Vendor: Cisco

Exam Code: 642-642

Exam Name: Quality of Service (QoS)

Version: Demo

QUESTION 1
Which of the following configurations requires the use of hierarchical policy maps?

A. the use of nested class-maps with class-based marking
B. the use of a strict priority-class queue within CBWFQ
C. the use of class-based WRED within a CBWFQ class queue
D. the use of CBWFQ inside class-based shaping
E. the use of both the bandwidth and shape statements within a CBWFQ class queue

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

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.

QUESTION 2
In a managed CE scenario, the customer's network is supporting VoIP and bulk file transfers. According to the best practices, which QoS mechanisms should be applied on the WAN edge CE-PE 56-kbps Frame Relay link on the CE outbound direction?

A. LLQ, CB-WRED, CB-Marking, FRTS, FRF.12, and CB-RTP header compression
B. CBWFQ, FRTS, FRF.12, and CB-RTP header compression
C. WRR, CB-WRED, CB-Marking, FRF.12, and CB-RTP header compression
D. WRR, FRTS, FRF.12, and CB-RTP header compression
E. LLQ, CB-WRED, CB-Policing, and CB-TCP and CB-RTP header compressions
F. CBWFQ, CB-WRED, CB-Marking, CB-Policing, and FRTS

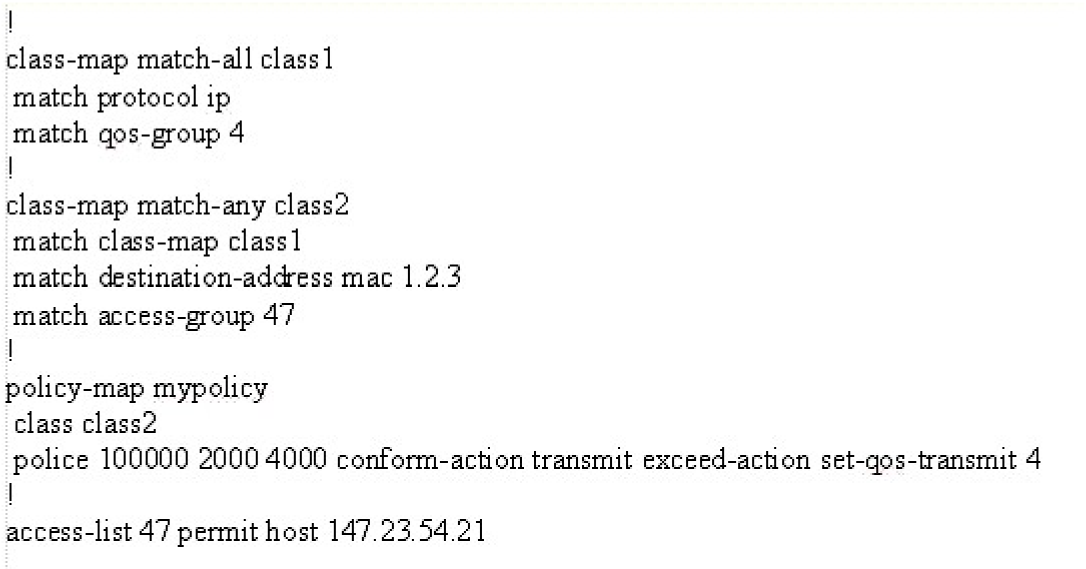
Correct Answer: A
Explanation

Explanation/Reference:
Explanation:

1. WRED can be combined with CBWFQ. In this combination CBWFQ provides a guaranteed percentage of the output bandwidth, WRED ensures that TCP traffic is not sent faster than CBWFQ can forward it. The abbreviated configuration below shows how WRED can be added to a policy-map specifying CBWFQ: Router(config)#policy-map prioritybwRouter(config-pmap)#class class-default fair- queueRouter(config-pmap-c)#class prioritytraffic bandwidth percent 40 random-detect The random-detect parameter specifies that WRED will be used rather than the default tail-drop action.
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. 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 3
Refer to the partial router configuration. Which two of the following statements are true? (Choose two.)



```
!
class-map match-all class1
 match protocol ip
 match qos-group 4
!
class-map match-any class2
 match class-map class1
 match destination-address mac 1.2.3
 match access-group 47
!
policy-map mypolicy
 class class2
 police 100000 2000 4000 conform-action transmit exceed-action set-qos-transmit 4
!
access-list 47 permit host 147.23.54.21
```

A. Regardless of destination IP address, all traffic sent to Mac address 1.2.3 will be subject to policing
B. All traffic from a server with the IP address of 147.23.54.21 will be subject to policing.
C. Any IP packet will be subject to policing.
D. The class-map class1 command will set the qos-group value to 4 for all IP packets.
E. Only those packets which satisfy all of the matches in class1 and class2 will be subject to policing.
F. The configuration is invalid since it refers to a class map within a different class.

Correct Answer: AB
Explanation

Explanation/Reference:
Explanation:

The class-map command is used to define a traffic class. The purpose of a traffic class is to classify traffic that should be given a particular QoS. A traffic class contains three major elements, a name, a series of match commands, and if more than one match command exists in the traffic class, an instruction on how to

evaluate these match commands. The traffic class is named in the class-map command line. For example, if the class-map cisco command is entered while configuring the traffic class in the CLI, the traffic class would be named cisco.
Switch(config)#class-map ciscoSwitch(config-cmap)#
match commands are used to specify various criteria for classifying packets. Packets are checked to determine whether they match the criteria specified in the match commands. If a packet matches the specified criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class and will be subject to a separate traffic policy The policy-map command is used to create a traffic policy. The purpose of a traffic policy is to configure the QoS features that should be associated with the traffic that has been classified in a user- specified traffic class. A traffic policy contains three elements:
The policy-map shown below creates a traffic policy named policy1. The policy applies to all traffic classified by the previously defined traffic-class "cisco" and specifies that traffic in this example should be allocated bandwidth of 3000 kbps. Any traffic which does not belong to the class "cisco" forms part of the catch-all class-default class and will be given a default bandwidth of 2000 kbps. Switch(config)#policy-map policy1Switch(config-pmap)#class ciscoSwitch(config-pmap- c)#bandwidth 3000Switch(config-pmap-c) #exitSwitch(config-pmap)#class class-defaultSwitch(config- pmap-c)#bandwidth 2000Switch(config-pmap) #exit

QUESTION 4
In an unmanaged CE router implementation, how does the service provider enforce the SLA?

A. by marking on the CE to PE link and using CBWFQ and CB-WRED on the PE to P link
B. by marking on the CE to PE link and using class-based policing on the PE to P link
C. by using class-based policing on the CE to PE link to limit the customer's input rate
D. by using class-based random discard on the CE to PE link to limit the customer's input rate

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:

In an unmanaged Router Implementation, Service provider can enforce SLA By using class based policy on the CE to PE link to limit the customer's input rate.

QUESTION 5
When configuring a Cisco Catalyst switch to accommodate an IP phone with an attached PC, it is desired that the trust boundary be set between the IP phone and the switch. Which two commands on the switch are recommended to set the trust boundary as described? (Choose two.)

A. mls qos trust device cisco-phone
B. switchport priority extend trust
C. mls qos trust cos
D. no mls qos trust dscp
E. mls qos trust extend [cos value]
F. mls qos cos 5

Correct Answer: AC
Explanation

Explanation/Reference:
Explanation:

mls qos trust [cos] :
By default, the port is not trusted. All traffic is sent through one egress queue. Use the cos keyword to classify ingress packets with the packet CoS values. The egress queue assigned to the packet is based on the packet CoS value. When this keyword is entered, the traffic is sent through the four QoS queues.
Normally, the QoS information from a PC connected to an IP Phone should not be trusted. This is because the PC's applications might try to spoof CoS or Differentiated Services Code Point (DSCP) settings to gain

premium network service. In this case, use the cos keyword so that the CoS bits are overwritten to value by the IP Phone as packets are forwarded to the switch. If CoS values from the PC cannot be trusted, they should be overwritten to a value of 0.

QUESTION 6
According to the best practices, in a service provider network, which statement is true as related to the QoS policy that should be implemented on the inbound provider (P) to provider (P) router link?

A. In the DiffServ model, all ingress and egress QoS processing are done at the network edge (for example, PE router), so no input or output QoS policy will be needed on the P to P link.
B. Class-based marking should be implemented because it will be needed for the class-based queuing that will be used on the P router output.
C. Traffic policing should be implemented to rate-limit the ingress traffic into the P router.
D. Because traffic should have already been policed and marked on the upstream ingress PE router, no input QoS policy is needed on the P to P link.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
A Frame Relay interface has been configured for adaptive shaping with a minimum rate of 15 kbps. The current maximum transmit rate is 56 kbps.

If three FECNs are received over the next 4 seconds, what will be the maximum transmit rate after the last FECN has been received?

A. 10 kbps
B. 37 kbps
C. 7 kbps
D. 15 kbps
E. 28 kbps
F. 56 kbps

Correct Answer: F
Explanation

Explanation/Reference:
Explanation:

User specified traffic shaping can be performed on a Frame Relay interface or sub-interface with the traffic-shape rate command. The traffic-shape adaptive command can be specified to allow the shape of the traffic to dynamically adjust to congestion experienced by the Frame-Relay provider. This is achieved through the reception of Backward Explicit Congestion Notifications (BECN) from the Frame Relay switch. When a Frame Relay switch becomes congested it sends BECNs in the direction the traffic is coming from and it generates Forward Explicit Congestion Notifications (FECN) in the direction the traffic is flowing to. If the traffic-shape fecn-adapt command is configured at both ends of the link, the far end will reflect FECNs as BECNs. BECNs notify the sender to decrease the transmission rate. If the traffic is one-way only, such as multicast traffic, there is no reverse traffic with BECNs to notify the sender to slow down. Therefore, when a DTE device receives a FECN, it first determines if it is sending any data in return. If it is sending return data, this data will get marked with a BECN on its way to the other DTE device. However, if the DTE device is not sending any data, the DTE device can send a Q.922 TEST RESPONSE message with the BECN bit set.

QUESTION 8
Based on the following show output, which statement is true?

```
WG1S1#sh mls qos interface fa0/1
FastEthernet0/1
```

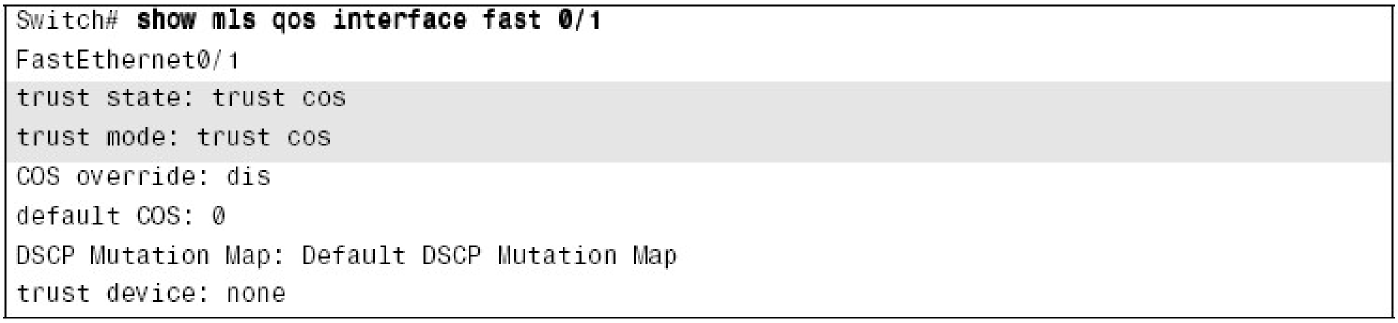
```
trust state: not trusted
trust mode: trust cos
COS override: dis
default COS: 0
pass-through: none
trust device: cisco-phone
```

A. A Cisco IP Phone is not connected to the fa0/1 switch port.
B. All incoming DSCP markings are trusted.
C. All incoming CoS markings are trusted.
D. DSCP markings from the Cisco IP Phone are trusted.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation:

mls qos trust [cos] :
By default, the port is not trusted. All traffic is sent through one egress queue. Use the cos keyword to classify ingress packets with the packet CoS values. The egress queue assigned to the packet is based on the packet CoS value. When this keyword is entered, the traffic is sent through the four QoS queues. The Output shown that Phone is not connected with Switch Port.



```
Switch# show mls qos interface fast 0/1
FastEthernet0/1
trust state: trust cos
trust mode: trust cos
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
trust device: none
```

QUESTION 9
In a typical converged campus network, which two of the following are considered QoS best practices? (Choose two.)

A. Traffic classification and marking is performed as close to the traffic source as possible.
B. NBAR is used at the high speed core layer to discover and classify network applications.
C. Catalyst switches should use weighted round robin (WRR) queuing giving the voice traffic the highest priority.
D. Ensure voice traffic is serviced by a weighted fair queue.
E. Traffic classification and marking is performed at the high speed core layer.
F. Only a reasonable number of applications should be classified into the mission-critical traffic class.

Correct Answer: AF
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
A Cisco Catalyst switch has an IP phone connected to its Fastethernet0/2 port. The IP phone has an attached PC. The Fastethernet0/2 port on the switch has been configured with the commands mls qos trust cos, mls qos trust device cisco-phone, and switchport priority extend trust.

What will happen to a data frame with a CoS of 5 that is sent from the PC through the IP phone to port

Fastethernet0/2 on the switch?

A. While the packet will pass through the IP phone without modification, the switch will, by default, override the CoS priority with the switch default CoS priority.
B. The switch will instruct the phone to allow the packet through without modification only if the phone has been configured to do so.
C. The IP phone will allow the data packet through without modifying the CoS settings of the data frame.
D. The IP phone will, by default, overwrite the switch CoS value and mark the data packet as CoS 0.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:

In a typical network, you connect a Cisco IP Phone to a switch port. Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the CoS 3-bit field, which determines the priority of the packet. For most Cisco IP Phone configurations, the traffic sent from the telephone to the switch is trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network. By using the mls qos trust cos interface configuration command, you can configure the switch port to which the telephone is connected to trust the CoS labels of all traffic received on that port. In some situations, you also might connect a PC or workstation to the IP phone. In these cases, you can use the switchport priority extend cos interface configuration command to configure the telephone through the switch CLI to override the priority of the traffic received from the PC. With this command, you can prevent a PC from taking advantage of a high-priority data queue. However, if a user bypasses the telephone and connects the PC directly to the switch, the CoS labels generated by the PC are trusted by the switch (because of the trusted CoS setting) and can allow misuse of high-priority queues. The trusted boundary feature solves this problem by using the CDP to detect the presence of a Cisco IP Phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a switch port. If the telephone is not detected, the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue.

QUESTION 11
What does the following command accomplish?

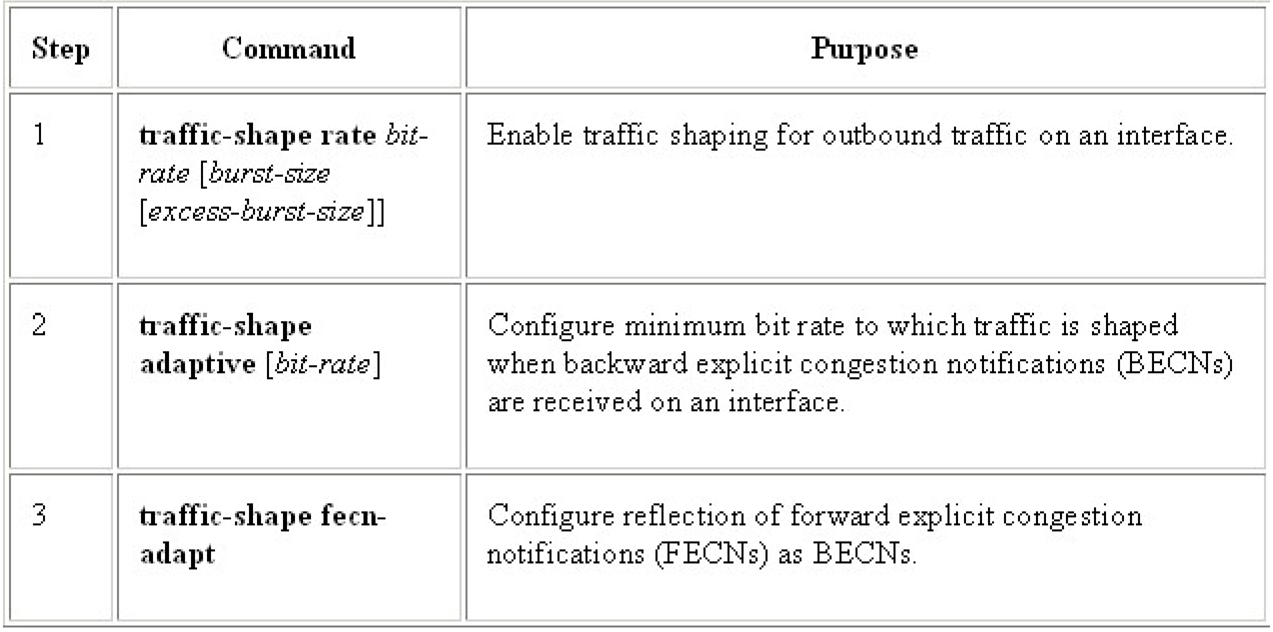
```
router(config-pmap-c)# shape fecn-adapt
```

A. enables the router to lower the shaping rate when FECN bits are received
B. enables the router to increase the shaping rate when BECN bits are received
C. enables the router to respond to FECN bits by creating test frames in the opposite direction with the BECN bit set
D. enables the router to lower the shaping rate when BECN bits are received
E. enables the router to respond to BECN bits by creating test frames in the opposite direction with the FECN bit set
F. enables the router to increase the shaping rate when FECN bits are received

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:

Configure Adaptive Generic Traffic Shaping for Frame Relay Networks If traffic shaping is performed on a Frame Relay network using the traffic-shape rate command, you can also use the traffic-shape adaptive command to specify the minimum bit rate to which the traffic is shaped.
To configure adaptive GTS for outbound traffic on an interface or subinterface, use the following commands in interface configuration mode:



Step	Command	Purpose
1	**traffic-shape rate** *bit-rate* [*burst-size* [*excess-burst-size*]]	Enable traffic shaping for outbound traffic on an interface.
2	**traffic-shape adaptive** [*bit-rate*]	Configure minimum bit rate to which traffic is shaped when backward explicit congestion notifications (BECNs) are received on an interface.
3	**traffic-shape fecn-adapt**	Configure reflection of forward explicit congestion notifications (FECNs) as BECNs.

With adaptive GTS, the router uses backward explicit congestion notifications (BECNs) to estimate the available bandwidth and adjust the transmission rate accordingly. The actual maximum transmission rate will be between the rate specified in the traffic-shape adaptive command and the rate specified in the traffic-shape rate command.

QUESTION 12
To determine the bandwidth requirement for each VoIP call, not including Layer 2 overhead, how much bandwidth per call should be added to account for the voice signaling traffic?

A. 20 bps
B. 640 bps
C. 40 bps
D. 480 bps
E. 150 bps
F. 240 bps

Correct Answer: E
Explanation

Explanation/Reference:
Explanation:

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 13
Which mechanism is used for the prioritizing, protection, and isolation of traffic based on marking?

A. policing
B. metering
C. shaping

D. classification and marking
E. congestion avoidance
F. congestion management

Correct Answer: F
Explanation

Explanation/Reference:
Explanation:

Congestion management is needed here. It deals with prioritization, protection and isolation of traffic. All this mechanisms are used for congestion avoidance.

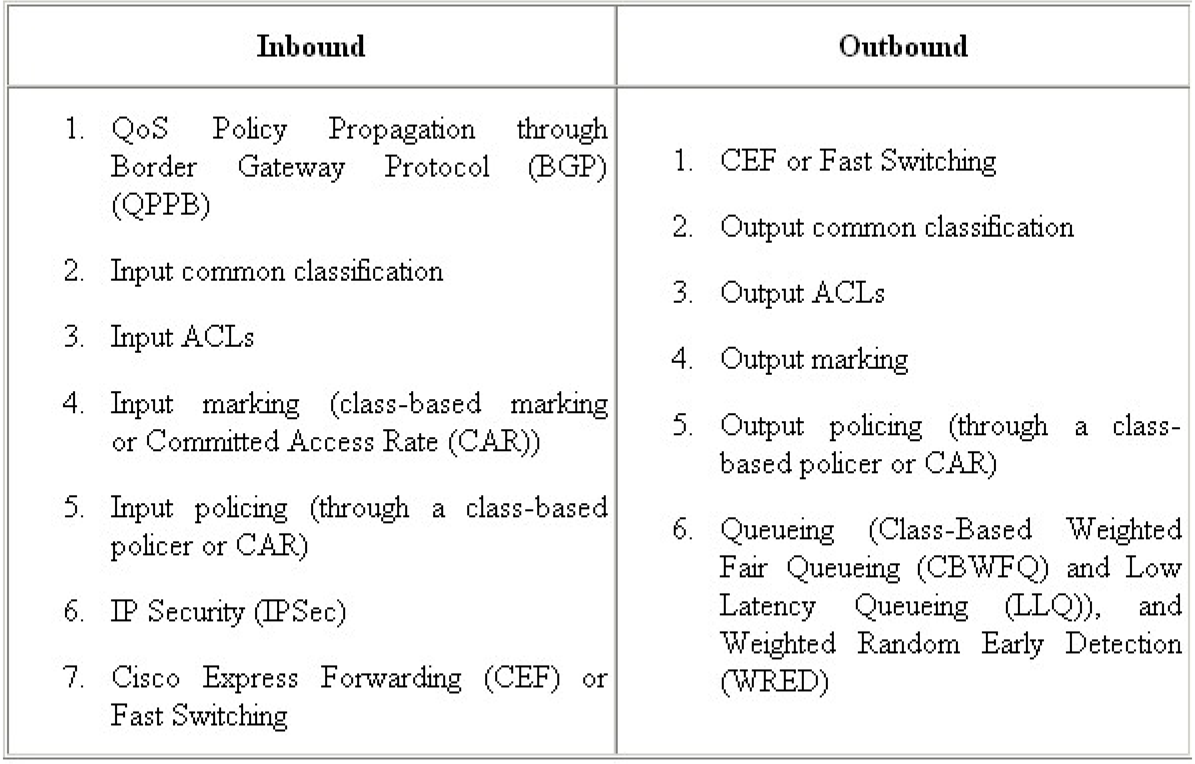
QUESTION 14
Which element is mandatory for QoS policy propagation through BGP operations?

A. MQC
B. QoS pre-classify
C. policy-based routing
D. NBAR
E. CEF
F. MPLS

Correct Answer: E
Explanation

Explanation/Reference:
Explanation:

Common Classification
Classification is the process of defining traffic classes that sort traffic into categories groups of flows. Classification defines the "match criteria" for each class of traffic that is to be treated by a QoS policy. More specifically, it defines the "traffic filter" that packets are checked against when a service-policy is applied. Both distributed and non-distributed platforms match packets to a single class in a policy-map. Matching terminates at the first matching class. If two classes within a policy-map match the same IP precedence or IP address range, the packet always belongs to the first matching class. For this reason, class order within a policy-map is very important.
This classification approach is called "common classification" and has these benefits:
Common classification is enabled automatically when you attach an input or output policy-map with the service-policy command.
The table below illustrates the order of operation with common classification. It is important to understand from the table when classification occurs in the context of QoS features. On the inbound path, a packet is classified before it is switched. On the outbound path, a packet is classified after it is switched.



Inbound	Outbound
1. QoS Policy Propagation through Border Gateway Protocol (BGP) (QPPB) 2. Input common classification 3. Input ACLs 4. Input marking (class-based marking or Committed Access Rate (CAR)) 5. Input policing (through a class-based policer or CAR) 6. IP Security (IPSec) 7. Cisco Express Forwarding (CEF) or Fast Switching	1. CEF or Fast Switching 2. Output common classification 3. Output ACLs 4. Output marking 5. Output policing (through a class-based policer or CAR) 6. Queueing (Class-Based Weighted Fair Queueing (CBWFQ) and Low Latency Queueing (LLQ)), and Weighted Random Early Detection (WRED)

Note: Inbound Network-Based Application Recognition (NBAR) happens after ACLs and before policy-based routing.
Important changes have been implemented regarding feature ordering and remarked value usage. These changes include moving input CAR, input MAC, and IP precedence accounting functions to occur before MQC output classification:

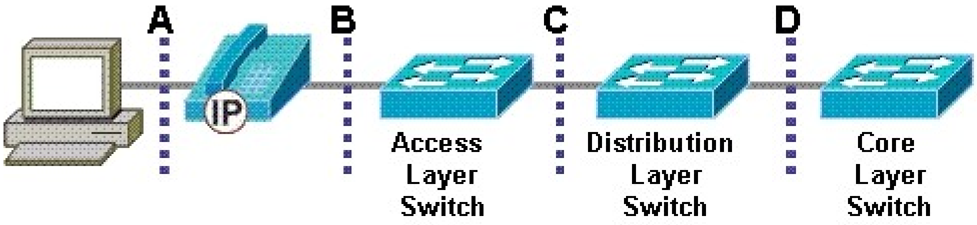
QUESTION 15
Which two commands are typically applied to the voice traffic class within a policy-map? (Choose two.)

A. bandwidth {kbps}
B. random-detect dscp-based
C. shape peak {bps}
D. compress header ip rtp
E. priority {kbps}
F. random-detect ecn

Correct Answer: DE
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
Refer to the exhibit. A typical configuration involving an IP phone with an attached PC is shown. According to QoS recommendations, at which demarcation line (shown as dotted lines) would the trust boundary normally exist?



A. B
B. A
C. D
D. C

Correct Answer: A
Explanation

Explanation/Reference:
Explanation:

In a typical network, you connect a Cisco IP Phone to a switch port. Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the CoS 3-bit field, which determines the priority of the packet. For most Cisco IP Phone configurations, the traffic sent from the telephone to the switch is trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network. By using the mls qos trust cos interface configuration command, you can configure the switch port to which the telephone is connected to trust the CoS labels of all traffic received on that port. In some situations, you also might connect a PC or workstation to the IP phone. In these cases, you can use the switchport priority extend cos interface configuration command to configure the telephone through the switch CLI to override the priority of the traffic received from the PC. With this command, you can prevent a PC from taking advantage of a high-priority data queue. However, if a user bypasses the telephone and connects the PC directly to the switch, the CoS labels generated by the PC are trusted by the switch (because of the trusted CoS setting) and can allow misuse of high-priority queues. The trusted boundary feature solves this problem by using the CDP to detect the presence of a Cisco IP Phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a switch port. If the telephone is not detected, the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue.
So, boundary exists between PC Phone and Switch.

QUESTION 17
At the network layer, IP packets are typically classified based on which three items? (Choose three.)

A. source and destination IP addresses
B. flow control bits
C. VLAN Identifier
D. packet length
E. content of the ToS byte

Correct Answer: ADE
Explanation

Explanation/Reference:
Explanation:

References:

QUESTION 18
A major media company recently deployed a new converged network. The original network design used separate networks for graphics and video, interactive data, and voice. The company has been experiencing problems with voice traffic in the new converged network. Most of the time voice quality is perfectly acceptable. Periodically voice quality exhibits unacceptable choppy voice signals, and occasionally calls are dropped. At this time the company is not willing to simply add bandwidth to the network.

Which QoS solution would most likely help to resolve the problem?

A. Prioritize voice traffic as the highest priority to ensure that voice traffic is always serviced by the priority queue.
B. Use advanced technologies to compress all video and graphics traffic on the network.

C. Use TCP header compression and LFI to reduce delays.
D. Use class-based weighted fair queuing to prioritize voice traffic with a higher weight than all other traffic.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation:
The need to prioritize packets arises from the diverse mixture of protocols and their associated behaviors found in the data networks of today. Different types of traffic that share a data path through the network can impact each other.
Depending on the application and overall bandwidth, users may perceive performance degradation. Interactive audio data is delay sensitive, and transaction-based applications may require a higher priority than a file transfer. Videoconferencing requires a specified amount of bandwidth for acceptable performance. If the network is designed so that multiple protocols share a single data path between routers, prioritization may be necessary at the congestion points. Prioritization is most effective on WAN links where the combination of traffic bursts and relatively lower data rates can cause temporary congestion. Depending on the average packet size, prioritization is most effective when applied to links at T1/E1 bandwidth speeds or lower. If there is no congestion on the WAN link, traffic prioritization is not necessary. If a WAN link is constantly congested, traffic prioritization may not resolve the problem. Adding bandwidth might be the appropriate solution.

QUESTION 19
Where is the error in the following policy-map configuration?

```
policy-map test
class voice
priority 168
class mission-critical
bandwidth 192
random-detect
class class-default
fair-queue
bandwidth 128
```

A. The bandwidth command is not a valid command for the class-default traffic class in this case.
B. The mission-critical traffic class is missing the queue-limit command.
C. The voice traffic class is missing the random-detect command.
D. The mission-critical traffic class bandwidth guarantee should be lower than the voice traffic class priority bandwidth guarantee.
E. Fair-queue should be enabled for the mission-critical traffic class.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation:

The simplicity of configuration is made possible through the use of a common configuration structure for all QoS components within the MQC. That is, the basic configuration steps for configuring all QoS mechanisms is the same, with only small variations in the configuration that are specific to the actual mechanism. You can configure all the mechanisms through a three-step process:
Step 1. Class map configuration
Step 2. Policy map configuration
Step 3. Service policy application

The Class-map

The first step for configuring any QoS mechanism in the MQC is the configuration of a class-map. Simply stated, the class map defines which traffic you want the router to match. This is the fundamental step that allows the router to differentiate one traffic type from another. This is traffic classification, and without classification there can be no QoS. To differentiate traffic, it is possible to match on one traffic characteristic or multiple characteristics. If you need to differentiate between traffic from 10.1.1.1 and traffic from 10.1.1.2, for example, the source IP address is the only characteristic that you need to configure. If you have multiple traffic streams from 10.1.1.1 and need to differentiate between those, however, as well as differentiate between multiple streams from 10.1.1.2, you probably need to classify traffic based on multiple criteria, such as TCP or UDP port.

A possible scenario in which this would come into play might be server 10.1.1.1 that serves production HTTP and FTP to the Accounting department, and server 10.1.1.2 that serves nonproduction HTTP and FTP to the IT group that develops applications for the Accounting department. Understanding that production traffic is the top priority, the development group needs their traffic to have a minimum bandwidth guarantee to enable that group to properly test a new HTTP application before delivering it to the Accounting department for production use.
This means that there will be QoS requirements for all traffic from 10.1.1.1 and some traffic from 10.1.1.2. As such, just matching by IP address does not suffice. In this case, there is a requirement to match on multiple characteristics.

Example of Creating class-map

```
R1(config)# class-map ?
WORD class-map name
match-all Logical-AND all matching statements under this classmap match-any Logical-OR all matching
statements under this classmap
```

QUESTION 20
Which two different traffic types have the most similar sensitivity to latency, jitter, and packet loss? (Choose two.)

A. streaming video
B. video conferencing
C. peer-to-peer file sharing
D. voice
E. voice signaling
F. SQL transactions

Correct Answer: BD
Explanation

Explanation/Reference:
Explanation:

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 21
Which three characteristics best describe a converged network? (Choose three.)

A. the random dropping of lower priority traffic to ensure that high-priority traffic gets through
B. prioritization and congestion management to ensure voice quality
C. the potential for poor voice quality due to other traffic
D. the use of overprovisioning to ensure voice quality
E. the use of a separate high-speed link for bulk traffic to avoid interference with other traffic

F. the separation of the voice and data networks into two networks to ensure voice quality

Correct Answer: ABC
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
Which technology is required when configuring FRF.12 on a Cisco device?

A. WRED
B. FRF.8
C. VoFR
D. FRTS
E. FRF11.c
F. MLP with interleaving

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

Page 500, IP Telephony Self-Study Cisco DQOS Exam Certification Guide, http//www.ciscopress.com/title/1587200589

QUESTION 23
Mission-critical traffic is not getting a minimum bandwidth of 192 kbps in this policy-map configuration.
What should be done to correct the problem?

```
policy-map test
class mission-critical
bandwidth 192
shape average 128000
queue-limit 64
```

A. Change the bandwidth statement to the bandwidth 192000 command.
B. Increase the maximum queue size for the mission-critical traffic class using the queue-limit 128 command.
C. Use the shape peak command instead of the shape average command.
D. Decrease the maximum queue size for the mission-critical traffic class using the queue-limit 40 command.
E. Replace the bandwidth statement with the priority 192 command.
F. Set the shape rate to a CIR that is higher than 192 kbps.

Correct Answer: F
Explanation

Explanation/Reference:
Explanation:
Traffic shaping allows rate control of traffic leaving an interface in order to match its flow to the speed of the remote target interface and to ensure that the traffic conforms to policies defined for it. Therefore, traffic adhering to a particular profile can be shaped to meet downstream requirements, eliminating bottlenecks in topologies with data-rate mismatches. GTS can be configured to shape traffic for all traffic exiting an interface using the traffic-shape command:
Router(config-if)#traffic-shape rate bit-rate [burst-size [excess-burst-size]] Alternatively, traffic defined by an ACL can be shaped independently of other traffic exiting an interface using the command:
Router(config-if)#traffic-shape group access-list-number bit-rate [burst-size [excess-burst-size]]

QUESTION 24
According to the best practices, which statement is true as related to the QoS policy that should be implemented on the outbound provider (P) to provider (P) router link in a service provider network that is supporting both VoIP and data?

A. LLQ and CB-WRED should be implemented on the P router egress to support both VoIP and data traffic.
B. In the DiffServ model, ingress and egress QoS mechanisms are only required on the provider edge (PE) routers, so no QoS policy is needed on the P to P link.
C. CBWFQ and CB-WRED should be implemented on the P router egress to provide a maximum bandwidth guarantee for the VoIP traffic.
D. CBWFQ and CB-RTP header compression should be implemented on the P router egress to ensure minimum latency for VoIP traffic.

Correct Answer: A
Explanation

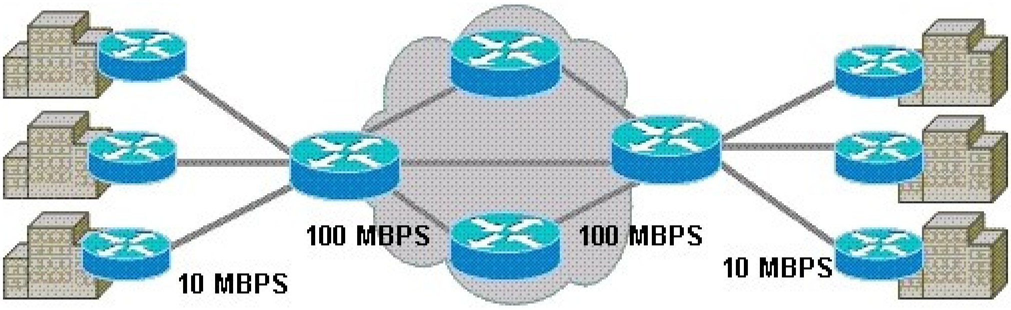
Explanation/Reference:
Explanation:

1. Weighted random early detection (WRED) is a queuing technique for congestion avoidance. WRED manages how packets are handled when an interface starts becoming congested. When traffic begins to exceed the interface traffic thresholds prior to any congestion, the interface starts dropping packets from selected flows. If the dropped packets are TCP, the TCP source recognizes that packets are getting dropped, and lowers its transmission rate. The lowered transmission rate then reduces the traffic to the interface, avoiding congestion. Because TCP retransmits dropped packets, no actual data loss occurs.
WRED drops packets according to the following criteria:
WRED can be combined with CBWFQ. In this combination CBWFQ provides a guaranteed percentage of the output bandwidth, WRED ensures that TCP traffic is not sent faster than CBWFQ can forward it. The abbreviated configuration below shows how WRED can be added to a policy-map specifying CBWFQ:
Router(config)#policy-map prioritybwRouter(config-pmap)#class class-default fair- queueRouter(config-pmap-c)#class prioritytraffic bandwidth percent 40 random-detect The random-detect parameter specifies that WRED will be used rather than the default tail-drop action.
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. 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 25
Refer to the exhibit. A service provider is considering several alternative provisioning schemes for a new network. One proposed scheme involves aggregating 10-Mbps links from customers into a network with

multiple 100-Mbps links to ensure that the network links have at least two times the capacity of the aggregate of the customer links.

What is the most appropriate description for the proposed scheme?



A. oversubscription
B. Bandwidth-on-Demand
C. CIR of 0
D. overprovisioning
E. overaggregate

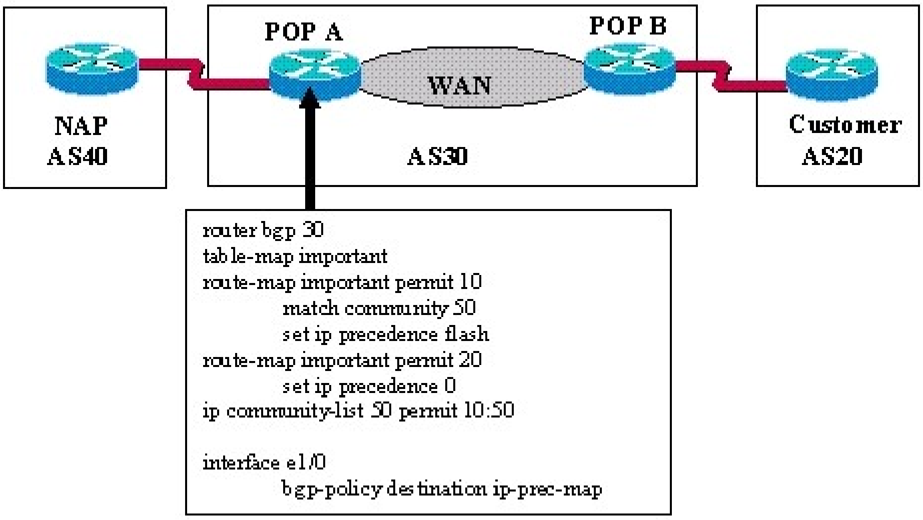
Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

Overprovisioning means ensuring quality of service by providing more than the aggregate bandwidth required.

QUESTION 26
Refer to the exhibit. QPPB is being used by the service provider (AS30). The table-map and route-map called "important" are implemented on router POP A. The command bgp-policy destination ip-prec- map is applied to the interface between POP A in AS30 and NAP (AS40).

Which QoS action would have to be applied on POP B in AS30 to ensure that the traffic from the NAP (AS40) to the customer (AS20) will be marked with an IP precedence of flash?



```
router bgp 30
table-map important
route-map important permit 10
          match community 50
          set ip precedence flash
route-map important permit 20
          set ip precedence 0
ip community-list 50 permit 10:50

interface e1/0
          bgp-policy destination ip-prec-map
```

A. No actions are needed. Traffic must be marked in AS20 by the customer as 10:50 before it arrives at the service provider.
B. Traffic from AS20 must be automatically marked via an inbound QoS map on POP B, resulting in the

community attribute set to 10:50.

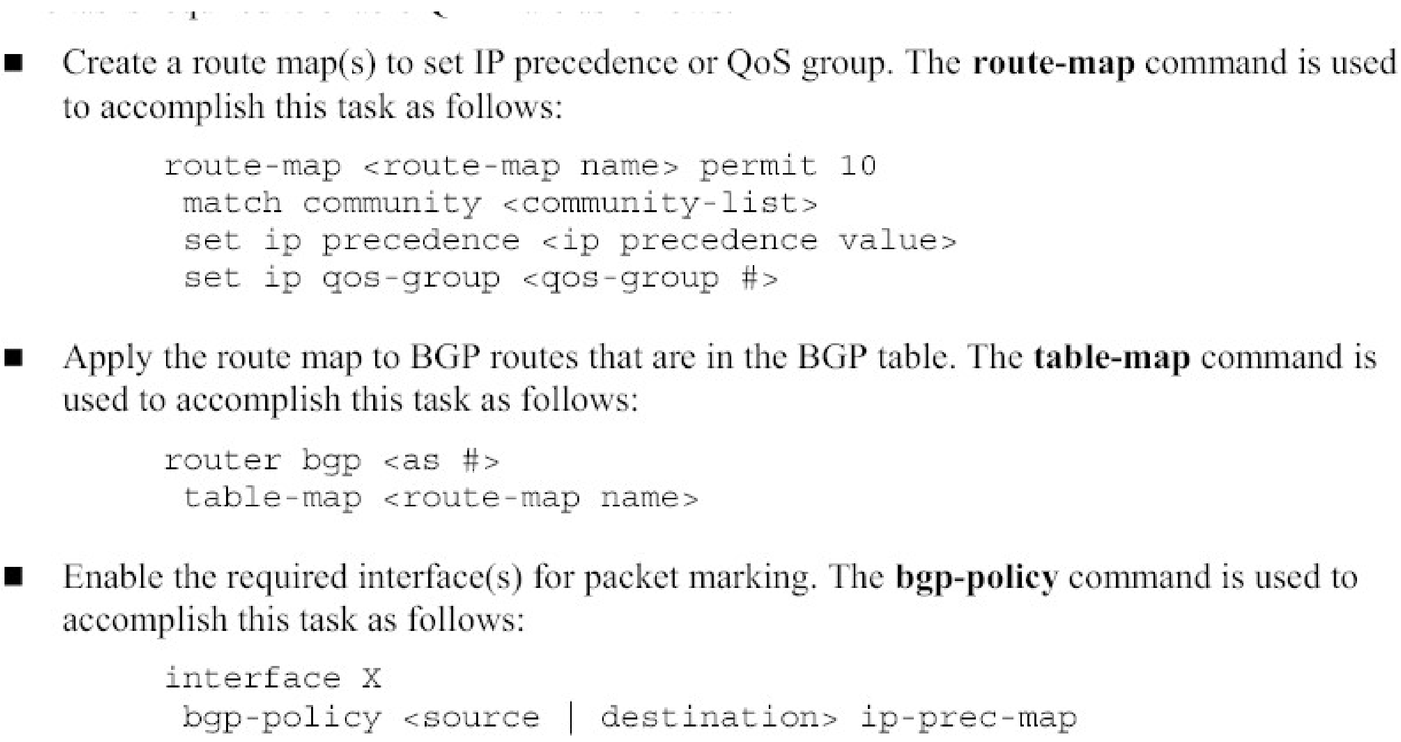
C. Traffic from AS20 must have the community attribute set to 10:50 in a route-map, and send- community must be specified.

D. Traffic from AS20 must have the extended community attribute set to 10:50 in a route-map, and send-community extended (or send-community both) must be specified.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:

BGP is an inter-domain routing protocol that exchanges reachability information with other BGP systems. The QoS policy propagation via the BGP feature allows classifying packets based on access lists, BGP community lists, and BGP AS paths.



- Create a route map(s) to set IP precedence or QoS group. The **route-map** command is used to accomplish this task as follows:

```
route-map <route-map name> permit 10
 match community <community-list>
 set ip precedence <ip precedence value>
 set ip qos-group <qos-group #>
```

- Apply the route map to BGP routes that are in the BGP table. The **table-map** command is used to accomplish this task as follows:

```
router bgp <as #>
 table-map <route-map name>
```

- Enable the required interface(s) for packet marking. The **bgp-policy** command is used to accomplish this task as follows:

```
interface X
 bgp-policy <source | destination> ip-prec-map
```

QUESTION 27
Which QoS mechanism adds IP Precedence information for prefixes into the FIB table?

A. Class-Based WRED
B. QoS pre-classify
C. AutoQoS
D. Class-Based Marking
E. LLQ
F. QPPB

Correct Answer: F
Explanation

Explanation/Reference:
Explanation:

The QoS Policy Propagation is Border Gateway Protocol (BGP) feature allows you to classify packets based on access lists, BGP community lists and BGP autonomous system (AS) paths. The supported classification policies include IP precedence setting and the ability to tag the packet with a QoS class identifier internal to the router. After a packet has been classified, you can use other QoS features such as CAR and WRED to specify and enforce business policies to fit your business model.

QUESTION 28
When LLQ is being configured, which IOS command is used to limit the traffic rate on the priority queue even when the other class queues are not congested?

A. hold-queue
B. bandwidth
C. priority
D. police
E. queue-limit

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

bandwidth-- Allows for the configuration of CBWFQ. The specifics of CBWFQ operation are beyond the scope of this explanation, but this command provides a minimum bandwidth guarantee to this class of traffic.
fair-queue-- Not available in all classes. This command enables Flow-based Weighted Fair Queuing within this class.
police-- Allows for the configuration of a policer, also known as rate limiting. The police command, when used within a class, is called class-based policing. priority-- Designates that this class is a Low Latency Queuing (LLQ) class, which should receive strict scheduling priority to minimize delay, jitter and packet loss. Also specifies the amount of bandwidth for this class.
queue-limit-- Designates the maximum number of packets that can be in this queue. random-detect-- Enables Weighted Random Early Detection (WRED) for congestion avoidance. By default, IP precedence is used for weight determination, but additional options within this command allow for the WRED algorithm to look at the DSCP. This command also provides an option for enabling explicit congestion notification (ECN) on this class. service-policy-- Allows for the configuration of hierarchical policies (policy within a policy), which may be used to achieve functionality not possible in a single policy. For example, a T1 can be shaped to 512 kbps via a top-level policy, and then that 512 kbps can be divided (using CBWFQ/LLQ) within a second-level policy. Top-level policies are

QUESTION 29
Based on the following 2950 switch configurations, which statement is correct?

```
no wrr-queue cos-map
wrr-queue bandwidth 20 10 70 1
wrr-queue cos-map 4 5
wrr-queue cos-map 1 0 1 2 3
wrr-queue cos-map 3 6 7
```

A. Queue 4 is setup as the expedite queue.
B. Queue 1 is setup as the expedite queue.
C. No queue is setup as the expedite queue.
D. Queue 3 is setup as the expedite queue.
E. Queue 2 is setup as the expedite queue.

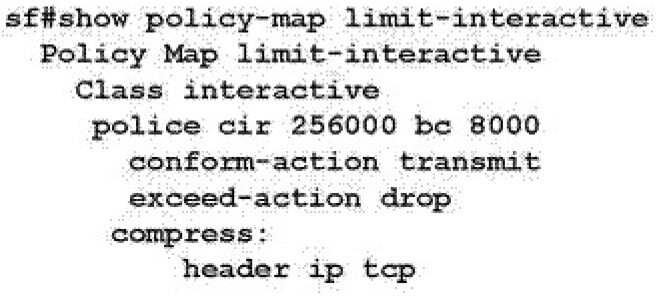
Correct Answer: C
Explanation

Explanation/Reference:
Explanation:

To allocate bandwidth between standard transmit queue 1 (low priority) and standard transmit queue 2 (high priority), use the wrr-queue bandwidth command. Use the no form of this command to return to the default settings.
wrr-queue bandwidth weight-1 weight-2 [weight-3]
no wrr-queue bandwidth

QUESTION 30
Refer to the exhibit. Why would applying the limit-interactive policy-map to the fa0/0 interface as shown below cause an error?

interface fa0/0
service-policy input limit-interactive



```
sf#show policy-map limit-interactive
  Policy Map limit-interactive
    Class interactive
     police cir 256000 bc 8000
       conform-action transmit
       exceed-action drop
      compress:
          header ip tcp
```

A. Class-based policing can only be applied in the output direction.
B. There is already an output service-policy defined on the fa0/0 interface.
C. The interactive class-map has not been configured.
D. The interactive traffic class is missing the bandwidth {kbps} command.
E. TCP header compression can only be applied in the output direction.

Correct Answer: E
Explanation

Explanation/Reference:
Explanation:

cRTP is a hop-by-hop compression scheme. cRTP must be configured on both ends of the link, unless the passive option is configured. To configure cRTP, use the following command at interface level:
Router(config-if)#ip rtp header-compression [passive]
Note: When the command ip rtp header-compression is used, the router adds the command ip tcp header-compression to the configuration by default. This is used to compress the headers of TCP/IP packets. Header compression is particularly useful on networks with a large percentage of small packets, such as those supporting many Telnet connections. The TCP header compression technique is supported on serial lines using HDLC or PPP encapsulation. To compress the TCP headers without enabling cRTP, use the command:
Router(config-if)#ip tcp header-compression [passive]
cRTP is not required to ensure good voice quality. It is a feature that reduces bandwidth consumption. Configure cRTP after all other conditions are met and the voice quality is good. This procedure can save troubleshooting time by isolating potential cRTP issues.

QUESTION 31
The qos pre-classify command can be configured under which two configuration modes? (Choose two.)

A. router(config-cmap)#
B. router(config-pmap-c)#
C. router(config-if)#
D. router(config)#

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

One Year Free Update

Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee

To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.