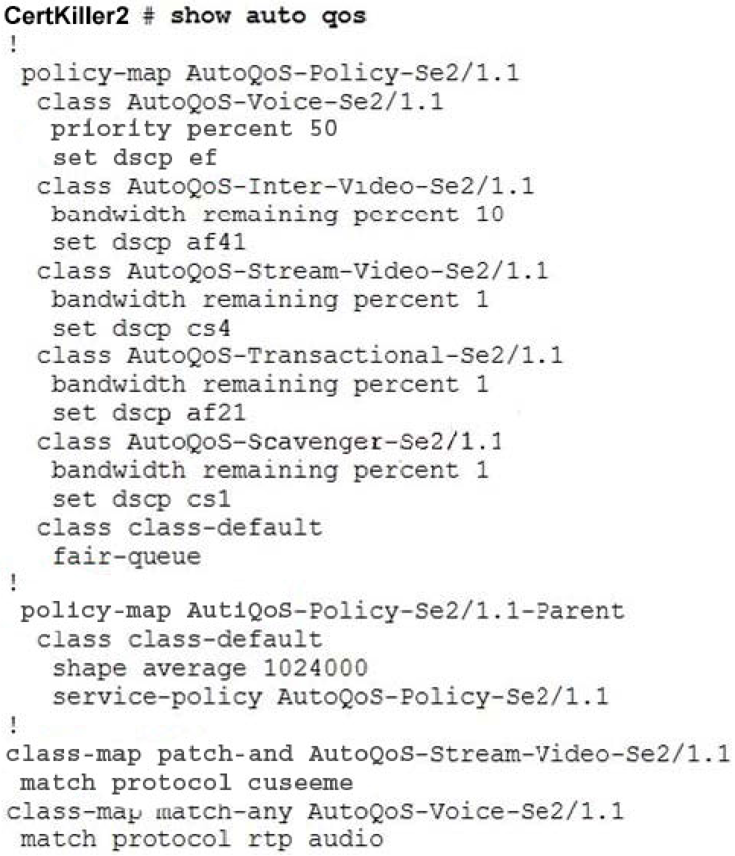
Answer: A, F

Explanation:

The bandwidth remaining percent command is used to allocate the amount of guaranteed bandwidth based on a relative percentage of available bandwidth. When the bandwidth remaining percent command is configured, hard bandwidth guarantees may not be provided, and only relative per-class bandwidths are assured. That is, class bandwidths are always proportionate to the specified percentages of the interface bandwidth. When the link bandwidth is fixed, class bandwidth guarantees are in proportion to the configured percentages. If the link bandwidth is unknown or variable, class bandwidth guarantees in kilobits per second cannot be computed.

QUESTION 146

The following output was seen on a Certkiller router:



```
CertKiller2 # show auto qos
!
 policy-map AutoQoS-Policy-Se2/1.1
  class AutoQoS-Voice-Se2/1.1
   priority percent 50
   set dscp ef
  class AutoQoS-Inter-Video-Se2/1.1
   bandwidth remaining percent 10
   set dscp af41
  class AutoQoS-Stream-Video-Se2/1.1
   bandwidth remaining percent 1
   set dscp cs4
  class AutoQoS-Transactional-Se2/1.1
   bandwidth remaining percent 1
   set dscp af21
  class AutoQoS-Scavenger-Se2/1.1
   bandwidth remaining percent 1
   set dscp cs1
  class class-default
   fair-queue
!
 policy-map AutiQoS-Policy-Se2/1.1-Parent
  class class-default
   shape average 1024000
   service-policy AutoQoS-Policy-Se2/1.1
!
class-map patch-and AutoQoS-Stream-Video-Se2/1.1
 match protocol cuseeme
class-map match-any AutoQoS-Voice-Se2/1.1
 match protocol rtp audio
```

Based on the output shown above, which statement is true?

A. Seven classes were created from AutoQoS.
B. Audio will be policed into the remaining 10 percent of bandwidth.
C. The CUSeeMe protocol will have its DSCP set to cs4.
D. Any traffic not specified will be in the remaining 1 percent of bandwidth.
E. None of the above.

Answer: C

QUESTION 147

You need to configure auto QOS on a new Certkiller router. What is required when configuring AutoQoS on a Cisco router?

A. If a QoS policy exists on an interface, the interface needs to be enabled with CEF.
B. No QoS policies can exist on the interface.
C. The SNMP community string "AutoQoS" needs to be configured with "read" permission only.
D. CEF must be disabled, unless a current QOS policy exists.
E. None of the above.

Answer: B

Explanation:
Before configuring Cisco AutoQoS, these prerequisites must be met:
* You must ensure that no QoS policies (service policies) are attached to the interface. Cisco AutoQoS cannot be configured if a QoS policy is attached to the interface.
* Cisco Express Forwarding (CEF) must be enabled. Cisco AutoQoS uses NBAR to identify various applications and traffic types, and CEF is a prerequisite for NBAR.
* Cisco AutoQoS classifies links as either low speed or high speed depending on the link bandwidth. Remember that on a serial interface, if the default bandwidth is not specified, it is 1.544 Mbps. Therefore, it is important that the correct bandwidth be specified on the interface or subinterface where Cisco AutoQoS is to be enabled:
- For all interfaces or subinterfaces, be sure to properly configure the bandwidth by using the bandwidth command. The amount of bandwidth that is allocated should be based on the link speed of the interface.
- If the interface or subinterface has a link speed of 768 kbps or lower, an IP address must be configured on the interface or subinterface using the ip address command. By default, Cisco AutoQoS enables MLP and copies the configured IP address to the multilink bundle interface.

QUESTION 148
You need to configure the auto QOS feature on a new Certkiller router. Before AutoQoS can be configured, what two prerequisites must be met? (Select two)

A. The SNMP community string "AutoQoS" should have "read" permission only.
B. The SNMP community string "AutoQoS" should have "write" permission.
C. Ensure that no QoS policies are attached to the interface.
D. The device must be reloaded and Remote Monitoring (RMON) threshold warning messages must be addressed.
E. The SNMP traps (monitored events) and the SNMP server must be enabled.
F. CEF must be enabled on the interface.

Answer: C, F

Explanation:
Before configuring Cisco AutoQoS, these prerequisites must be met:
* You must ensure that no QoS policies (service policies) are attached to the interface. Cisco AutoQoS cannot be configured if a QoS policy is attached to the interface.

* Cisco Express Forwarding (CEF) must be enabled. Cisco AutoQoS uses NBAR to identify various applications and traffic types, and CEF is a prerequisite for NBAR.
* Cisco AutoQoS classifies links as either low speed or high speed depending on the link bandwidth. Remember that on a serial interface, if the default bandwidth is not specified, it is 1.544 Mbps. Therefore, it is important that the correct bandwidth be specified on the interface or subinterface where Cisco AutoQoS is to be enabled:
- For all interfaces or subinterfaces, be sure to properly configure the bandwidth by using the bandwidth command. The amount of bandwidth that is allocated should be based on the link speed of the interface.
- If the interface or subinterface has a link speed of 768 kbps or lower, an IP address must be configured on the interface or subinterface using the ip address command. By default, Cisco AutoQoS enables MLP and copies the configured IP address to the multilink bundle interface.
* Cisco AutoQoS is supported only on these interfaces and PVCs:
* ATM PVCs
* Serial interfaces with PPP or HDLC
* Frame Relay DLCIs (point-to-point subinterfaces only, because Cisco AutoQoS does not support Frame Relay multipoint interfaces)
* A configuration template generated by configuring Cisco AutoQoS on an interface or PVC can be tuned manually (via CLI configuration) if desired.
* To include SNMP traps (monitored events), SNMP support must be enabled on the router. Cisco AutoQoS SNMP traps are delivered only when an SNMP server is used in conjunction with Cisco AutoQoS and the router is familiar with how to reach the SNMP server.
* The SNMP community string "AutoQoS" should have write permission.
* If the device is reloaded with the saved configuration after configuring Cisco AutoQoS and saving the configuration to NVRAM, some warning messages may be generated by Remote Monitoring (RMON) threshold commands. These warning messages can be ignored. (To avoid further warning messages, save the configuration to NVRAM again without making any changes to the QoS configuration.)

QUESTION 149
You want to use the Auto QoS feature on a new Certkiller VOIP router. What two steps need to be taken to deploy AutoQoS for Enterprise on routers? (Select two)

A. Profile the traffic with Auto-Discovery.
B. Generate and deploy MQC-based QoS policies.
C. Enable the AutoQoS VoIP for voice traffic.
D. Provide visibility into the classes of service deployed using system logging and SNMP traps.
E. Determine the WAN settings for fragmentation, compression, encapsulation, and Frame Relay-ATM inter-working.

Answer: A, B

Explanation:

The first release of Cisco AutoQoS provides the necessary AutoQoS VoIP feature to automate QoS settings for VoIP deployments. This feature automatically generates interface configurations, policy maps, class maps, and ACLs. Cisco AutoQoS VoIP will automatically employ Cisco NBAR to classify voice traffic and mark the traffic with the appropriate DSCP value. AutoQoS VoIP can be instructed to rely on, or trust, the DSCP markings previously applied to the packets.
In general, an MQC configuration can be divided into four sections:
ACLs: Matching the traffic that needs QoS. These matches can be based on IP precedence bits, IP differentiated services code point (DSCP), IP addresses, and TCP/IP ports.
Class maps: Classifying the traffic according to its importance.
Policy maps: Applying parameters such as bandwidth, queuing mechanisms, or priorities to the classified traffic.
Service policy: Applied to the interface.

QUESTION 150
Auto QoS has been implemented throughout the Certkiller network. Which two steps are executed in the deployment of Cisco AutoQoS for Enterprises? (Select two)

A. QoS policy templates are generated and installed on the interface.
B. RTP is used to generate the policy.
C. The customer uses SNMP statistics to create the policy.
D. Auto-discovery is used to determine what traffic is on the interface.
E. The auto-generated policy is manually optimized before implementation.
F. LLQ, cRTP, and LFI are used to automatically discover the policy.

Answer: A, D

Explanation:
The Auto-Discovery phase uses NBAR to detect network applications and protocols as they leave an interface, collect data from the offered traffic, and perform statistical analysis. The information collected will be used to build the AutoQoS templates
The auto qos command generates Cisco AutoQoS for the Enterprise templates on the basis of the data collected during the autodiscovery phase and then installs the templates on the interface. These templates are then used to create class maps and policy maps for use on your network. After they are created, the class maps and policy maps are also installed on the interface.

QUESTION 151
The AutoQoS feature has been enabled on a Certkiller router. Cisco AutoQoS takes the interface type and bandwidth into consideration when configuring which three QoS features? (Select three)

A. Routing protocol
B. Voice compression methodology
C. LFI

D. LLQ
E. Compressed RTP
F. Trust boundary

Answer: C, D, E

Explanation:
AutoQoS takes the interface type and bandwidth into consideration when implementing these QoS features:
1. LLQ: The LLQ (specifically, PQ) is applied to the voice packets to meet the latency requirements.
2. cRTP: With cRTP, the 40-byte IP header of the voice packet is reduced to 2 or 4 bytes (without or with cyclic redundancy check [CRC]), reducing voice bandwidth requirements. cRTP must be applied at both ends of a network link.
3. LFI: LFI is used to reduce the jitter of voice packets by preventing voice packets from being delayed behind large data packets in a queue. LFI must be applied at both ends of a network link.

QUESTION 152
You need to determine the most secure authentication method for use in the Certkiller wireless network. Which WLAN authentication security statement is true?

A. Cisco LEAP is more secure than the IEEE 802.11i standard because Cisco LEAP is proprietary.
B. Cisco LEAP is more secure that WPA but not as secure as WEP.
C. The IEEE 802.11i standard is a version of Cisco LEAP.
D. The IEEE 802.11i standard is more secure than LEAP but not as secure as WPA.
E. The IEEE 802.11i standard is more secure than WPA but not as secure as LEAP.
F. Cisco LEAP is more secure than WEP but not as secure as WPA.
G. None of the above.

Answer: F

Explanation:
LEAP is a Cisco proprietary wireless encryption technique offering dynamic WEP keys and mutual authentication (between a wireless client and a RADIUS server). LEAP allows for clients to reauthenticate frequently.
LEAP made WLANs more secure, but the encryption was not strong enough. New attacks were showed that improvements were required. An interim solution called Wi-Fi Protected Access (WPA) provides standardized improved encryption and stronger user-based authentication (PEAP, EAP, and EAP-FAST).

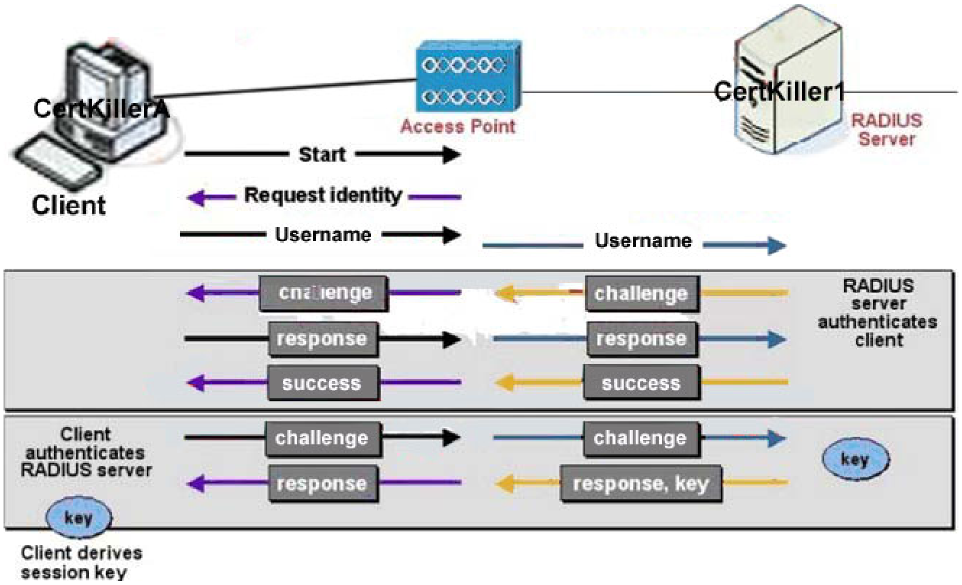
QUESTION 153
You want to increase the security of the Certkiller wireless network. Which two wireless security statements are true? (Select two)

A. The 802.1x standard provides encryption services for wireless clients.
B. The AES (symmetric block cipher) is specified in the IEEE 802.11i specification.
C. MIC protects against man-in-the-middle and replay attacks.
D. A TACACS+ server is required to implement 802.1x.
E. The IEEE 802.11i specification uses RC4 as its encryption mechanism.
F. WPA requires CKIP and AES as encryption methods.

Answer: B, C

Explanation:
Encryption is the mechanism that is used to protect the data flowing over the actual data pathway. A common example of encryption is Triple-Data Encryption Standard (3DES), used in many Cisco wired network environments. Typically, a data connection between two devices is encrypted after the user is authenticated and authorized to use the resource.
Wi-Fi WPA2, or IEEE 802.11i, is a security standard that was ratified in June 2004. This standard encompasses the prior WPA features plus a number of security improvements. 802.11i standardized on a new form of encryption for 802.11 wireless-AES, called "WPA2." AES is recognized as a stronger security algorithm than the RC4 stream cipher used with WEP, although AES is undeniably more processor-intensive. Hardware updates will be required to move to AES encryption while maintaining comparable throughput.
AES uses a 128-bit block cipher and requires newer or current radio cards on both access points and clients to eliminate throughput reduction stemming from an increase in computational load for encryption and decryption. If you are planning to implement AES on existing equipment, check Cisco.com documentation to verify whether your current hardware supports AES or whether upgrades are required.
Message integrity check (MIC) is a mechanism for protecting the wireless system from inductive attacks, which seek to induce the system to send either key data or a predictable response that can be analyzed to derive the WEP key.

QUESTION 154
A portion of the Certkiller wireless network is shown in the following exhibit:



Based on the diagram shown above, what variation of the 802.1x Extensible Authentication Protocol (EAP) uses this authentication process?

A. EAP-TLS
B. LEAP
C. PEAP
D. EAP-FAST
E. None of the above

Answer: B

Explanation:
LEAP is a Cisco proprietary wireless encryption technique offering dynamic WEP keys and mutual authentication (between a wireless client and a RADIUS server). LEAP allows for clients to reauthenticate frequently.
LEAP made WLANs more secure, but the encryption was not strong enough. New attacks were showed that improvements were required. An interim solution called Wi-Fi Protected Access (WPA) provides standardized improved encryption and stronger user-based authentication (PEAP, EAP, and EAP-FAST).

QUESTION 155
Certkiller uses EAP to authenticate users on the network. What are three valid Extensible Authentication Protocol (EAP) types? (Select three)

A. EAP-AES
B. EAP-FAST
C. WEP
D. LEAP
E. WEAP
F. EAP-TLS

Answer: B, D, F

Explanation:
1. Lightweight Extensible Authentication Protocol (LEAP) is an 802.1x-compliant authentication mechanism developed by Cisco and made available on Cisco NICs and NICs from other vendors.
2.
Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a client-server security architecture that encrypts EAP transactions with a TLS tunnel. Although it is similar to Protected Extensible Authentication Protocol (PEAP) in this respect, it differs significantly in that EAP-FAST tunnel establishment is based on strong secrets called the "protected access credential" (PAC) that are unique to users.
3. Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) uses certificates to authenticate both the server (network) and client.
4. PEAP is a "protected" authentication mechanism that uses a certificate to encrypt the authentication exchange between the client and the EAP server. The authentication exchange may be either Generic Token Card (GTC) or Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2).

QUESTION 156
The Certkiller wireless network has been upgraded to support WPA2. What are two features of the Wi-Fi Protected Access 2 (WPA2) standard? (Select two)

A. Reduced CPU usage over WPA
B. 3DES Encryption
C. AES Encryption
D. RC4
E. 802.1X Authentication

Answer: C, E

Explanation:
Wi-Fi WPA2, or IEEE 802.11i, is a security standard that was ratified in June 2004. This standard encompasses the prior WPA features plus a number of security improvements. 802.11i standardized on a new form of encryption for 802.11 wireless-AES, called "WPA2." AES is recognized as a stronger security algorithm than the RC4 stream cipher used with WEP, although AES is undeniably more processor-intensive. Hardware updates will be required to move to AES encryption while maintaining comparable throughput.
AES uses a 128-bit block cipher and requires newer or current radio cards on both access points and clients to eliminate throughput reduction stemming from an increase in computational load for encryption and decryption. If you are planning to implement AES on existing equipment, check Cisco.com documentation to verify whether your current hardware supports AES or whether upgrades are required.

QUESTION 157
EAP is being used to authenticate Certkiller users. What three statements are true about the various deployments of the 802.1x Extensible Authentication Protocol (EAP)? (Select three)

A. EAP-FAST has the ability to tie login with non-Microsoft user databases.
B. LEAP does not support multiple operating systems.
C. LEAP supports Layer 3 roaming.
D. PEAP supports one-time passwords.
E. PEAP does not work with WPA.
F. EAP-TLS supports static passwords.

Answer: A, C, D

Explanation:
1. Lightweight Extensible Authentication Protocol (LEAP) is an 802.1x-compliant authentication mechanism developed by Cisco and made available on Cisco NICs and NICs from other vendors.
2. Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a client-server security architecture that encrypts EAP transactions with a TLS tunnel. Although it is similar to Protected Extensible Authentication Protocol (PEAP) in this respect, it differs significantly in that EAP-FAST tunnel establishment is based on strong secrets called the "protected access credential" (PAC) that are unique to users.
3. Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) uses certificates to authenticate both the server (network) and client.
4. PEAP is a "protected" authentication mechanism that uses a certificate to encrypt the authentication exchange between the client and the EAP server. The authentication exchange may be either Generic Token Card (GTC) or Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2).

QUESTION 158
A new Certkiller user has been added to the wireless LAN. How can a remote wireless client obtain its Service Set Identifier (SSID)?

A. If a client does not have a SSID configured; it can obtain it from the AP.
B. If a client has the incorrect SSID configured; it can obtain it from the AP.
C. A client can access a centralized server to obtain the SSID.
D. A client must have the SSID entered manually in its configuration.
E. None of the above.

Answer: A

Explanation:
The SSID is a network-naming scheme and configurable parameter that both the client and the access point must share. If the client does not have the proper SSID, it is unable

to associate with the access point and would have no access to the network. The SSID feature serves to logically segment the users and access points that form part of a wireless subsystem. Under 802.11 specifications, an access point may advertise, or broadcast, its SSID. During the association process, any 802.11 wireless client with a null string (no value entered in the SSID field) requests that the access point broadcast its SSID. If the access point is so configured, it sends the SSID to the client. The client then uses this SSID to associate with the access point. For these reasons, the SSID should not be considered a security feature of WLAN products.

QUESTION 159
The WEP security feature has been implemented throughout the Certkiller wireless network. Which two statements about the Wired Equivalent Privacy (WEP) encryption mechanism are true? (Select two)

A. WEPv2 offers improved encryption by replacing the RC4 encryption mechanism with the AES (symmetric block cipher) mechanism.
B. WEP security provides only one-way authentication.
C. The two methods of authentication using the WEP encryption are open and shared key.
D. WEP can provide stronger authentication through the use of LEAP, PEAP, or EAP-FAST.
E. WEP is a scalable encryption solution that uses static keys for authentication.
F. The 802.11 standard defines WEP security using 128-bit keys.

Answer: B, C

Explanation:
Basic 802.11 WEP security is designed to guard against the threat to network security from unauthorized 802.11 devices outside the LAN. Any device with a valid WEP key is considered a legitimate and authorized user. If the WEP key was obtained through hardware loss, theft, or a wireless security exploit, the network and wireless users are rendered vulnerable, and keys must be changed. Note that persistent WEP keys may be assigned to a client adapter (keys stored in nonvolatile memory on the card itself) via most WLAN client utilities.
Basic 802.11 WEP security provides only one-way authentication. The client is authenticated with the access point (the WEP key is checked), but not vice versa. The client has no way of knowing whether the access point is a legitimate part of the WLAN or a rogue device (that uses same WEP key).

QUESTION 160
EAP is being used to authenticate Certkiller users. Which 802.1x Extensible Authentication Protocol (EAP) type supports authentication using digital certificates?

A. EAP-FAST
B. WPA

C. EAP-TLS
D. LEAP
E. None of the above

Answer: C

Explanation:
Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) uses certificates to authenticate both the server (network) and client.

QUESTION 161
The Certkiller wireless network utilizes both WPA and WPA2. Which two statements below are true about the Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access version 2 (WPA2) security solutions? (Select two)

A. Both WPA and WPA2 address all known Wired Equivalent Privacy (WEP) vulnerabilities in the IEEE 802.11i security implementation.
B. Both WPA and WPA2 require authentication support via IEEE 802.1X and Pre-Shared Key (PSK).
C. WPA requires encryption support via Temporal Key Integrity Protocol (CKIP). WPA2 provides encryption support via (symmetric block cipher) AES-CCMP.
D. WPA is supported on client devices only. WPA2 is supported on both access point (AP) and client devices.
E. WPA provides only a standard for authentication. WPA2 provides a standard for authentication and encryption.

Answer: B, C

Explanation:
1. WPA
WPA provides a standard for authentication and encryption of WLANs that is intended to solve known security problems up to and including 2003. These problems include the well-publicized AirSnort and man-in-the-middle WLAN attacks. The WPA mechanisms were designed to be implemented by vendors in current hardware, meaning that users should be able to implement WPA on their current systems with only a firmware or software modification.
WPA has these elements:
1. A mechanism for authenticated key management, where the user is first authenticated, and then a master key is derived at server and client. This master key is used to generate the actual keys used in encrypting the user session. The master key is not directly used.
2. Key validation mechanisms are in place for both unicast and broadcast keys.
3. CKIP is used, which for WPA includes both per-packet keying and MIC.
4. The IV is expanded from 24 to 48 bits, which prevents "collisions" or reuse of the same vector, which can be used in exploits to attempt to derive an encryption key. IV collisions are one of the primary mechanisms used by tools such as AirSnort.
2. WPA2

WPA2 is a new security standard developed by the IEEE 802.11i task group. The Robust Security Network (RSN) specification is the IEEE equivalent of WPA2. WPA2 generally uses AES block ciphers with Cipher Block Chaining Message Authentication Code Protocol (CCMP) for encryption and supports CKIP:
* Generally uses 802.1x authentication methods-supports preshared keys
* Comparable to WPA-the same authentication architecture, key distribution, and key renewal
* Supports Proactive Key Caching (PKC) and preauthentication
* IDS added to identify and protect against attacks

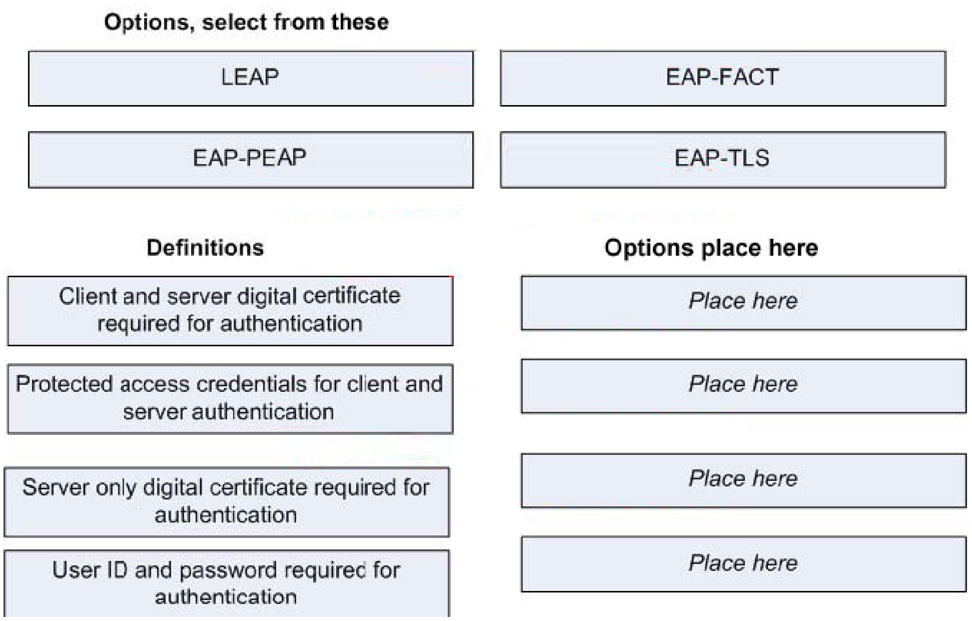
QUESTION 162
You want to implement a new security strategy for the Certkiller wireless LAN.
Which two statements best describe enhanced wireless security encryption? (Select two)

A. CKIP protects RC4 encryption keys.
B. WPA requires CKIP encryption, whereas WPA2 supports AES encryption.
C. CKIP encryption is more processor intensive than AES encryption is.
D. WPA requires AES encryption, whereas WPA2 supports CKIP encryption.
E. CKIP and CKIP protect AES encryption keys.

Answer: A, B

Explanation:
Temporal Key Integrity Protocol (CKIP) protects the WEP key from exploits that seek to derive the key using packet comparison. Message integrity check (MIC) is a mechanism for protecting the wireless system from inductive attacks, which seek to induce the system to send either key data or a predictable response that can be analyzed to derive the WEP key.
CKIP and MIC are both elements of the WPA standard, which is intended to secure a system against all known WEP key vulnerabilities. Note that Cisco implemented a prestandard version of CKIP and MIC in late 2001, known as CKIP and CMIC, before WPA was available for customers. Current Cisco equipment supports prior CKIP and CMIC and the Wi-Fi WPA and WPA2 standards as well. Different algorithms are used in CKIP and CKIP, making them imcompatible between wireless client and access point. Both the access point and the client must use the same protocol. Although access points can be configured to support both security protocols in a mixed environment, it is always recommended that you use CKIP.

QUESTION 163
DRAG DROP
Drag each wireless EAP authentication protocol definition on the left to the appropriate box on the right:

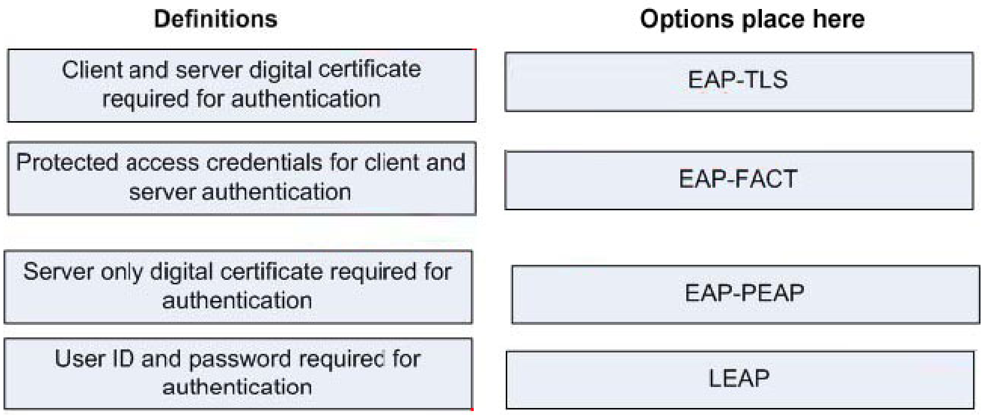


Options, select from these

LEAP	EAP-FACT
EAP-PEAP	EAP-TLS

Definitions	Options place here
Client and server digital certificate required for authentication	Place here
Protected access credentials for client and server authentication	Place here
Server only digital certificate required for authentication	Place here
User ID and password required for authentication	Place here

Answer:



Definitions	Options place here
Client and server digital certificate required for authentication	EAP-TLS
Protected access credentials for client and server authentication	EAP-FACT
Server only digital certificate required for authentication	EAP-PEAP
User ID and password required for authentication	LEAP

Explanation:

1. Lightweight Extensible Authentication Protocol (LEAP) is an 802.1x-compliant authentication mechanism developed by Cisco and made available on Cisco NICs and NICs from other vendors.
2. Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a client-server security architecture that encrypts EAP transactions with a TLS tunnel. Although it is similar to Protected Extensible Authentication Protocol (PEAP) in this respect, it differs significantly in that EAP-FAST tunnel establishment is based on strong secrets called the "protected access credential" (PAC) that are unique to users.
3. Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) uses certificates to authenticate both the server (network) and client.
4. PEAP is a "protected" authentication mechanism that uses a certificate to encrypt the authentication exchange between the client and the EAP server. The authentication exchange may be either Generic Token Card (GTC) or Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2).

QUESTION 164

You need to implement an authentication method for the Certkiller wireless network. Which two statements about the open and shared key wireless-authentication methods are true? (Select two)

A. If the WEP keys do not match using the open authentication method, the client will still be able to authenticate, associate, and transfer data.
B. If the WEP keys do not match using the open authentication method, the client will not authenticate, associate, and transfer data.
C. If the WEP keys do not match using the open authentication method, the client will still be able to authenticate and associate, but will not transfer data.
D. Shared key authentication is considered less secure than open authentication.
E. Shared key authentication is considered more secure than open authentication.

Answer: C, D

Explanation:
The 802.11 standard defines a type of security: WEP using 40-bit keys. This method uses a wireless client and access point sharing static WEP keys. This key is checked during the authentication process. If the client WEP key does not match that of the access point, the client is not allowed to associate and is unable to connect to the network.
Shared key authentication is considered less secure than open authentication because of the challenge text packet. Because this packet is sent unencrypted and then returned as an encrypted packet, it may be possible to capture both packets and determine the stream cipher.

QUESTION 165

The Certkiller network administrator needs to implement a management system for the wireless network. Which three devices are used by the Cisco Wireless Control System (WCS) for wireless management? (Select three)

A. WLAN Solution Engine (WLSE)
B. Lightweight access point (AP)
C. Cisco Wireless Control System (WCS)
D. Autonomous access point (AP)
E. WLAN controllers
F. Cisco Wireless Location Appliance

Answer: B, E, F

Explanation:
Cisco WCS is supported under Microsoft Windows 2000, Windows 2003, and Red Hat Enterprise Linux ES v.3 servers as either a normal application or a service. The Cisco WLAN solution consists of Cisco Wireless LAN Controllers and their associated lightweight access points controlled by the operating system, all concurrently managed

by any or all of the operating system user interfaces. One of them is Cisco WCS. Cisco Wireless Location Appliance can be used to improve the functionality of Cisco WCS Location. Cisco Wireless Location Appliance performs location computations based on the RSSI information received from Cisco Wireless LAN Controllers. The Cisco Wireless LAN Controllers that gather the RSSI information must be associated with the Cisco Wireless Location Appliance. The Cisco 2700 Series Location Appliance is a Cisco Wireless Location Appliance that can be used.

QUESTION 166

You need to increase the security of the Certkiller wireless network. What are three security problems with Wi-Fi Protected Access (WPA)? (Select three)

A. WPA is susceptible to a DoS attack when it receives two packets in quick succession with bad MICs, forcing the AP to shut down the entire Basic Service Set (BSS) for one minute.
B. WPA uses CKIP, which uses the same base encryption algorithm as WEP
C. WPA is susceptible to a security weakness when preshared keys are used.
D. WPA is based on the outdated IEEE 802.11i standard.
E. WPA uses RSN, which uses the same base encryption algorithm as RC4.
F. WPA requires a hardware upgrade that may not be supported by all vendors.

Answer: A, B, C

Explanation:
WPA is the Wi-Fi Alliance standards-based mechanism to create secure and interoperable WLAN networks. WPA provides a mechanism to authenticate keys for use in 802.11 environments as well as providing enhancements to WEP encryption to increase the robustness of the security protocol.
The Temporal Key Integrity Protocol (CKIP) used with WPA is an enhancement to the basic security mechanism defined by 802.11 WEP (RC4 encryption). Note that CKIP is a "wrapper" around the WEP and RC4 encryption mechanism. WPA relies on RC4 instead of 3DES, AES, or another encryption algorithm.
WPA is susceptible to a new type of DoS attack based on countermeasure techniques employed by MIC. If an access point running WPA receives two packets in quick succession with bad MICs, it shuts down the entire basic service set (BSS) for one minute. WPA is susceptible to a recently discovered weakness when preshared keys are used instead of 802.11i or EAP; the use of a small, noncomplex passphrase can allow an attacker to perform a dictionary attack on captured traffic and recover the passphrase.

QUESTION 167

The Cisco WCS is used in the Certkiller wireless network. Which two Cisco Wireless Control System (WCS) statements are true? (Select two)

A. WCS uses the CDP protocol to communicate with the controllers.
B. The WCS Base version provides on-demand location of rogue access points and clients to within 33 feet (10 meters).

C. WCS adds a graphical view of multiple Cisco Wireless LAN controllers and managed access points.
D. WCS includes a network management tool which is similar to a site survey tool.
E. The WCS Base version includes all the features of the WCS Location version as well as additional enhancements.

Answer: C, D

Explanation:
Cisco WCS is a Cisco WLAN solution network-management tool that adds to the capabilities of the web user interface and CLI, moving from individual controllers to a network of controllers. Cisco WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points. The Cisco WCS user interface enables operators to control all permitted Cisco WLAN solution configuration, monitoring, and control functions through Microsoft Internet Explorer 6.0 or later. Operator permissions are defined by the administrator using the Cisco WCS user interface Administration menu, which enables the administrator to manage user accounts and schedule periodic maintenance tasks. Cisco WCS simplifies controller configuration and monitoring while reducing data-entry errors with the Cisco Wireless LAN Controller autodiscovery algorithm. Cisco WCS uses SNMP to communicate with the controllers.

QUESTION 168
A Cisco 2700 is being utilized in the Certkiller wireless network. Which statement best describes the Cisco 2700 Location Appliance collection of location information for wireless devices?

A. An AP collects RSSI information which is forwarded to wireless controllers through LWAPP. Wireless controllers forward aggregated RSSI to the location appliance through SNMP.
B. The Cisco WLAN controllers bypass the received signal strength indication (RSSI) information from all Wi-Fi devices to the Cisco Wireless Location Appliance through LWAPP.
C. All Wi-Fi devices on the WLAN send directly received signal strength indication (RSSI) information to the Cisco Wireless Location Appliance through SNMP.
D. The APs collect received signal strength indication (RSSI) information from all Wi-Fi devices and forward the information to the Cisco Wireless Location Appliance through the LWAPP.
E. None of the above.

Answer: A

Explanation:
Cisco Wireless Location Appliance can be used to improve the functionality of Cisco WCS Location. Cisco Wireless Location Appliance performs location computations

based on the RSSI information received from Cisco Wireless LAN Controllers. The Cisco Wireless LAN Controllers that gather the RSSI information must be associated with the Cisco Wireless Location Appliance. The Cisco 2700 Series Location Appliance is a Cisco Wireless Location Appliance that can be used.

QUESTION 169

Cisco's WLSE is being used to manage the Certkiller wireless network. Which two statements regarding the Wireless LAN Solution Engine (WLSE) are true? (Select two)

A. WLSE can locate rogue APs and automatically shut them down.
B. WLSE configuration is done using the command line interface (CLI) or a WEB based template.
C. To support fault and policy reporting, the WLSE requires a Wireless Control System (WCS).
D. When WLSE detects an AP failure, it automatically increases the power and cell coverage of nearby APs.
E. WLSE requires the 2700 location appliance to offer location tracking.

Answer: A, D

Explanation:
CiscoWorks WLSE is a systems-level solution for managing the entire Cisco Aironet WLAN infrastructure based on autonomous access points. The RF and device-management features of CiscoWorks WLSE simplify the everyday operation of WLANs, helping to ensure smooth deployment of security and network availability while reducing deployment and operating expense. CiscoWorks WLSE operates by gathering fault, performance, and configuration information about Cisco devices that it discovers in the network. The access points, WDS, switches, and routers must be properly configured with Cisco Discovery Protocol (CDP) and Simple Network Management Protocol (SNMP) to provide information to CiscoWorks WLSE for the access point discovery process. After devices are discovered, you decide which devices to manage with CiscoWorks WLSE. CiscoWorks WLSE is a core component of the WLAN autonomous access-point
CiscoWorks WLSE can detect that an access point has failed. It compensates for the loss by automatically increasing the power and cell coverage of nearby access points. The Self Healing feature minimizes the outage impact to wireless client devices and maximizes the availability of wireless applications. Self Healing also recalculates power coverage when the radio comes back up.

QUESTION 170

A Cisco WCS is being utilized to manage the Certkiller wireless network. What are two features of the Wireless Control System (WCS) wireless management? (Select two)

A. Centralized management for autonomous access points

B. Centralized management for lightweight access points
C. An external AAA-server requirement
D. Integration with the Location Appliance to expand real time tracking to 1500 devices for 30 days
E. The inclusion of an integrated AAA server
F. Integration with the Location Appliance to expand real time tracking to 2500 devices for 15 days

Answer: B, D

Explanation:
Cisco WCS is a Cisco WLAN solution network-management tool that adds to the capabilities of the web user interface and CLI, moving from individual controllers to a network of controllers. Cisco WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points. Cisco Wireless Location Appliance can be used to improve the functionality of Cisco WCS Location. Cisco Wireless Location Appliance performs location computations based on the RSSI information received from Cisco Wireless LAN Controllers. The Cisco Wireless LAN Controllers that gather the RSSI information must be associated with the Cisco Wireless Location Appliance. The Cisco 2700 Series Location Appliance is a Cisco Wireless Location Appliance that can be used.

QUESTION 171
A Cisco WCS is being installed to manage the Certkiller wireless network. Which two statements about the Wireless Control System (WCS) are true? (Select two)

A. An example of the WLSE server is the Cisco 2700 series location appliance.
B. The WCS is a client application that supports centralized configuration, firmware, and radio management.
C. The Cisco 2700 series appliance can store historical data for up to 15,000 wireless devices.
D. Initial configuration of the Cisco 2700 series appliance is done using a CLI console session.
E. The Cisco 2700 series appliance can collect data from radio frequency identifiers (RFID) asset tags.

Answer: D, E

Explanation:
Cisco WCS is a Cisco WLAN solution network-management tool that adds to the capabilities of the web user interface and CLI, moving from individual controllers to a network of controllers. Cisco WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points. Cisco Wireless Location Appliance can be used to improve the functionality of Cisco

WCS Location. Cisco Wireless Location Appliance performs location computations based on the RSSI information received from Cisco Wireless LAN Controllers. The Cisco Wireless LAN Controllers that gather the RSSI information must be associated with the Cisco Wireless Location Appliance. The Cisco 2700 Series Location Appliance is a Cisco Wireless Location Appliance that can be used.

QUESTION 172
Certkiller uses the Cisco WLSE to manage the wireless network. What are three benefits of the Wireless LAN Solution Engine (WLSE)? (Select three)

A. WLSE provides AP utilization and client association reports, features which help with capacity planning.
B. WLSE can respond to required changes that are requested by APs.
C. WLSE minimizes security vulnerabilities by providing security policy misconfiguration alerts and rogue AP detection.
D. WLSE increases productivity through customization with three possible levels of management: lightweight, extended, and advanced.
E. WLSE helps simplify large-scale deployments by providing automatic configuration of new APs.
F. The decentralized nature of WLSE helps reduce the time and resources that are required to manage a large number of WLAN devices.

Answer: A, C, E

Explanation:
CiscoWorks WLSE is a systems-level solution for managing the entire Cisco Aironet WLAN infrastructure based on autonomous access points. The RF and device-management features of CiscoWorks WLSE simplify the everyday operation of WLANs, helping to ensure smooth deployment of security and network availability while reducing deployment and operating expense. CiscoWorks WLSE operates by gathering fault, performance, and configuration information about Cisco devices that it discovers in the network. The access points, WDS, switches, and routers must be properly configured with Cisco Discovery Protocol (CDP) and Simple Network Management Protocol (SNMP) to provide information to CiscoWorks WLSE for the access point discovery process. After devices are discovered, you decide which devices to manage with CiscoWorks WLSE. CiscoWorks WLSE is a core component of the WLAN autonomous access-point
CiscoWorks WLSE can detect that an access point has failed. It compensates for the loss by automatically increasing the power and cell coverage of nearby access points. The Self Healing feature minimizes the outage impact to wireless client devices and maximizes the availability of wireless applications. Self Healing also recalculates power coverage when the radio comes back up.

QUESTION 173
A new wireless office has just been installed in the Certkiller network. What are two components of the Cisco Lightweight WLAN solution? (Select two)

A. Location Appliance
B. WLSE-Express
C. WCS
D. WLSE
E. WDS

Answer: A, C

Explanation:
Cisco WCS is a Cisco WLAN solution network-management tool that adds to the capabilities of the web user interface and CLI, moving from individual controllers to a network of controllers. Cisco WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.
Cisco Wireless Location Appliance can be used to improve the functionality of Cisco WCS Location. Cisco Wireless Location Appliance performs location computations based on the RSSI information received from Cisco Wireless LAN Controllers. The Cisco Wireless LAN Controllers that gather the RSSI information must be associated with the Cisco Wireless Location Appliance. The Cisco 2700 Series Location Appliance is a Cisco Wireless Location Appliance that can be used.

QUESTION 174
A new Cisco WCS was installed in the Certkiller wireless network. Which two statements correctly describe the Cisco Wireless Control System (WCS)? (Select two)

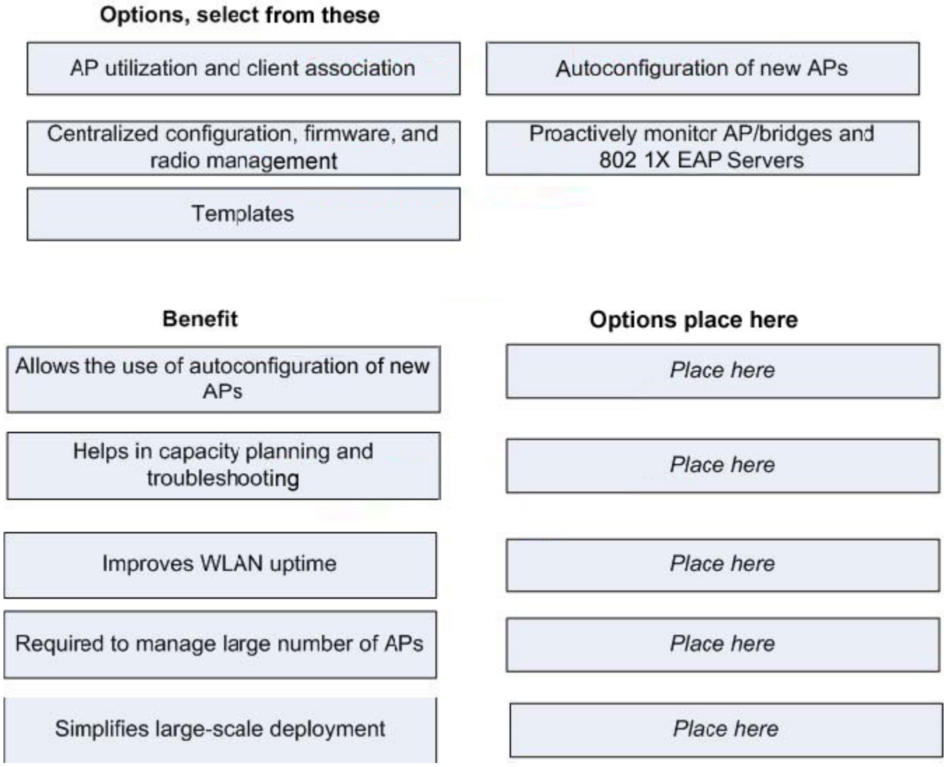
A. It supports SSH.
B. It is supported on the Windows and Linux platforms.
C. It supports SNMPv1 and SNMPv2 only.
D. It can be configured using HTTPS.
E. It is supported on Linux platforms only.

Answer: B, D

Explanation:
Cisco WCS is a Cisco WLAN solution network-management tool that adds to the capabilities of the web user interface and CLI, moving from individual controllers to a network of controllers. Cisco WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.
Cisco WCS is supported under Microsoft Windows 2000, Windows 2003, and Red Hat Enterprise Linux ES v.3 servers as either a normal application or a service.
The Cisco WLAN solution consists of Cisco Wireless LAN Controllers and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the operating system user interfaces. One of them is Cisco

WCS. The following user interfaces exist:
1. An HTTPS full-featured web user interface hosted by Cisco controllers can be used to configure and monitor individual controllers.
2. A full-featured CLI can be used to configure and monitor individual controllers. Cisco WCS can be used to configure and monitor one or more controllers and associated access points.
3. Cisco WCS has tools to facilitate large-system monitoring and control.
4.
An industry-standard SNMPv1, SNMP 2c, and SNMPv3 interface can be used with any SNMP-compliant third-party network management system.

QUESTION 175
DRAG DROP
Drag each WLSE feature to the appropriate benefit.



Options, select from these

AP utilization and client association

Autoconfiguration of new APs

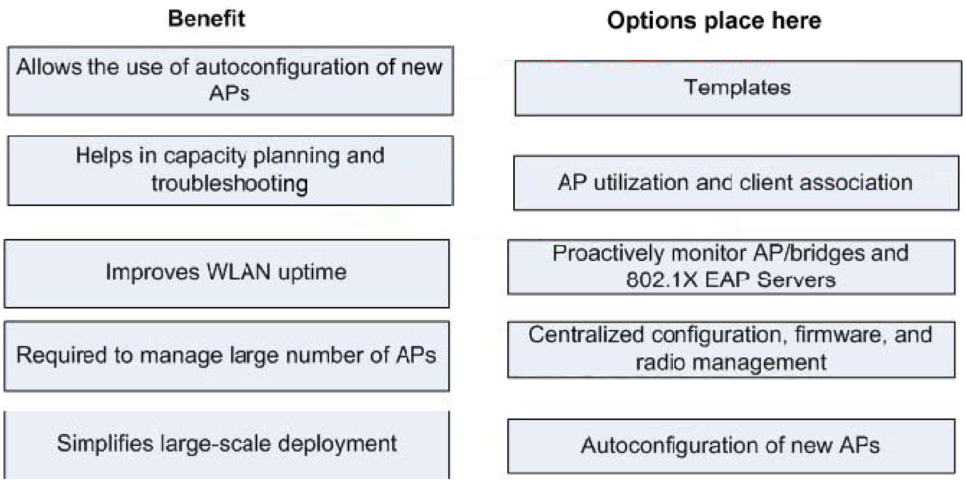
Centralized configuration, firmware, and radio management

Proactively monitor AP/bridges and 802 1X EAP Servers

Templates

Benefit	Options place here
Allows the use of autoconfiguration of new APs	Place here
Helps in capacity planning and troubleshooting	Place here
Improves WLAN uptime	Place here
Required to manage large number of APs	Place here
Simplifies large-scale deployment	Place here

Answer:



Benefit	Options place here
Allows the use of autoconfiguration of new APs	Templates
Helps in capacity planning and troubleshooting	AP utilization and client association
Improves WLAN uptime	Proactively monitor AP/bridges and 802.1X EAP Servers
Required to manage large number of APs	Centralized configuration, firmware, and radio management
Simplifies large-scale deployment	Autoconfiguration of new APs

Explanation:
1. CiscoWorks WLSE supports centralized configuration, firmware, and radio management, which reduces WLAN total cost of ownership by saving the time and resources required to manage large numbers of access points. CiscoWorks WLSE aggregates all configurations, images, and management information in one place.
2. Templates, one of the features of CiscoWorks WLSE, allow autoconfiguration of new access points for simplified large-scale deployment of access points. When a new access point is added to the system, you can use the template to configure it.
3. Access points added to the system require correct configuration. CiscoWorks WLSE detects misconfiguration and follows with an alert, the process used to detect a rogue access point and to minimize security vulnerabilities.
4. CiscoWorks WLSE is capable of monitoring access point utilization and client association. A report that includes the number of access points and clients can be used for capacity planning and troubleshooting.
5. The CiscoWorks WLSE configuration templates are not only used for new access points. The system allows you to proactively monitor access points, bridges, and 802.1x EAP servers. The system is able to push down to an access point configuration changes or any other changes required, which improves WLAN uptime.

QUESTION 176
WCS is being used to manage the Certkiller wireless network and detect rogue access points. Which statement best describes the rogue AP location display of the WCS wireless management server?

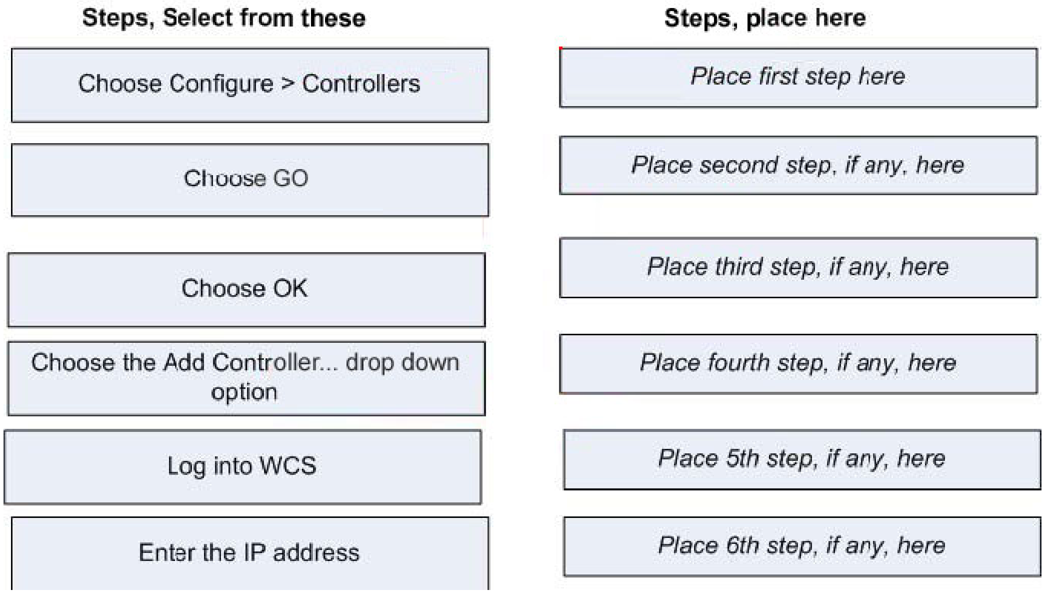
A. Cisco WCS Base identifies the general location of rogue APs based on the signal strength received by the nearest managed Cisco APs, whereas Cisco WCS Location adds high-accuracy location tracking to within a few meters of the rogue AP.
B. Cisco WCS Base and Cisco WCS Location both indicate rogue AP location only in a Rogue AP Alarm text file.
C. Cisco WCS Base does not have this feature, whereas Cisco WCS Location can indicate rogue AP location in a map at the most probable location that is calculated by two or more APs.
D. Cisco WCS Base does not have this feature, whereas Cisco WCS Location can

indicate rogue AP location in a map beside the nearest associated AP.
E. Cisco WCS Base and Cisco WCS Location both indicate rogue AP location in a map at the most probable location that is calculated by two or more APs.
F. None of the above.

Answer: A

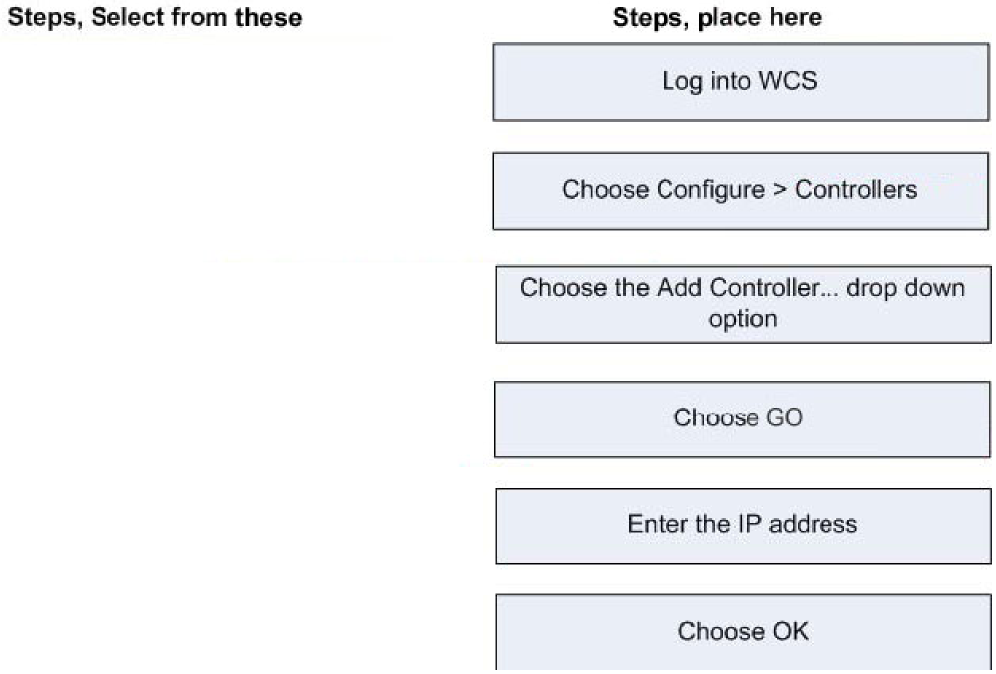
Explanation:
Cisco WCS is a Cisco WLAN solution network-management tool that adds to the capabilities of the web user interface and CLI, moving from individual controllers to a network of controllers. Cisco WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.
Cisco WCS software features include graphical views of the following:
* Autodiscovery of access points as they associate with controllers
* Autodiscovery and containment or notification of rogue access points
* Map-based organization of access point coverage areas, which is helpful when the enterprise spans more than one geographical area
* User-supplied campus, building, and floor plan graphics, which show this information:
* Locations and status of managed access points.
* Locations of rogue access points based on the signal strength received by the nearest managed Cisco access points.
* Coverage hole alarm information for access points based on the received signal strength from clients. This information appears in tabular rather than map format.
* RF coverage maps.
When the lightweight access points on your WLAN are powered up and associated with controllers, Cisco WCS immediately starts listening for rogue access points. When Cisco Wireless LAN Controller detects a rogue access point, it immediately notifies Cisco WCS, which creates a rogue access point alarm. When Cisco WCS receives a rogue access point message from Cisco Wireless LAN Controller, an alarm indicator appears in the lower-left corner of all Cisco WCS user interface pages.

QUESTION 177
DRAG DROP
You need to add a new wireless LAN controller (WLC) to the WCS wireless management server within the Certkiller wireless network. Put the proper procedure into the appropriate step sequence order below:



Steps, Select from these	Steps, place here
Choose Configure > Controllers	*Place first step here*
Choose GO	*Place second step, if any, here*
Choose OK	*Place third step, if any, here*
Choose the Add Controller... drop down option	*Place fourth step, if any, here*
Log into WCS	*Place 5th step, if any, here*
Enter the IP address	*Place 6th step, if any, here*

Answer:



Steps, Select from these	Steps, place here
	Log into WCS
	Choose Configure > Controllers
	Choose the Add Controller... drop down option
	Choose GO
	Enter the IP address
	Choose OK

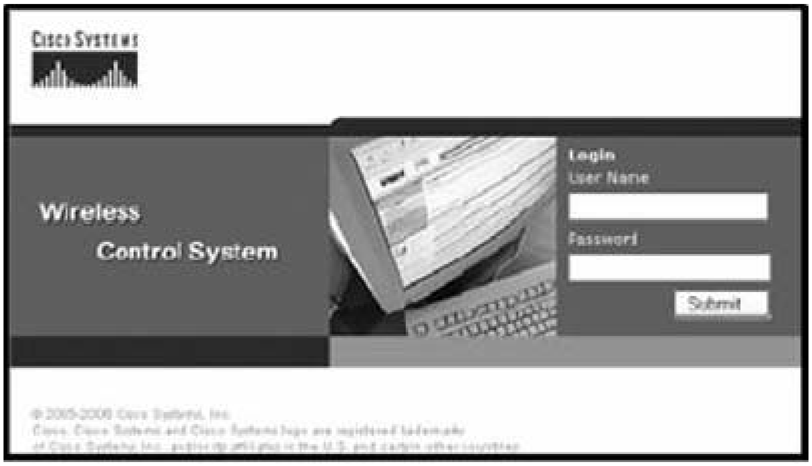
Explanation:

Cisco WCS Configuration

Step 1 Launch Microsoft Internet Explorer version 6.0 or later

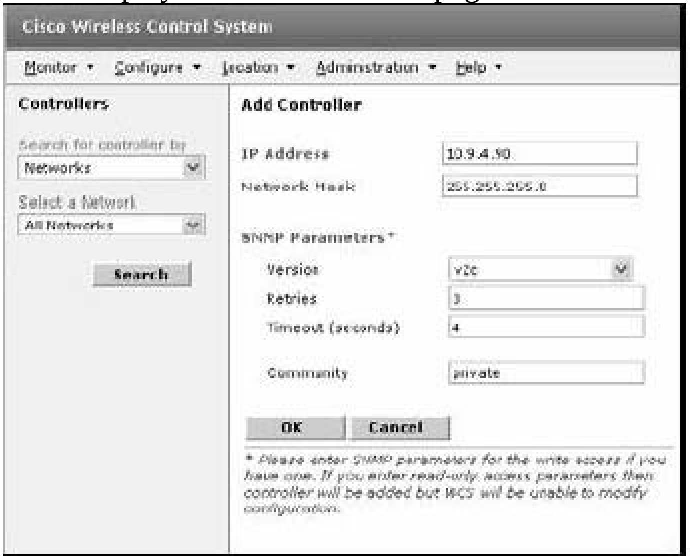
Step 2 In the browser address line, enter https://localhost when the Cisco WCS user interface is on a Cisco WCS server. Or Enter https://wcs-ip-address when the Cisco WCS interface is on any other workstation.

Step 3 The Cisco WCS user interface displays the Cisco WCS Login page. On the login page, enter your username and password. The default username is root and the default password is public.



© 2005-2006 Cisco Systems, Inc.
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks
of Cisco Systems Inc. and/or its affiliates in the U.S. and certain other countries.

Step 4 Log in to the Cisco WCS user interface.
Step 5 Choose Configure > Controllers to display the All Controllers page.
Step 6 From the Select a Command drop-down menu, choose Add Controller and click Go to display the Add Controller page.



Search for controller by: Networks
Select a Network: All Networks

IP Address: 10.9.4.90
Network Mask: 255.255.255.0

SNMP Parameters *
Version: v2c
Retries: 3
Timeout (seconds): 4
Community: private

* Please enter SNMP parameters for the write access if you have one. If you enter read-only access parameters then controller will be added but WCS will be unable to modify configuration.

Step 7 Enter the controller IP address, network mask, and required SNMP settings in the Add Controller fields.
Step 8 Click OK. Cisco WCS displays the Please Wait dialog box while it contacts the controller, adds the current controller configuration to the Cisco WCS database, and then displays the Add Controller page

---

QUESTION 178
You need to install WCS on a management station to monitor the Certkiller wireless network. Which two operating systems are supported by Cisco for WCS wireless management installation and operation? (Select two)

A. MAC OS X v10.3 or later
B. Red Hat Enterprise Linux ES 3
C. Solaris 2.5.1 or later
D. Windows XP Professional

E. Windows 2000 Server with SP4 or later

Answer: B, E

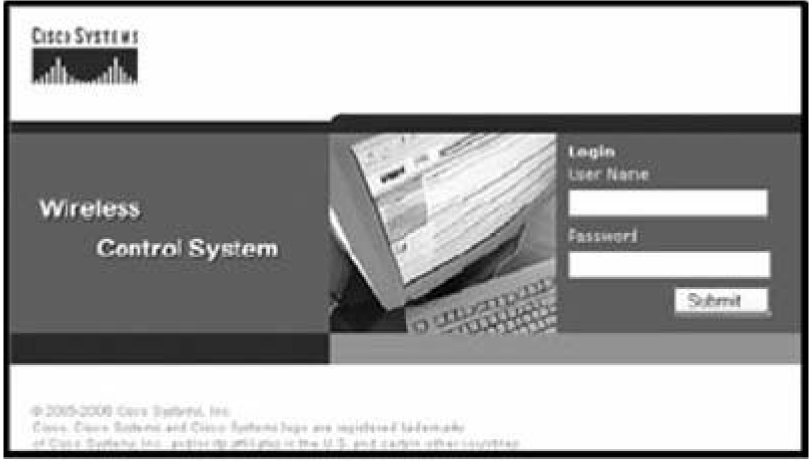
Explanation:
Cisco WCS is supported under Microsoft Windows 2000, Windows 2003, and Red Hat Enterprise Linux ES v.3 servers as either a normal application or a service. The Cisco WLAN solution consists of Cisco Wireless LAN Controllers and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the operating system user interfaces. One of them is Cisco WCS.

QUESTION 179
The Certkiller wireless administrator needs to add a new AP in the WCS. What is the correct procedure for adding an access point in WCS?

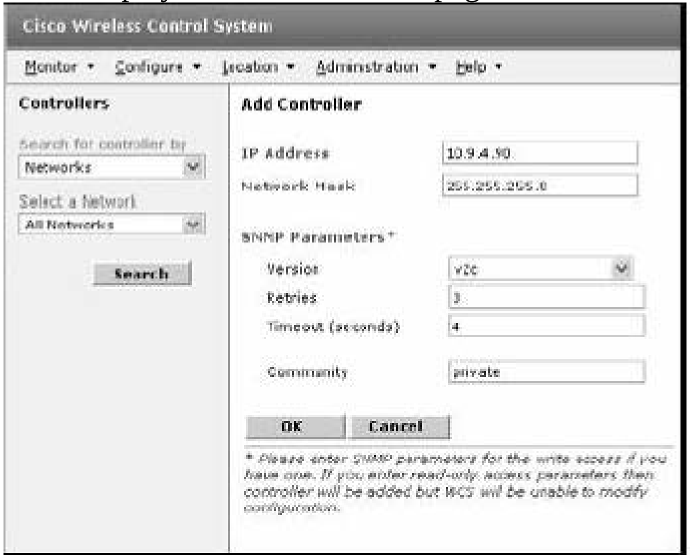
A. Choose Configure > Controller, then enter the IP address of the WLC.
B. Wait until the WLC downloads its code from the WCS and then choose the access point from the list under the WLC option of the Configure menu.
C. Choose Configure > Access_Point, then enter the IP address of the AP.
D. Wait until the AP downloads its code from the WCS and then choose the access point from the list under the Access_Point option of the Configure menu.
E. Choose Configure > Access_Point, then enter the AP MAC address.

Answer: A

Explanation:
Cisco WCS Configuration
Step 1 Launch Microsoft Internet Explorer version 6.0 or later
Step 2 In the browser address line, enter https://localhost when the Cisco WCS user interface is on a Cisco WCS server. Or Enter https://wcs-ip-address when the Cisco WCS interface is on any other workstation.
Step 3 The Cisco WCS user interface displays the Cisco WCS Login page. On the login page, enter your username and password. The default username is root and the default password is public.



Step 4 Log in to the Cisco WCS user interface.
Step 5 Choose Configure > Controllers to display the All Controllers page.
Step 6 From the Select a Command drop-down menu, choose Add Controller and click Go to display the Add Controller page.



Search for controller by: Networks

Select a Network: All Networks

Add Controller

IP Address: 10.9.4.90

Network Mask: 255.255.255.0

SNMP Parameters*

Version: v2c

Retries: 3

Timeout (seconds): 4

Community: private

* Please enter SNMP parameters for the write access if you have one. If you enter read-only access parameters then controller will be added but WCS will be unable to modify configuration.

Step 7 Enter the controller IP address, network mask, and required SNMP settings in the Add Controller fields.
Step 8 Click OK. Cisco WCS displays the Please Wait dialog box while it contacts the controller, adds the current controller configuration to the Cisco WCS database, and then displays the Add Controller page

---

QUESTION 180
Cisco's Wireless LAN management tools have been implemented within your enterprise network. What are two components of the Cisco Autonomous WLAN solution? (Select two)

A. WCS
B. WLSE
C. WLC
D. WDS
E. LWAPP
F. CSA

Answer: B, D

Explanation:
The two WLAN solutions have different characteristics and advantages. Autonomous access points are configured per access point. Their Cisco IOS software operates independently. Centralized configuration, monitoring, and management can be done through CiscoWorks WLSE. Radio monitoring and management communication is facilitated between the autonomous access points and CiscoWorks WLSE through use of WDS. WDS is a feature enabled in any access point that forwards aggregated RF

information from a grouping of access points to CiscoWorks
CiscoWorks WLSE is a systems-level solution for managing the entire Cisco Aironet WLAN infrastructure based on autonomous access points. The RF and device-management features of CiscoWorks WLSE simplify the everyday operation of WLANs, helping to ensure smooth deployment of security and network availability while reducing deployment and operating expense. CiscoWorks WLSE operates by gathering fault, performance, and configuration information about Cisco devices that it discovers in the network. The access points, WDS, switches, and routers must be properly configured with Cisco Discovery Protocol (CDP) and Simple Network Management Protocol (SNMP) to provide information to CiscoWorks WLSE for the access point discovery process. After devices are discovered, you decide which devices to manage with CiscoWorks WLSE. CiscoWorks WLSE is a core component of the WLAN autonomous access-point solution.

QUESTION 181
A Cisco Wireless Location Appliance has been implemented to enhance the management of the Certkiller WLAN. Which two statements about this appliance are true? (Select two)

A. The Wireless Location Appliance visually tracks up to 15,000 WLAN devices and can store this information for 90 days.
B. The Cisco 2000, 2700, 4100, and 4400 are examples of Wireless Location Appliances.
C. The Wireless Location Appliance visually displays the location information of WLAN devices and forwards this information to third-party applications using the Simple Network Management Protocol (SNMP).
D. Before using the Web interface, the initial configuration of the Wireless Location appliance must be done using the command-line interface (CLI).
E. A Wireless Location Appliance acts as a server to one or more Cisco WCSs. It collects, stores, and passes on data from its associated Cisco WLAN controllers.

Answer: D, E

Explanation:
Cisco 2700 Series Wireless Location Appliances are servers that enhance the high-accuracy built-in Cisco WCS:
-Computing historical location data
-Collecting historical location data
-Storing historical location data
Configuration and operation uses Cisco WCS, which has an easy-to-use GUI.
Initial configuration using a CLI console session is required before you use the GUI.
The Cisco Wireless Location Appliance is an innovative, easy-to-deploy solution that uses advanced RF fingerprinting technology to simultaneously track thousands of 802.11 wireless devices from directly within a WLAN infrastructure, increasing asset visibility and control of the airspace.
Cisco 2700 Series Wireless Location Appliances are servers that enhance the high-accuracy built-in Cisco WCS location abilities by computing, collecting, and storing

historical location data for up to 1500 laptop clients, palmtop clients, VoIP telephone clients, radio frequency identifier (RFID) asset tags, rogue access points, and rogue access point clients.
A Cisco 2700 Series Wireless Location Appliance acts as a server to one or more Cisco WCS devices, collecting, storing, and passing on data from its associated Cisco Wireless LAN Controllers. Additionally, the appliance provides location-based alerts for business policy enforcement and records rich historical location information that can be used for location trending, rapid problem resolution and RF capacity management.

QUESTION 182
Cisco's WCS has been installed to manage the Certkiller WLAN. Which two statements about the Wireless Control System (WCS) are true? (Select two)

A. The Cisco WCS is designed to support 1500 Cisco WLAN controllers and up to 50 APs.
B. The Cisco WCS uses the SNMP protocol to communicate with the controllers.
C. The Cisco WCS runs on a dedicated network device such as the Cisco 2700 network appliance.
D. The Cisco WCS screen displays four main menu sheet tabs consisting of Monitor, Configure, Security, and Alarm.
E. The Cisco WCS runs on various Windows and Linux platforms.

Answer: B, E

Explanation:
Cisco WCS is a Cisco WLAN solution network-management tool that adds to the capabilities of the web user interface and CLI, moving from individual controllers to a network of controllers. Cisco WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.
Cisco WCS is supported under Microsoft Windows 2000, Windows 2003, and Red Hat Enterprise Linux ES v.3 servers as either a normal application or a service.
The Cisco WLAN solution consists of Cisco Wireless LAN Controllers and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the operating system user interfaces. One of them is Cisco WCS. The following user interfaces exist:
1. An HTTPS full-featured web user interface hosted by Cisco controllers can be used to configure and monitor individual controllers.
2. A full-featured CLI can be used to configure and monitor individual controllers. Cisco WCS can be used to configure and monitor one or more controllers and associated access points.
3. Cisco WCS has tools to facilitate large-system monitoring and control.
4. An industry-standard SNMPv1, SNMP 2c, and SNMPv3 interface can be used with any SNMP-compliant third-party network management system.

QUESTION 183
A Cisco WLSE-Express has been implemented to manage part of the Certkiller wireless network. What are two features of WLSE-Express wireless management? (Select two)

A. Centralized management that requires an external AAA server
B. Centralized management for autonomous access points
C. Centralized management with integrated AAA server
D. Integration with the Location Appliance to expand real time tracking to 1500 devices for 30 days
E. Integration with the Location Appliance to expand real time tracking to 2500 devices for 30 days
F. Centralized management for lightweight access points

Answer: B, C

Explanation:
The two versions of CiscoWorks WLSE available scale to different network sizes. CiscoWorks WLSE is used for medium to large enterprise and wireless verticals (up to 2500 WLAN devices). CiscoWorks WLSE Express is used for SMBs (250 to 1500 employees) and commercial and branch offices (up to 100 WLAN devices) looking for a cost-effective solution with integrated WLAN management and security services. Enterprise branch office deployments usually want to localize WLAN security and management services to provide WLAN access survivability during WAN failures. They do not want to use WAN bandwidth for WLAN and RF management traffic. Some service providers can use CiscoWorks WLSE Express, because public WLAN (PWLAN) hot-spot management requires fewer WLAN devices. CiscoWorks WLSE requires an external AAA server, which is already included with CiscoWorks WLSE Express. CiscoWorks WLSE Express has integrated WLAN security and management services supporting 802.1x LEAP, Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), and Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). The user directory supports Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory, and a local user database. Both wired and wireless user authentication are supported. WLAN IDS features are supported, too.

QUESTION 184
A new Certkiller office is implementing a Wireless LAN. Which two WLAN implementation statements are true? (Select two)

A. A lightweight wireless solution consists of autonomous access points (APs), which are managed by a WLAN solution engine (WLSE/WLSM).
B. A lightweight wireless solution includes lightweight APs and WLAN controllers. The APs and the WLAN controllers are managed by the Cisco Wireless Control System (WCS).
C. A lightweight wireless solution includes lightweight APs and WLAN controllers. The

APs and the WLAN controllers are managed by a WLAN solution engine (WLSE/WLSM).
D. An autonomous wireless solution includes lightweight APs and WLAN controllers. The APs and the WLAN controllers are managed by a WLAN solution engine (WLSE/WLSM).
E. A lightweight wireless solution includes lightweight APs and WLAN controllers. The APs and the WLAN controllers are managed by a WLAN solution engine (WLSE/WLSM).
F. An autonomous wireless solution includes lightweight APs and WLAN controllers. The APs and the WLAN controllers are managed by the Cisco Wireless Control System (WCS).

Answer: B, D

Explanation:
The two WLAN solutions have different characteristics and advantages. Autonomous access points are configured per access point. Their Cisco IOS software operates independently. Centralized configuration, monitoring, and management can be done through CiscoWorks WLSE. Radio monitoring and management communication is facilitated between the autonomous access points and CiscoWorks WLSE through use of WDS. WDS is a feature enabled in any access point that forwards aggregated RF information from a grouping of access points to CiscoWorks
CiscoWorks WLSE is a systems-level solution for managing the entire Cisco Aironet WLAN infrastructure based on autonomous access points. The RF and device-management features of CiscoWorks WLSE simplify the everyday operation of WLANs, helping to ensure smooth deployment of security and network availability while reducing deployment and operating expense. CiscoWorks WLSE operates by gathering fault, performance, and configuration information about Cisco devices that it discovers in the network. The access points, WDS, switches, and routers must be properly configured with Cisco Discovery Protocol (CDP) and Simple Network Management Protocol (SNMP) to provide information to CiscoWorks WLSE for the access point discovery process. After devices are discovered, you decide which devices to manage with CiscoWorks WLSE. CiscoWorks WLSE is a core component of the WLAN autonomous access-point solution.

QUESTION 185
A Cisco WLSE is being used to manage the Certkiller wireless network. Which two features are supported by the WLAN Solution Engine (WLSE)? (Select two)

A. Graphical view of multiple controllers and managed APs
B. WLSE in two versions: base and location
C. Reporting
D. Auto discovery of rogue APs
E. Configuration of APs

Answer: C, E

Explanation:
The two WLAN solutions have different characteristics and advantages. Autonomous access points are configured per access point. Their Cisco IOS software operates independently. Centralized configuration, monitoring, and management can be done through CiscoWorks WLSE. Radio monitoring and management communication is facilitated between the autonomous access points and CiscoWorks WLSE through use of WDS. WDS is a feature enabled in any access point that forwards aggregated RF information from a grouping of access points to CiscoWorks
CiscoWorks WLSE is a systems-level solution for managing the entire Cisco Aironet WLAN infrastructure based on autonomous access points. The RF and device-management features of CiscoWorks WLSE simplify the everyday operation of WLANs, helping to ensure smooth deployment of security and network availability while reducing deployment and operating expense. CiscoWorks WLSE operates by gathering fault, performance, and configuration information about Cisco devices that it discovers in the network. The access points, WDS, switches, and routers must be properly configured with Cisco Discovery Protocol (CDP) and Simple Network Management Protocol (SNMP) to provide information to CiscoWorks WLSE for the access point discovery process. After devices are discovered, you decide which devices to manage with CiscoWorks WLSE. CiscoWorks WLSE is a core component of the WLAN autonomous access-point solution.

QUESTION 186
A Cisco WCS is being utilized to manage the Certkiller wireless network. Which Cisco Wireless Control System (WCS) statement is true?

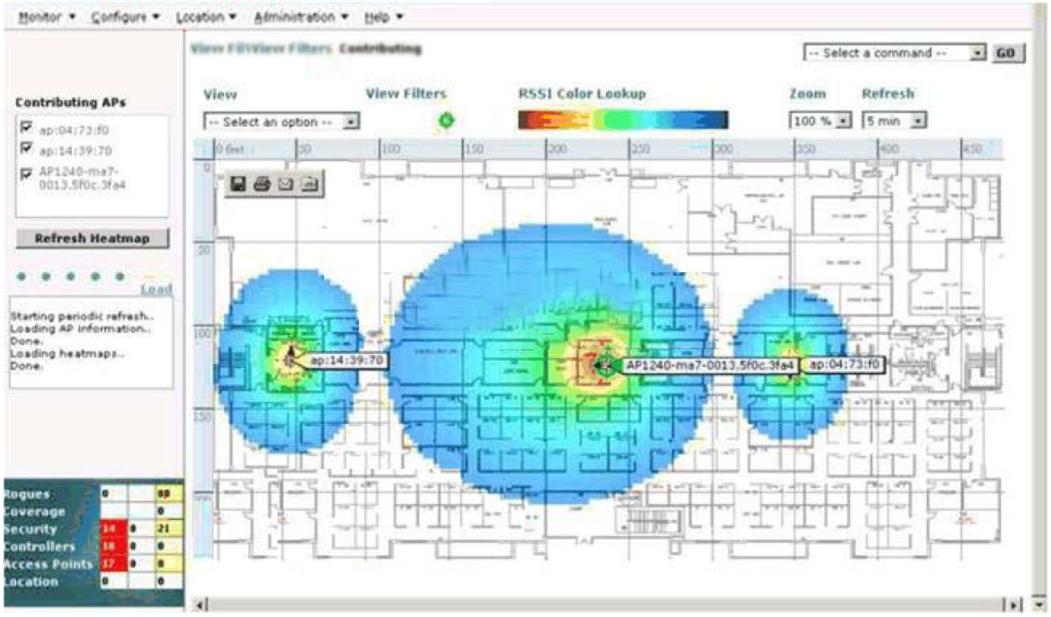
A. Cisco WCS software is used for WLAN planning, configuration, and management.
B. The three versions of Cisco WCS are WCS Base, WCS Location, and WCS Express.
C. Up to 2,500 APs can be supported from a single Cisco WCS console.
D. The Cisco WCS base software provides on-demand location of rogue APs and clients to within 33 feet (10 meters).
E. None of the above.

Answer: A

Explanation:
Cisco WCS is a Cisco WLAN solution network-management tool that adds to the capabilities of the web user interface and CLI, moving from individual controllers to a network of controllers. Cisco WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.
Cisco WCS is supported under Microsoft Windows 2000, Windows 2003, and Red Hat Enterprise Linux ES v.3 servers as either a normal application or a service.
The Cisco WLAN solution consists of Cisco Wireless LAN Controllers and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the operating system user interfaces. One of them is Cisco

WCS. The following user interfaces exist:
1. An HTTPS full-featured web user interface hosted by Cisco controllers can be used to configure and monitor individual controllers.
2. A full-featured CLI can be used to configure and monitor individual controllers. Cisco WCS can be used to configure and monitor one or more controllers and associated access points.
3. Cisco WCS has tools to facilitate large-system monitoring and control.
4. An industry-standard SNMPv1, SNMP 2c, and SNMPv3 interface can be used with any SNMP-compliant third-party network management system.

QUESTION 187
The following was seen on a management station in the Certkiller NOC:



Zoom: 100 %
Refresh: 5 min

Contributing APs
☑ ap:04:73:f0
☑ ap:14:39:70
☑ AP1240-ma7-0013.5f0c.3fa4

Starting periodic refresh..
Loading AP information..
Done.
Loading heatmaps..
Done.

Rogues	0		89
Coverage			0
Security	14	0	21
Controllers	18	0	0
Access Points	17	0	0
Location	0		0

Study the exhibit carefully. Based on the partial screen capture in the exhibit, which software package is being used?

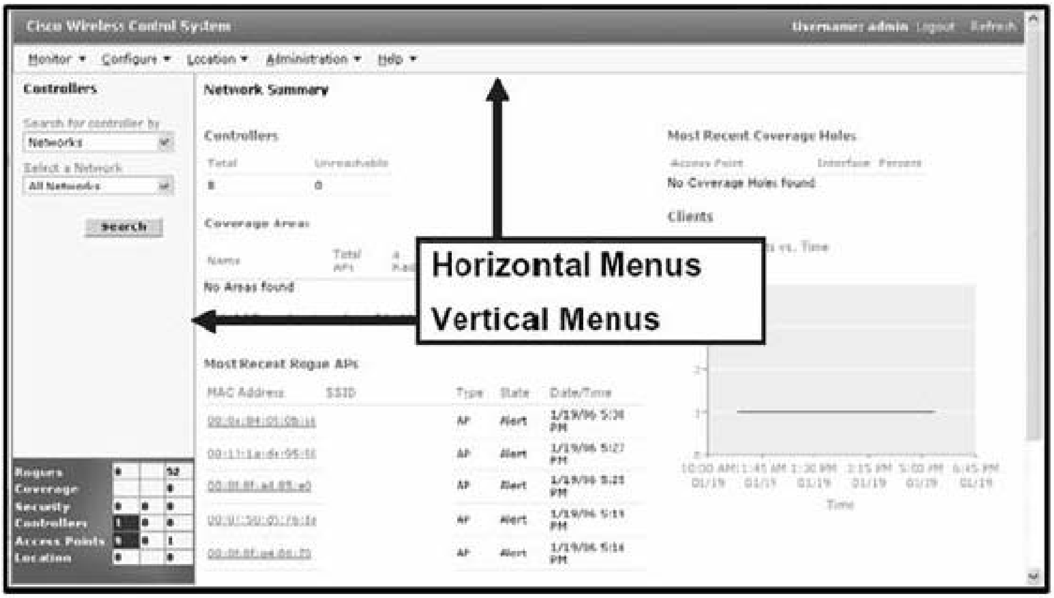
A. WLAN Services Module (WLSM)
B. Wireless Control System (WCS)
C. WLAN Solution Engine (WLSE)
D. WLAN Solution Engine Express (WLSE Express)
E. None of the above

Answer: B

Explanation:
Cisco WCS is a Cisco WLAN solution network-management tool that adds to the capabilities of the web user interface and CLI, moving from individual controllers to a network of controllers. Cisco WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points. Cisco WCS is supported under Microsoft Windows 2000, Windows 2003, and Red Hat

Enterprise Linux ES v.3 servers as either a normal application or a service.
The Cisco WLAN solution consists of Cisco Wireless LAN Controllers and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the operating system user interfaces. One of them is Cisco WCS. The following user interfaces exist:
1. An HTTPS full-featured web user interface hosted by Cisco controllers can be used to configure and monitor individual controllers.
2. A full-featured CLI can be used to configure and monitor individual controllers. Cisco WCS can be used to configure and monitor one or more controllers and associated access points.
3. Cisco WCS has tools to facilitate large-system monitoring and control.
4. An industry-standard SNMPv1, SNMP 2c, and SNMPv3 interface can be used with any SNMP-compliant third-party network management system.

Cisco WCS Network Summary



MAC Address	SSID	Type	State	Date/Time
[illegible]		AP	Alert	1/19/06 5:30 PM
[illegible]		AP	Alert	1/19/06 5:27 PM
[illegible]		AP	Alert	1/19/06 5:21 PM
[illegible]		AP	Alert	1/19/06 5:11 PM
[illegible]		AP	Alert	1/19/06 5:14 PM

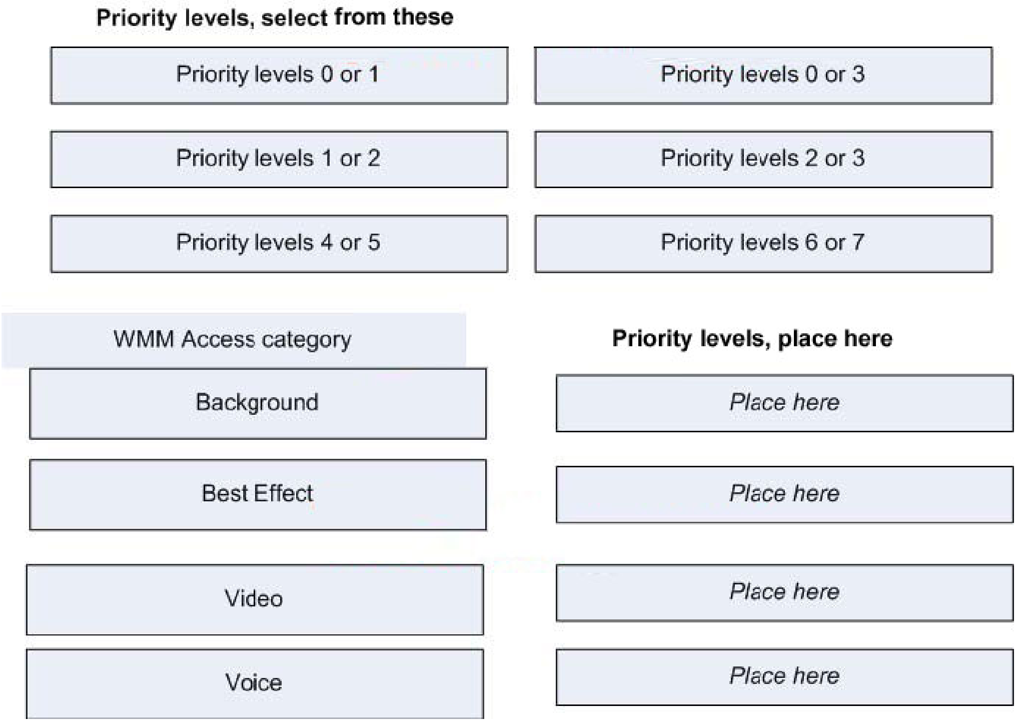
QUESTION 188
You have been tasked with extending QoS in the Certkiller network to include wireless LAN. In which device or devices is wireless QoS implemented for Cisco Lightweight AP split-MAC architecture?

A. The AP only
B. Between the AP and Catalyst switch via 802.1p
C. The Wireless LAN Controller only
D. Between the AP and Wireless LAN Controller via LWAPP
E. The Catalyst switch only
F. None of the above

Answer: D

Explanation:
Lightweight Access Point Protocol (LWAPP) changed the way that WLAN deployments were managed with the concept of a "split MAC"-the ability to separate the real-time aspects of the 802.11 protocol from most of its management aspects.
The lightweight access point WLAN solution uses the Layer 3 IP DSCP marking of packets sent by wireless LAN controllers and lightweight access points. The lightweight access point WLAN solution also enhances the way access points use Layer 3 information to ensure that packets receive the correct over-the-air prioritization when transmitted from the access point to the wireless client. In the lightweight WLAN solution, wireless LAN data is tunneled between the access point and the wireless LAN controller via LWAPP. To maintain the original QoS classification across an LWAPP tunnel, the QoS settings of the encapsulated data packet must be appropriately mapped to the Layer 2 (802.1p) and Layer 3 (IP DSCP) fields of the outer tunnel packet.

QUESTION 189
DRAG DROP
Drag the wireless 802.1e priority level groupings on the left to the appropriate Wi-Fi Multimedia (WMM) access categories on the right. (Note: Not all groupings will be used)

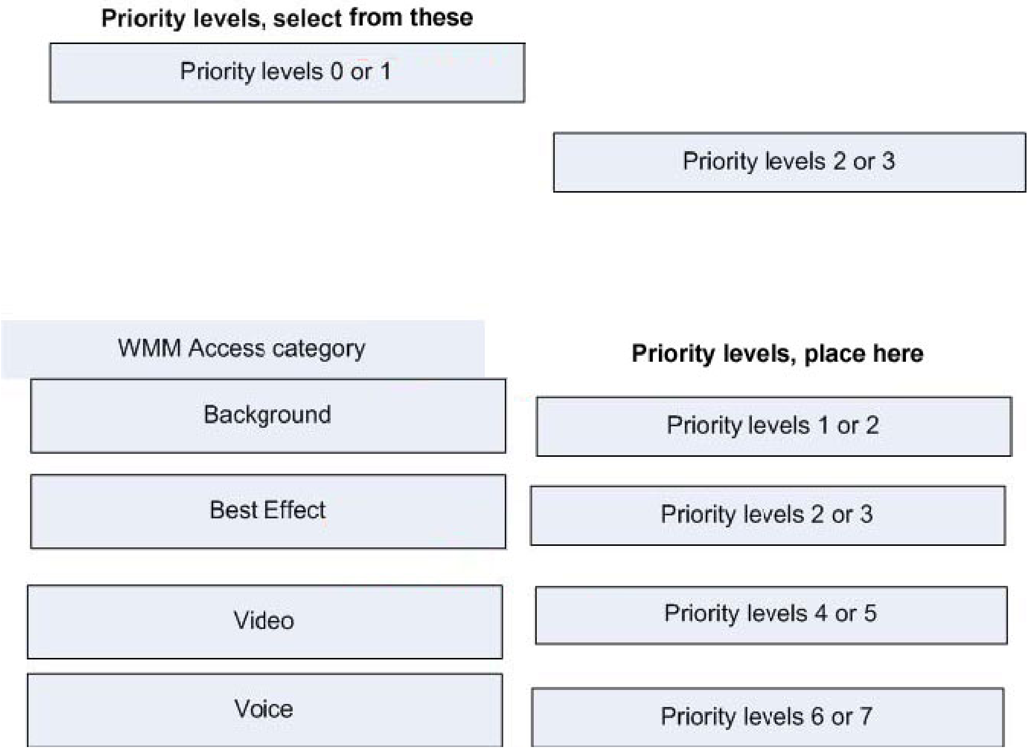


Priority levels, select from these

Priority levels 0 or 1
Priority levels 0 or 3
Priority levels 1 or 2
Priority levels 2 or 3
Priority levels 4 or 5
Priority levels 6 or 7

WMM Access category	**Priority levels, place here**
Background	*Place here*
Best Effect	*Place here*
Video	*Place here*
Voice	*Place here*

Answer:



Priority levels, select from these

Priority levels 0 or 1

Priority levels 2 or 3

WMM Access category

Priority levels, place here

Background

Priority levels 1 or 2

Best Effect

Priority levels 2 or 3

Video

Priority levels 4 or 5

Voice

Priority levels 6 or 7

Explanation:

The WMM traffic prioritization method put forward by the Wi-Fi Alliance is used to determine the assignment of application data headed to the client. WMM is an enhancement to the MAC sublayer to add QoS functionality to Wi-Fi networks. WMM is an extension to the prior CSMA/CA-based DCF mechanism that gives all devices the same priority and that is based on a best-effort, "listen-before-talk" algorithm. Each client waits a random backoff time, and then it transmits only if no other device is transmitting at that time. This collision-avoidance method gives all the devices the opportunity to transmit, but when traffic demand is high and networks can become overloaded, the performance of all devices will be equally affected.

WMM introduces traffic-prioritization capabilities based on the four defined access categories. RF prioritization allows a higher access category the increased probability of being transmitted first. This allows the platinum level to obtain RF access for transmission before the gold, silver, or bronze levels. The access categories were designed to correspond to 802.1p or DSCP priorities to facilitate interoperability with QoS policy-management mechanisms. WMM priorities coexist with legacy devices that are not WMM-enabled. Packets not assigned to a specific access category are categorized by default as the best-effort access category. WMM prioritization maps four independent transmit queues to eight 802.1e priority levels, as listed in the table.

WMM	802.1e
Voice	6 or 7
Video	4 or 5

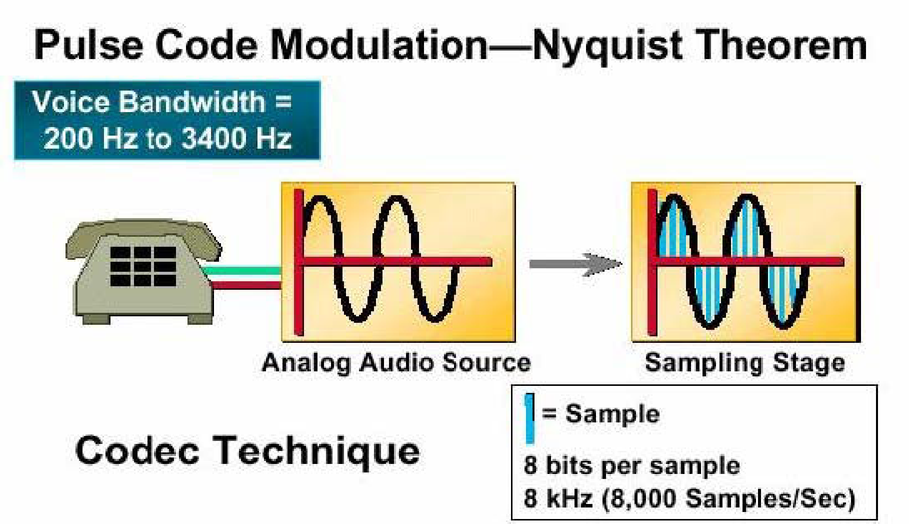
Background	1 or 2
Best Effort	0 or 3

QUESTION 190
One of the most important rules of sampling is called the Nyquist Theorem, which states that the highest frequency which can be accurately represented is less than one-half of the sampling rate. Based on the Nyquist theorem, what sampling rate is required to support voice frequencies of up to 4000 Hz?

A. 2000 samples per second
B. 6000 samples per second
C. 4000 samples per second
D. 8000 samples per second
E. 10,000 samples per second
F. 12,000 samples per second
G. None of the above

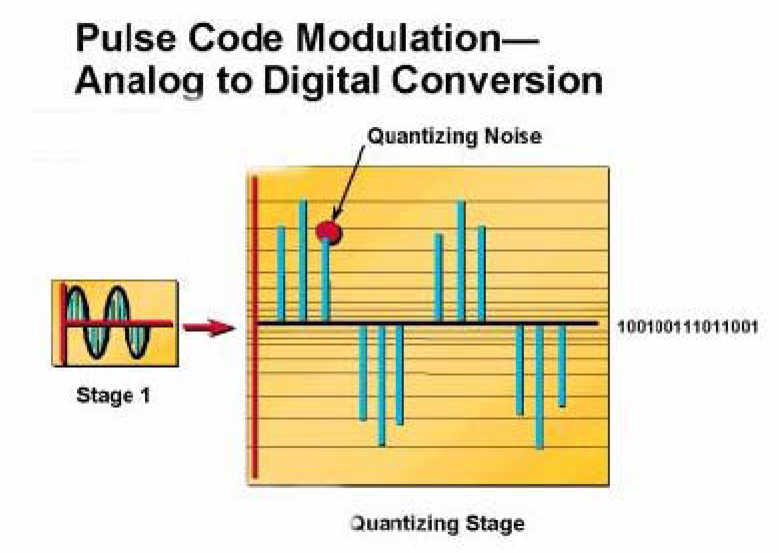
Answer: D

Explanation:


Pulse Code Modulation—Nyquist Theorem
Voice Bandwidth = 200 Hz to 3400 Hz
Analog Audio Source
Sampling Stage
= Sample
8 bits per sample
8 kHz (8,000 Samples/Sec)
Codec Technique

Quantization is the process of converting each analog sample value into a discrete value that can be assigned a unique digital code word.
As the input signal samples enter the quantization phase, they are assigned to a quantization interval. All quantization intervals are equally spaced (uniform quantization) throughout the dynamic range of the input analog signal. Each quantization interval is assigned a discrete value in the form of a binary code word. The standard word size used is eight bits. If an input analog signal is sampled 8000 times per second and each sample is given a code word that is eight bits long, then the maximum transmission bit rate for Telephony systems using PCM is 64,000 bits per second. Figure 2 illustrates how bit rate is derived for a PCM system.

Each input sample is assigned a quantization interval that is closest to its amplitude height. If an input sample is not assigned a quantization interval that matches its actual height, then an error is introduced into the PCM process. This error is called quantization noise. Quantization noise is equivalent to the random noise that impacts the signal-to-noise ratio (SNR) of a voice signal. SNR is a measure of signal strength relative to background noise. The ratio is usually measured in decibels (dB). If the incoming signal strength in microvolts is Vs, and the noise level, also in microvolts, is Vn, then the signal-to-noise ratio, S/N, in decibels is given by the formula S/N = 20 log10(Vs/Vn). SNR is measured in decibels (dB). The higher the SNR, the better the voice quality. Quantization noise reduces the SNR of a signal. Therefore, an increase in quantization noise degrades the quality of a voice signal. Figure 3 shows how quantization noise is generated. For coding purpose, an N bit word yields 2N quantization labels.



One way to reduce quantization noise is to increase the amount of quantization intervals. The difference between the input signal amplitude height and the quantization interval decreases as the quantization intervals are increased (increases in the intervals decrease the quantization noise). However, the amount of code words also need to be increased in proportion to the increase in quantization intervals. This process introduces additional problems that deal with the capacity of a PCM system to handle more code words.
SNR (including quantization noise) is the single most important factor that affects voice quality in uniform quantization. Uniform quantization uses equal quantization levels throughout the entire dynamic range of an input analog signal. Therefore, low signals have a small SNR (low-signal-level voice quality) and high signals have a large SNR (high-signal-level voice quality). Since most voice signals generated are of the low kind, having better voice quality at higher signal levels is a very inefficient way of digitizing voice signals. To improve voice quality at lower signal levels, uniform quantization (uniform PCM) is replaced by a nonuniform quantization process called companding.
Reference:
http://www.cisco.com/en/US/tech/ CK1 077/technologies_tech_note09186a00801149b3.shtml

QUESTION 191
You want to ensure that QoS mechanisms are preserved over a wireless network.
Which certification-based protocol is implemented for wireless QoS between an AP and a wireless client over RF media?

A. 802.1e using DCF
B. WMM using DCF
C. WMM using EDCAF
D. 802.1e using EDCAF
E. None of the above

Answer: C

Explanation:
The IEEE 802.11e supplements to 802.11, and therefore the WMM subset, replace the use of DCF with EDCF for CSMA/CA wireless frame transmission. WMM provides priority access to the RF medium in two ways. First, the wireless access point must prioritize the data into four access categories (from highest to lowest, platinum, gold, silver, and bronze). Second, the lower-priority traffic must use longer interframe wait timers allowing higher-priority traffic access to the wireless network first. The timers result from a summarization of the fixed short interframe space (SIFS), slot times (fixed-length time intervals based on priority), and a random slot timer (based on priority). The random backoff slot timers prevent media contention among traffic from within the same access category.

QUESTION 192
In the context of traffic descriptors, what is used for marking?

A. MPLS experimental bits
B. WRED (Weighted RED) orange or green labels
C. Header compression tags
D. FIFO Layer 2 descriptor labels (L2DL)
E. DRR (Deficit Round Robin) precedence bits.

Answer: B

QUESTION 193
Your boss, Mrs. Certkiller, is interested in voice gateway router capabilities.
What could you tell her?

A. Voice gateways with Cisco Unified CallManager Express (CME) can permanently act as a call agent for IP phones.
B. Voice gateways equipped with a DSP module can take the role of the call agent during WAN failure.
C. Voice gateways need a gatekeeper to interconnect the VoIP networks with the PSTN network.

D. Voice gateways with analog interfaces need a gatekeeper to convert analog signals into digital format before voice is encapsulated into IP packets.

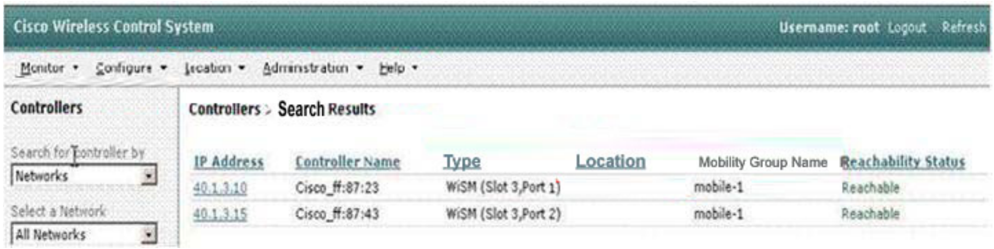
Answer: A

QUESTION 194
What type of services are provided by the Cisco IOS gateways in a VoIP network with Cisco CallManger functionality?

A. Zone management for all registered endpoints in the network.
B. Media termination and signal translation between the public switched telephone network (PSTN) and IP networks.
C. Services such as address translation and network access control for the devices on the network.
D. Services such as bandwidth management and accounting.

Answer: B

QUESTION 195
Exhibit:



Controllers > Search Results

IP Address	Controller Name	Type	Location	Mobility Group Name	Reachability Status
40.1.3.10	Cisco_ff:87:23	WiSM (Slot 3,Port 1)		mobile-1	Reachable
40.1.3.15	Cisco_ff:87:43	WiSM (Slot 3,Port 2)		mobile-1	Reachable

You work as a network technician at Certkiller .com. Please study the exhibit carefully
You want to view the status of one specific wireless controller.
What should you select?

A. Controller Name link
B. IP address link
C. IP address of the controller
D. Reachability Status link

Answer: C

QUESTION 196
You work as a network technician at Certkiller .com. Your boss, Mrs. Certkiller, is interested in traffic shaping. In particular she curious about in preventing and managing congestion. She asks you in what network technologies this can be used. What should you tell her? Select three.

A. Metro Ethernet
B. Asynchronous Transfer Mode (ATM)

C. Frame Relay (FR)
D. Multiprotocol Label Switching (MPLS)
E. Data-link switching (DLSw)
F. Route Processor Redundancy (RPR)

Answer: A,B,C

QUESTION 197
You work as a network technician at Certkiller .com. Your boss, Mrs. Certkiller, is interested in AutoQoS interface and bandwidth considerations. In particular she wants to know which QoS features implementations takes interface type and bandwidth into consideration.
What should you tell her? Select three.

A. cRTP
B. LFI
C. RIP
D. LLQ
E. CBWFQ
F. WRED
G. LFI

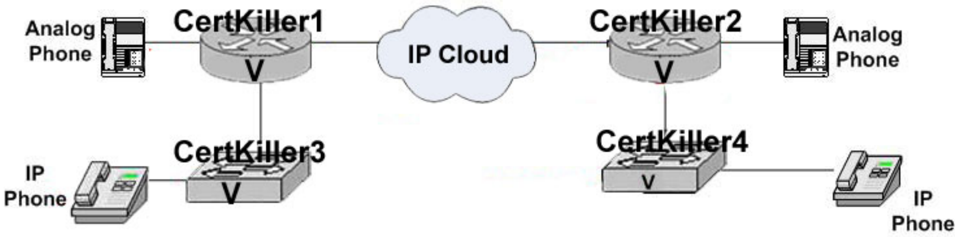
Answer: A,B,D

QUESTION 198
You work as a network technician at Certkiller .com. Your boss, Mrs. Certkiller, is interested in voice traffic transmitting protocols. What can you tell her? Select two.

A. UDP provides multiplexing
B. UDP is used to ensure e reliable transmission from sender to receiver
C. RTP multiplexing is used to keep multiple phone conversations separate.
D. RTP provides end-to-end delivery services for voice traffic.
E. RTP is used to provide resource reservation for the voice stream

Answer: A,D

QUESTION 199
Network topology exhibit:

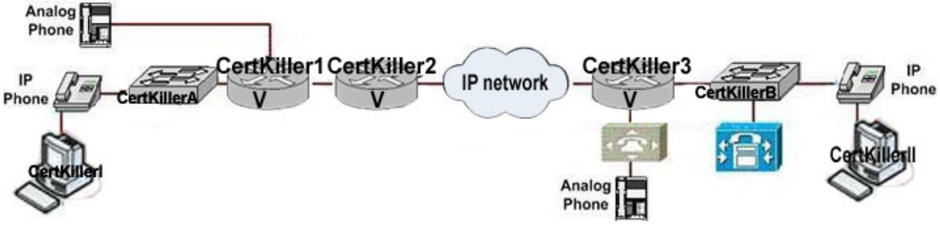


You work as a network engineer at Certkiller .com. Study the exhibit carefully. You are required to select appropriate QoS model that meets the following requirement to reserve the requested bandwidth and delay needed for each allowed VoIP call regardless of changing network conditions?

A. differentiated services (DiffServ)
B. best-effort delivery
C. shaping and policing
D. egress committed rate (ECR)
E. ingress committed rate (ICR)
F. Integrated Services (IntServ)

Answer: F

QUESTION 200
Network topology exhibit:

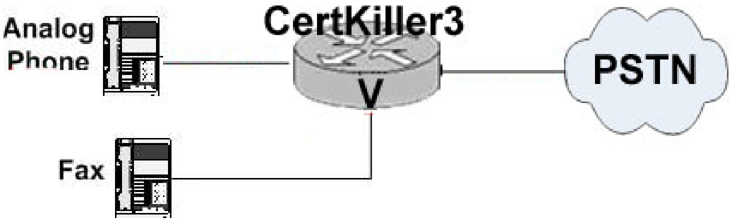


You work as a network engineer at Certkiller .com. Study the exhibit carefully. Your boss, Mrs. Certkiller, has asked you to optimize link usage throughput for voice traffic and increase bandwidth availability.
What method should you apply?

A. Payload compression on router Certkiller 1.
B. Payload compression on router Certkiller 2.
C. TCP header compression on router Certkiller 1.
D. TCP header compression on router Certkiller 2.
E. RTP header compression on router Certkiller 1.
F. RTP header compression on router Certkiller 2.

Answer: A

QUESTION 201
Network topology exhibit:



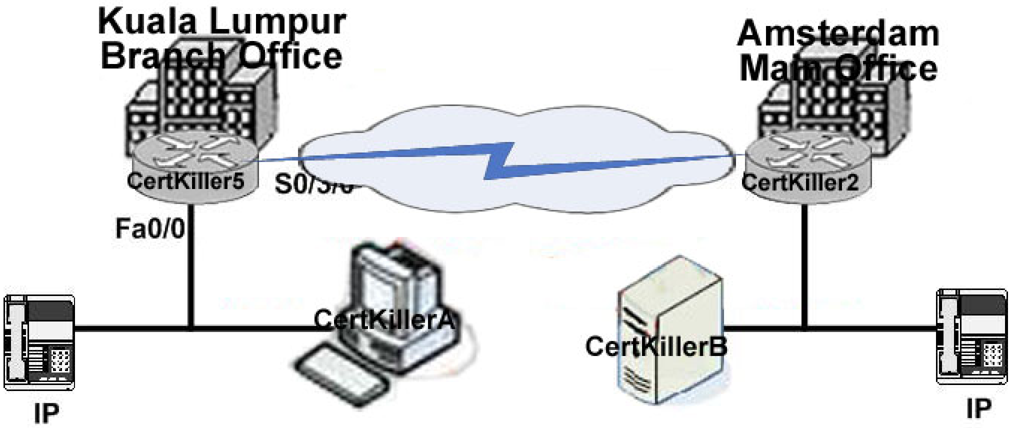
You work as a network engineer at Certkiller .com. Study the exhibit carefully. You are required to finalize the configuration of router Certkiller 3 in this scenario. In particular you need to decide which interface types should be used for connecting router Certkiller 3 to the phone and fax respectively. Select two.

A. Connect the analog phone to an FXS port.
B. Connect the fax to an FXS port.
C. Connect the analog phone to an FXO port.
D. Connect the fax to an FXO port.
E. Connect the analog phone to the E and M ports.
F. Connect the fax to the E and M ports.

Answer: A,B

Topic 1, Certkiller 1, Scenario

Network topology exhibit:

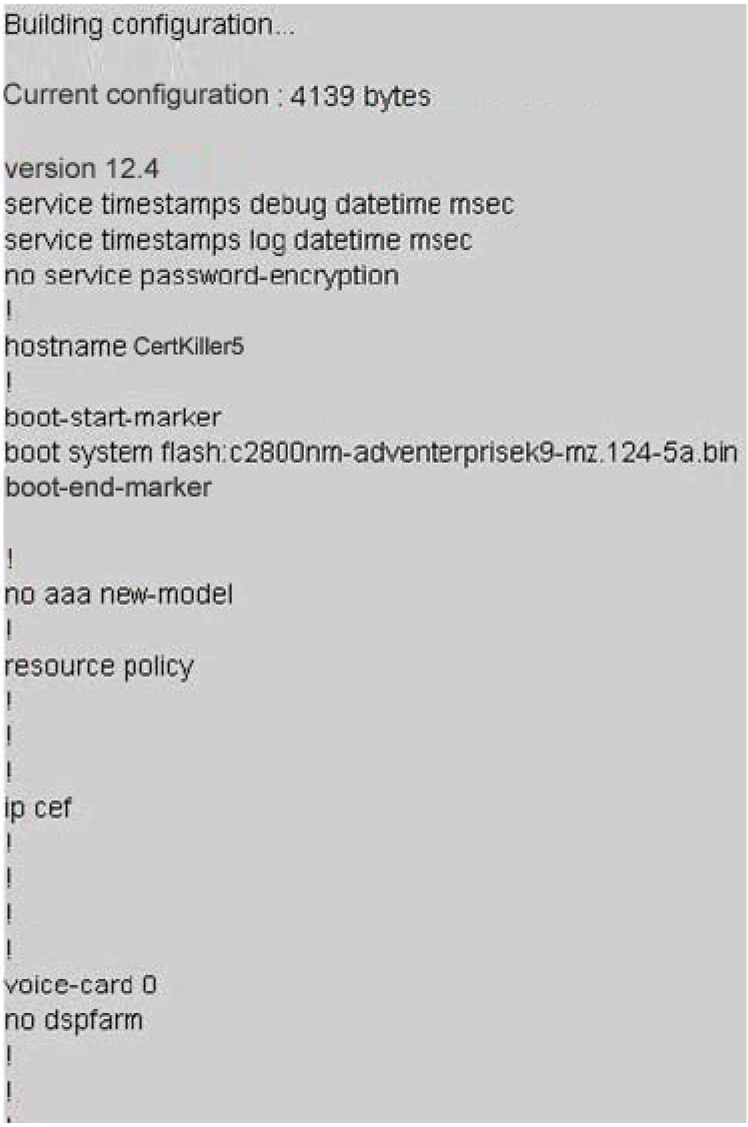


You are an employee of Certkiller .com, which is a large company with offices in the US, Europe, Asia, and Africa. You work a network technician at the Kuala Lumpur branch office of Certkiller .com. During the last month Certkiller .com has applied QoS policies at the Kuala Lumpur branch office router Certkiller 5. The Certkiller .com Luala Lumpur boss, Miss Certkiller, has asked you personally to provide important documentation regarding this upgrade.

There is also a known issue at the Kuala Lumpur office. The recently installed video-conference equipment often has poor video quality. After some investigation you conclude that the video problems only occur during office peak hours, when some network congestion is to be expected.

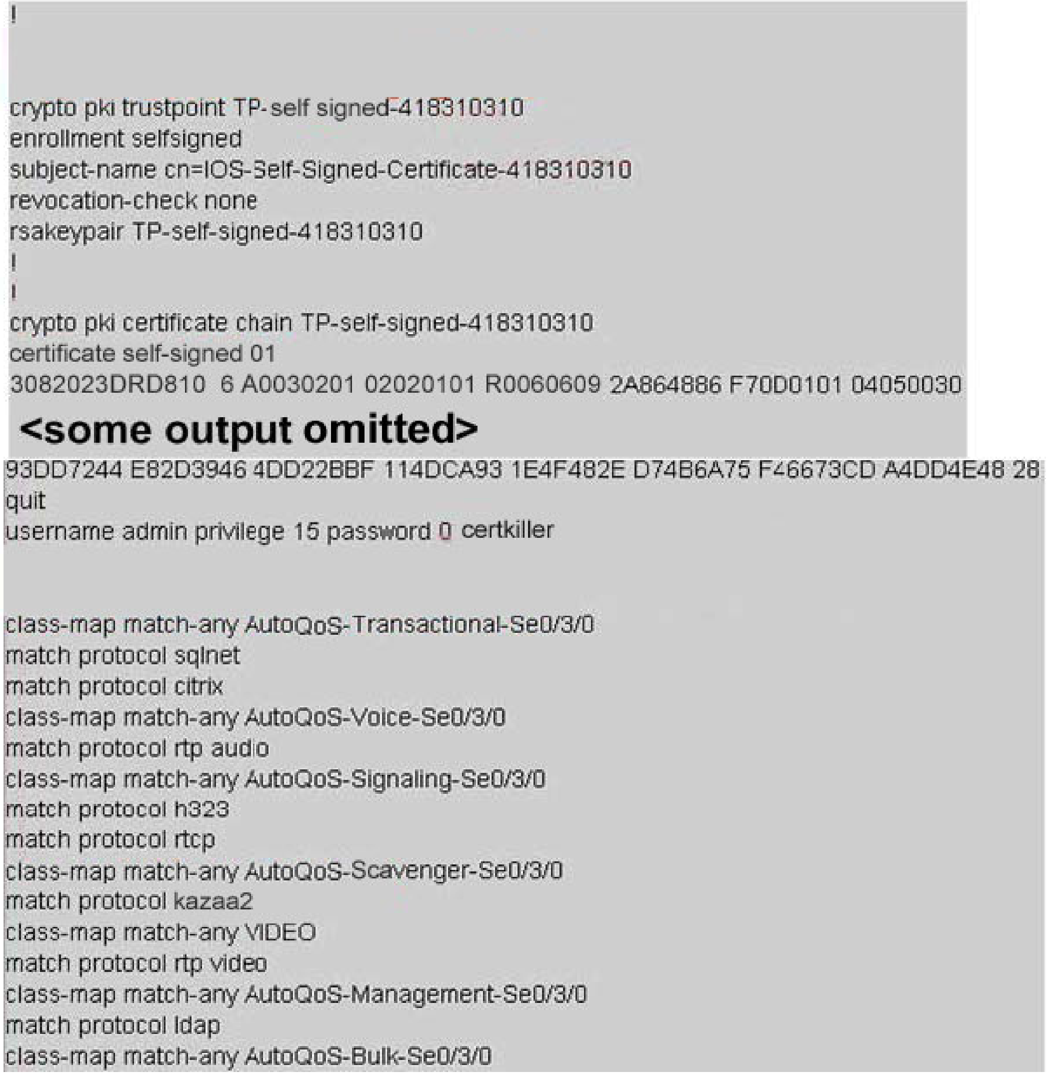
You need to use show run command outputs on Certkiller 5 to obtain the information which would be necessary to answer the questions of this scenario. Study the configuration exhibits carefully.

Configuration exhibit #1



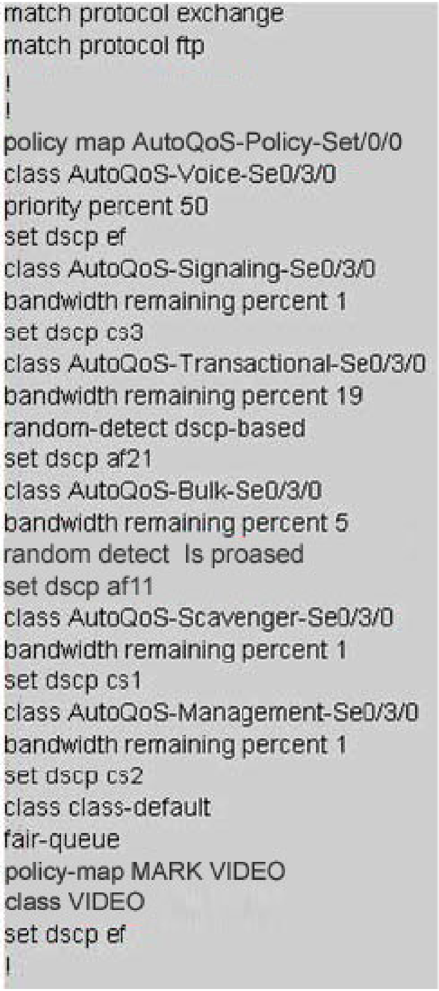
```
Building configuration...

Current configuration : 4139 bytes

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CertKiller5
!
boot-start-marker
boot system flash:c2800nm-adventerprisek9-mz.124-5a.bin
boot-end-marker

!
no aaa new-model
!
resource policy
!
!
!
ip cef
!
!
!
!
voice-card 0
no dspfarm
!
!
```

Configuration exhibit #2 (continued)



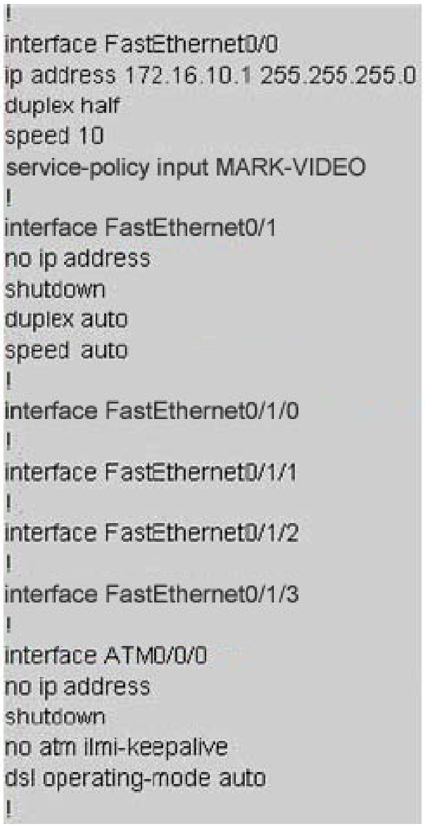
```
!


crypto pki trustpoint TP-self signed-418310310
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-418310310
revocation-check none
rsakeypair TP-self-signed-418310310
!
!
crypto pki certificate chain TP-self-signed-418310310
certificate self-signed 01
3082023DRD810  6 A0030201 02020101 R0060609 2A864886 F70D0101 04050030
 <some output omitted>
93DD7244 E82D3946 4DD22BBF 114DCA93 1E4F482E D74B6A75 F46673CD A4DD4E48 28
quit
username admin privilege 15 password 0 certkiller


class-map match-any AutoQoS-Transactional-Se0/3/0
match protocol sqlnet
match protocol citrix
class-map match-any AutoQoS-Voice-Se0/3/0
match protocol rtp audio
class-map match-any AutoQoS-Signaling-Se0/3/0
match protocol h323
match protocol rtcp
class-map match-any AutoQoS-Scavenger-Se0/3/0
match protocol kazaa2
class-map match-any VIDEO
match protocol rtp video
class-map match-any AutoQoS-Management-Se0/3/0
match protocol ldap
class-map match-any AutoQoS-Bulk-Se0/3/0
```

Configuration exhibit #3 (continued)



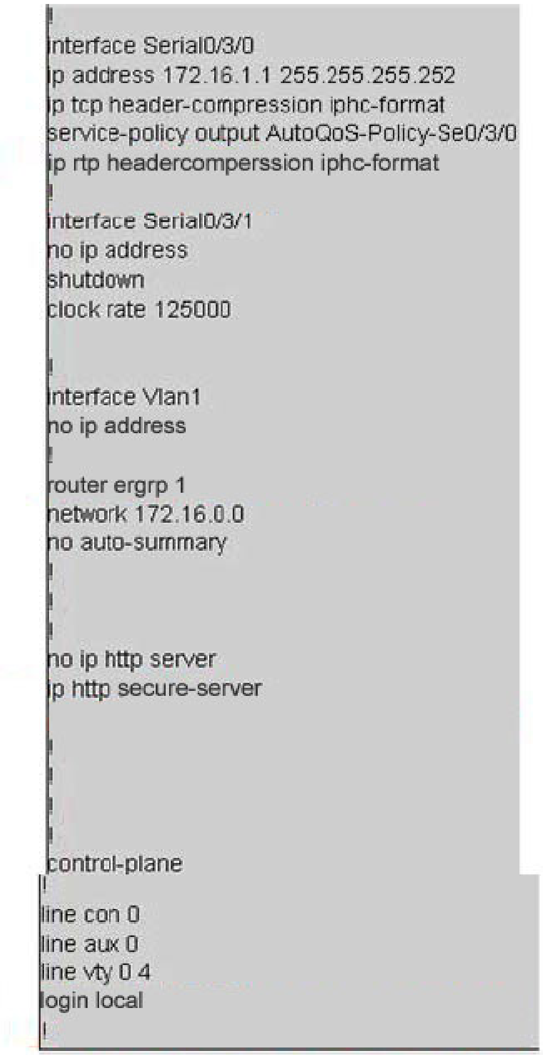
```
match protocol exchange
match protocol ftp
!
!
policy map AutoQoS-Policy-Set/0/0
class AutoQoS-Voice-Se0/3/0
priority percent 50
set dscp ef
class AutoQoS-Signaling-Se0/3/0
bandwidth remaining percent 1
set dscp cs3
class AutoQoS-Transactional-Se0/3/0
bandwidth remaining percent 19
random-detect dscp-based
set dscp af21
class AutoQoS-Bulk-Se0/3/0
bandwidth remaining percent 5
random detect  Is proased
set dscp af11
class AutoQoS-Scavenger-Se0/3/0
bandwidth remaining percent 1
set dscp cs1
class AutoQoS-Management-Se0/3/0
bandwidth remaining percent 1
set dscp cs2
class class-default
fair-queue
policy-map MARK VIDEO
class VIDEO
set dscp ef
!
```

Configuration exhibit #4 (continued)



```
!
interface FastEthernet0/0
ip address 172.16.10.1 255.255.255.0
duplex half
speed 10
service-policy input MARK-VIDEO
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1/0
!
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
!
interface ATM0/0/0
no ip address
shutdown
no atm ilmi-keepalive
dsl operating-mode auto
!
```

Configuration exhibit #5 (continued)



```
!
interface Serial0/3/0
ip address 172.16.1.1 255.255.255.252
ip tcp header-compression iphc-format
service-policy output AutoQoS-Policy-Se0/3/0
ip rtp headercomperssion iphc-format
!
interface Serial0/3/1
no ip address
shutdown
clock rate 125000

!
interface Vlan1
no ip address
!
router ergrp 1
network 172.16.0.0
no auto-summary
!
!
!
no ip http server
ip http secure-server

!
!
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
login local
!
```

Topic 1, Certkiller 1 (4 Questions)

QUESTION 202
Note: Please refer to Certkiller Scenario 1
Which DSCP value will the Branch router apply to video traffic destined for the Central site from the video equipment on the local network?

A. 46 (ef)
B. 24 (cs3)
C. 18 (af21)
D. 8 (cs1)
E. no value
F. 10 (af11)
G. None of the above

Answer: A

Explanation:
The classification is carried in the IP packet header, using either the IP precedence or the preferred Differential Services Code Point (DSCP). These are represented using the first three or six bits of the Type of Service (ToS) field. Classification can also be carried in the Layer 2 frame in the form of the Class of Service (CoS) field embodied in ISL and 802.1Q frames.
Once packets are classified at the edge by access layer switches or by border routers, the network uses the classification to determine how the traffic should be queued, shaped, and policed.

QUESTION 203
Note: Please refer to Certkiller Scenario 1
Which QoS model has been implimented on the Branch router by Auto QoS for the various expected traffic types?

A. IntServ
B. Priority Queuing
C. Best Effort
D. DiffServ
E. None of the above

Answer: C

Explanation:
Best-effort model: With the best-effort model, QoS is not applied to packets. If it is not important when or how packets arrive, the best-effort model is appropriate.

QUESTION 204
Note: Please refer to Certkiller Scenario 1
During periods of congestion, how has AutoQoS configured the router to facilitate outbound video traffic on the Serial0/3/0 interface?

A. Video traffic will be associated with the priority queue by using a DSCP value of 46 (ef).
B. Video traffic will only be queued on the local FastEthernet0/0 interface using a DSCP value of 46 (ef).
C. Video traffic will be associated with the "class-default" and use WFQ.
D. Video traffic will be associated with the AutoQoS-Signaling-Se0/3/0 class and its related policy through use of the H.323 protocol.
E. None of the above.

Answer: A

Explanation:
Classification is the process of identifying traffic and categorizing that traffic into classes. Classification uses a traffic descriptor to categorize a packet within a specific

group to define that packet. Typically used traffic descriptors include these:
1. Incoming interface
2. IP precedence
3. differentiated services code point (DSCP)
4. Source or destination address
5. Application
After the packet has been classified or identified, the packet is then accessible for quality of service (QoS) handling on the network.
Using classification, network administrators can partition network traffic into multiple classes of service (CoSs). When traffic descriptors are used to classify traffic, the source implicitly agrees to adhere to the contracted terms and the network promises QoS.
Various QoS mechanisms, such as traffic policing, traffic shaping, and queuing techniques, use the traffic descriptor of the packet (that is, the classification of the packet) to ensure adherence to that agreement.
Classification should take place at the network edge, typically in the wiring closet, within IP phones, or at network endpoints. It is recommended that classification occur as close to the source of the traffic as possible.

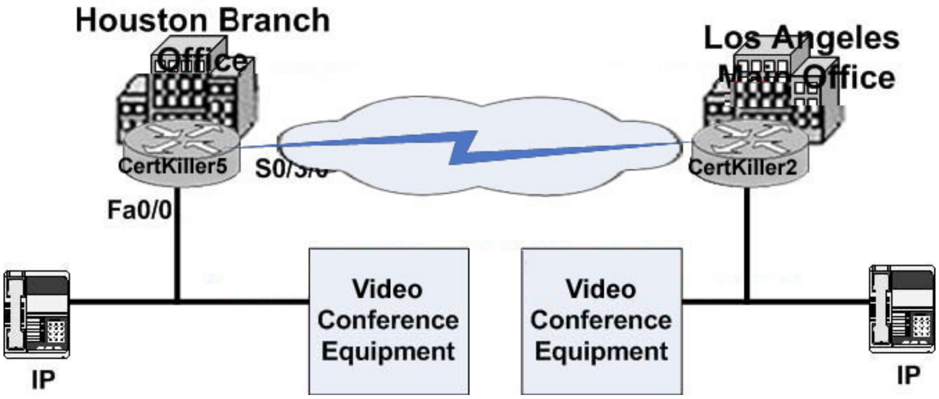
QUESTION 205
Note: Please refer to Certkiller Scenario 1
Which two statements most accurately identify what has caused the occasional poor video quality experienced by the Law Solutions, Inc.? (Select two.)

A. AutoQoS was implemented on the incorrect interface
B. Auto-Discovery did not have an opportunity to detect the video traffic.
C. Insufficient bandwidth is creating a bottleneck transiting from the FastEthernet0/0 to the Serial0/3/0 interface.
D. A policy matching DSCP value 46 (ef) was not applied on the outbound interface.
E. None of the above

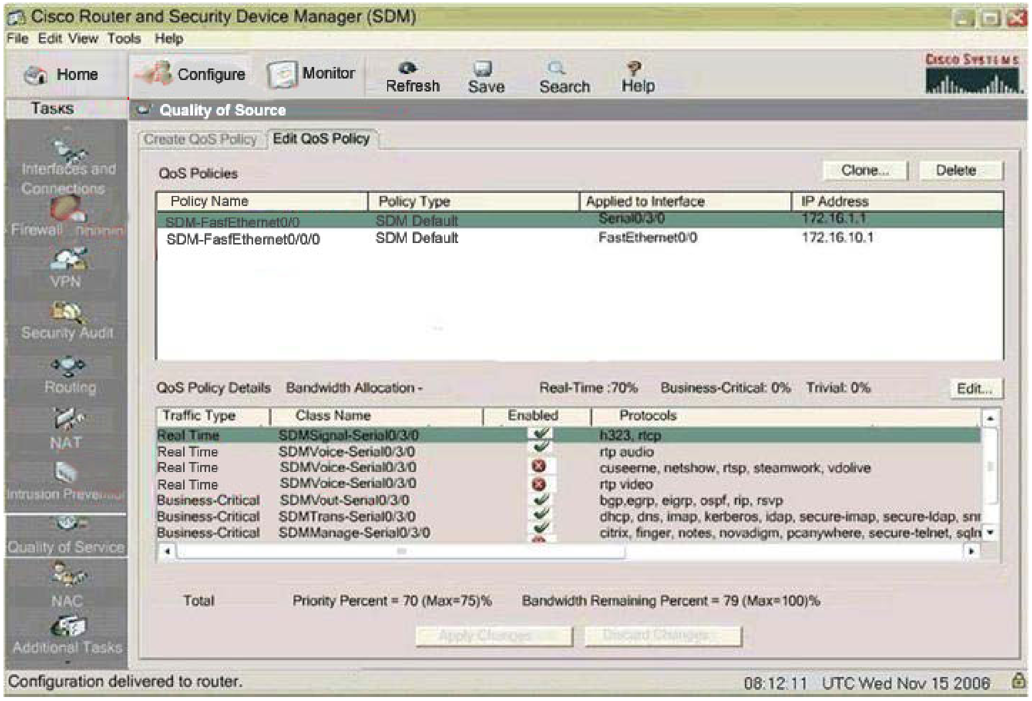
Answer: B, D

Topic 2: Certkiller 2, Scenario

Network topology exhibit:



SDM Output exhibit:



Quality of Source

QoS Policies

Policy Name	Policy Type	Applied to Interface	IP Address
SDM-FasfEthernet0/0	SDM Default	Serial0/3/0	172.16.1.1
SDM-FasfEthemet0/0/0	SDM Default	FastEthernet0/0	172.16.10.1

QoS Policy Details Bandwidth Allocation - Real-Time :70% Business-Critical: 0% Trivial: 0%

Traffic Type	Class Name	Enabled	Protocols
Real Time	SDMSignal-Serial0/3/0	✓	h323, rtcp
Real Time	SDMVoice-Serial0/3/0	✓	rtp audio
Real Time	SDMVoice-Serial0/3/0	☒	cuseeme, netshow, rtsp, steamwork, vdolive
Real Time	SDMVoice-Serial0/3/0	☒	rtp video
Business-Critical	SDMVout-Serial0/3/0	✓	bgp.egrp, eigrp, ospf, rip, rsvp
Business-Critical	SDMTrans-Serial0/3/0	✓	dhcp, dns, imap, kerberos, idap, secure-imap, secure-ldap, snr
Business-Critical	SDMManage-Serial0/3/0	✓	citrix, finger, notes, novadigm, pcanywhere, secure-telnet, sqln

Total Priority Percent = 70 (Max=75)% Bandwidth Remaining Percent = 79 (Max=100)%

Configuration delivered to router. 08:12:11 UTC Wed Nov 15 2006

You are an employee of Certkiller .com, which is a large company with offices in the US and Europe You work a network technician at the Houston branch office of Certkiller .com. During the last month Certkiller .com has applied QoS policies at Houston branch office router Certkiller 5. The Certkiller .com Houston boss, Miss Certkiller, has asked you personally to provide important documentation regarding this upgrade.

You need to use the SDM output on Certkiller 5 to obtain the information which would be necessary to answer the questions of this scenario. Study the SDM output exhibits carefully.

Topic 2, Certkiller 2 (3 Questions)

QUESTION 206

Note: Please refer to Certkiller Scenario 2

Which DSCP value will the Certkiller 5 branch router apply to voice traffic destined for the IP Phone on the local network from the Certkiller 2 router at the main site?

A. 56 (cs7)
B. 70
C. 46 (ef)
D. 50
E. 48 (cs6)
F. None of the above

Answer: C

QUESTION 207
Note: Please refer to Certkiller Scenario 2
Which DSCP value will the Certkiller 5 ranch router apply to voice traffic destined for the Main office from the IP Phone on the local network?

A. 48 (vs6)
B. 50
C. 56(cs7)
D. 70
E. 46 (ef)
F. 48 (cs6)
G. None of the above

Answer: F

QUESTION 208
Note: Please refer to Certkiller Scenario 2
Which QoS model has been implemented on the Branch router by the SDM wizard for the various expected traffic types?

A. IntServ
B. Priority Queuing
C. Best Effort
D. DiffServ
E. None of the above

Answer: D

Explanation:
Differentiated Services (DiffServ): DiffServ provides the greatest scalability and flexibility in implementing QoS in a network. Network devices recognize traffic classes and provide different levels of QoS to different traffic classes.